



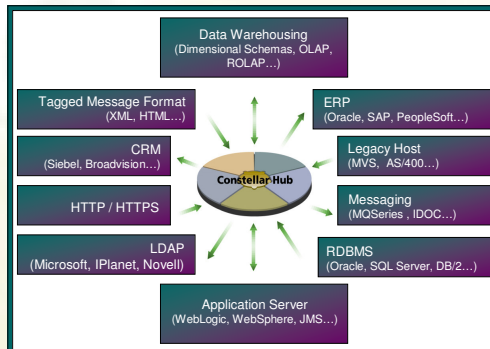
Achieving Enterprise Wide Authentication using EAI

Martin Flanagan, Eucalypt Software Partners
mflanagan@eucalypt.com.au

Introduction

- Founded in 1997
- Head office in Canberra
- Operations across Australia/New Zealand
 - Distributor of DataMirror products
- Consulting expertise in
 - Data Migration projects
 - Data Warehousing projects
 - Integration projects
- Developers of "The Right Approach" Development Methodology

Enterprise Application Integration



Introduction

- About the University of Western Sydney (UWS)
- Where have we come from?
- Teething troubles for a unified UWS
- Improving the situation
- Using the technology

University of Western Sydney



- 35,000 students
- 2,500 staff
- 6 major campuses across Western Sydney

UWS pre-2000

- 3 largely autonomous Federated Network Members
- 3 separately maintained IT departments
- 3 different approaches to networking
- "if there are two ways of doing it, UWS will find a third"




Unified UWS' teething troubles

eucalypt.net.au

- Difficulties creating a single set of computing standards from three
- Confusion about which workflows are in use at various campus locations
- Little structure to the management of devices, users, and applications
- Data too distributed for effective use




What is the Answer?

eucalypt.net.au

- 42?
- Blame someone else?
- Enterprise Architecture Project




Enterprise Architecture (EA)

eucalypt.net.au

- Overview
- Desktop Services (Standard Operating Environment)
- Print Services
- Application Services
- Data Services




EA Overview

eucalypt.net.au

- Part of an overall Quality of Service initiative sponsored by the Vice-Chancellor
- Incorporates both UWS ITD strategic vision and recommendations from a Price Waterhouse independent assessment
- Current phase - to deploy critical infrastructure services that are necessary to stabilise the IT environment within UWS and to provide an agile and robust platform for the future




EA Desktop Services

eucalypt.net.au

- Incorporates the delivery of a Desktop Standard Operating Environment
- Standardises access to IT services across all campuses
- Includes the introduction of Microsoft Exchange 2000 as a calendar mail and file sharing solution
- Provides the ability for a user to access their own data, and the same range of shared data, applications etc. from almost any machine across the university




EA Print Services

eucalypt.net.au

- Allows for seamless access to network printing devices from Office Desktop applications and corporate systems from any UWS campus location
- Centralised management allows for better device access security
- Incorporates a sensible set of naming standards for print devices




EA Application Services

- Development of a central directory service storing info on Staff, Students and relevant external people, to be used for applications' authentication of users
- Aims to provide a base portal environment (including personalised content) for Staff, Students and Authorised Guests to access the UWS Intranet and systems delivered through it




EA Data Services (EADS)

- Provides the required systems integration on which the rest of the EA project relies
- Provides a pilot warehousing solution in the form of a database of members of the greater UWS Community
- Provides a methodology for future UWS data warehousing exercises

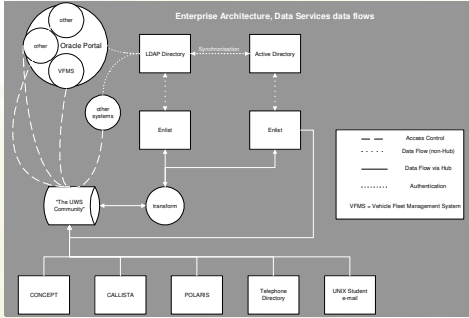



The Core of EADS

- UWS Community Database
- SunOne LDAP Directory Server
- Microsoft Active Directory



