WHITE PAPER | SEPTEMBER 2014

Governance and Control of Privileged Identities to Reduce Risk

Merritt Maxim
CA Security Management

Table of Contents

Executive Summary

Challenge

Organizations must manage ongoing IT security challenges and changing regulatory requirements that require them to control and govern the actions of privileged identities.

Failure to govern and control privileged identities could result in data loss or destruction, malicious or inadvertent damage, fines, and even lawsuits. The processes for reviewing and approving administrators' access rights and policies are often manual, labor-intensive and inefficient, making real-time adherence to segregation of duties and other compliance policies very difficult.

Opportunity

While organizations may have implemented some form of privileged identity management to better protect and control sensitive servers, these deployments often lack automated processes for verifying administrator access rights on an ongoing basis. Privileged identity management and identity governance are areas that can provide significant value independently, but may now be combined to enable organizations to secure and govern their privileged identities more efficiently and in complementary ways. CA Technologies calls this privileged identity governance.

Benefits

Implementing privileged identity governance can deliver significant benefits to all organizations. First, automated governance processes around privileged users can help prevent breaches due to improper administrator actions or data exposure. Using identity governance with privileged identity management also provides visibility into administrator access and actual usage, which can greatly assist with ongoing audit and compliance efforts. Lastly, privileged identity governance can also help reduce risk and improve efficiencies associated with existing processes around entitlement certification.

Section 1: Challenge

Governing Privileged Identities and Shared Accounts: The Risks

Organizations of all types must regularly provide IT administrators with access to shared and privileged accounts, such as Oracle and root. Because these accounts enable access to a wide range of capabilities, access to these accounts is often restricted and “controlled” via the use of passwords. However, passwords present additional risks. Not only can passwords be cracked or guessed, but they can also be easily shared with unauthorized people.

Shared accounts create additional problems, starting with the difficulty of holding individuals accountable for privileged activity. For example, if five IT staffers know a password and each one logs into a given system with the same credentials, it could be impossible to trace any activity—illicit or otherwise—back to a single person. If administrators do not possess unique credentials for systems, databases and other critical systems, malicious users can hide behind the anonymity provided by a shared account.

The combination of privileged user access with administrator carelessness can often impact business continuity. Meanwhile, the lack of accountability makes it almost impossible to trace back to the specific administrator who committed the errors, resulting in both security and accountability issues. The potential risks posed by privileged identities means this is an issue that organizations cannot ignore.

Complexity of managing privileged user passwords.

In addition to maintaining accountability for privileged user access, these shared passwords must be stored, changed and distributed in a timely and secure manner in order to comply with corporate security policy. Many applications also use hard-coded passwords in shell scripts and batch files, which actually make the problem worse. These passwords are static and available to anyone who has access to the script file, including malicious intruders.

Increased administrative burden of managing UNIX identities.

UNIX access today is managed in silos with multiple distributed account stores, where users have many accounts on different systems. This increases administration costs and overhead, and also the overall complexity of the environment, as a large number of mission-critical applications rely on UNIX for uptime and availability.

Log integrity and quality.

Another audit challenge comes from system log integrity. If users are provided with privileged credentials that offer unlimited access, they can take any actions they want, and delete or modify the system logs to eliminate evidence of their malicious actions. And even if log integrity is preserved, the logs often do not contain all the necessary information for privileged user identity governance.

As if the above listed challenges for privileged users are not enough, organizations face additional challenges around how to cost-effectively demonstrate compliance with corporate and regulatory policies. In today’s highly distributed and evolving organizational structures, enterprises require business-wide processes to review and approve entitlements, maintain accurate roles and help ensure identity compliance.

Such processes should involve the business (since line managers often best understand their users' needs), so it is important to minimize the time and cost of reviewing, editing and approving entitlements, while providing the proper business context.

Unfortunately, the framework and processes incorporating business review and approval of privileged users is often highly manual. For instance, many IT organizations still manually email spreadsheets to business managers, listing their privileged users' roles and entitlements for review.

Similarly, they send printed reports of user entitlements as an ad-hoc dump to auditors. Not only are these approaches labor-intensive and inefficient, but they also make adherence to segregation of duties and other compliance policies very difficult.

