

# OEM 12/13c Setup Security in Cloud Control

**Angelika Gallwitz**  
freiberufliche Beraterin  
Bad Homburg

## **Schlüsselworte**

Administratoren Notification

Sichere OMS Konfiguration

Verschlüsselungsschlüssel

Incident Rules

Secure Console

Secure Upload

Feingranulierte Zugriffskontrolle

Zugangsdatenverwaltung

Auditkonfiguration

Security Best Practices Implementierung und Analyse in OEM

## **Einleitung**

In Oracle 13c gibt es neue Monitoring und Inzident Management Features.  
Oracle empfiehlt den Enterprise Manager Benutzern so wenig Privilegien wie möglich zu erteilen.  
Welche Privilegien sind notwendig, um eine sinnvolle Administration zu gewährleisten?

Es wird gezeigt welche Best Practices Security Features mit dem Enterprise Manager 13 implementiert werden können.

---

## Datenbank Access Control

In OEM 13c wird ein flexibler Datenbankzugriff über Enterprise Manager Database Plugins eingeführt. Neue Rollen in Relation zu Benutzern erlauben einen engeren Zugriff auf Datenbank Management Feature.

- DBA
- Applikations DBA
- Applikations Entwickler
- Infrastruktur DBA

## Gesicherte Kommunikation ( Secured Communication)

- TCPS ACCESS
- TCPS Listener

## Account Management

In OEM13c wurden neue EM CLI Verben für die Benutzer Verwaltung eingeführt.

- Get\_db\_profile

Details des Datenbankprofils werden angezeigt:

Profile,

Resource Name ,

Resource type und definierte

Limits

```
emcli get_db_profile
-target_name=ORCL
-profile=DEFAULT
-connect_as='DBNamedCreds:SYS_ORCL'
```

- **Get\_db\_account**

Username, Profil, Account Status Authentifizierung und Suchkriterien werden angezeigt.

```
emcli get_db_account
-target_name=ORCL
-username=Angelika
-connect_as='DBNamedCreds:SYS_ORCL'
```

- **update\_db\_account\_status**

Im folgenden Beispiel wird ein DB Account gelockt.

---

---

```
emcli update_db_account_status
  -target_name=ORCL
  -username=Angelika
  -action=LOCK
  -connect_as='DBNamedCreds:SYS_ORCL'
```

- **update\_db\_password**

Das Target Database Password wird in der Target Database und den Agents geändert.

Im folgenden Beispiel

```
emcli update_db_password
  -target_name=ORCL
  -username=Angelika
  -action=LOCK
  -connect_as='DBNamedCreds:SYS_ORCL'
```

### **In der Enterprise Manager Security-Konsole**

können Benutzerklassen, Berechtigungen und Rollen sowie Ziel- und Ressourcen-Berechtigungen vergeben werden.

---

The screenshot displays the Oracle Enterprise Manager Security Console interface. The top navigation bar includes the Oracle logo, 'Enterprise Manager Cloud Control 12c', and user information 'Setup | SYSMAN'. Below the navigation bar, the page title is 'Security-Konsole' and the status is 'Seite aktualisiert 10.05.2016 14:25:31 MESZ'. The main content area is divided into two sections:

- Enterprise Manager-Sicherheit**: A sidebar menu with the following items:
  - Überblick
  - Pluggable Authentication** (highlighted)
  - Feingranulierte Zugriffskontrolle
  - Sichere Kommunikation
  - Zugangsdatenverwaltung
  - Umfassendes Auditing
  - Anzahl aktiver Benutzersessions
  - Best Practices-Analyse
- Pluggable Authentication**: The main content area, with sub-tabs for 'Überblick' (selected) and 'Konfiguration'.
 