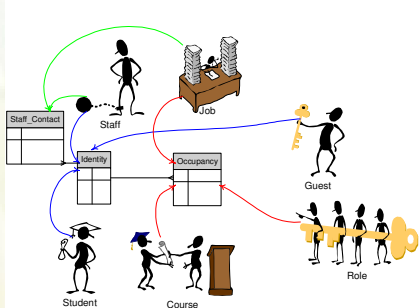

EADS Project at a glance



The diagram illustrates the Enterprise Architecture, Data Services data flows. It shows a central 'UWS Community' database connected to various systems including 'Oracle Portal', 'LDAP Directory', 'Active Directory', 'Enter', 'Exit', 'Information', 'CONCEPT', 'CALLISTA', 'POLARS', 'Telephone Directory', and 'UWS Student email'. A legend indicates that solid lines represent 'Access Control', dashed lines represent 'Data Flow (non-PHS)', dotted lines represent 'Data Flow via PHS', and a thick solid line represents 'Authentication'. A note specifies 'VPMS - Vehicle Fleet Management System'.




The UWS Community Database



The diagram shows the UWS Community Database structure. It includes entities like 'Staff', 'Student', 'Course', 'Guest', and 'Role'. Relationships are depicted with lines connecting these entities to a central 'Identity' and 'Occupancy' table. A 'Job' icon is also shown near the 'Staff' entity.




Directories

- SunOne Directory
- Microsoft Active Directory




Populating LDAP

- EnList:
ODBC to LDAP enabled Directory Services




Using the solution - VFMS

- The Vehicle Fleet Management System (VFMS)
- VFMS utilises LDAP authentication
- VFMS gathers additional data from the UWS Community database
- VFMS has put the EADS solution to the test by using both the authentication and UWS Community as an integral part of its working.



Welcome

UWS Portal



UWS Login

Change Password

Enter your user name and password to login.

User Name

Password

Login

IMPORTANT MESSAGES

SYSTEM OUTAGE

The Vehicle Fleet Management System will be unavailable between 5pm and 6pm on Tuesday 23rd March due to system maintenance.

ALL USERS

As from 9th February this application uses MyUWSAccount authentication, based on your Staff or Student ID. If you have not activated your MyUWSAccount please do so before proceeding.

NEW STAFF MEMBERS

Staff members commencing at UWS after 3rd February will need to email [Christina Davison](#), your name and Staff or Student ID number to [christina.davison@uws.edu.au](#) before proceeding.

Welcome to the UWS Portal

Click to enter the Financials Reporting Portal

Provides access to Oracle Financials Portlets including:

- Accounts Payable (Paid & Unpaid Invoices)
- Accounts Receivable (Paid & Unpaid Invoices)
- Open Purchase Orders
- Fixed Assets
- Unapproved Mastercards Vouchers
- Budget Report

All Portlets are categorised to Cost Centre and Project levels

Click to enter the Vehicle Fleet Management System (VFMS)

Book a UWS pool car



Janette Towell



UWS Login

Change Password

UWS Login

IMPORTANT MESSAGES

SYSTEM OUTAGE

The Vehicle Fleet Management System will be unavailable between 5pm and 6pm on Tuesday 23rd March due to system maintenance.

ALL USERS

As from 9th February this application uses MyUWSAccount authentication, based on your Staff or Student ID. If you have not activated your MyUWSAccount please do so before proceeding.

NEW STAFF MEMBERS

Staff members commencing at UWS after 3rd February will need to email [Christina Davison](#), your name and Staff or Student ID number to request registration before accessing the VFMS System. Please allow 1 working day before your registration becomes effective. You will also need to activate your MyUWSAccount.

Welcome to the UWS Portal

Click to enter the Financials Reporting Portal

Provides access to Oracle Financials Portlets including:

- Accounts Payable (Paid & Unpaid Invoices)
- Accounts Receivable (Paid & Unpaid Invoices)
- Open Purchase Orders
- Fixed Assets
- Unapproved Mastercards Vouchers
- Budget Report

All Portlets are categorised to Cost Centre and Project levels

Click to enter the Vehicle Fleet Management System (VFMS)

Book a UWS pool car



Vehicle Fleet Management System



UWS Home

Change Driver Profile

Change Password

Welcome

The UWS Vehicle Fleet Management System has been introduced to:

- Enable staff to book any vehicle available on campus for business purposes
- Automate the charge-out & recovery of cost of each trip
- Manage fuel card expenditure
- Monitor fuel consumption

Booking Procedure:

- Book a car for:
 - Single same day trips
 - Overnight trips
 - Multiple same day trips
- Print the booking slip
- Bring the booking slip when you collect keys
- Fill in the booking slip when you return
- Hand in the keys & booking slip



