

Configuración ODBC en ISE 2.3 con la base de datos Oracle

Contenido

[Introducción](#)

[prerrequisitos](#)

[Requisitos](#)

[Componentes Utilizados](#)

[Configurar](#)

[Paso 1. Configuración básica del Oracle](#)

[Paso 2. Configuración básica ISE](#)

[Paso 3. Autenticación de usuario de la configuración](#)

[Paso 4. Extracción del grupo de la configuración](#)

[Paso 5. La configuración atribuye la extracción](#)

[Paso 6. Directivas de la autenticación/de la autorización de la configuración](#)

[Paso 7. Agregue el Oracle ODBC a las secuencias de la fuente de la identidad](#)

[Verificación](#)

[Registros vivos RADIUS](#)

[Informe de la reunión](#)

[Troubleshooting](#)

[Se utilizan las credenciales incorrectas](#)

[Nombre incorrecto DB \(nombre del servicio\)](#)

[Autenticaciones de usuarios del Troubleshooting](#)

[Referencias](#)

Introducción

Este documento describe cómo configurar el Identity Services Engine (ISE) con la base de datos Oracle para la autenticación ISE usando la Conectividad abierta de base de datos (ODBC).

La autenticación de la Conectividad abierta de base de datos (ODBC) requiere el ISE poder traer una contraseña del usuario del sólo texto. La contraseña se puede cifrar en la base de datos, pero tiene que ser descriptada por el procedimiento almacenado.

Prerrequisitos

Requisitos

Cisco recomienda que tenga conocimiento sobre estos temas:

- Cisco Identity Services Engine 2.3
- Base de datos y conceptos ODBC
- Oracle

Componentes Utilizados

La información que contiene este documento se basa en las siguientes versiones de software y hardware.

- Identity Services Engine 2.3.0.298
- Centos 7
- Base de datos Oracle 12.2.0.1.0
- Desarrollador 4.1.5 del Oracle SQL

Configurar

Nota: Procedimientos SQL de la invitación presentados en este documento como ejemplos. Ésta no es un funcionario y una manera recomendada de configuración del Oracle DB. Asegúrese de que usted entienda el resultado y el impacto de cada consulta SQL que usted confía.

Paso 1. Configuración básica del Oracle

En este ejemplo el Oracle fue configurado con los parámetros siguientes:

- Nombre DB: **ORCL**
- Nombre del servicio: **orcl.vkumov.local**
- Puerto: **1521** (valor por defecto)
- Creado explique el ISE con el **ise del** nombre de usuario

Configure su base de datos Oracle antes de progresar.

Paso 2. Configuración básica ISE

Cree una fuente de la identidad ODBC en la *administración > fuente externa de la identidad > ODBC* y conexión de prueba:

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

Nota: El ISE conecta con el Oracle usando el nombre del servicio, por lo tanto el campo del [Database name] se debe llenar del nombre del servicio que existe en el Oracle, nombre no SID (o DB). Debido a los puntos del bug [CSCvf06497](#) (.) no puede ser utilizado en el campo del [Database name]. Este bug se repara en ISE 2.3.

