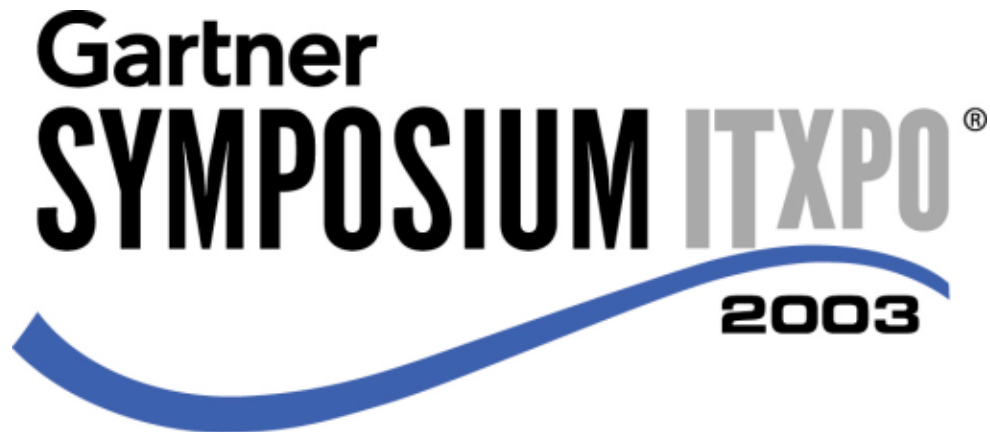

User Provisioning: Identity and Access Management in the Real-Time Enterprise



Florence, Italy
10–12 March

European Symposium

Ant Allan

10–12 March 2003
Fortezza da Basso
Florence, Italy

Key Issues

1. What are the drivers for user provisioning in the RTE?
2. Where does user provisioning fit in the IAM space?
3. What features and functions should an enterprise look for in a user provisioning product?

User Provisioning

“The management activities centering on the creation, modification and deletion of user account credentials (such as user ID, password, group connections and privileges) for access to IT resources (such as operating systems, databases and applications) and (sometimes) physical resources (such as office space, mobile telephone and corporate credit cards).”

By 2005, user provisioning solutions will perform user account and privilege management functions for internal and external users of Web and non-Web applications; extranet access management (EAM) systems will perform the real-time enforcement of privileges for the user and transactions for Web-based applications (0.8 probability).

By 2005, the capabilities of metadirectory and user provisioning products will have effectively merged (0.8 probability).

Gartner

Copyright © 2003

Managing enterprise identity and access information becomes more demanding with the proliferation of user accounts and granular privileges across multiple platforms and applications. User provisioning (UP) products offer identity and access management (IAM) features that are a good fit to the real-time enterprise (RTE). This presentation will examine how UP products differ from extranet access management products and metadirectories, and present what UP functionality an enterprise must consider when selecting a product.

Key Issue: What are the drivers for user provisioning in the RTE?

Identity and Access Management

Authentication:

- Who am I? How can I prove it? Do I have multiple identities across multiple systems?

Authorization:

- What do I have access to?

Policies:

- What do the enterprise's business rules say I can do?

Profiles:

- What attributes and characteristics do I have?

Relationships:

- What role do I have? (Am I an employee, customer, supplier or trading partner?) What org. units and group(s) am I in?



- New "business ecosystems" expand the scope of IAM:
 - Directories become critical infrastructure:
 - Already used to store access management information
 - Well-suited to represent relationships
 - Support scalability requirements in the millions
 - Easily manageable and highly available
 - LDAP is the *de facto* look-up protocol
 - More granular security
 - Requires support for sophisticated authentication and authorization
 - Security needs to be broken out from the OS and applications

Copyright © 2003

Key Issue: What are the drivers for user provisioning in the RTE?

Identity Management: The capability to manage (across multiple target systems) all user accounts, user profiles (etc.) that can be identified with each person. Also, the capability to abstract and automatically correlate data from HR/HCM systems (and other "identity stores"), and from the managed systems. Also here is the ability to create, modify and delete one or many user accounts / profiles for a single user, in response to a self-service request (such as self-registration); a line-management request (such as, to provide a user with an e-mail account); or a change in an HR/HCM system (such as, an employee termination).

