INTERNET2 TECHEX26

OCT 26-30 | MINNEAPOLIS MN





UNIVERSITY of VIRGINIA

Information Technology Services

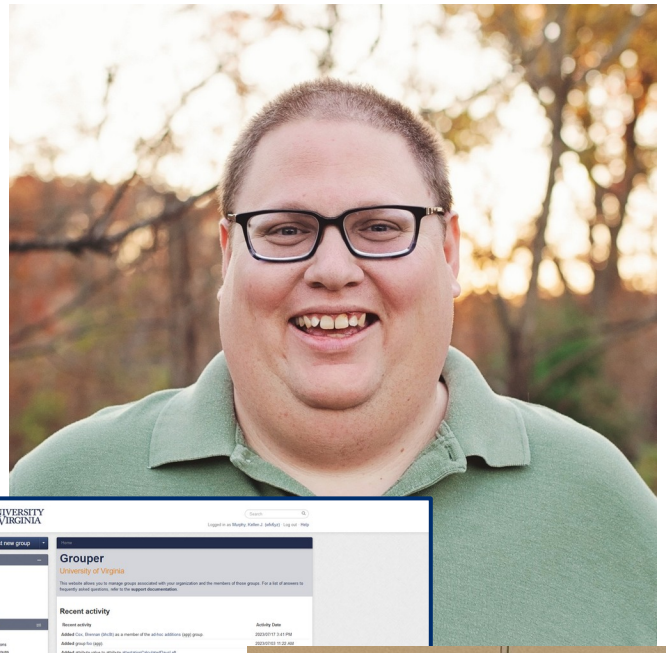
NetBadge Reborn

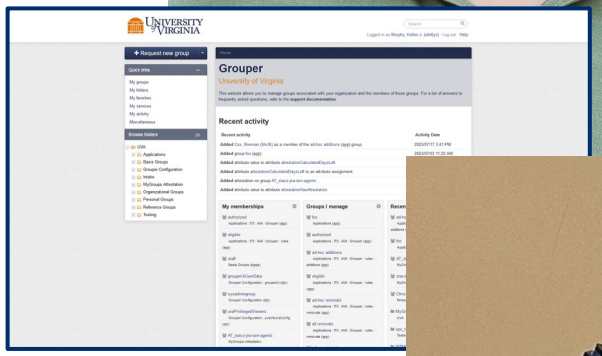
Shibboleth Under New Stewardship at the University of Virginia

Kellen Murphy, Identity Architect, University of Virginia

October 27th, 2026

About Me







At UVA…

Senior IAM architectural resource and technical SME for Shibboleth, Grouper, Keycloak, AuthN/Z, etc.

Before UVA…

Nerd → Nuclear Physics M.S. → Cosmology Ph.D. → SAML Consultant

¯_(ツ)_/¯

In the community…

Technical Advisory Committee, RPDO-WG, TAC liaison to CACTI, various other working groups, BaseCAMP planning, etc.

About NetBadge (Shibboleth IdP)

24.4M

successful sign-ins in the last 12 months

540+

applications in use in the latest quarter

~67,000

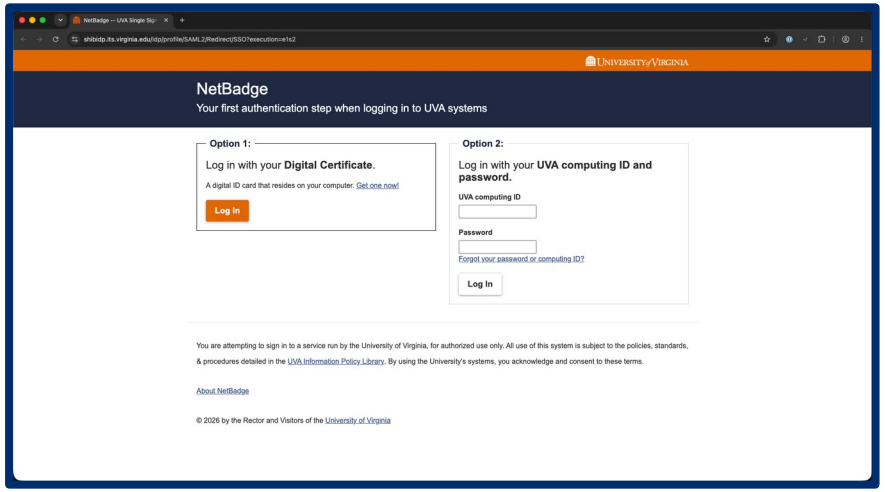
sign-ins on an average day

2

Duo integrations fronting all of it: regular and step-up

> **“This page has not changed in years. Everything behind it has.”**

Source: Splunk, production nodes, Oct 16, 2025 – Oct 15, 2026. 540 is the quarterly distinct-application floor.



