

Stay Secure With Oracle Solaris

Marcel Hofstetter

hofstetter@jomasoft.ch

<https://www.jomasoftmarcel.blogspot.ch>

**CEO / Enterprise Consultant
JomaSoft GmbH**

 **Oracle ACE „Solaris“**

Agenda

- About JomaSoft
- Oracle ACE Program
- Solaris 11: Secure by Default
- Virtualization
- Compliance tool
- SPARC Silicon Secured Memory
- Compliance and Hardening using VDCF

About JomaSoft

- Engineering company founded July 2000
- specialized in **Solaris** and software development, operations and consulting
- Product **VDCF** (Virtual Datacenter Cloud Framework)
Installation, Management, Operations, Monitoring,
Security and DR for Solaris 10/11,
Virtualize using LDoms and Solaris Zones
- VDCF is used in production since 2006



Specialized
Oracle Solaris 11



Specialized
SPARC T5-Based Servers



About JomaSoft

- Flexible and Customer focused
- Oracle Certified Employees
- 17 Years Solaris Experience
- Regular Oracle Solaris Beta Tester
- Well connected with Oracle Solaris & LDOM Engineering Teams



Specialized
Oracle Solaris 11



Specialized
SPARC T5-Based Servers

500+ Technical Experts Helping Peers Globally



3 Membership Tiers

- Oracle ACE Director
- Oracle ACE
- Oracle ACE Associate

bit.ly/OracleACEProgram

Connect:

✉ oracle-ace_ww@oracle.com

📘 Facebook.com/oracleaces

🐦 [@oracleace](https://twitter.com/oracleace)



Nominate yourself or someone you know: acenomination.oracle.com

IT Security

- Not Topic of this Session
 - Firewalls
 - Applikation Development
- OS Security with Oracle Solaris
 - What's there by default
 - How can I check my Servers?
 - How can I protect my Applications?
 - Hardening

Solaris 11 – Secure by Default (1/7)

- No direct root Login

```
g0086 console login: root
```

```
Password:
```

```
Roles can not login directly
```

```
Login incorrect
```

```
g0086 console login: marcel
```

```
Password:
```

```
Last login: Wed Sep 20 15:42:30 2017 from g0069.jomasoft-
```

```
Oracle Corporation      SunOS 5.11      11.3      March 2017
```

```
-bash-4.4$ su
```

```
Password:
```

```
Sep 20 17:16:55 g0086 su: 'su root' succeeded for marcel on /dev/console
```

Solaris 11 – Secure by Default (2/7)

- No direct root Login

```
-bash-4.4$ id  
uid=501(larry) gid=10(staff)
```

```
-bash-4.4$ su  
Password:  
Roles can only be assumed by authorized users  
su: Sorry
```

```
-bash-4.4$ grep roles=root /etc/user_attr  
admin::::lock_after_retries=no;profiles=System Administrator;roles=root  
marcel::::profiles=VDCF Logger,VDCF admin Module;roles=root
```


Solaris 11 – Secure by Default (3/7)

- Auditing is activated (for Logins)

```
# auditreduce -c lo | praudit -l | tail -4
```

```
header,69,2,login - ssh,fe,g0087,2017-09-01 15:37:32.707
```

```
+02:00,subject,root,root,root,root,root,6021,3233957173,15531 196630
```

```
g0069.jomasoft-lab.ch,return,failure,Permission denied
```

```
header,69,2,login - ssh,na:fe,g0087,2017-09-01 15:37:38.864 +02:00,subject,-
```

```
1,-1,-1,-1,-1,6023,3999938775,12434 196630 g0069.jomasoft-
```

```
lab.ch,return,failure,No account present for user
```

```
header,69,2,login - ssh,,g0087,2017-09-01 15:37:42.013
```

```
+02:00,subject,marcel,marcel,staff,marcel,staff,6026,3889292888,15007 65558
```

```
g0069.jomasoft-lab.ch,return,success,0
```

```
file,2017-09-01 15:37:42.000 +02:00,
```

