SUNGARD®
HIGHER EDUCATION

Foothill De Anza College District Education Information System Initiative

Education Information System Systems Configuration Strategy

Prepared by:	Hank Classe
Version:	1.9
Last Revision Date:	November 12, 2008
Create Date:	September 8, 2008

Table of Contents

1. Executive Summary

The Education Information System Initiative is Foothill De Anza College District's multi-year initiative for technology transformation that seeks to modernize, streamline, and enhance administrative services throughout the District's two campuses. Through the *Education Information System* initiative, Foothill De Anza College District is implementing the SunGard® Higher Education's Unified Digital Campus ("UDC") solutions, including the SunGard Banner® administrative system and other integrated component systems including the Luminis Platform, Banner Operational Data Store and Enterprise Data Warehouse, Integration Technologies, Banner Document Management Suite, E~Print, Appworx Enterprise Scheduler, and DegreeWorks.

This Systems Configuration Strategy report identifies the servers, network, and storage systems acquired by the customer to support the UDC solutions. SGHE analyzed the Hewett Packard Servers with the HP-UX and Linux operating system as an already procured platform that is in the process of being configured for the UDC solutions. A disaster recover (DR) architecture is desired, along with database and Application Tier High Availability (HA) where possible. A shared DR / Test platform is desired that will in the future be hosted off of the main campus at a secondary DR / Test site. Oracle Real Application Clusters (RAC) is not a consideration. Dual SANs and tape libraries were acquired as part of EIS for backup and recovery operations. Demographics include a Full Time Enrollment (FTE) of up to 30,000 students, 1,600 employees, 600 concurrent logged in employees, 12,000 concurrent logged in students, and 2 campuses supported in a centralized database.

1.1. *Assumptions*

- 30,000 students; 1,600 employees; 600 active concurrent logged in faculty/staff accounts, 12,000 concurrently logged in students; and 2 campuses
- HP-UX is the selected database platform. Redhat Linux is the selected application tier platform with exception of the Banner Document Management Suite, which will be Windows Server.
- Combined High Availability and Disaster Recovery architecture desired.
- Oracle RAC is not being considered.
- All new server hardware has been acquired.
- New storage has been acquired.
- Separate test/development/QA and production environments
- Disaster Recovery and test/development/QA to be combined

1.2. Recommendations for Systems Deployment

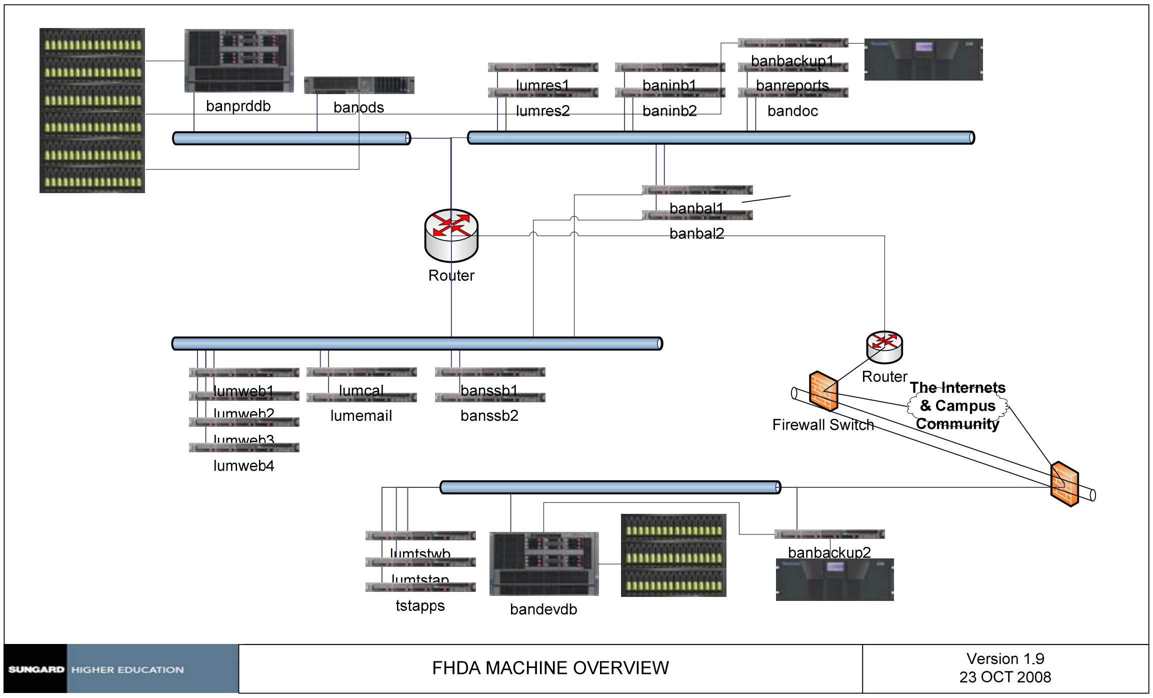
The District has already invested in a hardware solution in support of Sungard Higher Education's UDC Solutions (the UDC). In many cases, the recommendations listed below were planned by the College and are along similar or identical approaches and best practices that SGHE would consider essential to a successful implementation. The text 'SGHE recommends' exemplifies where we recommend a modified approach versus the College's original plan.

- Use Vertical Scaling for Database servers (more CPUs).
- Use Horizontal Scaling for application servers (more machines).
- Use Network Load Balancers for high-availability for application servers.
- Disaster Recovery servers to be hosted at a location greater than 75 miles from the campuses and outside of the three fault lines that transverse the city of Los Altos Hills; the Berrocal, Altamont, and Monte Vista fault lines.
- Secondary Disaster Recovery / Test Site to host servers that will both serve test / non-production applications as well as disaster recovery.
- Implement identical hardware for production and recovery/test database servers and application tier servers at both sites.
- Implement a lesser number of application tier servers at the secondary DR / Testing site with the understanding that the raw performance and number of concurrently supported users will be less versus the production site in the event of a fail-over.
- Initially implement at the primary site on the production machine for Oracle Database.
- Implement site-to-site VPN and all required infrastructure at the secondary DR / Test site, such as DNS and LDAP, so as to support fully functional DR.
- Implement a new network core of Cisco enterprise class switches in support of EIS in a fully resilient and redundant configuration with active/active on uplinks on fully meshed inter-switch links.
- SGHE recommends implementation of the actual test application tier machines (not DR / Test database server or SAN) at the primary site during early pre-production deployment with a slightly modified layer-3 network topology that could easily be modified without major address modifications once these machines can be moved to the secondary DR / Test site.
- SGHE recommends use of Oracle Dataguard for transaction oriented database recovery at the DR site. Use of Grid Control and Dataguard Broker for increased manageability of the Dataguard instance on a small Intel server is recommended. Additional license fees from Oracle may apply dependent on FHDA's licensing of Oracle product.
- SGHE would recommend dedicated hardware for the batch and AppWorx rather than shared with INB. The sharing of these resources should only be done in a situation where hardware resources were restricted. Limiting the ability of the batch sub system to run jobs in real time would need to be tested thoroughly and is generally not recommended. Select out specific tasks to throttle would be a better approach than throttle the entire system. Online processes (such as financial aid needs analysis and letter generation

variable compilation) need to be executed immediately as requested or the users INB session will hang and eventually timeout. Approaches to resolution include acquisition of a dedicated INTEL based server running a supported OS, such as Redhat Linux AS 4.x, or running on a hard partition on the HP6600. The District should consider the total cost of all required hardware and software resources, inclusive of compiler costs, and select the solution with the best total cost of ownership. SGHE is agnostic as to what OS and machine platform the Appworx / Batch server is run on so long as a supported OS/compiler combination are chosen.

- SGHE recommends the College exploit SAN replication technology as planned with exception of the Oracle Database SAN volumes to provide for protection of critical logical disk volumes between the primary and secondary sites as needed.
- SGHE recommends the College exploit its already acquired Backbon Netvault and dual tape library configuration for e-Vaulting of off-site media between sites.
- SGHE recommends implementation of some virtualization on INTEL/Linux in a non-production and DR fail-over capability for select UDC application tier components at the secondary DR / Test site so as to decrease TCO and increase the value of the college’s investment in hardware.
- SGHE recommends the College acquire firewall switching and network security technology prior to implementation of the production UDC so as to insure adequate protective measures are employed at both sites.
- SGHE recommends the College to acquire network packet shaping technology.
- SGHE recommends Foothill De Anza College District engage in rigorous business continuity planning and system-by-system disaster recovery documentation as part of its overall systems strategy. This should be coupled with regular testing of the system DR recovery plans by validating fail-over scenarios to the secondary DR / Test site.
- SGHE recommends Foothill De Anza College District purchase at least one additional DL 360 server for the secondary DR / Test site for use . This may be needed to provide enough hardware resources for the District to support Banner Test and DR as three machines may not provide enough resources to fully support both a Test and DR Recovery environment.

2. Detailed Analysis & Recommendations



2.1. Servers and Storage

Summary

- Servers Selected for Database and ODS are well chosen, with exceptional resources, scalability, and support for hardware based virtualization
- Servers selected for the Banner and Luminis application tier are well suited for both the test and pre-production environment.
- Addition of a server for Appworx/Batch or for hard partitioning on the RX-6600 of a virtual machine is recommended.
- Addition of HBA adapters, shared SAN volumes, and Linux clustering software is recommended for Luminis Resource servers.
- Addition of clustering plus 2 servers for the Luminis calendaring is recommended prior to the District moving into production.
- Addition of at least one or two servers at the secondary DR / Test site so as to provide sufficient servers for a fully functional DR / Test environment.

Production Database Server

The database server selected by the College is a Hewett Packard Integrity RISC server model RX-6600, configured with 4 processor boards in an 8 core 1.6Ghz/24MB cache configuration with 64 gigabytes of physical memory. The selected operating system will be HP-UX version 11i. This server machine type will be hosted at both the primary and secondary DR / Test sites and is an exceptional choice to host the Banner/Luminis UDC database components in a production capacity. Typical Oracle databases sized for large institutions like the College typically requires 16 gigabytes physical RAM. In the case of Foothill De Anza College District, the tuning of Oracle SGA may be set to very generous values at the main site whilst still allowing plenty of RAM for growth.

DR / Test Database Server

This machine is identically the same as the production database server. Sufficient RAM and CPU processing is present for non production test, quality assurance, and training instances in addition for an Oracle Dataguard instance. Risks are relatively low provided that strong change control measures are applied to the environment that appropriately document and mitigate risk associated with changes to the Oracle Dataguard instance and/or the oratab file on the machine.

ODS Database Server

The ODS server selected by Foothill De Anza College District is an excellent machine resource for report warehousing. ODS is a ‘replicate once always incremental’ system that will efficiently replicate changes in the Banner production database system to the ODS server in ODS format. A full resync would be a rare event typically associated with maintenance upgrades, patches, etc. Configured with 32 gigabytes of RAM, a pair of dual-core processors, sufficient SAN resources, and HP-UX, this machine will keep up with a demanding report load from many concurrent users in a large school environment.

Application Tier Server Machine Architecture

All application tier machines are the Prolient DL360 G5 server, with 2 each X5450 3.0GHz dual-core CPUs and 24 gigabytes RAM, dual NICs, and two 140 gigabyte locally attached disks.

Primary Site INB and SSB Servers

The HP Prolient DL360 G5 server was selected by Foothill De Anza College District as a horizontally scaled server solution at the application tier to support thin WEB clients that connect to the UDC. Configured with 24 gigabytes RAM each, these machines should prove adequate for supporting concurrency requirements for the College. There are no concerns regarding INB connection concurrency given the estimated total active connection estimate of 600. Some concern exists regarding the two SSB machines versus the number of potential clients that may connect to SSB. The Luminis SSB portal builds a frame set around SSB. Traffic from the client to the SSB server is direct from the thin WEB client to the SSB server. Addition of more servers for SSB may be necessary as the UDC matures and usage increases.

FHDA may consider collapsing Batch and Appworx onto one of the primary site's INB machines as an effective measure to save resources on Cobol compiler licensing. Performance should be carefully monitored. It may be necessary to add a dedicated server for batch and Appworx dependent on FHDA's use of the product. This is a critical consideration when considering the collapsing of this UDC component onto the INB servers.

Luminis Portal WEB Servers

The Luminis WEB portal servers are capable of supporting approximately 600-800 concurrent sessions per WEB portal machine, dependent on how Luminis is implemented at the District. Clearly with more complex the portal configuration, the more channels and news feeds, etc, increased RAM and CPU resources per session shall be consumed. SGHE recommends that the District remain at the planned 4 WEB portal machines as originally planned for the deployment.

Luminis Resource Servers

SGHE sees no potential issues with the two machines reserved for Luminis Resource.

Luminis Calendaring and Email Servers

The College has two machines reserved for Luminis Calendaring and email. It is plausible that the College *may* need to increase resources to these UDC components in the future dependent on how it deploys the final product configuration.

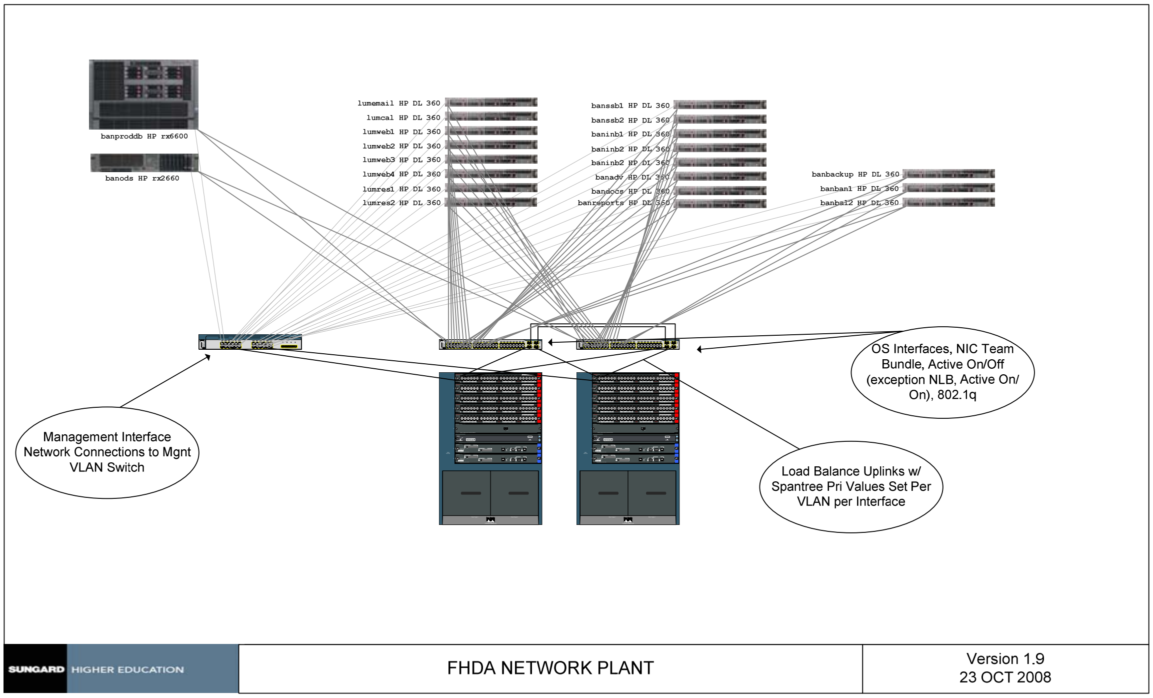
Banner Reporting Server

The reporting server that will host Hyperion is well sized. According to Oracle, the machine sizing requirements for Hyperion are relatively small in comparison to the generous resources available to the application within the HP DL360 server reserved for this application.

Storage

SGHE considers the SANs acquired as more than acceptable for the soon to be implemented UDC. The SANs are a pair of DS4700 enterprise class storage systems with a fiber channel network. The fiber channel network operates at 4 gigabyte per second with active/active on controller connections from the SAN into the switch fabric at 2 gigabyte per second. There will be 60 disks available to the production Oracle database server with DASD capable of delivering 250 to 275 IOPS per device. It is estimated that the IOPS capacity of the system will range between 15,000 and 20,000 IOPS. This is in addition to trays of SATA disks that will provide IOPS for other applications such as ODS and the network backup application at an IOPS capacity of greater than 7,500. The SAN acquired for the secondary DR / Test site also is sufficiently for both DR and non-production applications.

2.2. Network Considerations



Network Summary

- Layer-2 and Layer-3 EIS network core an ideal fit for the UDC.
- Planned fully meshed configuration considered a best practice approach to providing fault tolerant and resiliant transport network services
- Application of Zeus network load balancing a good choice, but recommend that the use of VLAN tagging be employed so as to load balance application tiers in both DMZs.
- Acquisition of firewall switching and implementation of a secured, stateful packet inspection layer between multiple network DMZs is recommended.
- Acquisition of packet shaping technology is recommended.

