An Integrated Architecture for Identity and Access Management
Table of Contents

Executive Summary 1

SECTION 1: CHALLENGE 2
The Need for Enterprise Identity and Access Management (IAM)
New Architectures Require Additional IAM Tools
The Need for Integration within IAM

SECTION 2: OPPORTUNITY 4
The CA IAM Solution
An Architecture to Integrate Identity with Access

Core Services of the Solution
Identity Provisioning and Life Cycle Management
Single Sign-On
Access Control

Management Services of the Solution
Administrative Interface
Event Collection
Standards in IAM
The CA Integration Architecture Beyond IAM

SECTION 3: BENEFITS 9
The CA IAM Solution Lowers Costs and Improves Risk Management

SECTION 4: CONCLUSIONS 10

ABOUT CA 11
Back Cover
Executive Summary

Challenge

With every new wave of technology innovation, organizations enjoy powerful new tools and methods for extending the creation, storage and use of critical business information. However, every new wave of technology also brings with it new security risks and management challenges. Often, identity and access management (IAM) tools have been added piecemeal to new application and computing architectures, making the IAM function less efficient and effective overall. Increasing compliance requirements further complicate the problems with IAM products that are not integrated across the organization.

Opportunity

The CA Identity and Access Management (IAM) solution features an architecture that allows tight integration of user identities with access management policies across all forms of applications and information sources. The two-layer architecture offers Identity Provisioning and Life Cycle Management, Single Sign-On, Access Control and Centralized Event reporting. The solution supports a wide range of industry standards as a critical part of its architecture, and can be implemented in steps based on your organization's priorities.

Benefits

CA's IAM solution architecture and services are designed to reduce costs while enabling your organization to meet compliance requirements and ensure appropriate levels of security throughout the enterprise. Through its two-layered service architecture, the CA IAM solution is:

COMPLETE  Covers the broad range of IT end points from the Web service to the mainframe
INTEGRATED  Connects provisioning, identity management, access management and auditing
MODULAR  Can be implemented in steps based on an organization's priorities
The Need for Enterprise Identity and Access Management (IAM)

Network technology, distributed computing and the Internet have made it possible to dramatically extend application and information access to users well beyond your typical organizational boundaries. Handheld computing devices have increased the end points from which business-critical data is accessed. Now the emergence of dynamically assembled software and hardware through federation, service-oriented architectures and grid computing hold the promise of even greater agility from a web of interconnected users, data, machines and even organizations. Never before has such a range of powerful technologies been at your organization’s disposal. In order to take advantage of these new tools, your organization must address the related security risks, management issues and compliance requirements. Your organization must be able to answer three simple questions that represent the challenge:

1. Who is accessing my applications or data?
2. What are they authorized to do?
3. Should they have those authorizations?

The tools that allow your organization to answer these questions and maintain control over users and their access make up an identity and access management (IAM) solution.

New Architectures Require Additional IAM Tools

The scope of the IAM challenge has changed. Each new wave of technology introduces a need for new IAM tools that will allow your organization to maintain the required level of control. Rarely is an older technology driven into immediate and complete retirement at the point a new technology is added.

Mainframe computing illustrates this point. While this cornerstone of the centralized computing model was introduced decades ago, many organizations continue to run business-critical applications on the mainframe in spite of the Internet revolution. In fact, the mainframe platform has evolved too, fulfilling new roles as other technologies were introduced around it. As a result, access control for the mainframe continues to be an important element of an overall IAM solution architecture. Thousands of organizations use CA-ACF2 and CA-Top Secret Security to control access to information on that platform.

With each new computing architecture, organizations have had to adopt additional IAM tools that were typically unique to that new technology. While these tools included some basic levels of interconnection, such as supporting administrative GUIs in a browser interface, referring to a common LDAP repository for basic user information, or publishing event information to syslog, more often than not these tools were developed by different vendors and had very minimal forms of integration.

The Need for Integration within IAM

Your organization is likely to have mainframe access management products, identity provisioning products, web access management products, enterprise single sign-on products, Web services access management products, role management products, host access management products and more. Your organization is also likely to be struggling under this growing load of IAM tools. Lack of integration between these tools makes management and
maintenance more difficult, reduces your IT staff’s ability to deliver the service levels needed from the new computing architectures and drives up management costs.

