IDENTITY & ACCESS MANAGEMENT

IAM Roadmap

Modernization Journey & Forward Plan

IAM Team

Weber State University

May 2026

Key Roadmap Priorities

Strategic themes shaping our work

01

Identity Governance

Modernize identity lifecycle and group management using midPoint and Grouper, replacing the legacy Weber IDM system.

02

Directory Services

Introduce OpenLDAP alongside Active Directory to support a clear separation between active and inactive identities.

03

Legacy System Retirement

Gradually retire the Weber IDM system and reduce reliance on legacy data warehouse triggers and custom code.

04

Continuous Improvement

Build foundational capabilities for identity lifecycle, password management, and self-service across the university.

Roadmap Overview

A phased journey from Weber IDM to a modern, standards-based platform

PHASE 1

Completed

September 2025

Group Management Foundation

- Centralized group membership control using midPoint and Grouper.
- Employee lifecycle group

PHASE 2

In Progress

Targeting July 2026

IAM Platform Takeover

- IAM takes over user management
- Identity created in midPoint
- AD provisioning & password flow

PHASE 3

Upcoming

Starting ~July 2026

OpenLDAP & Lifecycle End

- Introduce OpenLDAP
- Split active vs inactive directories
- End-of-lifecycle handling

Phase 1: Group Management Foundation

Completed - September 2025

COMPLETED — *Centralized group membership control using midPoint and Grouper.*

Objective

Implement the new IAM (Identity and Access Management) architecture in a production environment, beginning with centralized group membership control using midPoint and Grouper. Phase 1 marks the start of this transition, with the primary goal of replacing the current group management functionality performed by Weber IDM with midPoint.

Project Scope

1

Test Integrations

Setting up test integrations.

2

Production Specifications

Defining production specifications.

3

Infrastructure Deployment

Deploying infrastructure.

4

Group Provisioning & Access Control

Ensuring seamless group provisioning and access control through the new system.

Phase 2: IAM Platform Takeover

In Progress - Targeting July 2026

IN PROGRESS — *midPoint fully takes over user creation, centralizing governance and automating identity flows.*

Overview

Phase 2 focuses on enhancing and streamlining enterprise identity lifecycle management by consolidating user provisioning, authentication, and authorization processes. The IAM platform (midPoint) fully takes over user creation responsibilities, ensuring centralized governance and automated identity flows across systems.

Key Deliverables

1 Password Management

With the completion of Create WCID / Password SS 2.0, user passwords are sent to midPoint only - establishing midPoint as the single authoritative source for password management.

2 Identity Synchronization to AD

Once a user sets their initial password, the user account and credentials flow automatically to Active Directory - placed into the correct home OU and into all of their assigned groups.

Phase 3: OpenLDAP & Lifecycle End

Upcoming - Starting ~July 2026 (~4 month duration)

UPCOMING — *Introduce OpenLDAP and reshape directory services around identity status.*

Introduce OpenLDAP

Stand up OpenLDAP as a new directory service, with identity provisioning and password flows integrated with midPoint.

Active vs. Inactive Split

Active students and employees remain in Active Directory. All other identities (inactive, retired, alumni, vendors) move to OpenLDAP.

End-of-Lifecycle Handling

Gradually migrate inactive identities out of AD into OpenLDAP, implementing a clean end-of-lifecycle process.

Key Architectural Shift

Active Directory becomes the privileged directory for active populations only. OpenLDAP serves as the universal directory for all identities, with passthrough authentication for users who still have AD accounts. The migration is intentionally gradual rather than a single cutover.

