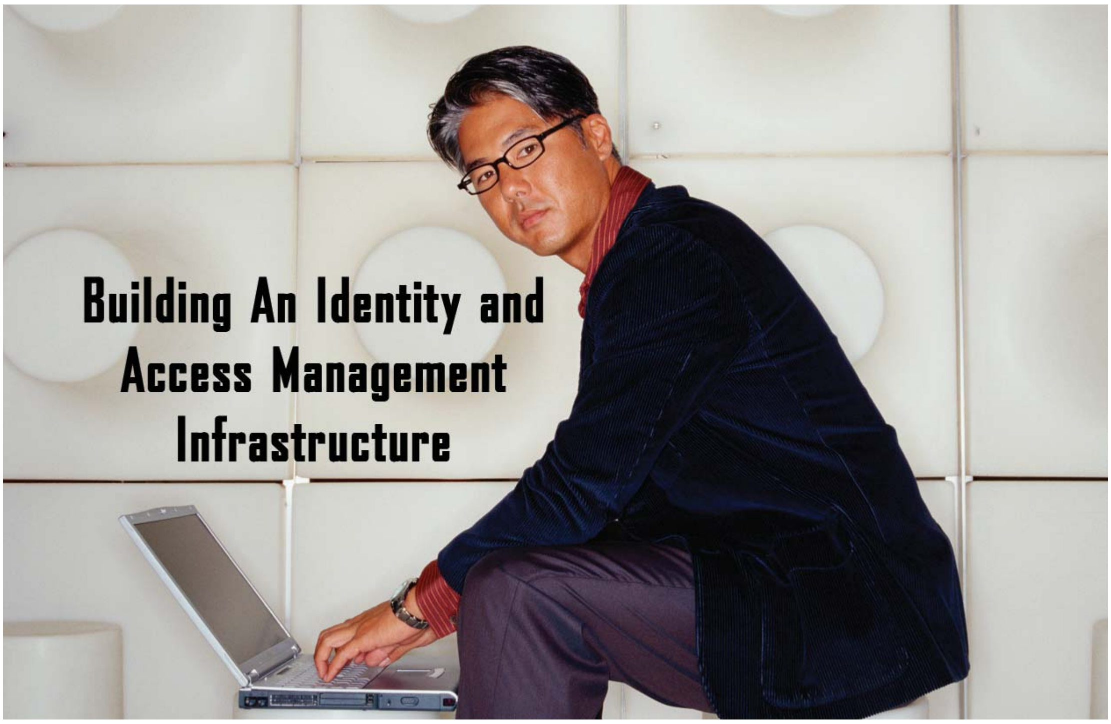
connet consultancy | continuity | consumerization | convergence



Building An Identity and Access Management Infrastructure

Introduction

Identity and Access Management (IAM) is not new in IT security. For many years, services such as password management and self-registration could easily be found in many computer systems and enterprises. During the last few decades, enterprises have been developing computer applications and building systems to conduct business electronically with clients, partners, vendors, contractors, and employees over the networks, and now across the Internet. In order to adapt to the new Internet-based economy and Web services business model, companies have to implement an integrated, centrally managed, role-based and policy-based IAM infrastructure to reduce security risk and manage trust and identity with other entities.

The Problem

Not surprisingly, almost all corporations in America would have many applications, hundreds of servers, and thousands of workstations for thousands, even millions, of internal and external users. Compared to other areas in IT such as usability, functionality, performance, and time to market, security has been undervalued by most business managers and IT professionals. The homegrown IAM mechanisms for existing security systems were usually poorly designed or poorly managed.

Storing redundant user information in multiple independent user repositories, using weak or even no password policy, allowing users to have more than required accesses, and providing the same user with many IDs are some of the most common IAM problems for most companies. With a rapidly growing population of users, enterprises are facing challenges to create, delete, reset, and manage those user accounts in a cost-effective way.

Moreover, with devastating attacks by identity thefts, rising uncertainty over terrorism and global stability, and increasing involvement of government regulations such as the Health Insurance Portability and Accountability Act (HIPAA) and the Sarbanes-Oxley Act (SOX), the next generation of IAM infrastructure is back to the top of the IT agenda for many CIOs and CSOs.

