

用Oracle数据库配置在ISE 2.3的ODBC

目录

[简介](#)

[先决条件](#)

[要求](#)

[使用的组件](#)

[配置](#)

[步骤1. Oracle基本配置](#)

[步骤2. ISE基本配置](#)

[步骤3.配置用户认证](#)

[步骤4.配置组检索](#)

[步骤5.配置属性检索](#)

[步骤6.配置认证/授权策略](#)

[步骤7.添加Oracle ODBC到身份来源顺序](#)

[验证](#)

[RADIUS实际日志](#)

[详细资料报表](#)

[故障排除](#)

[使用不正确证件](#)

[错误的DB名字\(服务名称\)](#)

[排除用户认证故障](#)

[参考](#)

简介

本文描述如何用ISE认证的Oracle数据库配置身份服务引擎(ISE)使用开放数据库连接(ODBC)。

开放数据库连接(ODBC)认证要求ISE能拿来一个纯文本用户密码。密码在数据库被加密，但是必须由存储过程解码。

先决条件

要求

Cisco 建议您了解以下主题：

- 思科身份服务引擎2.3
- 数据库和ODBC概念
- Oracle

使用的组件

本文档中的信息基于以下软件和硬件版本：

- 身份服务引擎2.3.0.298
- Centos 7
- Oracle数据库12.2.0.1.0
- Oracle SQL开发者4.1.5

配置

注意：对待在本文提交的SQL存储过程作为示例。这不是Oracle DB配置一个正式和推荐的方式。保证您了解您做每次SQL查询的结果和影响。

步骤1. Oracle基本配置

在本例中Oracle配置有以下参数：

- DB名字：**ORCL**
- 服务名称：**orcl.vkumov.local**
- 端口：**1521** (默认值)
- ISE的被创建的帐户与用户名**ise**

在将来发生前配置您的Oracle数据库。

步骤2. ISE基本配置

创建一个ODBC身份来源在Administration >外部身份来源> ODBC和测试连接：

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

注意：使用服务名称，ISE连接到Oracle，因此在Oracle中存在，不是SID应该充满的 [Database name] 字段服务名称(或DB名字)。由于Bug [CSCvf06497](#) 小点(.)不能用于 [Database name] 字段。此Bug在ISE 2.3被修复。