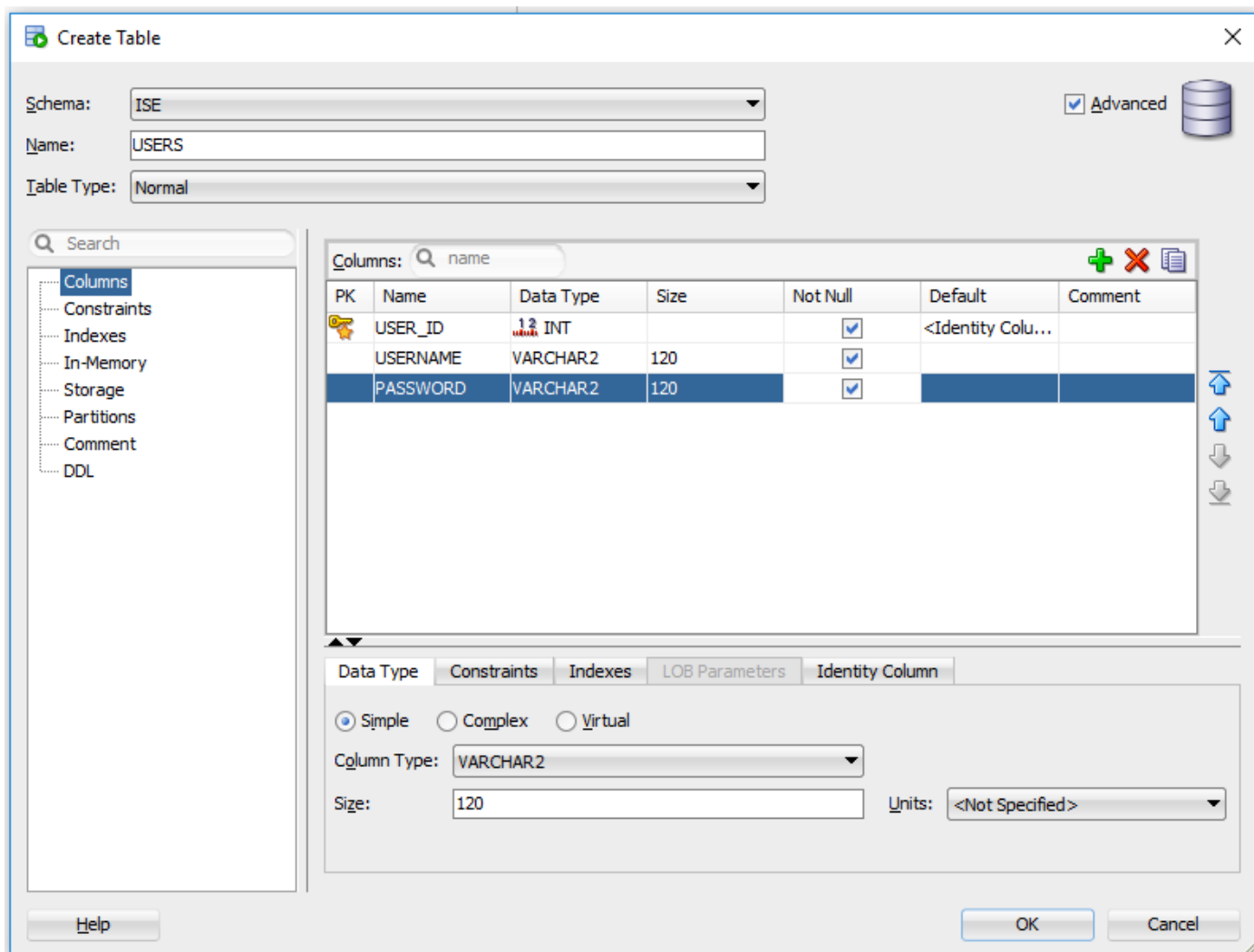
Paso 3. Autenticación de usuario de la configuración

La autenticación ISE al ODBC utiliza los procedimientos almacenados. Es posible seleccionar el tipo de procedimientos. En este ejemplo utilizamos los recordsets como vuelta.

Para otros procedimientos, refiera al [guía del administrador del Cisco Identity Services Engine, la versión 2.3](#)

Consejo: Es posible volver los parámetros Nombrados en vez del resultSet. Es apenas un tipo diferente de salida, las funciones es lo mismo.

1. Cree la tabla con las credenciales de los usuarios. Asegurese le fijan las configuraciones de la identidad en la **Clave primaria**.



