

Password Management

Before User Provisioning



Identity management spans technologies including password management, user profile management, user provisioning directories, meta directories, virtual directories and single sign-on (SSO).

Two technologies that are frequently purchased and deployed together are password management and user provisioning. In such projects, one technology must normally be deployed first and act as the technical foundation for the other.

This paper discusses technical and practical considerations that impact the sequence of these two deployments, and concludes that in most cases it is best to begin with password management, and follow up with account management.

Contents

- 1 Introduction** **1**

- 2 Identity management technologies** **2**
 - 2.1 Password management 2
 - 2.2 User provisioning 2
 - 2.3 Combined solutions 3

- 3 Technical and business requirements** **4**
 - 3.1 Password management 4
 - 3.1.1 Functionality 4
 - 3.1.2 Scalability 4
 - 3.2 User provisioning 5
 - 3.2.1 Functionality 5
 - 3.2.2 Scalability 6
 - 3.3 Manage passwords before provisioning accounts 6

- 4 Deployment complexity** **8**
 - 4.1 Password management 8
 - 4.2 User provisioning 8
 - 4.3 Passwords before accounts 9

- 5 Conclusions** **10**

- 6 References** **10**

1 Introduction

Identity management spans technologies including password management, user profile management, user provisioning directories, meta directories, virtual directories and single sign-on (SSO).

Two technologies that are frequently purchased and deployed together are password management and user provisioning. In such projects, one technology must normally be deployed first and act as the technical foundation for the other.

This paper discusses technical and practical considerations that impact the sequence of these two deployments, and concludes that in most cases it is best to begin with password management, and follow up with account management.

The remainder of this paper is organized as follows:

- **Identity management technologies:**

A description of how password management and user provisioning fit into the identity management market, and what each technology does.

- **Technical and business requirements:**

A characterization of the technical and business requirements most organizations place on each type of technology.

- **Deployment complexity:**

A description of typical deployment tasks in both password management and user provisioning projects, and how business complexity impacts the time-to-ROI in each case.

- **Conclusions:**

A summary of why password management should, in general, precede user provisioning in an identity management project.

2 Identity management technologies

The following sections describe the basic capabilities that password management and user provisioning solutions may incorporate, respectively.

2.1 Password management

Password management systems generally include some subset of the following capabilities:

- Password reset for help desk analysts.
- Self-service password reset for users who forgot or locked out their own passwords.
- Password synchronization, from a web browser.
- Password synchronization, triggered by a native password change on some system.
- An administrative capability to update user profiles (e.g., login IDs, Q&A authentication data).
- A self-service capability for users to update their own profiles.
- Password policy enforcement.
- Two-factor token administration (help desk, self-service).
- A user registration system.
- Support for a variety of operating systems, DBMS servers, standard applications and custom / vertical market applications.
- Accessibility from workstations, web browsers and telephones.
- Integration with help desk call tracking systems.
- Integration with user authentication systems and databases.
- Integration with corporate directories or meta directories.
- Integration with e-mail systems.

2.2 User provisioning

User provisioning systems generally include some subset of the following capabilities:

- The ability to create new user login accounts on various systems.
- The ability to alter existing user login accounts on various systems, including enable, disable, delete, change attributes, change membership in groups and rename.
- A work-flow automation system to track and authorize change requests.

- A consolidated console for managing users across systems.
- A batch load facility to perform many administrative actions at once.
- Directory synchronization, to monitor administrative changes made on one or more systems, and propagate those changes to other changes.
- Directory cleanup, to find, disable and remove unused accounts.
- Programming interfaces to support integration with other systems, such as external work-flow systems, new target systems, etc.
- Various security enforcement mechanisms, to manage password rules, automatic creation of IDs, automatic termination of IDs, creating standards-compliance IDs and ensuring that changes are properly authorized.
- Reporting tools to calculate account allocation and administrative activity.
- Integration with help desk call tracking systems.
- Integration with user authentication systems and databases.
- Integration with human resources and payroll systems.
- Integration with corporate directories or meta directories.
- Integration with e-mail systems.

