Sicher unterwegs mit Oracle Solaris

Marcel Hofstetter
Oracle ACE
JomaSoft GmbH
St. Gallen / Schweiz

Schlüsselworte
Betriebssysteme, Oracle Solaris, RZ Security, Compliance, Virtualisierung

Einleitung
IT Sicherheit ist wichtiger denn je. Dieser Vortrag erläutert die vorhandenen Technologien in Oracle Solaris 11. Die einzelnen Technologien werden anhand von praktischen Beispielen erklärt.
Nicht behandelt werden die Themenbereiche Firewalls und Applikationssicherheit.

Oracle Solaris 11
Solaris weist eine sehr lange Geschichte im Datacenter auf. Mit seiner Robustheit und Qualität konnte es immer gut überzeugen. Solaris 11 ist seit dem Jahr 2011 auf dem Markt und wird durch monatliche Updates weiterentwickelt. Das Betriebssystem enthält zahlreiche Funktionen für die Sicherheit.

Dieser Vortrag erläutert die verfügbaren Technologien im Bereich der Sicherheit. Solaris 11 wird "Secure by Default" installiert. Konfigurationsanpassungen können durch Security Compliance checks erkannt werden. Auf SPARC Systemen können Buffer Overflows verhindert werden. Die Virtualisierungs Lösungen führen mit der Separation von Applikationen zu höherer Sicherheit des Gesamtsystems.

JomaSoft GmbH
Die JomaSoft wurde als Software und Beratungs-Unternehmen im Jahr 2000 gegründet. Als Oracle Gold Partner sind wir insbesondere auf Oracle Solaris 11 und SPARC Server spezialisiert. Wir bieten Software-Entwicklung, Consulting, Implementation und Administration im Bereich Solaris. Abgerundet wird unser Angebot durch das Produkt VDCF (Virtual Datacenter Cloud Framework). Eine Management Software für System Administratoren, welches die Installation, das Management und Desaster Recovery von Solaris Servern, Solaris Zonen und LDoms vereinfacht und automatisiert. Selbstverständlich sind auch hilfreiche Monitoring und Sicherheits Funktionen integriert. Unterstützt sind die Betriebssystem Versionen Solaris 10 und Solaris 11 auf den Plattformen SPARC und x86. Dieses Framework wird bei zahlreichen Kunden in Europa seit mehr als 10 Jahren produktiv eingesetzt.

Secure by Default
Logins werden per default in Audit Logs festgehalten und man kann nicht direkt als root User einloggen. Damit ist sichergestellt, dass nachvollzogen werden kann, wer als root arbeitet.
Unsichere Services (ftp, telnet, usw) sind nicht aktiviert und die Daemons laufen nicht unter root, sondern unter separaten Usern, welche nur mit den notwendigen Privilegien ausgestattet sind.
Falls User höhere Rechte benötigen, sind sie nicht gezwungen als root User zu arbeiten, sondern für entsprechende Tätigkeiten liegen RBAC (Role Based Access Control) Profiles vor. Wenn ein User beispielsweise ZFS Filesysteme erstellen muss, reicht die Zuordnung das RBAC Profiles „ZFS Filesystem Management“ an den entsprechenden User.

Compliance Tool
Das Solaris Tool 'compliance' basiert auf OpenSCAP. Ein laufendes System kann gegen vordefinierte Sicherheits Benchmark geprüft werden. Ein Benchmark besteht aus einer Anzahl Rules. Solaris enthält ab der Version 11.1 die drei Benchmarks „Solaris/Baseline“, „Solaris/Recommended“ und „pci-dss“. Zudem sind system-spezifische Anpassungen (Tailoring) seit Solaris 11.3 unterstützt, damit Systeme gegen individuelle Benchmarks geprüft werden können. Basierend auf einem der drei oben erwähnten Benchmarks werden einzelne Rules entfernt (exclude) oder ergänzt (include).
Das Tool produziert detaillierte HTML Reports, welche genau auflisten, welche Regeln nicht eingehalten sind und was auf dem System durchgeführt werden muss um die Regeln einzuhalten.

SPARC Silicon Secured Memory (SSM)
Buffer Overflows und andere Memory Handling Fehler von Applikationen können auf den aktuellen SPARC CPU's (S7, M7 und M8) durch die Hardware erkannt werden. Greift eine Applikation auf fremdes Memory zu, wird die Applikation mit einem core beendet. Damit kann sichergestellt werden, dass Hacker keine Daten erhalten, wie es beispielsweise mit dem OpenSSL Heartbleed Bug der Fall war.

Die Oracle Developer Studio Compiler enthalten ebenfalls Unterstützung für SSM und ermöglichen den Software Entwicklern Memory Handling Fehler frühzeitig und effizient zu finden.

