GIAC
CERTIFICATIONS

Global Information Assurance Certification Paper

Copyright SANS Institute
Author Retains Full Rights

This paper is taken from the GIAC directory of certified professionals. Reposting is not permited without express written permission.

Interested in learning more?

Check out the list of upcoming events offering
"Security Essentials: Network, Endpoint, and Cloud (Security 401)"
at http://www.giac.org/registration/gsec

Establishing Enterprise Identity Management

Soon Sian Tan

GSEC Practical (version 1.4b Option 1)

March 30, 2003.

Abstract

Identity management is basically an integrated set of technologies and processes that allow an enterprise to centralize the management of user digital identity and user resource access. With the increasing complexity of existing IT infrastructure and expansion of new information systems for e-business purposes, it has become a high priority for an organization to have an enterprise identity management system to improve existing inefficient identity management practice. It helps an organization to reduce operation costs, reduce internal and external risks as well as improving business processes.

Establishing an enterprise identity management system is a challenging task, long cycle implementation and it involves whole organization participation to make it successful. However, the return of investment will be significant in the long run if it is implemented properly. This paper aims to provide an introduction to identity management, the building blocks of a typical enterprise identity management and the benefits of enterprise identity management. It also provides insights into current available solutions, challenges and strategies for those who are planning or evaluating of setting up enterprise identity management.

Introduction to Identity Management

In most enterprise current computing environment, identity management is mostly performed through individual system or application administration software, people and processes. There was no centralized identity management system. This conventional identity management practice was sufficient previously without any inefficiency service level. However, the increasing application of information technology into enterprise business process has resulted in proliferation of technology infrastructure – operating systems, databases, web servers and applications. Furthermore, organizations are rushing to exploit e-business initiatives by extending existing enterprise IT systems or applications to external customers, suppliers, partners and vendors. With all these changes, conventional identity management practice has become inefficient and the degree of security risks an organization has to absorb has increased as well. Some of the challenges that enterprise start to discover are poor quality of service due to long cycle of user IDs creation, weaker security due to complexity in managing security access, higher IT operation cost due to increasing workload on IDs management. According to Meta Group research on existing user provisioning process, "it shows that on average, the process of providing a new internal user with computing privileges occurs 28 hours more slowly than business requirements, resulting in a 36% loss of productivity and 26% loss of efficiency over that time period."[1]

These identity management issues apply to external user as well. Take for example in an environment with the deployment of e-business applications to external

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

customers. Each application, portal, or web server that an external customer need to access requires a different user account. If the number of external customers required accessing the e-business applications increases tremendously, using conventional identity management system would take an organization long time to process all those requests. This prevents customers having timely access, degrades the customer service level and slow down business growth; thus creating business disadvantages when competing with other industry competitors. From the security point of view, the requirement of customer accessing multiple applications or systems also results in the complexity of managing security access on the application and system as well. This complexity results further in confusion in providing correct access and thus increasing an organization information security risk.

In view of the new challenges to existing identity management, development of a more effective identity management solution is of high priority. And an enterprise-wide identity management which provides automated and centralized identity management is the solution. Traditionally identity management has been defined as purely for user account management. However, nowadays the definition of identity management can be defined as identity and access management as the scope of identity management has been extended to include access management as well. The primary objective of an enterprise identity management is to provide a central repository where user identity information can be stored and a shared platform where user provisioning and resource access management can be centrally managed based on user roles. As PricewaterhouseCoopers's Peter Shilito put it,

"A better definition of identity management is the collection of technologies and processes that enable appropriate user access to resources across the enterprise, technologies with which organizations may authenticate, authorize, provision and store user access rights in a secure and scalable manner, based on business roles."[2]

Building Blocks of Enterprise Identity Management System

To establish enterprise identity management, an understanding of the building blocks or components of identity management would help an organization on establishing a comprehensive and complete identity management. For a typical enterprise identity management system, there are basically four main building blocks: Enterprise Directory, User Provisioning, Authentication Management and Access Management.

Enterprise Directory
This component is basically the heart of the whole enterprise identity management. It is the central identity repository to store all user information. It is shared by all applications in the organization as a central user identity repository. User personal data like name, address, department, contact number etc can be stored in the enterprise directory. With the central repository, each application will link with the enterprise directory to provide consistent user information across all applications. So whenever user information is changed in the enterprise directory, all applications will get updated user information. The usage of the enterprise directory can be extended to store user authentication and access information like user password or digital

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

certificate, the list of applications that user has access to, the access permissions on each of the application etc.

