ORACLE®

ORACLE®

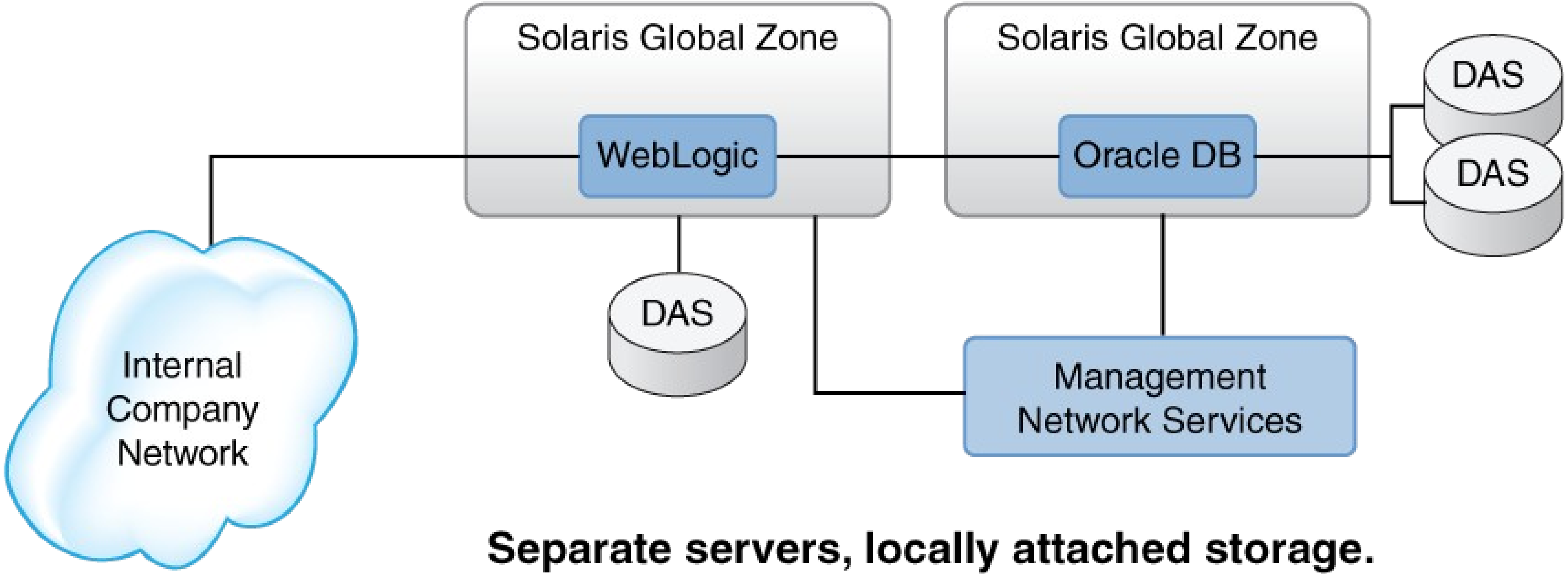
# Oracle Solaris Security:
# Mitigate Risk by Isolating Users, Applications, and Data

Will Fiveash presenter, Darren Moffat author
Staff Engineer – Solaris Kerberos Development

