
ORACLE®

ORACLE

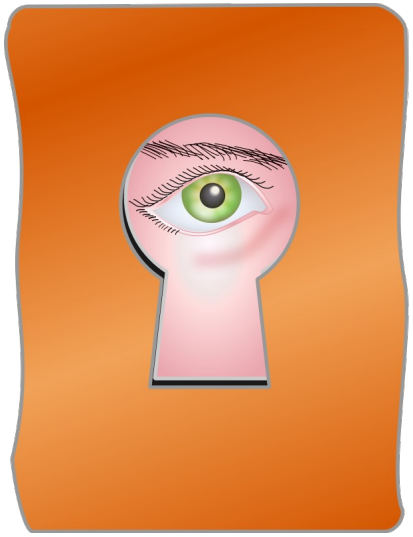
(Some) Lesser Known Solaris Features

paul.roberts@oracle.com

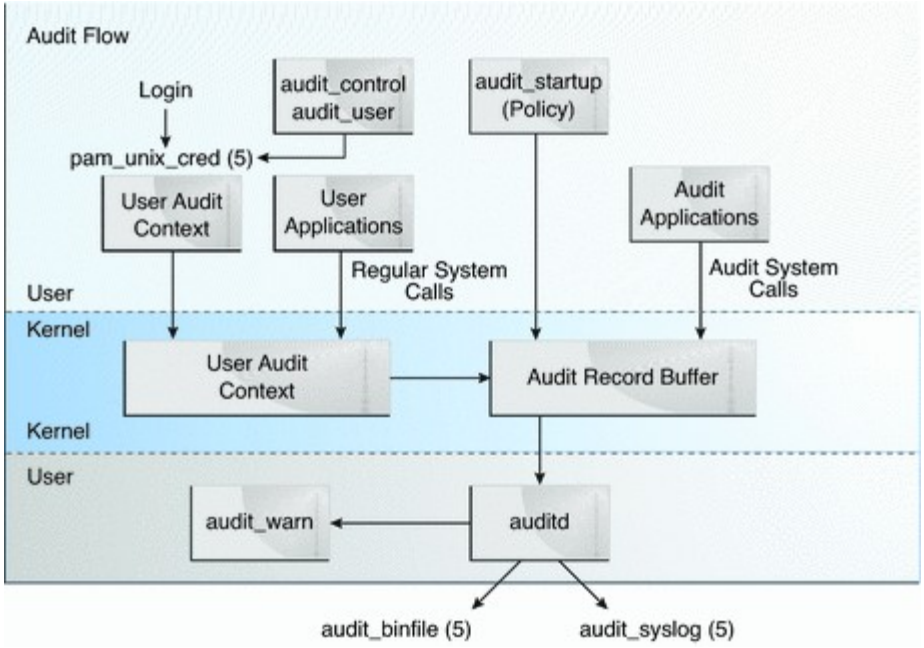
Solaris Auditing

¿Qué?

- Tool for monitoring and logging system activities
- Assigns a unique persistent session ID
- Doesn’t prevent malicious activity
- Used for post-mortem analysis
- Records written by auditd(1M)
- Userland API used by, for example
  - passwd(1), in.ftpd(1M), su(1M)



Solaris Auditing



BART

Basic Audit Reporting Tool

- Simple tool for detecting file-level changes
- E.g., “why is this service broken, what changed?”
- Saves attributes for files in to a manifest
  - ACL, contents checksum, mtime, size etc.
- Then compare current state to saved manifest
- Programmatic or human-readable output
- Fine-grained control with a rules file

Service Management Facility

Service Management Facility (SMF)

- Describes to the OS what services are running on it
- Allows for complicated metadata
  - Such as dependency trees
  - Multiple statuses
  - How / if the processes should be restarted
  - What to do if a service that is depended on goes away
  - Human readable information and documentation pointers

Some building blocks of SMF

- Service
  - General definition of something running on a machine
- Service instance
  - A specific running service which may have specialised config
- Milestone
  - Grouped dependencies
- FMRI
  - Unique service name
- Methods
- Service states
- Manifest
  - Describes the service in XML

/var/svc/manifest/network/login.xml

```
<?xml version='1.0'?>
<!DOCTYPE service_bundle SYSTEM
'/usr/share/lib/xml/dtd/service_bundle.dtd.1'>

<!--
    Copyright 2009 Sun Microsystems, Inc.  All rights reserved.
    Use is subject to license terms.
[… ]
-->

<service_bundle type='manifest' name='SUNWrcmdr:rlogin'>
<service
    name='network/login'
    type='service'
    version='1'>

    <restarter>
        <service_fmri value='svc:/network/inetd:default' />
    </restarter>
```

/var/svc/manifest/network/login.xml

```
<instance name='rlogin' enabled='false' >
        <exec_method
                type='method'
                name='inetd_start'
                exec='/usr/sbin/in.rlogind'
                timeout_seconds='0'>
                <method_context>
                        <method_credential user='root' group='root' />
                </method_context>
        </exec_method>
[...]
</instance>

<instance name='klogin' enabled='false' >
        <exec_method
                type='method'
                name='inetd_start'
                exec='/usr/sbin/in.rlogind -kc'
                timeout_seconds='0'>
                <method_context>
                        <method_credential user='root' group='root' />
                </method_context>
        </exec_method>
```

Kernel SSL

KSSL (Kernel SSL)

- In-kernel implementation of SSL
- Application need know nothing of SSL
- Handshaking done asynchronously by kernel
- PKCS#11 support
- Performance improvement
- DTrace and kstat

Crashdumps

Crashdump analysis

- Kernel writes memory contents to disk
- Use `dumpadm(1M)` to configure the location etc
- `uadmin(1M)` or `savecore(1M)` to take a dump at will
- Use the extensible debugger `mdb(1)` for Solaris dumps

Other features

- Resource management
- AutoFS, lockfs, CacheFS, tmpfs
- RBAC, least privilege
- pfexec
- Crossbow
- Multipathing
- fssnap
- SamFS
- IPS
- and more ...

References

- www.c0t0d0s0.org - book this talk is based on
- docs.sun.com – manuals for all the stuff talked about here
- http://blogs.sun.com/lianep - SMF (and other stuff) blog
- http://bit.ly/c41E0A - KSSL DTrace probes blog post
- http://amzn.com/0131493868 - Panic!, Chris Drake, Kimberley Brown (Author)