While approaches like creating an optimal role structure for all administrators can assist in understanding how users actually access computing systems and which groups of users should have access to what resources, organizations often struggle with developing and maintaining a role structure that accurately covers the most privileged assignments with as few roles as possible, especially as the organization evolves.

Analytics can reveal the patterns that are hidden in existing sets of privileges, as well as discover out-of-pattern privileges that indicate unnecessary access which may require removal. This process is not trivial—modern organizations that have evolved through mergers, acquisitions and organizational restructuring often end up with excessive privilege assignments. Adding to this complexity is the amount of data and relationships that must be analyzed, since even medium-sized organizations with only a few thousand employees can often have hundreds of thousands of access assignments.

The combination of managing privileged users and shared accounts with inefficient processes for approving and managing privileged users' entitlements can often impact business continuity and demonstrates why organizations should assess what technology solutions can help address the challenge of managing privileged users.

This leaves many organizations struggling to answer such critical questions as:

- How do you control which users can access which privileged accounts?
- How do you ensure accountability for the privileged accounts?
- How can you ensure that service accounts passwords are being rotated regularly?
- How can you give programs and scripts access to privileged accounts in a controlled way?
- How can you give users temporary or emergency access to privileged accounts?
- How can you automate the process of verifying administrator's entitlements?
- How can you prove to auditors that privileged accounts, even if controlled, have been reviewed periodically as required by regulations or business policies?

Section 2: Opportunity

Governance of Privileged Identities with Process Automation

The previously discussed challenges, such as account/password sharing, lack of accountability and log integrity and manual entitlement review processes can be overcome with a privileged identity governance solution. Organizations can also address this in a modular way. Usually the first step is to address the issues associated with privileged users, and follow that with process automation for entitlement certification and governance.

For example, with fine-grained access controls that empower administrators to customize entitlements based on roles and their privileges (e.g., the Web administrator can only access Web applications), organizations can limit unauthorized access and maintain accountability. Such technology could also prevent logs from being altered, averting the prospect of a malicious user modifying or deleting them to avoid detection.

Automatic login technology that ties entitlements to a user's main system ID could be similarly beneficial, as it would eliminate the need for additional passwords, along with the possibility of sharing among employees. This also creates benefits from an ease-of-use perspective, as administrators no longer have to create and manage multiple passwords—they can simply set up entitlements on the backend and let the technology do the rest.

What's more, such features as fine-grained access and automatic login help administrators proactively comply with PCI, NIST and other standards by eliminating or reducing security risks, increasing transparency and improving accountability. And, if the privileged user management solution works across physical and virtual servers and hypervisors, executives can feel confident that their entire IT infrastructure will be secured.

With technology in place to manage privileged identities, the next step is to deploy a technology solution that can periodically validate that privileged users have appropriate access to corporate resources. During entitlements certification, managers are typically asked to review lists of their direct reports' privileges and either confirm or reject the need for this access. Features such as flexible workflows to help ensure entitlement campaigns progress according to requirements and the ability to provide email notifications, reminder alerts and escalation processes for requesting approval from higher-level managers are all essential requirements.

Additionally, delivering analytics that can examine user, role and privilege relationships and suggest candidate roles are also an essential component for privileged identity governance. The analytics engine applies pattern recognition and other advanced algorithms to automatically discover common access assignments that may represent roles.

As the need to control privileged users grows, CA Technologies is the first vendor to combine host access control with a comprehensive privileged user management solution—including privileged user password management, fine-grained access controls and privileged user auditing and reporting.

CA Privileged Identity Manager

CA Privileged Identity Manager (formerly CA ControlMinder) helps satisfy internal policies and external compliance regulations by centrally controlling and managing privileged user access to a diverse set of servers, devices, and applications. Enabling cross-platform creation, deployment and management of complex, fine-grained access control policies, all from a single management console, CA Privileged Identity Manager surpasses the basic controls available within native operating systems and enables compliance with stringent corporate policies and regulations.

