Symantec™ Data Center Security: Server Advanced 6.5 Detection Policy Guide

Documentation version: 1.0

Legal Notice

Copyright © 2015 Symantec Corporation. All rights reserved.

Symantec, the Symantec Logo, the Checkmark Logo and 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, et seq. "Commercial Computer Software and Commercial Computer Software Documentation," as applicable, and any successor regulations, whether delivered by Symantec as on premises or hosted services. 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.
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 website 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, DVDs, 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_apj@symantec.com
Europe, Middle-East, and Africa  seMEA@Symantec.com
North America and Latin America  supportsolutions@symantec.com
Contents

Technical Support ........................................................................................................... 4

Chapter 1 Detection Policy Overview ................................................................. 11
  About the detection policies ..................................................................................... 11
  About rulesets and rules ....................................................................................... 12
  About policy options ............................................................................................. 14
  About monitored files ............................................................................................. 14
  About date and time restrictions .......................................................................... 15
  Using the management console to learn more about policy options ................. 15
  Viewing the policy option settings ....................................................................... 16

Chapter 2 Windows Detection Policy Reference .............................................. 17
  About the Windows detection policies .................................................................. 17
  List of policies ......................................................................................................... 18
    Agent_Diagnostics .............................................................................................. 18
    Agent_Status ....................................................................................................... 20
    Server_Monitor .................................................................................................. 21
    Global_Watch_Policy ......................................................................................... 21
    Windows_Template_Policy ................................................................................. 24
    Kill_Prevention_PSET ....................................................................................... 25
    Creating custom rules ......................................................................................... 26
  Host Intrusion detection policies enhancements ................................................. 39

Chapter 3 UNIX Detection Policy Reference ..................................................... 43
  About the UNIX detection policies ....................................................................... 43
  List of policies ........................................................................................................ 44
    UNIX_SDCSS_Agent_Diagnostics ................................................................. 44
    UNIX_SDCSS_Agent_Status ............................................................................. 45
    UNIX_Template_Policy .................................................................................... 45

Chapter 4 Policy Examples .................................................................................... 48
  About policy examples .......................................................................................... 48
  Forcing rollover of the agent event log file ......................................................... 48
# Chapter 7 UNIX Baseline Detection Policy

- Introduction ............................................................................... 173
- File monitoring improvements .................................................. 176
- Advanced per-rule tuning improvements .................................... 177
- Console changes ........................................................................ 177
- Unicode Log Monitoring for UNIX ............................................. 178
- How wildcard characters and recursion levels work in IDS file monitoring ........................................................... 178

# Chapter 8 UNIX Policy Options

- System User and Group Change Monitor ........................................ 180
  - Global User and Group Change Monitor Settings ...................... 180
  - System User Configuration Changes ........................................ 181
  - System Group Configuration Changes .................................... 187
  - Privileged User and Group Configuration Activity .................... 189
- System Login Activity and Access Monitor .................................... 191
  - System Login Success Monitor ............................................. 191
  - System Logoff Monitor ..................................................... 196
  - System Failed Login Monitor .............................................. 199
- System Privileged Command and Bash History Monitor .................. 209
  - Sudo Monitoring Options .................................................. 210
  - User Command History Options ......................................... 212
  - Superuser (Root Level) Command History Options ................ 213
- System Hardening Monitor ........................................................... 214
- System File and Directory Monitor ............................................ 215
  - System FileWatch Monitor ................................................ 216
- System Symantec Software Monitor ........................................... 229
- System External Device Activity Monitor .................................... 233
- System Attack Detection .............................................................. 234
  - Generic Web Attack Detection Options .................................. 235
  - UNIX Rootkit File / Directory Detection ................................. 239
  - UNIX WormFile / Directory Detection .................................... 260
  - Malicious Module Detection ................................................ 263
  - Suspicious Permission Change Detection ................................. 264

# Appendix A Parameter Reference Syntax

- Parameter reference syntax overview ............................................. 266
- Simple policy parameter ............................................................. 267
- Compound policy parameter ....................................................... 268
  - Process list ........................................................................... 269
  - Process list without arguments .............................................. 269
Appendix B  Translator Function Reference ........................................ 273

Generic functions ........................................................................ 273
%?LocalIPs()% ................................................................. 273
%?LocalIPAddresses()% ..................................................... 274
%?AgentParams(<param name>)% ........................................ 274
%?SplitPath(<path>)% ......................................................... 274
%?ImportFileList(<filepath>)% ............................................... 274
Detection Policy Overview

This chapter includes the following topics:

- About the detection policies
- About rulesets and rules
- About policy options
- About monitored files
- About date and time restrictions
- Using the management console to learn more about policy options
- Viewing the policy option settings

About the detection policies

Symantec™ Data Center Security: Server Advanced includes detection policies for computers that run the following operating systems:

- Microsoft® Windows®
- IBM® AIX®
- Sun™ Solaris™
- Red Hat® Enterprise Linux
- SUSE® Linux Enterprise
- Hewlett-Packard® HP-UX®
- Ubuntu

A detection policy is a collection of rules that are configured to detect specific events and take action. Detection policies define which system events or user-defined
criteria are selected, which criteria are ignored, and what actions are performed after select and ignore criteria are met.

The Symantec Data Center Security: Server Advanced detection policies monitor events and syslogs, and report anomalous behavior. Features include sophisticated policy-based auditing and monitoring; log consolidation for easy search, archival, and retrieval; advanced event analysis and response capabilities; and file and registry protection and monitoring.

About rulesets and rules

Every Symantec Data Center Security: Server Advanced detection policy contains exactly one ruleset, and each ruleset contains one or more rules. Each rule is grouped by type.

The rule types are as follows:

- NT event log
- Filewatch
- Prevention watch
- Text log
- Generic
- C2 log
- Syslog
- UNIX activity log

Rule types are associated with collectors that gather data from a host system. The collectors format data from events, system logs, application logs, file systems, the Windows registry, and other sources. The collectors compare events with rules to determine matches.

The detection policies use the following collectors:

<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Text log</td>
<td>Looks for matches in user-specified text logs. You can specify the path to a log file, and a text pattern that determines how data from the log file is parsed and recorded.</td>
</tr>
</tbody>
</table>
Registry

Watches changes to user-specified registry keys. You can watch changes to key/value, operations (created, modified, deleted), operation results (success, failure, either), and process.

The key/value string supports wildcard characters. Multiple key/value strings are allowed in a rule. The filtered keys appear in the Registry.ini file on the agent computer.

You can watch all operations or none (meaning any activity). You can filter the result of the operation. The process can be specified only once in the rule.

File

Determine how agents monitor files. Intruders often attempt to replace critical system files with Trojan horse versions, or alter system files to create a back door for future intrusions. The file collector detects changes to these system critical files.

The file collector is associated with the filewatch rule type, which logs activity to files and directories. You can specify the file/directory to watch, the file operation, and the protection settings.

Syslog

Watches for syslog daemon tampering on UNIX operating systems. The syslog daemon must run for the syslog collector to work. Normally, syslog runs at all times on a secured UNIX system. Upon initialization, the syslog collector checks that syslogd is running and starts it if it is not running.

Subsequently, if syslogd is killed while an agent is running, an error event is generated and matched against a suitable Syslogd Tampering policy. No attempts are made to restart syslogd.

The syslog collector monitors and parses the following pipe:

/var/log/ids_syslog.pipe

This pipe is specified in /etc/syslog.conf.

C2 log

Looks for matches in the C2 audit logs on agent computers that run Solaris, HP-UX, and AIX operating systems.
WTMP  
Looks for matches in the WTMP file on UNIX operating systems (and BTMP file on some operating systems). This file collects user authentication and account information. You can specify text patterns to parse.

The WTMP file captures successful login events. The WTMP file that is watched varies, depending on the operating system. All UNIX operating systems at one point used the WTMP format, but many now use the newer WTMPX format. On some systems, this filename may be WTMP, WTMPX, or WTMPS, even though the format internally is WTMPX.

BTMP/BTMPS (HP-UX only) is read to capture failed login attempts. If the WTMP or BTMP file does not exist when the agent is started, an error is reported, and events are not captured. If the file is created while the agent is running, the agent captures the events without a restart. Also, on HP-UX, the collector watches WTMP, WTMPS, BTMP, and BTMPS for events.

Generic  
Looks for matches from all collectors, as well as internal agent status and error messages including Symantec Data Center Security: Server Advanced agents. The status and error messages are specified in status and error rule types.

Error  
Looks for matches in Symantec Data Center Security: Server Advanced agent error messages. You can specify text patterns to parse.

Status  
The status collector looks for matches in Symantec Data Center Security: Server Advanced agent status messages. You can specify text patterns to parse.

About policy options  
You use policy options to configure a detection policy for assignment to a target computer. Policy options comprise a simplified set of controls that you can use to enable or disable features in a policy. Some options have associated parameters, which let you customize the behavior of an option.

About monitored files  
Detection policies monitor files that are listed under the File Monitor Groups and File Path Groups policy options.

For example, the Windows Baseline Detection policy for Windows contains the following under Monitor System-Critical Files:

- Monitor System-Critical Files
To view the Monitor System-Critical Files in the Windows Baseline Detection policy

1. In the management console, click Policies.
2. Under the Policies tab, click Detection.
3. On the Policies page, in the Workspace tree, click the Symantec folder.
5. In the Policy Editor dialog box, select System File and Directory Monitor.

About date and time restrictions

Many of the Symantec Data Center Security: Server Advanced detection policies include rules for date restrictions. You use date restrictions to select or ignore events that occur within a specified time frame. Date restrictions are active when a rule is enabled, and inactive when a rule is disabled.

When enabling a date restriction rule, you must specify the following:

- Start of time interval
- Duration of time interval
- Frequency of time interval

Using the management console to learn more about policy options

To learn more about a policy option, use the Symantec Data Center Security: Server Advanced management console in conjunction with this manual.

To use the management console to learn more about policy options

1. In the management console, on the Policies page, click Detection, and then edit a policy.
2. In the Policy Editor dialog box, select any options to know more about the policy options.

See the Symantec Data Center Security: Server Advanced Administrator’s Guide for instructions on how to use the management console.
Viewing the policy option settings

You use the management console to view a summary of the policy option settings for the detection policies.

To view the policy option settings

1. In the management console, click **Policies**.
2. Under the **Policies** tab, click **Detection**.
3. On the Policies page, click the **Symantec** folder.
4. In the workspace pane, double-click a Symantec Data Center Security: Server Advanced detection policy.
5. In the policy dialog box, under **Policy Changes and Summary**, click **Summary**.

A summary of the policy options is shown in tree form. The tree includes only those options that are enabled (shown in bold text) and the parameters that have values.

---

**Note:** The Windows Baseline Detection policy does not support the SymIDS ISAPI filter anymore. Older detection policies required the SymIDS ISAPI filter to be installed and they monitored the filter’s log file. The new Windows Baseline Detection policy monitors IIS log files directly and it does not require the SymIDS ISAPI filter to provide additional information.
Windows Detection Policy Reference

This chapter includes the following topics:

- About the Windows detection policies
- List of policies
- Host Intrusion detection policies enhancements

About the Windows detection policies

Symantec Data Center Security: Server Advanced includes detection policies for computers that run supported Windows operating system. Some policies require that you enable Windows features; these features may also require a configuration change. In this manual, when an enabled Windows feature is required, the policy description identifies the feature that you must enable.

For example, the System_User_Configuration policy detects changes made to user accounts. To enable this policy, you must enable the Windows Security Policy auditing system for user account management actions at the following location:

Settings > Control Panel > Administrative Tools > Local Security Policy > Security Settings > Local Policies > Audit Policy > Audit account management

In this manual, features that you must enable are marked with the word Configuration. The policy descriptions also indicate if other types of configuration changes are needed.
List of policies

This section describes the Symantec Data Center Security: Server Advanced Windows detection policies.

Agent_Diagnostics

This Windows detection policy includes options for the following:

- Run the collect info script
- Restart the IDS service
- Restart the IPS service
- Restart the UTIL service
- Force log rollover of the agent event log file
- Modify the management server list for an agent
- Edit agent configuration files

By default, all the options in the policy are disabled. You must enable an option for the policy to work. The policy performs the enabled option immediately after being applied to the agent. After confirming that the policy performed the enabled option, you must clear the policy from the agent.

See "Enabling an option in the policy" on page 20.

The policy options are as follows:
Perform the following diagnostic functions on an agent computer:

- Take no action
- Run the collect info script
- Restart the IDS Service
- Restart the IPS Service
- Restart the UTIL Service
- Force log rollover

You use the options to run diagnostic functions to troubleshoot problems with Symantec Data Center Security: Server Advanced. Generally, you will not enable these options unless instructed by Symantec Support.

Default: Take no action

The collect info script collects information about an agent. The agent automatically uploads the collect info output file to the management server. Log on to the management server to get the output file from the server directory:

C:\Program Files\Symantec\Data Center Security\Server\Server\logfiles\<hostname>\<date>\n
The options to restart the IDS, IPS, and UTIL services restarts these services on the agent computer.

Forcing rollover (rotation) of the current agent event log file closes the current log file and opens a new log file.

See the Symantec Data Center Security: Server Advanced Administrator's Guide for information on collect info and log file rotation.

Updates the management server list for an agent. The management server list is used in conjunction with simple failover. You can use this option to change the primary and alternate servers in the list (for example, if an alternate server is unavailable).

See the Symantec Data Center Security: Server Advanced Administrator's Guide for information on simple failover.

Enable the option, and then specify the servers in a comma-separated list. You must specify the primary management server as the first server, followed by any optional alternate servers. Specify the IP address or fully qualified host name of each server in the list. All the servers in the list must use the same server certificate and agent port.

You use this option to edit agent configuration files.

**Note:** Do not enable this option unless instructed by Symantec Support.
Enabling an option in the policy

The following instructions enable an option in the SDCSS_Agent_Diagnostics policy, apply the policy to an agent, and clear the policy from the agent.

Note: Instead of applying the SDCSS_Agent_Diagnostics policy directly to an agent, you can create a group and then apply the policy to the group. When you need to perform an enabled option in the policy, simply add the agent to the group. You must delete the agent from the group after the policy has performed the enabled option.

To enable an option in the policy

1. Log on to the management console as an administrator.
2. In the management console, on the Policies page, in the Symantec folder, edit the SDCSS_Agent_Diagnostics policy.
3. In the policy editor dialog box, under Policy Settings, click Diagnostic functions.
4. In the policy editor dialog box, check Select a function to run on the agent and click Edit.
5. In the Value list, select the option for a desired function.
   For example, to run the collect info script, select Run the collect info script to enable the option.
6. Click OK.
7. Apply the policy to the agent.
   The policy performs the enabled option immediately after being applied to the agent.
8. In the management console, on the Monitors tab, under Events, monitor the events to determine if the enabled option was performed.
   For example, to determine if the collect info output file was uploaded to the management server, look for management events of type Agent Status. The event message contains the name of the collect info output file.
9. In the management console, on the Assets page, select the agent, and then right-click Clear Policy to clear the policy from the agent.

Agent_Status

This Windows detection policy detects changes to the Symantec Data Center Security: Server Advanced registry keys. The policy also detects if the
SymIDSFilter.ddl, which monitors Microsoft Internet Information Services (IIS) activity, fails to load.

The policy options are as follows:

SDCSS Registry Settings Modified
Detects changes to the Symantec Data Center Security: Server Advanced registry keys.

SymIDSFilter Load Failed
Detects if the SymIDSFilter.ddl, which monitors IIS activity, fails to load.

Server_Monitor

This Windows detection policy watches the DCS:SA Server Tomcat logs and, if the built-in SQL Server 2005 Express database is used, the SQL Server 2005 Express DB logs. The policy sends error messages to the management console when a listed error occurs.

The policy options are as follows:

Failure to send email alert
Detects that an error occurred while sending an alert email.

Evaluation database is full
Detects that an SQL Server 2005 Express database instance used by an evaluation installation of DCS:SA is full.

Server startup
Detects that management server servlets started.

Server shutdown
Detects that management server servlets stopped.

Database cleanup started
Detects that period database cleanup activities started.

Global_Watch_Policy

This Windows detection policy monitors alert text files. An alert text file is a user-specified text file that contains alert-captured events.

Administrators create alerts in the management console. Administrators use alerts to send email messages and SNMP traps when Symantec Data Center Security: Server Advanced observes specific events.

When creating an alert, administrators can set up an alert text file to save events of interest. The alert text file can contain text strings and event fields. The file is
created when the alert captures an event; subsequent records are appended to the file.

You can use the policy to analyze alert-captured events. The policy includes rule options to define which records in the alert text file are selected and ignored, and how to extract event data.

The policy includes rule options to aggregate events, which can potentially originate from multiple agents. Events are aggregated based on event count, time interval, and optional field value.

When an event in an alert text file matches the criteria specified in the policy, the policy sends the event to the management console.

To use this policy effectively, you must understand how the alert text file is constructed, including the following:

- Name and path of the alert text file
- Record content
- Record format (fields and field order)

See the Symantec Data Center Security: Server Advanced Administration Guide for information on alerts and alert files.

Alert text files reside on the Symantec Data Center Security: Server Advanced management server computer. The default alerts directory is as follows:

C:\Program Files\Symantec\Data Center Security Server\Server\alerts\n
You apply the Global_Watch_Policy to the Symantec Data Center Security: Server Advanced management server computer.

The policy rules are as follows:
File description

Specify the alert text file to monitor.

The rule options are as follows:

- **File path**
  Specify the complete file path of the alert text file. Wildcard characters are not permitted in the file path. Use the percent sign (%) to delimit variables.

- **Parse definitions**
  Select this check box to define the parse definitions in the alert text file, and then specify the parse pattern.
  Parse definitions define how to extract fields from the alert text file and assign the fields to variables. You format variables as `{variable}`.
  Example: `*user_name={user name},*`
  This parse definition extracts user_name from the alert text file and assigns it to the variable `{user_name}`.
  Parse strings support wildcard characters. Type an asterisk (*) as the wildcard character for zero or more characters.

Event counting

Select this check box to aggregate events.

The rule options are as follows:

- **Number of occurrences during time interval**
- **Time interval**

The policy records an event when the event count equals the specified number of occurrences, during the specified time interval.

See also Grouped counting.
Event counting: Grouped counting

Select this check box to count events in groups.

Events are grouped based on a field value. For example, suppose the alert text file contains events from multiple agents, and each record contains agent name. You can select the Grouped counting check box to group event counting based on agent name.

When using grouped counting, use parse definitions to define the fields to extract from the alert text file.

The rule options are as follows:

- Count repetition of the same field value
  Select this check box to have the policy record an event based on the number of repetitions of the same field value, during the specified time interval.
  Example: You specify that the policy record an event if three records during a one-minute interval contain the same agent name.

- Count number of different field values
  Select this check box to have the policy record an event based on the number of different field values, during the specified time interval.
  Example: You specify that the policy record an event if three records during a one-minute interval contain different agent names.

Matching criteria

Select this check box to define which records in the alert text file the policy should select and ignore. The policy selects and ignores records based on text patterns.

The rule options are as follows:

- Patterns to match on
  Specify a list of text patterns to match. The policy selects a record if it contains a specified pattern.

- Patterns to ignore
  Select this check box to have the policy ignore records that contain a specified text pattern. Specify the list of patterns to ignore.

Windows_Template_Policy

The Windows_Template_Policy is a reusable workspace container policy that creates custom rules.

The policy includes rule options for the following rule types:

- NT event log
- Filewatch
- Registry watch
- Prevention watch
Each rule that you create in the policy is controlled by rule options that are enabled or disabled in the management console. You can customize the rule options by editing the rule parameters.

Management console functions are available to help you maintain custom rules. You can modify a custom rule name, description, and options. A special copy command lets you reuse custom rules across multiple policies; you can copy the options for a custom rule that is defined in the template policy to another workspace policy, without re-keying the options.

When importing and exporting workspace policies, the options to control custom rules are also imported and exported. When updating workspace policies, the options to control custom rules are also updated.

The template policy is intended for use as a container policy for managing custom rules. The policy contains only the rules that you define.

When creating a custom rule, you specify general rule options and rule-specific options.

See “About registry watch rules” on page 35.
See “About prevention watch rules” on page 36.
See “About text log rules” on page 37.
See “About generic rules” on page 39.

**Kill_Prevention_PSET**

This Windows detection policy attempts to kill any process that acts as an injectee or an injector. The Kill_Prevention_PSET policy is used in combination with the prevention policies. When Kill_Prevention_PSET policy is applied to an agent, all processes routed to thread_injectee_nopriv_ps or thread_injector_nopriv_ps are killed by using the taskkill.exe application.

*Note:* The processes are routed to thread_injectee_nopriv_ps or thread_injector_nopriv_ps PSETs only when you apply the IPS policy and configure the policy to detect thread injection. By default, the thread injection is enabled in the core, strict, and limited execution prevention policies.
Following are the Kill_Prevention_PSET policy options:

- **Kill all thread injectee processes**
  The prevention policy applies this option only when it finds that the unauthorized code is injected into a specific process.

- **Kill all thread injector processes**
  The prevention policy applies this option only when it finds that the process has injected the code into another process against the policy restrictions.

- **Kill New Processes in a Specific PSET**
  It kills any process that is routed to it.
  To enable this option, check Show advanced options.

**Creating custom rules**

You can create as many custom rules as you need. You can create multiple rules of different types and multiple rules of the same type. You can create the rules in the original template policy or in a template copy.

Verify the rule order. Detection rules are ordered top to bottom. Changing the rule order changes the meaning of the rules.

As an example, the following instructions create a text log rule.

**To create custom rules**

1. In the management console, click **Policies**.
2. Under the **Policies** tab, click **Detection**.
3. On the policies page, double-click **Windows_Template_Policy**.
4. In the policy editor dialog box, under **Policy Settings**, click **My Custom Rules**, and then click **Add a new Custom Control** icon.
5 In the **New Custom Rule Wizard** dialog box, specify the following information.

**Display Name**
- Type a descriptive name for the custom rule.
- This text appears in the policy editor, under My Custom Rules.
- In the text log rule example, type Text Log Rule.

**Category**
- Select a rule type.
- In the text log rule example, select Text Log.

**Identifier**
- Type a name that the policy uses internally to identify the custom rule. The name must not include spaces or special characters.
- In the text log rule example, type textlog.

**Description**
- Type a full description of the custom rule.

6 Click **Finish**.

7 In the policy editor dialog box, click **Edit** to view the policy options.

8 In the policy editor dialog box, check **Text log rule options** and then click **Edit**.

9 In the policy editor dialog box, enable or disable the rule options, and modify the rule parameters as needed.

10 If the rules need reordering, select a rule, and then click **Move Up** or **Move Down**; repeat as needed.

11 Click **OK**.

**Reusing custom rules**

You can copy a custom rule that is defined in the template policy to another workspace policy. The options that control the custom rule are copied to the workspace policy.

You can copy a rule using the following methods:

- On the Policies page, select the template policy, and then right-click Copy Custom Controls.

- Edit the template policy, select one or more custom rules, and then click Copy To Other Policy.

If the custom rule being copied does not exist in the target policy, the rule is added to the target policy. If the custom rule being copied already exists in the target policy, the rule is updated in the target policy.

The Copy Policy Options Wizard prompts you to select one of the following merge options:
Take the new option settings

Ignores the target policy and uses the option settings in the template policy.

Default

If the custom rule does not exist in the target policy, you will select this option.

Merge the changed options

Merges the option settings in the target policy with the option settings in the template policy.

**Note:** Only the options for the selected custom rules are merged.

After copying a custom rule to a workspace policy, you should verify the rule options. Verify that the custom rule appears in the policy; click Settings to view the options. Verify that the custom rule is enabled in the policy.

To reuse custom rules

1. In the management console, click **Policies**.
2. Under the **Policies** tab, click **Detection**.
3. On the policies page, select **Windows_Template_Policy**, and then right-click **Copy Custom Controls**.
4. In the **Copy Policy Options Wizard** dialog box, select a custom rule, and then click **Next**.

   To select multiple custom rules, press and hold the Shift or Ctrl key while selecting the rules.

5. In the **Copy Policy Options Wizard** dialog box, select one or more target policies to receive the selected custom rules, and then click **Next**.

   To select multiple target policies, press and hold the Shift or Ctrl key while selecting the policies.

6. In the **Copy Policy Options Wizard** dialog box, select the merge option, and then click **Finish**.

**About general rule options**

The following rule options apply to all rule types:
Rule name

In the Value box, type the rule name. This value appears in the management console. Required.

In the Rule Name box, type a name to associate internally with the rule. Rules names are carried throughout the system and are recorded in each event that is generated by the policy. Rule names help provide insight into why an event was recorded. Optional.

In the Comment box, type notes or comments about the rule. Optional.

Rule severity

Select the severity number from the following range of rule severity numbers:

- Info: Events with a severity of 0-19 contain information about normal system operation.
- Notice: Events with a severity of 20-39 contain information about normal system operation.
- Warning: Events with a severity of 40-59 indicate unexpected activity or problems that have already been handled by Symantec Data Center Security: Server Advanced.
- Major: Events with a severity of 60-79 imply more impact than Warning and less impact than Critical.
- Critical: Events with a severity of 80-99 indicate activity or problems that might require administrator intervention to correct.

Matching event patterns

Specify additional patterns to match in an event.

If specifying multiple patterns, any matching pattern triggers the rule.

Select the check box to enable the option, and then specify the event patterns to match.

To ignore events containing specific patterns, select the ignore check box, and then specify the event patterns to ignore.

When specifying a text pattern, you can use the following wildcard characters:

- Use a question mark (?) to match a single character, including the question mark itself. Examples: ab?c matches abcxc or ab?c, but not abc.
- Use an asterisk (*) to match zero or more characters, including asterisks embedded in a text pattern. Examples: *abc matches a*b*cabc, where the initial asterisk is equivalent to a*b*c.
- Use a backward slash (\) as an escape character. Use two backward slashes (\) for a backward slash embedded in a text pattern.
- Use a percent sign (%) to delimit variables, including environment variables. Use one backward slash and one percent sign (\%) for a percent sign embedded in a text pattern.
<table>
<thead>
<tr>
<th>Record event to DCS:SA console</th>
<th>Select this check box to send the event to the management console when activity matches the conditions. This rule option creates a record in the event log (.CSV) file.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Execute command</td>
<td>Specify a command-line string, including path and arguments, to execute when the rule to execute the specified command is triggered. For an agent to properly execute a command, you should create the commands.txt file on the agent computer, in the \IDS\System directory. List each command-line string, including path and arguments, on a separate line in the commands.txt file. The commands.txt file must not require user interaction at a command line or with a graphical user interface.</td>
</tr>
<tr>
<td>Date and time restrictions</td>
<td>Add date restrictions that specify a time interval when a rule is active or inactive. Date restrictions are active when the rule is enabled, inactive when the rule is disabled. Select the check box to enable the option. Specify whether to select or ignore events during the time interval. Specify the start, duration, and frequency of the time interval.</td>
</tr>
<tr>
<td>Files to monitor</td>
<td>Specify the full path and name of the file to be monitored. You can specify multiple files. If the path refers to a directory, then only the changes to the directory are monitored. Click the Add button, and then in the Value box, type the path and name of the file. Repeat to specify another file. Unless otherwise stated, you can use wildcard characters in path and file name specifications. To monitor all files and subdirectories (up to two subdirectory levels), type an asterisk (*) for the file name.</td>
</tr>
</tbody>
</table>

### About NT event log rules

This rule type monitors user-specified events in the Windows event log.

The NT event log rule type is associated with the NT event log collector. The NT event log collector looks for matches in Windows event log files. These event log files are the Microsoft standard format .evt files. In standard installations, three event log files exist: Security, System, and Application.

The rule is created with the following rule options:

<table>
<thead>
<tr>
<th>NT event log rule options</th>
<th>Select this check box to enable the rule.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Rule name</td>
<td></td>
</tr>
<tr>
<td>Rule severity</td>
<td></td>
</tr>
<tr>
<td>Windows event ID to monitor</td>
<td>Type a comma-separated list of Windows event IDs to monitor. You can specify event IDs as the following:</td>
</tr>
<tr>
<td>■ Unsigned integer (for example, 529)</td>
<td></td>
</tr>
<tr>
<td>■ Variable (for example, %EventID%)</td>
<td></td>
</tr>
<tr>
<td>■ Comma-separated list of unsigned integers (for example, 617,618,619)</td>
<td></td>
</tr>
<tr>
<td>Windows event log file name</td>
<td>Type the name of the Windows event log to monitor (System, Security, or Application).</td>
</tr>
<tr>
<td>Record event to SDCSS console</td>
<td></td>
</tr>
<tr>
<td>Execute command</td>
<td></td>
</tr>
<tr>
<td>Event patterns</td>
<td></td>
</tr>
<tr>
<td>Date and time restrictions</td>
<td></td>
</tr>
</tbody>
</table>

### About filewatch rules

This rule type monitors changes to user-specified files, and ignores changes to user-specified files. These changes comprise creating, deleting, modifying, and accessing user-specified files. You can enable or disable monitoring or ignoring specific files, and you can adjust the list of files that are monitored or ignored.

The filewatch rule type is associated with the file collector, which determines how agents monitor files. Intruders often attempt to replace critical system files with Trojan horse versions, or alter system files to create a back door for future intrusions. The file collector detects changes to these system critical files. Also, the FileWatch collector monitors all NTFS alternative data streams that are associated with a file name for creations, deletion, and changes. Symantec Data Center Security: Server Advanced does not support automatic file comparison of alternate data streams. You can compare individual data streams by specifying the absolute path for alternate data streams in a policy. Use `file_path:stream_name` to specify the absolute path.

The Windows filewatch implementation monitors files and directories on removable media. Filewatch generates a single Mount or Unmount event for each monitored path whenever a watched file or directory appears or disappears because of a mount, dismount, insertion or removal. Filewatch monitors removable media such as floppy drives, CD/DVD drives, USB drives, and firewire drives. The state of a removable drive is maintained across IDS Service restarts. (If a removable drive is
being monitored when the IDS Service is stopped, and the drive is removed before the service is restarted, filewatch recognizes that the drive was removed and avoids generating File Deleted events for the contents of the drive.) The Mount and Unmount events are generated directly into the CSV event log and do not have to match a policy rule. If you are not interested in these events, you can filter the events using log rules or real-time monitor filters.

The filewatch rule is created with the following rule options:

- **filewatch rule options**: Select this check box to enable the rule.
- **Rule name**: .
- **Rule severity**: .
- **Polling interval**: The frequency at which files are polled for changes. All files listed in a filewatch rule are monitored based on the polling interval. A low polling interval value might impact system performance. For high-priority files, polling interval is typically set to 60 seconds.
- **Search depth**: The number of directory levels to monitor for file differences. Select a value (1-10) from the list or type a value. File differences include file creation, deletion, modification, and access.
- **Monitor file creation**: Select this check box to monitor user-specified files for creation.
- **Monitor file deletion**: Select this check box to monitor user-specified files for deletion.
- **Monitor file modification**: Select this check box to monitor user-specified files for modification.

Additionally, you can enable or disable the following options:

- Use file checksum to check if files are modified
  Select this check box to compare the current contents of a file with the previous version's contents. A file's checksum is calculated at agent startup to determine whether the file was modified since Symantec Data Center Security: Server Advanced was last shut down.

- Report file differences
  Select this check box to report the file differences in the event, and then select the differences algorithm (TXT for generic text files or INI for Windows .ini configuration files).

- **Monitor file access**: Select this check box to monitor user-specified files for file access.

- **Additional patterns to match**: .
Files to watch
Select this check box to monitor specific files, and then list the files to monitor.

Files to ignore
Select this check box to ignore specific files, and then list the files to ignore.

Record event to SDCSS console

Execute command

Date and time restrictions

The FileWatch feature monitors changes in the following file system attributes.

<table>
<thead>
<tr>
<th>Attribute</th>
<th>Old and New values recorded</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Unix Permission bitmask</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>■ User</td>
<td></td>
<td></td>
</tr>
<tr>
<td>■ Group</td>
<td></td>
<td></td>
</tr>
<tr>
<td>■ Other</td>
<td></td>
<td></td>
</tr>
<tr>
<td>■ Setuid bit</td>
<td></td>
<td></td>
</tr>
<tr>
<td>■ Setgid bit</td>
<td></td>
<td></td>
</tr>
<tr>
<td>■ Sticky bit</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Windows Permission bitmask</td>
<td>Yes</td>
<td>Changes to attributes marked with an asterisk (*) are only recorded if changes to the file’s access time are being monitored.</td>
</tr>
<tr>
<td>■ Archive*</td>
<td></td>
<td></td>
</tr>
<tr>
<td>■ Directory</td>
<td></td>
<td></td>
</tr>
<tr>
<td>■ Encrypted</td>
<td></td>
<td></td>
</tr>
<tr>
<td>■ Hidden</td>
<td></td>
<td></td>
</tr>
<tr>
<td>■ Indexed*</td>
<td></td>
<td></td>
</tr>
<tr>
<td>■ Offline</td>
<td></td>
<td></td>
</tr>
<tr>
<td>■ Read Only</td>
<td></td>
<td></td>
</tr>
<tr>
<td>■ System</td>
<td></td>
<td></td>
</tr>
<tr>
<td>■ Temporary*</td>
<td></td>
<td></td>
</tr>
<tr>
<td>File size</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>Attribute</td>
<td>Old and New values recorded</td>
<td>Notes</td>
</tr>
<tr>
<td>--------------------</td>
<td>-----------------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Modification Date</td>
<td>Yes</td>
<td>Windows FAT file systems have a two second resolution on their timestamps. If multiple changes happen within a two second window, Symantec Data Center Security: Server Advanced may not record them as separate events.</td>
</tr>
<tr>
<td>Access Date</td>
<td>Yes</td>
<td>Symantec Data Center Security: Server Advanced monitors the access time only if the underlying file system supports recording access time. Following are the situations where file systems do not record access time:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>■ Most current releases of Windows (Windows 2008 and newer, Windows Vista and newer) do not record access time by default. It must be explicitly enabled. For example, fsutil.exe behavior set disablelastaccess 0.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>■ Windows FAT file systems do not record access time even if the operating system has it enabled.</td>
</tr>
<tr>
<td>Creation Date</td>
<td>Yes</td>
<td>UNIX and Linux only</td>
</tr>
<tr>
<td># of Hard Links</td>
<td>Yes</td>
<td>UNIX and Linux only</td>
</tr>
<tr>
<td>Symlink value</td>
<td>Yes</td>
<td>UNIX and Linux only</td>
</tr>
<tr>
<td>Owner</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>Group</td>
<td>Yes</td>
<td>Primary Group for Windows</td>
</tr>
<tr>
<td>File type</td>
<td>Yes</td>
<td>Flags indicating if the path or filename switched to or from a file, from or to a directory, or a symlink. UNIX and Linux only</td>
</tr>
<tr>
<td>NTFS Discretionary ACL</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>NTFS Extended File Attributes</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>NTFS Alternate Data Stream Size</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>File Checksum Value (SHA-256)</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>User that made change</td>
<td>N/A</td>
<td>RT-FIM platforms and events only</td>
</tr>
<tr>
<td>Attribute</td>
<td>Old and New values recorded</td>
<td>Notes</td>
</tr>
<tr>
<td>-----------------------------------</td>
<td>-----------------------------</td>
<td>------------------------------------------</td>
</tr>
<tr>
<td>Process that made change</td>
<td>N/A</td>
<td>RT-FIM platforms and events only</td>
</tr>
<tr>
<td>Process ID that made change</td>
<td>N/A</td>
<td>RT-FIM platforms and events only</td>
</tr>
<tr>
<td>User Session # that made change</td>
<td>N/A</td>
<td>RT-FIM platforms and events only</td>
</tr>
</tbody>
</table>

In addition to monitoring the file system attributes, Symantec Data Center Security: Server Advanced records detailed changes made to the content of text files. The changes are recorded in a typical diff format with old and new lines from the file shown.

**About registry watch rules**

This rule type monitors changes to user-specified registry keys, and ignores changes to user-specified registry keys. These changes comprise creating, deleting, and modifying user-specified registry keys. You can enable or disable monitoring or ignoring specific registry keys, and you can adjust the list of registry keys that are monitored or ignored.

The registry watch rule type is associated with the registry collector. The registry collector watches for changes made to user-specified registry keys.

The rule is created with the following rule options:

Registry watch rule options

- Rule name
- Rule severity
- Monitor creation of registry keys
- Monitor deletion of registry keys
- Monitor modification of registry keys
Additional patterns to match

Registry keys to watch
Select this check box to monitor specific registry keys, and then list the keys to monitor.

Registry keys to ignore
Select this check box to ignore specific registry keys, and then list the keys to ignore.

Record event to SDCSS console

Execute command

date and time restrictions

About prevention watch rules

This rule type monitors user-specified prevention events.

The rule is created with the following rule options:

Prevention watch rule options
Select this check box to enable the rule.

Rule name

Rule severity

Prevention event fields to match on
This option matches event fields. It is always enabled.
Select one of the following prevention event types:
- All prevention events
- Buffer overflow
- File access
- Mount
- Network access
- OS Call
- Process assignment
- Process create
- Process destroy
- Registry access

Specify the event variables to monitor, with values for each variable.
Specify any additional patterns to match and patterns to ignore.
About text log rules

This rule type monitors user-specified text patterns in user-specified text logs. The rule type is associated with the text log collector, which watches for matches in user-specified text logs.

The text log rule type is also used with virtual agents. Symantec Data Center Security: Server Advanced recognizes and processes virtual event data indirectly via a text log rule, where you designate resulting events as originating from virtual agents. In a manner similar to specifying a user-defined text string, you can identify a source system identification tag that indicates the events are from an agent other than the host machine that processed the events.

See the Symantec Data Center Security: Server Advanced Administration Guide for information on virtual agents.

The text log rule is created with the following rule options:

- Text log rule options
  - Select this check box to enable the text log rule.

- Rule name
  -

- Rule severity
  -

- Text log path
  - Specify the text log file to monitor. Specify the complete file path. Wildcard characters are not permitted in the path. Use the percent sign (%) to delimit variables.

- Log file structure definitions
  - This rule option defines the text log file structure. It is always enabled.
<table>
<thead>
<tr>
<th>Feature</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Log file contains events coming from a virtual agent</td>
<td>Select this check box to indicate that the records in the text log file are from a virtual agent, and then specify the virtual agent name. You can specify the virtual agent name as a text string. Use this format when all the records in the text log file are from the same virtual agent. Example: Mainframe01 You can specify the virtual agent name as a variable. You must define the variable using the parse definitions option. Use this format when the records in the text log file are from multiple virtual agents. Example: {Virtual Agent Tag}</td>
</tr>
<tr>
<td>Parse definitions</td>
<td>Select this check box to indicate that the virtual agent name is specified in a parse string, and then specify the parse string. Example: <em>agent name={Virtual Agent Tag},</em> Use this option when the records in the text log file are from multiple virtual agents. Parse strings support wildcard characters. Type an asterisk (*) as the wildcard character for zero or more characters. When mixing literal text strings with wildcard characters, do not precede the literal text string with a delimiter character (space or tab), unless the character is not found anywhere before the literal text string. For example, if the space delimiter is found before the following literal text string, then the text pattern will not match <em>user=</em>: a string user=joe a string The pattern parser algorithm works from left to right to match <em>&lt;space&gt;user=</em> with a&lt;space&gt;string user=joe a string. When specifying a variable, include a literal delimiter/terminator after the variable. Otherwise, the pattern parser algorithm cannot determine where the variable data ends. For example: user={UserName} * Note the space after the variable. If it were defined as <em>user={UserName}</em> then the algorithm would fail to extract the {UserName} portion of the string.</td>
</tr>
<tr>
<td>Records in file contain multiple lines</td>
<td>If the records in the text log file contain multiple lines, select this check box, and then specify the character used to use to delimit the records.</td>
</tr>
<tr>
<td>Record event to SDCSS console</td>
<td></td>
</tr>
</tbody>
</table>
About generic rules

This rule type monitors user-specified events from any of the Symantec Data Center Security: Server Advanced event sources.

The generic rule is created with the following rule options:

- **Select this checkbox to enable the generic rule.**
- **Rule name**
- **Rule severity**
- **Record event to SDCSS console**
- **Execute command**
- **Event patterns**
- **Date and time restrictions**

Host Intrusion detection policies enhancements

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 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 Data Center Security: Server Advanced console. These rules now also use ignore logic and select logic methodology.

You can now configure and view all rule content from the Symantec Data Center Security: Server Advanced console.

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.

Table 2-1 illustrates how the existing policies from previous releases were combined with new options into the 5.2.6 top-level option groups.

<table>
<thead>
<tr>
<th>Options in previous releases, with new material noted</th>
<th>Detection option organization in release 5.2.6</th>
</tr>
</thead>
<tbody>
<tr>
<td>System_Group_Management_Change</td>
<td>System User and Group Change Monitor</td>
</tr>
<tr>
<td>System_User_Configuration</td>
<td></td>
</tr>
<tr>
<td>Enhanced_System_Group_Change (NEW)</td>
<td></td>
</tr>
<tr>
<td>Domain_Trust_Configuration</td>
<td>System Active-Directory Change Monitor</td>
</tr>
<tr>
<td>MS_ActiveDirectory_FSMO_Changed</td>
<td></td>
</tr>
<tr>
<td>System_AuthEncrypt_Configuration</td>
<td></td>
</tr>
<tr>
<td>AD_Privileged_Group/User_Change (NEW)</td>
<td></td>
</tr>
<tr>
<td>Options in previous releases, with new material noted</td>
<td>Detection option organization in release 5.2.6</td>
</tr>
<tr>
<td>-----------------------------------------------------</td>
<td>-----------------------------------------------</td>
</tr>
<tr>
<td>System_Logoff</td>
<td>System Login Activity and Access Monitor</td>
</tr>
<tr>
<td>System_Logon_Success</td>
<td></td>
</tr>
<tr>
<td>System_Failed_Access_Status</td>
<td></td>
</tr>
<tr>
<td>Domain_Privileged_User_Login (NEW)</td>
<td></td>
</tr>
<tr>
<td>System_Autorun_Configuration</td>
<td>System Hardening Monitor</td>
</tr>
<tr>
<td>Network_Comm_Configuration</td>
<td></td>
</tr>
<tr>
<td>System_File_Protection_Status</td>
<td></td>
</tr>
<tr>
<td>System_Security_Configuration</td>
<td></td>
</tr>
<tr>
<td>System_StartStop_Options</td>
<td></td>
</tr>
<tr>
<td>System_Audit_Tampering</td>
<td></td>
</tr>
<tr>
<td>System_Hardening</td>
<td></td>
</tr>
<tr>
<td>System_Shares_Configuration</td>
<td>System File and Directory Monitor</td>
</tr>
<tr>
<td>Host_IDS_File_Tampering</td>
<td></td>
</tr>
<tr>
<td>Critical_System_File_Monitor (NEW)</td>
<td></td>
</tr>
<tr>
<td>Critical_Registry_StartPath_Monitor</td>
<td>System Registry Monitor</td>
</tr>
<tr>
<td>Critical_System_Registry_Monitor (NEW)</td>
<td></td>
</tr>
<tr>
<td>Symantec_AV_Client_Communication</td>
<td>Symantec Software Monitoring</td>
</tr>
<tr>
<td>SAV_Critical_Action_Monitor (NEW)</td>
<td></td>
</tr>
<tr>
<td>SEP_Critical_Action_Monitor (NEW)</td>
<td></td>
</tr>
<tr>
<td>USB_Device_Activity</td>
<td>External Device Activity Monitor</td>
</tr>
<tr>
<td>USB_Device_Vendor_Detection (NEW)</td>
<td></td>
</tr>
<tr>
<td>CD/DVD_Burning_Activity (NEW)</td>
<td></td>
</tr>
<tr>
<td>Generic/Web_Attack_Detection</td>
<td>System Attack Detection</td>
</tr>
<tr>
<td>Web_Attack_Detection (NEW)</td>
<td></td>
</tr>
</tbody>
</table>

The policies that perform administrative or troubleshooting activities for Symantec Data Center Security: Server Advanced agents and management server-specific policies were not combined with the Windows Baseline policy.
The following policies were not combined because they serve an administrative purpose outside of normal detection functionality or facilitate the Global Watch functionality:

- SDCSS_Agent_Diagnostics
- SDCSS_Agent_Status
- SDCSS_Server_Monitor
- Global_Watch_Policy
UNIX Detection Policy Reference

This chapter includes the following topics:

- About the UNIX detection policies
- List of policies

About the UNIX detection policies

Symantec Data Center Security: Server Advanced includes UNIX detection policies for computers that run the following operating systems:

- IBM AIX
- Sun Solaris
- Red Hat Enterprise Linux
- SUSE Linux Enterprise

You can apply the UNIX detection policies to any Solaris, Linux, AIX, and HP-UX agent or agent group.

The UNIX detection policies are as follows:

- UNIX_SDCSS_Agent_Diagnostics
- UNIX_SDCSS_Agent_Status
- UNIX_Host_IDS_File_Tampering
- UNIX_NetRecon_Scan_Detected
- UNIX_Sendmail_BrokenPipe_Messages
- UNIX_Stack_Execution_Denied (Solaris, HP-UX)
In addition to the UNIX policies, Symantec Data Center Security: Server Advanced includes OS-specific policies. A version of each OS-specific policy is provided for Solaris, Linux, AIX, and HP-UX agents.

The OS-specific policies are as follows:

- Apache_Vulnerable_CGI_Scripts
- SANS

**List of policies**

The section describes the Symantec Data Center Security: Server Advanced UNIX detection policies.

**UNIX_SDCSS_Agent_Diagnostics**

This UNIX detection policy includes options to do the following:

- Run the collect info script
- Restart the IDS service
- Restart the IPS service
- Restart the UTIL service
- Force log rollover of the agent event log file
- Modify the management server list for an agent
- Edit configuration files
- Enable or disable prevention

For more information, see the Windows version of this policy.
UNIX_SDCSS_Agent_Status

This UNIX detection policy runs scripts that provide health checks on IPS agents. The health check scripts run based on user-configurable timers. The timers are started when the policy is initially applied to an agent or when the agent is restarted.

The policy options are as follows:

- **IPS Health Check**: Periodically runs the IPS agent health check script. Specify the health check frequency in days, hours, minutes, and seconds. By default, the health check script runs every hour.

- **IPS Util Health Check**: Periodically runs the IPS Util health check script on Solaris or Linux agents. Specify the Util health check frequency in days, hours, minutes, and seconds. By default, the health check script runs every hour.

- **IPS Core Detection**: Monitors syslogs for detected sisipsagent core dump files.

UNIX_Template_Policy

The UNIX_Template_Policy is a reusable workspace container policy for managing custom rules.

The UNIX_Template_Policy policy includes rule options for the following rule types:

- Filewatch
- Text log
- Prevention watch
- Generic
- C2 log
- Syslog
- UNIX activity log

The UNIX_Template_Policy is intended for use as a container policy for managing custom rules. The policy contains only the rules that you define.

For more information on using the template policy, including how to create and reuse custom rules, see the Windows_Template_Policy.

About C2 log rules

This rule type monitors the C2 audit logs on Solaris, HP-UX, and AIX agents. The rule type is associated with the C2 collector, which looks for matches in the C2 audit logs.

Note: C2 logging must be turned on and configured on the agent computers.

The C2 log rule is created with the following rule options:

- **C2 rule options**: Select this check box to enable the C2 rule.
- **Rule name**: See the Windows_Template_Policy for details.
- **Rule severity**: See the Windows_Template_Policy for details.
- **Record event to SDCSS console**: See the Windows_Template_Policy for details.
- **Execute command**: See the Windows_Template_Policy for details.
- **Event patterns**: See the Windows_Template_Policy for details.
- **Date and time restrictions**: See the Windows_Template_Policy for details.

About syslog rules

This rule type monitors user-specified events in the UNIX syslog. The rule type is associated with the syslog collector, which watches for syslog daemon tampering on UNIX systems.

The syslog rule is created with the following rule options:

- **Syslog rule options**: Select this check box to enable the syslog rule.
- **Rule name**: See the Windows_Template_Policy for details.
- **Rule severity**: See the Windows_Template_Policy for details.
- **Record event to SDCSS console**: See the Windows_Template_Policy for details.
- **Execute command**: See the Windows_Template_Policy for details.
- **Event patterns**: See the Windows_Template_Policy for details.
About UNIX activity log rules

This rule type monitors user-specified events in the WTMP and BTMP files. The rule type is associated with the WTMP collector, which watches for matches in the WTMP and BTMP files.

The UNIX activity log rule is created with the following rule options:

- **UNIX activity log rule options**: Select this check box to enable the UNIX activity log rule.
- **Rule name**: See the Windows_Template_Policy for details.
- **Rule severity**: See the Windows_Template_Policy for details.
- **Record event to SDCSS console**: See the Windows_Template_Policy for details.
- **Execute command**: See the Windows_Template_Policy for details.
- **Event patterns**: See the Windows_Template_Policy for details.
- **Date and time restrictions**: See the Windows_Template_Policy for details.
- **Number of events in an interval**: See the Windows_Template_Policy for details.

**Note**: The latest detection policies added are OpenStack_Nova_Detection_Policy, vSphere_ESX_Detection_Policy, and vSphere_ESXi_Detection_Policy.
Policy Examples

This chapter includes the following topics:

- About policy examples
- Forcing rollover of the agent event log file
- Creating a filewatch rule

About policy examples

This chapter includes the following topics:

- Forcing rollover of the agent event log file
- Creating a filewatch rule

Forcing rollover of the agent event log file

Forcing rollover of the agent event log file closes the current log file and opens a new log file.

The agent event log file is stored in the following directories:

Windows: C:\Program Files\Symantec\Data Center Security Server\Agent\sdcsslog\n
UNIX: /var/log/sdcsslog/

The policy forces rollover of the log file immediately after being applied to the agent.
To force rollover of the agent event log file

1. Log on to the management console as an administrator.
2. In the management console, on the Policies page, in the Symantec folder, edit the SDCSS_Agent_Diagnostics policy.
3. Under Advanced Policy Settings > Diagnostic functions, enable Select a function to run on the agent.
4. Under the Select a function group box, select the value as Force log rollover.
5. Click OK to save the policy changes.
6. Apply the policy to the agent.
7. In the management console, monitor the events on the Monitors page to determine if the agent event log file rolled over.
8. Check the log file directory to confirm that rollover occurred.
9. On the Assets page, select the agent, and then right-click Clear Policy to clear the policy from the agent.

Creating a filewatch rule

Create a filewatch rule to monitor changes to user-specified files.

To create a filewatch rule

1. In the management console, click Policies.
2. Under the Policies tab, click Detection.
3. On the Policies page, double-click Windows_Template_Policy or UNIX_Template_Policy.
4. In the policy editor dialog box, under Advanced PolicySettings, click My Custom Rules, and then click Add a new Custom Control icon.
5. In the New Custom Rule Wizard dialog box, specify the following information:

<table>
<thead>
<tr>
<th>Display Name</th>
<th>Type a descriptive name for the filewatch rule.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Category</td>
<td>Select the filewatch rule type.</td>
</tr>
<tr>
<td>Identifier</td>
<td>Type a name that the policy uses internally to identify the filewatch rule.</td>
</tr>
<tr>
<td>Description</td>
<td>Type a full description of the filewatch rule.</td>
</tr>
</tbody>
</table>
6 Click Finish.

7 In the policy editor dialog box, click Edit to display the rule options.

8 In the policy editor dialog box, under Advanced Policy Settings > My Custom Rules, click Edit before Filewatch Rule Options, and then select the check box to enable the filewatch rule.

9 In the policy editor dialog box, enable the rule options to monitor file creation, deletion, modification, and access.

10 In the policy editor dialog box, enable Additional patterns to match on, and then specify the list of patterns.

11 In the policy editor dialog box, enable Files to watch, and then specify the list of files to watch.

12 Click OK.
Windows Baseline Detection policy

This chapter includes the following topics:

- Introduction
- File monitoring improvements
- Windows-specific policy improvements
- About rule options

Introduction

The Symantec Data Center Security: Server Advanced Host Intrusion Detection policies have been redesigned and rewritten. Multiple policies were reorganized into a baseline monitoring solution for the Windows operating system environment. The new policy provides enhanced stability, greater ease of use and detection accuracy, and added functionality.

The Windows policy includes the following improvements:

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

- Policy option group naming conventions have been standardized for ease of administration. You can 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 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 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 transversal, 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 mouse over parts of the user interface to display descriptions to assist in policy navigation and rule-by-rule overview.

Table 5-1 illustrates how the existing policies from previous releases were combined with new options into the 5.2.6 top level option groups.

