



Welcome

NASCIO's Disaster Recovery Webinar Series

**Moderator: Stephanie Czuhajewski,
NASCIO Communications Coordinator**



Asking Questions

- Please use the Question & Answer feature to ask questions at any time
- All questions will be addressed at the end of the presentation
- Responses to any questions not answered on the call will be distributed to all participants via email after the event



Technical Support

If you need technical assistance at any time:

- **Dial *0 (if you have joined by phone)**
- **Call Raindance Tech Support at 1-888-966-8686 (if you have selected the webcasting option)**



Disaster Recovery Webinar Series

*“The 10 Everyday Disasters that Nobody Prepares For”
...And how to prevent them.*

March 6, 2007

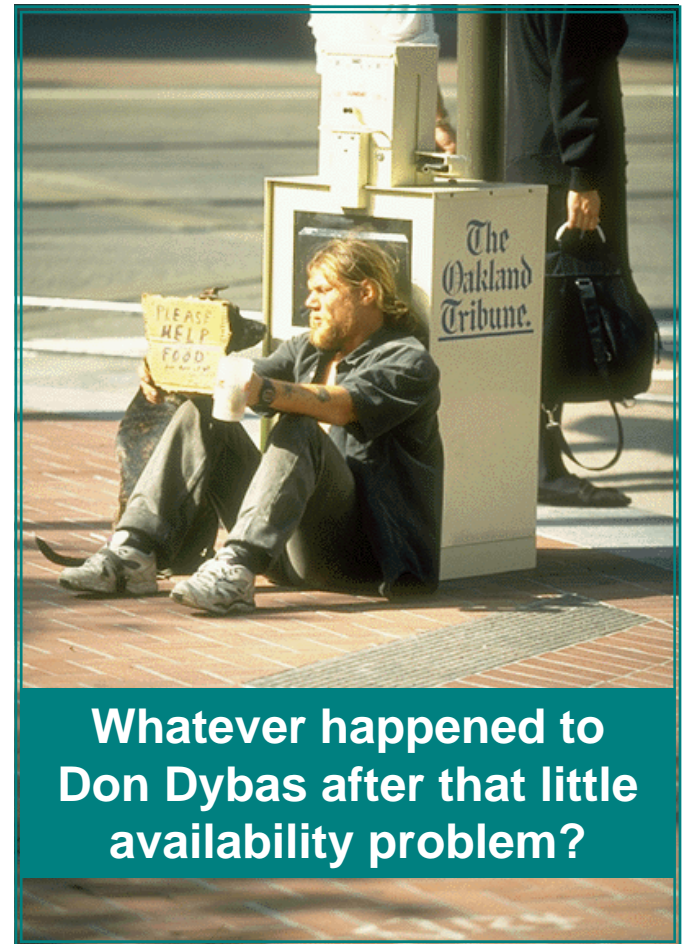
Don Dybas
Principal Solution Architect

ORACLE®
10g Certified Professional

Availability and Disasters

Architecting Availability into the System

- The degree to which an application or service is available when, and with the functionality, users expect
- By definition, if a mission critical application becomes unavailable, the Enterprise is placed in jeopardy



Whatever happened to
Don Dybas after that little
availability problem?

Availability and Disasters

All Shapes and Forms

- “Mythical”
 - Global, Regional, Continental
 - Flood, Famine, Earthquake
 - Flu Epidemic
 - Blizzard
- Response
 - Account for employees
 - Activate disaster plan / site
 - Drastic impact to operations
 - Realistic downtime: days / weeks???

Availability and Disasters

All Shapes and Forms

- “CNN Headline News”
 - Municipality or single location
 - Explosion, Fire
 - Building accident
 - Terrorism / Threat
- Response
 - Assess, triage, salvage, and restore operations
 - Temporary service disruption
 - Realistic downtime: hours / days ?????

Availability and Disasters

All Shapes and Forms

- “Garden Variety”
 - CPU Fan failed... Server melted down
 - Spilled coffee all over the SAN
 - Accidental halon release in computer room
 - Developer dropped a critical table in production
 - Operator ran payroll... TWICE
 - DBA broke leg skiing – out for 4 weeks
 - She’s the only one who knows how to back up the system
 - Disk Controller “hiccuped”
 - Data block corrupted in critical table

Availability and Disasters

Garden Variety Disasters

- Response ?
- Pretty similar to other types of disasters...
 - Assess, triage, salvage, and restore operations
 - Temporary service disruption
 - Realistic downtime: hours / days ?????

