COmanage midPoint Integration Approaches

Background

A common question amongst the InCommon Community has been the relationship between COmanage and midPoint. There is no one exact answer to this question, as with many integration problems the best answer for a given deployment will depend on the circumstances of that deployment. For example, a deployment with complicated enrollment and lifecycle policies may benefit more from COmanage, while a deployment with sophisticated provisioning requirements may benefit more from midPoint. (And of course these are not mutually incompatible requirements.) However, there are a few basic patterns that can be used as a reference point in understanding the possibilities.

Canonical Person Record

To best understand these patterns, it is helpful to introduce the concept of a *canonical person record*. In a typical higher education identity management system, one or more systems of record serves as an authoritative source of attributes about a person's specific affiliation with the institution. For example, the student system asserts the person's student role, but in general cannot say anything about any employment role the same person might have.

One of the responsibilities of the campus identity management system is to link these authoritative records together into a single view of the person. (As a side effect of this linkage, additional attributes may be assigned to the person, such as a netID or campus email address.) While many systems (such as the learning management system or the library management system) may receive versions of the canonical person record for their own use, only one system can maintain the canonical person record. This is the system where errors are fixed before propagating to downstream systems.

Assumptions

This document omits Grouper, ID Match, and other components for simplicity. There are numerous variations on these approaches utilizing some or all of these other components.

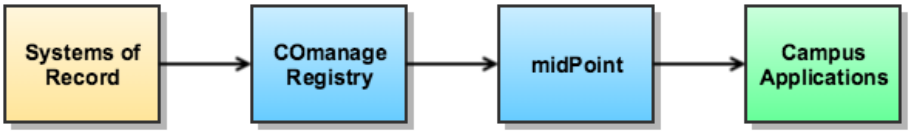
Integration Approaches

I. COmanage Only

In this approach, COmanage is responsible for all aspects of identity management, including receiving records from SORs and provisioning to downstream systems. midPoint is not deployed.

This approach is most suitable for smaller organizations, including virtual organizations, that do not require the complexity of additional components.

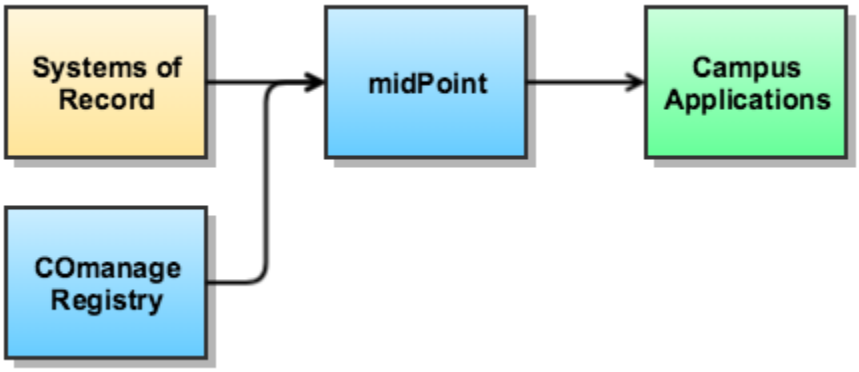
II. COmanage Primary, midPoint Downstream



In this approach, SOR data is linked together by COmanage, which is responsible for managing the canonical person record. This record is then synchronized to midPoint, which is responsible for provisioning the appropriate data to downstream systems.

This approach is most suitable for organizations with complex requirements for matching and merging records from multiple upstream sources.

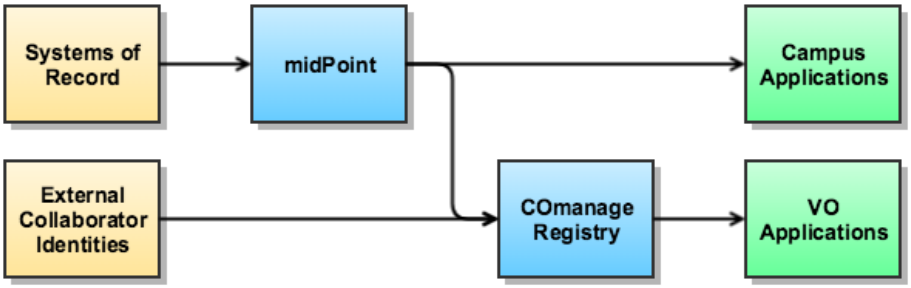
III. midPoint Primary, COmanage Upstream



In this approach, SOR data is linked together by midPoint, which is responsible for managing the canonical person record, as well as provisioning the appropriate data to downstream systems. COmanage operates as another SOR, providing guest management or similar capabilities.

This approach is most suitable for organizations with a single physical System of Record and relatively simple requirements for guest management.

IV. midPoint Primary, COmanage Downstream



In this approach, SOR data is linked together by midPoint, which is responsible for managing the canonical person record, as well as provisioning the appropriate data to downstream systems. COmanage operates as a downstream system, presumably using campus identity as a source in a separate VO identity management system.

This approach is most suitable for organizations with a single physical System of Record and a desire to "pre-provision" COmanage for campus-sponsored Virtual Organizations.

V. midPoint Only

In this approach, midPoint is responsible for all aspects of identity management, including receiving records from SORs and provisioning to downstream systems. COmanage is not deployed.

This approach is most suitable for organizations with a single physical System of Record.