

Oracle Database で ISE 2.3 の ODBC を設定して下さい

目次

[はじめに](#)

[前提条件](#)

[要件](#)

[使用するコンポーネント](#)

[設定](#)

[ステップ 1. Oracle 基本設定](#)

[ステップ 2. ISE 基本設定](#)

[ステップ 3. ユーザ認証を設定して下さい](#)

[ステップ 4. グループ検索を設定して下さい](#)

[ステップ 5. 属性検索を設定して下さい](#)

[ステップ 6. 認証/許可ポリシーを設定して下さい](#)

[ステップ 7. 識別ソース シーケンスに Oracle ODBC を追加して下さい](#)

[確認](#)

[RADIUS ライブ ログ](#)

[Detail レポート](#)

[トラブルシューティング](#)

[不正確な信任状は使用されません](#)

[間違った DB 名前 \(サービス名 \)](#)

[ユーザ認証を解決して下さい](#)

[参考資料](#)

概要

この資料に開放型データベース接続 (ODBC) を使用して ISE 認証のための Oracle Database で Identity Services Engine (ISE) を設定する方法を記述されています。

開放型データベース接続 (ODBC) 認証は ISE が平文 ユーザパスワードを抽出せません要求します。パスワードはデータベースで暗号化することができまじたり保存された手順によって復号化されなければなりません。

前提条件

要件

次の項目に関する知識が推奨されます。

- Cisco Identity Services Engine 2.3
- データベースおよび ODBC 概念
- Oracle

使用するコンポーネント

このドキュメントの情報は、次のソフトウェアとハードウェアのバージョンに基づくものです。

- Identity Services Engine 2.3.0.298
- Centos 7
- Oracle Database 12.2.0.1.0
- Oracle SQL 開発者 4.1.5

設定

注: 例としてこの資料で示される SQL 手順を扱って下さい。これは Oracle DB 設定の公式および推奨方法ではありません。託す各 SQL クエリの結果および影響を理解するようにして下さい。

ステップ 1. Oracle 基本設定

この例で Oracle は次のパラメータで設定されました:

- DB 名前: **ORCL**
- Service name : **orcl.vkumov.local**
- Port: **1521** (デフォルト)
- ユーザ名 **ise** との ISE のための作成されたアカウント

更に続行する前に Oracle を設定する必要があります。

ステップ 2. ISE 基本設定

Administration で ODBC 識別ソースを > 外部識別ソース > ODBC およびテスト接続作成して下さい:

ODBC Identity Source

General	Connection	Stored Procedures	Attributes	Groups
ODBC DB connection details				
* Hostname/IP[:port]	<input type="text" value="10.48.26.61"/>			
* Database name	<input type="text" value="orcl.vkumov.local"/>			
Admin username	<input type="text" value="ise"/>			
Admin password	<input type="password" value="....."/>			
* Timeout	<input type="text" value="5"/>			
* Retries	<input type="text" value="1"/>			
* Database type	<input type="text" value="Oracle"/>			
<input type="button" value="Test Connection"/>				

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

注: ISE はサービス名を使用して Oracle に接続しま、それ故に[データベース名]フィールドはサービス名で一杯にする必要がありま、ない SID Oracle で存在します (または DB 名前)。バグ [CSCVf06497](#) ドットが原因で (。) [データベース名]フィールドで使用することができません。このバグは ISE 2.3 でフィックスされます。

