PRODUCT SHEET:
CA Access Control

CA Access Control

we can

ca technologies

A US federal security agency terminated a privileged user but allowed him access to privileged systems for an additional two weeks. In that timeframe, the privileged user allegedly placed malware on a database server in an attempt to cause damage to the computer and database. Almost every organization is susceptible to this same risk. If the agency had immediately revoked the privileged user's credentials, it might have prevented his ability to access the computer and database. But sometimes even that is not sufficient; an organization also has to rigidly control what a properly authorized privileged user can (and cannot) do once they have access to a privileged system.

Overview

CA Access Control is designed to provide a robust solution for privileged user management, protecting servers, applications, and devices across platforms and operating systems. It provides a proactive approach to securing sensitive information and critical systems without impacting normal business and IT activities. CA Access Control helps to mitigate both internal and external risk by controlling how business or privileged users access and use enterprise data. This generally results in a higher level of security, a lower level of administrative costs, easier audit/compliance processes, and a better user experience.

Benefits

By combining host access control with privileged user management, CA Access Control can help reduce the risk and cost of managing privileged users. Access Control is designed to help your organization:

- Provide more powerful control (such as accountability and separation of duties) of privileged users over how they access and use enterprise data

- Reduce the cost of UNIX®/Linux account management by authenticating your users to Microsoft® Active Directory and provide single sign-on capabilities to streamline their administrative activity
- Reduce administrative cost and complexity by automating the password changes of Windows Services, Windows Scheduled Tasks, and Windows Run As service without installing agents
- Improve security and efficiency by controlling application IDs used for database connections from application scripts, web pages, and data source definitions for ODBC, OLEDB, OCI, and JDBC without the need to change the applications
- Enhance security with an automatic login feature by preventing "over the shoulder" password theft, which also helps eliminate the need to cut and paste passwords
- Facilitate audits via UNIX keyboard logging and enable VCR-type functionality for recording and playback of privileged user sessions via integration with third-party software
- Address regulatory compliance by proactively reporting on the status of key compliance policies
- Generate privileged user reports from secure activity logs in minutes, not days

A single central management console

CA Access Control r12.5 is capable of centrally controlling and auditing privileged users and providing temporary privileged access across servers, applications, and devices—all from a single, central management console. This unified console provides a single, Web user interface that consolidates all aspects of privileged user management under one console, including host access control and privileged user management across physical and virtual systems, devices, and applications.

Key capabilities

- **Fine-grained controls** CA Access Control provides access controls on all common operating systems. It is designed to control access to system resources, programs, files and processes through a stringent series of criteria: time, login method, network attributes, and access program. These controls are required in order to enforce separation of administrative duties on the servers, consistent with industry best practices; for example, separating system administration from application administration or virtualization administration, providing controlled rights to developers or support personnel, etc.

- **Privileged user password management (PUPM)** Even privileged users can make mistakes. By carefully segregating their duties and securely protecting the recording of their activities, organizations can protect against a privileged user making a mistake or committing a malicious act. PUPM provides secure access to privileged accounts and helps provide the accountability of privileged access through the issuance of passwords on a temporary, one-time use basis, or as necessary while providing user accountability of their actions through secure auditing.

  The automatic login feature streamlines and secures the process by allowing a user to request a password and utilize it with a click of a button by automatically logging the user to the target system as the privileged user, all while not seeing the actual password. This prevents "over-the-shoulder" password theft and speeds up the process for the password requestor. If the target system is a server protected by Access Control, the original identity of the user is propogated to AC to allow auditing the original user and providing additional segregation of duties. The session can be recorded leveraging integration with third party session recording software for additional security.

  PUPM is also designed to allow applications to programmatically access system passwords and, in so doing, remove hard coded passwords from scripts which are a potential security risk and allow to automatically reset application ID passwords. PUPM can manage service accounts used by an IIS or J2EE application server, and the applications hosted by them by intercepting ODBC and JDBC connections and replacing them with the current credentials of privileged accounts. In most cases, PUPM provides this functionality without requiring any changes to the applications.

