

UNIX Host Access Management with CA Access Control

Table of Contents

Executive Summary

SECTION 1 2

Today's Security Management Environment

SECTION 2 2

Robust Host Access Control

SECTION 3 6

Policy Management

SECTION 4 10

Secure Auditing

SECTION 5 12

Cross-platform Host Protection

SECTION 6 13

**CA Access Control — Part of a Bigger Identity
and Access Management Solution**

SECTION 7: CONCLUSIONS 14

Executive Summary

Challenge

Mandatory compliance requirements and pressure to prevent information leaks are driving companies to take action to protect their sensitive electronic assets against both external and internal threats. In addition, the challenge to ensure accountability across all levels of business operation while keeping costs down and increasing efficiency leaves little room for error. Open systems often serve as the backbone for key services and confidential data stores. Many critical applications and sensitive data, including customer information and financial data, are hosted on UNIX and now increasingly adopted Linux systems.

UNIX and Linux systems have inherent security issues that pose high risk to the business objectives of complying with regulations and data protection. Each system includes over-privileged accounts that can compromise vital system resources including sensitive files, critical services and vulnerable network ports. An inability to address segregation of duties often results in these accounts being shared without proper accountability.

Opportunity

In a large server environment, consistent enforcement of security policies across servers and platforms is essential. A single set of strong access controls that is enforceable across disparate platforms is needed to neutralize platform differences. Elevating protection in this manner reduces the cost of management and increases accountability.

Event auditing is essential for compliance reporting as well as security information management for a company. Of specific importance is ensuring that true user identity has been recorded despite various account privileges that a person might have assumed. In native UNIX and Linux systems, if a user performs a surrogate command, particularly to a shared privileged account, the traceability of user activities ends, leading to accountability gaps.

Benefits

CA Access Control can provide you with full superuser containment to greatly reduce security risks exposed by native privileged accounts. It enforces strict access control to critical system resources through centralized and automated policy management consistently across all common platforms. CA Access Control provides pluggable authentication module support, high password quality policies, stringent authorization enforcement, as well as secure auditing that preserves original user identity for all system activities. This enables companies to reduce security risks, particularly from internal unauthorized access, and fulfills compliance requirements through high integrity auditing and reporting.

SECTION 1

Today's Security Management Environment

Today's server environment typically supports a mix of business critical applications hosting corporate, customer and partner data. Maintaining these servers requires many "hands" using tools and the combined efforts of multiple administrators. Native UNIX security often lacks the ability to appropriately segregate administrative duties or trace actions back to a real person. Undelegated administrative roles allow even the least skilled to have access to the most powerful — and potentially dangerous — management tools.

Managing a mixed combination of UNIX servers further complicates the challenge of enterprise-wide system access management. Each UNIX operating system has its own distinct set of native security policy tools, access control structures and administration procedures. If each system is managed separately, inconsistent policy enforcement and unnecessary overhead can result from incompatible security models of each operating system. Compliance adds to the burden of the security administrators that need to ensure policy enforcement and generate reports from all managed systems. Enterprise-wide host access management solutions are key investments to protect critical data, fulfill compliance needs and enable cost-effective administration.

SECTION 2

Robust Host Access Control

Maintaining an enterprise's servers often requires many types of administrators. Among them are specialists in networking, database, email, applications and backup, all requiring various levels of access. UNIX systems have an all-powerful administrative superuser account, "root", that has the ability to run any program, modify any file or stop any running process, often anonymously. In practice, this account password is commonly shared amongst many administrators, each of whom requires only a subset of its permissions to perform their job responsibilities. This presents a significant security risk and an accountability gap. A core element to effective server resource protection is to fully contain such accounts while delegating necessary privileges so personnel can effectively perform their job function.

Superuser privilege delegation products providing password-controlled superuser account access or sudo replacement can still be bypassed and expose the superuser account. This leads to a false sense of security. The unique design of CA Access Control allows it to become a virtual part of the operating system. CA Access Control operates at the system level to monitor and control all critical system level access and supports an integrated host security management environment. In addition, CA Access Control daemons are self-protecting against malicious attacks, ensuring system security at all times.

