„-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-

erungen. Man kann jetzt Gruppen noch besser nutzen, um Zugriffsprivilegien zu vergeben. Bis Release 3 konnte eine Gruppe von Zielsystemen zwar als „Privilege Propagation Group“ erstellt werden. Das Zugriffs-Privileg (beispielsweise „View“ oder „Full“) wurde aber nur für die Gruppe inklusive der darin befindlichen Zielsysteme vergeben. Wenn ein EM-Benutzer also das „Full“-Recht an den Mitgliedern der Gruppe bekommen sollte, bekam er dieses Recht auch auf die Gruppe selbst. Das ist nun anders. Mit einer Checkbox „Advanced Privilege Settings“ lassen sich die vergebenen Privilegien trennen *(siehe Abbildung 1)*:

- Privilegien für Gruppe und Mitglieder
- Privilegien nur für die Gruppe
- Privilegien nur für die Mitglieder

Um Privilegien zu vergeben, ist ein Rollenkonzept sehr hilfreich, damit einem neuen EM-Benutzer alle notwendigen Privilegien schnell zugänglich gemacht werden können. Leider gab es hier Einschränkungen. So konnten zum Beispiel die Nutzung benanntern Credentials („Named Credentials“) und Rechte für Jobs nicht an Rollen vergeben werden. Jetzt gibt es neue „Private Rollen“, die jeder EM-Benutzer erstellen kann, der mit dem Privileg „CREATE ROLE“ ausgestattet ist. Diesen privaten Rollen können jetzt auch Rechte für „Named Credentials“ und „Jobs“ übertragen werden.

Ein neuer EM-Benutzer muss üblicherweise einige Einstellungen vornehmen, um später reibungslos arbeiten zu können. Dazu gehört die Definition von „Preferred Credentials“, also die Angabe, mit welchen Credentials (zum Beispiel „Benannte Credentials“) sich dieser Benutzer an einem Ziel anmelden möchte. Mit dem neuen Release kann der Super-Administrator dazu ein Default vorgeben, „Global Default Preferred Credentials“. Diese können zielbezogen oder global vorgegeben sein. Die Einstellung ist ein Default für jeden EM-Benutzer, der dieses aber auch für sich selbst überschreiben kann *(siehe Abbildung 2)*.

Die neue Security Console in Cloud Control gibt einen sehr guten Überblick über alle Einstellungen im Bereich „Security“. Vor allem die Best-Practice-Analyse hilft sehr bei der optimalen Absicherung des Systems *(siehe Abbildung 3)*.

Monitoring

Beim Monitoring gibt es auch einige Neuerungen. So wird für Benachrichtigungen jetzt auch der Versionsstandard „3“ für „SNMP Traps“ unterstützt. Eigene Metriken („Metric Extensions“) können ab sofort auch auf Daten im Repository zugreifen. Dazu wird unterschieden zwischen „Metric Extension“ und „Repository-Side Metric Extension“. Man gibt eine SQL-Query an, die auf eine Tabelle oder View im Repository zugreift. Diese wird als Datenbankbenutzer „MGMT_VIEW“ ausgeführt.

Für eine effektive Nutzung von Benachrichtigungsmethoden sind alle Events zu „Incidents“ zusammengefasst. Darauf lassen sich sogenannte „Incident Rules“ definieren, die angeben, wie bei einer Problemsituation zu verfahren ist. Mit einem neuen Simulator lässt sich vorab testen, ob die Definition dieser Regeln auch korrekt ist. Dabei wird das Auftreten eines Events simuliert und angezeigt, wie das Regelwerk darauf reagieren würde.