Network Transport Layer

SGHE views the recent network hardware acquisitions by the College for the EIS new intranetwork core to be best of breed and more than capable of supporting the UDC.

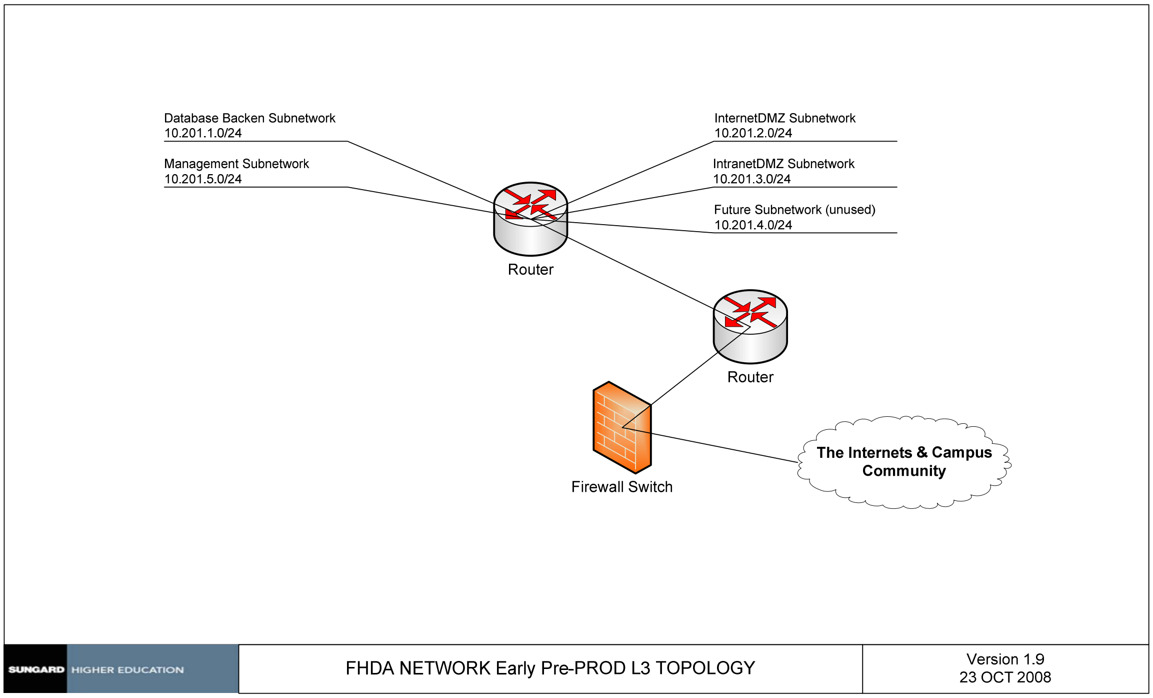
The College has acquired a pair of Cisco 6509 enterprise class switches to serve the new EIS intranetwork core in addition to a pair of Cisco 3750-G switches for connection of all servers at the primary site. A single Cisco 2950 switch has also been acquired as part of the server hardware acquisition for attachment of out-of-band server, SAN, and tape library console management.

The client has already planned on implementing a fully meshed network configuration for EIS. User workstations at the access layer will connect to the new intranetwork core with existing Acatel switch blocks from Acatel network core. Eventually, plans are in place to replacing fleet the switches at the access layer with newer switch technology. These switches will be attached to the new intranet core.

Network Layer-3 Topology Early Deployment Without Secondary DR / Testing Site

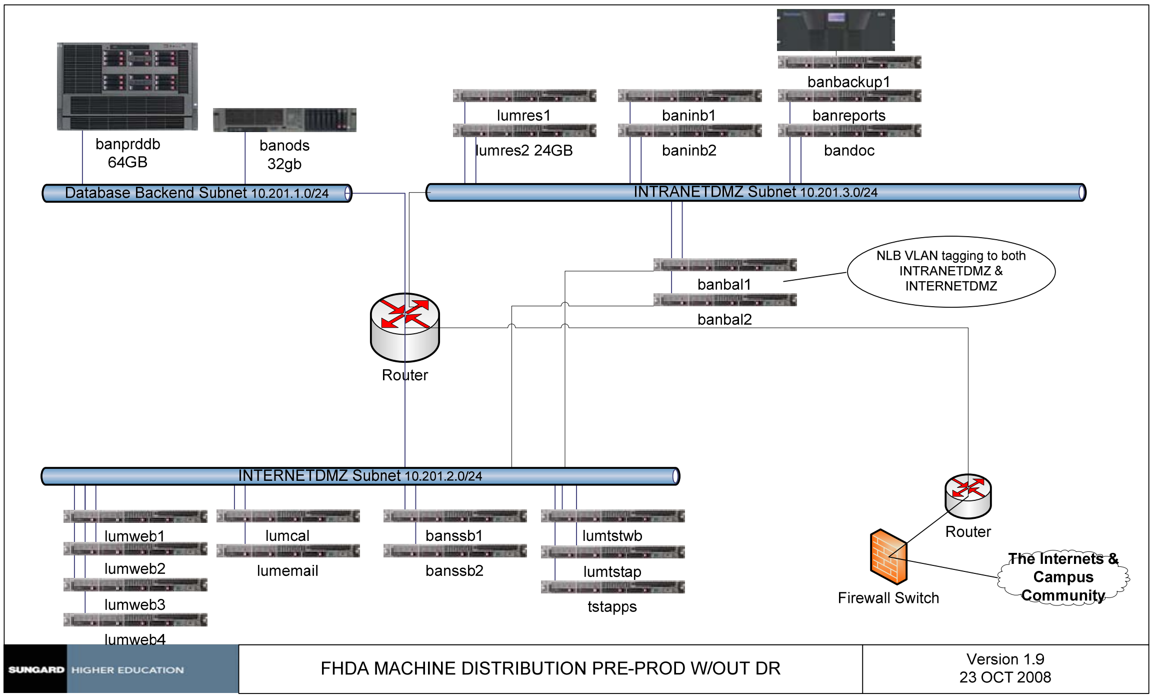
The College currently does not have a firewall switching system as part of their existing network communications infrastructure. Meetings with the Network Operations staff indicate this shortcoming in the network infrastructure should be corrected with a future acquisition. In preparation for a more secure EIS system, SGHE recommends deployment of a layer-3 network topology that would allow for deployment of the servers in a manner that places the machines in a topology that could be easily modified by College network staff persons once a firewall switch system has been obtained and installed into the intranetwork core.

The recommended network layer-3 architecture that could be deployed would be inclusive of a database subnetwork, both internet and intranet DMZ subnetworks, a management subnetwork, and a reserved subnetwork for future UDC application components.



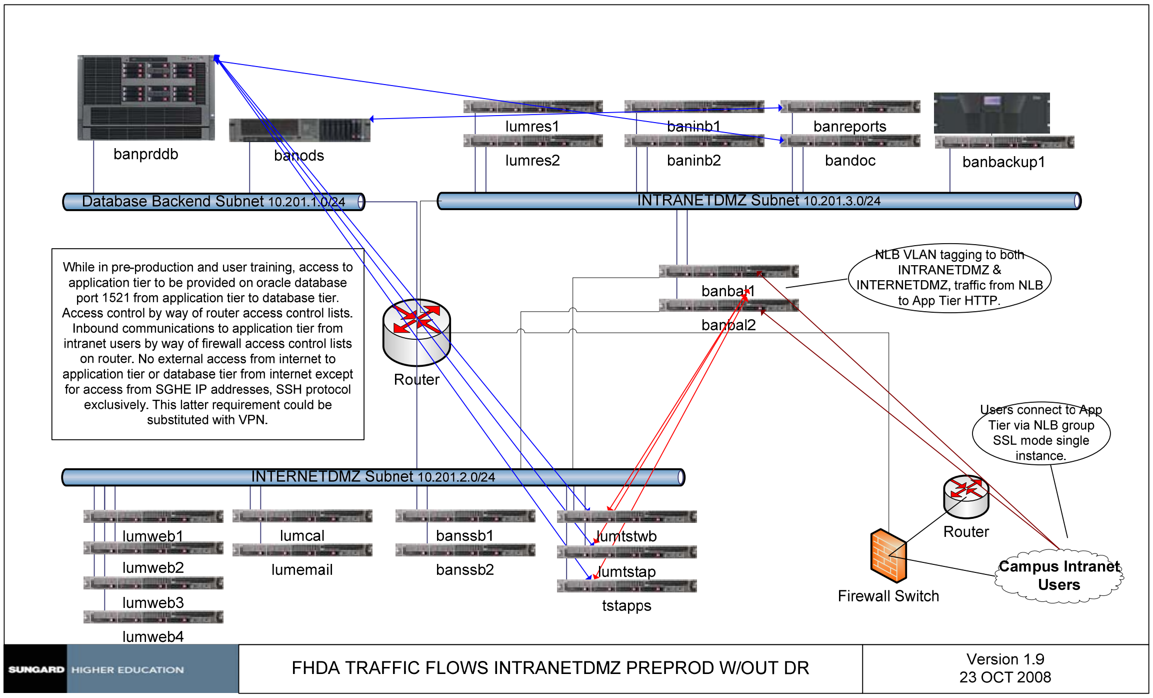
Early Deployment Machine Distribution

Early deployment of machines would involve installing of all machines for the primary site with *DR / Test* machines being held in storage by the College's hardware integrator. SGHE recommends that the College deploy the application tier test machines reserved for Luminis and Banner INB/SSB at the primary site but that these test machines be addressed in the upper range of the subnetwork 10.201.2.0/24. This would permit the subsequent splitting of this subnet into two /25 subnetworks and would thus allow the test machines to later be re-deployed to the secondary DR / Test site without re-addressing the machines other than the network mask and default route. The above would avoid potential support issues with SGHE and Oracle downstream in the project.



Early Deployment Traffic Flows and Load Balancing

SGHE suggests the Zeus network load balancers be configured with a virtual IP address (VIP) and SSL acceleration early on during the project. Traffic flows from the database servers to application tier (blue lines) as well as any inter-application tier communications would be HTTP peer-to-peer and would not pass through the NLB. Traffic flows from thin WEB clients to the application tier for training and testing would be through the NLB VIP and would be translated to SSL so as to enable the College to build and validate a configuration for later implementation in a production capacity. VLAN tagging should be implemented with the Zeus having virtual interfaces within the DMZ subnetworks. It is strongly suggested that the Zeus NLBs management interface be associated with the network management subnetwork (not shown). Also notable is the need to setup DNS addressing for all machine native IP addresses *as well as* NLB VIPs early on in the project.


banprddb
banods
lumres1
lumres2
baninb1
baninb2
banreports
bandoc
banbackup1
Database Backend Subnet 10.201.1.0/24
INTRANETDMZ Subnet 10.201.3.0/24
banbal1
banbal2
NLB VLAN tagging to both INTRANETDMZ & INTERNETDMZ, traffic from NLB to App Tier HTTP.
Router
Users connect to App Tier via NLB group SSL mode single instance.
INTERNETDMZ Subnet 10.201.2.0/24
lumweb1
lumweb2
lumweb3
lumweb4
lumcal
lumemail
banssb1
banssb2
lumtstwb
lumtstap
tstapps
Router
Firewall Switch
Campus Intranet Users
SUNGARD HIGHER EDUCATION

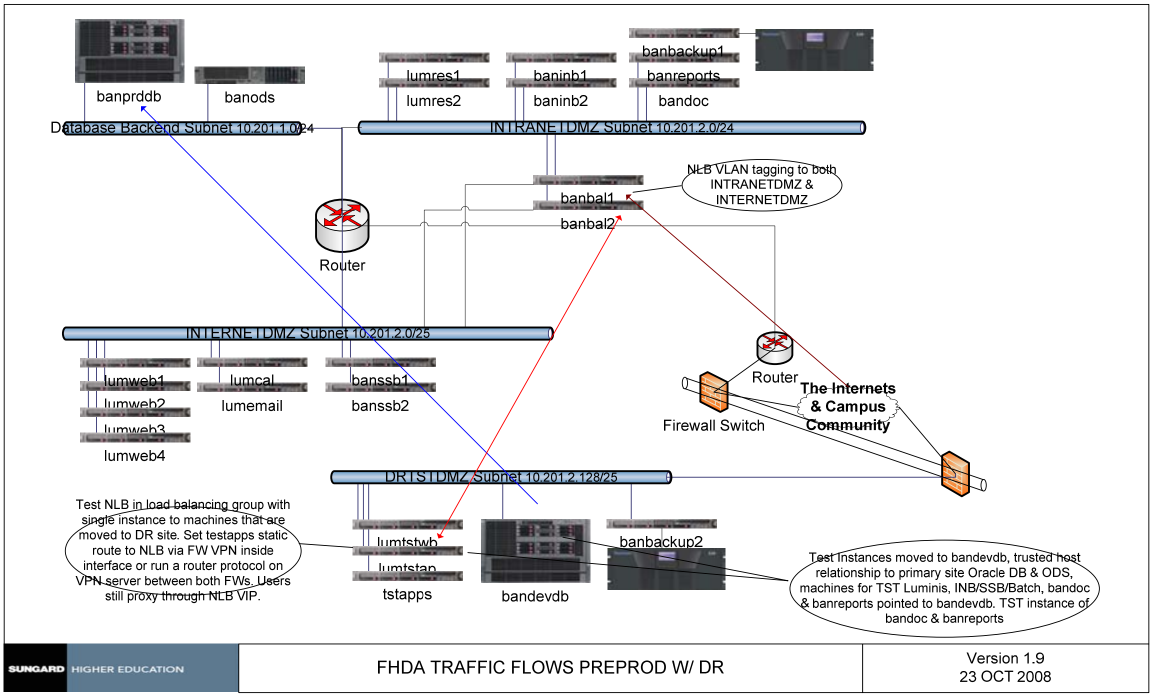
While in pre-production and user training, access to application tier to be provided on oracle database port 1521 from application tier to database tier. Access control by way of router access control lists. Inbound communications to application tier from intranet users by way of firewall access control lists on router. No external access from internet to application tier or database tier from internet except for access from SGHE IP addresses, SSH protocol exclusively. This latter requirement could be substituted with VPN.

FHDA TRAFFIC FLOWS INTRANETDMZ PREPROD W/OUT DR

Version 1.9
23 OCT 2008

Redeployment of Test to Secondary DR / Test Site

The test machines can be redeployed to the secondary DR / Test site once it is available. SGHE recommends that the subnetwork 10.201.2.0/24 be split into two distinct subnetworks of 10.201.2.0/25 and 10.201.2.128/25 respectively, with the test machines being redeployed without readdressing. The College Network Operations staff have indicated a preference for site-to-site VPN tunneling with routing between the primary and secondary sites. SGHE supports this position as a best practice taking into consideration the College's intranetwork and wide area network architectures. Some routing changes would have to be applied on the NLB and possibly the application tier testing machines to insure correct routing of traffic between the machines' native IP address and the NLBs' private IP address within 10.201.2.128/25. Test database instances are moved from the banprddb machine to bandevdb as part of this transition.



NLB VLAN tagging to both INTRANETDMZ & INTERNETDMZ

Test NLB in load balancing group with single instance to machines that are moved to DR site. Set testapps static route to NLB via FW VPN inside interface or run a router protocol on VPN server between both FWs. Users still proxy through NLB VIP.

