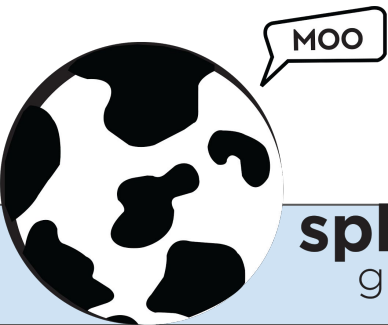


# What's New With COnanage

CAMP 2020 Zoom




**spherical cow**  
group

# Agenda

- Brief Overview of COmanage
- COmanage Registry v3.3.0
- COmanage Registry v4.0.0
- COmanage Match

# What is COmanage?

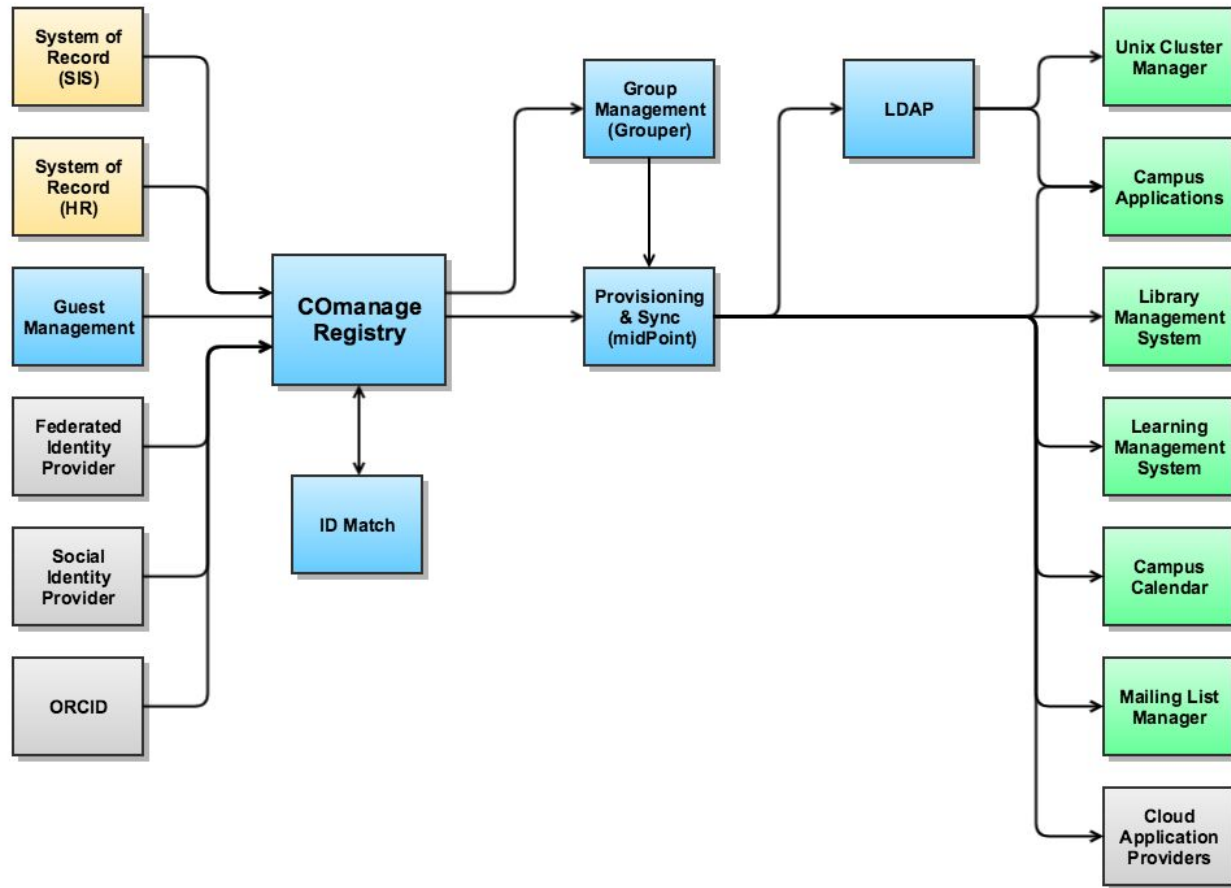
# What Is COmanage [Registry]?