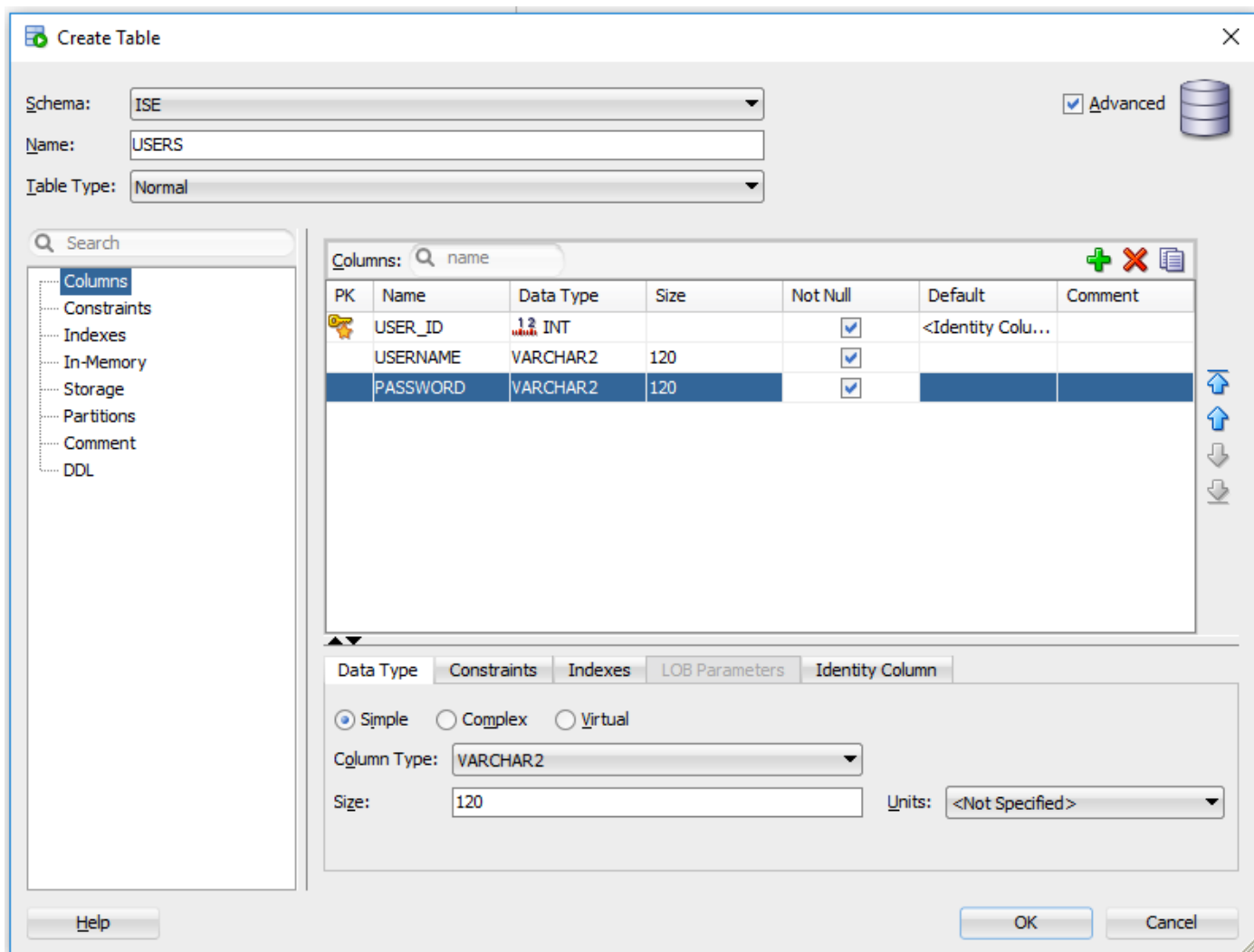
ステップ 3. ユーザ認証を設定して下さい

ODBC への ISE 認証は保存された手順を使用します。手順の『Type』を選択することは可能性のあるです。この例で戻りとしてレコードセットを使用します。

他の手順に関しては、[Cisco Identity Services Engine 管理者ガイドを、リリース 2.3](#) 参照して下さい

ヒント : resultSet の代わりに指定されたパラメータを戻すことは可能性のあるです。それは出力のちょうど異なる型、機能性です同じです。

1. ユーザの信任状で表を作成して下さい。主キーの識別設定を行ったことを確かめて下さい。



2. ユーザを追加して下さい

```
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. 平文 パスワード認証における手順を作成して下さい (PAP、EAP-GTC 内部方式に、TACACS 使用する)

