Safeguard for Sudo

Extend and Enhance Sudo through Centralized Management

Overview

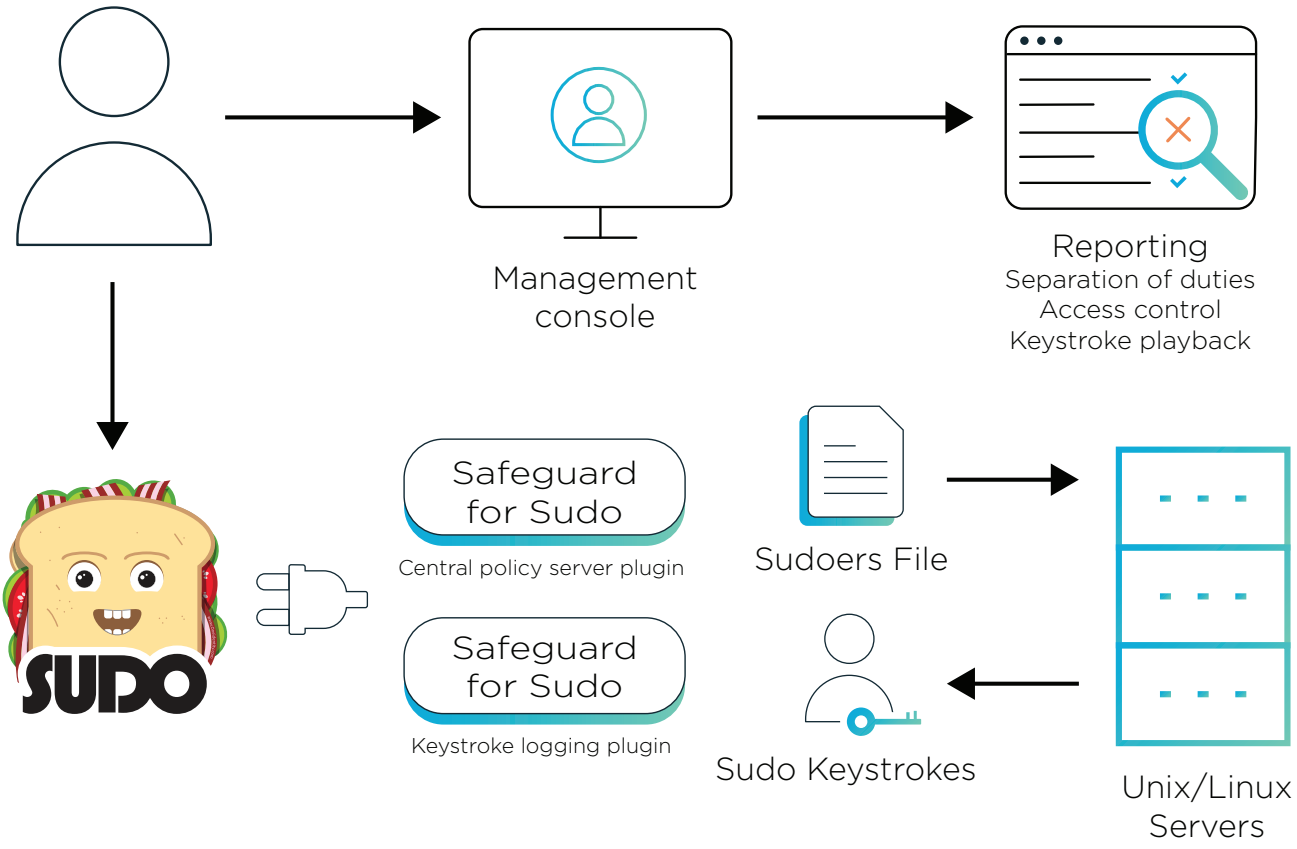
The vast majority of Unix/Linux organizations use the open-source sudo project to help delegate the Unix root account to achieve privileged account management objectives. Sudo has a proven history of delivering value; however, management of sudo can be cumbersome. Sudo policy is often inconsistently written and executed across multiple servers, and sudo does not include the ability to audit the important super user access and activities that are so critical to security and compliance initiatives.

