SOLUTION BRIEF

How Can I Protect Privileged Credentials Across my Traditional and Virtual Data Centers, Private and Public Clouds and Hybrid Environments?

ca technologies

Managing and protecting privileged credentials is essential to reducing risk and addressing compliance requirements. Organizations need to evaluate privileged password management solutions for the depth of controls, scope of coverage and degree of cloud alignment they provide. CA Privileged Access Manager delivers against all three of these dimensions, providing a next-generation solution for privileged credential management that drives IT risk reduction, improves operational efficiency and protects an organization's investment by supporting traditional, virtualized and hybrid-cloud infrastructure alike.

Executive Summary

Challenge

Virtualization and cloud computing adoption are elevating the importance and complexity of an age-old problem: effectively managing and protecting passwords for privileged accounts. Managing privileged passwords across the traditional infrastructure (network gear, servers, mainframes, etc.) has been a long-standing security and compliance problem. Further complicating matters is the multitude of privileged credentials hard-coded into applications. Examples of such credentials are SSH key pairs and the PEM-encoded keys used to access Amazon Web Services (AWS) resources.

Opportunity

Effective protection of privileged credentials across the hybrid enterprise can help an organization to mitigate the risk from exploitation by external attackers and malicious insiders. There is an opportunity for organizations adopting privileged access management approaches that deliver against the 12 must-have capabilities, explained in this brief, to reduce the risk from failed audits and compliance violations, high value data loss and costly service interruption—all of which can be traced to unprotected privileged accounts.

Benefits

CA Privileged Access Manager provides a comprehensive set of controls for protecting and managing all types of credentials for all types of resources, wherever they are located and in a way that keeps pace with today's hybrid cloud environments, allowing organizations to gain greater reductions in risk, cost of ownership and operational workload than are possible with alternate approaches that fail to provide comparable depth of controls, breadth of coverage and alignment with cloud computing.

Section 1:

Privileged Password Management Fundamentals

Privileged user passwords (hereafter, privileged passwords) are distinguished from ordinary end-user passwords in that they uniformly gate access to an organization's most sensitive resources—namely, the administrative accounts (e.g. admin, root, SYS and sa) and associated capabilities used to configure and control an organization's IT infrastructure. Given the risk involved, it's fairly obvious that managing and protecting such credentials is important—a point, by the way, that is validated by the numerous sets of associated requirements codified in commonly invoked security standards and regulations, such as NIST Special Publication 800-53 and the Payment Card Industry Data Security Standard (PCI-DSS).

Regulatory requirements aside, privileged password management is not only a good practice from a risk management perspective, it's also essential to overcoming the litany of insecure practices common in today's organizations. Weak, stale or exposed passwords (e.g., because they are kept on a post-it note or in a spreadsheet), having too many passwords, password sharing, having no clear attribution for shared accounts, having no option for strong authentication and having no option for centralized revocation are just a handful of the issues we routinely encounter.

2015 Verizon Data Breach Investigations Report, 95 percent of breaches could be traced to stolen credentials, while another 10 percent were the result of credential misuse by trusted insiders.[1]

The real problem though is the potential for any of these conditions to lead to successful spear phishing, targeted attacks and ultimately data theft—not to mention compliance violations. Need proof? According to the 2015 Verizon Data Breach Investigations Report, 95 percent of breaches could be traced to stolen credentials, while another 10 percent were the result of credential misuse by trusted insiders.[1] Findings such as these make it abundantly clear why today's organizations need to take advantage of an enterprise-class solution, like CA Privileged Access Manager, for privileged credential management, protection and access control.