INTERNET2 TECHEX26

OCT 26-30 | MINNEAPOLIS MN

What We Inherited



We inherited a system that only few *really* understood…

Ingress	An F5 terminates TLS and runs **certificate login using iRule.**
Infrastructure	**RHEL 8 VMs under Jetty 12**, five production nodes (7 subproduction).
Configuration	A **Ruby** join script assembles config; **Ansible deploys it from a laptop**, and the hosts' Python 3.6 pins the control node.
Documentation	The maintainers guide lived in an internal **ServiceNow KB**, our intake forms reflected outdated rules and our published attributes KB was **wrong about our own policies.**

Stable but stationary: it worked, but it wasn't innovative.

INTERNET2 TECHEX26

OCT 26-30 | MINNEAPOLIS MN

Making It Knowable



Git: the source of truth, every change goes through staging…

Git
The shibidp-conf build system produces every config file

→

Staging
Every change lands here first

→

Production
Deployed from the same build that staging ran

Drift-check: compares what is deployed in various environments with what is in Git, so the repo stays the truth

The guide moved into the repo…

The maintainers guide moved out of a ServiceNow KB and into the repo, next to the config it describes... published to Confluence (where it might get used).

Upgrades deserve a runbook…

The Shibboleth 5.2.3 upgrade (from 5.1.8) followed a written runbook, so the next upgrade will not depend on memory.

Our team can now see *what* we released, and to *whom*…



The default audit log, documented, enhanced.

Every field in the IdP audit format is written down, so a log line answers a question without guesswork.



Splunk across every node…

Audit logs from all nodes are searchable in one place. Every usage figure in this talk is a Splunk query. Documented. Explained.



aacli as self-service

A separate service shows which attributes a user would release to an SP, without touching the production cluster.

What's a *real* problem and what isn't?

