

ObserveIT Unix Agent: Feature Overview

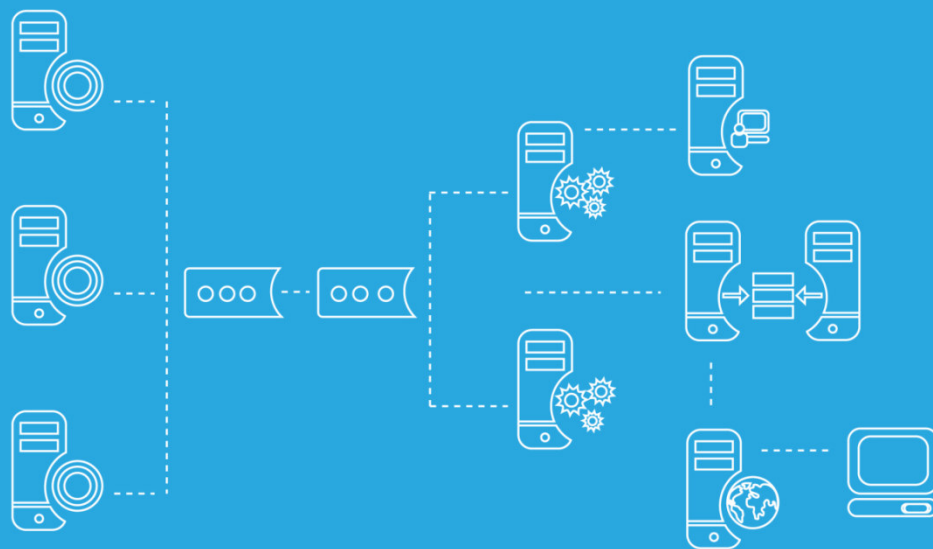


Table of Contents

- Overview 2
- What is Recorded..... 3
- Metadata Capturing..... 3
- Interaction with the User..... 3
- Config and Communication with ObserveIT Application Server..... 3

Overview

The ObserveIT Unix Agent works similarly to the ObserveIT Windows Agent, with some additional capabilities that are unique to the Unix and Linux environments.

The Unix Agent records user activity in any interactive shell running on the Unix machine, and transfers the data to the ObserveIT Management Server.

ObserveIT captures important hidden information about each user command, by capturing the resources affected and system calls made by each command. (See Metadata Capturing below)

In the initial release, the Agent will support RedHat Enterprise Linux 5.x and Solaris 10.

The screenshot displays the 'Activity View' for server 'solarism1' on 3/21/2010. A table lists sessions, with one session from 11:57 AM to 11:57 AM by Administrator. Below this, a detailed log shows system calls for 'chmod', 'rm', and 'mkdir' commands, including their process IDs and parameters. Red callout boxes provide context: 'List of sessions, including start and end time' points to the session table; 'Applications that were executed by the user on the Linux/Unix server' points to the command list; 'Commands + Parameters of each application executed' points to the system call parameters; 'View all sessions for this server' points to the server dropdown; 'Video icon for visual replay of the command' points to the video icons; and 'System calls triggered by the command that was issued' points to the system call log.

What is Recorded

- All interactive shell logins to the system
- The data stream to and from the terminal on which the login took place
- Each command line activity on the system
- The system calls triggered by the command line or script that are executed by the user

Metadata Capturing

ObserveIT captures all the internal actions and the names of files/resources affected by the command line operation.

- Ex: If the user types *rm *.txt*, ObserveIT will record the command that was typed, plus the exact name of each file that was deleted.

The Agent captures each system call performed by the command. Thus, each action performed by a script file or executable (including file create/delete/open/permission change, process creation, link creation) is fully exposed.

- Ex: If the user runs an alias script named *innocentScript* that includes system calls to delete files and change user permissions, this info will also be captured.

Interaction with the User

- The Agent can be configured to alert the user that all actions are being monitored.
- ObserveIT can also send custom messages to the user regarding company policy and server activity notifications

Config and Communication with ObserveIT Application Server

- The Agent receives policy rules and configuration updates from the server, and filters the recording activity accordingly
- Captured data is relayed to the server securely
- In the event of temporary loss of communication, data is buffered locally until network connection is restored
- The Agent provides activity and status indications to the server.