Managing and Using InCommon Metadata:

Federation Manager and MDQ Metadata Service

InCommon Steering Committee
October 7, 2019

In this segment...

- What is the InCommon metadata?
- Managing and using the InCommon metadata:
  Federation Manager and the *Metadata Distribution Service*.
- Federation Manager updates and roadmap
- Metadata Distribution Service: transition to MDQ (Metadata Query).

What is the InCommon metadata?

The InCommon metadata is InCommon's Trust Registry. It is the most tangible expression of the Federation's trust fabric.

Just as the DNS enables an efficient, scalable way for systems to find and connect to each other, the InCommon metadata provides the same trusted and scalable mechanism for a participating service to find the service/connection endpoints for systems it needs to integrate with during SSO.

Identity providers and service providers (also called "entity") publish connection information, links to contact individuals, documentation, and cryptographic signatures to allow others to easily locate and securely connect to their services.

The Federation operator "notarizes" the published information. It also annotates an entity with applicable any certification and/or capability, thus enhancing transparency and promote interoperability.

Managing and using InCommon metadata

Manage Metadata

Federation Manager

Federation Manager is the web portal for administering the InCommon metadata. Participants and Federation operator us this application to register, update, validate, and publish metadata.

Federation Manager enforces Baseline Expectation requirements.

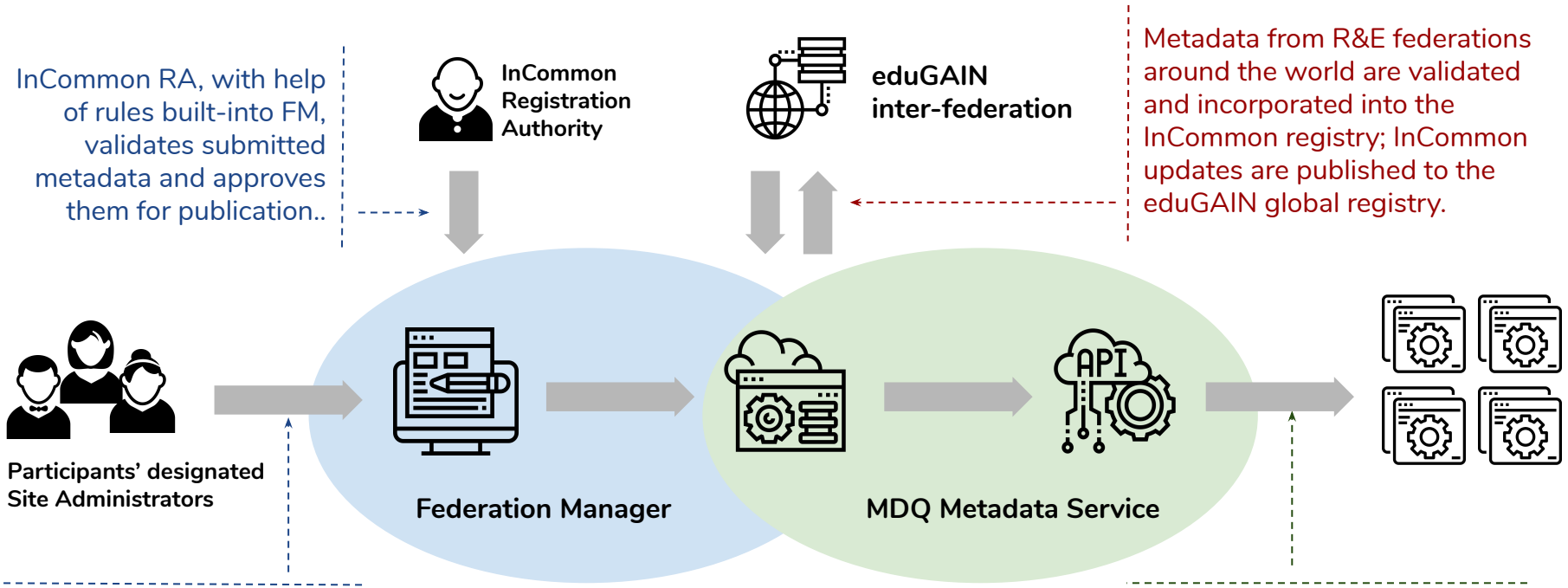
Use Metadata

Metadata Distribution Service

Metadata Service provides a trusted and scalable look up service for systems (Identity Providers and Service Providers) in the InCommon Federation to find and to connect to each other.