Every access policy your organization creates can be traced back to a business policy. Your organization probably has business policies that attempt to prevent violations of segregation of duties. An example of a violation would be a person having the privilege to open a purchase requisition who also has the privilege to approve payment for delivery of goods. This simple example of a business policy must be supported by, and enforced by, the IAM systems that are in place in your organization. In more complicated examples, business policies have to be implemented across a number of the IAM tools in your organization. Lack of integration across those tools means your organization needs to configure IAM policies repeatedly across different tools to ensure a business policy is implemented properly.

Working with more disparate tools creates more chances for an unintended inconsistency or hole in the implementation of the business policy. This creates a significant additional security risk for your organization.

Innovation in IT technology will continue, and market pressures that drive your organization to adopt technology innovations will not abate. The only path available for cost-effectively maintaining control over identities and information access is through greater integration of IAM tools.

An example of the value of tighter integration can be seen in the way organizations connect their identity management tools with their access management tools.

Most organizations have some form of user repository in their network, such as an LDAP directory. A typical organization will additionally have multiple layers of infrastructure where it needs to apply access management. Layers will include host systems (mainframe, UNIX, Linux or Windows), the off-the-shelf applications that run on those systems (ERP applications, Web Servers, Portals, etc.) and their own in-house-developed applications. As a result, enterprise access control can be required at layers that reach down to the very basic resource object level within applications.

Access management products provide value by binding users to access policies that determine who has access to what resources across these layers of the IT environment. Organizations that use a nonintegrated identity management product will have to develop custom connectors that allow the identity management product to manage the provisioning of users to the correct access policies or access roles in the access management products. This creates the ongoing burden of having to keep the custom-built connectors in sync with the identity management product and the access management products. Additionally, if the identity management and access management products are from different vendors, it also makes it likely that the level of integration between them will be rudimentary and less than an organization really needs.
The CA IAM Solution

An Architecture to Integrate Identity with Access

The CA IAM solution addresses the need for tight integration between identity management and access management products. The architecture is designed for the integration between CA Identity Manager and the industry’s leading access management components in the CA IAM solution.

THE CA IAM ARCHITECTURE

The architecture is composed of two basic layers of services — core services and management services — that work in combination with CA Connectors to deliver an integrated IAM solution.
Core Services of the Solution

Identity Provisioning and Life Cycle Management
Organizations have three general groups of users they need to successfully manage — employees, customers and partners. The CA IAM solution provides tools that support the creation and management of user identities for each of these user types in many different endpoint environments, such as directories, operating systems, ERP systems and other layered applications. However, the CA IAM solution does much more than just creating, provisioning and deprovisioning users and user attributes. The solution also provisions users to access roles in the access management components of the solution, thereby completing the loop of binding users to access policies which protect applications and resources within applications. The efficient association of identities to access policies represents the advanced value of a fully integrated IAM solution. As outlined above, this out-of-the-box integrated architecture of the overall CA IAM solution enables an organization to avoid the need for custom connectors.

Additionally, this integration will be extended in future releases. Examples include the ability to:
- Explore and correlate user identities across user repositories and access management products, to facilitate separation of duty analysis
- Extend orchestrated workflow processes that cover the full range of identity and access management tasks linking identities to roles to policies to resources
- Provide a consistent entitlement certification process so application owners can certify that only approved users are gaining access to important and sensitive business information

Single Sign-On
Across any organization’s IT environment there is a wide range of applications supporting a wide range of authentication schemes such as x.509 certificates, SAML assertions or various forms of biometrics. However, due to the cost and complexity of other forms of authentication, most organizations continue to employ only a username and password combination as the primary method of user authentication for the vast majority of their applications. Organizations’ desire to reduce the variety of authenticators while increasing the overall security of user authentication has been unfulfilled. In fact, just the opposite is occurring. Recent regulations, such as FFIEC, HSPD-12 and SOX are continuing to drive the addition of even more authentication methods into the market.

