Springtime in the Rockies
Subnet Managers Meeting

April 21, 2021

And I Can’t Get Up!
Talkin Bout My…

IS Updates
Infrastructure
Microsoft 365
Identity Management / Middleware
Networking & Telecommunications
Security
Information Systems Updates

Josh Clark

• HR
  – Looking for new system level system.
  – Budget – 1 – 2 yrs.
  – Implementation – 3 – 5 yrs.

• KFS
  – Moving to cloud.
  – Migration efforts
  – Go live 1Q, FY 22.
Information System Updates

• Banner
  – Joint Banner project with Pueblo.
  – Registration module now live.
  – New integrations to follow over next 3 months.
  – Plan to move to Tomcat.
Infrastructure – James Cizek

• Campus cloud replacement hardware

• Team welcomes Stephen Oglesby
  - New CI Facilitator
Microsoft 365 – 3 Things
Lance Baatz, AppDev
1 – DUO w/Microsoft 365

**Who’s Impacted:** Active eIDs registered in DUO

**What:** Logging into M365 services will generate a DUO prompt…at least the 1st time

**When:** June 1st (a Tuesday)

**Why:** Improve security. Protect your information.

**More:**
- Review FAQs at [https://www.acns.colostate.edu/duo-faq/](https://www.acns.colostate.edu/duo-faq/)
2 – Recorded Teams Meetings Saved to OneDrive

Who’s Impacted: Anyone recording a Teams meeting

What: Teams meeting recordings will be saved in OneDrive (previously recordings were saved in Stream)

When: June 2021 (No change through the spring semester!)

Why: Microsoft mandate

More:

– http://help.mail.colostate.edu/m365teamsmeetingrecording.aspx
– Subnet Managers team announcements
3 – Moving to Teams Only (Sunsetting Skype)

Who’s Impacted: Most noticeable to the 200 or so active Skype users but it’s a tenant-wide setting

What: Skype usage will be disabled. People must use Teams instead.

When: May/June

Why: Pre-req for Teams Voice, Microsoft mandating, & it’s time.

More:
  – Subnet Managers team announcements
CSU - CSU System IAM Project – Randy Miotke

- **Goals**
  - Meet the needs of the Joint Banner Project
  - Improve account provisioning and de-provisioning
  - Identity synchronization and reconciliation
  - Integrations using identity connectors
    - Database
    - Active Directory
    - eduPerson directory
    - Grouper
  - Improve freshness of source data
  - Slowly integrate midPoint into CSU Identity operations
Phase Two Complete

December 2020 - CSU-Pueblo AD account provisioning

March 2021 – CSU-Pueblo students register for FA21 classes using NetID
Production Q1 2021

CSU Pueblo Data Sources
- Banner
- HR

NetID Self-Service
- Identity Data

CSU Pueblo IdP
- Supply AuthN and Attributes

SSO
- Access

Campus and SaaS Services

Identity Management
- midPoint
  - Account Lifecycle Identifier Management

Groups
- Provision

CSU Pueblo AD
- Supply Subjects

FC-Hosted eduPerson/MD
- Provision

Group Owner Jobs

Management of Reference Groups

Group Owners

Grouper PSPNC
- Provision

Rabbit MQ

Set Policy and Rules for Accounts and Membership Groups

IAM Admin
CSU Pueblo eAccount to NetID

Requirements

• CSU Pueblo data sources
  • HR
  • Student and Applicant Pre-Fall 21 Data in AIS
  • Fall 21 and forward in Banner MEP

• NetID Self-Service for account management

• midPoint Sync with CSU Pueblo AD

• Maintain CSU Pueblo IdPs

• Pueblo accounts in colostate-pueblo.edu AD will eventually be migrated to colostate.edu

• M365 services will be migrated to CSU tenant
midPoint Environments

• Highly Available PostgreSQL database
  • Transitioned from MySQL
  • Uses Spilo
    • Docker image that contains PostgreSQL, Patroni, pgBouncer and etcd
  • Spans two data centers
  • Swarm consists of four nodes across four VMs, only one node is a manager.

