The Identity and Access Management Scenario

Gartner The Future of IT Conference

October 4-6, 2011
Centro Banamex
Mexico City, Mexico

Notes accompany this presentation. Please select Notes Page view.
These materials can be reproduced only with written approval from Gartner.
Such approvals must be requested via email: vendor.relations@gartner.com.
Gartner is a registered trademark of Gartner, Inc. or its affiliates.

This presentation, including any supporting materials, is owned by Gartner, Inc.
and/or its affiliates and is for the sole use of the intended Gartner audience or
other authorized recipients. This presentation may contain information that is
confidential, proprietary or otherwise legally protected, and it may not be further
copied, distributed or publicly displayed without the express written permission
of Gartner, Inc. or its affiliates.

© 2011 Gartner, Inc. and/or its affiliates. All rights reserved.
Fundamental enterprise IAM processes and supporting products and services have matured. However, traditional IAM technologies have proved inadequate as computing models, and endpoint technologies have changed. Gartner inquiry data and search analytics show clear trends that mobility and cloud computing are stretching and breaking traditional IAM processes and infrastructures. Even as enterprises reduce complexity for internal environments and standardize on processes, protocols and products, the movement of applications and infrastructures to the cloud has undermined enterprise efforts to build effective and efficient IAM capabilities. The same IAM functions are needed for the cloud; however, they are not readily available as mature, abstracted or brokered services. Rather, each IAM function (administration, access and intelligence) is delivered independently by cloud application providers. Increasing employee and consumer mobility also challenges established IAM processes and infrastructure. More-capable smartphones and tablets break established provisioning capabilities and location-independence tests many authentication methods.

Conversely, mobile endpoints provide new capabilities to strengthen authentication. Enterprises have struggled with identity administration initiatives, and clients are telling us they have shifted emphasis to reporting and audit as a means to more effectively streamline audit and compliance efforts. This reactionary trend may present an emerging opportunity to mine entitlements and access data to provide "identity and access intelligence" data to support enterprise business processes and decision making.
Key Issues

1. What are the trends?
2. How is IAM governed effectively?
3. How can organizations move toward "mature" IAM programs?
Key Issues

1. What are the trends?
2. How is IAM governed effectively?
3. How can organizations move toward "mature" IAM programs?
As IAM requirements and markets have evolved, three significant categories have arisen around capability: access, administration, and intelligence. Access serves as a foundational platform to facilitate authentication and authorization, and the capabilities within them, from single sign-on to the enforcement of certificates. Access is the "engine" of IAM that takes identities and their information and uses them to effect. Administration is the construction phase of identity, and providing it with a "personality" by assigning attributes, entitlements, credentials — it is the create/maintain/retire capabilities of IAM. Administration is also focused on providing the platform for the intelligence — a means to make sense of the identity and access events. Intelligence generates reports for auditors, provides real-time monitors for operations and delivers the analytics necessary for analysts and business stakeholders to make intelligent, actionable decisions in the business and in IT.
The Identity and Access Management Scenario

Key Issue: What are the trends?

Gartner IT Leaders IAM analysts had over 2,000 client interactions during the last year. Several "traditional" topic areas continued to drive client interactions, particularly user provisioning and directory issues. Less than stellar outcomes for administration projects and increased auditor scrutiny have driven increased interest in intelligence topics. Cloud, particularly enterprise SaaS adoption, and increased proliferation of smart mobile devices have driven major shifts in Gartner's discussions with clients. These trends touch all aspects of IAM, but authentication especially. Clients have increasingly been looking to replace stand-alone hardware authentication tokens, and there is increased interest in reducing costs, improving ease-of-use and leveraging smart devices users already possess.

Gartner IAM Inquiry Trends — Hot Topics

<table>
<thead>
<tr>
<th>Overarching themes: Cloud and IAM, mobility, IAM program, IAM organization and governance</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Identity Administration</strong></td>
</tr>
<tr>
<td>User provisioning</td>
</tr>
<tr>
<td>Role and entitlements administration</td>
</tr>
<tr>
<td>Directory technology and migration</td>
</tr>
<tr>
<td>PAAM (SAPM)</td>
</tr>
<tr>
<td>PAAM (SAPM)</td>
</tr>
</tbody>
</table>

This presentation, including any supporting materials, is owned by Gartner, Inc. and/or its affiliates and is for the sole use of the intended Gartner audience or other authorized recipients. This presentation may contain information that is confidential, proprietary or otherwise legally protected, and it may not be further copied, distributed or publicly displayed without the express written permission of Gartner, Inc. or its affiliates.