User Provisioning
User provisioning component basically provides a central facility to administer user accounts and provision user access across multiple systems and applications. It enables administrators to perform user account creation, modification and deletion to individual systems or applications from a central server. Administrators no longer have to go to individual system or application to provision user access. Now, when it comes to providing user access, normally an organization would have policy that requires authorization approval before user accounts can be created. So this component normally incorporate a workflow system to implement corporate user account request policies where approval from appropriate people need to be obtained first before actual user account creation and access to applications can be conducted. In addition to user account management, this component provides password management as well. This is basically to facilitate synchronization of user password across all systems whenever the user password is changed from the user provisioning component. [3]User provisioning component normally integrates with the enterprise directory and use it as a repository to store its user data information. The enterprise directory will keep information on the list of application accounts each user has. So whenever an employee leaves the organization, user provisioning component can retrieve the application list for the user from the directory and delete user account on the respective application.

Authentication Management
Authentication is the process of verifying the identity of the user in order to grant user access to protected resources. Authentication management component basically deals with managing user authentication by providing automated logon or single sign on solution to multiple applications for users. One of the problems users encounter with identity management is they have to remember too many user IDs and password for all applications they need to access. Single sign on (SSO) solution is meant to allow users to access multiple applications or systems while only having to authenticate once.[4]User will just have to remember only one user ID and password to get authenticated to all the application he has access to; thus user will have fewer problems in remembering the password. And as a result, it will improve user productivity and there will be fewer calls to helpdesk requesting password reset.

Access Management
Access Management component provides centralized access control on resources. Currently, each system manages its own authorization function by itself. An enterprise would want to ensure effective management of user authorization and access rights policy. There is a need to have a centralized access management system that will enforce authorization policy imposed on each user to all systems. So that there will not be a situation where a user access right to systems is not consistent across all systems. As the number of users to be managed increases tremendously, this problem will be out of control. This is why centralized access management is considered one of the key requirements on enterprise identity management. On access management, there are basically two access control areas. One access control area is on controlling the list of applications that user has access to. The other access control area is on the resources in each application that user

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

has access to. On controlling the list of applications or systems that user has access to, the centralized access management is indirectly provided by the user provisioning component as it is the component which control user account creation in all applications. By creating or deleting user account in each application indirectly control access to the application.

Identity Management Benefits

By having an enterprise wide identity management, an organization would gain both business and security benefits, with business benefits having the more prevalent reason for implementing identity management.

Reduce Cost and Improve ROI
By automating through user provisioning system, it will reduce the operation cost of IT department in maintaining the number of staffs needed to cope with the increasing workload. The centralized user repository reduces redundant maintenance work and re-entry. It also save cost on helpdesk operation by providing end user self service interface that will help to reduce helpdesk calls on password resets or changes. In application development, with the centralized access management, new application can make use of it without having to develop its own access management and thus reduce development time and cost. The return of investment of enterprise identity management if properly implemented is tremendous. As Gartner report stated, "Identity and access management (IAM) solutions, which can offer three-year return on investment in the triple-digit-percent range, are becoming essential tools for effective management of user account and access rights information across heterogeneous IT environments, for web and non-web applications."[5]

Improve Security
With an enterprise identity management, the overall security of the organization will greatly improve. With the centralized user provisioning and access management, corporate authorization policy can be fully enforced on individual user and thus reducing the risk of unauthorized access to critical resources, or disclosure of confidential information. It also help in security audit in the sense that terminated employee are completely and automatically revoked of all access rights to systems with the identity management system.[6] It reduces human errors in manually deleting user account and access rights across multiple systems. In password management, it also allowed an organization to impose stringent password policy with the centralized password management and SSO. By having user to remember only one user ID and password, user will have fewer problems in remembering difficult password as compared to previously having to remember multiple passwords. With the centralized access management, it will help to reduce administrators' errors in inconsistent access permissions configuration across multiple applications.

Improve Productivity
With the automation and centralized management of identity, IT administrators will have more time to concentrate on other critical support tasks. On the end user end, user will be more productive due to faster user account creation and password reset processes that will reduce user waiting time and frustration. With SSO, end user will

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

have faster access to business application without having to re-logon. On the overall enterprise level, identity management will improve business processes.

Improve Service
With the centralized user provisioning, it will improve the customer service level in terms of user account creation for e-business applications that are extended for access to external customers and suppliers. It also prepares the organization readiness to accommodate large number of users in its e-business initiatives. It indirectly reduces the organization business transaction cycle with external parties and thus creates business growth and distinct advantage over other industry competitors.