Availability and Disasters

Common Questions...

- Q: What's worse...
 - A common human mistake?
 - A fire in the data center?
 - A natural disaster?
- A: It doesn't matter to your customers / users... if both result in the same or similar amount of downtime and/or data loss.



Availability and Disasters

Common Questions...

- Q: Which is more likely to happen?



- A: Human Error... by a large margin

Availability and Disasters

Common Questions...

- Q: Which “costs” more ?
 - Tangible
 - Intangible

- A: Human Error...
 - It’s less forgivable



Availability and Disasters

Implications for DR Architecture

- Goal is System Availability
 - All Disasters affect Availability to some degree
- Architecting Systems for High Availability
 - Understand Business Continuity Requirements
 - Recovery Point/Time Objectives (RPO/RTO)
 - Priorities and Limitations
 - Assumptions and Probabilities
 - *Data Protection / Redundancy is critical*
 - People Factor: desired is not always achievable

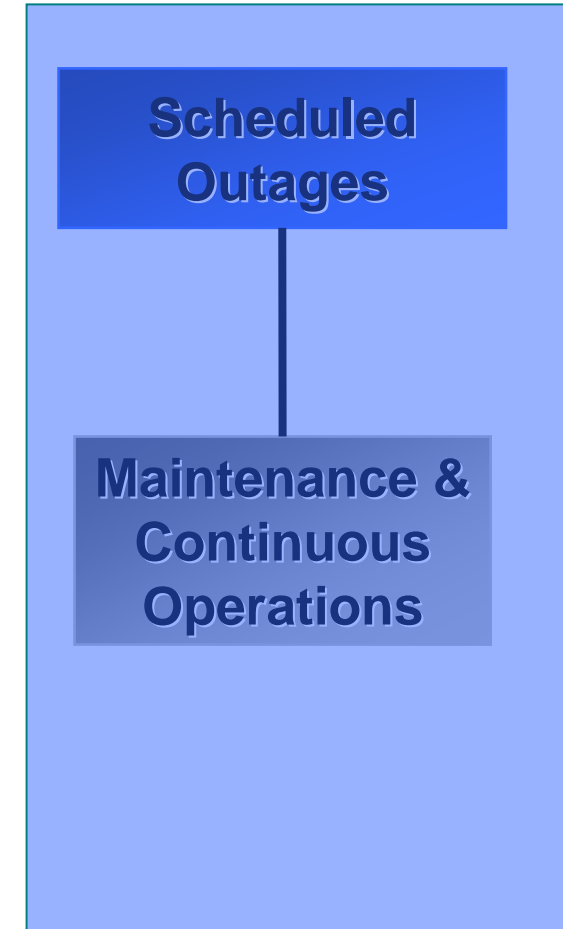
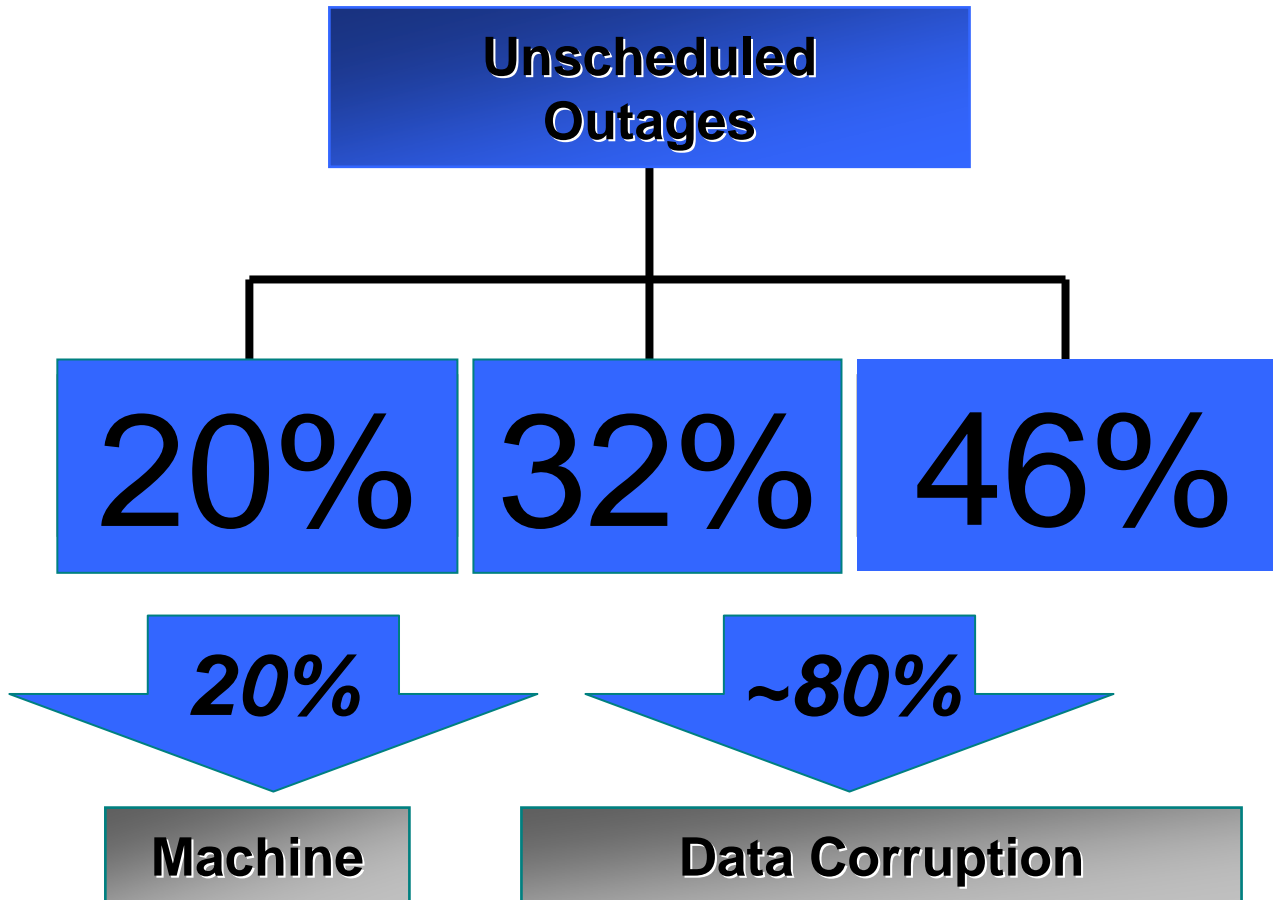
Availability and Disasters