© 2011 Gartner, Inc. and/or its affiliates. All rights reserved.
There are several use cases that Gartner discusses with clients. Prior to 2009, these interactions focused on enterprise access to enterprise systems within the perimeter, and on consumer access to enterprise systems. The greatest trend since 2009 has been the increased focus on access provided to cloud based applications, and enterprise-to-cloud has been the most common thread. This has given rise to increased interest in identity federation, and has spawned a market for IAMaaS. Each of the core IAM functions must still be addressed. Moving applications to the cloud does not undo the need for IAM, but does put an increased burden on enterprises to manage identity consistently and effectively.
The Identity and Access Management Scenario

Strategic Planning Assumption: By year-end 2015, over 50% of firms currently providing IAM-as-a-service (IAMaaS) and cloud-based IAM solutions will be acquired by larger service providers.

The current market for IAM services in all varieties is expanding rapidly, ranging from established managed/hosted service firms (e.g., HP and IBM) to small SaaS firms (e.g., Arcot Systems, Simplified and TriCipher). While managed/hosted firms have expanded IAM offerings to supplement broader IT outsourcing contracts, SaaS providers are experimenting with delivery and pricing models to determine how this new IAM delivery method can be effective and profitable. Within five years, SaaS and cloud provider markets will expand to include more startup service firms and some larger hosting firms. When (not if) delivery and pricing model issues are resolved, many smaller firms will be candidates for acquisition. Gartner believes that more than one-third of these firms will be acquired by 2015, signaling the start of the market consolidation of IAM services.

A key driver for ultimate success in the evolution of IAM services will be the ability to deliver the services at a less-expensive life cycle cost to the enterprise. The service providers that are able to provide the right combination of simple, scalable solutions with flexible pricing for well-defined delivery options will enjoy early success in the marketplace. Larger service providers must avoid the fundamental error of using acquisitions as a means of consolidating market penetration, which, as a result, will keep prices higher.
The Identity and Access Management Scenario

Strategic Planning Assumption: Through 2015, more than 50% of cloud-based IAM solutions will be hybrid; i.e., IAM software and scalable service-based solutions integrated for cloud computing.

The Hybrid IAM-as-a-Service World

Transitions from one technology inflection point to the next are messy. When the transition occurred between the mainframe and client/server as a platform choice, there was a period of more than a decade where such solutions coexisted. The same could be said of transitions to Web applications, Web services and service-oriented architectures. At each stage, more and more applications became adept at using one or more of those platforms to provide a usable environment for clients. Gartner believes history, to some extent, will repeat itself with transitions to cloud computing environments. But, as before, the transition will be messy, occurring in fits and starts. It will, however, provide enterprises with a foundation for "experimentation" at a relatively low risk, without the need to forsake major investments or compromise risk and privacy. Overall, the majority of IAMaaS implementations will have to support or integrate established on-premises target applications and IAM components.

© 2011 Gartner, Inc. and/or its affiliates. All rights reserved.

Gregg Kreizman
MEX38L_129, 10/11
Key Issue: What are the trends?

Key concepts:
- Accept that you can't/shouldn't provision everything.
- Manual provisioning (in many cases) is still less costly than deploying traditional connectors and the associated custom workflow.
- If your IAM goal is compliance, getting will always be broader than automated provisioning.
- "Success," in the mind of your auditor, is:
  - Visibility into what is going on in your environment
  - Proving that you see issues/gaps
  - Proving that you can and do close the gaps within a "reasonable" amount of time

If your goals are around saving time and money (efficiency), then automated provisioning is only a small part of that solution. Consider technologies that have proved to be successful for short and predictable deployments, such as self-service password reset, enterprise single sign-on, AD-Unix bridge tools and virtual directories. Your strategy should be to view your overall environment as a set of concentric circles. The outermost is the entire IT environment — where there is no "one size fits all solution." Then you move it to the subset of that environment that can be reported on for purposes of IAG (identity intelligence, analytics and governance). A subset of that reporting environment will include identities that are manually provisioned and managed. Last, the smallest subset is full, automated management of identities.
The Identity and Access Management Scenario

Key Issue: What are the trends?

