Yes, We're Open for Business!

Utilizing Identity Management's Open Services

By Chris Williams

OVER the past few years we have been witness to amazing growth within the computer security industry. Obviously, this is not startling news. A user can open any computer-related publication, or even just watch the evening news broadcasts, and arrive at the same conclusion. What is interesting, and not as widely known, is that the security discipline focused on people and their regulated access to resources, Identity Management (IdM), has also seen this same growth spurt. What once was a traditional exercise of maintaining user accounts on independent systems has evolved into a series of people-centric, meta-data exchange and management processes.

The key driver behind the growth of Identity Management has been the pursuit of secure commerce. Not only have businesses been required to protect their assets, they also have to ensure their customers have a safe and trusted environment in which they can conduct their transactions. Add to this the rash of regulatory acts that have been penned into existence over the past three years, and we begin to realize that this sudden growth is only the forefront of the Identity Management revolution.

Independent system and application user account administration has matured into the security discipline of Identity management. Having been spawned from a set of policies very rich in process and controls, the administrative routines used today are generally well-defined, efficient and deliver a safe environment where the modern provisioning process is automated. Of course, having overcome one set of obstacles, we now find ourselves faced with a new set of challenges; Identity Management data sources have proliferated. Their locations and formats have become more widely diverse and distributed, and the need to leverage a common set of technologies to manipulate and share that data has become imperative. On top of this, we still have the basic requirement to foster the responsible management of identity information and to facilitate the ongoing life-cycle issues of access provisioning.

To satisfy these requirements, the Identity Management industry has developed a number of technologies and processes. Collectively, they are sometimes referred to as Open-Services architectures, an integral hub in the Identity Management environment. This integration middle-tier is designed to provide a common and consistent interface for interconnecting identity services and processes with various front-end applications, data stores and application clients.

Acting as an intermediary for data consolidation, federation, and common provisioning processes, the Open-Services architecture is a strong conduit for exchanging data between IdM sources: business partners, contracting service providers, your employees and, of course, customers. Where as Service-Oriented Architectures are more generally focused on web-based business applications, Open-Service architectures facilitate the exploitation of data regardless of location.

APPLICATION INTEROPERABILITY

The basic mission of an Open-Services provisioning architecture is to translate various IdM requests for services or data from the client systems and applications. The translation of the system or application service request and logic of the target clients is done at a service parameter level. An example of this request can be found in the Service Provisioning Mark-up Language (SPML), which is quickly becoming a readily available provisioning standard. SPML allows the declaration of provisioning actions through the articulation of very basic verbs. Like all mark-up language standards, SPML is designed to simplify the programming process required to incorporate both "off-the-shelf" vendor-provided solutions, as well as unique or internally developed applications. It offers a core and common set of exposed services, in turn offering a simplified development process and eliminating the need to create new API procedures.

WHAT STANDARD SERVICES SHOULD BE PROVIDED?

User data definitions reside everywhere: mainframes, midrange servers, desktop systems, and a wide variety of hand-held mobile devices. By utilizing the resources of each system, an Open-Services middle-tier exposes the complete range of functionality within each of the environments that house user data definitions. For example, if a UNIX server houses web-based applications, then the Open-Services architecture could call upon XML Web Services or Web Services Description Languages (WSDL) to execute Identity Provisioning activities.

To further illustrate, if an application has been developed using .NET, those standard system calls need to be made and properly translated to the IdM engine. Basically, the availability of these standard services enables developers to access Open-Service functionality using any preferred programming language such as C++, C, or .NET due to the language-neutral alternative to working directly with the source API's.

GREATER BUSINESS SERVICE

So what does this Open-Services Architecture and increase in IdM data portability mean to an organization? To begin, stronger authentication practices can be incorporated, such as multi-factor authentication processes and both Reduced and Single Sign-On.

New industry standards, such as SPML, are easier to utilize, promoting the inclusion of Operating Systems, Human Resource applications, business application suites, or any environment with user data definition integrated within IdM efforts. LDAP directories can be used both as authoritative sources and as recipients of data, promoting a singular system of record or distributed federated cells of data. In essence, it means more secure business practices due to the ability to execute more granular identity processes with greater ease.

However, one of the greatest advantages of leveraging Open Services architecture is interoperability beyond a singular IT discipline. This need has driven organizations to begin following disciplines created by the Information Technology Infrastructure Library (ITIL). ITIL requires and enables interoperability across all IT layers including service level, security, change, and configuration management.

Achieving this goal is hastened by the need for common actions, common code, and common processes. The Open Services middle-tier allows each native computing entity to use the same interactive verbiage eliminating redundancy of design and custom coding. Also, once a standard methodology has been approved by the Change/Configuration/Release Management teams, evaluation and acceptance test time is drastically reduced.

Ultimately, success is not measured by how unique or ingenious IT solutions are designed and operate; organizations are simply measured by how well business is executed. IT supports a company's critical business services and a well-defined Identity Management environment can improve business performance. Utilizing Open-Services architecture enables greater visibility into a company's critical business services, and makes sure that the right people have access to the right resources for the right amount of time. This combination enables businesses to meet and/or exceed service level agreements, increase customer satisfaction and augment business agility.

Christopher Williams is the Marketing Manager for BMC Software's Identity Management Business Unit. With over 23 years of experience in the IT industry, Williams has served in a variety of data management organizations whose businesses ranged within a number of different industries including textiles, financial, retail, defense contractors and software vendors. Throughout his career, Williams has been centered on managing various technical implementation and support teams, data center management, enterprise-wide project management, as well as infrastructure management. He also performed numerous tasks including implementing operational and security oriented solutions and strategies affecting all disciplines within the IT industry.