Implications for DR Architecture

- **Best Practice #1:** Disaster Response and Recovery should be driven by business need.
 - All too often, disaster response is limited (or dictated) by the type of disaster that occurred.
 - DR Plan should dictate hardware, software, and operational requirements according to clearly defined RTO and RPO.

Causes of Downtime

Recovery Service Requests



Availability and Disasters

Implications for System Architecture

- Eliminate all SPOFs
 - Server
 - CPUs, Power Supplies, Fans
 - Storage
 - Disk Arrays, “Hot Spares”, Controllers
 - Network
 - NICs, HBAs, etc.
- Common Server Configurations
 - Servers with “Dual-everything”
 - RAID Storage is everywhere

Availability and Disasters

Implications for System Architecture

- What about the Human Factor?
 - All the hardware redundancy in the world will not prevent any of the Garden Variety disasters noted in Slide 3.
- Hardware is generally extremely reliable
 - But even seasoned DBAs and SAs make mistakes
 - Accidents happen
 - Data gets corrupted

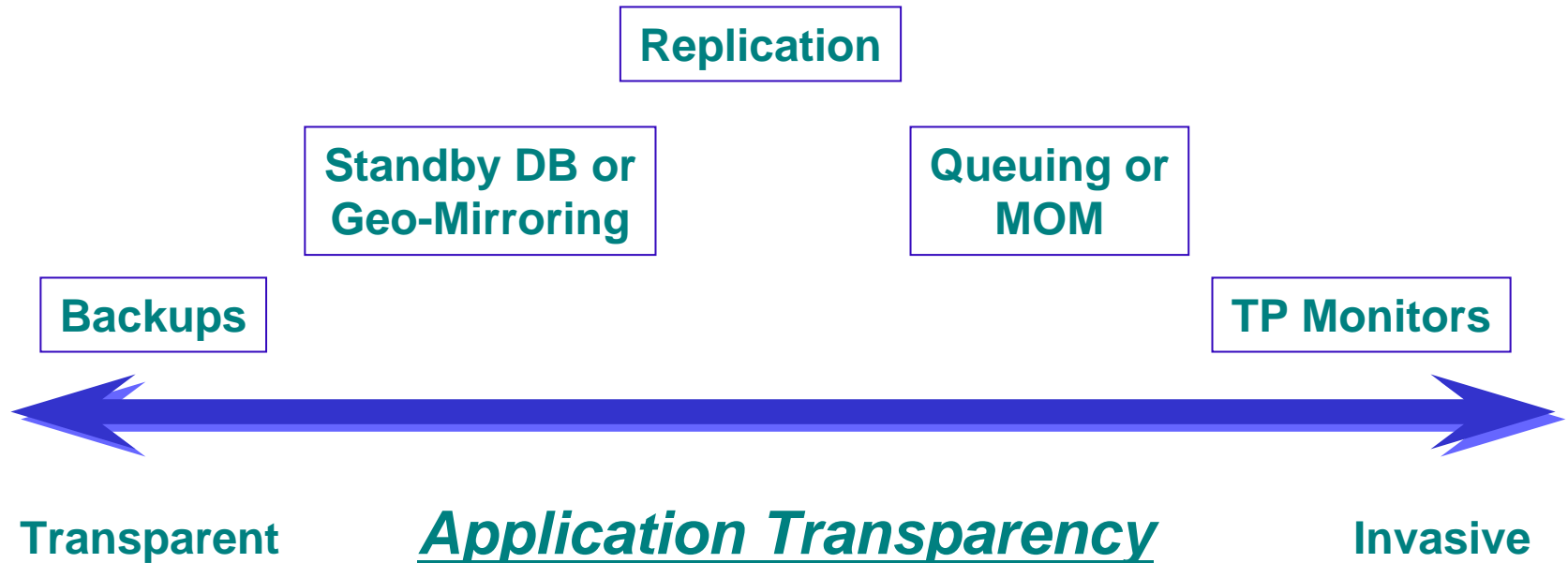
Availability and Disasters

Implications for System Architecture

- **Best Practice #2:** Redundancy should be extended beyond...
 - The physical system / server hardware
 - The primary storage mechanism
 - The data center itself
- Redundant server configurations are becoming more commonplace
 - A/A and A/P Clustering
- A Standby Data Center (“Hot/Warm Site”) is no longer an expensive luxury

