Federated Provisioning and Deprovisioning

What is federated provisioning and deprovisioning?

> *A large research-focused virtual organization has a collaboration management platform (CMP) that members use to access the different applications and services used by the VO. All applications and services are federated, having local accounts but expect authentication information to come from external sources. The CMP automatically provisions members in the appropriate applications and services based on the attribute information coming in from member institutions. The CMP will remove access when affiliation changes at the home institution. All the provisioning and deprovisioning happens based on information outside the VO's direct control.*

Intro

From small, single service environments to large service providers, anyone offering services outside a very small community has experienced the challenges in provisioning and deprovisioning accounts. In a small environment, the process of provisioning is usually manual - a request comes in that a new account be added to the system and an administrator creates that account. In a large environment, a central HR or student system may provide the necessary data that a certain amount of automation can be put in place to create new accounts as individuals come in to the environment. Removing accounts, or even just removing account access, is again an either very manual process or one that may have some (usually minimal) level of automation. Cases of individuals moving to different departments and therefore needing different access to different tools, or cases where someone leaves and the next person needs exactly the same levels of access are common and increase the complexity around provisioning and deprovisioning within an institution. When you add to the existing challenges within an institution the possibilities around federated access - where provisioning and deprovisioning will be fed by authoritative systems beyond an organizations control - an already challenging problem gets bigger.

In all cases, federated or not, there must be policies surrounding who may be provisioned in a service, and even more around when an account must be removed. While most institutions have policies and procedures that work for the majority of cases in the area of provisioning, deprovisioning remains a significant challenge. What is better, to err on the side of allowing access to services and not disrupting research and learning, or to err on the side of security and cost containment?

When looked at from the viewpoint of a virtual organization that depends on federated technologies, the provisioning and deprovisioning questions become significantly more complex. When an organization has no control or insight in to the account provisioning and deprovisioning practices of the identity providers, how can they control their service environment? The answer lies in the strength of the federation, understanding Levels of Assurance and gathering the VOs requirements.

Excerpt from SURFnet draft "Architecture and design of a provisioning/de-provisioning solution"
Provisioning
One key step in connecting federated services is provisioning: providing services with the (expected) users and user information. For a lot of cases real-time provisioning (provisioning at login time) is used, therefore requiring no additional effort from the side of the institutions. However, a few services will - for different reasons - not be able to deal with real time provisioning:

- live@edu and google apps are both very attractive services that expect users to be provisioned upfront.
- Other collaboration tools will for cultural reasons need provisioning of users upfront as well:
  o LMS's (Learning Management Systems), PLE's (Personal Learning Environments), etc .
- Legacy systems that can use the federation for authentication but not for authorisation (systems that SHOULD be rewritten but where the cost is too big.

De-provisioning
Besides provisioning, the aspect of de-provisioning should also be taken into account. De-provisioning from a federated identity management aspect consists of removing a user account from the IdP. This is enough to bar a user from accessing a service via WebSSO. However, in the service itself the user continues to exist - even if the service relies on just-in-time provisioning – unless the service employs some sort of time-out mechanism to clean up accounts after some predefined period of inactivity; this is usually not the case.

In the service itself the user may have shared content, workflows or application specific roles in which the user is involved. Therefore it should be possible to deactivate and remove the user from the service as well. The engine should provide one or more possibilities to de-provision users from the Service Provider's side. Note that the de-provisioning activity may consist of moving the user from the 'active' service to some form of backup (possibly for a specified duration before final clean up), ensuring that the de-provisioned user has reasonable time to request his or her content; this is at the discretion of the service itself.

end excerpt

Questions and Requirements

Many vendors are out there offering a variety of service models (Software as a Service, Storage as a Service, Infrastructure as a Service) designed to make outsourcing common components of the IT environment a sensible alternative. They too have the interesting challenges around provisioning and deprovisioning accounts to meet the needs of an institution or a VO. When thinking about a provisioning/deprovisioning service, whether it is created in-house or from a vendor, there are several areas that should be considered:

Security and Legalities

- Does your organization have any specific grant or legal requirements regarding the existence of accounts, their creation or removal? Policies generated out of grant or legal requirements may require a high level of security and assurance around the identity of the users of a service, and in turn require immediate, automated removal of those accounts when an individual is no longer associated with an organization.
- Does your organization have an international constituency? The differences in privacy requirements across geopolitical borders are significant enough to require much more research around what local laws and regulations will require of your system or service.

Cultural requirements

- Your organization may have a strong expectation around automated action. Or, alternatively, it may require explicit, manual, auditable administrative approvals. At whatever point of the spectrum you might be on, this feeds in to how accounts and service access should be created and removed.

Service and technology

- Some services can only handle batch creations and deletions. Others can handle real-time, or at least close to real-time, provisioning and deprovisioning. What do you need? What applications and services do you have in your organization, and what are they capable of?
- Do your requirements include adding and removing privileges? Groups? Provisioning and deprovisioning is often more than just account creation.

Cost

- Many institutions have annual license renewals based on the number of users of a service. If this is the case, then automated provisioning and in particular, automated deprovisioning are a great cost-saving measure that should feed in to your considerations of a provisioning service.

Use Cases

Virtual Organization

A research-focused virtual organization invites a research group to join the collaboration. The VO shares wiki space, access to critical data sets, and certain domain-specific tools, all of which will need to be available to the new researchers immediately. The collaboration and domain-science tools need to be automatically provisioned with the new accounts, adding to groups and access control lists, and accept federated authentication. The goal is to have the researchers immediately able to contribute to the collaboration, without creating a high-level of overhead to approve, create, track, and remove accounts.

Interdisciplinary degrees

A top-tier university consists of several smaller, almost independent schools that want to retain their specific branding while allowing for interdisciplinary degrees between the schools. Each school has its own set of specialized applications and services which need to accept students that may have had their accounts initially associated with another school. Rather than manually add students as they take classes outside their primary school, the applications need to be federated and able to automatically provision and deprovision accounts as students take classes or indicate multiple majors in the centralized student information system.

Transfers

A chemistry postdoc moves from research university A to become a junior faculty member at research university B. She is also a member of an international research group of chemists. While her affiliation and institution are changing, the access she requires to the collaboration remains the same. All current authentication and group information is handled via federated technologies. As she is deprovisioned at one institution and provisioned at another, her access in the collaboration will need to change to match her affiliations, possibly involving a deprovisioning and re-provisioning along with ownership transfer to her data.https://spaces.at.internet2.edu/pages/editpage.action?pageId=25855589

Library access and publisher requirements

Current tools

IdM systems that explicitly support federated provisioning

Vendor or Service	Federated?	Provisioning?	De-provisioning?	API	Comments
Ping Identity	✓	✓			"Built-in interoperability exists for ADFS 2.0, Sharepoint 2010, Visual Studio 2010, WIF/WCF, Oracle, MySQL and MS SQL Server. Integration kits, connectors, and translators are available as add-on modules."

_Note that many institutions are using home-grown tools for their provisioning services, all of which require tie-ins to local systems.*

Applications that can handle federated provisioning

See the Domestication Wiki for a growing list of "domesticated" tools - applications that may accept federated authentication, group management, access management, and provisioning/deprovisioning.

Working groups

Kantara Initiative

What's next?