Access Management: The capability to manage (across multiple target systems) an access control policy (or policies), including both policy administration and enforcement. As intranets, extranets and corporate Internet access evolves, security will become an even bigger issue than it is today. Access by more users, from more locations, using more types of devices will become the norm. Today's security models are typically "coarse grain," while "fine grain" security is the future. We believe that directory services will become the *de facto* repository for this "fine grained" access management information. Why directories? Think of them as a function-specific database tuned for authorization and access control information. Furthermore, the hierarchical nature of a directory assumed by LDAP is well-suited to represent relationships — internal structures and external e-business relationships. Enterprisewide directory services will become the home for authentication and authorization data.

User Provisioning in the RTE

- User provisioning technologies are a good fit to the key principles of the RTE:
 - Internal efficiency attracts capital
 - Focus on improving speed of response
 - Technologies bring a new level of capability that can be focused on speeding up information flows and automating tasks
 - The management of elapsed time is given much higher priority
 - Managers must understand recipients' current tolerance windows
 - Focusing on dramatic, elapsed-time reduction will often be a more powerful way to indirectly achieve core goals
 - Improvements in business performance will be measurable
 - Focus on processes that span organizations horizontally and vertically
 - Transparency requires the timely production of information



Copyright © 2003

Key Issue: What are the drivers for user provisioning in the RTE?

UP products improve the internal efficiency of security administration functions by automating multiple tasks around IAM, and improving information flows (status of requests, elapsed time reporting).

Such automation can dramatically reduce the elapsed time around user life-cycle changes — especially “day one” tasks — ensuring that users can work productively from the start, but also day-to-day changes, where manual processes may often extend beyond users’ “tolerance windows.”

UP products yield measurable performance improvements (and the means to measure them, with timely reporting). Impact spans the whole enterprise.

Business Drivers ... and Buyers



Gartner

Copyright © 2003

Key Issue: What are the drivers for user provisioning in the RTE?

There are five main business drivers for an overall IAM solution, some more applicable for one aspect of the solution than another. 1) *Business facilitation*: The organizational structure for security administration activities, which must match that of the enterprise. Some are centralized, some decentralized and others are pushing self-service for internal and external users. The IAM solution must handle all models. User information can be leveraged in many business processes that provide a consistent and more-secure access control infrastructure. 2) *Improved service level*: Achieving an access request turnaround time of 24 hours or less is only doable via automation. 3) *Cost reduction or cost containment*: With growing numbers of users, staffing volume cannot accommodate the enterprise's needs. In an economic downturn, enterprises are looking for cost-cutting measures. When rolling out new technology, hiring a new security administrator does not have to be part of the implementation. 4) *Security risk management*: The ability to prove the security of an enterprise's access control infrastructure is important for maintaining customers, as well as obtaining them. In addition, easing the electronic data processing audit process is of primary concern to many enterprises. 5) *Regulatory compliance*: Financial services, healthcare, pharmaceuticals and the energy industries require the establishment of a secure access-control infrastructure.

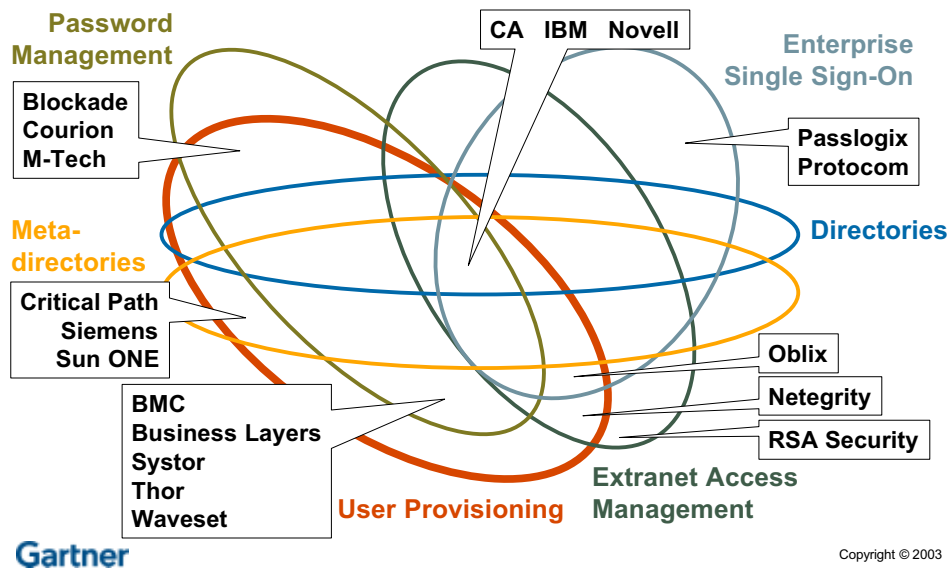
There are multiple buying centers and reasons for implementing an IAM solution. In an economic downturn, the focus is on cost reduction/containment, and the CFO tends to be more interested in the project. Because of the enterprisewide impact, the CIO and/or CISO are most often involved. When separate components of the solution are implemented separately, the buyers tend to be focused on a particular problem to solve — the help desk manager, the business unit and the security administrator.