步骤3.配置用户认证

对ODBC用途存储过程的ISE认证。选择程序的类型是可能的。在本例中我们使用recordsets作为回归。

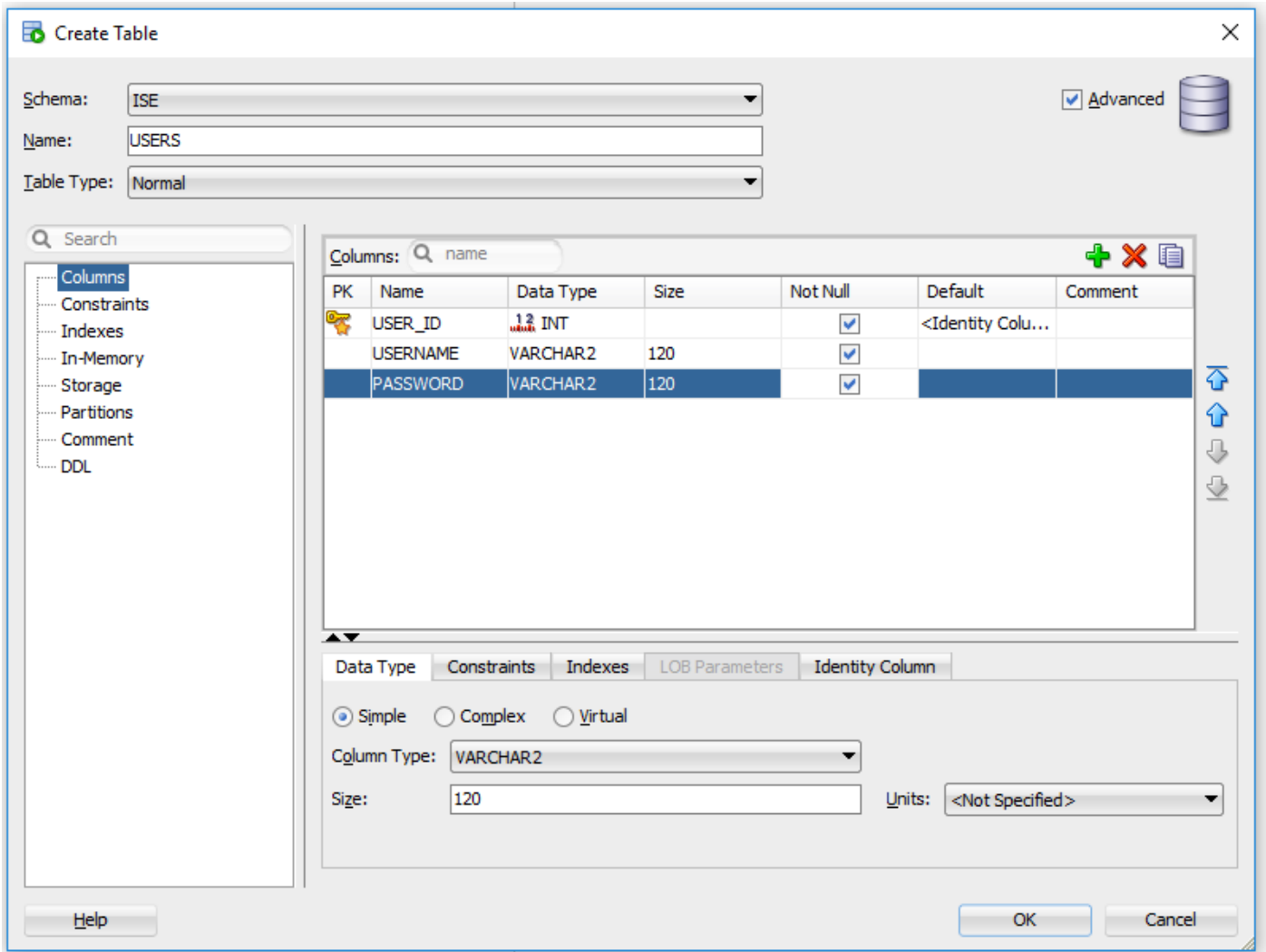
关于其他程序，请参见[思科身份服务引擎管理员指南，版本2.3](#)

提示：返回已命名参数而不是resultSet是可能的。它是不同种输出，功能是相同的。

1. 用用户的证件创建表。确定您设了在主密钥的身份设置。

```
-----
-- DDL for Table USERS
-----

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

2. 添加用户

```
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. 创建纯文本密码验证一个程序(用于PAP，EAP-GTC内在方法，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;
  return resultSet;
END
```