CA Privileged Identity Manager is comprised of the following components:

- CA Shared Account Manager (formerly CA ControlMinder Shared Account Management) provides secure storage and access to privileged user passwords
- End-point protection and server hardening includes the core elements of CA Privileged Identity Manager which are used to harden the operating system and enforce granular role-based access control
- UNIX Authentication Bridge (UNAB) allows UNIX and Linux users to authenticate using their Active Directory credentials
- Integration with CA Identity Governance (formerly CA GovernanceMinder) to conduct certification campaigns on privileged users and administrators

For privileged identity governance, the most relevant CA Privileged Identity Manager component is CA Shared Account Manager which provides secure access to privileged accounts, manages password complexity, and helps provide accountability for privileged access through the issuance of passwords on a temporary, one-time use basis and through secure auditing of shared account accesses. CA Shared Account Manager is also designed to allow applications to programmatically access system passwords and, in so doing, remove hard-coded passwords from scripts. Support is available for a multitude of servers, applications (including databases), and devices in physical and virtual environments.

CA Privileged Identity Manager can help deliver:

- Increased control of powerful users
- Accountability of shared account activity
- Reduced administrative costs
- Easier audit and compliance processes
- A better user experience

CA Identity Governance

CA Identity Governance is designed to automate identity and access governance processes and provide continuous identity controls. This starts with leveraging a business-friendly role foundation to present information to users in the context that makes sense to them. It also checks security policies and highlights violations to business managers during identity processes such as entitlements certification.

CA Identity Governance's advanced analytics improve the time-to-value of activities such as privilege cleanup and role discovery. Combined with a powerful policy engine, this provides the foundation to help align security, IT, and business organizations.

CA Identity Governance also exposes its analytic capabilities for use during everyday identity processes. Applying analytics in this manner is based on a fundamental observation that role-based management revolves around patterns of privileges and access. Even in organizations where privileges are not currently managed via roles, the actual assignment of privileges can roughly follow role-based patterns. Deviations and exceptions that become readily apparent can be surfaced in identity processes, helping to make them more effective.

CA Identity Governance's robust analytic capabilities (in terms of scalability and the strength of algorithms used) uniquely leverage these capabilities not only as a preliminary role-discovery tool, but also as a strategic decision-support engine that streamlines many identity-related business processes.

Examples of activities which may benefit from analytics include:

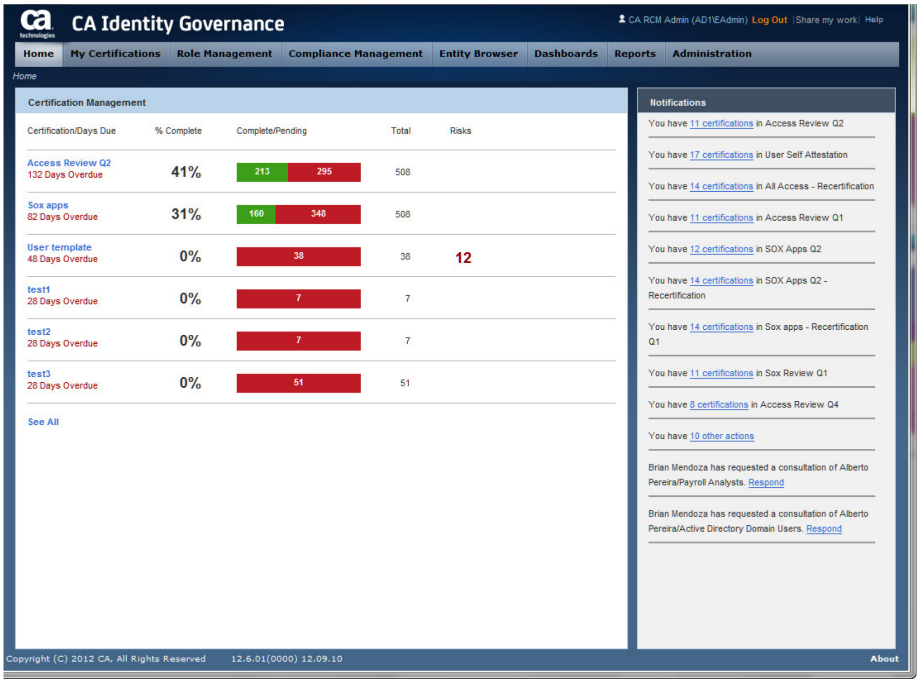
- Mapping of administrators to the accounts they own across enterprise applications
- Cleaning up of excess and erroneous access rights
- Discovering candidate roles using existing users and account information or optimizing role structures
- Comparing different strategies for role modeling and finding an optimal approach for balancing business and IT requirements with the reality of current access assignments
- Highlighting suspected assignments in entitlement certification processes
- Highlighting suspected privilege assignments as a preventative control during provisioning actions