Implementing Enterprise Identity Management
Having understood the necessary building blocks of an enterprise identity management, to implement it, one has to know what current identity management technologies and solutions available as well as their limitation. This section intends to provide some insights into available technology, implementation challenges and considerations for each identity management component.

Enterprise Directory
The current solution to setup central identity repository for the entire identity management system is basically using LDAP/X.500 Directory. LDAP/X.500 is an open standard which we are seeing more applications or systems supporting integration with LDAP/X.500 directory to store its user data repository. For organization which has existing LDAP directories on certain applications, some may even use Meta-directory which provides centralized management of disparate directories within the enterprise.[7] Some of the key providers of LDAP/X.500 directory solutions are Sun, Novell, Critical Path and Microsoft. Ideally, the enterprise directory should be used as a single user data repository for all applications in the enterprise. However, not all existing applications are directory-enabled. And if the applications are directory enabled, one would have to figure out each application user record directory structure and merge them into one single directory structure for the enterprise directory schema. This is one of the difficult challenges when implementing enterprise directory. Currently, the idea of migrating all existing applications user data repository into an enterprise directory is difficult. Based on most of the identity management solution available, the enterprise directory is implemented by having connectors or agents on each application or system to replicate user data back to the enterprise directory. This is normally implemented with vendor identity management software that provides connectors or agents that run on each system or application to collect user data. The identity management software translates user data from different applications into a single user record structure that encompass user attributes from all applications and store it in the enterprise directory. The advantages of this technology is it enables existing non directory enabled applications or systems to integrate its user data repository with the enterprise directory. Normally the available solution using this technology provides a mechanism to synchronize changes between the individual application user data repository and the enterprise directory. Any changes on user data from each end would automatically replicate back to the other end.[8]

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

When implementing enterprise directory, one would have to consider the scalability and fault tolerance of the directory infrastructure. Considering the enterprise directory will be storing all applications or systems user data, the architecture of the enterprise directory infrastructure need to be scalable to accommodate large number of user information. It should be able to distribute or load balance the user data into multiple directory servers. And the enterprise directory should have failover facility as well considering each identity management component and application will be accessing it. With only one directory server, there will be a single point of failure for the whole identity management system.

When the enterprise directory is in place, new applications to be deployed in the enterprise should start incorporating integration with the directory in order to retrieve user info and access info from the directory. The idea of individual user repository should only be acceptable for existing application but not any new applications. This is to achieve an environment in the long term where all applications are integrated with the enterprise directory in the future. For existing applications that are not directory enabled but using the connector technology, future plan should be work out to upgrade them or replace with one that is directory enabled.

User Provisioning

This component is considered to have the most established solutions. There are many solution providers like Waveset, Access360, Business Layers, blockade system and Oblix, that provides user provisioning solutions. The current technology available to provide enterprise user provisioning mostly uses manager and agent concept.[9] Whereby in each system or application to be managed, there will be agent software running on the system. The agent software would understand how user accounts are managed in the particular application and perform user account creation, update or deletion. Some vendor solution provides only one way synchronization of user data between the manager and the agent while some vendor solution provides bi-directional synchronization. The advantage of bi-directional synchronization is that whenever there are changes in the local application user data, the agent will update the manager with the changes. This makes sure both ends having identical user data. The manager/server component basically provides the administrator a single console to manage user data across all applications.

As far as the current user provisioning solutions available, most of them support managing user accounts in major operating systems, databases and applications. Operating systems like UNIX, NetWare and Windows, Oracle and MS SQL databases, MS Exchange and Lotus Domino, ERP applications like SAP and Peoplesoft, are mostly supported. And if certain application is not currently supported, normally the solution providers provide API toolkits to extend support to customized applications. So if one has certain in-house developed applications, these applications can still be integrated with the enterprise user provisioning component using the toolkit. This will enable centralized management of user data on those applications as well.

As stated earlier, one of the key requirements of enterprise user provisioning system is the availability of a workflow system to implement the organization user account creation or deletion approval procedures. Most user provisioning solutions available

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

provides a workflow engine. The workflow engine allows one to pre-define the approval process and it automated routing of the approvals by notifying the respective approver via email. Then the approver can approve the request via a web interface provided. The mapping of organization workflow to technical solution is not a simple task. Although almost all vendor solutions provide the workflow engine, one would have to look detail into the capability of the workflow engine in terms of availability of multi-step approval process that can meet your organization workflow process.

