Security in Solaris 11.2 – eingebaut, nicht nur angebaut

Jörg Möllenkamp, ORACLE Deutschland B.V. Co & KG

Ende April 2014 hat Oracle mit der Ankündigung von Solaris 11.2 und der Freigabe einer Public Beta für diese Version dem Nutzer einen ersten Blick auf die Neuheiten im bevorstehenden Release des bewährten Enterprisebetriebssystems ermöglicht. Mehr als 500 neue Funktionen – von der OpenStack-Integration über ein an Solaris angepasstes mitgeliefertes Puppet bis hin zu einer Erweiterung der Virtualisierungsfunktionen von Solaris mit den Kernelzonen – können so jetzt schon getestet werden. Auch im Bereich „Security" wurde die Entwicklung konsequent weitergeführt. Dieser Artikel greift aus diesem Bereich einige Neuheiten heraus, die den Nutzer bei der Bereitstellung sicherer Systeme auf Basis von Solaris 11.2 unterstützen.

Eine herausragende Neuerung in diesem Bereich ist die Integration eines Compliance-Frameworks in Solaris 11.2. Es gibt im Sicherheitsbereich das geflügelte Wort, dass Sicherheit zu einem Prozent aus Tools besteht, aber zu 99 Prozent aus der korrekten Implementation dieser Tools und der korrekten Implementation der zu betreibenden Applikation und des Betriebssystems. Das könnte man fast so stehen lassen, ist aber so nicht ganz vollständig: Mindestens so wichtig wie Tools und korrekte Konfiguration ist die stete und ständige Überprüfung. Entspricht ein System initial einem Satz von Best Practices, die entweder man selbst, eine Organisation oder ein Hersteller, definiert haben, ist das System nach einer Vielzahl von administrativen Maßnahmen über die Monate und Jahre immer noch in diesem Zustand. Jedoch wird es mit der Anzahl von physikalischen und virtuellen Servern immer schwieriger diese Kontrollen manuell durchzuführen.

Solaris 11.2 bietet nun die Möglichkeit, die Antwort auf diese Fragestellungen zu automatisieren. Schon für Solaris 11.1 wurde „openscap" als Paket bereitgestellt und somit die technische Grundlage zur Verfügung gestellt. Es ist eine Implementierung des Security Content Automation Protocol und gibt dem Administrator ein Werkzeug an die Hand, automatisiert ein System hinsichtlich der Befolgung von in XML definierten Regeln zu überprüfen. Bisher musste man für Solaris diese Regeln allerdings selber bereitstellen respektive öffentlich verfügbare Regelsätze selbst an Solaris anpassen.

Solaris 11.2 integriert nun mehrere Standardsätze von Regeln, die dem Nutzer zur Verfügung stehen: Dies ist zum einen ein Oracle-spezifischer Regelsatz, der in zwei Stufen „recommended" und „baseline" benutzt werden kann. Interessanter ist aber die an Solaris angepasste Darstellung des Payment Card Industry Data Security Standards (PCI-DSS). Oracle hat diese Vorgaben in ein Regelwerk umgesetzt, das die Besonderheiten von Solaris berücksichtigt (und seien es nur Namen oder Lokationen für bestimmte wichtige Dateien). Nach der Installation des entsprechenden Pakets reichen zwei Befehle, um einen Report zu erhalten, ob man sich an dieses vielfach genutzte und oft auch vorgeschriebene Regelwerk hält *(siehe Listing 1)*. Daraus resultiert ein HTML-Report, der zu den Punkten Erläuterungen gibt, in denen das System noch Anpassungsbedarf hat *(siehe Abbildung 1)*.