# Safe Harbor Statement

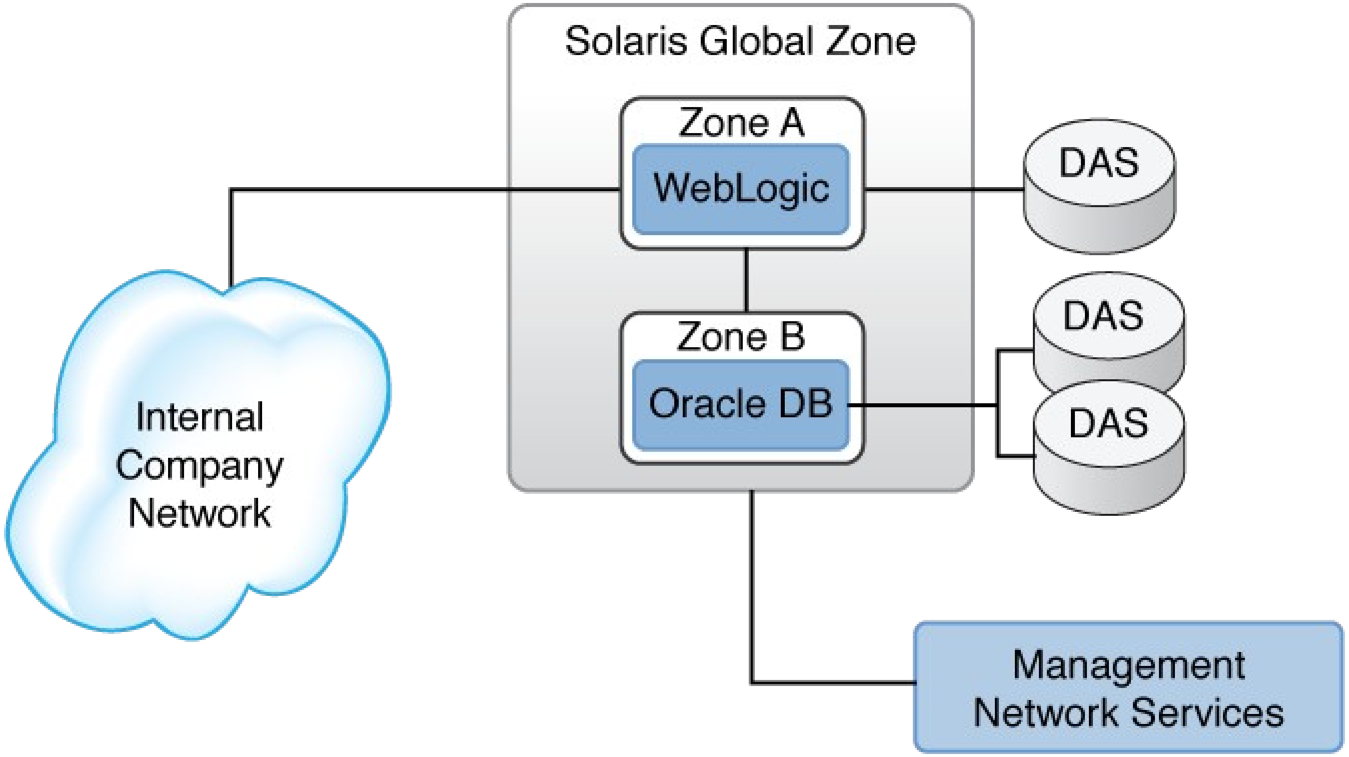
The following is intended to outline our general product direction. It is intended for information purposes only, and may not be incorporated into any contract. It is not a commitment to deliver any material, code, or functionality, and should not be relied upon in making purchasing decisions. The development, release, and timing of any features or functionality described for Oracle's products remains at the sole discretion of Oracle.

# Is this Risky/Scary ?



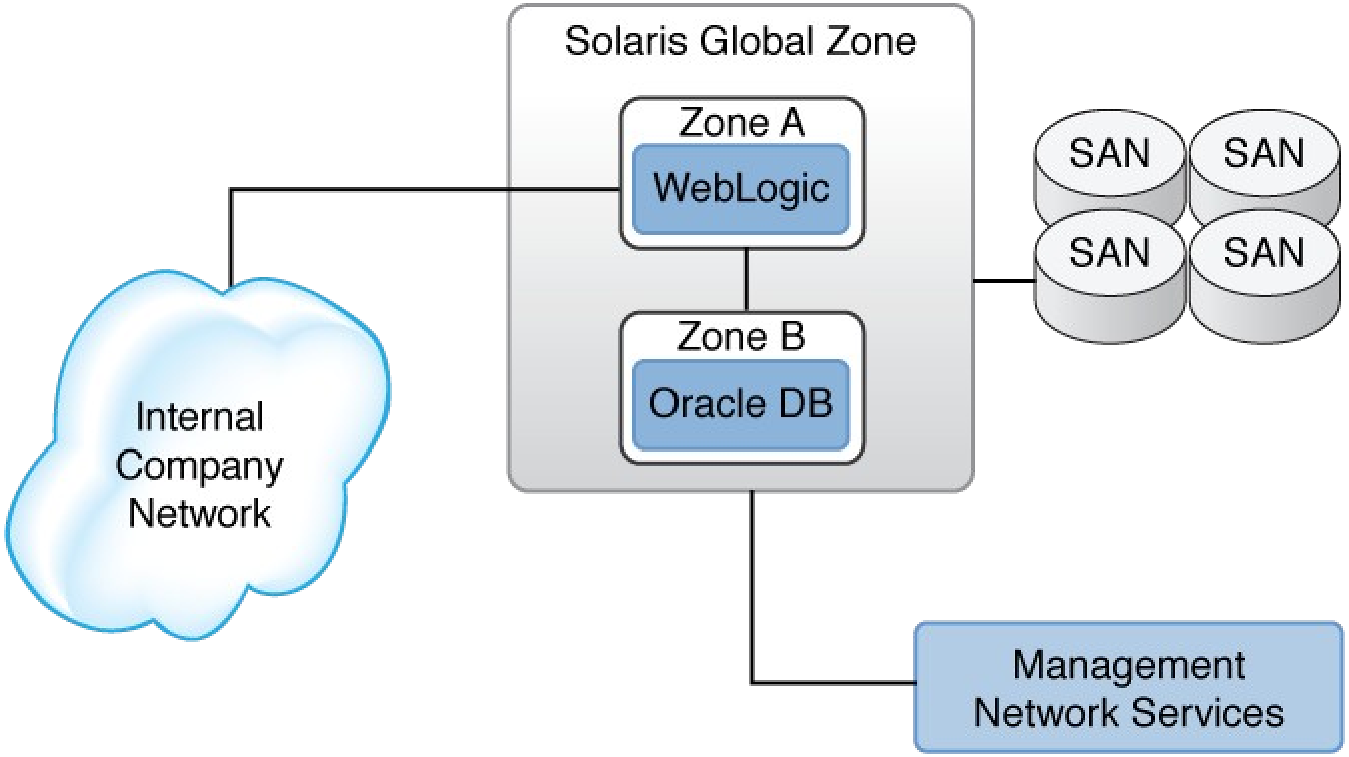
**Separate servers, locally attached storage.**