Another important requirement of enterprise user provisioning system is the ability to delegate user provisioning functions to other department administrators.[10] As one of the purpose of centralized user provisioning is to allow other departments like human resource department to be able to create user accounts for multiple systems. This will solve the problem on existing identity management method which depends mainly on IT staff to perform the user account administration. When looking for available solution on user provisioning software, one has to make sure this feature exist on the solution.

Another feature that currently most user provisioning solution providers includes is the user self service web interface.[11] The self service web interface allows users to address identity management problem themselves. They can use it to reset, change passwords across all systems without having to go through IT administrators or helpdesk staffs. They can also request application access to the system and the system will automatically trigger the workflow process for access approval. This feature enables cost saving in terms helpdesk operation costs as the volume of helpdesk calls on password reset will be greatly reduced. It also helps in user productivity as he/she does not have to wait for others to execute the password reset request. For external user, specifically when the organization has established customer based extranet applications, the self service interface can be used to provide convenient customer self registration facility for them to access to those applications. Based on Meta Group recent survey, with the self service user provisioning interface, organizations gain 13% employee productivity improvement and 14% increased in operation efficiency.[1] Organization planning to implement user provisioning system should make sure the self service interface is included in the requirements.

Another common feature in current available user provisioning solution is role based access assignment. Basically the system allows one to associate list of application or system access to user job role. So when a new user come into the organization, the administrator just have to assign the user to its job role and the system will automatically create the respective user account on all the systems or applications.

Other than features, when implementing user provisioning solution, one has to look into the scalability of the system. Considering that user provisioning will be done centrally for all applications, the solution must be able to cope with large number of user identity as well as the future growth of user identity. Another concern would be the secure communication between user provisioning system and the application systems. As user IDs and passwords will be sent across the network when the manager instructing the agent on the application system to create user accounts, it is important to provide proper encryption for the communication link.

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

When implementing enterprise user provisioning system, there are certain non-technical challenges that the implementer has to face. Specifically on defining business rules on user provisioning, there will be numerous hurdles in getting corporation from different department of the organization in releasing the rights to control application access to another entity or department in the organization. There will be political issues that one has to confront. In order to avoid these types of issues, it is important that one get management support in terms getting their participation in the project committee in the beginning. It will help also in terms of getting individual department allocating adequate resources.[2]

Authentication Management

As stated earlier, authentication management deals with providing single sign on. The current SSO technology provides single sign on for both non-web application and web-based applications. But majority of the solutions available in the market provides single sign on solution on web based application only. Some of the key solution providers in this area are RSA, BNX Systems, Oblix, Computer Associates, Blockade and Netegrity. One of the existing SSO technology is using network operating system based SSO. Like Microsoft and Novell, when a user logon to NT domain, Win2K Active Directory, or Novell NDS, the user does not have to re-logon again for those resources like printers and file shares that are using network operating system security. Existing applications that integrate network operating system security to provide access control can be accessed without re-logon as well. This technology however forces one to standardize all applications running on a single operating system. It limits the choices of applications that can be deployed to those that can run on the particular OS. Nevertheless, for those organizations that have all applications integrated with operating system security, this technology can still be used to provide single sign on solution. [12]

Another current technology how SSO is implemented is using "automated insertions".[13] Automated insertions basically use scripts to send the user credentials like username and password to the application logon window when it is launched. This type of technology stores every user's login ID and password to every supported application in the SSO server. And normally there will be SSO client software installed on the user PC. Upon authenticated at the primary single sign on using the SSO client software, user will launch various applications through the SSO client program and the SSO client program will get the respective user credentials for the particular application and send keystrokes to that program simulating as though the user is typing his own ID and password. One advantage of this SSO technology is that it can support SSO on different types of applications like windows-based, web-based and even terminal emulated applications. Another advantage of this technology is there are no configuration changes or code modifications required on the application. So the deployment of SSO solution is much easier and faster. The way how it knows how to feed user credentials to the application logon is by capturing the logon attributes inside a window in the non-web application and the logon fields in the forms of web based application respectively. So the script will basically detect these attributes or fields and send the relevant user credentials. Normally solution providers of this type of Single Sign On technology provides communication encryption between the SSO server and the SSO client considering

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

that user credentials will be forwarded from server to client for logon. If one is planning to use this type of technology, the encryption used and how the user credentials are handled in the SSO client should be carefully look into to avoid any security vulnerability on the SSO solution. Another area of concern when implementing this SSO technology is the SSO server fault tolerance. Considering all user PCs with SSO client will need to communicate with the SSO server for single sign on, the solution should have fault tolerance and load balancing features that allow multiple SSO servers to handle the services. Although this technology is easier to implement, the disadvantage of this technology is it does not resolve the multiple authentications issue. It simply masks the problem. In the long term, when more and more applications are deployed, it makes the idea of reducing authentication systems more difficult to achieve.