Other technologies help reduce administration complexity and improve time to value.
The real drivers behind IAM programs map into three areas: efficiency, effectiveness and business enablement.
If you do an honest evaluation of your goals for IAM administration, you will likely discover that the "build a lot of connectors" approach isn't necessarily best suited to achieve your goals. Some technologies that may help achieve your goals include:
- Virtual directories to create an interface layer across multiple identity and data silos
- AD-Unix bridge to allow you to abstract authentication and management away from Unix so that they can be maintained in Active Directory
- Privileged account activity management to provide greater control and auditing around the use of highly privileged accounts (i.e., domain administrators) and shared accounts (i.e., root)
- Role life cycle management to help ensure that you understand the access rights of your users, and that you have a method for attesting to and certifying access for compliance purposes.
In the end, you may still have some manual provisioning. And that is not necessarily bad.
Action Item: Consider the inherent costs in developing connectors or using other technologies to manage accounts versus the continued cost of manually provisioning some of your environment.
The Identity and Access Management Scenario

Key Issue: What are the trends?

Three types of credentials can be used as a basis for user authentication:

- Something known — for example, a password or PIN.
- Something owned — for example, a token such as a one-time password (OTP) device.
- Something inherent — in other words, a biometric characteristic, such as face topography.

Fewer than 10 years ago, this broad classification of authentication methods was enough to distinguish among the options commonly in use for remote and local network access — passwords and PINs, tokens (with a choice between dedicated OTP devices and smart cards with public-key credentials and, in each case, typically used in conjunction with a PIN or password to provide two-factor authentication) and biometric technologies (most often fingerprint). While other options, such as OTP software for smartphones, certainly were available at that time, uptake was low.

During the past few years, the variety of distinct authentication methods has increased significantly, making it more difficult for organizations to:

- Select new authentication methods that will be appropriate for their needs.
- Ensure like-to-like comparisons of different authentication products and services.

Gartner's taxonomy describes the elementary classes of authentication methods in the three canonical types: something known to the user, something held by the user and something inherent to the user. The taxonomy provides a language that can be used to describe with precision the variety of authentication products that instantiate these classes singly or in combination. It is foundational to Gartner research that describes the authentication marketplace, and that provides a methodology for comparing different methods (see "A Taxonomy of Authentication Methods" G00154522).
The Identity and Access Management Scenario

Strategic Planning Assumption: By year-end 2013, less than 10% of all authentication events will involve discrete, specialized authentication hardware of any kind.

Focus of Authentication Needs Will Shift to User Experience

By year-end 2013, less than 10% of all authentication events will involve discrete, specialized authentication hardware of any kind.

Analysis supporting the SPA:
- A method that can leverage an existing device (for example, a cell phone) or do away with a device altogether (KBA, face, voice, typing rhythm) is easier to use.
- Such methods typically have lower capital costs than legacy tokens or biometric methods.
- Ease of use further reduces TCO (dealing with lost tokens, etc.), and can improve assurance (fewer "cheats").
- Adaptive access control will allow continued use of legacy passwords.

Analyzing the alternative view:
- Some kinds of hardware (for example, smart cards) may be mandated by regulations.
- Such hardware may still be indicated for other high-risk use cases.
- Adjacent needs (such as CAC, digital signature) may require such hardware anyway.

Gartner
Key Issue: What are the trends?

What is the future of IAI in enterprises, and what effects will it have on business intelligence (BI) and business processes?

Think of IAI as a branch of a tree that has its roots in operations, but those roots absorb enormous quantities of data from the foundation of the business. The data is pulled upward to bring life to other parts of the business, from IT itself to other disciplines that can analyze and shape that data into information and knowledge to be put to practical use. In some cases, IAI may be the entire report — in other cases, it represents a modest input. IAI will go through several iterations of processing and analyses to become what each discipline needs, whether BI, GRC or ESI.
Key Issues

1. What are the trends?
2. How is IAM governed effectively?
3. How can organizations move toward "mature" IAM programs?
The Identity and Access Management Scenario

Key Issue: What are the trends?

What are the key processes of IAM?

The IAM program experience has traditionally not been a good one. Although some things have improved, major efforts to formally implement such systems overlook a key lesson — planning for them starts from the wrong direction with the wrong people or, at least, not everyone affected. In defense of IT, the IAM experience started out as a "fix the plumbing" issue. However, with the advent of compliance concerns, this changed, and changed dramatically. Now the basis of good IAM involves a very active role for the enterprise. Only it can truly say what and how that plumbing should be used, and what aspect of the "water" delivered is most important. In an era where accountability and transparency are required (and must be formalized), this means a more focused and structured approach for all parties affected, not just IT. IAM should not be planned with operations in mind. Rather, it should be based on the foundations of the enterprise relative to policies, processes and people. Products are a relatively small part of the decision process in an IAM program.
The Identity and Access Management Scenario

Key Issue: How is IAM governed effectively?