Solaris 11 – Secure by Default (4/7)

- Unsafe Services are not running or not installed

```
-bash-4.4$ telnet g0086
Trying 192.168.100.86...
telnet: Unable to connect to remote host: Connection refused
```

```
-bash-4.4$ ftp g0086
ftp: connect: Connection refused
```

```
-bash-4.4$ ssh g0086
Last login: Wed Sep 20 17:18:35 2017 from g0069.jomasoft-
Oracle Corporation      SunOS 5.11      11.3      March 2017
-bash-4.4$
```

Solaris 11 – Secure by Default (5/7)

- Daemons as non-root with Privileges

```
# ps -f -u netadm,daemon,smmsp,dladm
```

UID	PID	PPID	C	STIME	TTY	TIME	CMD
daemon	75	1	0	Aug 28	?	0:00	/lib/crypto/kcfd
netadm	46	1	0	Aug 28	?	0:00	/usr/sbin/ibmgmt
netadm	66	1	0	Aug 28	?	0:02	/lib/inet/ipmgmt
dladm	52	1	0	Aug 28	?	0:02	/usr/sbin/dlmgmt
daemon	448	1	0	Aug 28	?	0:00	/usr/sbin/rpcbind -w
daemon	204	1	0	Aug 28	?	0:00	/usr/lib/utmpd
netadm	315	1	0	Aug 28	?	0:02	/lib/inet/nwamd
smmsp	644	1	0	Aug 28	?	0:00	/usr/lib/inet/sendmail -Ac-q15m

Solaris 11 – Secure by Default (6/7)

- Restrictive umask

```
-bash-4.4$ umask
```

```
0022
```

```
-bash-4.4$ touch /tmp/test
```

```
-bash-4.4$ ls -l /tmp/test
```

```
-rw-r--r--  1 marcel  staff           0 Sep  1 15:53 /tmp/test
```

Solaris 11 – Secure by Default (7/7)

- Role-based access control (RBAC)

```
-bash-4.4$ profiles -a | grep ZFS  
ZFS File System Management  
ZFS Storage Management
```

```
# usermod -P+"ZFS File System Management" marcel
```

```
-bash-4.4$ zfs create rpool/test1  
cannot create 'rpool/test1': permission denied
```

```
-bash-4.4$ pfbash  
bash-4.4$ zfs create rpool/test1
```

Solaris 11 – pkg verify

- Detect changes

```
-# ls -l /etc/shadow
-r----- 1 root      sys          807 May  8  2017 /etc/shadow

# chmod o+r /etc/shadow

# ls -l /etc/shadow
-r-----r-- 1 root      sys          807 May  8  2017 /etc/shadow

# pkg verify
PACKAGE                                STATUS
pkg://solaris/system/core-os           ERROR
    file: etc/shadow
        ERROR: Mode: 0404 should be 0400
```

Solaris 11 – pkg fix

- Revert changes

```
# pkg fix core-os
```

```
    Packages to fix: 1
```

```
    Create boot environment: No
```

```
    Create backup boot environment: Yes
```

```
    Repairing: pkg://solaris/system/core-os@0.5.11,5.11-  
0.175.3.14.0.5.0:20161105T004625Z
```

```
PACKAGE                                STATUS  
pkg://solaris/system/core-os           ERROR  
    file: etc/shadow                    ERROR: Mode: 0404 should be 0400
```

```
PHASE                                ITEMS  
Updating modified actions              1/1  
Updating package state database        Done  
Updating package cache                 0/0  
Updating image state                   Done  
Creating fast lookup database          Done  
Updating package cache                 2/2
```

```
# ls -l /etc/shadow
```

```
-r----- 1 root sys 807 May 8 2017 /etc/shadow
```

CVE

- **Common Vulnerabilities and Exposures**

Industrie Standard

Namingconvention for Security Bugs

Format: CVE-<jahr>-<nr>

Sample: CVE-2014-7187 (Bash/Shellshock)

Scoring: Common Vulnerability Scoring System (CVSS)