2.3 Combined solutions

Vendors typically have a rich heritage in either user provisioning or password management, but rarely both.

Some user provisioning vendors have “tacked on” a very simple password management capability for example a simple web-based self-service password reset, where users are authenticated by answering one or two personal questions.

Similarly, some password management vendors have “tacked on” a very simple user provisioning capability for example to create user IDs on just one or two kinds of managed systems, with only a very simple user interface.

3 Technical and business requirements

3.1 Password management

Password management systems must meet, at a minimum, both functional and scalability requirements:

3.1.1 Functionality

1. Manage passwords on all or nearly all systems that users log into.
2. Synchronize passwords between some or all systems.
3. Enforce a sufficiently strong password policy.
4. Allow users to reset their own forgotten passwords (self-service password reset).
5. Allow help desk analysts to reset forgotten passwords on behalf of callers (assisted password reset).
6. Integrate with relevant IT infrastructure (e-mail, call tracking systems, web services, corporate directories, etc.)

3.1.2 Scalability

Most users only change their passwords when they are prompted to. In practice, users are prompted to change their passwords when they log in – normally in the first hour of each day.

This means that password changes, and in particular password synchronization, produces very pronounced peaks in transaction rate.

A simple calculation illustrates the high peak transaction rate that a password synchronization system must handle:

- Variables:

- N users.
- A accounts per user, on average.
- D days password expiration.

- Peak times:

Approximately 3/7 of passwords are changed on Monday mornings – or during approximately a 50 hour window, annually.

- Maximum transaction rate:

The peak rate of password changes is therefore:

$$\text{Peak rate} = [N \times A \times \frac{365}{D} \times \frac{3}{7}] / 50 \quad (1)$$

- Example calculations:

For example, a company with 10,000 users, an average of 4 login IDs/passwords per user and a 90 day password expiration period will generate a peak rate of about 1400 password changes/hour.

$$\text{Peak rate} = [10000 \times 4 \times \frac{365}{90} \times \frac{3}{7}] / 50 = 1390. \quad (2)$$

These transactions are not evenly distributed, so the peak rate per minute could easily be over 200 passwords/minute.

These figures scale linearly. A similar company with 50,000 users could generate a peak rate of 1000 passwords/minute.

Clearly, password management in general, and password synchronization in particular, requires a solution that is very scalable. It should support multiple servers, high availability, load balancing, server fail-out or fail-over, etc.

3.2 User provisioning

User provisioning systems must meet extensive functional requirements, but in practice do not demand extreme scalability.

3.2.1 Functionality

1. Be able to manage login IDs on all or nearly all systems that users log into.
2. Be able to streamline account creation with some combination or subset of the following features:
 - (a) Automated work-flow to submit systems access requests, route them to the appropriate authorizers, accept approvals, and finally create accounts.
 - (b) Consolidated user administration, so that a single administrator can manage multiple systems in a single step.
 - (c) Batch load facility, so that multiple accounts can be created at once.
3. Be able to streamline account termination with some combination or subset of the following features:
 - (a) Automated work-flow.
 - (b) Consolidated administration.
 - (c) Integration with human resources or payroll systems.
4. Be able to streamline account changes with some combination or subset of the following features:
 - (a) Automated work-flow.
 - (b) Consolidated administration.
 - (c) Integration with human resources or payroll systems.
5. Integrate with relevant IT infrastructure, such as a corporate directory, HR systems, e-mail systems, call tracking systems, etc.

3.2.2 Scalability

User provisioning is a continuous process, not normally impacted by the kinds of peak activity seen in password management systems.

A simple calculation illustrates the normal transaction rate for a user provisioning system:

- Variables:

- N users.
- A accounts per user, on average.
- X percent staff turnover per year.
- G percent staff growth per year.

- Peak times:

User provisioning happens throughout the day and year. Peak events such as corporate mergers or system migrations are handled through a batch load facility, can be performed off-hours, and do not affect system scalability requirements.