# More or less Risky/Scary ?



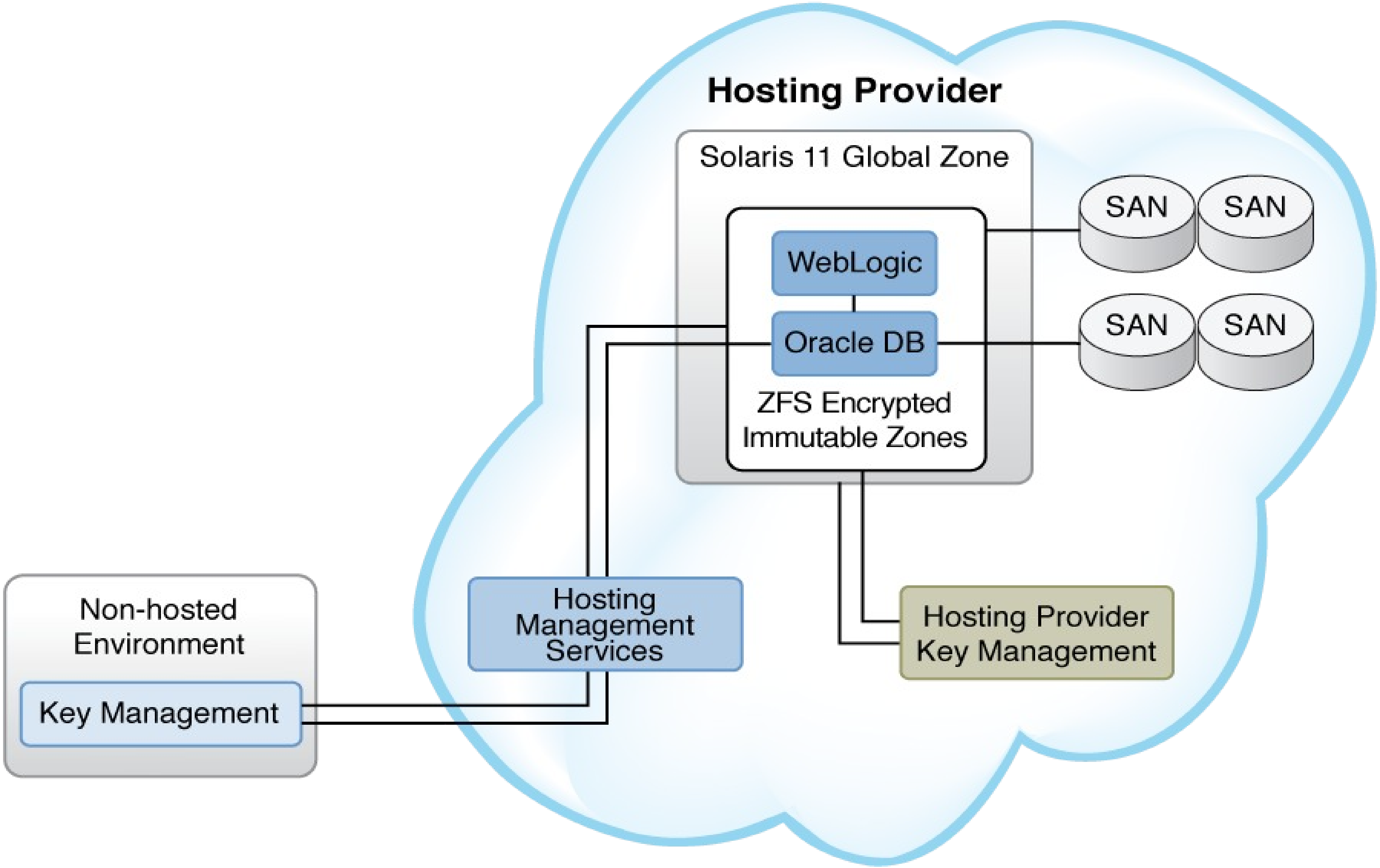
Servers now zones, locally attached storage.