User Provisioning: Identity and Access Management in the Real-Time Enterprise

Conclusion: Enterprises will use multiple products to manage the complexity of user authentication and authorization in a heterogeneous environment.

Strategic Planning Assumptions: By 2005, user provisioning solutions will perform user account and privilege management functions for internal and external users of Web and non-Web applications; EAM systems will perform the real-time enforcement of privileges for the user and transactions for Web-based applications (0.8 probability). By 2004, the complexity of IAM solutions means that customer buying patterns will lean toward product suites rather than best-of-breed products (0.7 probability).

User Provisioning in the IAM Marketplace




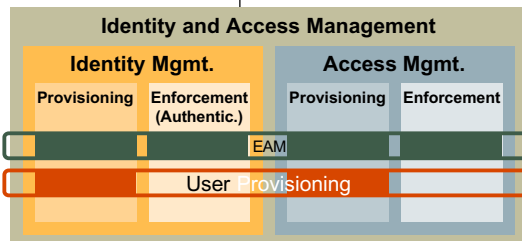
Key Issue: Where does user provisioning fit in the IAM space?

We need a detailed look at the technologies that have evolved to address the user account and privilege administration problem. Many of these technologies have overlapping functionalities. For example, UP tools perform password synchronization and support single sign-on solutions. Extranet access management (EAM) tools enforce user privileges and perform single sign-on to Web applications. However, there are few products in the market that do everything — user account creation, privilege creation, password management and single sign-on — across all platforms and for all application types. A multiproduct implementation has been the only solution to all of these enterprise requirements. All vendors in these markets are forming partnerships with each other. We see that a number of these markets are likely to collapse in the next 12-to-18 months; for example, the key vendors in the password management area now have UP solutions. UP and EAM solutions are complementary, not competitive.

Action Item: Prioritize the overall IAM solution implementation — don't do it all at once.

User Provisioning vs. Extranet Access Management

- | | | |
|---|---|---|
| <ul style="list-style-type: none"> • EAM <ul style="list-style-type: none"> – Single point of administration – Password management – User self-service – Single sign-on – Access-control policy model and real-time enforcement – Workflow (sometimes) |  | <ul style="list-style-type: none"> • User Provisioning <ul style="list-style-type: none"> – Single point of administration – Password management – User self-service – Access-control policy model – Workflow and automated fulfillment |
|---|---|---|



Gartner

Copyright © 2003

Key Issue: Where does user provisioning fit in the IAM space?