INTERNET2 TECHEX26

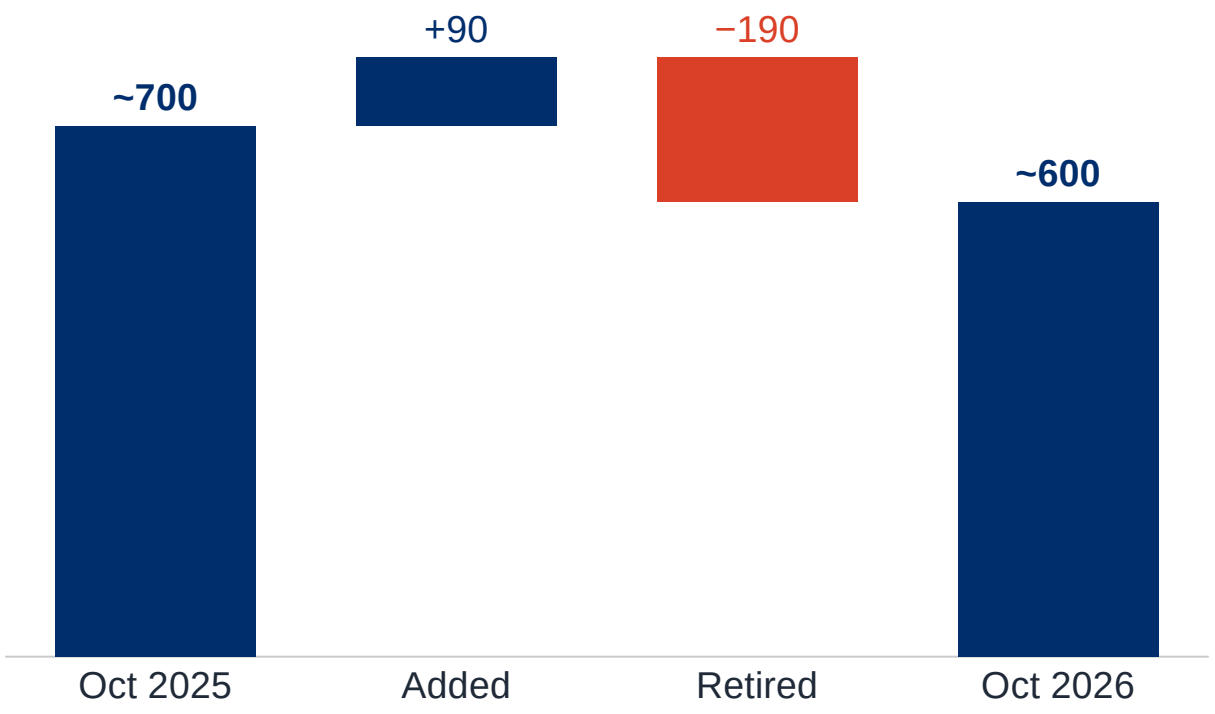
OCT 26-30 | MINNEAPOLIS MN

Attribute Hygiene and Onboarding



In one year, added ~90 applications and retired ~190…

Registered Relying Parties (entityIDs), Oct 2025 to Oct 2026



Source: shibidp-conf repository tree on Oct 15, 2025.

The onboarding path…

129 Unique ServiceNow Requests
RITMs that drove config changes over the year.

Accountability
Technical owner, management, service owner.

Companion tooling
Makes the routine integration steps repeatable.

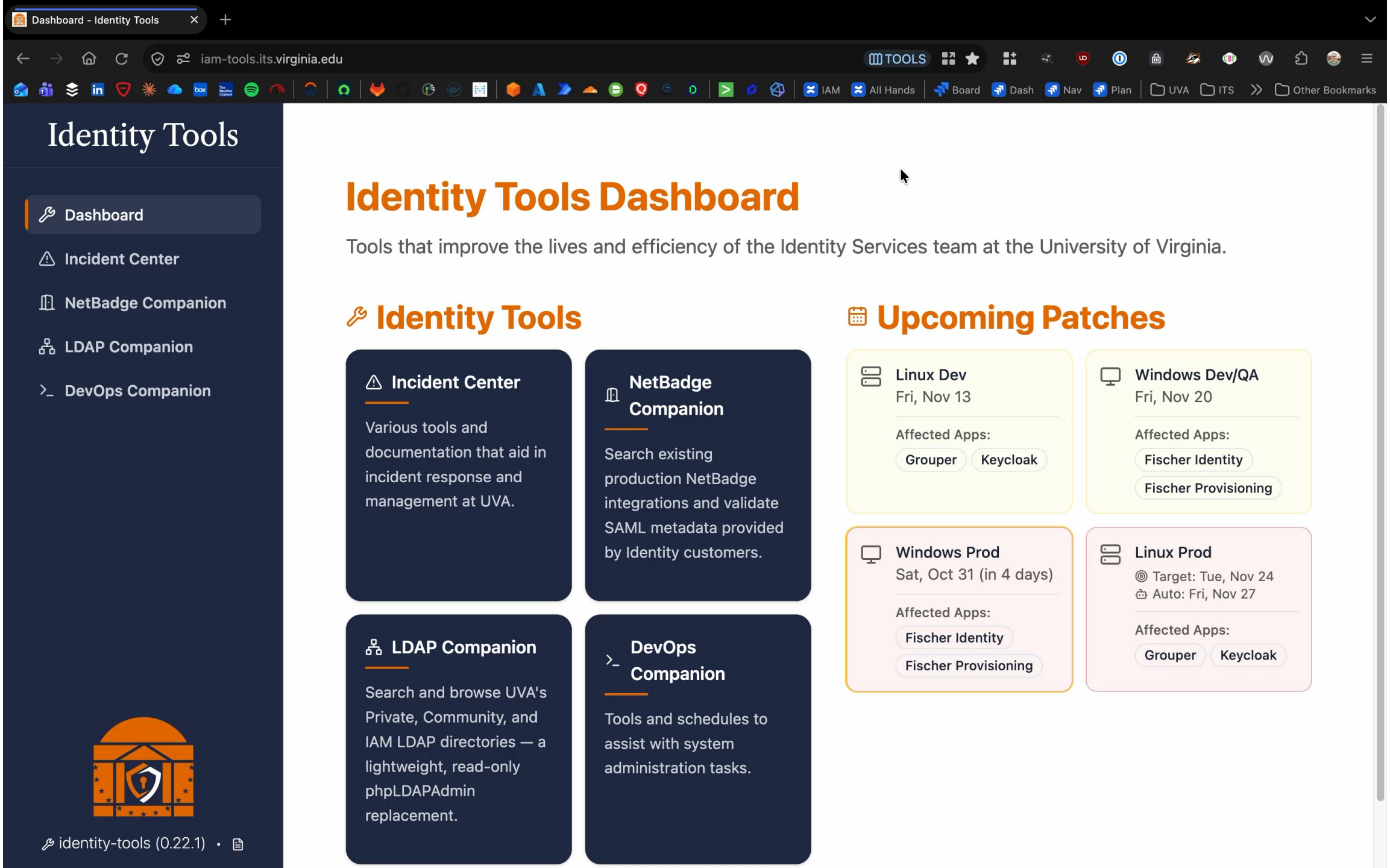
One integration methodology
Applied the same way to every application.