Janette Towell



UWS Home

Change Driver Profile

Change Password

Welcome

The UWS Vehicle Fleet Management System has been introduced to:

- Enable staff to book any vehicle available on campus for business purposes
- Automate the charge-out & recovery of cost of each trip
- Manage fuel card expenditure
- Monitor fuel consumption

Booking Procedure:

- Book a car for:
 - Single same day trips
 - Overnight trips
 - Multiple same day trips
- Print the booking slip
- Bring the booking slip when you collect keys
- Fill in the booking slip when you return
- Hand in the keys & booking slip

4

Address: http://uws.uws.edu.au/7778/...
 University of Western Sydney
 Janette Towell
 UWS Home
 Change Drive Profile Change Password
 Home Bookings Services Admin Developers
 Daily Bookings Overnight Bookings Bulk Bookings Return Cancellations Bookings Pending Workflows Connect
 Help
Vehicles Available on a Daily Basis
 Use this form to book a vehicle for a specific day or part thereof
 Pool: All pools for Campbelltown Campus
 Date vehicle required: 23 Mar 2004
 Time required (optional) From: To:
 Rego No. (optional): All Regos for selected Pool
 Show Available Vehicles Reset Form
Show Daily Bookings
 Use this form to view / amend daily bookings
 Booked By: Janette Towell
 Pool: All pools for Campbelltown Campus
 Date From: 23 Mar 2004
 Date To (optional):
 Show Bookings My Bookings
 Show Bookings Reset Form
 Copyright (c) University of Western Sydney 2003
 While the University of Western Sydney (UWS) attempts to ensure accuracy and reliability of the information contained on the UWS web site, UWS makes no warranty.

Project Implementation

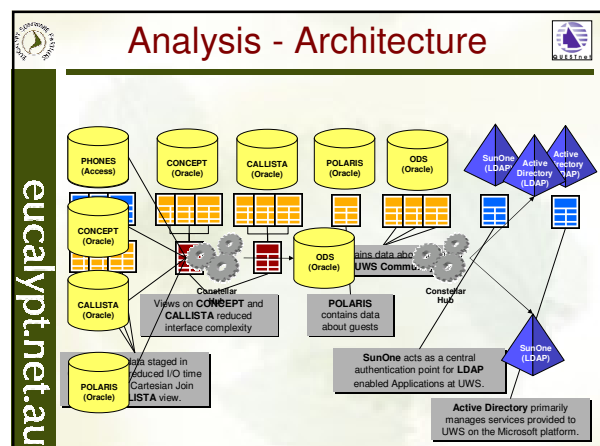
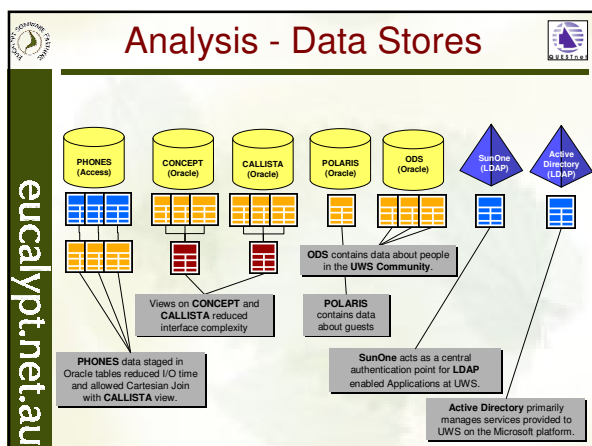
- Eucalypt Software Partners
 - Integration Design
 - Integration Development
 - Used existing DataMirror Constellar Hub license (DataMirror EAI tool)
 - Purchased Enlist Report Server (Persistent Systems)
- UWS
 - Acceptance Testing
 - Operational Deployment

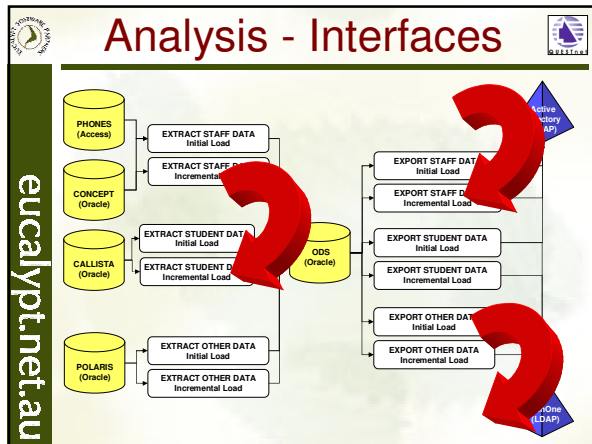
The EADS Project Interfaces

- Requirements
- Analysis
- Design Challenges
- Future

Requirements

- The EADS project was concerned with the population of directories for authentication and access controls for various UWS systems (including VFMS)
- Data was sourced from authoritative systems including Concept, Callista and Polaris.
- The project also saw the creation of a UWS Community database, housing the relevant information on all members of the UWS community