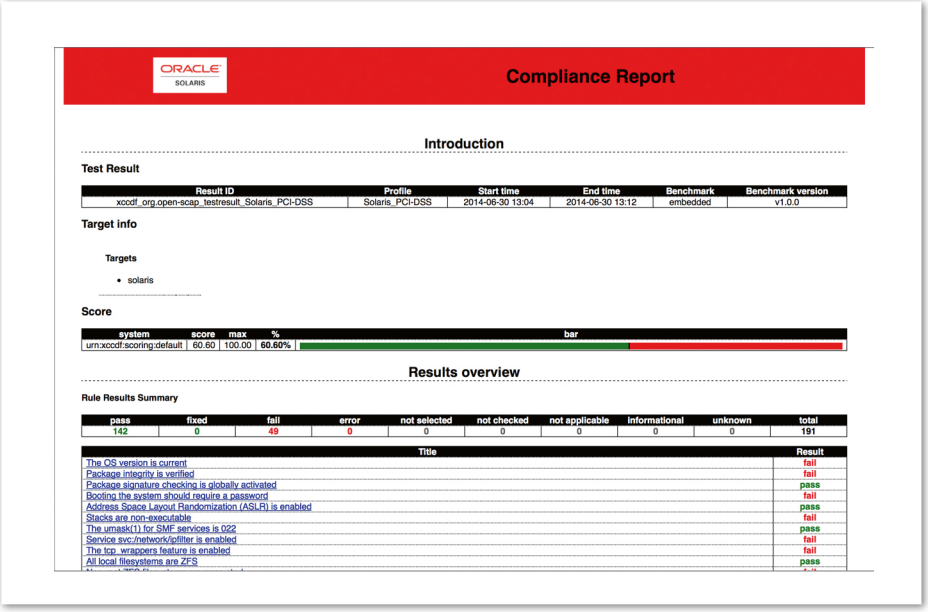
Zones weiterentwickelt

Schon seit Version 10 existiert in Solaris eine Virtualisierungstechnik namens „Solaris Zones". Es handelt sich um eine Technologie, die auf Basis eines einzelnen Kernels Nutzern und Applikationen einzelne voneinander gekapselte Instanzen des Betriebssystems zur Verfügung stellt. Für viele Solaris-Administratoren ist es damit seit geraumer Zeit selbstverständlich, Applikationen in eigenen virtuellen Betriebssystem-Umgebungen zu kapseln. Sie müssen aber dafür nicht den Overhead in Kauf nehmen, der vielen anderen Virtualisierungslösungen zu eigen ist. Dieser Overhead entsteht bei Solaris Zonen durch das Funktionsprinzip bedingt nicht oder nur sehr minimal.

Von einer Betriebssystem-Instanz, der „Global Zone" ausgehend, die vereinfacht gesagt den Kernel bereitstellt und die Interaktion mit der Hardware durchführt, kann eine Vielzahl von weiteren Betriebssystem-Instanzen installiert und gestartet werden. Diese erscheinen dem User oder der Applikation als unabhängiges Be-

```
# pkg install security/compliance
# compliance assess -b pci-dss
Assessment will be named 'pci-dss.Solaris_PCI-DSS.2014-04-14,16:39'
# compliance report -a pci-dss.Solaris_PCI-DSS.2014-04-14,16:39
```

Listing 1



ORACLE SOLARIS

Compliance Report

Introduction

Test Result

Result ID	Profile	Start time	End time	Benchmark	Benchmark version
xccdf_org.open-scap_testresult_Solaris_PCI-DSS	Solaris_PCI-DSS	2014-06-30 13:04	2014-06-30 13:12	embedded	v1.0.0

Target info

Targets

- solaris

Score

system	score	max	%	bar
urn:xccdf:scoring:default	60.60	100.00	60.60%	

Results overview

Rule Results Summary

pass	fixed	fail	error	not selected	not checked	not applicable	informational	unknown	total
142	0	49	0	0	0	0	0	0	191

Title	Result
The OS version is current	fail
Package integrity is verified	fail
Package signature checking is globally activated	pass
Booting the system should require a password	fail
Address Space Layout Randomization (ASLR) is enabled	pass
Stacks are non-executable	fail
The umask(1) for SMF services is 022	pass
Service svc:/network/ipfilter is enabled	fail
The tcp_wrappers feature is enabled	fail
All local filesystems are ZFS	pass

Abbildung 1: Darstellung der Ergebnisse aus dem Solaris 11 Compliance Framework

```
# zlogin fixed
[Connected to zone 'fixed' pts/3]
Oracle Corporation      SunOS 5.11      11.2    April 2014
root@fixed:~# ppriv -De touch /etc/passwd
touch[117063]: MWAC(5) policy violation (euid = 0, syscall = "utimen-
sat") for "/etc/passwd" at fop_setattr+0x10b
touch: cannot change times on /etc/passwd: Read-only file system
root@fixed:~# logout
[Connection to zone 'fixed' pts/3 closed]
# zlogin -T fixed
[Connected to zone 'fixed' pts/3]
Oracle Corporation      SunOS 5.11      11.2    April 2014
root@fixed:~# ppriv -De touch /etc/passwd
root@fixed:~#
```

Listing 2

triebssystem unter anderem mit eigenem User-Namensraum und eigenem -Filesystem, gegebenenfalls auch eigenem TCP-Stack, verfügen aber nicht über einen eigenen Kernel.