-  **COmanage**™ Is The **Project**
- Registry Is The **Product**
  - *(Like “Shibboleth” and “IdP”)*
  - A Person\* Registry: A place to store information about people associated with your organization
    - *\*also groups, departments, organizations, email lists, services, authenticators, servers, and some other things*

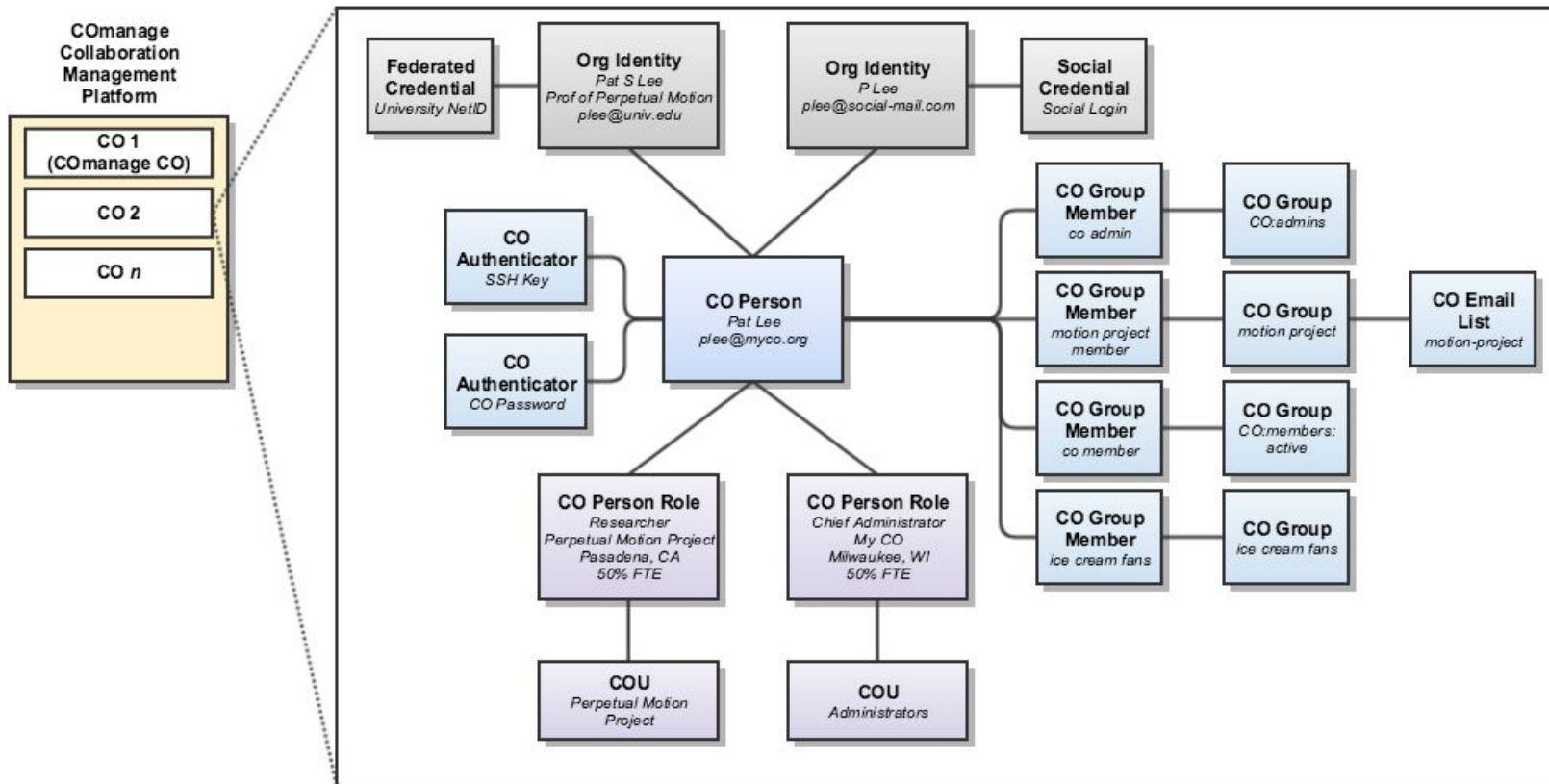
# What Is COmanage?

