

ODBC op ISE 2.3 configureren met Oracle Database

Inhoud

[Inleiding](#)

[Voorwaarden](#)

[Vereisten](#)

[Gebruikte componenten](#)

[Configureren](#)

[Stap 1: Oracle Basis Configuration](#)

[Stap 2. ISE-basisconfiguratie](#)

[Stap 3. Gebruikersverificatie configureren](#)

[Stap 4. groepsvernieuwing instellen](#)

[Stap 5. Eigenschappen opnieuw instellen](#)

[Stap 6. Verificatie-/autorisatiebeleid configureren](#)

[Stap 7. Voeg Oracle ODBC toe aan Identity Source Seques](#)

[Verifiëren](#)

[RADIUS-bewegende documenten](#)

[Detail-rapport](#)

[Problemen oplossen](#)

[Onjuiste referenties worden gebruikt](#)

[Fout in DB \(Service Name\)](#)

[Verificaties van probleemoplossing](#)

[Referenties](#)

Inleiding

Dit document beschrijft hoe u Identity Services Engine (ISE) kunt configureren met Oracle Database voor ISE-verificatie met behulp van Open Database Connectivity (ODBC).

Voor Open Database Connectivity (ODBC)-verificatie moet ISE een eenvoudig wachtwoord voor tekstgebruikers kunnen genereren. Het wachtwoord kan in de database worden versleuteld, maar moet worden gedecrypteerd volgens de opgeslagen procedure.

Voorwaarden

Vereisten

Cisco raadt kennis van de volgende onderwerpen aan:

- Cisco Identity Services Engine 2.3
- Database- en ODBC-concepten
- Oracle

Gebruikte componenten

De informatie in dit document is gebaseerd op de volgende software- en hardware-versies:

- Identity Services Engine 2.3.0.298
- Centos 7
- Oracle Database 12.2.0.1.0
- Oracle SQL Development er 4.1.5

Configureren

Opmerking: Behandel SQL-procedures die in dit document worden gepresenteerd als voorbeelden. Dit is geen officiële en aanbevolen manier van Oracle DB-configuratie. Zorg ervoor dat u resultaat en impact van elke SQL query die u vastlegt, begrijpt.

Stap 1: Oracle Basis Configuration

In dit voorbeeld werd Oracle met de volgende parameters ingesteld:

- DB naam: **ORCL**
- Servicenaam: **orcl.vkumov.plaatselijk**
- Port: **1521** (standaard)
- Gecreëerde account voor ISE met **gebruikersbenaming**

Configureer de Oracle-database voordat u verder gaat.

Stap 2. ISE-basisconfiguratie

Maak een ODBC Identity Bron bij *Beheer > Externe Identity Bron > ODBC* en testverbinding:

ODBC Identity Source

General **Connection** Stored Procedures Attributes Groups

ODBC DB connection details

* Hostname/IP[:port]

* Database name

Admin username ⓘ

Admin password

* Timeout

* Retries

* Database type

Test connection X

Connection succeeded

Stored Procedures

- Plain text password authentication - Not Configured
- Plain text password fetching - Not Configured
- Check username or machine exists - Not Configured
- Fetch groups - Not Configured
- Fetch attributes - Not Configured

Opmerking: ISE verbindt zich met Oracle met gebruikmaking van Service Name, zodat het veld [Database name] moet worden ingevuld met servicenaam die in Oracle, niet SID (of DB naam) bestaat. Vanwege het bug [CSCvf06497](#) punten (..) kunnen niet in het veld [Databasenaam] worden gebruikt. Deze bug zit in ISE 2.3.