Das Konzept der Zone ist schon an sich ein interessantes Sicherheits-Feature: Es ermöglicht die Trennung von administrativen Sphären. Ein Administrator der globalen Zone sieht sämtliche Vorgänge im System. Ein Super-User in der non-global Zone hat aber nur genau diese Zone im Zugriff. Er kann nicht auf andere Zonen einwirken, in seiner eigenen Zone aber frei walten.

Praktisch gesagt: Der Super-User einer Webserver-Zone hat keinen Zugriff auf die Komponenten der Datenbank-Zone und umgekehrt.

Nun möchte man aber selbst dieses freie Walten zumindest zeitweilig einschränken beziehungsweise es nur erlauben, wenn es unbedingt notwendig ist. Hierzu konnte Solaris 11 schon in der Vergangenheit mit den „Immutable Non-Global Zones“ eine entsprechende Konfigurationsoption bieten. Diese ermöglicht dem Administrator der globalen Zone, eine nicht-globale Zone in einen Zustand zu versetzen, in der von innerhalb der Zone keine Änderung an der Betriebssysteminstanz mehr möglich ist.

In der Innensicht ist die Zone „read only“ (genau genommen betrifft dies nur den sogenannten „zone root“, das Filesystem der Zone). Andere Filesysteme können je nach Konfiguration durchaus beschreibbar sein.

Egal, welche Privilegien ein User in einer Zone hat, er kann beispielsweise keine Files des Betriebssystems editieren, Binaries austauschen, Pakete installieren oder Services aktivieren oder deaktivieren. Dieses Feature ist nicht nur nützlich, um einen Angreifer, der irgendwie durch ein Sicherheitsproblem einer Applikation in das System gelangt ist, von der Änderung des Systems abzuhalten. Gleichzeitig unterbindet es wirkungsvoll Änderungen am System an Change-Prozessen vorbei.

Natürlich unterliegen auch diese Zonen der Notwendigkeit gelegentlicher Änderung. Damit in diesen Immutable Zones Konfigurationen durchgeführt werden können, war es bisher erforderlich, die Zone in einem speziellen Modus neu zu starten oder die Änderungen mit „root“-Rechten von der globalen Zone aus durchzuführen. Allerdings sind oft weder der Neustart noch die Weitergabe entsprechender Rechte wünschenswert. In Oracle Solaris 11.2 ist daher die Funktion des „trusted path“ hinzugekommen. Loggt sich ein User damit ein, kann er Änderungen als Administrator auch innerhalb der Zone ausführen. Erfolgt der Login nicht über „trusted path“, ist dies nicht möglich. Für „non-global zones“ ist dieser „trusted path“ mit der Option „-T“ beim Befehl „zlogin“ erreichbar *(siehe Listing 2)*.

Globale Zonen

Die logische Weiterentwicklung war es nun, diese Option der nicht änderbaren Zone auch für die globale Zone zu ermöglichen, um Änderungen in diesem bisher nicht eingeschränkten Bereich zu unterbinden. Dies wurde in Solaris 11.2 implementiert und ermöglicht es dem Administrator, das vollständige System gegen Änderungen abzusichern. Eine Änderung ist dann nur noch über „trusted path“ möglich. Anders als jener der „non-global zone“ ist dieser nur über die Console erreichbar und wird über das Senden der Breaksequenz erreicht.

