Oracle Audit Vault

How can you increase the safety and security of your Oracle database while minimizing the cost of regulatory compliance.

Introduction

- Daniel Morgan
- Oracle Ace Director
- University of Washington
  - Wrote UW Oracle curricula
  - Primary program instructor - 8 years
- Education Chair: PSOUG

- Member: UKOUG

- Frequent speaker – OOW and user group events
- 10g, 11g, and TimesTen Beta tester
- Oracle since version 6
- Too many years of Fortran and COBOL
- Contact: damorgan@u.washington.edu

Uncommon IT Issues to

msnbc

A Fuller Spectrum of News

Home » Technology & Science » Tech News & Reviews

sponsored by hp

- Video
- U.S. News
- Politics
- World News
- Business
- Sports
- Entertainment
- Health
- Tech / Science
  - Space News
  - Science
  - Tech News/Reviews
  - Online World
  - Security
  - Wireless
  - Games
  - Innovation
- Travel
- Weather
- Blogs Etc.
- Local News

Microsoft Excel fails math test

Employee blogger wrote that some multiplication results incorrect

Associated Press

Updated: 10:29 a.m. PT Sept 28, 2007

SEATTLE – Microsoft Corp.'s Excel 2007 spreadsheet program is going to have to relearn part of its multiplication table.

In a blog post, Microsoft employee David Gainer said that when computer users tried to get Excel 2007 to multiply some pairs of numbers and the result was 65,535, Excel would incorrectly display 100,000 as the answer.

Gainer said Excel makes mistakes multiplying 77.1 by 850, 10.2 by 6,425 and 20.4 by 3,212.5, but the program appears to be able to handle 16,383.75 times 4.

Story continues below ↓

MSN TECH AND GADGETS

Slide show: Hot TVs for fall

How to buy a mobile phone

Spam that could kill you

Related Stories What's this?

Games boost Microsoft's search engine

Microsoft rolls out Live Search improvements

Visa issue spurs Microsoft office in Canada

Most popular

Most Viewed | Top Rated | Most E-mailed

The biggest sex mistakes men and women make

Emerging Threats

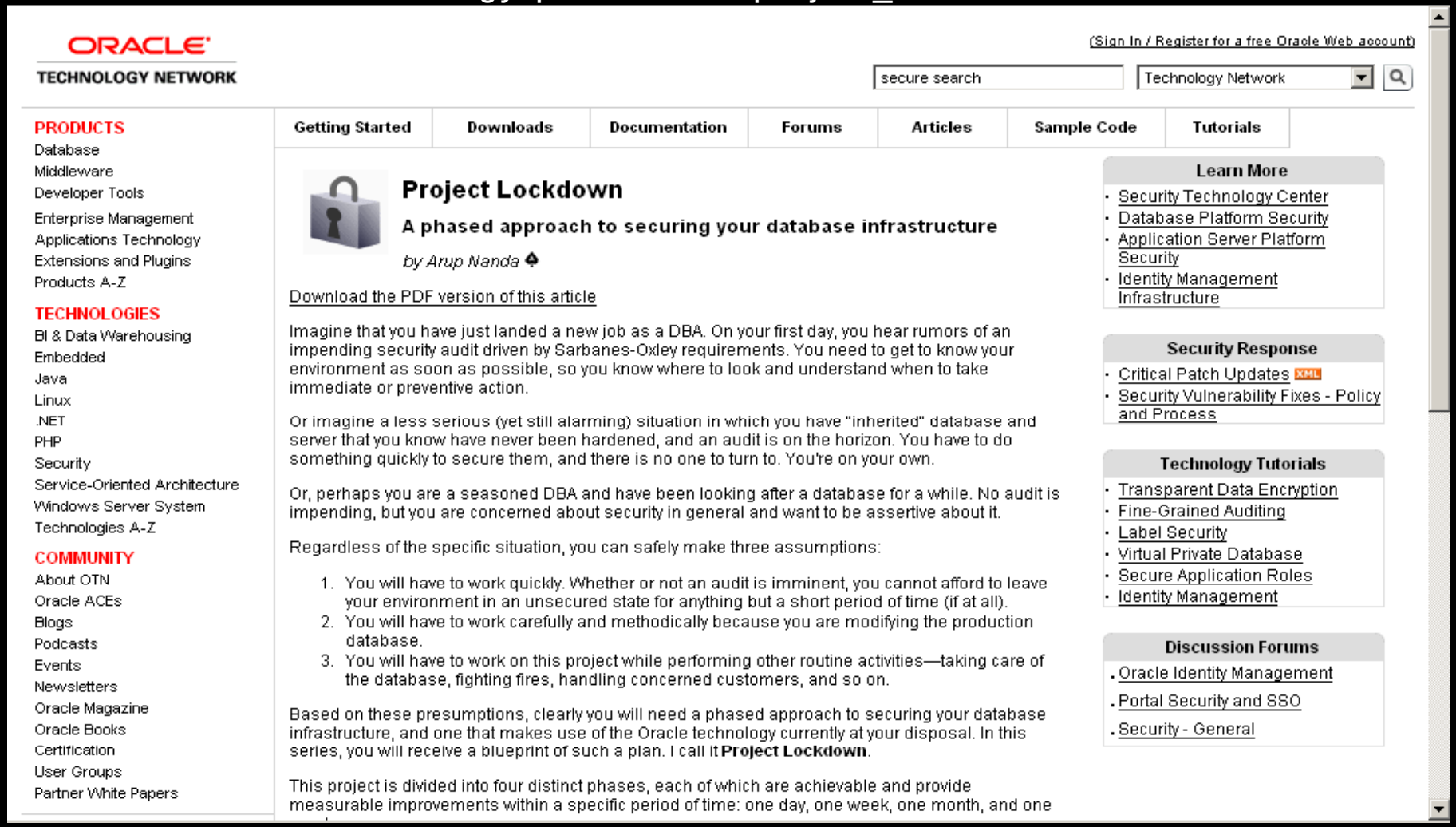
Attacking via DB-Clients - I

- Very often the easiest way to hack a protected Oracle database is via the workstation of the DBA / Developer
- Easiest attack for all databases
- No database account or password necessary
- Potential attack vector
  - **USB U3 stick**
  - **Browser exploits**
  - **Physical modification of the workstation**
  - **...**

Source: Alexander Kornbrust: Red Database Security, GmbH

Project Lockdown

www.oracle.com/technology/pub/articles/project_lockdown/index.html



ORACLE
TECHNOLOGY NETWORK

(Sign In / Register for a free Oracle Web account)

secure search | Technology Network

PRODUCTS
Database
Middleware
Developer Tools
Enterprise Management
Applications Technology
Extensions and Plugins
Products A-Z

TECHNOLOGIES
BI & Data Warehousing
Embedded
Java
Linux
.NET
PHP
Security
Service-Oriented Architecture
Windows Server System
Technologies A-Z

COMMUNITY
About OTN
Oracle ACEs
Blogs
Podcasts
Events
Newsletters
Oracle Magazine
Oracle Books
Certification
User Groups
Partner White Papers

Getting Started | Downloads | Documentation | Forums | Articles | Sample Code | Tutorials

Project Lockdown

A phased approach to securing your database infrastructure

by Arup Nanda

Download the PDF version of this article

Imagine that you have just landed a new job as a DBA. On your first day, you hear rumors of an impending security audit driven by Sarbanes-Oxley requirements. You need to get to know your environment as soon as possible, so you know where to look and understand when to take immediate or preventive action.

Or imagine a less serious (yet still alarming) situation in which you have "inherited" database and server that you know have never been hardened, and an audit is on the horizon. You have to do something quickly to secure them, and there is no one to turn to. You're on your own.

Or, perhaps you are a seasoned DBA and have been looking after a database for a while. No audit is impending, but you are concerned about security in general and want to be assertive about it.

Regardless of the specific situation, you can safely make three assumptions:

1. You will have to work quickly. Whether or not an audit is imminent, you cannot afford to leave your environment in an unsecured state for anything but a short period of time (if at all).
2. You will have to work carefully and methodically because you are modifying the production database.
3. You will have to work on this project while performing other routine activities—taking care of the database, fighting fires, handling concerned customers, and so on.

Based on these presumptions, clearly you will need a phased approach to securing your database infrastructure, and one that makes use of the Oracle technology currently at your disposal. In this series, you will receive a blueprint of such a plan. I call it **Project Lockdown**.

This project is divided into four distinct phases, each of which are achievable and provide measurable improvements within a specific period of time: one day, one week, one month, and one

Learn More
- Security Technology Center
- Database Platform Security
- Application Server Platform Security
- Identity Management Infrastructure

Security Response
- Critical Patch Updates XML
- Security Vulnerability Fixes - Policy and Process

Technology Tutorials
- Transparent Data Encryption
- Fine-Grained Auditing
- Label Security
- Virtual Private Database
- Secure Application Roles
- Identity Management

Discussion Forums
- Oracle Identity Management
- Portal Security and SSO
- Security - General

Default Passwords

```
SQL> SELECT d.username, u.account_status
  2  FROM dba_users_with_defpwd d, dba_users u
  3  WHERE d.username = u.username
  4  ORDER BY 2,1;

USERNAME                       ACCOUNT_STATUS
------------------------------ ----------------
CTXSYS                         EXPIRED & LOCKED
DIP                            EXPIRED & LOCKED
EXFSYS                         EXPIRED & LOCKED
MDDATA                         EXPIRED & LOCKED
MDSYS                          EXPIRED & LOCKED
ORDPLUGINS                     EXPIRED & LOCKED
ORDSYS                         EXPIRED & LOCKED
OUTLN                          EXPIRED & LOCKED
SI_INFORMTN_SCHEMA             EXPIRED & LOCKED
WK_TEST                        EXPIRED & LOCKED
WMSYS                          EXPIRED & LOCKED
XDB                            EXPIRED & LOCKED
HR                             OPEN
OE                             OPEN
SCOTT                          OPEN
SH                             OPEN

16 rows selected.

SQL>
```

One of Oracle's Best Error Message

ORA-28365: wallet is not open

Cause: The security module wallet has not been opened.

Action: Open the wallet.

Discussion

What Management Is Hearing

Sarbanes Oxley Act (SOX, SarbOx)

- Passed by Congress on January 23rd, 2002 and signed by President Bush on July 30th, 2002
- Industrial engine manufacturing FUD

SOX Requirements

Section 302

Requires the Management to:

- Disclose all controls
- Certify that the controls are designed and implemented in management's supervision
- Disclose all changes to controls in quarterly statements
- Disclosure about the purpose of change – if the change was due to a material weakness

Section 404

Requires the Management to annually:

- State the framework used to conduct assessment of the effectiveness of the company's internal controls
- Conduct an assessment of the effectiveness of the company's internal controls and procedures for financial reporting

Requires the independent external Auditor to provide two opinions:

- An assessment of management's evaluation of the company's internal control over financial reporting
- Its own independent evaluation based on its review and testing of the company's internal control over financial reporting

HIPAA Requirements

- Give patients access to their information and ability to request change
- Restrict access to a patients information to others
- Restrict disclosure of protected information to minimum required for healthcare treatments & transitions
- Establish controls for access to records by researchers
- Assign a privacy officer that will administer the privacy policy programs and enforce compliance
- Maintain confidentiality, integrity and availability of healthcare information

Electronic Storage of Broker-Dealer Records

- Electronic records must be preserved exclusively in a non-rewriteable and non-erasable format
- Broker-dealers may employ a storage system that prevents alteration or erasure of the records for their required retention period.

FACTA Requirements (1 of 2)

- Fair Credit Reporting Act
- Required as of June 1, 2005
- FACTA provisions consumer reporting agencies and any business that uses a consumer report must adopt procedures for proper document disposal.

FACTA Requirements (2 of 2)

- The FTC, the federal banking agencies, and the National Credit Union Administration (NCUA) have published final regulations to implement the new FACTA Disposal Rule. The FTC's disposal rule applies to consumer reporting agencies as well as individuals and any sized business that uses consumer reports. The FTC lists the following as among those that must comply with the rule:
  - Lenders
  - Insurers
  - Employers
  - Landlords
  - Government agencies
  - Mortgage brokers
  - Automobile dealers
  - Attorneys and private investigators
  - Debt collectors

Gramm-Leach-Bliley Requirements (GLB)

- Establish an information security program to assess and control risks to customer NPI.
- Protect against any anticipated threats or hazards to the security or integrity of such records
- Protect against unauthorized access to or use of such records that could result in harm or inconvenience to any customer
- Install access controls on customer information systems, including controls to authenticate and permit access only to authorized individuals as well as prevent employees from providing customer information to unauthorized individuals

PCI Requirements (1 of 2)

- Payment Card Industry Data Security Standard
- Required by September 2007 if your organization accepts credit cards
- The TJX Companies breach
  - The TJX Companies Inc. breach is the largest known data theft to date. Hackers invaded the TJX systems resulting in at least 45.7 million credit and debit card numbers stolen over an 18-month period. As well as the stolen personal data, including driver's license numbers of another 455,000 customers who returned merchandise without receipts.

PCI Requirements (2 of 2)

- Requirement 2.2.4 - Remove all unnecessary functionality
- Requirement 2.3 - Encrypt all non-console administrative access
- Requirement 4 - Encrypt transmission of cardholder data across open, public networks
- Requirement 6 - Develop and maintain secure systems and applications
- Requirement 6.5.1 - Unvalidated Input
- Requirement 6.5.2 - Broken Access Control
- Requirement 6.5.3 - Broken Authentication and Session Management
- Requirement 6.5.4 - Cross Site Scripting (XSS) Flaws
- Requirement 6.5.5 - Buffer Overflows
- Requirement 6.5.6 - Injection Flaws
- Requirement 6.5.7 - Improper Error Handling
- Requirement 6.5.8 - Insecure Storage
- Requirement 6.5.9 - Denial of Service
- Requirement 6.5.10 - Insecure Configuration Management

PIPEDA Requirements (1 of 2)

- The PCI DSS is a multifaceted security standard that includes requirements for security management, policies, procedures, network architecture, software design and other critical protective measures.