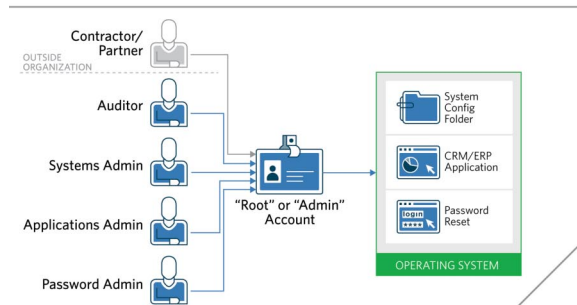
FIGURE A

Separate administrators require distinct privileges.

SEGREGATION OF DUTIES

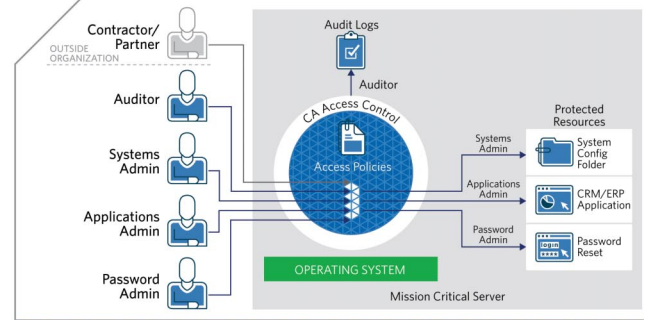
BEFORE

Unsecure Server Environment



AFTER

Secure Server Environment



Superuser Containment

The root account is a significant source of vulnerability because it allows applications or users to assume a more powerful level of privilege than needed. The superuser account is always a target for hackers and Trojan applications as gaining access to this account gives outsiders access to anything in the system.

CA Access Control inspects all relevant incoming requests at the system level, and enforces authorization based on the defined rules and policies. Not even the privileged root account can bypass this level of control. Through CA Access Control, all privileged users become managed users and are accountable for their activities on the system. At the same time, it greatly reduces system security risks by removing the single point of failure inherent to the superuser.

Role-based Access Control

Non-administrative accounts can have limited authorization to perform administrative duties such as database application maintenance. This limits the practice of sharing the superuser password and all its privileges. By default, CA Access Control provides popular administrative and auditing roles that can be customized and expanded, for example:

- Auditor User can assign audit attributes and display user and user group characteristics.
- Operator User can display user and user group characteristics.
- Password Manager User can change the passwords of other users.

Fine-grained Enforcement

UNIX systems lack the granularity to effectively delegate certain system administration rights to less powerful user accounts. Without proper privilege delegation, the same, powerful superuser account is shared amongst administrators for operations that may not require total system control. This greatly compromises access accountability. CA Access Control provides fine-grained enforcement and regulates access based on many criteria including network attributes, time of day, calendar or access program.

Flexible Access Control Lists

UNIX provides a basic access control list (ACL) model, which is usually insufficient for today's complex access requirements. CA Access Control adds many ACL capabilities to enhance the security administrator's ability to properly assign access rights to authorized users.

CONDITIONAL ACCESS CONTROL LIST (CAACL) Enforces user access based on the various criteria such as default access mode or time and date, across a wide list of system resources including file, directory, TCP traffic and network ports.

PROGRAM ACCESS CONTROL LIST (PAACL) OR PROGRAM PATHING At times, users should never have access rights to certain data files, such as RDBMS database files, except using approved programs. CA Access Control can enforce user access only through certain designated programs, denying any other programs or methods of access to ensure strict security.

NEGATIVE ACCESS CONTROL LIST (NAACL) A NAACL lists specific access rights that should be denied to a system resource. This model provides the added power to block certain users and group access without creating complex ACLs.

Login Control

Every access to a UNIX system begins with the login process. Traditional UNIX systems have a simplistic view towards login and lack the ability to incorporate situational security context into the process. Merely present the correct username and password and you are inside the network without consideration to the source of the login request, login program type, time of the login or concurrent login instances.

CA Access Control can enhance login security by limiting user login by originating terminal ID, type of login program or time of the day. CA Access Control can also limit the concurrent login sessions of a user to enforce stringent user access to a terminal. Grace login features can automatically suspend a user after too many failed login attempts, protecting systems against repetitive hackings. Additionally, CA Access Control provides secure suspension and revocation of user accounts in distributed environments. This flexible set of login controls provides the enterprise with enhanced protection from hackers and unauthorized access.

