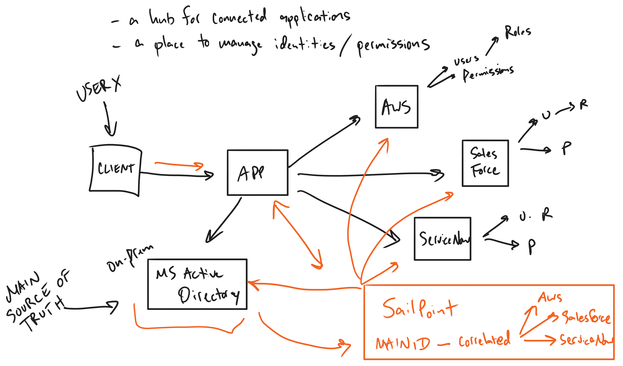
SAILPOINT (HIGH-LEVEL)

SailPoint

- a hub for connected applications
- a place to manage identities / permissions



SSO → Single Sign On

IDENTITY → Person, their data/characteristics/permissions, login information, org hierarchical information
- Can also be an API/instance

ROLE → a set of permissions, usually centered around job function - can be requested/revoked/timed
- easier to manage than individual permissions
- can be combined w/ individual perms

POLICY → a rule about how something must be done
- ex. can't have both Role A and Role B
- Separation of Duties — a workflow must be started by Emp A and finished by Emp B
- Can be preventative or detective

ENTITLEMENT — a permission to do a specific thing
- Entitlement Catalog stores all Entitlements from all connected applications

APPLICATION — any system connected to Sailpoint that has identities correlated w/ SailPoint identities

CORRELATION — matching up external Identities to those in SailPoint and (optional) syncing properties
- this requires mapping of properties
  ex. AWS 'id' = SailPoint 'userId'

We're using Identity IQ v8.3 — on-prem version of SailPoint Software

Identity Now — cloud version (similar but not exactly the same)
Identity Security Cloud

by default: Java 8
Runs on a Tomcat Server v.9.x (Apache)
MySQL
Basic Authorization

CERTIFICATION → a review of current entitlements
→ Campaign → a company/dept-wide review of all entitlements, roles, etc.

PRINCIPLE OF LEAST PRIVILEGE → only grant the minimum required access to complete work tasks