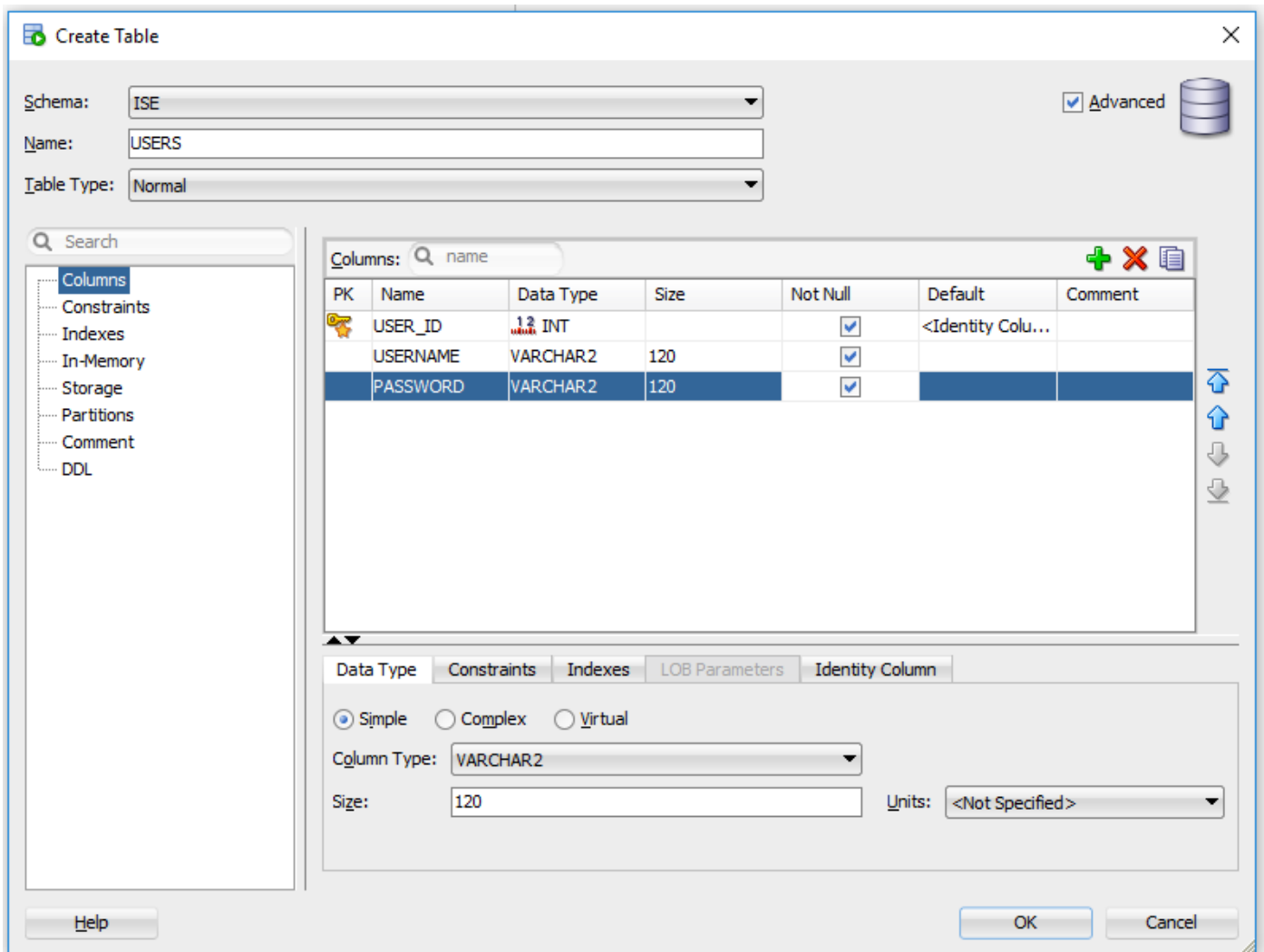
Stap 3. Gebruikersverificatie configureren

ISE-verificatie op ODBC-toepassingen van opgeslagen procedures. Het is mogelijk het type procedure te selecteren. In dit voorbeeld gebruiken we opnames als terugkeer.

Raadpleeg voor andere procedures de [Administrator Guide van Cisco Identity Services Engine, release 2.3](#)

Tip: Het is mogelijk om genoemde parameters terug te geven in plaats van resultSet. Het is gewoon een ander type output, functionaliteit is hetzelfde.

1. Maak de tabel met gebruikersreferenties. Stel de instellingen voor de identiteit in op de **primaire toets**.



2. Gebruikers toevoegen

```
INSERT INTO "ISE"."USERS" (USERNAME, PASSWORD) VALUES ('alice', 'password1')
INSERT INTO "ISE"."USERS" (USERNAME, PASSWORD) VALUES ('bob', 'password1')
INSERT INTO "ISE"."USERS" (USERNAME, PASSWORD) VALUES ('admin', 'password1')
```

3. Maak een procedure voor eenvoudige tekstwachtwoordverificatie (gebruikt voor PAP, EAP-GTC binnenmethode, TACACS)

```
create or replace function ISEAUTH_R
(
  ise_username IN VARCHAR2,
  ise_userpassword IN VARCHAR2
) return sys_refcursor AS
BEGIN
  declare
    c integer;
    resultSet SYS_REFCURSOR;
  begin
    select count(*) into c from USERS where USERS.USERNAME = ise_username and USERS.PASSWORD =
ise_userpassword;
    if c > 0 then
      open resultSet for select 0 as code, 11, 'good user', 'no error' from dual;
    ELSE
      open resultSet for select 3, 0, 'odbc','ODBC Authen Error' from dual;
    END IF;
  END IF;
```

```

return resultSet;
end;
END ISEAUTH_R;

```

4. Maak een procedure voor het opvragen van een gewoon tekstwachtwoord (gebruikt voor CHAP, MSCHAPv1/v2, EAP-MD5, LEAP, EAP-MSCHAPv2 binnenmethode, TACACS)

```

create or replace function ISEFETCH_R
(
ise_username IN VARCHAR2
) return sys_refcursor AS
BEGIN
declare
c integer;
resultSet SYS_REFCURSOR;
begin
select count(*) into c from USERS where USERS.USERNAME = ise_username;
if c > 0 then
open resultSet for select 0, 11, 'good user', 'no error', password from USERS where
USERS.USERNAME = ise_username;
DBMS_OUTPUT.PUT_LINE('found');
ELSE
open resultSet for select 3, 0, 'odbc','ODBC Authen Error' from dual;
DBMS_OUTPUT.PUT_LINE('not found');
END IF;
return resultSet;
end;
END;

