User-Provisioning in EMCC 12c

Dr. Günter Unbescheid
Database Consult GmbH, Jachenau

Database Consult GmbH

- Gegründet 1996
- Kompetenzen im Umfeld von ORACLE-basierten Systemen
- Tätigkeitsbereiche
  - Security, Identity Management
  - Tuning, Installation, Konfiguration, Systemanalysen
  - Support, Troubleshooting, DBA-Aufgaben
  - Datenbankdesign, Datenmodellierung und –design
  - Maßgeschneiderte Workshops
  - www.database-consult.de
- Seit 2012 – Kooperation mit trivadis makes IT easier.

Inhalte und Ziele

- Thema
  - Einrichtung, Authentifizierung und Autorisierung von EMCC-Benutzern
  - Sicherer Zugriff auf über EMCC verwaltete Target-Systeme
  - Kontext: Administratoren und Entwickler
  - Bei den Targets liegt der Schwerpunkt auf Oracle Datenbanken
- Zielsetzung
  - Weitgehend automatisierte Integration vorhandener Benutzer und Benutzergruppen, Nutzung von Gruppeninformationen
  - Integration vorhandener (zentralisierter) Benutzer-Repositories und Authentifizierungs-Komponenten
  - Unkomplizierte Integration von Targets unter Beibehaltung bestehender Sicherheits- und anderweitiger Regelvorgaben

Empfehlung

Benutzerverwaltung

Durch die Konfiguration von Benutzerrollen und Gruppenrechten sorgt die Benutzerverwaltung dafür, dass einzelne Benutzer nicht mit mehr Rechten ausgestattet werden, als sie für ihre eigentliche Aufgabenerfüllung benötigen. Wird jeder Benutzer lokal auf einem Server verwaltet, so ist die Gefahr groß, dass Fehler bei der Rechtevergabe vorkommen. Deshalb ist eine zentrale Benutzerverwaltung vorzuziehen. Eine zentrale Vergabe der Berechtigungen verringert die Gefahr von Fehlkonfigurationen. Zusätzlich lässt sich über eine zentrale Benutzerverwaltung sicherstellen, dass alle Passwörter eine ausreichende Komplexität beinhalten, die automatisierten Angriffen standhält.

(Bundesamt für Sicherheit in der Informationstechnik)

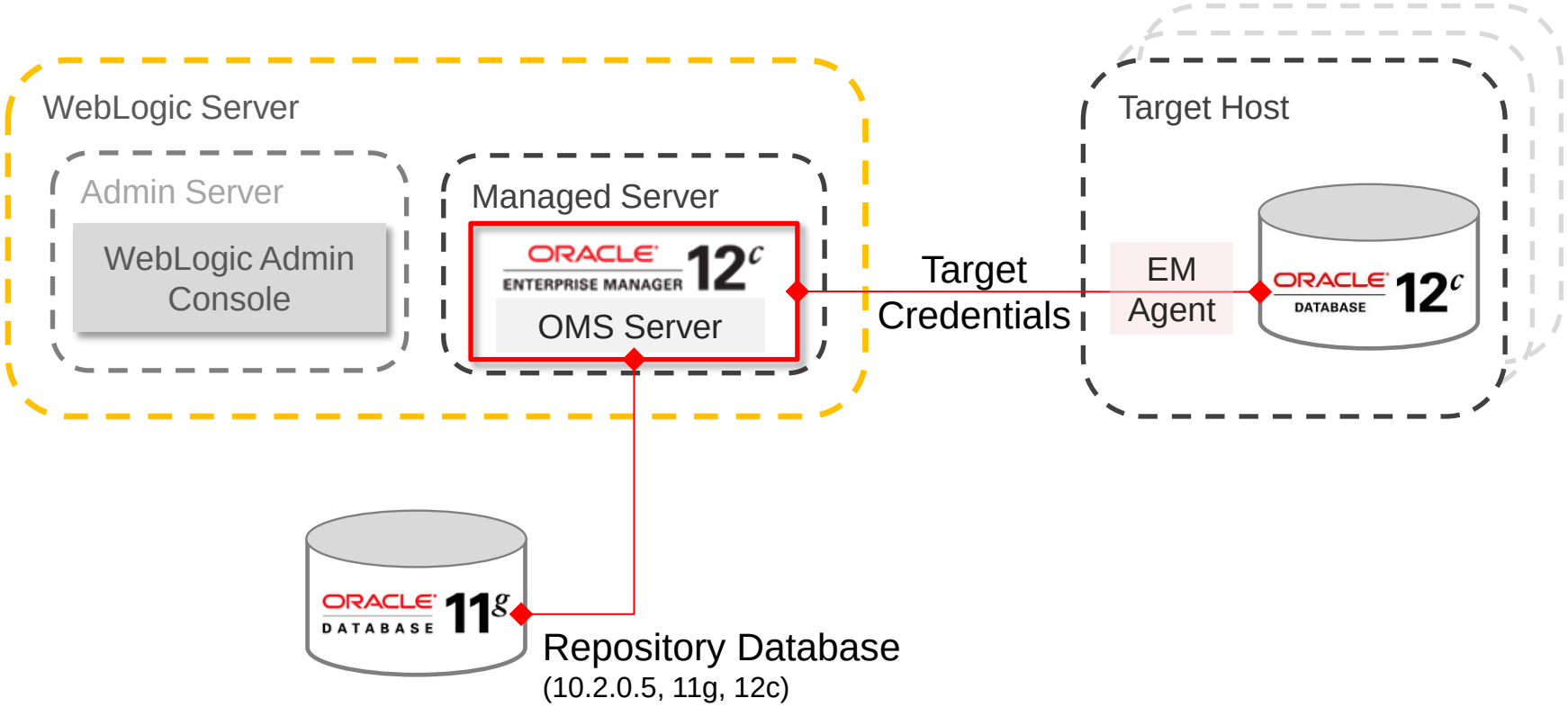
Enterprise Manager Cloud Control

- Signifikante Erweiterungen in Sachen „Security“ in dem/den letzten Releases – insbesondere 12.1.0.4
- In unserem Kontext
  - Support for LDAP authentication and Kerberos strong authentication
  - Nonpassword credentials for host and database target authentication
  - SSH key-based authentication for host access
  - Kerberos tickets database authentication.
  - Mapping von LDAP Attributen
  - Verbessertes Credential Management
  - Fine-grained Privileges and Out-of-Box Roles, private Roles
  - Dynamic Groups
- Nach wie vor: Komplexes Setup
- Partielle “Kinderkrankheiten” – jedoch Workarounds verfügbar

Stand der Technik/Testsystem

- Enterprise Manager Cloud Control 12.1.0.4
- WebLogic Server 10.3.6
- Repository Datenbank
  - Oracle Database 11.2.0.3.0
    (with PSU 11.2.0.3.10, which has CPUAPR2014)
- Target Systems
  - Diverse 11g und 12c unter Linux
- Host System – Linux
  - Oracle Linux Server release 5.7 (Kernel 2.6.32-200.13.1.el5uek)

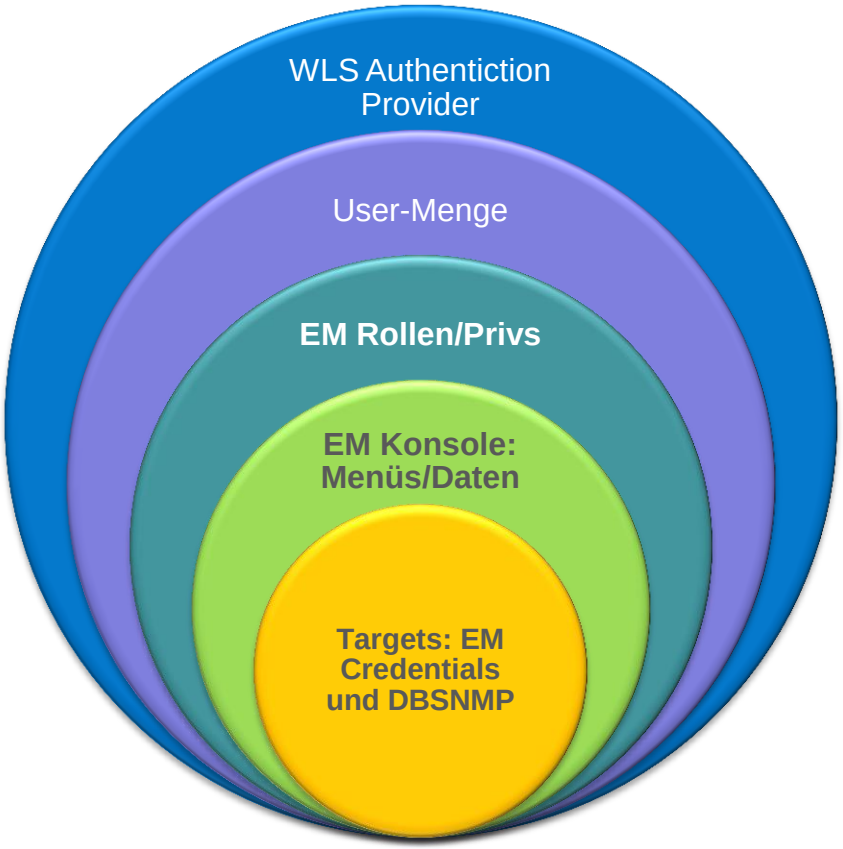
EMCC Basisarchitektur



EMCC Begriffe

- EM Base Platform (BP) für OMS-Server und Basis Framework/Java Applikation mit Subsystemen – UI und Backend Services
- Management Plug-Ins („integrated code“) für Target-spezifische Funktionalitäten , einzeln „patchbar“
  - Im Kontext vom OMA und Base Platform
  - Einzeln installierbar, daher minimaler Footprint des Agents möglich
  - Unabhängige Release Nummern und Zyklen
- OMR (Management Repository) gespeichert im Schema SYSMAN
- OMA (Management Agent) erhebt Daten auf den integrierten Targets und übermittelt an BP

EMCC Security Konzepte



- WLS Authentication Provider
  - Konfiguriert Authentication Kontexte (GUI oder **`emctl`**)
- Abhängig davon ergibt sich eine User-Menge
  - z.B. externes Repository (AD)
- User sind mit EM-Rollen im OMR verknüpft
  - Auch externe Rollen (Gruppen)
- Abhängig davon sind EM Menüs und Targets sichtbar
- Credentials öffnen den Weg zu „internen“ Target-Daten

WLS Authentication Provider

- Definieren grundlegende Authentifizierungsquellen und –Verfahren
  - Spezifische Parametrierung
- Konfiguriert im Kontext von WebLogic Server
  - dort über GUI im Rahmen von Security Realms (Default „myrealm“)
  - Damit prinzipiell nutzbar für „deployte“ Applikationen/Consolen
- Mehrere sind pro Realm hierarchisch konfigurierbar
  - Control flags regeln den Umgang mit Returns (required/sufficient etc.)
- WLS erlaubt die Konfiguration von mehreren Security Realms
- DefaultAuthenticatior
  - Standard-Provider. Nutzt internes WLS LDAP Verzeichnis
  - Genutzt für Default Administratoren

WLS Authentication Provider

- EM Repos Authentication Provider
  - Ermöglicht die Authentifizierung der User im OMS (EMCC Standard)
  - EM Administratoren sind DB-User in OMR-Datenbank mit DB-Rolle MGMT-User und **`create session`** Privileg
  - Zusätzlich in Tabelle **`MGMT_CRATED_USERS`** erfasst (Metadaten)
- Oracle Internet Directory Authenticator
  - Ermöglicht die Einbindung von OID Benutzern in WLS-Applikationen
  - Wird im Kontext des (aktiven) Security Realms angelegt und zeigt dann OID-User im WLS Realm (Users and Groups)
  - DN, Port und Host sowie LDAP-Filter für den OID-Zugriff konfigurieren
- Active Directory Authenticator mit vergleichbaren Funktionen
- NegotiateIdentityAsserter – Verarbeitung von Kerberos Tickets
  - Ermöglicht SSO für Admins an EMCC-Konsole

CLI Vorgehen


```
emctl config auth oid \
 -ldap_host „oidserver.dbc.de" -ldap_port "7022" \
 -ldap_principal"cn=oraemcc,cn=Users,dc=dbc,dc=de" \
 -ldap_credential "<secret>" \
 -user_base_dn "cn=ADMIN,cn=users,dc=dbc,dc=de" \
 -group_base_dn "cn=groups,dc=dbc,dc=de" \
 -enable_auto_provisioning
```

- Analoge Calls (**`auth ad`**) für Active Directory Einbindung
- Autoprovisioning
  - bedeutet, dass Benutzer, die über die vorstehend beschriebenen Authencation Provider identifiziert wurden, bei der ersten Anmeldung an EMCC automatisch in das EMCC Repository übernommen werden (OMR Tabelle MGMT_CREATED_USERS)
  - Zudsätzlich muss für die Zuteilung von Privilegien gesorgt werden

Provider Stack in WLS

Name (freibleibend)	Typ	Verwendungszweck
For_Kerberos	WebLogic Negotiate Identity Assertion provider	Kerberos Autentifizierung für Weblogic
EM_OID_Provider	OID LDAP Authentication	Einbindung der OID-Benutzer und Gruppen in Weblogic
DefaultAuthenticator	WebLogic Authentication Provider	Einbindung der Benutzer aus dem in Weblogic eingebetteten LDAP-Server
DefaultIdentityAsserter	WebLogic Identity Assertion provider	Validieren von X.509 Zertifikaten u.a.
EM_Repos_Authenticator	EM Repos Authentication Provider	Authentifizierung über das interne EM Repository.

- Der vorstehende Stack bietet folgende Verbindungsmöglichkeiten (nur wenn auch die Privilegierung entsprechend konfiguriert ist)
  - Kerberos Authentifizierung für OID-User an EMCC-Konsole (hierzu sind zusätzliche Schritte nötig(!): keyfile, krb5.conf, krb5login.conf)
  - Authenfizierung über WLS-Ldap User
  - Authentifizierung über OID-User und OID-Password
- Über Chaining oder DIP können auch AD-User bereitstehen

Überprüfung


```
emctl list properties -module emoms -sysman_pwd <pwd> | \
egrep 'emSDK.sec|core.security.auth|Management Server'

Management Server : omsserver:4889_Management_Service
oracle.sysman.core.security.auth.autoprovisioning=true
oracle.sysman.core.security.auth.autoprovisioning_minimum_role=null
oracle.sysman.core.security.auth.enable_username_mapping=null
oracle.sysman.core.security.auth.is_external_authentication_enabled=true
oracle.sysman.core.security.auth.ldapuserattributes_emuserattributes_mappings
= null
oracle.sysman.core.security.auth.redirect_to_canonicalUrl=false
oracle.sysman.emSDK.sec.DirectoryAuthenticationType=EnterpriseUser
oracle.sysman.emSDK.sec.eus.DASHostUrl=http://oidhost.dbc.de:7022
oracle.sysman.emSDK.sec.eus.Domain=dc=dbc,dc=de
```

EMCC User

- Gespeichert im OMR Repository
- Provisioniert und authentifiziert über unterschiedliche ggf. „externe" Provider
- Dienen der Privilegienzuteilung im Rahmen der EMCC Konsole
  - Nicht im Rahmen der Targets! (Ausnahmen)
- Unterschiedliche Typen, z.B.:
  - Repository – angelegt im OMR-Repository
  - SSO – provisioniert aus externer Quelle (z.B. LDAP Repository) und übernommen in das OMR
  - SSO fähig
- Weitere Klassifizierung:
  - Repository Owner, Superuser, Administrator

EMCC Privilegien und Rollen

- Bündelung von Privilegien
  - Regulierung von Menü- und Managementoperationen
  - Sichtbarkeit von Targets im GUI Kontext
  - SUPERUSER übersteuern alle Rollen
- 41 vordefinierte Rollen (nicht modifizierbar) + PUBLIC (leer aber modifizierbar)
- Jede Rolle kann enthalten
  - Weitere vordefinierte und eigene Rollen
  - Target-Privilegien – wirksam auf allen oder spezifischen Targets, z.B. „Operator any Target“
  - Resource Privilegien – Berechtigungen für EMCC Funktionalitäten, z.B. „named credential“ zum Anlegen von named credentials.
- Irritierend: Privilegiennamen unterliegen der Sprachpräferenz