Analysis - Interfaces

EXTRACT/EXPORT STAFF/STUDENT/GUEST DATA
Initial Load

- Initial Load
 - High volume of data
 - Only run once
 - Provides baseline for change detection
 - Will be used for Disaster Recovery

Analysis - Interfaces

EXTRACT/EXPORT STAFF/STUDENT/GUEST DATA
Initial Load

EXTRACT/EXPORT STAFF/STUDENT/GUEST DATA
Incremental Load

- Initial Load
 - High volume of data
 - Only run once
 - Provides baseline for change detection
 - Will be used for Disaster Recovery

- Incremental Load
 - Low volume of data
 - Run daily
 - Populates changes from source systems

Design Challenges

- Directory Services as Data Sources/Targets
 - DataDirect Sequelink 5.0
 - Persistent Systems EnList
- Directory Service Metadata
 - Single-Valued Attributes
 - Multi-Valued Attributes
- Transactional Control
 - Detecting failed Commit-Groups

What is LDAP?

- Lightweight Directory Access Protocol
- Originated from X.500 on 7 layer ISO stack degenerated into LDAP on 5 layer TCP/IP stack
- Used daily in DNS, eMail etc.

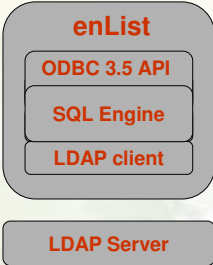
LDAP	vs.	RDBMS
• Hierarchical		• Relational
• Entries, Indexes		• Tables, Views, Indexes
• Entry (DN-DistinguishedName)		• Row
• Attribute, Objectclass		• Column
• Data Types		• Data Types
• Primarily for Read		• Read as well as Write

Example of LDAP Hierarchy

- o=enListDemo.com (OC-top, organization, Attributes - o,oc)
- |---- ou=administrators,o=enListDemo.com
- |---- ou=groups,o=enListDemo.com
- |---- ou=partners,o=enListDemo.com
- |---- ou=contractors,o=enListDemo.com
- |---- ou=employees,o=enListDemo.com
- |---- uid=Albert.Fox,ou=employees,o=enListDemo.com
- |---- uid=Joe.Blow,ou=employees,o=enListDemo.com
- |---- uid=Mary.Snow,ou=employees,o=enListDemo.com
- .
- OC = objectclass

enList SQL Gateway engine

- Scalable, Read/Write SQL access to directories
- Staging data facilities and report synchronisation
- Enabling existing SQL applications with directories

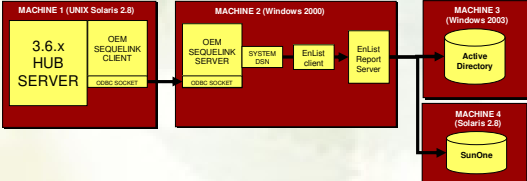


The diagram shows a stack of components: enList at the top, followed by ODBC 3.5 API, SQL Engine, and LDAP client. Below this stack is the LDAP Server.

enList is a JDBC and ODBC-application connector for LDAP directories.

Directory Services as Sources/Targets

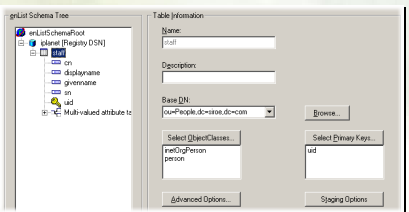
- DataDirect Sequelink and Persistent Systems EnList enables the Hub to
 - Retrieve Metadata from Directory Service
 - Extract/Export data to/from Directory Service



The diagram shows four machines: MACHINE 1 (UNIX Solaris 2.8) with a 3.6.x HUB SERVER and OEM SEQUELINK CLIENT; MACHINE 2 (Windows 2000) with OEM SEQUELINK SERVER, SYSTEM DSN, EnList client, and EnList Report Server; MACHINE 3 (Windows 2000) with Active Directory; and MACHINE 4 (Solaris 2.8) with SunOne.

Directory Service Metadata

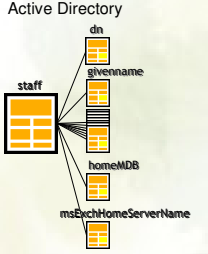
- The enList Admin Console defines the 'tabular view' of Directory Service data.
- Base DN defines the level that data is drawn from
- ObjectClasses determine available attributes



The screenshot shows the enList Admin Console interface with fields for Name, Description, Base DN, and ObjectClasses.

Directory Service Metadata

Active Directory



The diagram shows a tree structure for Active Directory with nodes for staff, givenname, homeMDB, and msExchHomeServerName.

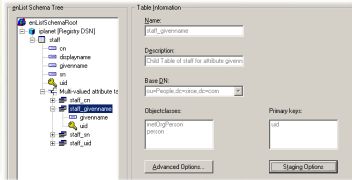
Name	DataType	Length	CP	Other	Mand	Used
cn	ALPHANUMERIC	255	2	N	Y	
givenname	ALPHANUMERIC	255	3	N	Y	
sn	ALPHANUMERIC	255	4	N	Y	
displayName	ALPHANUMERIC	255	5	N	Y	
mail	ALPHANUMERIC	255	6	N	Y	
telephoneNumber	ALPHANUMERIC	255	7	N	Y	
physicalDeliveryOfficeName	ALPHANUMERIC	255	8	N	Y	
homeMDB	ALPHANUMERIC	255	10	N	Y	
msExchHomeServerName	ALPHANUMERIC	255	11	N	Y	
department	ALPHANUMERIC	255	12	N	Y	
location	ALPHANUMERIC	255	13	N	Y	
locationTelephoneNumber	ALPHANUMERIC	255	14	N	Y	
pager	ALPHANUMERIC	255	15	N	Y	
mobile	ALPHANUMERIC	255	16	N	Y	
fax	ALPHANUMERIC	255	17	N	Y	
faxHome	ALPHANUMERIC	255	18	N	Y	
countryCode	ALPHANUMERIC	255	19	N	Y	
internationalization	ALPHANUMERIC	255	20	N	Y	
mailAlias	ALPHANUMERIC	255	21	N	Y	
mailNickname	ALPHANUMERIC	255	22	N	Y	
homeMDB	ALPHANUMERIC	255	23	N	Y	
msExchHomeServerName	ALPHANUMERIC	255	24	N	Y	
msExchMailboxGuid	ALPHANUMERIC	255	25	N	Y	

- Each person type (staff/student/guest) has an associated table.
- Single-Valued attributes only.

Directory Service Metadata

Multi-Valued Attributes

- M-V Attribute has a Column in base table AND Has its own separate table



The screenshot shows the enList Admin Console interface with fields for Name, Description, Base DN, and ObjectClasses.

staff

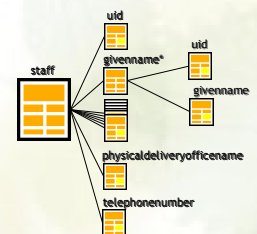
uid	cn	displayname	givenname	sn
12345	John Doe	John C. Doe	John	Doe
67890	Jane Smith	Jane A. Smith	Jane	Smith

staff_givenname

uid	givenname
12345	John
12345	Robert
67890	Jane
67890	Elizabeth

Directory Service Metadata

SunOne



The diagram shows a tree structure for SunOne with nodes for staff, uid, givenname, physicalDeliveryOfficeName, and telephoneNumber.

Name	DataType	Length	CP	Other	Mand	Used
cn	ALPHANUMERIC	255	2	N	N	
givenname	ALPHANUMERIC	255	3	N	N	
sn	ALPHANUMERIC	255	4	N	Y	
physicalDeliveryOfficeName	ALPHANUMERIC	255	5	N	N	
telephoneNumber	ALPHANUMERIC	255	6	N	N	
uid	ALPHANUMERIC	255	7	N	N	
mail	ALPHANUMERIC	255	8	N	N	
mailAlias	ALPHANUMERIC	255	9	N	N	

Attributes in staff_givenname

Name	DataType	Length	CP	Other	Mand	Used
givenname	ALPHANUMERIC	255	1	N	Y	
uid	ALPHANUMERIC	255	2	N	Y	

- Each person type (staff/student/guest) has an associated table.
- Some Multi-Valued Attributes with associated tables



Directory Service Metadata



eucalypt.net.au

Working with Multi-Valued Attributes

staff

uid	cn	displayname	givenname	sn
12345	Joe Smith	Joe G. Smith	Joe	Smith
67890	Janet Dickson	Janet Dickson	Janet	Dickson

staff_givenname

uid	givenname
12345	Joe
12345	Garry
67890	Janet

- The multi-valued attribute table acts like a FIFO queue when accessed through the base table.

```

UPDATE staff
SET givenname =
'Jane'
WHERE uid = '67890'

```



Directory Service Metadata



eucalypt.net.au

Working with Multi-Valued Attributes

staff

uid	cn	displayname	givenname	sn
12345	Joe Smith	Joe G. Smith	Joe	Smith
67890	Janet Dickson	Janet Dickson	Jane	Dickson

staff_givenname

uid	givenname
12345	Joe
12345	Garry
67890	Jane

- The multi-valued attribute table acts like a FIFO queue when accessed through the base table.

```

UPDATE staff
SET givenname =
'Jane'
WHERE uid = '67890'

```



Directory Service Metadata



eucalypt.net.au

Working with Multi-Valued Attributes

staff

uid	cn	displayname	givenname	sn
12345	Joe Smith	Joe G. Smith	Joe	Smith
67890	Janet Dickson	Janet Dickson	Jane	Dickson

staff_givenname

uid	givenname
12345	Joe
12345	Garry
67890	Jane

- The multi-valued attribute table acts like a FIFO queue when accessed through the base table.

```

UPDATE staff
SET givenname =
'Joseph'
WHERE uid = '12345'

```



Directory Service Metadata



eucalypt.net.au

Working with Multi-Valued Attributes

staff

uid	cn	displayname	givenname	sn
12345	Joe Smith	Joe G. Smith	Garry	Smith
67890	Janet Dickson	Janet Dickson	Janet	Dickson

staff_givenname

uid	givenname
12345	Garry
12345	Joseph
67890	Janet

- The multi-valued attribute table acts like a FIFO queue when accessed through the base table.

```

UPDATE staff
SET givenname =
'Joseph'
WHERE uid = '12345'

```



Directory Service Metadata



eucalypt.net.au

- Impact on design
 - Separate design strategies for Active Directory and SunOne
- Active Directory
 - Data is 'flattened' from ODS relational schema
 - Where multiple values exist one is arbitrarily chosen
- SunOne
 - Multiple values for a staff/student/guest attribute are exported where they exist.
 - Data is modified directly in the M-V Attribute table



Transactional Control



eucalypt.net.au

- Detecting failed records for incremental interfaces
 - Each record in the ODS has a status that indicates that it should be (I)nserted/(U)pdated/(D)eleted or has been (E)xported.
 - Mandatory caching of Source/Target records
 - Use Output cache record status to determine successful records
 - Join back to ODS and update successfully (E)xported records.




Deployment

eucalypt.net.au

- What
 - At least 6 interfaces
 - Some run more than once with different configurations
- When
 - Initial Load - run once
 - Incremental Load - run daily, but when?
- How
 - Transformation Manager?
 - Scheduler?
 - Command Line?




Deployment

eucalypt.net.au

- The hub ARUN package used to start interfaces from PL/SQL, e.g.


```
ARUN.EXECUTE (SYS: 'hub run <connect_string> int=<interface_name>
tx_enable=<tx1>,FALSE tx_enable=<tx2>,TRUE, NULL, TRUE, var_retcode,
vResp1, vResp2, 60, FALSE);
```
- PL/SQL package
 - Controls/Monitors interface execution
 - Abort execution or Warn on non-zero return code from listener
- Scheduler
 - Calls shell/sql script to run PL/SQL package at designated time




Future

eucalypt.net.au

- Further Applications have already been modified to authenticate against directory information
 - PlatformWeb (SQLServer database)
 - Unix home directory assignment (Solaris Posix)
 - Concept Financial Reporting (Oracle Portal)
 - Password reset/change (HTML/Web Server)
- Immediate path to achieving common sign-on
 - Once ERP applications support LDAP
- Future path to achieving single sign-on (OS embedded authentication)




Questions

eucalypt.net.au

?