- Normal transaction rate:

The rate of account creation is therefore:

$$\text{Creation rate} = [N \times A \times (X + G)] / (2000 \text{ hours/year}) \quad (3)$$

- Example calculations:

For example, a company with 10,000 users, an average of 4 login IDs/passwords per user, a 20% staff turnover rate and 10% staffing growth will generate just six (6) account creation transactions per hour.

$$\text{Peak rate} = [10000 \times 4 \times (0.2 + 0.1)] / 2000 = 6. \quad (4)$$

It is important to note that while the peak rate of transactions in a user provisioning system is low, the value of each transaction to the organization is typically very high, so this calculation should be taken to clarify scalability requirements, rather than economic value.

3.3 Manage passwords before provisioning accounts

Given the above analysis, it is clear that password management systems require a degree of scalability that user provisioning systems do not. In practice, password management systems must be able to field about 100 to 1000 times as many transactions per hour, at peak.

Scalability is not a trivial aspect of system design. It must be designed into the system from the ground up. Architectural features that yield scalability, such as support for load balancing, server fail-out, retrying transactions, and data replication between servers are difficult to implement, and impossible to retrofit.

For this reason, it is important to start an identity management project with password management. If the chosen technology fails to scale adequately, it will fail early in the project, and the remaining time can be effectively spent in finding a new solution.

Projects that begin with user provisioning risk a scalability failure late in the project, when it may be prohibitively difficult or costly to change technologies.

4 Deployment complexity

Password management projects are significantly shorter than user provisioning projects. As both projects leverage a nearly identical team to implement, it makes sense to validate the ability of the team to execute with a small project – password management, before attempting a more complex project – user provisioning.

4.1 Password management

Password management systems are relatively simple:

- Users are only impacted in the way they routinely change their own passwords, or reset forgotten passwords.
- Help desk analysts can be trained to use a system in minutes.
- Deployment and configuration can generally be completed in 5-15 days of effort, spread over 1-2 months.

In practice, password management systems can be activated in a large organization in 1-4 months calendar time, and just 5-15 days of billable time.

Once deployed, a password management system starts to yield cost savings to users and the help desk immediately. Password problem rates decline, and password-related help desk call volume and call duration are reduced.

4.2 User provisioning

User provisioning systems are more complex to deploy, primarily due to a more far-reaching business process:

- The organization must define every kind of account that will be created on managed systems.
- Accounts are normally grouped into roles, which must also be carefully defined.
- Authorization and approvals processes must be defined, including roles, authorizers, escalation paths, etc.
- Processes must be defined and implemented to assign new login IDs, to look-up user information in a corporate directory or human resources system, etc.

This complexity means that the design process can span several months, before a product can be activated.

Once a system is installed and activated, many users in the organization must be trained to use it to request new systems access. Authorizers must be trained to use the system to approve open requests.

The business complexity of a user provisioning system means that normally at least 4-6 months, and in some cases 2-3 years of business process discovery and design precede system activation. During this time, the system yields little or no value to the organization.

4.3 Passwords before accounts

Clearly, a simple deployment and short time-to-ROI means that password management should be activated early in an identity management project. Early deployment gives the organization early ROI, and gives the project visibility and credibility that it can leverage to carry out the business process discovery and design required to activate a user provisioning system.

5 Conclusions

Password management systems must field from 100 to 1000 times as many transactions per hour as user provisioning systems, at peak. It is therefore prudent to commence a deployment of a combined password- and account-management system with the password management component, because scalability problems will be found earlier this way.

User provisioning systems can take from 4 months to 3 years to activate, primarily due to the complex business processes that they replace. In contrast, password management systems can be activated within just 1-4 months. As a result, it makes sense to start a project with password management, in order to start realizing return on investment (ROI) early, and establish project credibility.

6 References

Hitachi ID is a security products and services company. This document is based on our experience with product deployments.

For further information, refer to our web sites:

Hitachi ID corporate web site

<http://Hitachi-ID.com/>

Hitachi ID Password Manager: a total password management system

<http://Password-Manager.Hitachi-ID.com/>

Hitachi ID Identity Manager: an enterprise user administration system

<http://Identity-Manager.Hitachi-ID.com/>