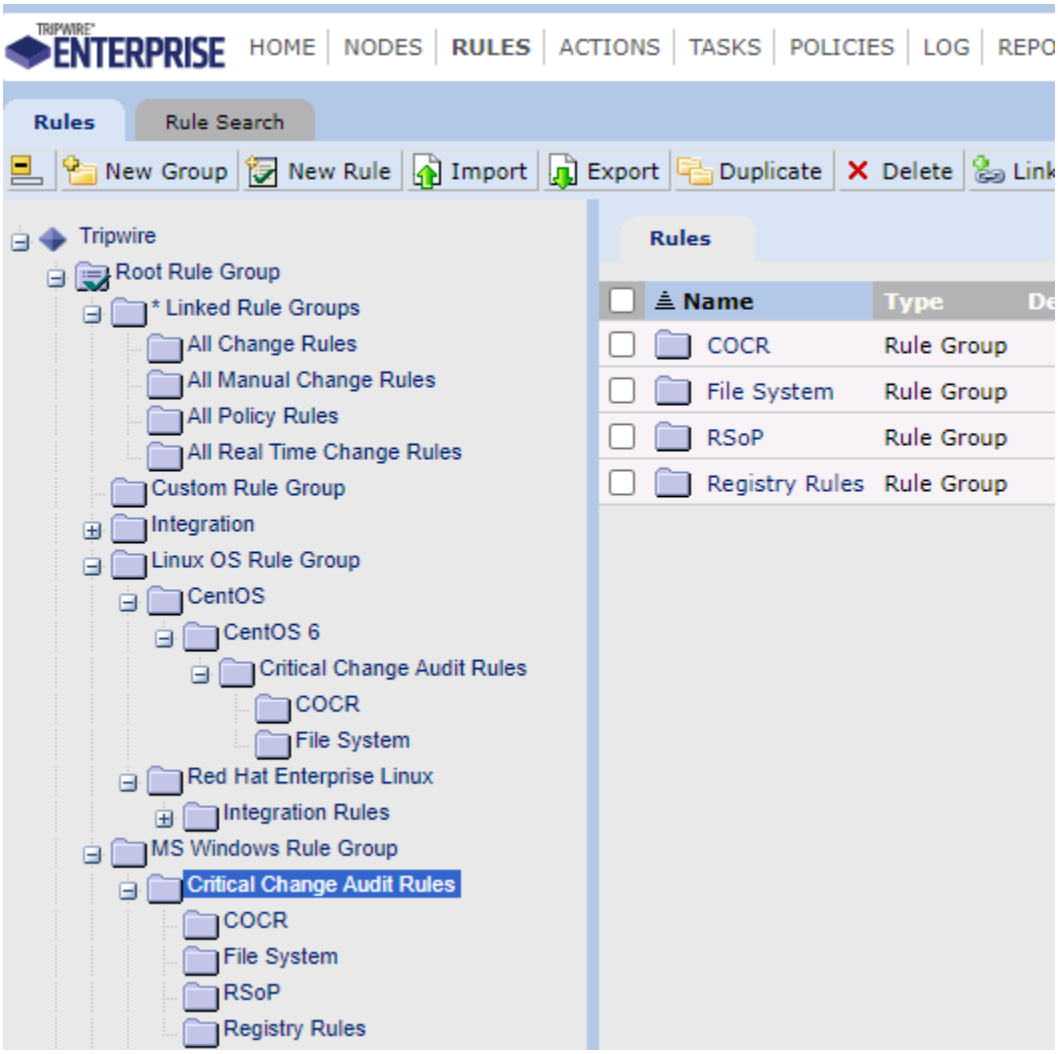
Contents

Critical Change Audit Rule in the left pane was assigned to our test server.

Right Pane you see what type of monitoring is included.



How Does a File System Rule Work?

A **UNIX file system rule** or **Windows file system rule** identifies files and directories in a file system.

Components of a UNIX or Windows file system rule

Component	Description
start points	A start point specifies a file or directory for the rule.
stop points	A stop point specifies a file or directory to be excluded from operations run with the rule. If a stop point specifies a directory, you can also exclude the directory's contents.
criteria sets	In a file system rule, a criteria set specifies attributes of files and directories. When a new element version is created for a file or directory identified by the rule, TE saves the object's values for the specified attributes in the new version. To create a criteria set for a file system rule For a list of attributes that may be added to a criteria set for a UNIX file system rule For a list of attributes that may be added to a criteria set for a Windows file system rule
actions	An action initiates a response if the rule identifies a monitored object for which a change version is created. For more information

How Does a Windows Registry Rule Work?

The information in a registry is organized hierarchically in a collection of keys, entries, and values.

A **key** is an object containing related registry information.