Another approach how SSO is implemented is having agent software running on application and the agent intercepts user access. This approach normally works on web based application only. There will be web server agent or web application agent installed on each web server. Whenever user tries to access a resource like a web page in the web server, the web agent will intercept the URL request and request authentication from the user. The user supplied user credentials will then pass to a central policy server that will validate the access. Upon validated, an encrypted cookie or ticket containing the user session info will be created at the user end. When user tries to access other resources on the same web server or other web servers that has agent software installed, the agent software again will retrieve session information from the cookie and verify with the central policy server as to whether the user has logon and have proper access rights. If validated, the user will be allowed to access the resources without having to re-logon again; thus providing single sign on for user.[13] The advantage of this approach is that there is no SSO client software need to be deployed to all PCs. This approach will be useful for providing single sign on solution to external parties like customers, partners or suppliers as no SSO client software need to be deployed to the external users. So the deployment of SSO feature on web applications that external party need to access will be fast and easy to maintain.

So which type of Single Sign On approach should be applied? Well, it will depend on the type of applications that requires automated logon. If there is a mixture of Windows based application and web based application, the automated insertion method will be more appropriate. However, if the organization is planning migrating existing applications to web based application, then it will be much easier to maintain the SSO system using agents on web server as this approach is normally implemented by the centralized web access management solution that we will be explaining on the Access Management section.

On the integration of Single Sign On system with the enterprise directory, it is mostly done on sharing the user repository whereby SSO system will either store its user repository in enterprise directory or synchronize its local user repository with the enterprise directory.

Although Single Sign On helps users in automating logon, one would have to look into the single logon security requirement when implementing Single Sign On. As now with just a single logon, users can have access to all authorized applications. If

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

the existing password policy is not strong and users use easy guessable password, it will be a security concern as potential hackers would be able to crack the password easily. Therefore, more stringent password policy or stronger authentication method like smart card, token devices should be implemented to enhance the primary logon security.

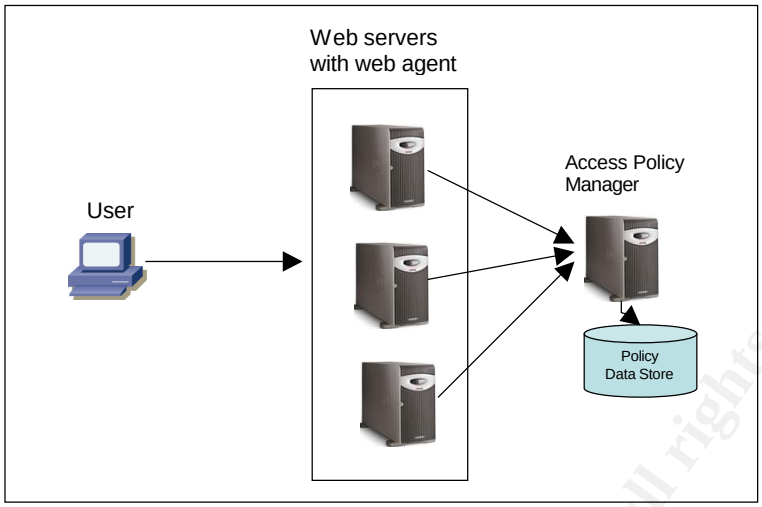
Access Management

To implement centralized access management across the enterprise, ideally using the enterprise directory to store user privilege information for all application and all applications verifying user access rights from the directory would be the best solution. However, this approach is difficult to achieve. To consolidate user privilege information from all systems and applications is a challenging task due to different user access definition. Moreover, most existing applications do not support integration with LDAP directory to synchronize user access rights with the directory. This approach will only be feasible as and when new version of software applications started to support directory and new application are developed with storing user access privilege information in the directory. In order to achieve using directory to manage user privilege information down the road, one should start planning for subsequent new application rollout to have this integration.

Based on current available solutions, the practical solution to implement centralized access management is to provide a separate layer of access control module running on the application server or an access control proxy server in front of all application servers.[12] Instead of developing security access control locally within the application that can not be centrally managed, the new access control module or the access control proxy will intercept access requests and communicate with a central policy server to verify access. Based on available vendors providing this technology, most of them provide web access management only. The solution only supports web server and certain application server like WebLogic and WebSphere. Although some of the vendors provide APIs for one to extend access management to non-web based applications, normally the development is complex and time consuming. On the architecture of this type of solution, it uses the manager/agent model or proxy model.