<table>
<thead>
<tr>
<th>Options in previous releases, with new material noted</th>
<th>Detection option organization in release 5.2.6</th>
</tr>
</thead>
<tbody>
<tr>
<td>System_Group_Management_Change</td>
<td>System User and Group Change Monitor</td>
</tr>
<tr>
<td>System_User_Configuration</td>
<td></td>
</tr>
<tr>
<td>Enhanced_System_Group_Change (NEW)</td>
<td></td>
</tr>
<tr>
<td>Domain_Trust_Configuration</td>
<td>System Active-Directory Change Monitor</td>
</tr>
<tr>
<td>MS_ActiveDirectory_FSMO_Changed</td>
<td></td>
</tr>
<tr>
<td>System_AuthEncrypt_Configuration</td>
<td></td>
</tr>
<tr>
<td>AD_Privileged_Group/User_Change (NEW)</td>
<td></td>
</tr>
<tr>
<td>Options in previous releases, with new material noted</td>
<td>Detection option organization in release 5.2.6</td>
</tr>
<tr>
<td>------------------------------------------------------</td>
<td>------------------------------------------------</td>
</tr>
<tr>
<td>System_Logoff</td>
<td>System Login Activity and Access Monitor</td>
</tr>
<tr>
<td>System_Logon_Success</td>
<td>System Hardening Monitor</td>
</tr>
<tr>
<td>System_Failed_Access_Status</td>
<td>System Hardening Monitor</td>
</tr>
<tr>
<td>Domain_Privileged_User_Login (NEW)</td>
<td>System Hardening Monitor</td>
</tr>
<tr>
<td>System_Autorun_Configuration</td>
<td>System File and Directory Monitor</td>
</tr>
<tr>
<td>Network_Comm_Configuration</td>
<td>System Registry Monitor</td>
</tr>
<tr>
<td>System_File_Protection_Status</td>
<td>System Registry Monitor</td>
</tr>
<tr>
<td>System_Security_Configuration</td>
<td>Symantec Software Monitoring</td>
</tr>
<tr>
<td>System_StartStop_Options</td>
<td>System Attack Detection</td>
</tr>
<tr>
<td>System_Audit_Tampering</td>
<td>System Attack Detection</td>
</tr>
<tr>
<td>System_Hardening</td>
<td>System Attack Detection</td>
</tr>
<tr>
<td>System_FileandDirectoryMonitor</td>
<td>System Attack Detection</td>
</tr>
<tr>
<td>Host_IDS_File_Tampering</td>
<td>System Attack Detection</td>
</tr>
<tr>
<td>Critical_System_File_Monitor (NEW)</td>
<td>System Attack Detection</td>
</tr>
<tr>
<td>Critical_RegistryStartPath_Monitor</td>
<td>System Attack Detection</td>
</tr>
<tr>
<td>Critical_System_Registry_Monitor (NEW)</td>
<td>System Attack Detection</td>
</tr>
<tr>
<td>Symantec_AV_Client_Communication</td>
<td>System Attack Detection</td>
</tr>
<tr>
<td>SAV_Critical_Action_Monitor (NEW)</td>
<td>System Attack Detection</td>
</tr>
<tr>
<td>SEP_Critical_Action_Monitor (NEW)</td>
<td>System Attack Detection</td>
</tr>
<tr>
<td>USB_Device_Activity</td>
<td>System Attack Detection</td>
</tr>
<tr>
<td>USB_Device_Vendor_Detection (NEW)</td>
<td>System Attack Detection</td>
</tr>
<tr>
<td>CD/DVD_Burning_Activity</td>
<td>System Attack Detection</td>
</tr>
<tr>
<td>Generic_Web_Attack_Detection</td>
<td>System Attack Detection</td>
</tr>
<tr>
<td>Web_Attack_Detection (NEW)</td>
<td>System Attack Detection</td>
</tr>
</tbody>
</table>

The policies that perform administrative or troubleshooting activities for Symantec Data Center Security: Server Advanced agents and management server-specific policies were not combined with the Windows Baseline policy.
The following policies were not combined because they serve an administrative purpose outside of normal detection functionality or facilitate the Global Watch functionality:

- SDCSS_Agent_Diagnostics
- SDCSS_Agent_Status
- SDCSS_Server_Monitor
- Global_Watch_Policy

File monitoring improvements

Symantec Data Center Security: Server Advanced has some file monitoring improvements.

Specific file monitoring changes include the following improvements:

- You can control and enable the access, delete, modify, and create change monitoring functions on a group-by-group basis.
- You can control modification differentiating, including algorithm selection on a group-by-group basis.
- You can set date and time restrictions within each specific file monitoring group.
- You can tune the file monitor modified detection operation for specific criteria, such as only for permission changes, size changes, bitmask changes, and so on.
- You can use specific ignore logic criteria and select logic criteria in each file monitoring group.
  For example, you can independently configure each file monitoring group to ignore file paths or strings.

Symantec Data Center Security: Server Advanced includes the following enhancements for monitoring files:

- Symantec Data Center Security: Server Advanced monitors Access Control Lists (ACLs) in file attributes.
  Table 1-8 describes the Access Control List strings that Symantec Data Center Security: Server Advanced returns.
- To provide granular control over Windows file change monitoring, Symantec Data Center Security: Server Advanced monitors near real-time changes on local file systems and fixed file systems. It does not monitor changes on removable media or remote network drives.
  It no longer uses polling intervals. Symantec Data Center Security: Server Advanced uses the FIPS 180-2-compliant Secure Hash Algorithm (SHA-256)
to calculate file hashes or checksums at runtime. The MD5 algorithm is no longer used or available.
For performance efficiency, you can enable or disable the checksum calculation for each filewatch list. A single hash algorithm is used on all the files in a watched list.

**Note:** Symantec Data Center Security: Server Advanced continues to poll remote files, such as files on network drives or removable media, every specified interval to detect changes.

- Symantec Data Center Security: Server Advanced tracks the user names and processes associated with file modifications within Windows Host-based Intrusion Detection Systems. Modifications that are tracked include file opens, file writes, file creations, and file deletions. This feature lets you determine who has accessed and who changed the local files that were accessed through a file share.

Symantec Data Center Security: Server Advanced captures the local user names or remote user names of the users that access a file. This feature does not rely on Windows Event Monitoring, Windows Audit Object Access logging, or UNIX Event Monitoring. Local user names are resolved locally. Remote users' names are obtained by using Active Directory queries. If no names are provided, Symantec Data Center Security: Server Advanced captures the Windows Security Identifier (SID). The Symantec Data Center Security: Server Advanced detection agent service must be running for the user name and process tracking functionality to work. If the Symantec Data Center Security: Server Advanced detection agent service is stopped, then the moment that it is restarted it reports the file modification events that took place during the time that it was stopped. However, the user names and processes that are associated with the modifications that took place while the service was stopped are not included for those modifications.

**Note:** This feature makes use of a file filter driver to capture user name and processes for file modifications. If you use only IDS, you do not need to restart after installation. If you enable IPS features during installation, you do need to restart.

---

**Windows-specific policy improvements**

Windows-specific policy changes include the following improvements:
■ Product-specific monitoring areas for key Symantec applications such as Symantec AntiVirus and Symantec Endpoint Protection. Improved monitoring of endpoint security products provides administrators more finite events that are tailored for compatibility.

■ Improved external device detection now includes event generation for CD and DVD burning activity.

■ Critical Windows registry change detection has been added. Critical auto start areas of the Windows operating system are monitored to ensure that the host system security is maintained. New registry paths for Auto Start Keys have been added.

Note: Registry monitoring has the same options as the rewritten file and directory monitoring.

About rule options

Symantec Data Center Security: Server Advanced provides specific content control per rule from the console. Each rule in the Baseline policy has required parameters. These rules can be viewed and customized from the console.

The options in Table 5-2 are available for each rule that is displayed in the Policy Settings pane.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Rule Name</td>
<td>The name that is associated with the rule that generates the specific event. A single string value is allowed in the string field.</td>
</tr>
<tr>
<td>Severity</td>
<td>The severity of event. Available for each rule of the policy. You can only select one severity level, Info, Notice, Warning, Major, or Critical, for each rule.</td>
</tr>
<tr>
<td>Event IDs</td>
<td>Parameter options for Windows event log watch rules. Separate multiple event IDs with a comma (,) in this string list. You can add, edit, and remove event IDs.</td>
</tr>
<tr>
<td>File Paths</td>
<td>Parameter options for filewatch rules. You can use multiple file paths with associated wildcard entries in this string list. You can add, edit, and remove file paths.</td>
</tr>
<tr>
<td>Option</td>
<td>Description</td>
</tr>
<tr>
<td>--------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Registry Paths</td>
<td>Parameter options for registry watch rules. You can use multiple Windows registry paths with associated wildcard entries in this string list. You can add, edit, and remove registry paths.</td>
</tr>
</tbody>
</table>
| Select Strings     | Used in rule select logic. Symantec Data Center Security: Server Advanced uses primary logic or initial sifting method for rule event generation. Use an asterisk (*) to select all the events that the criteria that you entered previously generate.  
For example, criteria such as event IDs, file paths, registry paths, or log strings previously defined. With this option you can specifically tune rules for administrator needs.  
For example, if you change the select string on a file watch rule from * to "Permission", then that rule only generates a file watch event if that event contains the string “Permission.” You can have multiple select strings in this string list. All strings are case insensitive. You can add, edit, and remove select strings. |
| Ignore Strings     | Used in rule ignore logic. Symantec Data Center Security: Server Advanced uses secondary ignore logic or ignore sifting method for rule event generation. Almost all rule parameter options contain a blank value, which signifies that a null value or no value is associated with the ignore logic statement. Symantec Data Center Security: Server Advanced ignores any string in this field other than blank value upon pattern matching on the final event generation. Ignore strings also provide you with the ability to perform advanced rule-by-rule tuning. You can have multiple ignore strings in this string list. All strings are case insensitive. You can add, edit, and remove ignore strings.  
The ignore criteria ignores items that have a tendency to change frequently or items that are not a part of the core system and configuration. These ignore items are items such as logs, temp directory and so on. |

**Note:** Each parameter is preconfigured with default values to ensure the functionality of the rule. Changes to rule name and severity do not affect the overall operation of the rule.
Windows Policy Options

This chapter includes the following topics:

■ System user and group change monitor
■ System Active Directory Change Monitor
■ System login activity and access monitor
■ System hardening monitor
■ System file and directory monitor
■ System registry monitor
■ System Symantec software monitor
■ System external device activity
■ System attack detection

System user and group change monitor

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

System user configuration changes

This option group subsection monitors user changes from local account manipulation to the user activity that warrants event detection in Active Directory environments.
### Table 6-1  Description of the **Account Changed** parameters used

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Option Path</td>
<td>System User and Group Change Monitor &gt; System User Configuration Changes</td>
</tr>
<tr>
<td>Option</td>
<td>Account Changed</td>
</tr>
<tr>
<td>Rule Name</td>
<td>ZZ_Account_Changed</td>
</tr>
<tr>
<td>Severity</td>
<td>Warning</td>
</tr>
<tr>
<td>Event IDs</td>
<td>642, 4738, 685</td>
</tr>
<tr>
<td>Description</td>
<td>Detects the changes that are made to user accounts on the local system.</td>
</tr>
</tbody>
</table>

### Table 6-2  Description of the **Account Created** parameters used

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Option Path</td>
<td>System User and Group Change Monitor &gt; System User Configuration Changes</td>
</tr>
<tr>
<td>Option</td>
<td>Account Created</td>
</tr>
<tr>
<td>Rule Name</td>
<td>AA_Account_Created</td>
</tr>
<tr>
<td>Severity</td>
<td>Warning</td>
</tr>
<tr>
<td>Event IDs</td>
<td>629, 4720</td>
</tr>
<tr>
<td>Description</td>
<td>Detects the creation of user accounts on the local system.</td>
</tr>
</tbody>
</table>

### Table 6-3  Description of the **Account Deleted** parameters used

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Option Path</td>
<td>System User and Group Change Monitor &gt; System User Configuration Changes</td>
</tr>
<tr>
<td>Option</td>
<td>Account Deleted</td>
</tr>
<tr>
<td>Rule Name</td>
<td>Account_Deleted</td>
</tr>
<tr>
<td>Severity</td>
<td>Warning</td>
</tr>
<tr>
<td>Event IDs</td>
<td>630, 4726</td>
</tr>
<tr>
<td>Description</td>
<td>Detects the deletion of user accounts on the local system.</td>
</tr>
</tbody>
</table>
Table 6-4  Description of the **Account Disabled** parameters used

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Option Path</td>
<td>System User and Group Change Monitor &gt; System User Configuration Changes</td>
</tr>
<tr>
<td>Option</td>
<td>Account Disabled</td>
</tr>
<tr>
<td>Rule Name</td>
<td>Account_Disabled</td>
</tr>
<tr>
<td>Severity</td>
<td>Warning</td>
</tr>
<tr>
<td>Event IDs</td>
<td>629, 4725</td>
</tr>
<tr>
<td>Description</td>
<td>Detects the disabling of user accounts on the local system.</td>
</tr>
</tbody>
</table>

Table 6-5  Description of the **Account Enabled** parameters used

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Option Path</td>
<td>System User and Group Change Monitor &gt; System User Configuration Changes</td>
</tr>
<tr>
<td>Option</td>
<td>Account Enabled</td>
</tr>
<tr>
<td>Rule Name</td>
<td>Account.Enabled</td>
</tr>
<tr>
<td>Severity</td>
<td>Warning</td>
</tr>
<tr>
<td>Event IDs</td>
<td>626, 4722</td>
</tr>
<tr>
<td>Description</td>
<td>Detects the enabling of user accounts on the local system.</td>
</tr>
</tbody>
</table>

Table 6-6  Description of the **Local Account Locked Out** parameters used

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Option Path</td>
<td>System User and Group Change Monitor &gt; System User Configuration Changes</td>
</tr>
<tr>
<td>Option</td>
<td>Local Account Locked Out</td>
</tr>
<tr>
<td>Rule Name</td>
<td>System_User_Configuration_Local_AccountLocked_Out</td>
</tr>
<tr>
<td>Severity</td>
<td>Warning</td>
</tr>
<tr>
<td>Event IDs</td>
<td>644, 4740</td>
</tr>
<tr>
<td>Description</td>
<td>Detects the locking of a user account on the local system.</td>
</tr>
</tbody>
</table>
### Table 6-7  Description of the Local Account Lock Out Threshold, Time Interval, and Severity parameters used

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Option Path</td>
<td>System User and Group Change Monitor &gt; System User Configuration Changes</td>
</tr>
<tr>
<td>Option</td>
<td>Local Account Lock Out Threshold, Time Interval, and Severity</td>
</tr>
<tr>
<td>Severity</td>
<td>Critical</td>
</tr>
<tr>
<td>Count</td>
<td>10</td>
</tr>
<tr>
<td>Interval</td>
<td>3</td>
</tr>
<tr>
<td>Description</td>
<td>Detects the locking of a user account on the local system then generates a higher severity event based on user-defined threshold values.</td>
</tr>
</tbody>
</table>

### Table 6-8  Description of the Local Account Unlocked parameters used

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Option Path</td>
<td>System User and Group Change Monitor &gt; System User Configuration Changes</td>
</tr>
<tr>
<td>Option</td>
<td>Local Account Unlocked</td>
</tr>
<tr>
<td>Rule Name</td>
<td>Local_Account_Unlocked</td>
</tr>
<tr>
<td>Severity</td>
<td>Warning</td>
</tr>
<tr>
<td>Event IDs</td>
<td>671, 4767</td>
</tr>
<tr>
<td>Description</td>
<td>Detects the unlocking of a user account on the local system.</td>
</tr>
</tbody>
</table>

### Table 6-9  Description of the Admin Passwd Change Failed parameters used

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Option Path</td>
<td>System User and Group Change Monitor &gt; System User Configuration Changes</td>
</tr>
<tr>
<td>Option</td>
<td>Admin Passwd Change Failed</td>
</tr>
<tr>
<td>Rule Name</td>
<td>Admin_Passwd_Change_Failed</td>
</tr>
<tr>
<td>Severity</td>
<td>Critical</td>
</tr>
<tr>
<td>Event IDs</td>
<td>627, 4723</td>
</tr>
</tbody>
</table>
### Table 6-9  Description of the **Admin Passwd Change Failed** parameters used

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Description</td>
<td>Detects the failed attempts to change the administrator password.</td>
</tr>
</tbody>
</table>

### Table 6-10  Description of the **User Added to Global Group** parameters used

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Option Path</td>
<td>System User and Group Change Monitor &gt; System User Configuration Changes</td>
</tr>
<tr>
<td>Option</td>
<td>User Added to Global Group</td>
</tr>
<tr>
<td>Rule Name</td>
<td>User_Added_to_Global_Group</td>
</tr>
<tr>
<td>Severity</td>
<td>Warning</td>
</tr>
<tr>
<td>Event IDs</td>
<td>632, 4728</td>
</tr>
<tr>
<td>Description</td>
<td>Detects the addition of a user to a global group. This rule applies to Windows servers that act as domain controllers.</td>
</tr>
</tbody>
</table>

### Table 6-11  Description of the **User Removed from Global Group** parameters used

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Option Path</td>
<td>System User and Group Change Monitor &gt; System User Configuration Changes</td>
</tr>
<tr>
<td>Option</td>
<td>User Removed from Global Group</td>
</tr>
<tr>
<td>Rule Name</td>
<td>User_Removed_from_Global_Group</td>
</tr>
<tr>
<td>Severity</td>
<td>Warning</td>
</tr>
<tr>
<td>Event IDs</td>
<td>633, 4729</td>
</tr>
<tr>
<td>Description</td>
<td>Detects the addition of a user to a global group. This rule applies to Windows servers that act as domain controllers.</td>
</tr>
</tbody>
</table>

### Table 6-12  Description of the **Guest Password Change Failed** parameters used

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Option Path</td>
<td>System User and Group Change Monitor &gt; System User Configuration Changes</td>
</tr>
</tbody>
</table>
### Table 6-12 Description of the **Guest Password Change Failed** parameters used (continued)

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Option</td>
<td>Guest Password Change Failed</td>
</tr>
<tr>
<td>Rule Name</td>
<td>Guest_Passwd_Change_Failed</td>
</tr>
<tr>
<td>Severity</td>
<td>Critical</td>
</tr>
<tr>
<td>Event IDs</td>
<td>627, 4723</td>
</tr>
<tr>
<td>Description</td>
<td>Detects a failed attempt to change the guest's password.</td>
</tr>
</tbody>
</table>

### Table 6-13 Description of the **User Added to Local Group** parameters used

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Option Path</td>
<td>System User and Group Change Monitor &gt; System User Configuration Changes</td>
</tr>
<tr>
<td>Option</td>
<td>User Added to Local Group</td>
</tr>
<tr>
<td>Rule Name</td>
<td>User_Added_to_Local_Group</td>
</tr>
<tr>
<td>Severity</td>
<td>Warning</td>
</tr>
<tr>
<td>Event IDs</td>
<td>636, 4732</td>
</tr>
<tr>
<td>Description</td>
<td>Detects the addition of a user to a local group.</td>
</tr>
</tbody>
</table>

### Table 6-14 Description of the **User Removed from Global Group** parameters used

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Option Path</td>
<td>System User and Group Change Monitor &gt; System User Configuration Changes</td>
</tr>
<tr>
<td>Option</td>
<td>User Removed from Global Group</td>
</tr>
<tr>
<td>Rule Name</td>
<td>User_Removed_from_Global_Group</td>
</tr>
<tr>
<td>Severity</td>
<td>Warning</td>
</tr>
<tr>
<td>Event IDs</td>
<td>637, 4733</td>
</tr>
<tr>
<td>Description</td>
<td>Detects the removal of a user from a global group. This rule applies to the Windows servers that act as domain controllers.</td>
</tr>
</tbody>
</table>
### Table 6-15  Description of the **Right Assigned** parameters used

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Option Path</strong></td>
<td>System User and Group Change Monitor &gt; System User Configuration Changes</td>
</tr>
<tr>
<td><strong>Option</strong></td>
<td>Right Assigned</td>
</tr>
<tr>
<td><strong>Rule Name</strong></td>
<td>Right_Assigned</td>
</tr>
<tr>
<td><strong>Severity</strong></td>
<td>Warning</td>
</tr>
<tr>
<td><strong>Event IDs</strong></td>
<td>608, 4704, 4717</td>
</tr>
<tr>
<td><strong>Description</strong></td>
<td>Detects that an access right has been assigned to a user.</td>
</tr>
</tbody>
</table>

### Table 6-16  Description of the **Right Removed** parameters used

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Option Path</strong></td>
<td>System User and Group Change Monitor &gt; System User Configuration Changes</td>
</tr>
<tr>
<td><strong>Option</strong></td>
<td>Right Removed</td>
</tr>
<tr>
<td><strong>Rule Name</strong></td>
<td>Right_Removed</td>
</tr>
<tr>
<td><strong>Severity</strong></td>
<td>Warning</td>
</tr>
<tr>
<td><strong>Event IDs</strong></td>
<td>609, 4705, 4718</td>
</tr>
<tr>
<td><strong>Description</strong></td>
<td>Detects that an access right has been removed from a user.</td>
</tr>
</tbody>
</table>

### Table 6-17  Description of the **User Password Change Failed** parameters used

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Option Path</strong></td>
<td>System User and Group Change Monitor &gt; System User Configuration Changes</td>
</tr>
<tr>
<td><strong>Option</strong></td>
<td>User Password Change Failed</td>
</tr>
<tr>
<td><strong>Rule Name</strong></td>
<td>User_Password_Change_Failed</td>
</tr>
<tr>
<td><strong>Severity</strong></td>
<td>Warning</td>
</tr>
<tr>
<td><strong>Event IDs</strong></td>
<td>627, 4723</td>
</tr>
<tr>
<td><strong>Description</strong></td>
<td>Detects the failed attempt to change a user's password.</td>
</tr>
</tbody>
</table>
Table 6-18  Description of the **User Added to Universal Group** parameters used

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Option Path</td>
<td>System User and Group Change Monitor &gt; System User Configuration Changes</td>
</tr>
<tr>
<td>Option</td>
<td>User Added to Universal Group</td>
</tr>
<tr>
<td>Rule Name</td>
<td>User_Added_to_Universal_Group</td>
</tr>
<tr>
<td>Severity</td>
<td>Warning</td>
</tr>
<tr>
<td>Event IDs</td>
<td>660, 4756</td>
</tr>
<tr>
<td>Description</td>
<td>Detects the addition of a user to a universal group. This rule applies to the Windows servers that act as domain controllers.</td>
</tr>
</tbody>
</table>

Table 6-19  Description of the **User Removed from Universal Grp** parameters used

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Option Path</td>
<td>System User and Group Change Monitor &gt; System User Configuration Changes</td>
</tr>
<tr>
<td>Option</td>
<td>User Removed from to Universal Grp</td>
</tr>
<tr>
<td>Rule Name</td>
<td>User_Removed_from_Universal_Grp</td>
</tr>
<tr>
<td>Severity</td>
<td>Warning</td>
</tr>
<tr>
<td>Event IDs</td>
<td>661, 4757</td>
</tr>
<tr>
<td>Description</td>
<td>Detects the removal of a user from a universal group. This rule applies to the Windows servers that act as domain controllers.</td>
</tr>
</tbody>
</table>

Table 6-20  Description of the **User Added to Local Distribution Group** parameters used

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Option Path</td>
<td>System User and Group Change Monitor &gt; System User Configuration Changes</td>
</tr>
<tr>
<td>Option</td>
<td>User Added to Local Distribution Group</td>
</tr>
<tr>
<td>Rule Name</td>
<td>User_Add_Local_Distribution_Grp</td>
</tr>
<tr>
<td>Severity</td>
<td>Warning</td>
</tr>
</tbody>
</table>
### Table 6-20 Description of the **User Added to Local Distribution Group** parameters used (continued)

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Event IDs</td>
<td>650, 4746</td>
</tr>
<tr>
<td>Description</td>
<td>Detects the addition of a user to a local distribution group.</td>
</tr>
</tbody>
</table>

### Table 6-21 Description of the **User Added to Global Distribution Group** parameters used

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Option Path</td>
<td>System User and Group Change Monitor &gt; System User Configuration Changes</td>
</tr>
<tr>
<td>Option</td>
<td>User Added to Global Distribution Group</td>
</tr>
<tr>
<td>Rule Name</td>
<td>User_Add_Global_Distribution_Grp</td>
</tr>
<tr>
<td>Severity</td>
<td>Warning</td>
</tr>
<tr>
<td>Event IDs</td>
<td>655, 4751</td>
</tr>
<tr>
<td>Description</td>
<td>Detects the addition of a user to a global distribution group.</td>
</tr>
</tbody>
</table>

### Table 6-22 Description of the **User Added to Universal Distribution Group** parameters used

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Option Path</td>
<td>System User and Group Change Monitor &gt; System User Configuration Changes</td>
</tr>
<tr>
<td>Option</td>
<td>User Added to Universal Distribution Group</td>
</tr>
<tr>
<td>Rule Name</td>
<td>User_Add_Univ_Distribution_Grp</td>
</tr>
<tr>
<td>Severity</td>
<td>Warning</td>
</tr>
<tr>
<td>Event IDs</td>
<td>665, 4761</td>
</tr>
<tr>
<td>Description</td>
<td>Detects the addition of a user to a universal distribution group.</td>
</tr>
</tbody>
</table>
### Table 6-23: Description of the Administrator Changed Admin Password parameters used

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Option Path</td>
<td>System User and Group Change Monitor &gt; System User Configuration Changes</td>
</tr>
<tr>
<td>Option</td>
<td>Administrator Changed Admin Password</td>
</tr>
<tr>
<td>Rule Name</td>
<td>Admin_Changed_Admin_Passwd</td>
</tr>
<tr>
<td>Severity</td>
<td>Warning</td>
</tr>
<tr>
<td>Event IDs</td>
<td>627, 628, 4723, 4724</td>
</tr>
<tr>
<td>Description</td>
<td>Detects that the administrator changed the administrator's own password.</td>
</tr>
</tbody>
</table>

### Table 6-24: Description of the Guest Changed Admin Password parameters used

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Option Path</td>
<td>System User and Group Change Monitor &gt; System User Configuration Changes</td>
</tr>
<tr>
<td>Option</td>
<td>Guest Changed Admin Password</td>
</tr>
<tr>
<td>Rule Name</td>
<td>Guest_Changed_Admin_Passwd</td>
</tr>
<tr>
<td>Severity</td>
<td>Critical</td>
</tr>
<tr>
<td>Event IDs</td>
<td>627, 628, 4723, 4724</td>
</tr>
<tr>
<td>Description</td>
<td>Detects that a guest changed the administrator password.</td>
</tr>
</tbody>
</table>

### Table 6-25: Description of the User Changed Admin Password parameters used

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Option Path</td>
<td>System User and Group Change Monitor &gt; System User Configuration Changes</td>
</tr>
<tr>
<td>Option</td>
<td>User Changed Admin Password</td>
</tr>
<tr>
<td>Rule Name</td>
<td>User_Changed_Admin_Passwd</td>
</tr>
<tr>
<td>Severity</td>
<td>Major</td>
</tr>
<tr>
<td>Event IDs</td>
<td>627, 628, 4723, 4724</td>
</tr>
<tr>
<td>Table 6-25</td>
<td>Description of the <strong>User Changed Admin Password</strong> parameters used (continued)</td>
</tr>
<tr>
<td>-------------</td>
<td>--------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Parameter</td>
<td>Description</td>
</tr>
<tr>
<td>Description</td>
<td>Detects that a user changed the administrator password.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Table 6-26</th>
<th>Description of the <strong>Administrator Changed Guest Password</strong> parameters used</th>
</tr>
</thead>
<tbody>
<tr>
<td>Parameter</td>
<td>Description</td>
</tr>
<tr>
<td>Option Path</td>
<td>System User and Group Change Monitor &gt; System User Configuration Changes</td>
</tr>
<tr>
<td>Option</td>
<td>Administrator Changed Guest Password</td>
</tr>
<tr>
<td>Rule Name</td>
<td>Admin_Changed_Guest_Passwd</td>
</tr>
<tr>
<td>Severity</td>
<td>Warning</td>
</tr>
<tr>
<td>Event IDs</td>
<td>627, 628, 4723, 4724</td>
</tr>
<tr>
<td>Description</td>
<td>Detects that the administrator changed the guest password.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Table 6-27</th>
<th>Description of the <strong>Guest Changed Guest Password</strong> parameters used</th>
</tr>
</thead>
<tbody>
<tr>
<td>Parameter</td>
<td>Description</td>
</tr>
<tr>
<td>Option Path</td>
<td>System User and Group Change Monitor &gt; System User Configuration Changes</td>
</tr>
<tr>
<td>Option</td>
<td>Guest Changed Guest Password</td>
</tr>
<tr>
<td>Rule Name</td>
<td>Guest_Changed_Guest_Passwd</td>
</tr>
<tr>
<td>Severity</td>
<td>Notice</td>
</tr>
<tr>
<td>Event IDs</td>
<td>627, 628, 4723, 4724</td>
</tr>
<tr>
<td>Description</td>
<td>Detects that the guest changed the guest password.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Table 6-28</th>
<th>Description of the <strong>User Changed Guest Password</strong> parameters used</th>
</tr>
</thead>
<tbody>
<tr>
<td>Parameter</td>
<td>Description</td>
</tr>
<tr>
<td>Option Path</td>
<td>System User and Group Change Monitor &gt; System User Configuration Changes</td>
</tr>
</tbody>
</table>
### Table 6-28
Description of the **User Changed Guest Password** parameters used

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Option</td>
<td>User Changed Guest Password</td>
</tr>
<tr>
<td>Rule Name</td>
<td>User_Changed_Guest_Passwd</td>
</tr>
<tr>
<td>Severity</td>
<td>Notice</td>
</tr>
<tr>
<td>Event IDs</td>
<td>627, 628, 4723, 4724</td>
</tr>
<tr>
<td>Description</td>
<td>Detects that a user changed the guest password.</td>
</tr>
</tbody>
</table>

### Table 6-29
Description of the **Administrator Changed User Password** parameters used

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Option Path</td>
<td>System User and Group Change Monitor &gt; System User Configuration Changes</td>
</tr>
<tr>
<td>Option</td>
<td>Administrator Changed User Password</td>
</tr>
<tr>
<td>Rule Name</td>
<td>Admin_Changed_User_Passwd</td>
</tr>
<tr>
<td>Severity</td>
<td>Notice</td>
</tr>
<tr>
<td>Event IDs</td>
<td>627, 628, 4723, 4724</td>
</tr>
<tr>
<td>Description</td>
<td>Detects that the administrator changed a user's password.</td>
</tr>
</tbody>
</table>

### Table 6-30
Description of the **Guest Changed User Password** parameters used

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Option Path</td>
<td>System User and Group Change Monitor &gt; System User Configuration Changes</td>
</tr>
<tr>
<td>Option</td>
<td>Guest Changed User Password</td>
</tr>
<tr>
<td>Rule Name</td>
<td>Guest_Changed_User_Passwd</td>
</tr>
<tr>
<td>Severity</td>
<td>Warning</td>
</tr>
<tr>
<td>Event IDs</td>
<td>627, 628, 4723, 4724</td>
</tr>
<tr>
<td>Description</td>
<td>Detects that the guest changed the user's password.</td>
</tr>
</tbody>
</table>
Table 6-31  Description of the **User Changed User Password** parameters used

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Option Path</td>
<td>System User and Group Change Monitor &gt; System User Configuration Changes</td>
</tr>
<tr>
<td>Option</td>
<td>User Changed User Password</td>
</tr>
<tr>
<td>Rule Name</td>
<td>User_Changed_User_Passwd</td>
</tr>
<tr>
<td>Severity</td>
<td>Notice</td>
</tr>
<tr>
<td>Event IDs</td>
<td>627, 628, 4723, 4724</td>
</tr>
<tr>
<td>Description</td>
<td>Detects that the user changed another user's password.</td>
</tr>
</tbody>
</table>

Table 6-32  Description of the **Administrator Changed Guest Password** parameters used

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Option Path</td>
<td>System User and Group Change Monitor &gt; System User Configuration Changes</td>
</tr>
<tr>
<td>Option</td>
<td>Administrator Changed Guest Password</td>
</tr>
<tr>
<td>Rule Name</td>
<td>Admin_Changed_Guest_Passwd</td>
</tr>
<tr>
<td>Severity</td>
<td>Notice</td>
</tr>
<tr>
<td>Event IDs</td>
<td>627, 628, 4723, 4724</td>
</tr>
<tr>
<td>Description</td>
<td>Detects that the administrator changed the guest password.</td>
</tr>
</tbody>
</table>

System group changes

This option group subsection detects group changes by monitoring the manipulation of the following groups:

- Global groups
- Local groups
- Universal groups
- Local distribution groups
- Global distribution groups
- Universal distribution groups
It monitors the security-relevant changes that warrant event detection.

Event detection includes administrator actions such as creation, change, or deletion of security-enabled local, global, or universal groups. Security groups allow the system administrator or domain administrator to establish a standard set of user permissions for application groups of users. Changes, additions, or deletions to the security groups are normal behavior in an extended enterprise if the system administrator actively manipulates these groups. If the system administrator or domain administrator does not actively manipulate security groups, these events can indicate illegitimate activity.

Table 6-33 Description of the Global Group Changed parameters used

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Option Path</td>
<td>System User and Group Change Monitor &gt; System Group Changes</td>
</tr>
<tr>
<td>Option</td>
<td>Global Group Changed</td>
</tr>
<tr>
<td>Rule Name</td>
<td>Global_Group_Changed</td>
</tr>
<tr>
<td>Severity</td>
<td>Information</td>
</tr>
<tr>
<td>Event IDs</td>
<td>641, 4737</td>
</tr>
<tr>
<td>Description</td>
<td>Detects that a global group was changed.</td>
</tr>
</tbody>
</table>

Table 6-34 Description of the Global Group Created parameters used

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Option Path</td>
<td>System User and Group Change Monitor &gt; System Group Changes</td>
</tr>
<tr>
<td>Option</td>
<td>Global Group Created</td>
</tr>
<tr>
<td>Rule Name</td>
<td>Global_Group_Created</td>
</tr>
<tr>
<td>Severity</td>
<td>Warning</td>
</tr>
<tr>
<td>Event IDs</td>
<td>631, 4727</td>
</tr>
<tr>
<td>Description</td>
<td>Detects that a global group was created.</td>
</tr>
</tbody>
</table>

Table 6-35 Description of the Global Group Deleted parameters used

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Option Path</td>
<td>System User and Group Change Monitor &gt; System Group Changes</td>
</tr>
<tr>
<td>Option</td>
<td>Global Group Deleted</td>
</tr>
</tbody>
</table>
### Table 6-35 Description of the **Global Group Deleted** parameters used (continued)

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Rule Name</td>
<td>Global_Group_Deleted</td>
</tr>
<tr>
<td>Severity</td>
<td>Warning</td>
</tr>
<tr>
<td>Event IDs</td>
<td>634, 4730</td>
</tr>
<tr>
<td>Description</td>
<td>Detects that a global group was deleted.</td>
</tr>
</tbody>
</table>

### Table 6-36 Description of the **Local Group Changed** parameters used

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Option Path</td>
<td>System User and Group Change Monitor &gt; System Group Changes</td>
</tr>
<tr>
<td>Option</td>
<td>Local Group Changed</td>
</tr>
<tr>
<td>Rule Name</td>
<td>Local_Group_Changed</td>
</tr>
<tr>
<td>Severity</td>
<td>Info</td>
</tr>
<tr>
<td>Event IDs</td>
<td>639, 4735</td>
</tr>
<tr>
<td>Description</td>
<td>Detects that a local group was changed.</td>
</tr>
</tbody>
</table>

### Table 6-37 Description of the **Local Group Created** parameters used

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Option Path</td>
<td>System User and Group Change Monitor &gt; System Group Changes</td>
</tr>
<tr>
<td>Option</td>
<td>Local Group Created</td>
</tr>
<tr>
<td>Rule Name</td>
<td>Local_Group_Created</td>
</tr>
<tr>
<td>Severity</td>
<td>Warning</td>
</tr>
<tr>
<td>Event IDs</td>
<td>635, 4731</td>
</tr>
<tr>
<td>Description</td>
<td>Detects that a local group was created.</td>
</tr>
</tbody>
</table>

### Table 6-38 Description of the **Local Group Deleted** parameters used

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Option Path</td>
<td>System User and Group Change Monitor &gt; System Group Changes</td>
</tr>
<tr>
<td>Option</td>
<td></td>
</tr>
<tr>
<td>Rule Name</td>
<td></td>
</tr>
<tr>
<td>Severity</td>
<td></td>
</tr>
<tr>
<td>Event IDs</td>
<td></td>
</tr>
<tr>
<td>Description</td>
<td></td>
</tr>
</tbody>
</table>
Table 6-38  Description of the **Local Group Deleted** parameters used *(continued)*

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Option</td>
<td>Local Group Deleted</td>
</tr>
<tr>
<td>Rule Name</td>
<td>Local_Group_Deleted</td>
</tr>
<tr>
<td>Severity</td>
<td>Warning</td>
</tr>
<tr>
<td>Event IDs</td>
<td>638, 4734</td>
</tr>
<tr>
<td>Description</td>
<td>Detects that a local group was deleted.</td>
</tr>
</tbody>
</table>

Table 6-39  Description of the **Universal Group Changed** parameters used

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Option Path</td>
<td>System User and Group Change Monitor &gt; System Group Changes</td>
</tr>
<tr>
<td>Option</td>
<td>Universal Group Changed</td>
</tr>
<tr>
<td>Rule Name</td>
<td>Universal_Group_Changed</td>
</tr>
<tr>
<td>Severity</td>
<td>Info</td>
</tr>
<tr>
<td>Event IDs</td>
<td>659, 4755</td>
</tr>
<tr>
<td>Description</td>
<td>Detects that a universal group was changed.</td>
</tr>
</tbody>
</table>

Table 6-40  Description of the **Universal Group Created** parameters used

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Option Path</td>
<td>System User and Group Change Monitor &gt; System Group Changes</td>
</tr>
<tr>
<td>Option</td>
<td>Universal Group Created</td>
</tr>
<tr>
<td>Rule Name</td>
<td>Universal_Group_Created</td>
</tr>
<tr>
<td>Severity</td>
<td>Warning</td>
</tr>
<tr>
<td>Event IDs</td>
<td>658 4754</td>
</tr>
<tr>
<td>Description</td>
<td>Detects that a universal group was created.</td>
</tr>
</tbody>
</table>

Table 6-41  Description of the **Universal Group Deleted** parameters used

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Option Path</td>
<td>System User and Group Change Monitor &gt; System Group Changes</td>
</tr>
</tbody>
</table>
### Table 6-41
Description of the **Universal Group Deleted** parameters used (continued)

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Option</td>
<td>Universal Group Deleted</td>
</tr>
<tr>
<td>Rule Name</td>
<td>Universal_Group_Deleted</td>
</tr>
<tr>
<td>Severity</td>
<td>Warning</td>
</tr>
<tr>
<td>Event IDs</td>
<td>662, 4758</td>
</tr>
<tr>
<td>Description</td>
<td>Detects that a universal group was deleted.</td>
</tr>
</tbody>
</table>

### Table 6-42
Description of the **Local Distribution Group Created** parameters used

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Option Path</td>
<td>System User and Group Change Monitor &gt; System Group Changes</td>
</tr>
<tr>
<td>Option</td>
<td>Local Distribution Group Created</td>
</tr>
<tr>
<td>Rule Name</td>
<td>Local_Distribution_Grp_Created</td>
</tr>
<tr>
<td>Severity</td>
<td>Warning</td>
</tr>
<tr>
<td>Event IDs</td>
<td>648, 4744</td>
</tr>
<tr>
<td>Description</td>
<td>Detects when a local distribution group was created. The distribution lists</td>
</tr>
<tr>
<td></td>
<td>can be created and managed through Active Directory MMC. Local distribution</td>
</tr>
<tr>
<td></td>
<td>groups can include other groups and accounts from Windows Server 2003,</td>
</tr>
<tr>
<td></td>
<td>Windows 2000, or Windows NT domains, and can be granted permissions only</td>
</tr>
<tr>
<td></td>
<td>within a domain.</td>
</tr>
</tbody>
</table>

### Table 6-43
Description of the **Local Distribution Group Changed** parameters used

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Option Path</td>
<td>System User and Group Change Monitor &gt; System Group Changes</td>
</tr>
<tr>
<td>Option</td>
<td>Local Distribution Group Changed</td>
</tr>
<tr>
<td>Rule Name</td>
<td>Local_Distribution_Grp_Changed</td>
</tr>
<tr>
<td>Severity</td>
<td>Warning</td>
</tr>
<tr>
<td>Event IDs</td>
<td>649, 4745</td>
</tr>
<tr>
<td>Parameter</td>
<td>Description</td>
</tr>
<tr>
<td>-----------</td>
<td>-------------</td>
</tr>
<tr>
<td>Description</td>
<td>Detects when a local distribution group was changed.</td>
</tr>
</tbody>
</table>

### Table 6-44 Description of the Local Distribution Group Deleted parameters used

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Option Path</td>
<td>System User and Group Change Monitor &gt; System Group Changes</td>
</tr>
<tr>
<td>Option</td>
<td>Local Distribution Group Deleted</td>
</tr>
<tr>
<td>Rule Name</td>
<td>Local_Distribution_Grp_Delete</td>
</tr>
<tr>
<td>Severity</td>
<td>Warning</td>
</tr>
<tr>
<td>Event IDs</td>
<td>652, 4748</td>
</tr>
<tr>
<td>Description</td>
<td>Detects when a local distribution group was deleted.</td>
</tr>
</tbody>
</table>

### Table 6-45 Description of the Global Distribution Group Created parameters used

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Option Path</td>
<td>System User and Group Change Monitor &gt; System Group Changes</td>
</tr>
<tr>
<td>Option</td>
<td>Global Distribution Group Created</td>
</tr>
<tr>
<td>Rule Name</td>
<td>Global_Distribution_Grp_Created</td>
</tr>
<tr>
<td>Severity</td>
<td>Warning</td>
</tr>
<tr>
<td>Event IDs</td>
<td>653, 4749</td>
</tr>
<tr>
<td>Description</td>
<td>Detects when a global distribution group was created. The distribution lists can be created and managed through Active Directory MMC. Local distribution groups can include other groups and accounts only from the domain in which the group is defined. They can be granted permissions in any domain in the forest.</td>
</tr>
</tbody>
</table>
**Table 6-46**  Description of the **Global Distribution Group Changed** parameters used

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Option Path</td>
<td>System User and Group Change Monitor &gt; System Group Changes</td>
</tr>
<tr>
<td>Option</td>
<td>Global Distribution Group Changed</td>
</tr>
<tr>
<td>Rule Name</td>
<td>Global_Distribution_Grp_Changed</td>
</tr>
<tr>
<td>Severity</td>
<td>Warning</td>
</tr>
<tr>
<td>Event IDs</td>
<td>654, 4750</td>
</tr>
<tr>
<td>Description</td>
<td>Detects when a global distribution group was changed.</td>
</tr>
</tbody>
</table>

**Table 6-47**  Description of the **Global Distribution Group Deleted** parameters used

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Option Path</td>
<td>System User and Group Change Monitor &gt; System Group Changes</td>
</tr>
<tr>
<td>Option</td>
<td>Global Distribution Group Deleted</td>
</tr>
<tr>
<td>Rule Name</td>
<td>Global_Distribution_Grp_Deleted</td>
</tr>
<tr>
<td>Severity</td>
<td>Warning</td>
</tr>
<tr>
<td>Event IDs</td>
<td>657, 4753</td>
</tr>
<tr>
<td>Description</td>
<td>Detects when a global distribution group was deleted.</td>
</tr>
</tbody>
</table>

**Table 6-48**  Description of the **Universal Distribution Group Created** parameters used

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Option Path</td>
<td>System User and Group Change Monitor &gt; System Group Changes</td>
</tr>
<tr>
<td>Option</td>
<td>Universal Distribution Group Created</td>
</tr>
<tr>
<td>Rule Name</td>
<td>Univ_Distribution_Grp_Created</td>
</tr>
<tr>
<td>Severity</td>
<td>Warning</td>
</tr>
<tr>
<td>Event IDs</td>
<td>663, 4759</td>
</tr>
</tbody>
</table>
### Table 6-48 Description of the Universal Distribution Group Created parameters used (continued)

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Description</td>
<td>Detects when a universal distribution group was created. The distribution lists can be created and managed through Active Directory MMC. Universal distribution groups can include other groups and accounts from any domain in the domain tree or forest. They can be granted permissions in any domain in the domain tree or forest.</td>
</tr>
</tbody>
</table>

### Table 6-49 Description of the Universal Distribution Group Changed parameters used

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Option Path</td>
<td>System User and Group Change Monitor &gt; System Group Changes</td>
</tr>
<tr>
<td>Option</td>
<td>Universal Distribution Group Changed</td>
</tr>
<tr>
<td>Rule Name</td>
<td>Univ_Distribution_Grp_Changed</td>
</tr>
<tr>
<td>Severity</td>
<td>Warning</td>
</tr>
<tr>
<td>Event IDs</td>
<td>664, 4760</td>
</tr>
<tr>
<td>Description</td>
<td>Detects when a universal distribution group was changed.</td>
</tr>
</tbody>
</table>

### Table 6-50 Description of the Universal Distribution Group Deleted parameters used

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Option Path</td>
<td>System User and Group Change Monitor &gt; System Group Changes</td>
</tr>
<tr>
<td>Option</td>
<td>Universal Distribution Group Deleted</td>
</tr>
<tr>
<td>Rule Name</td>
<td>Univ_Distribution_Grp_Deleted</td>
</tr>
<tr>
<td>Severity</td>
<td>Warning</td>
</tr>
<tr>
<td>Event IDs</td>
<td>667, 4763</td>
</tr>
<tr>
<td>Description</td>
<td>Detects when a universal distribution group was deleted.</td>
</tr>
</tbody>
</table>

## System Active Directory Change Monitor

This option group section of the policy monitors specific Active Directory-based events. These events include potentially suspicious domain trust events, FSMO
changes, and authentication or encryption configuration changes. These events may be indicative of malicious configuration, which may affect the Active Directory system itself, as well as downstream systems.

Active directory domain trust configuration

This portion of the policy detects the creation or removal of a trusted domain relationship and changes to the Windows Domain Policy. Domain Trust relationships allow multiple Windows domains to share resources. They also allow users from one domain to log on and interact as trusted users in a foreign domain. Creation or removal of trusted domain relationships is expected behavior in extended enterprises. If this behavior is unexpected, it could indicate a serious security compromise at the domain level. Configuration: Settings > Control Panel > Administrative Tools > Local Security Policy > Security Settings > Local Policies > Audit Policy > Audit account management for success and failure, Audit policy change for success or failure.

Table 6-51 Description of the Trusted Domain Created parameters used

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Option Path</td>
<td>System Active Directory Change Monitor &gt; Active Directory Domain Trust Configuration</td>
</tr>
<tr>
<td>Option</td>
<td>Trusted Domain Created</td>
</tr>
<tr>
<td>Rule Name</td>
<td>Trusteded_Domain_Created</td>
</tr>
<tr>
<td>Severity</td>
<td>Warning</td>
</tr>
<tr>
<td>Event IDs</td>
<td>610, 4706</td>
</tr>
<tr>
<td>Description</td>
<td>Detects the creation of a trusted domain relationship with the primary domain controller.</td>
</tr>
</tbody>
</table>

Table 6-52 Description of the Domain Policy Changed parameters used

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Option Path</td>
<td>System Active Directory Change Monitor &gt; Active Directory Domain Trust Configuration</td>
</tr>
<tr>
<td>Option</td>
<td>Domain Policy Changed</td>
</tr>
<tr>
<td>Rule Name</td>
<td>Domain_Policy_Changed</td>
</tr>
<tr>
<td>Severity</td>
<td>Warning</td>
</tr>
</tbody>
</table>
Table 6-52  Description of the **Domain Policy Changed** parameters used (continued)

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Event IDs</td>
<td>643, 4739</td>
</tr>
<tr>
<td>Description</td>
<td>Detects all Windows Domain Policy changes.</td>
</tr>
</tbody>
</table>

Table 6-53  Description of the **Trusted Domain Changed** parameters used

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Option Path</td>
<td>System Active Directory Change Monitor &gt; Active Directory Domain Trust Configuration</td>
</tr>
<tr>
<td>Option</td>
<td>Trusted Domain Changed</td>
</tr>
<tr>
<td>Rule Name</td>
<td>Trusted_Domain_Changed</td>
</tr>
<tr>
<td>Severity</td>
<td>Warning</td>
</tr>
<tr>
<td>Event IDs</td>
<td>620, 4716</td>
</tr>
<tr>
<td>Description</td>
<td>Detects the modification of the trusted domain information.</td>
</tr>
</tbody>
</table>

Table 6-54  Description of the **Trusted Domain Removed** parameters used

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Option Path</td>
<td>System Active Directory Change Monitor &gt; Active Directory Domain Trust Configuration</td>
</tr>
<tr>
<td>Option</td>
<td>Trusted Domain Removed</td>
</tr>
<tr>
<td>Rule Name</td>
<td>Trusted_Domain_Removed</td>
</tr>
<tr>
<td>Severity</td>
<td>Warning</td>
</tr>
<tr>
<td>Event IDs</td>
<td>611, 4707</td>
</tr>
<tr>
<td>Description</td>
<td>Detects the removal of a trusted domain relationship from the primary domain controller.</td>
</tr>
</tbody>
</table>

**Active directory FSMO changes**

This option group sub-section monitors changes to Active Directory’s Flexible Single Master of Operation (FSMO). Changes to Schema Master, Domain Master, RID Master, PDCEmulator, and Infrastructure Master are critical functions of Active
Directory that should be monitored. Changes to these settings outside normal administrative tasks can indicate illegitimate activity.