Die Möglichkeiten der Einschränkungen sind genau wie bei den nicht-globalen Zonen: Ein „strict“, das jedwedes Schreiben ohne Ausnahmen unterbindet, ein „fixed-configuration“, das zumindest den Schreibzugriff auf „/var“ ermöglicht und ein „flexible-configuration“, das Änderungen an der Konfiguration, nicht aber am installierten Betriebssystem zulässt.

```
# zonecfg -z global
zonecfg:global> set file-mac-profile=flexible-configuration
zonecfg:global> commit
```

Listing 3

```
# usermod -K access_times='{sshd-none,sshd-password,sshd-kbdint,sshd-
pubkey,sshd-hostbased}:Wk0900-1700' junior
```

Listing 4

```
root@solaris# profiles -p "MySQL Service"
MySQL Service> set desc="Locking down the MySQL Service"
MySQL Service> add cmd=/lib/svc/method/mysql_51
MySQL Service:mysql_51> set privs=basic
MySQL Service:mysql_51> add privs={file_write}:/var/mysql/5.1/data/*
MySQL Service:mysql_51> add privs={file_write}:/tmp/mysql.sock
MySQL Service:mysql_51> add privs={file_write}:/var/tmp/ib*
MySQL Service:mysql_51> end
MySQL Service> set uid=mysql
MySQL Service> set gid=mysql
MySQL Service> exit
root@solaris#
```

Listing 5

Eine globale Zone kann sehr einfach in den "immutable"-Zustand versetzt werden *(siehe Listing 3)*. Nach dem nächsten Reboot ist die globale Zone dann "immutable".

Interessant ist hier zusätzlich, das der „trusted path“ einen getrennten PAM-Service („tdplogin“) nutzt und so die Möglichkeiten von PAM zur Absicherung gesondert konfiguriert werden können (siehe auch nachfolgend unten der neu hinzugekommenen Möglichkeit zur zeitlichen Einschränkung).

Minimalismus

Insbesondere im Security-Bereich ist weniger oft mehr. So wenig wie möglich zu installieren, um ein System zu betreiben, gilt als Standard in der Installation sicherer Systeme. Ziel ist es oft, keine Pakete auf dem System zu haben, die nicht unmittelbar für den Betrieb notwendig sind, weil jedes weitere Paket aus Sicht dieser Denkweise nur unnötige mögliche Angriffsvektoren öffnet.

In der Praxis verhält es sich allerdings so, dass die Standard-Installation eine sehr reichhaltige Anzahl von Paketen enthält, um einer großen Anzahl von Usern gleichzeitig gerecht zu werden. In der Folge stellt sich die Frage, was davon wieder sicher entfernt werden kann, ohne die Funktion des Betriebssystems einzuschränken.

Solaris unterstützt hier jetzt mit einer fertigen Zusammenstellung des Systems, die das absolute Minimum einer unterstützten Solaris-Umgebung darstellt. Diese Umgebung stellt so eine gute Ausgangsbasis für einen minimierten Server dar. Dem Zweck entsprechend heißt dieser Paket-Cluster „solaris-minimal-server“.

Darüber hinaus soll das Feature der „Baseline Installation“ nicht unerwähnt bleiben. Mit dem neuen Kommando „pkg exact-install“ kann das Paketverwaltungs-System IPS von Solaris ein Paket installieren. In dieser Hinsicht unterscheidet es sich nicht von einer normalen Installation. Die Besonderheit von „exact-install“ ist aber, dass gleichzeitig alle Pakete entfernt werden, von denen dieses neue Paket nicht abhängig ist. So lassen sich elegant Pakete bauen, die nichts anderes als Paket-Abhängigkeiten enthalten, um eine Art Baseline zu definieren. Nennt man dieses Paket praktischerweise „baseline“, kann mit dem Befehl „# pkg exact-install baseline“ das System auf diese Baseline zurückversetzt werden, indem man es mit

„-n“ in einer Art Trockenlauf benutzt. Es kann auch alternativ dazu verwendet werden, um festzustellen, welche Pakete auf einem System zusätzlich zu dieser Baseline installiert worden sind und welche Pakete gegenüber dieser Basis fehlen.

Seit 11.2 ist nun in Solaris die Möglichkeit eingebaut, eine Funktion sowohl zeitlich als auch räumlich eingeschränkt zu nutzen. Mit räumlich ist hier natürlich der Server gemeint. Ein einfaches „usermod“ reicht hier aus, um beispielsweise dem User „junior“ nur wochentags zwischen 9 und 17 Uhr den login via SSH zu erlauben *(siehe Listing 4)*.

