Banner Architecture Renewal

Banner in the Cloud

June 2016

Tim Olesen/Bob Cutler
Project Director/Project Manager

UCDAVIS

Why

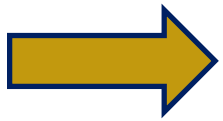
- Technology Currency
- Scalable Performance
- Dedicated Technology Experts
- Improve System Reliability, Availability
- Improve Security

What's moving

UC Davis

- Database Servers (Iris/Lobo)
- Forms Server
- Web Server

- SAOT Administration
  - Patching
  - Backups
  - Etc.



Hosted site

- Database Servers
- Job Server (new)
- Forms Server
- Web Server

- Ellucian Administration
  - Patching
  - Backups
  - Etc.

Who Will Be Impacted

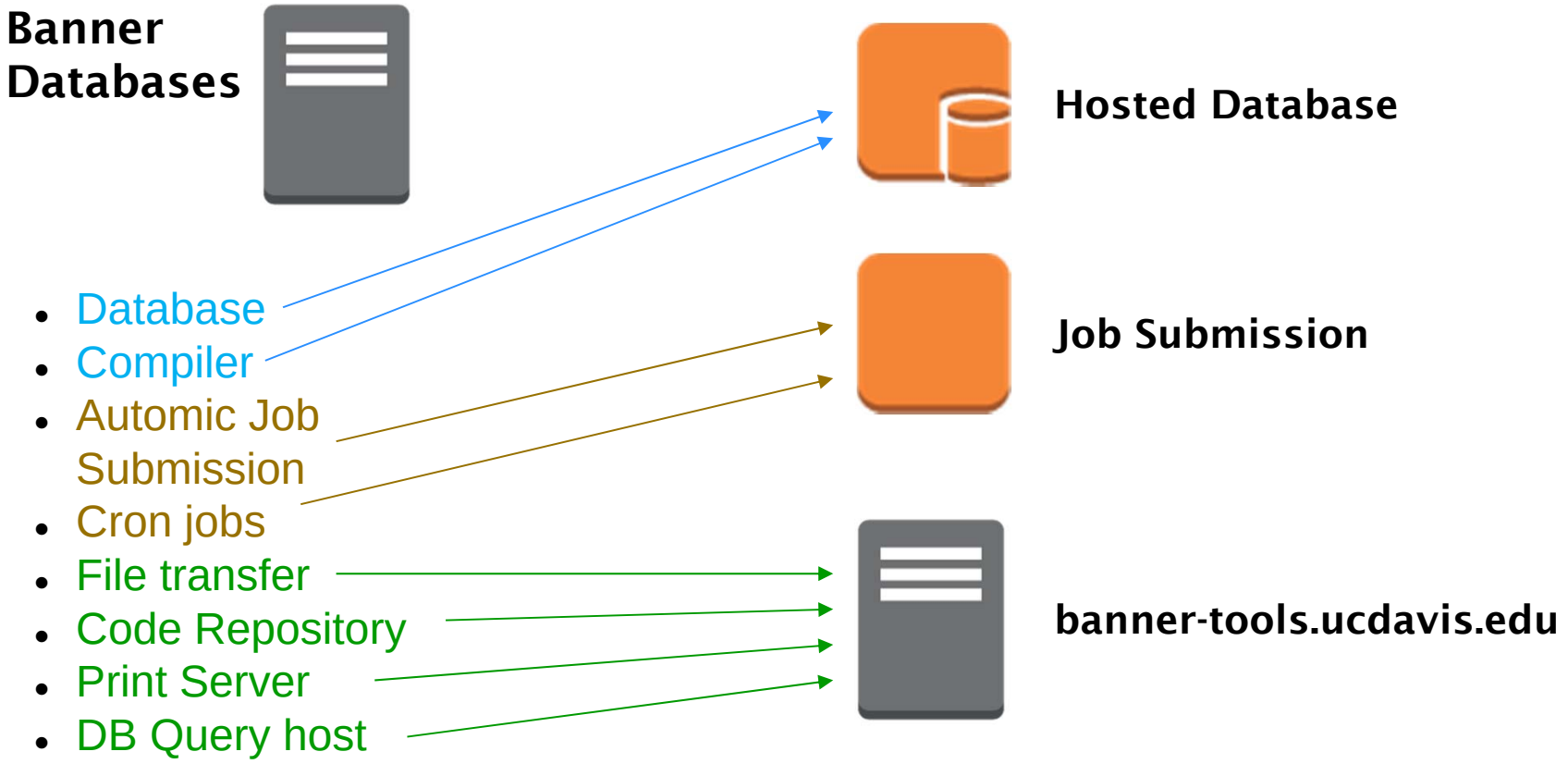
- All business processes will be supported with some minor usage changes
- Banner Users (operational staff)
  - System Access Changes
    - Single Sign-on (Duo)
    - Folder-based File Access
    - Job Scheduling
    - File transfers
    - Printing (hoping for reduction)
- External/Internal Application Interfaces
  - Service Name/Host/Port changes

What will not change?