### Table 6-55  
**Description of the Schema Master Changed parameters used**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Option Path</td>
<td>System Active Directory Change Monitor &gt; Active Directory FSMO Changes</td>
</tr>
<tr>
<td>Option</td>
<td>Schema Master Changed</td>
</tr>
<tr>
<td>Rule Name</td>
<td>Schema_Master_Changed</td>
</tr>
<tr>
<td>Severity</td>
<td>Warning</td>
</tr>
<tr>
<td>Event IDs</td>
<td>565, 566, 4661, 4662</td>
</tr>
<tr>
<td>Description</td>
<td>Detects a change to the Active Directory FSMO schema master role.</td>
</tr>
</tbody>
</table>

### Table 6-56  
**Description of the Domain Master Changed parameters used**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Option Path</td>
<td>System Active Directory Change Monitor &gt; Active Directory FSMO Changes</td>
</tr>
<tr>
<td>Option</td>
<td>Domain Master Changed</td>
</tr>
<tr>
<td>Rule Name</td>
<td>Domain_Master_Changed</td>
</tr>
<tr>
<td>Severity</td>
<td>Warning</td>
</tr>
<tr>
<td>Event IDs</td>
<td>565, 566, 4661, 4662</td>
</tr>
<tr>
<td>Description</td>
<td>Detects a change to the Active Directory FSMO domain master role.</td>
</tr>
</tbody>
</table>

### Table 6-57  
**Description of the RID Master Changed parameters used**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Option Path</td>
<td>System Active Directory Change Monitor &gt; Active Directory FSMO Changes</td>
</tr>
<tr>
<td>Option</td>
<td>RID Master Changed</td>
</tr>
<tr>
<td>Rule Name</td>
<td>RID_Master_Changed</td>
</tr>
<tr>
<td>Severity</td>
<td>Warning</td>
</tr>
<tr>
<td>Event IDs</td>
<td>565, 566, 4661, 4662</td>
</tr>
</tbody>
</table>
Table 6-57 Description of the **RID Master Changed** parameters used (continued)

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Description</td>
<td>Detects a change to the Active Directory FSMO RID master role.</td>
</tr>
</tbody>
</table>

Table 6-58 Description of the **PDCEmulator Changed** parameters used

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Option Path</td>
<td>System Active Directory Change Monitor &gt; Active Directory FSMO Changes</td>
</tr>
<tr>
<td>Option</td>
<td>PDCEmulator Changed</td>
</tr>
<tr>
<td>Rule Name</td>
<td>PDCEmulator_Changed</td>
</tr>
<tr>
<td>Severity</td>
<td>Warning</td>
</tr>
<tr>
<td>Event IDs</td>
<td>565, 566, 4661, 4662</td>
</tr>
<tr>
<td>Description</td>
<td>Detects a change to the Active Directory FSMO PDCEmulator.</td>
</tr>
</tbody>
</table>

Table 6-59 Description of the **Infrastructure Master Changed** parameters used

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Option Path</td>
<td>System Active Directory Change Monitor &gt; Active Directory FSMO Changes</td>
</tr>
<tr>
<td>Option</td>
<td>Infrastructure Master Changed</td>
</tr>
<tr>
<td>Rule Name</td>
<td>Infrastructure_Changed</td>
</tr>
<tr>
<td>Severity</td>
<td>Warning</td>
</tr>
<tr>
<td>Event IDs</td>
<td>565, 566, 4661, 4662</td>
</tr>
<tr>
<td>Description</td>
<td>Detects a change to the Active Directory FSMO Infrastructure Master.</td>
</tr>
</tbody>
</table>

**Authentication and encryption configuration**

This option group sub-section detects normal Active Directory authentication activity as well as changes to Windows Active Directory authentication and encryption settings. Changes to these settings are normally necessary to allow non-Windows clients to access the domain. Windows writes the events to event logs, and Symantec Data Center Security: Server Advanced monitors the registry keys or Event IDs.
### Table 6-60  Description of the Authentication Packages Changed parameters used

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Option Path</td>
<td>System Active Directory Change Monitor &gt; Authentication and Encryption Configuration</td>
</tr>
<tr>
<td>Option</td>
<td>Authentication Packages Changed</td>
</tr>
<tr>
<td>Rule Name</td>
<td>Authentication_Packages_Changed</td>
</tr>
<tr>
<td>Severity</td>
<td>Warning</td>
</tr>
<tr>
<td>Registry Paths</td>
<td>%HKEY_LOCAL_MACHINE\SYSTEM*ControlSet\Control\Lsa\Authentication Packages</td>
</tr>
<tr>
<td>Description</td>
<td>Detects the changes to the Windows authentication packages, according to the registry settings monitored.</td>
</tr>
</tbody>
</table>

### Table 6-61  Description of the Auth Ticket Request Failure parameters used

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Option Path</td>
<td>System Active Directory Change Monitor &gt; Authentication and Encryption Configuration</td>
</tr>
<tr>
<td>Option</td>
<td>Auth Ticket Request Failure</td>
</tr>
<tr>
<td>Rule Name</td>
<td>Auth_Ticket_Request_Failure</td>
</tr>
<tr>
<td>Severity</td>
<td>Notice</td>
</tr>
<tr>
<td>Event IDs</td>
<td>676, 672, 4772, 4768</td>
</tr>
<tr>
<td>Description</td>
<td>Detects the failure of Windows to receive an authentication ticket on request by Active Directory.</td>
</tr>
</tbody>
</table>

### Table 6-62  Description of the EnableSecuritySignature Changed parameters used

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Option Path</td>
<td>System Active Directory Change Monitor &gt; Authentication and Encryption Configuration</td>
</tr>
<tr>
<td>Option</td>
<td>EnableSecuritySignature Changed</td>
</tr>
<tr>
<td>Rule Name</td>
<td>EnableSecuritySignature_Changed</td>
</tr>
<tr>
<td>Severity</td>
<td>Warning</td>
</tr>
<tr>
<td>Parameter</td>
<td>Description</td>
</tr>
<tr>
<td>-----------</td>
<td>-------------</td>
</tr>
<tr>
<td>Registry Paths</td>
<td><code>\HKEY_LOCAL_MACHINE\SYSTEM\*ControlSet*\Services\LanMan\Parameters\EnableSecuritySignature</code></td>
</tr>
<tr>
<td>Description</td>
<td>Detects the changes to the Windows Security Signature state.</td>
</tr>
</tbody>
</table>

**Table 6-63** Description of the **Kerberos Ticket Request Failed** parameters used

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Option Path</td>
<td>System Active Directory Change Monitor &gt; Authentication and Encryption Configuration</td>
</tr>
<tr>
<td>Option</td>
<td>Kerberos Ticket Request Failed</td>
</tr>
<tr>
<td>Rule Name</td>
<td>Kerberos_Service_Ticket_Request_Failed</td>
</tr>
<tr>
<td>Severity</td>
<td>Notice</td>
</tr>
<tr>
<td>Event IDs</td>
<td>677, 673, 4773, 4769</td>
</tr>
<tr>
<td>Description</td>
<td>Detects the failure of Windows to be granted with a Kerberos service ticket on request by an Active Directory server. This failure may happen while satisfactory security credentials are negotiated between the clients and the Active Directory server. This failure can also indicate that an untrusted client has attempted to access the resources in this Active Directory domain.</td>
</tr>
</tbody>
</table>

**Table 6-64** Description of the **LMCompatibilityLevel Changed** parameters used

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Option Path</td>
<td>System Active Directory Change Monitor &gt; Authentication and Encryption Configuration</td>
</tr>
<tr>
<td>Option</td>
<td>LMCompatibilityLevel_Changed</td>
</tr>
<tr>
<td>Rule Name</td>
<td>LMCompatibilityLevel_Changed</td>
</tr>
<tr>
<td>Severity</td>
<td>Warning</td>
</tr>
<tr>
<td>Registry Paths</td>
<td><code>\HKEY_LOCAL_MACHINE\SYSTEM\*ControlSet*\Control\Lsa\Lmcompatibilitylevel</code></td>
</tr>
</tbody>
</table>
### Table 6-64  
Description of the **LMCompatibilityLevel Changed** parameters used (continued)

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Description</td>
<td>Detects the failure of Windows to be granted with a Kerberos service ticket on request by an Active Directory server. This failure may happen while satisfactory security credentials are negotiated between the clients and the Active Directory server. This failure can also indicate that an untrusted client has attempted to access the resources in this Active Directory domain.</td>
</tr>
</tbody>
</table>

### Table 6-65  
Description of the **NotificationPackages Changed** parameters used

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Option Path</td>
<td>System Active Directory Change Monitor &gt; Authentication and Encryption Configuration</td>
</tr>
<tr>
<td>Option</td>
<td>NotificationPackages Changed</td>
</tr>
<tr>
<td>Rule Name</td>
<td>NotificationPackages_Changed</td>
</tr>
<tr>
<td>Severity</td>
<td>Warning</td>
</tr>
<tr>
<td>Registry Paths</td>
<td><code>\HKEY_LOCAL_MACHINE\SYSTEM\ControlSet\Control\Lsa\Notification Packages</code></td>
</tr>
<tr>
<td>Description</td>
<td>Detects the changes in the state of the Windows Local Security Authority Notification Packages.</td>
</tr>
</tbody>
</table>

### Table 6-66  
Description of the **Pre Authentication Failure** parameters used

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Option Path</td>
<td>System Active Directory Change Monitor &gt; Authentication and Encryption Configuration</td>
</tr>
<tr>
<td>Option</td>
<td>Pre Authentication Failure</td>
</tr>
<tr>
<td>Rule Name</td>
<td>Pre_Authentication_Failure</td>
</tr>
<tr>
<td>Severity</td>
<td>Warning</td>
</tr>
<tr>
<td>Event IDs</td>
<td>675, 4771</td>
</tr>
</tbody>
</table>
### Table 6-66

Description of the **Pre Authentication Failure** parameters used (continued)

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Description</td>
<td>Detects the failure of Windows to pre-authenticate with Active Directory. This event happens while satisfactory security credentials are negotiated between the clients and Active Directory server. This detection can also indicate that an untrusted client has attempted to access the resources in this Active Directory domain.</td>
</tr>
</tbody>
</table>

### Table 6-67

Description of the **RequireSecureSign Changed** parameters used

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Option Path</td>
<td>System Active Directory Change Monitor &gt; Authentication and Encryption Configuration</td>
</tr>
<tr>
<td>Option</td>
<td>RequireSecureSign Changed</td>
</tr>
<tr>
<td>Rule Name</td>
<td>RequireSecureSign_Changed</td>
</tr>
<tr>
<td>Severity</td>
<td>Warning</td>
</tr>
<tr>
<td>Registry Paths</td>
<td><code>\HKEY_LOCAL_MACHINE\SYSTEM\*ControlSet\*\Services\LanMan\*\Parameters\RequireSecuritySignature</code></td>
</tr>
<tr>
<td>Description</td>
<td>Detects the changes in the Windows Lan Manager Security Signature requirement.</td>
</tr>
</tbody>
</table>

### Table 6-68

Description of the **RestrictNullSessAccess Changed** parameters used

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Option Path</td>
<td>System Active Directory Change Monitor &gt; Authentication and Encryption Configuration</td>
</tr>
<tr>
<td>Option</td>
<td>RestrictNullSessAccess Changed</td>
</tr>
<tr>
<td>Rule Name</td>
<td>RestrictNullSessAccess_Changed</td>
</tr>
<tr>
<td>Severity</td>
<td>Warning</td>
</tr>
<tr>
<td>Registry Paths</td>
<td><code>\HKEY_LOCAL_MACHINE\SYSTEM\*ControlSet\*\Services\LanmanServer\Parameters\RestrictNullSessAccess</code></td>
</tr>
<tr>
<td>Description</td>
<td>Detects the changes in the Windows Null Session Access restrictions.</td>
</tr>
</tbody>
</table>
### Table 6-69  Description of the **Authentication Ticket Granted** parameters used

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Option Path</td>
<td>System Active Directory Change Monitor &gt; Authentication and Encryption Configuration</td>
</tr>
<tr>
<td>Option</td>
<td>Authentication Ticket Granted</td>
</tr>
<tr>
<td>Rule Name</td>
<td>Authentication_Ticket_Granted</td>
</tr>
<tr>
<td>Severity</td>
<td>Notice</td>
</tr>
<tr>
<td>Event IDs</td>
<td>672, 4768</td>
</tr>
<tr>
<td>Description</td>
<td>Detects when an Active Directory server grants an authentication ticket to a computer that runs Windows. This behavior is normal and often indicates that a domain user has logged on to a Windows client.</td>
</tr>
</tbody>
</table>

### Table 6-70  Description of the **Kerberos Policy Changed** parameters used

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Option Path</td>
<td>System Active Directory Change Monitor &gt; Authentication and Encryption Configuration</td>
</tr>
<tr>
<td>Option</td>
<td>Kerberos Policy Changed</td>
</tr>
<tr>
<td>Rule Name</td>
<td>Kerberos_Policy_Changed</td>
</tr>
<tr>
<td>Severity</td>
<td>Notice</td>
</tr>
<tr>
<td>Event IDs</td>
<td>617, 4713</td>
</tr>
</tbody>
</table>
| Description        | Detects the updates to the Kerberos authentication policy. This normal activity occurs at 5-minute intervals when the domain group policy object is updated every 16 hours, regardless of the following items:  
  - Policy object status  
  - When the group policies are manually propagated |

### Table 6-71  Description of the **Kerberos Service Ticket Granted** parameters used

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Option Path</td>
<td>System Active Directory Change Monitor &gt; Authentication and Encryption Configuration</td>
</tr>
<tr>
<td>Option</td>
<td>Kerberos Service Ticket Granted</td>
</tr>
</tbody>
</table>
Table 6-71 Description of the **Kerberos Service Ticket Granted** parameters used (continued)

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Rule Name</td>
<td>Kerberos_Service_Ticket_Granted</td>
</tr>
<tr>
<td>Severity</td>
<td>Notice</td>
</tr>
<tr>
<td>Event IDs</td>
<td>673, 4769</td>
</tr>
<tr>
<td>Description</td>
<td>Detects the grant of a Kerberos service ticket to Windows by Active Directory. This event indicates that a client has been granted permission to interact in this Active Directory domain.</td>
</tr>
</tbody>
</table>

Table 6-72 Description of the **Trusted Logon Process Register** parameters used

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Option Path</td>
<td>System Active Directory Change Monitor &gt; Authentication and Encryption Configuration</td>
</tr>
<tr>
<td>Option</td>
<td>Trusted Logon Process Register</td>
</tr>
<tr>
<td>Rule Name</td>
<td>Trusted_Logon_Process_Register</td>
</tr>
<tr>
<td>Severity</td>
<td>Notice</td>
</tr>
<tr>
<td>Event IDs</td>
<td>515, 4611</td>
</tr>
<tr>
<td>Description</td>
<td>Detects the Windows registration of a trusted logon process to the Local Security Authority.</td>
</tr>
</tbody>
</table>

Table 6-73 Description of the **Encrypted Data Policy Change** parameters used

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Option Path</td>
<td>System Active Directory Change Monitor &gt; Authentication and Encryption Configuration</td>
</tr>
<tr>
<td>Option</td>
<td>Encrypted Data Policy Change</td>
</tr>
<tr>
<td>Rule Name</td>
<td>Encrypted_Data_Policy_Change</td>
</tr>
<tr>
<td>Severity</td>
<td>Notice</td>
</tr>
<tr>
<td>Event IDs</td>
<td>618, 4714</td>
</tr>
<tr>
<td>Description</td>
<td>Detects the changes to the encrypted data recovery policy.</td>
</tr>
<tr>
<td>Parameter</td>
<td>Description</td>
</tr>
<tr>
<td>--------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Option Path</td>
<td>System Active Directory Change Monitor &gt; Authentication and Encryption Configuration</td>
</tr>
<tr>
<td>Option</td>
<td>Quality Service Policy Changes</td>
</tr>
<tr>
<td>Rule Name</td>
<td>Quality_Service_Policy_Changed</td>
</tr>
<tr>
<td>Severity</td>
<td>Notice</td>
</tr>
<tr>
<td>Event IDs</td>
<td>619, 4715</td>
</tr>
<tr>
<td>Description</td>
<td>Detects the changes to the quality of service policy.</td>
</tr>
</tbody>
</table>

**System login activity and access monitor**

This option group section of the policy monitors the system access activity that may indicate illegitimate activity. Portions of this section also monitor the successful logon attempts of individuals through various means. These monitoring areas can be used for the following tasks:

- To acquire a timeline of when an individual logon to a specific system has occurred.
- To detect other suspicious system access activity.
- To alert on brute force password attempts.

**System login success monitor**

This option group subsection monitors for successful logons by using various means of remote desktop, FTP, and logon attempts based on user-defined non-working hours. You can match these rules with System Logoff Monitoring to formulate a time line of individual logon activity.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Option Path</td>
<td>System Login Activity and Access Monitor &gt; System Login Success Monitor</td>
</tr>
<tr>
<td>Option</td>
<td>Account Used for Logon</td>
</tr>
<tr>
<td>Rule Name</td>
<td>System_Logon_Success_Account_Used_for_Logon</td>
</tr>
</tbody>
</table>
Table 6-75  Description of the **Account Used for Logon** parameters used

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Severity</td>
<td>Notice</td>
</tr>
<tr>
<td>Event IDs</td>
<td>680, 4776</td>
</tr>
<tr>
<td>Description</td>
<td>Detects the account that was used for the logon. You can configure the Windows Security Policy auditing system to monitor the status of the logon attempts. When the Windows Security Policy auditing system determines that an account has been used to log on, it reports this event.</td>
</tr>
</tbody>
</table>

Table 6-76  Description of the **by Admin to Desktop** parameters used

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Option Path</td>
<td>System Login Activity and Access Monitor &gt; System Login Success Monitor</td>
</tr>
<tr>
<td>Option</td>
<td>by Admin to Desktop</td>
</tr>
<tr>
<td>Rule Name</td>
<td>System_Logon_Success_by_Admin_to_Desktop</td>
</tr>
<tr>
<td>Severity</td>
<td>Notice</td>
</tr>
<tr>
<td>Event IDs</td>
<td>528, 4624</td>
</tr>
<tr>
<td>Description</td>
<td>Detects a successful administrator logon to a system's desktop, including local and terminal service logons. You can configure the Windows Security Policy auditing system to monitor the status of logon attempts. When the Windows Security Policy auditing system determines that an administrator successfully logged on, it reports this event.</td>
</tr>
</tbody>
</table>

Table 6-77  Description of the **by Admin via Remote Connection** parameters used

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Option Path</td>
<td>System Login Activity and Access Monitor &gt; System Login Success Monitor</td>
</tr>
<tr>
<td>Option</td>
<td>by Admin via Remote Connection</td>
</tr>
<tr>
<td>Rule Name</td>
<td>Successful_Login_Admin_via_Remote_Connection</td>
</tr>
<tr>
<td>Severity</td>
<td>Notice</td>
</tr>
</tbody>
</table>
Table 6-77  Description of the **by Admin via Remote Connection** parameters used (continued)

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Event IDs</td>
<td>528, 540, 4624</td>
</tr>
<tr>
<td>Description</td>
<td>Detects a successful administrator logon from a shared network resource, for example, IIS, FTP, or Telnet. You can configure the Windows Security Policy auditing system to monitor the status of the logon attempts. When the Windows Security Policy auditing system determines that an administrator successfully logged on from a remote connection, it reports this event.</td>
</tr>
</tbody>
</table>

Table 6-78  Description of the **by Anonymous to IIS or FTP** parameters used

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Option Path</td>
<td>System Login Activity and Access Monitor &gt; System Login Success Monitor</td>
</tr>
<tr>
<td>Option</td>
<td>by Anonymous to IIS or FTP</td>
</tr>
<tr>
<td>Rule Name</td>
<td>Successful_Login_Anon_to_IIS_or_FTP</td>
</tr>
<tr>
<td>Severity</td>
<td>Notice</td>
</tr>
<tr>
<td>Event IDs</td>
<td>528, 540, 4624, 4636</td>
</tr>
<tr>
<td>Description</td>
<td>Detects a successful anonymous access by IIS or FTP. This rule triggers only during the initial access to the Web site by any browser. If Web traffic is sporadic, the inactive connection time expires the logon.</td>
</tr>
</tbody>
</table>

Table 6-79  Description of the **by Guest to Desktop** parameters used

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Option Path</td>
<td>System Login Activity and Access Monitor &gt; System Login Success Monitor</td>
</tr>
<tr>
<td>Option</td>
<td>by Guest to Desktop</td>
</tr>
<tr>
<td>Rule Name</td>
<td>Successful_Login_Guest_to_Desktop</td>
</tr>
<tr>
<td>Severity</td>
<td>Notice</td>
</tr>
<tr>
<td>Event IDs</td>
<td>528, 4624</td>
</tr>
</tbody>
</table>
### Table 6-79 Description of the by Guest to Desktop parameters used (continued)

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Description</strong></td>
<td>Detects a successful guest logon to a system's desktop. This detection includes local logons and terminal service logons. You can configure the Windows Security Policy auditing system to monitor the status of the logon attempts. When the Windows Security Policy auditing system determines that a guest successfully logged on, it reports this event.</td>
</tr>
</tbody>
</table>

### Table 6-80 Description of the by Guest via Remote Connection parameters used

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Option Path</strong></td>
<td>System Login Activity and Access Monitor &gt; System Login Success Monitor</td>
</tr>
<tr>
<td><strong>Option</strong></td>
<td>by Guest via Remote Connection</td>
</tr>
<tr>
<td><strong>Rule Name</strong></td>
<td>Successful_Login_Guest_via_Remote_Connection</td>
</tr>
<tr>
<td><strong>Severity</strong></td>
<td>Notice</td>
</tr>
<tr>
<td><strong>Event IDs</strong></td>
<td>528, 540, 4624, 4636</td>
</tr>
<tr>
<td><strong>Description</strong></td>
<td>Detects a successful guest logon by a shared network resource, for example, IIS, FTP, or Telnet. You can configure the Windows Security Policy auditing system to monitor the status of the logon attempts. When it determines that a guest successfully logged on by a remote connection, it reports this event</td>
</tr>
</tbody>
</table>

### Table 6-81 Description of the by User to Desktop parameters used

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Option Path</strong></td>
<td>System Login Activity and Access Monitor &gt; System Login Success Monitor</td>
</tr>
<tr>
<td><strong>Option</strong></td>
<td>by User to Desktop</td>
</tr>
<tr>
<td><strong>Rule Name</strong></td>
<td>Successful_Login_User_to_Desktop</td>
</tr>
<tr>
<td><strong>Severity</strong></td>
<td>Notice</td>
</tr>
<tr>
<td><strong>Event IDs</strong></td>
<td>528, 4624</td>
</tr>
</tbody>
</table>
Table 6-81  Description of the by User to Desktop parameters used (continued)

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Description</strong></td>
<td>Detects a successful user logon to a system's Desktop, including local logons and terminal service logons. You can configure the Windows Security Policy auditing system to monitor the status of the logon attempts. When the Windows Security Policy auditing system determines that a user successfully logged on, it reports this event.</td>
</tr>
</tbody>
</table>

Table 6-82  Description of the by User via Remote Connection parameters used

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Option Path</strong></td>
<td>System Login Activity and Access Monitor &gt; System Login Success Monitor</td>
</tr>
<tr>
<td><strong>Option</strong></td>
<td>by User via Remote Connection</td>
</tr>
<tr>
<td><strong>Rule Name</strong></td>
<td>Successful_Login_User_via_Remote_Connection</td>
</tr>
<tr>
<td><strong>Severity</strong></td>
<td>Notice</td>
</tr>
<tr>
<td><strong>Event IDs</strong></td>
<td>528, 540, 4624, 4636</td>
</tr>
<tr>
<td><strong>Description</strong></td>
<td>Detects a successful user logon by a shared network resource, for example, IIS, FTP, or Telnet. You can configure the Windows Security Policy auditing system to monitor the status of the logon attempts. When it determines that a user has logged on by a remote connection, it reports this event.</td>
</tr>
</tbody>
</table>

Table 6-83  Description of the Non Working Hours Rules Login Success parameters used

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Option Path</strong></td>
<td>System Login Activity and Access Monitor &gt; System Login Success Monitor</td>
</tr>
<tr>
<td><strong>Option</strong></td>
<td>Non Working Hours Rules Login Success</td>
</tr>
<tr>
<td><strong>Rule Name</strong></td>
<td>System_Unlocked_After_Hours</td>
</tr>
<tr>
<td><strong>Severity</strong></td>
<td>Warning</td>
</tr>
<tr>
<td><strong>Event IDs</strong></td>
<td>528, 4624</td>
</tr>
</tbody>
</table>
Table 6-83  Description of the Non Working Hours Rules Login Success parameters used (continued)

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Description</td>
<td>Detects when a system desktop is unlocked after normal business hours. By default, after business hours is defined as Monday through Friday from 7:00 P.M. to 6:00 A.M. You can configure the Windows Security Policy auditing system to monitor the status of unlocking events. When the Windows Security Policy auditing system determines that a user successfully unlocked the workstation outside of normal working hours, it reports this event.</td>
</tr>
</tbody>
</table>

Table 6-84  Description of the System Unlocked During Weekends parameters used

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Option Path</td>
<td>System Login Activity and Access Monitor &gt; System Login Success Monitor</td>
</tr>
<tr>
<td>Option</td>
<td>System Unlocked During Weekends</td>
</tr>
<tr>
<td>Rule Name</td>
<td>System_Unlocked_During_Weekends</td>
</tr>
<tr>
<td>Severity</td>
<td>Warning</td>
</tr>
<tr>
<td>Event IDs</td>
<td>528, 4624</td>
</tr>
<tr>
<td>Description</td>
<td>Detects when a system desktop is unlocked during weekends. By default, weekend is defined as Friday 7:00 P.M. to Monday 6:00 A.M. You can configure the Windows Security Policy auditing system to monitor the status of unlocking events. When the Windows Security Policy auditing system determines that a user successfully unlocked the workstation outside of normal working hours, it reports this event.</td>
</tr>
</tbody>
</table>

System logoff monitor

This portion of the policy detects all successful Windows logoff events. You can acquire individual user logon times from the events that this portion of the policy generates. Acquire these times by comparing the logoff events with successful logon events.

Table 6-85  Description of the by Admin parameters used

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Option Path</td>
<td>System Login Activity and Access Monitor &gt; System Logoff Monitor</td>
</tr>
</tbody>
</table>
### Table 6-85 Description of the **by Admin** parameters used (continued)

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Option</td>
<td>by Admin</td>
</tr>
<tr>
<td>Rule Name</td>
<td>Logoff_by_Admin</td>
</tr>
<tr>
<td>Severity</td>
<td>Warning</td>
</tr>
<tr>
<td>Event IDs</td>
<td>538, 4634, 4647</td>
</tr>
<tr>
<td>Description</td>
<td>Detects that an administrator has successfully logged off a system from a remote location. You can configure the Windows Security Policy auditing system to monitor the status of the logoff attempts. When the auditing system determines that an administrator successfully logged off the workstation from a local location or a remote location, it reports this event.</td>
</tr>
</tbody>
</table>

### Table 6-86 Description of the **by Guest** parameters used

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Option Path</td>
<td>System Login Activity and Access Monitor &gt; System Logoff Monitor</td>
</tr>
<tr>
<td>Option</td>
<td>by Guest</td>
</tr>
<tr>
<td>Rule Name</td>
<td>Logoff_by_Guest</td>
</tr>
<tr>
<td>Severity</td>
<td>Notice</td>
</tr>
<tr>
<td>Event IDs</td>
<td>538, 4634, 4647</td>
</tr>
<tr>
<td>Description</td>
<td>Detects that a guest has successfully logged off a system. You can configure the Windows Security Policy auditing system to monitor the status of logoff attempts. When the auditing system determines that a guest has successfully logged off the workstation from a local location or a remote location, it reports this event.</td>
</tr>
</tbody>
</table>

### Table 6-87 Description of the **by User** parameters used

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Option Path</td>
<td>System Login Activity and Access Monitor &gt; System Logoff Monitor</td>
</tr>
<tr>
<td>Option</td>
<td>by User</td>
</tr>
<tr>
<td>Rule Name</td>
<td>Logoff_by_User</td>
</tr>
<tr>
<td>Severity</td>
<td>Notice</td>
</tr>
</tbody>
</table>
Table 6-87  Description of the **by User** parameters used *(continued)*

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Event IDs</td>
<td>538, 4634, 4647</td>
</tr>
<tr>
<td>Description</td>
<td>Detects that a user has successfully logged off a system. You can configure the Windows Security Policy auditing system to monitor the status of logoff attempts. When the auditing system determines that a user successfully logged off the workstation from a local location or a remote location, it reports this event.</td>
</tr>
</tbody>
</table>

Table 6-88  Description of the **by Specific User** parameters used

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Option Path</td>
<td>System Login Activity and Access Monitor &gt; System Logoff Monitor</td>
</tr>
<tr>
<td>Option</td>
<td>by Specific User</td>
</tr>
<tr>
<td>Rule Name</td>
<td>System_Logoff_by_SpecificUser</td>
</tr>
<tr>
<td>Severity</td>
<td>Notice</td>
</tr>
<tr>
<td>Event IDs</td>
<td>538, 4634, 4647</td>
</tr>
<tr>
<td>Description</td>
<td>Detects that a specific user-defined user or users have successfully logged off a system. You can configure the Windows Security Policy auditing system to monitor the status of logoff attempts. When the auditing system determines that a user successfully logged off the workstation from a local location or a remote location, it reports this event.</td>
</tr>
</tbody>
</table>

**System failed login monitor**

This option group subsection detects when a user has failed to authenticate. That is, has failed to log on to a Windows system either as a local user or as a member of a domain. This activity most often indicates normal behavior, ranging from expired passwords to a user who forgets a current password. However, it may also indicate attempts by an unauthorized user to gain illegitimate access to the system or the domain.
Note: The first option under System Failed Login Monitor, N Tries, allows the administrator to set thresholds based alerting on all failed logon events. For example, an N Tries setting of 3 and an Interval of 1 minute only generates an alert if a user makes more than three failed logon attempts within the interval time of 1 minute. You can use this option to detect brute force-based credential attacks.

Table 6-89 Description of the Account Disabled parameters used

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Option Path</td>
<td>System Login Activity and Access Monitor &gt; System Failed Login Monitor</td>
</tr>
<tr>
<td>Option</td>
<td>Account Disabled</td>
</tr>
<tr>
<td>Rule Name</td>
<td>Account_Disabled</td>
</tr>
<tr>
<td>Severity</td>
<td>Warning</td>
</tr>
<tr>
<td>Event IDs</td>
<td>531, 4625</td>
</tr>
<tr>
<td>Description</td>
<td>Detects when a user has failed to access the client, due to a disabled account. You can configure the Windows Security Policy auditing system to monitor the status of logon attempts. When the auditing system determines that a logon failed because the account was disabled, it reports this event.</td>
</tr>
</tbody>
</table>

Table 6-90 Description of the Account Expired parameters used

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Option Path</td>
<td>System Login Activity and Access Monitor &gt; System Failed Login Monitor</td>
</tr>
<tr>
<td>Option</td>
<td>Account Expired</td>
</tr>
<tr>
<td>Rule Name</td>
<td>Account_Expired</td>
</tr>
<tr>
<td>Severity</td>
<td>Notice</td>
</tr>
<tr>
<td>Event IDs</td>
<td>532, 4625</td>
</tr>
<tr>
<td>Description</td>
<td>Detects when a user has failed to access the client, due to an expired account. You can configure the Windows Security Policy auditing system to monitor the status of logon attempts. When the auditing system determines that a logon has failed because the account has expired, it reports this event.</td>
</tr>
</tbody>
</table>
### Table 6-91 Description of the Account Locked Out parameters used

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Option Path</td>
<td>System Login Activity and Access Monitor &gt; System Failed Login Monitor</td>
</tr>
<tr>
<td>Option</td>
<td>Account Locked Out</td>
</tr>
<tr>
<td>Rule Name</td>
<td>Account_Locked_Out</td>
</tr>
<tr>
<td>Severity</td>
<td>Warning</td>
</tr>
<tr>
<td>Event IDs</td>
<td>539, 4740</td>
</tr>
<tr>
<td>Description</td>
<td>Detects when a user has failed to access the client, due to a lock on the account. You can configure the Windows Security Policy auditing system to monitor the status of logon attempts. When the auditing system determines that a logon has failed because the account was locked out, it reports this event.</td>
</tr>
</tbody>
</table>

### Table 6-92 Description of the By Admin to Desktop parameters used

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Option Path</td>
<td>System Login Activity and Access Monitor &gt; System Failed Login Monitor</td>
</tr>
<tr>
<td>Option</td>
<td>By Admin to Desktop</td>
</tr>
<tr>
<td>Rule Name</td>
<td>Login_Failed_Admin_to_Desktop</td>
</tr>
<tr>
<td>Severity</td>
<td>Warning</td>
</tr>
<tr>
<td>Event IDs</td>
<td>529, 4625</td>
</tr>
<tr>
<td>Description</td>
<td>Detects when an administrator has failed to log on to a system's desktop, either locally or by Terminal Services. You can configure the Windows Security Policy auditing system to monitor the status of logon attempts. When the auditing system determines that an administrator has failed to log on to the local desktop or through the Terminal Services, it reports this event.</td>
</tr>
</tbody>
</table>

### Table 6-93 Description of the By Admin via Remote Connection parameters used

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Option Path</td>
<td>System Login Activity and Access Monitor &gt; System Failed Login Monitor</td>
</tr>
<tr>
<td>Description</td>
<td></td>
</tr>
</tbody>
</table>
Table 6-93 Description of the **By Admin via Remote Connection** parameters used *(continued)*

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Option</td>
<td>By Admin via Remote Connection</td>
</tr>
<tr>
<td>Rule Name</td>
<td>Login_Failed_Admin_via_Roomote_Connection</td>
</tr>
<tr>
<td>Severity</td>
<td>Warning</td>
</tr>
<tr>
<td>Event IDs</td>
<td>529, 4625</td>
</tr>
<tr>
<td>Description</td>
<td>Detects when an administrator has failed to log on to a system or to a domain on the network. You can configure the Windows Security Policy auditing system to monitor the status of logon attempts. When the auditing system determines that an administrator has failed to log on through a remote connection, it reports this event.</td>
</tr>
</tbody>
</table>

Table 6-94 Description of the **By Guest to Desktop** parameters used

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Option Path</td>
<td>System Login Activity and Access Monitor &gt; System Failed Login Monitor</td>
</tr>
<tr>
<td>Option</td>
<td>By Guest to Desktop</td>
</tr>
<tr>
<td>Rule Name</td>
<td>Login_Failed_Guest_to_Desktop</td>
</tr>
<tr>
<td>Severity</td>
<td>Warning</td>
</tr>
<tr>
<td>Event IDs</td>
<td>529, 4625</td>
</tr>
<tr>
<td>Description</td>
<td>Detects when a guest has failed to log on to a system's desktop, either locally or by Terminal Services. You can configure the Windows Security Policy auditing system to monitor the status of logon attempts. When the auditing system determines that a guest has failed to log on, it reports this event.</td>
</tr>
</tbody>
</table>

Table 6-95 Description of the **By Guest via Remote Connection** parameters used

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Option Path</td>
<td>System Login Activity and Access Monitor &gt; System Failed Login Monitor</td>
</tr>
<tr>
<td>Option</td>
<td>By Guest via Remote Connection</td>
</tr>
</tbody>
</table>
Table 6-95  Description of the **By Guest via Remote Connection** parameters used (continued)

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Rule Name</td>
<td>Login_Failed_Guest_via_Remote_Connection</td>
</tr>
<tr>
<td>Severity</td>
<td>Warning</td>
</tr>
<tr>
<td>Event IDs</td>
<td>529, 4625</td>
</tr>
<tr>
<td>Description</td>
<td>Detects when a guest has failed to log on to a system or domain on the network. You can configure the Windows Security Policy auditing system to monitor the status of logon attempts. When the auditing system determines that a guest has failed to log on by a remote connection, it reports this event.</td>
</tr>
</tbody>
</table>

Table 6-96  Description of the **By User to Desktop** parameters used

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Option Path</td>
<td>System Login Activity and Access Monitor &gt; System Failed Login Monitor</td>
</tr>
<tr>
<td>Option</td>
<td>By User to Desktop</td>
</tr>
<tr>
<td>Rule Name</td>
<td>Login_Failed_User_to_Desktop</td>
</tr>
<tr>
<td>Severity</td>
<td>Notice</td>
</tr>
<tr>
<td>Event IDs</td>
<td>529, 4625</td>
</tr>
<tr>
<td>Description</td>
<td>Detects when a user has failed to log on to a system's desktop, either locally or by Terminal Services. You can configure the Windows Security Policy auditing system to monitor the status of logon attempts. When the auditing system determines that a user has failed to log on to the local desktop, it reports this event.</td>
</tr>
</tbody>
</table>

Table 6-97  Description of the **By User via Remote Connection** parameters used

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Option Path</td>
<td>System Login Activity and Access Monitor &gt; System Failed Login Monitor</td>
</tr>
<tr>
<td>Option</td>
<td>By User via Remote Connection</td>
</tr>
<tr>
<td>Rule Name</td>
<td>Login_Failed_User_via_Remote_Connection</td>
</tr>
</tbody>
</table>
Table 6-97  Description of the **By User via Remote Connection** parameters used (continued)

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Severity</td>
<td>Notice</td>
</tr>
<tr>
<td>Event IDs</td>
<td>529, 4625</td>
</tr>
<tr>
<td>Description</td>
<td>Detects when a user has failed to log on to a system or domain on the network. You can configure the Windows Security Policy auditing system to monitor the status of logon attempts. When the auditing system determines that a user has failed to log on by a remote connection, it reports this event.</td>
</tr>
</tbody>
</table>

Table 6-98  Description of the **Logon Failure** parameters used

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Option Path</td>
<td>System Login Activity and Access Monitor &gt; System Failed Login Monitor</td>
</tr>
<tr>
<td>Option</td>
<td>Logon Failure</td>
</tr>
<tr>
<td>Rule Name</td>
<td>Login_Failed_Generic</td>
</tr>
<tr>
<td>Severity</td>
<td>Notice</td>
</tr>
<tr>
<td>Event IDs</td>
<td>537</td>
</tr>
<tr>
<td>Description</td>
<td>Detects when an unexpected error has occurred during logon. A failed authentication by a cleartext password, Windows NT Lan Manager, or Windows Kerberos security authentication system can cause this error. This detection may also indicate a failure to access the File Transfer Protocol (FTP) services that are related to the Microsoft Internet Information Server (IIS).</td>
</tr>
</tbody>
</table>

Table 6-99  Description of the **Logon to Account** parameters used

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Option Path</td>
<td>System Login Activity and Access Monitor &gt; System Failed Login Monitor</td>
</tr>
<tr>
<td>Option</td>
<td>Logon to Account</td>
</tr>
<tr>
<td>Rule Name</td>
<td>Logon_to_Account_Failed</td>
</tr>
<tr>
<td>Severity</td>
<td>Notice</td>
</tr>
</tbody>
</table>
Table 6-99  Description of the **Logon to Account** parameters used (continued)

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Event IDs</td>
<td>681</td>
</tr>
<tr>
<td>Description</td>
<td>Detects when a down-level client fails a logon attempt. Windows generates an error message on the Windows domain controller. You can configure the Windows Security Policy auditing system to monitor the status of logon attempts. When the auditing system determines that a domain logon failed, it reports this event.</td>
</tr>
</tbody>
</table>

Table 6-100  Description of the **Password Expired** parameters used

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Option Path</td>
<td>System Login Activity and Access Monitor &gt; System Failed Login Monitor</td>
</tr>
<tr>
<td>Option</td>
<td>Password Expired</td>
</tr>
<tr>
<td>Rule Name</td>
<td>Password_Expired</td>
</tr>
<tr>
<td>Severity</td>
<td>Notice</td>
</tr>
<tr>
<td>Event IDs</td>
<td>535, 4625</td>
</tr>
<tr>
<td>Description</td>
<td>Detects when a user has failed to access a client, due to an expired account password. You can configure the Windows Security Policy auditing system to monitor the status of logon attempts. When the auditing system determines that a logon failed, due to an expired account, it reports this event.</td>
</tr>
</tbody>
</table>

Table 6-101  Description of the **Unauthorized Access** parameters used

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Option Path</td>
<td>System Login Activity and Access Monitor &gt; System Failed Login Monitor</td>
</tr>
<tr>
<td>Option</td>
<td>Unauthorized Access</td>
</tr>
<tr>
<td>Rule Name</td>
<td>Unauthorized_Access</td>
</tr>
<tr>
<td>Severity</td>
<td>Warning</td>
</tr>
<tr>
<td>Event IDs</td>
<td>534, 4625</td>
</tr>
</tbody>
</table>
Table 6-101  Description of the **Unauthorized Access** parameters used  

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Description</td>
<td>Detects when a user has failed to access a client because the local access rights or the remote access rights have not been granted to the user. You can configure the Windows Security Policy auditing system to monitor the status of the logon attempts. When the auditing system determines that a logon failed due to a disabled account, it reports this event.</td>
</tr>
</tbody>
</table>

Table 6-102  Description of the **Unauthorized Location** parameters used  

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Option Path</td>
<td>System Login Activity and Access Monitor &gt; System Failed Login Monitor</td>
</tr>
<tr>
<td>Option</td>
<td>Unauthorized Location</td>
</tr>
<tr>
<td>Rule Name</td>
<td>Unauthorized_Location</td>
</tr>
<tr>
<td>Severity</td>
<td>Warning</td>
</tr>
<tr>
<td>Event IDs</td>
<td>533, 4625</td>
</tr>
<tr>
<td>Description</td>
<td>Detects when a user has failed to access the domain because the client is not authorized to participate in the domain. You can configure the Windows Security Policy auditing system to monitor the status of the logon attempts. When the auditing system determines that a logon has failed because the logon was attempted from an unauthorized client, it reports this event.</td>
</tr>
</tbody>
</table>

Table 6-103  Description of the **Unauthorized Time** parameters used  

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Option Path</td>
<td>System Login Activity and Access Monitor &gt; System Failed Login Monitor</td>
</tr>
<tr>
<td>Option</td>
<td>Unauthorized Time</td>
</tr>
<tr>
<td>Rule Name</td>
<td>Unauthorized_Time</td>
</tr>
<tr>
<td>Severity</td>
<td>Warning</td>
</tr>
<tr>
<td>Event IDs</td>
<td>530, 4625</td>
</tr>
</tbody>
</table>
Table 6-103

Description of the Unauthorized Time parameters used (continued)

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Description</td>
<td>Detects when a domain user has failed to access a client, because the account is not authorized to access the domain during this time period. You can configure the Windows Security Policy auditing system to monitor the status of logon attempts. When the auditing system determines that the failure has occurred because the account was not allowed to log on during this time period, it reports this event.</td>
</tr>
</tbody>
</table>

System hardening monitor

This option group section detects changes to the user-configurable registry keys that are considered sensitive in maintaining the security posture of the operating system. 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

System autorun configuration

This option group subsection detects modifications of the system configuration that change whether it automatically runs code during system startup or from newly inserted CD-ROMs. 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. This policy should be applied on all Windows agents and no configuration changes are required for this policy to work.

Note: The final option set, User Desktop Logon Check, enables a function of these rules to only monitor and generate an event if a user is logged on.

Table 6-104

Description of the CDROM Value Changed parameters used

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Option Path</td>
<td>System Hardening Monitor &gt; System AutoRun Configuration</td>
</tr>
<tr>
<td>Option</td>
<td>CDROM Value Changed</td>
</tr>
<tr>
<td>Rule Name</td>
<td>CDROM_Value_Changed</td>
</tr>
</tbody>
</table>
### Table 6-104  Description of the **CDROM Value Changed** parameters used (continued)

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Severity</td>
<td>Warning</td>
</tr>
<tr>
<td>Registry Paths</td>
<td><code>\HKEY_LOCAL_MACHINE\SYSTEM\*ControlSet*\Services\Cdrom\Autorun</code></td>
</tr>
<tr>
<td>Description</td>
<td>Detects the changes to the CD-ROM AutoRun behavior, according to the registry setting: HKLM\System\CurrentControlSet\Services\CD-ROM key Autorun value. This value determines whether the system automatically runs code from the newly inserted CD-ROMs.</td>
</tr>
</tbody>
</table>

### Table 6-105  Description of the **Run Key Changed** parameters used

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Option Path</td>
<td>System Hardening Monitor &gt; System AutoRun Configuration</td>
</tr>
<tr>
<td>Option</td>
<td>Run Key Changed</td>
</tr>
<tr>
<td>Rule Name</td>
<td>Run_Key_Changed</td>
</tr>
<tr>
<td>Severity</td>
<td>Warning</td>
</tr>
<tr>
<td>Registry Paths</td>
<td><code>\HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run\*</code></td>
</tr>
<tr>
<td>Description</td>
<td>Detects the changes to the Run registry key, according to the registry setting: HKLM\Software\Microsoft\Windows\CurrentVersion\Run key.</td>
</tr>
</tbody>
</table>

### Table 6-106  Description of the **RunOnceEx Key Changed** parameters used

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Option Path</td>
<td>System Hardening Monitor &gt; System AutoRun Configuration</td>
</tr>
<tr>
<td>Option</td>
<td>RunOnceEx Key Changed</td>
</tr>
<tr>
<td>Rule Name</td>
<td>RunOnceEx_Key_Changed</td>
</tr>
<tr>
<td>Severity</td>
<td>Warning</td>
</tr>
<tr>
<td>Registry Paths</td>
<td><code>\HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\RunOnceEx\*</code></td>
</tr>
</tbody>
</table>
# Table 6-106  Description of the **RunOnceEx Key Changed** parameters used (continued)

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Description</strong></td>
<td>Detects the changes to the RunOnceEx registry key, according to the registry setting: HKLM\Software\Microsoft\Windows\CurrentVersion\RunOnceEx key. The system configuration has been modified to change the behavior of the system the next time a user logs on. This key allows a specified routine or a list of routines to execute once. It then clears itself so that it does not run on the next logon.</td>
</tr>
</tbody>
</table>

# Table 6-107  Description of the **Userinit Value Changed** parameters used

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Option Path</strong></td>
<td>System Hardening Monitor &gt; System AutoRun Configuration</td>
</tr>
<tr>
<td><strong>Option</strong></td>
<td>Userinit Value Changed</td>
</tr>
<tr>
<td><strong>Rule Name</strong></td>
<td>Userinit_Value_Changed</td>
</tr>
<tr>
<td><strong>Severity</strong></td>
<td>Warning</td>
</tr>
<tr>
<td><strong>Registry Paths</strong></td>
<td>\HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon\Userinit</td>
</tr>
<tr>
<td><strong>Description</strong></td>
<td>Detects the changing of the Userinit key, according to registry setting: HKLM\Software\Microsoft\WindowsNT\CurrentVersion\Winlogon key Userinit value. This key specifies the program that Winlogon runs when a user logs on. This program is typically Userinit.exe. This behavior is unusual, however. It would be expected if the system was updated to run the enterprise-unique routines first, then run the Userinit.exe or Explorer.exe.</td>
</tr>
</tbody>
</table>

# Table 6-108  Description of the **User Desktop Logon Check** parameters used

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Option Path</strong></td>
<td>System Hardening Monitor &gt; System AutoRun Configuration</td>
</tr>
<tr>
<td><strong>Description</strong></td>
<td>Detects a successful user logon and sets a flag. This setting ensures that the rules within this portion of the policy do not create false positives with a normal non-administrative user setting specific areas that are otherwise monitored. It is recommended that this setting remain turned on to thwart false positives.</td>
</tr>
</tbody>
</table>
Network comm configuration

This option group subsection detects changes to the various registry keys that deal with network and communication settings. This policy can be applied to any Windows server. Unauthorized or unknown network changes as monitored in this portion of the policy may indicate suspicious activity.

Table 6-109 Description of the **Autodisconnect Changed** parameters used

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Option Path</td>
<td>System Hardening Monitor &gt; Network Comm Configuration</td>
</tr>
<tr>
<td>Option</td>
<td>Autodisconnect Changed</td>
</tr>
<tr>
<td>Rule Name</td>
<td>Autodisconnect_Changed</td>
</tr>
<tr>
<td>Severity</td>
<td>Warning</td>
</tr>
<tr>
<td>Registry Paths</td>
<td><code>\HKEY_LOCAL_MACHINE\SYSTEM\*ControlSet*\Services\LanmanServer\Parameters\autodisconnect</code></td>
</tr>
<tr>
<td>Description</td>
<td>Detects the changes to the <code>HKEY_LOCAL_MACHINE\SYSTEM\*ControlSet*\Services\LanmanServer\Parameters\autodisconnect</code> registry key. This registry key determines the time that is allowed for an inactive connection before it is automatically disconnected.</td>
</tr>
</tbody>
</table>

Table 6-110 Description of the **TcpMaxDupAcks Changed** parameters used

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Option Path</td>
<td>System Hardening Monitor &gt; Network Comm Configuration</td>
</tr>
<tr>
<td>Option</td>
<td>TcpMaxDupAcks Changed</td>
</tr>
<tr>
<td>Rule Name</td>
<td>TcpMaxDupAcks_Changed</td>
</tr>
<tr>
<td>Severity</td>
<td>Warning</td>
</tr>
<tr>
<td>Registry Paths</td>
<td><code>\HKEY_LOCAL_MACHINE\SYSTEM\*ControlSet*\Services\Tcpip\Parameters\TcpMaxDupAcks</code></td>
</tr>
<tr>
<td>Description</td>
<td>Detects the changes to the <code>HKEY_LOCAL_MACHINE\SYSTEM\*ControlSet*\Services\Tcpip\Parameters\TcpMaxDupAcks</code> registry key. This registry key determines the number of duplicate ACKs, which must be received for the same sequence number of sent data, before a fast retransmit is triggered to resend the segment that was dropped in transit.</td>
</tr>
</tbody>
</table>
System file protection status

This option group subsection detects the events that the Windows File Protection (WFP) System reports. The WFP monitors the critical operating system files that should remain available, but should not change during the course of operation. If a monitored file is deleted or modified, or its attributes are changed, the WFP immediately restores the file to its original configuration. These events can occur for a number of reasons. The reasons include third-party software installation, system misconfiguration, or illegitimate manipulation. Activation of WFP file restoration procedures may be a response to illegitimate activity.

Table 6-111 Description of the File Restoration Failed parameters used

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Option Path</td>
<td>System Hardening Monitor &gt; System File Protection Status</td>
</tr>
<tr>
<td>Option</td>
<td>File Restoration Failed</td>
</tr>
<tr>
<td>Rule Name</td>
<td>File_Restoration_Failed</td>
</tr>
<tr>
<td>Severity</td>
<td>Critical</td>
</tr>
<tr>
<td>Event IDs</td>
<td>64004, 64007, 64006, 64021, 64005, 64008</td>
</tr>
<tr>
<td>Description</td>
<td>Detects when a file that the Windows File Protection System protects cannot be restored. The Windows File Protection System monitors the status of protected files and attempts to restore them to their original condition when it detects any changes. If the Windows File Protection System determines that it cannot successfully restore the file, it reports this error.</td>
</tr>
</tbody>
</table>

Table 6-112 Description of the File Restoration Success parameters used

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Option Path</td>
<td>System Hardening Monitor &gt; System File Protection Status</td>
</tr>
<tr>
<td>Option</td>
<td>File Restoration Success</td>
</tr>
<tr>
<td>Rule Name</td>
<td>File_Restoration_Success</td>
</tr>
<tr>
<td>Severity</td>
<td>Warning</td>
</tr>
<tr>
<td>Event IDs</td>
<td>64000, 64003, 64019, 64020, 64001, 64002</td>
</tr>
</tbody>
</table>
### Table 6-112  Description of the **File Restoration Success** parameters used (continued)

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Description</td>
<td>Detects when a file that the Windows File Protection System protects has been restored. The Windows File Protection System monitors the status of protected files and restores them to their original condition when it detects any changes. If the Windows File Protection System determines that it successfully restored a file, it reports this status.</td>
</tr>
</tbody>
</table>

### Table 6-113  Description of the **WFP Errors** parameters used

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Option Path</td>
<td>System Hardening Monitor &gt; System File Protection Status</td>
</tr>
<tr>
<td>Option</td>
<td>WFP Errors</td>
</tr>
<tr>
<td>Rule Name</td>
<td>WFP_Errors</td>
</tr>
<tr>
<td>Severity</td>
<td>Critical</td>
</tr>
<tr>
<td>Event IDs</td>
<td>64034, 64033, 64032</td>
</tr>
<tr>
<td>Description</td>
<td>Detects when the Windows File Protection System has detected a configuration error. The Windows File Protection System monitors its ability to access a protected file cache. It also monitors the active state or initialized state of the File Protection System. If the Windows File Protection System determines that it cannot access the cache, or that its state is inactive or not initialized, it reports these errors.</td>
</tr>
</tbody>
</table>

### Table 6-114  Description of the **Scanning Started** parameters used

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Option Path</td>
<td>System Hardening Monitor &gt; System File Protection Status</td>
</tr>
<tr>
<td>Option</td>
<td>Scanning Started</td>
</tr>
<tr>
<td>Rule Name</td>
<td>Scanning_Started</td>
</tr>
<tr>
<td>Severity</td>
<td>Notice</td>
</tr>
<tr>
<td>Event IDs</td>
<td>64016</td>
</tr>
</tbody>
</table>
Table 6-114  Description of the **Scanning Started** parameters used *(continued)*

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Description</td>
<td>Detects when the Windows File Protection System has started a scan of critical system files. The Windows File Protection System scans the protected files to determine their condition. When the Windows File Protection System determines that it successfully started a scan, it reports this status.</td>
</tr>
</tbody>
</table>

Table 6-115  Description of the **Scanning Completed** parameters used

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Option Path</td>
<td>System Hardening Monitor &gt; System File Protection Status</td>
</tr>
<tr>
<td>Option</td>
<td>Scanning Completed</td>
</tr>
<tr>
<td>Rule Name</td>
<td>Scanning_Completed</td>
</tr>
<tr>
<td>Severity</td>
<td>Notice</td>
</tr>
<tr>
<td>Event IDs</td>
<td>64017</td>
</tr>
<tr>
<td>Description</td>
<td>Detects when the Windows File Protection System has completed a scan of critical system files. The Windows File Protection System scans these protected files to determine their condition. When the Windows File Protection System determines that it successfully completed a scan, it reports this status.</td>
</tr>
</tbody>
</table>

Table 6-116  Description of the **Scanning Canceled** parameters used

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Option Path</td>
<td>System Hardening Monitor &gt; System File Protection Status</td>
</tr>
<tr>
<td>Option</td>
<td>Scanning Canceled</td>
</tr>
<tr>
<td>Rule Name</td>
<td>Scanning_Canceled</td>
</tr>
<tr>
<td>Severity</td>
<td>Warning</td>
</tr>
<tr>
<td>Event IDs</td>
<td>64018</td>
</tr>
<tr>
<td>Description</td>
<td>Detects when a Windows File Protection System scan has been canceled. The Windows File Protection System scans these protected files to determine their condition. When the Windows File Protection System determines that a command has interrupted the scanning process, it reports this status.</td>
</tr>
</tbody>
</table>
System security configuration

This option group subsection detects changes to the various registry keys that deal with the typical security settings of a host system. These settings range from protection mode changes to how legal captions are viewed upon logon. See the individual rule description for more information.