```
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. 平文パスワード取出す手順を作成して下さい (CHAP、MSCHAPv1/v2 に、EAP-MD5、LEAP、EAP-MSCHAPv2 内部方式、TACACS 使用する)

```
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. チェック ユーザ名またはマシン作成して下さい (MAB に存在 する手順を、速く PEAP、EAP-FAST および EAP-TTLS の再接続して下さい使用する)

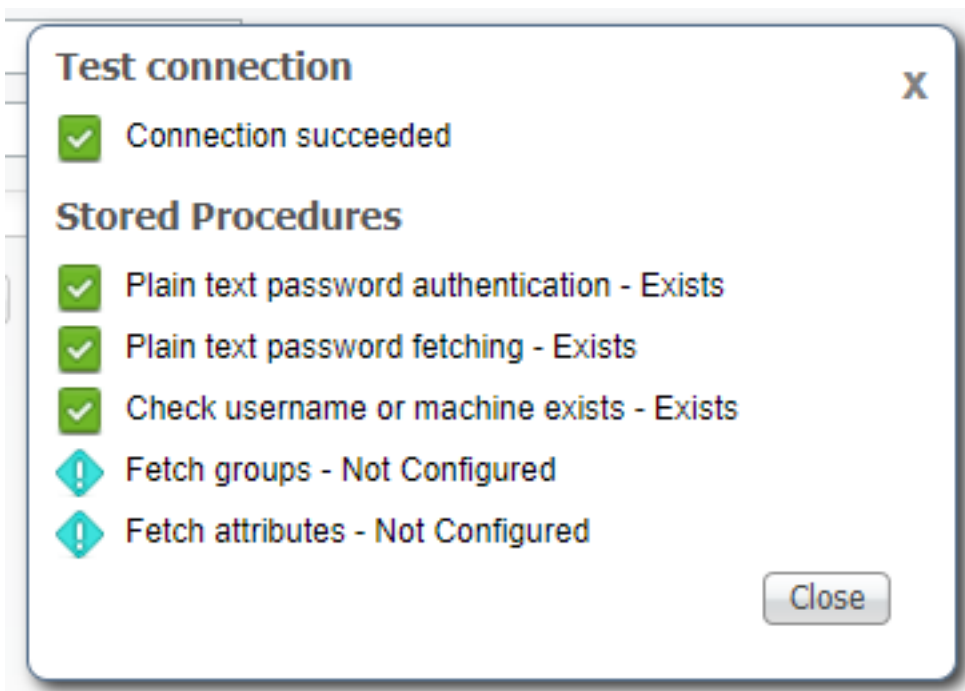
```
create or replace function ISELOOKUP_R  
(  
  ise_username IN VARCHAR2  
) return sys_refcursor AS  
BEGIN  
  declare  
    c integer;  
    resultSet SYS_REFCURSOR;  
  begin  
    select count(*) into c from USERS where USERS.USERNAME = ise_username;  
    if c > 0 then  
      open resultSet 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. ISE の手順を設定し、保存して下さい

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. Connection タブに戻り、ボタンを[Test Connection]をクリックする



ステップ 4.グループ検索を設定して下さい

1. ユーザグループが含まれている表および多対多マッピングに使用する別のものを作成して下さい

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

GUI から :