Safeguard for Sudo helps Unix/Linux organizations take privileged account management through sudo to the next level. The Safeguard for Sudo plugins enhance sudo 1.8.1 (and newer) with a central policy server, centralized management of sudo and the sudoers policy file, centralized reporting on sudoers access rights and activities, as well as keystroke logging of all activities performed through sudo.

Using Safeguard for Sudo administering sudo across a few, dozens, hundreds or thousands of Unix/Linux servers is easy, intuitive and consistent. It eliminates the box-by-box management of sudo that is the source of so much inefficiency and inconsistency and enables organizations to actually see who is doing what with sudo. And because Safeguard for Sudo enhances sudo instead of replacing it there is no end-user or administrator retraining required, which results in no increased help desk calls and a faster time-to-value. In addition, the centralized approach delivers the ability to report on sudo activities, sudo policy (sudoers) and even change history of sudoers, simplifying access control and reporting for auditing and compliance. Finally, a separate plug-in expands the centralized administration of sudo to also include keystroke logging complete with search and playback capabilities.

Benefits

- Improves efficiency and policy consistency with centralized management of sudo across all your Unix/Linux servers
- Increases security by logging and reporting on all sudo keystroke activity
- Simplifies adherence to compliance and audit requirements by providing access control and user activity reports
- Streamlines administration using a single, convenient console to manage sudo, Active Directory and enterprise root delegation



Features

Extends Sudo
Enhance sudo with new capabilities using plug-ins (central policy server and keystroke logging) that embrace and extend the sudo modular framework.

Central Sudo Policy
Use a central service to enforce policy across all of your Unix/ Linux servers. This removes the need for administrators to manage the deployment of sudoers on every system, improving security and reducing administrative effort.

Centralized Reporting
Easily track who, what and when changes were made to sudoers, including versioning with the ability to revert to any previous version. You can see who made what changes to the sudo policy file and when, as well as track who ran what sudo accepted and rejected commands across all managed systems.

No Training Required
Avoid training and minimize calls to the help desk. Safeguard for Sudo's plug-ins extend sudo's capabilities, enabling users to take advantage of their existing sudo knowledge and realize a faster time-to-value. Other solutions require learning new commands and syntax, resulting in more training and calls to the help desk.

Keystroke Logging
Track keystrokes for administrators who perform actions through sudo. The Safeguard for Sudo Keystroke Logging plug-in provides a comprehensive log of activities performed and commands executed across all systems. The report can be filtered in many ways to help you quickly find the data you need. For example, you can filter on specific commands or see commands run during a particular time period.

Centralized Management
Use the Management Console for Unix to manage sudo and other One Identity solutions. This greatly simplifies administration and audit-related tasks across your entire UNIX environment.

Separation of Duty Enforcement
Using the Management Console for Unix, you can enforce separation of duties (SoD) and assign users a specific role, which allows them to only execute a defined set of tasks and no more.

Sudo Offline Policy Cache
Provide continuity of service in the event of a network or server outage.

Script Compatibility
Ensure compatibility with existing script files that include embedded sudo commands. Other privileged management solutions use different commands and syntax resulting in existing scripts fail to run and in potentially huge costs to test and fix scripts across multiple Unix systems.

About One Identity

One Identity delivers unified identity security solutions that help customers strengthen their overall cybersecurity posture and protect the people, applications and data essential to business. Our Unified Identity Security Platform brings together best-in-class Identity Governance and Administration (IGA), Access Management (AM), Privileged Access Management (PAM) and Active Directory Management (AD Mgmt) capabilities to enable organizations to shift from a fragmented to a holistic approach to identity security. One Identity is trusted and proven on a global scale – managing more than 250 million identities for more than 5,000 organizations worldwide. For more information, visit www.oneidentity.com.

© 2023 One Identity LLC ALL RIGHTS RESERVED. One Identity, and the One Identity logo are trademarks and registered trademarks of One Identity LLC in the U.S.A. and other countries. For a complete list of One Identity trademarks, please visit our website at www.oneidentity.com/legal. All other trademarks, servicemarks, registered trademarks, and registered servicemarks are the property of their respective owners. Datasheet-SafeguardSudo-KA-83694

ONE IDENTITY by Quest