An enterprise needs an infrastructure to manage user accounts on different platforms and applications, secure valuable data and resources, trust and interact with other companies on the Web, and assign user permissions quickly, easily and securely.

The Solution: IAM Infrastructure

An enterprise needs an infrastructure to manage user accounts on different platforms and applications, secure valuable data and resources, trust and interact with other companies on the Web, and assign user permissions quickly, easily and securely. An IAM solution basically includes authentication and authorization control, password management, user provisioning, user directory management, Web services security, enterprise, and Web single sign-on.

The business workflow engine, self-registration, and delegated administration of the solution enable a company to automate the management of user identity and therefore reduce costs. The IAM infrastructure can also provide a centralized user and access control platform to handle all user authentication and authorization to almost every resource in a company, offer enterprise and Web single sign-on, and secure newly developed applications or systems with a reusable security module to lower cost of maintenance.

Indeed, Gartner Group, a research company, estimates that as much as 40% of all support calls are password-related, and the cost of these calls ranges from $25 to $45 each. Annually, a typical company spends about $225 per user resetting passwords or handling password-related issues. For a company with 5,000 users, the cost to maintain these services alone can easily be over one million dollars! Just because of the high return on investment (ROI) of the solution, many companies are driven and committed to implement an IAM infrastructure within their IT environment to cut costs.

Nine Basic Steps to Build a Successful IAM Infrastructure

Step 1: Get the Support From Top Management

Unfortunately, and unavoidably, this is the very first step. Without support from executives, it is almost impossible to build a successful IAM infrastructure!

The ownership of user identity and access control is shared by almost every organization within a company. Human resources, corporate IT, customer support, application development, operations, and the information security team are only some of the stakeholders of the user IDs that you will be consolidating into the new infrastructure.

IAM infrastructure is not just related to technology. It centers on a fundamental business concept: An enterprise must interact with its employees, clients, partners, and other entities. Business analysts, security professionals, application developers, as well as executives have to be involved in defining these relationships clearly. Also, a successful IAM project requires a huge amount of investment and the collaboration of many organizations and people within your company. Therefore, the support from top management is extremely crucial to your project. Without the “blessing” of your CEO, CIO and CSO, your IAM project can be very political.

Step 2: Do the Research

The next step is to know what applications and systems are in your company as of today. There are many types of IT resources in a corporation: operating systems, databases, ERP systems, directories, security managers, Web access controls, and e-mail systems. Gathering the basic information such as ownership, number of users, user types, IP address, physical locations, resource roles, and level of security for your company’s resources will definitely help you better understand the IT topography and draw the future IAM roadmap for your company.

Questionnaires and interviews are some of the best ways to collect this information from resource owners in different organizations. If your HR manager cannot answer all your questions, he/she should be able to point you in the right direction for a talk with the technical folks.

The process can take weeks, even months, depending on the amount of resources and the complicity of your IT structure. The goal of this exercise is to generate a list of resources and to understand the value, impact and risk of the resources in your company

Step 3: Group the Resources and Create a Plan

Building an IAM infrastructure can take more than a year. One of the most common mistakes for most project owners is trying to do too much in an unrealistically short timeframe. The rule of thumb is to limit your scope and manage expectations carefully. Using a phasing approach and taking baby steps are smart ways to minimize the possibility of future embarrassment. Also, you first may want to take care of the resources that are less mission-critical, more easily integrated, or absolutely required by external authorities, such as your management or government regulations.

Group the resources by their similarity, physical location, function, or ownership. Usually, e-mail systems, domain logins, employee benefits, and customer service applications are some of the resources that should be first integrated because of the huge user population and the higher ROI. However, you have to integrate these systems slowly and carefully. You may want to test the water by rolling out a pilot or testing the concept with a smaller group of users in order to prove your IAM infrastructure.

Keep in mind that taking small steps forward is always better than taking even one step back.