The Hybrid Cloud Impact

The traditional issues cataloged above are only the tip of the iceberg. Given the compelling cost, adaptability and responsiveness advantages of hybrid cloud configurations—where IT services and applications utilize both traditional and virtualized infrastructure spanning both enterprise and cloud datacenters—widespread adoption is inevitable. Along with all their benefits, however, hybrid clouds also introduce several new challenges for privileged password management, including:

- Greater volume/scale—as operational demands and the ease of deploying virtual machines result in more entities requiring privileged access (and, therefore, privileged passwords)
- Greater scope—as the concentrated power of virtualization and cloud management consoles add a new type of privileged resource/account into the mix
- Greater dynamism—as new servers/systems can be added on-demand, not to mention in bulk (e.g., 10, 20 or more at a time)
- The potential for creating islands of identity—as each different cloud service has its own identity store and infrastructure[2]

Beyond the challenges presented by the hybrid cloud, IT security managers also need to keep two other aspects of the privileged password management problem in mind when evaluating potential solutions. First, they need to account for the machine-to-machine or application-to- application (A2A) scenario, where passwords used by one system or application for gaining access to another system or application are hard-coded in the accessing application or made available to it in a plain-text configuration file. The second item to consider is the often-overlooked issue that most organizations may also have thousands of keys (e.g., for SSH implementations) that, although they are not traditional, phrase-oriented passwords, still operate as authentication credentials to privileged accounts and, therefore, still require management and protection to reduce associated risks.

The net result is that, in the hybrid cloud era, privileged password management is now more important and complex than ever before.

Section 2:

The Privileged Access Management Solution From CA Technologies

CA Privileged Access Manager is a comprehensive solution for privileged access management. As such, in addition to being able to control access and monitor and record the activities of privileged users across hybrid cloud environments, CA Privileged Access Manager also incorporates capabilities required of a next-generation solution for privileged password management. In fact, it's important for IT security teams to recognize that, although managing and protecting passwords is valuable in its own right, it's also the means to a greater end. In particular it's the initial (or complementary) step in the broader and equally important process of actually controlling and managing access to high-risk resources. If the distinction here seems subtle, it's largely because, in practice, functional implementations of authentication mechanisms (i.e., passwords) and access control rarely involve one without the other, and thus, they are often lumped together in our minds.

In any event, the design objectives for the privileged password management capabilities included within CA Privileged Access Manager are the same as those applied across the remainder of the solution. Specifically, our goal is to deliver a solution that not only provides a comprehensive set of controls and capabilities for a comprehensive set of targets and use cases but that also does so in a manner consistent with cloud-era delivery options, practices and architectures.

Comprehensive Controls

When it comes to evaluating privileged password management solutions, we recommend looking first at whether the solution incorporates a comprehensive set of controls for helping the security team overcome the risks posed by traditional approaches to creating, managing and using sensitive administrative credentials. Specific areas to examine include discovery, vaulting, policy enforcement, retrieval and the ability to support seamless evolution to a full-featured privileged access management implementation.

Section 3:

Top 12 Must-Have Capabilities for Privileged Access Management

#1. Automated/Facilitated Discovery

Without a means for automated or facilitated discovery, the process of bringing privileged passwords under management can be onerous—not to mention fraught with errors or omissions that leave an organization's computing environment vulnerable to today's sophisticated attacks. For this reason, CA Privileged Access Manager includes a variety of methods for discovering devices, systems, applications, services and accounts, including leveraging well-known port associations, directory information, management consoles and APIs. E.g., CA Privileged Access Manager leverages available APIs for supported virtualization and cloud management solutions to alert administrators when new virtual machines are created. In addition, the solution makes it easy to bulk-import system lists from text files, as well as to make ad-hoc entries through the management console. Finally, it's also important to understand that it is "by design" that we have chosen to avoid more disruptive (and potentially riskier) discovery techniques requiring target-based agents that hook or shim the local TCP stack.

#2. Secure Storage/Vaulting

An encrypted vault provides a centralized point of control and is the key to eliminating insecure storage methods (like spreadsheets) that make it easy to share and compromise credentials. The CA Privileged Access Manager vault is credential safe, a FIPS 140-2 Level 1 compliant solution that leverages AES 256-bit encryption to securely store all types of credentials, not just passwords. Additional compelling features of the solution include:

- The option to take advantage of integrated hardware security modules (HSM), such as that from SafeNet and Thales, to field a FIPS 140-2 Level 2 or Level 3 implementation is included. This is particularly important for high-profile, risk adverse clients and use cases, such as those involved with financial and banking systems where it is desired to store the keys used to encrypt credentials separately from the encrypted credentials. Multiple deployment options are supported, including CA Privileged Access Manager hardware appliances with onboard PCI cards, CA Privileged Access Manager virtual appliances making calls to network-attached HSM appliances and CA Privileged Access Manager appliances of either type making calls to an AWS "HSM-as-a-service" offering.
- Proven, white-box cryptographic routines protect encryption keys while they are in use (i.e. in memory) on a system. This approach is designed to prevent hackers from grabbing/piecing together keys by monitoring standard cryptographic APIs and memory and overcoming inferior alternatives based on key chunking or simple obfuscation. The inclusion of this technology is particularly important for A2A use cases where the accessing system must also "vault" credentials and there is greater potential for the system to become compromised (e.g., due to it being in a relatively exposed location).

#3. Automated Policy Enforcement

CA Privileged Access Manager automates the creation, use and change of passwords thereby eliminating the tendency to reuse passwords or rely on passwords that are weak (and easy to remember). With CA Privileged Access Manager, flexible policies can be set to enforce password complexity, implement change requirements—such as rotating passwords based on time (e.g., daily or weekly) or in response to a specific event (e.g., after each use) and govern use (e.g., allowing access only during specified time windows or requiring dual/multiple authorizations for password access). Because these policies can be applied in a hierarchical manner and to groups of target resources, not only can different requirements and capabilities be accommodated for different targets, but their enforcement also effectively becomes dynamic as any resource added to a group automatically inherits the policies for that group. Behind the scenes, CA Privileged Access Manager also interacts directly with affected target resources to provide that all credentials remain synchronized (i.e., when they are changed at one end, they are also changed at the other).

#4. Secure Retrieval and Presentation/Use

Putting privileged credentials into a vault is pointless if they can't also be securely retrieved and used. The first step in this process is accurate authentication of whomever, or whatever in the case of applications and scripts, is looking to access/use a credential. In this regard, CA Privileged Access Manager fully leverages your existing identity infrastructure, with integration to Active Directory and LDAP-compliant directories, as well as authentication systems like RADIUS. Support is also included for:

- Two-factor tokens (e.g., via CA Advanced Authentication or others like from RSA and SafeNet)
- X.509/PKI certificates
- Personal Identity Verification and Common Access Cards (PIV/CAC) necessary for federal sector compliance with HSPD-12 and OMB-11-11 mandates
- SAML
- Composite multi-factor techniques (e.g., combining passwords with RSA tokens)

In the preferred mode of operations, CA Privileged Access Manager subsequently presents the requested credential to the target system on behalf of the accessing entity (e.g., user or application). This approach conveys several additional security benefits. First, in contrast to simple check-in/check-out solutions, credentials are never seen by or distributed to the accessing entity. This greatly reduces their potential for exposure. In addition, because authentication to the target system is completely automated and users never need to handle/ remember their passwords, policies can be implemented to dramatically increase password complexity. Because all access to targets occurs via CA Privileged Access Manager, the solution can also provide full attribution of privileged user activities, even for shared admin accounts.

For the sake of completeness, it's also worth noting that all network communications between accessing entities, CA Privileged Access Manager and managed targets are SSL encrypted. In addition, CA Privileged Access Manager supports an alternate mode of operation whereby accessing entities can directly retrieve and submit required credentials to target systems on their own.

#5. Seamless Transition to Full Privileged Access Management

CA Privileged Access Manager provides organizations originally focused solely on password management with everything they need to transition to a full-featured privileged access management implementation if and when they realize the need to do so. Some of the more notable capabilities at the IT security department's disposal when it's ready to take advantage of them include:

- Granular role-based access control and associated workflows (e.g., for requesting/authorizing additional permissions)
- Automated connection/session establishment with target resources (with support for RDP, SSH, Web and several other access modes/options)
- Real-time monitoring of privileged user sessions, along with policy-based enforcement of allowed/ denied activities (e.g., which commands a specific user can employ)
- Logging, including syslog-based SIEM integration
- Full session recording with DVR-like playback for "jumping" directly to events of interest
- Leapfrog prevention that keeps users from circumventing their permissions by leveraging accessible targets to gain access to other, unauthorized targets

Furthermore, implementing these additional capabilities couldn't be easier. CA Privileged Access Manager delivers all of its privileged password management and access control functionality as one, tightly integrated solution. CA Privileged Access Manager also provides unified policy management across the entire solution, an approach that further simplifies implementation and administration.