• Complete Environments
  • Development – single node
  • Staging – two nodes
  • Production - two nodes
midPoint Operations

Table Connectors - READ
- Pueblo HR – Person - Employee
- Pueblo Student Temp – Person - Student
- Banner Fall 21 – Person – Student

Table Connectors – Read/Write
- Banner accounts - SSO
- PostgreSQL - self-service

AD Connectors
- csupueblo.edu
- colostate.edu

LDAP Connectors
- eduPerson directory

Live Synchronization – Reconciliation Process
midPoint Lifecycle Rules & Orgs.

Use of Organization Hierarchy

- Campus
- Student Types
- Employee Types
- Activation Status
midPoint Lifecycle Rules & Orgs.

Use of Organization Hierarchy

- Activation Status
  - Active Account
  - Awaiting Activation
  - Expiration Cycle
  - Expired Account
  - Manually Disabled
Test and Stage Environments
NetID Self-Service

NetID - Colorado State University System

Your NetID is an uppercase C followed by your 9-digit CSU ID, for example: C899456789.

The CSU System NetID will eventually replace the CSU-Pueblo eAccount and the CSU Fort Collins eID.

When will you need an active NetID?

- Fall 2020 for CSU-Pueblo faculty, students and staff.
  - Important! CSU-Pueblo employees will need a NetID to access KFS beginning March 17.
- Summer 2021 for CSU Fort Collins students, faculty and staff.

New to the University or need to activate your NetID?
The Planned CSU Transition

- Person and Directory Data
- HR and SIS Identity Sources
- Identity Data
- eD Self-Service
- Supply AuthN and Attributes
- OpenLDAP/Active Directory
- Provision
- CSU IdP
- Access
- SSO
- Campus and SaaS Services
- Provision
- RabbitMQ
- Grouper PSPNG
- Grouper Loader Jobs
- Groups
- Provision External IDs to LDAP
- Groups
- Supply Subjects
- Grouper Access Governance, Policy, Audit, Compliance, and Reference Groups
- Set Policy and Rules for Accounts and Membership Groups
- Group Owners
- IAM Admin
- Grouper UI
- Management of Reference Groups
- CDmanage
- External/Sponsored Accounts
- Source of Record

Colorado State University
Work In-Process

- Step up campus communications & training
- CSU HR data integration must be completed
- Migrate eID accounts to midPoint
  - Currently testing with BANPPRD data
- WEID/ODS directory replaced with midPoint data
  - EID_INT_REF_ID is a legacy value
  - Testing BANPPRD, ODSPPRD
- Preferred Last Name – midPoint as SoR
- NetID email alias management CSU/CSU-Pueblo
- Treatment of Secondary eIDs
- Grouper moving to full Docker environment
What's Next?
Questions?
Networking & Telecom Updates

Jason Huit
Subnet Managers
April 21, 2021
Agenda

- Housekeeping
- Networking Updates
- Telecom Updates
- Teams for Voice
Support from NOC and Telecom

Please use help ticket system.

Please do Not use Teams for support issues.

Order Listing
Support from NOC and Telecom

- Need help?
  - help@colostate.edu | 1-7276

- Need work performed?
  - Cable pulls, hardware installation/replacement
    - Telecom_Projects@mail.colostate.edu
  - Telephony services
    - TelecomServiceOrder.colostate.edu

- Business hours emergency?
  - Networking: NOC@colostate.edu
  - Telecom: 1-5881
Support from NOC and Telecom

- Emergency Support
  - 491-2345
    - *Subnet Managers only, please*

- Option 1: Networking Emergencies
- Option 2: Telecom Emergencies
- Option 3: Telecom Field Emergencies
- Option 4: Cybersecurity Emergencies
And now…
Securing the Network

• **Partnership**
  – UTFAB: $100k
  – CSU System one-time: $800k
  – Central IT capital reserves: $427k

• **Next-generation firewall**
  – Designed for 100Gb+ throughput
  – Threat Detection & Prevention
  – Intrusion Detection & Prevention
  – Network Address Translation & IPv6 capability
VPN Updates

- In production since H1N1
- Performance limited
- Recently not ideal

- Global Protect VPN
- *Coming to an endpoint near year H2 2021!*
VPN Updates

- In production since H1N1
- Performance limited
- Recently not ideal
- Thanks for your patience – we’re doing our best

- Global Protect VPN
  - Coming to an endpoint near you H2 2021!
Subnet Reclamation

1. You have IP addresses

2. We need ‘em

NOC@colostate.edu
FIN
And now…

TELECOM NEWS
In brief…

- Nationwide 10-digit dialing is required after April 24th
  - Supported systems are already compliant
  - On-campus 5-digit calling will continue to be supported

- 988 now routes to the Suicide Prevention Hotline
  - Ahead of national deadline to implement of July ‘22

- Teams for Voice approved
Teams for Voice!