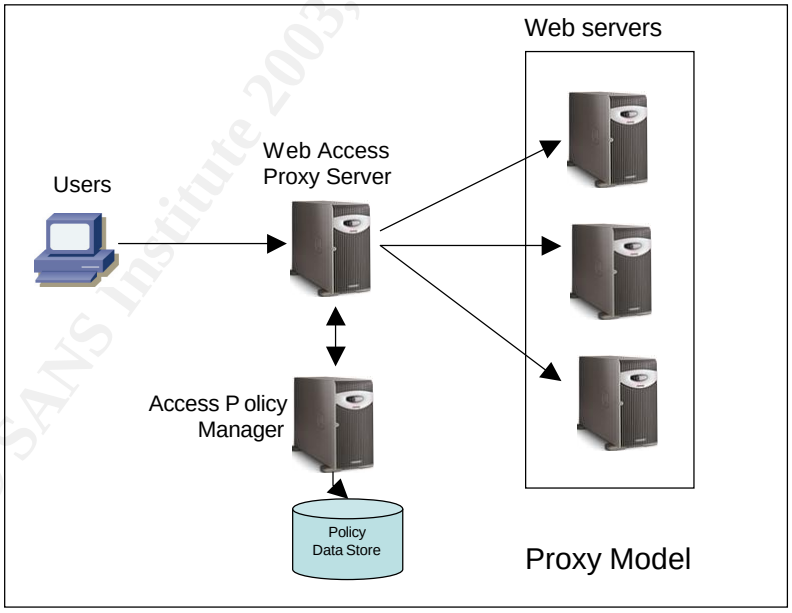
The following diagram is an example of manager/agent model.

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.



Manager/Agent Model

In the manager/agent model, by defining user access rights on the manager, whenever user try to access certain web application on the web servers, the agent sitting on the web application server will intercept the request and request authentication from the user, verified with the manager on user access rights before allowing access. The disadvantage of this model is the overhead of deployment and maintenance of agents on the web servers. It also places extra load on web servers due to the agent. On the proxy model, as shown below:



It works like a conventional proxy server where it intercepts all HTTP/HTTPS traffic flowing to the web servers and verify with the access policy server as to whether the access is allowed or not. The advantage of this model is it is much easier to manage as there is no agent required on the web servers. However, if the web proxy server does not have any failover or load balancing feature, it would be a single point of

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

failure. Some of the vendors using this approach of access management using either model are Netegrity, Tivoli, Oblix, RSA and Computer Associates. Normally the types of web resources that this solution can manage are URLs, files, documents, servlets, JSPs, EJB components etc. Looking into the current solution available, to implement centralized access management across the enterprise, it is only possible for web enabled applications only.

In terms of defining user access privileges, one of features current access management solutions provides is Role based Access Control (RBAC).[14] The concept is to define user access privileges based on user job functions or roles. With this method, one can have more effective access management. Basically RBAC allows administrators to associate access to resources to individual job role and the administrator just have to assign each user to its respective job role and the relevant access rights will be given. This is based on the fact that each job role irrespective of multiple users having the same job role logically should have the same access rights. RBAC makes managing access easy as when user move from one job role to another, one just have to change his access rights by just migrating between job roles only. RBAC reduces changes to access control definition, reduce duplication of access control definition and improve accuracy of access control information. When implementing access management component, one should make sure this feature is provided by the chosen vendor solution. The other requirement that one should look into is access administration delegation. Upon establishing enterprise access management, one would want to delegate other department administrators to be able to perform access management of applications.

On integration of access management with the enterprise directory, most of the current access management solutions provide integration with the enterprise directory through linking user repository. The access management solutions either synchronize its user repository with the directory or store its user repository in the directory. Most of the solutions do not provide integration of user access policy or rules with the enterprise directory but store its policy information locally on its own repository. The fact is that each vendor solution would have its own format for access policy. It is difficult to come out with a structure that will integrate with enterprise directory structure.