Availability and Disasters

Data Redundancy Architecture Options

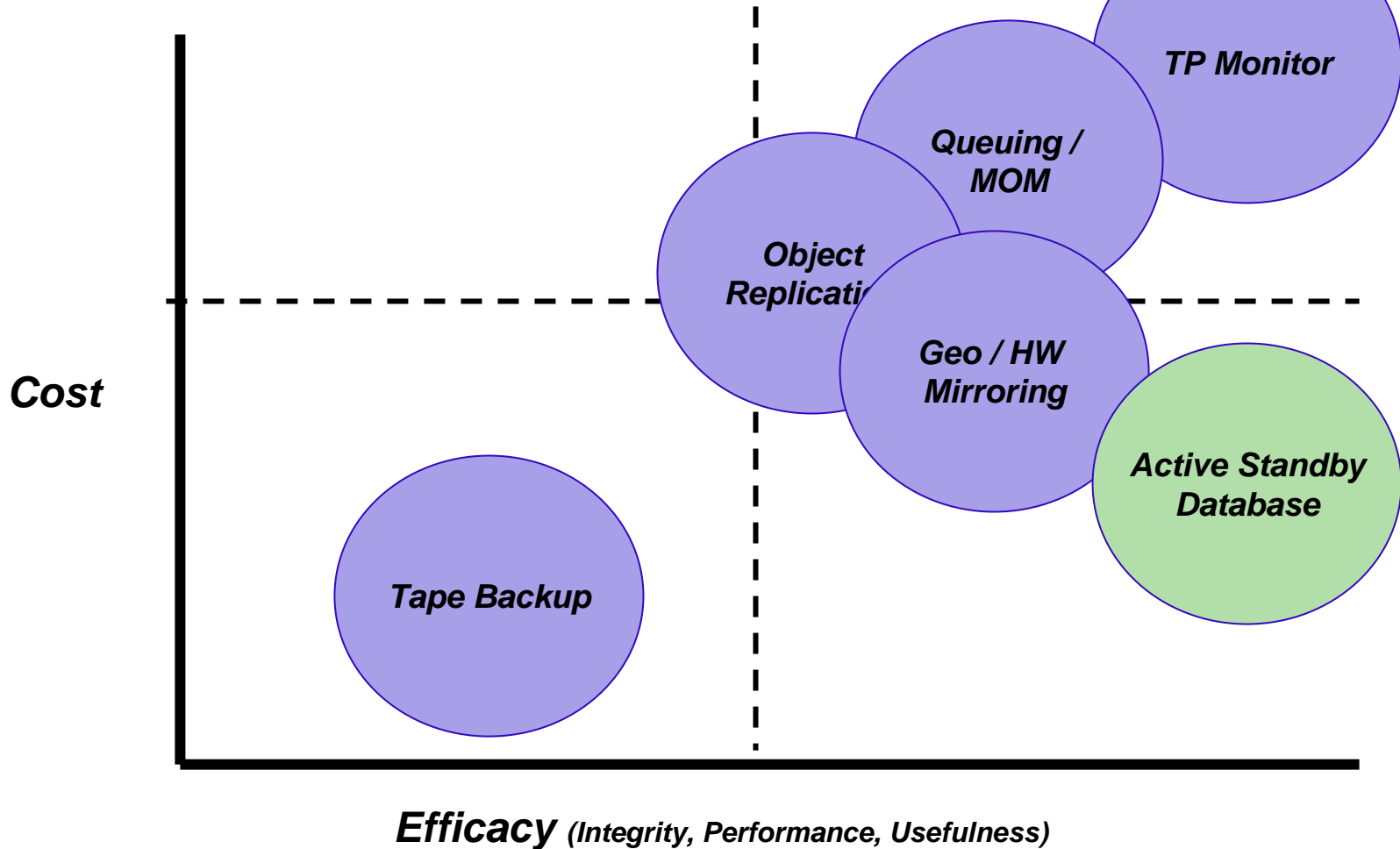


- Other Dimensions of DR Architecture

- Cost
- Complexity
- Performance
- Data Integrity

Availability and Disasters

Data Redundancy Architecture Options



Availability and Disasters

Data Redundancy Architecture Options

- Tape Backup
 - Inexpensive and simple
 - But potential for data loss
- TP Monitor, Queuing, & Replication
 - Flexible and Efficient
 - Good data protection (RT or near RT)
 - But coupled to application
 - Expensive to build / maintain / modify

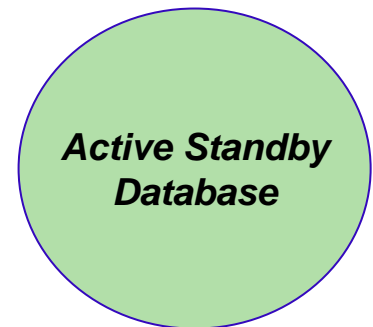
Data Redundancy Options

Hardware Mirroring –vs- Active Standby DB

- Network Efficiency
 - Disk block –vs- Tx Log
 - Protocol strengths and limitations
- Data Protection
 - Data block validation
- Usability
 - Always Active –vs- Mirror on/off
- Flexibility
 - Hardware
 - Operational