The new “MDQ” metadata service dramatically improves performance and scalability.

How does InCommon metadata work?

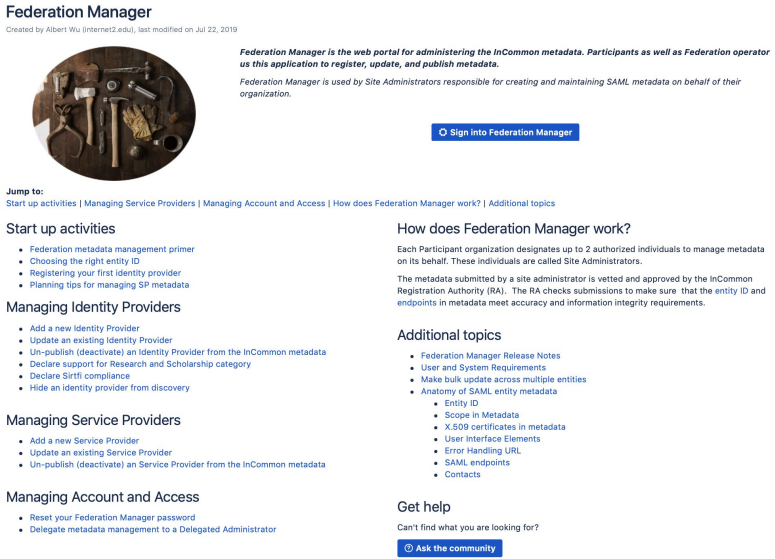


Improving metadata management experience

Since 2017 (the last InCommon fee increase), we have been updating Federation Manager to:

- **Simplify workflow and reduce unnecessary delays** - automate publishing approval

Entity ID	Organization	Status	Type
https://corp.collegenet.com/shibboleth-sp/	CollegeNET, Inc.	Auto Approved	Sp
https://myla.umn.sit.cloud.unizin.org//shibboleth	Unizin	Auto Approved	Sp



- Update user interface with better validation and **friendlier user experience**
- Better user documentation to **help users get work done with ease**
- **Future-proof the foundation** - leverage the cloud, streamline deployment, refactor aging codebase, and more
- Facilitate and **enforce Baseline Expectations**

Coming additions to Federation Manager

Improved self-service experience

- New “executive portal” allows InCommon Execs to assign roles via a self-service portal
- Improved dashboard and reporting

Automation via API

- Federation Manager API to enable automated metadata submission
- Important for those supporting many SPs
- Potentially lets admins manage metadata once (locally) and submit without making double entry

Help for those new to InCommon

- Revise metadata update interface to help those new to and unfamiliar with SAML and the InCommon Federation.
- Simpler, easier-to-understand documentation; better integration with app.

Better Baseline tracking

- Periodic validation of endpoints and contacts to ensure entities remain in compliance with Baseline Expectations requirements.

What’s new with the “MDQ” Metadata Service?