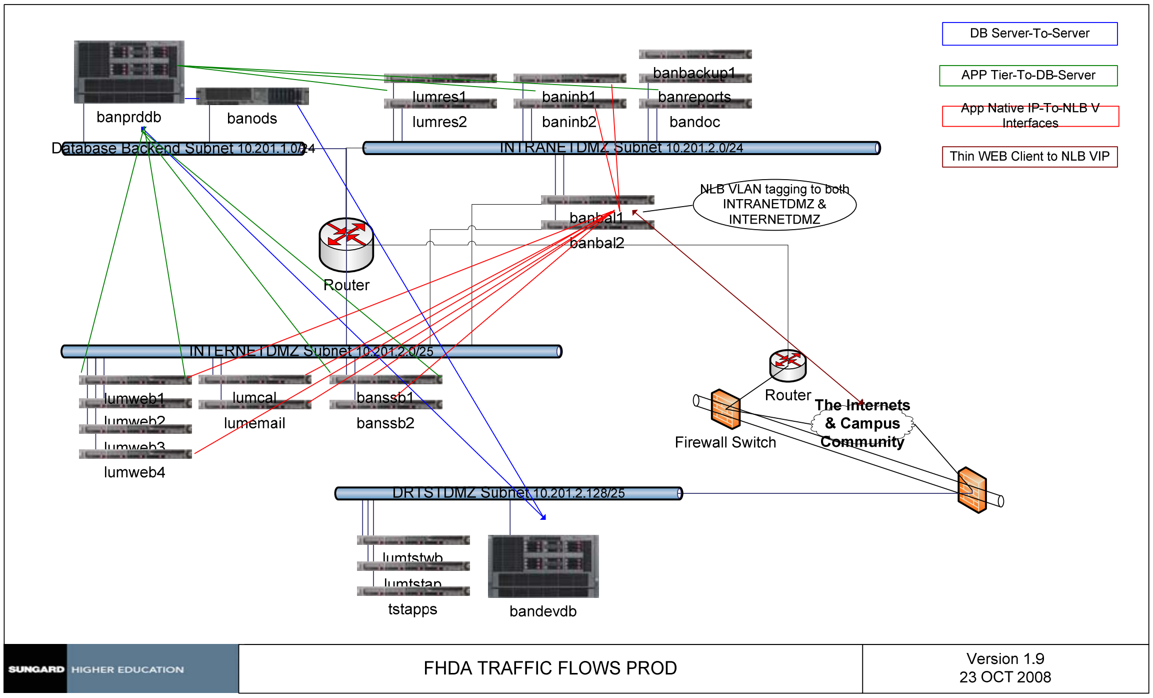
Test Instances moved to bandevdb, trusted host relationship to primary site Oracle DB & ODS, machines for TST Luminis, INB/SSB/Batch, bandoc & banreports pointed to bandevdb. TST instance of bandoc & banreports

FHDA TRAFFIC FLOWS PREPROD W/ DR

Version 1.9
23 OCT 2008

Traffic Flows in a Production Capacity

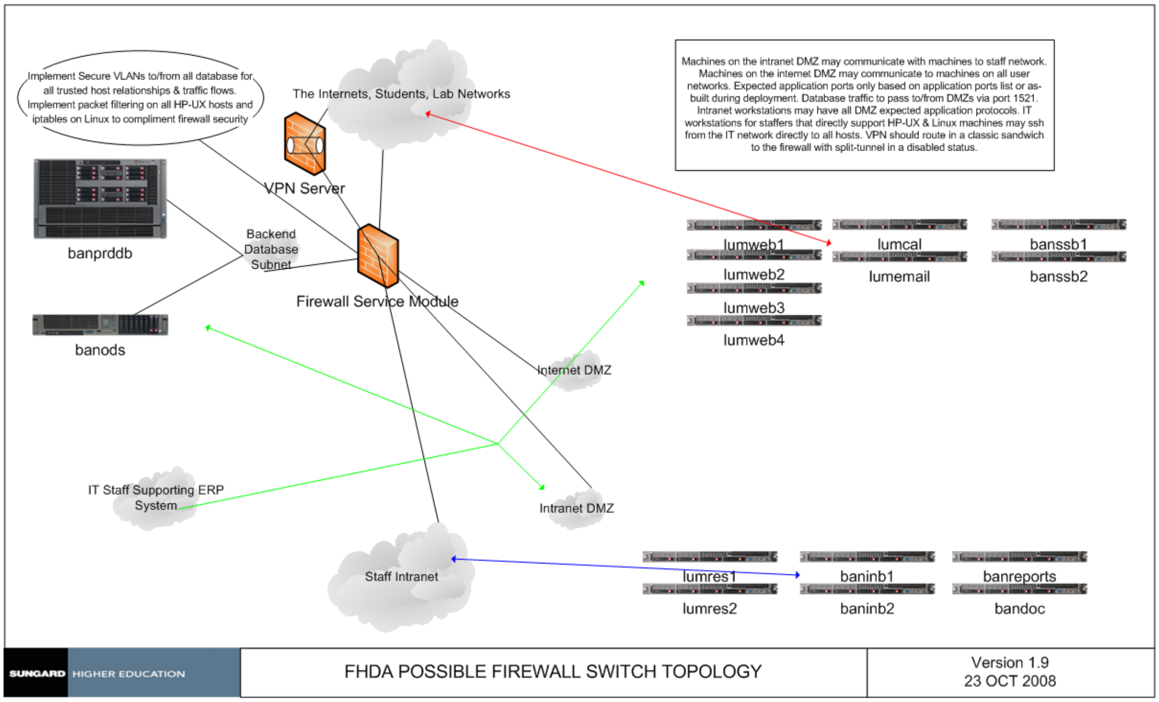
Traffic flows between the database server and application tier machines would be similar as in pre-production (green lines), with flows in HTTP from the application tier machines to the NLB, and flows from thin WEB clients to the application tier by way of the NLB VIP with a TCP datagram rewrite to SSL. The Oracle Dataguard instance would be installed at the secondary DR / Testing site and would share resources on the native HP-UX OS with TST/TRN/PPRD database instances.



Firewall Switching and Network Security Recommendations

Effective firewalling between the application layers and database servers is a first minimalist step in the direction towards a multi-layered approach for maintaining a high security stance relative to protecting Institutional information technology assets. Far better are multiple firewalled subnetworks between areas of defined and distinct security policies, with the subnetwork of the highest security stance being the location of Oracle Database servers, the crown jewel information resources for any institution. Consider that these machines will host personal identifiable information, inclusive of SSN, DOB, and other sensitive data. Institutions are obligated to make a best and reasonable effort to "controlling the use, dissemination, and protection of such data". This obligation stems primarily from both federal law and the courts, the most notable example being FERPA (US Code T20C31S 3,P4,1232g, Sections B & C). Other law and regulatory requirements that may apply dependent on access and use of data are inclusive of HIPPA, PCI, FFIEC, and FISMA. Similar laws for the European Union apply as well, most notably the Personal Data Protection Act.

SGHE highly recommends that the District obtain a firewall switch, such as the Cisco Firewall Service Module, in a stateful fail-over configuration between the Cisco 6509 chassis'. Ideally secure VLANs should be mapped to all server and user networks that are not sensitive to packet delay (such as Voice IP). Implementation of an appropriate network intruder prevention system is also recommended.



Implement Secure VLANs to/from all database for all trusted host relationships & traffic flows. Implement packet filtering on all HP-UX hosts and iptables on Linux to compliment firewall security

Machines on the intranet DMZ may communicate with machines to staff network. Machines on the internet DMZ may communicate to machines on all user networks. Expected application ports only based on application ports list or as-built during deployment. Database traffic to pass to/from DMZs via port 1521. Intranet workstations may have all DMZ expected application protocols. IT workstations for staffers that directly support HP-UX & Linux machines may ssh from the IT network directly to all hosts. VPN should route in a classic sandwich to the firewall with split-tunnel in a disabled status.

Application network ports vary from site-to-site and are customer specific. In-bound application service to UDC components are to administered TCP sockets. Outbound traffic flows from servers to clients are classically sequential but are not server initiated. All client initiated connections are ideally routed through the network load balancer with a TCP datagram rewrite from SSL to HTTP as previously discussed. Firewalling to clients should be implemented at the NLB virtual interface, with the NLB virtual interface facing the inside virtual firewall interface. Server-to-server peer-to-peer communications should also flow through the firewall interfaces. Ideally, firewalling may also be implemented on Linux and Windows hosts, plus TCP filtering on the HP-UX machines. Any non-essential services on servers should be disabled, especially those services which are considered insecure, such as telnet and ftp. The management interfaces for the HP servers require the use of telnet. As such, access to these interfaces should be tightly controlled, with communications flows to trusted networks through a securely managed bastion host if possible.

For host based security, turn off ftp and telnet on the HP UX machines as these are not required and are not secure. Turn off other unsecure services that are not required. Oracle database will bind to port 1521. iptables should be left enabled on INB/SSB Linux machines but should be configured to permit inbound traffic to TCP ports that will be defined during installation. Until then, it is suggest leaving the range of 7000-9999 open. This can be further hardened later on post install.

Disable all access to ports used by vncserver. vnc traffic should be tunneled securely within ssh (port 22). All vnc traffic to the port range of 5700-6200 should be blocked. ssh must be permitted to all machines from expected locations, ideally not from user networks.

Lock down telnet remote access to the servers' telnet management interface. Use a bastion host for remote access to these interfaces, such as the Windows management station. Do not allow direct telnet access from any user station to the machines except within IT, and then only telnet to the management interface should this be required to IT staff only from secured IT network locations.

Application port assignments are listed on the next page. The reader should note these represent *potential* administered ports that may differ during an actual implementation.

TCP Application Network Port Assignments

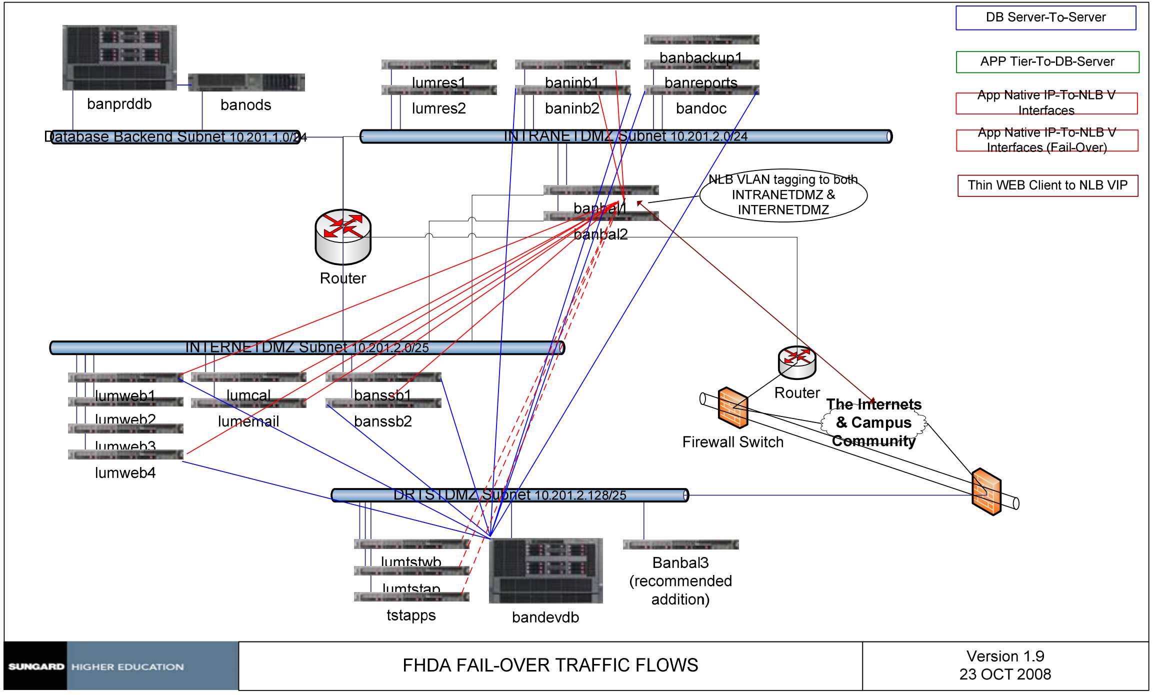
Internet DMZ Publicly Accessible Application Ports			
Product	**Default Administered Port**	**Server**	**FWSM ACL Example**
Self Service Banner	443	selfservice	acl outside p t a h selfservice eq https
Web Server	80	Resource Tier	acl outside p t a h lumresource eq http
Web Server	443	Resource Tier	acl outside p t a h lumresource eq https
Chat	9256	Resource Tier	acl outside p t a h lumresource eq 9256
GCF	8008	Resource Tier	acl outside p t a h lumresource eq 8008
Calendar	6785	Calendar Server	acl outside p t a h lumresource eq h6785
ComExp	6788	Messaging Server	acl outside p t a h lumcal eq 6788
ComExp	6777	Messaging Server	acl outside p t a h lumMesg eq 6777
Intranet DMZ Accessible Application Ports			
Product	**Default Administered Port**	**Server**	**FWSM ACL Example**
Self Service Banner	443	selfservice	acl intranet p t a h selfservice eq https
Workflow	9099	workflow	acl intranet p t a h workflow eq 9099
Ports to be Opened to IT Administator Network			
Product	**Default Administered Port**	**Server or Subnetwork**	**FWSM ACL Example**
OAS EM	7777	Internet DMZ	acl Itintranet p t <IT subnet & mask> 10.51.2.0 255.255.255.0 eq 7777
Luminis Communications Express	6788	LumResource	acl Itintranet p t <IT subnet & mask> h LumResource eq 6788
Luminis Sun Console & WebAdmin	9999	LumResource	acl Itintranet p t <IT subnet & mask> h LumResource ra 9998 9999
Messenger Admin	9999	LumMesg	acl Itintranet p t <IT subnet & mask> h LumCal eq 9999
Oracle Server Network	All TCP	10.51.0.0/24	acl Itintranet p t <IT subnet & mask) 10.51.0.0 255.255.255.0
Intranet Server Network	All TCP	10.51.1.0/24	acl Itintranet p t <IT subnet & mask> 10.51.1.0 255.255.255.0
Trusted Host - to - Host Relationships			
Host	**Source Machine Port**	**Destination Port**	**FWSM ACL Example**
databasesvr	selfservice sequential	1521	acl databasenet p t h selfservice h databasesvr eq 1521
databasesvr	INB sequential	1521	acl databasenet p t h INB h databasesvr eq 1521
databasesvr	workflow sequential	1521	acl databasenet p t h workflow h databasesvr eq 1521
databasesvr	LumResource sequencial	1521	acl databasenet p t h tstLumResource h databasesvr eq 1521
databasesvr	Database server sequential	389	acl databasenet p t h databasesvr h tstLumResource eq 389
Workflow to INB	workflow sequencial	9099	acl intranetdmz p t h workflow h INB eq 9099
Test INB/SSB	7778-7780	7778 - 7790	acl intranet p t a h testapps ra 7778 7780
Test INB/SSB	9030 9405	9030 - 9405	acl intranet p t a h testapps ra 9030 9405
Test Luminis Chat	9256	tstLumResource	acl intranet p t a h tstLumResource eq 9256
Test Luminis CPIP	8008	tstLumResource	acl intranet p t a h tstLumResource eq 8008
Test Luminis Messenger Express	6777	tstLumResource	acl intranet p t a h tstLumResource eq 6777
Test Luminis Chat	9256	tstLumResource	acl intranet p t a h tstLumResource eq 9256
LDAP to Lum Resource Tier	389	EAS	acl intranet p t h ActiveDirectory h tstLumResource eq 389
Luminis Resource Server to INB	443	INB SERVER	acl intranet p t h tstLumResource h databasesvr eq 1521
Luminis SSO to SSB Resource	HPPT or HTTPS, HTTP in NLB for server peer-to-peer	http	non-applicable ACL if both servers in same VLAN
Resource to SMTP Server	LumResource sequencial	SMTP	acl intranet p t h tstLumResource h mailsrvr eq smtp
Cal to Lum Resource	Lum Resource sequential	389	non-applicable ACL if both servers in same VLAN
Msg Srvr to Lum Resource	Msg Srvr sequential	389	non-applicable ACL if both servers in same VLAN
Internal	All resource teir internal, sequential	9998-9999	non-applicable ACL if both servers in same VLAN

Although many port requirements in this document are static, others represent "standard but configurable" ports (e.g. Chat, DB listeners, etc.). Please review port values carefully before implementing firewall and load balancer settings to ensure they match your environment.

2.3. Fail-Over Scenario and DR Planning

Ideally, fail-over scenarios are well thought out, are incorporated into systems disaster recovery documented plans that are also integrated into an institutional business continuity plan. The College currently does not have a business continuity plan. As such, some assumptions must be made with respect to DR recovery levels for various UDC components. See APPENDIX A for a descriptive text of the Disaster Recovery Tiers.