```
end;  
END ISEAUTH_R;
```

4. 创建纯文本密码拿来一个程序(用于CHAP , MSCHAPv1/v2 , EAP-MD5 , LEAP , EAP-MSCHAPv2内在方法 , 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. 创建检查用户名一个程序或机器存在(使用MAB , 快速地请重新连接PEAP、EAP-FAST和EAP-TTLS)

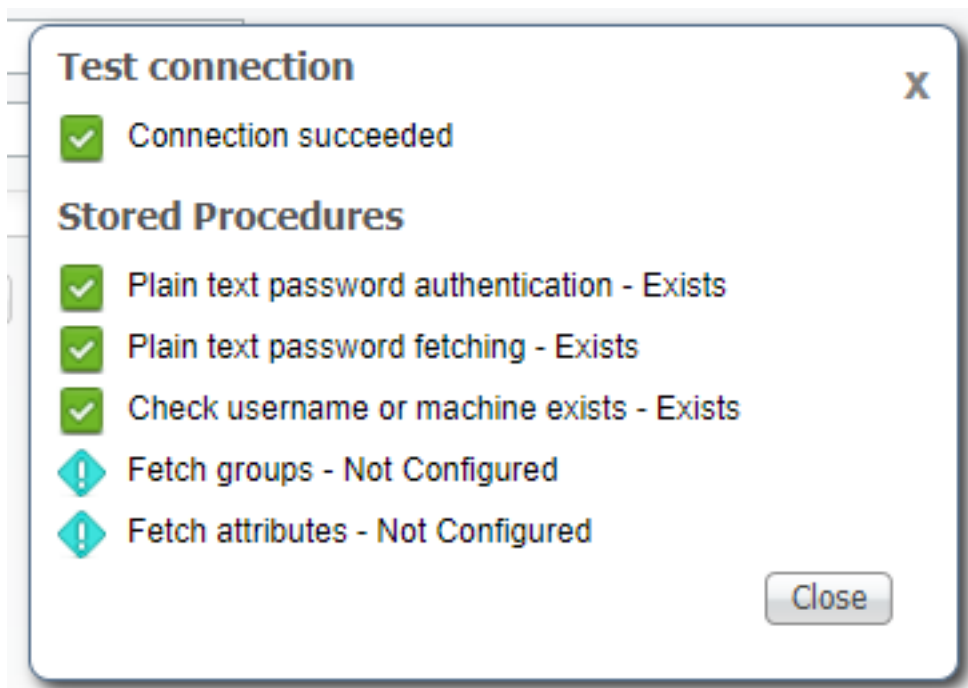
```
create or replace function ISELOOKUP_R  
(  
    ise_username IN VARCHAR2  
) return sys_refcursor AS  
BEGIN  
    declare  
        c integer;  
        resultSet SYS_REFCURSOR;  
    begin  
        select count(*) into c from USERS where USERS.USERNAME = ise_username;  
        if c > 0 then  
            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. 配置在ISE的程序并且保存

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. 回到Connection选项并且点击测试连接按钮



步骤4.配置组检索

1. 创建用于越来越多的映射的表包含用户组的和别的

```
-----  
-- DDL for Table GROUPS  
-----  
  
CREATE TABLE "ISE"."GROUPS"  
  ("GROUP_ID" NUMBER(*,0) GENERATED ALWAYS AS IDENTITY MINVALUE 1 MAXVALUE  
9999999999999999999999999999999999999999999 INCREMENT BY 1 START WITH 1 CACHE 20 NOORDER NOCYCLE NOKEEP
```

```

NOSCALE ,
"GROUP_NAME" VARCHAR2(255 BYTE),
"DESCRIPTION" CLOB
  ) 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"
LOB ("DESCRIPTION") STORE AS SECUREFILE (
  TABLESPACE "USERS" ENABLE STORAGE IN ROW CHUNK 8192
  NOCACHE LOGGING NOCOMPRESS KEEP_DUPLICATES
  STORAGE(INITIAL 106496 NEXT 1048576 MINEXTENTS 1 MAXEXTENTS 2147483645
  PCTINCREASE 0
  BUFFER_POOL DEFAULT FLASH_CACHE DEFAULT CELL_FLASH_CACHE DEFAULT)) ;

```

```

-----
-- DDL for Table USER_GROUPS_MAPPING
-----

```

```

CREATE TABLE "ISE"."USER_GROUPS_MAPPING"
  ("USER_ID" NUMBER(*,0),
"GROUP_ID" NUMBER(*,0)
  ) 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 GROUPS_PK
-----

```

```

CREATE UNIQUE INDEX "ISE"."GROUPS_PK" ON "ISE"."GROUPS" ("GROUP_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" ;

```

```

-----
-- DDL for Index USER_GROUPS_MAPPING_UK1
-----

```

```

CREATE UNIQUE INDEX "ISE"."USER_GROUPS_MAPPING_UK1" ON "ISE"."USER_GROUPS_MAPPING" ("USER_ID",
"GROUP_ID")
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" ;