Besides from technical issues during implementation of access management across the enterprise, one would have to expect political issues abound during implementation. As the implementation involves reviewing and defining access policy for all users based on the job roles, it requires a thorough review of the existing individual department, function, role and human resource policies. And this requires cooperation from all business units in the enterprise. When it comes to deciding about who and what access to give to each key corporate resources based on user job role, it is not the IT department that will decide it. Instead, the business owner of the resources would need to decide what roles will have access to the system and what access rights of each role have. The implementation of role based access control in identity management requires clear definition of roles from business rules. And if individual business unit leaders who own the resources would not cooperate on defining access, it will delay the whole implementation. Furthermore, with the centralized access management, there will be changes to business rules or procedures that release the control on applications from existing administrators or

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

owners to other departments. Certain administrators would not be happy with this. Similar to implementing user provisioning component, it is important that one get management support in terms getting their participation in the project committee. It will help in terms of getting individual department cooperation during implementation in order to implement successfully. [2]

For all components of enterprise identity management, one should make sure proper security auditing facility is in place. As with the enterprise identity management system, it has control of all application systems in the enterprise in terms of providing access as well as defining what access privileges. Keeping track of who create/delete user account, when accounts or access rights given and what applications been given access etc is important for future referral when any incidents of improper access happens. Besides from security audit logging, security report generation should be built into the identity management system to provide overall access privileges based on individual users. For example, one would want to generate reports on list of applications that user has access to and what are the access privileges given. So when it comes to security audit, one is able to present user access privileges when requested.

Having gone through the current technology, implementation consideration of each of the identity management building blocks, it has not been discussed on the integration between the components. When it comes to integration, what we are looking for are mainly sharing of repository between components, having a single management interface and cross integration of policy.[12] Assuming that each component would be pretty much implemented using vendor provided solutions instead of developing from scratch, how integration can be done will require further understanding the architecture of each solution. Looking at the current solutions available, One possible integration between the components that can be done is on the user repository where each component can shared a single user repository using the enterprise directory. This is provided each component has the option to store user repository in the directory and one would have to work out on combining each component user record structure into a single structure for use in the enterprise directory. Other than that, the full integration of all components of identity management can only be achieved if one vendor is providing all components of identity management with integrated functionality. Be aware on certain vendors that provide all components of identity management solutions but without integration.

Overall Implementation Strategy

After understanding the technology and implementation requirements of individual component of enterprise identity management, it is best that organization follow certain strategy or best practices in order to setup a successful identity management system and avoiding common mistakes.

Set Clear Goals

It is important to define clear objectives for the establishment of enterprise identity management. And the objectives defined should be based on business needs instead of just purely on security. Perform an assessment on internal organization processes that look for areas where identity management will be able to help in improving the process and thus improving business and use it as goals for the

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

project. Try to set objectives that are more incline towards solving key business process obstacles or creating more business opportunities to the organization.[12] One example would be certain compliance requirements or laws on information security that organization must comply before it can extend business transaction with external users. This will help one in getting management approval for the investment on the system. If return of investment can be calculated, that would be even better to justify the investment.

Obtain Management Support

As stated earlier, one of the challenges of implementing identity management is getting cooperation from various business units in the organization to decide on access rules and define roles. In order to get their support, one has to get the recognition from the senior management on the benefits of identity management as well as getting them involved in the project committee. The upper management has to communicate the message down to each business unit involved. By doing so, only then the changes required on the existing organizational processes can be executed. With the identity management project committee encompassing cross-organizational team members, representative from each business unit in the project committee can ensure the project implementation get appropriate attentions and adequate resources.[5]

Implement in Stages

Implementation of enterprise identity management should be deployed in stages as the implementation process is complex and time consuming. Implement first those solutions that will immediately solve the pain of the organization and it is not difficult to implement. The other reason of implementing in stages would be to assess the outcome of each phase before proceeding to next phase. By assessing the previous phase and knowing all the issues during implementation, one could avoid repeating those mistakes on the subsequent phases.[15] To implement in stages, one can separate the enterprise identity management implementation based on identity management component basis and also scope the group of applications or systems involved in each phase. In terms of implementing identity management in phases by prioritizing different group of application systems, one would have to depend on the current immediate requirements of the organization as well as the ease of integration. One might prioritize those application groups that have severe, immediate identity management issues to be implemented first as the benefits outcome from these applications will be significant and this will help the overall support from the organization for the subsequent phases. Although implementation in phases is important, one thing must be keep in mind as well is the design of each component's architecture. The individual component design architecture must be able to cater to the final overall architecture design of the whole identity management.

Select Solution

When it comes to evaluating and selecting vendor solutions for each component of identity management, it is important to select the solution that can meet your organization identity management goals and objectives. The solution must be able to meet the requirements of the existing infrastructure, workflow processes and

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

applications involved.[12]The selection criteria would have to look into the ease of integration between the components as well. Don't just blindly select best of breed products in the market.