Wenn ein Agent auf einem Zielsystem ausfällt, kann das verschiedene Gründe haben, die bislang nicht alle erkannt wurden. Aus diesem Grund wird ab Release 4

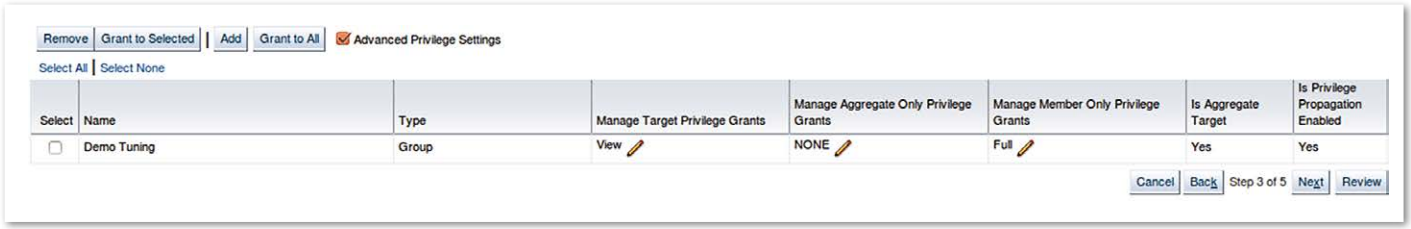

Abbildung 1: Privilegien-Vergabe für Gruppen

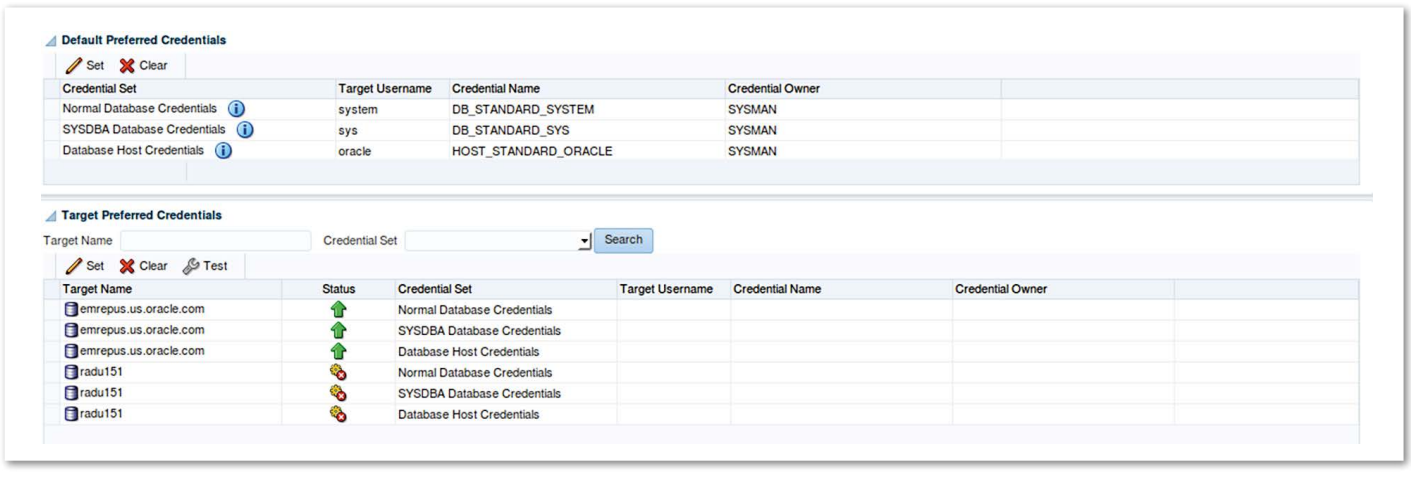

Abbildung 2: Default Preferred Credentials

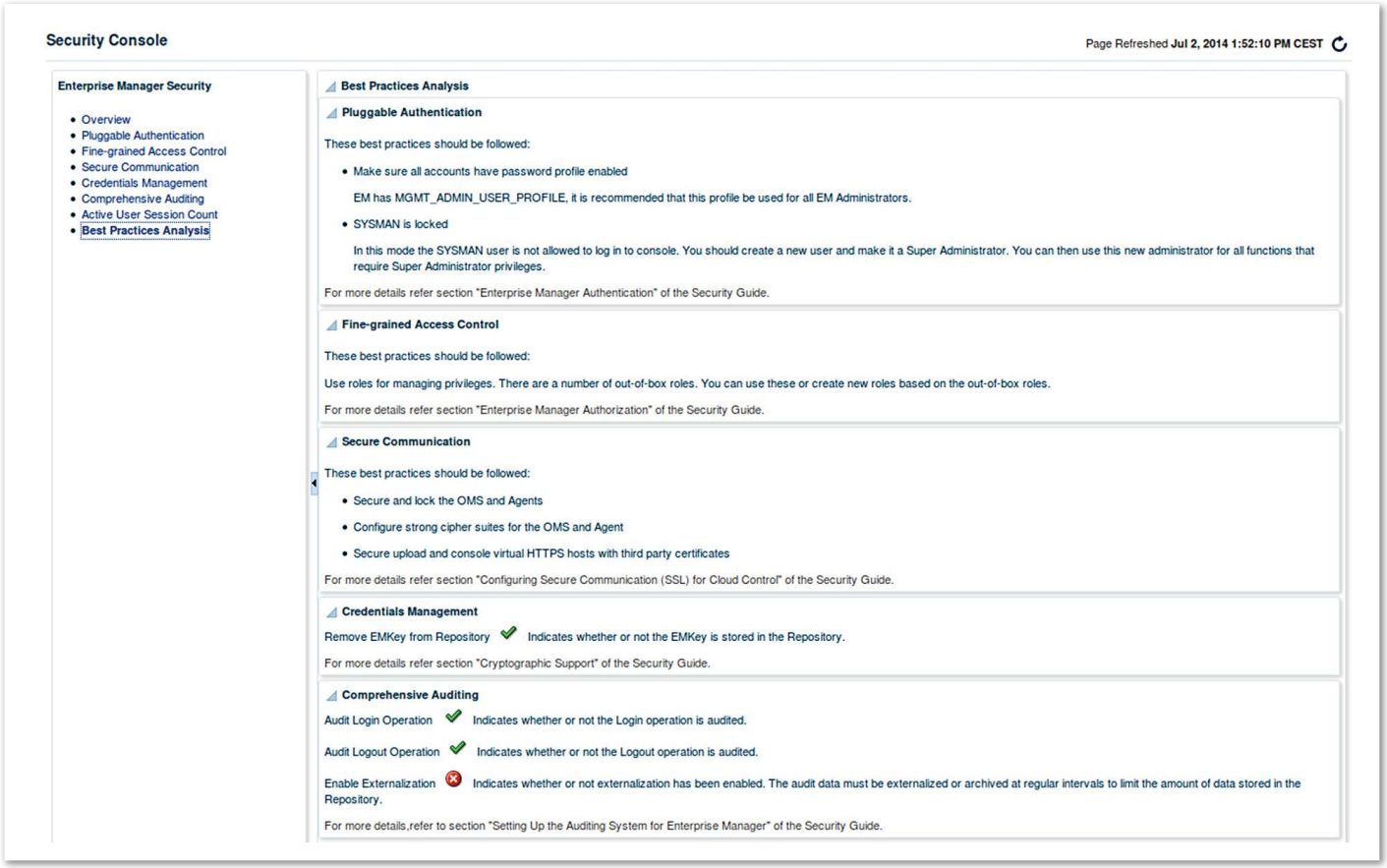

Abbildung 3: Security Console

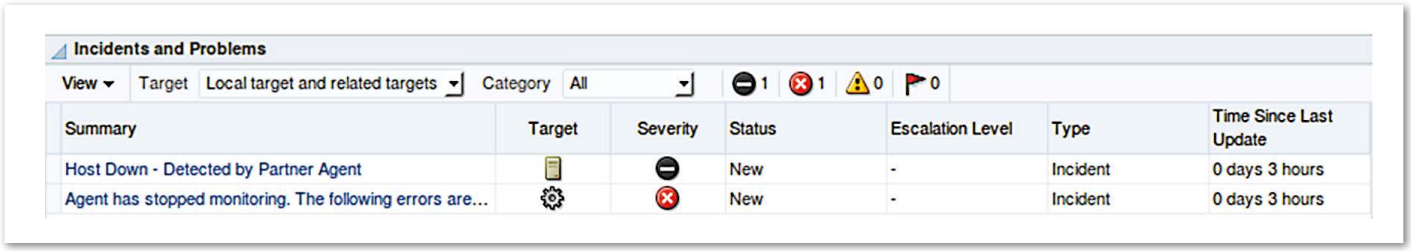

Abbildung 4: Überwachung durch Partner-Agent

von Cloud Control jedem Agenten ein sogenannter „Partner-Agent" automatisch zugeordnet. Dieser beobachtet, ob der Agent noch ordentlich funktioniert. Dadurch kann zum Beispiel besser ermittelt werden, ob ein Host noch verfügbar ist, obwohl der eigentlich zuständige Agent sich nicht mehr meldet. Entsprechend genauer sind auch die Meldungen im Bereich „Incidents and Problems".
Abbildung 4 zeigt die Situation eines heruntergefahrenen Host, dessen Zustand durch den Partner-Agenten ermittelt wurde.