Surrogate Access Accountability

UNIX provides the "su" command for a substitute user — a common practice, especially for superuser accounts. However, this can be dangerous for inexperienced users or those with the wrong intentions. Perhaps worst of all, the user's identity is lost after surrogate actions which lead to a severe lack of accountability in a shared account environment.

CA Access Control preserves the original user ID even after surrogate actions, ensuring user access records in audit logs show the original account. This allows users to login using their own ID and safely surrogate to the privileged accounts without loss of accountability.

Network-based Access Control

Today's open environments require strong control over user access and information flowing over the network. Network-based access control adds another layer of protection to regulate access to the network. CA Access Control can manage access to network ports or network access programs and network security policies can manage bi-directional access by terminal ID, hostname, network address, segments or other attributes. By limiting outgoing connections within the network based on the user's identity, CA Access Control minimizes the risk of allowing external access through a firewall. Legitimate Internet visitors can also be confined to a specific set of services and systems within the network. For example, an organization might choose to allow external contractors into specific servers via VPN but restrict them from propagating to additional servers on the network.

Secure UNIX Kernel Module Load and Unload

CA Access Control can enforce the authority to load and unload kernel modules. This can limit the ability of system administrators from leveraging their root access to load dangerous kernel level devices, such as debug tools or network sniffers that may be used for malicious activity or inadvertently expose the systems.

User-defined Classes

CA Access Control provides the ability to define custom enforcement classes to control business functions beyond existing CA Access Control objects. For example, fund transfers in a bank can be defined as a class, and various controls can be applied to a transfer based on the access authorization with business applications using CA Access Control Application Programming Interfaces (APIs).

Trusted Program Execution

Applications with SETUID capability are commonly used in UNIX systems. Because a SETUID program can assume superuser functions, enforcing appropriate access rights on these applications is vital to system integrity. CA Access Control can tag specific applications, programs or files with unique signatures, designating that they can be safely executed or accessed. If the contents of these executables or files are compromised, failure to have a matching signature will lead CA Access Control to block the execution of the application.

Stack Overflow Protection (STOP) and Trojan Horse Prevention

External threats that compromise critical services or damage the integrity of executables are a high risk factor in protecting production servers. These threats include worms that exploit program memory stack overflows or Trojan Horse attacks on normal executable programs.

CA Access Control's STOP function can stop these malware attacks and prevent spreading of viruses to other servers on the network. Through the trusted file execution function, Trojan Horse-injected executables will be labeled as untrusted and execution will be blocked, preventing potential malware damages. By restricting use of relative PATH, CA Access Control also reduces the possibility of Trojan Horse programs being executed.

Application APIs, Exits and Scripting

CA Access Control provides an open and secure interface through a Software Development Kit (SDK) for external application integration. The SDK provides various functional APIs for different purposes:

AUTHORIZATION AND AUTHENTICATION APIS Provide policy decision information to third-party applications about whether a user can access a resource or not. This also provides an avenue to integrate external application authorization policies with CA Access Control system access policies.

EXITS APIS Allow additional applications to be executed during CA Access Control operations in a safe and secure manner. This allows CA Access Control capabilities to perform custom operations to be integrated with other applications.

AUDIT LOGGING APIS Additional alerts can be added through the LogRoute API calls into audit logs. They also provide the necessary functions to external security information management applications to integrate CA Access Control logs as a log source.

Additionally, controlled custom exits can be added to normal CA Access Control operations to perform additional functions that interact with external user sources or alerting administrative parties of certain operations.

Performance Considerations

System response time for security checks is a critical factor when considering a host security solution. CA Access Control includes many tunable performance components to minimize system resource consumption. Extensive caching mechanisms are available including multi-kernel extension, resource and network caches. In the majority of cases, the performance implication of CA Access Control is negligible.

SECTION 3

Policy Management

Security policies govern who can access what resource or perform a certain function. By defining administrative roles and corresponding privileges, policies can efficiently maintain the appropriate permissions. UNIX operating systems force security administrators to manage policies independently and lack the desired level of flexibility. The cost of maintaining one-off security scripts accumulates quickly as different environments and business requirements grow.

CA Access Control Policy Management supports the ability to define, store and propagate security management data across the network. Policy Management provides centralized administration which enables the management of large numbers of servers from a single location. In a diverse environment, automating policy management processes and managing them centrally can greatly reduce management costs and effort.