# Now ?



**Internet facing and now using SAN.**

# Solaris 11 Secured Cloud Hosting



# Security Is An Arms Race

- Constant race between the attackers and defenders.
  - Mostly the same old bugs for 20+ years
  - More ways to exploit the bugs in new and old code
- Solaris needs to provide:
  - Security features
  - Solid runtime environment
- A lot of Solaris Security Engineering is small focused changes to other parts of the system to add more **built in** security assurance and features.
  - We can and do change any part of Solaris for security features
- Cloud and Virtualization don't really add new problems
  - But they do change the deployment threat model and assumptions around security...

# A *“Cloud/Visualization”* Threat Model

- Hosting provider and the hosted environment have complementary but differing views of the threat model
  - In a data centre these might be the same groups
- Both care about securing the system
- Client may be mostly concerned with:
  - Unauthorized access to their data
  - *“All disks/tapes leave the data centre eventually”*
  - Attack on running system, eg website defacement
  - Trojaned runtime environment
- Provider may be mostly concerned with
  - Unauthorized access to hosting environment
  - Resource utilization
  - Reputation for providing a secure system

# Key Messages

- Protect data at Rest and in Motion
- Prevent unauthorised access
- Delegation of control / Separation of Duty
- Reduce risk of “damage” or “theft” if unauthorised access does happen
- Audit trail of change for Compliance
- Highlights of some Solaris 11 security features

# Mitigating the Risk
## *“Some Security Features”*

- Many levels of “access control”
- Traditional UNIX permissions
- ZFS has NFSv4/Windows NT style ACLs
  - CIFS shares have ABE for share level restrictions
- Mandatory Access Control
  - ***New*** Zone file-mac-profile
  - Trusted Extensions labeling
- File System & block device encryption
- Application Sandboxes via Zones, privileges and resource controls

## System Integrity Protection
## *“Get the right bits on disk and keep them right”*

- Network package installation over HTTPS
  - Protect sensitive package content in transit
- Solaris 11 packages are cryptographically signed
  - You can add additional signatures
- System policy to require and verify signatures
  - YOU choose who to trust per system image
- ELF binaries are still cryptographically signed
  - Know they came from Oracle RE process
- For non packaged files bart(1M) provides a passive manifest comparison system using cryptographic hashes

# System Integrity Protection
# “But some things are editable”

- Solaris 10 “sparse root zones” partially read-only
  - wasn't really a security feature
- Solaris 11 zone “file-mac-profile”
  - Controls which parts of the zone are writeable even for root
    - *none, flexible-configuration,fixed-configuration,strict*
  - Underlying technology based on whitelist & blacklist, maybe extended to other sandboxing use cases in future releases
- ZFS checksums and self healing
- ZFS encryption for data file systems & ZVOLs
  - Can encrypt Zone file systems

# Isolating Applications

- Solaris Zones as an application fault boundary
  - Service Management Framework
    - Restart & notification (SMTP, SNMP),
    - Per service firewall rule
  - Resource Controls (CPU, Memory, ...)
  - File system name space isolation
  - Solaris 11 per Zone administration delegation
- Privileges for sub-zone security boundary
  - Including removing new basic privileges:
    - net_access, file_write,file_read
- Zone system integrity via “file-mac-profile”

# Remote User Authentication

- Solaris defaults to ONLY SSH remotely accessible
- No remote root login & root is a role by default
- SSH & Kerberos easier to manage centrally using X.509 certificate based authentication
  - YOUR Certificate Authorities as Trust Anchors
- Kerberos protection for NFSv3 & NFSv4 traffic
- Active Directory/Kerberos authentication for CIFS/SMB network shares