Onboarding the Old Way

1	**Submit RITM**	**ServiceNow form that's NetBadge specific.** With a lot of often-ignored inputs.
2	**RITM Accepted**	**One Team**. Time split between running NetBadge and ITS Storage.
3	**Engineer Build Loop**	**Busy guy.** Deals with assessment for interfacing with requestors, talking to vendors, monitoring health, upgrades, basically the whole shebang.
4	**Delivery**	**Integration eventually works**. Next!

Onboarding the New Way

1	**Submit RITM**	**ServiceNow form that's NetBadge specific.** With a lot of often-ignored inputs.
2	**RITM Accepted**	**IAM Operations w/ Tooling.** Load spread between three people, never one.
3	**Jira Created**	**IAM Engineering w/ Tooling.** Load spread between 2-3 people, never one.
4	**Build Loop is Shared**	**Ops talks, Tools build, Engineers tweak.** Shared work keeps faster pace, happier customers, and fewer engineering hours eaten.
5	**Delivery**	**Integration works**. Next!


Dashboard - Identity Tools
iam-tools.its.virginia.edu
TOOLS
IAM
All Hands
Board
Dash
Nav
Plan
UVA
ITS
Other Bookmarks
Identity Tools
Dashboard
Incident Center
NetBadge Companion
LDAP Companion
DevOps Companion
Identity Tools Dashboard
Tools that improve the lives and efficiency of the Identity Services team at the University of Virginia.
Identity Tools
Incident Center
Various tools and documentation that aid in incident response and management at UVA.
NetBadge Companion
Search existing production NetBadge integrations and validate SAML metadata provided by Identity customers.
LDAP Companion
Search and browse UVA's Private, Community, and IAM LDAP directories — a lightweight, read-only phpLDAPAdmin replacement.
DevOps Companion
Tools and schedules to assist with system administration tasks.
Upcoming Patches
Linux Dev
Fri, Nov 13
Affected Apps:
Grouper
Keycloak
Windows Dev/QA
Fri, Nov 20
Affected Apps:
Fischer Identity
Fischer Provisioning
Windows Prod
Sat, Oct 31 (in 4 days)
Affected Apps:
Fischer Identity
Fischer Provisioning
Linux Prod
Target: Tue, Nov 24
Auto: Fri, Nov 27
Affected Apps:
Grouper
Keycloak
identity-tools (0.22.1)

Claude as a Force Multiplier

- Take policies around integrations and automate them.
- Let Operations know when something isn’t valid: less engineering time.
- Faster time from submission to acceptance to integration creation.
- Less work on the engineering team, more time for harder work.
- Less dependence on *deep* knowledge for the process.

INTERNET2 TECHEX26

OCT 26-30 | MINNEAPOLIS MN

Single Sign-On or *Same* Sign-On?



The *only* SSO… *that serves both Academic and UVA Health



Every identifier problem in this section starts here.

Source: active users by computed role, IAM reporting, Oct 16, 2026. Medical includes roles that do not clear NetBadge today.