CA Identity Governance includes an extensive set of out-of-the-box reports and dashboards while supporting ad-hoc queries for forensic requirements. Reports vary in the level of business and technical information provided in order to address the needs of different user types. This includes separate reports for business managers, role engineers, compliance officers, auditors and IT personnel. Some example reports relevant for privileged users include:

Privilege quality. Provides key metrics and supporting details about the quality of existing or proposed access. This includes statistics on users, roles, resources, lists of overlapping roles and suspected inappropriate access. These reports are often used to understand the gap between the current and desired state or to highlight areas for privilege cleanup.

Role analysis. Compares the results of various role modeling methodologies and provides detailed analysis of current role structure (e.g. users with similar privileges that are currently not members of the same roles). Role engineers can use these reports to review suspected roles or to provide evidence that roles conform to best business practices.

Compliance. Provide business managers, compliance officers and auditors with a robust view of policy controls, campaign progress and associated risk. This includes audit card reports which review key findings such as explicit policy violations and suspicious assignments. Entitlement certification reports display the process progress status as well as the process details.



Certification Management

Certification/Days Due	% Complete	Complete/Pending	Total	Risks
Access Review Q2 132 Days Overdue	41%	🟩 213 🟥 295	508	
Sox apps 82 Days Overdue	31%	🟩 160 🟥 348	508	
User template 48 Days Overdue	0%	🟥 38	38	12
test1 28 Days Overdue	0%	🟥 7	7	
test2 28 Days Overdue	0%	🟥 7	7	
test3 28 Days Overdue	0%	🟥 51	51	

See All

Notifications

You have 11 certifications in Access Review Q2

You have 17 certifications in User Self Attestation

You have 14 certifications in All Access - Recertification

You have 11 certifications in Access Review Q1

You have 12 certifications in SOX Apps Q2

You have 14 certifications in SOX Apps Q2 - Recertification

You have 14 certifications in Sox apps - Recertification Q1

You have 11 certifications in Sox Review Q1

You have 8 certifications in Access Review Q4

You have 10 other actions

Brian Mendoza has requested a consultation of Alberto Pereira/Payroll Analysts. Respond

Brian Mendoza has requested a consultation of Alberto Pereira/Active Directory Domain Users. Respond

Copyright (C) 2012 CA, All Rights Reserved 12.6.01(0000) 12.09.10

Figure A.

CA Identity Governance Certification Dashboard displays current status of all active certification campaigns.

CA Identity Governance among other capabilities provides automatic and periodic attestation processes for privileged accounts. Periodically validating privileged accounts to confirm users have appropriate access helps meet compliance requirements. CA Identity Governance now provides a specific entitlement certification campaign for Shared Accounts along with an easy-to-use interface that reviewers can easily view to certify that privileges and accounts are either appropriate or should be removed. Additionally, to help reviewers make faster, more accurate decisions, CA Identity Governance can also provide business context such as how frequently a resource was accessed or if an entitlement causes a security policy violation. This combination of solution completes the Shared Account Management and Governance Lifecycle.

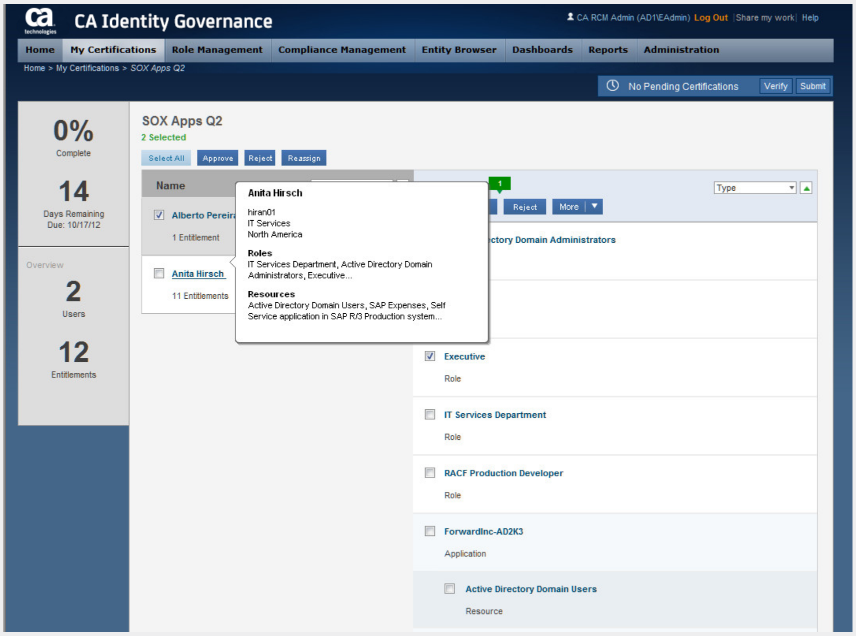
Here are two specific examples where CA Identity Governance can assist in ensuring administrators get the appropriate level of privileges.

Access Roles. In CA Identity Governance, you can define Access Roles for administrators which provide some level of control over what entitlements are granted. As an example, you could create roles such as: Database administrator, Active Directory Security Admin and Sys Admin with each role specifically defining what is/is not allowed.

Segregation of Duties (SoD) Rules. CA Identity Governance supports the ability to define and test SoD rules. So for privileged users, you can create rules that if an administrator can access the system resources, they cannot make changes to the DB. You could also assign a risk level-based on the level of clearance as a way to assess your level of risk.

Figure B.

CA Identity Governance reports from a specific campaign.



SOX Apps Q2

2 Selected

0% Complete

14 Days Remaining
Due: 10/17/12

Overview

2 Users

12 Entitlements

☑ Alberto Pereira
1 Entitlement

□ Anita Hirsch
11 Entitlements

Anita Hirsch

hiran01
IT Services
North America

Roles
IT Services Department, Active Directory Domain Administrators, Executive...

Resources
Active Directory Domain Users, SAP Expenses, Self Service application in SAP R/3 Production system...

ctory Domain Administrators

☑ Executive
Role

□ IT Services Department
Role

□ RACF Production Developer
Role

□ ForwardInc-AD2K3
Application

□ Active Directory Domain Users
Resource

Reporting

In addition to the process automation that CA Identity Governance and CA Privileged Identity Manager can deliver, another key imperative is being able to produce reports for auditors that demonstrate that privileged accounts, even if controlled, have been reviewed periodically as required. In some cases, these auditors' requirements may be driven by external compliance regulations or internal business policies.

CA Privileged Identity Manager provides proactive reporting on user access privileges and proof of existing access controls. Out-of-the-box, the CA Privileged Identity Manager reporting service comes with more than 60 standard reports detailing information on entitlements and the current status of (and deviation from) deployed policies as part of the default product installation. They provide immediate value by complementing existing event-based auditing to monitor compliance requirements and highlight existing discrepancies. The standard reports include:

- Policy management reports allow you to view the status of policy deployment and deviations from the standard policies.
- Entitlements reports allow you to view the entitlement users and groups have over system resources—or show who can access specific resources. A common use would be to see who has root access to the systems.
- User management reports provide you the ability to view inactive accounts, user, group membership and administrative accounts, and manage segregation of duties.
- Password management reports deliver information on password aging, password policy compliance, etc.
- Privileged user access reports detail information on all privileged user activity including check-in, check-out, workflow approvals and other actions.

