Pacific Gas and Electric
Backup & Recovery Case Study

Eugene Psoter
Pacific Gas and Electric Company
PG&E Agenda

- Introduction
- Background on the Company and Application
- Drivers for Change and the Solution
- Designing for Failures
- High Level Principles and Trade-offs
- Failure Analysis and Recovery by Design
PG&E Company Info

- Service Area- 70,000 sq. mi. in northern and central California
- Service Area Population – 15 million people (about 5% of US pop)
- Electric Distribution customer accounts – 5.0 million
- Natural Gas Distribution Customer Accounts – 4.2 million
- Revenue $11.7 Billion
- Assets: $34 Billion
- System: 146,744 circuit miles of electric transmission and distribution lines, 46,832 miles of natural gas transmission and distribution pipelines, 6420 MW of generation
- Electricity delivered in 2005: 81,626 GWh
- Natural Gas Throughput in 2005: 844,068 Million Cubic Feet MMcf
- Employees 19,800
- Shareholders: approx 200,000

Our Vision
To become the leading utility in the United States
The Application
Customer Care & Billing

**Application**
- CC&B 1.5 from SPL Worldgroup
- 2300 concurrent online users, 300,000+ bills per day, Internet presence
- Supports operational systems for field force dispatch, outage management, etc.
- Nearly 7x24x7 uptime requirement (20 minute read-only nightly window in place, scheduled weekend outages usually acceptable, weather dependent)

**Technology**
- Database: 14 TB of data using DB2 on a zSeries mainframe
- App servers: 3 Tuxedo (online), 4 batch
- Web Servers: 9 servers with 24 instances of WebLogic
- Daily – 1 Billion select/fetch, 100 Million insert/update/delete

**Backup and Recovery**
- SAN SNAPSHOT, backed up to tape daily, PPRC to DR center
- DB2 online image copies daily to tape -- all data and catalog.
Business Drivers for Change

- Increasing loads due to data growth + internet growth
- Long (7yr) data retention requirements from various regulatory and legislative rules
- SmartMeter initiative will significantly increase database size (45+ TB)
- Costs associated with supporting growth on the mainframe platform (Unit of Measure is Millions$ for mainframe, 100Ks$ Mid-Tier)

Key Project Drivers

- Support the business requirements
- Simplify operations
- Reduce costs
  - Note potential conflict with above 2 items
Solution

• Move to Oracle database running on Mid-Tier Unix servers

• Utilize Oracle RAC to provide incrementally scalable growth and high availability to the system

• Utilize Oracle technologies to the max (ASM, RMAN, Flashback, etc) to simplify the software stack

• Move away from a reliance on tapes as a first tier recovery mechanism
Database Server Design
Project Timelines

Jan 05 Mar 05 Jun 05 Sep 05 Dec 05 Jan 06 Mar 06 Jun 06 Sept 06 Dec 06 Jan 07 Mar 07 Apr 07

- **Project Inception**
  - Business Case
  - Requirements
  - Initial Design
  - Cost Estimate

- **Small Scale RAC Cluster**
  - Acquire
  - Install
  - Large Scale POC

- **Full Scale Hardware**
  - Specify Requirements
  - Acquire & Install DR/Test System
  - Configure DR/Test System
  - Acquire & Install PROD System

- **Data Conv**
  - Full Scale Data Conversion 14TB

- **Production**

- **Testing**
  - Backup & Recovery/Data Guard
    - Sept – Nov ‘06
  - Application & Interface
    - Oct – Dec ‘06
  - ORT - Jan ‘07 (Cycle 1), Feb ‘07 (Cycle 2), Mar ‘07 (Cycle 3)
Why Worry?