Every identifier we tried failed for its own reason

1	**mail**	**A mailbox**, and at the wrong institution for Health staff
2	**mailForwardingAddress**	**User-set**, not reliably @uvahealth.org: some physician faculty point it elsewhere on purpose to keep their two identities apart
3	**University ID**	**FERPA-protected**: stable and institution-wide, but every release needs its own clearance, so it cannot be the default
4	**ePPN**	**The right key**, but it looks like an address, so SPs and users treat it as one

We kept asking one attribute to be both the account key and the contact address. The Health population proved those are two entirely different jobs.

Separate the jobs: one identifier to know you, another to recognize you… Entity Access Categories

subject-id
for SPs that need to know who you are

- Computing IDs are never reassigned
- Identifier-typed, so nobody mistakes it for a mailbox
- **mail** rides along under Personalized Access as contact data

pairwise-id
for SPs that only need to recognize you

- Opaque and different for every SP
- Nothing FERPA-sensitive to clear
- Keeps a physician's Health and academic worlds unlinked



Direction, it's not done…

Built and previewed. Production is targeted for the end of January, because the NIH requirements need the same work.

The requestor vets an SP's need instead of a ticket negotiating it with us.

82
EAC-tagged SPs in InCommon

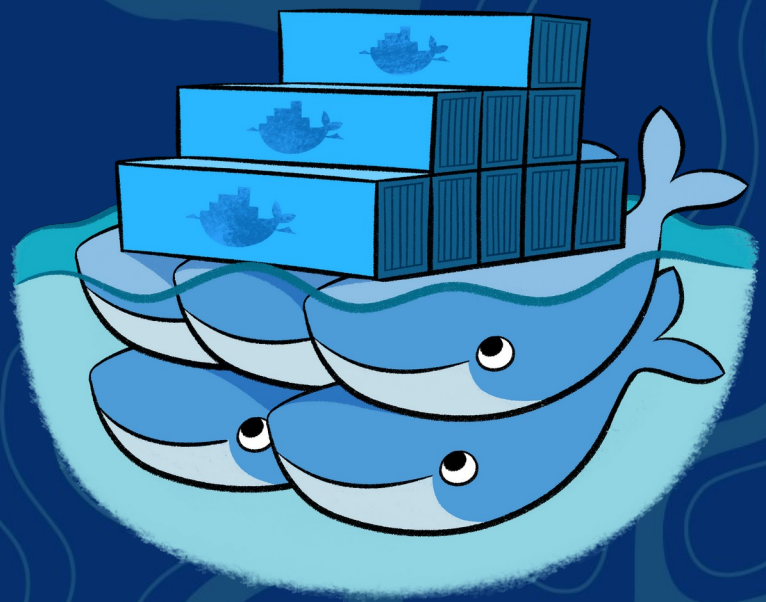
11
of them see UVA traffic

6
MDQ-served SPs gain attributes

INTERNET2 TECHEX26

OCT 26-30 | MINNEAPOLIS MN

Rebuilding It: Containers



The new image builds our existing config on InCommon's TAP base image

shibidp-conf

The same config repo, pulled in as a submodule and never modified

→

Builder stage

make joins the config artifacts, as it does for the VMs

→

TAP base image

InCommon's Shibboleth image, with several plugins enabled

→

Docker Swarm

One image…

On Grounds + in Azure

The beachhead…

The attribute-check service (aacli) already runs this image: attribute resolution and filtering only, no sign-in traffic.

A new release pipeline…

Every commit builds a tagged image, and the last good one stays as the rollback target. Patching becomes an image rebuild.

Certificate login, 2.3 million sign-ins a year, moves off the load balancer… *maybe?*

2.3M

certificate logins in the last 12 months, about 1 in 10 sign-ins

Certificate login is not a niche path at UVA.

TODAY

Browser
presents a certificate

→

F5 load balancer
terminates TLS and runs cert login in an iRule

→

IdP on VMs
receives the result

CONTAINERIZED

Browser
presents a certificate

→

Pass-through ingress (Avi)
hands TLS straight to our service

→

nb-cert-auth
our own tested service, in front of the IdP

Proven end to end on the dev stack on August 22, 2026.