Table 6-117 Description of the **AllocateCdroms Changed** parameters used

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Option Path</td>
<td>System Hardening Monitor &gt; System Security Configuration</td>
</tr>
<tr>
<td>Option</td>
<td>AllocateCdroms Changed</td>
</tr>
<tr>
<td>Rule Name</td>
<td>AllocateCdroms_Changed</td>
</tr>
<tr>
<td>Severity</td>
<td>Warning</td>
</tr>
<tr>
<td>Registry Keys</td>
<td>\HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon\AllocateCDRoms</td>
</tr>
<tr>
<td>Description</td>
<td>Detects any changes or attempted changes to the HKLM\SOFTWARE\Microsoft\WindowsNT\CurrentVersion\Winlogon key AllocateCdroms value. This value determines whether data in the CD-ROM drive is accessible to other users.</td>
</tr>
</tbody>
</table>

Table 6-118 Description of the **AllocateFloppies Changed** parameters used

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Option Path</td>
<td>System Hardening Monitor &gt; System Security Configuration</td>
</tr>
<tr>
<td>Option</td>
<td>AllocateFloppies Changed</td>
</tr>
<tr>
<td>Rule Name</td>
<td>AllocateFloppies_Changed</td>
</tr>
<tr>
<td>Severity</td>
<td>Warning</td>
</tr>
<tr>
<td>Registry Keys</td>
<td>Warning \HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon\AllocateFloppies</td>
</tr>
<tr>
<td>Description</td>
<td>Detects any changes or attempted changes to the HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon key AllocateFloppies value. This value determines whether data in the floppy disk drive is accessible to other users.</td>
</tr>
</tbody>
</table>
## Table 6-119 Description of the **AutoShareServer Changed** parameters used

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Option Path</td>
<td>System Hardening Monitor &gt; System Security Configuration</td>
</tr>
<tr>
<td>Option</td>
<td>AutoShareServer Changed</td>
</tr>
<tr>
<td>Rule Name</td>
<td>AutoShareServer_Changed</td>
</tr>
<tr>
<td>Severity</td>
<td>Warning</td>
</tr>
<tr>
<td>Registry Keys</td>
<td>\HKEY_LOCAL_MACHINE\SYSTEM*ControlSet*\Services\LanmanServer\Parameters\AutoShareServer</td>
</tr>
<tr>
<td>Description</td>
<td>Detects any changes or attempted changes to the <code>\HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\LanManServer\Parameters\AutoShareServer</code> key. This value creates the administrative shares (C, D, ADMIN) for the physical drives.</td>
</tr>
</tbody>
</table>

## Table 6-120 Description of the **AutoShareWks Changed** parameters used

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Option Path</td>
<td>System Hardening Monitor &gt; System Security Configuration</td>
</tr>
<tr>
<td>Option</td>
<td>AutoShareWks Changed</td>
</tr>
<tr>
<td>Rule Name</td>
<td>AutoShareWks_Changed</td>
</tr>
<tr>
<td>Severity</td>
<td>Warning</td>
</tr>
<tr>
<td>Registry Keys</td>
<td>\HKEY_LOCAL_MACHINE\SYSTEM*ControlSet*\Services\LanmanServer\Parameters\AutoShareWks</td>
</tr>
<tr>
<td>Description</td>
<td>Detects any changes or attempted changes to the <code>\HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\LanManServer\Parameters\AutoShareWks</code> key. This value is responsible for enabling and disabling the automatic sharing of hidden shares.</td>
</tr>
</tbody>
</table>

## Table 6-121 Description of the **ComSpec Changed** parameters used

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Option Path</td>
<td>System Hardening Monitor &gt; System Security Configuration</td>
</tr>
<tr>
<td>Option</td>
<td>ComSpec Changed</td>
</tr>
<tr>
<td>Rule Name</td>
<td>ComSpec_Changed</td>
</tr>
<tr>
<td>Severity</td>
<td>Warning</td>
</tr>
</tbody>
</table>
### Table 6-121  Description of the **ComSpec Changed** parameters used (continued)

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Registry Keys</td>
<td><code>\HKEY_LOCAL_MACHINE\SYSTEM\*ControlSet\Control\Session Manager\Environment\ComSpec</code></td>
</tr>
<tr>
<td>Description</td>
<td>Detects any changes or attempted changes to the <code>HKLM\SYSTEM\CurrentControlSet\Control\Session Manager\Environment</code> key <code>ComSpec</code> value. This value is responsible for defining the path to the DOS command interpreter, <code>Command.com</code>.</td>
</tr>
</tbody>
</table>

### Table 6-122  Description of the **Debugger Changed** parameters used

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Option Path</td>
<td>System Hardening Monitor &gt; System Security Configuration</td>
</tr>
<tr>
<td>Option</td>
<td>Debugger Changed</td>
</tr>
<tr>
<td>Rule Name</td>
<td>Debugger_Changed</td>
</tr>
<tr>
<td>Severity</td>
<td>Warning</td>
</tr>
<tr>
<td>Registry Keys</td>
<td><code>\HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\AeDebug\Debugger</code></td>
</tr>
<tr>
<td>Description</td>
<td>Detects any changes or attempted changes to the <code>HKLM\Software\Microsoft\Windows NT\CurrentVersion\AeDebug</code> key <code>Debugger</code> value. This value is responsible for determining whether to automatically spawn the Win32 debugger during an application fault.</td>
</tr>
</tbody>
</table>

### Table 6-123  Description of the **Directory Changed** parameters used

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Option Path</td>
<td>System Hardening Monitor &gt; System Security Configuration</td>
</tr>
<tr>
<td>Option</td>
<td>Directory Changed</td>
</tr>
<tr>
<td>Rule Name</td>
<td>Directory_Changed</td>
</tr>
<tr>
<td>Severity</td>
<td>Critical</td>
</tr>
<tr>
<td>Registry Keys</td>
<td><code>\HKEY_LOCAL_MACHINE\SYSTEM\*ControlSet\Control\Windows\Directory</code></td>
</tr>
<tr>
<td>Description</td>
<td>Detects any changes or attempted changes to the <code>HKLM\SYSTEM\CurrentControlSet\Control\Windows</code> key <code>Directory</code> value. This value contains the information that helps to define the system directories for the Win32 subsystem.</td>
</tr>
</tbody>
</table>
### Table 6-124  Description of the **DisableTaskMgr Changed** parameters used

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Option Path</td>
<td>System Hardening Monitor &gt; System Security Configuration</td>
</tr>
<tr>
<td>Option</td>
<td>DisableTaskMgr Changed</td>
</tr>
<tr>
<td>Rule Name</td>
<td>DisableTaskMgr_Changed</td>
</tr>
<tr>
<td>Severity</td>
<td>Warning</td>
</tr>
<tr>
<td>Registry Keys</td>
<td>\HKEY_USERS\Software\Microsoft\Windows\CurrentVersion\Policies\System\DisableTaskMgr</td>
</tr>
<tr>
<td>Description</td>
<td>Detects any changes or attempted changes to the HKU\Software\Microsoft\Windows\CurrentVersion\Policies\System key DisableTaskMgr value. This value controls the ability of users to start Task Manager and view processes and view running applications. It also controls the ability of users to make changes to the priority or state of the individual processes.</td>
</tr>
</tbody>
</table>

### Table 6-125  Description of the **DontDisplayLastUserName Changed** parameters used

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Option Path</td>
<td>System Hardening Monitor &gt; System Security Configuration</td>
</tr>
<tr>
<td>Option</td>
<td>DontDisplayLastUserName Changed</td>
</tr>
<tr>
<td>Rule Name</td>
<td>DontDisplayLastUserName_Changed</td>
</tr>
<tr>
<td>Severity</td>
<td>Warning</td>
</tr>
<tr>
<td>Registry Keys</td>
<td>\HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\policies\system\dontdisplaylastusername</td>
</tr>
<tr>
<td>Description</td>
<td>Detects any changes or attempted changes to the HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\policies\system key DontDisplayLastUserName value. If you enable this value, the user name box on the logon screen is blank. This behavior prevents the people that log on from knowing the last user to access the system.</td>
</tr>
</tbody>
</table>

### Table 6-126  Description of the **Hidden Changed** parameters used

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Option Path</td>
<td>System Hardening Monitor &gt; System Security Configuration</td>
</tr>
</tbody>
</table>
Table 6-126  Description of the **Hidden Changed** parameters used *(continued)*

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Option</td>
<td>Hidden Changed</td>
</tr>
<tr>
<td>Rule Name</td>
<td>Hidden_Changed</td>
</tr>
<tr>
<td>Severity</td>
<td>Warning</td>
</tr>
<tr>
<td>Registry Keys</td>
<td>HKLM\SYSTEM\CurrentControlSet\Services\LanManServer\Parameters\hidden</td>
</tr>
<tr>
<td>Description</td>
<td>Detects any changes or attempted changes to the HKLM\SYSTEM\CurrentControlSet\Services\LanManServer\Parameters key hidden value. This value is responsible for hiding a server from the Network Browser.</td>
</tr>
</tbody>
</table>

Table 6-127  Description of the **LegalNoticeCaption Changed** parameters used

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Option Path</td>
<td>System Hardening Monitor &gt; System Security Configuration</td>
</tr>
<tr>
<td>Option</td>
<td>LegalNoticeCaption Changed</td>
</tr>
<tr>
<td>Rule Name</td>
<td>LegalNoticeCaption_Changed</td>
</tr>
<tr>
<td>Severity</td>
<td>Info</td>
</tr>
<tr>
<td>Registry Keys</td>
<td>HKLM\SOFTWARE\Microsoft\WindowsNT\CurrentVersion\Winlogon\LegalNoticeCaption  HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System\legalnoticecaption</td>
</tr>
<tr>
<td>Description</td>
<td>Detects any changes or attempted changes to HKLM\SOFTWARE\Microsoft\WindowsNT\CurrentVersion\Winlogon\LegalNoticeCaption value or to HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System\legalnoticecaption value. This value creates a dialog box that is presented to any users before they log onto the system.</td>
</tr>
</tbody>
</table>

Table 6-128  Description of the **LegalNoticeText Changed** parameters used

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Option Path</td>
<td>System Hardening Monitor &gt; System Security Configuration</td>
</tr>
<tr>
<td>Option</td>
<td>LegalNoticeText Changed</td>
</tr>
<tr>
<td>Rule Name</td>
<td>LegalNoticeText_Changed</td>
</tr>
</tbody>
</table>
### Table 6-128
Description of the **LegalNoticeText Changed** parameters used (continued)

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Severity</td>
<td>Info</td>
</tr>
<tr>
<td>Registry Keys</td>
<td>\HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\WindowsNT\CurrentVersion\Winlogon\LegalNoticeText \HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\policies\system\LegalNoticeText</td>
</tr>
<tr>
<td>Description</td>
<td>Detects any changes or attempted changes to the HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon key LegalNoticeCaption value or to HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\policies\system key LegalNoticeText value. This value creates a dialog box that is presented to any users before they log onto the system.</td>
</tr>
</tbody>
</table>

### Table 6-129
Description of the **PasswordExpiryWarning Changed** parameters used

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Option Path</td>
<td>System Hardening Monitor &gt; System Security Configuration</td>
</tr>
<tr>
<td>Option</td>
<td>PasswordExpiryWarning Changed</td>
</tr>
<tr>
<td>Rule Name</td>
<td>PasswordExpiryWarning_Changed</td>
</tr>
<tr>
<td>Severity</td>
<td>Info</td>
</tr>
<tr>
<td>Registry Keys</td>
<td>\HKEY_LOCAL_MACHINE\software\Microsoft\WindowsNT\CurrentVersion\Winlogon\PasswordExpiryWarning</td>
</tr>
<tr>
<td>Description</td>
<td>Detects any changes or attempted changes to the HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon key PasswordExpiryWarning value. This value is responsible for informing users of how many days are left until their password expires.</td>
</tr>
</tbody>
</table>

### Table 6-130
Description of the **Path Changed** parameters used

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Option Path</td>
<td>System Hardening Monitor &gt; System Security Configuration</td>
</tr>
<tr>
<td>Option</td>
<td>Path Changed</td>
</tr>
<tr>
<td>Rule Name</td>
<td>Path_Changed</td>
</tr>
</tbody>
</table>
### Table 6-130 Description of the **Path Changed** parameters used (continued)

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Severity</td>
<td>Warning</td>
</tr>
<tr>
<td>Registry Keys</td>
<td><code>\HKEY_LOCAL_MACHINE\SYSTEM\*ControlSet\Control\Session Manager\Environment\Path</code></td>
</tr>
<tr>
<td>Description</td>
<td>Detects any changes or attempted changes to the <code>HKLM\SYSTEM\CurrentControlSet\Control\Session Manager\Environment</code> key <code>Path</code> value. This value determines the directory search order for all open applications on your target system.</td>
</tr>
</tbody>
</table>

### Table 6-131 Description of the **SubmitControl Changed** parameters used

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Option Path</td>
<td>System Hardening Monitor &gt; System Security Configuration</td>
</tr>
<tr>
<td>Option</td>
<td>SubmitControl Changed</td>
</tr>
<tr>
<td>Rule Name</td>
<td>SubmitControl_Changed</td>
</tr>
<tr>
<td>Severity</td>
<td>Warning</td>
</tr>
<tr>
<td>Registry Keys</td>
<td><code>\HKEY_LOCAL_MACHINE\SYSTEM\*ControlSet\Control\Lsa\SubmitControl</code></td>
</tr>
<tr>
<td>Description</td>
<td>Detects any changes or attempted changes to the <code>HKLM\SYSTEM\CurrentControlSet\Control\Lsa</code> key <code>SubmitControl</code> value. This value gives other users (e.g., Server Operators) permission to issue AT commands.</td>
</tr>
</tbody>
</table>

### Table 6-132 Description of the **SystemDirectoryChanged** parameters used

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Option Path</td>
<td>System Hardening Monitor &gt; System Security Configuration</td>
</tr>
<tr>
<td>Option</td>
<td>SystemDirectory Changed</td>
</tr>
<tr>
<td>Rule Name</td>
<td>SystemDirectory_Changed</td>
</tr>
<tr>
<td>Severity</td>
<td>Warning</td>
</tr>
<tr>
<td>Registry Keys</td>
<td><code>\HKEY_LOCAL_MACHINE\SYSTEM\*ControlSet\Control\Windows\SystemDirectory</code></td>
</tr>
<tr>
<td>Description</td>
<td></td>
</tr>
</tbody>
</table>
Table 6-132  Description of the **SystemDirectory Changed** parameters used (continued)

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Description</strong></td>
<td>Detects any changes or attempted changes to the HKLM\SYSTEM\CurrentControlSet\Control\Windows key SystemDirectory value. This value contains the entries that define the system directories for the Win32 subsystem.</td>
</tr>
</tbody>
</table>

Table 6-133  Description of the **Users Connect Count Changed** parameters used

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Option Path</strong></td>
<td>System Hardening Monitor &gt; System Security Configuration</td>
</tr>
<tr>
<td><strong>Option</strong></td>
<td>Users Connect Count Changed</td>
</tr>
<tr>
<td><strong>Rule Name</strong></td>
<td>Users_Connect_Count_Changed</td>
</tr>
<tr>
<td><strong>Severity</strong></td>
<td>Info</td>
</tr>
<tr>
<td><strong>Registry Keys</strong></td>
<td><code>\HKEY_LOCAL_MACHINE\SYSTEM\*\ControlSet*\Services\LanmanServer\Parameters\Users</code></td>
</tr>
<tr>
<td><strong>Description</strong></td>
<td>Detects any changes or attempted changes to the HKLM\SYSTEM\CurrentControlSet\Services\LanManServer\Parameters key Users value for changes. This value is responsible for allowing more than 10 clients to connect to a computer.</td>
</tr>
</tbody>
</table>

Table 6-134  Description of the **VDD Changed** parameters used

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Option Path</strong></td>
<td>System Hardening Monitor &gt; System Security Configuration</td>
</tr>
<tr>
<td><strong>Option</strong></td>
<td>VDD Changed</td>
</tr>
<tr>
<td><strong>Rule Name</strong></td>
<td>VDD_Changed</td>
</tr>
<tr>
<td><strong>Severity</strong></td>
<td>Warning</td>
</tr>
<tr>
<td><strong>Registry Keys</strong></td>
<td><code>\HKEY_LOCAL_MACHINE\SYSTEM\*\ControlSet*\Control\VirtualDeviceDrivers\VDD</code></td>
</tr>
<tr>
<td><strong>Description</strong></td>
<td>Detects any changes or attempted changes to the HKLM\SYSTEM\CurrentControlSet\Control\VirtualDeviceDrivers key VDD value. This value is responsible for determining which virtual device drivers are used on program install.</td>
</tr>
</tbody>
</table>
Table 6-135  Description of the **AddPrintDrivers Changed** parameters used

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Option Path</td>
<td>System Hardening Monitor &gt; System Security Configuration</td>
</tr>
<tr>
<td>Option</td>
<td>AddPrintDrivers Changed</td>
</tr>
<tr>
<td>Rule Name</td>
<td>AddPrintDrivers_Changed</td>
</tr>
<tr>
<td>Severity</td>
<td>Warning</td>
</tr>
<tr>
<td>Registry Keys</td>
<td>\HKEY_LOCAL_MACHINE\SYSTEM*\ControlSet\Control\Print\Providers\LanMan Print Services\Servers\AddPrinterDrivers</td>
</tr>
<tr>
<td>Description</td>
<td>Detects any changes or attempted changes to the \HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Print\Providers\LanMan Print Services\Servers key AddPrinterDrivers value. This value restricts the installation of printer drivers to only Administrators and Print Operators.</td>
</tr>
</tbody>
</table>

Table 6-136  Description of the **RestrictAnonymous Changed** parameters used

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Option Path</td>
<td>System Hardening Monitor &gt; System Security Configuration</td>
</tr>
<tr>
<td>Option</td>
<td>RestrictAnonymous Changed</td>
</tr>
<tr>
<td>Rule Name</td>
<td>RestrictAnonymous_Changed</td>
</tr>
<tr>
<td>Severity</td>
<td>Warning</td>
</tr>
<tr>
<td>Registry Keys</td>
<td>\HKEY_LOCAL_MACHINE\SYSTEM*\ControlSet\Control\Lsa\RestrictAnonymous</td>
</tr>
<tr>
<td>Description</td>
<td>Detects any changes to the \HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Lsa\RestrictAnonymous key. This value is responsible for restricting who has access to the registry.</td>
</tr>
</tbody>
</table>

Table 6-137  Description of the **Driver Signing Changed** parameters used

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Option Path</td>
<td>System Hardening Monitor &gt; System Security Configuration</td>
</tr>
<tr>
<td>Option</td>
<td>Driver Signing Changed</td>
</tr>
<tr>
<td>Rule Name</td>
<td>Driver_Signing_Changed</td>
</tr>
</tbody>
</table>
### Table 6-137 Description of the **Driver Signing Changed** parameters used (continued)

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Severity</td>
<td>Warning</td>
</tr>
<tr>
<td>Registry Keys</td>
<td>\HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\DriverSigning\PolicyRegistryKeys</td>
</tr>
<tr>
<td>Description</td>
<td>Detects any changes or attempted changes to the \HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Driver Signing key Policy value. This value is responsible for determining what to do when an attempt is made to install a driver without a valid Catalog file.</td>
</tr>
</tbody>
</table>

### Table 6-138 Description of the **Non Driver Signing Changed** parameters used

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Option Path</td>
<td>System Hardening Monitor &gt; System Security Configuration</td>
</tr>
<tr>
<td>Option</td>
<td>Non Driver Signing Changed</td>
</tr>
<tr>
<td>Rule Name</td>
<td>Non_Driver_Signing_Changed</td>
</tr>
<tr>
<td>Severity</td>
<td>Warning</td>
</tr>
<tr>
<td>Registry Keys</td>
<td>\HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Non-DriverSigning\PolicyRegistryKeys</td>
</tr>
<tr>
<td>Description</td>
<td>Detects any changes or attempted changes to the \HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Non-Driver Signing key Policy value. This value is responsible for allowing unsigned drivers to be installed.</td>
</tr>
</tbody>
</table>

### Table 6-139 Description of the **Local Auto Logoff Changed** parameters used

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Option Path</td>
<td>System Hardening Monitor &gt; System Security Configuration</td>
</tr>
<tr>
<td>Option</td>
<td>Local Auto Logoff Changed</td>
</tr>
<tr>
<td>Rule Name</td>
<td>Local_Auto_Logoff_Changed</td>
</tr>
<tr>
<td>Severity</td>
<td>Warning</td>
</tr>
<tr>
<td>Registry Keys</td>
<td>\HKEY_LOCAL_MACHINE\SYSTEM*ControlSet*\Services\lanmanserver\parameters\enableforcedlogoff</td>
</tr>
</tbody>
</table>
Table 6-139 Description of the **Local Auto Logoff Changed** parameters used

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Description</td>
<td>Detects any changes or attempted changes to the HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\lanmanserver\parameters\enableforcedlogoff key. This key is responsible for automatically logging off users when logon time expires (local).</td>
</tr>
</tbody>
</table>

Table 6-140 Description of the **FullPrivilegeAuditing Changed** parameters used

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Option Path</td>
<td>System Hardening Monitor &gt; System Security Configuration</td>
</tr>
<tr>
<td>Option</td>
<td>FullPrivilegeAuditing Changed</td>
</tr>
<tr>
<td>Rule Name</td>
<td>FullPrivilegeAuditing_Changed</td>
</tr>
<tr>
<td>Severity</td>
<td>Warning</td>
</tr>
<tr>
<td>Registry Keys</td>
<td>\HKEY_LOCAL_MACHINE\SYSTEM*ControlSet*\Control\Lsa\fullprivilegeauditing</td>
</tr>
<tr>
<td>Description</td>
<td>Detects any changes or attempted changes to the \HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Lsa\fullprivilegeauditing value. This value is responsible for the Backup and Restore privileges in the user rights audit class.</td>
</tr>
</tbody>
</table>

Table 6-141 Description of the **SmartCard Behavior Changed** parameters used

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Option Path</td>
<td>System Hardening Monitor &gt; System Security Configuration</td>
</tr>
<tr>
<td>Option</td>
<td>SmartCard Behavior Changed</td>
</tr>
<tr>
<td>Rule Name</td>
<td>SmartCard_Behavior_Changed</td>
</tr>
<tr>
<td>Severity</td>
<td>Warning</td>
</tr>
<tr>
<td>Registry Keys</td>
<td>\HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon\scremoveoption</td>
</tr>
<tr>
<td>Description</td>
<td>Detects any changes or attempted changes to the HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon\scremoveoption key scremoveoption value. This value locks the computer when a smart card is removed.</td>
</tr>
</tbody>
</table>
### Table 6-142: Description of the **Recovery Console Changed** parameters used

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Option Path</td>
<td>System Hardening Monitor &gt; System Security Configuration</td>
</tr>
<tr>
<td>Option</td>
<td>Recovery Console Changed</td>
</tr>
<tr>
<td>Rule Name</td>
<td>Recovery_Console_Changed</td>
</tr>
<tr>
<td>Severity</td>
<td>Warning</td>
</tr>
<tr>
<td>Registry Keys</td>
<td><code>\HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\WindowsNT\CurrentVersion\Setup\RecoveryConsole\*</code></td>
</tr>
<tr>
<td>Description</td>
<td>Detects any changes or attempted changes to the HKLM\SOFTWARE\Microsoft\WindowsNT\CurrentVersion\Setup\RecoveryConsole\SecurityLevel and SetCommand keys. These keys determine if the Recovery Console is to be used when Windows crashes.</td>
</tr>
</tbody>
</table>

### Table 6-143: Description of the **NTFS MediaEject Changed** parameters used

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Option Path</td>
<td>System Hardening Monitor &gt; System Security Configuration</td>
</tr>
<tr>
<td>Option</td>
<td>NTFS MediaEject Changed</td>
</tr>
<tr>
<td>Rule Name</td>
<td>NTFS_MediaEject_Changed</td>
</tr>
<tr>
<td>Severity</td>
<td>Warning</td>
</tr>
<tr>
<td>Registry Keys</td>
<td><code>\HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon\allocatedasd</code></td>
</tr>
<tr>
<td>Description</td>
<td>Detects any changes or attempted changes to the HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon\allocatedasd key. This value determines whether the ability to access removable drives is available to other users.</td>
</tr>
</tbody>
</table>

### Table 6-144: Description of the **CTRL ALT DEL for Logon Changed** parameters used

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Option Path</td>
<td>System Hardening Monitor &gt; System Security Configuration</td>
</tr>
<tr>
<td>Option</td>
<td>CTRL ALT DEL for Logon Changed</td>
</tr>
</tbody>
</table>
Table 6-144  Description of the **CTRL ALT DEL for Logon Changed** parameters used (continued)

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Rule Name</td>
<td>CTRL_ALTERN_BYTE_DEL for Logon Changed</td>
</tr>
<tr>
<td>Severity</td>
<td>Warning</td>
</tr>
<tr>
<td>Registry Keys</td>
<td><code>\HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\policies\system\disablecad</code></td>
</tr>
<tr>
<td>Description</td>
<td>Detects any changes or attempted changes to the <code>HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\policies\system\disablecad</code> key. This value controls whether users are required to press Ctrl + Alt + Delete before logging into the system.</td>
</tr>
</tbody>
</table>

Table 6-145  Description of the **Protection Mode Changed** parameters used

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Option Path</td>
<td>System Hardening Monitor &gt; System Security Configuration</td>
</tr>
<tr>
<td>Option</td>
<td>Protection Mode Changed</td>
</tr>
<tr>
<td>Rule Name</td>
<td>Protection_Mode_Changed</td>
</tr>
<tr>
<td>Severity</td>
<td>Warning</td>
</tr>
<tr>
<td>Registry Keys</td>
<td><code>\HKEY_LOCAL_MACHINE\SYSTEM\*ControlSet\Control\Session Manager\ProtectionMode</code></td>
</tr>
<tr>
<td>Description</td>
<td>Detects any changes to the <code>HKEY_LOCAL_MACHINE\SYSTEM\*ControlSet\Control\Session Manager\ProtectionMode</code> key. This key is responsible for strengthening default permissions of global system objects.</td>
</tr>
</tbody>
</table>

Table 6-146  Description of the **Plaintext Password Changed** parameters used

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Option Path</td>
<td>System Hardening Monitor &gt; System Security Configuration</td>
</tr>
<tr>
<td>Option</td>
<td>Plaintext Password Changed</td>
</tr>
<tr>
<td>Rule Name</td>
<td>Plaintext_Password_Changed</td>
</tr>
<tr>
<td>Severity</td>
<td>Warning</td>
</tr>
</tbody>
</table>

### Table 6-146
Description of the **Plaintext Password Changed** parameters used (continued)

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Registry Keys</td>
<td>HKEY_LOCAL_MACHINE\SYSTEM*ControlSet*\Services\lanmanworkstation\parameters\enableplaintextpassword</td>
</tr>
<tr>
<td>Description</td>
<td>Detects any changes to the HKEY_LOCAL_MACHINE\SYSTEMCurrentControlSet\Services\lanmanworkstation\parameters\enableplaintextpassword key. This key enables unencrypted passwords to connect to third-party SMB servers.</td>
</tr>
</tbody>
</table>

### Table 6-147
Description of the **CrashOnAuditFail Changed** parameters used

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Option Path</td>
<td>System Hardening Monitor &gt; System Security Configuration</td>
</tr>
<tr>
<td>Option</td>
<td>CrashOnAuditFail Changed</td>
</tr>
<tr>
<td>Rule Name</td>
<td>CrashOnAuditFail_Changed</td>
</tr>
<tr>
<td>Severity</td>
<td>Warning</td>
</tr>
<tr>
<td>Registry Keys</td>
<td>\HKEY_LOCAL_MACHINE\SYSTEM*ControlSet*\Control\Lsa\crashonauditfail</td>
</tr>
<tr>
<td>Description</td>
<td>Detects any changes or attempted changes to the \HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Lsa key crashonauditfail value. This value determines system behavior when the Security log (Event Viewer) is full.</td>
</tr>
</tbody>
</table>

### Table 6-148
Description of the **Sys Maintenance RegKey Changed** parameters used

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Option Path</td>
<td>System Hardening Monitor &gt; System Security Configuration</td>
</tr>
<tr>
<td>Option</td>
<td>Sys Maintenance RegKey Changed</td>
</tr>
<tr>
<td>Rule Name</td>
<td>Sys_Maintenance_RegKey_Changed</td>
</tr>
<tr>
<td>Severity</td>
<td>Warning</td>
</tr>
<tr>
<td>Registry Keys</td>
<td>\HKEY_LOCAL_MACHINE\SYSTEM*ControlSet*\Services\Netlogon\Parameters\DisablePasswordChange</td>
</tr>
</tbody>
</table>
Table 6-148 | Description of the **Sys Maintenance RegKey Changed** parameters used (continued)

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Description</td>
<td>Detects any changes to the HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Netlogon\Parameters\DisablePasswordChange key. This key enables system maintenance of account passwords.</td>
</tr>
</tbody>
</table>

Table 6-149 | Description of the **Secure Channel Sign RegKey Changed** parameters used

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Option Path</td>
<td>System Hardening Monitor &gt; System Security Configuration</td>
</tr>
<tr>
<td>Option</td>
<td>Secure Channel Sign RegKey Changed</td>
</tr>
<tr>
<td>Rule Name</td>
<td>Secure_Ch_Sign_Regkey_Changed</td>
</tr>
<tr>
<td>Severity</td>
<td>Warning</td>
</tr>
<tr>
<td>Registry Keys</td>
<td>\HKEY_LOCAL_MACHINE\SYSTEM*ControlSet*\Services\Netlogon\Parameters\signsecurechannel</td>
</tr>
<tr>
<td>Description</td>
<td>Detects any changes to the HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Netlogon\Parameters\signsecurechannel key. This key determines whether or not you require Secure Channel to digitally sign secure channel data, when possible.</td>
</tr>
</tbody>
</table>

Table 6-150 | Description of the **Secure Channel Always RegKey Changed** parameters used

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Option Path</td>
<td>System Hardening Monitor &gt; System Security Configuration</td>
</tr>
<tr>
<td>Option</td>
<td>Secure Channel Always RegKey Changed</td>
</tr>
<tr>
<td>Rule Name</td>
<td>Secure_Ch_Always_Regkey_Changed</td>
</tr>
<tr>
<td>Severity</td>
<td>Warning</td>
</tr>
<tr>
<td>Registry Keys</td>
<td>\HKEY_LOCAL_MACHINE\SYSTEM\ControlSet\Services\Netlogon\Parameters\requiresignorseal</td>
</tr>
</tbody>
</table>
Table 6-150  Description of the **Secure Channel Always RegKey Changed** parameters used *(continued)*

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Description</td>
<td>Detects any changes to the HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Netlogon\Parameters\requiresignorseal key. This key determines whether or not you always require Secure Channel to digitally encrypt or sign secure channel data.</td>
</tr>
</tbody>
</table>

Table 6-151  Description of the **Secure Channel Strong RegKey Changed** parameters used

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Option Path</td>
<td>System Hardening Monitor &gt; System Security Configuration</td>
</tr>
<tr>
<td>Option</td>
<td>Secure Channel Strong RegKey Changed</td>
</tr>
<tr>
<td>Rule Name</td>
<td>Secure_Ch_Strong_Regkey_Changed</td>
</tr>
<tr>
<td>Severity</td>
<td>Warning</td>
</tr>
<tr>
<td>Registry Keys</td>
<td><code>\HKEY_LOCAL_MACHINE\SYSTEM\*ControlSet\Services\Netlogon\Parameters\requirestrongkey</code></td>
</tr>
<tr>
<td>Description</td>
<td>Detects any changes to the HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Netlogon\Parameters\requirestrongkey key. This key determines whether or not you require Secure Channel to require strong session key.</td>
</tr>
</tbody>
</table>

Table 6-152  Description of the **Secure Channel Encrypt Required RegKey Changed** parameters used

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Option Path</td>
<td>System Hardening Monitor &gt; System Security Configuration</td>
</tr>
<tr>
<td>Option</td>
<td>SecureChannel Encrypt Required RegKey Changed</td>
</tr>
<tr>
<td>Rule Name</td>
<td>SecureCh_Encrypt_RegKey_Changed</td>
</tr>
<tr>
<td>Severity</td>
<td>Warning</td>
</tr>
<tr>
<td>Registry Keys</td>
<td><code>\HKEY_LOCAL_MACHINE\SYSTEM\*ControlSet\Services\Netlogon\Parameters\sealsecurechannel</code></td>
</tr>
</tbody>
</table>
Table 6-152 Description of the Secure Channel Encrypt Required RegKey Changed parameters used (continued)

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Description</td>
<td>Detects any changes to the HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Netlogon \Parameters\sealsecurechannel key. This key determines whether or not you require Secure Channel to digitally encrypt secure channel data, when possible.</td>
</tr>
</tbody>
</table>

System startstop options

This option group subsection detects changes to the various registry keys that deal with typical startup and shutdown settings. See the rule descriptions for further information on rule function.

Table 6-153 Description of the BootExecute Changed parameters used

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Option Path</td>
<td>System Hardening Monitor &gt; System StartStop Options</td>
</tr>
<tr>
<td>Option</td>
<td>BootExecute Changed</td>
</tr>
<tr>
<td>Rule Name</td>
<td>BootExecute_Changed</td>
</tr>
<tr>
<td>Severity</td>
<td>Critical</td>
</tr>
<tr>
<td>Registry Keys</td>
<td>\HKEY_LOCAL_MACHINE\SYSTEM*ControlSet*Control\Session Manager\BootExecute</td>
</tr>
<tr>
<td>Description</td>
<td>Detects any changes or attempted changes to the HKLM\SYSTEM\CurrentControlSet\Control\SessionManager key BootExecute value. This value contains the names and arguments of programs that the Session Manager executes.</td>
</tr>
</tbody>
</table>

Table 6-154 Description of the CacheLogonsCount Changed parameters used

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Option Path</td>
<td>System Hardening Monitor &gt; System StartStop Options</td>
</tr>
<tr>
<td>Option</td>
<td>CacheLogonsCount Changed</td>
</tr>
<tr>
<td>Rule Name</td>
<td>CacheLogonsCount_Changed</td>
</tr>
<tr>
<td>Severity</td>
<td>Warning</td>
</tr>
</tbody>
</table>
### Table 6-154 Description of the CacheLogonsCount Changed parameters used

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Registry Keys</td>
<td>HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon\cachedlogonscount</td>
</tr>
<tr>
<td>Description</td>
<td>Detects any changes or attempted changes to the HKLM\SOFTWARE\Microsoft\WindowsNT\CurrentVersion\Winlogon key CachedLogonsCount value. This value controls the number of allowable cached logon attempts when the domain controller is unavailable.</td>
</tr>
</tbody>
</table>

### Table 6-155 Description of the ClearPageFileAtShutdown Changed parameters used

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Option Path</td>
<td>System Hardening Monitor &gt; System StartStop Options</td>
</tr>
<tr>
<td>Option</td>
<td>ClearPageFileAtShutdown Changed</td>
</tr>
<tr>
<td>Rule Name</td>
<td>ClearPageFileAtShutdown_Changed</td>
</tr>
<tr>
<td>Severity</td>
<td>Warning</td>
</tr>
<tr>
<td>Registry Keys</td>
<td>HKEY_LOCAL_MACHINE\SYSTEM*ControlSet\Control\Session Manager\Memory Management\ClearPageFileAtShutdown</td>
</tr>
<tr>
<td>Description</td>
<td>Detects any changes or attempted changes to the HKLM\SYSTEM\CurrentControlSet\Control\SessionManager\Memory Management key ClearPageFileAtShutdown value. This value determines whether Windows should clear the page file when the system is shut down.</td>
</tr>
</tbody>
</table>

### Table 6-156 Description of the PendingFileRenames Changed parameters used

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Option Path</td>
<td>System Hardening Monitor &gt; System StartStop Options</td>
</tr>
<tr>
<td>Option</td>
<td>PendingFileRenames Changed</td>
</tr>
<tr>
<td>Rule Name</td>
<td>PendingFileRenames_Changed</td>
</tr>
<tr>
<td>Severity</td>
<td>Warning</td>
</tr>
<tr>
<td>Registry Keys</td>
<td>HKEY_LOCAL_MACHINE\SYSTEM*ControlSet\Control\Session Manager\FileRenameOperations\PendingFileRenameOperations</td>
</tr>
<tr>
<td>Description</td>
<td></td>
</tr>
</tbody>
</table>
Table 6-156  Description of the **PendingFileRenames Changed** parameters used (continued)

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Description</td>
<td>Detects any changes or attempted changes to the HKLM\SYSTEM\CurrentControlSet\Control\SessionManager\FileRenameOperations key and the PendingFileRenameOperations value. This value determines which operations are run at system shutdown.</td>
</tr>
</tbody>
</table>

Table 6-157  Description of the **ReportBootOK Changed** parameters used

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Option Path</td>
<td>System Hardening Monitor &gt; System StartStop Options</td>
</tr>
<tr>
<td>Option</td>
<td>ReportBootOK Changed</td>
</tr>
<tr>
<td>Rule Name</td>
<td>ReportBootOK_Changed</td>
</tr>
<tr>
<td>Severity</td>
<td>Warning</td>
</tr>
<tr>
<td>Registry Keys</td>
<td>\HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon\ReportBootOk</td>
</tr>
<tr>
<td>Description</td>
<td>Detects any changes or attempted changes to the HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon key ReportBootOK value. This value helps to determine the meaning of the ControlSet.</td>
</tr>
</tbody>
</table>

Table 6-158  Description of the **ShutdownWithoutLogon Changed** parameters used

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Option Path</td>
<td>System Hardening Monitor &gt; System StartStop Options</td>
</tr>
<tr>
<td>Option</td>
<td>ShutdownWithoutLogon Changed</td>
</tr>
<tr>
<td>Rule Name</td>
<td>ShutdownWithoutLogon_Changed</td>
</tr>
<tr>
<td>Severity</td>
<td>Warning</td>
</tr>
<tr>
<td>Registry Keys</td>
<td>\HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon\ShutdownWithoutLogon</td>
</tr>
</tbody>
</table>
Table 6-158  Description of the **ShutdownWithoutLogon Changed** parameters used (continued)

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Description</td>
<td>Detects any changes or attempted changes to the HKLM\SOFTWARE\Microsoft\WindowsNT\CurrentVersion\Winlogon key ShutdownWithoutLogon value. This value determines whether you can shut down a system without logging on.</td>
</tr>
</tbody>
</table>

Table 6-159  Description of the **SystemStartOptions Changed** parameters used

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Option Path</td>
<td>System Hardening Monitor &gt; System StartStop Options</td>
</tr>
<tr>
<td>Option</td>
<td>SystemStartOptions Changed</td>
</tr>
<tr>
<td>Rule Name</td>
<td>SystemStartOptions_Changed</td>
</tr>
<tr>
<td>Severity</td>
<td>Warning</td>
</tr>
<tr>
<td>Registry Keys</td>
<td>\HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control \SystemStartOptions</td>
</tr>
<tr>
<td>Description</td>
<td>Detects any changes or attempted changes to the HKLM\SYSTEM\CurrentControlSet\Control key SystemStartOptions value. This value contains the text of system arguments that are passed to the system by the firmware. These values can be used to determine whether the debugger is enabled, the options that are set for ports and speed, and other configuration parameters.</td>
</tr>
</tbody>
</table>

**System audit tampering**

This option group subsection detects system auditing changes and the clearing of audit logs, which may be indicative of malicious activity or internal policy violation. The clearing of audit logs without legitimate intent is usually a sign of a malicious user or program attempting to hide its behavior.

**Note:** The first option, **Enable Date Restriction in Rule(s)**, provides the ability to only generate events in this section of the policy during a specific time window. This option provides tuning capabilities to monitor at specific times of the day that would make an administrator more suspicious of audit log mismanagement. For example, you would be more suspicious of such activity during non-business hours.
Table 6-160  Description of the **Audit Policy Changed** parameters used

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Option Path</td>
<td>System Hardening Monitor &gt; System Audit Tampering</td>
</tr>
<tr>
<td>Option</td>
<td>Audit Policy Changed</td>
</tr>
<tr>
<td>Rule Name</td>
<td>Audit_Policy_Changed</td>
</tr>
<tr>
<td>Severity</td>
<td>Warning</td>
</tr>
<tr>
<td>Description</td>
<td>Detects the changes to the system audit policy. See User Manager &gt; Policies &gt; Audit. The Windows operating system determines when the status of the auditing system has changed. When Windows determines the Audit Policy has changed, it reports the event.</td>
</tr>
</tbody>
</table>

Table 6-161  Description of the **Auditing Turned Off** parameters used

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Option Path</td>
<td>System Hardening Monitor &gt; System Audit Tampering</td>
</tr>
<tr>
<td>Option</td>
<td>Auditing Turned Off</td>
</tr>
<tr>
<td>Rule Name</td>
<td>Auditing_Turned_Off</td>
</tr>
<tr>
<td>Severity</td>
<td>Critical</td>
</tr>
<tr>
<td>Description</td>
<td>Detects Windows auditing being turned off. The Windows operating system determines when the status of the auditing system has changed. When Windows determines the auditing system has been turned off, it reports this event.</td>
</tr>
</tbody>
</table>

Table 6-162  Description of the **Auditing Turned On** parameters used

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Option Path</td>
<td>System Hardening Monitor &gt; System Audit Tampering</td>
</tr>
<tr>
<td>Option</td>
<td>Auditing Turned On</td>
</tr>
<tr>
<td>Rule Name</td>
<td>Auditing_Turned_On</td>
</tr>
<tr>
<td>Severity</td>
<td>Warning</td>
</tr>
<tr>
<td>Description</td>
<td>Detects Windows when the auditing system has been turned on. The Windows operating system determines when the status of the auditing system has changed. When Windows determines that the auditing system has been turned on, it reports this event.</td>
</tr>
</tbody>
</table>
**Table 6-163**  Description of the **Data Retention Changed** parameters used

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Option Path</td>
<td>System Hardening Monitor &gt; System Audit Tampering</td>
</tr>
<tr>
<td>Option</td>
<td>Data Retention Changed</td>
</tr>
<tr>
<td>Rule Name</td>
<td>Data_Retention_Changed</td>
</tr>
<tr>
<td>Severity</td>
<td>Warning</td>
</tr>
<tr>
<td>Registry Keys</td>
<td><code>\HKEY_LOCAL_MACHINE\SYSTEM\*ControlSet\Services\EventLog\Retention</code></td>
</tr>
<tr>
<td>Description</td>
<td>Detects the changes or attempted changes to the Retention value of the HKLM\System\CurrentControlSet\Services\EventLog\Application or System or Security&quot; key. This value determines the number of days for which audit logs are retained.</td>
</tr>
</tbody>
</table>

**Table 6-164**  Description of the **Security Log Events Deleted** parameters used

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Option Path</td>
<td>System Hardening Monitor &gt; System Audit Tampering</td>
</tr>
<tr>
<td>Option</td>
<td>Security Log Events Deleted</td>
</tr>
<tr>
<td>Rule Name</td>
<td>Security_Log_Events_Deleted</td>
</tr>
<tr>
<td>Severity</td>
<td>Critical</td>
</tr>
<tr>
<td>Event IDs</td>
<td>517, 1102</td>
</tr>
<tr>
<td>Description</td>
<td>Detects the clearing of security events from the Windows Event Viewer. The Windows operating system determines when the status of the auditing system has changed. When Windows determines that the security events log has been cleared, it reports this event.</td>
</tr>
</tbody>
</table>

**Table 6-165**  Description of the **Log File Size Changed** parameters used

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Option Path</td>
<td>System Hardening Monitor &gt; System Audit Tampering</td>
</tr>
<tr>
<td>Option</td>
<td>Log File Size Changed</td>
</tr>
<tr>
<td>Rule Name</td>
<td>Log_File_Size_Changed</td>
</tr>
<tr>
<td>Severity</td>
<td>Warning</td>
</tr>
</tbody>
</table>
### Table 6-165  Description of the **Log File Size Changed** parameters used (continued)

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Registry Keys</td>
<td><code>\HKEY_LOCAL_MACHINE\SYSTEM\*ControlSet\Services\EventLog\*\MaxSize</code></td>
</tr>
<tr>
<td>Description</td>
<td>Detects the changes or attempted changes to the MaxSize value of the HKLM\System\CurrentControlSet\Services\EventLog\Application or System or Security key. This value determines the maximum size of the audit log.</td>
</tr>
</tbody>
</table>

### Table 6-166  Description of the **Log File Location Changed** parameters used

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Option Path</td>
<td>System Hardening Monitor &gt; System Audit Tampering</td>
</tr>
<tr>
<td>Option</td>
<td>Log File Location Changed</td>
</tr>
<tr>
<td>Rule Name</td>
<td>Log_File_Location_Changed</td>
</tr>
<tr>
<td>Severity</td>
<td>Warning</td>
</tr>
<tr>
<td>Registry Keys</td>
<td><code>\HKEY_LOCAL_MACHINE\SYSTEM\*ControlSet\Services\EventLog\*\File</code></td>
</tr>
<tr>
<td>Description</td>
<td>Detects the changes or attempted changes to the File value of the HKLM\System\CurrentControlSet\Services\EventLog\Application or System or Security key. This value determines to which file the event log is written.</td>
</tr>
</tbody>
</table>

### Table 6-167  Description of the **Audit Changed thru HiddenKey** parameters used

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Option Path</td>
<td>System Hardening Monitor &gt; System Audit Tampering</td>
</tr>
<tr>
<td>Option</td>
<td>Audit Changed thru HiddenKey</td>
</tr>
<tr>
<td>Rule Name</td>
<td>Audit_Changed_thru_HiddenKey</td>
</tr>
<tr>
<td>Severity</td>
<td>Warning</td>
</tr>
<tr>
<td>Registry Keys</td>
<td><code>\HKEY_LOCAL_MACHINE\Security\Policy\PolAdtEv\*</code></td>
</tr>
<tr>
<td>Description</td>
<td>Detects the changes or attempted changes to HKLM\Security\Policy\PolAdtEv key. This value controls the auditing policy of the OS when it is read on an interval timeline.</td>
</tr>
</tbody>
</table>
System hardening user interactive

This option group subsection detects changes to the user-configured registry keys that affect the way the operating system handles various forms of network traffic. Changes to these areas may lower the security posture of the host system.

Table 6-168 Description of the EnableICMPRedirect Changed parameters used

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Option Path</td>
<td>System Hardening Monitor &gt; System Hardening User Interactive</td>
</tr>
<tr>
<td>Option</td>
<td>EnableICMPRedirect Changed</td>
</tr>
<tr>
<td>Rule Name</td>
<td>EnableICMPRedirect_Changed</td>
</tr>
<tr>
<td>Severity</td>
<td>Warning</td>
</tr>
<tr>
<td>Registry Keys</td>
<td>\HKEY_LOCAL_MACHINE\SYSTEM*ControlSet\Services\Tcpip\Parameters\EnableICMPRedirect</td>
</tr>
<tr>
<td></td>
<td>\HKEY_LOCAL_MACHINE\SYSTEM*ControlSet\Services\Tcpip\Parameters\EnableICMPRedirects</td>
</tr>
<tr>
<td>Description</td>
<td>Detects the changes to the \HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters key EnableICMPRedirect value. This value controls whether Windows alters its route table in response to ICMP redirect messages.</td>
</tr>
</tbody>
</table>

Table 6-169 Description of the KeepAliveTime Changed parameters used

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Option Path</td>
<td>System Hardening Monitor &gt; System Hardening User Interactive</td>
</tr>
<tr>
<td>Option</td>
<td>KeepAliveTime Changed</td>
</tr>
<tr>
<td>Rule Name</td>
<td>KeepAliveTime_Changed</td>
</tr>
<tr>
<td>Severity</td>
<td>Warning</td>
</tr>
<tr>
<td>Registry Keys</td>
<td>\HKEY_LOCAL_MACHINE\SYSTEM*ControlSet\Services\Tcpip\Parameters\KeepAliveTime</td>
</tr>
<tr>
<td>Description</td>
<td>Detects the changes to the \HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters key KeepAliveTime value. This value specifies the idle time of the connection in milliseconds, before the TCP begins sending the keepalives, if keepalives are enabled on the connection.</td>
</tr>
</tbody>
</table>
### Table 6-170 Description of the *PerformRouterDiscover Changed* parameters used

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Option Path</td>
<td>System Hardening Monitor &gt; System Hardening User Interactive</td>
</tr>
<tr>
<td>Option</td>
<td>PerformRouterDiscover Changed</td>
</tr>
<tr>
<td>Rule Name</td>
<td>PerformRouterDiscover_Changed</td>
</tr>
<tr>
<td>Severity</td>
<td>Warning</td>
</tr>
<tr>
<td>Registry Keys</td>
<td><code>\HKEY_LOCAL_MACHINE\SYSTEM\*ControlSet\Services\Tcpip\Parameters\PerformRouterDiscovery</code></td>
</tr>
<tr>
<td>Description</td>
<td>Detects the changes to the <code>\HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters</code> key <code>PerformRouterDiscovery</code> value. This value determines whether the ICMP Router Discovery Protocol is enabled, disabled, or enabled only if the DHCP sends the router discovery option.</td>
</tr>
</tbody>
</table>

### Table 6-171 Description of the *SynAttackProtect Changed* parameters used

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Option Path</td>
<td>System Hardening Monitor &gt; System Hardening User Interactive</td>
</tr>
<tr>
<td>Option</td>
<td>SynAttackProtect Changed</td>
</tr>
<tr>
<td>Rule Name</td>
<td>SynAttackProtect_Changed</td>
</tr>
<tr>
<td>Severity</td>
<td>Warning</td>
</tr>
<tr>
<td>Registry Keys</td>
<td><code>\HKEY_LOCAL_MACHINE\SYSTEM\*ControlSet\Services\Tcpip\Parameters\SynAttackProtect</code></td>
</tr>
<tr>
<td>Description</td>
<td>Detects the changes to the <code>\HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters</code> key <code>SynAttackProtect</code> value. This value controls the protection level for your computer against any SYN attacks.</td>
</tr>
</tbody>
</table>

### Table 6-172 Description of the *TcpMaxHalfOpen Changed* parameters used

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Option Path</td>
<td>System Hardening Monitor &gt; System Hardening User Interactive</td>
</tr>
<tr>
<td>Option</td>
<td>TcpMaxHalfOpen Changed</td>
</tr>
</tbody>
</table>

Table 6-172 Description of the **TcpMaxHalfOpen Changed** parameters used (continued)

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Rule Name</td>
<td>TcpMaxHalfOpen_Changed</td>
</tr>
<tr>
<td>Severity</td>
<td>Warning</td>
</tr>
<tr>
<td>Registry Keys</td>
<td>\HKEY_LOCAL_MACHINE\SYSTEM*ControlSet*\Services\Tcpip \Parameters\TcpMaxHalfOpen</td>
</tr>
<tr>
<td>Description</td>
<td>Detects the changes to the \HKEY_LOCAL_MACHINE\SYSTEM*ControlSet*\Services \Tcpip \Parameters key TcpMaxHalfOpen value. This value controls the number of connections in the SYN-RCVD state that are allowed before the SYN-ATTACK protection begins to operate.</td>
</tr>
</tbody>
</table>

Table 6-173 Description of the **TcpMaxHalfOpenRetried** parameters used

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Option Path</td>
<td>System Hardening Monitor &gt; System Hardening User Interactive</td>
</tr>
<tr>
<td>Option</td>
<td>TcpMaxHalfOpenRetried Changed</td>
</tr>
<tr>
<td>Rule Name</td>
<td>TcpMaxHalfOpenRetried_Changed</td>
</tr>
<tr>
<td>Severity</td>
<td>Warning</td>
</tr>
<tr>
<td>Registry Keys</td>
<td>\HKEY_LOCAL_MACHINE\SYSTEM*ControlSet*\Services\Tcpip \Parameters\TcpMaxHalfOpenRetried</td>
</tr>
<tr>
<td>Description</td>
<td>Detects the changes to the \HKEY_LOCAL_MACHINE\SYSTEM*ControlSet*\Services \Tcpip \Parameters key TcpMaxHalfOpenRetried value. This value controls the number of connections in the SYN-RCVD state for which there has been at least one retransmission of the SYN, before the SYN-ATTACK attack protection begins to operate.</td>
</tr>
</tbody>
</table>

**System file and directory monitor**

This option group section of the policy monitors for file and directory changes as well as for Windows share volume creation and deletion. 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 file shares configuration monitor

This option group section of the policy monitors file share creation and deletion. Unauthorized file share creation and deletion can indicate malicious activity or possible malware activity. In addition, the creation of unauthorized or unknown file shares on host systems may lower their security posture.

