

PRODUCT SHEET:
CA Virtual Privilege Manager

CA Virtual Privilege Manager

secure privileged access to the virtual environment



CA Virtual Privilege Manager provides broad capabilities to secure privileged access to the virtual environment—helping organizations expand virtualization enterprise-wide.

Business need

Server virtualization promotes flexible utilization of IT resources, reduced capital costs, high-energy efficiency, highly-available applications, and improved business continuity. However, virtualization brings along with it a unique set of challenges around the management and security of the virtual infrastructure, especially privileged user management. Privileged users enjoy much more leverage in the virtual environment as they have access to all the virtual machines running on a host—hence tight control of privileged user entitlements is essential. A broad range of capabilities to secure the virtual environment are necessary for organizations to prevent virtual-stall, expand virtualization enterprise-wide, and reap the benefits promised by this emerging technology.

Product overview

CA Virtual Privilege Manager secures privileged user access to virtual machines, hypervisor service consoles, and virtual appliances—helping organizations control privileged user actions, secure access to the virtual environment, and comply with industry mandates. It delivers key capabilities to manage privileged user passwords, harden the hypervisor service console, and monitor privileged user activity. CA Virtual Privilege Manager also provides a centralized foundation for privileged user management that serves as a single portal for securing privileged user access across virtual and physical environments.

CA Technologies advantage

Virtualization technology adopts many concepts from the mainframe world. With product offerings like CA ACF2, CA Top Secret and CA Access Control, CA Technologies has a long history in providing robust security for the mainframe and distributed environments. To meet the needs of its customers, CA Technologies now introduces CA Virtual Privilege Manager – a scalable and extensible product that secures access to the virtual environment.

CA Virtual Privilege Manager provides a proactive approach to securing sensitive information and critical systems without impacting normal business and IT activities. It helps to mitigate both internal and external risk by controlling how business or privileged users access and use enterprise data. This can result in a higher level of security, lower administrative costs, easier audit/compliance processes and a better user experience.

CA Virtual Privilege Manager, in addition to securing virtual environments, provides heterogeneous platform support, a centralized foundation for privileged user management, and an on-ramp to an enterprise-wide Access Control suite that spans beyond the virtual environment and includes support for applications, databases, and infrastructure components in the physical environment.

Key capabilities

CA Virtual Privilege Manager is capable of centrally controlling and auditing privileged users and providing temporary privileged access across virtual and physical servers, applications and devices—all from a single, central management console. Key Capabilities of the product include:

Privileged-user password management

Privileged users have extensive access to critical IT resources, but even they can make mistakes. CA Virtual Privilege Manager provides secure access to privileged accounts and helps maintain the accountability of privileged users. It enables the issuance of passwords on a temporary, one-time use basis, or as necessary, while providing accountability of privileged user actions through secure auditing. A simple workflow for requesting and checking out a system-generated, one-time use password facilitates password checkout. Users can check in the password once their task is completed, or CA Virtual Privilege Manager can be configured to automatically check in the password after a specific time period.

CA Virtual Privilege Manager comes with fully functional and customizable workflows that enable common out-of-the-box use cases—examples include break glass and password request scenarios. A break glass scenario occurs when privileged users need immediate access to accounts that they are not authorized to manage. It allows users to obtain an account password immediately without approval, eliminating the possibility of delay in case of emergency, but securely logs all transactions for audit purposes. In contrast, a password request scenario allows the organization to only authorize passwords per request for a limited period of time. In this scenario, user requests go to their managers for approval, and can include a time-period required for accessing the account. Once the request is approved, users can check out the password and have access to the requested systems only for the approved time period.

CA Virtual Privilege Manager is designed to provide third-party applications with programmatic access to passwords—removing the need to hard code passwords in scripts. It supports a multitude of servers, applications (including databases) and devices in a physical or virtual environment. CA Virtual Privilege Manager also features a ‘Discover Privileged Accounts’ wizard, and a feed that allows target systems and privileged accounts to be automatically fed into the system.