CA Access Control has a small system footprint but provides flexible rule definition and policy management. It is ideal for phased deployment, as it provides immediate benefits to localized deployments, but can scale to larger networks of servers as a standard configuration component.

Centralized and Remote Administration

CA Access Control enables security administration of endpoint systems from a central location using a standard, lightweight Web-based user interface. This can greatly reduce administration costs and strengthen security by restricting administration to only authorized system terminals.

Advanced Policy Management Architecture*

CA Access Control's enterprise-class scalability results from a distributed model of distributing policies to all managed servers. This Advanced Policy Distribution Architecture uses a central Deployment Map Server (DMS) and Distribution Hosts (DH) to distribute policy deployments to endpoints, and send back deployment information from the endpoints to the DMS. This infrastructure is decoupled from the logical assignment of the policies and is easy to set up, extend, and configure for high availability, failover and disaster recovery.

CA Access Control supports running the DH in a clustered environment (server farms), which increases the number of endpoints nodes that can be supported. The policy architecture relies on the following server components:

ENTERPRISE MANAGEMENT USER INTERFACE Lets you perform advanced policy management, while providing an integrated view of your entire CA Access Control environment of servers. The Web-based interface also allows you to manage individual endpoints or Policy Models. The user interface is consistent across all CA Identity & Access Management offerings utilizing the common CA framework for look and feel and administrative scoping and task delegation.

DEPLOYMENT MAP SERVER Sits at the core of advanced policy management. The purpose of the DMS is to store policy management data. You manage a single database (the DMS), which then sends events to distribution hosts.

DISTRIBUTION HOST Is responsible for distributing policy deployments, made on the DMS, to endpoints, and for receiving deployment status from endpoints to send to the DMS.

Modeled after the time-tested model of anti-virus signature distribution, CA Access Control endpoint agents check regularly for new deployments on the DH, and download and apply these as necessary. Execution results are then sent back to the DH, which sends them to the DMS for centralized auditing. Also, a heartbeat lets the DMS (through a DH) know that the endpoint agent is operational and the host is running.

*Some features listed are only available in CA Access Control Premium Edition

Built for Reliability

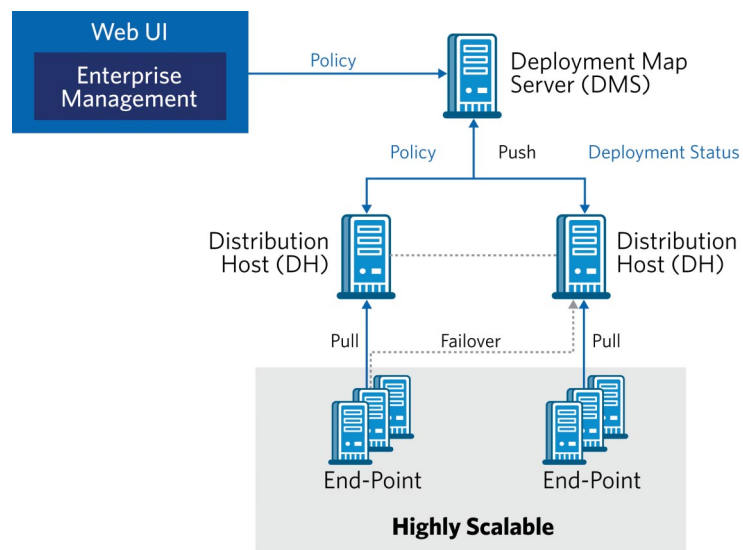
A key compliance requirement is the knowledge that all managed servers are protected and applicable security policies are continuously in effect. In the event of network connectivity issues or system unavailability during policy updates, the security system must identify policy distribution issues to avoid gaps in compliance.

The Advanced Policy Management architecture* within CA Access Control enables quick evaluation of policy delivery status and alerting of any unreachable hosts. Policy deviation reports compare the policies that should be active on a particular system and identify those that are actually installed so action can be taken to resolve potential discrepancies. In this manner, CA Access Control keeps the enterprise in compliance on an ongoing basis.

FIGURE B

The architecture provides a distributed, highly scalable model to distribute policies to all managed servers.

CA ACCESS CONTROL POLICY MANAGEMENT ARCHITECTURE



Logical Host Grouping*

CA Access Control allows you to group endpoints into logical host groups and then assign policies based on this host group membership, regardless of how your endpoints are organized in the Policy Model hierarchy. Hosts can be members of a number of logical host groups depending on their properties and policy demands. For example, if you have hosts running a Red Hat operating system and Oracle, these can be members of a Red Hat logical host group to get the baseline Red Hat access control policy, and also members of the Oracle logical host group to get the Oracle access control policy.

Logical host groups decouple policy assignment from policy distribution. This simplifies policy management as it does not require you to change your hierarchy to fit policy assignment requirements and lets you manage smaller, more specific policies and more focused host groups.

*Some features listed are only available in CA Access Control Premium Edition

POLICY VERSIONING* For more flexible control over policy changes and distribution, CA Access Control provides a policy versioning capability that allows the policy maker to define versions of policy rule sets. The policy version will be used in comparing the central policy store and deployed policy versions. In conjunction with deviation reports, this ensures the correct policy versions are deployed to each endpoint.

POLICY DEPLOY AND UN-DEPLOY* Another byproduct of the policy versioning feature is the ability to deploy policy versions to targeted endpoints. If a version needs to be rolled back, then that policy set can be un-deployed to ensure consistency from the top of a policy hierarchy down to the enforcement endpoints.

POLICY DEVIATION REPORTS* It is naïve to think that monolithic policies can be deployed across a large server environment without allowing exceptions. These exceptions might be imposed due to legitimate business or legacy requirements but they must be managed properly and done with accountability. CA Access Control provides a reporting feature to let you measure the compliance of your entire environment to specified policies and allows you to compare policies that should be active on a particular machine to policies actually deployed. This ability to quickly identify policy gaps supports your efforts to continuously meet compliance standards.

Policy and Entitlements Reporting*

CA Access Control simplifies security assessment tasks through reports about compliance exposures associated with operating systems, databases and applications. This report data can also be exported to other data analysis tools. CA Access Control host reports present system-centric information such as configuration, security and policy status.

Policy-based reports provide proactive views of who has access to what resources across your distributed and virtual server environment. These reports allow you to generate reports required by your auditors, such as User and Group Entitlement Reports, Policy Compliance Reports and Orphan Account Reports, among others. These proactive reports complement existing event-based auditing by allowing you to monitor compliance requirements and highlight existing discrepancies before incidents occur.

BASELINE SECURITY DEPLOYMENT AND POLICY GENERATION CA Access Control provides the capability to create a baseline security model by placing single systems in “warning mode”. In this mode, all system activities are observed and logged, but not enforced. Based on these observations, CA Access Control will automatically generate allowable access security policies. Having this initial set to build from greatly reduces the complexity, risk and effort required in building security policies.

APPLICATION PROFILING CA Access Control also has native utilities for building security policies around applications using warning mode. Gathered security monitoring data is converted into access control rules which can serve as a baseline for protecting an application. This Policy Generation allows new applications to be installed and made operational in much less time. These policies can be used as “Application Jailing” rules to protect critical applications from malicious attack as well.

*Some features listed are only available in CA Access Control Premium Edition

SAMPLE SECURITY POLICY SETS To speed up policy deployment and provide more comprehensive protection, CA Access Control provides out-of-the-box policy sample sets designed for commonly deployed applications and UNIX environments. CA Access Control has sample sets for UNIX and UNIX system applications including Apache, Linux and Solaris. Sample policies can be modified, allowing organizations to focus their efforts on making the minor modifications to fit their specific security needs.

PASSWORD QUALITY POLICIES CA Access Control goes far beyond default password creation mechanisms to give the enterprise complete control of both the user experience and security policies. The password management functionality of CA Access Control includes password aging, password quality, re-use restriction and dictionary support. CA Access Control can also monitor the number of consecutive failed login attempts to initiate an alarm condition indicating potential network intrusions via password attacks.

MAINFRAME PASSWORD SYNCHRONIZATION CA Access Control supports password synchronization between mainframes running CA Top Secret®, CA ACF2™ or IBM RACF and distributed systems running CA Access Control. Synchronization is accomplished using the standard CA Access Control PMDB method. Any password change a mainframe user makes is propagated to all machines in the password policy model hierarchy.