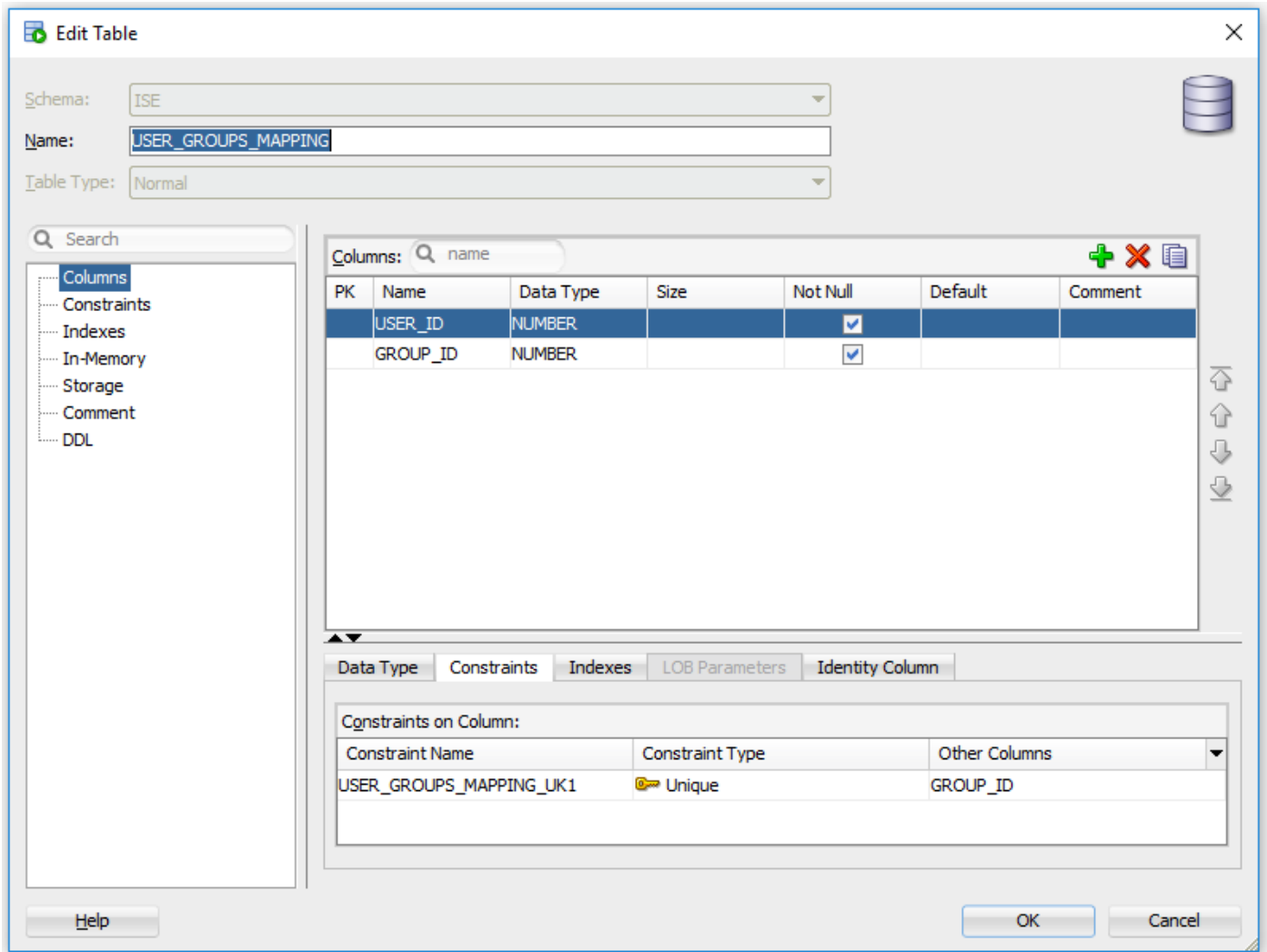
The screenshot shows the 'Edit Table' dialog box for the 'GROUPS' table in the 'ISE' schema. The table type is 'Normal'. The columns are listed as follows:

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 'Help' button on the bottom left and 'OK' and 'Cancel' buttons on the bottom right.



2. ユーザをグループ化するためにアリスおよび下げ振が属し、Admin をグループ化するために admin が属するように、グループおよびマッピングを追加して下さい

```
-- 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. グループ検索手順を作成して下さい。それはユーザ名が「*」ある場合すべてのグループを戻します