Source: successful redirects through the certificate login endpoint, Jetty access logs, Oct 2025 to Oct 2026. Approximate.

Two findings in deployment affects our design decisions…

FINDING 1

HTTP/2 connection coalescing

Browsers reuse one HTTP/2 connection for two hostnames that share an address and certificate, so a request meant for one host can arrive at the other.

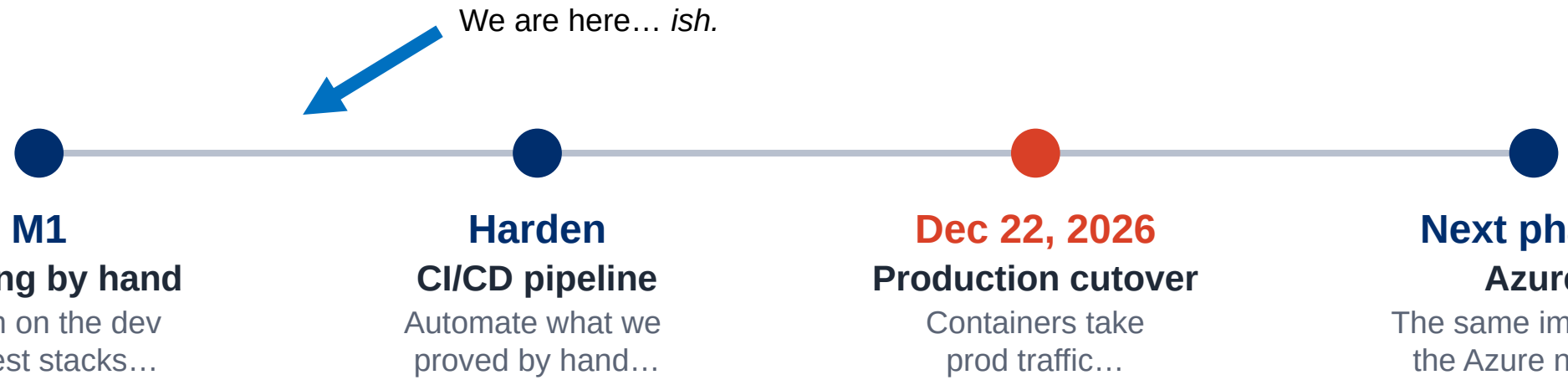
FINDING 2

The __Host- cookie prefix

A __Host- cookie is locked to the exact host that set it, so it cannot carry a session from one of our hostnames to the other.

Both surfaced in deployment, not in the design.

We prove it by hand first; production cuts over December 22



Why this order… Minimum Viable Product.

Grouper went the same way: show it working by hand, harden the pipeline after, go to production last.

A pipeline built for a target nobody has agreed on is backwards.

Still open?

- Avi and certificate authentication…
- Revocation checking for certificate login in the container…
- CI/CD + cert container hardening/vetting ahead of the cutover…