Bei der Enterprise Manager-Authentifizierung wird die Gültigkeit des Benutzers bestimmt, der auf Enterprise Manager zugreift. Das Authentifizierungsprotokoll ist über die verschiedenen Schnittstellen hinweg verfügbar, wie Enterprise Manager-Konsole und Enterprise Manager Command Line Interface (EM CLI). Oracle Enterprise Manager 12c verwendet WebLogic Server für externe Authentifizierungsmethoden. Deshalb kann Enterprise Manager 12c mit jeder Authentifizierungsmethode authentifiziert werden, die von Oracle WebLogic Server unterstützt wird.

Enterprise Manager unterstützt die folgenden Authentifizierungsschemata:

  - Repository-basierte Authentifizierung**: Dies ist die Standardauthentifizierungsoption. Ein Enterprise Manager Administrator ist gleichzeitig ein Repository-Benutzer (Datenbankbenutzer). Mit dieser Option können Sie alle Vorteile dieser Authentifizierungsmethode nutzen, wie Kennwortkontrolle über Kennwortprofil, durchgesetzte Kennwortkomplexität, Gültigkeitsdauer des Kennwortes und Anzahl von zulässigen nicht erfolgreichen Versuchen.
  - Oracle Access Manager (OAM)-SSO**: Oracle Access Manager ist die Oracle Fusion Middleware Single Sign-On-Lösung. Die zugrunde liegenden Identitätsspeicher sind die Enterprise Directory-Identitätsspeicher, die von Oracle Access Manager unterstützt werden.
  - SSO-basierte Authentifizierung**: Die Single Sign-On-basierte Authentifizierung stellt eine verstärkte, zentralisierte Verwaltung der Benutzeridentität über das gesamte Unternehmen bereit. Nachdem Sie Enterprise Manager zur Verwendung von Oracle Application Server Single Sign-On konfiguriert haben, können Sie jeden Single Sign-On-Benutzer als Enterprise Manager Administrator registrieren.
  - Auf Enterprise User Security basierende Authentifizierung**: Mit der Enterprise User Security (EUS)-Option können Sie Enterprise-Benutzer und -Rollen für die Oracle-Datenbank in einem LDAP-konformen Directory-Server speichern. Sie können jeden EUS-Benutzer als Enterprise Manager Administrator registrieren. Mit EUS kann die Verwaltung von Benutzern und Rollen über mehrere Datenbanken hinweg zentralisiert werden.
  - LDAP-Authentifizierungsoption**
    - Auf Oracle Internet Directory (OID) basierte Authentifizierung
    - Auf Microsoft Active Directory basierte Authentifizierung

Über die Feingranulierte Zugriffskontrolle können Zielberechtigungen an User oder Rollen vergeben werden.

Security-Konsole

Seite aktualisiert 10.05.2016 14:25:31 MESZ

Enterprise Manager-Sicherheit

- Überblick
- Pluggable Authentication
- **Feingranulierte Zugriffskontrolle**
- Sichere Kommunikation
- Zugangsdatenverwaltung
- Umfassendes Auditing
- Anzahl aktiver Benutzersessions
- Best Practices-Analyse

Feingranulierte Zugriffskontrolle

Überblick Administratoren **Berechtigungen** Rollen Berechtigungspropagierung in Aggregaten

Bei EM können folgende Berechtigungen einem Benutzer oder einer Rolle erteilt werden.

Zielberechtigungen

Mit Zielberechtigungen kann ein Administrator Vorgänge mit einem Ziel ausführen. In der Tabelle werden die Zielberechtigungen aufgeführt, die einem Administrator erteilt werden können, zusammen mit anderen Informationen, z.B. ob die Berechtigungen für eine Klasse von Zielen oder ein bestimmtes Ziel angewendet werden können.

Ansicht + Zuordnung aufheben

Berechtigungsname	Berechtigungstyp	Beschreibung	Enthaltene Berechtigungen	Anwendbare Ziele
Alle Java-Servicezi...		Möglichkeit, alle Java-Serviceziele anzuzeigen		Oracle WebLogic...
Anzeigen		Möglichkeit, Eigenschaften, Bestandsverze...		
Ausführen-Befehl		Beliebigen BS-Befehl ausführen	Anzeigen	Host
Befehl als Agent a...		Beliebigen BS-Befehl als Agent-Benutzer au...	Anzeigen	Agent
Befehl als beliebig...		Beliebigen BS-Befehl als Agent-Benutzer auf...		Agent
Befehl an beliebig...		Beliebigen BS-Befehl auf beliebigem Agent...		Host
Beliebige Zielmetri...		Möglichkeit, die Metrik für jedes Ziel zu ver...		
Beliebigen Datenb...		Möglichkeit, alle Datenbankdienstziele anzu...		Schemaservice
Beliebigen Ressou...		Beliebigen Ressourcenprovider anzeigen		Cloudressourcenpr...
Beliebiges Beacoh...		Beliebiges Beacon in einem überwachten H...		
Beliebiges Ziel anz...		Möglichkeit, alle verwalteten Ziele in Enterp...	Enterprise Manag...	
Beliebiges Ziel Nin...		Beliebiges Ziel in Enterprise Manager hinzuf...		Beliebiges benutze...
Beliebiges benutze...		Möglichkeit, beliebige benutzerdefinierte Ag...		
Berechtigungsprop...		Möglichkeit, Berechtigungspropagierungsg...	Beliebiges benutze...	
Blackout-Ziel		Möglichkeit, ein Blackout auf dem Ziel zu er...	Anzeigen	
Cloud Home anzei...		Cloud Home anzeigen		Oracle Cloud
Compliance von b...		Möglichkeit, die Compliance eines beliebige...		
Datei als Agent sp...		Beliebige Datei im Agent-Datensystem als A...	Anzeigen	Agent
Datei als beliebig...		Beliebige Datei in beliebigem Agent-Datensy...		Agent
Enterprise Manag...		Referenzen von Enterprise Manager über...		

ORACLE Enterprise Manager Cloud Control 12c Setup | SYSMAN

Enterprise → Ziele → Erweiteren → Historie → Zielname suchen

### Security-Konsole Seite aktualisiert 10.05.2016 14:25:31 MESZ

**Enterprise Manager-Sicherheit**

- Überblick
- Pluggable Authentication
- **Feingranulierte Zugriffskontrolle**
- Sichere Kommunikation
- Zugangsdatenverwaltung
- Umfassendes Auditing
- Anzahl aktiver Benutzersessions
- Best Practices-Analyse

#### Feingranulierte Zugriffskontrolle

**Überblick** Administratoren Berechtigungen Rollen Berechtigungspropagierung in Aggregaten

Es ist gefährlich, allen Administratoren auf allen Systemen dieselbe Zugriffsebene zu erteilen. Allerdings ist die individuelle Erteilung von Zugriffsberechtigungen für zehni, Hunderte oder ganz Tausende von Zielen für jedes neue Mitglied der Gruppe zeitaufwändig. Mit dem Enterprise Manager-Feature der Administratorberechtigungen und -rollen kann diese Aufgabe innerhalb von Sekunden anstelle von Stunden ausgeführt werden. Mit der Autorisierung wird der Zugriff auf die sicheren Ressourcen, die von Enterprise Manager verwaltet werden, über Berechtigungen und Rollen auf System-, Ziel- und Objektebene kontrolliert.