Comprehensive Coverage

The second high-level area to evaluate when selecting a solution for privileged password management is the scope of coverage that it provides. In other words, for the comprehensive set of controls identified above, what types of accessing entities, credentials and target systems does the solution actually support?

#6. Comprehensive Coverage for Traditional Targets

CA Privileged Access Manager includes a wide array of target system connectors providing out-of-the-box integration for all types of IT infrastructure, network devices, systems and applications, including:

- Windows® Domain, Local Administrator and Service Accounts
- Popular Linux® and UNIX® distributions
- AS/400
- Cisco and Juniper networking devices
- Telnet/SSH-based systems
- SAP
- Remedy
- ODBC/JDBC databases
- Systems and applications servers

An extensible solution, CA Privileged Access Manager also provides flexible customization capabilities so that organizations can more easily extend support to proprietary and internally developed systems.

#7. Support for Virtualization and Cloud Management Consoles

CA Privileged Access Manager's out-of-the-box coverage for managing and protecting credentials is not limited to traditional targets; it also extends to popular virtualization and cloud solutions, including VMware vSphere, VMware NSX, Amazon Web Services and Microsoft® Online Services. Moreover, the capabilities that apply for these solutions are not limited to the individual instances of associated virtual machines, applications or services. Coverage extends also to the corresponding management consoles, which due to the power they command, must be recognized as privileged resources in their own right.

#8. Support for Machine to Machine Authentication

As alluded to earlier, humans are not the only users of privileged credentials. For most organizations, numerous applications and systems are also enabled to access sensitive resources, such as other applications or databases. This is typically accomplished by embedding associated credentials into the accessing application's code or making it available at run-time via a configuration file—neither of which is a particularly secure or manageable option. CA Privileged Access Manager provides coverage for these A2A use cases by enabling developers to inject a lightweight CA Privileged Access Manager client into their applications. This approach provides "privileged applications" with everything they need to register with CA Privileged Access Manager, dynamically retrieve required passwords and subsequently protect them while in memory on the local system. In addition, multiple mechanisms are available to authenticate the privileged applications and verify their integrity prior to CA Privileged Access Manager releasing requested credentials.

By leveraging CA Privileged Access Manager for A2A scenarios organizations can more effectively eliminate exposed/insecure A2A credentials by vaulting them centrally, automate A2A credential management and policy enforcement and simplify related auditing and compliance activities.

#9. Support for Key Management

In addition to supporting cryptographic operations, many types of keys also serve as tokens to confirm identity. Although such keys are not passwords in the traditional sense, they still operate like passwords and are still subject to similar threats, risks and challenges, such as copying, sharing, unintended exposure and unaudited backdoors. Because such keys are typically embedded or transparently used in solutions to shield users from their relative complexity, they're also more likely to be orphaned and/or proliferate over time. It makes sense, therefore, to apply many of the same controls used to manage and protect passwords to these alternate credentials as well. Indeed, recommended best practices for thwarting related threats include:

- Moving authorized keys to protected locations
- Rotating all keys regularly (to guarantee the eventual termination of access in the event of leaked keys)
- Enforcing source restrictions for authorized keys[3]
- Enforcing command restrictions for authorized keys

Accordingly, CA Privileged Access Manager has controls and other capabilities to account for alternate credential types, including SSH keys and the PEM-encoded keys used to access AWS resources and management consoles. In other words, with CA Privileged Access Manager such credentials can be: (1) vaulted, (2) rotated and controlled by configured policies and (3) retrieved and used in a manner that minimizes the potential for their theft or exposure.

Cloud-Era Delivery

In the hybrid cloud era, another major gating factor for the success of a privileged password management solution is how well it “fits in” not only physically but also in terms of aligning with cloud networking needs and capabilities.

