C-4 Scoping: Reorganizing Organizational Identities

Background

Organizational Identities are intended to record representations of identities created outside Registry, such as those from Identity Providers or Systems of Records. However, in the early days of COmanage, pulling these identities from outside sources was challenging, and so early on the ability to manually create Organizational Identities via Enrollment Flows (or directly via the UI) was added. In retrospect, this was probably a mistake.

In Registry v2.0.0, Organizational Identity Sources were introduced as a first step towards fixing this problem. Organizational Identity Sources are basically interfaces to external data sources, and create read-only Organizational Identity records that can only be updated when the authoritative upstream record is updated.

However, the gathering of external identity, especially in a federated context, is unreliable. Attributes might be released, but might not be accurate or corrected in a timely manner. Attributes might not be released at all. Identity providers might not even participate in the federation. As such, there will still be a need manually enter or override Organizational Identity information.

Proposal

Shadow Organizational Identities

Organizational Identities will become read only entities that can only be created from an Organizational Source. To allow for corrections and manual entry, the concept of *Shadow Organizational Identities* (CO-1635) will be introduced. Shadow Organizational Identities will be implemented using the existing OrgIdentity model, and can be used in one of two ways:

1. **Linked**: A Shadow OrgIdentity can be linked to an OrgIdentity that was created from an Organizational Identity Source. In this case, the Shadow OrgIdentity's attributes will override the OrgIdentity's attributes in context like Pipelines, allowing corrections and changes to authoritative attributes.
2. **Independent**: A Shadow OrgIdentity can be created independently of an existing OrgIdentity. In this case, they can be used to represent an external affiliation without a proper link to an authoritative source. It will not be possible to attach login identifiers to Independent Shadow OrgIdentities, since these identities are not bound to an identity provider. (An OIS like EnvSource should be used to create a proper OrgIdentity if an authoritative source is available.)

Shadow OrgIdentities can only be created by being attached to an existing CO Person. It will not be possible to create a standalone Shadow OrgIdentity.

Transition

In Registry v6.0.0, it will no longer be possible to manually create or edit "normal" Organizational Identities. Identities created directly in Registry will consist only of CO Person attributes.

1. The user interface for manually creating Organizational Identities will move from being a top level Registry Object (ie: a link in the main menu) to being an additional attribute on a CO Person record (similar to CO Person Roles).
2. The OrgIdentity REST API will not permit a record to be created without a CO Person ID.
3. Enrollment Flows will no longer be configurable to collect Organizational Identity attributes as part of the Petitioner Attributes step.
    a. This implies that features like "Copy Org Identity Attributes to CO Person Record" will go away.
    b. A new step will allow for the creation of Shadow Organizational Identities after the CO Person is created, similar to how Identity Documents can be attached via the NationalityEnroller (but maybe not via a plugin). This will allow for prompts like "please indicate your institutional affiliation". Fields for this step will be configurable, and fields like name might default to the CO Person values.
    c. See also Org Identity Enrollment Refactoring Design Discussion.
4. Existing OrgIdentities that are not linked to an Organizational Identity Source will automatically become Shadow Organizational Identities.
    a. If there is a Login Identifier attached, the OrgIdentity will become a Shadow OrgIdentity attached to an OrgIdentity that in turn is attached to an EnvSource OIS.
5. It will be possible to create records directly in Registry consisting of CO Person attributes only (CO-870).
    a. In order for these identities to be able to login to Registry, either an external Organizational Identity must be attached, or an Authenticator must be used.
    b. For Authenticators, Identifiers attached to a CO Person can be flagged as *login*. Then, the SP protecting Registry can be configured to authenticate against an IdP the uses the appropriate Authenticator repository for authentication.

(Note it would be possible to sync CO Person records from one COmanage CO to become Organizational Identities in another COmanage CO, but this is something of a special case.)

Transmogrification

When importing records from earlier versions of Registry, Registry PE will:

1. Remove Organizational Identity attributes from Enrollment Flows. These attributes *may* be converted to Shadow OrgIdentity attributes if a straightforward conversion process can be developed. Otherwise, Administrators will need to manually reconfigure their Enrollment Flows.
2. Existing OrgIdentities will be transitioned as described above. Note this transition may happen in Registry v5.0.0, as part of the Org Identity Enrollment Refactoring Design Discussion.
3. Provisioners will no longer look at Org Identity data, even as exceptions. Old configurations will (probably) not be migrated.

Benefits

1. There is a significant amount of complex logic for handling Organizational Identities, particularly in Enrollment Flows. This reorganization will simplify that logic.
2. The distinction between Organizational Identities and CO Person records will become clearer.
3. Removing this option will simplify deployment for new adopters.

Drawbacks

1. This will require some form of migration for almost every existing deployment, especially older ones.

Conclusion

TBD.

Related JIRA Issues

- CO-421 Add New Org ID Should Become Enroll
- CO-635 Default Enrollment Without Email Confirmation
- CO-753 Refactor CoInvites
- CO-757 Verify Petition Email Addresses
- CO-870 CO Person Without Org Identity
- CO-1545 Remove CMP Enrollment Attributes and Old Style REMOTE_USER Enrollment
- ~~CO-1624 EnvSource with Self Signup Cannot Verify Email~~
- CO-1635 Shadow Organizational Identities
- CO-1636 EnvSource based account link does not work when the new login method is from the same source
- CO-1671 Re-enrolling does not allow creating a new OrgIdentitySource record
- CO-1997 Identity linking flow using EnvSource creates additional CoPerson record
- Various tickets become invalid:
    - CO-460 Authenticated Identifier Type Forced to ePPN
    - CO-862 Copy To CO Person Should Support Types
    - CO-1380 Pipelines Attached To Enrollment Flows
    - CO-1381 Execute Pipeline For Default Enrollment
    - CO-1578 Enrollment Source Invitation Single Org Identity
    - CO-1647 Petition verifies OrgIdentity email, even if already confirmed
    - CO-1761 For Self-Signup, OrgIdentity attributes are not copied to COPerson