The keys at the highest level of a registry hierarchy are known as **root keys** or **hives**. Root keys vary between operating systems

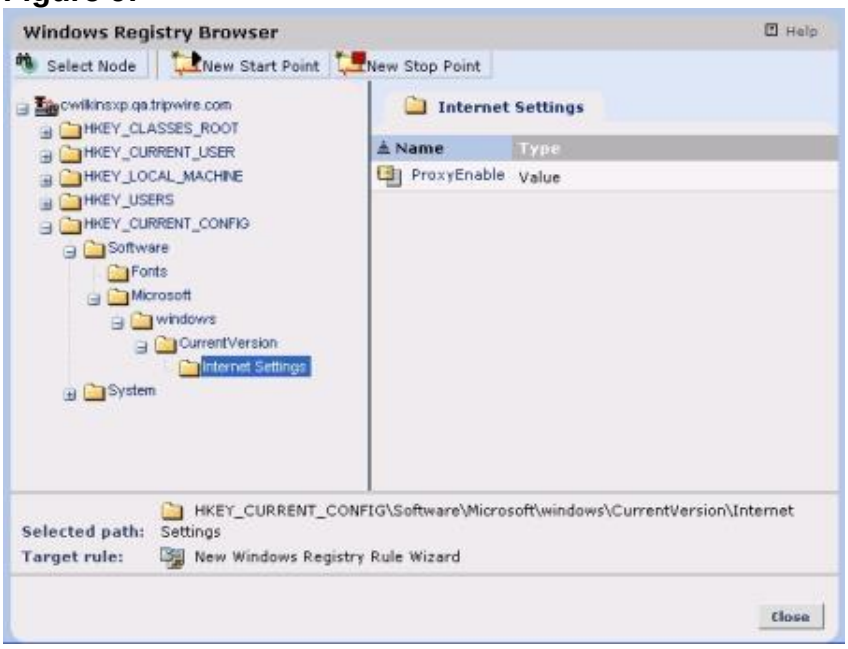
Each key may contain a number of named **entries**. Each entry has one or more **values**, including a single, unnamed **default value**. With the exception of some default values, each value consists of data in numeric, text, or binary format.

Common root keys in a Windows registry

Root Key Name	Contains ...
HKEY_CLASSES_ROOT	... Object linking and embedding (OLE) information, along with file associations (the application with which each file type is associated by default).
HKEY_CURRENT_USER	... All preference settings for the current user.
HKEY_USERS	... All preference settings for all users of the system.
HKEY_LOCAL_MACHINE	... Settings for the operating system, system hardware, and installed applications.
HKEY_CURRENT_CONFIG	... Configuration data for the current hardware profile.

Figure 9 shows an example of a Windows registry hierarchy in a Tripwire Enterprise dialog known as the Windows Registry Browser. In this example, the registry tree is expanded to display the keys within the **HKEY_CURRENT_CONFIG** root key. The displayed keys include **System** and **Software**, along with the keys descended from the `Software` key (`Fonts`, `Microsoft`, `windows`, `Current Version`, and `Internet Settings`). In addition, the `Proxy Enable` entry is displayed in the right-hand pane of **Figure 9.**

Figure 9:



How Does a Windows RSoP Rule Work?

In a Windows environment, a **Group Policy Object** (GPO) stores policy settings for users and computers. For instance, a GPO could define the following settings:

Windows Registry permissions

Audit and security policies

Login/logout scripts

Each Windows system stores a single **local Group Policy Object**. In an Active Directory environment, a local GPO has a subset of the settings stored in a **non-local Group Policy Object**. Stored on a domain controller, a non-local GPO is linked to an Active Directory site, domain, or organizational unit. (For a discussion of directory terms and concepts.

If the settings in a local GPO conflict with those of a single non-local GPO, the non-local GPO takes precedence. However, multiple non-local GPOs can apply to the same user or computer. In this case, a **Resultant Set of Policy plug-in** calculates the cumulative effect of multiple GPO settings for each user on the local system. A **Resultant Set of Policy (RSoP)** is the group of policy settings that are actually in effect for a specific user.

To monitor the RSoP of a Windows user for changes, you can use a **Windows RSoP rule**. A Windows RSoP rule defines one or more queries, and each query retrieves a report on the RSoP of a specified Windows user. To identify any changes, Tripwire Enterprise compares the following attributes with a previous version of the report:

A static set of attributes that indicate the values of common Group Policy settings.

The MD5 and/or SHA-1 hash of the RSoP report's content. These hashes are specified by the criteria set assigned to the rule.

How Does a Command Output Capture Rule (COCR) Work?

A command output capture rule (COCR) runs a command or script on a **file server** to generate and capture output. In Tripwire Enterprise, the output is represented by a single element that adopts a name specified in the properties of the COCR. To identify changes, TE compares generated command output with a baseline version of the output.

In the properties of a COCR, you define the command or script to be run on targeted file servers. These features are configured with regular expressions.

If you have implemented whitelists on Agents, the command specified in a COCR must exactly match a command in a whitelist file

Command output capture rule (COCR) features

Feature	Description
Filtering command output	**Filtering** is the process of excluding content from command output monitored by Tripwire Enterprise. For example, you could instruct TE to remove all instances of a password from command output.
Search-and-replace	With the search-and-replace feature, you can replace every instance of a string in command output with another string. For instance, you could conceal passwords in command output by replacing them with other text.

If a COCR generates output for a new element version created by a baseline operation or version check, TE saves the output's content in the version, along with the following attributes:

An MD5 hash of the content. To calculate this hash, TE excludes any filtered output and includes any replacement strings

The return code (or exit code) of the command.