PIPEDA Requirements (2 of 2)

- Build and Maintain a Secure Network
  - **Install and maintain a firewall configuration to protect cardholder data**
  - **Do not use vendor-supplied defaults for system passwords and other security parameters**
- Protect Cardholder Data
  - **Protect stored cardholder data**
  - **Encrypt transmission of cardholder data across open, public networks**
- Maintain a Vulnerability Management Program
  - **Use and regularly update anti-virus software**
  - **Develop and maintain secure systems and applications**
- Implement Strong Access Control Measures
  - **Restrict access to cardholder data by business need-to-know**
  - **Assign a unique ID to each person with computer access**
  - **Restrict physical access to cardholder data**
- Regularly Monitor and Test Networks
  - **Track and monitor all access to network resources and cardholder data**
  - **Regularly test security systems and processes**
- Maintain an Information Security Policy
  - **Maintain a policy that addresses information security**

Basel II Requirements

- To be in compliance with Basel II, a banking institution must deliver appropriate reporting of operational risk exposures and loss data to its board of directors and senior management. These reports must:
  - Address both company-wide and line of business results.
  - Summarize operational risk exposure, loss experience, relevant business environment and internal control assessments.
  - Identify and assess the operational risk inherent in all material products, activities, processes and systems.

The Cost

- A study conducted by Ponemon Institute estimates an average cost of $14 million per security breach incident, with costs ranging as high as $50 million.
  - Study covered 14 separate incidents, encompassing 1.4 million compromised data records and an estimated total of $200 million in resulting losses
  - Total cost estimates include the actual cost of internal investigations, outside legal defense fees, notification and call center costs, PR and investor relations efforts, discounted services offered, lost employee productivity and the effect of lost customers.

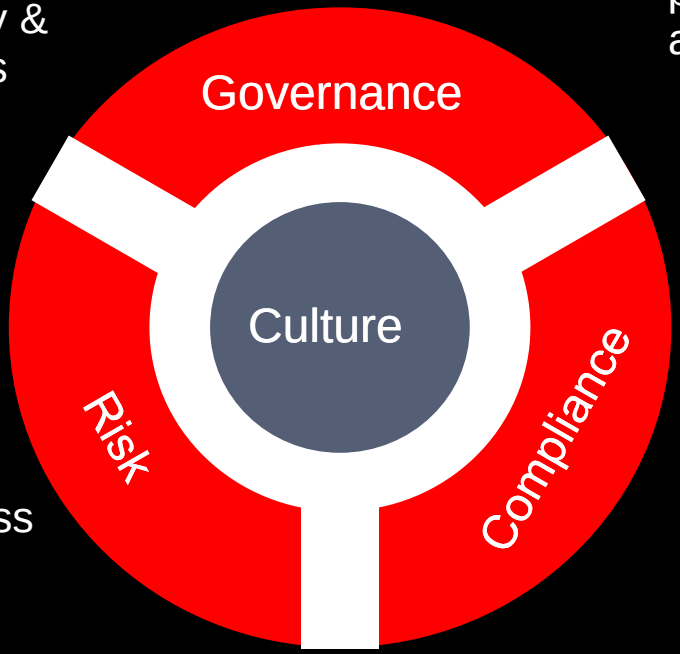
Governance, Risk, and Compliance (GRC)

Governance

- Set and evaluate performance against objectives
- Authorize business strategy & model to achieve objectives

Culture

- Establish organizational climate and mindset that promote trust, integrity, & accountability



Risk Management

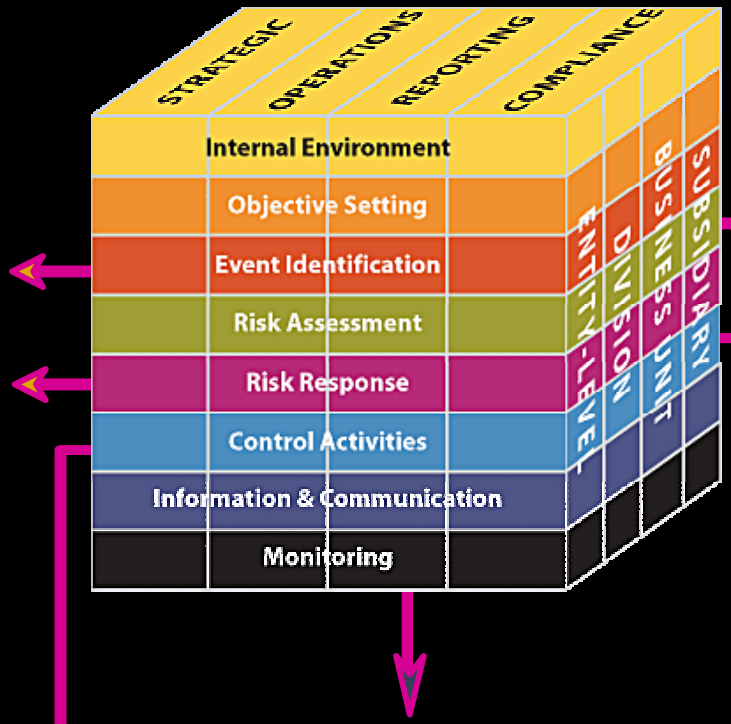
- Identify, assess, and address potential obstacles to achieving objectives
- Identify / address violation of mandated and voluntary boundaries

Compliance

- Encourage / require compliance with established policies and boundaries
- Detect non-compliance and respond accordingly

Source: Open Compliance and Ethics Group

COSO Cube & Compliance Reference Model



Event Identification

- Exception thresholds

Risk Response

- Corrective Workflows

Information & Communication

- Approval Workflows
- Attestation Workflows
- Exception Notifications
- Delegated Administration
- Automated Provisioning
- Password Reset

Monitoring

- Continuous Exception Detection & Monitoring
- Periodic Reports and Attestations

Risk Assessment

- Model Risk assessment around resources with sensitive data – financial, ePHI, NPI
  - Electronic Transactions
  - Application, Application Server, DB, OS
- Predictive Risk Analysis

Control Activities

- Entitlement Policies: RBAC, ABAC, SoD
- Strong Authentication
- Exception Detection & Remediation
- Employee termination
- Policy Retrofits & Revocations

- Committee Of Sponsoring Organizations of the Treadway Commission
- Most accepted framework for financial controls

Expanding Regulatory Requirements

Map View: Robinson Projection

AMERICAS

- HIPAA
- FDA CFR 21 Part 11
- OMB Circular A-123
- SEC and DoD Records Retention
- USA PATRIOT Act
- Gramm-Leach-Bliley Act
- Federal Sentencing Guidelines
- Foreign Corrupt Practices Act
- Market Instruments 52 (Canada)

EMEA

- EU Privacy Directives
- UK Companies Law
- Restriction of Hazardous Substances (ROHS/WEE)

APAC

- J-SOX (Japan)
- CLERP 9: Audit Reform and Corporate Disclosure Act (Australia)
- Stock Exchange of Thailand Code on Corporate Governance

GLOBAL

- International Accounting Standards
- Basel II (Global Banking)
- OECD Guidelines on Corporate Governance

What Management Wants

- You need to know who did what and when
- You need to know who accessed what data both generally and under specified conditions
- You need to protect the audit trail from tampering and be able to prove it is authentic
- Adequately guard against security threats without choking the business

What Auditors Want

- Separation of duties
- Reporting
- Notification
- Proven audit data integrity
- Internal Controls
  - Effectiveness and efficiency of operations
  - Reliability of financial reporting
  - Compliance with laws and regulations

What IT Wants

- Performance and scalability
- Minimal constraints while getting the job done
- Evenings and weekends off

Discussion

Traditional Auditing

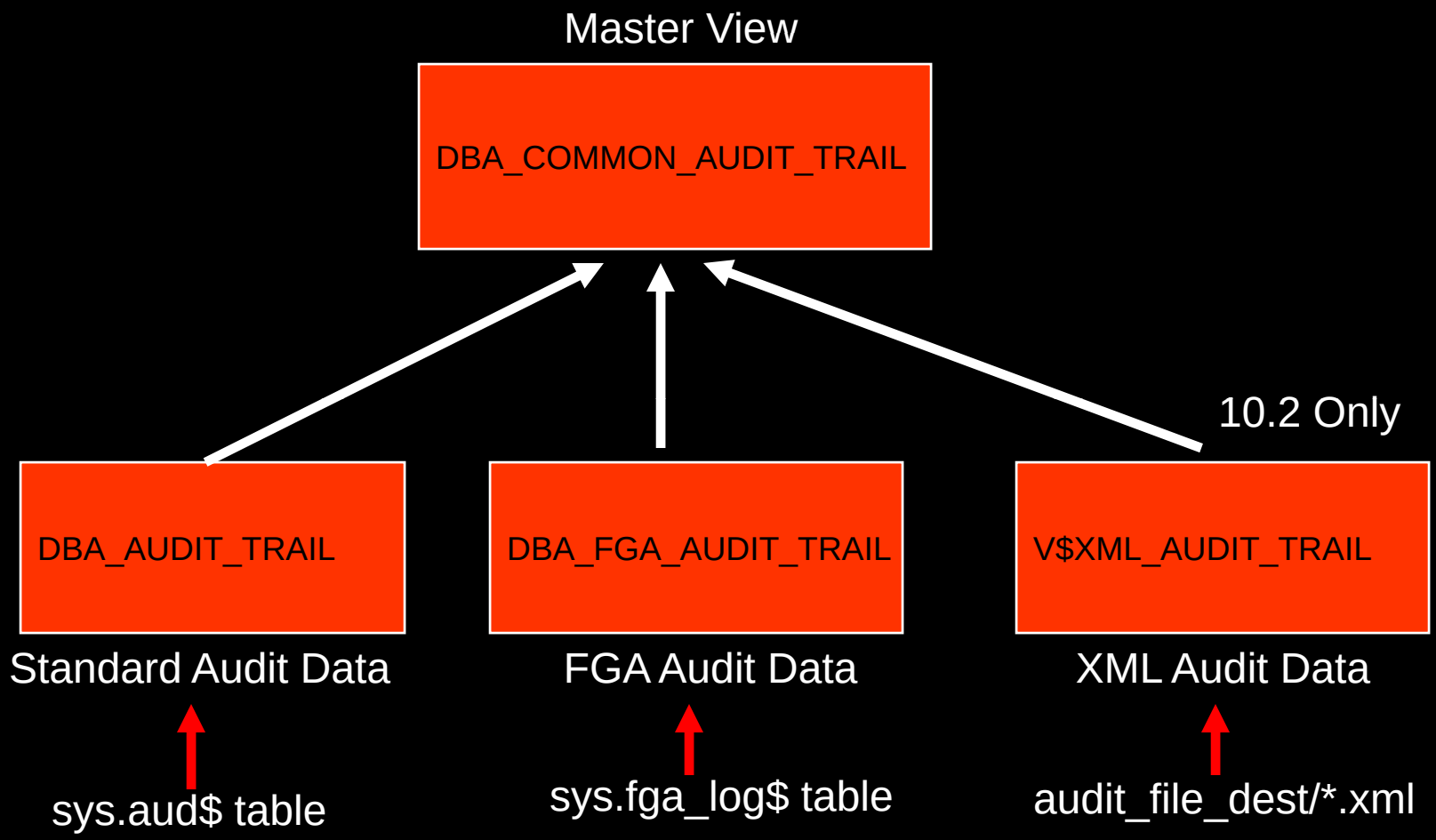
Traditional Auditing Methods

- Standard Auditing
- Fine Grained Auditing
- Event Triggers
- Application Auditing
- Log Miner
- Data Vault / Audit Vault

Standard Auditing

```
SQL> select name, value from gv$parameter
  2  where name like '%audit%';

NAME                           VALUE
------------------------------ ------------------------------
audit_sys_operations           FALSE
audit_file_dest                C:\ORACLE\ADMIN\ORABASE\ADUMP
audit_trail                    DB

SQL>
```

Database Auditing



Fine Grained Auditing (FGA)

- Best solution for some problems
- No overhead when conditions are not met
- No overhead when policy exists on different statement types
- XML auditing performs better than DB_EXTENDED
- Still need standard auditing for coverage of areas not provided by FGA

Discussion

Audit Vault Concepts and Architecture

Why Audit Vault?

- Comply with the law
- Protect the organization from insiders
- Proof for auditors
- Protection from lawsuits
- Mitigates many security risks

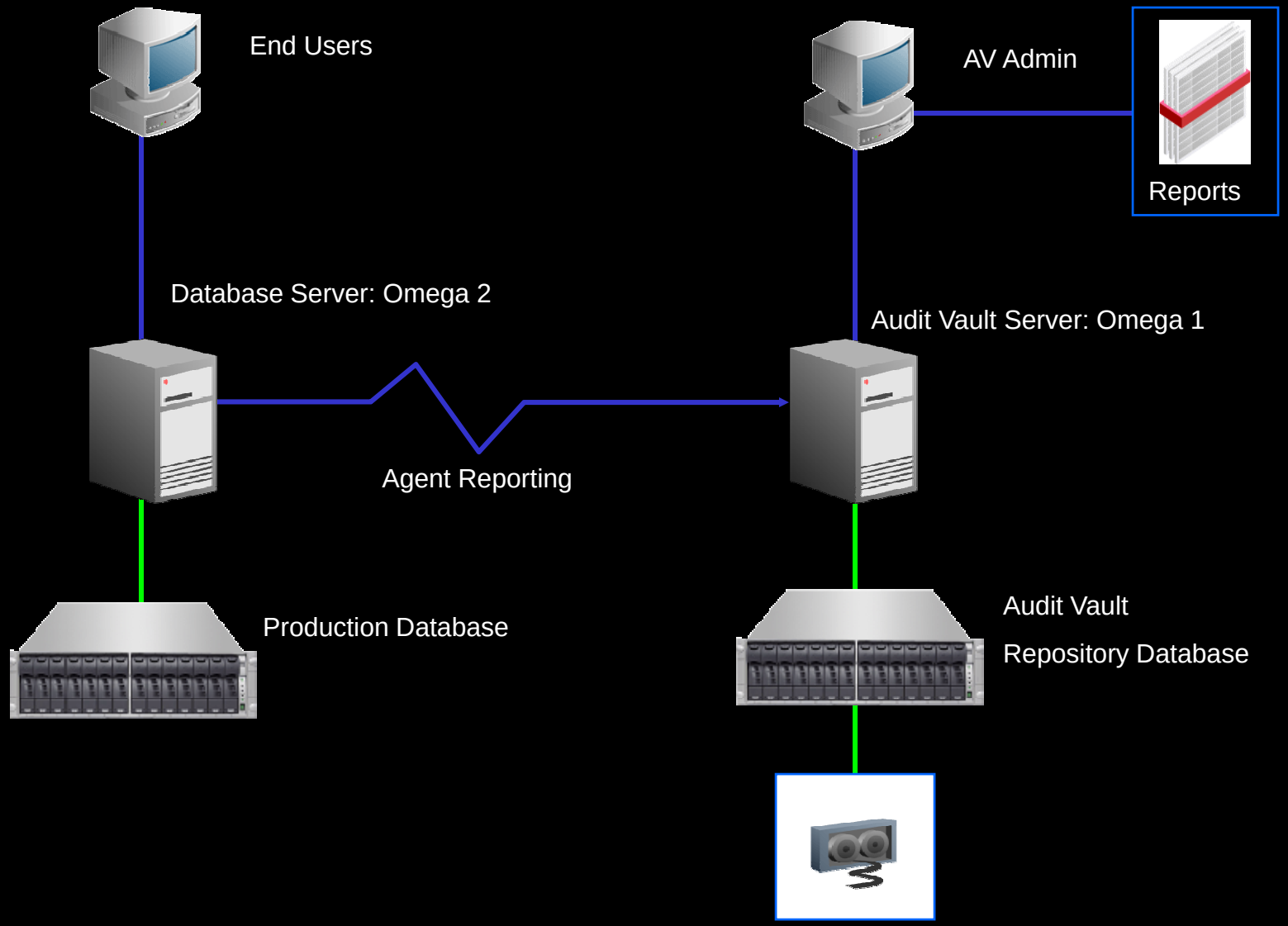
What is Audit Vault?

- A secure tamper-proof Oracle database
- A consolidated repository for audit logs from across the enterprise
- Protects audit data from modification and tampering
- Consolidates audit trails by mapping audit data to a common audit format
- Centralized audit policy management
- Enables analysis of audit data including timely detection of policy violations
- Report from a single repository

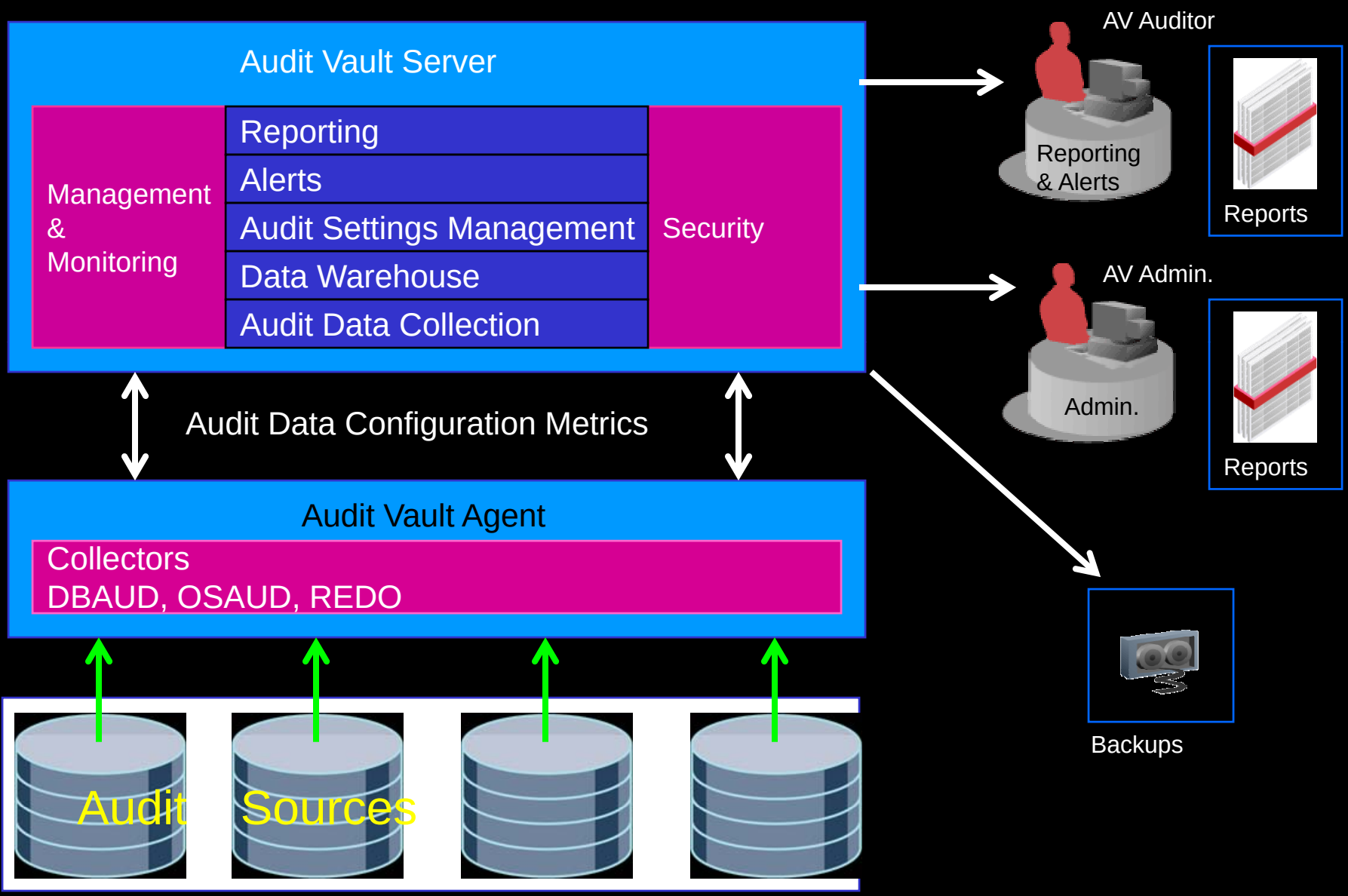
Audit Vault's History

- 10gR2
  - Released August '06

Audit Vault Architecture (50,000 ft.)



Audit Vault Architecture (500 ft.)



Audit Vault Server

- Audit Event Repository
- Audit Vault Console
- Audit Vault Services
  - Consolidating and storing of audit data
  - Creating and managing alerts
  - Managing and monitoring collectors
  - Defining and configuring source information
  - Creating and manging reports
  - Reporting
  - Audit policy management

Audit Vault Agents

- Oracle Container for Java (OC4J)
- Instant Client components
- Audit Vault management services
- Audit data collectors for Oracle Database
  - Operating system audit log collection (OSAUD)
    - Requires o/s file system access
  - Database audit log collection (DBAUD)
  - Redo log collection (REDO)
- Receives configuration information using a communication channel based on OCI (AQ)
  - Can be secured with X.509 certificates

Interfaces and Administrator Access

- Audit Vault Configuration Assistant (AVCA)
- Audit Vault Control (AVCTL)
- Audit Vault Oracle Database (AVORCLDB)

Audit Vault Oracle Database

```
Oracle DB Setup for Audit Vault
-------------------------------
  Usage :
    avorcldb help
    avorcldb <command> -help
    avorcldb <command> <arguments>

Source setup commands
    verify
          -src <host:port:service> -srcusr <usr>/<pwd>
          -colltype [OSAUD,DBAUD,REDO,EVTLOG,ALL]

    add_source
          -src <host:port:service> -srcusr <usr>/<pwd> -avsrcusr <usr>
          [-srcname <srcname>] [-desc <desc>] [-agentname <agentname>]

    alter_source
          -srcname <srcname> [attrname=value]+

    drop_source
          -srcname <srcname>
```

Audit Vault Oracle Database

Collector setup commands

```
add_collector
      -srcname <srcname> -srcusr <usr>/<pwd> -agentname <agentname>
      -colltype [OSAUD|DBAUD|REDO|EVTLOG] [-collname <collname>]
      [-desc <desc>] [-avsrcusr <usr>/<pwd>] [-av <host:port:service>]
      [-instname <instname>]

alter_collector
      -srcname <srcname> -collname <collname> [attrname=value]+

drop_collector
      -srcname <srcname> -collname <collname>
```

Compared with Competitive Solutions

- Network Traffic Monitor
  - Misses server-side code
  - Impacts every statement not on DB server
- Database Transaction Monitoring
  - More overhead (CPU)
  - Captures all activity

Compared with Competitive Solutions

- Log Readers
  - Platform dependencies
  - Select Statements not audited
- Application Auditing
  - Non-Application Access unmonitored
  - Auditing is expressed in application transactions not database transactions

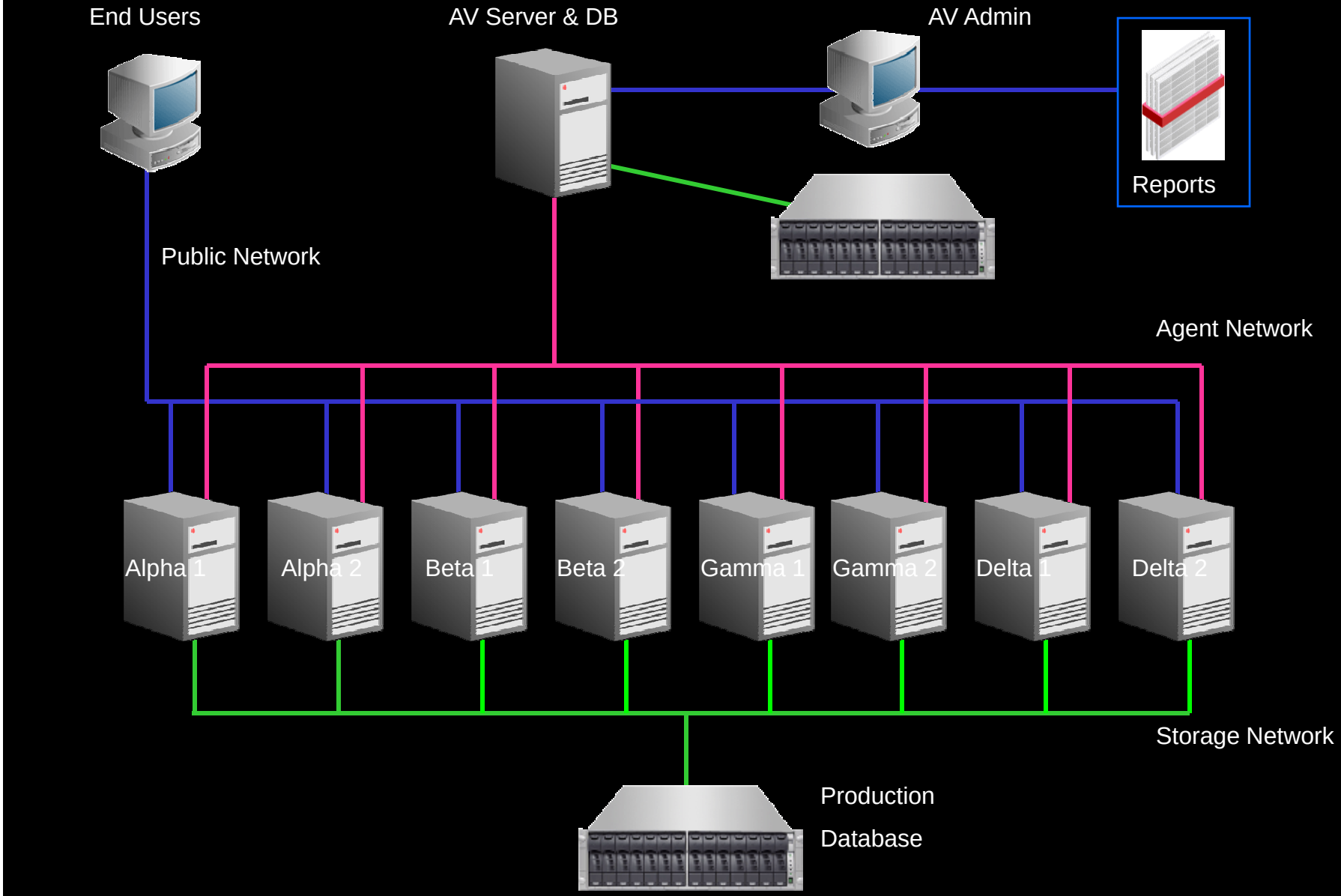
Only One Piece of the Puzzle

- Profiles
  - password complexity & expiration
- Roles
- System Privileges
  - Minimum required
- Object Privileges
  - Minimum required
- Database Auditing
- Fine Grained Auditing
- Fine Grained Access Control
- Identity Management

Lab One

Network Configuration

PSOUG Lab


End Users
AV Server & DB
AV Admin
Reports
Public Network
Agent Network
Alpha 1
Alpha 2
Beta 1
Beta 2
Gamma 1
Gamma 2
Delta 1
Delta 2
Storage Network
Production
Database

Lab Two

Operating System Installation and Configuration

Hardware and Operating System Requirements

- The hardware can be different for the primary and standby databases
- The operating system and platform architecture for the primary and standby databases must be the same
- The operating system for the primary and standby databases must be the same, but the operating system releases can be different
- If all databases are on the same system, verify that the OS allows you to mount more than one database with the same name

Server Requirements

Available RAM	Swap Space Required
1 – 2 GB	1.5X amount of RAM
2 – 8 GB	Equal to amount of RAM
More than 8 GB	0.75X amount of RAM

- 1.4GB disk space for Audit Vault Server software files in the Oracle base directory
- 700MB of additional disk space for the Audit Vault database files in the Oracle base directory

Agent Requirements

- Less than 500MB of disk
- If you have a target database installed you have sufficient resources

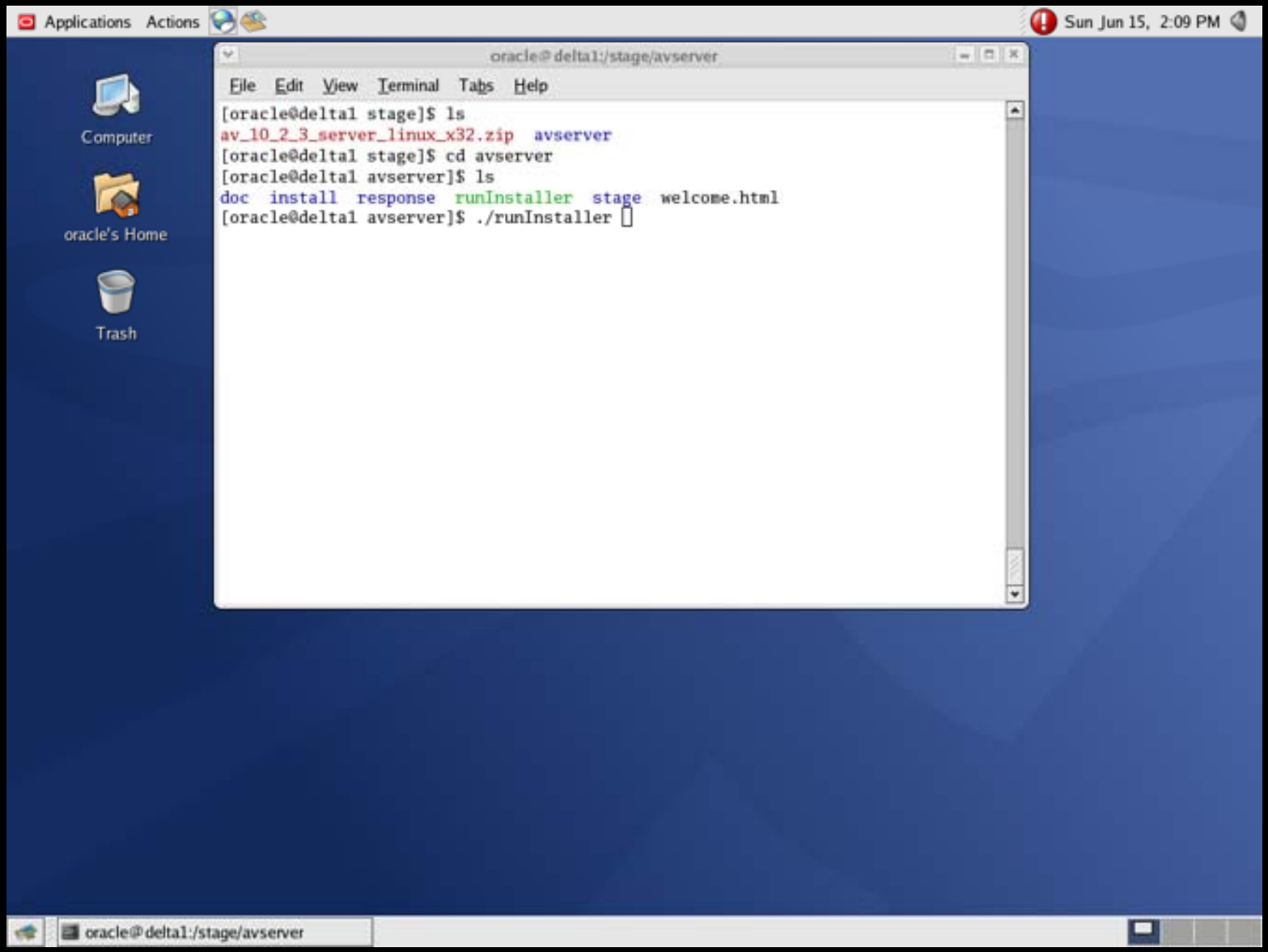
Storage

- May be installed on top of ASM
- May be installed (Advanced install) on RAC

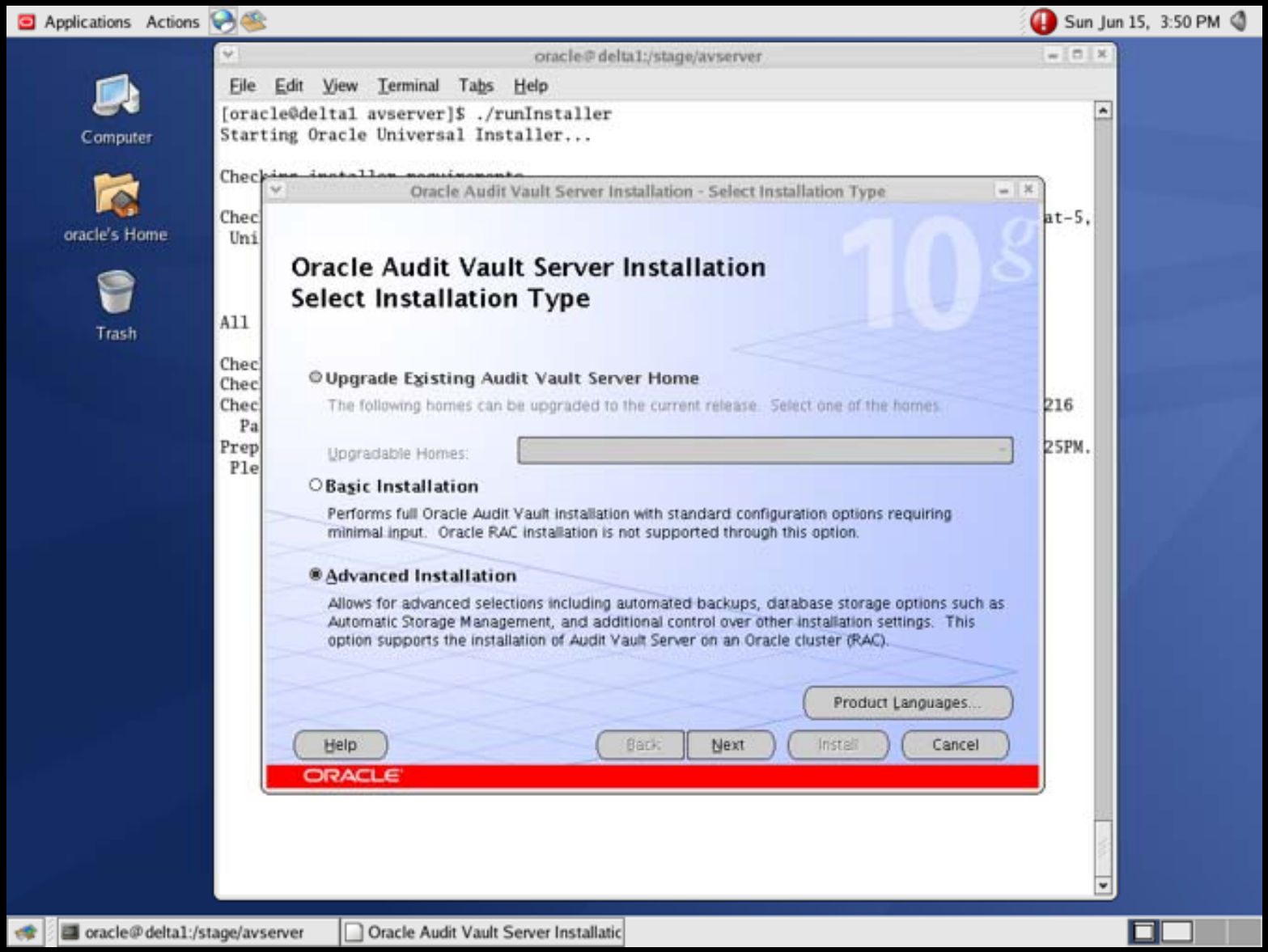
SQLNET.ORA

```
# begining of Audit Vault configuration

SQLNET.AUTHENTICATION_SERVICES= (BEQ, TCPS)
SSL_VERSION = 0
SSL_CLIENT_AUTHENTICATION = TRUE
SQLNET.WALLET_OVERRIDE = TRUE
WALLET_LOCATION =
  (SOURCE = (METHOD = FILE)
  (METHOD_DATA = (DIRECTORY = /apps/oracle/product/10.2.2/av_1/network/admin/avwallet)))

# end of Audit Vault configuration
```

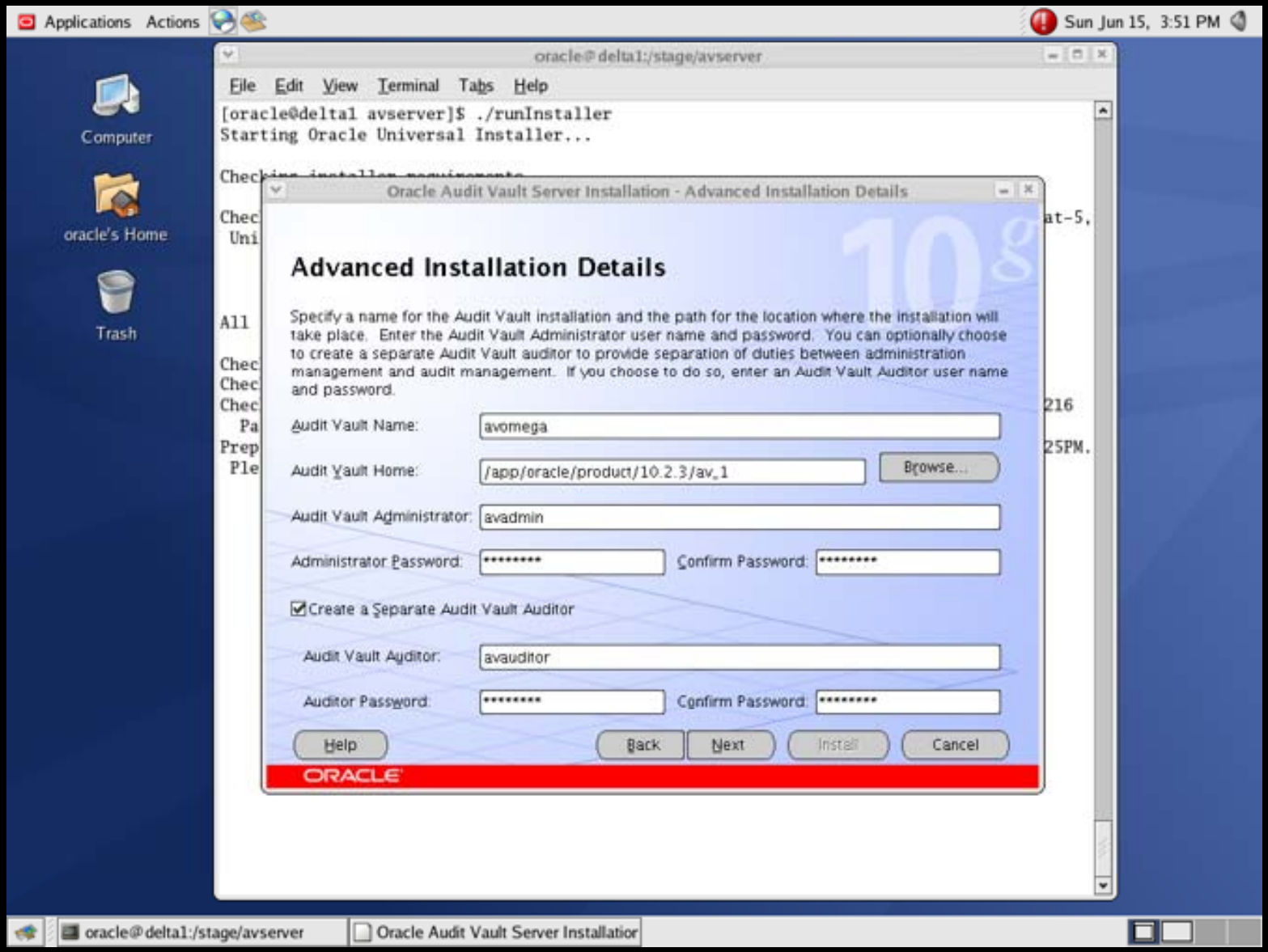
Server Install Step 1



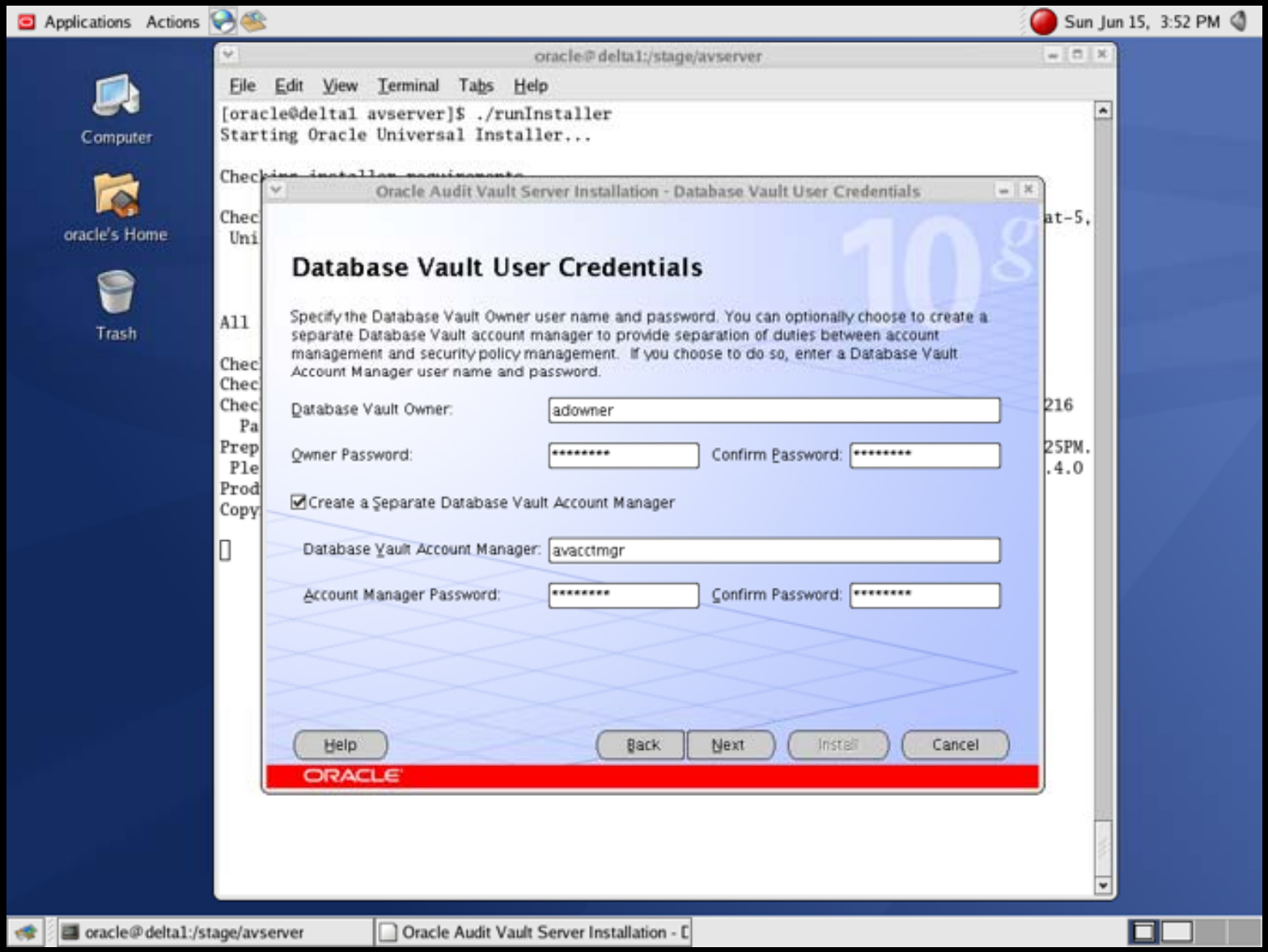
Server Install Step 2



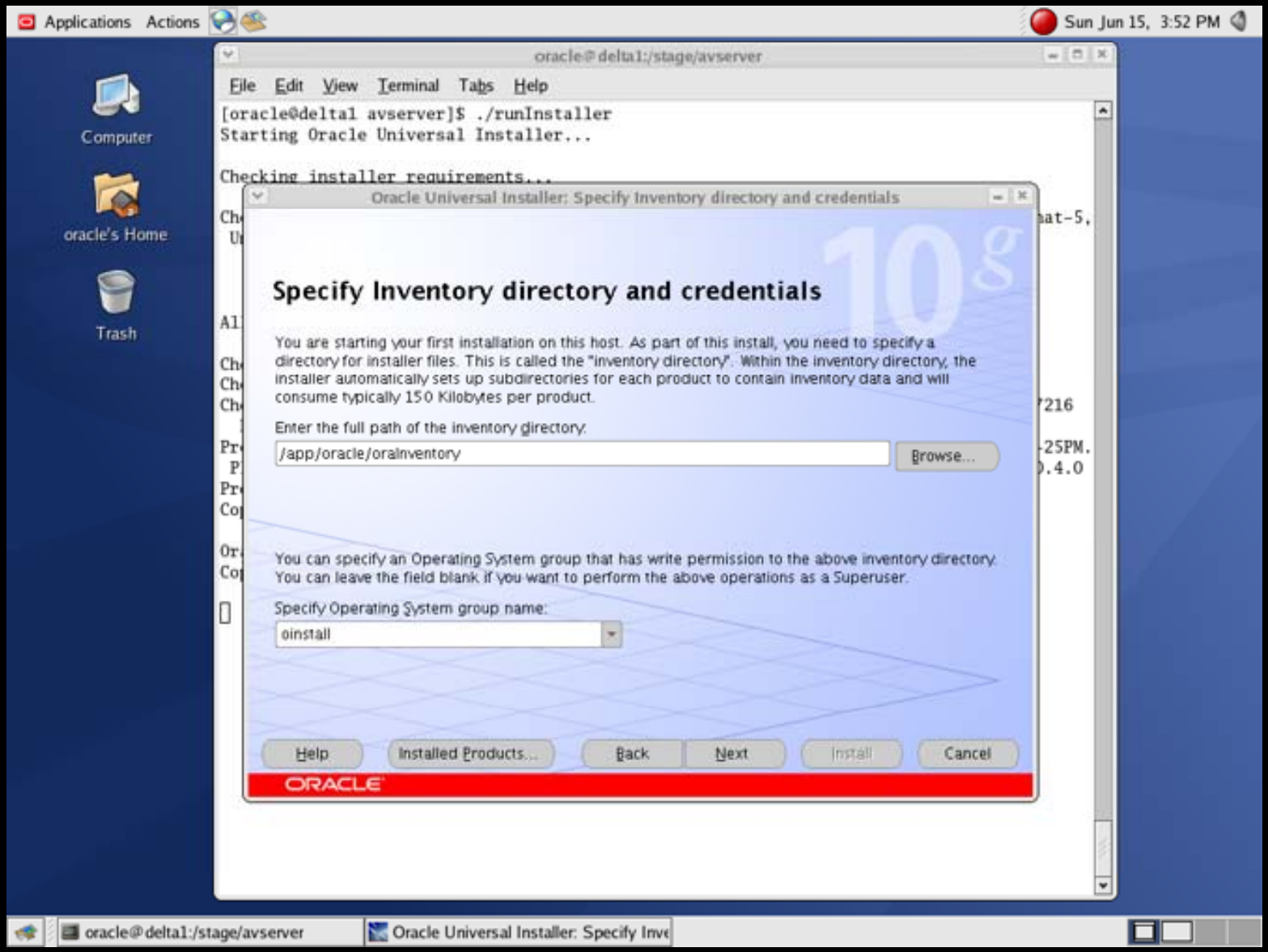
Server Install Step 3



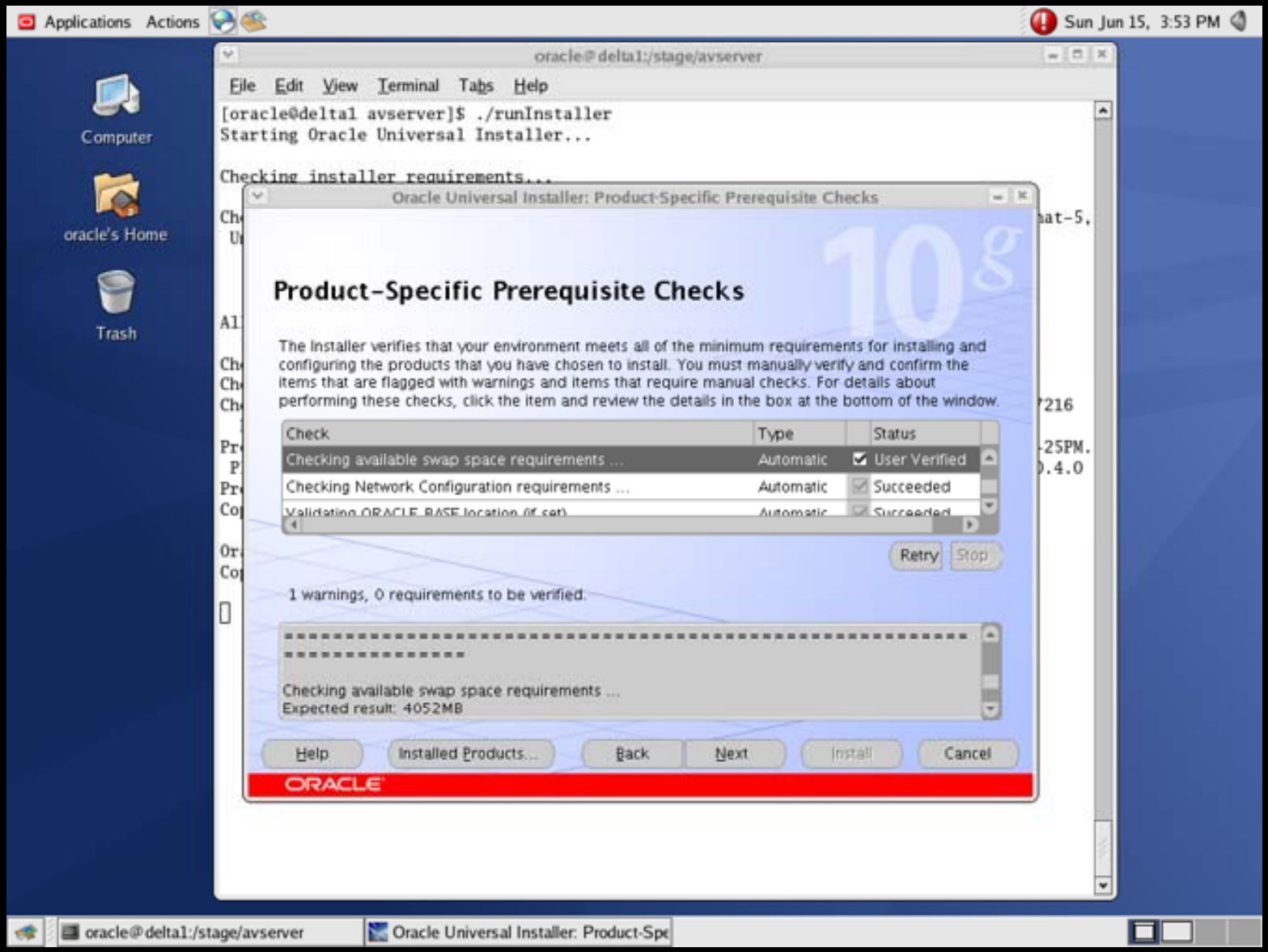
Server Install Step 4



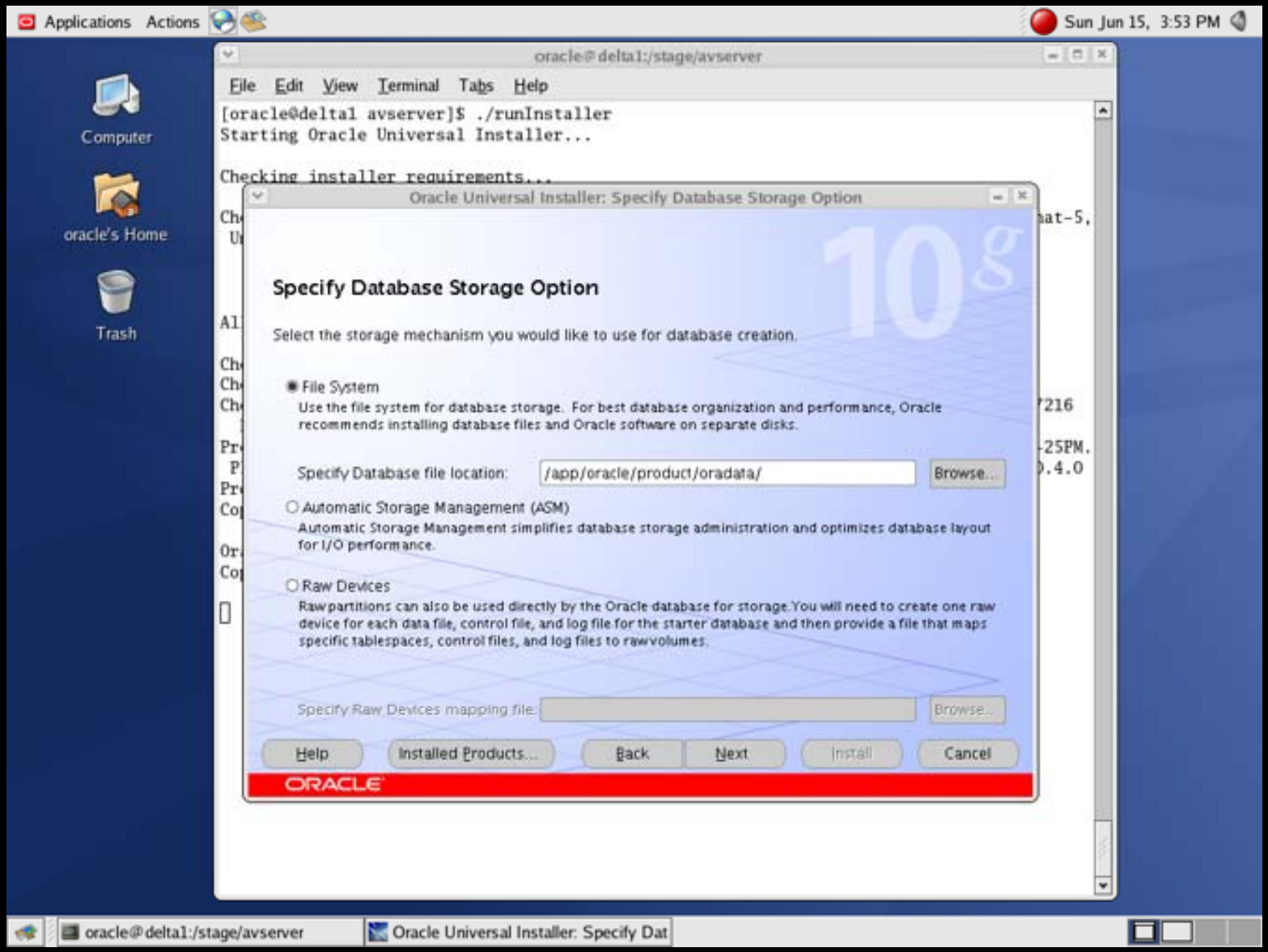
Server Install Step 5



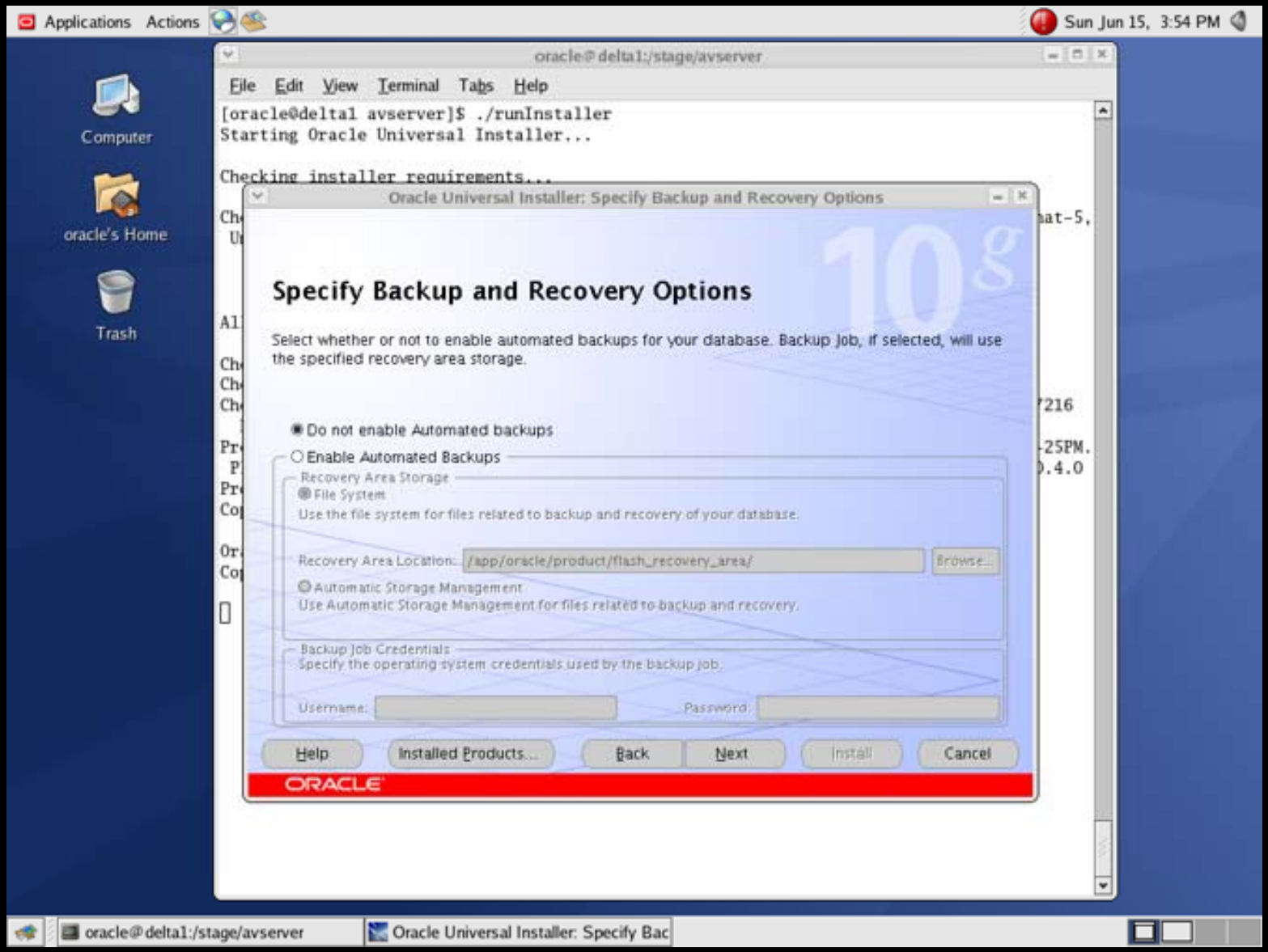
Server Install Step 6



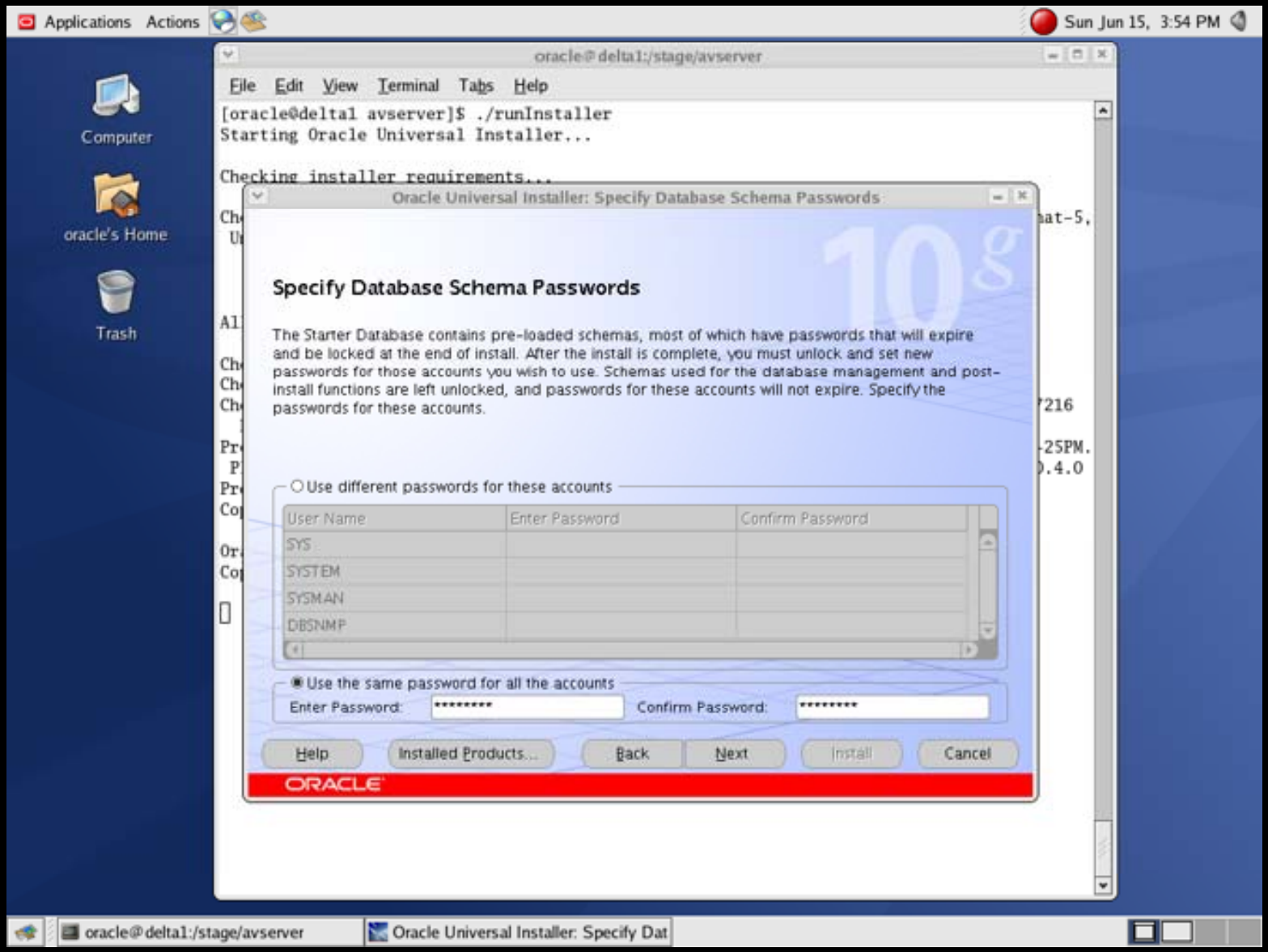
Server Install Step 7



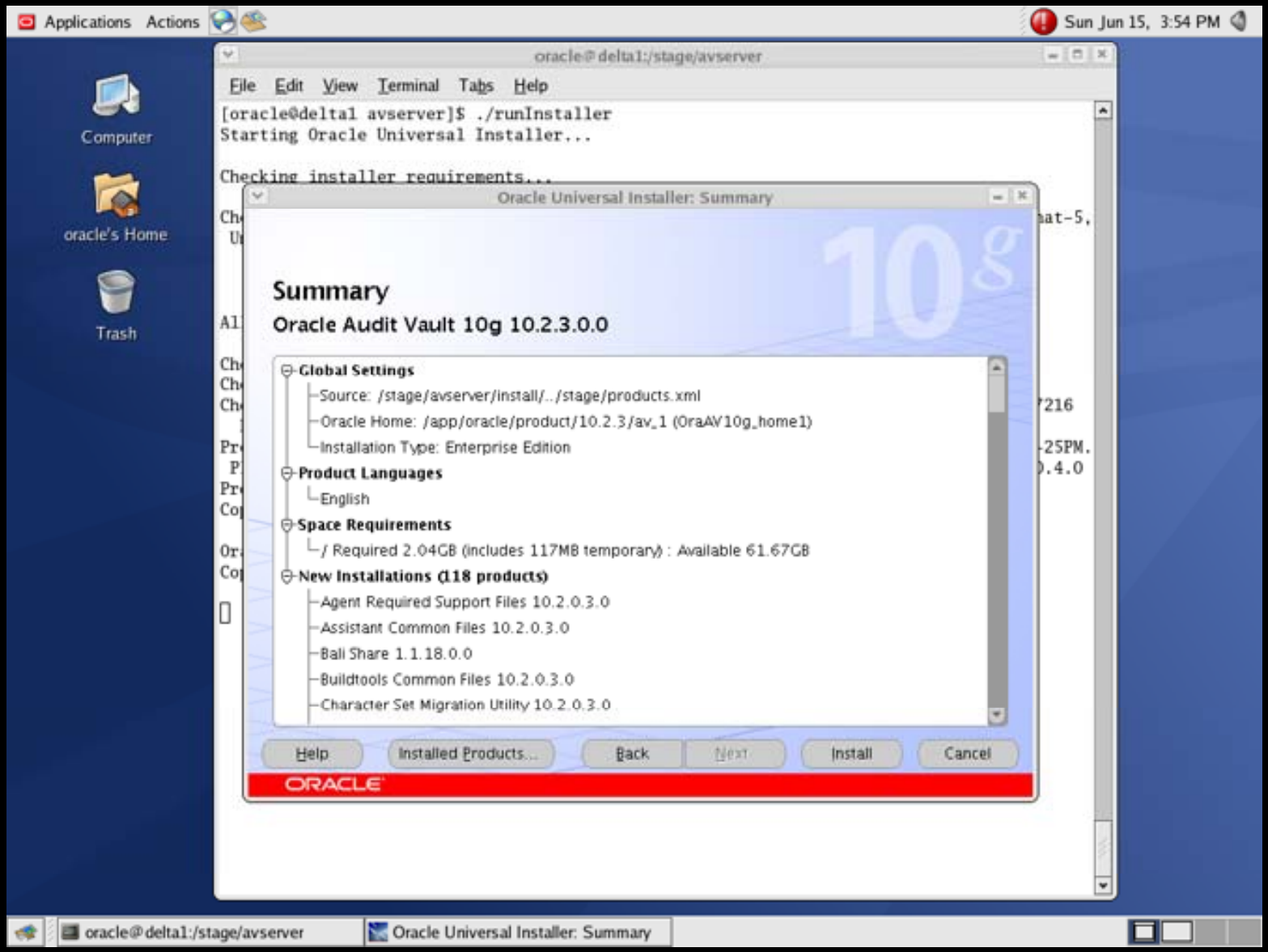
Server Install Step 8



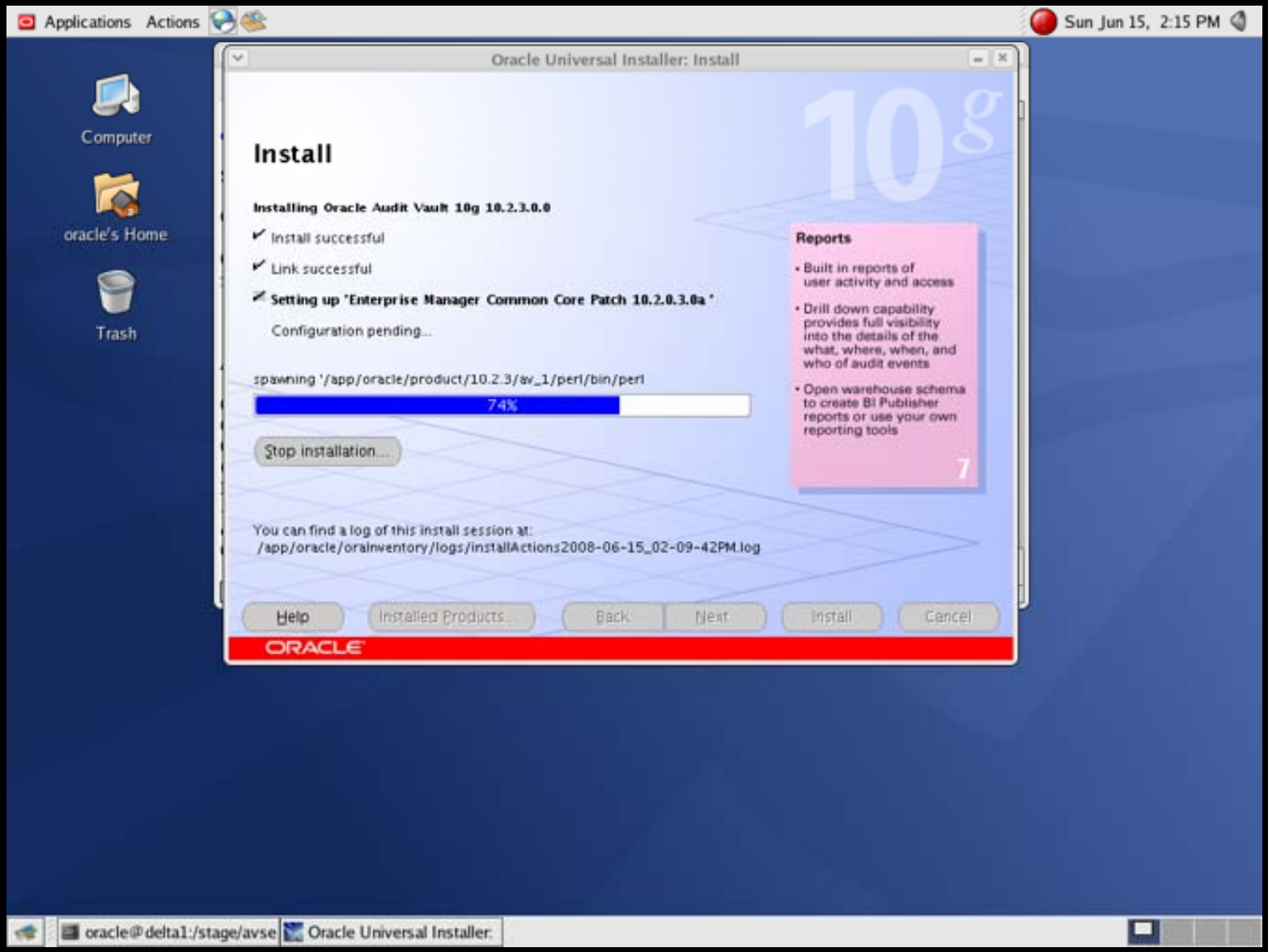
Server Install Step 9



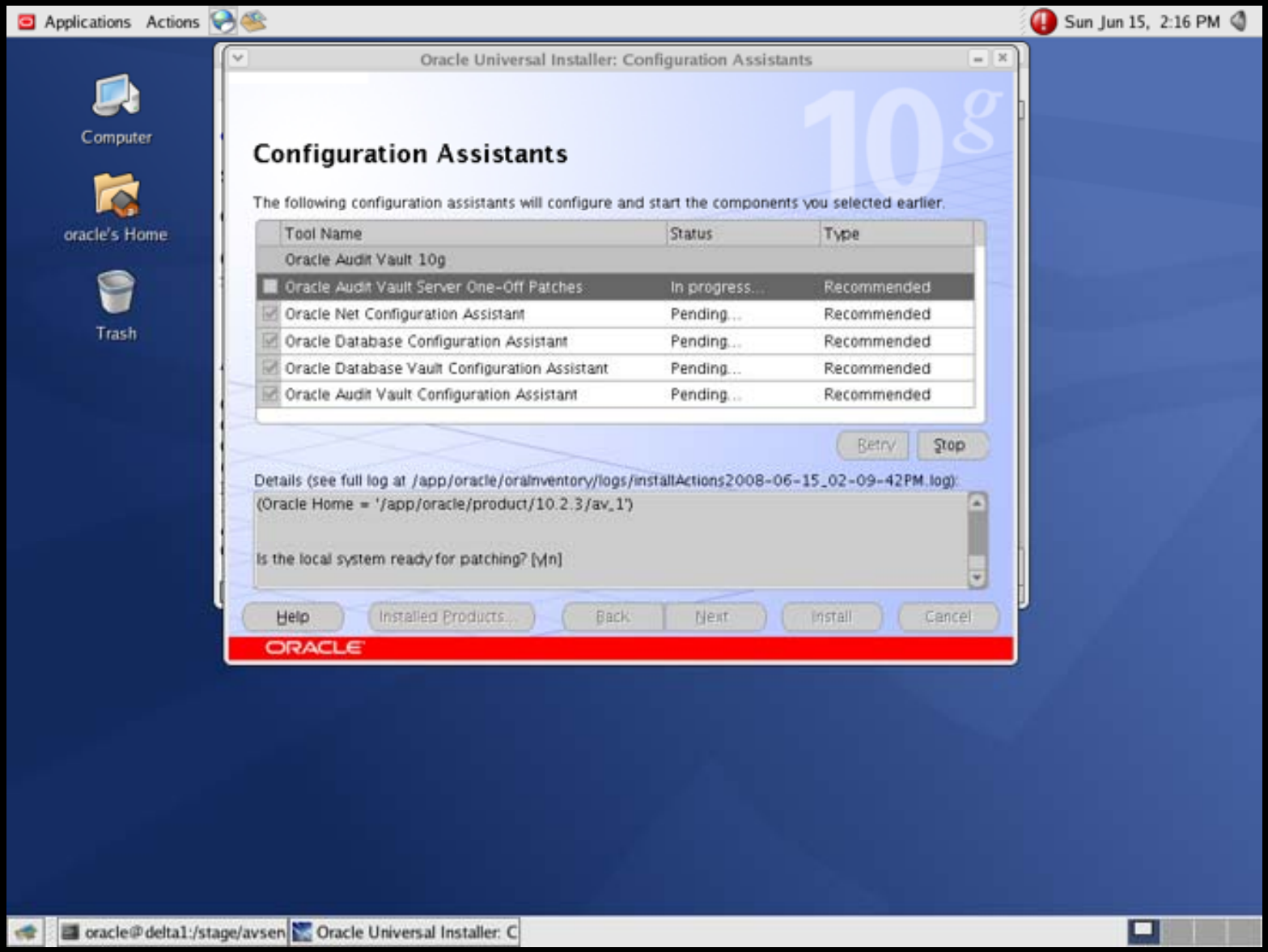
Server Install Step 10



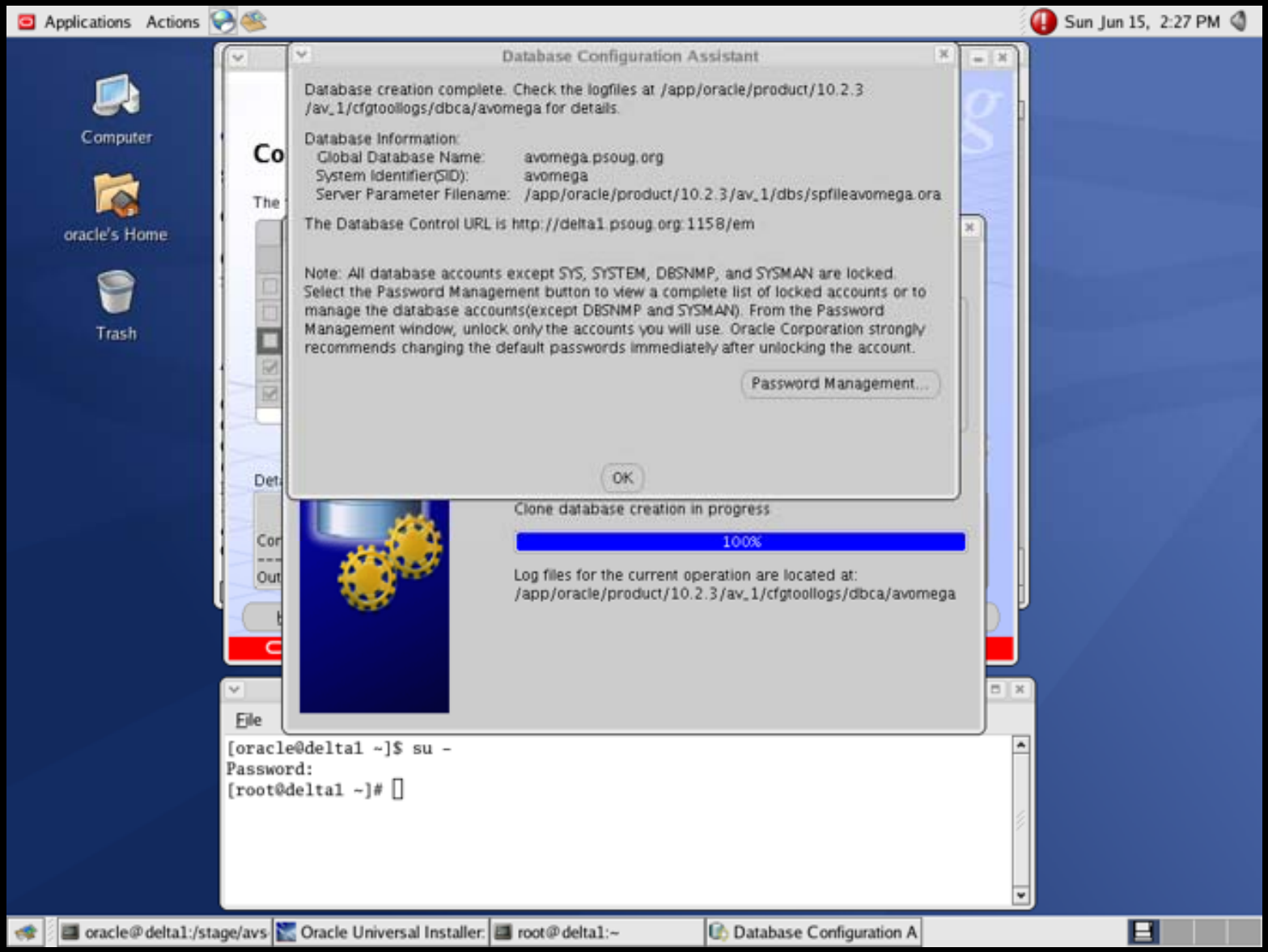
Server Install Step 11



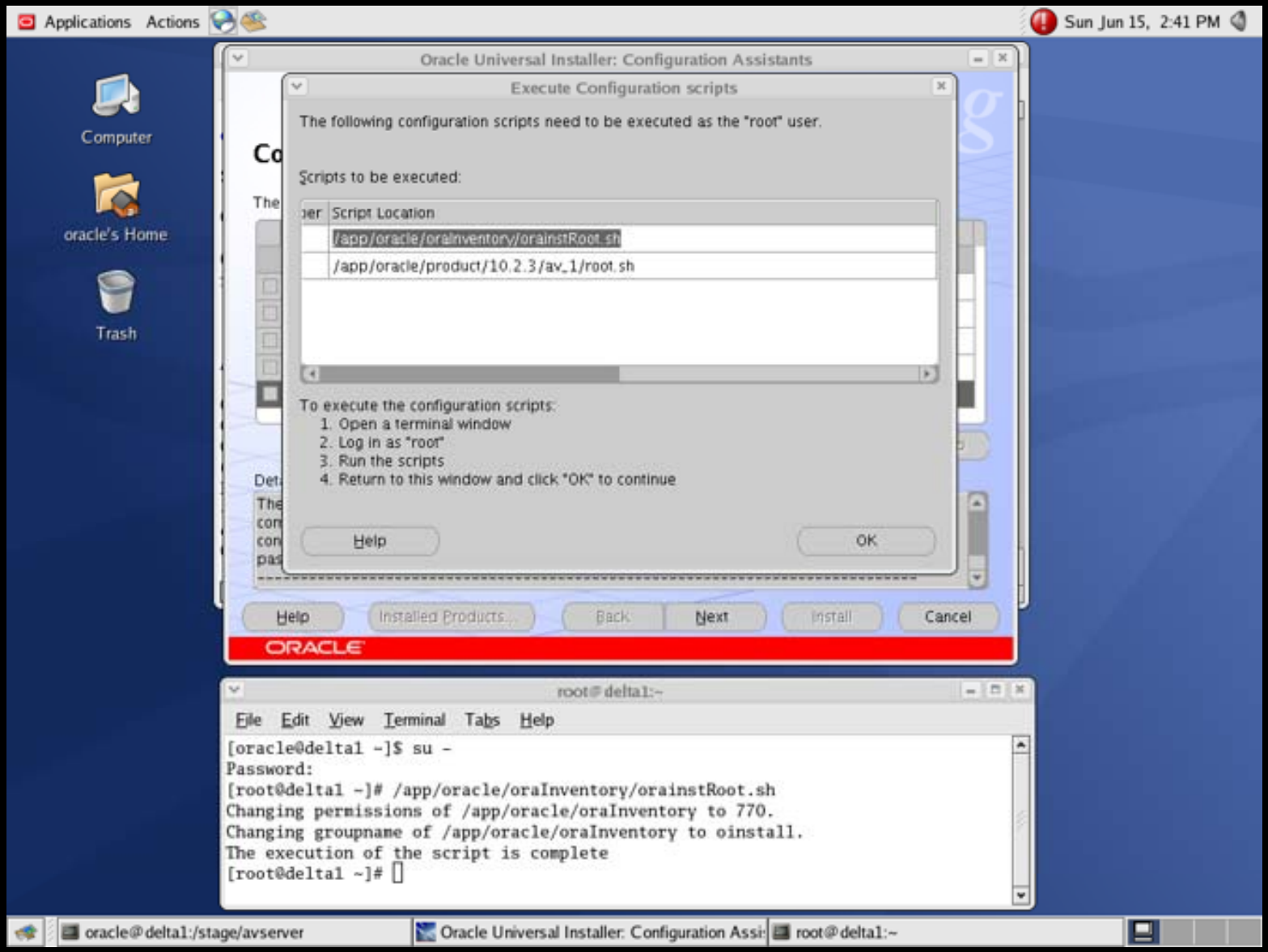
Server Install Step 12



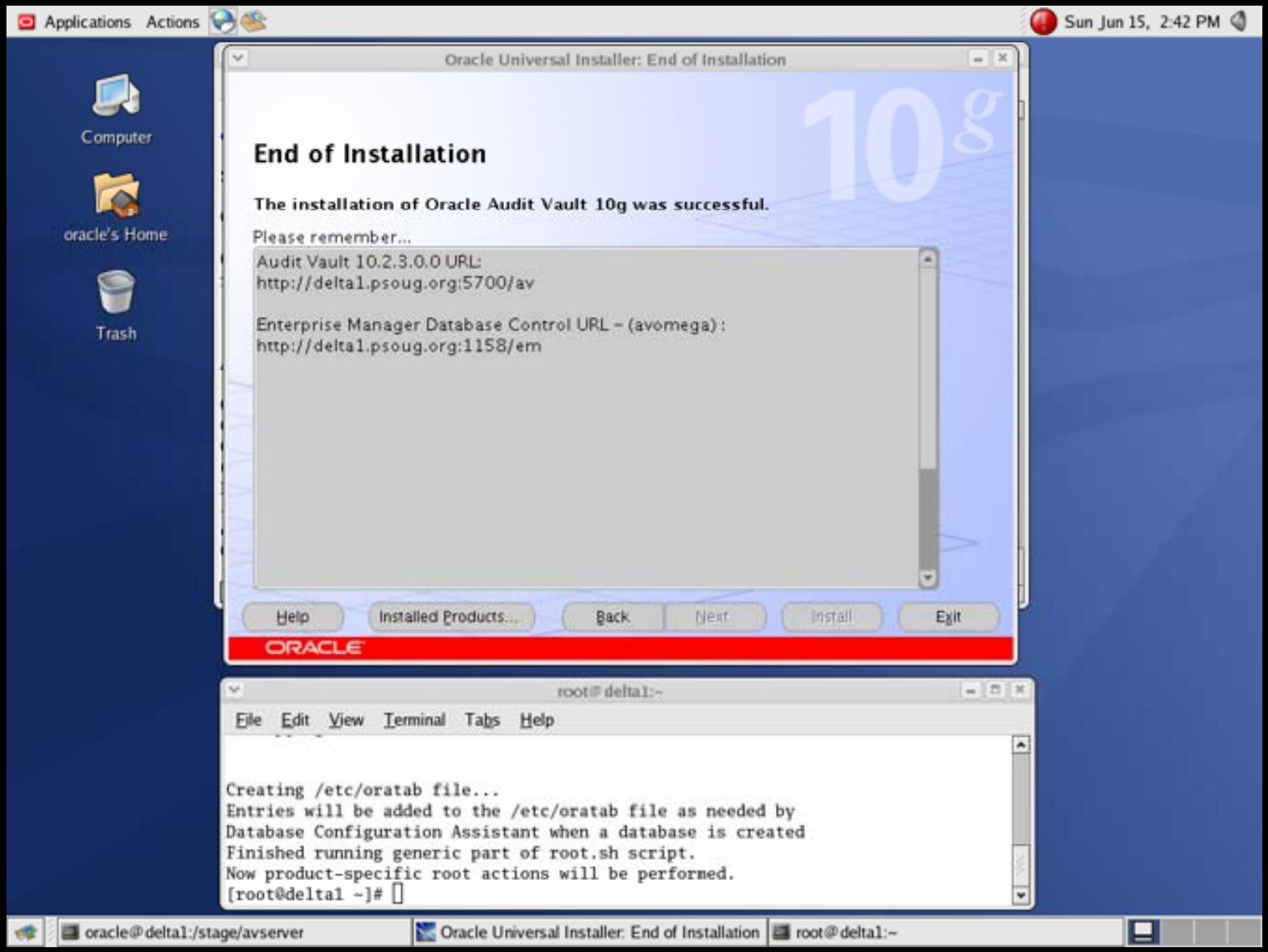
Server Install Step 13



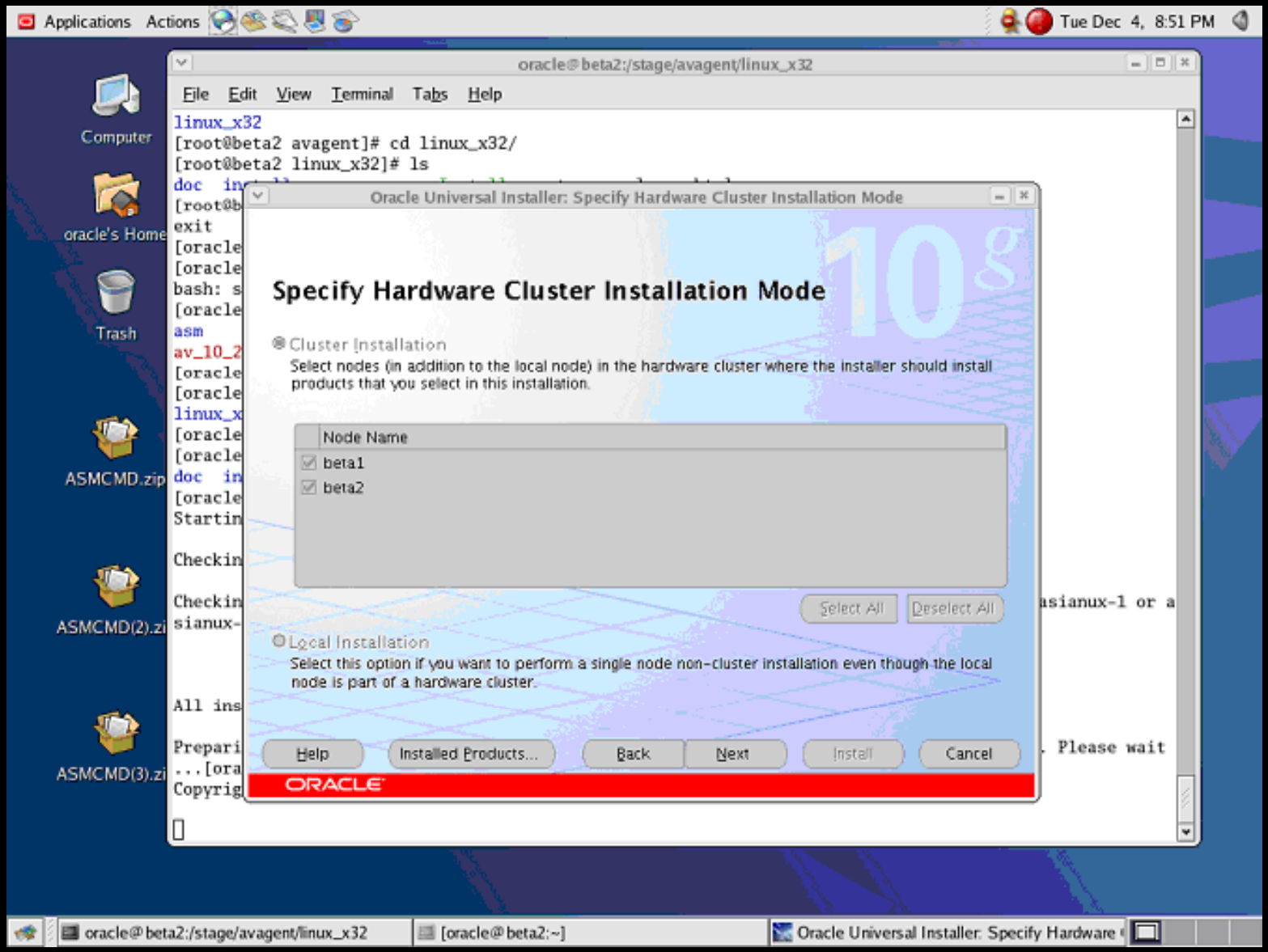
Server Install Step 14



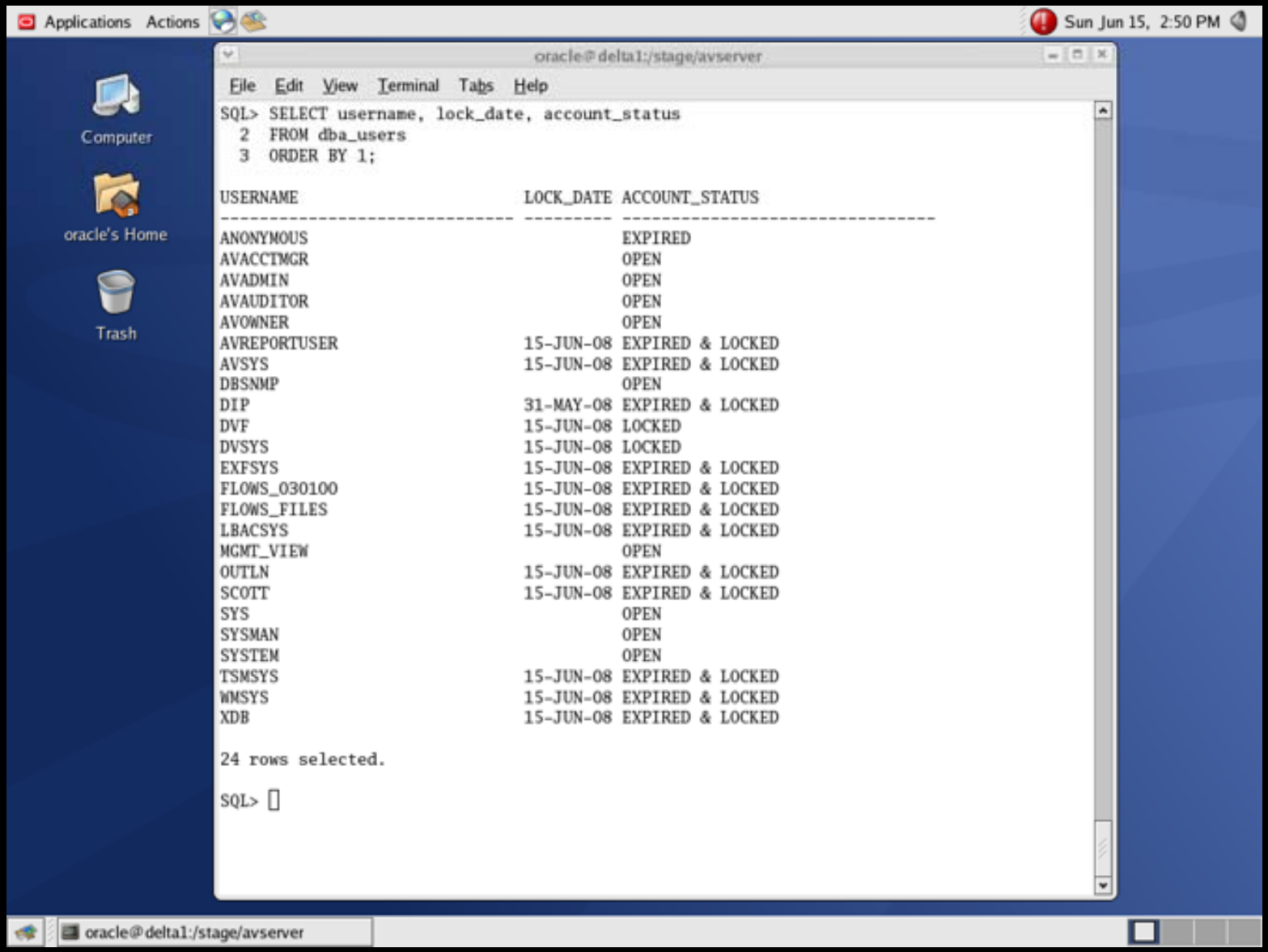
Server Install Step 15



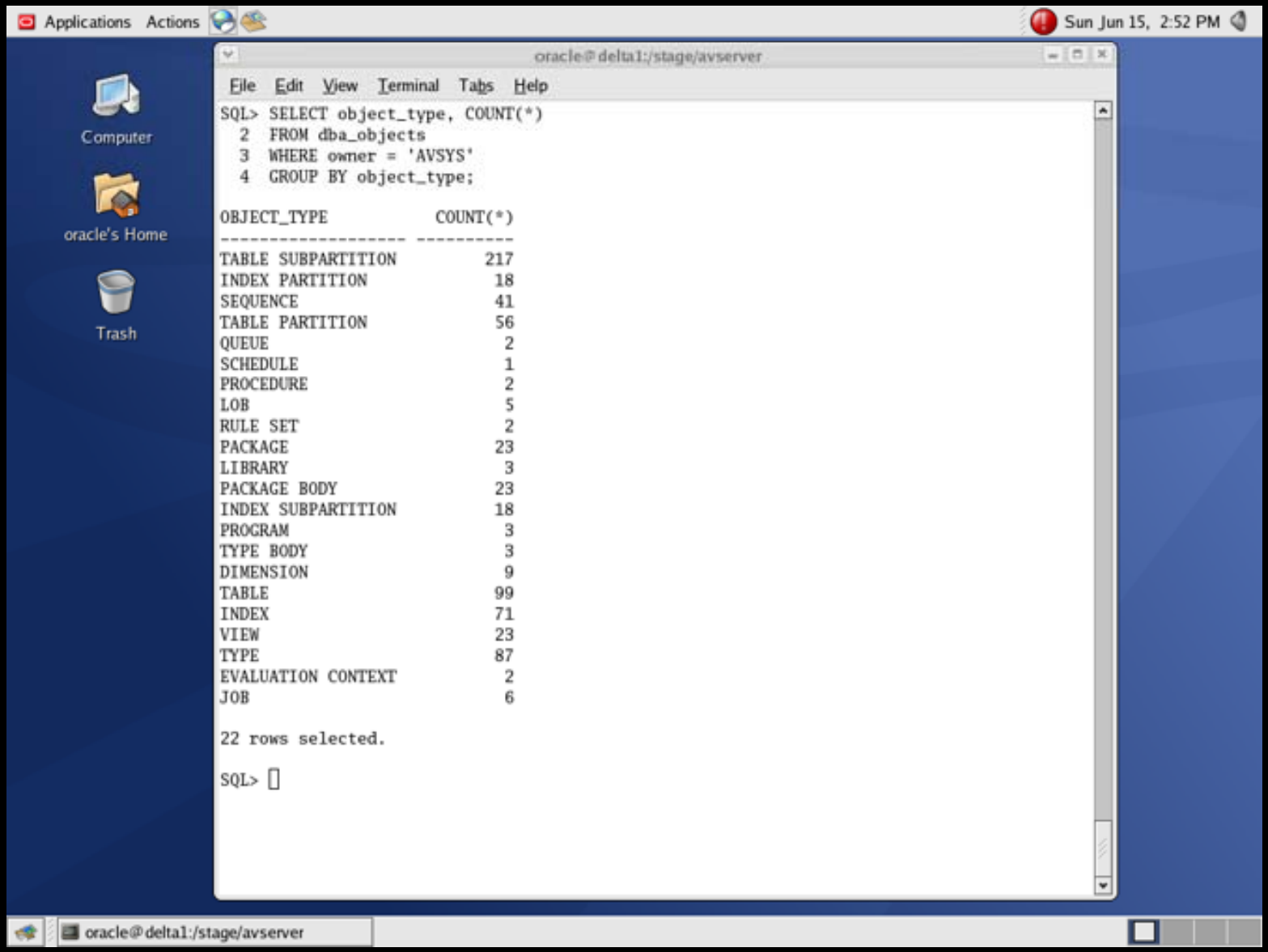
Agent Install: RAC



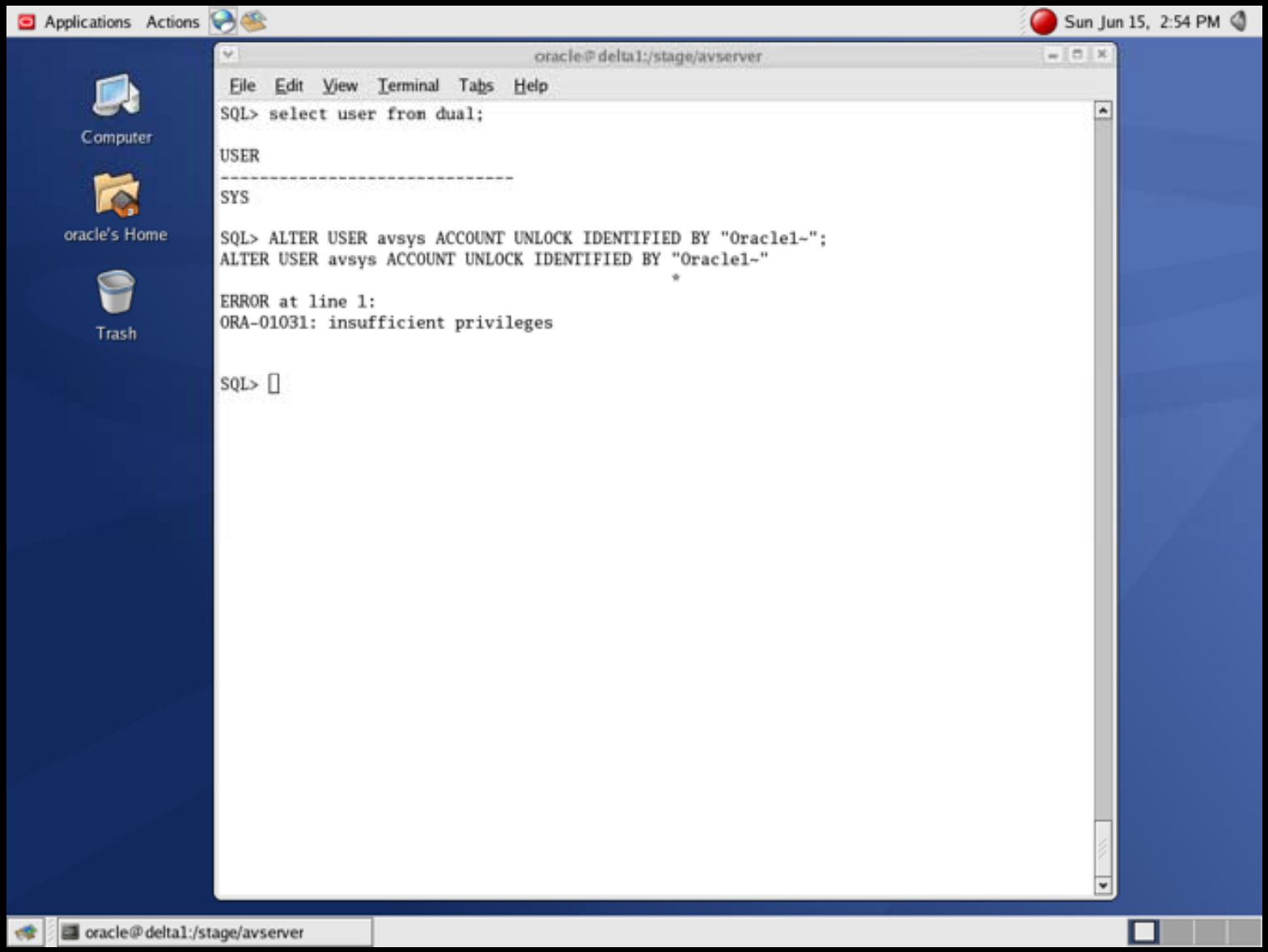
Installed Schemas



What is AVSYS?



Separation of Duties




Closing Remarks