SECTION 4

Secure Auditing

While proactive access control is a necessary measure for securing host systems, it is also important to be able to resolve access incidents after they occur. Compliance often requires critical user actions within the system to be controlled and provable through an audit trail. In order to efficiently address regular compliance audits, this data should also be centrally collected and securely managed.

UNIX operating systems lack the ability to track a user's actions at the granular level required by compliance and often cannot trace superuser account usage appropriately. Without this, damage to a system might be impossible to detect or unable to connect back to an actual user. Native UNIX operating system's auditing services and logs are also susceptible to privileged account suspension, corruption or even termination.

CA Access Control generates secure and reliable audit logs which associate true user IDs to all protected resource actions (even after surrogate operations). Any action attempted by the user relating to an access policy can be recorded, including whether or not the user was allowed to successfully complete this request. If the need for an investigation arises, this complete, detailed and accurate audit data can greatly expedite the identification process of the attack source and activities.

Comprehensive Audit Modes

CA Access Control provides several auditing modes to accommodate different auditing needs. Audit modes can be set at the time of rule construction and includes the following modes:

- Success Mode records successful authorized access events.
- Failed Mode records denied access events.
- Warning Mode records access events without enforcing rules.

Additionally, user-specific events can be recorded in the following modes:

- Failed Login records failed user login events.
- Successful Login records successful authorized user login events.
- Trace In-depth tracking of a particular user's activities.

Log Routing

Routing all relevant access events to a single, secure location is a key requirement for efficiently managing compliance. CA Access Control solves this problem by providing the capability to route and centralize all access control logs. This has the benefit of not only log consolidation, but also ensures the availability of these logs in case of network breach or system compromise.

Real-time Notification

CA Access Control supports immediate notification about security events. Events can be routed to pagers or external consoles for quick problem resolution. Alerts can also be routed to other security information management systems, such as CA Security Command Center or system management systems like CA Unicenter® management consoles.

Self Protection

Auditing daemons and logs themselves need protection from potential attacks, shutdowns or tampering. CA Access Control auditing services and logs are self-protected and cannot be shutdown or modified. This ensures the log integrity and complete information available for any future investigation.

Integration with CA Audit

CA Access Control is fully integrated with CA Audit. Events in CA Access Control are sent to CA Audit for further handling, enabling aggregation of log files and creation of policy specific reports, which facilitates the audit process, provides detailed investigations and validates key compliance metrics. Features of CA Audit include:

- Cross-Platform Data Collection: CA Audit collects event data from an extensive variety of sources, including: operating systems, business applications, network devices, security devices, mainframes, access control systems and Web services.
- Real-time Tools for Collection, Viewing and Reporting: CA Audit provides customizable viewers and reports available to users that are relative to their role.

- Alert Management: CA Audit logs, filters and monitors critical events and execute alerts and other actions based on established policies.
- Central Security Data Repository: CA Audit stores audit data in a central repository, built around a scalable relational database for easy access, provides reporting for historical and post-event analysis.

SECTION 5

Cross-platform Host Protection

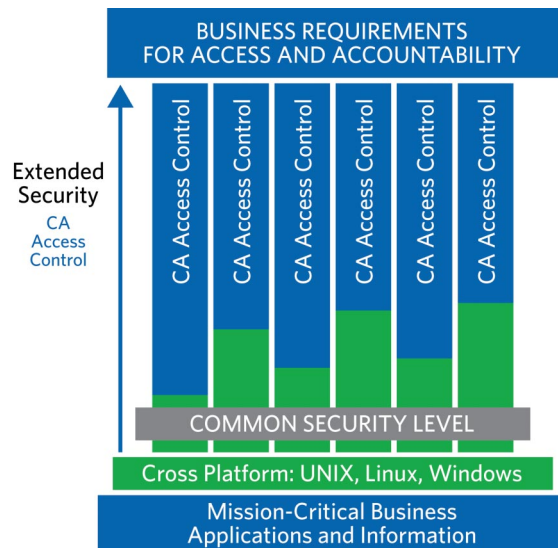
As companies evolve, they acquire a mix of technologies and systems to meet the prevailing need of the organization. From a server perspective, this often includes a diverse mix of UNIX, Linux and Windows systems. While different operating system platforms play an important IT role, unfortunately, each has its own security model.