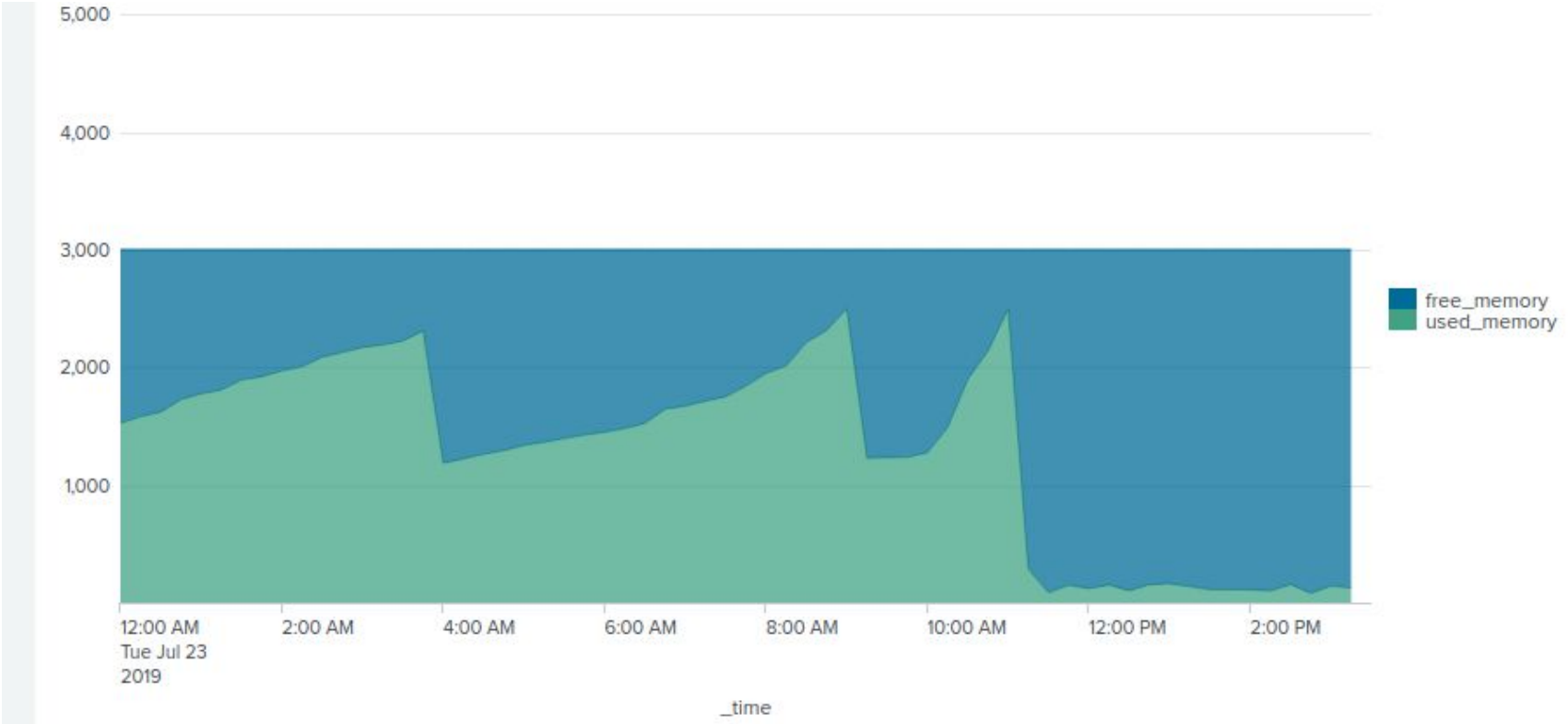
Legacy Metadata Service

- Distributed as aggregate only
- Over 65 MB; requires significant system memory and can over 15 minutes to load
- Updated daily
- Error in a single record corrupts the entire aggregate

MDQ Metadata Service

- Queryable via a web API
- Look up takes milliseconds
- (coming) near real-time updates - metadata available as soon as it is approved
- Scales well with commercial SaaS vendors - one entity record per customer

Using MDQ saves system memory



Retrieving and using metadata via MDQ

- Web API: retrieve an entity's metadata by constructing a web URL, e.g., https://mdq.incommon.org/entities/urn:mace:incommon:internet2.edu
- Backward compatible: still supports aggregate download: https://mdq.incommon.org/entities/all
- Shibboleth supports MDQ out of the box
- Easier for software that can't natively consume metadata aggregate
- Enables new possibilities for implementing discovery service

Transitioning the Community to MDQ

- In release candidate **now**
- Targeting official launch around TechEx time
- Finalizing production operation procedures
- Gathering early adopter feedback; improve documentation

- **First half 2020**
- Step up communication and support - ***every participant will need to take action***
- Goal: migrate everyone to new service location by Fall 2020
- Assess feedback and adjust

- **Second half 2020**
- If necessary, encourage use of new per-entity query capability
- Nudge the stragglers
- Goal: shut down legacy service by end of 2020

Thank you.

How does InCommon metadata work?

Federation Manager

“MDQ” Metadata Service