Working with Vendors for K12 Federation

Working with Vendors for K12 Federation

Email from Bernie A'cs for All Pilots call of March 12, 2015

There are multiple points-of-view needing some illumination to establish a baseline of objectives, goals, and experiences that will help frame responses to the questions. (Click to see questions submitted by Shaun Abshere below on this page) . Here is a primer for discussion.

Introduction

IlliniCloud is the "owner"/"operator" of what we call the Federated Service Stack (FSS). The business objective for this is to establish an operational reference model and implementation catering to the special needs of the K12 community to adopt, participate, and leverage the strengths and advantages federated identity, centralized data automation services, and the means access applications that are easy to access by the user community supported by a Local Education Authority (LEA or school district).

Background Context
The three pillars: data, identity, and presentation are intimately inter-woven in the day to day activities of students orchestrated by LEA administration, faculty, and employees in very general terms using a given Student Information System (SIS). The activities from the perspective FSS fall neatly into just hand full of baskets:

- enterprise-application (in-house resource, LEA operated); examples are
  - Supportive services for Educators and Students.
    - Support Staff services
    - Parent services
  - wireless tablets, phones, laptops, and other technologies
  - Office/Desktop common-tools

- operational-applications (business needs of LEA);
  - SIS data ETL operations for State and Federal Reporting requirements
  - Time-card systems, RFI monitors, and other accounting tools
  - HR management tools
  - Food Service tools
  - Transportation Service tools
  - Shared collaboration resources (disk space, folders, files, or other)
  - Integration of (de- &) provisioning Students and Staff enterprise-wide including critical SP applications

- external service provider applications (could be sub-population specific Teacher/Student/Section-Course);
  - SIS data ETL to provide "roster-feeds" for some SP applications to function
  - Shared collaboration resources (disk space, folders, files, or other)
  - Integration of (de- &) provisioning Students and Staff with SP applications

- federated services and applications provided directly by the "operator" for federation members.
  - Data Service Objective: provide a means by which LEA partners are empowered to leverage a common data-model structure that can be used validate data-values, facilitate automated operations to support ETL needs, and support migration of values between predominate data-models.
  - Identity Service Objective: provide a means by which LEA partners are empowered to leverage federated identity and Single Sign On (SSO) features for web-based applications (most SPs) and to the degree possible enterprise-applications required to conduct the day-to-day business including Students.
  - Presentation Service: provide a means by which LEA partners are empowered to leverage applications on any-device from any-where using a very simple portal interface that enables segregation of content presented to users by
    - Org (Org) and/or
    - School (OrgUnit) and/or
    - Affilitation (Faculty, Staff,Employee, or Student)
  - The fourth pillar, Infrastructure Service: provide a means by which LEA partners are empowered provision virtual machines, persistent sto rage, and disaster/recovery services.

With context presented in the course-grained outline and bullets above, as IlliniCloud's significant investment in design, development, discovery, and deployment has produced an operational representation of the three pillars of support with predominately open-source software resource.

Identity Service
The strategy for the FSS focused on implementing a Shibboleth IDP equipped with a custom JAAS implementation that functionally determines the demographics defined for an authoritative source system to be consulted based upon user-input at the challenge prompt. This module returns these connection parameters to the IDP and interrogates additional authoritative source system values for assertion assembly, packaging, and delivery to SP. The interrogation processor collects and writes the resultant values to a database service (MySQL) that is use store minimum schema needed to satisfy the core general purpose attributes defined. The database service is exposed to the IDP service as resource that is consulted during the attribute-resolution phase of the assertion preparation logic including complex LEA specific attribute-resolution rules. The attribute-filter phase of IDP processing is used primarily to implement rules that constraint attributes for delivery and provide the mechanical means to arbitrate LEA/SP attribute agreements. One design goal for this functional model to realized is that the "operator" of the FSS maybe a single LEA or a regional service facilitator like the IlliniCloud where many LEA organization tenants use a centrally managed deployment, the model accommodates both of these scenarios, for example for a single-site deployment with the Shibboleth IDP would be sufficient, in the regional case and more complex scenarios the IDP/Proxy hybrid deployment described here could be implemented.