- Banner Application Interface
- Banner Application Development
- Banner Database Content/Structure

Project Participants

- SAOT
- IET
  - PMO
  - Data Center
  - Network Operations Center
  - CISO Office
  - IT Express
- Ellucian



IP Range is 172.30.0.0/23

Printing

- Print server remaining at UC Davis
- Hostname is banner-tools.ucdavis.edu
  - 128.120.41.57
- Local firewalls with Banner printers will need to open port 9100 to this address
- An email will be sent to all VLAN owners who use Banner printers to have this port opened

Access Changes

- Currently the Banner database is open to all UCD IP addresses
- With the hosting migration we are going to implement an IP whitelist to limit database access to Banner
- We will divide this into to types of access
  - Server/Application access
  - Workstation/User access

Server/Application Access

- All servers that need to communicate to a Banner database will need to be registered with the Banner team
- This includes workstations that do specific automatic tasks (for example, AggieCard creation)

Workstation/User Access

- Access to the Banner databases will be limited to approved IP addresses
- All access to Banner databases will require Duo
- There are currently three methods to connect
  - Banner VPN (Campus Only)
  - Bastion Hosts
  - Banner-tools (Oracle tools only)
  -

Banner VPN

- Pulse VPN based
- Uses AD and Duo for authentication
- Split-tunneling
- 16 hour timeout
- Limited to campus IP space

Testing

- We are asking all application teams to test against the hosted database
  - By October 27
- The database is a copy of UCD Production
-
- Primarily focused on latency/performance issues.

Cutover

- Transition scheduled for Mid December
  - 3 day outage
  - Friday Evening→ Tuesday Morning
- LDAP service name will remain the same
- IP address will change
- Application validation

When?

- Host Environment Development (Completed)
- Banner Servers Test Environment (Completed)
- UCD Adaptations Expected (In Progress)
- Functional/Stress Testing (Fall)
- Go Live! (December)

Ellucian AHS

Client Responsibilities

Ellucian Responsibilities

- Management (Chief Information Officer / Director)
- Functional Experts
- Programmer Analysts / Report Writers
- Application Licenses
- Internet Connectivity

Application Hosting Services

AHS Management

- Engagement Manager
- Application Administration
- Database Administration
- Operation System Administration
- Systems Monitoring
- 24x7 Service
- Information Security
- Disaster Recovery
- Server & Network Administration
- Infrastructure Hardware
- Hosting Infrastructure and Licensing

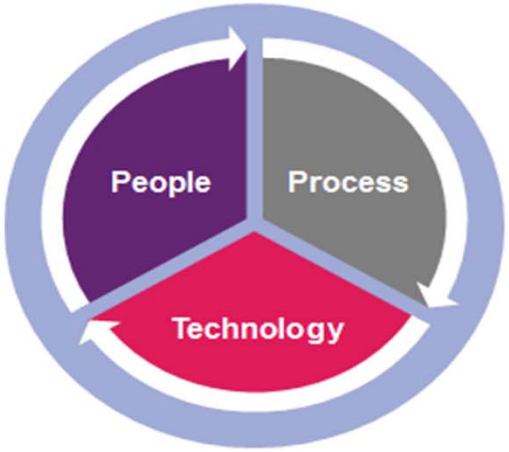
Ellucian Operations Center

24x7 team of engineers and analysts providing:

- Multilayer monitoring
  - SLA Reporting
  - Trending
- Notification Response
  - Ticket generation
  - Triage support
  - Alerting
  - Escalation

UCDAVIS
UNIVERSITY OF CALIFORNIA

Ellucian Data Security



People

- Training for handling protected data
- Policy training
- Dedicated Security Response Team
- Access Control
- Security training for ops teams

Process

- ISO-27001 based policies
- SANS Top 20 Critical Controls
- SSAE 16 Audit
- ITIL
- Security Incident Response

Technology

- Hardened facility, cameras, guards.
- Biometrics, Keycards, Physical keys
- Firewall (source/destination port and protocol)
- Automated Vulnerability Scanning
- Intrusion Detection
- Encryption & privileged VPN access
- Secured VPN for back-end communications to on-campus systems
- Encryption of data when transmitted in/out of the secure facility
- 2-Factor Authentication
- Automated Patch Mgmt.
- Tools to secure staff access

Questions?