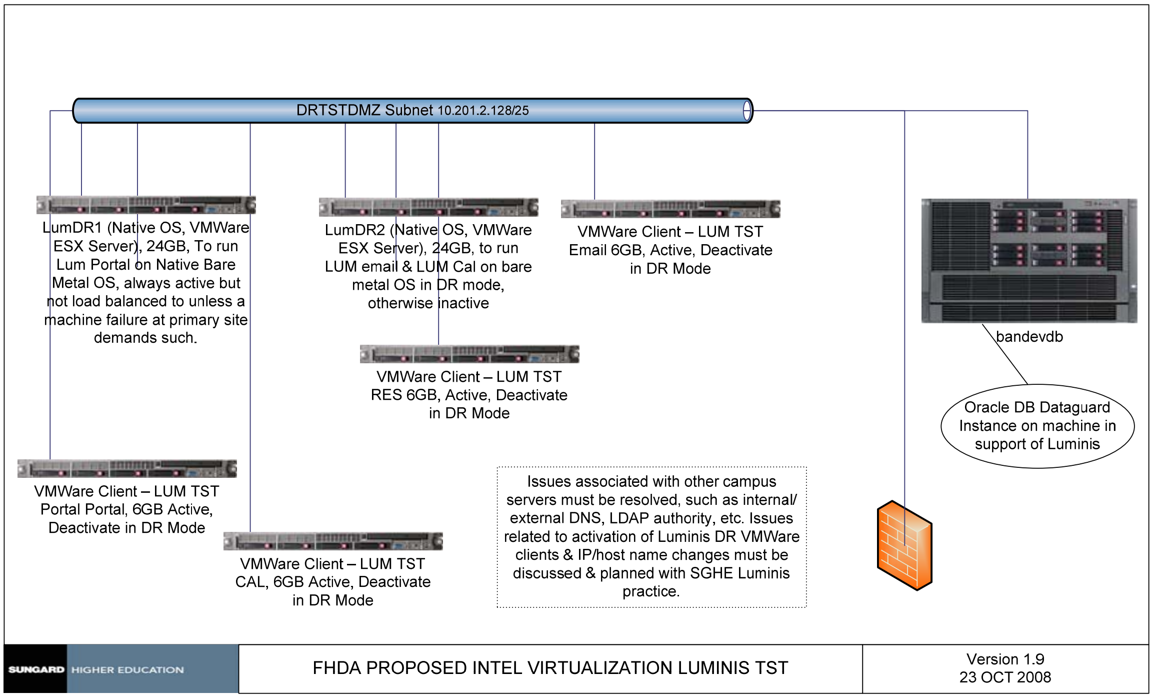
- The database server at the primary site should be configured at DR Tier 5 using Oracle Dataguard. It may fail over automatically or as a declared fail-over as determined by the College.
- The application tier for INB, SSB, and Luminis WEB Portal will be scaled horizontally, operating at DR Tier 7, with multiple instances of the Luminis Web application at the Portal Tier. The Zeus NLB will be an essential component in this solution. OS clustering must be used for high availability of the email, calendaring, and resource servers (see below).
- Luminis resource, calendaring, and email do not implement replication and fail-over technology within the product. Fail-over for Luminis Resource, Luminis CAL, and Luminis email must be clustered at the operating system level. SGHE recommends that FHDA consult with HP and its value added reseller for best approaches to clustering these three platforms. Although servers exists for clustering servers at the Luminis Resource Tier, no such hardware exists for Calendaring and email in the existing equipment plant and would have to be acquired for this functionality.
- Major components such as public/private DNS, LDAP, and NLB will have to be duplicated at the secondary DR / Test site. Educause’s DNS database will have to be updated to reflect the addition of public DNS servers at the secondary DR / Test site as the lowest order of precedence for DNS lookups.
- Fail-over may necessitate some virtualization (see below).


DB Server-To-Server
APP Tier-To-DB-Server
App Native IP-To-NLB V Interfaces
App Native IP-To-NLB V Interfaces (Fail-Over)
Thin WEB Client to NLB VIP
banprddb
banods
Database Backend Subnet 10.201.1.0/24
lumres1
lumres2
baninb1
baninb2
banbackup1
banreports
bandoc
INTRANETDMZ Subnet 10.201.2.0/24
NLB VLAN tagging to both INTRANETDMZ & INTERNETDMZ
banbal1
banbal2
Router
INTERNETDMZ Subnet 10.201.2.0/25
lumweb1
lumweb2
lumweb3
lumweb4
lumcal
lumemail
banssb1
banssb2
Router
Firewall Switch
The Internets & Campus Community
DRTSTDMZ Subnet 10.201.2.128/25
lumtstwb
lumtstap
tstapps
bandevdb
Banbal3 (recommended addition)
SUNGARD HIGHER EDUCATION
FHDA FAIL-OVER TRAFFIC FLOWS
Version 1.9
23 OCT 2008

Virtualization Strategy for Luminis Platform

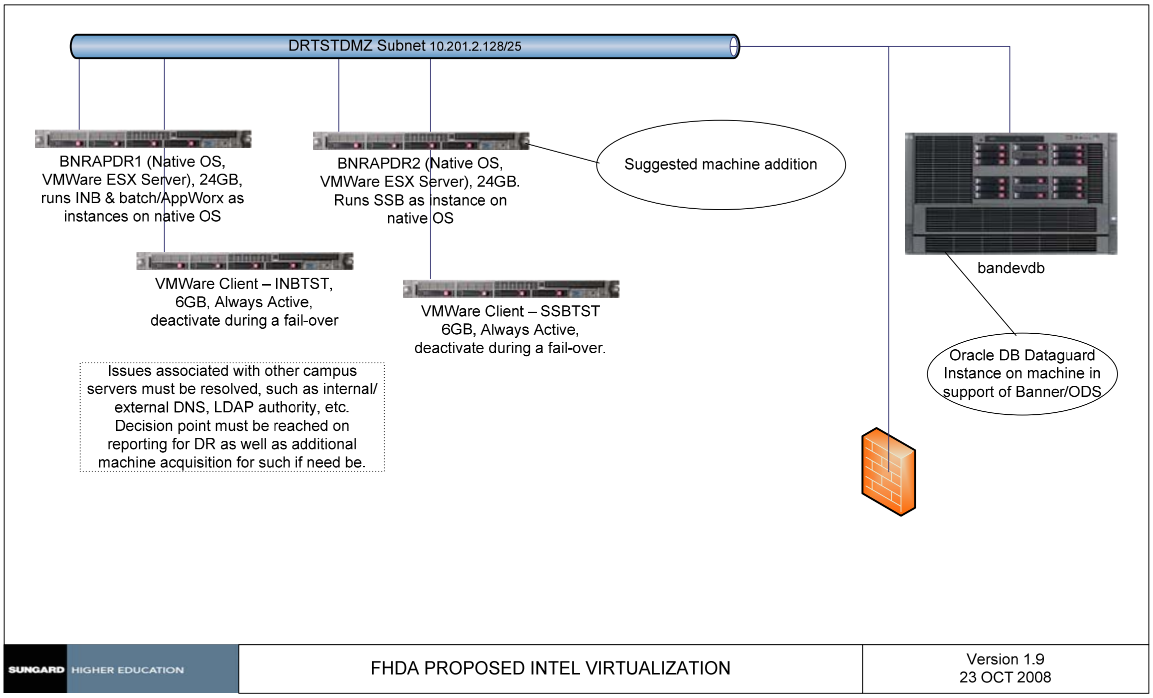
Virtualization with VMWare ESX Server operates its hypervisor within software. SGHE recommends that production instances of any UDC component not be virtualized in a VMWare environment. Virtualization of non-production instances is acceptable with the understanding that should a program error or defect be discovered that could not be duplicated by SGHE or Oracle Technical Support that such would have to be duplicated by the College on the bare metal OS to assure support.

SGHE recognizes the value that can be gained from virtualization. A potential approach for the secondary DR / Test site may be to virtualize the Luminis test instances *and disable them* during a fail-over of production. Actively run instances on the DR machines' bare metal OSs'.


DRTSTDMZ Subnet 10.201.2.128/25
LumDR1 (Native OS, VMWare ESX Server), 24GB, To run Lum Portal on Native Bare Metal OS, always active but not load balanced to unless a machine failure at primary site demands such.
LumDR2 (Native OS, VMWare ESX Server), 24GB, to run LUM email & LUM Cal on bare metal OS in DR mode, otherwise inactive
VMWare Client – LUM TST Email 6GB, Active, Deactivate in DR Mode
bandevdb
Oracle DB Dataguard Instance on machine in support of Luminis
VMWare Client – LUM TST RES 6GB, Active, Deactivate in DR Mode
VMWare Client – LUM TST Portal Portal, 6GB Active, Deactivate in DR Mode
VMWare Client – LUM TST CAL, 6GB Active, Deactivate in DR Mode
Issues associated with other campus servers must be resolved, such as internal/ external DNS, LDAP authority, etc. Issues related to activation of Luminis DR VMWare clients & IP/host name changes must be discussed & planned with SGHE Luminis practice.
SUNGARD HIGHER EDUCATION
FHDA PROPOSED INTEL VIRTUALIZATION LUMINIS TST
Version 1.9
23 OCT 2008

Virtualization Strategy for INB and SSB Hosts

SGHE recommends the same strategy be employed for DR recovery of INB / SSB machines as would be the case for Luminis during a failover. Please note the figure below.

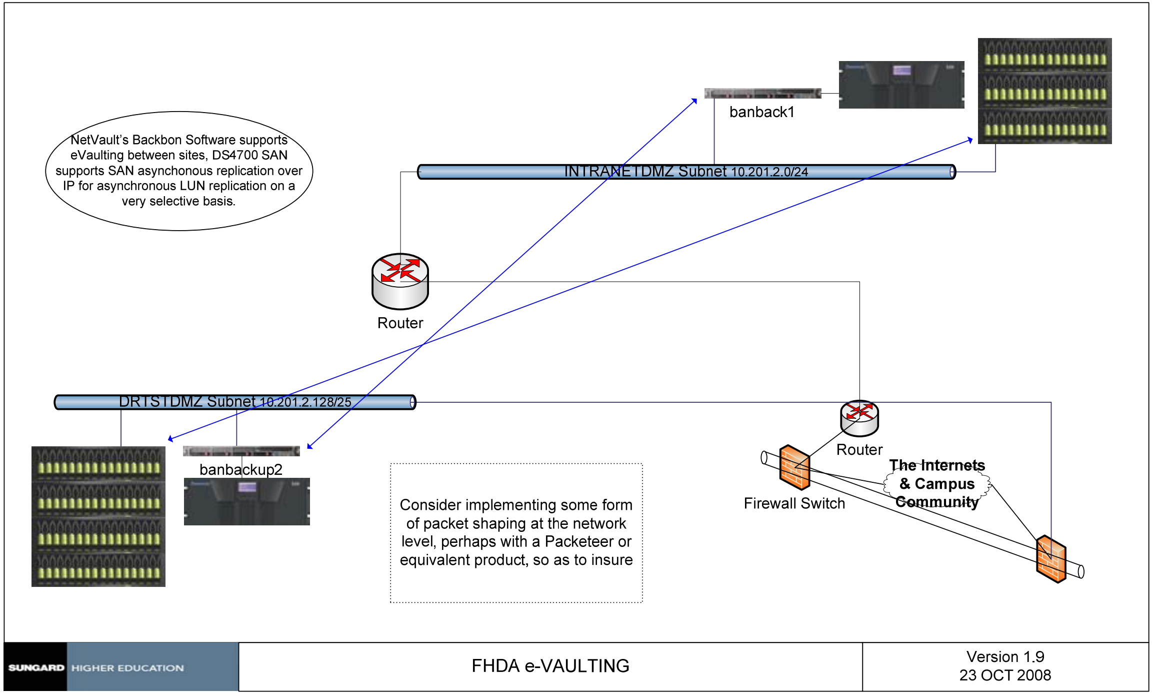

DRTSTDMZ Subnet 10.201.2.128/25
BNRAPDR1 (Native OS, VMWare ESX Server), 24GB, runs INB & batch/AppWorx as instances on native OS
BNRAPDR2 (Native OS, VMWare ESX Server), 24GB. Runs SSB as instance on native OS
Suggested machine addition
bandevdb
VMWare Client – INBTST, 6GB, Always Active, deactivate during a fail-over
VMWare Client – SSBTST 6GB, Always Active, deactivate during a fail-over.
Oracle DB Dataguard Instance on machine in support of Banner/ODS
Issues associated with other campus servers must be resolved, such as internal/ external DNS, LDAP authority, etc. Decision point must be reached on reporting for DR as well as additional machine acquisition for such if need be.
SUNGARD HIGHER EDUCATION
FHDA PROPOSED INTEL VIRTUALIZATION
Version 1.9
23 OCT 2008

e-Vaulting and SAN Replication

The College has made an excellent investment in both tape and SAN technology. This technology will enable the college to potentially implement DR Tiers 3 and 4 for many of the UDC components.

The College can configure its tape libraries, SANs, and NetVault backup software to provide for automatic e-Vaulting of dual collocated storage pools between the primary and secondary sites at DR Tier 3. In simpler words, the secondary DR / Test site can serve to collocate a copy of primary storage pools at the primary site. Conversely, the primary storage pool at the secondary DR / Testing site can be collocated at the primary site. Near-line backups can be stored in dynamic access storage devices (DASD) within the SAN which can then be migrated to the primary and collocated storage pools. The College should strongly consider the implementation of packet shaping without data compression at ingress to the VPN tunnel using a packet shaper, such as a Packeteer 10000 enterprise class shaper. The shaper at the primary site could be outfitted with multiple network interfaces and could conceivably serve both mission critical application flows for the UDC in addition to other applications.

Asynchronous SAN replication could also be employed to provide DR Tier 4 protection. Caution must be employed with SAN replication as replicating large SAN LUNs can consume copious bandwidth in high IO environments and potentially slow production LUNs substantially when very busy.



NetVault's Backbon Software supports eVaulting between sites, DS4700 SAN supports SAN asynchonous replication over IP for asynchronous LUN replication on a very selective basis.

Consider implementing some form of packet shaping at the network level, perhaps with a Packeteer or equivalent product, so as to insure

2.4. Technical Detail Regarding Virtualization of UDC Components

Virtualization is a hot topic these days in the Information Technology field. . Virtualization allows for server consolidation, with potential savings in hardware acquisition and maintenance, operating costs, and administrative time. Virtualization can also play an important role in High Availability and Disaster Recovery strategies. Virtualization of Luminis is not supported at this time and is also not recommended for use on Oracle Database. With respect to Oracle products, Oracle's position with regards to virtualization is stated in Oracle Metalink document *NOTE:249212.1*, and makes no reference to hardware based virtualization. The text is as follows:

Support Status for VMware Virtualized Environments

```
--------------------------------------------------
Oracle has not certified any of its products on VMware virtualized
environments. Oracle Support will assist customers running Oracle
products on VMware in the following manner: Oracle will only provide
support for issues that either are known to occur on the native OS, or
can be demonstrated not to be as a result of running on VMware.

If a problem is a known Oracle issue, Oracle support will recommend the
appropriate solution on the native OS.  If that solution does not work in
the VMware virtualized environment, the customer will be referred to
VMware for support.   When the customer can demonstrate that the Oracle
solution does not work when running on the native OS, Oracle will resume
support, including logging a bug with Oracle Development for
investigation if required.

If the problem is determined not to be a known Oracle issue, we will
refer the customer to VMware for support.   When the customer can
demonstrate that the issue occurs when running on the native OS, Oracle
will resume support, including logging a bug with Oracle Development for
investigation if required.

NOTE: Oracle has not certified any of its products on VMWare, and use of
Oracle products in the RAC environment is also not supported.
--------------------------------------------------
```

Generally speaking, virtualization with server virtualization technology that is hardware based can be considered a stable approach for Oracle Database. That is to say that where the hypervisor that arbitrates access to the hardware by virtual clients of system is stable. This is attributed to hardware based hypervisor technology as being able to properly arbitrate access to the core processors and memory when under extremely heavy loads. HP's approach to virtualization with the HP 6600 line of servers is to provide for support of "hard partitions" by specifically allocating hardware resources to each specified partition. Resources such as RAM, CPU, and adapters are allotted to specific virtual clients of the hypervisor and are thus guaranteed resource allotments. Acquisition of dedicated adapters, disks, CPUs, RAM, and SAN LUNs would be required in order to virtualize HP-UX machines onto the platform. Foothill De Anza College District could conceivably partition its HP RX6600 servers in support of multiple hard partitions on its server, Note however it is recommended that the District first assess how its use of the Banner product consumes server resources prior to committing its machines into a virtualized environment.

Software based partitioning or virtualization is not recommended for production systems that are placed under heavy IO load for both performance and reliability, such as Oracle Database. Software based virtualization, such as VMware, loads the hypervisor, or machine emulator as VMware refers to it, as a software component within a general purpose operating system on GSX server, or a customized version of Linux for ESX server. With VMware GSX server, it is possible to over-commit memory resources on a machine, potentially leading to excessive swapping to disk. Use of GSX Server is discouraged for this reason. VMware's ESX Server can prevent this type of over-allocation through policy enforcement within the product. Other risks are associated with software based virtualization. Specifically, a heavily IO burdened system may experience a scenario where clients are unable to keep pace with a machine's time. Thus it is possible for time reported to applications that are very time sensitive, such as Oracle, to fall behind current time, thus rendering an unstable application environment. This is particularly prevalent with Linux operating systems that predate the Linux kernel version 2.6.21.