Videos zu SSM/ADI mit OpenSSL Heartbleed Demo
https://swisdev.oracle.com/_files/ADI-Demo.html

Virtualisierung
Applikationen können unter Solaris einfach separiert werden durch den Einsatz von Logical Domains und/oder Solaris Zonen. Jede Solaris Zone ist von den anderen isoliert, hat eigene Prozesse und Filesysteme und individuelle User. Ein Sicherheitsmangel einer Applikation hat dadurch keinen Einfluss auf die anderen Applikationen, welche auf demselben physischen Server betrieben werden.
Auch ein Einbruch eines Hackers auf eine Solaris Zone hat deshalb nur limitiertes Potential.

Solaris Zonen können sogar gehärtet als read-only Images betrieben werden, damit ein Angreifer keine Möglichkeit für Manipulationen hat.

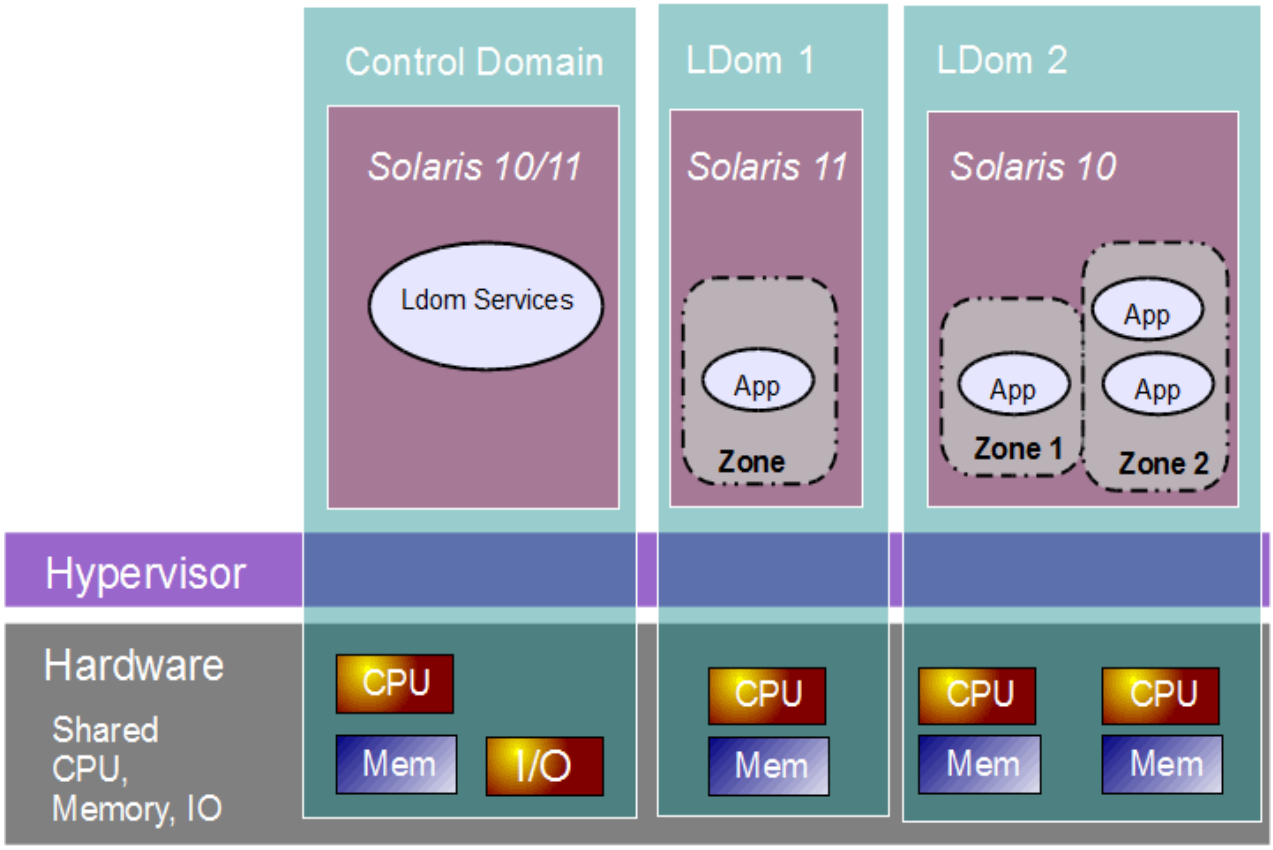
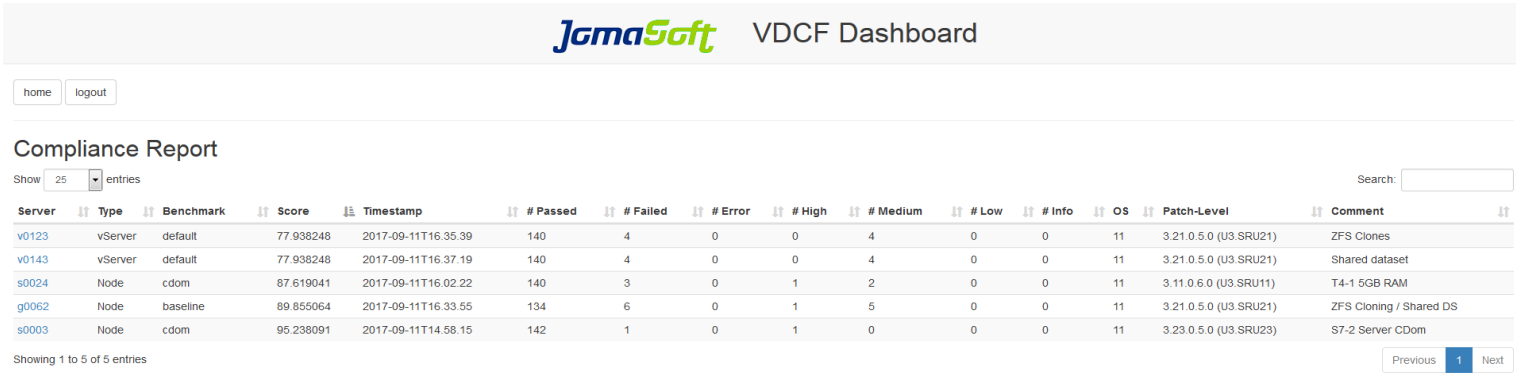


Abbildung 1: Solaris/SPARC Virtualisierung mit Logical Domains (Doms) und Solaris Zonen.

Compliance und Hardening mit VDCF
Das JomaSoft VDCF Management Framework enthält im neuesten Release 7.0 Unterstützung für Compliance Assess und Hardening. Mittels einem Aufruf können die Solaris Systeme im Rechenzentrum auf Ihren Sicherheitstand überprüft werden.

Das VDCF Dashboard bietet mit dem Compliance Report eine zentrale Übersicht über die durchgeführten Compliance Assessments. Für jedes System ist ein detaillierter Report abrufbar.



Server	Type	Benchmark	Score	Timestamp	# Passed	# Failed	# Error	# High	# Medium	# Low	# Info	OS	Patch-Level	Comment
v0123	vServer	default	77.938248	2017-09-11T16.35.39	140	4	0	0	4	0	0	11	3.21.0.5.0 (U3.SRU21)	ZFS Clones
v0143	vServer	default	77.938248	2017-09-11T16.37.19	140	4	0	0	4	0	0	11	3.21.0.5.0 (U3.SRU21)	Shared dataset
s0024	Node	cdom	87.619041	2017-09-11T16.02.22	140	3	0	1	2	0	0	11	3.11.0.6.0 (U3.SRU11)	T4-1 5GB RAM
g0062	Node	baseline	89.855064	2017-09-11T16.33.55	134	6	0	1	5	0	0	11	3.21.0.5.0 (U3.SRU21)	ZFS Cloning / Shared DS
s0003	Node	cdom	95.238091	2017-09-11T14.58.15	142	1	0	1	0	0	0	11	3.23.0.5.0 (U3.SRU23)	S7-2 Server CDom

Abbildung 2: VDCF Dashboard mit Compliance Report

Der grösste Aufwand für die System Administration besteht beim Hardenen eines System, weil dies häufig manuell erfolgen muss und fehleranfällig ist.

Um diesen Aufwand zu minimieren enthält unser VDCF Management Framework seit der neusten Version 7.0 Funkionen und Hardening Profile um Systeme automatisiert zu härten. Die Hardening Profile referenzieren die Regeln aus den Compliance Benchmarks. So wird es zum Kinderspiel die vom Compliance Assesssment gelisteten Regeln, welche nicht erfüllt sind via VDCF Hardening korrekt umzusetzen.

Sample Output

```
-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
```

Die gesamte VDCF Produkt Dokumentation ist öffentlich. Eine frei verfügbare Test-Version "VDCF Free Edition" ist auf unserer Website ebenfalls zu finden: **https://www.jomasoft.ch/vdcf**

Kontaktadresse:
Marcel Hofstetter
JomaSoft GmbH
Falkensteinstrasse 54a
CH-9000 St. Gallen

Telefon		+41 (0)71-288 92 11
E-Mail		hofstetter@jomasoft.ch
Blog		https://jomasoftmarcel.blogspot.ch/
Twitter		https://twitter.com/marcel_jomasoft
Oracle ACE Solaris		Oracle ACE Listing
Firmen Webpage		https://www.jomasoft.ch

V1.0 (25.09.2017)