Reporting

Im Bereich „Reporting" hat sich seit Release 1 von Cloud Control einiges verändert. Das Reporting, das auch noch von Grid Control bekannt ist („Information Publisher"), ist ein Auslaufmodell. Die bevorzugte Variante setzt auf den BI Publisher. Dieser ist im Rahmen der Nutzung für Cloud Control auch in der „Restricted Use"-Lizenz enthalten.
Der große Vorteil des BI Publishers liegt neben den größeren Möglichkeiten bei der Visualisierung vor allem in der flexibleren Nutzung der Inhalte des EM-Repository.

Bisher musste der BI Publisher separat installiert und konfiguriert werden. Ab Release 4 wird er automatisch installiert und verbraucht dabei wesentlich weniger Plattenplatz. An dieser Stelle sei auch auf die mögliche Nutzung des „Database Usage Tracking Reports" hingewiesen, der einen guten Überblick über alle Datenbank-Optionen gibt, die in den von EM verwalteten Datenbanken genutzt werden.

Lifecyle von Cloud Control

Der große Vorteil von Cloud Control im Vergleich zu Grid Control besteht im modularen Aufbau. Neben dem zentralen Framework wird die Unterstützung verschiedener Zielsysteme und Funktionalitäten durch Plug-ins realisiert, die eine eigene Versionierung haben. Das Deployment neuer Plug-ins beziehungsweise neuer Versionen von Plug-ins ist oft mit einem Neustart des Oracle Management

Servers (OMS) verbunden. Daher liegt der Wunsch nahe, ein Deployment mehrerer Plug-ins gleichzeitig vorzunehmen. Mit Release 3 war dies mit Enterprise Manager Command Line Interface (EMCLI) möglich, ab Release 4 funktioniert es auch in der grafischen Oberfläche.

Die Installation des Agenten auf Windows-Servern wurde im Handbuch immer mit der Installation von „CYGWIN", einer Open-Source-Software, beschrieben. Vielen Kunden ist deren Nutzung jedoch nicht möglich. Technisch gab es auch schon in den Releases 2 und 3 eine Alternative, die ab sofort auch offiziell im Handbuch beschrieben ist. Sie ist mit einer neuen Integration in die Windows-spezifische Lösung „PSExec" verbunden.

Download

Cloud Control 12*c* Release 4 steht nicht nur als Installationsmedium zur Verfügung. Es gibt auch vorgefertigte VMs für Oracle VM und VirtualBox. Erstere ist gedacht für den produktiven Einsatz, zum Beispiel in einer ODA. Die VM für VirtualBox ist dagegen zum Testen oder für den Einsatz in kleinen Umgebungen gedacht. Alle Downloads sind auf OTN zu finden.

Fazit

Das Release 4 von Cloud Control 12*c* bietet viele Neuerungen. Dieser Artikel kann nur eine kleine Auswahl vorstellen. Ein Upgrade von älteren Releases auf Release 4 ist jedenfalls sehr zu empfehlen.

Weitere Informationen

- Zertifizierung: https://support.oracle.com/CSP/ui/flash.html#tab=CertifyHomePageV2%28page=CertifyHomePageV2&id=gqttszvh%28%29%29
- Handbücher: http://docs.oracle.com/cd/E24628_01/index.htm
- Download: http://www.oracle.com/technetwork/oem/grid-control/downloads/index.html
- Tipps zu Oracle Enterprise Manager Cloud Control: http://www.oracle.com/webfolder/technetwork/de/community/dbadmin/contents.html#CC

Ralf Durben
ralf.durben@oracle.com