Single point of administration: EAM has one “access” data store; one or many “identity” stores; for Web applications, UP has one master “identity and access” store (usually); many “identity and access” stores across multiple target systems — for example, operating systems, DBMSs, ERPs, EAMs. *Access control policy model:* EAM has simple access control lists (ACLs) (maybe), plus user attributes, application data, environmental data, authentication strength (“dynamic trust”); UP has access control enforced in real time on individual target systems. The optimized IAM architecture has one authoritative identity repository, which the IAM components access for user authentication and authorization information. This repository may be the only version, or it may push down the identity information to distributed repositories. An integrated administrator console is the other key feature; it provides a common interface for all UP activities — account management, group management, role/policy/rule management and workflow. It also serves as the common end-user console for self-service activities. An enterprise identity management (EIM) product is an abstraction of some features found in both UP and EAM products — such as workflow, role management, self-service password reset — rolled into a common, Web-based GUI so that all users can be managed from a common “dashboard.” An EIM product allows a role to be defined as soon as it’s in the EIM, and then directs the UP and/or EAM product to take appropriate action. EIM products see UP, EAM and portals as platforms to manage. Examples include: Oblix NetPoint’s COREid component, Netegrity IdentityMinder and Waveset Identity Broker. The move to a single administrator console for EAM and UP has been demonstrated by Oblix/BMC and Waveset/OpenNetworks.

Strategic Planning Assumption: By 2005, the capabilities of metadirectory and user provisioning products will have effectively merged (0.8 probability).

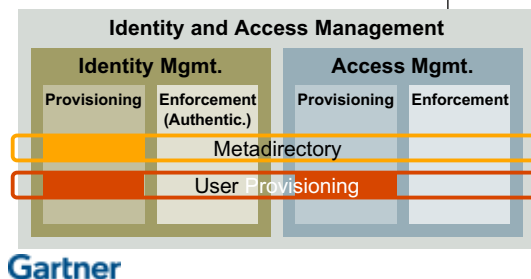
User Provisioning vs. Metadirectories

- **Metadirectories**

- Single point of administration
- Data accuracy and precedence
- Multidirectional data synchronization

- **User Provisioning**

- Single point of administration
- Data accuracy and precedence
- Multidirectional data synchronization (sometimes)
- Password management
- User self-service
- Workflow and automated fulfillment
- Sometimes including procurement and manual work orders
- Access-control policy model



Copyright © 2003

Key Issue: Where does user provisioning fit in the IAM space?

Despite their similarities (such as user account creation and bidirectional synchronization), UP and metadirectory products' *dissimilarities* make them complementary rather than competitive. Features traditionally excluded from metadirectory products are workflow (or business process automation), password management and access control management. Customers relying on metadirectory products for account management tend to do so for operational rather than security purposes (that is, metadirectory products serve an infrastructure rather than a business or security role). Customers that are looking to manage IAM securely will often do better with a user provisioning product (instead of, or in addition to, a metadirectory product).

In 2002, many metadirectory vendors began to add UP-like features to metadirectory products. At the same time, many UP vendors began adding metadirectory-like features to UP products. As a result, we see these product areas merging over time. By 2005, the modern capabilities of metadirectory products and UP products will effectively have merged (0.8 probability).

Action Item: Enterprises evaluating metadirectory or UP products should study vendors' product road maps to determine if both products will be needed, or if one type can be deployed and adapted into a solution that addresses both metadirectory and UP needs.

User Provisioning Features and Functions

- | | |
|--|--|
| <ul style="list-style-type: none">• Architecture<ul style="list-style-type: none">– Repository<ul style="list-style-type: none">– LDAP, X.500, RDBMS– Pointers vs. data replication– Robust<ul style="list-style-type: none">– Secure, auditable– Reliable, scalable, available | <ul style="list-style-type: none">• Target System Integration<ul style="list-style-type: none">– Connectors (or agents)<ul style="list-style-type: none">– OS, DBMS, ERP, EAM, etc.– Connector “factory”– Synchronization |
| <ul style="list-style-type: none">• Administration<ul style="list-style-type: none">– Delegated– Workflow<ul style="list-style-type: none">– Approvals, escalation and notification– Automated fulfillment– Access-control policy model<ul style="list-style-type: none">– RBAC, etc. | <ul style="list-style-type: none">• Usability<ul style="list-style-type: none">– Web GUI (preferred)– User self-service<ul style="list-style-type: none">– Password reset– Self-registration– Password synchronization<ul style="list-style-type: none">– Or single sign-on? |



Copyright © 2003

Key Issue: What features and functions should an enterprise look for in a user provisioning product?

There are features and functions common to UP and other major IAM components (password management, EAM and enterprise single sign-on).

Architecture: Distributed identity repository — a master/slave replication model, multiple replicated masters or multimasters that house different user populations.