Summary

Enterprise identity management basically deals with authenticating, authorizing, provisioning and storing user access information in a secured, scalable repository based on business roles. Considering the complexity and challenges of establishing enterprise identity management system, enterprise identity management is considered one of the most difficult IT infrastructures to implement. Looking at the current development of identity management technology and solution, it is still difficult for one to establish a fully integrated enterprise identity management. However, it is still possible for one to establish some of the identity management components that have much mature solution. As and when new technology is developed, the rest of the components can then be implemented in stages and at the end one would be able to establish a complete enterprise identity management system. No matter how difficult it is, it is better off one start to consider implementing it now then later when it is out of control. Furthermore, with the current continuous trend of organizations extending more e-business initiatives, enterprise identity management is becoming a vital enabler of e-business strategy. Organization that fails to implement enterprise identity management now will be at a distinct competitive disadvantage. By knowing the challenges ahead and applying proper implementation strategy, organization would be in a much better position during implementation of enterprise identity management. And when the enterprise identity management is in place, it enables the organization to provide a much secured, efficient environment for customers, business partners and employees to access various business applications.

© SANS Institute 2003, Author retains full rights.

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

References

[1] Meta Group, Inc. “The Value of Identity Management: How securing identity management provides value to the enterprise.” August 2002. URL: http://www.pwcglobal.com/Extweb/service.nsf/8b9d788097dff3c9852565e00073c0ba/88a387cdb58b4c0085256c6a006e0036/$FILE/ValueofIMWhitePaper.pdf (March 9, 2003).

[2] PricewaterhouseCoopers. “Identity Management: The business context of security: a white paper.” Jan 2002. URL: http://www.pwcglobal.com/extweb/manissue.nsf/2e7e9636c6b92859852565e00073d2fd/090fbb3500f5b14380256b0a003b998a/$FILE/IM%20White%20Paper.pdf (Feb 27, 2003).

[3] M-Tech Information Technology, Inc. “Defining Enterprise Identity Management.” June 28, 2002. URL: http://www.idsynch.com/docs/identity_management_defined.html (Feb 27, 2003).

[4] Yasin, RutRell. “What is Identity Management?” April 2002. URL:http://www.infosecuritymag.com/2002/apr/cover_casestudy.shtml (March 2, 2003).

[5] Witty, Roberta. “ROI Drives Identity and Access Management Implementation.” Feb 6, 2003. URL: http://www.csoonline.com/analyst/report858.html (March 1, 2003).

[6] Shillito, Peter. “Identity Management – Delivering Security and Value.” June 12, 2002. URL:http://www.nifosecnews.com/opinion/2002/06/12_04.htm (Feb 27, 2003).

[7] isode. “Meta-Directories: Cutting Through the Hype.” Nov 26, 2002. ULR: http://www.isode.com/whitepapers/ic-6087.html (March 24, 2003).

[8] Napoleone, Fino. “Blockade ManageID Life Cycle Management of User Identities.” Jan 17, 2003. URL: http://www2.blockade.com/products/WhitePapeLifeCycleManagement.pdf (March 22, 2003).

[9] Berndl, Walter. “Scalable, Resilient Architecture for User Provisioning.” Feb 3, 2003. URL: http://www2.blockade.com/products/ArchitectureforUserProvisioning.pdf (March 22, 2003).

[10] Waveset. “White Paper: Identity management trends, challenges and solutions.” 2003. URL: http://www.waveset.com/Solutions/Resources/WP_IdentityMgt.pdf (March 22, 2003).

[11] Hurwitz Group. “Identity Management – A Fundamental Discipline in Security.” October 2001. URL: http://www.courion.com/products/idc_self-service.pdf (March 1, 2003).

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

[12] Reed, Archie. “The Definitive Guide To Identity Management.” 2003. URL: http://www.rainbow.com/idebook/chapters.asp (March 22, 2003).

[13] BNX Systems. “Enterprise Single Sign-On: Balancing Security & Productivity.” 2002. URL: http://www.bnx.com/pdf/Enterprise%20Single%20Sign-On%20-%20Balancing%20Security%20&%20Productivity.pdf (March 22, 2003).

[14] Netegrity. “Netegrity SiteMinder 5.5- Technical White Paper.” Sept 2,3 2002. URL: http://members.netegrity.com/access/files/Siteminder55.pdf (March 22, 2003).

[15] Ford, Mark. “Guest Column:Identity Management’s Role In The Enterprise.” June 5, 2002. URL: http://www.internetwk.com/story/showArticle.jhtml?articleID=6406259 (Feb 27, 2003).

© SANS Institute 2003, Author retains full rights.

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.