

Sicher unterwegs mit Oracle Solaris

Marcel Hofstetter

hofstetter@jomasoft.ch

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

Geschäftsführer / Enterprise Consultant
JomaSoft GmbH

 **Oracle ACE „Solaris“**

Inhalt

- Wer ist JomaSoft?
- Solaris 11: Secure by Default
- Compliance tool
- SPARC Silicon Secured Memory
- Virtualisierung
- Compliance und Hardening mit VDCF

Wer ist JomaSoft?

- Software Unternehmen gegründet im Juli 2000
- Spezialisiert im Bereich **Solaris**,
Software Entwicklung & Services/Beratung
- Produkt **VDCF** (Virtual Datacenter Cloud Framework):
Installation, Management, Betrieb, Monitoring, Security
und DR von Solaris 10/11, sowie Virtualisierung
mittels LDoms und Solaris Zonen
- VDCF wird seit 2006 produktiv in Europa genutzt



Specialized
Oracle Solaris 11



Specialized
SPARC T5-Based Servers



Wer ist JomaSoft?

- Flexibel und Kunden fokussiert
- Oracle zertifizierte Mitarbeiter
- 17 Jahre Solaris Erfahrung
- Regelmäßige Oracle Solaris Beta Tester
- Gute Beziehungen zu Oracle Solaris & LDom Engineering Teams



Specialized
Oracle Solaris 11



Specialized
SPARC T5-Based Servers

IT Security

- Kein Thema in diesem Vortrag
 - Firewalls
 - Applikationsentwicklung
- Sicherheit mit Oracle Solaris
 - Was ist per Default vorhanden
 - Wie kann ich meinen Server prüfen?
 - Wie kann ich meine Applikation schützen?
 - Hardening

Solaris 11 – Secure by Default (1/6)

- Kein direkter 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 (2/6)

- Auditing ist aktiviert (für 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 (3/6)

- Unsichere Services sind nicht aktiv

```
-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 (4/6)

- Daemons als non-root mit Privilegien

```
# 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 (5/6)

- Restriktive 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 (6/6)

- 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

- Änderungen entdecken

```
-# 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

- Änderungen zurücksetzen

```
# 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**

Industriestandard

Namenskonvention für Sicherheitslücken

Format: CVE-<jahr>-<nr>

Beispiel: 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 Metadaten

- Voraussetzung: Metadaten Package installiert

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

- Auswertungen


Ist ein Fix für CVE-2014-7187 (Bash/Shellshock) installiert?

```
-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
```



Und CVE-2017-3629 (Local Privilege Escalation) installiert?

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



Welcher Update ist notwendig für 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
```

Solaris 11.3 – Compliance tool

- Basiert auf OpenSCAP
- Prüft Systeme gegen vordefinierte Regeln
- Damit können Änderungen am System erkannt werden
- Produziert HTML Report
- Ausführung:

```
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

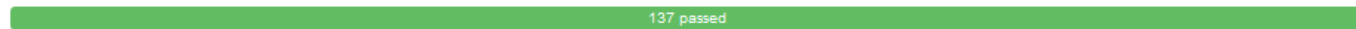
- cpe:/o:oracle:solaris:11

Addresses

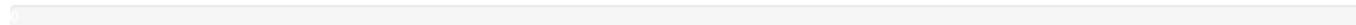
Compliance and Scoring

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

Rule results



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

- In den SPARC CPU M7/M8 und S7 integriert
- Damit entdeckt und verhindert man
 - Memory Referenz Fehler
 - Buffer Overruns
 - Memory Nutzung nach Freigabe
- Alternativen in Software sind teuer und 30x – 70x mal langsamer
- Oracle Developer Studio Compiler enthält Unterstützung für Discover während Entwicklung
- Demo Video zu 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

Mit SSM (ADI) aktiviert, wird Programm beendet und kann nicht auf fremdes Memory zugreifen

```
-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

Entwickler untersucht mit Compiler Tools

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