- Registry
  - Enrollment, Lifecycle, and Attribute Management
  - Complex representations of people with multiple components to their identity
    - Virtual Organization / Collaboration Management
    - Guest / Non-Traditional Population Management
    - University Identity Registry
- Match
  - Rule based record matching from multiple sources

# CManage Institutional Reference Architecture



# COmanage Registry Data Model



# COmanage Registry Capabilities

- Most non-core features are designed to provide common capabilities out of the box, but allow replacement or integration with more comprehensive products, eg:
  - Group Management
  - Provisioning
- UI driven configuration and operation
- REST API



# CManage Registry Capabilities

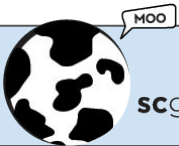
- Person & Role Attribute Management
  - Normalization
  - Attribute Enumerations
  - Multi-valued Names, Addresses, Email Addresses, etc
- Identifier Assignment and Management
  - Pattern based sequential or random identifier assignment
  - Tracking of external (non-Registry) identifiers

# CManage Registry Capabilities

- Population Organization
  - COUs & Departments
  - Basic Group Management
- Human Readable Transaction History
  - Person / Group / Email List / Petition
- Database Level “Changelog” (Copy-On-Write)

# COmanage Registry Capabilities

- Self Service & Delegated Enrollment & Lifecycle Management
  - Enrollment Flows
  - Early Onboarding
  - Duplicate Management / Relinking
  - Sponsors
  - Expiration Policies
  - Basic Matching \*more to come
  - Terms & Conditions



# COmanage Registry Capabilities (Plugin based)

- Organizational Identity Sources
  - For creating records from external sources
  - API, Env, File, LDAP, Salesforce, etc
- Provisioners
  - API, GitHub, Grouper, LDAP, Mailman, Salesforce, SQL, etc
- Authenticators
  - SSH Keys, Service Tokens, Certificates, Passwords, MFA

**(lots more in COmanage training)**

# COmanage Registry v3.3.0

# CManage Registry v3.3.0

- Probably the biggest release in the project's history
  - 127 resolved JIRA issues
  - 19 months since v3.2.0 (Jan 2019 → Aug 2020)
- First maintenance release (v3.3.1) Oct 2020
- Second maintenance release est Dec 2020

# New Release Schedule

- Feature releases (x.y.0) every 6 months
  - Roughly aligned with I2 conferences
  - Scope freeze one month prior to expected release
- Next feature freeze: Jan 15, 2021
- Next expected feature release (v4.0.0): Mid-late Feb 2021
- Maintenance releases as needed
  - Every couple of months, typically



# New in v3.3.0: Cluster Management

- Plugin based approach to managing server accounts
- UnixCluster Plugin
  - Map CO Person Identifiers to Usernames and UIDs
  - Autogenerate Home Directories
  - Map CO Groups to Unix Groups and GIDs
  - LdapProvisioner support for writing Cluster info to LDAP
    - voPerson support for multiple Unix Clusters per CO Person

# New in v3.3.0: Nested Groups

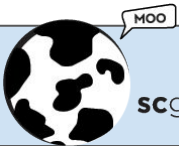
- Members of CO Group A automatically become members of CO Group B
  - Intended for smaller deployments looking to minimize components, will not scale to larger deployments
  - Nested Groups do not behave the same as Grouper groups with Indirect members
- v4.0.0 adds support for AND/OR and NOT logic

# New in v3.3.0: Ad Hoc Attributes

- Key/Value Pairs attached (for now) to CO Person Roles
- Replaces (eventually) Extended Attributes
  - Non-dynamic data model
  - Full REST API support
  - Org Identity Source support
  - Pipeline support
  - Provisioner support

# New in v3.3.0: BulkLoad Shell

- Improved Tooling For Initial Loads
- BulkLoad Shell intended for ~50k+ records
- Can load ~500k records in ~10 minutes on 1 vCPU with 2GB RAM with a local database
- Prepare JSON file of supported data model elements



# New in v3.3.0: BulkLoad Shell

- Some Important Constraints
  - Most automatic processing (Identifier Assignment, Provisioning, etc) is skipped
  - Only supports Postgres (for now)
  - Requires Registry application to be off line
  - Suitable for "flag day" conversions
- Looking at additional improvements or new tooling to facilitate extended transition conversions