```
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 ;

```

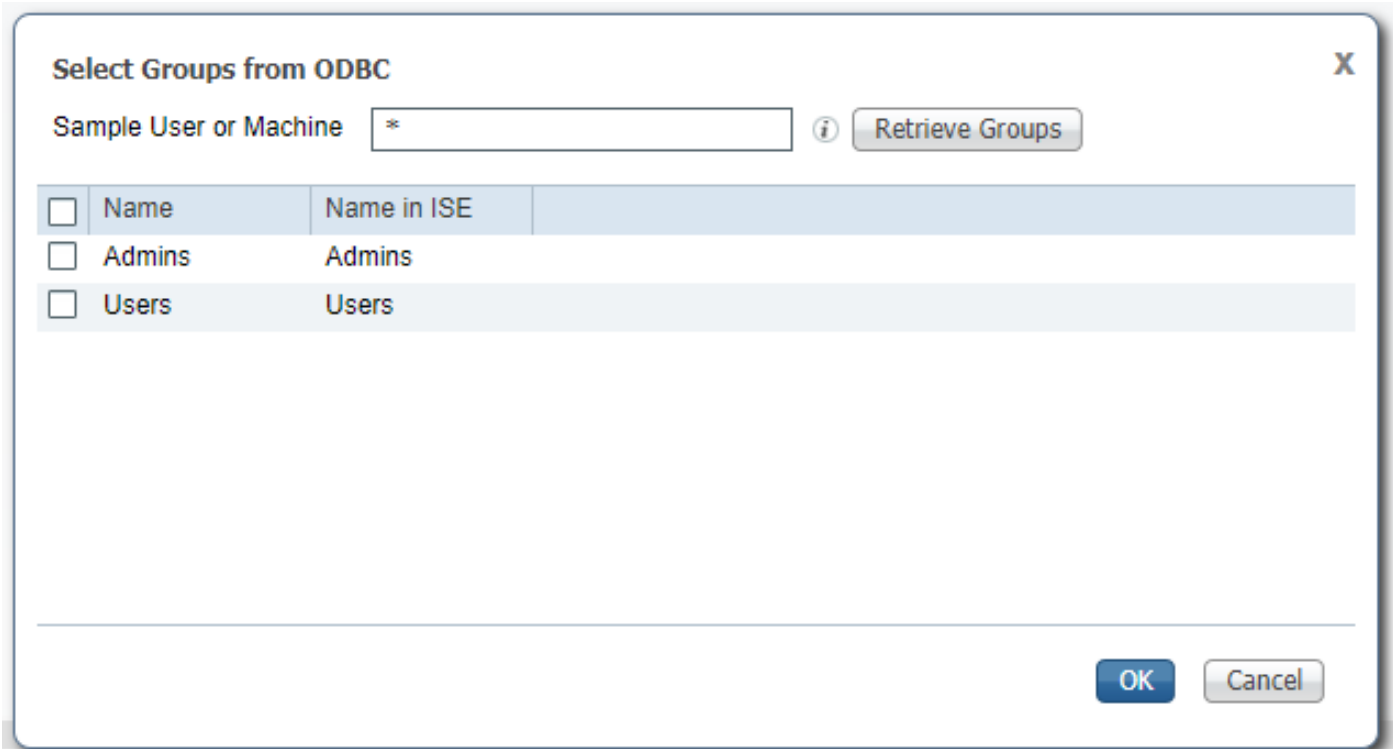
4. グループを抽出するためにそれをマップして下さい

[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	+
Fetch groups		ISEGROUPSH	i	+
Fetch attributes			i	+
Search for MAC Address in format		XX-XX-XX-XX-XX-XX	i	

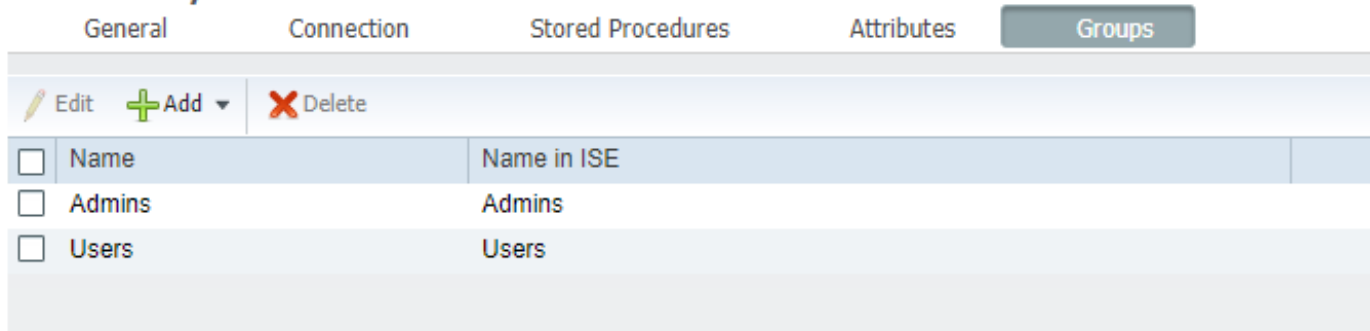
5. グループを抽出し、ODBC 識別ソースにそれらを追加して下さい



select 「グループ」タブでグループを必要とし、彼ら現われます[OK]をクリックする

ODBC List > OracleDB

ODBC Identity Source



ステップ 5.属性検索を設定して下さい

1. この例を簡素化するために、平らな表は属性のために使用されます