```

5. Er bestaat een procedure voor controle van de gebruikersnaam of -machine (gebruikt voor MAB, snelle heraanluiting van PEAP, EAP-FAST en EAP-TTLS).

```

create or replace function ISELOOKUP_R
(
ise_username IN VARCHAR2
) return sys_refcursor AS
BEGIN
declare
c integer;
resultSet SYS_REFCURSOR;
begin
select count(*) into c from USERS where USERS.USERNAME = ise_username;
if c > 0 then
open resultSet for select 0, 11, 'good user', 'no error' from USERS where USERS.USERNAME =
ise_username;
ELSE
open resultSet for select 3, 0, 'odbc','ODBC Authen Error' from dual;
END IF;
return resultSet;
end;
END;

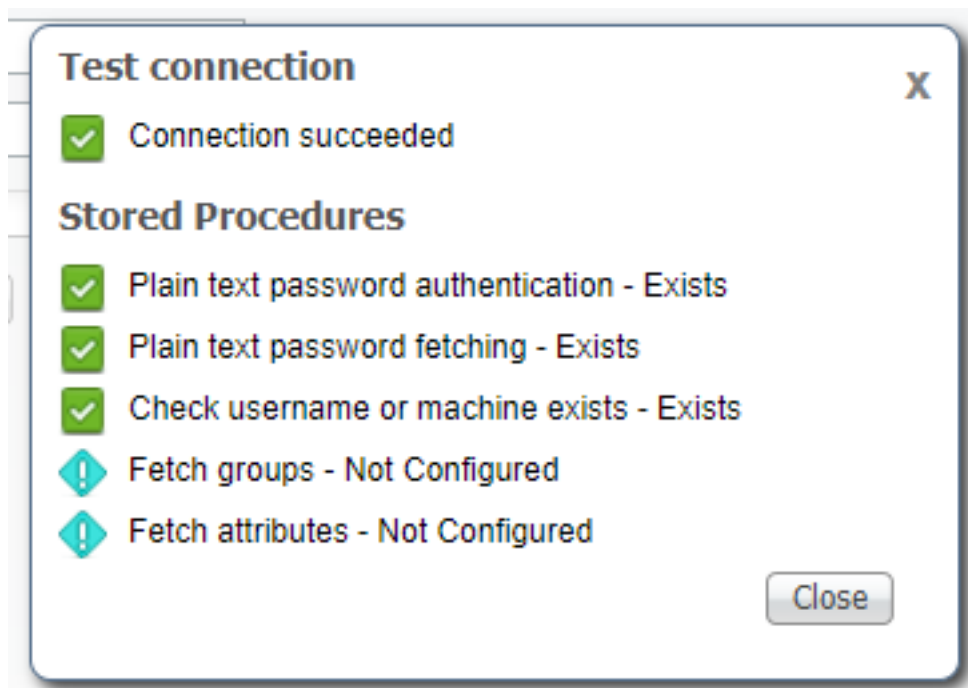
```

6. Procedures op ISE configureren en opslaan

ODBC Identity Source

| General | Connection | Stored Procedures | Attributes | Groups |
|------------------------------------|------------|-------------------|------------|--------|
| Stored procedure type | | Returns recordset | | |
| Plain text password authentication | | ISEAUTH_R | i | + |
| Plain text password fetching | | ISEFETCH_R | i | + |
| Check username or machine exists | | ISELOOKUP_R | i | + |
| Fetch groups | | | i | + |
| Fetch attributes | | | i | + |
| Search for MAC Address in format | | XX-XX-XX-XX-XX-XX | i | |

7. Ga terug naar het tabblad Connection en klik op de knop Test Connection



Stap 4. groepsvernieuwing instellen

1. Maak tabellen met gebruikersgroepen en een andere die voor veel-naar-veel-omzetting wordt gebruikt

```
-----
-- DDL for Table GROUPS
-----
```

```
CREATE TABLE "ISE"."GROUPS"
 ("GROUP_ID" NUMBER(*,0) GENERATED ALWAYS AS IDENTITY MINVALUE 1 MAXVALUE
```

-- Constraints for Table USER_GROUPS_MAPPING

```
ALTER TABLE "ISE"."USER_GROUPS_MAPPING" MODIFY ("USER_ID" NOT NULL ENABLE);  
ALTER TABLE "ISE"."USER_GROUPS_MAPPING" MODIFY ("GROUP_ID" NOT NULL ENABLE);  
ALTER TABLE "ISE"."USER_GROUPS_MAPPING" ADD CONSTRAINT "USER_GROUPS_MAPPING_UK1" UNIQUE  
( "USER_ID", "GROUP_ID")  
USING INDEX PCTFREE 10 INITRANS 2 MAXTRANS 255 COMPUTE STATISTICS  
STORAGE(INITIAL 65536 NEXT 1048576 MINEXTENTS 1 MAXEXTENTS 2147483645  
PCTINCREASE 0 FREELISTS 1 FREELIST GROUPS 1  
BUFFER_POOL DEFAULT FLASH_CACHE DEFAULT CELL_FLASH_CACHE DEFAULT)  
TABLESPACE "USERS" ENABLE;
```

Van GUI:

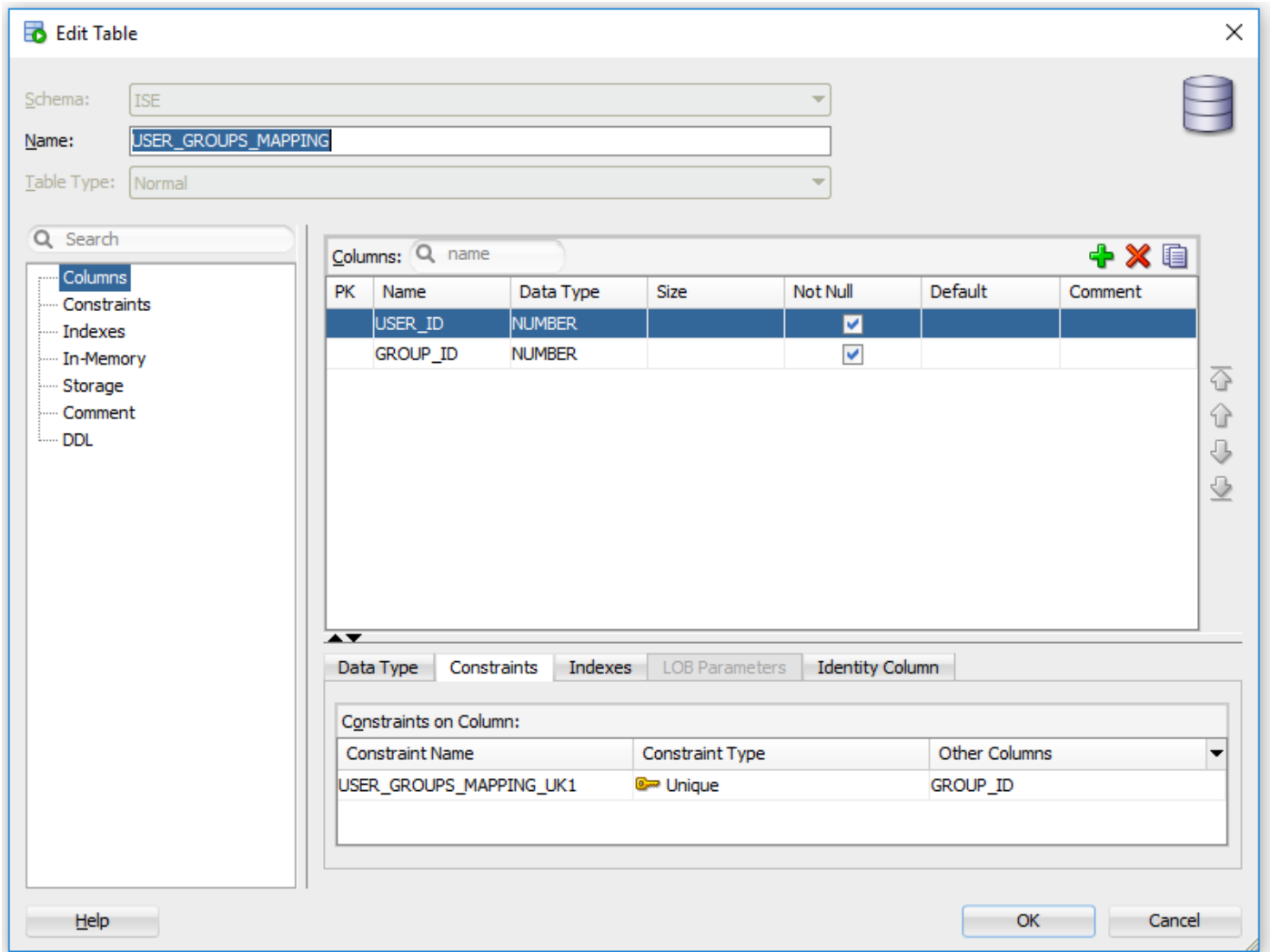
The screenshot shows the 'Edit Table' window for the 'GROUPS' table in the 'ISE' schema. The table type is 'Normal'. The columns are:

| PK | Name | Data Type | Size | Not Null | Default | Comment |
|----|-------------|-----------|------|-------------------------------------|-------------------|---------|
| | GROUP_ID | NUMBER | | <input checked="" type="checkbox"/> | <Identity Colu... | |
| | GROUP_NAME | VARCHAR2 | 255 | <input checked="" type="checkbox"/> | | |
| | DESCRIPTION | CLOB | | <input type="checkbox"/> | | |

The 'Constraints' tab is selected, showing a table of constraints on the column:

| Constraint Name | Constraint Type | Other Columns |
|-----------------|-----------------|---------------|
| GROUPS_PK | Primary Key | |

Buttons for 'Help', 'OK', and 'Cancel' are visible at the bottom.