Medium 4 – 6.9 / High 7 – 8.9 / Critical 9 – 10

Search u.v.a. <https://www.cvedetails.com/>

Oracle Solaris	376
Redhat Enterprise Linux	426
Windows 7	820

Solaris 11.3 – CVE Metadata

- Required: Metadata Package installed

```
# pkg install solaris-11-cpu
```

- Analysis

Is Fix installed for CVE-2014-7187 (Bash/Shellshock)?

```
-bash-4.4$ pkg search -l CVE-2014-7187
```

INDEX	ACTION	VALUE	PACKAGE
info.cve	set	CVE-2014-7187	pkg:/support/critical-patch-update/solaris-11-cpu@2017.6-1



Is CVE-2017-3629 (Local Privilege Escalation) installed?

```
-bash-4.4$ pkg search -l CVE-2017-3629
```

```
-bash-4.4$
```



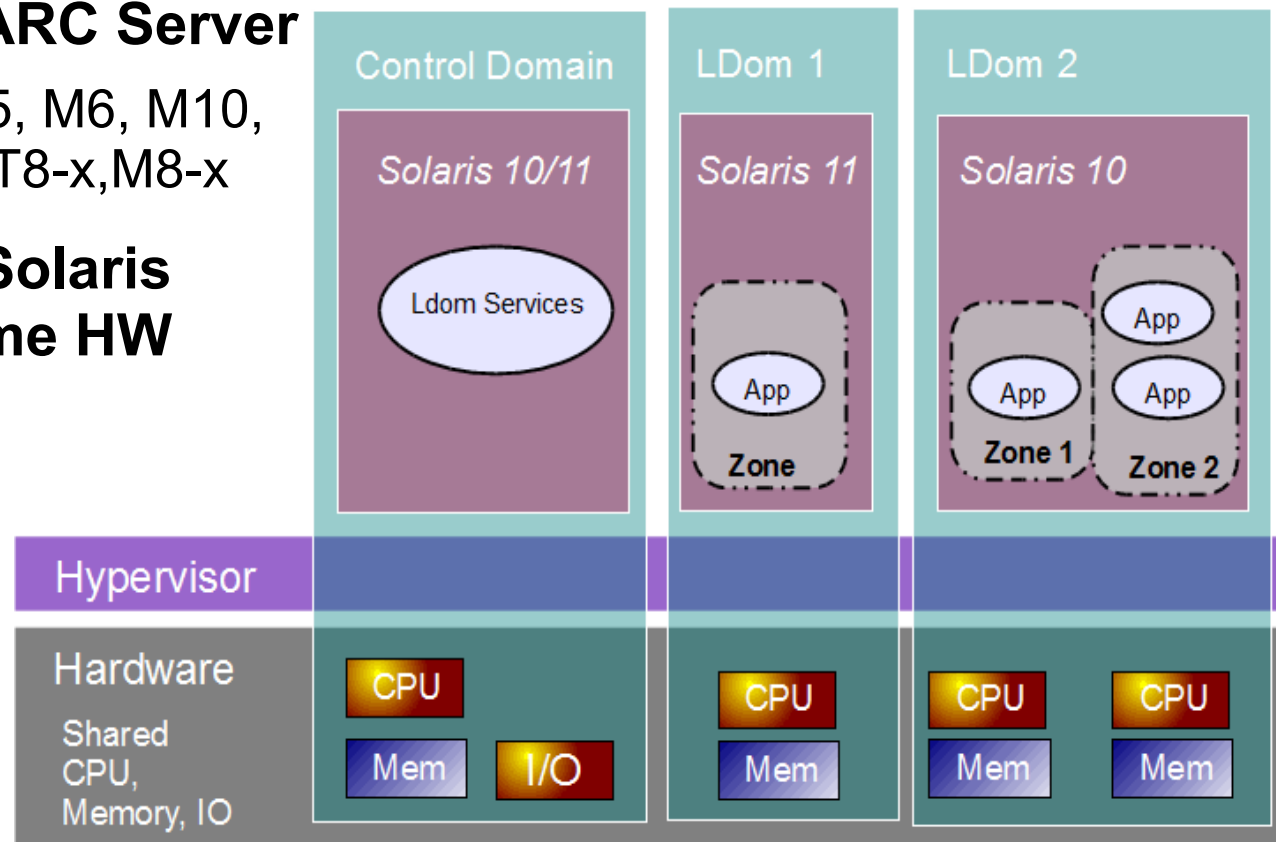
Which Update is required for CVE-2017-3629?

```
-bash-4.4$ pkg search CVE-2017-3629: | head -2
```