Target System Integration: Easy agent/connector generation — engines that can discover exposed target attributes, map them to enterprise attributes and automatically generate the connector according to the access protocols of the target (little or no programming required). This feature enables fast and customized application integration.

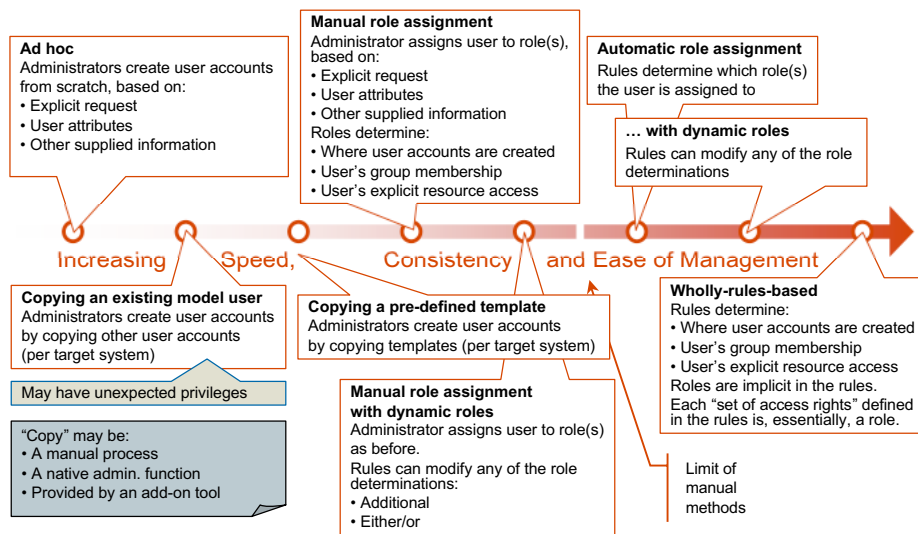
Native target change detection — via a local agent or remote connector, changes made at the native target level must be communicated back to the centralized policy engine for action — accept or deny/rollback.

Administration: Delegated administration, including self-service — the ultimate.

Multistep workflow: Enables automation of the way administrators actually accomplish their jobs.

Rules-based access control provides the most flexible method for assigning privileges to users, based on attribute values.

User Provisioning Methods Compared



Gartner

Copyright © 2003

Key Issue: What features and functions should an enterprise look for in a user provisioning product?

A *role* is a set of access rights (such as applications, ACLs, privileges), and a *policy* is something that exists on paper, such as password policy, separation of duties, users of type X only work from 8 a.m. to 5 p.m., Monday through Friday. A rule is used to implement a role or roles, a policy or policies, and any combination of a role and a policy. Paper is to policy as a UP tool is to a rule. Roles, policies and rules can be implemented manually or automatically. Examples include: *Ad Hoc*: Give Joe Unix access; *Cloning*: Make Joe just like Sue (where Sue has Unix access); *Templates*: Make Joe like this template (template includes Unix access); *Manual Role Assignment*: Add Joe to role called "sales" (role "sales" has Unix access); *Automatic Role Assignment*: If Job:Sales, then add to role called "sales" (role "sales" has Unix access); *Rule*: If Job:Sales and Level:VP, then grant access to Unix.

Prioritized Rules:

If Job:Sales and Level:VP, then grant access to Unix.

If Location:Africa, then remove any access to Unix.

Concatenated Rules:

If Job:Sales and Level:VP, then grant access to Unix.

If Unix:Access, then grant access to "DL Unix Users" e-mail distribution list.

Role-Based Access Control vs. Role-Based Provisioning

- **RBAC**
 - Implemented within a single system with a single access control policy
 - Access-control policy enforcement can be aware of role assignments
 - Supports static and dynamic separation of duties
 - Works within a single schema
- **Role-Based Provisioning**
 - Uses RBAC concepts to map enterprise access-control policy model to multiple target systems
 - Access-control policy enforcement is unaware of high-level role assignments
 - Cannot support separation of duties
 - Must interoperate with multiple schemas
 - Support for groups or roles?
 - Inheritance?
 - Precedence?