#### Table 6-174 Description of the **System Share Creation** parameters used

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Option Path</td>
<td>System Hardening Monitor &gt; System File Shares Configuration Monitor</td>
</tr>
<tr>
<td>Option</td>
<td>System Share Creation</td>
</tr>
<tr>
<td>Rule Name</td>
<td>Share_Creation</td>
</tr>
<tr>
<td>Severity</td>
<td>Warning</td>
</tr>
<tr>
<td>Registry Keys</td>
<td><code>\HKEY_LOCAL_MACHINE\SYSTEM\*ControlSet\*Services\LanmanServer\Shares\*</code></td>
</tr>
<tr>
<td>Description</td>
<td>Detects the creation of values under the HKLM\SYSTEM\CurrentControlSet\Services\LanmanServer\Shares key. This value determines whether a shared drive or folder is created on the system.</td>
</tr>
</tbody>
</table>

#### Table 6-175 Description of the **System Share Deletion** parameters used

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Option Path</td>
<td>System Hardening Monitor &gt; System File Shares Configuration Monitor</td>
</tr>
<tr>
<td>Option</td>
<td>System Share Deletion</td>
</tr>
<tr>
<td>Rule Name</td>
<td>Share_deletion</td>
</tr>
<tr>
<td>Severity</td>
<td>Warning</td>
</tr>
<tr>
<td>Registry Keys</td>
<td><code>\HKEY_LOCAL_MACHINE\SYSTEM\*ControlSet\*Services\LanmanServer\Shares\*</code></td>
</tr>
<tr>
<td>Description</td>
<td>Detects the deletion of values under the HKLM\SYSTEM\CurrentControlSet\Services\LanmanServer\Shares key. This value determines whether a shared drive or folder is deleted on the system.</td>
</tr>
</tbody>
</table>
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 Data Center Security: Server Advanced 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 filewatch 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.

A Monitor File Checksums option is available under the Monitor File Modification option for each type of file watched. This option enables the monitoring of a file’s checksum during a file modification event. It reports the real-time SHA-256 hash comparison to the Symantec Data Center Security: Server Advanced 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 Data Center Security: Server Advanced was last shut down. This option provides detection ability even if the Symantec Data Center Security: Server Advanced service or daemon is shut down. If a monitored file is changed, once the Symantec Data Center Security: Server Advanced 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.

For more information, see the file monitoring enhancements section of the Release Notes for Version 5.2.6 of the product.

Table 6-176  Description of the Dll Cache Files parameters used

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Option Path</td>
<td>System File and Directory Monitor &gt; System FileWatch Monitor</td>
</tr>
</tbody>
</table>
### Table 6-176 Description of the **Dll Cache Files** parameters used (continued)

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Option</td>
<td>Dll Cache Files</td>
</tr>
<tr>
<td>Rule Name</td>
<td>Baseline_FileWatch_Sys_Dll_Cache_Files</td>
</tr>
<tr>
<td>Severity</td>
<td>Warning</td>
</tr>
<tr>
<td>Monitor Paths</td>
<td>%SystemRoot\System32\dllcache*.cpl</td>
</tr>
<tr>
<td></td>
<td>%SystemRoot\System32\dllcache*.dll</td>
</tr>
<tr>
<td></td>
<td>%SystemRoot\System32\dllcache*.exe</td>
</tr>
<tr>
<td></td>
<td>%SystemRoot\System32\dllcache*.ocx</td>
</tr>
<tr>
<td></td>
<td>%SystemRoot\System32\dllcache*.sys</td>
</tr>
<tr>
<td>Monitor Ops</td>
<td>Deleted, Created, Modified</td>
</tr>
<tr>
<td>Report File Differences</td>
<td>Available, Not Enabled</td>
</tr>
<tr>
<td>Date and Time Restriction</td>
<td>Available, Not Enabled</td>
</tr>
<tr>
<td>Description</td>
<td>Lets you monitor the DLL cache files that the system maintains.</td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> 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.</td>
</tr>
</tbody>
</table>

### Table 6-177 Description of the **Driver Cache Files** parameters used

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Option Path</td>
<td>System File and Directory Monitor &gt; System FileWatch Monitor</td>
</tr>
<tr>
<td>Option</td>
<td>Driver Cache Files</td>
</tr>
<tr>
<td>Rule Name</td>
<td>Baseline_Filewatch_SYS_DriverCache_Files</td>
</tr>
<tr>
<td>Severity</td>
<td>Warning</td>
</tr>
<tr>
<td>Monitor Paths</td>
<td>%SystemRoot\DriverCache*</td>
</tr>
<tr>
<td>Monitor Ops</td>
<td>Deleted, Created, Modified</td>
</tr>
</tbody>
</table>
### Table 6-177  Description of the **Driver Cache Files** parameters used *(continued)*

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Report File Differences</td>
<td>Available, Not Enabled</td>
</tr>
<tr>
<td>Date and Time Restriction</td>
<td>Available, Not Enabled</td>
</tr>
<tr>
<td>Description</td>
<td>Lets you monitor the driver cache files that the system maintains.</td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> Symantec recommends that you only use the Report File Differences option on a select number of files. Enabling the reporting of file differences for a very large number of files, that is, more than 1000, 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.</td>
</tr>
</tbody>
</table>

### Table 6-178  Description of the **Security Database Files** parameters used

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Option Path</td>
<td>System File and Directory Monitor &gt; System FileWatch Monitor</td>
</tr>
<tr>
<td>Option</td>
<td>Security Database Files</td>
</tr>
<tr>
<td>Rule Name</td>
<td>Baseline_FileWatch_Sys_SecurityDB_Files</td>
</tr>
<tr>
<td>Severity</td>
<td>Warning</td>
</tr>
<tr>
<td>Monitor Paths</td>
<td>%SystemRoot%\security\templates*.inf</td>
</tr>
<tr>
<td></td>
<td>%SystemRoot%\security\database*.sdb</td>
</tr>
<tr>
<td>Monitor Ops</td>
<td>Deleted, Created, Modified</td>
</tr>
<tr>
<td>Report File Differences</td>
<td>Available, Not Enabled</td>
</tr>
<tr>
<td>Date and Time Restriction</td>
<td>Available, Not Enabled</td>
</tr>
<tr>
<td>Description</td>
<td>Lets you monitor the security database files that the system maintains.</td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> Symantec recommends that you only use the Report File Differences option on a select number of files. Enabling the reporting of file differences for a very large number of files, that is, more than 1000, 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.</td>
</tr>
<tr>
<td>Parameter</td>
<td>Description</td>
</tr>
<tr>
<td>-------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Option Path</td>
<td>System File and Directory Monitor &gt; System FileWatch Monitor</td>
</tr>
<tr>
<td>Option</td>
<td>Core System Files</td>
</tr>
<tr>
<td>Rule Name</td>
<td>Baseline/FileWatch/Sys/SecurityDB/Files</td>
</tr>
<tr>
<td>Severity</td>
<td>Warning</td>
</tr>
<tr>
<td>Monitor Paths</td>
<td>%ProgramFiles%/windows nt*.dll</td>
</tr>
<tr>
<td></td>
<td>%ProgramFiles%/windows nt*.exe</td>
</tr>
<tr>
<td></td>
<td>%ProgramFiles%/windows nt\accessories*.exe</td>
</tr>
<tr>
<td></td>
<td>%SystemRoot%/*.dll</td>
</tr>
<tr>
<td></td>
<td>%SystemRoot%/*.exe</td>
</tr>
<tr>
<td></td>
<td>%SystemRoot%/System32*.acm</td>
</tr>
<tr>
<td></td>
<td>%SystemRoot%/System32*.ax</td>
</tr>
<tr>
<td></td>
<td>%SystemRoot%/System32*.com</td>
</tr>
<tr>
<td></td>
<td>%SystemRoot%/System32*.cpl</td>
</tr>
<tr>
<td></td>
<td>%SystemRoot%/System32*.dll</td>
</tr>
<tr>
<td></td>
<td>%SystemRoot%/System32*.drv</td>
</tr>
<tr>
<td></td>
<td>%SystemRoot%/System32*.exe</td>
</tr>
<tr>
<td></td>
<td>%SystemRoot%/System32*.ocx</td>
</tr>
<tr>
<td></td>
<td>%SystemRoot%/System32*.scr</td>
</tr>
<tr>
<td></td>
<td>%SystemRoot%/System32*.sys</td>
</tr>
<tr>
<td></td>
<td>%SystemRoot%/System32\drivers*.dll</td>
</tr>
<tr>
<td></td>
<td>%SystemRoot%/System32\drivers*.sys</td>
</tr>
<tr>
<td></td>
<td>%SystemRoot%/System32\dsound.vxd</td>
</tr>
<tr>
<td></td>
<td>%SystemRoot%/system*.dll</td>
</tr>
<tr>
<td></td>
<td>%SystemRoot%/system*.drv</td>
</tr>
<tr>
<td>Monitor Ops</td>
<td>Deleted, Created, Modified</td>
</tr>
<tr>
<td>Report File</td>
<td>Available, Not Enabled</td>
</tr>
<tr>
<td>Differences</td>
<td></td>
</tr>
<tr>
<td>Date and Time</td>
<td>Available, Not Enabled</td>
</tr>
<tr>
<td>Restriction</td>
<td></td>
</tr>
</tbody>
</table>
### Table 6-179
**Description of the Core System Files parameters used (continued)**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Description</td>
<td>Lets you monitor Core System Executable Files. <strong>Note:</strong> Symantec recommends that you only use the Report File Differences option on a select number of files. Enabling the reporting of file differences for a very large number of files, that is, more than 1000, 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.</td>
</tr>
</tbody>
</table>

### Table 6-180
**Description of the Core System Configuration Files parameters used**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Option Path</td>
<td>System File and Directory Monitor &gt; System FileWatch Monitor</td>
</tr>
<tr>
<td>Option</td>
<td>Core System Configuration Files</td>
</tr>
<tr>
<td>Rule Name</td>
<td>Baseline_FileWatch_Sys_Core_Configuration_Files</td>
</tr>
<tr>
<td>Severity</td>
<td>Warning</td>
</tr>
<tr>
<td>Monitor Paths</td>
<td>%SystemRoot%\System32\AUTOEXEC.NT</td>
</tr>
<tr>
<td></td>
<td>%SystemRoot%\System32\CONFIG.NT</td>
</tr>
<tr>
<td></td>
<td>%SystemRoot%\System32\desktop.ini</td>
</tr>
<tr>
<td></td>
<td>%SystemRoot%\desktop.ini</td>
</tr>
<tr>
<td></td>
<td>%SystemRoot\system.ini</td>
</tr>
<tr>
<td></td>
<td>%SystemRoot%\win.ini</td>
</tr>
<tr>
<td>Monitor Ops</td>
<td>Deleted, Created, Modified</td>
</tr>
<tr>
<td>Report File Differences</td>
<td>Enabled</td>
</tr>
<tr>
<td>Date and Time Restriction</td>
<td>Available, Not Enabled</td>
</tr>
<tr>
<td>Description</td>
<td>Lets you monitor Core System Configuration Files. <strong>Note:</strong> You enable the Report File Differences option in this portion of the filewatch rule set. This option provides a good example of specific ini files. In them, reporting differences, such as strings that are removed or added, let you determine if the event should be escalated for investigation.</td>
</tr>
</tbody>
</table>
### Table 6-181  Description of the **Setup Dlls & Binaries** parameters used

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Option Path</td>
<td>System File and Directory Monitor &gt; System FileWatch Monitor</td>
</tr>
<tr>
<td>Option</td>
<td>Setup Dlls &amp; Binaries</td>
</tr>
<tr>
<td>Rule Name</td>
<td>Baseline_FileWatch_Sys_Setup_Files</td>
</tr>
<tr>
<td>Severity</td>
<td>Warning</td>
</tr>
</tbody>
</table>
| Monitor Paths      | %SystemRoot%\System32\Setup\*.dll  
                     | %SystemRoot%\System32\Setup\*.exe                                                                                                           |
| Monitor Ops        | Deleted, Created, Modified                                                                                                                   |
| Report File Differences | Available, Not Enabled                                                                                   |
| Date and Time Restriction | Available, Not Enabled                                                                                   |
| Description        | Lets you monitor setup DLLs & binaries.                                                                                                        |
| Note: Symantec recommends that you only use the Report File Differences option on a select number of files. Enabling the reporting of file differences for a very large number of files, that is, more than 1000, 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 6-182  Description of the **System WBEM Files** parameters used

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Option Path</td>
<td>System File and Directory Monitor &gt; System FileWatch Monitor</td>
</tr>
<tr>
<td>Option</td>
<td>System WBEM Files</td>
</tr>
<tr>
<td>Rule Name</td>
<td>Baseline_FileWatch_Sys_WBEM_Files</td>
</tr>
<tr>
<td>Severity</td>
<td>Warning</td>
</tr>
</tbody>
</table>
| Monitor Paths      | %SystemRoot%\System32\wbem\*.dll  
<pre><code>                 | %SystemRoot%\System32\wbem\*.exe                                                                                                           |
</code></pre>
<p>| Monitor Ops        | Deleted, Created, Modified                                                                                                                   |</p>
<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Report File Differences</td>
<td>Available, Not Enabled</td>
</tr>
<tr>
<td>Date and Time Restriction</td>
<td>Available, Not Enabled</td>
</tr>
<tr>
<td>Description</td>
<td>Lets you monitor System WBEM Files. <strong>Note:</strong> Symantec recommends that you only use the Report File Differences option on a select number of files. Enabling the reporting of file differences for a very large number of files, that is, more than 1000, 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.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Option Path</td>
<td>System File and Directory Monitor &gt; System FileWatch Monitor</td>
</tr>
<tr>
<td>Option</td>
<td>System Export Files</td>
</tr>
<tr>
<td>Rule Name</td>
<td>Baseline_FileWatch_Sys_Export_Files</td>
</tr>
<tr>
<td>Severity</td>
<td>Warning</td>
</tr>
<tr>
<td>Monitor Paths</td>
<td>%SystemRoot%\System32\export*.dll %SystemRoot%\System32\export*.exe</td>
</tr>
<tr>
<td>Monitor Ops</td>
<td>Deleted, Created, Modified</td>
</tr>
<tr>
<td>Report File Differences</td>
<td>Available, Not Enabled</td>
</tr>
<tr>
<td>Date and Time Restriction</td>
<td>Available, Not Enabled</td>
</tr>
<tr>
<td>Description</td>
<td>Lets you monitor System Export Files. <strong>Note:</strong> Symantec recommends that you only use the Report File Differences option on a select number of files. Enabling the reporting of file differences for a very large number of files, that is, more than 1000, 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.</td>
</tr>
</tbody>
</table>
### Table 6-184  Description of the **System OLE Support files** parameters used

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Option Path</strong></td>
<td>System File and Directory Monitor &gt; System FileWatch Monitor</td>
</tr>
<tr>
<td><strong>Option</strong></td>
<td>System OLE Support files</td>
</tr>
<tr>
<td><strong>Rule Name</strong></td>
<td>Baseline_FileWatch_Sys_OLESupport_Files</td>
</tr>
<tr>
<td><strong>Severity</strong></td>
<td>Warning</td>
</tr>
<tr>
<td><strong>Monitor Paths</strong></td>
<td>%CommonProgramFiles%\system\ado*.dll</td>
</tr>
<tr>
<td></td>
<td>%CommonProgramFiles%\system\oledb*.dll</td>
</tr>
<tr>
<td></td>
<td>%CommonProgramFiles%\system\msadc*.dll</td>
</tr>
<tr>
<td><strong>Monitor Ops</strong></td>
<td>Deleted, Created, Modified</td>
</tr>
<tr>
<td><strong>Report File Differences</strong></td>
<td>Available, Not Enabled</td>
</tr>
<tr>
<td><strong>Date and Time Restriction</strong></td>
<td>Available, Not Enabled</td>
</tr>
<tr>
<td><strong>Description</strong></td>
<td>Lets you monitor OLE Support Files.</td>
</tr>
</tbody>
</table>

**Note:** Symantec recommends that you only use the Report File Differences option on a select number of files. Enabling the reporting of file differences for a very large number of files, that is, more than 1000, 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 6-185  Description of the **Common Program Files** parameters used

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Option Path</strong></td>
<td>System File and Directory Monitor &gt; System FileWatch Monitor</td>
</tr>
<tr>
<td><strong>Option</strong></td>
<td>Common Program Files</td>
</tr>
<tr>
<td><strong>Rule Name</strong></td>
<td>Baseline_FileWatch_Sys_Common_Program_Files</td>
</tr>
<tr>
<td><strong>Severity</strong></td>
<td>Warning</td>
</tr>
<tr>
<td><strong>Monitor Paths</strong></td>
<td>%CommonProgramFiles%\system*.dll</td>
</tr>
<tr>
<td><strong>Monitor Ops</strong></td>
<td>Deleted, Created, Modified</td>
</tr>
</tbody>
</table>
Table 6-185  Description of the **Common Program Files** parameters used (continued)

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Report File Differences</td>
<td>Available, Not Enabled</td>
</tr>
<tr>
<td>Date and Time</td>
<td>Available, Not Enabled</td>
</tr>
<tr>
<td>Description</td>
<td>Lets you monitor Common Program Files.</td>
</tr>
<tr>
<td><strong>Note:</strong> Symantec</td>
<td>recommends that you only use the Report File Differences option on a select</td>
</tr>
<tr>
<td></td>
<td>number of files. Enabling the reporting of file differences for a very large</td>
</tr>
<tr>
<td></td>
<td>number of files, that is, more than 1000, may affect system resources.</td>
</tr>
<tr>
<td></td>
<td>Symantec recommends that you test scenarios if large numbers of files</td>
</tr>
<tr>
<td></td>
<td>require this detection functionality or if wildcard paths are used with this</td>
</tr>
<tr>
<td></td>
<td>feature.</td>
</tr>
</tbody>
</table>

Table 6-186  Description of the **Group Policy Files** parameters used

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Option Path</td>
<td>System File and Directory Monitor &gt; System FileWatch Monitor</td>
</tr>
<tr>
<td>Option</td>
<td>Group Policy Files</td>
</tr>
<tr>
<td>Rule Name</td>
<td>Baseline_FileWatch_Sys_Group_Policy_Files</td>
</tr>
<tr>
<td>Severity</td>
<td>Warning</td>
</tr>
<tr>
<td>Monitor Paths</td>
<td>%SystemRoot%\System32\GroupPolicy\gpt.ini</td>
</tr>
<tr>
<td></td>
<td>%SystemRoot%\System32\GroupPolicy\Machine\Scripts*</td>
</tr>
<tr>
<td></td>
<td>%SystemRoot%\System32\GroupPolicy\Machine\Registry.pol</td>
</tr>
<tr>
<td></td>
<td>%SystemRoot%\System32\GroupPolicy\User\Scripts*</td>
</tr>
<tr>
<td>Monitor Ops</td>
<td>Created, Accessed, Modified</td>
</tr>
<tr>
<td>Report File Differences</td>
<td>Available, Not Enabled</td>
</tr>
<tr>
<td>Date and Time</td>
<td>Available, Not Enabled</td>
</tr>
<tr>
<td>Restriction</td>
<td></td>
</tr>
</tbody>
</table>
### Table 6-186 Description of the **Group Policy Files** parameters used (continued)

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Description</td>
<td>Lets you monitor Group Policy Files. Symantec recommends that you only use the Report File Differences option on a select number of files. Enabling the reporting of file differences for a very large number of files, that is, more than 1000, 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.</td>
</tr>
</tbody>
</table>

### Table 6-187 Description of the **System IME Files** parameters used

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Option Path</td>
<td>System File and Directory Monitor &gt; System FileWatch Monitor</td>
</tr>
<tr>
<td>Option</td>
<td>System IME Files</td>
</tr>
<tr>
<td>Rule Name</td>
<td>Baseline_FileWatch_SysIME_Files</td>
</tr>
<tr>
<td>Severity</td>
<td>Warning</td>
</tr>
</tbody>
</table>
| Monitor Paths | %SystemRoot%\ime\*.dll  
%SystemRoot%\ime\*.exe  
%SystemRoot%\ime\chsime\applets\*.dll  
%SystemRoot%\ime\chtime\applets\*.dll  
%SystemRoot%\ime\shared\*.dll  
%SystemRoot%\ime\shared\*.exe  
%SystemRoot%\ime\shared\res\*.dll |
| Monitor Ops | Created, Delete, Modified |
| Report File Differences | Available, Not Enabled |
| Date and Time Restriction | Available, Not Enabled |
### Table 6-187 Description of the **System IME Files** parameters used (continued)

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Description</strong></td>
<td>Lets you monitor system IME Files. Symantec recommends that you only use the Report File Differences option on a select number of files. Enabling the reporting of file differences for a very large number of files, that is, more than 1000, 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.</td>
</tr>
</tbody>
</table>

### Table 6-188 Description of the **Monitor Script Files in System Folders** parameters used

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Option Path</strong></td>
<td>System File and Directory Monitor &gt; System FileWatch Monitor</td>
</tr>
<tr>
<td><strong>Option</strong></td>
<td>Monitor Script Files in System Folders</td>
</tr>
<tr>
<td><strong>Rule Name</strong></td>
<td>Baseline_FileWatch_Sys_Script_Files</td>
</tr>
<tr>
<td><strong>Severity</strong></td>
<td>Warning</td>
</tr>
<tr>
<td><strong>Monitor Paths</strong></td>
<td>%SystemRoot%*.js %SystemRoot%*.vbs %SystemRoot%\System32*.js %SystemRoot%\System32*.vbs</td>
</tr>
<tr>
<td><strong>Monitor Ops</strong></td>
<td>Deleted, Created, Modified</td>
</tr>
<tr>
<td><strong>Report File Differences</strong></td>
<td>Available, Not Enabled</td>
</tr>
<tr>
<td><strong>Date and Time Restriction</strong></td>
<td>Available, Not Enabled</td>
</tr>
<tr>
<td><strong>Description</strong></td>
<td>Lets you monitor Script Files, for example, JavaScript and VBScript files. Symantec recommends that you only use the Report File Differences option on a select number of files. Enabling the reporting of file differences for a very large number of files, that is, more than 1000, 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.</td>
</tr>
</tbody>
</table>
### Table 6-189  Description of the **Other Files (All Windows)** parameters used

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Option Path</td>
<td>System File and Directory Monitor &gt; System FileWatch Monitor</td>
</tr>
<tr>
<td>Option</td>
<td>Other Files (All Windows)</td>
</tr>
<tr>
<td>Rule Name</td>
<td>Baseline_FileWatch_Sys_Other_Files_All_Windows</td>
</tr>
<tr>
<td>Severity</td>
<td>Warning</td>
</tr>
<tr>
<td>Monitor Paths</td>
<td>%SystemRoot%\apppatch*.dll</td>
</tr>
<tr>
<td></td>
<td>%SystemRoot%\System32\os2\dll*.dll</td>
</tr>
<tr>
<td></td>
<td>%SystemRoot%\System32\CertSrv\cafixweb.exe</td>
</tr>
<tr>
<td></td>
<td>%SystemRoot%\System32\spool\drivers\w32x86*</td>
</tr>
<tr>
<td>Monitor Ops</td>
<td>Deleted, Created, Modified</td>
</tr>
<tr>
<td>Report File Differences</td>
<td>Available, Not Enabled</td>
</tr>
<tr>
<td>Date and Time Restriction</td>
<td>Available, Not Enabled</td>
</tr>
<tr>
<td>Description</td>
<td>Lets you monitor Other Critical System Files that are not included in any of the previous groups. Symantec recommends that you only use the Report File Differences option on a select number of files. Enabling the reporting of file differences for a very large number of files, that is, more than 1000, 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.</td>
</tr>
</tbody>
</table>

### Table 6-190  Description of the **Other Files (Not in NT)** parameters used

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Option Path</td>
<td>System File and Directory Monitor &gt; System FileWatch Monitor</td>
</tr>
<tr>
<td>Option</td>
<td>Other Files (Not in NT)</td>
</tr>
<tr>
<td>Rule Name</td>
<td>Baseline_FileWatch_Sys_Other_Files_Not_NT</td>
</tr>
<tr>
<td>Severity</td>
<td>Warning</td>
</tr>
</tbody>
</table>
Table 6-190  Description of the Other Files (Not in NT) parameters used (continued)

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
</table>
| Monitor Paths   | %SystemRoot%\msagent\*.dll  
|                 | %SystemRoot%\msagent\*.exe  
|                 | %SystemRoot%\msagent\intl\*.dll  
|                 | %SystemRoot%\srchasst\msgr3en.dll  
|                 | %SystemRoot%\srchasst\srchctls.dll  
|                 | %SystemRoot%\pchealth\helpctr\binaries\*.dll  
|                 | %SystemRoot%\pchealth\helpctr\binaries\*.exe  
|                 | %SystemRoot%\pchealth\uploadlb\binaries\*.exe  
|                 | %SystemRoot%\System32\ShellExt*  
|                 | %SystemRoot%\System32\Microsoft\Crypto\*  
|                 | %SystemRoot%\System32\Microsoft\Protect\*  
|                 | %SystemRoot%\System32\rpcproxy  |
| Monitor Ops     | Deleted, Created, Modified  |
| Report File Differences | Available, Not Enabled  |
| Date and Time Restriction | Available, Not Enabled  |
| Description     | Lets you monitor Other Critical System Files that are not present in NT and that are not included in any of the previous groups. Symantec recommends that you only use the Report File Differences option on a select number of files. Enabling the reporting of file differences for a very large number of files, that is, more than 1000, 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 6-191  Description of the Other Files (NT Only) parameters used

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Option Path</td>
<td>System File and Directory Monitor &gt; System FileWatch Monitor</td>
</tr>
<tr>
<td>Option</td>
<td>Other Files (NT Only)</td>
</tr>
</tbody>
</table>
Table 6-191: Description of the Other Files (NT Only) parameters used (continued)

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Rule Name</td>
<td>Baseline_FileWatch_Sys_Other_Files_NT_Only</td>
</tr>
<tr>
<td>Severity</td>
<td>Warning</td>
</tr>
<tr>
<td>Monitor Paths</td>
<td>%SystemRoot%System32\viewers*.<em>.dll %SystemRoot%System32\viewers*.</em>.exe</td>
</tr>
<tr>
<td>Monitor Ops</td>
<td>Deleted, Created, Modified</td>
</tr>
<tr>
<td>Report File Differences</td>
<td>Available, Not Enabled</td>
</tr>
<tr>
<td>Date and Time Restriction</td>
<td>Available, Not Enabled</td>
</tr>
<tr>
<td>Description</td>
<td>Lets you monitor Other Critical System Files that are not present in NT and that are not included in any of the previous groups. Symantec recommends that you only use the Report File Differences option on a select number of files. Enabling the reporting of file differences for a very large number of files, that is, more than 1000, 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.</td>
</tr>
</tbody>
</table>

System registry monitor

This option group section monitors addition, deletion, and modification attempts to critical Windows registry locations that are listed as monitored areas within this option group. If you use a default security posture, Symantec Data Center Security: Server Advanced automatically sets up the registry monitor for you. If you use your own security posture, you must select the registry paths that you want to monitor so that the registry monitor functions correctly.

A wide range of options are available for each rule to enable very specific tuning of how the registry entries are monitored.

System registry monitor - AutoStart keys

This subsection area of the policy monitors critical system auto start locations. Auto start registry key locations specify how specific software is started. Malware may
also use this location to add malicious entries to auto start applications without an administrator's knowledge.

Table 6-192 Description of the **AutoStart System Keys** parameters used

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Option Path</td>
<td>System Registry Monitor &gt; System Registry Monitor - AutoStart Keys</td>
</tr>
<tr>
<td>Option</td>
<td>AutoStart System Keys</td>
</tr>
<tr>
<td>Rule Name</td>
<td>Sys_AutoStart_Keys</td>
</tr>
<tr>
<td>Severity</td>
<td>Warning</td>
</tr>
<tr>
<td>Monitor Paths</td>
<td>\HKEY_LOCAL_MACHINE\Software\Classes*\shell*\command\</td>
</tr>
<tr>
<td></td>
<td>\HKEY_LOCAL_MACHINE\Software\Microsoft\Windows NT\CurrentVersion\Winlogon\</td>
</tr>
<tr>
<td></td>
<td>\HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\</td>
</tr>
<tr>
<td></td>
<td>Policies\System\</td>
</tr>
<tr>
<td></td>
<td>\HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run*</td>
</tr>
<tr>
<td></td>
<td>\HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\Windows\System\Scripts\</td>
</tr>
<tr>
<td></td>
<td>\HKEY_USERS*\Software\Classes*\shell*\command\</td>
</tr>
<tr>
<td></td>
<td>\HKEY_USERS*\Software\Microsoft\Windows NT\CurrentVersion\Windows\</td>
</tr>
<tr>
<td></td>
<td>\HKEY_USERS*\Software\Microsoft\Windows\NT\CurrentVersion\Winlogon*</td>
</tr>
<tr>
<td></td>
<td>\HKEY_USERS*\Software\Microsoft\Windows\CurrentVersion\Policies\System\</td>
</tr>
<tr>
<td></td>
<td>\HKEY_USERS*\Software\Microsoft\Windows\CurrentVersion\Run*</td>
</tr>
<tr>
<td></td>
<td>\HKEY_USERS*\Software\Policies\Microsoft\Windows\System\Scripts\</td>
</tr>
<tr>
<td>Monitor Ops</td>
<td>Created, Modified</td>
</tr>
<tr>
<td>Date and Time Restriction</td>
<td>Available, Not Enabled</td>
</tr>
<tr>
<td>Description</td>
<td>Lets you monitor default auto start registry key locations.</td>
</tr>
</tbody>
</table>

**Note:** This option group is set up to be very similar to the functions available in the System FileWatch Monitor.
### Table 6-193 Description of the **AutoStart Service Keys** parameters used

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Option Path</td>
<td>System Registry Monitor &gt; System Registry Monitor - AutoStart Keys</td>
</tr>
<tr>
<td>Option</td>
<td>AutoStart Service Keys</td>
</tr>
<tr>
<td>Rule Name</td>
<td>Sys_AutoStart_Service_Keys</td>
</tr>
<tr>
<td>Severity</td>
<td>Warning</td>
</tr>
</tbody>
</table>
| Monitor Paths| `\HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\WOW`  
                `\HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\*` |
| Monitor Ops  | Created, Modified                                                           |
| Date and Time| Available, Not Enabled                                                      |
| Restriction  |                                                                             |
| Description  | Lets you monitor service-specific auto start registry key locations.        |
|              | **Note:** This option group is set up to be very similar to the functions  |
|              | available in the System FileWatch Monitor.                                 |

### Table 6-194 Description of the **AutoStart System CMD Keys** parameters used

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Option Path</td>
<td>System Registry Monitor &gt; System Registry Monitor - AutoStart Keys</td>
</tr>
<tr>
<td>Option</td>
<td>AutoStart System CMD Keys</td>
</tr>
<tr>
<td>Rule Name</td>
<td>Sys_AutoStart_Injection_Keys</td>
</tr>
<tr>
<td>Severity</td>
<td>Warning</td>
</tr>
</tbody>
</table>
| Monitor Paths| `\HKEY_LOCAL_MACHINE\Software\Microsoft\Command Processor`  
                `\HKEY_USERS\Software\Microsoft\Command Processor\*` |
| Monitor Ops  | Created, Modified, Deleted                                                  |
| Date and Time| Available, Not Enabled                                                      |
| Restriction  |                                                                             |
| Description  | Lets you monitor system command processor auto start registry key locations.|
|              | **Note:** This option group is set up to be very similar to the functions  |
|              | available in the System FileWatch Monitor.                                 |
Table 6-195  Description of the **AutoStart Explorer Keys** parameters used

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Option Path</td>
<td>System Registry Monitor &gt; System Registry Monitor - AutoStart Keys</td>
</tr>
<tr>
<td>Option</td>
<td>AutoStart Explorer Keys</td>
</tr>
<tr>
<td>Rule Name</td>
<td>Sys_AutoStart_Explorer_Keys</td>
</tr>
<tr>
<td>Severity</td>
<td>Warning</td>
</tr>
<tr>
<td>Monitor Paths</td>
<td>\HKEY_LOCAL_MACHINE\Microsoft\Windows\CurrentVersion\ShellServiceObjectDelayLoad\</td>
</tr>
<tr>
<td></td>
<td>\HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\WOW\Control\Session Manager\Environment\</td>
</tr>
<tr>
<td></td>
<td>\HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer\Run\</td>
</tr>
<tr>
<td></td>
<td>\HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\ShellServiceObjectDelayLoad</td>
</tr>
<tr>
<td></td>
<td>\HKEY_USERS.Default\Environment\</td>
</tr>
<tr>
<td></td>
<td>\HKEY_USERS\S-?-???.\Environment\</td>
</tr>
<tr>
<td></td>
<td>\HKEY_USERS\S-?-???.\Environment\</td>
</tr>
<tr>
<td></td>
<td>\HKEY_USERS\S-?-???.\Environment\</td>
</tr>
<tr>
<td></td>
<td>\HKEY_USERS\S-?-???.\Environment\</td>
</tr>
</tbody>
</table>

| Monitor Ops        | Created, Modified                                                           |
| Date and Time      | Available, Not Enabled                                                      |
| Restriction        |                                                                             |
| Description        | Lets you monitor explorer environment-specific auto start registry key locations. |
| **Note:**          | This option group is set up to be very similar to the functions available in the System FileWatch Monitor. |

Table 6-196  Description of the **AutoStart System Injection Keys** parameters used

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Option Path</td>
<td>System Registry Monitor &gt; System Registry Monitor - AutoStart Keys</td>
</tr>
<tr>
<td>Option</td>
<td>AutoStart System Injection Keys</td>
</tr>
</tbody>
</table>
### System Symantec software monitor

This option group area of the policy contains monitoring functions for Symantec software. Currently the monitored ancillary applications are Symantec AntiVirus and Symantec Endpoint Security. The policy automatically detects if the host machine has Symantec AntiVirus and Symantec Endpoint Security installed. Therefore, even if both areas of monitoring are enabled, only one area detects and generates events. This behavior is to thwart double event generation, which could confuse an administrator.
Symantec antiVirus client communication

This portion of the policy detects alerts from Symantec AntiVirus client installations. This policy can be applied to all Windows hosts with Symantec AntiVirus client installations.

<table>
<thead>
<tr>
<th>Table 6-197</th>
<th>Description of the Virus Detected parameters used</th>
</tr>
</thead>
<tbody>
<tr>
<td>Parameter</td>
<td>Description</td>
</tr>
<tr>
<td>Option Path</td>
<td>System Symantec Software Monitor &gt; Symantec AntiVirus Client Communication</td>
</tr>
<tr>
<td>Option</td>
<td>Virus Detected</td>
</tr>
<tr>
<td>Rule Name</td>
<td>Virus_Detection</td>
</tr>
<tr>
<td>Severity</td>
<td>Critical</td>
</tr>
<tr>
<td>Event IDs</td>
<td>5</td>
</tr>
<tr>
<td>Description</td>
<td>Detects the discovery of a virus or Trojan horse by Symantec AntiVirus. 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.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Table 6-198</th>
<th>Description of the AntiVirus Service Stopped parameters used</th>
</tr>
</thead>
<tbody>
<tr>
<td>Parameter</td>
<td>Description</td>
</tr>
<tr>
<td>Option Path</td>
<td>System Symantec Software Monitor &gt; Symantec AntiVirus Client Communication</td>
</tr>
<tr>
<td>Option</td>
<td>AntiVirus Service Stopped</td>
</tr>
<tr>
<td>Rule Name</td>
<td>Antivirus_Service_Stopped</td>
</tr>
<tr>
<td>Severity</td>
<td>Warning</td>
</tr>
<tr>
<td>Event IDs</td>
<td>13</td>
</tr>
<tr>
<td>Description</td>
<td>Detects the stopping of the Symantec AntiVirus 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.</td>
</tr>
</tbody>
</table>
### Table 6-199  Description of the **AntiVirus Service Started** parameters used

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Option Path</td>
<td>System Symantec Software Monitor &gt; Symantec AntiVirus Client Communication</td>
</tr>
<tr>
<td>Option</td>
<td>AntiVirus Service Started</td>
</tr>
<tr>
<td>Rule Name</td>
<td>Antivirus_Service_Started</td>
</tr>
<tr>
<td>Severity</td>
<td>Notice</td>
</tr>
<tr>
<td>Event IDs</td>
<td>14</td>
</tr>
<tr>
<td>Description</td>
<td>Detects the starting of the Symantec AntiVirus 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.</td>
</tr>
</tbody>
</table>

### Table 6-200  Description of the **AntiVirus Scan Started** parameters used

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Option Path</td>
<td>System Symantec Software Monitor &gt; Symantec AntiVirus Client Communication</td>
</tr>
<tr>
<td>Option</td>
<td>AntiVirus Scan Started</td>
</tr>
<tr>
<td>Rule Name</td>
<td>AntiVirus_Scan_Started</td>
</tr>
<tr>
<td>Severity</td>
<td>Notice</td>
</tr>
<tr>
<td>Event IDs</td>
<td>3</td>
</tr>
<tr>
<td>Description</td>
<td>Detects the starting of a manual scan of a host with Symantec Antivirus. 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.</td>
</tr>
</tbody>
</table>

### Table 6-201  Description of the **AntiVirus Scan Canceled** parameters used

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Option Path</td>
<td>System Symantec Software Monitor &gt; Symantec AntiVirus Client Communication</td>
</tr>
<tr>
<td>Option</td>
<td>AntiVirus Scan Canceled</td>
</tr>
<tr>
<td>Rule Name</td>
<td>AntiVirus_Scan_Canceled</td>
</tr>
</tbody>
</table>
Table 6-201  Description of the **AntiVirus Scan Canceled** parameters used (continued)

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Severity</td>
<td>Warning</td>
</tr>
<tr>
<td>Event IDs</td>
<td>21</td>
</tr>
<tr>
<td>Description</td>
<td>Detects the canceling of a manual scan of a host with Symantec Antivirus. 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.</td>
</tr>
</tbody>
</table>

Table 6-202  Description of the **AntiVirus Scan Complete** parameters used

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Option Path</td>
<td>System Symantec Software Monitor &gt; Symantec AntiVirus Client Communication</td>
</tr>
<tr>
<td>Option</td>
<td>AntiVirus Scan Complete</td>
</tr>
<tr>
<td>Rule Name</td>
<td>AntiVirus_Scan_Complete</td>
</tr>
<tr>
<td>Severity</td>
<td>Notice</td>
</tr>
<tr>
<td>Event IDs</td>
<td>2</td>
</tr>
<tr>
<td>Description</td>
<td>Detects the completion of a manual scan of a host with Symantec Antivirus. 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.</td>
</tr>
</tbody>
</table>

Table 6-203  Description of the **New Virus Definition Loaded** parameters used

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Option Path</td>
<td>System Symantec Software Monitor &gt; Symantec AntiVirus Client Communication</td>
</tr>
<tr>
<td>Option</td>
<td>New Virus Definition Loaded</td>
</tr>
<tr>
<td>Rule Name</td>
<td>New_Virus_Defination_Loaded</td>
</tr>
<tr>
<td>Severity</td>
<td>Notice</td>
</tr>
<tr>
<td>Event IDs</td>
<td>7</td>
</tr>
</tbody>
</table>
Table 6-203 Description of the **New Virus Definition Loaded** parameters used (continued)

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Description</td>
<td>Detects the updating of Symantec Antivirus 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.</td>
</tr>
</tbody>
</table>

Table 6-204 Description of the **Virus Definitions are Current** parameters used

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Option Path</td>
<td>System Symantec Software Monitor &gt; Symantec AntiVirus Client Communication</td>
</tr>
<tr>
<td>Option</td>
<td>Virus Definitions are Current</td>
</tr>
<tr>
<td>Rule Name</td>
<td>Virus_Definitions_are_Current</td>
</tr>
<tr>
<td>Severity</td>
<td>Notice</td>
</tr>
<tr>
<td>Event IDs</td>
<td>16</td>
</tr>
<tr>
<td>Description</td>
<td>Detects that the installed virus definitions are current. Symantec AntiVirus issues the status messages for various application conditions and errors. When Symantec AntiVirus determines that the definitions are current, it reports this status.</td>
</tr>
</tbody>
</table>

Table 6-205 Description of the **AntiVirus Realtime Protection Loaded** parameters used

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Option Path</td>
<td>System Symantec Software Monitor &gt; Symantec AntiVirus Client Communication</td>
</tr>
<tr>
<td>Option</td>
<td>AntiVirus Realtime Protection Loaded</td>
</tr>
<tr>
<td>Rule Name</td>
<td>AntiVirus_Realtime_Protection_Loaded</td>
</tr>
<tr>
<td>Severity</td>
<td>Notice</td>
</tr>
<tr>
<td>Event IDs</td>
<td>23</td>
</tr>
<tr>
<td>Select Strings</td>
<td>:?Norton AntiVirus Source:*Symantec AntiVirus</td>
</tr>
</tbody>
</table>
### Table 6-205 Description of the **AntiVirus Realtime Protection Loaded** parameters used (continued)

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Description</td>
<td>Detects the enabling of the Symantec AntiVirus 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 enabled, it reports this status.</td>
</tr>
</tbody>
</table>

### Table 6-206 Description of the **AntiVirus Realtime Protection Disabled** parameters used

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Option Path</td>
<td>System Symantec Software Monitor &gt; Symantec AntiVirus Client Communication</td>
</tr>
<tr>
<td>Option</td>
<td>AntiVirus Realtime Protection Disabled</td>
</tr>
<tr>
<td>Rule Name</td>
<td>AntiVirus_Realtime_Protection_Disabled</td>
</tr>
<tr>
<td>Severity</td>
<td>Critical</td>
</tr>
<tr>
<td>Event IDs</td>
<td>24</td>
</tr>
<tr>
<td>Description</td>
<td>Detects the disabling of the Symantec AntiVirus 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.</td>
</tr>
</tbody>
</table>

### Table 6-207 Description of the **Virus Detected - Cleaned Failed** parameters used

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Option Path</td>
<td>System Symantec Software Monitor &gt; Symantec AntiVirus Client Communication</td>
</tr>
<tr>
<td>Option</td>
<td>Virus Detected - Cleaned Failed</td>
</tr>
<tr>
<td>Rule Name</td>
<td>Virus_Detected_Cleaned_Failed</td>
</tr>
<tr>
<td>Severity</td>
<td>Critical</td>
</tr>
<tr>
<td>Event IDs</td>
<td>5, 46, 51</td>
</tr>
</tbody>
</table>
Table 6-207  Description of the **Virus Detected - Cleaned Failed** parameters used *(continued)*

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Description</td>
<td>Detects the discovery of a virus or Trojan horse by Symantec AntiVirus. 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.</td>
</tr>
</tbody>
</table>

**Symantec Endpoint Protection client communication**

This portion of the policy detects alerts from Symantec Endpoint Protection client installations. This policy can be applied to all Windows hosts with Symantec Endpoint Protection client installations.

**Note:** This policy auto-detects if the client is running either Symantec Endpoint Protection or previous versions of Symantec AntiVirus.

Table 6-208  Description of the **Virus Detected** parameters used

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Option Path</td>
<td>System Symantec Software Monitor &gt; Symantec AntiVirus Client Communication</td>
</tr>
<tr>
<td>Option</td>
<td>Virus Detected</td>
</tr>
<tr>
<td>Rule Name</td>
<td>Virus_Detection</td>
</tr>
<tr>
<td>Severity</td>
<td>Critical</td>
</tr>
<tr>
<td>Event IDs</td>
<td>5, 46, 51</td>
</tr>
<tr>
<td>Description</td>
<td>Detects the discovery of a virus or Trojan horse by Symantec Endpoint Protection. 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.</td>
</tr>
</tbody>
</table>

Table 6-209  Description of the **SEP Service Stopped** parameters used

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Option Path</td>
<td>System Symantec Software Monitor &gt; Symantec AntiVirus Client Communication</td>
</tr>
</tbody>
</table>
### Table 6-209
Description of the **SEP Service Stopped** parameters used (continued)

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Option</td>
<td>SEP Service Stopped</td>
</tr>
<tr>
<td>Rule Name</td>
<td>SEP_Service_Stopped</td>
</tr>
<tr>
<td>Severity</td>
<td>Warning</td>
</tr>
<tr>
<td>Event IDs</td>
<td>13</td>
</tr>
</tbody>
</table>
| Select Strings     | !Norton AntiVirus  
Source:*Symantec AntiVirus  
Symantec?Endpoint?Protection?Services                                                                                                                                 |
| Description        | Detects the stopping of the Symantec Endpoint Protection service. Symantec Endpoint Protection issues the status messages for various application conditions and errors. When Symantec Endpoint Protection determines that SAV service has stopped, it reports this status. |

### Table 6-210
Description of the **SEP Service Started** parameters used

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Option Path</td>
<td>System Symantec Software Monitor &gt; Symantec AntiVirus Client Communication</td>
</tr>
<tr>
<td>Option</td>
<td>SEP Service Started</td>
</tr>
<tr>
<td>Rule Name</td>
<td>SEP_Service_Started</td>
</tr>
<tr>
<td>Severity</td>
<td>Notice</td>
</tr>
<tr>
<td>Event IDs</td>
<td>14</td>
</tr>
</tbody>
</table>
| Select Strings     | !Norton AntiVirus  
Source:*Symantec AntiVirus  
Symantec?Endpoint?Protection?Services                                                                                                                                 |
| Description        | Detects the starting of the Symantec Endpoint Protection service. Symantec Endpoint Protection issues the status messages for various application conditions and errors. When Symantec Endpoint Protection determines that the Symantec AntiVirus service has started, it reports this status. |
### Table 6-211  Description of the **SEP Scan Started** parameters used

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Option Path</td>
<td>System Symantec Software Monitor &gt; Symantec AntiVirus Client Communication</td>
</tr>
<tr>
<td>Option</td>
<td>SEP Scan Started</td>
</tr>
<tr>
<td>Rule Name</td>
<td>SEP_Scan Started</td>
</tr>
<tr>
<td>Severity</td>
<td>Notice</td>
</tr>
<tr>
<td>Event IDs</td>
<td>3</td>
</tr>
<tr>
<td>Select Strings</td>
<td>:?Norton AntiVirus Source:*Symantec AntiVirus</td>
</tr>
<tr>
<td>Description</td>
<td>Detects the starting of a manual scan of a host with Symantec Endpoint Protection. Symantec Endpoint Protection issues the status messages for various application conditions and errors. When Symantec Endpoint Protection determines that it has initiated a manual scan of the host, it reports this status.</td>
</tr>
</tbody>
</table>

### Table 6-212  Description of the **Scan Canceled** parameters used

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Option Path</td>
<td>System Symantec Software Monitor &gt; Symantec AntiVirus Client Communication</td>
</tr>
<tr>
<td>Option</td>
<td>Scan Canceled</td>
</tr>
<tr>
<td>Rule Name</td>
<td>SEP_Scan_Canceled</td>
</tr>
<tr>
<td>Severity</td>
<td>Warning</td>
</tr>
<tr>
<td>Event IDs</td>
<td>21</td>
</tr>
<tr>
<td>Select Strings</td>
<td>:?Norton AntiVirus Source:*Symantec AntiVirus</td>
</tr>
<tr>
<td>Description</td>
<td>Detects the canceling of a manual scan of a host with Symantec Endpoint Protection. Symantec Endpoint Protection issues the status messages for various application conditions. When Symantec Endpoint Protection determines that it has been commanded to cancel a manual scan, it reports this status.</td>
</tr>
</tbody>
</table>
Table 6-213  Description of the **SEP Scan Complete** parameters used

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Option Path</td>
<td>System Symantec Software Monitor &gt; Symantec AntiVirus Client Communication</td>
</tr>
<tr>
<td>Option</td>
<td>SEP Scan Complete</td>
</tr>
<tr>
<td>Rule Name</td>
<td>SEP_Scan_Complete</td>
</tr>
<tr>
<td>Severity</td>
<td>Notice</td>
</tr>
<tr>
<td>Event IDs</td>
<td>2</td>
</tr>
<tr>
<td>Select Strings</td>
<td>:?Norton AntiVirus Source:*Symantec AntiVirus</td>
</tr>
<tr>
<td>Description</td>
<td>Detects the completion of a manual scan of a host with Symantec Endpoint Protection. Symantec Endpoint Protection issues the status messages for various application conditions and errors. When Symantec Endpoint Protection determines that it has successfully completed a manual scan, it reports this status.</td>
</tr>
</tbody>
</table>

Table 6-214  Description of the **New Virus Definition Loaded** parameters used

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Option Path</td>
<td>System Symantec Software Monitor &gt; Symantec AntiVirus Client Communication</td>
</tr>
<tr>
<td>Option</td>
<td>New Virus Definition Loaded</td>
</tr>
<tr>
<td>Rule Name</td>
<td>New_Virus_Definition_Loaded</td>
</tr>
<tr>
<td>Severity</td>
<td>Notice</td>
</tr>
<tr>
<td>Event IDs</td>
<td>7</td>
</tr>
<tr>
<td>Description</td>
<td>Detects the updating of Symantec Endpoint Protection with the latest virus definitions. Symantec Endpoint Protection issues the status messages for various application conditions and errors. When Symantec Endpoint Protection determines that it has loaded a new virus definition file, it reports this status.</td>
</tr>
</tbody>
</table>
### Table 6-215  Description of the Virus Definitions are Current parameters used

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Option Path</td>
<td>System Symantec Software Monitor &gt; Symantec AntiVirus Client Communication</td>
</tr>
<tr>
<td>Option</td>
<td>Virus Definitions are Current</td>
</tr>
<tr>
<td>Rule Name</td>
<td>Virus_Definitions_are_Current</td>
</tr>
<tr>
<td>Severity</td>
<td>Notice</td>
</tr>
<tr>
<td>Event IDs</td>
<td>16</td>
</tr>
<tr>
<td>Description</td>
<td>Detects that the installed virus definitions are current. Symantec Endpoint Protection issues the status messages for various application conditions and errors. When Symantec Endpoint Protection determines that the definitions are current, it reports this status.</td>
</tr>
</tbody>
</table>

### Table 6-216  Description of the SEP Realtime Protection Loaded parameters used

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Option Path</td>
<td>System Symantec Software Monitor &gt; Symantec AntiVirus Client Communication</td>
</tr>
<tr>
<td>Option</td>
<td>SEP Realtime Protection Loaded</td>
</tr>
<tr>
<td>Rule Name</td>
<td>SEP_Realtime_Protection_Loaded</td>
</tr>
<tr>
<td>Severity</td>
<td>Notice</td>
</tr>
<tr>
<td>Event IDs</td>
<td>23</td>
</tr>
<tr>
<td>Select Strings</td>
<td>:?Norton AntiVirus Source:*Symantec AntiVirus</td>
</tr>
<tr>
<td>Description</td>
<td>This rule detects the enabling of the Symantec AntiVirus 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 enabled, it reports this status.</td>
</tr>
</tbody>
</table>
Table 6-217 Description of the **SEP Realtime Protection Disabled** parameters used

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Option Path</td>
<td>System Symantec Software Monitor &gt; Symantec AntiVirus Client Communication</td>
</tr>
<tr>
<td>Option</td>
<td>SEP Realtime Protection Disabled</td>
</tr>
<tr>
<td>Rule Name</td>
<td>SEP_Realtime_Protection_Disabled</td>
</tr>
<tr>
<td>Severity</td>
<td>Critical</td>
</tr>
<tr>
<td>Event IDs</td>
<td>24</td>
</tr>
<tr>
<td>Select Strings</td>
<td>:?Norton AntiVirus Source:*Symantec AntiVirus</td>
</tr>
<tr>
<td>Description</td>
<td>Detects the disabling of the Symantec Endpoint Protection real-time system protection option. Symantec Endpoint Protection issues the status messages for various application conditions and errors. When Symantec Endpoint Protection determines that the real-time protection option has been disabled, it reports this status.</td>
</tr>
</tbody>
</table>

Table 6-218 Description of the **Virus Detected - Cleaned Failed** parameters used

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Option Path</td>
<td>System Symantec Software Monitor &gt; Symantec AntiVirus Client Communication</td>
</tr>
<tr>
<td>Option</td>
<td>Virus Detected - Cleaned Failed</td>
</tr>
<tr>
<td>Rule Name</td>
<td>Virus_Detected_Cleaned_Failed</td>
</tr>
<tr>
<td>Severity</td>
<td>Critical</td>
</tr>
<tr>
<td>Event IDs</td>
<td>5, 46, 51</td>
</tr>
<tr>
<td>Description</td>
<td>Detects the discovery of a virus or Trojan horse by Symantec Endpoint Protection. 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 that the Symantec Endpoint Protection client was unable to clean, remove, or quarantine the identified malware. It also indicates that the risk is still present on the system. Immediate investigation is required.</td>
</tr>
</tbody>
</table>
System external device activity

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

USB device activity

This portion of the policy detects activity that is associated with USB devices.