2. Voeg groepen en afbeeldingen toe zodat **alice** en **bob** tot **groepsgebruikers** behoren en **admin** tot groep **Admins** behoort

```
-- Adding groups
INSERT INTO "ISE"."GROUPS" (GROUP_NAME, DESCRIPTION) VALUES ('Admins', 'Group for administrators')
INSERT INTO "ISE"."GROUPS" (GROUP_NAME, DESCRIPTION) VALUES ('Users', 'Corporate users')

-- Alice and Bob are users
INSERT INTO "ISE"."USER_GROUPS_MAPPING" (USER_ID, GROUP_ID) VALUES ('1', '2')
INSERT INTO "ISE"."USER_GROUPS_MAPPING" (USER_ID, GROUP_ID) VALUES ('2', '2')

-- Admin is in Admins group
INSERT INTO "ISE"."USER_GROUPS_MAPPING" (USER_ID, GROUP_ID) VALUES ('3', '1')
```

3. Maak een groep herhaal procedure. Het geeft alle groepen terug als de gebruikersnaam "" is

```
create or replace function ISEGROUPSH
(
  ise_username IN VARCHAR2,
  ise_result OUT int
) return sys_refcursor as
BEGIN
  declare
    c integer;
    userid integer;
```

```

resultSet SYS_REFCURSOR;
begin
  IF ise_username = '*' then
    ise_result := 0;
    open resultSet for select GROUP_NAME from GROUPS;
  ELSE
    select count(*) into c from USERS where USERS.USERNAME = ise_username;
    select USER_ID into userid from USERS where USERS.USERNAME = ise_username;
    IF c > 0 then
      ise_result := 0;
      open resultSet for select GROUP_NAME from GROUPS where GROUP_ID IN ( SELECT m.GROUP_ID
from USER_GROUPS_MAPPING m where m.USER_ID = userid );
    ELSE
      ise_result := 3;
      open resultSet for select 0 from dual where 1=2;
    END IF;
  END IF;
  return resultSet;
end;
END ;

```

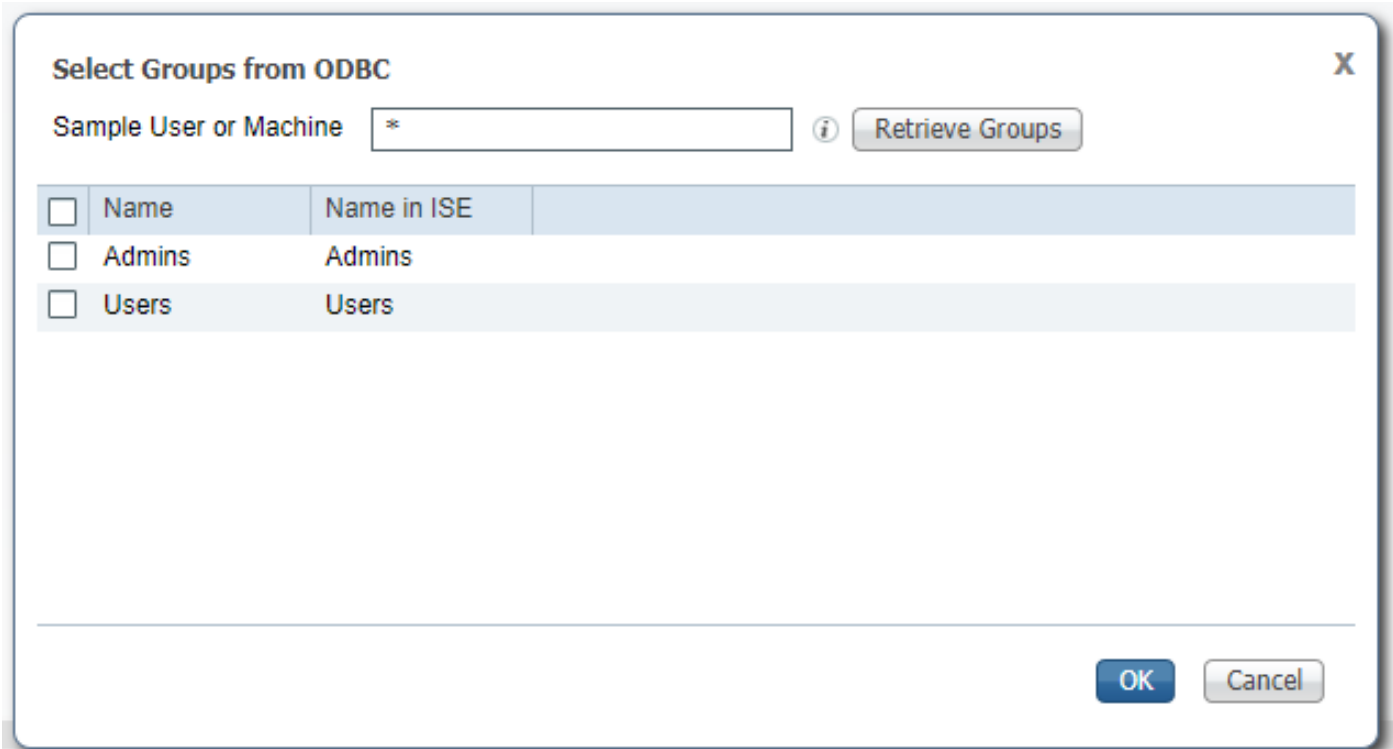
4. Breng de trommel in kaart in de technische groepen