Step 4: Design the Business Processes

Now you have prioritized your resources, and you have a high-level plan to save some money for your company. So, you are ready to start to do the fun stuff like development, right? Not yet! Before programming the new infrastructure, testing connectivity, or integrating user IDs, your company must first formalize or standardize the business processes. There are five major business aspects in an IAM infrastructure:

1 User Structure

In an IAM infrastructure, user identities are usually stored in a centralized user directory and organized in multiple organizational units (OUs) in the directory tree. Each OU can represent a user type, a location, or a department, and the design of your directory can closely resemble the user structure of your company.

Design tips: make it simple, logical, and flexible for changes. Don't try to group too many or too few users into a single organizational unit because it is difficult for administrators to manage users effectively.

2 Enterprise Roles

Every user can have one or more roles to access various resources and perform various tasks in a company. An HR manager may have an HR administrator role to access the HR system. An accounting clerk may have both data entry associate and financial report analyst roles to modify data and generate financial reports in accounting applications. Also, a customer in a healthcare company can be a policyholder, who is allowed to submit claim and check claim status, and a primary policy administrator who can add, remove, or update other policy holders' information under the same policy.

Vaguely or implicitly, enterprise roles are defined by business owners in most companies. Most companies still do not have a clear definition of the enterprise roles, how these roles interact, and what the roles entitle users to do exactly. Documenting the details about enterprise roles may take great effort, but it can provide a company with better visibility, efficiency and security in its business processes.

3 IAM Roles

One of the main purposes for building an IAM infrastructure is to manage users effectively and securely. Delegated administration allows business managers or administrators to manage, update and approve users directly. However, there should be boundaries for or rules limiting what managers can do within the IAM infrastructure. For example, a manager in California can only modify user identities and privileges in California, and a customer service representative can change passwords for users but cannot modify access policies in resources. Defining IAM roles for your system provides controls for your IAM environment. IAM roles provide different levels of administrative rights to administrators to manage their users and policies.

Some of the common IAM roles are IAM super administrator, user administrator, access administrator, user approver, password administrator, resource administrator, resource approver, and application access administrator.

4 Enterprise Security Policies

Very likely, you will be integrating user IDs from different resources, and those resources could have conflicting security policies. For example, your UNIX system might allow only user IDs with less than 8 characters, but the domain ID might be between 6 to 12 characters. The password policy for your HR application might require at least one uppercase and one numeric character, but the policy for a Web application allows any password with more than 8 characters. It's obvious that a company will have to iron out their enterprise security policies before building the infrastructure. Some common enterprise policies are: User ID—In a sophisticated IAM system, a company can have different user ID policies for different types of users. For example, customers may have some level of freedom to choose their IDs, but employee IDs are usually generated by the system. Password—Passwords can be compromised. Therefore, a strong password policy should be used to safeguard your company's resources. A combination of uppercase, lowercase, numeric, and special characters, as well as a minimum length requirement and a dictionary attack prevention mechanism are some of the ideas of a good password policy. Separation of Duties—In order to prevent fraud, no single user in a company should have total control of the mechanisms in a transaction. For example, no single individual should be able to both initiate a payment and authorize a payment in an accounting system. A company may assign portions of tasks to different administrators to avoid unauthorized execution of the process.

User Account Expiration—Set an expiration date on the user account to ensure that the account is disabled when the user no longer has access to enterprise resources. Unless being recertified by an administrator, the user account should be disabled.

5. Use Cases and Procedures

Use cases and procedures describe the whole lifecycle of a user identity and the management of resources and privileges. Some of the basic use cases are:

1 Create user
2 Delete user
3 Modify user
4 Enable/disable user
5 Lock/unlock user
6 User expiration/recertification
7 Auditing and reporting

A detailed description or sequence diagram should be included in the use cases. Approvals of the use cases and procedures from the stakeholders within your enterprise are absolutely necessary.