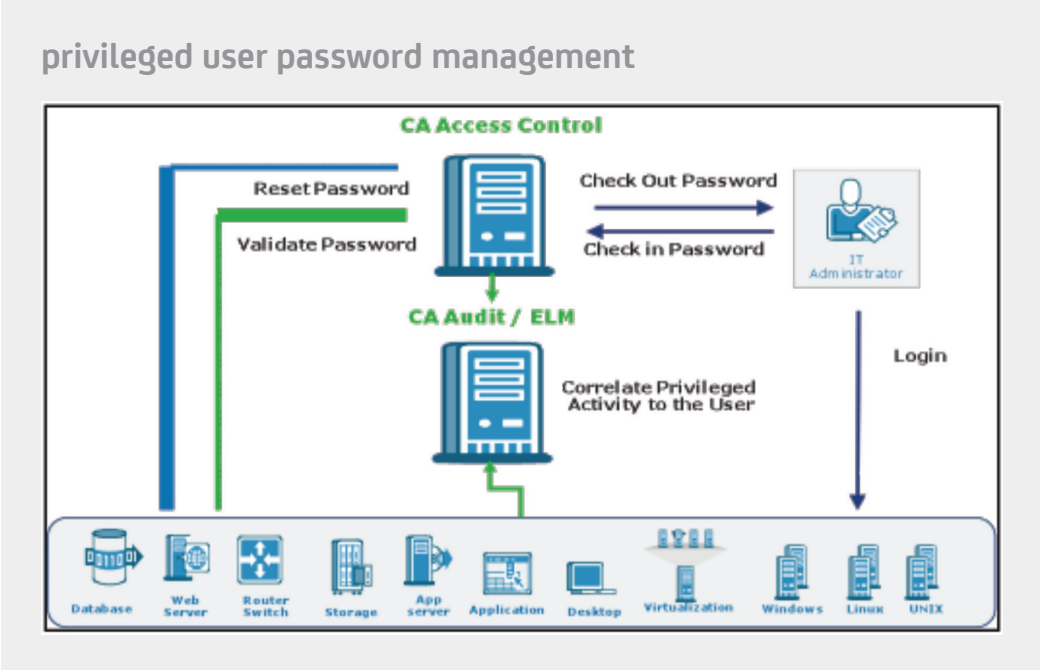
  PUPM also automates the management of service account passwords that would otherwise be manual (Windows Services), manages passwords used by Windows scheduled tasks that require login to the system (Windows Scheduled Tasks), and integrates with the Windows Run As mechanism to retrieve the password of the relevant privileged user from PUPM. PUPM features a 'Discover Privileged Accounts' wizard as well as a feed that allows target systems and privileged accounts to be automatically fed into the system.

Privileged access auditing and reporting CA Access Control is designed to audit the activities performed by privilged users and track their actions based on their original, unique user ID. All audit information is securely logged in a central location and rich interactive investigative reports on user activity can be viewed from the CA Access Control Enterprise Management Console.

Keyboard logging on UNIX and integration with privileged user session recording and playback software facilitate post-incident audits. The designed integration with CA Enterprise Log Manager allows you to more easily extend the auditing capabilities beyond CA Access Control Events to provide a holistic view of privileged activity performed in the IT environment. (A limited-use ELM license is included with AC for reporting on AC events only; the full Enterprise Log Manager product is separately licensed.)

Compliance policies are provided as an Out-of-the-Box (OOTB) policy object in the Enterprise Manager. A PCI compliance pack is also provided to help speed the generation and submission of PCI reports.