```
-----
-- 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" ;
```

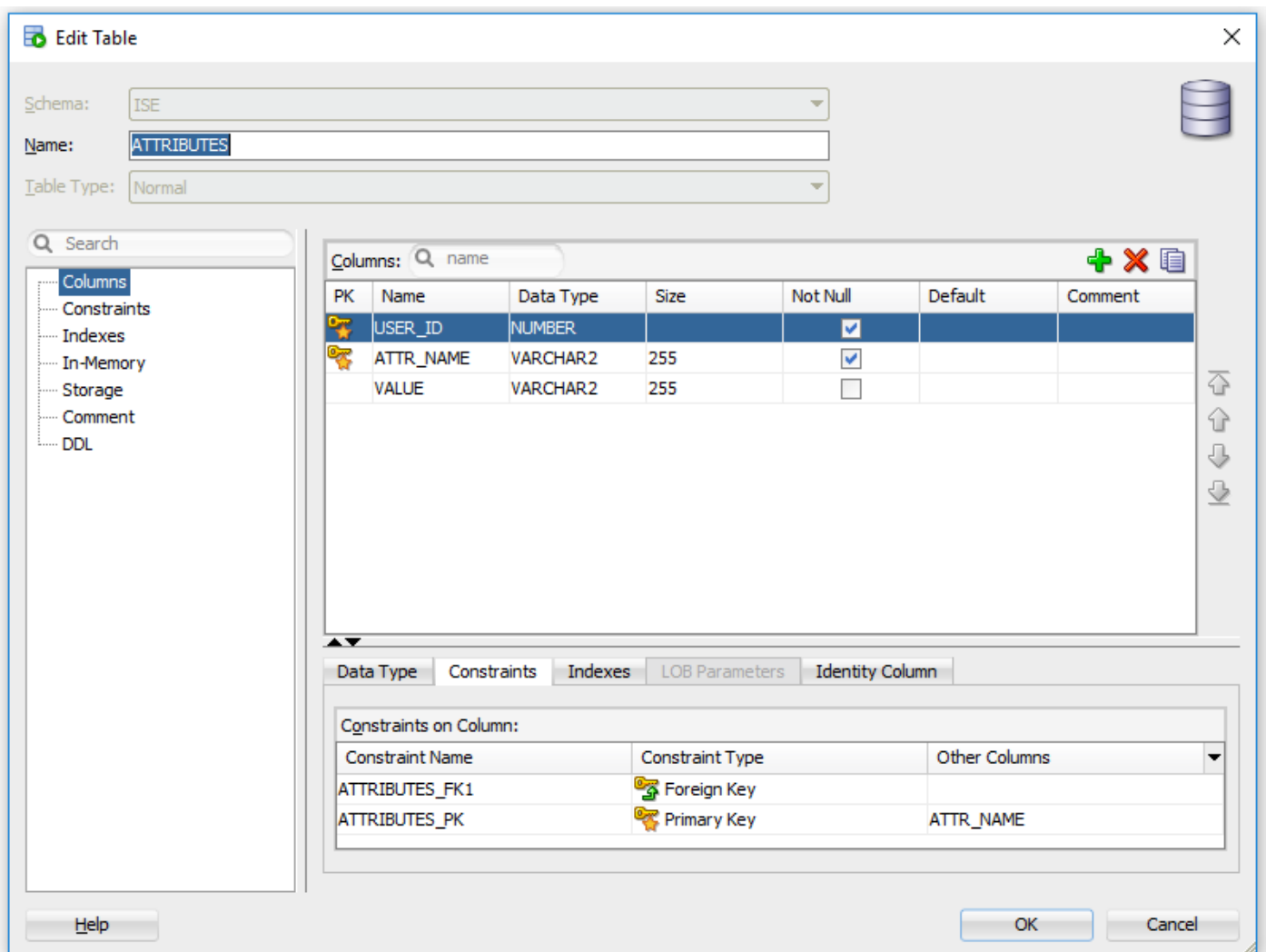
-- DDL for Index ATTRIBUTES_PK

```
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;
```

GUI から :



2. ユーザ向けのいくつかの属性を作成して下さい

```
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. 手順を作成して下さい。同じグループ検索と同様に、それはユーザ名が「*」ある場合すべての個別の属性を戻します

```
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 ;
```