Gartner

Copyright © 2003

Key Issue: What features and functions should an enterprise look for in a user provisioning product?

It is important to understand the limitations of role-based access control (RBAC) in a UP solution — it is not true RBAC; instead, call it role-based provisioning (RBP).

Each target-system access-control service (ACS) enforces its view of the access control policy, and that view has no knowledge of the roles defined at the UP level.

RBP may not, therefore, support the more sophisticated features of RBAC, such as static or dynamic separation of duties.

RBP may also be hamstrung by the “limitations” and “quirks” of a target-system ACS’s schema. For example, where a user has different levels of access to the same resource, via membership of two or more target-system groups (determined by assignment to two or more roles at the UP level), which takes precedence? As a matter of policy, you may want it to be the lower/lowest, but in some target systems (such as z/OS RACF), it is the higher/highest.

Role-Based vs. Rule-Based Provisioning

- | | |
|--|---|
| <ul style="list-style-type: none">• Role-Based Provisioning<ul style="list-style-type: none">– Requires definition of roles as data objects– Role definition may be analytic (top down) ...– ... or synthetic (bottom up)<ul style="list-style-type: none">– that is, based on inspection of common access that users currently have– but need analytical “tuning” | <ul style="list-style-type: none">• Rule-Based Provisioning<ul style="list-style-type: none">– Roles are only virtual objects– Rules allow existing, manual processes to be easily implemented in the provisioning system– Rules can be concatenated– Rules can easily handle additions or exceptions |
|--|---|



Copyright © 2003

Key Issue: What features and functions should an enterprise look for in a user provisioning product?

Top-down analysis requires a huge amount of work and cooperation from business units, application development, human resources and information security. Bottom-up synthesis can be simpler, but it is an iterative process; it will take time to have a full set of precise roles, and it may be automated (for example, Systor SAM Role Miner, Eurekify Sage Discovery and Audit). Also, there is the danger of “garbage in, garbage out” — you should first clean up the worst excesses on each target system.

RBAC can easily become overcomplicated, with a multiplicity of fine-grained roles that apply to small sets of users. Remember, it is a means to an end, not an end in itself. A UP product should support/allow access to be provisioned directly, as well as via roles.

Maybe roles define a set of access with which all assigned users are automatically provisioned, and additional access can be provided to all users on request.

Support for dynamic roles (that is, partially rules-based provisioning) can ease things considerably; some small differences between similar roles can be handled “on the fly.” Rule-based provisioning allows easier implementation and much greater flexibility. Exceptions and additions can be handled much more easily. Rule concatenation means that sets of access that “flow” from one another can be defined just once; several user-oriented rules might say “give A,” which can trigger another rule, “if A, then give X, Y and Z.”

Target System Integration

- | | |
|---|---|
| <ul style="list-style-type: none">• Connectors<ul style="list-style-type: none">– Target system cannot be provisioned without a suitable connector– Must cover all “important” systems<ul style="list-style-type: none">– Provisioning only some systems can add value, but it is not enough– Connector depth<ul style="list-style-type: none">– “Fine-grained” provisioning– Synchronization<ul style="list-style-type: none">– Preserve integrity of access-control policy model– Connector transparency<ul style="list-style-type: none">– Ease of implementation on any given target system– Generic and custom connectors<ul style="list-style-type: none">– Vendor must provide generic connectors or easily-built custom connectors; look for a connector “factory”– These connectors must be fully functional | <p>Operating Systems</p> <ul style="list-style-type: none">• Mainframe — e.g., z/OS• Unix — AIX, HP-UX, Solaris, etc.• Network — e.g., Windows <p>Databases</p> <p>Directories</p> <p>Groupware/e-mail</p> <p>ERP</p> <p>EAM</p> <p>Homegrown apps.</p> |
|---|---|



Copyright © 2003

Key Issue: What features and functions should an enterprise look for in a user provisioning product?

Target-system connectors are vital for UP.

A broad range of target-system support is a strength of a UP offering, but for any single organization, the most important thing is that the UP tool supports the target systems it uses.