EMCC Privilegien

- Target Privilegien – unterschiedliche Fokussierungen/Typen
  - Alle Targets und alle Targettypen – z.B „add Any Target“
  - Alle Targets, spezifische Targettypen – z.B. . „Execute Command Anywhere“ gilt für alle Host-Targets
  - Spezifische Targets unterschiedlicher Typen, z.B. View für DB-Instanz „db5“
- Aggregate Target Privileges
  - Gruppierung unterschiedlicher einzelner Targets oder Target-Gruppen
  - Privilegierung auf unterschiedlichen Ebenen ist möglich:
    - Bezogen auf Aggregat und Member gleichermassen
    - Bezogen nur auf das Aggregat, z.B. „View“ (Aggregat darf nicht verändert bzw. gelöscht werden)
    - Bezogen nur auf Gesamtheit der Member, z.B. „FULL“ (volle Operationalität auf allen enthaltenen Membern)

EMCC Rollen

- System Roles < 12.1.0.4
  - Erstellt und verwaltet nur über Super Administratoren
  - Ab 12.1.0.4 auch über Privileg **`manage_system_role`**
- Private Rolle – verfügbar ab 12.1.0.4
  - Erstellt von Super Admin oder über **`create_role`** Privileg
  - nicht standardmäßig für Superadministratoren wirksam
  - Explizit von Owner oder Berechtigtem (**`WITH_ADMIN`**) verwaltbar
  - Kann **`*credential*`** Privilegien enthalten
- Externe Rolle
  - Automatisierte Zuordnung der EM-Rolle zu LDAP-Gruppennamen
  - Identische Namen steuern die Zuordnung

EMCC Target Gruppen

- Selbst definierte Gruppierung von Targets
  - Gruppen können hierarchisch angelegt werden, d.h. in übergordneten Gruppen enthalten sein
- Privilege Propagating Groups
  - Privilegien, die für die Gruppe gegeben werden, gelten automatisch für alle Member
- Dynamische Gruppen
  - Die Gruppenzugehörigkeit wird über Kriterien bestimmt, die sich an Target Eigenschaften orientieren, z.B. Location, Lifecycle Status, Cost Center etc.
- Lifecycle Status – spezifische Target Eigenschaft
  - Festgelegte Hierarchie, Namen sind modifizierbar (MissionCritical, Production, Stage, Test, Development)
  - Ideal für dynamisch Gruppen