<table>
<thead>
<tr>
<th>Table 6-219</th>
<th>Description of the <strong>USB Registry Connect Activity</strong> parameters used</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Parameter</strong></td>
<td><strong>Description</strong></td>
</tr>
<tr>
<td>Option Path</td>
<td>System External Device Activity &gt; USB Device Activity</td>
</tr>
<tr>
<td>Option</td>
<td>USB Registry Connect Activity</td>
</tr>
<tr>
<td>Rule Name</td>
<td>USB_Registry_Connect_Activity</td>
</tr>
<tr>
<td>Severity</td>
<td>Warning</td>
</tr>
<tr>
<td>Noise Suppress</td>
<td>1 Minute. Suppress reporting of events from this rule for specified duration after the rule has triggered once.</td>
</tr>
<tr>
<td>Registry Paths</td>
<td><code>\HKEY_LOCAL_MACHINE\SYSTEM\*ControlSet\*ENUM\USB\*</code></td>
</tr>
<tr>
<td>Description</td>
<td>Detects the USB device connection activity that is associated with the Windows registry. This rule provides a noise suppression duration value to tune out the unnecessary noise that this rule may cause.</td>
</tr>
</tbody>
</table>

CD/DVD burning activity

This portion of the policy detects the various activities that are associated with CD and DVD burning.

**Note**: These rules function only in Windows 2000/2003 environments.

<table>
<thead>
<tr>
<th>Table 6-220</th>
<th>Description of the <strong>CD/DVD Burning Services Enabled</strong> parameters used</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Parameter</strong></td>
<td><strong>Description</strong></td>
</tr>
<tr>
<td>Option Path</td>
<td>System External Device Activity &gt; CD/DVD Burning Activity</td>
</tr>
<tr>
<td>Option</td>
<td>CD/DVD Burning Services Enabled</td>
</tr>
</tbody>
</table>
Table 6-220  Description of the **CD/DVD Burning Services Enabled** parameters used (continued)

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Rule Name</td>
<td>CD_DVD_Burning_Activity_Enabled</td>
</tr>
<tr>
<td>Severity</td>
<td>Warning</td>
</tr>
<tr>
<td>Event IDs</td>
<td>7040</td>
</tr>
<tr>
<td>Description</td>
<td>Detects when the CD/DVD service enters a running state from the Windows Event Log.</td>
</tr>
</tbody>
</table>

Table 6-221  Description of the **CD/DVD Burning Services Started** parameters used

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Option Path</td>
<td>System External Device Activity &gt; CD/DVD Burning Activity</td>
</tr>
<tr>
<td>Option</td>
<td>CD/DVD Burning Services Started</td>
</tr>
<tr>
<td>Rule Name</td>
<td>CD_DVD_Burning_Activity_Started</td>
</tr>
<tr>
<td>Severity</td>
<td>Warning</td>
</tr>
<tr>
<td>Event IDs</td>
<td>7036</td>
</tr>
<tr>
<td>Description</td>
<td>Detects a CD/DVD service auto start configuration event from the Windows Event Log.</td>
</tr>
</tbody>
</table>

Table 6-222  Description of the **CD/DVD Burning Services Stopped** parameters used

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Option Path</td>
<td>System External Device Activity &gt; CD/DVD Burning Activity</td>
</tr>
<tr>
<td>Option</td>
<td>CD/DVD Burning Services Stopped</td>
</tr>
<tr>
<td>Rule Name</td>
<td>CD_DVD_Burning_Activity_Stopped</td>
</tr>
<tr>
<td>Severity</td>
<td>Warning</td>
</tr>
<tr>
<td>Event IDs</td>
<td>7035</td>
</tr>
<tr>
<td>Description</td>
<td>Detects when the CD/DVD service enters a stopped state from the Windows Event Log.</td>
</tr>
</tbody>
</table>
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.

**Note:** The access log must follow W3C guidelines. The majority of Web server applications on Windows servers are Internet Information Services (IIS). By default, System Attack Detection is set up for IIS. You can set up this area for any Web hosting application. Within this option group subsection there is a global settings area to set several unique properties for the rest of the system attack monitor.

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 Data Center Security: Server Advanced provides a default IIS 7 location.

- 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 monitoring

**Table 6-223**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Option Path</td>
<td>System Web Attack Detection Monitor &gt; Generic VA Scan Attempt</td>
</tr>
<tr>
<td>Option</td>
<td>Generic VA scan Attempt</td>
</tr>
<tr>
<td>Rule Name</td>
<td>WebAttackDetection_Generic_VAScan</td>
</tr>
<tr>
<td>Severity</td>
<td>Warning</td>
</tr>
<tr>
<td>Invalid Count</td>
<td>20 Times in which a 404 or unknown request is received.</td>
</tr>
<tr>
<td>Interval</td>
<td>2 minutes Time frequency in which invalid count needs to occur to trigger event.</td>
</tr>
<tr>
<td>Description</td>
<td>Detects a possible VA scan by triggering an event within a specific administrator-defined threshold. If Symantec Data Center Security: Server Advanced 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.</td>
</tr>
</tbody>
</table>

**Table 6-224**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Option Path</td>
<td>System Web Attack Detection Monitor &gt; Generic VA Scan Attempt</td>
</tr>
<tr>
<td>Option</td>
<td>Generic Blacklisted IP Request Attempts</td>
</tr>
<tr>
<td>Rule Name</td>
<td>WebAttackDetection_Generic_BlackListedIP</td>
</tr>
<tr>
<td>Severity</td>
<td>Warning</td>
</tr>
<tr>
<td>Description</td>
<td>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.</td>
</tr>
</tbody>
</table>
### Table 6-225  Description of the **Generic SQL Injection Attack Attempts** parameters used

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Option Path</td>
<td>System Web Attack Detection Monitor &gt; Generic VA Scan Attempt</td>
</tr>
<tr>
<td>Option</td>
<td>Generic SQL Injection Attack Attempts</td>
</tr>
<tr>
<td>Rule Name</td>
<td>WebAttackDetection_Generic_SQLInjection</td>
</tr>
<tr>
<td>Severity</td>
<td>Warning</td>
</tr>
<tr>
<td>Description</td>
<td>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.</td>
</tr>
</tbody>
</table>

### Table 6-226  Description of the **Generic Directory Transversal Attempts** parameters used

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Option Path</td>
<td>System Web Attack Detection Monitor &gt; Generic VA Scan Attempt</td>
</tr>
<tr>
<td>Option</td>
<td>Generic Directory Transversal Attempts</td>
</tr>
<tr>
<td>Rule Name</td>
<td>WebAttackDetection_Generic_DirTransversal</td>
</tr>
<tr>
<td>Severity</td>
<td>Warning</td>
</tr>
<tr>
<td>Description</td>
<td>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.</td>
</tr>
</tbody>
</table>

### Table 6-227  Description of the **Generic Malicious User Agent Request Attempts** parameters used

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Option Path</td>
<td>System Web Attack Detection Monitor &gt; Generic VA Scan Attempt</td>
</tr>
<tr>
<td>Option</td>
<td>Generic Malicious User Agent Request Attempts</td>
</tr>
<tr>
<td>Rule Name</td>
<td>WebAttackDetection_Generic_MaliciousUserAgent</td>
</tr>
<tr>
<td>Severity</td>
<td>Warning</td>
</tr>
</tbody>
</table>
### Table 6-227
Description of the **Generic Malicious User Agent Request Attempts** parameters used (continued)

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Description</td>
<td>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.</td>
</tr>
</tbody>
</table>

### Table 6-228
Description of the **Generic Unwanted Extension Requests** parameters used

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Option Path</td>
<td>System Web Attack Detection Monitor &gt; Generic VA Scan Attempt</td>
</tr>
<tr>
<td>Option</td>
<td>Generic Unwanted Extension Requests</td>
</tr>
<tr>
<td>Rule Name</td>
<td>WebAttackDetection_Unwanted_Extension_Request</td>
</tr>
<tr>
<td>Severity</td>
<td>Warning</td>
</tr>
<tr>
<td>Description</td>
<td>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.</td>
</tr>
</tbody>
</table>

### Table 6-229
Description of the **Generic Unwanted Directory Requests** parameters used

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Option Path</td>
<td>System Web Attack Detection Monitor &gt; Generic VA Scan Attempt</td>
</tr>
<tr>
<td>Option</td>
<td>Generic Unwanted Directory Requests</td>
</tr>
<tr>
<td>Rule Name</td>
<td>WebAttackDetection_Unwanted_Directory_Request</td>
</tr>
<tr>
<td>Severity</td>
<td>Warning</td>
</tr>
<tr>
<td>Description</td>
<td>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.</td>
</tr>
</tbody>
</table>
**Table 6-230** Description of the **Generic Vulnerable CGI Requests** parameters used

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Option Path</td>
<td>System Web Attack Detection Monitor &gt; Generic VA Scan Attempt</td>
</tr>
<tr>
<td>Option</td>
<td>Generic Vulnerable CGI Requests</td>
</tr>
<tr>
<td>Rule Name</td>
<td>WebAttackDetection_Generic_VulnerableCGIRequest</td>
</tr>
<tr>
<td>Severity</td>
<td>Warning</td>
</tr>
<tr>
<td>Description</td>
<td>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.</td>
</tr>
</tbody>
</table>
This chapter includes the following topics:

- Introduction
- File monitoring improvements
- Advanced per-rule tuning improvements
- Console changes
- Unicode Log Monitoring for UNIX
- How wildcard characters and recursion levels work in IDS file monitoring

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 DCS:SA console. These rules now also use ignore logic and select logic methodology.

- You can now configure and view all rule content from the DCS:SA 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 (LKM) 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 7-1 illustrates how the existing policies from previous releases were combined with new options into the 5.2 RU7 top-level option groups.

<table>
<thead>
<tr>
<th>Options in previous releases</th>
<th>Detection option organization in release 5.2 RU7</th>
</tr>
</thead>
<tbody>
<tr>
<td>User/Group_Configuration</td>
<td>System User and Group Change Monitor</td>
</tr>
<tr>
<td>Privileged_User/Group_Configuration</td>
<td></td>
</tr>
<tr>
<td>System_Logon_Failure</td>
<td>System Login Activity and Access Monitor</td>
</tr>
<tr>
<td>System_Logoff_Success</td>
<td></td>
</tr>
<tr>
<td>System_Failed_Access_Status</td>
<td></td>
</tr>
<tr>
<td>System_SUDO_Monitor</td>
<td>System Privilege Command and Bash History Monitor</td>
</tr>
<tr>
<td>System_Root_Command_Monitor</td>
<td></td>
</tr>
<tr>
<td>System_User_Command_Monitor</td>
<td></td>
</tr>
<tr>
<td>System_AutoStart_Change(rc*.d)</td>
<td></td>
</tr>
<tr>
<td>System_Service_Config_Monitor</td>
<td></td>
</tr>
<tr>
<td>System_Xserver_Configuration</td>
<td></td>
</tr>
<tr>
<td>System_RunLevel_Monitor(Inittab)</td>
<td></td>
</tr>
<tr>
<td>System_Sysconfig_Monitor(Sysconfig)</td>
<td></td>
</tr>
<tr>
<td>Host_IDS_File_Tampering</td>
<td>System File and Directory Monitor</td>
</tr>
<tr>
<td>Critical_System_File_Monitor</td>
<td></td>
</tr>
<tr>
<td>Symantec_AV_Linux_Client_Comms</td>
<td>System Symantec Software Monitor</td>
</tr>
<tr>
<td>Symantec_AV_Unix_Client_Comms</td>
<td></td>
</tr>
</tbody>
</table>
### File monitoring improvements

To provide granular control over UNIX file change monitoring, DCS:SA monitors near real-time changes on local file systems and fixed file systems. It does not monitor changes on removable media or remote network drives.

It no longer uses polling intervals. DCS:SA uses the FIPS 140-2-compliant Secure Hash Algorithm (SHA-256) to calculate file hashes or checksums at runtime. The MD5 algorithm is no longer used or available.

For performance efficiency, you can enable or disable the checksum calculation for each filewatch list. A single hash algorithm is used on all the files in a watched list.

Specific file monitoring changes include the following improvements:

- You can control and enable the access, delete, modify, and create change monitoring functions on a group-by-group basis.
- You can control modification diff’ing, including algorithm selection on a group-by-group basis.
- You can set date and time restrictions within each specific file monitoring group.
- You can tune the file monitor modified detection operation for specific criteria, such as only for permission changes, size changes, bitmask changes, and so on.
- You can use specific ignore logic criteria and select logic criteria in each file monitoring group. For example, you can independently configure each file monitoring group to ignore file paths or strings.
Advanced per-rule tuning improvements

Advanced per-rule tuning includes the following options for configuration:

- Rule Name
- Rule Severity
- Rule monitoring content, such as file paths, log file strings, select criteria, and ignore criteria
- Select logic, in the form of strings
- Ignore logic, in the form of strings
- Date and time restrictions, as applicable

Console changes

DCS:SA provides specific content control per rule from the console. Each rule in the Baseline policy has required parameters. These rules are now viewable and customizable from the console.

The options in Table 7-2 are available for each rule that is displayed in the Policy Settings pane.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Rule Name</strong></td>
<td>The name that is associated with the rule that generates the specific event. A single string value is allowed in the string field.</td>
</tr>
<tr>
<td><strong>Severity</strong></td>
<td>The severity of event. Available for each rule of the policy. You can only select one severity level, Info, Notice, Warning, Major, or Critical, for each rule.</td>
</tr>
</tbody>
</table>
Table 7-2  Rule options (continued)

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Select Strings</strong></td>
<td>Used in rule select logic. DCS:SA uses primary logic or initial sifting method for rule event generation. Use an asterisk (*) to select all the events that the criteria that you entered previously generate. For example, criteria such as (event IDs, file paths, or log strings previously defined. With this option you can specifically tune rules for administrator needs. For example, if you change the select string on a filewatch rule from * to <em>Permission</em>, then that rule only generates a filewatch event if that event contains the string “Permission.” You can have multiple select strings in this string list. All strings are case insensitive. You can add, edit, and remove select strings.</td>
</tr>
<tr>
<td><strong>Ignore Strings</strong></td>
<td>Used in rule ignore logic. DCS:SA uses secondary ignore logic or ignore sifting method for rule event generation. Almost all rule parameter options contain a blank value, which signifies that a null value or no value is associated with the ignore logic statement. DCS:SA ignores any string in this field other than blank value upon pattern matching on the final event generation. Ignore strings also provide you with the ability to perform advanced rule-by-rule tuning. You can have multiple ignore strings in this string list. All strings are case insensitive. You can add, edit, and remove ignore strings. The ignore criteria ignores items that have a tendency to change frequently or items that are not a part of the core system and configuration. These ignore items are items such as logs, temp directory and so on.</td>
</tr>
</tbody>
</table>

Note: Each parameter is preconfigured with default values to ensure the functionality of the rule. Changes to rule name and severity do not affect the overall operation of the rule.

Unicode Log Monitoring for UNIX

The IDS agent logwatch collector reads Unicode text log files, so that you can monitor the applications that output to Unicode log files or to Unicode format.

How wildcard characters and recursion levels work in IDS file monitoring

When you use wildcard characters in IDS file monitoring, the following rules apply:

- Only the asterisk (*) and question mark (?) wildcard characters are allowed.
- The asterisk (*) stands for one or more characters.
The question mark (?) stands for a single character only.

Wildcard characters are allowed only in the last element of file path. You can only place a wildcard character after the last slash in a file path.

The following are examples of valid uses of wildcard characters in a file path:

- /tmp/*
- /tmp/L1/*.txt
- /tmp/L2/*file*.ini
- /tmp/L1/file?.ini
- /tmp/L1/file?.*

The following are examples of invalid uses of wildcard characters in a file path:

- /tmp/*/L3/*.txt
- /tmp/L2/*/file?.txt

Recursion levels only work with the use of one or more wildcard characters. If a file path specification contains no wildcard character, then the recursion level has no effect. Rules may have a specified recursion level and file paths with mixed entries, where only some of the file paths contain wildcard characters. Recursion works only with the file paths that contain one or more wildcard characters.

When both recursion and wildcard characters are specified, the folder path and file name are considered separately. A file name that is specified with one or more wildcard characters is searched for in the given path and in a number of subfolders. The number of subfolders that are searched is equal to the recursion level minus 1.

For example, if you configure a file path of /tmp/*.dll and a recursion level of 3, that requests to monitor all DLL files in the /tmp folder three levels deep, including /tmp.

The following DLL files are monitored for changes:

- /tmp/my.dll
- /tmp/L1/your.dll
- /tmp/D1/ours.dll
- /tmp/L1/L2/his.dll
- /tmp/D1/D2/her.dll

In this example, the /tmp/D1/D2/D3/bad.dll file would not be monitored.
UNIX Policy Options

This chapter includes the following topics:

- System User and Group Change Monitor
- System Login Activity and Access Monitor
- System Privileged Command and Bash History Monitor
- System Hardening Monitor
- System File and Directory Monitor
- System Symantec Software Monitor
- System External Device Activity Monitor
- System Attack Detection

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 8-1 Description of the **Monitor User and Group File(s) Checksum** parameters used

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Option Path</td>
<td>System User and Group Change Monitor &gt; Global User and Group Change Monitor Settings</td>
</tr>
<tr>
<td>Option</td>
<td>Monitor User and Group File(s) Checksum</td>
</tr>
<tr>
<td>Description</td>
<td>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 were modified since DCS:SA was last shut down.</td>
</tr>
</tbody>
</table>

Table 8-2 Description of the **User and Group Monitor Polling Interval** parameters used

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Option Path</td>
<td>System User and Group Change Monitor &gt; Global User and Group Change Monitor Settings</td>
</tr>
<tr>
<td>Option</td>
<td>User and Group Monitor Polling Interval</td>
</tr>
<tr>
<td>Description</td>
<td>Sets how often files are polled for changes in status. A short polling interval could possibly impact system performance.</td>
</tr>
</tbody>
</table>

Table 8-3 Description of the **User and Group Configuration File Paths** parameters used

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Option Path</td>
<td>System User and Group Change Monitor &gt; Global User and Group Change Monitor Settings</td>
</tr>
<tr>
<td>Option</td>
<td>User and Group Configuration File Paths</td>
</tr>
<tr>
<td>Description</td>
<td>Sets the configuration files to be monitored.</td>
</tr>
</tbody>
</table>

**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 8-4  Description of the **User Created** parameters used

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Option Path</td>
<td>System User and Group Change Monitor &gt; System User Configuration Changes</td>
</tr>
<tr>
<td>Option</td>
<td>User Created</td>
</tr>
<tr>
<td>Rule Name</td>
<td>User_Created RuleName</td>
</tr>
<tr>
<td>Severity</td>
<td>Warning</td>
</tr>
<tr>
<td>Description</td>
<td>Detects the creation of user accounts on the local system. <strong>Note:</strong> If this rule is unchecked, you cannot monitor user name change events.</td>
</tr>
</tbody>
</table>

### Table 8-5  Description of the **User Deleted** parameters used

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Option Path</td>
<td>System User and Group Change Monitor &gt; System User Configuration Changes</td>
</tr>
<tr>
<td>Option</td>
<td>User Deleted</td>
</tr>
<tr>
<td>Rule Name</td>
<td>User_Deleted RuleName</td>
</tr>
<tr>
<td>Severity</td>
<td>Warning</td>
</tr>
<tr>
<td>Description</td>
<td>Detects the deletion of user accounts on the local system.</td>
</tr>
</tbody>
</table>

### Table 8-6  Description of the **User's Password Changed** parameters used

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Option Path</td>
<td>System User and Group Change Monitor &gt; System User Configuration Changes</td>
</tr>
<tr>
<td>Option</td>
<td>User's Password Changed</td>
</tr>
<tr>
<td>Rule Name</td>
<td>User_Password_Changed RuleName</td>
</tr>
<tr>
<td>Severity</td>
<td>Notice</td>
</tr>
<tr>
<td>Description</td>
<td>Detects the changes to users' passwords in user accounts on the local system.</td>
</tr>
</tbody>
</table>
### Table 8-7  Description of the **User's Name Changed** parameters used

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Option Path</td>
<td>System User and Group Change Monitor &gt; System User Configuration Changes</td>
</tr>
<tr>
<td>Option</td>
<td>User's Name Changed</td>
</tr>
<tr>
<td>Rule Name</td>
<td>User_Name_Changed</td>
</tr>
<tr>
<td>Severity</td>
<td>Notice</td>
</tr>
<tr>
<td>Description</td>
<td>Detects the changes to users' names in user accounts on the local system.</td>
</tr>
</tbody>
</table>

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

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Option Path</td>
<td>System User and Group Change Monitor &gt; System User Configuration Changes</td>
</tr>
<tr>
<td>Option</td>
<td>User's ID Changed</td>
</tr>
<tr>
<td>Rule Name</td>
<td>User_ID_Changed</td>
</tr>
<tr>
<td>Severity</td>
<td>Notice</td>
</tr>
<tr>
<td>Description</td>
<td>Detects the changes that are made to users' IDs in system user accounts on the local system.</td>
</tr>
</tbody>
</table>

### Table 8-9  Description of the **User's Primary Group Changed** parameters used

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Option Path</td>
<td>System User and Group Change Monitor &gt; System User Configuration Changes</td>
</tr>
<tr>
<td>Option</td>
<td>User's Primary Group Changed</td>
</tr>
<tr>
<td>Rule Name</td>
<td>User_Primary_Group_ID_Changed</td>
</tr>
<tr>
<td>Severity</td>
<td>Notice</td>
</tr>
<tr>
<td>Specific Primary</td>
<td>Sets user-defined groups. Default value is all groups.</td>
</tr>
<tr>
<td>Groups</td>
<td></td>
</tr>
<tr>
<td>Description</td>
<td>Detects the changes that are made to users' primary group ID numbers in system user accounts on the local system.</td>
</tr>
</tbody>
</table>
### Table 8-10  Description of the **User's Full Name Changed** parameters used

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Option Path</td>
<td>System User and Group Change Monitor &gt; System User Configuration Changes</td>
</tr>
<tr>
<td>Option</td>
<td>User's Full Name Changed</td>
</tr>
<tr>
<td>Rule Name</td>
<td>User_Full_Name_Changed</td>
</tr>
<tr>
<td>Severity</td>
<td>Notice</td>
</tr>
<tr>
<td>Description</td>
<td>Detects the changes that are made to users' full names in system user</td>
</tr>
<tr>
<td></td>
<td>accounts on the local system.</td>
</tr>
</tbody>
</table>

### Table 8-11  Description of the **User's Home Directory Changed** parameters used

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Option Path</td>
<td>System User and Group Change Monitor &gt; System User Configuration Changes</td>
</tr>
<tr>
<td>Option</td>
<td>User's Home Directory Changed</td>
</tr>
<tr>
<td>Rule Name</td>
<td>User_Home_Directory_Changed</td>
</tr>
<tr>
<td>Severity</td>
<td>Warning</td>
</tr>
<tr>
<td>Description</td>
<td>Detects the changes that are made to users' home directories in system user</td>
</tr>
<tr>
<td></td>
<td>accounts on the local system.</td>
</tr>
</tbody>
</table>

### Table 8-12  Description of the **User's Login Shell Changed** parameters used

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Option Path</td>
<td>System User and Group Change Monitor &gt; System User Configuration Changes</td>
</tr>
<tr>
<td>Option</td>
<td>User's Login Shell Changed</td>
</tr>
<tr>
<td>Rule Name</td>
<td>User_Login_Shell_Changed</td>
</tr>
<tr>
<td>Severity</td>
<td>Warning</td>
</tr>
<tr>
<td>Description</td>
<td>Detects the changes that are made to users' login shells in system user</td>
</tr>
<tr>
<td></td>
<td>accounts on the local system.</td>
</tr>
</tbody>
</table>
### Table 8-13 Description of the **User’s Minimum Password Age Changed** parameters used

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Option Path</td>
<td>System User and Group Change Monitor &gt; System User Configuration Changes</td>
</tr>
<tr>
<td>Option</td>
<td>User's Minimum Password Age Changed</td>
</tr>
<tr>
<td>Rule Name</td>
<td>User_Minimum_Password_Age_Changed</td>
</tr>
<tr>
<td>Severity</td>
<td>Warning</td>
</tr>
<tr>
<td>Description</td>
<td>Detects the changes that are made to users’ minimum password age parameter in system user accounts on the local system.</td>
</tr>
</tbody>
</table>

### Table 8-14 Description of the **User’s Maximum Password Age Changed** parameters used

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Option Path</td>
<td>System User and Group Change Monitor &gt; System User Configuration Changes</td>
</tr>
<tr>
<td>Option</td>
<td>User's Maximum Password Age Changed</td>
</tr>
<tr>
<td>Rule Name</td>
<td>User_Maximum_Password_Age_Changed</td>
</tr>
<tr>
<td>Severity</td>
<td>Warning</td>
</tr>
<tr>
<td>Description</td>
<td>Detects changes in users’ maximum days between password changes parameter in system user accounts on the local system.</td>
</tr>
</tbody>
</table>

### Table 8-15 Description of the **User’s Maximum Days of Account Inactivity Changed** parameters used

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Option Path</td>
<td>System User and Group Change Monitor &gt; System User Configuration Changes</td>
</tr>
<tr>
<td>Option</td>
<td>User's Maximum Days of Account Inactivity Changed</td>
</tr>
<tr>
<td>Rule Name</td>
<td>User_Passwd_Inactivity_Days_Changed</td>
</tr>
<tr>
<td>Severity</td>
<td>Warning</td>
</tr>
<tr>
<td>Description</td>
<td></td>
</tr>
</tbody>
</table>
### Table 8-15
**Description of the User's Maximum Days of Account Inactivity Changed** parameters used

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Description</td>
<td>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.</td>
</tr>
</tbody>
</table>

### Table 8-16
**Description of the User's Account Expiry Date Changed** parameters used

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Option Path</td>
<td>System User and Group Change Monitor &gt; System User Configuration Changes</td>
</tr>
<tr>
<td>Option</td>
<td>User's Account Expiry Date Changed</td>
</tr>
<tr>
<td>Rule Name</td>
<td>User_Account_Expiry_Date_Changed</td>
</tr>
<tr>
<td>Severity</td>
<td>Warning</td>
</tr>
<tr>
<td>Description</td>
<td>Detects changes in the date when users' logins automatically expire.</td>
</tr>
</tbody>
</table>

### Table 8-17
**Description of the User's Password Expire Warning Date Changed** parameters used

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Option Path</td>
<td>System User and Group Change Monitor &gt; System User Configuration Changes</td>
</tr>
<tr>
<td>Option</td>
<td>User's Password Expire Warning Date Changed</td>
</tr>
<tr>
<td>Rule Name</td>
<td>User_Password_Expire_Warning_Date_Changed</td>
</tr>
<tr>
<td>Severity</td>
<td>Warning</td>
</tr>
<tr>
<td>Description</td>
<td>Detects changes in the date when users are warned that their password is about to expire.</td>
</tr>
</tbody>
</table>

### Table 8-18
**Description of the User's Attribute Changed** parameters used

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Option Path</td>
<td>System User and Group Change Monitor &gt; System User Configuration Changes</td>
</tr>
<tr>
<td>Option</td>
<td>User's Attribute Changed</td>
</tr>
</tbody>
</table>
Table 8-18 Description of the User’s Attribute Changed parameters used (continued)

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Rule Name</td>
<td>User_Attributes_Changed</td>
</tr>
<tr>
<td>Severity</td>
<td>Warning</td>
</tr>
<tr>
<td>Description</td>
<td>Detects changes in users’ attributes that are located in the /etc/user_attr file on the local system.</td>
</tr>
</tbody>
</table>

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 8-19 Description of the Group Created parameters used

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Option Path</td>
<td>System User and Group Change Monitor &gt; System Group Configuration Changes</td>
</tr>
<tr>
<td>Option</td>
<td>Group Created</td>
</tr>
<tr>
<td>Rule Name</td>
<td>Group_Created</td>
</tr>
<tr>
<td>Severity</td>
<td>Warning</td>
</tr>
<tr>
<td>Description</td>
<td>Detects the creation of a group.</td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> If this rule in unchecked, you cannot monitor changes in a group's name.</td>
</tr>
</tbody>
</table>

Table 8-20 Description of the Group Deleted parameters used

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Option Path</td>
<td>System User and Group Change Monitor &gt; System Group Configuration Changes</td>
</tr>
<tr>
<td>Option</td>
<td>Group Deleted</td>
</tr>
<tr>
<td>Rule Name</td>
<td>Group_Deleted</td>
</tr>
<tr>
<td>Severity</td>
<td>Warning</td>
</tr>
</tbody>
</table>
### Table 8-20  
**Description of the Group Deleted parameters used (continued)**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Description</td>
<td>Detects the deletion of a group. <strong>Note:</strong> If this rule is unchecked, you cannot monitor changes in a group's name.</td>
</tr>
</tbody>
</table>

### Table 8-21  
**Description of the Group Membership Changed parameters used**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Option Path</td>
<td>System User and Group Change Monitor &gt; System Group Configuration Changes</td>
</tr>
<tr>
<td>Option</td>
<td>Group Membership Changed</td>
</tr>
<tr>
<td>Rule Name</td>
<td>Group_Membership_Change</td>
</tr>
<tr>
<td>Severity</td>
<td>Warning</td>
</tr>
<tr>
<td>Specific Membership Groups</td>
<td>Sets user-defined membership groups. Default value is all groups.</td>
</tr>
<tr>
<td>Description</td>
<td>Detects the addition or deletion of a user from a group.</td>
</tr>
</tbody>
</table>

### Table 8-22  
**Description of the Group Name Change parameters used**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Option Path</td>
<td>System User and Group Change Monitor &gt; System Group Configuration Changes</td>
</tr>
<tr>
<td>Option</td>
<td>Group Name Change</td>
</tr>
<tr>
<td>Rule Name</td>
<td>Group_Name_Changed</td>
</tr>
<tr>
<td>Severity</td>
<td>Warning</td>
</tr>
<tr>
<td>Description</td>
<td>Detects a change in the name of a group. Group created and group deleted events are generated for group name changes.</td>
</tr>
</tbody>
</table>

### Table 8-23  
**Description of the Group Lock Flag Changed parameters used**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Option Path</td>
<td>System User and Group Change Monitor &gt; System Group Configuration Changes</td>
</tr>
</tbody>
</table>
Table 8-23  Description of the **Group Lock Flag Changed** parameters used
\[(continued)\]

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Option</td>
<td>Group Lock Flag Changed</td>
</tr>
<tr>
<td>Rule Name</td>
<td>Group_LockFlag_Changed</td>
</tr>
<tr>
<td>Severity</td>
<td>Warning</td>
</tr>
<tr>
<td>Description</td>
<td>Detects the changes to a group's lock flag.</td>
</tr>
</tbody>
</table>

Table 8-24  Description of the **Group ID Changed** parameters used

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Option Path</td>
<td>System User and Group Change Monitor &gt; System Group Configuration Changes</td>
</tr>
<tr>
<td>Option</td>
<td>Group ID Changed</td>
</tr>
<tr>
<td>Rule Name</td>
<td>Group_ID_Changed</td>
</tr>
<tr>
<td>Severity</td>
<td>Warning</td>
</tr>
<tr>
<td>Description</td>
<td>Detects the changes to a group's ID.</td>
</tr>
</tbody>
</table>

**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 8-25  Description of the **Superuser (root level) User Created** parameters used

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Option Path</td>
<td>System User and Group Change Monitor &gt; Privileged User and Group Configuration Activity</td>
</tr>
<tr>
<td>Option</td>
<td>Superuser (root level) User Created</td>
</tr>
<tr>
<td>Rule Name</td>
<td>Superuser_Account_Created</td>
</tr>
<tr>
<td>Severity</td>
<td>Major</td>
</tr>
<tr>
<td>Description</td>
<td>Detects the creation of a superuser account.</td>
</tr>
</tbody>
</table>
### Table 8-26 Description of the *Superuser (root level) Group Created* parameters used

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Option Path</td>
<td>System User and Group Change Monitor &gt; Privileged User and Group Configuration Activity</td>
</tr>
<tr>
<td>Option</td>
<td>Superuser (root level) Group Created</td>
</tr>
<tr>
<td>Rule Name</td>
<td>Superuser_Group_Created</td>
</tr>
<tr>
<td>Severity</td>
<td>Major</td>
</tr>
<tr>
<td>Description</td>
<td>Detects the creation of a superuser group.</td>
</tr>
</tbody>
</table>

### Table 8-27 Description of the *User's Global ID Changed to Superuser* parameters used

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Option Path</td>
<td>System User and Group Change Monitor &gt; Privileged User and Group Configuration Activity</td>
</tr>
<tr>
<td>Option</td>
<td>User's Global ID Changed to Superuser</td>
</tr>
<tr>
<td>Rule Name</td>
<td>User_ID_Changed_to_Superuser</td>
</tr>
<tr>
<td>Severity</td>
<td>Critical</td>
</tr>
<tr>
<td>Description</td>
<td>Detects when a user's ID is changed to be a member of a superuser global group.</td>
</tr>
</tbody>
</table>

### Table 8-28 Description of the *Group's Global ID Changed to Superuser* parameters used

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Option Path</td>
<td>System User and Group Change Monitor &gt; Privileged User and Group Configuration Activity</td>
</tr>
<tr>
<td>Option</td>
<td>Group's Global ID Changed to Superuser</td>
</tr>
<tr>
<td>Rule Name</td>
<td>Group_ID_Changed_to_Superuser</td>
</tr>
<tr>
<td>Severity</td>
<td>Critical</td>
</tr>
<tr>
<td>Description</td>
<td>Detects when a group's ID is changed to be a member of a superuser global group.</td>
</tr>
</tbody>
</table>
Table 8-29  Description of the **User’s Primary Group ID Changed to Superuser** parameters used

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Option Path</td>
<td>System User and Group Change Monitor &gt; Privileged User and Group Configuration Activity</td>
</tr>
<tr>
<td>Option</td>
<td>User’s Primary Group ID Changed to Superuser</td>
</tr>
<tr>
<td>Rule Name</td>
<td>User_PrimaryID_Added_SuperuserID_Change</td>
</tr>
<tr>
<td>Severity</td>
<td>Critical</td>
</tr>
<tr>
<td>Description</td>
<td>Detects when a user's primary group ID is changed to be a member of a root group.</td>
</tr>
</tbody>
</table>

Table 8-30  Description of the **Group Membership Changed User to Superuser** parameters used

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Option Path</td>
<td>System User and Group Change Monitor &gt; Privileged User and Group Configuration Activity</td>
</tr>
<tr>
<td>Option</td>
<td>Group Membership Changed User to Superuser</td>
</tr>
<tr>
<td>Rule Name</td>
<td>Root_Group_Added_SuperuserID_Change</td>
</tr>
<tr>
<td>Severity</td>
<td>Critical</td>
</tr>
<tr>
<td>Description</td>
<td>Detects when a user is added as a member of the root superuser group.</td>
</tr>
</tbody>
</table>

**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 8-31 Description of the Root logon parameters used

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Option Path</td>
<td>System Login Activity and Access Monitor &gt; System Login Success Monitor &gt; FTP logon Options &gt; FTP server reports to Syslog</td>
</tr>
<tr>
<td>Option</td>
<td>Root logon</td>
</tr>
<tr>
<td>Rule Names</td>
<td>Root_FTP_Logon_Success_syslog</td>
</tr>
<tr>
<td>Severity</td>
<td>Warning</td>
</tr>
<tr>
<td>Description</td>
<td>Detects users who use FTP to log on as root.</td>
</tr>
</tbody>
</table>

Table 8-32 Description of the Non-root logon parameters used

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Option Path</td>
<td>System Login Activity and Access Monitor &gt; System Login Success Monitor &gt; FTP logon Options &gt; FTP server reports to Syslog</td>
</tr>
<tr>
<td>Option</td>
<td>Non-root logon</td>
</tr>
<tr>
<td>Rule Names</td>
<td>User_FTP_Logon_Success_syslog</td>
</tr>
<tr>
<td>Severity</td>
<td>Warning</td>
</tr>
<tr>
<td>Description</td>
<td>Detects non-root users who use FTP to log on.</td>
</tr>
</tbody>
</table>

Server reports to a log file

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

Table 8-33 Description of the Log Location parameters used

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Option Path</td>
<td>System Login Activity and Access Monitor &gt; System Login Success Monitor &gt; FTP logon Options &gt; FTP server reports to a log file</td>
</tr>
<tr>
<td>Option</td>
<td>Log Location</td>
</tr>
<tr>
<td>Path</td>
<td>/var/log/vsftpd.log</td>
</tr>
<tr>
<td>Table 8-33</td>
<td>Description of the <strong>Log Location</strong> parameters used (continued)</td>
</tr>
<tr>
<td>-------------</td>
<td>---------------------------------------------------------------</td>
</tr>
<tr>
<td>Parameter</td>
<td>Description</td>
</tr>
<tr>
<td>Description</td>
<td>Sets the path to the FTP log file.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Table 8-34</th>
<th>Description of the <strong>Root logon</strong> parameters used</th>
</tr>
</thead>
<tbody>
<tr>
<td>Parameter</td>
<td>Description</td>
</tr>
<tr>
<td>Option Path</td>
<td>System Login Activity and Access Monitor &gt; System Login Success Monitor &gt; FTP logon Options &gt; FTP server reports to a log file</td>
</tr>
<tr>
<td>Option</td>
<td>Root logon</td>
</tr>
<tr>
<td>Rule Name</td>
<td>Root_FTP_Logon_Success_Text_Log</td>
</tr>
<tr>
<td>Severity</td>
<td>Notice</td>
</tr>
<tr>
<td>Description</td>
<td>Detects root logon events that occur over FTP.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Table 8-35</th>
<th>Description of the <strong>Non-root logon</strong> parameters used</th>
</tr>
</thead>
<tbody>
<tr>
<td>Parameter</td>
<td>Description</td>
</tr>
<tr>
<td>Option Path</td>
<td>System Login Activity and Access Monitor &gt; System Login Success Monitor &gt; FTP logon Options &gt; FTP server reports to a log file</td>
</tr>
<tr>
<td>Option</td>
<td>Non-root logon</td>
</tr>
<tr>
<td>Rule Name</td>
<td>User_FTP_Logon_Success_Text_Log</td>
</tr>
<tr>
<td>Severity</td>
<td>Notice</td>
</tr>
<tr>
<td>Description</td>
<td>Detects non-root user logon events that occur over FTP.</td>
</tr>
</tbody>
</table>

**Telnet and Rlogin logon Options**

This option group section of the policy monitors logons 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>
<thead>
<tr>
<th>Table 8-36</th>
<th>Description of the <strong>Root logon</strong> parameters used</th>
</tr>
</thead>
<tbody>
<tr>
<td>Parameter</td>
<td>Description</td>
</tr>
<tr>
<td>Option Path</td>
<td>System Login Activity and Access Monitor &gt; System Login Success Monitor &gt; Telnet and Rlogin logon Options</td>
</tr>
</tbody>
</table>
Table 8-36  Description of the **Root logon** parameters used (continued)

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Option</td>
<td>Root logon</td>
</tr>
<tr>
<td>Rule Name</td>
<td>Root_Telnet_Rlogin_Logon_Success</td>
</tr>
<tr>
<td>Severity</td>
<td>Warning</td>
</tr>
<tr>
<td>Description</td>
<td>Detects root logon events that occur over Telnet and rlogin.</td>
</tr>
</tbody>
</table>

Table 8-37  Description of the **Non-root logon** parameters used

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Option Path</td>
<td>System Login Activity and Access Monitor &gt; System Login Success Monitor &gt; Telnet and Rlogin logon Options</td>
</tr>
<tr>
<td>Option</td>
<td>Non-root logon</td>
</tr>
<tr>
<td>Rule Name</td>
<td>User_Telnet_Rlogin_Logon_Success</td>
</tr>
<tr>
<td>Severity</td>
<td>Warning</td>
</tr>
<tr>
<td>Description</td>
<td>Detects non-root users that log on over Telnet and rlogin.</td>
</tr>
</tbody>
</table>

**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 8-38  Description of the **Root logon** parameters used

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Option Path</td>
<td>System Login Activity and Access Monitor &gt; System Login Success Monitor &gt; SU Operation Options</td>
</tr>
<tr>
<td>Option</td>
<td>SU to root</td>
</tr>
<tr>
<td>Rule Name</td>
<td>SU_ToRoot_Success</td>
</tr>
<tr>
<td>Severity</td>
<td>Warning</td>
</tr>
<tr>
<td>Description</td>
<td>Detects the successful logons as root, monitored in the UNIX syslog.</td>
</tr>
</tbody>
</table>
Table 8-39  Description of the **Non-root logon** parameters used

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Option Path</td>
<td>System Login Activity and Access Monitor &gt; System Login Success Monitor &gt; SU Operation Options</td>
</tr>
<tr>
<td>Option</td>
<td>SU to non-root</td>
</tr>
<tr>
<td>Rule Name</td>
<td>SU_ToUser_Success</td>
</tr>
<tr>
<td>Severity</td>
<td>Notice</td>
</tr>
<tr>
<td>Description</td>
<td>Detects the successful logons of non-root users.</td>
</tr>
</tbody>
</table>

**SSH Remote logon Options**

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

Table 8-40  Description of the **Root logon** parameters used

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Option Path</td>
<td>System Login Activity and Access Monitor &gt; System Login Success Monitor &gt; SSH Remote logon Options</td>
</tr>
<tr>
<td>Option</td>
<td>Root logon</td>
</tr>
<tr>
<td>Rule Name</td>
<td>Root_SSH_Logon_Success</td>
</tr>
<tr>
<td>Severity</td>
<td>Warning</td>
</tr>
<tr>
<td>Description</td>
<td>Detects logons as root that occur over SSH.</td>
</tr>
</tbody>
</table>

Table 8-41  Description of the **Non-root logon** parameters used

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Option Path</td>
<td>System Login Activity and Access Monitor &gt; System Login Success Monitor &gt; SSH Remote logon Options</td>
</tr>
<tr>
<td>Option</td>
<td>Non-root logon</td>
</tr>
<tr>
<td>Rule Name</td>
<td>User_SSH_Logon_Success</td>
</tr>
<tr>
<td>Severity</td>
<td>Notice</td>
</tr>
<tr>
<td>Description</td>
<td>Detects non-root user logons that occur over SSH.</td>
</tr>
</tbody>
</table>
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 8-42 Description of the Root logon parameters used

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Option Path</td>
<td>System Login Activity and Access Monitor &gt; System Login Success Monitor &gt; Local Console logon Options</td>
</tr>
<tr>
<td>Option</td>
<td>Root logon</td>
</tr>
<tr>
<td>Rule Name</td>
<td>Root_Local_Logon_Success</td>
</tr>
<tr>
<td>Severity</td>
<td>Warning</td>
</tr>
<tr>
<td>Description</td>
<td>Detects root user logon events that occur over the console.</td>
</tr>
</tbody>
</table>

Table 8-43 Description of the Non-root logon parameters used

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Option Path</td>
<td>System Login Activity and Access Monitor &gt; System Login Success Monitor &gt; Local Console logon Options</td>
</tr>
<tr>
<td>Option</td>
<td>Non-root logon</td>
</tr>
<tr>
<td>Rule Name</td>
<td>User_Local_Logon_Success</td>
</tr>
<tr>
<td>Severity</td>
<td>Warning</td>
</tr>
<tr>
<td>Description</td>
<td>Detects non-root user logon events that occur over the console.</td>
</tr>
</tbody>
</table>

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 8-44  Description of the **SU to root Logoff** parameters used

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Option Path</td>
<td>System Login Activity and Access Monitor &gt; System Logoff Monitor &gt; SU Operation Options</td>
</tr>
<tr>
<td>Option</td>
<td>SU to root Logoff</td>
</tr>
<tr>
<td>Rule Name</td>
<td>SU_ToRoot_Logoff</td>
</tr>
<tr>
<td>Severity</td>
<td>Warning</td>
</tr>
<tr>
<td>Description</td>
<td>Detects the successful logoff by user from SU to root.</td>
</tr>
</tbody>
</table>

Table 8-45  Description of the **SU to non-root Logoff** parameters used

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Option Path</td>
<td>System Login Activity and Access Monitor &gt; System Logoff Monitor &gt; SU Operation Options</td>
</tr>
<tr>
<td>Option</td>
<td>SU to non-root Logoff</td>
</tr>
<tr>
<td>Rule Name</td>
<td>SU_ToUser_Logoff</td>
</tr>
<tr>
<td>Severity</td>
<td>Warning</td>
</tr>
<tr>
<td>Description</td>
<td>Detects the successful logoff by user from SU to a non-root user.</td>
</tr>
</tbody>
</table>

**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 8-46  Description of the **Root logoff** parameters used

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Option Path</td>
<td>System Login Activity and Access Monitor &gt; System Login Success Monitor &gt; SSH Remote logoff Options</td>
</tr>
<tr>
<td>Option</td>
<td>Root logoff</td>
</tr>
<tr>
<td>Rule Name</td>
<td>Root_SSH_Logoff</td>
</tr>
<tr>
<td>Severity</td>
<td>Warning</td>
</tr>
</tbody>
</table>
Table 8-46 Description of the Root logoff parameters used (continued)

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Description</td>
<td>Detects root user logoff events that occur over SSH from a remote console.</td>
</tr>
</tbody>
</table>

Table 8-47 Description of the Non-root logoff parameters used

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Option Path</td>
<td>System Login Activity and Access Monitor &gt; System Login Success Monitor &gt; SSH Remote logoff Options</td>
</tr>
<tr>
<td>Option</td>
<td>Non-root logoff</td>
</tr>
<tr>
<td>Rule Name</td>
<td>User_SSH_Logoff</td>
</tr>
<tr>
<td>Severity</td>
<td>Warning</td>
</tr>
<tr>
<td>Description</td>
<td>Detects non-root user logoff events that occur over SSH from a remote console.</td>
</tr>
</tbody>
</table>

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 8-48 Description of the Root Logoff parameters used

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Option Path</td>
<td>System Login Activity and Access Monitor &gt; System Login Success Monitor &gt; SSH Remote logoff Options</td>
</tr>
<tr>
<td>Option</td>
<td>Root Logoff</td>
</tr>
<tr>
<td>Rule Name</td>
<td>Root_Local_Logoff</td>
</tr>
<tr>
<td>Severity</td>
<td>Warning</td>
</tr>
<tr>
<td>Description</td>
<td>Detects root user logoff events that occur on the local console.</td>
</tr>
</tbody>
</table>
Table 8-49 Description of the Non-Root Logoff parameters used

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Option Path</td>
<td>System Login Activity and Access Monitor &gt; System Login Success Monitor &gt; SSH Remote logoff Options</td>
</tr>
<tr>
<td>Option</td>
<td>Non-Root_Logoff</td>
</tr>
<tr>
<td>Rule Name</td>
<td>User_Local_Logoff</td>
</tr>
<tr>
<td>Severity</td>
<td>Warning</td>
</tr>
<tr>
<td>Description</td>
<td>Detects non-root user logoff events that occur on the local console.</td>
</tr>
</tbody>
</table>

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 8-50 Description of the Number of logon failures in time interval parameters used

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Option Path</td>
<td>System Login Activity and Access Monitor &gt; System Failed Login Monitor &gt; FTP logon failure&gt;Repeated FTP logon failures</td>
</tr>
<tr>
<td>Option</td>
<td>Number of logon failures in time interval</td>
</tr>
<tr>
<td>Value</td>
<td>blank value</td>
</tr>
<tr>
<td></td>
<td>The user specifies this value.</td>
</tr>
<tr>
<td>Description</td>
<td>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.</td>
</tr>
</tbody>
</table>
### Table 8-51: Description of the **Time interval** parameters used

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Option Path</td>
<td>System Login Activity and Access Monitor &gt; System Failed Login Monitor &gt; FTP logon failure&gt;Repeated FTP logon failures</td>
</tr>
<tr>
<td>Option</td>
<td>Time interval</td>
</tr>
<tr>
<td>Duration</td>
<td>In days, hours, minutes, and seconds.</td>
</tr>
<tr>
<td>Description</td>
<td>Sets a specific time interval during which the failed logon attempts have to take place to generate an event.</td>
</tr>
</tbody>
</table>

### Table 8-52: Description of the **FTP Repeated Failed Severity** parameters used

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Option Path</td>
<td>System Login Activity and Access Monitor &gt; System Failed Login Monitor &gt; FTP logon failure&gt;Repeated FTP logon failures</td>
</tr>
<tr>
<td>Option</td>
<td>FTP Repeated Failed Severity</td>
</tr>
<tr>
<td>Severity</td>
<td>Major</td>
</tr>
<tr>
<td>Description</td>
<td>Sets the severity of failed logon attempts.</td>
</tr>
</tbody>
</table>

### 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 8-53: Description of the **Root logon failure** parameters used

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Option Path</td>
<td>System Login Activity and Access Monitor &gt; System Failed Login Monitor &gt; FTP server reports to Syslog or WTMP</td>
</tr>
<tr>
<td>Option</td>
<td>Root logon failure</td>
</tr>
<tr>
<td>Rule Name</td>
<td>Root_FTP_Logon_Failure</td>
</tr>
<tr>
<td>Severity</td>
<td>Notice</td>
</tr>
<tr>
<td>Description</td>
<td>Detects failed attempts to log on over FTP as a root user that are reported in the syslog or wtmp file.</td>
</tr>
<tr>
<td>Parameter</td>
<td>Description</td>
</tr>
<tr>
<td>--------------</td>
<td>----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Option Path</td>
<td>System Login Activity and Access Monitor &gt; System Failed Login Monitor &gt; FTP server reports to Syslog or WTMP</td>
</tr>
<tr>
<td>Option</td>
<td>Non-root logon failure</td>
</tr>
<tr>
<td>Rule Name</td>
<td>User_FTP_Logon_Failure</td>
</tr>
<tr>
<td>Severity</td>
<td>Warning</td>
</tr>
<tr>
<td>Description</td>
<td>Detects failed attempts to log on as a non-root user over FTP that are reported in the syslog or wtmp file.</td>
</tr>
</tbody>
</table>

**FTP server reports to a log file**
Set this option if your FTP servers report to a log file. You must specify the path to the FTP log file.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Option Path</td>
<td>System Login Activity and Access Monitor &gt; System Failed Login Monitor &gt; FTP logon failure &gt; FTP server reports to a log file</td>
</tr>
<tr>
<td>Option</td>
<td>Path to FTP server log file</td>
</tr>
<tr>
<td>Path</td>
<td>/var/log/vsftpd.log</td>
</tr>
<tr>
<td>Description</td>
<td>Sets the path to the FTP server log file.</td>
</tr>
</tbody>
</table>

**Path to FTP server log file parameters used**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Option Path</td>
<td>System Login Activity and Access Monitor &gt; System Failed Login Monitor &gt; FTP logon failure &gt; FTP server reports to a log file</td>
</tr>
<tr>
<td>Option</td>
<td>Root logon failure</td>
</tr>
<tr>
<td>Rule Name</td>
<td>Root_FTP_Logon_Failure_Text_Log</td>
</tr>
<tr>
<td>Severity</td>
<td>Notice</td>
</tr>
<tr>
<td>Description</td>
<td>Detects failed attempts to log on over FTP as a root user.</td>
</tr>
</tbody>
</table>
### Table 8-57 Description of the Non-root logon failure parameters used

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Option Path</td>
<td>System Login Activity and Access Monitor &gt; System Failed Login Monitor &gt; FTP logon failure &gt; FTP server reports to a log file</td>
</tr>
<tr>
<td>Option</td>
<td>Non-root logon failure</td>
</tr>
<tr>
<td>Rule Name</td>
<td>User_FTP_Logon_Failure_Text_Log</td>
</tr>
<tr>
<td>Severity</td>
<td>Notice</td>
</tr>
<tr>
<td>Description</td>
<td>Detects failed attempts to log on over FTP as a regular user.</td>
</tr>
</tbody>
</table>

### 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 8-58 Description of the Number of Logon Failures in Time Interval parameters used

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Option Path</td>
<td>System Login Activity and Access Monitor &gt; System Failed Login Monitor &gt;Telnet and Rlogin logon failure&gt;Repeated Telnet or Rlogin logon failures</td>
</tr>
<tr>
<td>Option</td>
<td>Number of Logon Failures in Time Interval</td>
</tr>
<tr>
<td>Value</td>
<td>blank value</td>
</tr>
<tr>
<td></td>
<td>The user specifies this value.</td>
</tr>
<tr>
<td>Description</td>
<td>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.</td>
</tr>
</tbody>
</table>
**Table 8-59**  Description of the Time interval parameters used

