Identity Management

What the Software Vendors *Won't* Tell You!

BY TED BALFOUR

With the current regulations and audit requirements being placed on organizations, many companies are looking to Identity Management (IdM) solutions to help achieve control of who within the organization has access to what resources. This includes not only the provisioning of access rights, but also the ability to change access when individuals change positions, and rapidly and completely remove access when employment in terminated.

The available commercial off-the-shelf (COTS) applications are very capable of performing these tasks in an automated fashion and include many features such as enterprise wide password management, self serve functionality, approval workflows, timed events, high privilege account management (firecall accounts), Role Based Access Control (RBAC), and compliance reporting. With all these capabilities, it becomes obvious in a very short period of time that these features will provide great value to an organization by eliminating or reducing manual processes, decreasing potential for human error, improving the time to productivity of new employees, and maintaining control of who is accessing what resources.

The identity management companies will be more then happy to tell you all the wonderful benefits available with their products, these benefits can be huge. What you may have difficulty determining is what it is going to take to deploy this software. During the sales cycle, you will hear many grand stories of how a vendor can assess your environment and accurately design an implementation solution within a couple of brief weeks -- and that the actual deployment will take place and be in production in no time. This is also where the flashing red lights should go off with a large blinking "warning" sign in your head.

Let's face it, in order to properly deploy an enterprise-wide IdM solution, you are redefining how a critical component of your business operates, or, in other words, you're taking on a business re-engineering effort. To suggest that this can be done in a short period of time with little design effort is not only unrealistic, but rather insulting. Now with a bit of the dirty laundry about identity management on the table, let's talk about a realistic approach if you truly plan on succeeding with this endeavor.

Key Success Factors

Implementing an identity management solution is tangled with complexities. A winning identity management strategy should address several key considerations.

Tackle the provisioning problem first.
Since creating, revoking and managing access credentials is a core function, proper design can make or break any identity management deployment.

Consider identity management as a core service.
Do not attempt to cost justify IdM on the basis of one or two applications. IdM is complicated and crosscuts most administrative functions in a company. Done right, it can enable tremendous employee and customer benefits.

Create globally unique identifiers.
Consider the use of human resources data as a means for creating the unique identifier and eliminate the temptation of allowing application, group or regionally specific identities.

Strive for role-based access controls.
When combined with business rules and policy enforcement, roles can be very granular. Individual access control profiles are nearly unmanageable in most organizations. Roles and rules offer the same benefit with dramatically reduced administrative burden.

Keep the technology hidden from users.
Wherever possible, use vendors of custom connectors to shield the user from authentication technologies. The less often users have to deal with them, the more comfortable they will be in adhering to the policies set by the organizations. PKI, certificates, tokens, biometrics and the like all have their place.

Consulting Versus In-House

Many companies have attempted to deploy IdM solutions on their own with varied levels of success. Unless you have resources on staff with a significant amount of experience in this area, experts suggest you consider hiring a company that is well versed in the technology you choose. These projects consist of a plethora of integration activities along with very detailed configuration parameters, requiring individuals skilled in many different areas. Of course, there are many training courses available to teach the technology. However, it has been proven time and again that, without real world deployment experience, the information gained in the training class will only take you about half the distance required to handle a full blown production deployment.

In the interest of becoming self sufficient in the shortest order of time, sending your staff to training just before the implementation activities begin, and then having them work side by side with the consulting team, produces the best results. This allows the freshly trained staff member to work with an experienced individual in their own environment.

Over the past several years, best practices have proven that multi-phased implementations are truly the only realistic approach. By training your staff early and then having them work with the consultant on the first couple of phases, they will be much better prepared to proficiently handle the additional phases with little or no assistance.

Design As You Go – Not Likely

If you are led down a path that suggests the assessment, design, and deployment of your IdM solution can be done in a few weeks, be assured that what will really be happening is a "design as it's built" approach, and you will be riddled with change orders.

A similar scenario would be to hire a builder who presents you with a plan for a house that has a foundation, four walls, and a roof and will cost you $100,000 for live-in conditions. You sign the contract, and when the job is just about done, the contractor approaches you and inquires if you would also like windows in this house. Rather perplexed that this had not already been done in the initial phase of the project, you nod yes. He then tells you that an additional $50,000 is required to have that feature and he has to cut holes in the new walls. He then asks if you plan on having separate rooms in the house, which, again, of course you do, so now you need an additional $250,000. Next comes questions about lights, bathrooms, kitchen, doors, etc. You get the point. For an additional $500,000 above the original estimate, you get the house you really wanted.

Bottom line: you realize if you had hired an architect, all these things would have been handled initially. You would have known the true cost of the project at the get-go.

Like this scenario above, the proper approach to an IdM deployment is for your vendor to understand your requirements at the beginning, perform an assessment, and then develop a solution design. Of course, throughout the design, you should be interacting closely with the vendor to make sure that the end result is what you really want implemented.

Process is King

The way your company has evolved has been the impetus for many of your current methods of getting the job done. At the time it was done, it probably was the most efficient way to resolve the issue at hand, but over time you add more complexity, more features, more functionality, but rarely re-evaluate the method in which access is granted. This results in "wedging" in a quick fix to get the desired solution accessible in the quickest manner possible. This is all done to meet business requirements and to ignore that in the design phase would be irresponsible.