[ODBC List > OracleDB](#)

ODBC Identity Source

| General | Connection | Stored Procedures | Attributes | Groups |
|------------------------------------|-------------------|-------------------|------------|--------|
| Stored procedure type | | Returns recordset | | |
| Plain text password authentication | ISEAUTH_R | | i | + |
| Plain text password fetching | ISEFETCH_R | | i | + |
| Check username or machine exists | ISELOOKUP_R | | i | + |
| <hr/> | | | | |
| Fetch groups | ISEGROUPSH | | i | + |
| Fetch attributes | | | i | + |
| Search for MAC Address in format | XX-XX-XX-XX-XX-XX | | i | |

5. Selecteer de groepen en voeg ze toe aan de ODBC-identiteitsbron



Selecteer de gewenste groepen en klik op OK. Deze verschijnen op het tabblad **Groepen**

[ODBC List](#) > **OracleDB**

ODBC Identity Source

General Connection Stored Procedures Attributes **Groups**

Edit + Add X Delete

| <input type="checkbox"/> | Name | Name in ISE |
|--------------------------|--------|-------------|
| <input type="checkbox"/> | Admins | Admins |
| <input type="checkbox"/> | Users | Users |

Stap 5. Eigenschappen opnieuw instellen

1. Om dit voorbeeld te vereenvoudigen, wordt een vaste tabel gebruikt voor eigenschappen

```
-----
-- DDL for Table ATTRIBUTES
-----
```

```
CREATE TABLE "ISE"."ATTRIBUTES"
  ("USER_ID" NUMBER(*,0),
  "ATTR_NAME" VARCHAR2(255 BYTE),
  "VALUE" VARCHAR2(255 BYTE)
  ) SEGMENT CREATION IMMEDIATE
  PCTFREE 10 PCTUSED 40 INITRANS 1 MAXTRANS 255
  NOCOMPRESS LOGGING
  STORAGE(INITIAL 65536 NEXT 1048576 MINEXTENTS 1 MAXEXTENTS 2147483645
  PCTINCREASE 0 FREELISTS 1 FREELIST GROUPS 1
  BUFFER_POOL DEFAULT FLASH_CACHE DEFAULT CELL_FLASH_CACHE DEFAULT)
  TABLESPACE "USERS" ;
```