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Option Path</td>
<td>System Login Activity and Access Monitor &gt; System Failed Login Monitor &gt; Repeated Telnet or Rlogin logon failures</td>
</tr>
<tr>
<td>Option</td>
<td>Time Interval</td>
</tr>
<tr>
<td>Duration</td>
<td>In days, hours, minutes, and seconds.</td>
</tr>
<tr>
<td>Description</td>
<td>Sets a specific time interval during which the failed logon attempts take place.</td>
</tr>
</tbody>
</table>

**Table 8-60**  Description of the Telnet Repeated Failed Severity parameters used

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Option Path</td>
<td>System Login Activity and Access Monitor &gt; System Failed Login Monitor &gt; Telnet and Rlogin logon failure &gt; Repeated Telnet or Rlogin logon failures</td>
</tr>
<tr>
<td>Option</td>
<td>Telnet Repeated Failed Severity</td>
</tr>
<tr>
<td>Severity</td>
<td>Major</td>
</tr>
<tr>
<td>Description</td>
<td>Sets the severity of the Telnet or rlogin failed logon attempts.</td>
</tr>
</tbody>
</table>

**Table 8-61**  Description of the Root logon failure parameters used

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Option Path</td>
<td>System Login Activity and Access Monitor &gt; System Failed Login Monitor &gt; Telnet and Rlogin logon failure</td>
</tr>
<tr>
<td>Option</td>
<td>Root logon failure</td>
</tr>
<tr>
<td>Rule Name</td>
<td>Root_Telnet_Rlogin_Logon_Failure</td>
</tr>
<tr>
<td>Severity</td>
<td>Warning</td>
</tr>
<tr>
<td>Description</td>
<td>Detects failed attempts to log on over Telnet or rlogin as a root user.</td>
</tr>
</tbody>
</table>

**Table 8-62**  Description of the Non-root logon failure parameters used

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Option Path</td>
<td>System Login Activity and Access Monitor &gt; System Failed Login Monitor &gt; Telnet and Rlogin logon failure</td>
</tr>
</tbody>
</table>
Table 8-62  Description of the Non-root logon failure parameters used  
(continued)

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Option</td>
<td>Non-root logon failure</td>
</tr>
<tr>
<td>Rule Name</td>
<td>User_Telnet_Rlogin_Logon_Failure</td>
</tr>
<tr>
<td>Severity</td>
<td>blank value</td>
</tr>
<tr>
<td></td>
<td>The user specifies this value.</td>
</tr>
<tr>
<td>Description</td>
<td>Detects failed attempts to log on over Telnet or rlogin as a regular user.</td>
</tr>
</tbody>
</table>

**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 8-63  Description of the Number of Logon Failures in Time Interval  
parameters used

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Option Path</td>
<td>System Login Activity and Access Monitor &gt; System Failed Login Monitor  &gt; SU failure &gt; Repeated SU failures</td>
</tr>
<tr>
<td>Option</td>
<td>Number of Logon Failures in Time Interval</td>
</tr>
<tr>
<td>Value</td>
<td>blank value</td>
</tr>
<tr>
<td></td>
<td>The user specifies this value.</td>
</tr>
<tr>
<td>Description</td>
<td>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.</td>
</tr>
</tbody>
</table>
### Table 8-64  Description of the **Time interval** parameters used

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Option Path</td>
<td>System Login Activity and Access Monitor &gt; System Failed Login Monitor &gt; SU failure &gt; Repeated SU failures</td>
</tr>
<tr>
<td>Option</td>
<td>Time Interval</td>
</tr>
<tr>
<td>Duration</td>
<td>In days, hours, minutes, and seconds.</td>
</tr>
<tr>
<td>Description</td>
<td>Sets a specific time interval during which the failed logon attempts take place.</td>
</tr>
</tbody>
</table>

### Table 8-65  Description of the **SU Repeated Failed Severity** parameters used

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Option Path</td>
<td>System Login Activity and Access Monitor &gt; System Failed Login Monitor &gt; SU failure &gt; Repeated SU failures</td>
</tr>
<tr>
<td>Option</td>
<td>SU Repeated Failed Severity</td>
</tr>
<tr>
<td>Severity</td>
<td>Major</td>
</tr>
<tr>
<td>Description</td>
<td>Sets the severity of the SU failed logon attempts.</td>
</tr>
</tbody>
</table>

### Table 8-66  Description of the **SU to root failure** parameters used

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Option Path</td>
<td>System Login Activity and Access Monitor &gt; System Failed Login Monitor &gt; SU failure</td>
</tr>
<tr>
<td>Option</td>
<td>SU to root failure</td>
</tr>
<tr>
<td>Rule Name</td>
<td>SU_ToRoot_Failure</td>
</tr>
<tr>
<td>Severity</td>
<td>Warning</td>
</tr>
<tr>
<td>Description</td>
<td>Detects failed attempts to log on as a root user.</td>
</tr>
</tbody>
</table>

### Table 8-67  Description of the **SU to non-root failure** parameters used

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Option Path</td>
<td>System Login Activity and Access Monitor &gt; System Failed Login Monitor &gt; SU failure</td>
</tr>
<tr>
<td>Option</td>
<td>SU to non-root failure</td>
</tr>
</tbody>
</table>
Table 8-67 Description of the **SU to non-root failure** parameters used (continued)

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Rule Name</td>
<td>SU_ToUser_Failure</td>
</tr>
<tr>
<td>Severity</td>
<td>Notice</td>
</tr>
<tr>
<td>Description</td>
<td>Detects failed attempts to log on as a regular user.</td>
</tr>
</tbody>
</table>

**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 8-68 Description of the **Number of Logon Failures in Time Interval** parameters used

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Option Path</td>
<td>System Login Activity and Access Monitor &gt; System Failed Login Monitor &gt; SSH logon failure&gt;Repeated SSH logon failures</td>
</tr>
<tr>
<td>Option</td>
<td>Number of Logon Failures in Time Interval</td>
</tr>
<tr>
<td>Value</td>
<td>blank value</td>
</tr>
<tr>
<td>Description</td>
<td>The user specifies this value.</td>
</tr>
<tr>
<td></td>
<td>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.</td>
</tr>
</tbody>
</table>

Table 8-69 Description of the **Time interval** parameters used

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Option Path</td>
<td>System Login Activity and Access Monitor &gt; System Failed Login Monitor &gt; SSH logon failure&gt;Repeated SSH logon failures</td>
</tr>
<tr>
<td>Option</td>
<td>Time Interval</td>
</tr>
<tr>
<td>Duration</td>
<td>In days, hours, minutes, and seconds.</td>
</tr>
</tbody>
</table>
### Table 8-69  
Description of the **Time interval** parameters used *(continued)*

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Description</td>
<td>Sets a specific time interval during which the failed logon attempts take place.</td>
</tr>
</tbody>
</table>

### Table 8-70  
Description of the **SSH Repeated Failed Severity** parameters used

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Option Path</td>
<td>System Login Activity and Access Monitor &gt; System Failed Login Monitor &gt; SSH logon failure&gt;Repeated SSH logon failures</td>
</tr>
<tr>
<td>Option</td>
<td>SSH Repeated Failed Severity</td>
</tr>
<tr>
<td>Severity</td>
<td>Major</td>
</tr>
<tr>
<td>Description</td>
<td>Sets the severity of the SSH failed logon attempts.</td>
</tr>
</tbody>
</table>

### Table 8-71  
Description of the **Root logon failure** parameters used

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Option Path</td>
<td>System Login Activity and Access Monitor &gt; System Failed Login Monitor &gt; SSH logon failure</td>
</tr>
<tr>
<td>Option</td>
<td>Root logon failure</td>
</tr>
<tr>
<td>Rule Name</td>
<td>Root_SSH_Logon_Failure</td>
</tr>
<tr>
<td>Severity</td>
<td>Warning</td>
</tr>
<tr>
<td>Description</td>
<td>Detects failed attempts to log on as a root user.</td>
</tr>
</tbody>
</table>

### Table 8-72  
Description of the **Non-Root logon failure** parameters used

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Option Path</td>
<td>System Login Activity and Access Monitor &gt; System Failed Login Monitor &gt; SSH logon failure</td>
</tr>
<tr>
<td>Option</td>
<td>Non-Root logon failure</td>
</tr>
<tr>
<td>Rule Name</td>
<td>User_SSH_Logon_Failure</td>
</tr>
<tr>
<td>Severity</td>
<td>Notice</td>
</tr>
<tr>
<td>Description</td>
<td>Detects failed attempts to log on as a regular user.</td>
</tr>
</tbody>
</table>
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 8-73 Description of the Number of Logon Failures in Time Interval parameters used

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Option Path</td>
<td>System Login Activity and Access Monitor &gt; System Failed Login Monitor &gt; Local logon failure&gt;Repeated local logon failures</td>
</tr>
<tr>
<td>Option</td>
<td>Number of Logon Failures in Time Interval</td>
</tr>
<tr>
<td>Value</td>
<td>blank value</td>
</tr>
<tr>
<td></td>
<td>The user specifies this value.</td>
</tr>
<tr>
<td>Description</td>
<td>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.</td>
</tr>
</tbody>
</table>

Table 8-74 Description of the Time interval parameters used

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Option Path</td>
<td>System Login Activity and Access Monitor &gt; System Failed Login Monitor &gt; Local logon failure&gt;Repeated local logon failures</td>
</tr>
<tr>
<td>Option</td>
<td>Time Interval</td>
</tr>
<tr>
<td>Duration</td>
<td>In days, hours, minutes, and seconds.</td>
</tr>
<tr>
<td>Description</td>
<td>Sets a specific time interval during which the failed logon attempts take place.</td>
</tr>
</tbody>
</table>

Table 8-75 Description of the Local Repeated Failed Severity parameters used

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Option Path</td>
<td>System Login Activity and Access Monitor &gt; System Failed Login Monitor &gt; Local logon failure&gt;Repeated local logon failures</td>
</tr>
</tbody>
</table>
### Table 8-75 Description of the Local Repeated Failed Severity parameters used (continued)

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Option</td>
<td>Local Repeated Failed Severity</td>
</tr>
<tr>
<td>Severity</td>
<td>Major</td>
</tr>
<tr>
<td>Description</td>
<td>Sets the severity of the failed logon attempts from the local console.</td>
</tr>
</tbody>
</table>

### Table 8-76 Description of the Root logon failure parameters used

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Option Path</td>
<td>System Login Activity and Access Monitor &gt; System Failed Login Monitor &gt; Local logon failure</td>
</tr>
<tr>
<td>Option</td>
<td>Root logon failure</td>
</tr>
<tr>
<td>Rule Name</td>
<td>Root_Local_Login_Failure</td>
</tr>
<tr>
<td>Severity</td>
<td>Warning</td>
</tr>
<tr>
<td>Description</td>
<td>Detects failed attempts to log on as a root user.</td>
</tr>
</tbody>
</table>

### Table 8-77 Description of the Non-root logon failure parameters used

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Option Path</td>
<td>System Login Activity and Access Monitor &gt; System Failed Login Monitor &gt; Local logon failure</td>
</tr>
<tr>
<td>Option</td>
<td>Non-root logon failure</td>
</tr>
<tr>
<td>Rule Name</td>
<td>User_Local_Login_Failure</td>
</tr>
<tr>
<td>Severity</td>
<td>Notice</td>
</tr>
<tr>
<td>Description</td>
<td>Detects repeated failed attempts to log on as a regular user.</td>
</tr>
</tbody>
</table>

### 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 8-78 Description of the Authorized Sudo Users, Strings, or Commands (whitelisted) parameters used

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

Table 8-79 Description of the Banned Sudo Commands (blacklisted) parameters used

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

Sudo Command Monitor

Table 8-80 Description of the Sudo Command Monitor parameters used

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Option Path</td>
<td>System Privileged Command and Bash History Monitor &gt; Sudo Monitoring Options</td>
</tr>
<tr>
<td>Option</td>
<td>Sudo Command Monitor</td>
</tr>
<tr>
<td>Rule Name</td>
<td>Baseline_Sudo_Command_Watch</td>
</tr>
</tbody>
</table>
Table 8-80  Description of the **Sudo Command Monitor** parameters used (continued)

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Severity</td>
<td>Notice</td>
</tr>
<tr>
<td>Description</td>
<td>Detects use of the sudo command.</td>
</tr>
</tbody>
</table>

**Sudo Command Failure Monitor**

Table 8-81  Description of the **Sudo Command Failure Monitor** parameters used

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Option Path</td>
<td>System Privileged Command and Bash History Monitor &gt; Sudo Monitoring Options</td>
</tr>
<tr>
<td>Option</td>
<td>Sudo Command Failure Monitor</td>
</tr>
<tr>
<td>Rule Name</td>
<td>Baseline_Sudo_Command_Failure</td>
</tr>
<tr>
<td>Description</td>
<td>Detects the failures of sudo command use.</td>
</tr>
</tbody>
</table>

**Sudo Authorization Failure Monitor**

Table 8-82  Description of the **Sudo Authorization Failure Monitor** parameters used

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Option Path</td>
<td>System Privileged Command and Bash History Monitor &gt; Sudo Monitoring Options</td>
</tr>
<tr>
<td>Option</td>
<td>Sudo Authorization Failure Monitor</td>
</tr>
<tr>
<td>Rule Name</td>
<td>Baseline_Sudo_Authentication_Failure</td>
</tr>
<tr>
<td>Severity</td>
<td>Warning</td>
</tr>
<tr>
<td>Description</td>
<td>Detects failures in the authorization of the sudo command.</td>
</tr>
</tbody>
</table>
**Additional Sudo Monitoring Options**

Table 8-83  Description of the **Additional Sudo Monitoring Options** parameters used

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Option Path</td>
<td>System Privileged Command and Bash History Monitor &gt; Sudo Monitoring Options</td>
</tr>
<tr>
<td>Option</td>
<td>Additional Sudo Monitoring Options</td>
</tr>
<tr>
<td>Rule Name</td>
<td>System_PrivCmd_BashHist_Sudo_AddContent</td>
</tr>
<tr>
<td>Severity</td>
<td>Info</td>
</tr>
<tr>
<td>Description</td>
<td>Detects use of the sudo command.</td>
</tr>
</tbody>
</table>

**User Command History Options**

Table 8-84  Description of the **User 1 Command History Monitor** parameters used

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Option Path</td>
<td>System Privileged Command and Bash History Monitor &gt; User Command History Options</td>
</tr>
<tr>
<td>Option</td>
<td>User 1 Command History Monitor</td>
</tr>
<tr>
<td>Rule Name</td>
<td>Baseline_User_Command_Watch</td>
</tr>
<tr>
<td>Severity</td>
<td>Notice</td>
</tr>
<tr>
<td>User's Bash History Log File Path</td>
<td>/home/user1/.bash_history</td>
</tr>
<tr>
<td>Description</td>
<td>Monitors the commands used by a specific user.</td>
</tr>
</tbody>
</table>

Table 8-85  Description of the **User 2 Command History Monitor** parameters used

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Option Path</td>
<td>System Privileged Command and Bash History Monitor &gt; User Command History Options</td>
</tr>
<tr>
<td>Option</td>
<td>User 2 Command History Monitor</td>
</tr>
</tbody>
</table>
Table 8-85  Description of the **User 2 Command History Monitor** parameters used (continued)

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Rule Name</td>
<td>Baseline_User2_Command_Watch</td>
</tr>
<tr>
<td>Severity</td>
<td>Notice</td>
</tr>
<tr>
<td>User's Bash History Log File Path</td>
<td>/home/user2/.bash_history</td>
</tr>
<tr>
<td>Description</td>
<td>Monitors the commands used by a second specific user.</td>
</tr>
</tbody>
</table>

Superuser (Root Level) Command History Options

Table 8-86  Description of the **Root Command History Monitor** parameters used

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Option Path</td>
<td>System Privileged Command and Bash History Monitor &gt; Superuser (Root Level) Command History Options</td>
</tr>
<tr>
<td>Option</td>
<td>Root Command History Monitor</td>
</tr>
<tr>
<td>Rule Name</td>
<td>Baseline_Root_Command_Watch</td>
</tr>
<tr>
<td>Severity</td>
<td>Notice</td>
</tr>
<tr>
<td>Root's Bash History Log File Path</td>
<td>/root/.bash_history</td>
</tr>
<tr>
<td>Description</td>
<td>Monitors the commands used by users who are logged in as root.</td>
</tr>
</tbody>
</table>

Table 8-87  Description of the **Superuser Command History Monitor** parameters used

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Option Path</td>
<td>System Privileged Command and Bash History Monitor &gt; Superuser (Root Level) Command History Options</td>
</tr>
<tr>
<td>Option</td>
<td>Superuser Command History Monitor</td>
</tr>
<tr>
<td>Rule Name</td>
<td>Baseline_Superuser_Command_Watch</td>
</tr>
</tbody>
</table>
Table 8-87 Description of the Superuser Command History Monitor parameters used (continued)

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Severity</td>
<td>Notice</td>
</tr>
<tr>
<td>Superuser's Bash History Log File Path</td>
<td>/home/superuser/.bash_history</td>
</tr>
<tr>
<td>Description</td>
<td>Monitors the commands used by users who are logged in as superuser.</td>
</tr>
</tbody>
</table>

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 8-88 Description of the Daemon Run Level RC.D Monitor parameters used

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Option Path</td>
<td>System Hardening Monitor &gt; System Auto Start Change Options</td>
</tr>
<tr>
<td>Option</td>
<td>Daemon Run Level RC.D Monitor</td>
</tr>
<tr>
<td>Rule Name</td>
<td>AutoStart_RC.D_Monitor</td>
</tr>
<tr>
<td>Severity</td>
<td>Warning</td>
</tr>
<tr>
<td>File Paths</td>
<td>/etc/rc.*</td>
</tr>
<tr>
<td></td>
<td>/etc/rc.d/*</td>
</tr>
<tr>
<td></td>
<td>/etc/init.d/*</td>
</tr>
</tbody>
</table>
Table 8-88  Description of the **Daemon Run Level RC.D Monitor** parameters used (continued)

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Additional Settings</td>
<td>You can also monitor the following events:</td>
</tr>
<tr>
<td></td>
<td>■ Monitor Value Addition to Run Level Files</td>
</tr>
<tr>
<td></td>
<td>■ Monitor Value Removal to Run Level Files</td>
</tr>
<tr>
<td></td>
<td>■ Monitor File Modification</td>
</tr>
<tr>
<td></td>
<td>■ Monitor File Creation</td>
</tr>
<tr>
<td></td>
<td>■ Monitor File Removal</td>
</tr>
<tr>
<td>Description</td>
<td>Detects changes to the daemon rc files on the computer.</td>
</tr>
</tbody>
</table>

Table 8-89  Description of the **System Run Level INITTAB Monitor** parameters used

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Option Path</td>
<td>System Hardening Monitor &gt; System Auto Start Change Options</td>
</tr>
<tr>
<td>Option</td>
<td>System Run Level INITTAB Monitor</td>
</tr>
<tr>
<td>Rule Name</td>
<td>AutoStart_Inittab_Monitor</td>
</tr>
<tr>
<td>Severity</td>
<td>Warning</td>
</tr>
<tr>
<td>File Paths</td>
<td>/etc/inittab</td>
</tr>
<tr>
<td>Additional Settings</td>
<td>You can also monitor the following events:</td>
</tr>
<tr>
<td></td>
<td>■ Monitor Value Additions to the Inittab File</td>
</tr>
<tr>
<td></td>
<td>■ Monitor Value Removal to the Inittab File</td>
</tr>
<tr>
<td></td>
<td>■ Monitor File Modification</td>
</tr>
<tr>
<td></td>
<td>■ Monitor File Creation</td>
</tr>
<tr>
<td></td>
<td>■ Monitor File Removal</td>
</tr>
<tr>
<td>Description</td>
<td>Detects changes to the inittab file on the computer.</td>
</tr>
</tbody>
</table>

**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 DCS:SA 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 filewatch 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 8-90 Description of the Core System Files parameters used

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Option Path</td>
<td>System File and Directory Monitor &gt; System FileWatch Monitor &gt; Monitor System-Critical Files</td>
</tr>
<tr>
<td>Option</td>
<td>Core System Files</td>
</tr>
<tr>
<td>Rule Name</td>
<td>FileWatch_Sys_Core_Files</td>
</tr>
<tr>
<td>Severity</td>
<td>Warning</td>
</tr>
<tr>
<td>Parameter</td>
<td>Description</td>
</tr>
<tr>
<td>----------------</td>
<td>--------------------------------------------------</td>
</tr>
<tr>
<td>Monitor Paths</td>
<td>/bin/*</td>
</tr>
<tr>
<td></td>
<td>/lib/*</td>
</tr>
<tr>
<td></td>
<td>/sbin/*</td>
</tr>
<tr>
<td></td>
<td>/stand/vmunix</td>
</tr>
<tr>
<td></td>
<td>/unix</td>
</tr>
<tr>
<td></td>
<td>/usr/bin/*</td>
</tr>
<tr>
<td></td>
<td>/usr/lib/*</td>
</tr>
<tr>
<td></td>
<td>/usr/sbin/*</td>
</tr>
<tr>
<td></td>
<td>/usr/spool/cron/*</td>
</tr>
<tr>
<td></td>
<td>/var/adm/cron/*</td>
</tr>
<tr>
<td></td>
<td>/var/lib/*</td>
</tr>
<tr>
<td></td>
<td>/var/spool/cron/*</td>
</tr>
<tr>
<td>Ignore Strings</td>
<td>/usr/lib/cron/log</td>
</tr>
<tr>
<td></td>
<td>/usr/lib/objrepos</td>
</tr>
<tr>
<td></td>
<td>/usr/spool/cron/tmp</td>
</tr>
<tr>
<td></td>
<td>/var/adm/cron/FIFO</td>
</tr>
<tr>
<td></td>
<td>/var/adm/cron/log</td>
</tr>
<tr>
<td></td>
<td>/var/lib/objrepos</td>
</tr>
<tr>
<td></td>
<td>/var/log</td>
</tr>
<tr>
<td></td>
<td>/var/spool/cron/tmp</td>
</tr>
<tr>
<td>Monitor Ops</td>
<td>Deleted, Created, Modified</td>
</tr>
<tr>
<td></td>
<td>Accessed (not enabled by default)</td>
</tr>
<tr>
<td>Report File Differences</td>
<td>Available, Not Enabled</td>
</tr>
<tr>
<td>Date and Time Restriction</td>
<td>Available, Not Enabled</td>
</tr>
</tbody>
</table>
### Table 8-90  Description of the Core System Files parameters used (continued)

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Description</td>
<td>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.</td>
</tr>
<tr>
<td>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.</td>
<td></td>
</tr>
</tbody>
</table>

### Table 8-91  Description of the Core System Configuration Files parameters used

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Option Path</td>
<td>System File and Directory Monitor &gt; System FileWatch Monitor &gt; Monitor System-Critical Files</td>
</tr>
<tr>
<td>Option</td>
<td>Core System Configuration Files</td>
</tr>
<tr>
<td>Rule Name</td>
<td>FileWatch_Sys_Core_Configuration_Files</td>
</tr>
<tr>
<td>Severity</td>
<td>Warning</td>
</tr>
</tbody>
</table>
| Monitor Paths      | /etc/*.conf  
                      /etc/*.config  
                      /etc/_conf  
                      /etc/_config  
                      /etc/sudoers |
### Description of the Core System Configuration Files parameters used (continued)

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ignore Strings</td>
<td>/etc/<em>.log&lt;br&gt; /etc/</em>.pid&lt;br&gt; /etc/btmp&lt;br&gt; /etc/btmps&lt;br&gt; /etc/cron.d/FIFO&lt;br&gt; /etc/security/<em>log&lt;br&gt; /etc/sisips&lt;br&gt; /etc/sisips/</em>&lt;br&gt; /etc/sulogin&lt;br&gt; /etc/symantec/*&lt;br&gt; /etc/utmp&lt;br&gt; /etc/utmppipe&lt;br&gt; /etc/utmps&lt;br&gt; /etc/utmpx&lt;br&gt; /etc/wtmps&lt;br&gt; /etc/wtmpx</td>
</tr>
<tr>
<td>Monitor Ops</td>
<td>Deleted, Created, Modified&lt;br&gt; Accessed (not enabled by default)</td>
</tr>
<tr>
<td>Report File Differences</td>
<td>Available, Not Enabled</td>
</tr>
<tr>
<td>Date and Time Restriction</td>
<td>Available, Not Enabled</td>
</tr>
<tr>
<td>Description</td>
<td>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. <strong>Note:</strong> 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.</td>
</tr>
<tr>
<td>Parameter</td>
<td>Description</td>
</tr>
<tr>
<td>----------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Option Path</td>
<td>System File and Directory Monitor &gt; System FileWatch Monitor &gt; Monitor System-Critical Files</td>
</tr>
<tr>
<td>Option</td>
<td>Setup Programs and Packages</td>
</tr>
<tr>
<td>Rule Name</td>
<td>FileWatch_Sys_Setup_Files</td>
</tr>
<tr>
<td>Severity</td>
<td>Warning</td>
</tr>
<tr>
<td>Monitor Paths</td>
<td>/usr/sbin/pkg*</td>
</tr>
<tr>
<td></td>
<td>/var/lib/rpm/*</td>
</tr>
<tr>
<td></td>
<td>/var/sadm/install/admin/*</td>
</tr>
<tr>
<td>Ignore Strings</td>
<td><em>.log</em></td>
</tr>
<tr>
<td>Monitor Ops</td>
<td>Deleted, Created, Modified</td>
</tr>
<tr>
<td></td>
<td>Accessed (not enabled by default)</td>
</tr>
<tr>
<td>Report File Differences</td>
<td>Available, Not Enabled</td>
</tr>
<tr>
<td>Date and Time Restriction</td>
<td>Available, Not Enabled</td>
</tr>
<tr>
<td>Description</td>
<td>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.</td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> 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.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Option Path</td>
<td>System File and Directory Monitor &gt; System FileWatch Monitor &gt; Monitor System-Critical Files</td>
</tr>
<tr>
<td>Option</td>
<td>Common Daemon Files</td>
</tr>
<tr>
<td>Rule Name</td>
<td>FileWatch_Sys_Common_Program_Files</td>
</tr>
</tbody>
</table>
Table 8-93  Description of the **Common Daemon Files** parameters used *(continued)*

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Severity</td>
<td>Warning</td>
</tr>
</tbody>
</table>
Table 8-93  Description of the Common Daemon Files parameters used (continued)

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Monitor Paths</td>
<td></td>
</tr>
<tr>
<td>Parameter</td>
<td>Description</td>
</tr>
<tr>
<td>-----------</td>
<td>-------------</td>
</tr>
<tr>
<td>/etc/cron.d/logchecker</td>
<td></td>
</tr>
<tr>
<td>/etc/fs/*/mount</td>
<td></td>
</tr>
<tr>
<td>/lib/svc/nfs/lockd</td>
<td></td>
</tr>
<tr>
<td>/lib/svc/nfs/statd</td>
<td></td>
</tr>
<tr>
<td>/opt/sbin/in.named</td>
<td></td>
</tr>
<tr>
<td>/opt/sbin/lwresd</td>
<td></td>
</tr>
<tr>
<td>/opt/sbin/name</td>
<td></td>
</tr>
<tr>
<td>/sbin/auditd</td>
<td></td>
</tr>
<tr>
<td>/sbin/klogd</td>
<td></td>
</tr>
<tr>
<td>/sbin/syslogd</td>
<td></td>
</tr>
<tr>
<td>/usr/lib/cups/daemon/cups-lpd</td>
<td></td>
</tr>
<tr>
<td>/usr/lib/ssh/sshd</td>
<td></td>
</tr>
<tr>
<td>/usr/lib/zones/zoneadmd</td>
<td></td>
</tr>
<tr>
<td>/usr/local/sbin/in.named</td>
<td></td>
</tr>
<tr>
<td>/usr/local/sbin/in.tnamed</td>
<td></td>
</tr>
<tr>
<td>/usr/local/sbin/lwresd</td>
<td></td>
</tr>
<tr>
<td>/usr/local/sbin/named</td>
<td></td>
</tr>
<tr>
<td>/usr/local/sbin/sshd</td>
<td></td>
</tr>
<tr>
<td>/usr/sbin/atd</td>
<td></td>
</tr>
<tr>
<td>/usr/sbin/automount</td>
<td></td>
</tr>
<tr>
<td>/usr/sbin/cron</td>
<td></td>
</tr>
<tr>
<td>/usr/sbin/crond</td>
<td></td>
</tr>
<tr>
<td>/usr/sbin/cupsd</td>
<td></td>
</tr>
<tr>
<td>/usr/sbin/in.named</td>
<td></td>
</tr>
<tr>
<td>/usr/sbin/inetd</td>
<td></td>
</tr>
<tr>
<td>/usr/sbin/in.tnamed</td>
<td></td>
</tr>
<tr>
<td>/usr/sbin/inetd</td>
<td></td>
</tr>
<tr>
<td>/usr/sbin/lwresd</td>
<td></td>
</tr>
</tbody>
</table>
Table 8-93  Description of the **Common Daemon Files** parameters used  
(continued)

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>/usr/sbin/named</td>
</tr>
<tr>
<td></td>
<td>/usr/sbin/nmbd</td>
</tr>
<tr>
<td></td>
<td>/usr/sbin/rpc.mountd</td>
</tr>
<tr>
<td></td>
<td>/usr/sbin/smbd</td>
</tr>
<tr>
<td></td>
<td>/usr/sbin/sshd</td>
</tr>
<tr>
<td></td>
<td>/usr/sbin/syslogd</td>
</tr>
<tr>
<td></td>
<td>/usr/sbin/xinetd</td>
</tr>
<tr>
<td></td>
<td>/usr/sfw/sbin/nmbd</td>
</tr>
<tr>
<td></td>
<td>/usr/sfw/sbin/smbd</td>
</tr>
<tr>
<td>Monitor Ops</td>
<td>Deleted, Created, Modified</td>
</tr>
<tr>
<td></td>
<td>Accessed (not enabled by default)</td>
</tr>
<tr>
<td>Report File Differences</td>
<td>Available, Not Enabled</td>
</tr>
<tr>
<td>Date and Time Restriction</td>
<td>Available, Not Enabled</td>
</tr>
<tr>
<td>Description</td>
<td>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.</td>
</tr>
</tbody>
</table>

**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 8-94  Description of the **Monitor Script Files and Cron Files** parameters used

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Option Path</td>
<td>System File and Directory Monitor &gt; System FileWatch Monitor &gt; Monitor System-Critical Files</td>
</tr>
<tr>
<td>Option</td>
<td>Monitor Script Files and Cron Files</td>
</tr>
</tbody>
</table>
Table 8-94 Description of the **Monitor Script Files and Cron Files** parameters used (continued)

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Rule Name</td>
<td>FileWatch_Sys_Script_Files</td>
</tr>
<tr>
<td>Severity</td>
<td>Warning</td>
</tr>
<tr>
<td>Monitor Paths</td>
<td>blank value</td>
</tr>
<tr>
<td></td>
<td>The user specifies this value.</td>
</tr>
<tr>
<td>Monitor Ops</td>
<td>Deleted, Created, Modified</td>
</tr>
<tr>
<td></td>
<td>Accessed (not enabled by default)</td>
</tr>
<tr>
<td>Report File Differences</td>
<td>Available, Not Enabled</td>
</tr>
<tr>
<td>Date and Time</td>
<td>Available, Not Enabled</td>
</tr>
<tr>
<td>Restriction</td>
<td></td>
</tr>
<tr>
<td>Description</td>
<td>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. <strong>Note:</strong> 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.</td>
</tr>
</tbody>
</table>

Table 8-95 Description of the **Solaris Specific Files** parameters used

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Option Path</td>
<td>System File and Directory Monitor &gt; System FileWatch Monitor &gt; Monitor System-Critical Files</td>
</tr>
<tr>
<td>Option</td>
<td>Solaris Specific Files</td>
</tr>
<tr>
<td>Rule Name</td>
<td>FileWatch_Sys_Other_Files_Solaris</td>
</tr>
<tr>
<td>Severity</td>
<td>Warning</td>
</tr>
<tr>
<td>Monitor Paths</td>
<td>blank value</td>
</tr>
<tr>
<td></td>
<td>The user specifies this value.</td>
</tr>
</tbody>
</table>
Table 8-95  Description of the **Solaris Specific Files** parameters used (continued)

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

Table 8-96  Description of the **AIX Specific Files** parameters used

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Option Path</td>
<td>System File and Directory Monitor &gt; System FileWatch Monitor &gt; Monitor System-Critical Files</td>
</tr>
<tr>
<td>Option</td>
<td>AIX Specific Files</td>
</tr>
<tr>
<td>Rule Name</td>
<td>FileWatch_Sys_Other_Files_AIX</td>
</tr>
<tr>
<td>Severity</td>
<td>Warning</td>
</tr>
<tr>
<td>Monitor Paths</td>
<td>blank value</td>
</tr>
<tr>
<td></td>
<td>The user specifies this value.</td>
</tr>
<tr>
<td>Monitor Ops</td>
<td>Deleted, Created, Modified</td>
</tr>
<tr>
<td></td>
<td>Accessed (not enabled by default)</td>
</tr>
<tr>
<td>Report File Differences</td>
<td>Available, Not Enabled</td>
</tr>
<tr>
<td>Date and Time</td>
<td>Available, Not Enabled</td>
</tr>
<tr>
<td>Restriction</td>
<td></td>
</tr>
</tbody>
</table>
Table 8-96  Description of the **AIX Specific Files** parameters used *(continued)*

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Description</td>
<td>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. <strong>Note:</strong> 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.</td>
</tr>
</tbody>
</table>

Table 8-97  Description of the **Linux Specific Files** parameters used

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Option Path</td>
<td>System File and Directory Monitor &gt; System FileWatch Monitor &gt; Monitor System-Critical Files</td>
</tr>
<tr>
<td>Option</td>
<td>Linux Specific Files</td>
</tr>
<tr>
<td>Rule Name</td>
<td>FileWatch_Sys_Other_Files_Linux</td>
</tr>
<tr>
<td>Severity</td>
<td>Warning</td>
</tr>
<tr>
<td>Monitor Paths</td>
<td>blank value</td>
</tr>
<tr>
<td></td>
<td>The user specifies this value.</td>
</tr>
<tr>
<td>Monitor Ops</td>
<td>Deleted, Created, Modified</td>
</tr>
<tr>
<td></td>
<td>Accessed (not enabled by default)</td>
</tr>
<tr>
<td>Report File Differences</td>
<td>Available, Not Enabled</td>
</tr>
<tr>
<td>Date and Time Restriction</td>
<td>Available, Not Enabled</td>
</tr>
</tbody>
</table>
### Table 8-97  
Description of the **Linux Specific Files** parameters used (continued)

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

### Table 8-98  
Description of the **HPUX Specific Files** parameters used

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Option Path</td>
<td>System File and Directory Monitor &gt; System FileWatch Monitor &gt;</td>
</tr>
<tr>
<td></td>
<td>Monitor System-Critical Files</td>
</tr>
<tr>
<td>Option</td>
<td>HPUX Specific Files</td>
</tr>
<tr>
<td>Rule Name</td>
<td>FileWatch_Sys_Other_Files_HPUX</td>
</tr>
<tr>
<td>Severity</td>
<td>Warning</td>
</tr>
<tr>
<td>Monitor Paths</td>
<td>blank value</td>
</tr>
<tr>
<td></td>
<td>The user specifies this value.</td>
</tr>
<tr>
<td>Monitor Ops</td>
<td>Deleted, Created, Modified</td>
</tr>
<tr>
<td></td>
<td>Accessed (not enabled by default)</td>
</tr>
<tr>
<td>Report File Differences</td>
<td>Available, Not Enabled</td>
</tr>
<tr>
<td>Date and Time</td>
<td>Available, Not Enabled</td>
</tr>
<tr>
<td>Restriction</td>
<td></td>
</tr>
</tbody>
</table>
Table 8-98 Description of the HP-UX Specific Files parameters used (continued)

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Description</td>
<td>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.</td>
</tr>
</tbody>
</table>

**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 8-99** Description of the Virus Detected parameters used

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Option Path</td>
<td>System Symantec Software Monitor &gt; Symantec AntiVirus for Linux (SAVFL) Client Communication</td>
</tr>
<tr>
<td>Option</td>
<td>Virus Detected</td>
</tr>
<tr>
<td>Rule Name</td>
<td>Virus_Detected</td>
</tr>
<tr>
<td>Severity</td>
<td>Critical</td>
</tr>
<tr>
<td>Description</td>
<td>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.</td>
</tr>
</tbody>
</table>

**Table 8-100** Description of the Service Stopped parameters used

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Option Path</td>
<td>System Symantec Software Monitor &gt; Symantec AntiVirus for Linux (SAVFL) Client Communication</td>
</tr>
<tr>
<td>Option</td>
<td>Service Stopped</td>
</tr>
</tbody>
</table>
Table 8-100  Description of the **Service Stopped** parameters used *(continued)*

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Rule Name</td>
<td>Service_Stopped</td>
</tr>
<tr>
<td>Severity</td>
<td>Warning</td>
</tr>
<tr>
<td>Description</td>
<td>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.</td>
</tr>
</tbody>
</table>

Table 8-101  Description of the **Service Started** parameters used

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Option Path</td>
<td>System Symantec Software Monitor &gt; Symantec AntiVirus for Linux (SAVFL) Client Communication</td>
</tr>
<tr>
<td>Option</td>
<td>Service Started</td>
</tr>
<tr>
<td>Rule Name</td>
<td>Service_STARTED</td>
</tr>
<tr>
<td>Severity</td>
<td>Notice</td>
</tr>
<tr>
<td>Description</td>
<td>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.</td>
</tr>
</tbody>
</table>

Table 8-102  Description of the **Scan Started** parameters used

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Option Path</td>
<td>System Symantec Software Monitor &gt; Symantec AntiVirus for Linux (SAVFL) Client Communication</td>
</tr>
<tr>
<td>Option</td>
<td>Scan Started</td>
</tr>
<tr>
<td>Rule Name</td>
<td>Scan_STARTED</td>
</tr>
<tr>
<td>Severity</td>
<td>Notice</td>
</tr>
<tr>
<td>Description</td>
<td>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.</td>
</tr>
</tbody>
</table>
Table 8-103  Description of the **Scan Canceled** parameters used

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Option Path</td>
<td>System Symantec Software Monitor &gt; Symantec AntiVirus for Linux (SAVFL) Client Communication</td>
</tr>
<tr>
<td>Option</td>
<td>Scan Canceled</td>
</tr>
<tr>
<td>Rule Name</td>
<td>Scan_Canceled</td>
</tr>
<tr>
<td>Severity</td>
<td>Warning</td>
</tr>
<tr>
<td>Description</td>
<td>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.</td>
</tr>
</tbody>
</table>

Table 8-104  Description of the **Scan Complete** parameters used

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Option Path</td>
<td>System Symantec Software Monitor &gt; Symantec AntiVirus for Linux (SAVFL) Client Communication</td>
</tr>
<tr>
<td>Option</td>
<td>Scan Complete</td>
</tr>
<tr>
<td>Rule Name</td>
<td>Scan_Complete</td>
</tr>
<tr>
<td>Severity</td>
<td>Notice</td>
</tr>
<tr>
<td>Description</td>
<td>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.</td>
</tr>
</tbody>
</table>

Table 8-105  Description of the **New Virus Definition Loaded** parameters used

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Option Path</td>
<td>System Symantec Software Monitor &gt; Symantec AntiVirus for Linux (SAVFL) Client Communication</td>
</tr>
<tr>
<td>Option</td>
<td>New Virus Definition Loaded</td>
</tr>
<tr>
<td>Rule Name</td>
<td>New_Virus_Definition_Loaded</td>
</tr>
<tr>
<td>Severity</td>
<td>Notice</td>
</tr>
</tbody>
</table>
### Table 8-105  Description of the **New Virus Definition Loaded** parameters used

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Description</td>
<td>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.</td>
</tr>
</tbody>
</table>

### Table 8-106  Description of the **Virus Definitions are Current** parameters used

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Option Path</td>
<td>System Symantec Software Monitor &gt; Symantec AntiVirus for Linux (SAVFL) Client Communication</td>
</tr>
<tr>
<td>Option</td>
<td>Virus Definitions are Current</td>
</tr>
<tr>
<td>Rule Name</td>
<td>Virus_Definitions_are_Current</td>
</tr>
<tr>
<td>Severity</td>
<td>Notice</td>
</tr>
<tr>
<td>Description</td>
<td>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.</td>
</tr>
</tbody>
</table>

### Table 8-107  Description of the **Realtime Protection Loaded** parameters used

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Option Path</td>
<td>System Symantec Software Monitor &gt; Symantec AntiVirus for Linux (SAVFL) Client Communication</td>
</tr>
<tr>
<td>Option</td>
<td>Realtime Protection Loaded</td>
</tr>
<tr>
<td>Rule Name</td>
<td>Realtime_Protection_Loaded</td>
</tr>
<tr>
<td>Severity</td>
<td>Notice</td>
</tr>
<tr>
<td>Description</td>
<td>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.</td>
</tr>
</tbody>
</table>
### Table 8-108  Description of the **Realtime Protection Disabled** parameters used

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Option Path</td>
<td>System Symantec Software Monitor &gt; Symantec AntiVirus for Linux (SAVFL) Client Communication</td>
</tr>
<tr>
<td>Option</td>
<td>Realtime Protection Disabled</td>
</tr>
<tr>
<td>Rule Name</td>
<td>Realtime_Protection_Disabled</td>
</tr>
<tr>
<td>Severity</td>
<td>Critical</td>
</tr>
<tr>
<td>Description</td>
<td>Detects the disabiling 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.</td>
</tr>
</tbody>
</table>

### Table 8-109  Description of the **Virus Detected - Cleaned Failed** parameters used

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Option Path</td>
<td>System Symantec Software Monitor &gt; Symantec AntiVirus for Linux (SAVFL) Client Communication</td>
</tr>
<tr>
<td>Option</td>
<td>Virus Detected - Cleaned Failed</td>
</tr>
<tr>
<td>Rule Name</td>
<td>Virus_Detected_Cleaned_Failed</td>
</tr>
<tr>
<td>Severity</td>
<td>Critical</td>
</tr>
<tr>
<td>Description</td>
<td>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.</td>
</tr>
</tbody>
</table>

### 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.
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. DCS:SA 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>
<thead>
<tr>
<th>Table 8-113</th>
<th>Description of the <strong>Generic VA Scan Attempt</strong> parameters used</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Parameter</strong></td>
<td><strong>Description</strong></td>
</tr>
<tr>
<td>Option Path</td>
<td>System Attack Detection &gt; Web Attack Detection Options &gt; Generic Web Attack Detection Options</td>
</tr>
<tr>
<td>Option</td>
<td>Generic VA Scan Attempt</td>
</tr>
</tbody>
</table>
Table 8-113  Description of the **Generic VA Scan Attempt** parameters used (continued)

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Rule Name</td>
<td>WebAttackDetection_Generic_VAScan</td>
</tr>
<tr>
<td>Severity</td>
<td>Warning</td>
</tr>
<tr>
<td>Invalid Count</td>
<td>20 Times in which a 404 or unknown request is received.</td>
</tr>
<tr>
<td>Invalid Interval</td>
<td>2 minutes Time frequency in which invalid count needs to occur to trigger event.</td>
</tr>
<tr>
<td>Description</td>
<td>Detects a possible VA scan by triggering an event within a specific administrator-defined threshold. If DCS:SA 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.</td>
</tr>
</tbody>
</table>

Table 8-114  Description of the **Generic Blacklisted IP Request Attempts** parameters used

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Option Path</td>
<td>System Attack Detection &gt; Web Attack Detection Options &gt; Generic Web Attack Detection Options</td>
</tr>
<tr>
<td>Option</td>
<td>Generic Blacklisted IP Request Attempts</td>
</tr>
<tr>
<td>Rule Name</td>
<td>Baseline_WebAttackDetection_Generic_BlackListedIP</td>
</tr>
<tr>
<td>Severity</td>
<td>Warning</td>
</tr>
<tr>
<td>Description</td>
<td>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.</td>
</tr>
</tbody>
</table>

Table 8-115  Description of the **Generic SQL Injection Attack Attempts** parameters used

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Option Path</td>
<td>System Attack Detection &gt; Web Attack Detection Options &gt; Generic Web Attack Detection Options</td>
</tr>
<tr>
<td>Option</td>
<td>Generic SQL Injection Attack Attempts</td>
</tr>
</tbody>
</table>
### Table 8-115: Description of the **Generic SQL Injection Attack Attempts** parameters used (continued)

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Rule Name</td>
<td>Baseline_WebAttackDetection_Generic_SQLInjection</td>
</tr>
<tr>
<td>Severity</td>
<td>Warning</td>
</tr>
<tr>
<td>Description</td>
<td>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.</td>
</tr>
</tbody>
</table>

### Table 8-116: Description of the **Generic Directory Transversal Attempts** parameters used

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Option Path</td>
<td>System Attack Detection &gt; Web Attack Detection Options &gt; Generic Web Attack Detection Options</td>
</tr>
<tr>
<td>Option</td>
<td>Generic Directory Transversal Attempts</td>
</tr>
<tr>
<td>Rule Name</td>
<td>Baseline_WebAttackDetection_Generic_DirTransversal</td>
</tr>
<tr>
<td>Severity</td>
<td>Warning</td>
</tr>
<tr>
<td>Description</td>
<td>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.</td>
</tr>
</tbody>
</table>

### Table 8-117: Description of the **Generic Malicious User Agent Request Attempts** parameters used

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Option Path</td>
<td>System Attack Detection &gt; Web Attack Detection Options &gt; Generic Web Attack Detection Options</td>
</tr>
<tr>
<td>Option</td>
<td>Generic Malicious User Agent Request Attempts</td>
</tr>
<tr>
<td>Rule Name</td>
<td>Baseline_WebAttackDetection_Generic_MaliciousUserAgent</td>
</tr>
<tr>
<td>Severity</td>
<td>Warning</td>
</tr>
</tbody>
</table>
Table 8-117 Description of the **Generic Malicious User Agent Request Attempts** parameters used *(continued)*

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Description</td>
<td>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.</td>
</tr>
</tbody>
</table>

Table 8-118 Description of the **Generic Unwanted Extension Requests** parameters used

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Option Path</td>
<td>System Attack Detection &gt; Web Attack Detection Options &gt; Generic Web Attack Detection Options</td>
</tr>
<tr>
<td>Option</td>
<td>Generic Unwanted Extension Requests</td>
</tr>
<tr>
<td>Rule Name</td>
<td>Baseline_WebAttackDetection_Unwanted_Extension_Request</td>
</tr>
<tr>
<td>Severity</td>
<td>Warning</td>
</tr>
<tr>
<td>Description</td>
<td>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.</td>
</tr>
</tbody>
</table>

Table 8-119 Description of the **Generic Unwanted Directory Requests** parameters used

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Option Path</td>
<td>System Attack Detection &gt; Web Attack Detection Options &gt; Generic Web Attack Detection Options</td>
</tr>
<tr>
<td>Option</td>
<td>Generic Unwanted Directory Requests</td>
</tr>
<tr>
<td>Rule Name</td>
<td>Baseline_WebAttackDetection_Unwanted_Directory_Request</td>
</tr>
<tr>
<td>Severity</td>
<td>Warning</td>
</tr>
<tr>
<td>Description</td>
<td>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.</td>
</tr>
</tbody>
</table>
Table 8-120 Description of the **Generic Vulnerable CGI Requests** parameters used

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Option Path</td>
<td>System Attack Detection &gt; Web Attack Detection Options &gt; Generic Web Attack Detection Options</td>
</tr>
<tr>
<td>Option</td>
<td>Generic Vulnerable CGI Requests</td>
</tr>
<tr>
<td>Rule Name</td>
<td>WebAttackDetection_Generic_VulnerableCGIRequest</td>
</tr>
<tr>
<td>Severity</td>
<td>Warning</td>
</tr>
<tr>
<td>Description</td>
<td>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.</td>
</tr>
</tbody>
</table>

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 DCS:SA 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 DCS:SA was last shut down. This option provides detection ability even if the DCS:SA service or daemon is shut down. If a monitored file is changed, once the DCS:SA 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 8-121 Description of the **Bash Door** parameters used

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Option Path</td>
<td>System Attack Detection &gt; UNIX Rootkit File / Directory Detection</td>
</tr>
</tbody>
</table>
### Table 8-121  Description of the **Bash Door** parameters used (continued)

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Option</td>
<td>Bash Door</td>
</tr>
<tr>
<td>Rule Name</td>
<td>Rootkit_Detection_BashDoor</td>
</tr>
<tr>
<td>Severity</td>
<td>Critical</td>
</tr>
<tr>
<td>Monitor Paths</td>
<td>/tmp/mcliZokhb</td>
</tr>
<tr>
<td></td>
<td>/tmp/mclzaKmfa</td>
</tr>
<tr>
<td>Description</td>
<td>Detects rootkit activity.</td>
</tr>
</tbody>
</table>

### Table 8-122  Description of the **VOLC Rootkit** parameters used

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Option Path</td>
<td>System Attack Detection &gt; UNIX Rootkit File / Directory Detection</td>
</tr>
<tr>
<td>Option</td>
<td>VOLC Rootkit</td>
</tr>
<tr>
<td>Rule Name</td>
<td>Rootkit_Detection_VOLC</td>
</tr>
<tr>
<td>Severity</td>
<td>Critical</td>
</tr>
<tr>
<td>Monitor Paths</td>
<td>/usr/lib/volc</td>
</tr>
<tr>
<td>Description</td>
<td>Detects rootkit activity.</td>
</tr>
</tbody>
</table>

### Table 8-123  Description of the **Illogic Rootkit** parameters used

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Option Path</td>
<td>System Attack Detection &gt; UNIX Rootkit File / Directory Detection</td>
</tr>
<tr>
<td>Option</td>
<td>Illogic Rootkit</td>
</tr>
<tr>
<td>Rule Name</td>
<td>Rootkit_Detection_Illogic</td>
</tr>
<tr>
<td>Severity</td>
<td>Critical</td>
</tr>
<tr>
<td>Monitor Paths</td>
<td>/etc/ld.so.hash</td>
</tr>
<tr>
<td></td>
<td>/lib/security/.config</td>
</tr>
<tr>
<td></td>
<td>/usr/bin/sia</td>
</tr>
<tr>
<td>Description</td>
<td>Detects rootkit activity.</td>
</tr>
</tbody>
</table>
Table 8-124: Description of the **T0rn Rootkit** parameters used

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Option Path</td>
<td>System Attack Detection &gt; UNIX Rootkit File / Directory Detection</td>
</tr>
<tr>
<td>Option</td>
<td>T0rn Rootkit</td>
</tr>
<tr>
<td>Rule Name</td>
<td>Rootkit_Detection_T0rn</td>
</tr>
<tr>
<td>Severity</td>
<td>Critical</td>
</tr>
<tr>
<td>Monitor Paths</td>
<td>/etc/ttyhash</td>
</tr>
<tr>
<td></td>
<td>/lib/ldlib.tk</td>
</tr>
<tr>
<td></td>
<td>/sbin/xlogin</td>
</tr>
<tr>
<td></td>
<td>/usr/info/.T0rn</td>
</tr>
<tr>
<td></td>
<td>/usr/src/.puta</td>
</tr>
<tr>
<td></td>
<td>/var/run/...dica</td>
</tr>
<tr>
<td>Description</td>
<td>Detects rootkit activity.</td>
</tr>
</tbody>
</table>

Table 8-125: Description of the **RK17 Rootkit** parameters used

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Option Path</td>
<td>System Attack Detection &gt; UNIX Rootkit File / Directory Detection</td>
</tr>
<tr>
<td>Option</td>
<td>RK17 Rootkit</td>
</tr>
<tr>
<td>Rule Name</td>
<td>Rootkit_Detection_RK17</td>
</tr>
<tr>
<td>Severity</td>
<td>Critical</td>
</tr>
<tr>
<td>Monitor Paths</td>
<td>/bin/rtty</td>
</tr>
<tr>
<td></td>
<td>/bin/squit</td>
</tr>
<tr>
<td></td>
<td>/sbin/pback</td>
</tr>
<tr>
<td></td>
<td>/usr/src/linux/modules/autod.o</td>
</tr>
<tr>
<td></td>
<td>/usr/src/linux/modules/soundx.o</td>
</tr>
<tr>
<td>Description</td>
<td>Detects rootkit activity.</td>
</tr>
</tbody>
</table>

Table 8-126: Description of the **RSHA Rootkit** parameters used

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Option Path</td>
<td>System Attack Detection &gt; UNIX Rootkit File / Directory Detection</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Option</td>
<td>RSHA Rootkit</td>
</tr>
<tr>
<td>Rule Name</td>
<td>Rootkit_Detection_RSHA</td>
</tr>
<tr>
<td>Severity</td>
<td>Critical</td>
</tr>
<tr>
<td>Monitor Paths</td>
<td>/etc/rc.d/arch/alpha/lib/.lib/*</td>
</tr>
<tr>
<td></td>
<td>/etc/rc.d/rsha/*</td>
</tr>
<tr>
<td></td>
<td>/usr/bin/chsh2</td>
</tr>
<tr>
<td></td>
<td>/usr/bin/kr4p</td>
</tr>
<tr>
<td></td>
<td>/usr/bin/n3tstat</td>
</tr>
<tr>
<td></td>
<td>/usr/bin/slice2</td>
</tr>
<tr>
<td>Description</td>
<td>Detects rootkit activity.</td>
</tr>
</tbody>
</table>

**Table 8-127** Description of the **RH-Sharpe Rootkit** parameters used

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Option Path</td>
<td>System Attack Detection &gt; UNIX Rootkit File / Directory Detection</td>
</tr>
<tr>
<td>Option</td>
<td>RH-Sharpe Rootkit</td>
</tr>
<tr>
<td>Rule Name</td>
<td>Rootkit_Detection_RHSharpe</td>
</tr>
<tr>
<td>Severity</td>
<td>Critical</td>
</tr>
</tbody>
</table>
### Table 8-127  Description of the RH-Sharpe Rootkit parameters used (continued)

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Monitor Paths</td>
<td>/bin/.lpstree</td>
</tr>
<tr>
<td></td>
<td>/bin/.ps</td>
</tr>
<tr>
<td></td>
<td>/bin/ldu</td>
</tr>
<tr>
<td></td>
<td>/bin/lkillall</td>
</tr>
<tr>
<td></td>
<td>/bin/inetstat</td>
</tr>
<tr>
<td></td>
<td>/usr/bin/.lpstree</td>
</tr>
<tr>
<td></td>
<td>/usr/bin/.ps</td>
</tr>
<tr>
<td></td>
<td>/usr/bin/cleaner</td>
</tr>
<tr>
<td></td>
<td>/usr/bin/ldu</td>
</tr>
<tr>
<td></td>
<td>/usr/bin/lkillall</td>
</tr>
<tr>
<td></td>
<td>/usr/bin/inetstat</td>
</tr>
<tr>
<td></td>
<td>/usr/bin/slice</td>
</tr>
<tr>
<td></td>
<td>/usr/bin/vadim</td>
</tr>
</tbody>
</table>

Description: Detects rootkit activity.