INDEX	ACTION	VALUE	PACKAGE
CVE-2017-3629	set	pkg://solaris/network/legacy-remote-utilities@0.5.11,5.11-0.175.3.22.0.3.0	pkg:/support/critical-patch-update/solaris-11-cpu@2017.7-1

SPARC-Virtualization: LDom / Zonen

- **Oracle & Fujitsu SPARC Server**
Systeme: T4-x, T5-x, M5, M6, M10, T7-x, M7-x, S7-2, M12, T8-x, M8-x
- **Multiple, separated Solaris Instances on the same HW**
- **Combine with Zones**
- **Dedicated Memory**
- **Hacker on one Zone or LDom has limited Impact**



Solaris – Virtualization using Zones

- Immutable (Read-Only) Zones

A) file-mac-profile=flexible-configuration

```
# touch /bla
touch: cannot change times on /bla: Read-only file system

# pkg install apache-22
pkg install: Could not complete the operation on /var/pkg/lock:
read-only filesystem.

# touch /etc/test
# touch /var/myfile
```

Solaris – Virtualization using Zones

- Immutable (Read-Only) Zones

B) file-mac-profile=fixed-configuration

```
# touch /bla
```

```
touch: cannot change times on /bla: Read-only file system
```

```
# pkg install apache-22
```

```
pkg install: Could not complete the operation on /var/pkg/lock:  
read-only filesystem.
```

```
# touch /etc/test
```

```
touch: cannot change times on /etc/test: Read-only file system
```

```
# touch /var/myfile
```

Solaris – Virtualization using Zones

- Immutable (Read-Only) Zones

C) file-mac-profile=strict

Completely Read-Only / Only Remote Logging

```
# touch /bla
touch: cannot change times on /bla: Read-only file system
# pkg install apache-22
pkg install: Could not complete the operation on /var/pkg/lock:
read-only filesystem.
# touch /etc/test
touch: cannot change times on /etc/test: Read-only file system
# touch /var/myfile
touch: cannot change times on /var/myfile: Read-only file system
```

Solaris – Virtualization using Zones

- Trusted Path for Immutable (Read-Only) Zones

Beispiel mit **file-mac-profile=strict**

```
-bash-4.1$ touch /etc/test  
touch: cannot change times on /etc/test: Permission denied
```

On the global Zone / No RW Reboot required

```
# zlogin -T v0128  
[Connected to zone 'v0128' pts/3]  
Oracle Corporation      SunOS 5.11      11.2      August 2014  
root@v0128:~# touch /etc/test
```

Solaris 11.3 – Compliance tool

- Based on OpenSCAP
- Checks Systems against predefined Rules
- Allows to detect changes on the System
- Produces detailed HTML Report

- **Execution:**

```
compliance assess -b solaris -p Baseline
```

```
compliance assess -b solaris -p Recommended
```

```
compliance assess -b pci-dss
```

Solaris 11.3 – Compliance tool



Compliance Report

Oracle Solaris Security Policy

Oracle Solaris Compliance baseline and recommended settings for general purpose operating systems installations.

Evaluation Characteristics

Target machine	v0175
Benchmark Title	Oracle Solaris Security Policy
Benchmark Version	1.14550
Benchmark Description	Oracle Solaris Compliance baseline and recommended settings for general purpose operating systems installations.
Profile ID	xccdf_tailored_profile__solaris_jomasoft
Started at	2017-04-26T18:35:14
Finished at	2017-04-26T18:35:42
Performed by	

CPE Platforms

- cpe:/o:oracle:solaris:11

Addresses

Compliance and Scoring

There were no failed or uncertain rules. It seems that no action is necessary.

Rule results

137 passed

Severity of failed rules

Score

Scoring system	Score	Maximum	Percent
urn:xccdf:scoring:default	100.000000	100.000000	100%

Solaris 11.3 – Compliance tool

- compliance Output

```
# compliance assess -b solaris -p Baseline
```

```
Assessment will be named 'solaris.Baseline.2017-09-01,16:37'
```

```
Package integrity is verified
```

```
OSC-54005
```

```
pass
```

```
The OS version is current
```

```
OSC-53005
```

```
pass
```

```
Service svc:/network/ftp:default is in disabled state
```

```
OSC-17510
```

```
pass
```

```
Service svc:/network/rpc/gss is enabled if and only if Kerberos is  
configured
```

```
OSC-63005
```

```
fail
```

SPARC – Silicon Secured Memory

- Integrated in SPARC CPU M7/M8 and S7
- You detect and prevent
 - Memory Reference Errors
 - Buffer Overruns
 - Memory Usage after free
- Alternatives in Software are expensive and 30x – 70x slower
- Oracle Developer Studio Compiler includes Support for Discovery at Development
- Demo Video about OpenSSL Heartbleed
https://swisdev.oracle.com/_files/ADI-Demo.html

SPARC – Silicon Secured Memory

```
void main(int argc, char *argv[])
{
    char *buffer = malloc( sizeof(char) * 10);
    strcpy(buffer, "Test-Text");
    for (int i = 0; i < 20; ++i)
        printf( "%c ", buffer[i] );
    printf("|\\n");
    free(buffer);
}
```

```
/opt/solarisstudio12.4/bin/cc -m64 -g -o buffer_overrun buffer_overrun.c
```

T	E	S	T	-	T	E	X	T			?		P	W	D				
---	---	---	---	---	---	---	---	---	--	--	---	--	---	---	---	--	--	--	--

```
-bash-4.4$ ./buffer_overrun
```

```
T e s t - T e x t |
```

SPARC – Silicon Secured Memory

With SSM (ADI) activated the Program is stopped and can't access foreign Memory.

```
-bash-4.4$ LD_PRELOAD_64=/lib/64/libadimalloc.so.1 ./buffer_overrun  
Segmentation Fault (core dumped)
```

```
-bash-4.4$ echo ::status | mdb core  
debugging core file of buffer_overrun (64-bit) from g0072  
file: /export/home/marcel/buffer_overrun  
initial argv: ./buffer_overrun  
threading model: native threads  
status: process terminated by SIGSEGV (Segmentation Fault), pc=100000bb0  
, ADI version d mismatch for VA ffffffff7e93ffc0
```

SPARC – Silicon Secured Memory

Detailed Results when using the Compiler Libraries

```
LD_PRELOAD_64=/opt/developerstudio12.5/lib/compiler/sparcv9/libdiscoverADI.so ./
```

```
buffer_overrun
```

```
T e s t - T e x t
```