To be more technical, VMware does not keep track of processor ticks and wakes up to request a client how many have passed when it is ready to check for an adjust relative time presented to client operating systems. This is in part due to the fact that the Intel X86 processor architecture was never designed to be virtualized, nor were many operating systems. On database servers and other machines that engage in heavy IO, VMware clients can potentially experience time slippage from absolute machine time due to adapters use of IO masked interrupts or just plain heavy IO, and thus may fall being on relative time. As the reader might imagine, some applications are very sensitive to time drift. Any slippage in time where the VMware client falls behind absolute time may result in VMware presenting corrected relative time to the client operating system that could result in the client's kernel time keeper algorithm in applying a time correction that over compensates for lost time. Thus time may oscillate ahead and behind of absolute time with the end result being application hangs on very busy machines. This has been found to be especially true of applications that are time sensitive, such as Oracle Database server. VMware attributes this issue primarily to implementers of various operating systems. Note however that the common use of mask interrupts in IO devices may have the same end result of time slippage, even when guest client kernels implement *tickless* time keeper algorithms. The above issue is not seen as prevalently seen with applications that are not sensitive to time drift or on machines that do not experience high IO.

The above may be resolved in the future given that INTEL and VMware are currently co-developing new software and chip technology to close the gap . In such a scenario, the product would theoretically eliminate the time drift issue and could more accurately present time to guest operating systems. More detail regarding VMware's position on time keeping in Vmware may be found at:
http://www.vmware.com/pdf/vmware_timekeeping.pdf

3. UDC Architecture

Banner Architecture

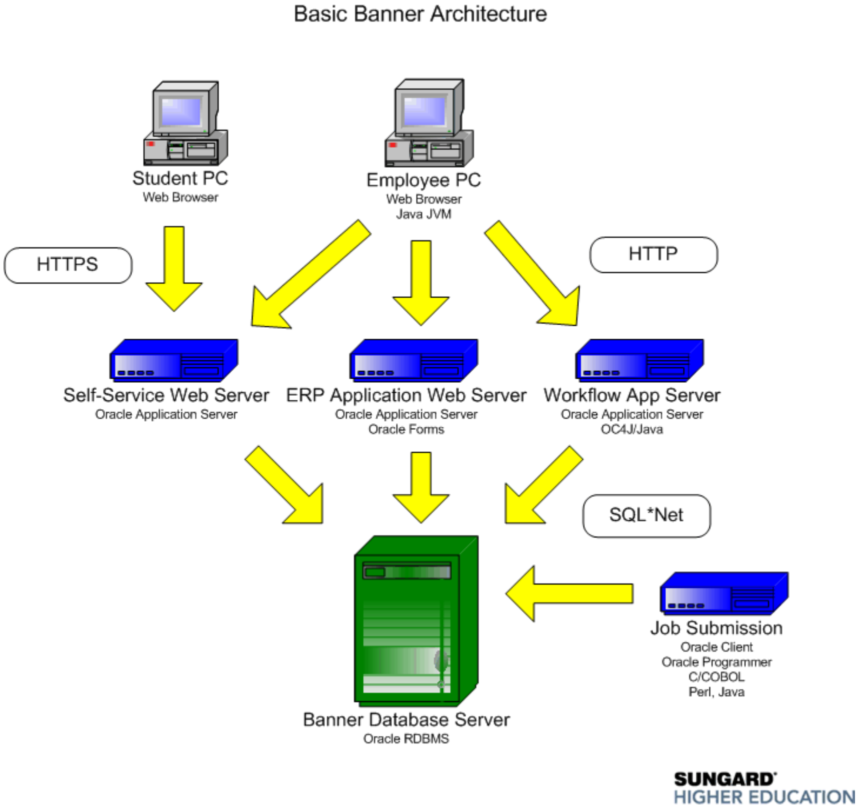
The Banner ERP system consists of an integrated Oracle database along with some front-end application servers. A single database will include tables, views, pl/sql packages and other components needed for the following products: Banner General, Accounts Receivable, Finance, Financial Aid, INAS, Human Resources, Position Control, Student, Faculty and Advisor Self Service, Finance Self Service, Financial Aid Self Service, Employee Self Service, Student Self Service and Web Tailor. Banner Workflow components can also reside in this database, or optionally be housed in a separate database instance.

The front-end applications include:

- Banner ERP Application – this Oracle Forms and Reports application is based on Oracle Application Server and can be accessed with a web browser.
- Banner Self Service – this is also an Oracle Application Server based product, but uses the web server and modplsql modules only.
- Banner Workflow – this is also and Oracle Application Server based product, but uses the J2EE (OC4J) module.
- Banner Job Submission – Banner comes with many batch reports and processes written in Oracle Pro*C and Pro*COBOL. These batch processes are initiated by forms in the ERP application, but they run in the background, usually on a separate server. This batch server will also require C and COBOL compilers (acquired separately). The Appworx Enterprise Scheduler can also reside on this server. The Evisions FormFusion software will also reside here.

Banner Architecture

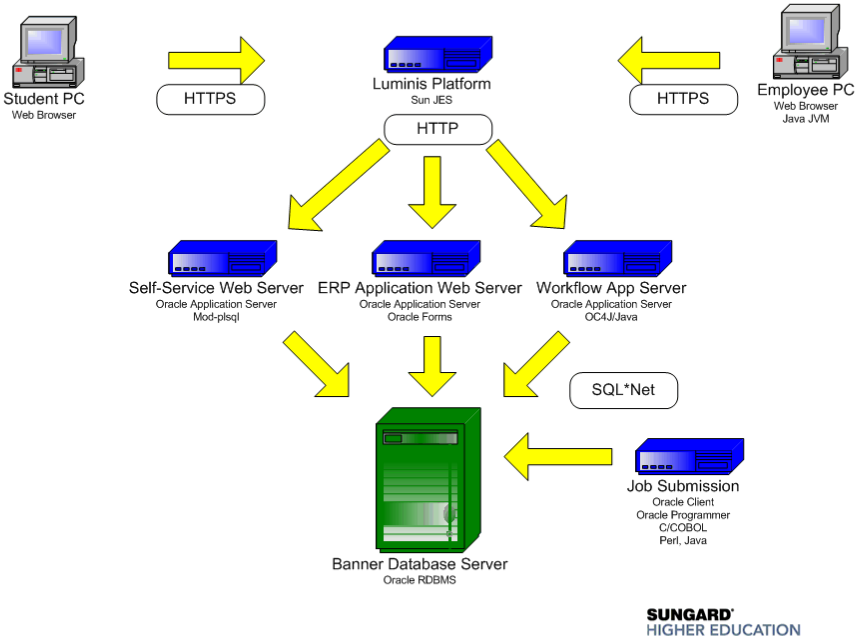
The diagram below depicts the typical Banner architecture.



Banner/Luminis Architecture

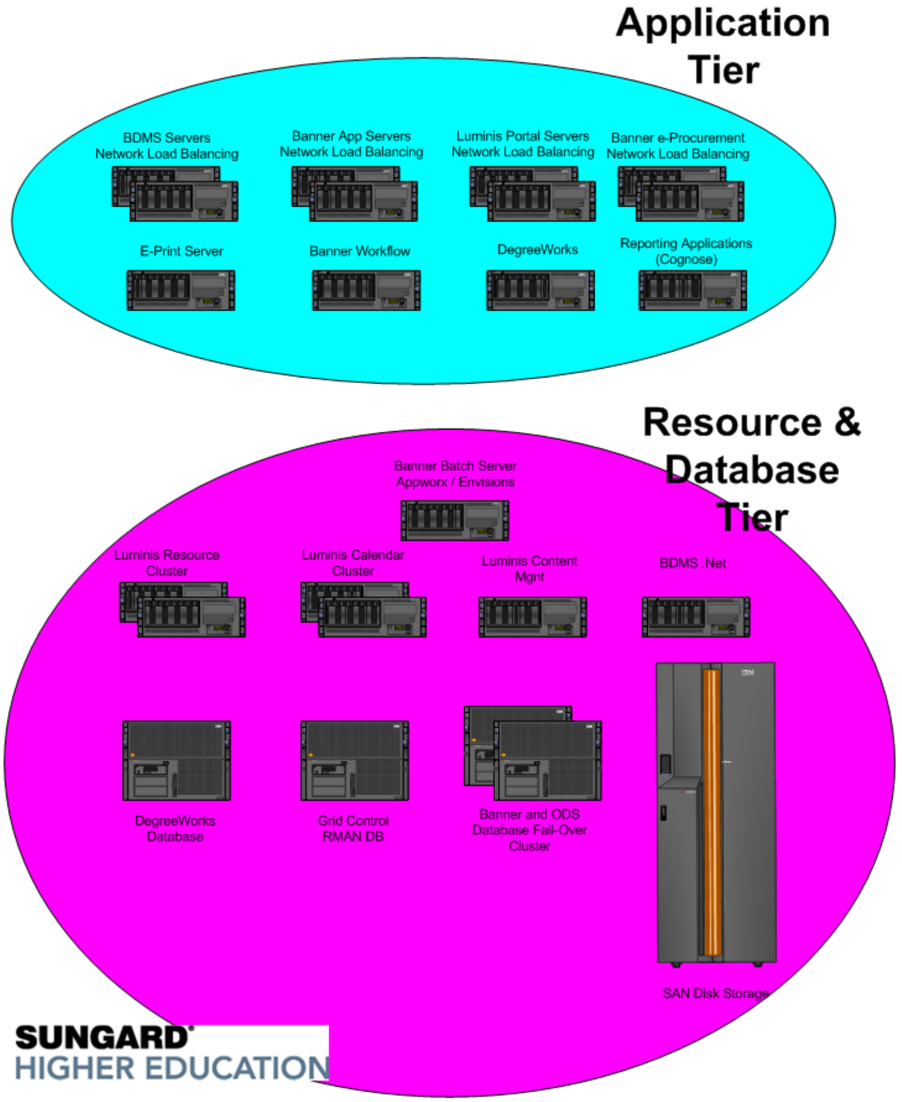
Although Banner can be run independently, many institutions select the Luminis Platform for the front-end web portal. End-users will first connect to the portal which will then access Banner or other applications as required. Note traffic from thin WEB clients to the middle application tier (SSB/INB/WF) is peer-to-peer. So, a revised diagram follows:

Basic Banner/Luminis Architecture



UDC Architecture

Although the Banner ERP system may be the largest component of a Unified Digital Campus environment, there are many other associated applications that can be implemented to create an integrated infrastructure. The servers for those applications are typically identified as application servers (those that end-users connect to directly), and the back-end resource and database servers. A diagram showing this, including some high-availability options follows:


Application Tier
BDMS Servers Network Load Balancing
Banner App Servers Network Load Balancing
Luminis Portal Servers Network Load Balancing
Banner e-Procurement Network Load Balancing
E-Print Server
Banner Workflow
DegreeWorks
Reporting Applications (Cognose)
Resource & Database Tier
Banner Batch Server Appworx / Envisions
Luminis Resource Cluster
Luminis Calendar Cluster
Luminis Content Mgnt
BDMS .Net
DegreeWorks Database
Grid Control RMAN DB
Banner and ODS Database Fail-Over Cluster
SAN Disk Storage
SUNGARD®
HIGHER EDUCATION

High Availability Options

For Database servers, two high-availability options exist:

1. Failover cluster using IBM HACMP, SUN Cluster, etc.
   - Pros – easier setup; possibly more cost effective
   - Cons - some downtime (5-10 minutes) while processes restart; some loss of performance until primary server repaired.

2. Oracle Real Application Clusters (RAC)
   - Pros – 100% uptime of databases
   - Cons – can be costlier; more difficult to configure and manage

For Application servers, Network Load Balancing is suggested for most applications.

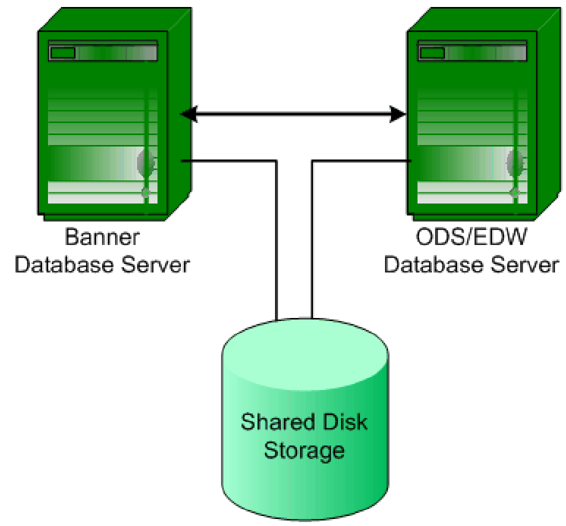
- Pros – highly available uptime for applications
- Cons – additional servers required, NLB hardware required

For Luminis, the "parallel deployment" option is recommended for high-availability.

- Pros – highly available uptime for applications
- Cons – additional servers required, NLB hardware required
- Highly recommended for institutions with over 25,000 users.

A picture of a possible database failover cluster follows. With appropriate cluster software and hardware configuration, if the primary database server fails, then the backup server will automatically restart the database processes resulting in less than 5 minutes of downtime.

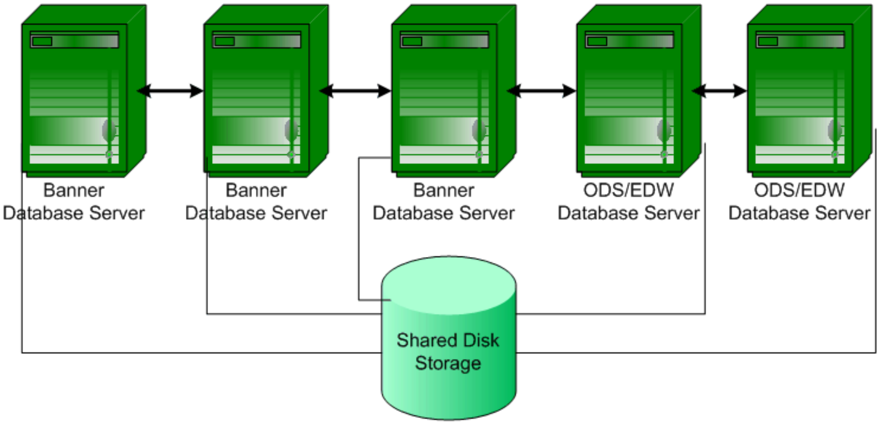
High Availability
Failover Cluster



SUNGARD HIGHER EDUCATION

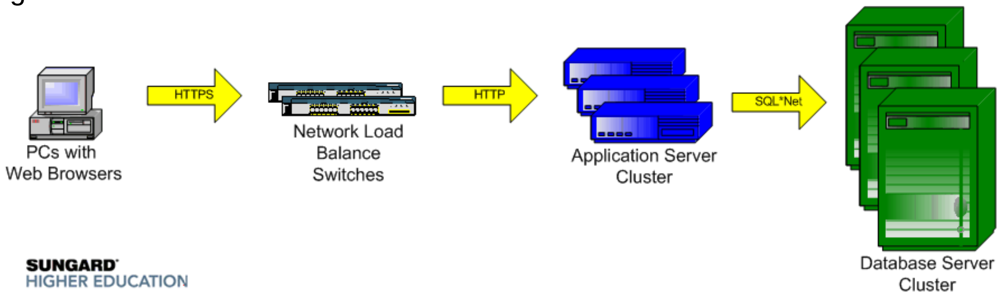
With Oracle RAC, database instances can be load-balanced across multiple servers so that even if one node fails, the others continue to operate. Depending on the application, the end-user may not even notice, or they may just need to reconnect. A picture of a RAC cluster follows:

Oracle RAC



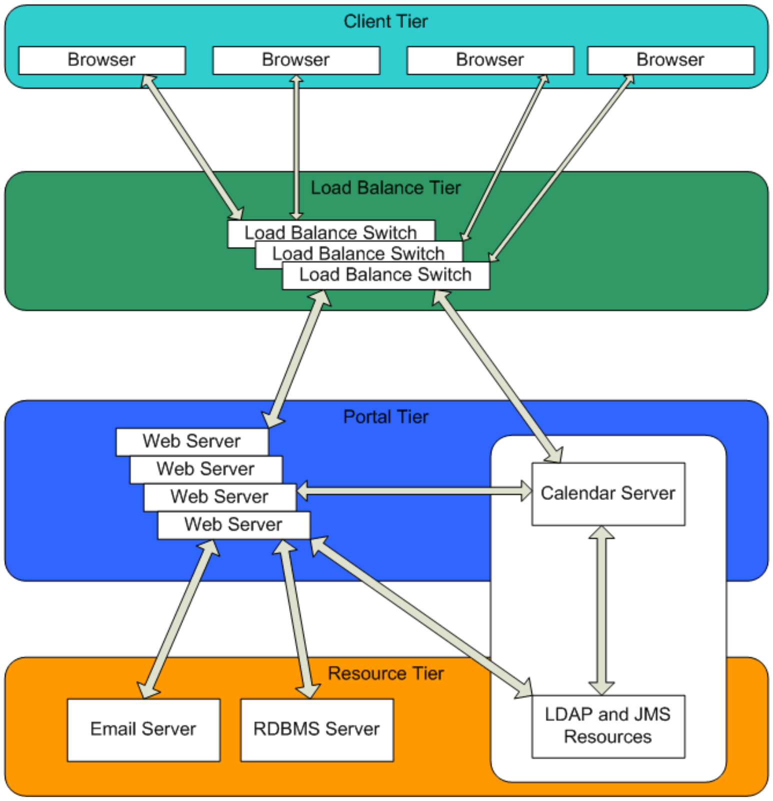
SUNGARD HIGHER EDUCATION

As previously mentioned, many applications are suitable for network load balancing. Multiple small application servers can be configured identically and placed behind a network load balancer device (such as BIG-IP from f5). The network load balancer device determines which application server an end-user connects to. If a server fails, the others are available. Again, end users may not even notice, or may be required to re-connect, depending on the application. A diagram follows:



The Luminis team calls their high-availability solution Parallel Deployment. In this diagram, you can see that there are multiple web portal servers behind a load balancer, but calendar, email and “resource” functions are on separate servers:

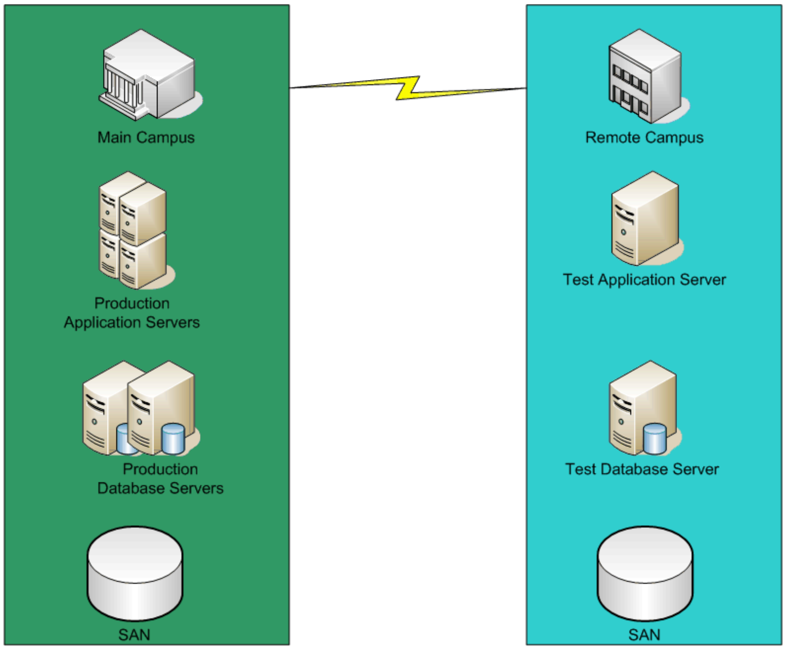
Luminis Parallel Deployment Architecture



Disaster Recovery

A Disaster Recovery solution is necessary to protect the University from a catastrophic failure in the primary data center. Although some institution budgets only allow for a low-cost off-site tape storage solution, a more robust remote data center solution can minimize downtime to hours, rather than days. To help minimize costs, the remote equipment could be the test servers or the Q/A servers.

Disaster Recovery Option



Multiple methods of data replication are possible:

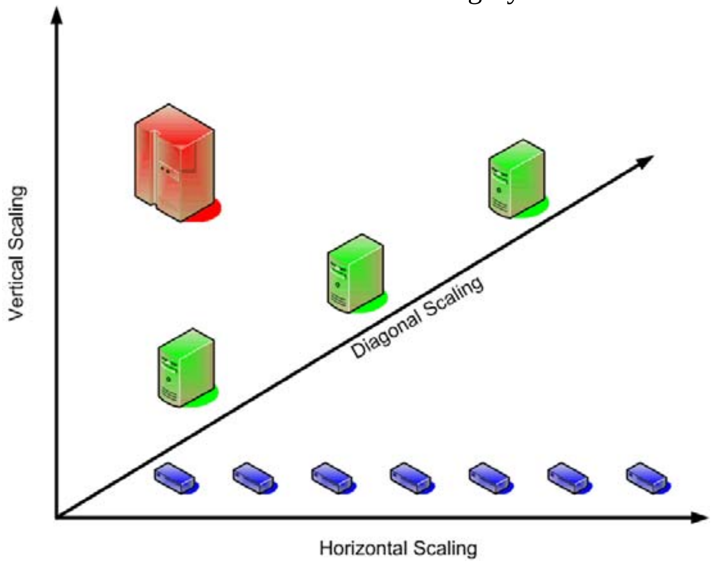
- SAN replication
- Oracle Data Guard
- Magnetic Tape
- Other software solutions

Oracle DataGuard is the preferred solution for maintaining a highly available standby database.

Hardware Scaling

Most large universities want to employ scaling in their hardware architecture plans so that if additional capacity is required, it is a simple upgrade rather than server replacement or architecture changes. Scaling options are generally defined as:

- Vertical Scaling – adding more processors and memory (RAM) to a server to increase capacity. Database servers are typically scaled this way.
- Horizontal Scaling – adding more, generally small, servers to increase capacity. Typically useful for web and application servers.
- Diagonal Scaling – a combination of the above methods. Perhaps using medium-size servers that can increase CPUs, or add additional machines as warranted. Oracle RAC would fit into this category.



Hardware Architecture Summary Recommendations

- Use Vertical Scaling for Database servers (more CPUs). Recommend that that the server model you select can accommodate additional processors if/when required.
- Use Horizontal Scaling for application servers (more machines).
- Use SUN Cluster for high-availability failover for database servers.
- Consider using the ODS/EDW database server as a failover for Banner database server to avoid purchasing standby servers.
- Use Network Load Balancers for high-availability for application servers (where applicable).
- Disaster Recovery servers should be placed in a remote location (prefer 50 miles or more).
- Consider placing Q/A (model office) servers in a remote location so that they can also be used for Disaster Recovery.
- Place multiple databases on the same database server, where appropriate.

- Create separate test, development, Q/A, and production databases.

4. Database Instance Management

4.1. Database instance management information for Banner ERP

Upon consultation with the Database Management team, the following is our suggested approach for instance control / database management.

SEED – Baseline Instance

1. Created with initial Banner software install.
2. This instance is intended for very limited access. Only DBAs should access this instance. No data conversion, dataloads or functional testing, training or processing should occur in this instance. This instance should be maintained with SunGard Higher Education BANNER releases.
    a. This instance serves as a baseline resource for SunGard Higher Education delivered database schema objects and source code (C, COBOL, Forms, Reports, and Java).
    b. Apply all upgrades and patches here first to test the upgrade and the upgrade process. If the upgrade will not apply here, we know we have a problem with the upgrade or the process.
3. This instance could be re-built in the future, if needed, as it only contains SunGard Higher Education data elements.

TRNG – Training Instance

1. Cloned from the SEED database instance.
2. Used for SunGard Higher Education training on the product features, playground for working through exercises with instructors etc.
3. This is ***not*** re-created from SEED as training progresses the training courses build on each other throughout the implementation.
4. Upgrades should be applied in this instance to train users on new features/bug fixes and should closely track the eventual production versioning.
5. Potentially lots of users and/or generic training exist in this environment.
6. Significant amount of test data will exist within this instance.

CONV – Conversion Instance

1. Cloned from the SEED database instance and SunGard's seed data removed.
2. This is where conversion activity occurs to get it tested, tried out, and prove the migration scripts are working as they should.
3. May be re-created or scrubbed (seed data removed) multiple times as conversion testing progresses.
4. Need to keep validation tables and rules tables current with the approved "live" configuration, so data conversion process is thoroughly tested.
5. Should be accessed by conversion staff only and security may be looser during the conversion processes to allow needed access for data input.
6. This instance can "go away" after **all** modules and components have been brought live into PROD and no other conversion efforts are needed.

PPRD – Pre-Production Instance

1. This instance is completely "scrubbed" of test and seed/training data elements, except system required values (requires work from functional and technical personnel).
2. Client work teams execute assignments into this environment (build requisite Rule & Validation Tables to support application).
3. Limited access to users authorized to enter approved validation and rules table data.
4. BANNER users and security should also be built within this instance. There should not be generic testing or training accounts in this system.
5. This instance can "go away" after all modules have been brought live into the PROD environment as a pristine instance is no longer needed. PROD will be the definitive source for all data elements once the data is "live".
6. This instance is cloned over as PROD when the first Banner module goes live in production.

QADB – Quality Assurance Instance

1. A copy of CONV replicated per a schedule for users to verify and validate converted data via the INB or SSB user interface.
2. Security and user access should be established and set in this environment to facilitate full testing scenarios.
3. Generic testing or training accounts should not have access to this system.
4. This instance can "go away" after all modules and components have been brought live into PROD and end user testing has been completed.

PROD – Production Instance

1. For the first Banner module going live this is cloned over from PPRD database instance.
2. For subsequent modules going live all rule & validation tables should be moved here.
3. Upon “Authorization to proceed” sign off at conversion milestones are delivered, the Converter Tool should be pointed to PROD and the scripts executed in this instance to bring over the legacy data into Banner.
4. Day-to-day instance, known as production. Once the data resides in PROD, this instance is the definitive source.

DEVL – Development Instance

1. Dedicated to IT use only. This is their "sandbox" for development.
2. Open access (security) and used for internal site specific modifications, Forms development, etc.
3. Usually a permanent instance for IT development work prior to moving it into TEST.

TEST – Test Instance

1. Ideally, a clone of PROD as often as possible to keep the data "fresh". Recommend nightly or weekly refresh after client is in production mode.
2. Used to assist helpdesk/IT staff replicate problems.
3. Where IT can first move modifications to that are “production” ready – before moving them directly to PROD.
4. Usually a permanent instance for all User Acceptance Testing (UAT) to occur on any patches, upgrades, IT development, etc. Prior to performing the same task in PROD.

4.2. Moving Data between Banner Database Instances

While a variety of methods may be employed, our suggestions are:

1. Validation tables (100 rows or fewer) should be manually entered by client team once agreement made and authorized at highest team level.
2. Export-Import or Oracle data pump utilities should be employed for tables of greater than 100 rows of information. DBLINK is also an option. As it is a more controlled process, ORDER IS ESSENTIAL.
3. Rules Tables that are hierarchical in nature with tables behind tables should be exported/imported with the joint effort of the functional and technical experts to ensure all applicable related tables are managed successfully. Again, DBLINK is also an option.
4. Once valid tables are in the PPRD instance, it is from here that they are copied into the CONV environment for conversion efforts to commence.
5. Data on a “mapped” spreadsheet used for mass uploading can be loaded to CONV and PPRD via sql*loader or the SunGard’s Converter tool as directed by the project team management.
6. For the first Banner module go-live, the PROD database is cloned over from PPRD database after validation and data insertion. For subsequent Banner modules go-live effort, export/import or Oracle data pump option will be used to copy tables from PPRD to PROD database instance.

4.3. Database instance management information for maintaining Oracle environment

RMANDB – Recovery Manager Instance

1. This database is the repository for Oracle Recovery Manager (RMAN).
2. It is highly recommended that all Oracle database backups are done using RMAN and the recovery repository.
3. This database is created on a separate server than all other Oracle databases as it stores backup and recovery information for all databases.
4. Backup of this database should also be taken on a daily basis and stored in a safe place.

GRIDDB – Enterprise Manager Grid Control Instance

1. It is recommended that Oracle Grid Control is installed and configured for managing Oracle database and application server instances throughout the campus.
2. This database is the Oracle Grid Control repository database.
3. Oracle Grid Control agent needs to be installed on every server which needs to be monitored by the Grid Control interface.

PSTBY – Physical Standby Instance

1. It is recommended to setup a Oracle DataGuard physical standby database for production database.
2. This database can be used as production database in case of a situation when production database is not available.
3. After the initial setup/configuration of the standby database this database is kept current with the production database by applying the archive logs shipped from the production server.
4. Manual intervention is needed by the DBA to switch the standby database to primary.

4.4. Database instance management information for other SGHE applications:

Application	**Database**
Luminis	Oracle
Banner Workflow	Oracle
Banner Document Management Suite (BDMS)	Oracle
Banner Enterprise Data Warehouse Workflow	Oracle
Degree Works	Oracle
AppWorx	Oracle
Luminis Content Management (LCMS)	Oracle/SQL Server/Sybase/DB2
E-Procurement	Oracle

Luminis –

Luminis application runs on Oracle database. Separate databases instances for test/development and production environment are recommended. Luminis application and the database are installed on separate servers.

Banner Workflow –

Banner Workflow application runs on Oracle database. Separate database instances for test/development and production environment are recommended. Workflow application and the database are installed on separate servers.

Banner Document Management Suite (BDMS) –

BDMS application runs on Oracle database. Separate database instances for test/development and production environment are recommended.

Banner Enterprise Data Warehouse Workflow –

Banner Enterprise Data Warehouse application runs on Oracle database. Separate databases instances for test/development and production environment are recommended.

Degree Works –

Degree Works application runs on Oracle database. Separate database instances for test/development and production environment are recommended.

AppWorx –

AppWorx application runs on Oracle database. Separate database instances for test/development and production environment are recommended.

Luminis Content Management (LCMS) –

LCMS application can run on any of these databases Oracle, SQL Server, Sybase and DB2. It is recommended to use Oracle as the database for LCMS. Separate database instances for test/development and production environment are recommended.

E-Procurement –

E~Procurement application runs on Oracle database. Separate database instances for test/development and production environment are recommended.

5. Banner Application Maintenance Information

Upon consultation with the Database Management team, the following is our suggested approach for application maintenance.

5.1. Banner

1. Banner ERP consists of the following modules for different areas of the institution:
    a. Accounts Receivable (AR)
    b. Advancement (Alumni)
    c. Financial Aid and INAS
    d. Finance
    e. General
    f. Human Resource (Payroll)
    g. Integration Components
    h. Student
    i. Web Tailor
    j. General Self Service
    k. Student Self Service
    l. Finance Self Service
    m. Faculty and Advisors Self Service
    n. Employee Self Service
    o. Alumni and Friends Self Service
    p. Financial Aid Self Service
2. Banner software is typically installed on the same server where the Oracle database is installed.
3. We recommend that Banner software should be installed on its own separate server called Batch server. This server will then host the Banner software and run the batch processes. This has several benefits:
    a. The C and Cobol processes do not compete with the database processes
    b. Database servers can be tightly secured for access by only DBAs and Sys Admins
4. The directory where Banner software is installed is referred to as BANNER_HOME and an environment variable stores the actual directory location of the Banner software.
5. Batch server runs a process named gurjobs which processes jobs submitted by users. These jobs can be running a C or Cobol program to create a desired report. The output and log files from these jobs are created in a directory owned

by the OS user who starts the gurjobs process. These output and log files need to be deleted from the OS to keep the system clean.

6. A schedule needs to be prepared with consulting the user community to delete the log and output files from the system.
7. There are several collector or work tables in a Banner database.
8. The ERP/INB interface for Banner Application will be installed on a separate server. This can be load balanced using a hardware load balancer in between several servers.
9. The SSB interface for Banner Application will also be installed on a separate server. This can also be load balanced using a hardware load balancer in between several servers.
10. Banner upgrades and/or patches need to be applied as they are released after confirming with the user community.
11. It is recommended to maintain a spreadsheet to keep track of Banner upgrades and patches applied to a Banner instance. There are tables in the Banner database for each module which can be queried to get the versions installed in that database. There is a common table for storing the information on all the patches applied to that database.

5.2. Oracle

1. Oracle Enterprise Edition software and Oracle Companion software is installed on the Database server.
2. Oracle Client software with Oracle ProC and ProCobol pre-compilers and Oracle Companion software is installed on the Batch server:
3. Oracle Application Server Forms and Reports version is installed on the ERP/INB server and executable Banner forms and reports are generated on this server.
4. Oracle Application Server J2EE and WebCache version is installed on the SSB server.
5. Oracle upgrades and/or patches need to be applied on database servers as well as the application servers.
6. It is recommended to use Oracle 10g Grid Control to maintain Oracle upgrades and patches.
7. Database backups should be taken on a regular basis.
8. It is recommended that Oracle RMAN (Recovery Manager) tool be used for taking database backups of all Oracle databases.
9. It is also recommended to use RMAN in conjunction with a recovery catalog database which stores the backup and recovery information for all the databases being backed up using RMAN.
10. RMAN recovery catalog database should be created on a separate server than the other databases rman is backing up.

11. RMAN can be used to take full or incremental hot backups and can compress/decompress backups on the fly which create small backup files.
12. It is recommended that Oracle Physical Standby database be created for the production database which can be used in case of a failure on the actual Production database.
13. The physical standby database is created on a separate server than the actual production server and if possible it can be housed in a separate building/campus.