Weitere neue Features

Über die genannten Features hinaus wurden in Solaris 11.2 weitere Funktionen hinzugefügt, die man als wesentliche Bestandteile eines Sicherheitskonzeptes sehen kann: Wie schon eingangs erwähnt ist in der neuen Version des Betriebssystems eine angepasste Version von Puppet verfügbar. Damit ist es dem Administrator möglich, seine Arbeit zu automatisieren und so der Fehleranfälligkeit dutzendfach manuell ausgeführter Prozesse zu entziehen. Mit den Solaris Kernel Zones existiert eine Form der Virtualisierung, die wie eine schon bekannte Zone administriert wird, aber einen eigenen Kernel verwendet und so aus Sicherheitssicht den gelegentlich geäußerten Einwand adressiert, dass sich nicht-globale Zonen einen Kernel teilen und darüber ein bestimmter Patch-Stand festgeschrieben wird.

Schon in Solaris 11.1 wurde mit „pfedit“ ein Tool hinzugefügt, das es dem Administrator ermöglicht, die Änderung an Konfigurationsfiles an nicht privilegierte User zu delegieren. Unterwirft man „pfedit“ dem Solaris Auditing – ein lange in Solaris verfügbares Features, das seit Solaris 11 per Default eingeschaltet ist und somit zur Aktivierung keines Neustarts mehr bedarf – werden im Auditlog sogar die Änderung in der Form von „diff“-Ausgaben protokolliert. Es wird somit nachvollziehbar, wer welche Veränderungen durchgeführt hat.

Ebenfalls schon seit dem letzten Release verfügbar ist die Funktion der Extended Policies. Dieses ermöglicht dem Administrator sehr fein granular die Rechte eines Prozesses zu beschränken über die normalen Unix-Mechanismen hinaus bis beispielsweise auf Port-, Datei- oder Verzeichnis-Ebene. Beispielsweise kann ein Prozess, der unter einem User läuft, auch alle Files dieses Users beschreiben. Oft ist dies aber weder erwünscht noch notwendig. Mit den in Solaris 11.1 hinzugefügten Extended Policies kann ich hier feiner eingreifen und beispielsweise einem Prozess das Schreiben nur in wenigen Verzeichnissen und in wenigen Dateien erlauben *(siehe Listing 5)*.

Fazit

Mit Solaris 11.2 konnte auf den bereits umfangreichen Sicherheitsmechanismen von Solaris aufgebaut werden, um diese neuen Anforderungen anzupassen. Sie stellen Sicherheit in einer Art und Weise zur Verfügung, die nicht nur angebaut ist, sondern eben als integraler Bestandteil eines Betriebssystems, das von vornherein mit einer übergreifenden, ineinandergreifenden Architektur geplant ist.

Literaturhinweise

1. Überblick über die großen Neuerungen in Solaris 11.2: www.oracle.com/technetwork/server-storage/solaris11/documentation/solaris11-2-whatsnew-2191087.pdf
2. Zusammenstellung von Links, die die beschriebenen Teilbereiche näher beleuchten: www.c0t0d0s0.org/doag-news-security

Joerg Moellenkamp
joerg.moellenkamp@oracle.com

Das vierte Release von Cloud Control 12c im Überblick

Ralf Durben, ORACLE Deutschland B.V. & Co. KG

Seit Anfang Juni 2014 ist das vierte Release von Cloud Control 12*c* verfügbar. Neben einigen Bugfixes wurden vor allem zahlreiche neue Features eingebaut. Gerade die kleinen Neuerungen sind für alle, die Cloud Control einsetzen, interessant und werden in diesem Artikel kurz vorgestellt.

Nach der Installation von Cloud Control 12*c* Release 4 fällt in der grafischen Benutzer-Oberfläche (GUI) sofort auf, dass deren Optik etwas moderner gestaltet ist. Bilder und Fonts sind leicht verändert, die Kopfzeile hat jetzt einen schwarzen Hintergrund und die Kontraste wurden optimiert. Die Benutzersteuerung selbst bleibt aber gleich, sodass sich die Nutzer von Cloud Control sofort damit zurechtfinden. Funktional sind sowohl im Basis-Framework als auch in den einzelnen Plug-ins viele Neuerungen zu finden, die die tägliche Arbeit erleichtern.

Security

Gerade im Bereich „Security“ gibt es mit dem neuen Release interessante Neu-