The Illcloud IDP/Proxy hybrid introduces LEA tenants using a common services deployment which seemed to poorly addressed in products that were evaluated. Given this fact, the design requirement dictates the need to develop interfacing that empower operators of the FSS model to establish two one-sided operational-partnerships: 1) LEA Operational Partners; and 2) SP Operational Partners; these partnerships represent a digital contract that defines how delegated administration and responsibilities are facilitated and how the IDP/Proxy operations are managed. A more complete executive-level summary of the operational-partnerships is available at: http://confluence.illinicloud.org:8090/display/TP/IDPOperationalPartners and this short article also explains that the AAF Federation Registry software has been adopted to provide "self-service" administrative interface to negotiate the workflows that are punctuated by sequences of human actions necessary to manage configuration of the central service. One of the primary design goals for the AAF software adoption was to address IDP/Proxy needs to define connection properties necessary to facilitate delegated authentication and interrogation of authoritative source systems operated by the LEA tenants served. Another goal was to facilitate establishing similar connectivity with SP entities enabling them to define their declared assertion attribute requirements, this was done in a fashion that strongly supports the core general-purpose-attributes and further provides the SP to define "application-specific" attributes. Iin the subsection Identity a table defining the "general-purpose-attributes" is presented in the document at: http://confluence.illinicloud.org:8090/display/TP/ThreePillars

Data Service
The most important component of adding value for LEA organizations revolves around the relationship of of the data service with the identity service. In most LEA cases the SP applications come with a prerequisite to supply some data-extracts that, in general, can be cast as "Roster" information. The spectrum of requirements ranges from heavy-weight extract, transform, and load (ETL) operations including list of Teachers, Students, and Section /Courses that are used to per-populate application-specific databases managed by the vendor to operator one or more applications. At the other end of the spectrum are vendors that are ready and able to dynamically provision application user-accounts based upon attribute assertions provided by the IDP. The mechanical requirement to prepare and deliver "Roster" data-feeds on a regularly scheduled basis, is a significant liability for LEA staff to enable the educators and students to use applications. Another flavor of ETL operations that every LEA are liable for on a regular basis is meeting reporting requirement for State and Federal entities. The data service pillar essentially provides a common-data-model schema that can be sourced to develop and implement logic once that can be used by many LEA organizations. For example, one of the districts engaged has been piloting a focused development effort to automate a series of State level reporting requirements, the logic implementation is constructed to enable re-use by other LEA entities. The estimated labor reduction benefit to the pilot district is approximately 5 hours per week for the staff member that was responsible for manually producing these data-feeds.
The predominate achievement has been that 32 LEA organization have adopted the use of this service pillar and in so doing are provided the immediate benefit of automated record validation enabling data-correction in their SIS source system. The IlliniCloud central data service implements a School Interchange Framework (SIF 2.6) Zone Integration Service (ZIS) and the primary reason for this is that many of the SIS vendors widely used by the LEA organizations support SIF agents, these can be used to migrate record-level details to the ZIS in real-time, transparent to the end-user that use the SIS. For cases where the SIS is not SIF ready/enabled alternative ETL tools are provided for LEA to define, implement, and manage data-migration on a scheduled basis to the Operational Data Store (ODS). An advantage of this ODS model is the ability to develop-once and to use those development for many organizations. In addition, the ODS has been enhanced to enable bidirectional automated data-model level migration between the SIF 2.6 ZIS service and an implementation of a SIF 3.0 ODS and/or a EdFI ODS. These function capacities open the doors of opportunity for the LEA entities to consider using applications that were developed to operate over one of these emerging and/or established standard data-models.