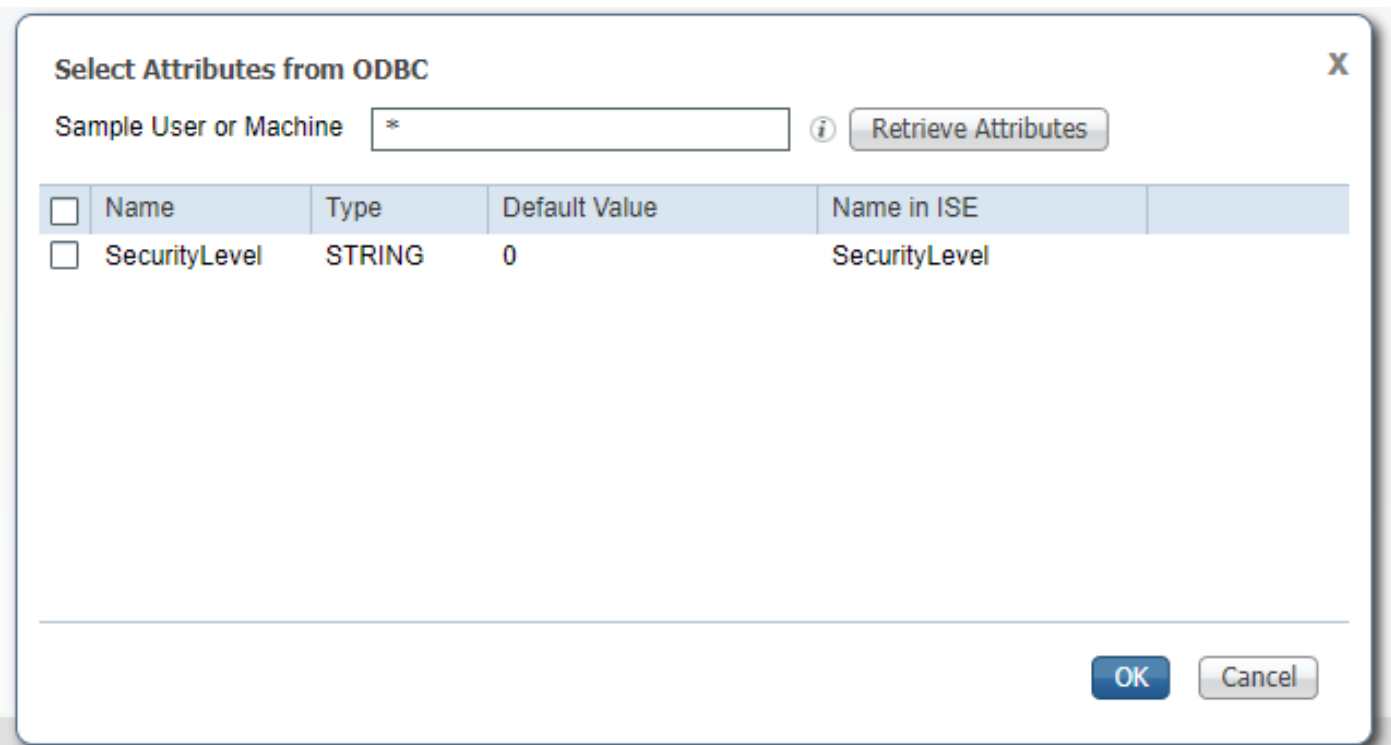
4. 属性を取出すためにそれをマップして下さい

[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. 属性を取出して下さい



『Attributes』を選択し、[OK]をクリックする。

ステップ 6. 認証/許可ポリシーを設定して下さい

この例で次の簡単な承認ポリシーは設定されました:

<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	

SecurityLevel のユーザは = 5 否定されます。

ステップ 7. 識別ソース シーケンスに Oracle ODBC を追加して下さい

Administration > アイデンティティ管理 > 識別ソース シーケンスにナビゲートし、シーケンスを選択し、シーケンスに ODBC を追加して下さい:

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

それを保存して下さい。

確認

ユーザを ODBC に対して今では認証し、グループおよび属性を取得今できるはずです。

RADIUS ライブ ログ

オペレーション > RADIUS にいくつかの認証およびナビゲートを > ライブ ログ行って下さい

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

見てわかるように、ユーザ アリスは SecurityLevel が = 5 あります、それ故にアクセスは拒否されました。

Detail レポート

フローをチェックするために興味深いセッションのための Details カラムのレポートを『Detail』をクリックして下さい。

ユーザ アリス (低い SecurityLevel が拒否された原因で) 向けの Detailed レポート:

