OEM 12c Cloud Control - mal ohne "Superuser für Alle"

Thomas Enders und Stefan Waldschmitt
Selbständige Berater
Region Frankfurt

Schlüsselworte

Oracle Enterprise Manager Cloud Control 12c, Security, Rechtekonzept, Zugriffsverwaltung, Administration Groups, Anbindung an LDAP / Active Directory, Named Credentials, Enterprise User Security, Superuser

Einleitung

Im Bereich der IT Infrastruktur ist Sicherheit eine der Schlüsselkomponenten, insbesondere die Verwaltung von Zugriffsrechten. In der Oracle Welt trifft man auf dieses Thema in allen Ebenen, beginnend bei dem Front-End, über die Middleware, bis hin zur Datenbank und den in diesem Zusammenhang verwendeten Tools.

Auch ein zentrales Verwaltungssystem, wie Oracle Enterprise Manager bildet hier keine Ausnahme. Mit der Einführung von Cloud Control 12c hat Oracle durch Einführung von mehr als 200 Detailberechtigungen und Konstrukten, wie „Administration Groups“ und „Named Credentials“, die Grundlage geschaffen, solchen Anforderungen gerecht zu werden.

Dieser Vortrag möchte die Möglichkeiten und Einschränkungen im Bereich der Rechteverwaltung aufzeigen und dem Anwender Konzepte und Anregungen an die Hand geben um die Sicherheitsanforderungen des eigenen Unternehmens zu erfüllen.

Anforderungen an das Enterprise Manager Security-Konzept

Gängige Anforderungen an das Security Konzept von Systemen, wie der Oracle Enterprise Manager, sind gerade in größeren Unternehmen unter Anderem:

- Einschränkung des Zugriffs auf eine untermenge der vorhandenen Targets (unterschiedliche Support Teams für Regionen oder Abteilungen)
- Umsetzung verschiedener Berechtigungsstufen für ein Target (Zugriff für Entwickler oder L1-, L2- und L3-Support mit unterschiedlichen Berechtigungen)
- Verwaltung von OEM internen Ressourcen (Designer konfiguriert Ressourcen für den Operator)

Die Umsetzung in OEM

Auch wenn die neuen Funktionen und Erweiterungen in der aktuellen Version des Enterprise Managers eine anforderungsgerechte Umsetzung von Security-Vorgaben ermöglichen, kann dies gerade in größeren Umgebungen schnell unübersichtlich werden. Eine gute Planung und ein detailliertes Konzept helfen dies zu vermeiden.

OEM 12c unterscheidet generell zwischen Privilegien für den Umgang mit Targets und mit OEM eigenen Ressourcen. Während Target-Privilegien den Zugriff auf Informationen zu einzelnen Targets, Target-Gruppen oder allen Targets gewähren, steuern Ressourcen-Privilegien die Verwendung von OEM-Ressourcen. Für eine bessere Wahrung der Übersicht, lässt sich diese Aufteilung auch gut im Rollenkonzept aufgreifen.

Während sich aufgabenbezogene Ressourcen-Rechte einfach in nur wenigen Rollen abbilden lassen, kann sich die Vergabe von Target-Rechten je nach Anforderung deutlich aufwändiger gestalten. Die neu eingeführten Administration Groups sind hierbei auch wichtiger Bestandteil des Security-Konzeptes, da hiermit eine automatische Zuordnung von Targets zu Gruppen anhand ihrer Target-Eigenschaften erfolgt. Diese Gruppierung bietet eine hervorragende Grundlage für die Vergabe von Rechten für eine Teilmenge der Targets. Beispielsweise könnte der Administrator nun eine Rolle mit Target Rechten für L1-Support, L2-Support und L3-Support für jede dieser Gruppen anlegen. Eine Abstufung der Rechte und Einschränkung auf Teilmengen wäre hiermit auf einfache Art und Weise umsetzbar. Jede dieser Rollen enthält dann lediglich die entsprechenden Target-Rechte der zugeordneten Gruppe. Je nach Anforderungen können sich hierdurch zwar eine sehr große Anzahl an Rollen ergeben, die sich aber unter Zuhilfenahme des Command Line Utility „emcli“ einfach verwalten lassen.

Um eine Zuordnung der einzelnen Benutzer zu den erstellten Target- und Ressource-Rollen zu verwirklichen, empfiehlt sich die Einführung eines weiteren Rollen-Typs. In Team-Rollen lassen sich einerseits mehrere Benutzer für die Rechtevergabe und andererseits alle benötigten Rollen mit Ressource- und Target-Rechten zuordnen. Dadurch wird jederzeit eine Konsistenz innerhalb der Teams sichergestellt. Die nachfolgende Abbildung illustriert ein solches Rollen Modell.

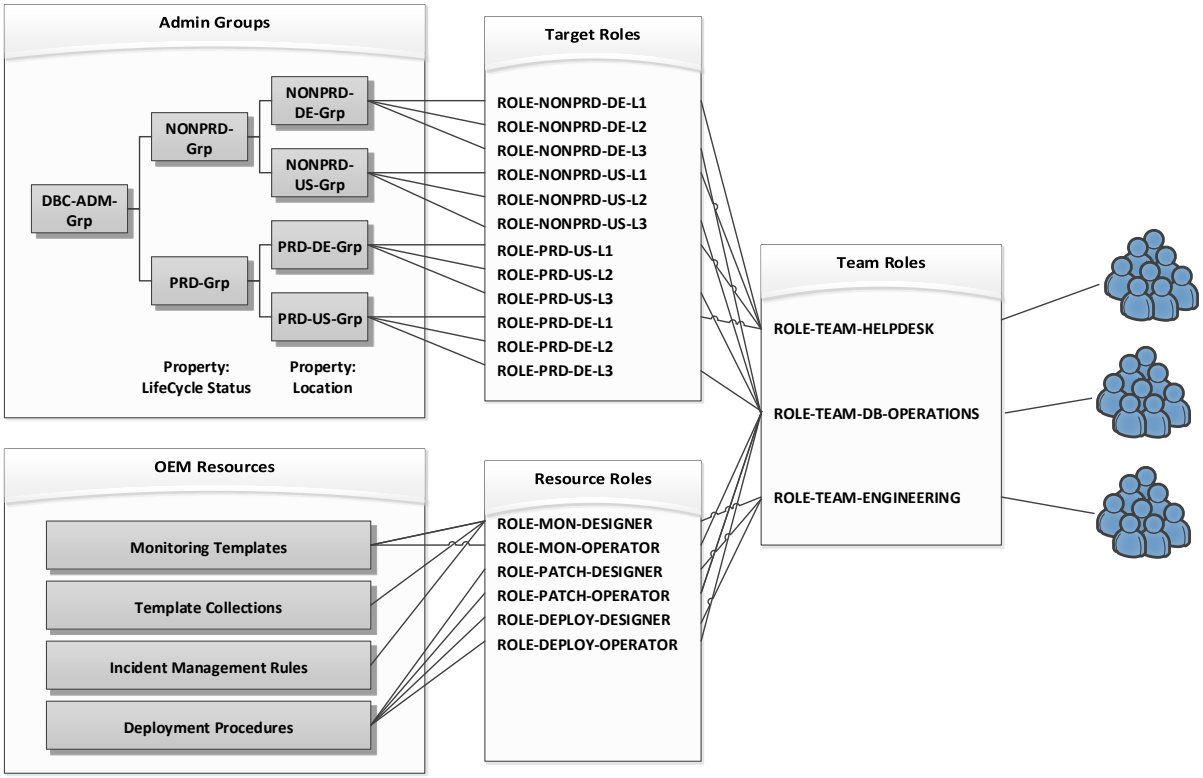

Abb. 1: Rollen für Target-Rechte mit Zuordnung zu automatisch verwalteten „Admin Groups“

LDAP und Microsoft Active Directory Authentifizierung

Mit der Verwaltung eigener Benutzer und Teams werden auch Begriffe, wie Re-Zertifizierung und „Joiner-Leaver-Process“ zum Thema für eine solche Anwendung. Diese meist unangenehmen Aufgaben lassen sich durch die Anbindung an bereits vorhandene „LDAP“ oder „MS Active Directory“ Systeme mit bestehenden Prozessen elegant umgehen. Durch einige wenige Konfigurationsänderungen in OEM lassen sich die Verwaltung von Benutzern und die Zuordnung zu Teams beinahe vollständig in ein solches externes System verlagern.

Die Anbindung an ein externes LDAP-System und die daraus resultierenden Vorteile werden hier im Folgenden näher betrachtet. Durch den folgenden Kommandozeilen-Aufruf wird OEM für die Authentifizierung mittels LDAP vorbereitet:

```
emctl config auth oid -ldap_host "ldap.dbc4oracle.de" -ldap_port "389" \
  -ldap_principal "cn=DBC_USR_ID_ADMIN" -user_base_dn "cn=users,dc=dbc4oracle,dc=de" \
  -group_base_dn "cn=groups,dc=dbc4oracle,dc=de" -ldap_credential "**" -sysman_pwd "**"
```

Neben den Verbindungsinformationen zum LDAP Server, wie dessen Hostnamen, Port und einem LDAP Benutzer mit ausreichenden Berechtigungen, werden hier zusätzlich der „Distinguished Name“ des Containers für Benutzer und Gruppen abgegeben. Dieser Vorgang legt für den Weblogic Server einen neuen „Authentication-Provider“ namens „EM_OID_Provider“ an. Weitere Details und Einstellungen, die OEM im Hintergrund vorgenommen hat, sind in der Datei „config.xml“ im Verzeichnis „…/gc_inst/user_projects/domains/YourDoainName/config“ einsehbar.

Nach der Umstellung lassen sich nun Benutzer ohne eigenes Kennwort im OEM anlegen. Die Zuordnung von Rollen kann weiterhin manuell in OEM oder aber durch Zuordnung der Benutzer zu LDAP Gruppen erfolgen (WICHTIG: nur Gruppen mit „ObjectClass=groupOfUniqueNames“ oder „ObjectClass=orclDynamicGroup“ werden hierfür berücksichtigt). Hierzu muss eine „Externe Rolle“ (in unserem Fall eine Team-Rolle) in OEM angelegt werden, die dem „CName“ einer LDAP Gruppe entspricht. Für diese Rollen erfolgt dann eine dynamische Zuordnung der Rollen beim Login eines LDAP Benutzers.

Durch Anpassung weiterer Parameter lassen sich noch zusätzliche Automatismen implementieren. Das Setzen des OMS-Parameters „oracle.sysman.core.security.auth.autoprovisioning“, bewirkt die automatische Anlage eines neuen Benutzers in OEM beim ersten Login. Möchte man jedoch nicht alle LDAP Benutzer als neue OEM Benutzer zulassen, kann dies mit dem Parameter „oracle.sysman.core.security.auth.autoprovisioning_minimum_role“ auf Mitglieder von bestimmten LDAP Rollen eingeschränkt werden. Durch die beiden weiteren „oracle.sysman.core.security.auth“-Parameter „enable_username_mapping“ und „ldapuserattributes_emuserattributes_mappings“ lassen sich zusätzlich sprechende Benutzernamen im OEM verwenden und LDAP Attribute für den Benutzer als Properties übernehmen.

Abb. 2: Einrichtung eines neuen Benutzers mit Datenübernahme aus LDAP (Schritt 1)

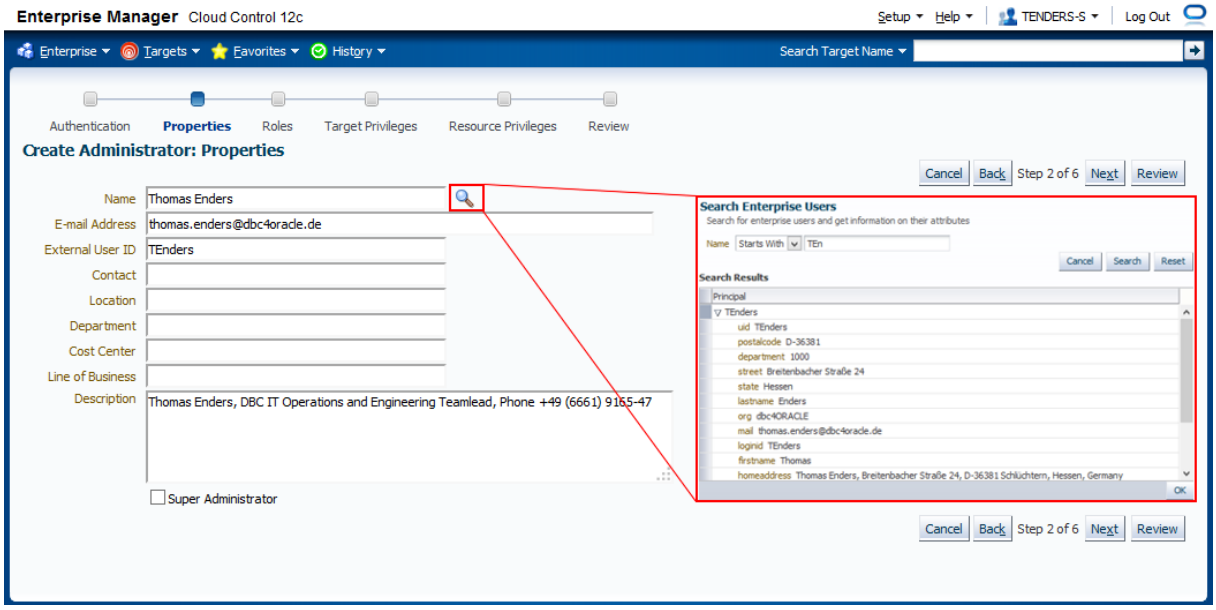

Abb. 3: Einrichtung eines neuen Benutzers mit Datenübernahme aus LDAP (Schritt 2)

Alle Befehle zum Einrichten dieser erweiterten Funktionen werden hier noch einmal im folgenden Beispiel zusammengefasst:

```
emctl set property -name "oracle.sysman.core.security.auth.autoprovisioning" -value "true"
emctl set property -name "oracle.sysman.core.security.auth.autoprovisioning_minimum_role" \
  -value "DBC_RL_EXT_OEM_USR"
emctl set property -name "oracle.sysman.core.security.auth.enable_username_mapping" \
  -value "true"
emctl set property \
  -name "oracle.sysman.core.security.auth.ldapuserattributes_emuserattributes_mappings" \
  -value "USERNAME={%displayname%},EXTERNALUSERID={%uid%},EMAIL={%mail%}"
```

Zugriff auf Datenbanken und Server

Alle bisherigen Betrachtungen haben sich nur auf Ressourcen und vom Agent zur Verfügung gestellte Informationen über die Targets beschränkt. Möchte man jedoch auch Server oder Datenbanken administrieren oder auf aktuelle Informationen zur Diagnose von Problemen zugreifen, ist hierfür ein direkter Zugriff auf das Target erforderlich. Wenn ein Administrator den benötigten Benutzernamen und dessen Passwort kennt, kann er dies natürlich für die Anmeldung verwenden. Jedoch dürfen gerade administrative Accounts oft so nicht verwendet werden. Dafür hat Oracle mit dem Enterprise Manager 12c die „Named Credentials“ eingeführt. Hiermit lassen sich Verbindungsinformationen in OEM verwalten und anderen Benutzern zur Verfügung stellen, ohne dass diese nähere Informationen zu dem verwendeten Account benötigen.

Was für kleinere bis mittlere Umgebungen eine gute Lösung darstellt, stößt in größeren Unternehmen schnell an seine Grenzen. So können „Named Credentials“ nur direkt an Benutzer vergeben werden, was eine einheitliche Vergabe für ganze Teams sehr schwierig macht. Auch Anforderungen, wie unterschiedliche Kennworte für administrative Benutzer in jeder Datenbank können dieses Konzept schnell beeinträchtigen. Man stelle sich eine Umgebung mit 1000 Datenbanken und 100 Administratoren vor, wobei nicht alle Administratoren den Zugriff auf alle Datenbanken erhalten sollen. Hier müssten nun 100 „Named Credentials“ selektiv auf die richtigen Administratoren verteilt werden.

Oracle Enterprise User Security Integration in OEM

Eine Lösung für den Datenbankzugriff mittels OEM kann in großen Unternehmen die Integration von „Enterprise User Security“ (EUS) in Enterprise Manager sein. Hierbei werden Datenbanken in einem LDAP-System registriert und in Gruppen (Domains) zusammengefasst. Nun können in der Datenbank Benutzer mit dem Zusatz „IDENTIFIED GLOBALLY“ angelegt werden. Diese Benutzer können nicht direkt für das Login verwendet werden, können aber als Mapping User für „EUS“ authentifizierte LDAP-User dienen. Dabei werden die LDAP (oder auch MS Active Directory) User während des Login diesen Benutzern zugeordnet und erhalten alle dem Account zugeordneten Privilegien.

Ein Administrator kann nun im Enterprise Manager seinen eigenen Namen als „Preferred Credential“ hinterlegen und sich so automatisch auf jeder Datenbank anmelden, für die ein User Mapping existiert.

Damit ist keine weitere Verwaltung von Passwörtern in der Datenbank oder in OEM mehr erforderlich.

Kontaktadresse:

Thomas Enders		Stefan Waldschmitt
Selbständiger Berater		Selbständiger Berater
Breitenbacher Straße, 24		Hanauer Landstraße, 25a
D-36381 Schlüchtern		D-63814 Mainaschaff
Telefon:	+49 (0) 1520-9855623	+49 (0) 152-33599126
Fax:	+49 (0) 6661-9165 45	+49 (0) 6021-73034
E-Mail:	thomas.enders@dbc4oracle.de	stefan.waldschmitt@dbc4oracle.de
Internet:	www.dbc4oracle.de	www.dbc4oracle.de