Presentation Service
The presentation service implementation has produced a number of contributions to the Apero foundation's uPortal platform, including an operational model that reflects upon the notion of the service "operator" and the relationship with LEA tenants. This strategy has empowered IlliniCloud to set a baseline of minimum requirements needed to present content tailored to targeted sub-population of LEA organizations based upon the eduPersonAffiliation and eduPersonOrgDN attributes. These values enable portal administrators to define content that will be conditionally provided for Fac ulty, Staff, Employees, Students and/or the building (school) where they are assigned. The operator manages and controls the "Public Apps" content which is optionally presented to all LEA tenants. This feature is intended to seed and nurture the development and implementation of an application market place that can be used by register SP partners to provide "public" user experience (demos) or to increase awareness of their product(s) and service(s) for educators and learners.
How Far Have We Gotten
The Registry focused initially as an aide to work with LEA operational-partners, the overall functional service is really about how these entities manage IDP /Proxy connectivity, provide core attributes, and subsequently enable register SP applications. The first application goal is enable the LEA to leverage the App-Launcher portal offered by the "operator".
The high-level workflow-segments for a new LEA operational partner are:

- "Organization Registration"
  - http://stream.illinicloud.org/step one.mp4 short demonstration video (good)
  - operator must screen and approve applications submitted.
- "Account Claim and Registry Activation"
  - http://stream.illinicloud.org/part two.mp4 short demonstration video (okay, needs some refinement)
  - organization account activated in the registry.
- "Connectivity"
  - http://stream.illinicloud.org/step three.mp4 short demonstration video (okay, needs some refinement)
  - LEA provides details necessary to delegate authentication and interrogate authorization attribute from source-systems
    - primary data source database OR directory service
    - multiple data sources may be required to answer some requirement authoritatively
  - minimal operational capability
- "Attribute-Resolution"
  - Video being produced (not yet available)
    - Entitlements are the challenge, the core general purpose attributes are generally easy to resolve.
    - Many case require interrogation of multiple source-systems, ie. teacher-of-record is not in directory, but rather in SIS.
  - Simple single-value attributes and complex multiple-value arrays
  - meets core general purpose attribute requirements (meets app-launcher requirements)
- "Registered SP Enrollment"
  - Custom application-specific attribute resolution rules
  - Authorize IDP to enable service operations with a SP on behalf of the LEA

The high-level workflow-segments for a new SP operational partner are:

- "Organization Registration"
  - http://stream.illinicloud.org/step one.mp4 short demonstration video (good)
  - operator must screen and approve applications submitted.
- "Account Claim and Registry Activation"

    - http://stream.illinicloud.org/part two.mp4 short demonstration video (okay, needs some refinement)
    - organization account activated in the registry.
- "Connectivity"
    - establish IDP/SP connectivity and minimal attribute assertion propagation (no LEA)
    - exchange metadata, declare attribute requirements, and provide any additional functional requirements

Active Partnerships achieved and in-progress:

- 18 LEA organizations registered (most are in progress)
- 7 SP integration completed with one or more LEA using service
    - Pearson
    - PowerMyLearning
    - BrainPop
    - Moodle
    - MasteryConnect
    - Isle Dashboard (NIU educator dashboard)
    - Isle OER (Search with CWD)
- 5 SP integration actively in progress
    - DiscoveryEd
    - ReadingPlus
    - iSafe
    - EdAutomate
    - Symphony Learning

What Have We Learned
The most significant challenge faced with the design, development, and implementation of the FSS for IlliniCloud has been ***to achieve a reference implem entation model that is vendor/product agnostic while utilizing vendor partners to help satisfy professional services demands to develop functionalists that mechanically satisfy the operational requirements without inherently creating dependencies on a particular vendor propriety products or tools***. This single objective has been difficult to manage and keep on track, primarily due to the fact that vendor partners come to the project with a vested interest in promoting wares and hedging their position with proprietary resources. In a matter of speaking, the potential conflict of interest is both a philosophical and physical hurdle that can only be mitigated by conscience and deliberate attention on modular component implementation where alternatives approaches would be supported.

- As the owner/operator, primary architect, and funding facilitator of the FSS concept, IlliniCloud as engaged several vendor (partners) to help achieve a vision that promotes and enhances the K12 community's ability to be competitive, cost effective, be more efficient, and to seed the need to flip the business equation from a vendor dominated market to a customer dominated market.
- IlliniCloud's central services Vendor/Partners (involved in the three pillars focal efforts) are:
    - CPSI an Illinois based company that specializes in K12 (SIF) implementations for States and LEAs.
    - Unicon an Arizona based software consultancy organization with strong roots in the Apero Foundation community.
    - Aegis Identity a Colorado based organization developing and marketing the TridentHE and TridentK12 (identity provisioning management)

Brief Question Lead-ins:
1. a. (I will use the word SP versus vendor). The strategy adopted to engage with potential SP-operational partnerships is to be lead by the LEA community (as an existing customer of a given product) to vendors to explore and/or implement integration where possible.
1.b. The IlliniCloud objective has been to develop the capacity to be vendor/product agnostic and with the description provided above in mind: in regards to the "operator" we have purposefully focused on instrumentation using open-source resources do nearly all the heavy lifting to manifest the IDP/Proxy.

- Vendor partnerships have been channeled into two camps:
    - software licensing: is always an equation focused on the potential to provide resources to community members (LEA partners)
    - professional services: development requirements and the artifacts produced are cast as "work-for-hire"
- Vendors that sell software services or professional services to LEA partners are:
    - FSS SP operational partners
    - professional service providers do not have a role in the FSS as it is currently manifested.

2. As an operator there is certainly an opportunity to engage with SP-partners where specifically the FSS mitigates LEA on-boarding with SSO and roster automation to negotiate terms:

- For example, DiscoveryEd is SAML ready and can be accommodated with a roster prerequisite and IDP configuration. However the use of this service option comes with a one-time professional service fees of ~3K. In the IlliniCloud case, as an IDP/Proxy the level of effort for all LEA enrollments beyond the first is greatly reduced on both sides (SP and IDP). This fact is a strong basis for negotiating reduction in the flat fee structure currently imposed and defined in context of business model that was based on a per LEA engagement basis.
- As general rule of thumb, all SP implementations must be performed on behalf of a member LEA and will use a strategy that:
    - must be configured in the per-production (dev) platform
    - must include a pilot group of users to validate and verify the functional goals are satified.
    - production promotion is generally cast as exposure to fully population of a given LEA (or building or classroom-set).
- Payments should always be contingent upon production deployment and use.

3. There is no circumstance where a vendor should be acting in the capacity of an agent for the operator, however as in many industries where IT consultants are engaged to enhance staffing and in-house expertise, there may be circumstances that would leverage external resource augmentations to perform well-defined and specific tasks at a customer's site on behalf the operator. The hardest earned assets an operator can hold is the "trust" of their community being serviced, it is so valuable and important that it is never worth risking by placing it in the hands with an interest that are NOT precisely focused on the tasks and goals set by the operator.

- A) upon successful implementation of the mechanical requirements to make functional the SSO (and other ETL requirements) the LEA should be working with the professional development component of the resource vendor to enhance their potential to realize the best benefits available to them through the use of the product(s) the LEA has selected to use.
- B) There is no direct role with the possible exception of direct or in-direct support (helpdesk, and issue resolution) where a vendor of the operator is acting a customer-facing representative of the operator (this is a potential conflict of interest scenario)
- Customer feedback and confirmation are always at the top of the list of evaluation, followed closely by peer feedback.
    - Choosing vendors and products will always be a decision process that is in the hands of the LEA customers.
    - As an operator, it is important to facilitate strong operational capacity with the broadest possible range of resources beneficial to their community of customers, as defined by the customers.

Questions from Shaun Abshere

From: qt-incommon-pilot-bounces@thequilt.net [qt-incommon-pilot-bounces@thequilt.net] on behalf of Shaun Abshere [sabshere@wiscnet.net]
Sent: Wednesday, March 11, 2015 1:33 PM
To: Quilt All Pilots List
Subject: Re: [Qt-incommon-pilot] Next All Pilots call: Thurs., March 12, 2015

Questions and Requests:

1) Compare and contrast lessons-learned from working with:

(a) vendors who are/want to be service providers
to your federation/consortium members versus
(b) vendors who provide identity and access management
infrastructure services to your federation's operator?

2) For vendor types 1a and 1b (above), what are the important deliverables
that the federation operator will buy? Which types of deliverables
ought to have a "positive-approval" requirement before payment
What's your process (e.g., test-in-lab; deploy-and-test) for deciding
to approve payment?

3) Under what circumstances should a vendor of type 1a or 1b (above)
work directly with a K12 member of your consortium?
What does the federation operator need to know/evaluate, and from whom,
following such an example interaction?