While organizations do need to implement stronger forms of authentication for some critical applications, they also need to find ways to reduce the overall cost of managing user authentication. Single sign-on implemented with appropriate support for stronger forms of authentication provides the best path to address this need. CA’s IAM solution offers an integrated approach to delivering single sign-on across a broad range of application environments. By supporting the native authentication interfaces of the various application environments, such as the HLLAPI interface for terminal emulators, GINA interface in Windows, PAM interface in UNIX and the available APIs interfaces on Web Servers and Application Servers, the CA IAM solution is able to integrate with authentication processes from the mainframe to a Web service. By further integrating the authentication ticket mechanisms in the different CA products, the CA IAM solution provides users with the experience of a single sign-on across all these disparate environments.
Access Control

Implementation of access control in an IAM architecture demands support for many different access enforcement points. CA's IAM solution provides the broadest array of capabilities for heterogeneous IT systems. Access control within the CA IAM solution includes support for controlling:

- Entry into virtually all z/OS subsystems and VTAM applications for the mainframe
- Root privileges on Unix and Linux host systems
- Administrator privileges on Windows systems
- Login to virtually any network and application accessed from a Windows client
- Access to URLs on a web server or portal
- Access to JAR and EJBs on J2EE Application Servers
- Access to applications exposed as Web Services

Support for this range of environments is accomplished by integrating CA's IAM solution both via public APIs and supported standards available from the applications, platforms or operating systems.

Management Services of the Solution

The CA IAM solution provides two additional, essential services for improving enterprise-wide management — the administrative interface and the collection and reporting of events generated by the solution.

Administrative Interface

Existing market research has demonstrated that the majority of the total cost of ownership for an application is not the purchase price, but rather the costs of deploying, managing and maintaining the application. This is also true for management applications that deliver IAM services. To help drive down the overall life cycle costs and provide a means of ensuring better IAM integration, the CA IAM solution provides integration of the administrative interface for a growing number of products within the solution. This enables an organization to move from siloed administration of IAM across the range of application environments to a more cost-efficient, centralized administrative model. This is important, given that access control policies are implemented to reflect business policies about who should have access to what.

Being able to set those access policies via fewer management interfaces reduces an organization's overall security risk by helping ensure that no unintended application or resource access gaps are created.
Event Collection
Being able to provision users, bind them to access policies that, in turn, are bound to applications and resources, is the function of an IAM solution. Once in place, a further critical need is to capture and collect runtime and administrative event information associated with the transactions of the solution. An architecture that supports collection of this information across the IAM solution to a centralized repository for reporting adds tremendous cost efficiency to the solution — particularly when compared with having to manually collect the information or having to build custom audit connectors. The CA IAM solution addresses this architectural need by providing the ability to collect and store IAM event data to a consolidated repository. This capability includes support for normalizing, aggregating and filtering the event data at its source in the IAM solution before delivering it to the central repository, thereby using network bandwidth as efficiently as possible. Encryption of the data stream is available to further protect the integrity of the event information. Once the event data is collected from the CA IAM management points, it can be viewed, graphed and used to generate reports.

Standards in IAM
In typical fashion any new IT technology or architecture will be developed with industry agreement on the basic protocols to make it work. As the technology’s adoption continues, other standards are developed to handle some of the critical integration and security needs that arise. For example, with the growth and adoption of directories came the IETF LDAP standard. With the growth of the web server came the IETF-based SSL/TLS standard. With the growth of web servers and web-based single sign-on came the OASIS SAML standard.

While standards in IAM are emerging, an enterprise IAM solution can’t be created by adherence to standards alone. But support for standards is a critical part of the architecture of the CA IAM solution and provides the means to integrate with other portions of your organization’s IT infrastructure. Some of the most important standards used by CA’s IAM solution are the following:

**LDAP LIGHTWEIGHT DIRECTORY ACCESS PROTOCOL** is an IETF standard for accessing and modifying a directory server or set of servers. Typically, the directory being accessed via the LDAP protocol contains information about users stored in a tree-like structure and organized along geographical or organizational units.

**SAML SECURITY ASSERTION MARKUP LANGUAGE** is an OASIS standard developed to provide an XML-based method for communicating authentication and authorization data between domains inside an organization or between organizations. A SAML assertion or artifact is issued by an identity provider to a principal (most often an end user). That assertion is subsequently provided to a service provider as a proof of authentication and/or authorization so the user gains the benefit of single sign-on.