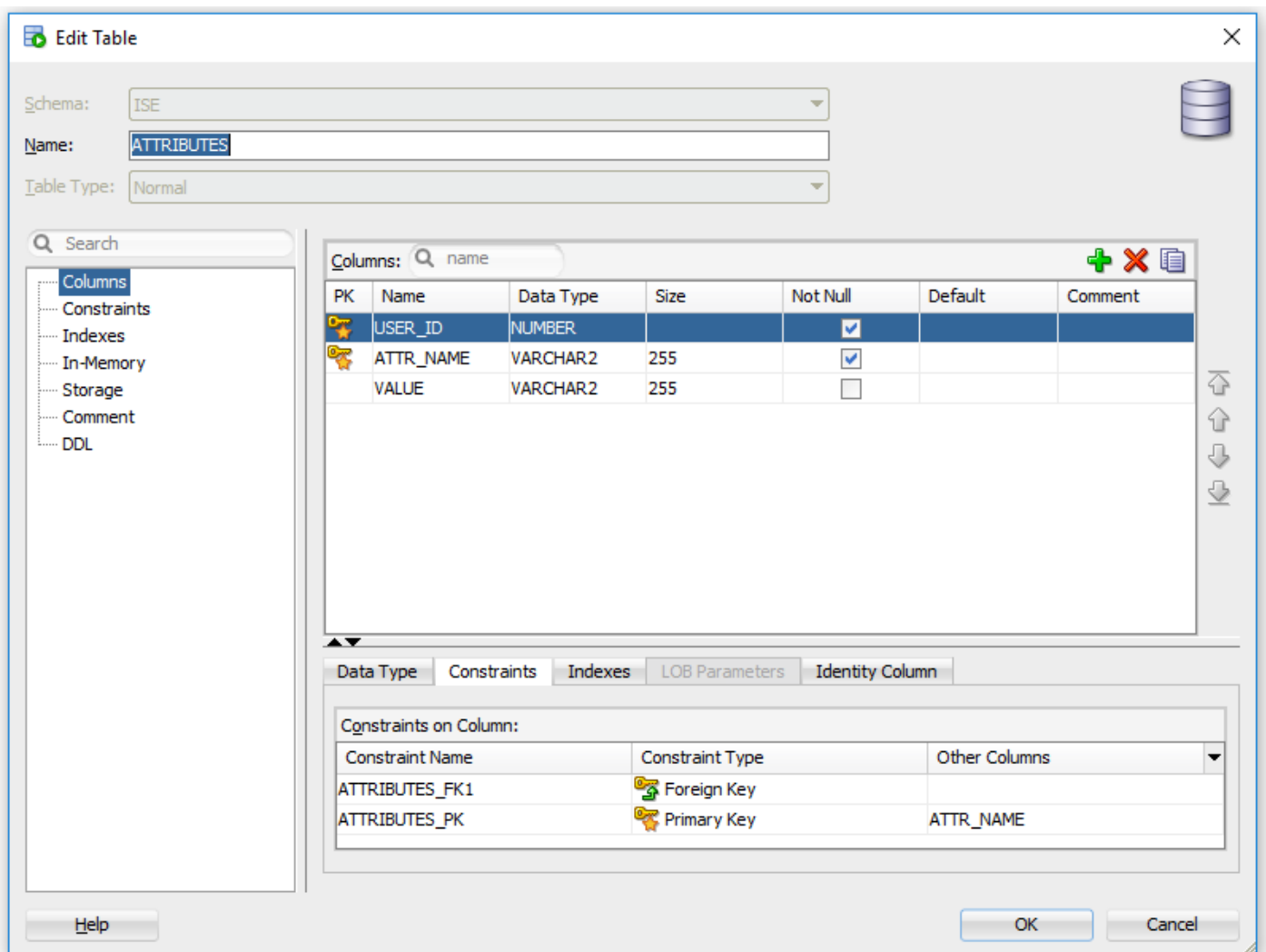
```
-- DDL for Index ATTRIBUTES_PK
```

```
CREATE UNIQUE INDEX "ISE"."ATTRIBUTES_PK" ON "ISE"."ATTRIBUTES" ("ATTR_NAME", "USER_ID")
PCTFREE 10 INITRANS 2 MAXTRANS 255
STORAGE(INITIAL 65536 NEXT 1048576 MINEXTENTS 1 MAXEXTENTS 2147483645
PCTINCREASE 0 FREELISTS 1 FREELIST GROUPS 1
BUFFER_POOL DEFAULT FLASH_CACHE DEFAULT CELL_FLASH_CACHE DEFAULT)
TABLESPACE "USERS" ;
```

```
-- Constraints for Table ATTRIBUTES
```

```
ALTER TABLE "ISE"."ATTRIBUTES" MODIFY ("USER_ID" NOT NULL ENABLE);
ALTER TABLE "ISE"."ATTRIBUTES" MODIFY ("ATTR_NAME" NOT NULL ENABLE);
ALTER TABLE "ISE"."ATTRIBUTES" ADD CONSTRAINT "ATTRIBUTES_PK" PRIMARY KEY ("ATTR_NAME",
"USER_ID")
USING INDEX PCTFREE 10 INITRANS 2 MAXTRANS 255
STORAGE(INITIAL 65536 NEXT 1048576 MINEXTENTS 1 MAXEXTENTS 2147483645
PCTINCREASE 0 FREELISTS 1 FREELIST GROUPS 1
BUFFER_POOL DEFAULT FLASH_CACHE DEFAULT CELL_FLASH_CACHE DEFAULT)
TABLESPACE "USERS" ENABLE;
```

Van GUI:



2. Maak enkele eigenschappen voor gebruikers

```
INSERT INTO "ISE"."ATTRIBUTES" (USER_ID, ATTR_NAME, VALUE) VALUES ('3', 'SecurityLevel', '15')
```

```
INSERT INTO "ISE"."ATTRIBUTES" (USER_ID, ATTR_NAME, VALUE) VALUES ('1', 'SecurityLevel', '5')
INSERT INTO "ISE"."ATTRIBUTES" (USER_ID, ATTR_NAME, VALUE) VALUES ('2', 'SecurityLevel', '10')
```

3. Maak een procedure. Hetzelfde als bij het ophalen van groepen, zal het alle verschillende kenmerken teruggeven als de gebruikersnaam "*" is

```
create or replace function ISEATTRSH
(
  ise_username IN VARCHAR2,
  ise_result OUT int
) return sys_refcursor as
BEGIN
  declare
    c integer;
    userid integer;
    resultSet SYS_REFCURSOR;
  begin
    IF ise_username = '*' then
      ise_result := 0;
      open resultSet for select DISTINCT ATTR_NAME, '0' as "VAL" from ATTRIBUTES;
    ELSE
      select count(*) into c from USERS where USERS.USERNAME = ise_username;
      select USER_ID into userid from USERS where USERS.USERNAME = ise_username;
      if c > 0 then
        ise_result := 0;
        open resultSet for select ATTR_NAME, VALUE from ATTRIBUTES where USER_ID = userid;
      ELSE
        ise_result := 3;
        open resultSet for select 0 from dual where 1=2;
      END IF;
    END IF;
    return resultSet;
  end;
END ;
```