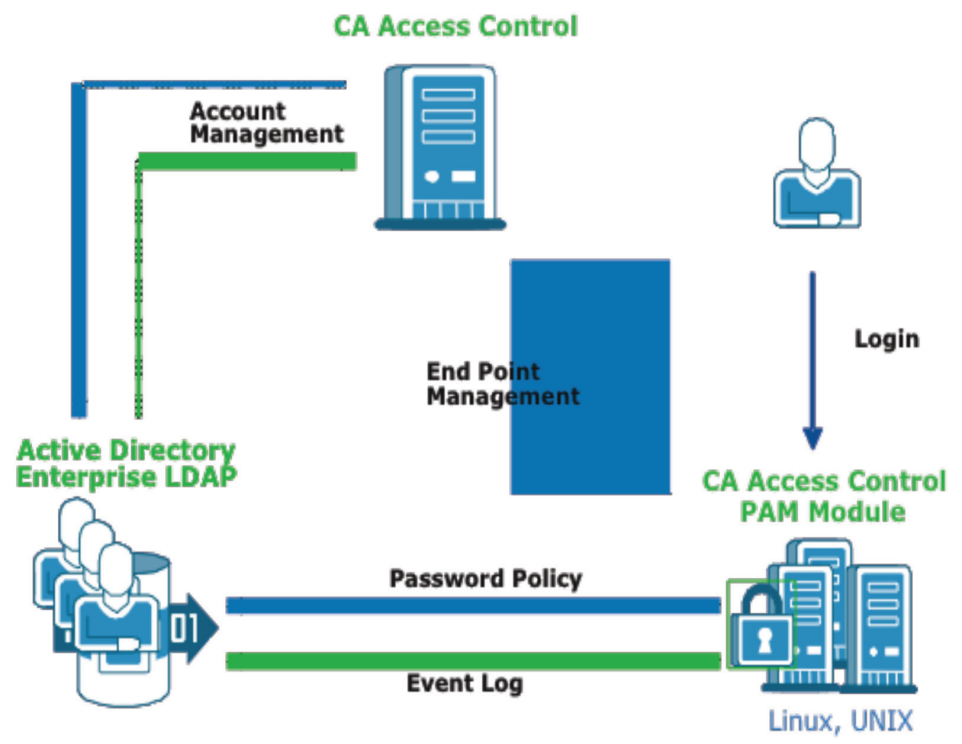
Figure A



- **UNIX authentication broker (UNAB)** Authenticating UNIX/Linux users typically means maintaining records separate from Windows users. This complicates password synchronization and can get in the way of quickly de-provisioning privileged users by adding time or errors. UNAB allows the management of UNIX users in Microsoft Active Directory (AD), which allows the consolidation of authentication and account information in the single enterprise AD user store as opposed to maintaining credentials on various UNIX/Linux systems. UNAB enables Single Sign-On from Windows to UNIX and from UNIX to UNIX systems through any standard Kerberos-enabled application.

Figure B

UNIX Authentication Broker



- **Dynamic policy management and automated distribution** CA Access Control is designed to streamline policy deployment and management by helping administrators to construct logical policy sets and deployment rules. Hosts can be associated to multiple logical host groups based on their characteristics, such as operating system, server type, or application. Thus when a new policy is added to a set it is automatically deployed to the appropriate hosts. From a single, unified console, policy versions are maintained, changes are tracked and deviations from the policies are reported. This helps clarify complex, cross-platform policy environments and simplify administrative tasks while also providing a compliant and accountable policy management process.
- **Broad platform coverage** The diversity of server platforms, operating systems and applications across your enterprise each represent a potential vulnerability; your infrastructure is only as strong as the weakest link. CA Access Control is designed to raise the level of controls consistently across multiple supported platforms and helps to protect distributed servers, with a variety of operating systems—including Linux, UNIX and Windows—supported.
-

- **Broad virtualization support** Organizations leverage virtualization to consolidate servers and lower total cost of ownership. Visualization technologies introduce new risks associated with virtualization platform system administration. CA Access Control is designed to support a wide range of virtualization platforms including: VMware ESX, Solaris 10 Zones and LDOMs, Microsoft Hyper-v, IBM VIO and AIX LPAR, HP-UX VPAR, Linux Xen, and Mainframe x/VM, providing for more consistent security management of access control risks across these virtual partitions.
- **Entitlements reporting** Policy-based reports provide proactive views of who has access to what across your distributed and virtual server environment. These reports rely on the effective policy being enforced and allow you to quickly and easily generate reports required by your auditors, such as User and Group Entitlement Reports, Policy Compliance Reports, Orphan Account Reports and more. These proactive reports complement existing event-based auditing by allowing you to monitor compliance requirements and highlight existing discrepancies before incidents occur. By exporting log data in industry-standard formats you are able to run policy reports through the reporting tool of your choice, create new reports based on a published schema, and customize report layouts to satisfy internal standards or auditor requests.
- **Integration with other CA Technologies solutions** Seamless integration with other CA Security Management solutions such as CA Identity Manager provides benefits such as rapid provisioning and de-provisioning. When combined with CA Role and Compliance Manager, AC can leverage the RCM role and group definitions and assign privileged user access rights automatically. AC will also quickly respond to role/group changes in RCM. Integration with CA Service Desk allows the addition of detailed service desk ticket information in both the privileged account request and break glass task forms, while allowing an approver to view the ticket for more information. CA Spectrum® Automation integration enables application of specific policies when resources like virtual machines are detected coming online, thus preventing the execution of a production application by mistake, before it is ready for release.

The CA Technologies advantage

CA Technologies is a recognized market leader in UNIX host access control. CA Technologies provides a comprehensive solution for many aspects of privileged user management in one product and one console. CA Access Control is part of the proven Data and Resource Protection solution from CA Technologies that helps you control your privileged users across multiple platforms and environments. By controlling your privileged users, IT is better able to reduce risk of compliance failure and increase efficiencies.

CA Services provides rapid implementation services for CA Access Control delivered through CA Technologies internal staff and a network of established partners chosen to help you 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 can help you achieve faster time-to-value for your CA Access Control implementation.

2587_0810