1. ABR: reading memory beyond array bounds at address 0x2ffffff7cc7e040

```
main() + 0x60 (line ~12) in "buffer_overrun.c"
9: strcpy(buffer, "Test-Text");
10:
11: for (int i = 0; i < 20; ++i)
12: printf("%c ", buffer[i]);
13: printf("\n");
14:
15: free(buffer);

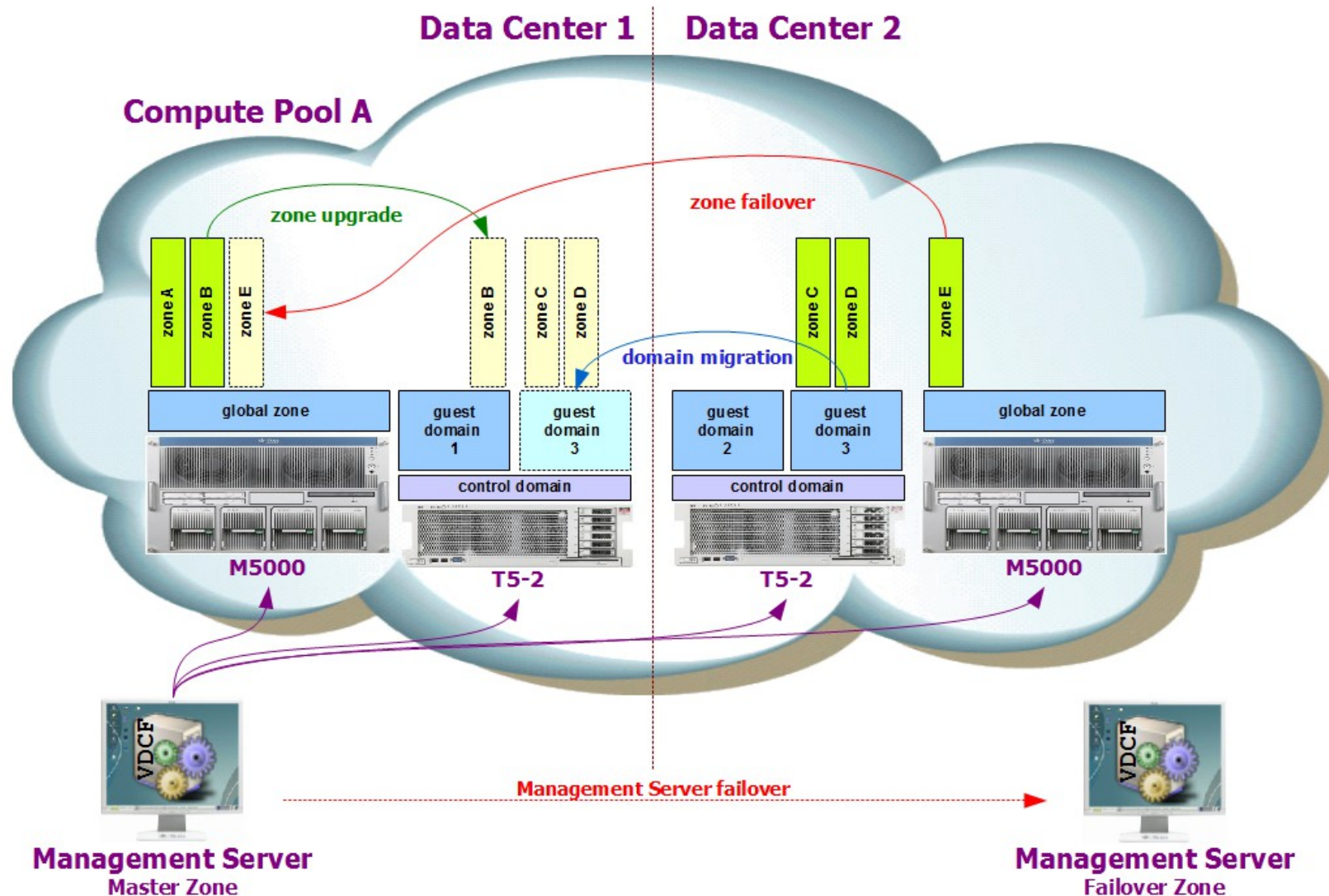
was allocated at (0x2ffffff7cc7e000, 64 bytes):

main() + 0x10 (line ~7) in "buffer_overrun.c"
4:
5: void main(int argc, char *argv[])
6: {
7: char *buffer = malloc( sizeof(char) * 10);
8:
9: strcpy(buffer, "Test-Text");
10:
```

VDCF – Virtual Datacenter Cloud Framework

- Management Tool for Zones and LDOMs
Installation, Operation, Migration,
Monitoring, Security and Failover/DR
- Supports Solaris 10 + 11 on SPARC/x86
- In productive use since 2006
- Dynamic Virtualization
Live / Cold Migration and Failover
- Resource Configuration and Monitoring
- Agility for your Enterprise Private Cloud
- Implemented by Admins for Admins