### Table 8-128  Description of the Showtee Romanian Rootkit parameters used

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Option Path</td>
<td>System Attack Detection &gt; UNIX Rootkit File / Directory Detection</td>
</tr>
<tr>
<td>Option</td>
<td>Showtee Romanian Rootkit</td>
</tr>
<tr>
<td>Rule Name</td>
<td>Rootkit_Detection_Showteeromaniam</td>
</tr>
<tr>
<td>Severity</td>
<td>Critical</td>
</tr>
<tr>
<td>Monitor Paths</td>
<td>/usr/lib/.egcs</td>
</tr>
<tr>
<td></td>
<td>/usr/lib/.kinetic</td>
</tr>
<tr>
<td></td>
<td>/usr/lib/.wormie</td>
</tr>
<tr>
<td></td>
<td>/usr/lib/libfl.so</td>
</tr>
<tr>
<td></td>
<td>/usr/lib/libfl.so</td>
</tr>
<tr>
<td></td>
<td>/usr/sbin/xntps</td>
</tr>
</tbody>
</table>

Description: Detects rootkit activity.
### Table 8-129  Description of the **Optickit Rootkit** parameters used

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Option Path</td>
<td>System Attack Detection &gt; UNIX Rootkit File / Directory Detection</td>
</tr>
<tr>
<td>Option</td>
<td>Optickit Rootkit</td>
</tr>
<tr>
<td>Rule Name</td>
<td>Rootkit_Detection_Optickit</td>
</tr>
<tr>
<td>Severity</td>
<td>Critical</td>
</tr>
</tbody>
</table>
| Monitor Paths | /usr/bin/xchk  
                 /usr/bin/xsf |
| Description | Detects rootkit activity. |

### Table 8-130  Description of the **Tele Rootkit** parameters used

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Option Path</td>
<td>System Attack Detection &gt; UNIX Rootkit File / Directory Detection</td>
</tr>
<tr>
<td>Option</td>
<td>Tele Rootkit</td>
</tr>
<tr>
<td>Rule Name</td>
<td>Rootkit_Detection_Telekit</td>
</tr>
<tr>
<td>Severity</td>
<td>Critical</td>
</tr>
</tbody>
</table>
| Monitor Paths | /dev/hda06  
                 /usr/info/libc1.so |
| Description | Detects rootkit activity. |

### Table 8-131  Description of the **LRK Rootkit** parameters used

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Option Path</td>
<td>System Attack Detection &gt; UNIX Rootkit File / Directory Detection</td>
</tr>
<tr>
<td>Option</td>
<td>LRK Rootkit</td>
</tr>
<tr>
<td>Rule Name</td>
<td>Rootkit_Detection_LRK</td>
</tr>
<tr>
<td>Severity</td>
<td>Critical</td>
</tr>
</tbody>
</table>
| Monitor Paths | /dev/ida/.inet  
                 /usr/lib/liblog.o |
| Description | Detects rootkit activity. |
### Table 8-132 Description of the ADORE Rootkit parameters used

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Option Path</td>
<td>System Attack Detection &gt; UNIX Rootkit File / Directory Detection</td>
</tr>
<tr>
<td>Option</td>
<td>ADORE Rootkit</td>
</tr>
<tr>
<td>Rule Name</td>
<td>Rootkit_Detection_Adore</td>
</tr>
<tr>
<td>Severity</td>
<td>Critical</td>
</tr>
<tr>
<td>Monitor Paths</td>
<td>/etc/bin/ava</td>
</tr>
<tr>
<td></td>
<td>/etc/sbin/ava</td>
</tr>
<tr>
<td>Description</td>
<td>Detects rootkit activity.</td>
</tr>
</tbody>
</table>

### Table 8-133 Description of the KNARK Rootkit parameters used

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Option Path</td>
<td>System Attack Detection &gt; UNIX Rootkit File / Directory Detection</td>
</tr>
<tr>
<td>Option</td>
<td>KNARK Rootkit</td>
</tr>
<tr>
<td>Rule Name</td>
<td>Rootkit_Detection_Knark</td>
</tr>
<tr>
<td>Severity</td>
<td>Critical</td>
</tr>
<tr>
<td>Monitor Paths</td>
<td>/dev/.pizda</td>
</tr>
<tr>
<td></td>
<td>/dev/.pula</td>
</tr>
<tr>
<td></td>
<td>/proc/knark</td>
</tr>
<tr>
<td>Description</td>
<td>Detects rootkit activity.</td>
</tr>
</tbody>
</table>

### Table 8-134 Description of the BOBkit Rootkit parameters used

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Option Path</td>
<td>System Attack Detection &gt; UNIX Rootkit File / Directory Detection</td>
</tr>
<tr>
<td>Option</td>
<td>BOBkit Rootkit</td>
</tr>
<tr>
<td>Rule Name</td>
<td>Rootkit_Detection_Boobkit</td>
</tr>
<tr>
<td>Severity</td>
<td>Critical</td>
</tr>
</tbody>
</table>
### Table 8-134
Description of the **BOBkit Rootkit** parameters used *(continued)*

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Monitor Paths</td>
<td>/tmp/.bkp/*</td>
</tr>
<tr>
<td></td>
<td>/usr/include/.../*</td>
</tr>
<tr>
<td></td>
<td>/usr/lib/.../*</td>
</tr>
<tr>
<td></td>
<td>/usr/lib/.bkit-*</td>
</tr>
</tbody>
</table>

Description: Detects rootkit activity.

### Table 8-135
Description of the **HID Rootkit** parameters used

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Option Path</td>
<td>System Attack Detection &gt; UNIX Rootkit File / Directory Detection</td>
</tr>
<tr>
<td>Option</td>
<td>HID Rootkit</td>
</tr>
<tr>
<td>Rule Name</td>
<td>Rootkit_Detection_Hid</td>
</tr>
<tr>
<td>Severity</td>
<td>Critical</td>
</tr>
<tr>
<td>Monitor Paths</td>
<td>/var/lib/games/.k</td>
</tr>
</tbody>
</table>

Description: Detects rootkit activity.

### Table 8-136
Description of the **ARK Rootkit** parameters used

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Option Path</td>
<td>System Attack Detection &gt; UNIX Rootkit File / Directory Detection</td>
</tr>
<tr>
<td>Option</td>
<td>ARK Rootkit</td>
</tr>
<tr>
<td>Rule Name</td>
<td>Rootkit_Detection_ARK</td>
</tr>
<tr>
<td>Severity</td>
<td>Critical</td>
</tr>
<tr>
<td>Monitor Paths</td>
<td>/dev/ptyxx /usr/lib/.ark?</td>
</tr>
</tbody>
</table>

Description: Detects rootkit activity.
Table 8-137  Description of the **Mithra Rootkit** parameters used

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Option Path</td>
<td>System Attack Detection &gt; UNIX Rootkit File / Directory Detection</td>
</tr>
<tr>
<td>Option</td>
<td>Mithra Rootkit</td>
</tr>
<tr>
<td>Rule Name</td>
<td>Rootkit_Detection_Mithra</td>
</tr>
<tr>
<td>Severity</td>
<td>Critical</td>
</tr>
<tr>
<td>Monitor Paths</td>
<td>/usr/sbin/uboot</td>
</tr>
<tr>
<td>Description</td>
<td>Detects rootkit activity.</td>
</tr>
</tbody>
</table>

Table 8-138  Description of the **LOC Rootkit** parameters used

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Option Path</td>
<td>System Attack Detection &gt; UNIX Rootkit File / Directory Detection</td>
</tr>
<tr>
<td>Option</td>
<td>LOC Rootkit</td>
</tr>
<tr>
<td>Rule Name</td>
<td>Rootkit_Detection_LOC</td>
</tr>
<tr>
<td>Severity</td>
<td>Critical</td>
</tr>
<tr>
<td>Monitor Paths</td>
<td>/tmp/kidd0</td>
</tr>
<tr>
<td></td>
<td>/tmp/kidd0.c</td>
</tr>
<tr>
<td></td>
<td>/tmp/xp</td>
</tr>
<tr>
<td></td>
<td>/usr/lib/libmen.oo/.LJK2</td>
</tr>
<tr>
<td>Description</td>
<td>Detects rootkit activity.</td>
</tr>
</tbody>
</table>

Table 8-139  Description of the **Anonoiyng Rootkit** parameters used

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Option Path</td>
<td>System Attack Detection &gt; UNIX Rootkit File / Directory Detection</td>
</tr>
<tr>
<td>Option</td>
<td>Anonoiyng Rootkit</td>
</tr>
<tr>
<td>Rule Name</td>
<td>Rootkit_Detection_Anonoiyng</td>
</tr>
<tr>
<td>Severity</td>
<td>Critical</td>
</tr>
<tr>
<td>Monitor Paths</td>
<td>/usr/sbin/kswapd</td>
</tr>
<tr>
<td></td>
<td>/usr/sbin/mech</td>
</tr>
<tr>
<td>Description</td>
<td></td>
</tr>
</tbody>
</table>
### Table 8-139  Description of the **Anonoiyng Rootkit** parameters used (continued)

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Description</td>
<td>Detects rootkit activity.</td>
</tr>
</tbody>
</table>

### Table 8-140  Description of the **ZK Rootkit** parameters used

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Option Path</td>
<td>System Attack Detection &gt; UNIX Rootkit File / Directory Detection</td>
</tr>
<tr>
<td>Option</td>
<td>ZK Rootkit</td>
</tr>
<tr>
<td>Rule Name</td>
<td>Rootkit_Detection_ZK</td>
</tr>
<tr>
<td>Severity</td>
<td>Critical</td>
</tr>
<tr>
<td>Monitor Paths</td>
<td>/etc/sysconfig/console/load.zk</td>
</tr>
<tr>
<td>Description</td>
<td>Detects rootkit activity.</td>
</tr>
</tbody>
</table>

### Table 8-141  Description of the **S-it Rootkit** parameters used

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Option Path</td>
<td>System Attack Detection &gt; UNIX Rootkit File / Directory Detection</td>
</tr>
<tr>
<td>Option</td>
<td>S-it Rootkit</td>
</tr>
<tr>
<td>Rule Name</td>
<td>Rootkit_Detection_Sit</td>
</tr>
<tr>
<td>Severity</td>
<td>Critical</td>
</tr>
<tr>
<td>Monitor Paths</td>
<td>/dev/sdhu0/tehdrakg/*</td>
</tr>
<tr>
<td></td>
<td>/etc/rc.d/rc?.d/S23kmdac</td>
</tr>
<tr>
<td></td>
<td>/lib/.x</td>
</tr>
<tr>
<td></td>
<td>/lib/sk</td>
</tr>
<tr>
<td>Description</td>
<td>Detects rootkit activity.</td>
</tr>
</tbody>
</table>

### Table 8-142  Description of the **F-it Rootkit** parameters used

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Option Path</td>
<td>System Attack Detection &gt; UNIX Rootkit File / Directory Detection</td>
</tr>
<tr>
<td>Option</td>
<td>F-it Rootkit</td>
</tr>
</tbody>
</table>
### Table 8-142  Description of the **F-it Rootkit** parameters used (continued)

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Rule Name</td>
<td>Rootkit_Detection_Fit</td>
</tr>
<tr>
<td>Severity</td>
<td>Critical</td>
</tr>
<tr>
<td>Monitor Paths</td>
<td>/dev/proc/fuckit/*</td>
</tr>
<tr>
<td></td>
<td>/dev/proc/system-bins/init</td>
</tr>
<tr>
<td>Description</td>
<td>Detects rootkit activity.</td>
</tr>
</tbody>
</table>

### Table 8-143  Description of the **Beastkit Rootkit** parameters used

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Option Path</td>
<td>System Attack Detection &gt; UNIX Rootkit File / Directory Detection</td>
</tr>
<tr>
<td>Option</td>
<td>Beastkit Rootkit</td>
</tr>
<tr>
<td>Rule Name</td>
<td>Rootkit_Detection_Beastkit</td>
</tr>
<tr>
<td>Severity</td>
<td>Critical</td>
</tr>
<tr>
<td>Monitor Paths</td>
<td>/lib/ldd.so/bktools</td>
</tr>
<tr>
<td></td>
<td>/usr/l/bin/idrun</td>
</tr>
<tr>
<td></td>
<td>/usr/local/bin/.../bktd</td>
</tr>
<tr>
<td></td>
<td>/usr/sbin/arobia/*</td>
</tr>
<tr>
<td>Description</td>
<td>Detects rootkit activity.</td>
</tr>
</tbody>
</table>

### Table 8-144  Description of the **Tuxkit Rootkit** parameters used

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Option Path</td>
<td>System Attack Detection &gt; UNIX Rootkit File / Directory Detection</td>
</tr>
<tr>
<td>Option</td>
<td>Tuxkit Rootkit</td>
</tr>
<tr>
<td>Rule Name</td>
<td>Rootkit_Detection_Tuxkit</td>
</tr>
<tr>
<td>Severity</td>
<td>Critical</td>
</tr>
<tr>
<td>Monitor Paths</td>
<td>/dev/tux</td>
</tr>
<tr>
<td>Description</td>
<td>Detects rootkit activity.</td>
</tr>
</tbody>
</table>
### Table 8-145  Description of the **Kenga3 Rootkit** parameters used

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Option Path</td>
<td>System Attack Detection &gt; UNIX Rootkit File / Directory Detection</td>
</tr>
<tr>
<td>Option</td>
<td>Kenga3 Rootkit</td>
</tr>
<tr>
<td>Rule Name</td>
<td>Rootkit_Detection_Kenga3</td>
</tr>
<tr>
<td>Severity</td>
<td>Critical</td>
</tr>
<tr>
<td>Monitor Paths</td>
<td>/usr/include/..</td>
</tr>
<tr>
<td>Description</td>
<td>Detects rootkit activity.</td>
</tr>
</tbody>
</table>

### Table 8-146  Description of the **ESRK Rootkit** parameters used

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Option Path</td>
<td>System Attack Detection &gt; UNIX Rootkit File / Directory Detection</td>
</tr>
<tr>
<td>Option</td>
<td>ESRK Rootkit</td>
</tr>
<tr>
<td>Rule Name</td>
<td>Rootkit_Detection_ESRK</td>
</tr>
<tr>
<td>Severity</td>
<td>Critical</td>
</tr>
<tr>
<td>Monitor Paths</td>
<td>/usr/lib/tcl5.3</td>
</tr>
<tr>
<td>Description</td>
<td>Detects rootkit activity.</td>
</tr>
</tbody>
</table>

### Table 8-147  Description of the **FU Rootkit** parameters used

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Option Path</td>
<td>System Attack Detection &gt; UNIX Rootkit File / Directory Detection</td>
</tr>
<tr>
<td>Option</td>
<td>FU Rootkit</td>
</tr>
<tr>
<td>Rule Name</td>
<td>Rootkit_Detection_FU</td>
</tr>
<tr>
<td>Severity</td>
<td>Critical</td>
</tr>
<tr>
<td>Monitor Paths</td>
<td>/sbin/xc</td>
</tr>
<tr>
<td></td>
<td>/usr/include/ivtype.h</td>
</tr>
<tr>
<td>Description</td>
<td>Detects rootkit activity.</td>
</tr>
</tbody>
</table>
### Table 8-148  
**Description of the SHKit Rootkit parameters used**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Option Path</td>
<td>System Attack Detection &gt; UNIX Rootkit File / Directory Detection</td>
</tr>
<tr>
<td>Option</td>
<td>SHKit Rootkit</td>
</tr>
<tr>
<td>Rule Name</td>
<td>Rootkit_Detection_Shkit</td>
</tr>
<tr>
<td>Severity</td>
<td>Critical</td>
</tr>
</tbody>
</table>
| Monitor Paths | /etc/ld.so.hash  
                | /lib/security/.config                               |
| Description | Detects rootkit activity.                             |

### Table 8-149  
**Description of the Ajakit Rootkit parameters used**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Option Path</td>
<td>System Attack Detection &gt; UNIX Rootkit File / Directory Detection</td>
</tr>
<tr>
<td>Option</td>
<td>Ajakit Rootkit</td>
</tr>
<tr>
<td>Rule Name</td>
<td>Rootkit_Detection_Ajakit</td>
</tr>
<tr>
<td>Severity</td>
<td>Critical</td>
</tr>
<tr>
<td>Monitor Paths</td>
<td>/lib/.libgh-gh</td>
</tr>
<tr>
<td>Description</td>
<td>Detects rootkit activity.</td>
</tr>
</tbody>
</table>

### Table 8-150  
**Description of the zaRwT Rootkit parameters used**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Option Path</td>
<td>System Attack Detection &gt; UNIX Rootkit File / Directory Detection</td>
</tr>
<tr>
<td>Option</td>
<td>zaRwT Rootkit</td>
</tr>
<tr>
<td>Rule Name</td>
<td>Rootkit_Detection_zarwt</td>
</tr>
<tr>
<td>Severity</td>
<td>Critical</td>
</tr>
</tbody>
</table>
| Monitor Paths | /bin/imin  
                | /bin/imout                                            |
| Description | Detects rootkit activity.                             |
### Table 8-151 Description of the Madalin Rootkit parameters used

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Option Path</td>
<td>System Attack Detection &gt; UNIX Rootkit File / Directory Detection</td>
</tr>
<tr>
<td>Option</td>
<td>Madalin Rootkit</td>
</tr>
<tr>
<td>Rule Name</td>
<td>Rootkit_Detection_Madalin</td>
</tr>
<tr>
<td>Severity</td>
<td>Critical</td>
</tr>
<tr>
<td>Monitor Paths</td>
<td>/usr/include/iceconf.h</td>
</tr>
<tr>
<td></td>
<td>/usr/include/icekey.h</td>
</tr>
<tr>
<td></td>
<td>/usr/include/iceseed.h</td>
</tr>
<tr>
<td>Description</td>
<td>Detects rootkit activity.</td>
</tr>
</tbody>
</table>

### Table 8-152 Description of the BMBL Rootkit parameters used

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Option Path</td>
<td>System Attack Detection &gt; UNIX Rootkit File / Directory Detection</td>
</tr>
<tr>
<td>Option</td>
<td>BMBL Rootkit</td>
</tr>
<tr>
<td>Rule Name</td>
<td>Rootkit_Detection_BMBL</td>
</tr>
<tr>
<td>Severity</td>
<td>Critical</td>
</tr>
<tr>
<td>Monitor Paths</td>
<td>/etc/.bmbl</td>
</tr>
<tr>
<td></td>
<td>/etc/.bmbl/sk</td>
</tr>
<tr>
<td>Description</td>
<td>Detects rootkit activity.</td>
</tr>
</tbody>
</table>

### Table 8-153 Description of the aPa Rootkit parameters used

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Option Path</td>
<td>System Attack Detection &gt; UNIX Rootkit File / Directory Detection</td>
</tr>
<tr>
<td>Option</td>
<td>aPa Rootkit</td>
</tr>
<tr>
<td>Rule Name</td>
<td>Rootkit_Detection_aPa</td>
</tr>
<tr>
<td>Severity</td>
<td>Critical</td>
</tr>
<tr>
<td>Monitor Paths</td>
<td>/usr/share/.aPa</td>
</tr>
<tr>
<td>Description</td>
<td>Detects rootkit activity.</td>
</tr>
<tr>
<td>Parameter</td>
<td>Description</td>
</tr>
<tr>
<td>----------------------------</td>
<td>----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Option Path</td>
<td>System Attack Detection &gt; UNIX Rootkit File / Directory Detection</td>
</tr>
<tr>
<td>Option</td>
<td>Enye-Sec Rootkit</td>
</tr>
<tr>
<td>Rule Name</td>
<td>Rootkit_Detection_EnyeSec</td>
</tr>
<tr>
<td>Severity</td>
<td>Critical</td>
</tr>
<tr>
<td>Monitor Paths</td>
<td>/etc/.enyelkmHIDE^IT.ko</td>
</tr>
<tr>
<td>Description</td>
<td>Detects rootkit activity.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Option Path</td>
<td>System Attack Detection &gt; UNIX Rootkit File / Directory Detection</td>
</tr>
<tr>
<td>Option</td>
<td>Override Rootkit</td>
</tr>
<tr>
<td>Rule Name</td>
<td>Rootkit_Detection_OVERRIDE</td>
</tr>
<tr>
<td>Severity</td>
<td>Critical</td>
</tr>
<tr>
<td>Monitor Paths</td>
<td>/dev/grid-hide-pid-</td>
</tr>
<tr>
<td></td>
<td>/dev/grid-hide-port-</td>
</tr>
<tr>
<td></td>
<td>/dev/grid-show-pids</td>
</tr>
<tr>
<td></td>
<td>/dev/grid-show-port-</td>
</tr>
<tr>
<td></td>
<td>/dev/grid-unhide-pid-</td>
</tr>
<tr>
<td>Description</td>
<td>Detects rootkit activity.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Option Path</td>
<td>System Attack Detection &gt; UNIX Rootkit File / Directory Detection</td>
</tr>
<tr>
<td>Option</td>
<td>PHALANX Rootkit</td>
</tr>
<tr>
<td>Rule Name</td>
<td>Rootkit_Detection_PHALANX</td>
</tr>
<tr>
<td>Severity</td>
<td>Critical</td>
</tr>
</tbody>
</table>
Table 8-156  Description of the **PHALANX Rootkit** parameters used *(continued)*

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Monitor Paths</td>
<td>/bin/host.ph1</td>
</tr>
<tr>
<td></td>
<td>/etc/host.ph1</td>
</tr>
<tr>
<td></td>
<td>/usr/share/.home/ph1</td>
</tr>
<tr>
<td>Description</td>
<td>Detects rootkit activity.</td>
</tr>
</tbody>
</table>

Table 8-157  Description of the **Monkit Rootkit** parameters used

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Option Path</td>
<td>System Attack Detection &gt; UNIX Rootkit File / Directory Detection</td>
</tr>
<tr>
<td>Option</td>
<td>Monkit Rootkit</td>
</tr>
<tr>
<td>Rule Name</td>
<td>Rootkit_Detection_Monkit</td>
</tr>
<tr>
<td>Severity</td>
<td>Critical</td>
</tr>
<tr>
<td>Monitor Paths</td>
<td>/lib/defs</td>
</tr>
<tr>
<td></td>
<td>/usr/lib/libpikapp.a</td>
</tr>
<tr>
<td>Description</td>
<td>Detects rootkit activity.</td>
</tr>
</tbody>
</table>

Table 8-158  Description of the **Balaur Rootkit** parameters used

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Option Path</td>
<td>System Attack Detection &gt; UNIX Rootkit File / Directory Detection</td>
</tr>
<tr>
<td>Option</td>
<td>Balaur Rootkit</td>
</tr>
<tr>
<td>Rule Name</td>
<td>Rootkit_Detection_Balaur</td>
</tr>
<tr>
<td>Severity</td>
<td>Critical</td>
</tr>
<tr>
<td>Monitor Paths</td>
<td>/usr/lib/.egcs</td>
</tr>
<tr>
<td></td>
<td>/usr/lib/.kinetic</td>
</tr>
<tr>
<td></td>
<td>/usr/lib/.wormie</td>
</tr>
<tr>
<td>Description</td>
<td>Detects rootkit activity.</td>
</tr>
</tbody>
</table>
### Table 8-159  Description of the **Bex2 Rootkit** parameters used

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Option Path</td>
<td>System Attack Detection &gt; UNIX Rootkit File / Directory Detection</td>
</tr>
<tr>
<td>Option</td>
<td>Bex2 Rootkit</td>
</tr>
<tr>
<td>Rule Name</td>
<td>Rootkit_Detection_Bex2</td>
</tr>
<tr>
<td>Severity</td>
<td>Critical</td>
</tr>
<tr>
<td>Monitor Paths</td>
<td>/usr/include/bex</td>
</tr>
<tr>
<td>Description</td>
<td>Detects rootkit activity.</td>
</tr>
</tbody>
</table>

### Table 8-160  Description of the **Dreams Rootkit** parameters used

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Option Path</td>
<td>System Attack Detection &gt; UNIX Rootkit File / Directory Detection</td>
</tr>
<tr>
<td>Option</td>
<td>Dreams Rootkit</td>
</tr>
<tr>
<td>Rule Name</td>
<td>Rootkit_Detection_Dreams</td>
</tr>
<tr>
<td>Severity</td>
<td>Critical</td>
</tr>
<tr>
<td>Monitor Paths</td>
<td>/dev/ida/.hpd</td>
</tr>
<tr>
<td></td>
<td>/dev/ttyoa</td>
</tr>
<tr>
<td></td>
<td>/dev/ttyof</td>
</tr>
<tr>
<td></td>
<td>/dev/ttyop</td>
</tr>
<tr>
<td></td>
<td>/usr/bin/logclear</td>
</tr>
<tr>
<td></td>
<td>/usr/bin/sense</td>
</tr>
<tr>
<td></td>
<td>/usr/bin/sl2</td>
</tr>
<tr>
<td></td>
<td>/usr/lib/libsss</td>
</tr>
<tr>
<td>Description</td>
<td>Detects rootkit activity.</td>
</tr>
</tbody>
</table>

### Table 8-161  Description of the **HJC Rootkit** parameters used

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Option Path</td>
<td>System Attack Detection &gt; UNIX Rootkit File / Directory Detection</td>
</tr>
<tr>
<td>Option</td>
<td>HJC Rootkit</td>
</tr>
</tbody>
</table>


**Table 8-161** Description of the **HJC Rootkit** parameters used  

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Rule Name</td>
<td>Rootkit_Detection_hjc</td>
</tr>
<tr>
<td>Severity</td>
<td>Critical</td>
</tr>
<tr>
<td>Monitor Paths</td>
<td>/dev/hijackerz</td>
</tr>
<tr>
<td>Description</td>
<td>Detects rootkit activity.</td>
</tr>
</tbody>
</table>

**Table 8-162** Description of the **Duarawkz Rootkit** parameters used  

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Option Path</td>
<td>System Attack Detection &gt; UNIX Rootkit File / Directory Detection</td>
</tr>
<tr>
<td>Option</td>
<td>Duarawkz Rootkit</td>
</tr>
<tr>
<td>Rule Name</td>
<td>Rootkit_Detection_Duarawkz</td>
</tr>
<tr>
<td>Severity</td>
<td>Critical</td>
</tr>
<tr>
<td>Monitor Paths</td>
<td>/usr/bin/duarawkz</td>
</tr>
<tr>
<td>Description</td>
<td>Detects rootkit activity.</td>
</tr>
</tbody>
</table>

**Table 8-163** Description of the **Oz Rootkit** parameters used  

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Option Path</td>
<td>System Attack Detection &gt; UNIX Rootkit File / Directory Detection</td>
</tr>
<tr>
<td>Option</td>
<td>Oz Rootkit</td>
</tr>
<tr>
<td>Rule Name</td>
<td>Rootkit_Detection_Oz</td>
</tr>
<tr>
<td>Severity</td>
<td>Critical</td>
</tr>
<tr>
<td>Monitor Paths</td>
<td>/dev/.oz/.nap/rkit/terror</td>
</tr>
<tr>
<td>Description</td>
<td>Detects rootkit activity.</td>
</tr>
</tbody>
</table>

**Table 8-164** Description of the **Portacelo Rootkit** parameters used  

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Option Path</td>
<td>System Attack Detection &gt; UNIX Rootkit File / Directory Detection</td>
</tr>
<tr>
<td>Option</td>
<td>Portacelo Rootkit</td>
</tr>
</tbody>
</table>
**Table 8-164**  Description of the **Portacelo Rootkit** parameters used *(continued)*

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Rule Name</td>
<td>Rootkit_Detection_Portacelo</td>
</tr>
<tr>
<td>Severity</td>
<td>Critical</td>
</tr>
<tr>
<td>Monitor Paths</td>
<td>/var/lib/.../.ak /var/lib/.../.getty /var/lib/.../.hk /var/lib/.../.p /var/lib/.../.rs /var/lib/.../sssh_known_hosts</td>
</tr>
<tr>
<td>Description</td>
<td>Detects rootkit activity.</td>
</tr>
</tbody>
</table>

**Table 8-165**  Description of the **Slapper Bot Rootkit** parameters used

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Option Path</td>
<td>System Attack Detection &gt; UNIX Rootkit File / Directory Detection</td>
</tr>
<tr>
<td>Option</td>
<td>Slapper Bot Rootkit</td>
</tr>
<tr>
<td>Rule Name</td>
<td>Rootkit_Detection_SlapperBot</td>
</tr>
<tr>
<td>Severity</td>
<td>Critical</td>
</tr>
<tr>
<td>Monitor Paths</td>
<td>/tmp/.b /tmp/.cinik /tmp/.font-unix-cinik</td>
</tr>
<tr>
<td>Description</td>
<td>Detects rootkit activity.</td>
</tr>
</tbody>
</table>

**Table 8-166**  Description of the **Scalper Bot Rootkit** parameters used

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Option Path</td>
<td>System Attack Detection &gt; UNIX Rootkit File / Directory Detection</td>
</tr>
<tr>
<td>Option</td>
<td>Scalper Bot Rootkit</td>
</tr>
<tr>
<td>Rule Name</td>
<td>Rootkit_Detection_ScalperBot</td>
</tr>
<tr>
<td>Severity</td>
<td>Critical</td>
</tr>
</tbody>
</table>
### Table 8-166  Description of the **Scalper Bot Rootkit** parameters used (continued)

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
</table>
| Monitor Paths | /tmp/.a  
|              | /tmp/.uua |
| Description | Detects rootkit activity. |

### Table 8-167  Description of the **Flea Rootkit** parameters used

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Option Path</td>
<td>System Attack Detection &gt; UNIX Rootkit File / Directory Detection</td>
</tr>
<tr>
<td>Option</td>
<td>Flea Rootkit</td>
</tr>
<tr>
<td>Rule Name</td>
<td>Rootkit_Detection_Flea</td>
</tr>
<tr>
<td>Severity</td>
<td>Critical</td>
</tr>
</tbody>
</table>
| Monitor Paths | /usr/lib/ldlibct.so  
|              | /usr/lib/ldlibdu.so  
|              | /usr/lib/ldlibns.so  
|              | /usr/lib/ldlibpst.so |
| Description | Detects rootkit activity. |

### Table 8-168  Description of the **Ignokit Rootkit** parameters used

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Option Path</td>
<td>System Attack Detection &gt; UNIX Rootkit File / Directory Detection</td>
</tr>
<tr>
<td>Option</td>
<td>Ignokit Rootkit</td>
</tr>
<tr>
<td>Rule Name</td>
<td>Rootkit_Detection_Ignokit</td>
</tr>
<tr>
<td>Severity</td>
<td>Critical</td>
</tr>
</tbody>
</table>
| Monitor Paths | /lib/defs/p  
|              | /lib/defs/q  
|              | /lib/defs/r  
|              | /lib/defs/s  
|              | /lib/defs/t  
<p>|              | /usr/lib/.libigno/pkunsec |</p>
<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Description</td>
<td>Detects rootkit activity.</td>
</tr>
</tbody>
</table>

**Table 8-169** Description of the **Ni0 Rootkit** parameters used

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Option Path</td>
<td>System Attack Detection &gt; UNIX Rootkit File / Directory Detection</td>
</tr>
<tr>
<td>Option</td>
<td>Ni0 Rootkit</td>
</tr>
<tr>
<td>Rule Name</td>
<td>Rootkit_Detection_Ni0</td>
</tr>
<tr>
<td>Severity</td>
<td>Critical</td>
</tr>
</tbody>
</table>
| Monitor Paths | /tmp/waza  
/var/lock/subsys/...datafile.../* |
| Description | Detects rootkit activity. |

**Table 8-170** Description of the **Devil Rootkit** parameters used

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Option Path</td>
<td>System Attack Detection &gt; UNIX Rootkit File / Directory Detection</td>
</tr>
<tr>
<td>Option</td>
<td>DevilRootkit</td>
</tr>
<tr>
<td>Rule Name</td>
<td>Rootkit_Detection_Devil</td>
</tr>
<tr>
<td>Severity</td>
<td>Critical</td>
</tr>
</tbody>
</table>
| Monitor Paths | /dev/caca  
/dev/dsx  
/var/lib/games/.src |
| Description | Detects rootkit activity. |

**Table 8-171** Description of the **Redstorm Rootkit** parameters used

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Option Path</td>
<td>System Attack Detection &gt; UNIX Rootkit File / Directory Detection</td>
</tr>
<tr>
<td>Option</td>
<td>Redstorm Rootkit</td>
</tr>
</tbody>
</table>
UNIX Policy Options

System Attack Detection

Table 8-171  Description of the Redstorm Rootkit parameters used (continued)

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Rule Name</td>
<td>Rootkit_Detection_Redstorm</td>
</tr>
<tr>
<td>Severity</td>
<td>Critical</td>
</tr>
<tr>
<td>Monitor Paths</td>
<td>/bin/…</td>
</tr>
<tr>
<td></td>
<td>/var/log/tk02/see_all</td>
</tr>
<tr>
<td>Description</td>
<td>Detects rootkit activity.</td>
</tr>
</tbody>
</table>

UNIX Worm File / Directory Detection

A global settings area sets the following parameters for all rules in the UNIX Worm 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 DCS:SA 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 DCS:SA was last shut down. This option provides detection ability even if the DCS:SA service or daemon is shut down. If a monitored file is changed, once the DCS:SA 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 8-172  Description of the Adore Worm parameters used

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Option Path</td>
<td>System Attack Detection &gt; UNIX Worm File / Directory Detection</td>
</tr>
<tr>
<td>Option</td>
<td>Adore Worm</td>
</tr>
<tr>
<td>Rule Name</td>
<td>Worm_Detection_AdoreWorm</td>
</tr>
<tr>
<td>Severity</td>
<td>Critical</td>
</tr>
</tbody>
</table>
### Table 8-172  Description of the Adore Worm parameters used (continued)

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Monitor Paths</td>
<td>/dev/.*/red.tgz</td>
</tr>
<tr>
<td></td>
<td>/usr/bin/adore</td>
</tr>
<tr>
<td></td>
<td>/usr/lib/libt</td>
</tr>
<tr>
<td></td>
<td>/usr/sbin/adore</td>
</tr>
<tr>
<td>Description</td>
<td>Detects worm activity.</td>
</tr>
</tbody>
</table>

### Table 8-173  Description of the 55808_A Worm parameters used

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Option Path</td>
<td>System Attack Detection &gt; UNIX WormFile / Directory Detection</td>
</tr>
<tr>
<td>Option</td>
<td>55808_A Worm</td>
</tr>
<tr>
<td>Rule Name</td>
<td>Worm_Detection_55808aWorm</td>
</tr>
<tr>
<td>Severity</td>
<td>Critical</td>
</tr>
<tr>
<td>Monitor Paths</td>
<td>/tmp/.../a</td>
</tr>
<tr>
<td></td>
<td>/tmp/.../r</td>
</tr>
<tr>
<td>Description</td>
<td>Detects worm activity.</td>
</tr>
</tbody>
</table>

### Table 8-174  Description of the Sadmind Worm parameters used

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Option Path</td>
<td>System Attack Detection &gt; UNIX WormFile / Directory Detection</td>
</tr>
<tr>
<td>Option</td>
<td>Sadmind Worm</td>
</tr>
<tr>
<td>Rule Name</td>
<td>Worm_Detection_Sadmind</td>
</tr>
<tr>
<td>Severity</td>
<td>Critical</td>
</tr>
<tr>
<td>Monitor Paths</td>
<td>/dev/cuc</td>
</tr>
<tr>
<td>Description</td>
<td>Detects worm activity.</td>
</tr>
</tbody>
</table>
### Table 8-175  Description of the **Omega Worm** parameters used

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Option Path</td>
<td>System Attack Detection &gt; UNIX WormFile / Directory Detection</td>
</tr>
<tr>
<td>Option</td>
<td>Omega Worm</td>
</tr>
<tr>
<td>Rule Name</td>
<td>Worm_Detection_Omega</td>
</tr>
<tr>
<td>Severity</td>
<td>Critical</td>
</tr>
<tr>
<td>Monitor Paths</td>
<td>/dev/chr</td>
</tr>
<tr>
<td>Description</td>
<td>Detects worm activity.</td>
</tr>
</tbody>
</table>

### Table 8-176  Description of the **LDP Worm** parameters used

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Option Path</td>
<td>System Attack Detection &gt; UNIX WormFile / Directory Detection</td>
</tr>
<tr>
<td>Option</td>
<td>LDP Worm</td>
</tr>
<tr>
<td>Rule Name</td>
<td>Worm_Detection_LDP</td>
</tr>
<tr>
<td>Severity</td>
<td>Critical</td>
</tr>
<tr>
<td>Monitor Paths</td>
<td>/bin/.login, /bin/.ps, /dev/.kork</td>
</tr>
<tr>
<td>Description</td>
<td>Detects worm activity.</td>
</tr>
</tbody>
</table>

### Table 8-177  Description of the **Lion Worm** parameters used

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Option Path</td>
<td>System Attack Detection &gt; UNIX WormFile / Directory Detection</td>
</tr>
<tr>
<td>Option</td>
<td>Lion Worm</td>
</tr>
<tr>
<td>Rule Name</td>
<td>Worm_Detection_LionWorm</td>
</tr>
<tr>
<td>Severity</td>
<td>Critical</td>
</tr>
</tbody>
</table>
Malicious Module Detection

A global settings area sets the following parameters for all rules in the UNIX Malicious Module Detection area / 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 DCS:SA 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 DCS:SA was last shut down. This option provides detection ability even if the DCS:SA service or daemon is shut down. If a monitored file is changed, once the DCS:SA 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 8-179 Description of the Suspicious Loadable Kernel Module (LKM) Detection parameters used

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Option Path</td>
<td>System Attack Detection &gt; Malicious Module Detection</td>
</tr>
<tr>
<td>Option</td>
<td>Suspicious Loadable Kernel Module (LKM) Detection</td>
</tr>
<tr>
<td>Rule Name</td>
<td>LKM_Suspicious_Module_Detection</td>
</tr>
<tr>
<td>Severity</td>
<td>Critical</td>
</tr>
<tr>
<td>Monitor Paths</td>
<td><code>/lib/ador_e_so</code></td>
</tr>
<tr>
<td></td>
<td><code>/lib/cleaner_o</code></td>
</tr>
<tr>
<td></td>
<td><code>/lib/flkm_o</code></td>
</tr>
<tr>
<td></td>
<td><code>/lib/modules/ador_e_so</code></td>
</tr>
<tr>
<td></td>
<td><code>/lib/phide_mod_o</code></td>
</tr>
<tr>
<td>Description</td>
<td>Detects suspicious activity related to Loadable Kernel Modules.</td>
</tr>
</tbody>
</table>

Suspicious Permission Change Detection

Table 8-180 Description of the Suspicious Permission Change Detection parameters used

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Option Path</td>
<td>System Attack Detection</td>
</tr>
<tr>
<td>Option</td>
<td>Suspicious Permission Change Detection</td>
</tr>
<tr>
<td>Rule Name</td>
<td>Suspicious_Perm_Change_Critical_Files</td>
</tr>
</tbody>
</table>
Table 8-180  Description of the **Suspicious Permission Change Detection** parameters used (continued)

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Severity</td>
<td>Critical</td>
</tr>
<tr>
<td>Monitor Paths</td>
<td>/bin/*</td>
</tr>
<tr>
<td></td>
<td>/usr/bin/*</td>
</tr>
<tr>
<td></td>
<td>/usr/local/bin*</td>
</tr>
<tr>
<td>Description</td>
<td>Detects suspicious changes in permissions in critical files and directories.</td>
</tr>
</tbody>
</table>
Parameter Reference Syntax

This appendix includes the following topics:

- Parameter reference syntax overview
- Simple policy parameter
- Compound policy parameter
- Operating system environment variable
- Windows registry value
- Agent translator function

Parameter reference syntax overview

Table A-1 lists the types of references that DCS:SA supports in parameter values. These can be references to parameters defined elsewhere in the policy or data on the operating system.

<table>
<thead>
<tr>
<th>Type</th>
<th>Syntax</th>
</tr>
</thead>
<tbody>
<tr>
<td>Simple policy parameter</td>
<td>%parameter%</td>
</tr>
<tr>
<td>Compound policy parameter</td>
<td>%parameter:field%</td>
</tr>
<tr>
<td>OS Environment variable</td>
<td>%environmentvariable%</td>
</tr>
<tr>
<td>Windows Registry value</td>
<td>%registrypath%</td>
</tr>
</tbody>
</table>
Table A-1  Types of references with syntax (continued)

<table>
<thead>
<tr>
<th>Type</th>
<th>Syntax</th>
</tr>
</thead>
<tbody>
<tr>
<td>Agent Translator Function</td>
<td>%?function(parameters)?%</td>
</tr>
</tbody>
</table>

Inside the reference delimiters, you must escape any special characters that are used in strings by using a forward slash (/) on Windows and a backslash (\) on UNIX.

**Note:** The syntax is the same for policy parameters and OS environment variables. The DCS:SA agent looks for a policy parameter with the given name first. If the policy parameter is not found, it looks for an OS environment variable.

See “Simple policy parameter” on page 267.
See “Compound policy parameter” on page 268.
See “Operating system environment variable” on page 271.
See “Windows registry value” on page 271.
See “Agent translator function” on page 272.

### Simple policy parameter

A simple parameter is a list of single values. You reference the parameter by its name – no field names are necessary since a simple parameter is a list of single values. The agent replaces the parameter reference with the values. Parameter names are case sensitive.

The simple policy parameter types are mentioned as follows:

- **String**  A single string value.
- **String List**  A list of string values.
- **Date/Time Duration**  A single duration value, e.g. 30 minutes.
- **Date/Time Interval**  A single repetition interval, e.g. hourly, daily.

See “Parameter reference syntax overview” on page 266.
Compound policy parameter

A compound policy parameter is a list of sets of values. In the console, a compound parameter is displayed as a table, where each row is one parameter value and the columns are the fields in the value. For each compound parameter type, there is a specific set of fields in the list. When referencing a compound parameter, you must use the parameter name followed by a colon and a field name. You must always refer to a specific field. For example, you might use %myparameter:prog%. Parameter and field names are case sensitive.

The compound policy parameter types along with their field names are mentioned as follows:

<table>
<thead>
<tr>
<th>Compound policy parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Process List</td>
<td>A list of processes, each element in the list consisting of one or more process attributes. See “Process list” on page 269.</td>
</tr>
<tr>
<td>Process List without Arguments</td>
<td>A list of processes, each element in the list consisting of one or more process attributes that excludes the command line arguments attribute. See “Process list without arguments” on page 269.</td>
</tr>
<tr>
<td>Resource List</td>
<td>A list of resources such as file paths and registry paths, where each element consists of a resource name and zero or more process attributes. See “Resource list” on page 269.</td>
</tr>
<tr>
<td>Network List with Processes</td>
<td>A list of network rules, where each element consists of network connection attributes, process attributes, and action attributes. See “Network list with processes” on page 270.</td>
</tr>
<tr>
<td>Network List</td>
<td>A list of network rules, where each element consists of network connection attributes and action attributes. See “Network list” on page 271.</td>
</tr>
<tr>
<td>Date/Time Value</td>
<td>A single date/time value with a timezone. See “Date/Time value” on page 271.</td>
</tr>
</tbody>
</table>

See “Parameter reference syntax overview” on page 266.
Process list

Process List is a list of processes, where each element in the list consists of one or more process attributes.

- The **prog** field is the **Program Path** column and is required in each row. It specifies the program running in the process.
- The **cmdline** field is the **Arguments** column, specifying the command line parameters for the process. This field is optional.
- The **id** field is the **User Name** column, specifying the username for the process. This field is optional.
- The **groupid** field is the **User Name** column, specifying the group name for the process. This field is optional.

**Note:** If you want to specify all processes for a specific user, you must still fill in the **Program Path** column, but you can use a * to specify all programs and then fill in the **User Name** column to specify the desired user account.

Process list without arguments

Process List without Arguments is a list of processes, where each element in the list consists of one or more process attributes that excludes the command line arguments attribute.

- The column and field names are identical to the Process List parameter type except the **Arguments** field is not included.

Resource list

Resource List is a list of resources such as file paths, registry paths, and process paths), where each element consists of a resource name and zero or more process attributes.

- The **value** field is the **Resource Path** column and is required in each row. It specifies the file or registry path you are controlling.
- The **prog** field is the **Program Path** column. This field is required if you want to specify other process attributes. Otherwise it is optional.
- The **cmdline** field is the **Arguments** column, specifying the command line parameters for the process. This field is optional.
- The **id** field is the **User Name** column, specifying the username for the process. This field is optional.
The **groupid** field is the **User Name** column, specifying the group name for the process. This field is optional.

**Note:** If you want to specify all processes for a specific user, you must still fill in the **Program Path** column, but you can use a * to specify all programs and then fill in the **User Name** column to specify the desired user account.

---

**Network list with processes**

Network List with Processes is a list of network rules, where each element consists of network connection attributes, process attributes, and action attributes.

- **Connection information:**
  - The **protocol** field is the **Protocol** column.
  - One or more additional connection elements are required:
    - **RPort** field is the **Remote Port** column and specifies the remote port or port range.
    - **LPort** field is the **Local Port** column and specifies the local port or port range.
    - **RIP** field is the **Remote IP** column and specifies the remote IP address or address range.

- **Action information:**
  - The **action** field is the **Action** column.
  - The **log** field is the **Logging** column.

- **Process information:**
  - The **prog** field is the **Program Path** column. This field is required if you want to specify other process attributes. Otherwise it is optional.
  - The **cmdline** field is the **Arguments** column, specifying the command line parameters for the process. This field is optional.
  - The **id** field is the **User Name** column, specifying the username for that process. This field is optional.
  - The **groupid** field is the **User Name** column, specifying the group name for the process. This field is optional.
Network list

Network List is a list of network rules, where each element consists of network connection attributes and action attributes.

- The column and field names are identical to the Network Process List parameter type, except the process-related fields are not included.

Date/Time value

Date/Time Value is a single date/time value with a timezone.

- This compound parameter type is not displayed as a table because it cannot be a list.
- The field name for the Date and Timezone fields in the Console are value and timezone, respectively.

Operating system environment variable

You can use an operating system environment variable as a variable in a policy. Environment variable names follow the operating system’s normal conventions for case sensitivity, so they are case sensitive on UNIX and case insensitive on Windows.

Note: The environment variables are evaluated in the context of the SDCSS agent IPS Service or daemon. Therefore, you should only reference the environment variables that have system-wide values. If you reference a variable with a user-specific value, you get the value for the IPS Service or daemon user, which is probably not the desired value.

See “Parameter reference syntax overview” on page 266.

Windows registry value

For registry references, the agent looks up the given value in the registry and replaces the reference with the data that the value contains.
The data must be one of the following types:

- REG_SZ (string)
- REG_EXPAND_SZ (string with environment variables that should be expanded)
- REG_MULTI_SZ (list of strings)
- REG_DWORD (32-bit integer)
- REG_QWORD (64-bit integer)

The agent expands an environment variable's REG_EXPAND_SZ values immediately, before it processes the resulting string. For REG_MULTI_SZ values, the reference expands to the list of strings.

On 64-bit versions of Windows, you can prefix registry paths with an optional redirection specification. This redirection specification specifies how registry redirection should be used when looking up the path.

The valid redirection specifications are as follows:

- 32: redirection is turned off or on to give a 32-bit program's view of the registry
- 64: redirection is turned off or on to give a 64-bit program's view of the registry
- 6432: looks in the 64-bit view of the registry first, and then if that fails, looks in the 32-bit view
- 3264: looks in the 32-bit view of the registry first, and then if that fails, looks in the 64-bit view
- ALL: looks in both the 32-bit view and 64-bit view of the registry

See “Parameter reference syntax overview” on page 266.

Agent translator function

A function reference provides a way to call an extension function from within a policy. The agent replaces the function reference with the return value or list of return values of the function.

In a function reference such as `%?function(parameters)?%`, the parameters may contain any characters, even special characters, except that you must escape a close parenthesis `)`. The function parameters are not processed, so if they contain a reference themselves, the text of the reference is passed to the function. For example, `%myvar%` is passed rather than myvar's value after evaluation. However, if a function's return value contains a reference, the reference is subsequently evaluated.

See “Translator Function Reference” on page 273.
Translator Function Reference

This appendix includes the following topics:

- Generic functions

Generic functions

The following functions can be used in both Prevention and Detection policies and can be used on all operating systems:

- `%?LocalIPs()?%`
  See “%?LocalIPs()?%” on page 273.

- `%?LocalIPAddress()?%`
  See “%?LocalIPAddress()?%” on page 274.

- `%?AgentParams(<param name>)?%`
  See “%?AgentParams(<param name>)?%” on page 274.

- `%?SplitPath(<path>)?%`
  See “%?SplitPath(<path>)?%” on page 274.

- `%?ImportFileList(<filepath>)?%`
  See “%?ImportFileList(<filepath>)?%” on page 274.

%?LocalIPs()?%

Returns the list of IP addresses for the system. Includes only IPv4 addresses.
%?LocalIPAddresses()%
Returns the list of IP addresses for the system. Includes both IPv4 and IPv6 addresses.

%?AgentParams(<param name>)% 
Looks in the IPS agent.ini file and returns the requested parameter. The following strings are valid as "param name":

- Notification Port: returns the port the agent listens on for notifications
- Server IP: returns the list of IP addresses for management servers this agent can connect to
- Server Port: returns the management server port this agent connects to

For example: %?AgentParams(Notification Port)%

%?SplitPath(<path>)% 
Takes a pathname and puts out a list consisting of the original pathname plus all the directory names on the pathname leading up to it.

For example, if you call %?SplitPath(C:\a\b\c)% you get:

- C:a
- C:a\b
- C:a\b\c

%?ImportFileList(<filepath>)% 
Takes a filepath and imports the data from the file into the policy as if a user had typed that data into the console. This data can be filepaths, registry keys, usernames, groupnames or any other strings that make sense at the point in the policy where the function is called.

By default, the file being imported is limited to 100 lines. This limit is defined in the ips.importfile.maxlines setting in the IPS/agent.ini file and can be adjusted if larger files are required.

**Note:** This function can be made optional by using in the following way:
%?-ImportFileList(<path>)% In this case, the translator will translate successfully even if the file to be imported is not available.
Note: To make the data inside the file to be optional, add a "-" in front of each optional line. For example, if the file you want to import has usernames in the file and certain user names are to be made optional then the file data should be:

admin

test1

-test2 (For an optional user)