5.3. Other required software

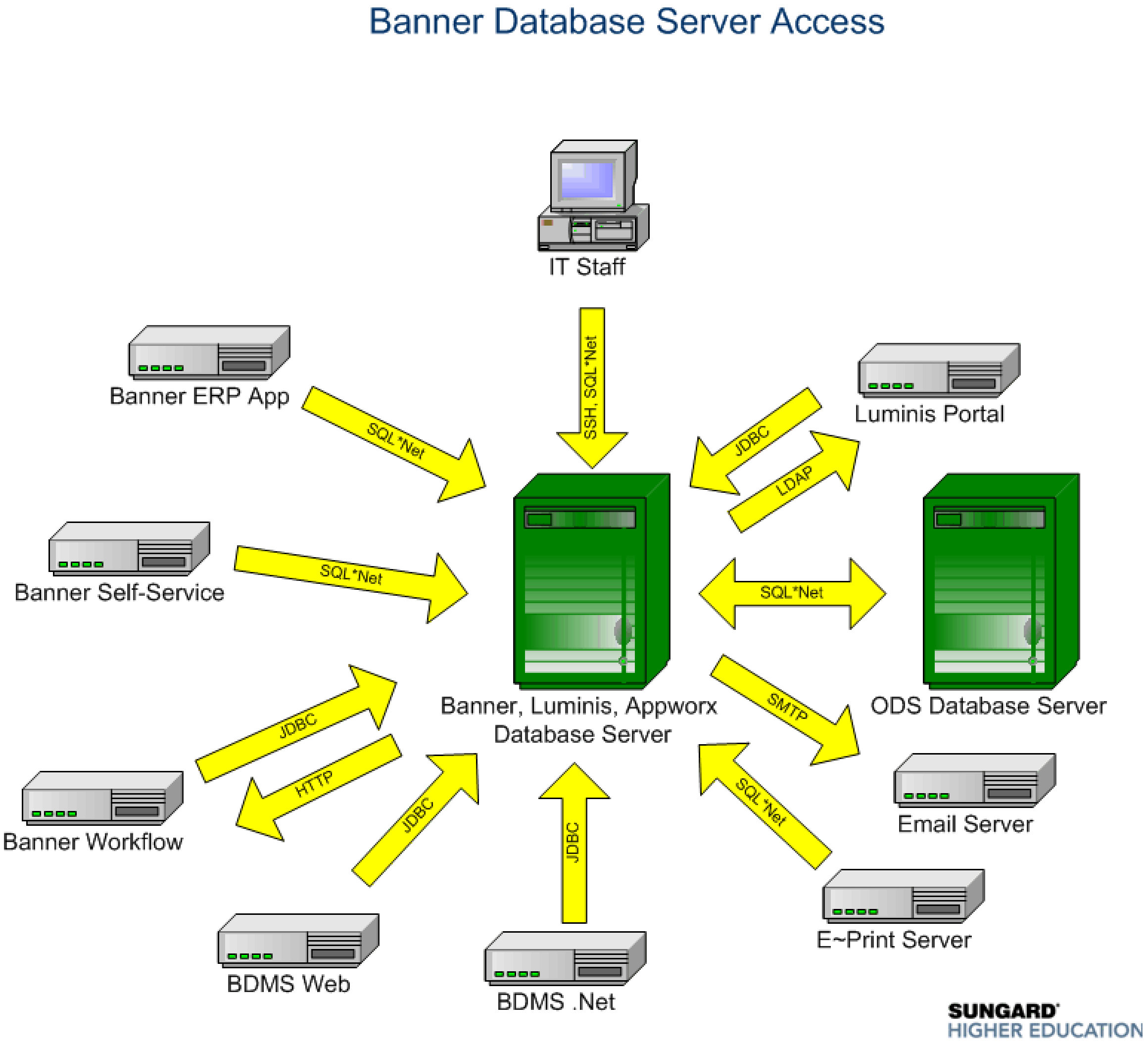
1. C++ and Cobol compilers are required for compiling C and Cobol programs on the batch server.
2. In addition starting with Banner 8 International Components for Unicode (ICU 3.6) is also required on the batch server for compiling C programs.
3. SUN Java JVM plug-in is required on the Client PC to access ERP/INB interface of Banner Application.

6. Server Access Requirements

The following charts show the typical way the primary UDC servers are accessed.

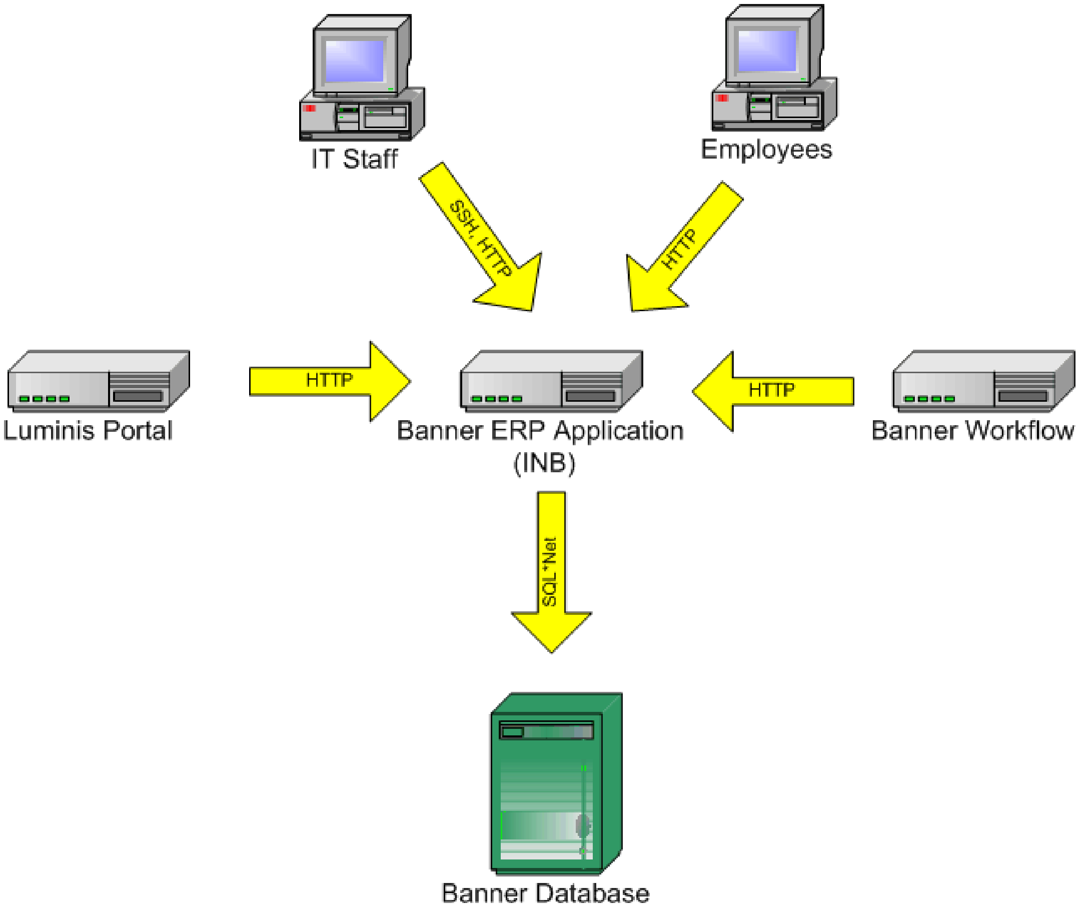
Please note that there may be other applications and/or access methods for a specific client environment that are not represented here.

Banner Database Server Access



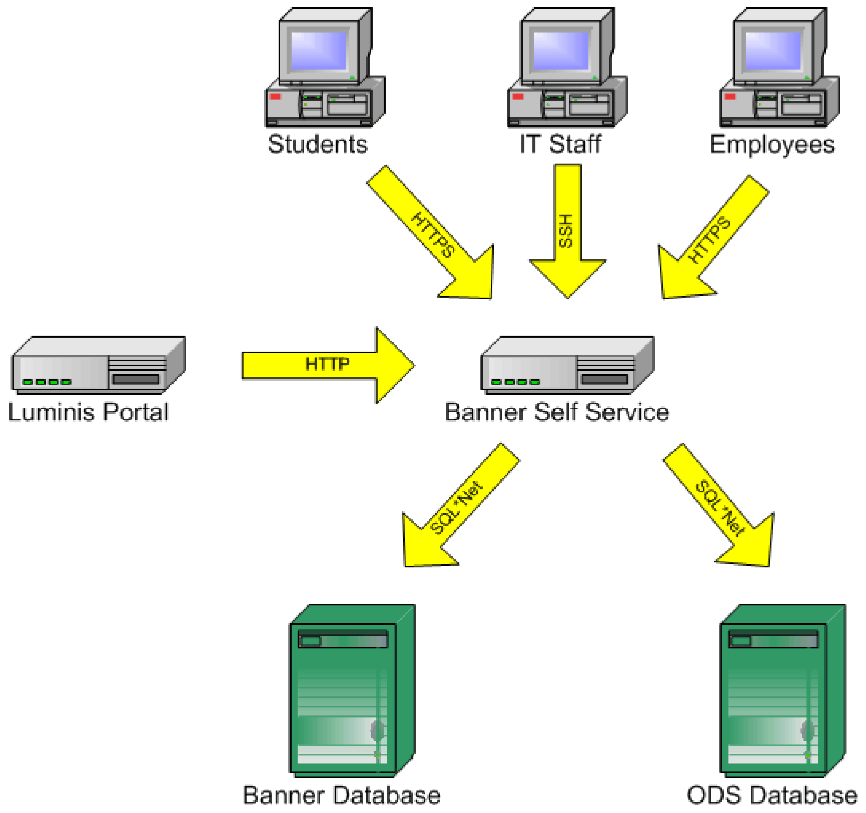
Banner ERP (INB) Application Server Access