In diesem Abschnitt wird das Autorisierungsmodell von Enterprise Manager beschrieben, einschließlich Benutzerklassen, Rollen und Berechtigungen, die jeder Benutzerklasse zugewiesen werden. Folgende Themen werden beschrieben:

- Benutzerklassen
- Berechtigungen und Rollen

**Benutzerklassen**

Oracle Enterprise Manager unterstützt verschiedene Klassen von Oracle-Benutzern, je nach verwalteter Umgebung und Kontext, in dem Oracle Enterprise Manager verwendet wird. Es gibt drei Zugriffskategorien für Administratoren:

- **Superadministrator** Leistungsstarker Enterprise Manager-Administrator mit vollständigen Zugriffsberechtigungen zu allen Zielen und Administratoraccounts innerhalb der Enterprise Manager-Umgebung. Der Superadministrator, SYSMAN, wird standardmäßig erstellt, wenn Enterprise Manager installiert wird. Der Superadministratoraccount kann alle anderen Administratoraccounts verwalten und alle Administratorzugangsdaten einrichten. Der Superadministrator kann:
  - Enterprise Manager-Berechtigungen und -Rollen erstellen
  - das anfängliche Setup von Enterprise Manager durchführen, wie z.B. E-Mail-Konfigurationen definieren und globale Benachrichtigungsregeln definieren
  - Ziele zu Enterprise Manager hinzufügen
  - beliebige Aktionen mit beliebigen Zielen in dem System ausführen
- **Administrator** Regulärer Enterprise Manager-Administrator.
- **Repository-Eigentümer** Datenbankadministrator für das Management-Repository. Dieser Account kann nicht geändert, dupliziert oder gelöscht werden.

**Berechtigungen und Rollen**

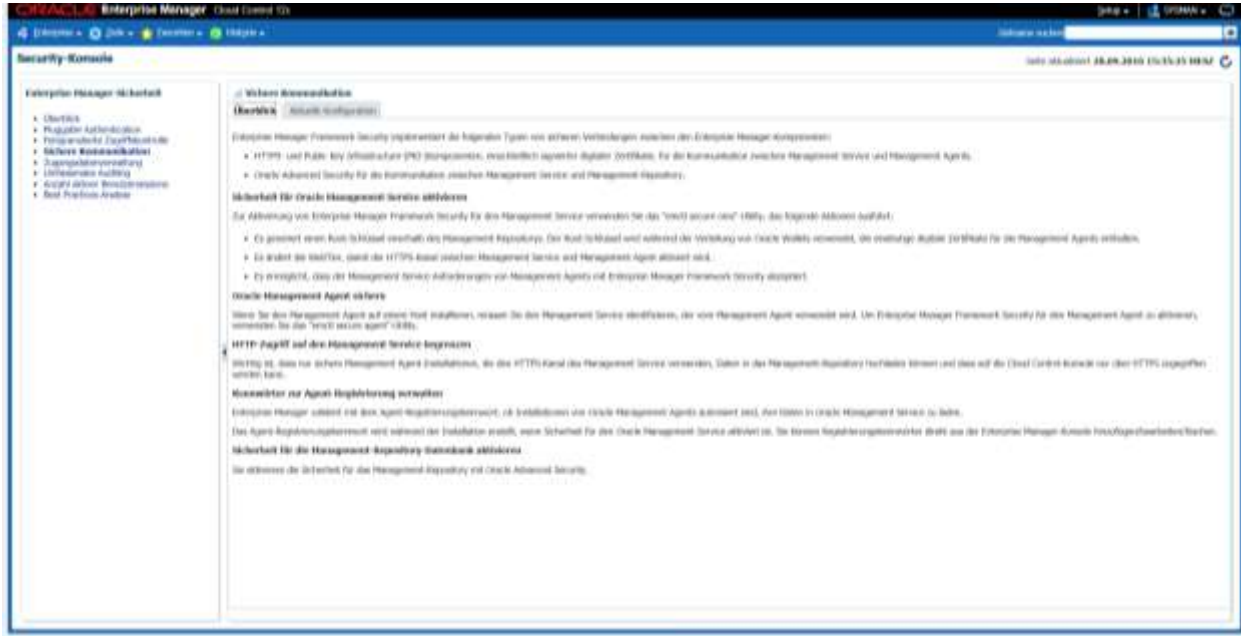
Benutzerberechtigungen stellen eine grundlegende Sicherheitsebene in Enterprise Manager dar.