Service console hardening

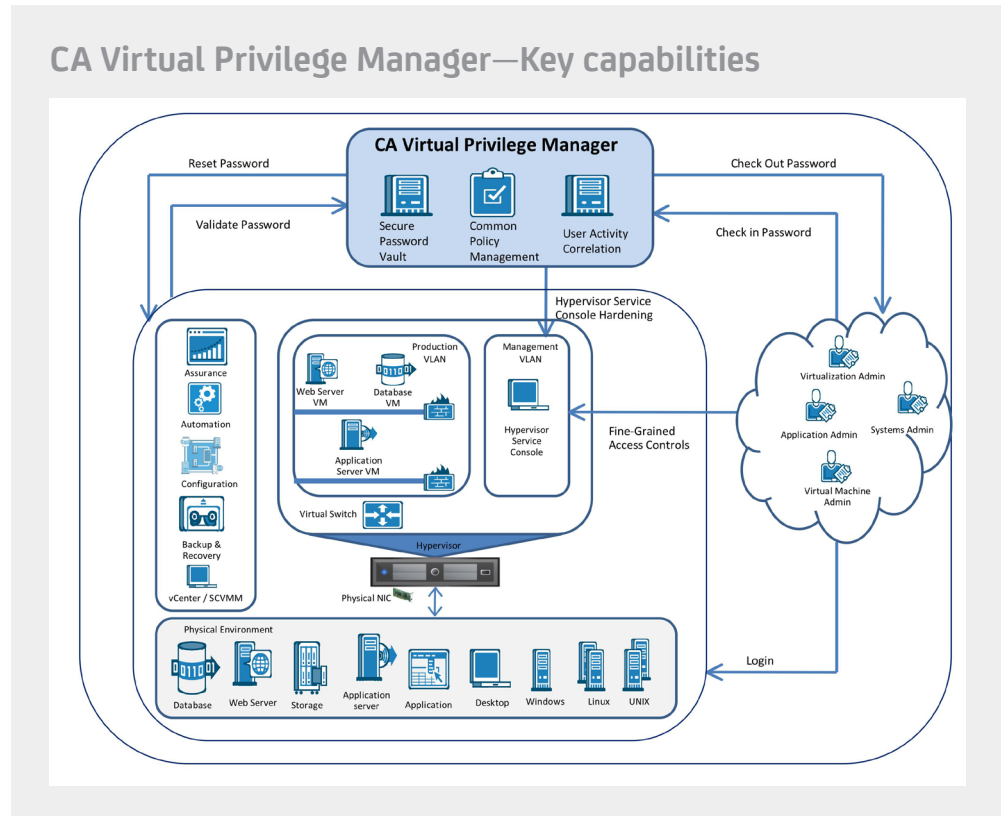
CA Virtual Privilege Manager provides a broad range of capabilities to harden the hypervisor service console. It controls access to the system resources, programs, files, and processes through a stringent series of criterion that includes time, login method, network attributes and access program. These controls are essential to enforce industry-standard Segregation of Duties (SoD) rules on the hypervisor service console. For example, the CA Virtual Privilege Manager can prevent the virtualization administrator from accessing virtual machine configurations via the service console—thus forcing all virtualization environment changes to be governed through the management consoles.

CA Access Control Premium Edition allows you to extend hardening capabilities to virtual machines, virtual appliances, and the physical environment – enabling consistent enforcement of security policies across physical and virtual environments.

User activity monitoring

CA Virtual Privilege Manager audits activity performed on the hypervisor service console, and keeps track of privileged account usage based on the original user. In addition, the designed integration with CA Enterprise Log Manager allows customers to extend auditing capabilities beyond CA Virtual Privilege Manager events – thus providing a holistic view of privileged activity performed in the IT environment.

Figure 1



Comprehensive reporting

Policy-based reports provide proactive views of who has access to what in the virtual environment. CA Virtual Privilege Manager provides detailed reports on User & Group Entitlements— reporting on usage of privileged accounts and privileged user entitlements across multiple hypervisor service consoles. Interoperability with external systems allows customers to run policy reports through the reporting tool of their choice, create new reports based on a published schema, and customize report layouts to satisfy internal standards or auditor requests.

Common policy management

CA Virtual Privilege Manager is designed to streamline the management of privileged user entitlements. It centralizes management policies that govern access to virtual servers across a large and heterogeneous virtual environment. The governing criterion includes access to the hypervisor service consoles, resources within the virtual environment, network access to and from the consoles, access to virtual machine configuration, etc. These policy management capabilities help clarify complex, cross-platform policy environments and simplify administrative tasks—providing a reliable common policy management process.

Delivery approach

CA Services provides CA Virtual Privilege Manager Rapid Implementation services delivered through CA internal staff and a network of established partners chosen to help customers achieve a successful deployment and get the desired business results as quickly as possible. Through our proven nine-stage methodology, best practices and expertise, we help customers achieve a faster Time-to-Value for their CA Virtual Privilege Manager implementation.

Why CA Technologies

Heterogeneous platform support

Although VMware has a large market share among hypervisor vendors, many key analysts predict its market share to reduce significantly moving forward due to competitive offerings from other vendors in this maturing market - this necessitates broad platform support in virtualization management products. CA Virtual Privilege Manager is designed to raise the level of control consistently across multiple virtualization platforms including VMware ESX, Microsoft Hypver-V, Solaris 10 Zones and LDOMs, Linux XEN, IBM AIX LPAR, HP-UX VPAR, Mainframe x/VM, and IBM VIO.

Rapid time-to-value (TTV)

CA Virtual Privilege Manager is part of the CA Virtual suite of products that are quick to deploy with extensive OOTB support, and easy-to-use with modern administrative interfaces and reporting dashboards – hence deliver a rapid TTV for customers. Other products in the CA Virtual suite include CA Virtual Assurance, CA Virtual Automation, and CA Virtual Configuration.

On-ramp to enterprise solutions

The CA Virtual Privilege Manager not only helps secure virtual-only deployments, but also provides an on-ramp to enterprise class solutions for securing virtual and physical environments - protecting virtualization security investments in the long run.