Dynamic Virtualization



VDCF – Compliance Assess

- 3 Standard Benchmarks: baseline, recommended, pci-dss

- VDCF Benchmarks: default & cdom

```
-bash-4.4$ more /var/opt/jomasoft/vdcf/conf/compliance/cdom.tailor
```

```
.....
# -----
# commented, activate if required
# -----

.....
# OSC-53005: The OS version is current
#exclude OSC-53005

...
# -----
# disabled to avoid failures
# -----
# OSC-55010: The r-protocols services are disabled in PAM
exclude OSC-55010
# OSC-73505: ssh(1) is the only service binding a listener to non-loopback addresses
exclude OSC-73505
# -----
# added to detect more than the baseline
# -----

.....
# OSC-47500: Passwords require at least 1 digits
include OSC-47500
# OSC-49500: Passwords require at least 1 upper-case characters
include OSC-49500
# OSC-93005: User home directories have appropriate permissions
include OSC-93005
.....
```

- Individual Benchmarks for Customers and Servers

VDCF – Compliance Assess

- Fully automated Compliance check over the Datacenter

```
osmon -c assess all all_vserver
```

- Compliance Report


[home](#)
[logout](#)

Compliance Report

Show entries

Server	Type	Benchmark	Score	Timestamp	# Passed	# Failed	# Error	# High	# Medium	# Low	# In
v0123	vServer	default	77.938248	2017-09-11T16.35.39	140	4	0	0	4	0	0
v0143	vServer	default	77.938248	2017-09-11T16.37.19	140	4	0	0	4	0	0
s0024	Node	cdom	87.619041	2017-09-11T16.02.22	140	3	0	1	2	0	0
g0062	Node	baseline	89.855064	2017-09-11T16.33.55	134	6	0	1	5	0	0
s0003	Node	cdom	95.238091	2017-09-11T14.58.15	142	1	0	1	0	0	0

Showing 1 to 5 of 5 entries

VDCF – Hardening

- Individual Hardening Profiles

```
-bash-4.4$ more /var/opt/jomasoft/vdcf/conf/compliance/baseline.hardening
OSC-12510: Service svc:/network/nfs/fedfs-client:default is in disabled state
OSC-63005: Service svc:/network/rpc/gss is enabled if and only if Kerberos is
configured
OSC-93005: User home directories have appropriate permissions
OSC-34010: Service svc:/application/cups/in-lpd:default is in disabled state
OSC-85000: The maximum number of waiting TCP connections is set to at least
1024
OSC-99011: Service svc:/system/rad:remote is in enabled state
```

- Hardening

```
-bash-4.4$ node -c harden name=g0087 profile=baseline
Hardening started ...
OSC-12510: Service svc:/network/nfs/fedfs-client:default is in disabled state
- DONE
OSC-34010: Service svc:/application/cups/in-lpd:default is in disabled state
- DONE
OSC-63005: Service svc:/network/rpc/gss is enabled if and only if Kerberos is
configured - DONE
OSC-85000: The maximum number of waiting TCP connections is set to at least
1024 - DONE (Changed from 128 to 1024)
OSC-93005: User home directories have appropriate permissions - DONE
OSC-99011: Service svc:/system/rad:remote is in enabled state - DONE
Hardening of 6 items on Node g0087 was successful
```

VDCF – Online Ressources

- **Produkt Documentation Online**

Complete Documentation and Videos on Webpage available

- **Free Edition**

No-Cost Test Version with limited number of managable Servers.

- **Test using combined POC**

Install and test together with JomaSoft on-site in your Test environment.

- **Webpage**

<https://www.jomasoft.ch/vdcf>

Ending Slide

Questions?

Marcel Hofstetter

hofstetter@jomasoft.ch

<http://www.jomasoftmarcel.blogspot.ch>

**CEO / Enterprise Consultant
JomaSoft GmbH**



Oracle ACE „Solaris“