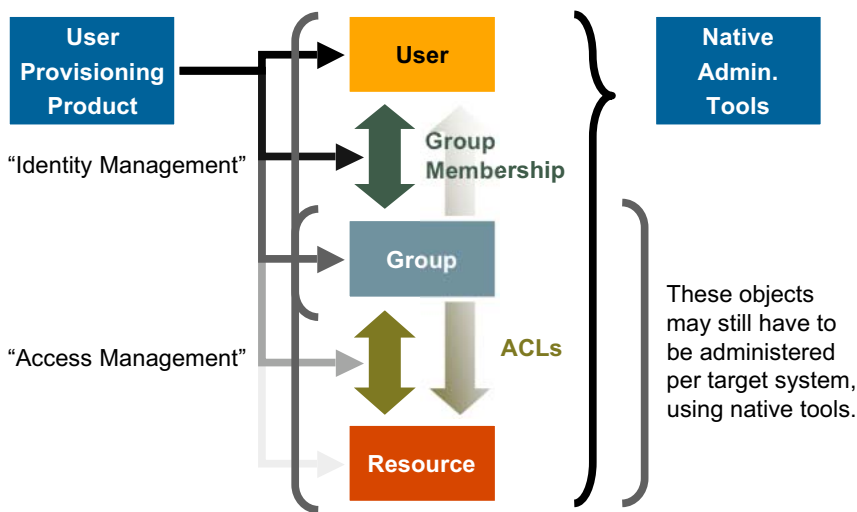
Connectors must be up-to-date with target-system releases. Ask how closely the vendor tracks release schedules. Is it a “development partner” with any/all of the target-system vendors?

If target systems are not supported specifically “out of the box,” does the tool offer a generic connector that can be used, or does it allow for the easy creation of a custom connector?

Caveat emptor: You must be sure that a custom connector offers the full functionality of standard connectors (or actively accepts the limitations, if that’s “good enough”).

In any case, does the connector do all you need it to do?

Connector Depth



Gartner

Copyright © 2003

Key Issue: What features and functions should an enterprise look for in a user provisioning product?

Native administration tools (maybe augmented by third-party utilities) necessarily allow full coverage of identity and access “provisioning” on each target system.

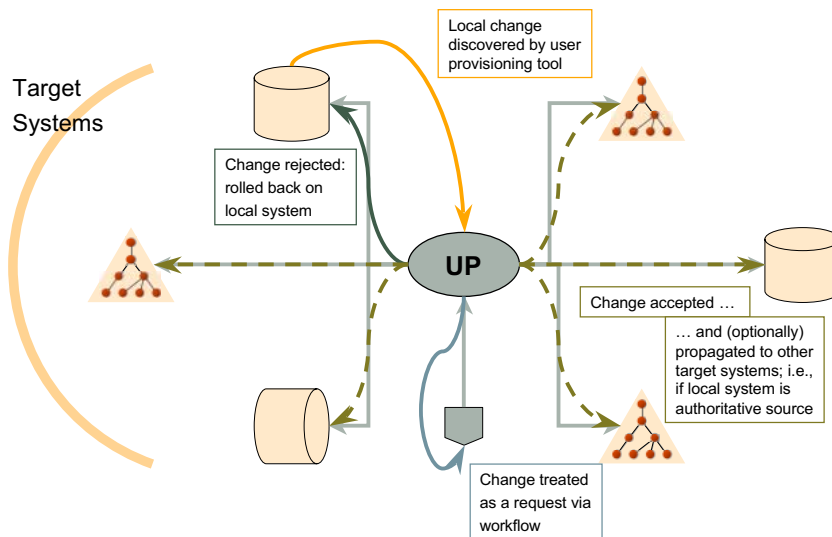
UP connectors may not allow the full range of coverage.

User accounts (create/modify/delete functions) are always supported, and group membership (connect/remove functions) very often is.

However, fewer and fewer tools can create/modify/delete groups, modify ACLs or create/modify/delete resource definitions.

These objects may have to be administered per target system, and you have to ensure that they dovetail with the UP tool.

