# Sudo or SuDon't: Are you managing privileged command execution?

**AUTHOR | DAVID DINGWALL, VP OF PRODUCT MARKETING**

## MANAGING PRIVILEGED ACCESS

Managing privilege in the enterprise server infrastructure can be a real challenge. For starters, Linux and Unix system administrators will need root level authority at times to do their jobs. Systems operations staff such as DBAs will also need periodic database and application account authority. And last, security administrators will need to protect the environment. Adding to the challenge, the security administrator role does not even exist in many organizations that have grown their infrastructure quickly.

The sudo utility offers a solution to delegate root authority for OS administration commands (for example, "backup") specific to the task without giving up full root access. It can also delegate applications or DBA authority to operations staff without giving up, say, the "oracle" account.

Sudo is most commonly managed with a policy text file local to each and every server, which can become a change management nightmare. In many instances, we find groups of policies allowing system administrators full root access… often without further challenge for authentication. At this point, the security administrator has effectively relinquished control of the root account and put the trust in the system administrator due to the fact that the administrator can now change the policy herself. Root authority is at the discretion of the administrator, and often influenced by help desk tickets in the day-job which tend to be more operationally focused than security minded.

In many cases, after a server has been commissioned and loaded, updates to sudo policies are unknown thereafter and not effectively audited by the security administrator nor reported to the line-of-business System Owners as ongoing risks to business data.

With more detailed inspection, the sudo configuration can also allow a lot more access than originally intended. Many system commands allow a user to 'shell out' to run commands with the effective user ID of the original command. Common examples include: vi, more, less, tee, man, awk, sed, find. Commands and management scripts for other applications, database, and programming environments (irb, l;ua, perl, python Sql*Net, ruby) have similar problems.

While a sudo rule may initially appear to grant limited scope and authority, in reality, they may have left root, application, or database access wide open on the server OS.

## SCALING AND AUTOMATION

Maintaining a consistent security policy on a large number of servers can also become a huge burden to the security administrator. Configuration tools like Puppet can mitigate the problem to some degree, but the policy is vulnerable to sudo file updates in the same way between configuration updates, leaving a window of opportunity to plant back-door mechanisms that circumvent the authorized security policy.

## IS THERE A BETTER WAY? "SUDO OR SODON'T?"

BoKS ServerControl offers a solution by defining and enforcing privileged command execution security policy in a central

database. The policy for an individual cannot be changed even when an administrator or operations user has been granted root, application or dba access on a server. With BoKS ServerControl, the security administrator maintains the security policy, and can grant the system administrator or operator the appropriate level of privilege to do her job, maintaining a clear segregation of duties.

Centralizing the security configuration eases the pain of maintaining a consistent policy across the enterprise so that even large environments become manageable. Privilege escalation is centrally logged and offers keystroke logging where appropriate, making audit and operations reporting trivial.

## GUT CHECK

Sudo can be an effective tool when used properly. Sadly, improper use is far too common either from inappropriate or ineffective configuration definitions, or simply due to the overwhelming task of maintaining the still-growing server environment with limited tools and over-extended administration and operations staff.

BoKS ServerControl can enable a security administrator to effectively manage least-privilege with better security, greater efficiency, and centralized auditing and logging for even the largest enterprise organizations.

## ABOUT FOXT

Fox Technologies, Inc. helps companies protect corporate information assets with network security and access management software as well as striving to simplify compliance and streamline administration with an award-winning access management and privileged account control solution. Our access management software centrally enforces granular access entitlements in real time across diverse server environments.

To learn more about Fox Technologies, please visit us at: **www.foxt.com**

## CONTACT INFO

**North America**
3300 Eagle Run Drive NE, Suite 202
Grand Rapids, MI 49525
+1 877 818 3698 (Toll Free)

**Sweden**
FoxT Sweden AB
Kungsängsgatan 18A
SE-753 22, Uppsala
+46 18 16 00 00 (Main)

**United Kingdom**
400 Thames Valley Park
Reading , Berkshire RG6 1PT
+44 1189 637 681 (Main)

www.foxt.com | info@foxt.com

foxtechnologies.

You may also be interested in: Best Practices for Unix/ Linux Privileged Identity and Access Management