Resolving these differences is an important factor in managing overall security as the strength of any network of systems is often only as strong as the weakest link. CA Access Control streamlines the management of security policy across a broad range of UNIX systems and beyond, to Windows and virtualization environments. With its centralized design philosophy, all platforms are managed from the same administration console using the same set of controls and mechanisms. This frees the organization from the limitations each individual operating system imposes, and enables them to pursue the best business-oriented solutions without worrying about differing native security models.

FIGURE C

CA Access Control elevates the collective level of access security across platforms and enables consistent administration.

ENABLE CONSISTENT, ELEVATED HOST ACCESS SECURITY



Central Administration

CA Access Control enables remote administration for nearly all security management operations. CA Access Control and its Advanced Policy Architecture makes it possible to control a variety of network servers from a single console. This centralization encompasses UNIX user and group management, all access control functions, monitoring and reporting.

Enterprise User Stores Support

CA Access Control supports enterprise user stores; that is, stores for users and groups that are native to the operating system. For example, it supports LDAP directories on UNIX and Active Directory on Windows. This support means that if the OS is configured to work with an enterprise user store, you can define access rules for your enterprise users and groups without having to synchronize or import the users and groups into the CA Access Control database. This greatly simplifies the deployment and management of AC in an enterprise environment.

Virtualization Support

Virtualization consolidates multiple server instances on a single physical machine, delivering lower total cost of ownership and improved machine utilization. Unfortunately, virtualization does not provide a solution for the consolidation of security management. Using CA Access Control, user accounts, passwords and security policies can be shared across all virtualized hosts and managed from a single administrative console either from the virtualization server or the workstation.

CA Access Control allows organizations to take advantage of a breadth of virtualization environments such as VMware ESX Server, Solaris 10 Zones, Citrix XenServer, AIX LPARS and HP/UX VPAR.

Native Installation Mechanisms

CA Access Control supports several installation options across native operating system features allowing for easier installation and tighter integration. These include a product install program, silent install option, remote installation and native operating system installation package. It can also be included as an initial installation kit to roll out to a large number of servers.

CA Access Control — Part of a Bigger Identity and Access Management Solution

CA Access Control can be installed independently and provide full server access protection without dependencies on other CA or third-party products. However, all products in the CA Identity & Access Management solution share common approaches and components for Web user interface, administration concepts, delegation of responsibilities and reporting to ensure a consistent administrative experience.

Given that operating system access protection may be a single component of a defense-in-depth strategy, CA Access Control provides integration with CA security products including:

CA IDENTITY MANAGER As a provisioning target for CA Identity Manager, the CA Access Control user base can be managed from and automatically kept in sync with CA Identity Manager.

CA SECURITY COMMAND CENTER CA Access Control security events can be collected by or automatically routed to any remote server defined by CA Security Command Center.

CA ACF2 AND CA TOP SECRET SECURITY CA Access Control can leverage the mainframe user store provided by CA CA-ACF2 Security or CA CA-Top Secret Security as a trusted repository or user passwords can be synchronized with those mainframe user stores. This assists organizations seeking to manage access to critical mainframe resources, privileges and utilities in the same way that CA Access Control provides protection for Windows and UNIX.

SECTION 7

Conclusion

In today's sensitive IT environments, security needs to be every organization's top priority. While IT managers should have a choice of UNIX, Linux and Windows application platforms to meet business needs, that choice should not compromise security. Having multiple operating systems does not mean that numerous error-prone manual security procedures need to be used.

CA Access Control improves the level of security on an individual machine basis, but also raises the level host security across all your UNIX systems. Centralized, policy-based management overcomes the disparate security models between operating systems without the high cost of fragmented, manual maintenance. Powerful user access control, advanced policy management and compliant auditing allow organizations to achieve the level of security required by compliance. These and other unique security management features combine to make CA Access Control the premier host access management solution.

To learn more about the CA Access Control architecture and technical approach, visit [ca.com/security/ac](https://www.ca.com/security/ac).

CA (NSD: CA), one of the world's leading independent, enterprise management software companies, unifies and simplifies complex information technology (IT) management across the enterprise for greater business results. With our Enterprise IT Management vision, solutions and expertise, we help customers effectively govern, manage and secure IT.

MP315680608

Learn more about how CA can help you transform your business at [ca.com](https://www.ca.com)