Synchronization



Gartner

Copyright © 2003

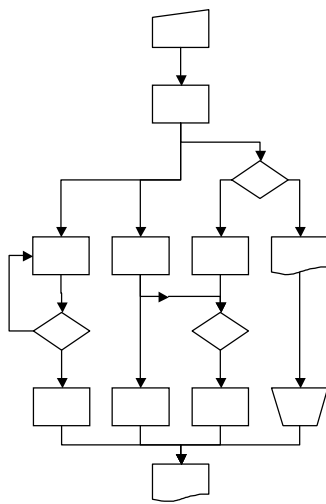
Key Issue: What features and functions should an enterprise look for in a user provisioning product?

A UP tool provides a universal access control policy model for the organization. Necessary changes are pushed out to the target systems. What happens when changes are made locally? (Remember, you will likely still need to have target-system-specific administration.)

The UP tool must have a way of discovering “local” changes, or deviations from its model. This might be a batch process, ad hoc or scheduled — for all or only selected users or target systems; or it might be a real-time process, where the connectors “listen” for local changes and flag them to the UP tool.

How can these be processed? A change can be handled manually (an administrator is notified of the change) or automatically, according to pre-defined rules. A change can be rejected and the target system changed back. A change can be accepted and maybe propagated to other target systems (such as change of e-mail address from the e-mail system). Also, a change can be treated as a request and routed through the workflow for approval.

Workflow



- Ability to set up and manage complex provisioning workflows
 - Task based
 - Pre- and co-requisites
 - Dependencies built into tasks
 - Rollback
 - Approval
 - Approvers
 - Notification
 - Escalation
 - Status
 - Progress tracking
 - Notification
 - Easy user interface

Gartner

Copyright © 2003

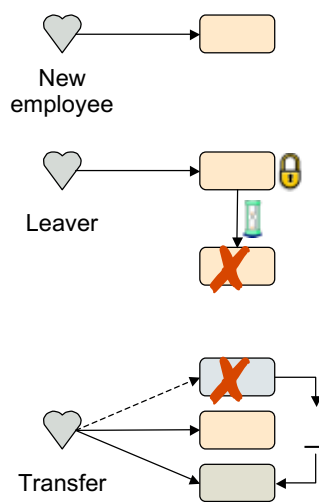
Key Issue: What features and functions should an enterprise look for in a user provisioning product?

Workflow is a key feature of modern UP tools. It should be as flexible and generic as possible.

Key functions are:

- Approval handling, ensuring that approval is given where appropriate, and with as little delay as possible
- Status tracking, providing management information on the progress of a request

HR-Driven Workflow



- Employee provisioning can be driven by the enterprise's HR system
 - New employee
 - Does HR capture necessary attributes?
 - Leaver
 - Revoke, do not delete — at least initially
 - Transfer
 - Most complex, often least-well-documented
 - Only the differences (Δ) need to be changed
 - How does the product deal with this?
 - Are HR updates timely?

Gartner

Copyright © 2003

Key Issue: What features and functions should an enterprise look for in a user provisioning product?

UP for employees can often be driven by your HR system. (Other “identity stores” can be the drivers for UP for other users, such as CRM for customers or partners’ HR systems) The interface can be batch or real-time.

New employees: All necessary attributes for a new hire might be captured by HR. The supervisor can be prompted for additional information via workflow.

Leavers: De-provisioning leavers have an important security benefit: no “ghost” accounts. It is probably inappropriate to delete users straight away, but they should at least be automatically revoked (accounts “locked”). Additional manual tasks may be required before users can be deleted (but “requests to delete” could be created automatically).

Movers: Most complex and often least-well-defined procedurally. Not effective to treat as delete plus (re)create. A particular problem is the timeliness of HR changes. “Before payday” is not good enough.

Recommendations

- Obtain cross-organizational buy-in.
 - Obtain executive sponsorship.
 - Form a cross-organizational project team.
 - Anticipate business process change and use a systems integrator when making business process changes.
- Balance access-control policy model, connectors, workflow (etc.) to best meet your needs.
 - Product functionality varies widely.
- Don't expect to find one authoritative source for user data ...
 - But expect to end up with one.
- Implement via a phased project plan.
 - Fit your strategy for Web-based applications, directory services, etc.
 - Understand the effort to integrate homegrown and "unusual" COTS target systems.
 - In other words, what custom connectors are needed?
 - Prioritize according to the importance to the enterprise.