2. Agregue a los usuarios

```
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. Cree un procedimiento para la autenticación de contraseña del sólo texto (usada para el método interno PAP, EAP-GTC, el 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. Cree un procedimiento para la recogida de la contraseña del sólo texto (usada para la GRIETA, MSCHAPv1/v2, EAP-MD5, SALTO, método interno del EAP MSCHAPv2, el 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. Cree un procedimiento para el nombre de usuario del control o la máquina existe (utilizado para el MAB, rápido vuelva a conectar del PEAP, del EAP-FAST y del 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;

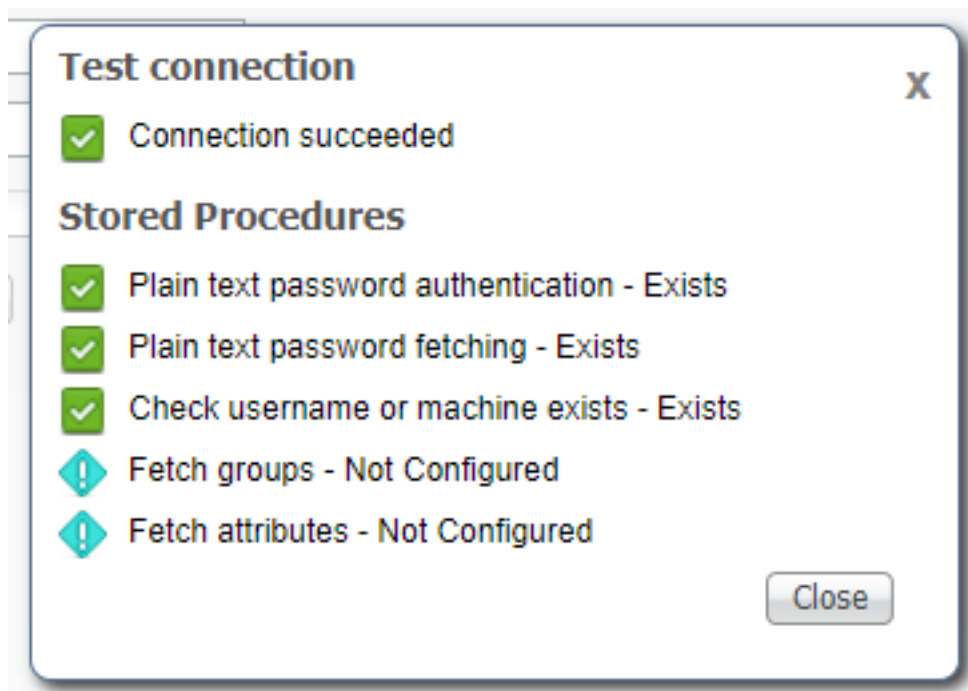
```

6. Configure los procedimientos en el ISE y sávelos

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. Vuelva a la lengüeta de la conexión y al botón del Haga clic en Probar conexión



Paso 4. Extracción del grupo de la configuración

1. Cree las tablas que contienen a los grupos de usuarios y otras usadas para la asignación múltiple

```
-----
-- 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;
```

Del GUI:

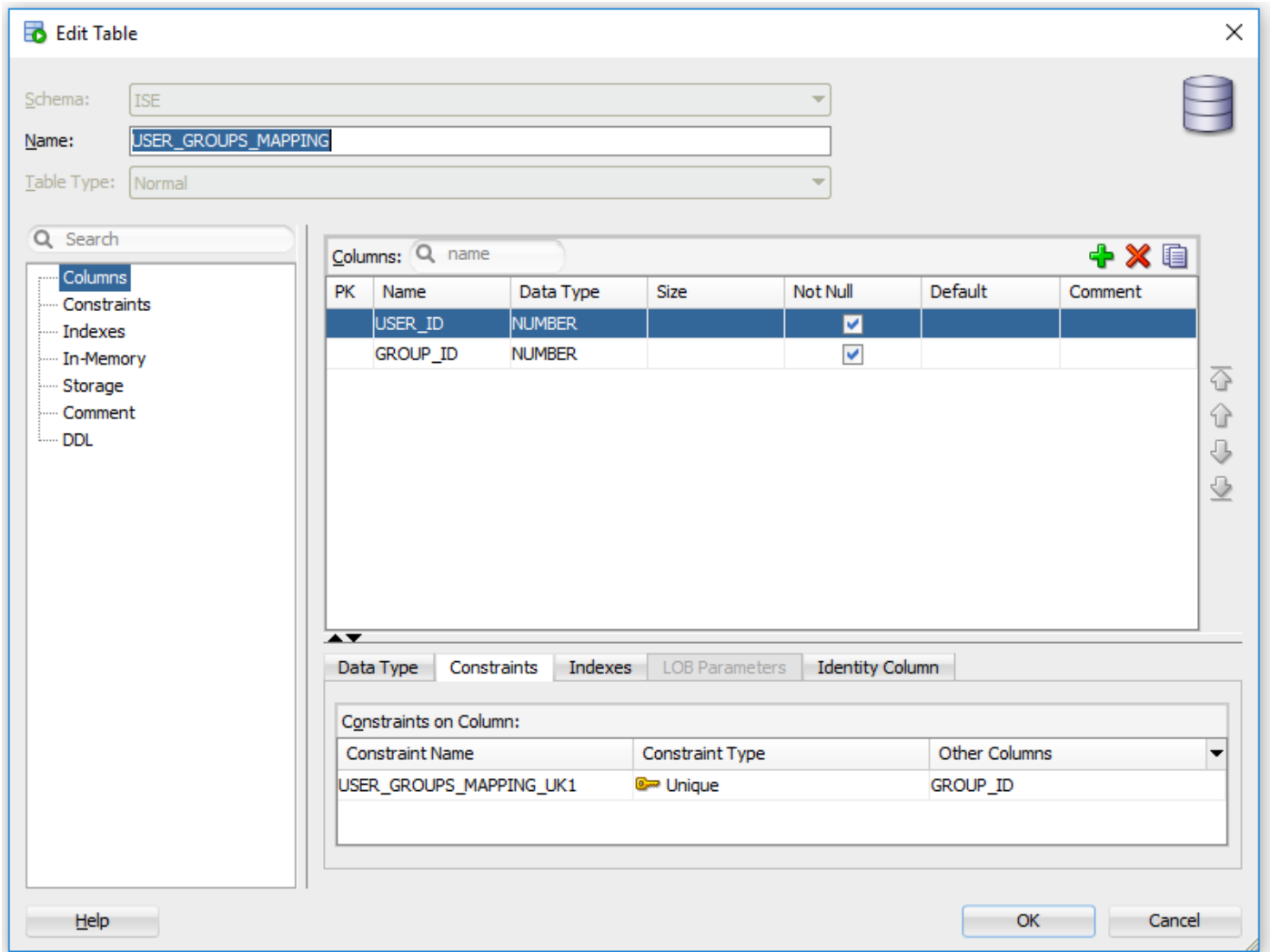
The screenshot shows the 'Edit Table' dialog box for the table 'GROUPS' in the 'ISE' schema. The table type is 'Normal'. The columns are listed in a table below:

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"/>		

Below the columns table, the 'Constraints' tab is active, showing a table of constraints on the column:

Constraint Name	Constraint Type	Other Columns
GROUPS_PK	Primary Key	

The dialog box includes a 'Search' field, a tree view on the left with 'Columns' selected, and 'Help', 'OK', and 'Cancel' buttons at the bottom.



2. Agregue los grupos y las asignaciones, de modo que **Alicia** y la **sacudida** pertenezcan para agrupar a los **usuarios** y el **admin** pertenezca para agrupar **Admins**

```
-- 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. Cree un procedimiento de la extracción del grupo. Vuelve a todos los grupos si es el nombre de usuario “*”

```
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 ;

```

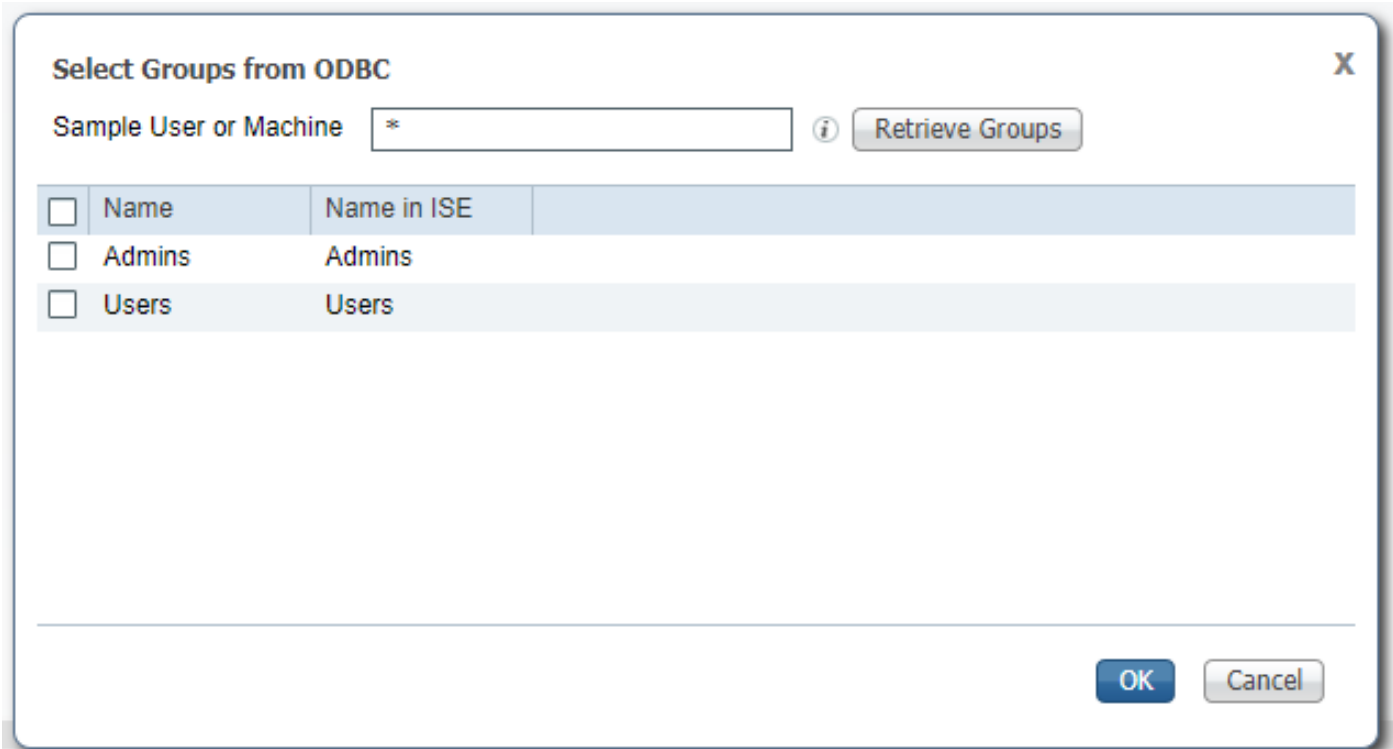
4. Asíelo para traer a los grupos

[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. Traiga a los grupos y agreguelos en la fuente de la identidad ODBC



Select necesitó a los grupos y AUTORIZACIÓN del teclado, aparecerán en la lengüeta de los grupos

[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

Paso 5. La configuración atribuye la extracción

1. Para simplificar este ejemplo, una tabla plana se utiliza para los atributos

```
-----
-- 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;
```

Del GUI:

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

PK	Name	Data Type	Size	Not Null	Default	Comment
	USER_ID	NUMBER		<input checked="" type="checkbox"/>		
	ATTR_NAME	VARCHAR2	255	<input checked="" type="checkbox"/>		
	VALUE	VARCHAR2	255	<input type="checkbox"/>		

The 'Constraints on Column' section shows:

Constraint Name	Constraint Type	Other Columns
ATTRIBUTES_FK1	Foreign Key	
ATTRIBUTES_PK	Primary Key	ATTR_NAME

2. Cree algunos atributos para los usuarios

```

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. Cree un procedimiento. Lo mismo que con la extracción de los grupos, volverá todos los atributos distintos si es el nombre de usuario "*"

```

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. Asíelo para traer los atributos

[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			
<hr/>				
Fetch groups	ISEGROUPSH			
Fetch attributes	ISEATTRSH			
Search for MAC Address in format	XX-XX-XX-XX-XX-XX			

5. Traiga los atributos

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

Seleccione los atributos y haga clic la AUTORIZACIÓN.

Paso 6. Directivas de la autenticación/de la autorización de la configuración

En este ejemplo las directivas simples siguientes de la autorización fueron configuradas:

<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	

Negarán los usuarios con **SecurityLevel = 5**.

Paso 7. Agregue el Oracle ODBC a las secuencias de la fuente de la identidad

Navigate a las *secuencias de la fuente de la administración* > de la *Administración de la identidad* > de la *identidad*, seleccione su secuencia y agregue el ODBC a la secuencia:

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

Sávelo.

Verificación

Usted debe ahora poder autenticar a los usuarios contra el ODBC ahora y extraer sus grupos y atributos.

Registros vivos RADIUS

Realice algunas autenticaciones y navegue a las *operaciones > al RADIUS > los registros vivos*

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

Como usted puede ver, el usuario Alicia tiene **SecurityLevel = 5**, por lo tanto el acceso fue rechazado.

Informe de la reunión

Haga clic en el **informe de la reunión** en la columna de los **detalles** para la sesión interesante para marcar el flujo.

Informe detallado para el usuario Alicia (rechazada debido a SecurityLevel bajo):