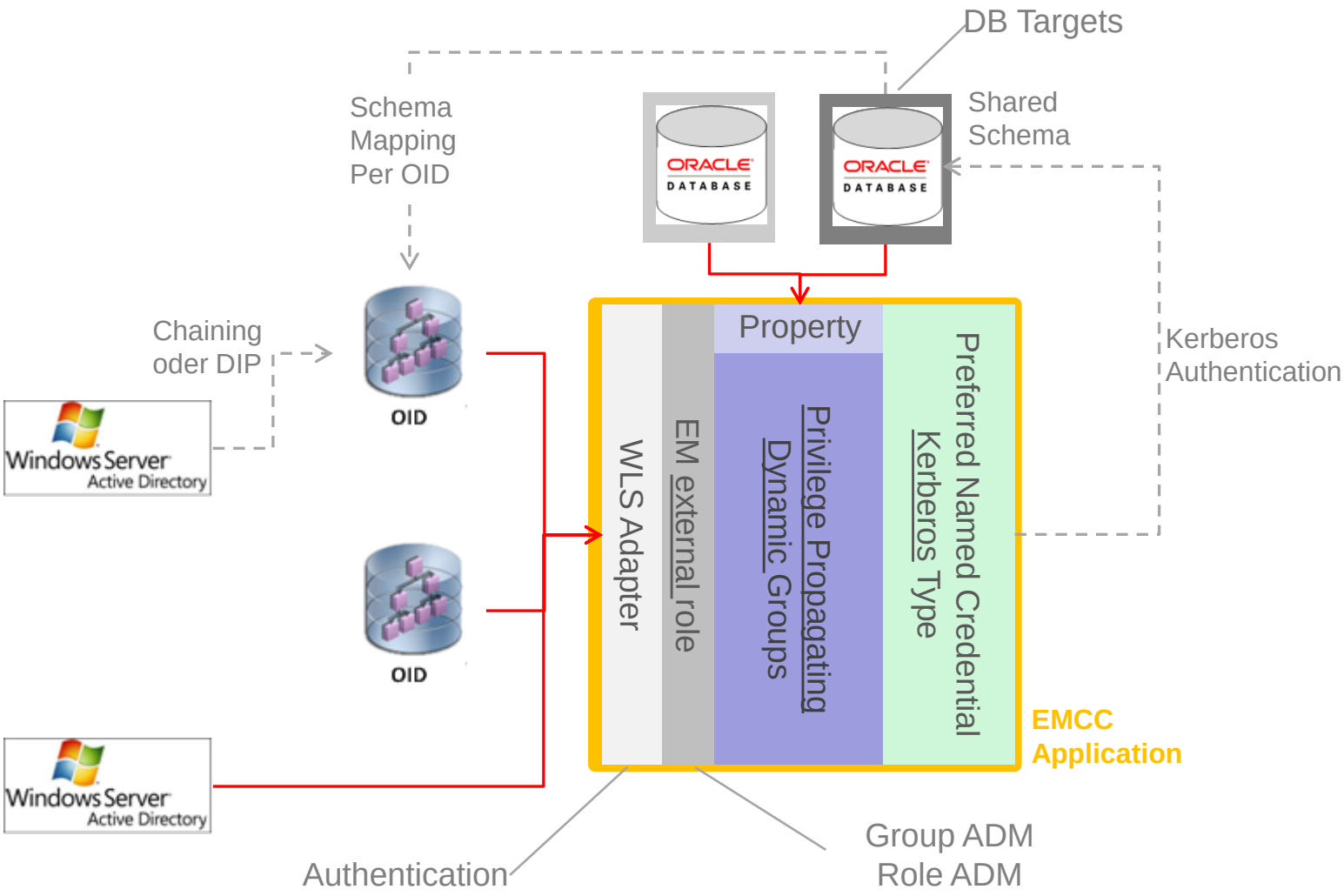
Named Credentials

- Benannter Set aus Benutzername/Passwort (*named credential*)
  - Abhängig vom Target-Typ
  - Für Einzel-Target oder global für alle Targets des Typs (pro Benutzer)
    - Untersdchiedliche Typen pro Target-Typ
  - Kann gegranted werden (*view/edit/full*)
- Steuern administrative Zugriffe auf Targets
  - Datenbank: DBSNMP nur für Übersichtsseiten
- Z.B. Database Instance Credentials als
  - Database Credentials oder Kerberos Credentials (AD username/PW)
- Preferred Credentials
  - Bevorzugt auf Basis der angelegten named credentials
  - Als „user preferences“ oder „global preferences“
  - Für alle oder einzelne Targets (Hierarchie)

Named Credentials

- NC können unterschiedliche DB-Benutzertypen referenzieren
  - Standard DB-Benutzer
  - Externe Benutzer (Kerberos/Zertifikat)
  - Shared Schemas

Zusammenspiel der Komponenten (Beispiel)



Fazit

- EMCC Release 4 (12.1.0.4) bietet wichtige Features für ein effizientes User-Deployment
- Komplexes Initial-Setup belohnt später im operativen Betrieb
  - Autoprovisioning, Role-Group Mapping, Dynamic Groups
  - Kerberos Authentication, Preferred Credentials, Private Roles
- Dokumentation an menchen Stellen lückenhaft/unverständlich
- Kleinere Stolpersteine – jedoch mit Workarounds
- Sorgfältige Vorbereitung und gutes Rollendesign empfehlenswert bzw. notwendig

Danke für's Zuhören

www.database-consult.de