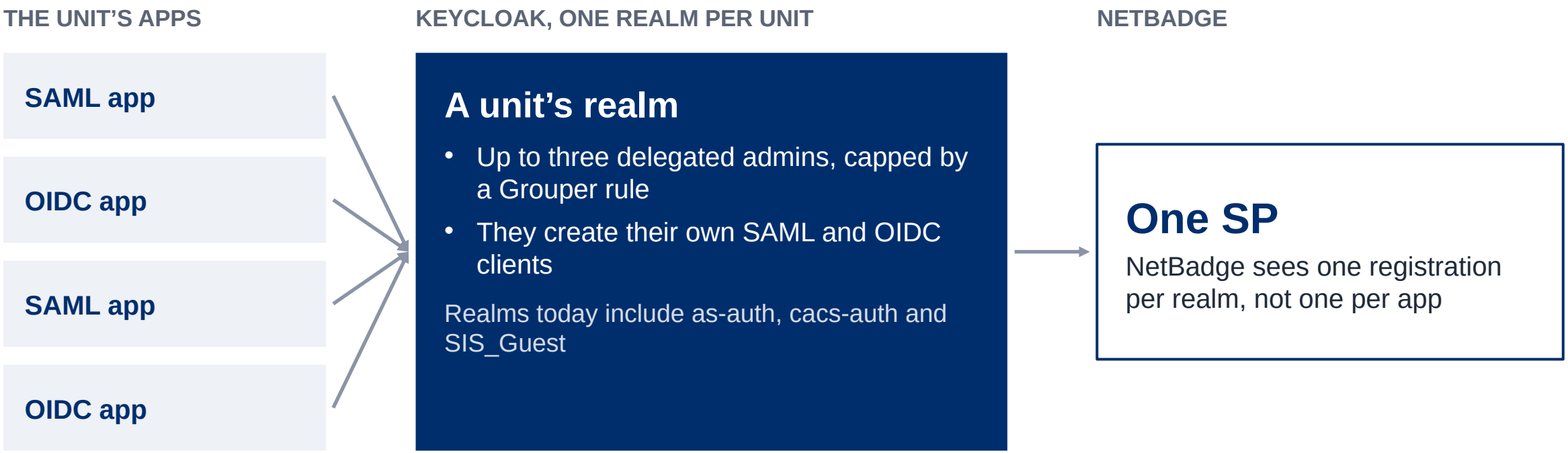
INTERNET2 TECHEX26

OCT 26-30 | MINNEAPOLIS MN

Keycloak Proxying for Bulk Integrations



A unit’s own Keycloak realm turns many integration tickets into one SP



A technically adept unit stops filing one integration ticket per app.

The proxy has costs, so we run it as a product too

No single logout

NetBadge does not support federated logout. Keycloak accepts a logout request, but nothing propagates upstream.

Logging out of an app is local to that app.

The inventory was wrong twice

- **Production held seven realms, not three.** Per-realm hostnames made one instance look like several.
- **Test had no realm behind one registered SP.** We removed the phantom registration.

Count realms from Keycloak itself, not from what NetBadge has registered.

Realm inventory audit, August 5, 2026.

INTERNET2 TECHEX26

OCT 26-30 | MINNEAPOLIS MN

Two Tenants, One SSO Experience



A few thousand people hold the same uid in two Entra tenants

The two-institution problem from earlier, one layer up.

Health tenant
uid@uvahealth.org

A few thousand
people with the same uid in both, out of about 60,000 active

Academic tenant
uid@virginia.edu

Why Entra multitenant organization does not get there

- There is **no Microsoft tooling to dedupe users** across tenants.
- It **assumes a consolidation** neither side is ever going to do.
- **Neither tenant is going away**, so this is not a lift and shift.

Proxying to both tenants could work, and every piece adds complexity

THE SKETCH

The NetBadge login page becomes a **discovery page**

@uvahealth.org
proxies to the Health tenant

@virginia.edu
proxies to the Academic tenant

NetBadge stays the SAML IdP to 540+ SPs
Attributes still come from Private LDAP, joined on the shared uid

Today the form strips everything from @ rightward and tries the bare ID against three directories in turn. Discovery makes the domain the routing decision.

WHAT IT COSTS

Sessions
Two Microsoft sessions and their cookies in one browser

Choosing a domain
Many Health staff do not know they have a virginia.edu address

Certificate login
Offload it into Entra, and then into both tenants?

MFA
One Duo integration becomes two tenants' policies

The question for the room

Proxying might partly solve it, but it adds a lot of complexity...

Who has run an IdP in front of two tenants that hold the same people?

What did you do about sessions and certificates?

INTERNET2 TECHEX26

OCT 26-30 | MINNEAPOLIS MN

This page has not changed in years. Everything behind it has.

24.4 million sign-ins last year. That is who it is for.



In one-year NetBadge became knowable, rebuildable and easier to reach

Knowable
Git is the source of truth, staging comes first, and the logs are documented

An onboarding path
New applications registered and stale ones retired the same way every time

Identifiers for both institutions
subject-id and pairwise-id instead of an email address doing two jobs

A rebuild with a date
Containers on InCommon's TAP image, production cutover December 22

Self-service for units
Keycloak realms for units that outgrow one ticket per app

What is next

December
Containerized production cutover

End of January
Entity categories, subject-id and pairwise-id in production

2027 Q3
Automated staging of integrations using an Anthropic AI CI/CD pipeline out of the Companion

An IdP operator's job is to make it easier for people to get to what they need.

INTERNET2 TECHEX26

OCT 26-30 | MINNEAPOLIS MN

Questions