4. Geef de eigenschap op aan **wikkel**

[ODBC List > OracleDB](#)

ODBC Identity Source

| General | Connection | Stored Procedures | Attributes | Groups |
|------------------------------------|------------|-------------------|------------|--------|
| Stored procedure type | | Returns recordset | | |
| Plain text password authentication | | ISEAUTH_R | | |
| Plain text password fetching | | ISEFETCH_R | | |
| Check username or machine exists | | ISELOOKUP_R | | |
| Fetch groups | | ISEGROUPSH | | |
| Fetch attributes | | ISEATTRSH | | |
| Search for MAC Address in format | | XX-XX-XX-XX-XX-XX | | |

5. Eigenschappen

Select Attributes from ODBC X

Sample User or Machine i Retrieve Attributes

| <input type="checkbox"/> | Name | Type | Default Value | Name in ISE |
|--------------------------|---------------|--------|---------------|---------------|
| <input type="checkbox"/> | SecurityLevel | STRING | 0 | SecurityLevel |

OK Cancel

Selecteer eigenschappen en klik op OK.

Stap 6. Verificatie-/autorisatiebeleid configureren

In dit voorbeeld werden de volgende eenvoudige autorisatiebeleid ingesteld:

| | | | | | | |
|-------------------------------------|----------------------------|---------------------------------------|--------------|------------------|---|--|
| <input checked="" type="checkbox"/> | Allow admin network access | OracleDB ExternalGroups EQUALS Admins | PermitAccess | Select from list | 1 | |
| <input checked="" type="checkbox"/> | SecurityLevel too low | OracleDB SecurityLevel EQUALS 5 | DenyAccess | Select from list | 0 | |
| <input checked="" type="checkbox"/> | Allow users network access | OracleDB ExternalGroups EQUALS Users | PermitAccess | Select from list | 2 | |

Gebruikers met **Security Level = 5** worden ontkend.

Stap 7. Voeg Oracle ODBC toe aan Identity Source Seques

Navigeer naar *Administratie > identiteitsbeheer > Vereveningen van Identity Bron*, selecteer uw reeks en voeg ODBC aan de reeks toe:

Identity Source Sequence

▼ Identity Source Sequence

* Name

Description

▼ Certificate Based Authentication

Select Certificate Authentication Profile

▼ Authentication Search List

A set of identity sources that will be accessed in sequence until first authentication succeeds

Available



Selected



▼ Advanced Search List Settings

If a selected identity store cannot be accessed for authentication

- Do not access other stores in the sequence and set the "AuthenticationStatus" attribute to "ProcessError"
- Treat as if the user was not found and proceed to the next store in the sequence

Opslaan.

Verifiëren

U zou nu in staat moeten zijn om gebruikers tegen ODBC voor authenticatie te verklaren en hun groepen en eigenschappen terug te winnen.

RADIUS-bewegende documenten

Voer bepaalde authenticaties uit en navigeer naar *bewerkingen > RADIUS > Live Logs*

| Time | Status | Details | Repeat ... | Identity | Endpoint ID | Endpoint P... | Authenticat... | Authorizati... | Authorizati... | IP Address | Network Device |
|------------------------------|--------|---------|------------|----------|-------------------|---------------|-----------------|-----------------|----------------|---------------|----------------|
| x | | | | Identity | Endpoint ID | Endpoint Prof | Authenticator | Authorization | Authorization | IP Address | Network Device |
| Aug 08, 2017 04:31:32.545 PM | | | | badUser | 92:77:F1:E4:D2:53 | | Default >> D... | Default | | | SWITCH |
| Aug 08, 2017 04:31:32.485 PM | | | 0 | admin | 61:AD:77:0F:DF:CF | FreeBSD-W... | Default >> D... | Default >> A... | PermitAccess | 83.133.106.96 | |
| Aug 08, 2017 04:31:32.460 PM | | | | admin | 61:AD:77:0F:DF:CF | | Default >> D... | Default >> A... | PermitAccess | | SWITCH |
| Aug 08, 2017 04:31:32.365 PM | | | 0 | bob | FC:F4:97:F2:F5:4F | | Default >> D... | Default >> A... | PermitAccess | 241.97.134.20 | |
| Aug 08, 2017 04:31:32.359 PM | | | | bob | FC:F4:97:F2:F5:4F | | Default >> D... | Default >> A... | PermitAccess | | SWITCH |
| Aug 08, 2017 04:31:32.237 PM | | | | alice | 42:27:B1:C6:F9:A4 | | Default >> D... | Default >> S... | DenyAccess | | SWITCH |

Zoals je kunt zien, heeft Alice **SecurityLevel = 5**, dus de toegang werd verworpen.

Detail-rapport

Klik op **Detail-rapport** in de kolom **Details** voor de interessante sessie om de stroom te controleren.

Gedetailleerd rapport voor gebruiker Alice (verworpen vanwege het lage veiligheidsniveau):