#10. On-Premises, Virtual Machine and Cloud-Based Delivery Options

CA Privileged Access Manager supports three convenient deployment options that help organizations to keep pace with complex hybrid-cloud architectures:

- A hardened physical appliance—available in multiple models for traditional rack-mounting in the enterprise data center
- An Amazon Machine Instance (AMI)—pre-configured for deployment with the Amazon EC2 infrastructure
- An OVF-compliant virtual appliance—ready-made and pre-configured for deployment in VMware environments

Regardless of the deployment option(s) used, organizations obtain a solution that enables management of their entire hybrid cloud infrastructure.

#11. Cloud-Aligned Architecture and Approach

CA Privileged Access Manager is purposely architected to incorporate numerous features that make it a “good citizen” in hybrid cloud environments. Three examples include the following:

- Auto-Discovery and Protection—In hybrid cloud environments, operators can create (or retire) any number of systems with a single command. CA Privileged Access Manager accounts for this situation by leveraging applicable APIs to automatically discover virtualized and cloud resources and then provision (or de- provision) appropriate credential and access management policies.
- Avoiding Islands of Identity (i.e., Identity Federation)—One way that CA Privileged Access Manager eliminates separate islands of identity information is by fully leveraging whatever identity infrastructure an organization already has in place. Another way, specific to AWS implementations, is by supporting ephemeral users—an approach that keeps organizations from having to maintain separate identity information in the AWS Identity and Access Management sub-system.
- Enabling Automation—A comprehensive API allows programmatic access to and automation of all CA Privileged Access Manager functionality (e.g., by external management and orchestration systems).

#12. Cloud-Ready Scalability and Reliability

Privileged credential management is a critical element of an organization’s IT infrastructure. This is doubly true when the implementation is extended to support A2A use cases, which operate in a fully automated manner. To this end, CA Privileged Access Manager includes native clustering and load distribution functionality capable of meeting the high availability and scalability requirements of the largest and most demanding environments. Compared to common alternatives, with CA Privileged Access Manager there is no need to invest in separate, external load balancers, no performance delays typical of active-passive approaches and no need to license additional “optional” features. If desired, and operationally acceptable from a latency perspective, CA Privileged Access Manager clusters can even be configured to enable redundancy across geographically dispersed data centers and cloud environments.

CA Privileged Access Manager delivers a next-generation solution for privileged credential management designed to drive security risk reduction and improve operational efficiency across the hybrid enterprise infrastructure.

Section 4:

Conclusion: Conquering Privileged Credential Management in the Cloud Era

Managing and protecting privileged credentials is essential to reducing risk and achieving compliance with related regulatory requirements. It's also a problem that is growing in complexity and significance, as hybrid cloud environments introduce management consoles with unprecedented power and the ability to add/remove literally hundreds of target systems with nothing more than a handful of mouse clicks.

Organizations looking to address this critically important area of their information security strategy need to evaluate candidate solutions for the depth of controls, scope of coverage and degree of cloud alignment they provide. As discussed herein, CA Privileged Access Manager delivers against all three of these dimensions to provide today's organizations with precisely what they need: a next-generation solution for privileged credential management designed to drive IT risk reduction, improve operational efficiency and protect their investment by supporting traditional, virtualized and hybrid-cloud infrastructure alike.

ca technologies

Connect with CA Technologies at ca.com

CA Technologies (NASDAQ: CA) creates software that fuels transformation for companies and enables them to seize the opportunities of the application economy. Software is at the heart of every business, in every industry. From planning to development to management and security, CA is working with companies worldwide to change the way we live, transact and communicate – across mobile, private and public cloud, distributed and mainframe environments. Learn more at ca.com.

[1] 2015 Verizon Data Breach Investigations Report

[2] *"New Platforms, New Requirements. Privileged Identity Management for the Hybrid Cloud"*, CA White Paper, March 2013

[3] *"Managing SSH Keys for Automated Access - Current Recommended Practice"*, IETF Draft, April 2013

Copyright placeholder: Please copy from the Word document and paste here.