- Pilot completed in November 2020
- Approved to move into production starting FY22
- Three-year agile project plan
- Planning continues; development commencing
Teams for Voice - Timeline

• May – June 2021
  – Pilot cleanup
  – Rollout planning
  – Development

• July-August 2021
  – “Typical User” use case onboarding
  – Targeted initially, with sustainable scaling

• Fall 2021 – Second two-month development sprint
Teams for Voice – Parallel Threads

• **E-911 Location Data**
  – Today – static, based on HR office location
  – Future – dynamic
    • *Please work with your HR coordinators to confirm primary location data is accurate!*

• **Support Model & Documentation**
  – We need your help!

• **Financial Model**
  – Revamp of network funding model coming in FY23
  – We’re planning to hold billing static for FY22
Teams for Voice – Handsets

- **Recommendation:**
  - Avoid planning to use traditional handsets
  - Focus investment in headsets and cameras
  - We’ll post a link in Teams with device recommendations

- **Strategy still in development**

- **Telecom will need to facilitate handset procurement**
  - Legal requirement due to E-911 regulations
  - Process for this also in development
Teams for Voice – Handsets

• **Devices we have deployed that have worked well:**
  - Jabra - Evolve 75 MS | Teams devices (microsoft.com)
  - Poly - Voyager 4200 series - Swappable battery / Monaural on the ear / Convertible | Teams devices (microsoft.com)

• **Full list of Teams Headset options:**
  - Headsets, Earbuds, and Headphones | Teams devices (microsoft.com)
Teams for Voice – Next Steps

• Hang in there
  – We’ll have more to share as we get past SP21
• Sunsetting the “Teams Voice Pilot” team
• Please deploy QoS GPOs for Windows machines
• Stay excited!
Questions?

Thanks!
Security Updates – Steve Lovaas

PLEASE WELCOME...

HIGHLIGHTED VULNERABILITY: MS EXCHANGE

HIGHER ED TARGETED

REMINDER: EXPECTATIONS
“New” to the Security Office

Kelly Poto

– A new, 55% position for Cybersecurity Awareness & Training
– Has been with us since 2018 as the coordinator of the Cybersecurity Internship program
– Continuing work on her Master’s
Highlighted Vulnerability: MS Exchange

- Four zero-day vulnerabilities, active exploits since March
- Remote code execution, server hijacking, back doors, data theft
- 100,000+ affected systems worldwide
- Lots of attention in the media and from federal agencies
  - FBI even got a subpoena to reach in and disable malicious web shells
- We acted immediately and followed up with Microsoft… no negative effects on CSU
Higher Ed Targeted

- Starting last summer, we started getting notices from federal agencies that known attackers were beginning to turn their attention toward higher education
  - Lots of targets, large networks to capture, potential for profit
- Since then, many EDUs have seen significant compromises
  - Active Directory compromise, ransomware/extortion
  - We’re learning from our peers, trying to avoid their fates
  - This trend has public visibility and high-level attention: an opportunity
  - Look for more evaluations, conversations, and strategic explorations
Reminder: Expectations

We provide alerts from a variety of sources, letting you know about system/application vulnerabilities (suspected or confirmed), configuration errors, and sometimes actual compromises.

Nessus, UT DorkBot, REN-ISAC/MS-ISAC, DHS/CISA CyberHygiene, etc.

Here’s the expectation for response (based on NIST and other best-practice sources for vulnerability management practices):

- **Live exploit/compromise:** immediate response (with us)
- **Critical vulnerability:** address within 15 days
- **High-risk vulnerability:** address within 30 days
- **Medium/Low-risk vulnerability:** fix as resources are available, goal = 90 days
Security Questions?
That’s A Wrap!