# New in v3.3.0: ID Match API Implementation

- Experimental integration with ID Match API (as implemented by COmanage Match)
- Some current limitations
  - Only supported via Pipelines (not Enrollment Flows)
  - Restricted to the usual "troika": Name, DoB, National ID
  - Match API is under (minor) revision as part of Software Integration Working Group documentation effort

# New in v3.3.0: New Provisioners

- midPoint Provisioner
  - Experimental, push COmanage → midPoint only
  - Likely to be superseded by new push/pull integration model
    - ApiProvisioner + consolidated CO Person API
    - midPoint Connector
- SQL Provisioner
  - Creates "cleaned up" representation of operational models
  - Suitable for building custom views on top of

# New in v3.3.0: Even More Stuff

- Identifiers attached to CO Groups
  - Identifier Assignment also supported
- Identifier Assignments using other Identifiers
- Data Filters
  - Plugin based mechanism for altering data in processing
  - Currently supports data prepared for Provisioners
    - Group Filter, Group Name Filter
- Finer grained REST Authz



# New in v3.3.0: Even More Stuff

- Provisioners support CO Services
- Ongoing improvements to Group management UI
- SSH Key management moved to Authenticator Plugin
- Department types
- Search-as-you-type People Picker for Sponsors
- Lots and lots of bug fixes

# COmanage Registry v4.0.0

# CManage Registry v4.0.0

- First release in the new semi-annual release cycle
- Some breaking changes
  - Enrollment Flow Plugins are instantiated
  - CManage CO Localization apply platform wide
  - Attribute Enumerations are based on Dictionaries
  - Probably more to come...
- Scope freeze 15 Jan 2021

# New in v4.0.0: Asynchronous Provisioning

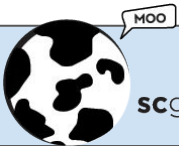
- Provisioning mode configurable per target
  - Queue Mode: Fully asynchronous
  - Queue on Error Mode: First attempt is synchronous, on failure queue for asynchronous retry
    - Subject to Retry Interval
- Queues processed via Registry Job Shell
  - Processing is currently serial, but may change in the future

# New in v4.0.0: Nested Groups Boolean Logic

- AND: CO Person must be in *all* Nested Groups to be a member in the Target Group
- OR: CO Person may be in *any* Nested Group to be a member in the Target Group
  - v3.3.0 behavior
- NOT: CO Person who is a member of the Nested Group *can not* be a member in the Target Group
  - Can create "exclusion" groups

# New in v4.0.0: Dictionaries

- Basically, a list of values
  - Optionally coded
  - Optionally ordered
- Used by
  - Dictionary Identifier Validator
    - Allows for rejection of Identifiers matching entries
  - Attribute Enumerations
    - Allows for reuse: the same Dictionary may be used in multiple enumerations



# New in v4.0.0: Identity Documents

- Attached to CO Person
- Typed
  - Passport, Visa, Drivers License, Self Asserted
- Issuing Authority, Subject, Verification Method
- Can be collected during enrollment
- Not currently tied to identity proofing standards (eg: NIST SP 800-63), but maybe in the future

# New in v4.0.0: Organizations

- Primary Registry Object
- Intended to represent entities outside the CO
  - vs Departments, which represent organizational structure within the CO
- Support most "MVPA" attributes
  - Identifiers, Addresses, URLs, etc
- Expected to be used for future functionality, TBD



# New in v4.0.0: MFA Enrollment Management

- Designed to integrate with multiple components to enforce MFA enrollment policies
  - MeemEnroller Plugin
    - Policy engine with REST API
    - Designed to integrate with (eg) SATOSA
  - PrivacyIdea Authenticator

# COmanage Match

# Moving Towards Match v1.0.0

- Working with Early Adopter campuses to smooth out rough edges, finish initial feature set
- Working with TAP Software Integration WG to finalize ~~Core Schema~~ Attribute Dictionary and ID Match API, with appropriate updates to Match implementation
- Improve integration between Registry and Match

# COmanage Stuff

- Wiki
  - <https://spaces.at.internet2.edu/display/COmanage>
  - <https://spaces.at.internet2.edu/display/COmanage/Email+Lists>
- Git
  - <https://github.com/Internet2/comanage-registry>
  - <https://github.internet2.edu/COmanage/match> (develop)
- TAP Packaging
  - <https://spaces.at.internet2.edu/display/TPD>