# Data in Motion Protection

- Zone file system security boundary now applies to NFS **server** as well.
  - Each zone can serve a separate NFSv4 domain
  - Each zone can be in a separate Kerberos Realm
- Per Zone IPsec policy
- Kernel SSL/TLS proxy
  - Allows keeping private keys outside of the zone
- Hardware crypto acceleration on SPARC and Intel CPUs reduces overhead of encrypting network traffic
  - SSH, IPsec/IKE, Kerberos, OpenSSL, KSSL

# Data at Rest Protection

- Encryption for UFS & other legacy filesystems via lofi driver.
- ZFS data set encryption (file system & ZVOL)
  - Comprehensive wrapping key management
    - Delegation: key use *vs* key change *vs* key location/type
    - Local or Centralised
    - Integrated with Oracle Key Manager via pkcs11_kms
    - 3rd Party key management integration
      - zfs(1M) key subcommand is scriptable
      - Keys from any https:// location – policy on server side
  - Data encryption key change at clone or on demand

# Unique in the Industry: Trusted Extensions (TX)

- Only enterprise OS that includes multilevel functionality as a bundled feature
  - Full support of TX included in standard Solaris license
  - TX benefits from all Solaris 11 enhancements
  - Zones architecture makes labeling completely transparent to applications
- Only OS to *ever* achieve Common Criteria certification for security target including a multilevel desktop
  - Unique integration with GNOME labeled workspaces
  - Integrated with Oracle's Virtual Desktop Infrastructure

# Data sensitivity labeling

- Tag the data everywhere
  - At rest in the file system
  - In motion in the network
  - In the application
- Allows controlling the data flow between applications, hosts and users
- Trusted Extensions provides:
  - Enhanced Zone based integrity & isolation boundary
  - File system level tagging of data sensitivity
  - IPsec based labeling of data in transit
  - Multi-level GNOME desktop with robust lockdown

# Solaris 11 New Trusted Extensions Features

- Automatic persistent labeling of ZFS datasets
  - Labels are encrypted objects on disk
- NFS now provided by per label (zone) server
  - Improved isolation of NFS server (per label IP address)
  - Allows for separate NFSv4/Kerberos domains per label
- Improved CLI & GUI management tools
  - tncfg (local & LDAP)
- Labelled IPsec
- **PLUS** Lots of generic Zone improvements:
  - Exclusive IP stack, auto VNIC, Auto Installer integration, file-mac-profile...
- Infiniband support

# Audit trail for Compliance and Reporting

- Comprehensive audit trail: 20+ years of development
  - System service & system call level
  - SMF is heavily audited – any property or service change
- Auditing now “ON” by default
  - Login/logout events
  - No reboot to change audit policy
- Audit inside or outside the zone
  - Can't see what auditing is happening or the audit trail
- Audit trail export to XML
- Client for transporting audit trail securely off the system
  - Protected by GSS/Kerberos for authentication/integrity/confidentiality

# “But it is all too hard to use”

- Some of this was traditionally hard to use
- Solaris 11 has much better scriptable CLI for user and RBAC management with support for LDAP
- Firewall rules integrated with services (svc.ipfd)
- 'zfs create -o encryption=on pool/data'
  - Yes it can be that simple!
- Hardware encryption use is transparent
  - Solaris, Java, OpenSSL, and Oracle RDBMS
  - Even more so with SPARC T4 and Intel AES-NI

# Solaris 11 Features Addressing Threats

- Multiple tenant application containment via Zones
  - RBAC Delegated administration  (i.e. give access to console & zone reboot only)
  - Read Only Zone Root *(Mandatory Access Control)*
  - ZFS data set encryption of zone & data
- Application Sandboxing
  - More “basic privileges” - read/write files, network access (to become fine-grained in S11 updates)
  - Read Only Zone Root
- Data at Rest Encryption (ZFS)
  - With centralized & delegated key management
- Assurance that software hasn’t been compromised
  - Signed packages & secure package transport
  - Signed binaries / libraries

# Solaris 11 Features Addressing Threats

- Accountability / Audit Trail
  - Now on by default (authentication events logged)
  - Near zero performance overhead
  - Audit trail off machine via secured transport
  - Many more things audited (lots via SMF) and more still to come
  - sudo is integrated with Solaris Audit trail
- Easier deployment of network security protocols:
  - X.509 support in Solaris 11 for SSH & Kerberos simplifies deployment and provides centralised management
  - NFS authentication, integrity, confidentiality via Kerberos
- Easier to user management tools
  - CLIs now support LDAP backend & more comprehensive
  - Fine grained delegation eg, change user but not root password

- Built for clouds
- Best for enterprise applications
- Best for Oracle

**Solaris 11 Launch Event**

**9th November**

**http://oracle.com/goto/solaris11event**

ORACLE®