What are the functions of an IAM program?
The functions of an IAM program are shown schematically in the IAM activity cycle, which maps directly onto that for information security:

- The plan function comprises developing, maintaining and implementing a vision and strategy, plans, budgets, roles and responsibilities, and an architecture for IAM.
- The build function encompasses defining, maintaining and implementing policies, controls and processes, and designing a solution infrastructure for IAM.
- The run function encompasses technology selection and implementation, operations (that is, day-to-day process execution — the routine activity around identity and entitlements life cycles) and communications.
- The govern function encompasses effective governance of all of an enterprise's IAM activities.
Key Issues

1. What are the trends?
2. How is IAM governed effectively?
3. How can organizations move toward "mature" IAM programs?
But why do we even care about IAM? What is its true purpose in the enterprise? How do the drivers evolve over time? We have noted a consistency in the drivers of IAM:

1. Efficiency, which is primarily an IT advantage, in streamlining those IT operations that usually require labor, time or cost-intensive procedures regarding the establishment and modification of access for people and systems. There are some business efficiencies, but not as much as IT.

2. Where the business does get more involved is in the effectiveness driver, where the enterprise leads in an effort to leverage IAM in pursuit of specific business requirements, commonly around compliance and risk.

3. Business enablement, where a transformational experience is possible in mergers, acquisitions or larger reorganizations. These can be more effectively enabled by specific IAM efforts. The aim is to move from IT to the enterprise, from merely an IT experience to a business experience using IAM.
Key Issue: How can organizations move toward "mature" IAM programs?

In IAM program maturity, there is actually a Level 0. In this level, little or no process and capability maturity exists. Tasks are performed informally and are uncoordinated. Processes are undefined, and staff changes cause failures. As the enterprise evolves, however, Level 1 brings a sense of the fact that processes at least exist, though they are ad hoc. An effort gets under way to assess requirements and responsibilities for the first time, and creates some sort of plan that leads to communications and even to technology selection. Level 3 evolves goals, practices and metrics, allows a formal program office to take over distinctive initiatives and introduces IT architecture to the effort. At this point, compliance requirements are being addressed. In a managed environment, architecture graduates to overall enterprise architecture, and there is linkage between the business and IT to realize specific business-driven targets. In the final phase of IAM maturity, continuous controls and performance monitoring are possible due to mature processes, and the IAM infrastructure and service has given the enterprise the ability to make transformational decisions (e.g., mergers, acquisitions and reorganizations) without sustaining undue effort.
Gartner established the IT scorecard for IAM in September 2010. It is still "early days" for data collection, but the small set of data points comes from enterprises with broad distribution across industries, geographies and organization sizes.

- Overall maturity averages 2.41, which is low compared with other roles for which Gartner collects IT score data.
- No disciplines approach Level 3 for average maturity, but business value and planning and budgeting receive the highest scores.
- Over one-third of respondents scored at Level 1 overall.

Recent data points include some organizations that scored themselves in the 4 to 5 range for some disciplines.

Bottom Line: More data points are needed to draw strong conclusions; however, early indications are that we have a way to go before IAM becomes a mature discipline.
Recommendations

✓ Review your current IAM program strategy in the light of changes in business strategy and in technologies, processes and service delivery models.

✓ Assess the security technologies and processes adjacent to IAM to determine their contribution to the IAM program.

✓ Invite more-direct enterprise participation from IT governance to ensure that the IAM life cycle supports the broader enterprise mission.
Action Plan for IAM Leaders

Monday Morning
- **Stop thinking** of IAM as IT technology to be deployed.
  - **Establish** a new planning session to review the current state.
- **Rethink** IAM’s role in the context of the enterprise strategy and architecture.

Next 90 Days
- **Revise** the IAM program design and operations as part of the IT governance function, incorporating the lessons learned here.
- **Deliver** a one-year plan for management review and approval for changes to the IAM program.

Next 12 Months
- **Evaluate** optional forms of IAM delivery based on enterprise needs.
Related Gartner Research

- ITScore for Identity and Access Management
  Ant Allan, Ray Wagner (G00201672)

  Ant Allan, Earl Perkins

- Hype Cycle for Identity and Access Management Technologies, 2010
  Gregg Kreizman (G00201318)

- Identity and Access Intelligence: Making IAM Relevant to the Business
  Earl Perkins (G00210038)

- Roundup of Identity and Access Management, 1Q11: Topics and Technologies
  Ray Wagner (G00212730)

For more information, visit gartner.com or email us at solutioncentral@gartner.com.