Berechtigungen können in zwei Kategorien unterteilt werden:

- Zielberechtigungen
- Ressourcenberechtigungen

Eine Rolle besteht aus einer Zusammenstellung von Enterprise Manager-Ressourcenberechtigungen und/oder Zielberechtigungen, die Sie Administratoren oder anderen Rollen erteilen können. Diese Rollen können auf einem geografischen Standort (Beispiel: Eine Rolle für die deutsche Administratoren von Oracle) oder einer Cloud-Instanz (Beispiel: Eine Rolle für die Administratoren von Oracle Cloud) erstellt werden.

## Sichere Kommunikation



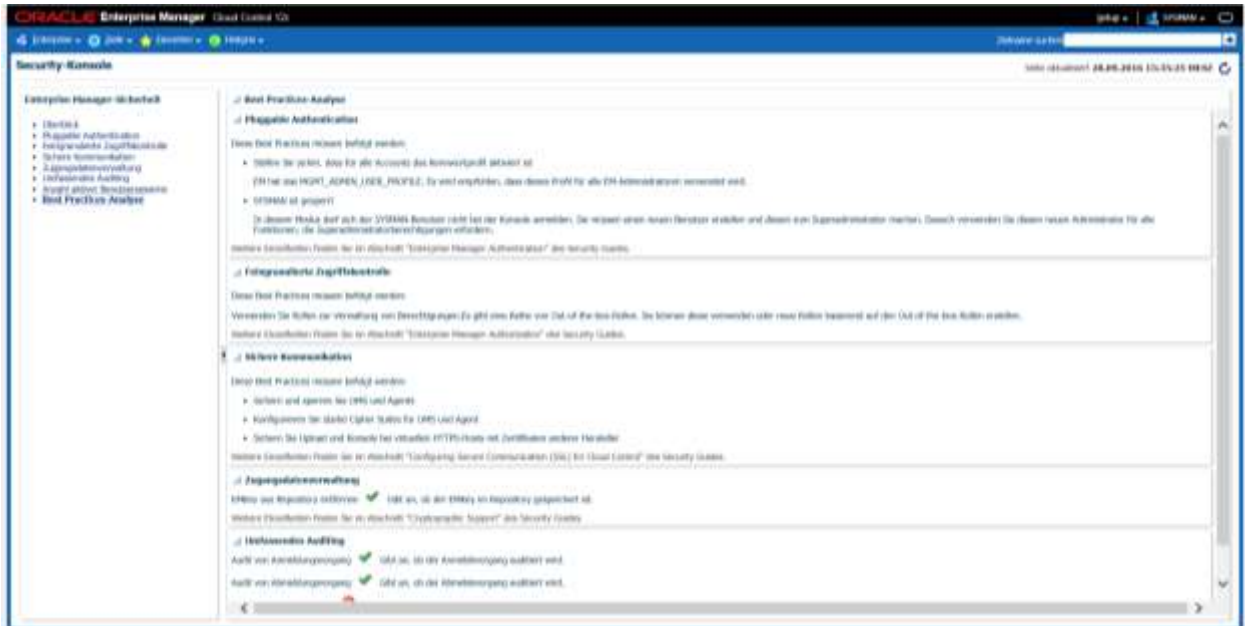
**Zugangsdatenverwaltung**



**Auditing**



## Best Practices-Analyse



Setting up the Auditing System for Enterprise Manager Security Guide  
EM13c uses Java 7, WebLogic 12.1.3, and disables SSLv3 out of the box.



---

**Kontaktadresse:**

Angelika Gallwitz  
Externe Beraterin  
In den Hessengärten 48  
D – 61352 Bad Homburg

Telefon: +49 (0) 6172-488602  
Fax +49(0)6172-944955  
E-Mail [angelika@gallwitz.de](mailto:angelika@gallwitz.de)  
homepage [www.gallwitz-it.de](http://www.gallwitz-it.de)

---