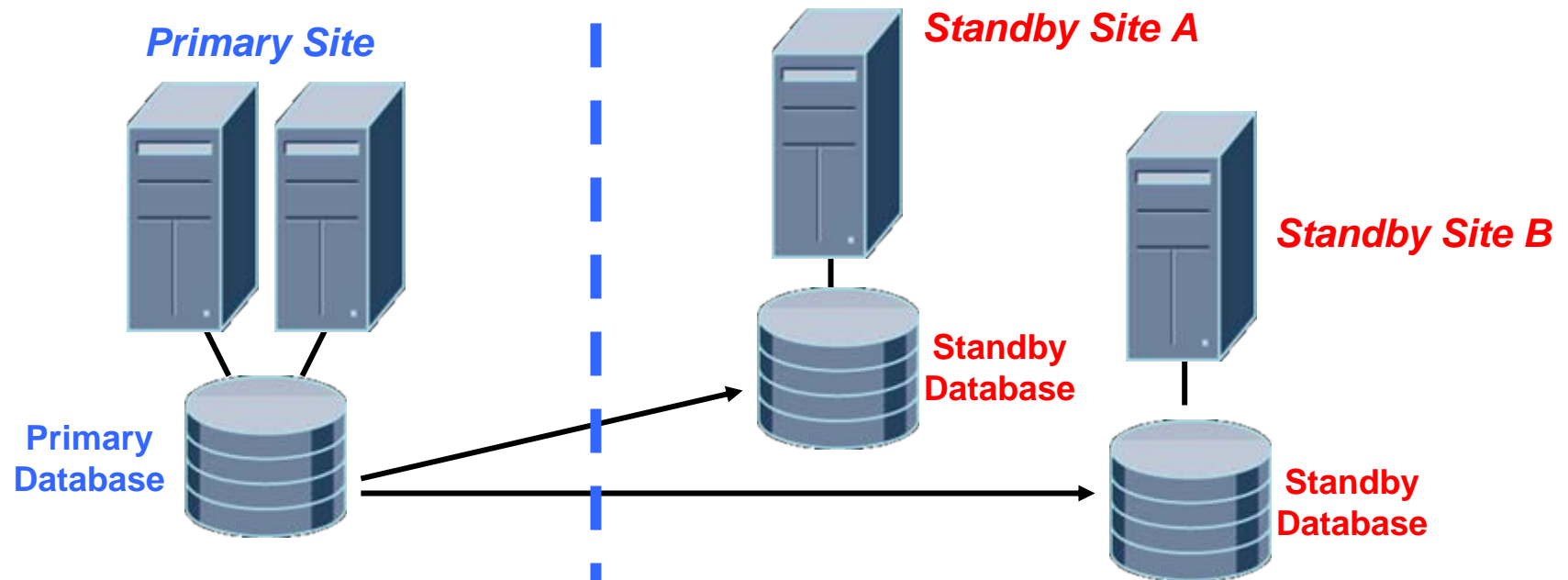


-VS-



Data Redundancy Options

Oracle Standby DB / Data Guard



- Managed as a single configuration
- Primary and standby DB can be clustered or non-clustered
- Up to nine standby databases supported in a single configuration

Operational Flexibility

Oracle Standby DB / Data Guard

- Primary and Standby role transitions
- Switchover
 - Planned role reversal
 - Used for maintenance of OS or hardware
- Failover
 - Unplanned failure (disasters) of primary
 - Automated –vs- Manual
- Primary Reinstantiation
 - Recovery of normal operations

Active Standby DB Technology

Secondary Value – Rolling Patch / Release Upgrade

- Switchover Production Load to Standby
- Patch / Upgrade Production
- Switchback to Upgraded Prod Server
- Patch / Upgrade Standby

Availability and Disasters

Implications for System Architecture

- **Best Practice #3:** Have a Disaster Recovery Plan... and Regular DR Drills
 - Great majority of customers don't have a plan
 - Those with a plan don't drill it often enough
 - Out of date?
 - Too resource intensive?

Availability and Disasters

Implications for System Architecture

- Customers who have done DR drills...
 - Exposed severe shortcomings in
 - Recovery process
 - DR Contract / expectations
 - Greatly improved their approach
 - Enhanced and simplified
 - Are much more confident
 - More value to organization
 - Achieved better return on DR investment
 - Used DR site for more than DR

Availability and Disasters

Contracted DR “Cold Site” Example 1

- Very well prepared
 - Complete set of backup tapes
 - Detailed DR plan
 - Management support
- Assigned incompatible DR hardware which wasn't specific in DR contract
 - Drill was over before it started
- Brought DR “in-house”
 - Simplified and enhanced recovery capabilities with dedicated DR hardware

Availability and Disasters

Contracted DR “Cold Site” Example 2

- Very well prepared
 - Complete set of backup tapes
 - Detailed DR plan (1 hour RPO, 4 hour RTO)
 - Management support
- Attempt to rebuild systems from bare metal and restore data exposed...
 - “Holes” in configurations
 - Complexities of process
 - Operational Limitations (skills, currency, etc.)
- Brought DR “in-house”
 - Simplified and enhanced recovery capabilities with dedicated DR hardware

Availability and Disasters

Implications for System Architecture

- **Best Practice #4:** Build advanced recovery technologies into your system infrastructure and operations
 - Physical Corruption Recovery
 - Precision block recovery from on-line backup
 - Roll forward to recover
 - Logical Corruption (Human Error) Recovery
 - Flashback Object or Transaction
 - Flashback entire DB to Savepoint

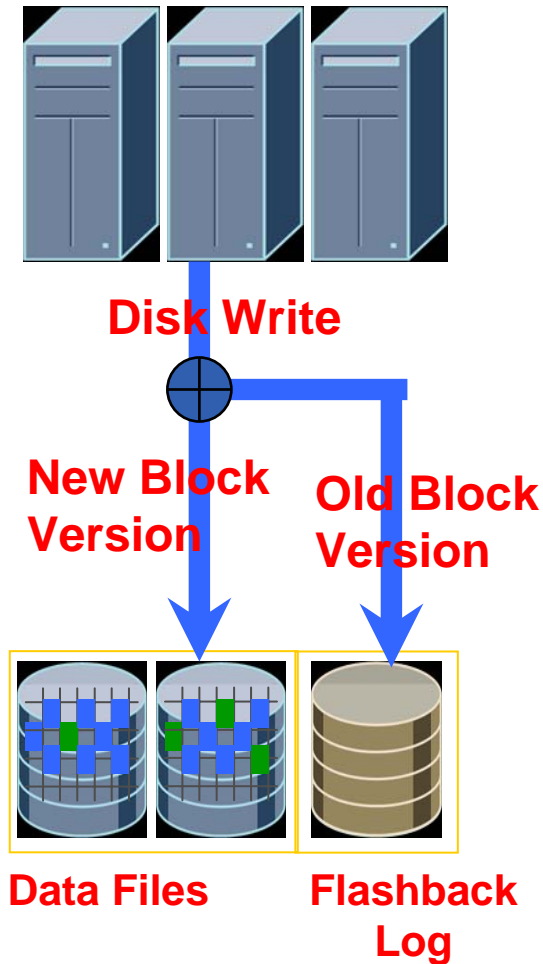
Availability and Disasters

Human Error – Single Biggest Cause of Downtime

- Goal is to quickly analyze and repair
- For Localized damage
 - Need surgical analysis and repair
 - Example – deleted wrong order
 - Back out (“rewind”) Transaction
- For Widespread damage
 - Need complete back-out to avoid long downtime
 - Example – batch job deletes this month’s orders
 - “Rewind” Database

General Data Disasters

Flashback Database



- A new strategy for point in time recovery
- Flashback Log captures old versions of changed blocks
 - Think of it as a continuous backup
 - Replay log to restore DB to time
 - Restores just changed blocks
- It's fast - recover in minutes, not hours
- It's easy - single command restore

Flashback Database to '2:05 PM'

“Rewind” button for the Database

Flashback Technology

Implications for Human Error Recovery

- Faster and more precise
- Operates on just the changed data
- Time to correct equals time to make error
 - Minutes instead of hours
 - Single command instead of complex procedure
 - Less risk and error prone

Flashback Technology

Implications for Human Error Recovery

- Without Flashback Technology

**Correction Time =
Error Time + $f(\text{DB_SIZE})$**

Flashback Technology

Implications for Human Error Recovery

- WITH Flashback Technology

**Correction Time =
Error Time**

Flashback Technology

Secondary Value – System/Load/DR Testing

- Run Transaction Load
 - Instrument, Measure, & Record
- Rewind DB to Initial State
 - Run another test
- Ideal Use for Active Standby DB
 - Use for more than just a mirrored data location

Availability and Disasters

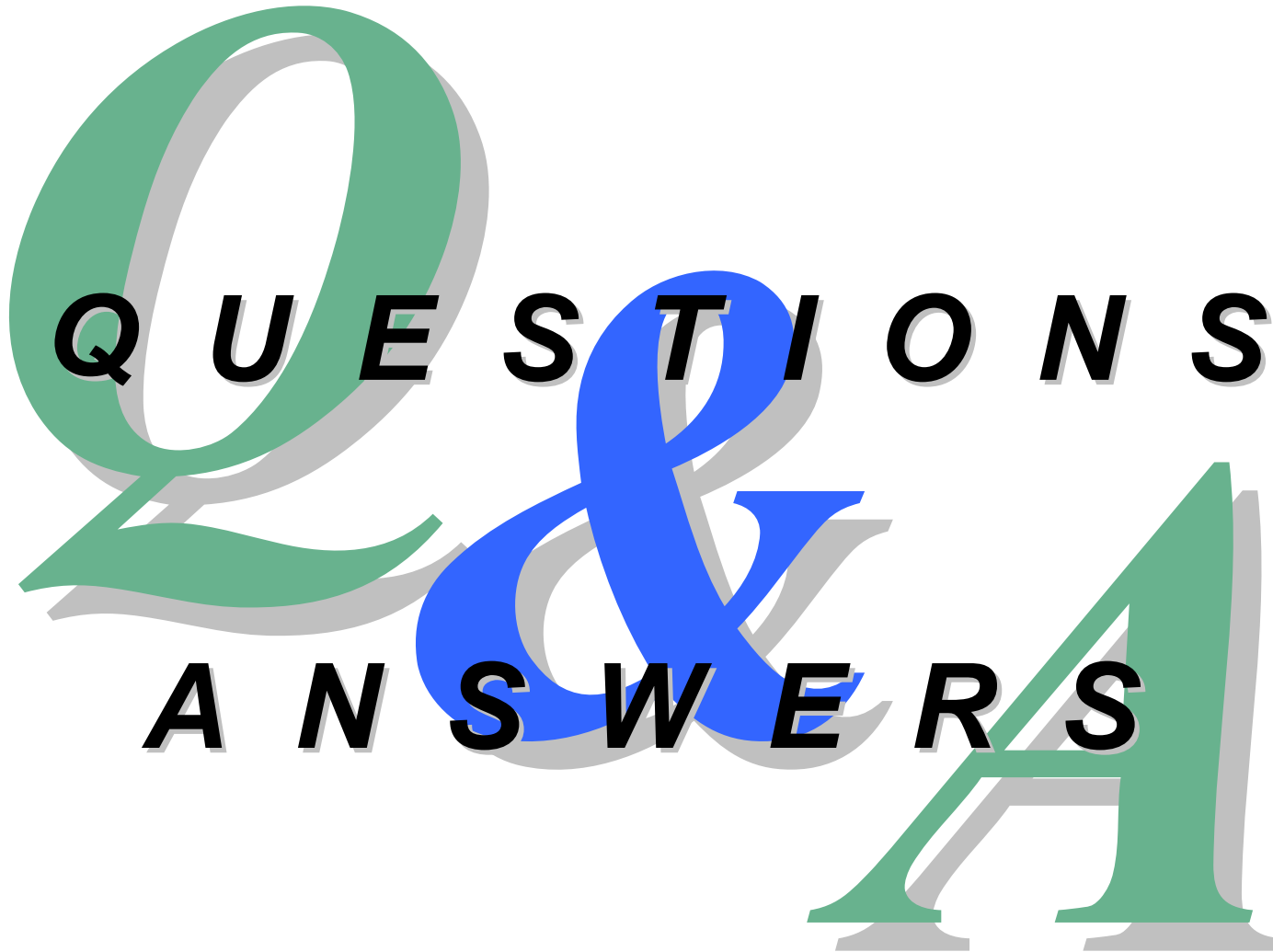
Final Thoughts

- Designing a DR Architecture and Process to recover from the “Garden Variety” disaster
 - Exposes DR shortcomings
 - Quick data recovery for **all circumstances**
 - Recasts DR as an HA Investment
 - Becomes part of SOP
 - Investment in HA resources
 - Leads to greater DR capabilities to protect from the other types of disasters
 - Example: Active Standby DB protects all types of disasters

Availability and Disasters

Final Thoughts

- You're not serious about DR until you...
 - Have run a DR drill and demonstrated you can achieve your RPO and RTO
 - “Hope is not a Strategy”
 - Create an Active Standby DB environment on **dedicated** hardware
 - Self-managed or Contracted
 - Build regular DR drills into your SOP
 - Switchover / Switchback



QUESTIONS
&
ANSWERS

The image features the words "QUESTIONS" and "ANSWERS" in a bold, black, sans-serif font. A large, stylized ampersand "&" is positioned between the two words. The ampersand is blue and has a 3D effect with a grey shadow. The letters "Q" and "A" are also stylized with a 3D effect and a grey shadow, appearing in a green color. The "Q" is at the start of "QUESTIONS" and the "A" is at the end of "ANSWERS".



Thank You

NASCIO's Disaster Recovery Webinar Series

www.nascio.org