Remember, an IdM deployment is a business process re-engineering effort. In order for any vendor to properly deploy the solution, they must first gain an understanding of your current processes and requirements in order to ensure that the desired end result is achieved in the new solution. Once they have done that, the design process can begin, which should also have clearly defined "to be" process models.

Now that the requirements have been gathered, assessment and design completed, the vendor should be in a position to give you a very accurate statement of work and project plan that ties back directly to the design document.

Up to this point we have discussed what it takes to get to the deployment stages of an IdM solution. By now you may realize that these are the most critical elements to achieve success. Let's face it, if you don't have a road map, you will get lost and will be asking for a lot of costly directions.

Ted Balfour is the senior vice president of NetworkingPS's Security Management Services Practice, as well as a partner within the company. He can be reached at tbalfour@networkingps.com.

MORE INFO

Read Part 2 of this article in TechNews Interactive.

(This is the second half of this article. The first half can be found in the print and interactive versions of TechNews.)

Identity Management Best Practices: What the Software Vendors Won’t Tell You

By Ted Balfour

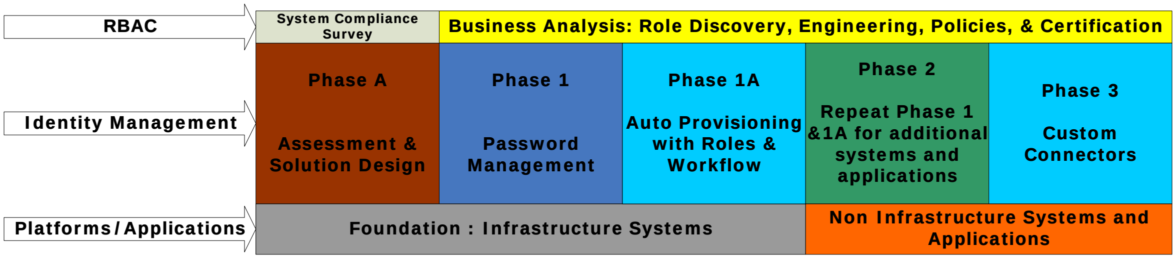
By reading the printed first half of this article, you have an idea of what it takes to get to the deployment stages of an Identity Management (IdM) solution. By now you may realize that these are the most critical elements to achieve success. Let’s face it, if you don’t have a road map, you will get lost and will be asking for a lot of costly directions.

Staged approach

A “phased” approach to implementing an IdM Solution is the only realistic approach. This “phased” approach creates an organized timeline and project plan for rolling out an IdM solution in the shortest possible amount of time and with the lowest possible costs for an organization, while at the same time minimizing risk in proportion to the scope and requirements of the entire project.

The simplest rationale to this implementation plan is to enable your internal staff with the appropriate skills as early as possible in each key stage and milestone to enable self-reliance as quickly as possible.

This approach also naturally restricts each phase into manageable chunks, while delivering clear, tangible value every step of the way, so your organization can commit to business-related deliverables and deliver those values and ROI as planned.



RBAC

System Compliance Survey

Business Analysis: Role Discovery, Engineering, Policies, & Certification

Identity Management

Phase A

Assessment & Solution Design

Phase 1

Password Management

Phase 1A

Auto Provisioning with Roles & Workflow

Phase 2

Repeat Phase 1 &1A for additional systems and applications

Phase 3

Custom Connectors

Platforms/Applications

Foundation : Infrastructure Systems

Non Infrastructure Systems and Applications

Phase 1: As soon as the base IdM solution is installed, the first few critical applications or back-end system should be integrated into the IdM system. Once those back-end resources are connected, orphan accounts will be identified, adopted and otherwise cleaned up, and self-service capabilities for that user base will be initiated for password resets and forgotten passwords.

Phase 1A should include the automatic provisioning and workflow for infrastructure accounts for those same critical systems. This process should be dynamically driven by attribute evaluation, based on organizational unit, job title, business role, etc. Once that process is complete, automated approval workflows and RFI workflows should be created.

Once Phase 1 and 1A are complete, they can be combined and repeated by your group to bring on other standard systems. We assume that during the first Phase 1 and Phase 1A, internal staff is learning the necessary skills in which to achieve this, so more activities can be conducted internally and in parallel as the project progresses, thus ultimately reducing your overall time-to-market and implementation costs.

Phases 2 will include all the non-infrastructure based applications and systems in your IdM implementation, and will be dependent on the integration of the systems rolled out in phases 1 and 1A.

Ultimately, lessons learned will enable refinement and replication across other business units. Although this project phase is the most complex and far-reaching, it ultimately will have the highest long-term rewards.

While implementing an IdM solution, it is recommended that to recognize the full value of that solution, organizations should be moving toward a role-based provisioning model. Phase 2 should include the formation of Role-Based Access Controls (RBAC) for out-of-the-box services and applications (services and applications which require custom connections into the system will be done in Phase 3). A full analysis of business role requirements will be conducted, as well as the mapping of business roles to actual user and group access rights. Depending on the size of the organization, this process can be conducted much more quickly and efficiently using a vendor-based solution.

Ultimately, once this mapping and analysis is complete, these roles and policies should be defined as either static or dynamic within the IdM system. Once this process is finished, provisioning and de-provisioning of access rights will be fully automated and role-driven.

Ted Balfour is the senior vice president of NetworkingPS's Security Management Services Practice, as well as a partner within the company. He can be reached at tbalfour@networkingps.com.