“Anything That Can Possibly Go Wrong, Does “

epigraph of John Sack’s
The Butcher: The Ascent of Yerupaja (1952)

BUT ->

“Failure is not an option“

Gene Kranz
Flight Director NASA
During the Apollo XIII Crisis
Designing for Failures

• What can fail (and how often)

• Business tolerance for outages
  – (PG&E) Planned weekend outages can be accommodated, weather permitting

• Business continuity requirements for disasters
  – (PG&E) 48 Hours to recover with < 24 hours data loss

• Strategies to accommodate failures while meeting requirements
Design Tradeoffs

• Meet the business requirements
  – Does the current requirement seem reasonable for a new system?
  – Can you do better without increasing costs / risks?
  – Do the new requirements change the design that you are currently using?

The fundamental question is:
How much do you overbuild?
Design Tradeoffs

- **Simplify Operations**
  - Operating a complex system introduces risks that something will go wrong
  - The operational costs for the system will, over time, exceed the construction costs
  - Your design can help compensate for this by:
    - Reduce the number of software & hardware technologies in the design
    - Automate processes as much as you can
    - Use redundancy for transparent failure recoveries

- **Reduce costs**
  - Reduce the number of software and hardware technologies
  - Use lower end hardware where possible
  - Simplify operations
Things to Consider…

• RAC vs single instance vs High Availability OS Cluster
• Storage arrays – Enterprise vs Mid-Tier
• RMAN vs other software
• Disk backups vs tape
• Flashback options vs restores
• SAN ‘SnapShot’ capabilities vs storage costs
• Spinning DR vs Restore from backup
• Network bandwidth between centers
Backup And Recovery Principles

• Failures will happen, so plan accordingly

• Prefer hardware redundancy where it is cost effective

• If a device is expected to fail occasionally (as opposed to rarely), assume you will have a concurrent double failure on that device (e.g. lose 2 disks on a raid array)

• Use the “defense in depth” approach where multiple layers of protection are built in to the design.

• Prefer to use database recovery tools (simplify software stack) over other options
Failure Analysis - what can fail and how to recover

- Single and Multiple hardware failures
- Physical database corruption
- Logical database corruption
- Disaster
Recovery by Design

Transparent recovery for routine failures
- Use RAID to protect:
  - Single Disk Drive, Multiple Disk Drives, Disk Array Drawer
- Use redundant hardware to protect:
  - Disk Array Controller, SAN Switch, SAN Network, HBA, RAC Node

Intervention recovery for rare failures:
- Use Recovery and DR to protect:
  - Multiple RAC node failures, Storage Subsystem failure, Physical and Logical database corruption, Data Center failure
Recovery Settings

• Daily backup to disk (Flash Recovery Area) on primary and standby database
  – Level 0 incremental first day, level 1 incremental on days thereafter
  – Incrementally Updated Backups (roll forward every 3 days)
  – Block Change Tracking enabled on primary database

• One month backup cycle (full level 0 each month)

• Keep previous month copy (2 full on-disk copies)
Recovery Settings

• Archive logs
  – On primary database -- multiplexed 3 ways (FRA, 1 local, 1 physical standby).
  – On physical standby database -- multiplexed 2 way (FRA, 1 local).
• Archive log switches tuned to 2-15 minute intervals
• Data Guard LGWR ASYNC mode
• Weekly full backup from physical standby database FRA to tape
Recovery Options

- **Physical Database Corruption**
  - RMAN datafile or tablespace restore and recovery
  - RMAN block media recovery

- **Logical Database Corruption**
  - Flashback Table
  - Flashback Query
  - Flashback Database
  - RMAN TSPITR or DBPITR
Recovery Options

• Disaster Recovery
  – If production storage affected, switch to Flash Recovery Area image copies
  – Data Guard Failover
  – Switch Back
PG&E Summary

- Failure will happen, so spend the effort to design for it
- Take a holistic view of the database system and realize your tradeoffs and leverage points
- Make the system as simple as possible, but no simpler

- Reference Documents
  - Backup and Recovery Basics – 10g Release 2
  - Backup and Recovery Advanced User’s Guide – 10g Release 2
  - Using Recovery Manager with Oracle Data Guard in Oracle Database 10g