Step 5: Pick the Right Architecture and Technology

The IAM infrastructure market is still relatively young, and there are many vendors competing in the marketplace. While some vendors present a full suite of identity and access management solutions including user directories, access management, user provisioning, customizable workflow engines, authentication and authorization, and delegated administration, other component vendors offer specific modules for companies to integrate into their existing environments. Because of the unique requirements of your enterprise, you will have to pick the right architecture and products to fit your company's special needs. Proof-of-concept or product demonstration may be set up with vendors to better understand your selections. Some of the criteria necessary for selecting the right products are:

1. Out-of-the-box functionality—Most IAM solutions provide many features that are used by enterprises and reduce development efforts.
2. Performance—If your company has or will have a million users in the future, performance of the solution is a must.
3. Scalability—Two servers may be enough to handle the load at the beginning. However, your IAM system should be scalable for future growth, and you should be able to add hardware to increase performance.
4. Reusability—An IAM solution that can reuse existing infrastructure or be reused by other components or applications in your environment is a cost-effective way to sell your idea!
5. Flexibility—Companies are rapidly changing the ways they do business in this new economy, and the structure of organizations, user roles, and user privileges are also continuously evolving. So, an IAM system that is flexible for changes is required.
6. Commitment towards standards—There are some standards related to IAM such as OASIS SAML, SPML, and the Liberty Alliance. Since federated identity is a hot topic in the IAM community, following a standard that is supported by leading vendors is essential for a smooth integration.
7. Learning curve for developers—Indeed, some software is easier for developers to learn than others. The steeper the learning curve, the longer the development time.

8. Ease of use—Identity is owned and used by humans. Thus, if the user interface of your IAM system is difficult for your users, you will have lots of trouble.

Step 6: Develop and Test the System

After you have the business processes and technical design, it's time to build the system! Depending on the size of your first phase, your company will need some or all common software developing environments such as development, integration testing, functional testing, quality assurance, staging, and production.

After you have set up the required hardware, you will have to test the technology and connectivity to the resources in all your environments. The next task is to customize or develop the product and workflows based on the business processes, policies, and use cases.

If you don't want the embarrassment, you better know for sure that you have tested your system thoroughly. Like all computer systems, your IAM infrastructure is not bulletproof. Unfortunately, Your IAM system is like a guard protecting the IT resources of your company. It is expected to be the last system to fail. So, make sure that you have tested your system for functional errors and performance as well as for any kind of possible system failures. Make sure that you have an automatic fail-over mechanism for your IAM infrastructure and a contingency plan if it doesn't work.

Step 7: Train Your Business and IT Folks

Education and training is another important aspect of your IAM project. When your users are accustomed to remembering or sticking 10 user-names and passwords to post-its, it may take them a while to believe the miracle of having only one ID and password. You may have to educate your co-workers in IT and application development teams about sharing enterprise identity instead of owning specific resource IDs. An IAM infrastructure can be a new and overwhelming concept for a corporation, but the learning curve can be less steep if you have a plan to educate your users. In your training document or presentation, you should explain the benefits of the IAM infrastructure, integration schedules, delegated administration structures, migration plans, policies, use cases, organizational changes, enterprise roles, etc.

Step 8: Bring It On

It’s a big day! If you have limited your scope at the beginning for your phase-one implementation and you have done all of the steps carefully and correctly, the transition from those old IAM systems to the new infrastructure should be very smooth and virtually invisible to users.

If the transition is not as effortless as you thought, don’t panic. Just make sure that you can roll back the changes and test it again before the next big day.

If the transition is a success, congratulations! You have the confidence and support from your management and peers to achieve more successes in the upcoming phases.

Step 9: Enhance and Upgrade the IAM Infrastructure

After you have finished phase one, you can move on to integrate other resources you have already planned on your roadmap. Keep in mind that IAM technology will continuously evolve and improve in the next few years. You may have to upgrade or replace the IAM infrastructure according to the needs of your enterprise. Be really careful, and again, make sure that you take baby steps in constructing the next phases.

Conclusion

The keys in building a successful identity and access management system is to understand the ultimate driving force behind the technology: the business of your company. By being familiar with the business processes and the relationships among customers, employees and partners, you will be able to provide a sophisticated design to better fit your company's needs. On the other hand, simply integrating different IAM components together without fulfilling the requirements may actually complicate the situation and can be really frustrating for everyone.

Remember, the best IAM solution for the users is the one that provides security, visibility and simplicity. But also remember, the best solution for your company is the one that attains a high ROI! Saving money for your enterprise is always important. So, happy developing!