Banner ERP Application (INB) Server Access

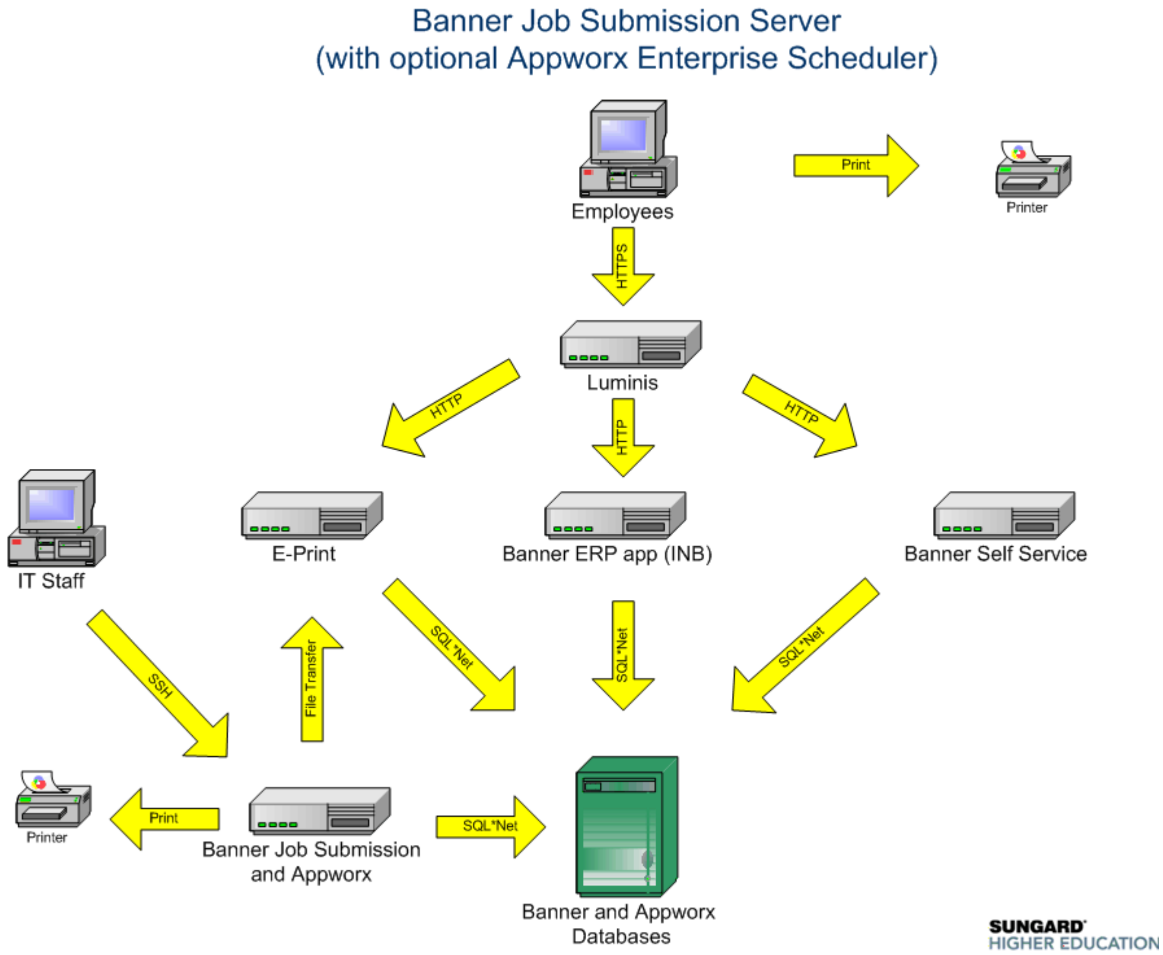


Banner Self Service Server Access

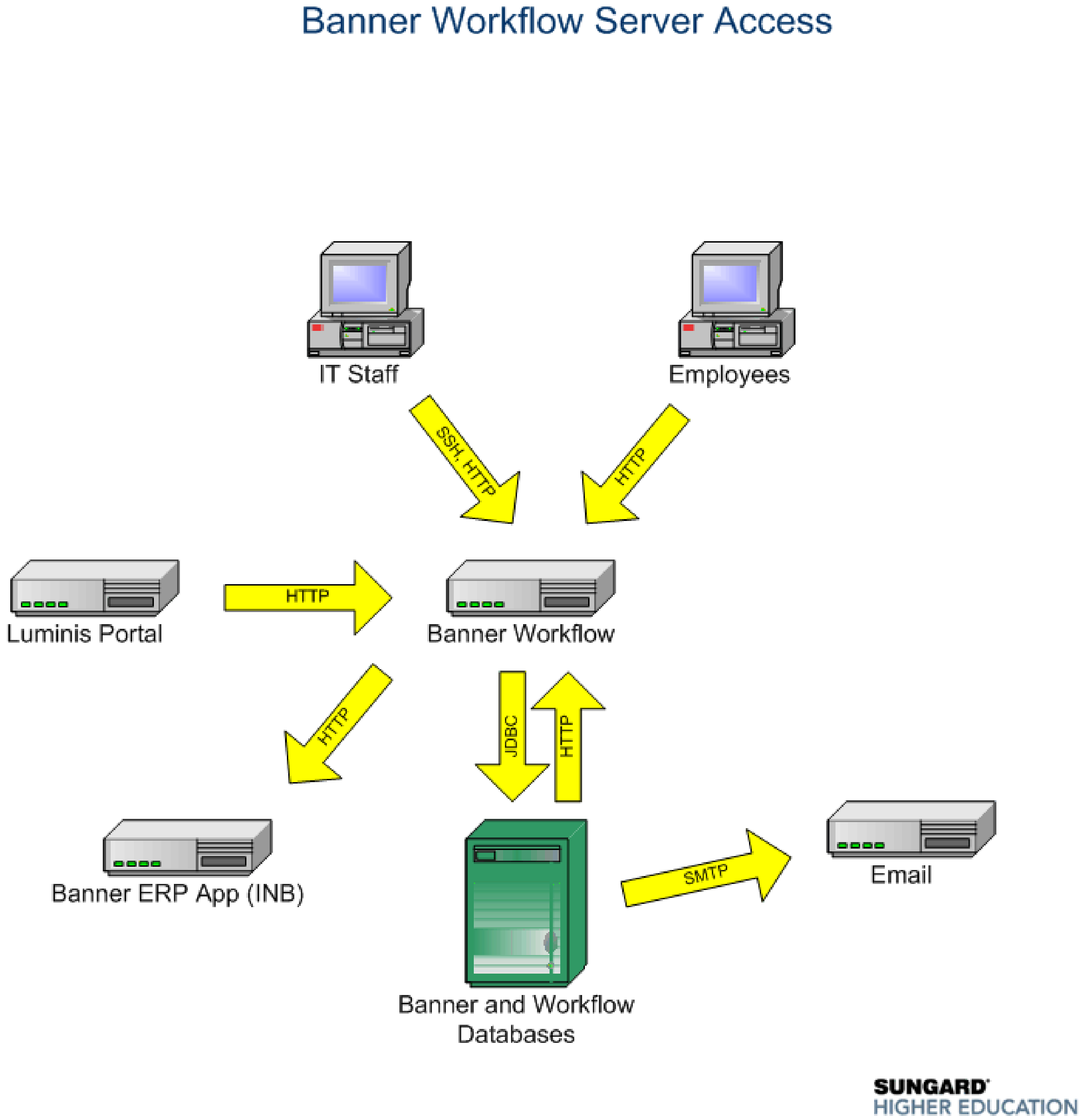
Banner Self Service Server Access



Banner Job Submission Server Access

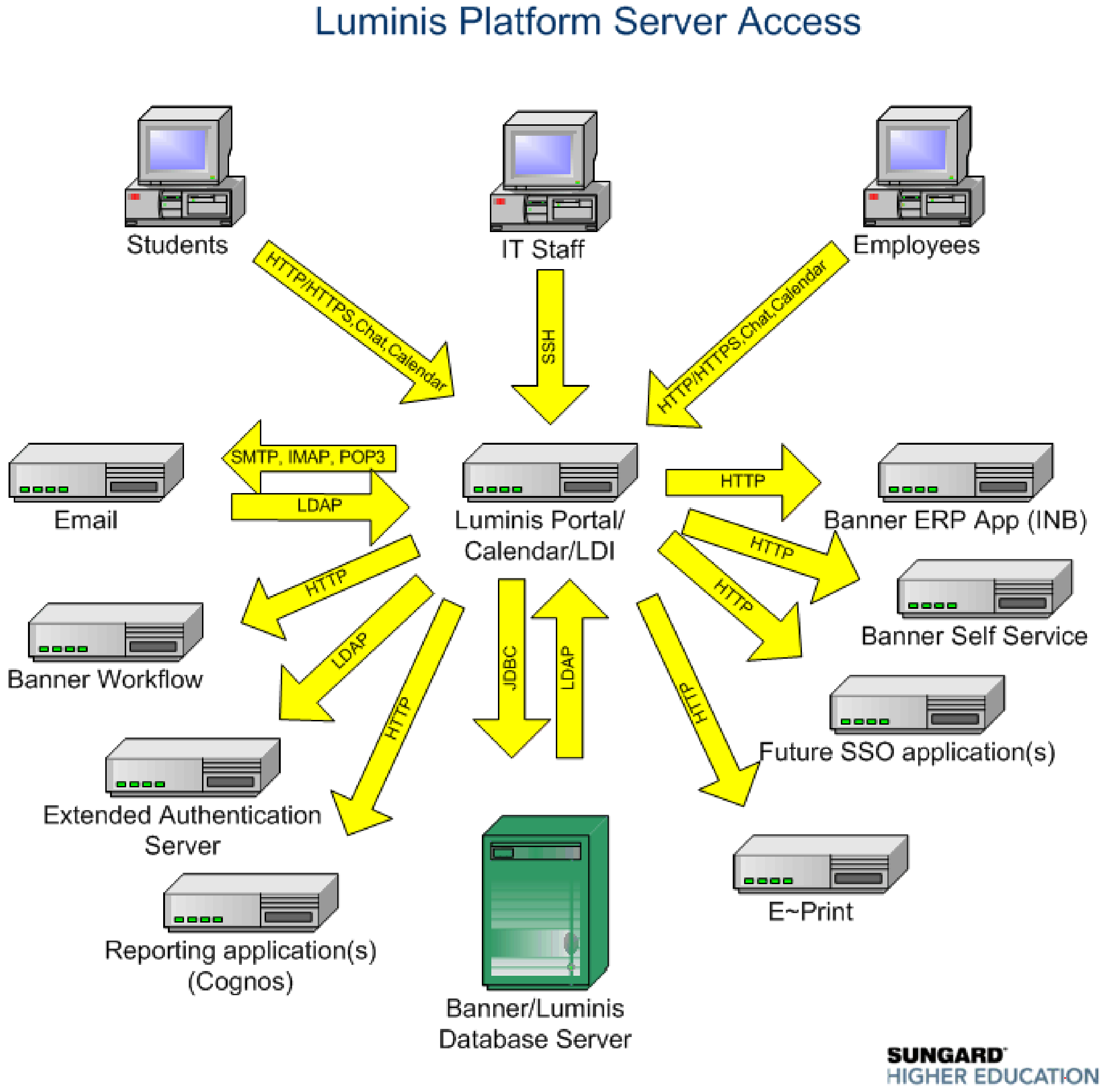


Banner Workflow Server Access

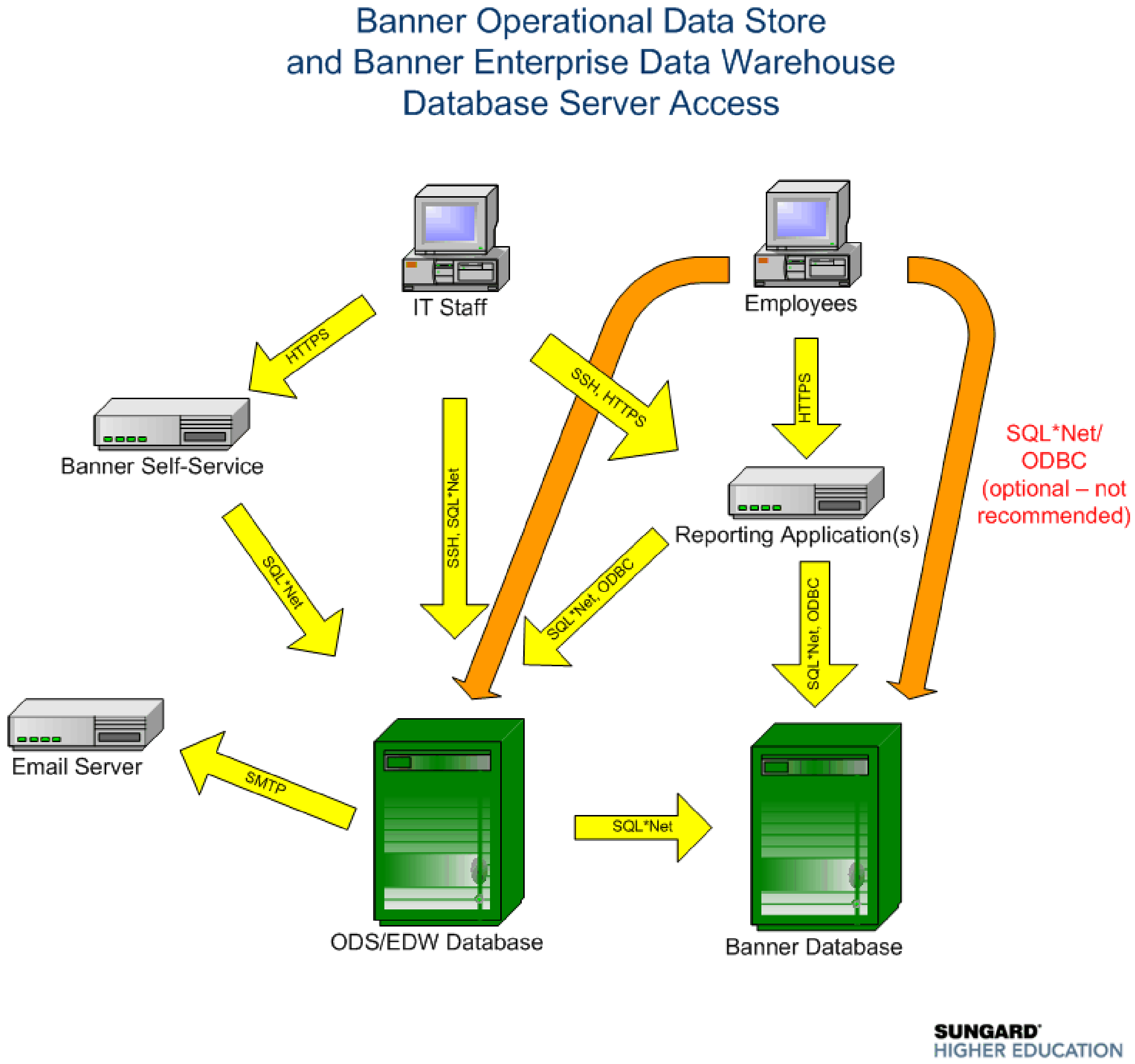


Banner Workflow Server Access

Luminis Server Access

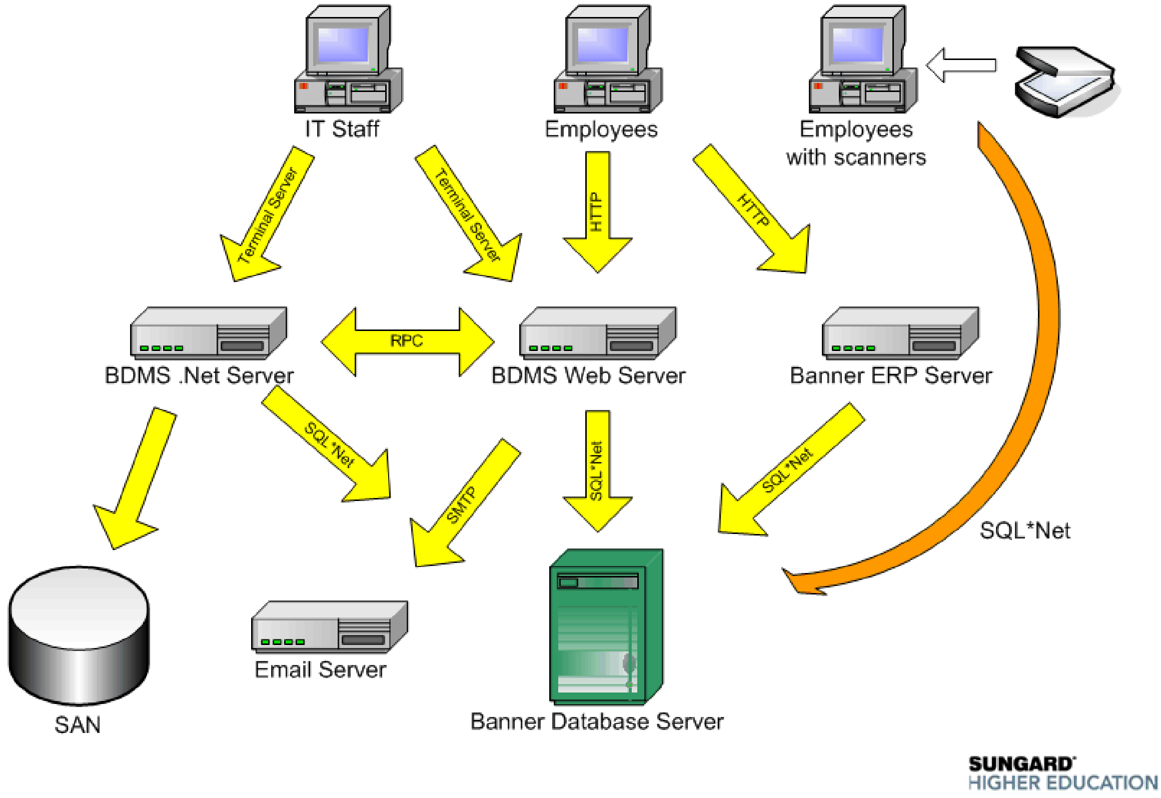


Banner Operational Data Store and Enterprise Data Warehouse Server Access



Banner Document Management Suite Server Access

Banner Document Management Suite
(formerly XtenderSolutions)
Server Access



7. Next Steps

7.1. Hardware Installation

Hardware to be installed by hardware vendor in accordance with the Banner pre-requirements documentation already provided.

Build out network in accordance with the best practices outlined in this document with modifications as deemed appropriate by the college.

Provide SGHE remote installers with remote access to machines in accordance with the Banner pre-requirements documentation already provided.

7.2. SunGard Higher Education Software Installation Process

As each SunGard Higher Education product is scheduled for implementation, a technical consultant will provide detailed pre-install requirements or checklist documents so that the servers are properly prepared prior to the software installation date. A pre-install verification will take place to make sure the servers are properly configured. Most installations are done remotely, with follow-up onsite visits for verification and knowledge transfer.

8. Disclaimer

The configuration described in this document is provided by SunGard Higher Education for illustrative purposes only and is not a recommendation by SunGard Higher Education that your institution should acquire the equipment reflected herein. SunGard Higher Education makes no guarantee or commitment that the equipment described will be sufficient for your institution's needs, and the equipment description is merely intended to reflect a starting point for your institution's consideration. Each software implementation is unique and each institution has different needs and/or requirements. Further, system performance and response times are dependent upon a variety of factors, including network latency, hardware and peripheral configuration, systems tuning, number of users at a given time, peak periods of usage, Internet connectivity, the number of applications being deployed on a processor, as well as hardware sizing and processor capability. Accordingly, the appropriate equipment and configuration for your institution may vary in many regards from the one described in this sheet. You must independently make the determination as to the equipment to acquire in connection with the implementation of the contemplated software. SunGard Higher Education recommends that you consult directly with your hardware vendor of choice regarding overall configuration selection and sizing recommendations. SunGard Higher Education has no responsibility or liability in connection with this determination, and SunGard Higher Education disclaims any warranties of any kind in connection with the hardware you select, including any warranties of merchantability or fitness for a particular purpose. The total number of processors in your final configuration may be different depending upon your hardware vendor's recommendations.

This system strategy document recommends best practices relative to deployment of the UDC. It does not imply, explicitly nor implicitly, that the described potential deployment strategies recommended within would be included within your institution's project scope. Please contact your project or account manager for specific details regarding what is included within scope of your particular project.

9. Document History

Revision Record

Number	Date and Sections	Author	Notes
0.1	September 12, 2008	Hank Classe	First version
0.2	September 14, 2008	Hank Classe	Additional edits applied, updates from Oracle and Packeteer technical consultants consulted with applied. Submitted for peer-review plus requests for comments to Oracle & Luminis subject matter experts (SME) for additional comment.
0.3	September 23, 2008	Ted Schmidt	Add comment regareding DG licensing, recommend Batch/Appworx on dedicated machine, correct lanuage regarding Luminis & remove references to proxying, remove dated reference to index rebuilding, correct traffic flow diagram discrepencies.
0.4	September 23, 2008	Scott Manley	Additions to describe
0.5	September 24, 2008	Gary Fitzgerald	Remove comments regarding virtualization of HP-UX machines. Recommmend Batch/Appworx on dedicated machines. Add lanuage regarding Grid Control & Dataguard Broker
0.6	October 2, 2008	Hank Classe	Final edits applied. Submitted team for final peer review.
1.7	October 14, 2008	Hank Classe	Final edits received and applied. consisting primarily of spelling errors not detected by Word.
1.8	October 20, 2008	Hank Classe	Modify to remove recommendation to reduce number of WEB portal machines from 3 to 4 (back to 4), add stronger language relative to clustering of certain Luminis UDC components, add additional detail regarding virtualization.
1.9	October 23, 2008 & November 12th, 2008	Hank Classe Russell Wright	Replace references of GSX to ESX Server. Apply verbage corrective changes to Luminis sections. Correct typos. Modify statement on soft virtualization. Replace v1.8 drawings w/ v1.9 drawings. Append disclaimer.

10. Appendix A – Disaster Recovery Tier Levels

Generally speaking, there are 7 layers of defined disaster recovery. Initially established in 1992 by the SHARE users group (www.share.org), the 7 tier Disaster Recovery methodology simplifies the process by which you can define service levels, risks, and target which recovery level is the correct one for your business application. Selecting the best recovery level requires that this model be understood as summarized in the table below.

DR Tier Level	**Description**
Tier 0 – No Off-Site Data	Businesses with a Tier 0 DR level have no disaster recovery plan. Recovery time is unpredictable and in some cases may not be possible.
Tier 1 – Data Backup Protection with no Hot Site	Businesses that employ Tier 1 DR backup their data. Businesses that adopt this tier may tolerate several days to weeks of data loss or loss of service.
Tier 2 – Data Backup with a Hot Site	Businesses make regular backups on tape and combine this with an off-site recovery facility and infrastructure in which to restore service in the event of loss of service.
Tier 3 – Electronic Vaulting	Tier 3 encompasses all of Tier 2 plus electronic vaulting of data to another site.
Tier 4 – Point-in-Time Copies	Tier 4 incorporates the use of disk solutions to electronically ship off data to a remote site. Tier 4 implementers may suffer up to several hours of data loss but offer more rapid recovery from a disk based backup solution versus tape.
Tier 5 – Transaction Integrity	Tier 5 is used by business for consistency of data between production and recovery systems. They provide for near real-time recovery of data. Applications must be Tier 5 capable. Oracle Dataguard is an example of a Tier 5 capable application.
Tier 6 – Zero or Little Data Loss	Tier DR 6 demands a high level of data concurrency and is used by businesses that must restore applications rapidly. Applications do not have to be Tier 6 capable.
Tier 7 – Highly Automated	Tier 7 applies all components used in Tier 6 plus automation. Recovery of applications is automated.