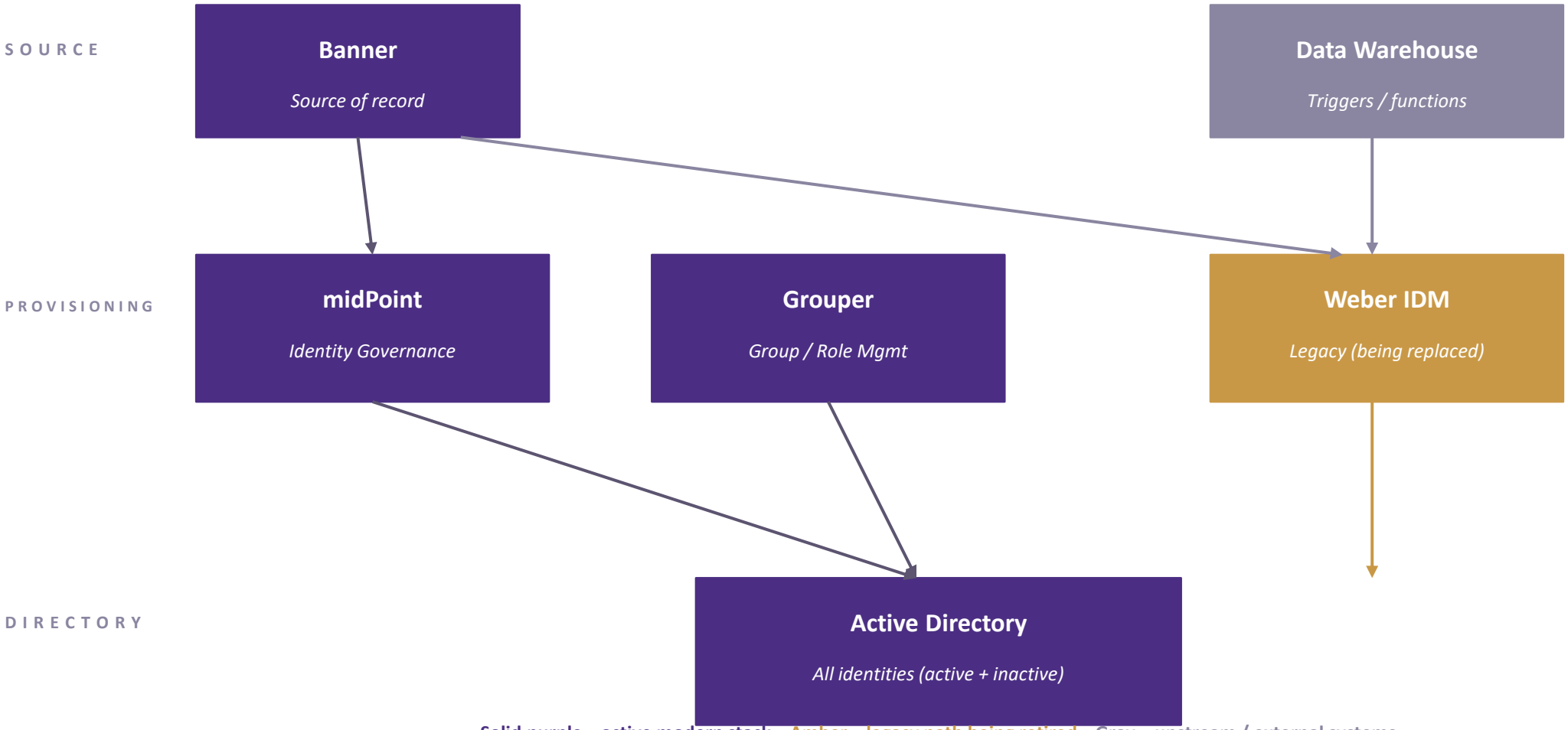
APPENDIX

Architecture

Current state vs. planned future state

Architecture: Current State

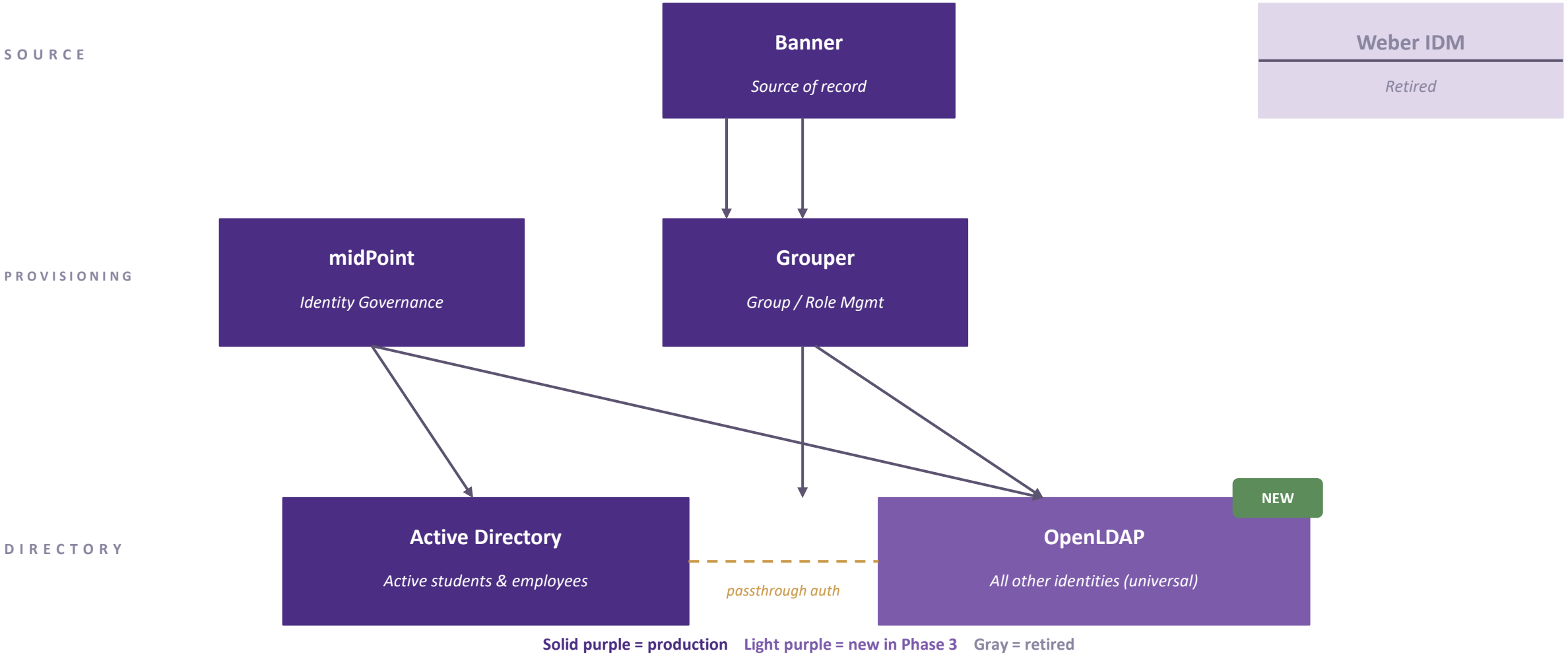
As of May 2026 (Phase 2 in progress)



Solid purple = active modern stack **Amber = legacy path being retired** **Gray = upstream / external systems**

Architecture: Planned Future State

After Phase 3 completion



What's Changing

Current state versus planned future state

CURRENT STATE

- Weber IDM is the active provisioning system
- Data Warehouse triggers feed legacy provisioning
- Active Directory holds all identities (active and inactive)
- midPoint and Grouper coming online during Phase 2
- OpenLDAP not yet in the architecture

PLANNED FUTURE STATE

- midPoint is the authoritative identity provisioning system
- Weber IDM retired
- Active Directory holds only active students and employees
- OpenLDAP serves as the universal directory for all other identities
- Passthrough authentication maintains continuity for users in both directories

Thank You

Questions, feedback, and discussion welcome.

IAM Team | Weber State University | May 2026