**XACML EXTENSIBLE ACCESS CONTROL MARKUP LANGUAGE** is an OASIS standard developed to provide an XML-based access policy language and model for interpreting the policies. Policies expressed in XACML can be used across policy enforcement points that support this standard.
SPML SERVICE PROVISIONING MARKUP LANGUAGE is an OASIS standard developed to provide an XML-based language for provisioning and managing the life cycle of users, system access entitlements or privileges.

WS-SECURITY WEB SERVICES SECURITY is an OASIS standard developed to provide security to Web services. The protocol, in turn, supports a variety of mechanisms, such as SAML, for ensuring confidentiality and integrity for Web service-based communication.

CA will continue to be an active contributor to, and user of, relevant IAM standards.

The CA Integration Architecture Beyond IAM
The value of the integrated architecture for the CA IAM solution is part of CA’s overall vision to unify and simplify the management of IT across the enterprise. That vision, called EITM (Enterprise IT Management), is illustrated in the following graphic:

The EITM vision is dedicated to the idea that all IT management functions should work together to meet the collective needs of IT and the business. CA delivers the key management functions of EITM in four main categories, each of which addresses management needs in a variety of areas:

BUSINESS SERVICE OPTIMIZATION includes IT resources and governance IT services and business process management.
ENTERPRISE SYSTEMS MANAGEMENT includes management of systems, networks, databases, applications, workloads, inventory and configuration.

SECURITY MANAGEMENT includes identity and access management, security information and vulnerabilities, and threats such as virus and spyware.

STORAGE MANAGEMENT includes management of storage resources, backup and recovery, and compliance and optimization.

The CA IAM Solution Lowers Costs and Improves Risk Management

The CA IAM solution lowers overall cost of ownership and improves your organization’s ability to manage risk. Through its two-layered service architecture the CA IAM solution is:

COMPLETE Covers the broad range of IT end points from the Web service to the mainframe

INTEGRATED Connects provisioning, identity management, access management and auditing

MODULAR Can be implemented in steps based on an organization’s priorities

Specific benefits of the CA IAM solution include:

IDENTITY PROVISIONING AND LIFE CYCLE MANAGEMENT The CA IAM solution helps your organization avoid customization expenses and complexities typically required for the association of identities to access policies.

SINGLE SIGN-ON The CA IAM solution delivers a seamless and comprehensive single sign-on experience for a user across a wide range of disparate environments.

ACCESS CONTROL The extensive coverage of the IT environment provides your organization with an unparalleled ability to manage access to applications and data centrally, and thus manage costs and risk and improve service.

ADMINISTRATIVE INTERFACE The administrative interface supports integrating IAM products within the solution, thereby helping to reduce your organization’s overall life cycle costs and security risk.

EVENT COLLECTION Centralized reporting of runtime and administrative event information associated with identity and access management is much more cost-efficient than having to collect the information manually or build and maintain custom audit connectors. Support for processing, paring down and encrypting the data at its source minimizes network traffic and provides greater security.
STANDARDS IN IAM The CA IAM solution uses and supports industry technology standards in order to facilitate integration with other portions of your organization’s IT infrastructure.

THE CA INTEGRATION ARCHITECTURE BEYOND IAM The solution is part of CA’s larger Enterprise IT Management (EITM) vision, which calls for unifying and simplifying IT management across the enterprise for greater business results.

SECTION 4: CONCLUSIONS

CA’s modular IAM solution provides the architectural foundation and services necessary to achieve the vision of unifying and simplifying the management and effectiveness of your IAM infrastructure.

With the continued innovation in IT architectures, the number of IAM tools in your network will only continue to add costs and create security headaches for your organization. The most efficient path to containing those costs, meeting your compliance requirements and ensuring appropriate levels of security is with a solution that integrates industry-leading capabilities across the different IT architectures that are deployed in your IT environment. CA’s IAM solution puts you on that efficient and effective path.

To learn more about the CA Identity and Access Management architecture and technical approach, visit ca.com/iam.
CA, one of the world’s largest information technology (IT) management software companies, unifies and simplifies the management of enterprise-wide IT for greater business results. Our vision, tools and expertise help customers manage risk, improve service, manage costs and align their IT investments with their business needs.

Learn more about how CA can help you transform your business at ca.com