Section 3: Benefits

CA Privileged Identity Manager and CA Identity Governance: A Robust Solution for Privileged Identity Governance

CA Privileged Identity Manager addresses your concerns about controlling privileged identity access, while delivering the flexibility to support local exceptions in an auditable and accountable manner. CA Privileged Identity Manager helps you:

- Mitigate risk
- Regulate and audit privileged user access
- Streamline allocation and removal of privileged access
- Reduce risk of passwords being shared
- Increase user accountability
- Enhance control of privileged users' access and use of enterprise data
- Improve security and compliance with regulatory standards
- Prove to auditors that reviews have been completed on regular intervals

CA Identity Governance has been architected to deliver superior scalability with easy customization that helps ensure processes and controls achieve high adoption and effectiveness in the organization.

With CA Identity Governance, you can address identity and access governance with an integrated lifecycle approach based on a centralized entitlements warehouse, process automation and powerful analytics engine. This approach can deliver rapid time-to-value, for example, enabling organizations to establish a role model quickly (weeks rather than months), with better access rights coverage (often 70 to 80 percent of the user population), and better alignment to business needs and preferences.

By automating processes and controls based on a more accurate entitlements, role and policy foundation, organizations can help ensure that the access is at the level they actually need. This can reduce the organization's security risk profile and enable it to more easily demonstrate compliance to internal and external auditors.

Using CA Shared Account Manager in conjunction with CA Identity Governance provides organizations with a solution that can address the ongoing challenges of managing and governing privileged users in a modular and integrated fashion.

Section 4:

Conclusions

Over the past few years, the challenges of effectively managing and governing privileged users have increased in complexity. Organizations have often relied on inefficient manual methods and processes to address this challenge, leading to increased administrative costs as well as increased risks arising from administrators with excessive or inappropriate privileges. For this reason, a solution that can manage and govern privileged identities is a key business imperative. Privileged identity governance can promote compliance efficiency as well as lower operational costs, while still keeping administrator productivity high.

Using identity governance with privileged identity management also provides visibility into administrator access and actual usage, which can greatly assist with ongoing audit and compliance efforts. Privileged identity governance can also help reduce risk and improve efficiencies associated with existing processes around entitlement certification.

By providing such a broad set of supported platforms and end points, enterprise scalability, and flexible workflow, organizations can be confident that CA Privileged Identity Manager and CA Identity Governance will support their privileged identity management and governance needs both now and well into the future.

Section 5:

About the Author

Merritt Maxim has 15 years of product management and product marketing experience in the information security industry, including stints at RSA Security, Netegrity and OpenPages. In his current role at CA Technologies, Merritt handles product marketing for identity management and cloud security initiatives. The co-author of "Wireless Security" Merritt blogs on a variety of IT security topics, and can be followed at www.twitter.com/merrittmaxim. Merritt received his BA cum laude from Colgate University and his MBA from the MIT Sloan School of Management.

Certain information in this publication may outline CA's general product direction. However, CA may make modifications to any CA product, software program, method or procedure described in this publication at any time without notice, and the development, release and timing of any features or functionality described in this publication remain at CA's sole discretion. CA will support only the referenced products in accordance with (i) the documentation and specifications provided with the referenced product, and (ii) CA's then-current maintenance and support policy for the referenced product. Notwithstanding anything in this publication to the contrary, this publication shall not: (i) constitute product documentation or specifications under any existing or future written license agreement or services agreement relating to any CA software product, or be subject to any warranty set forth in any such written agreement; (ii) serve to affect the rights and/or obligations of CA or its licensees under any existing or future written license agreement or services agreement relating to any CA software product; or (iii) serve to amend any product documentation or specifications for any CA software product. This document is for your informational purposes only and CA assumes no responsibility for the accuracy or completeness of the information contained herein. To the extent permitted by applicable law, CA provides this document "as is" without warranty of any kind, including, without limitation, any implied Warranties of merchantability, fitness for a particular purpose, or noninfringement. In no event will CA be liable for any loss or damage, direct or indirect, from the use of this document, including, without limitation, lost profits, business interruption, goodwill or lost data, even if CA is expressly advised in advance of the possibility of such damages.