```
buffer_overrun
```

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

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

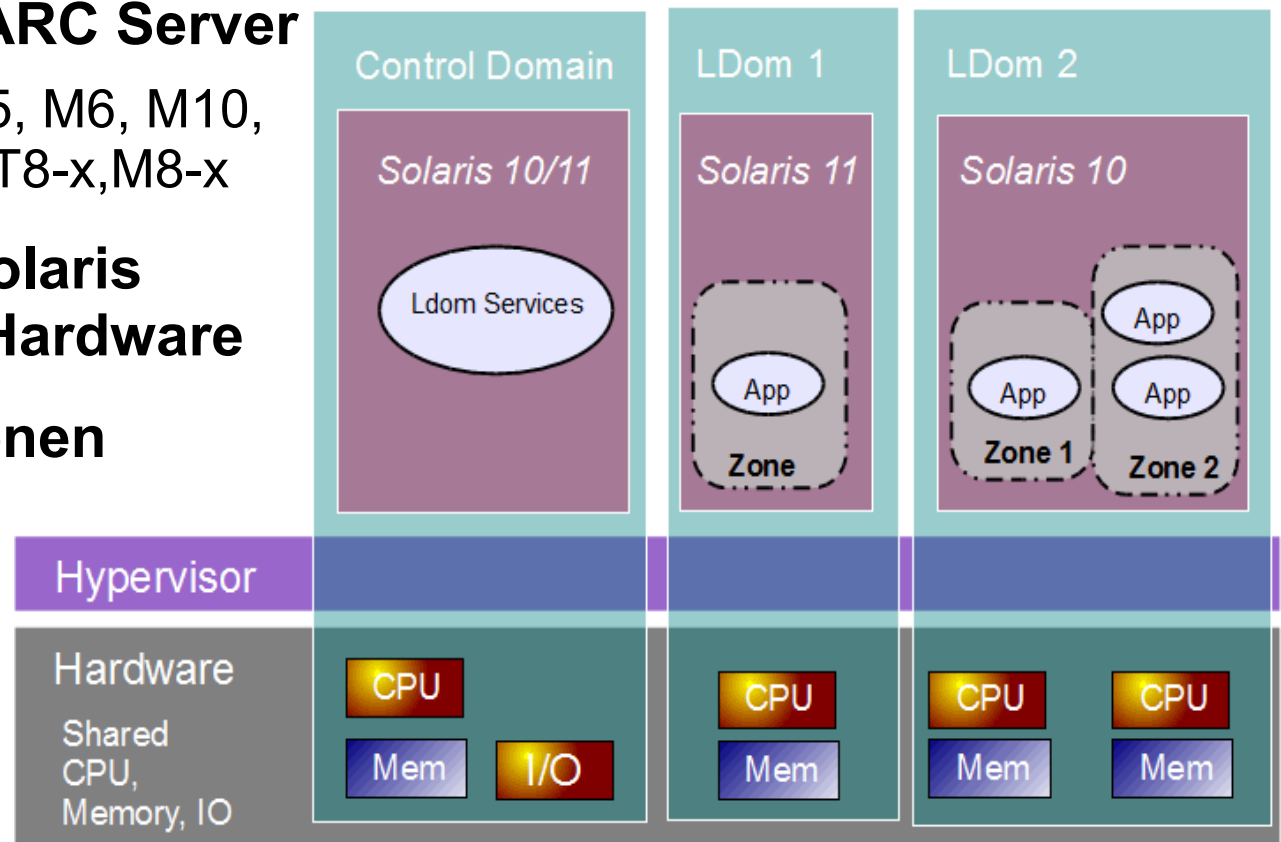
```
main() + 0x60 (line ~12) in "buffer_overrun.c"
9: strcpy(buffer, "Test-Text");
10:
11: for (int i = 0; i < 20; ++i)
12: printf("%c ", buffer[i]);
13: printf("\n");
14:
15: free(buffer);

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:
```

SPARC-Virtualisierung: LDomS / Zonen

- **Oracle & Fujitsu SPARC Server**
Systeme: T4-x, T5-x, M5, M6, M10, T7-x, M7-x, S7-2, M12, T8-x, M8-x
- **Mehrere, separate Solaris Instanzen auf einer Hardware**
- **Kombinierbar mit Zonen**
- **Dediziertes Memory**
- **Einbruch auf Zonen und LDomS hat begrenzte Auswirkung**



Solaris – Virtualisierung mit Zonen

- 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 – Virtualisierung mit Zonen

- 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 – Virtualisierung mit Zonen

- Immutable (Read-Only) Zones

C) file-mac-profile=strict

Wirklich Read-Only / Nur 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 – Virtualisierung mit Zonen

- Trusted Path für 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
```

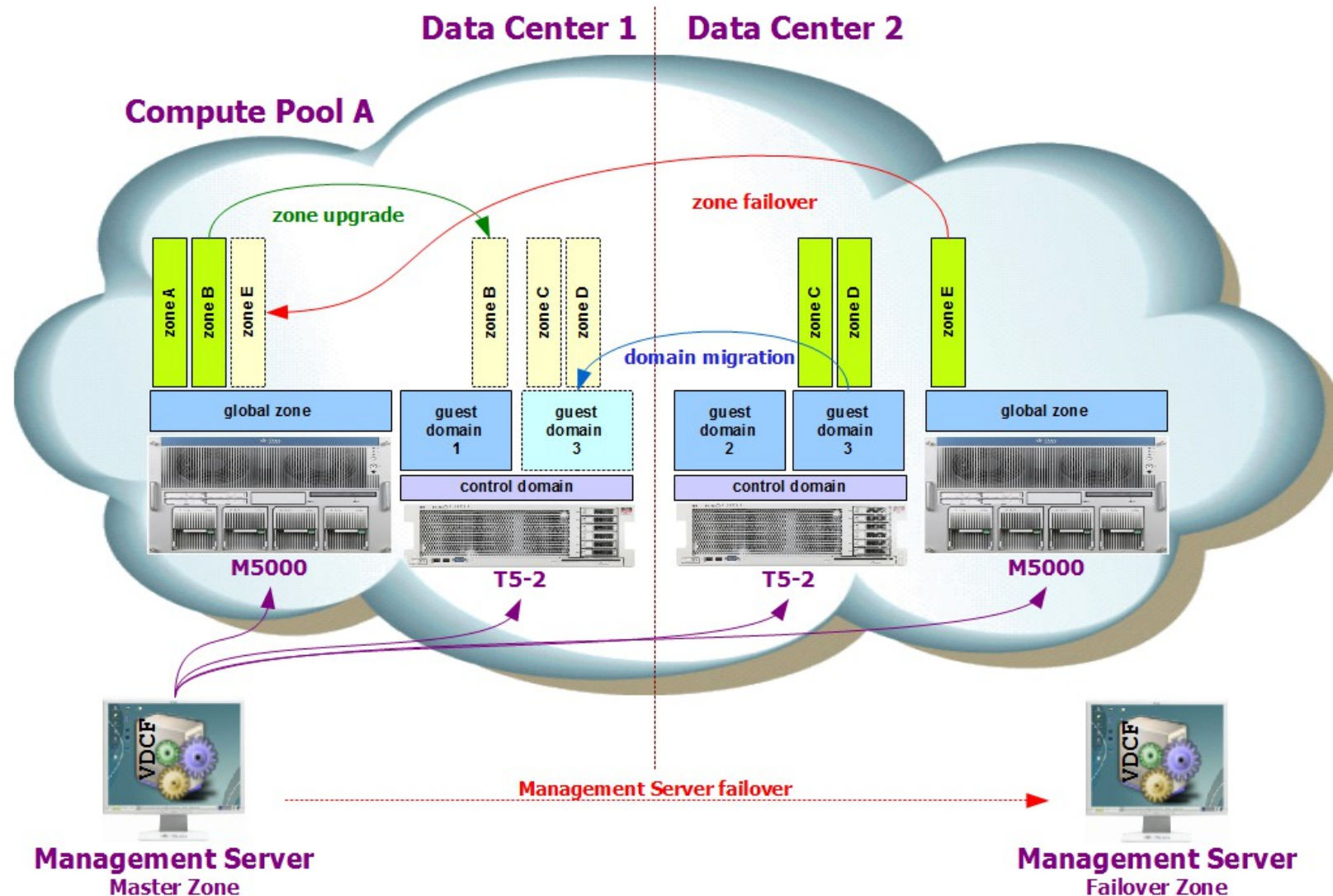
Aus globaler Zone / Kein RW Reboot notwendig

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

VDCF – Virtual Datacenter Cloud Framework

- Management Werkzeug für Zonen und LDoms:
Installation, Betrieb, Migration,
Monitoring, Security und DR/Failover
- für Solaris 10 + 11 / SPARC und X86
- Seit 2006 produktiv genutzt
- Dynamische Virtualisierung:
Live / Cold Migration und Failover
- Ressource Konfiguration und Monitoring
- Agilität für Enterprise Private Cloud
- Von Admins für Admins

Dynamische Virtualisierung



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  
.....
```

- Individuelle Benchmarks von Kunden und für Server

VDCF – Compliance Assess

- Automatisierter Compliance check übers Datacenter

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

- Compliance Report



VDCF Dashboard

[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

- Individuelle 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 – Mehr Infos

- **Produkt Dokumentation Online**

Komplette Dokumentation und Videos ab Webpage verfügbar

- **Free Edition**

Kostenlose Test-Version in der Anzahl verwaltbare Objekte limitiert.

- **Testen via POC**

Zusammen mit JomaSoft vor Ort eine Installation in Ihrer Testumgebung.

- **Webpage**

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

Sicher unterwegs mit Oracle Solaris

Fragen ?

Weitere interessante Vorträge zu Solaris an der #DOAG2017

Mi, 22.11. 11:00 Raum Budapest	„Angst vor dem Daten-Gau? Tipps für einen besseren Schlaf“ Thomas Nau
Mi, 22.11. 13:00 Raum Budapest	„Solaris 11 The Road Ahead“ Joost Pronk
Mi, 22.11. 15:00 Raum Neu Delhi	„Solaris 11.next für SAP“ Jan Brosowski
Do, 23.11. 10:00 Raum Hongkong	„DTrace Deep Dive“ Thomas Nau
Do, 23.11. 16:00 Raum Riga	„Rapid Deployment von OS, VM und App“ Marcel Hofstetter

Marcel Hofstetter

hofstetter@jomasoft.ch

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