```

```

-----
-- Constraints for Table GROUPS
-----

```

```

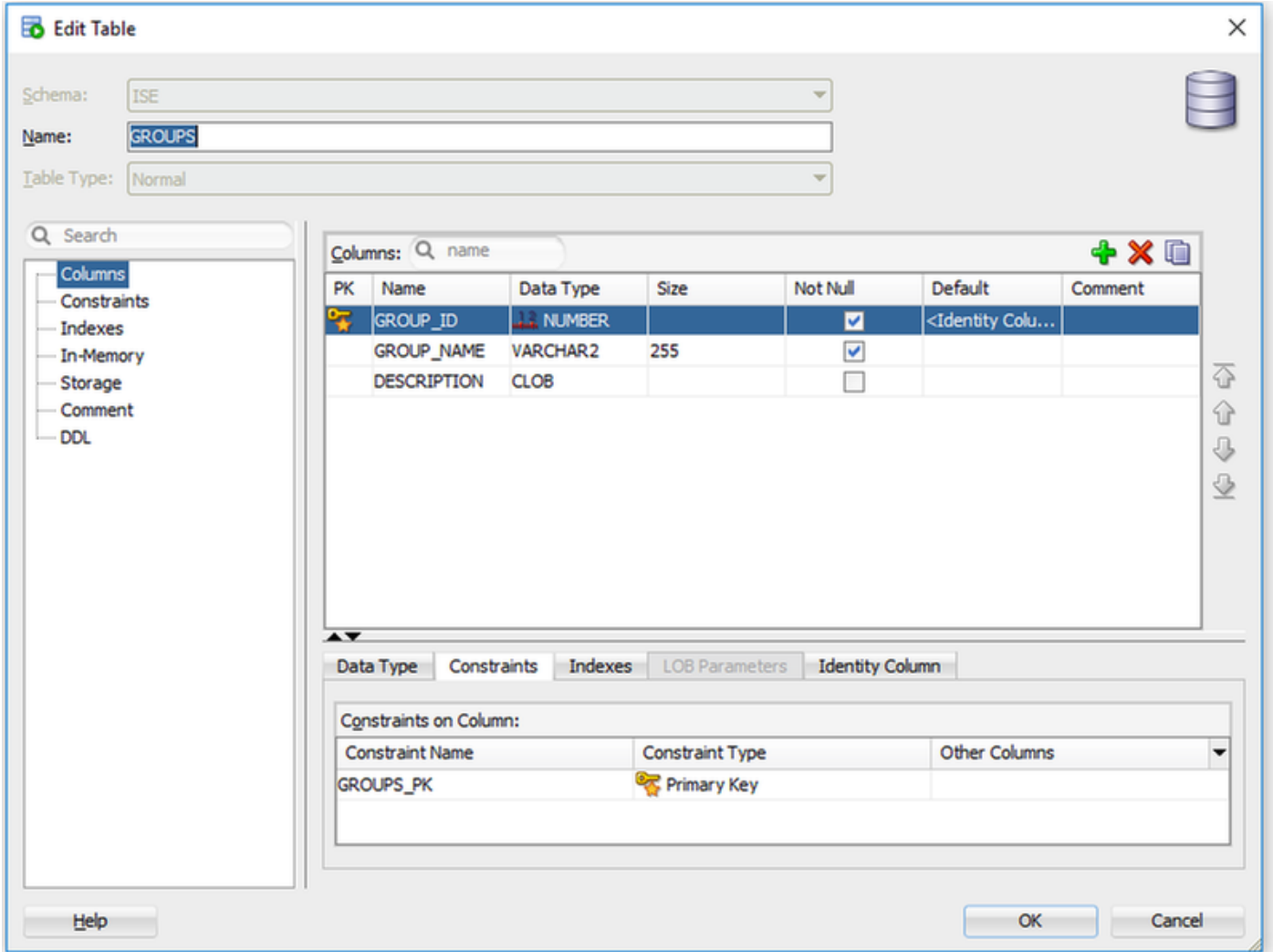
ALTER TABLE "ISE"."GROUPS" MODIFY ("GROUP_ID" NOT NULL ENABLE);
ALTER TABLE "ISE"."GROUPS" MODIFY ("GROUP_NAME" NOT NULL ENABLE);
ALTER TABLE "ISE"."GROUPS" ADD CONSTRAINT "GROUPS_PK" PRIMARY KEY ("GROUP_ID")
USING INDEX PCTFREE 10 INITRANS 2 MAXTRANS 255
STORAGE(INITIAL 65536 NEXT 1048576 MINEXTENTS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

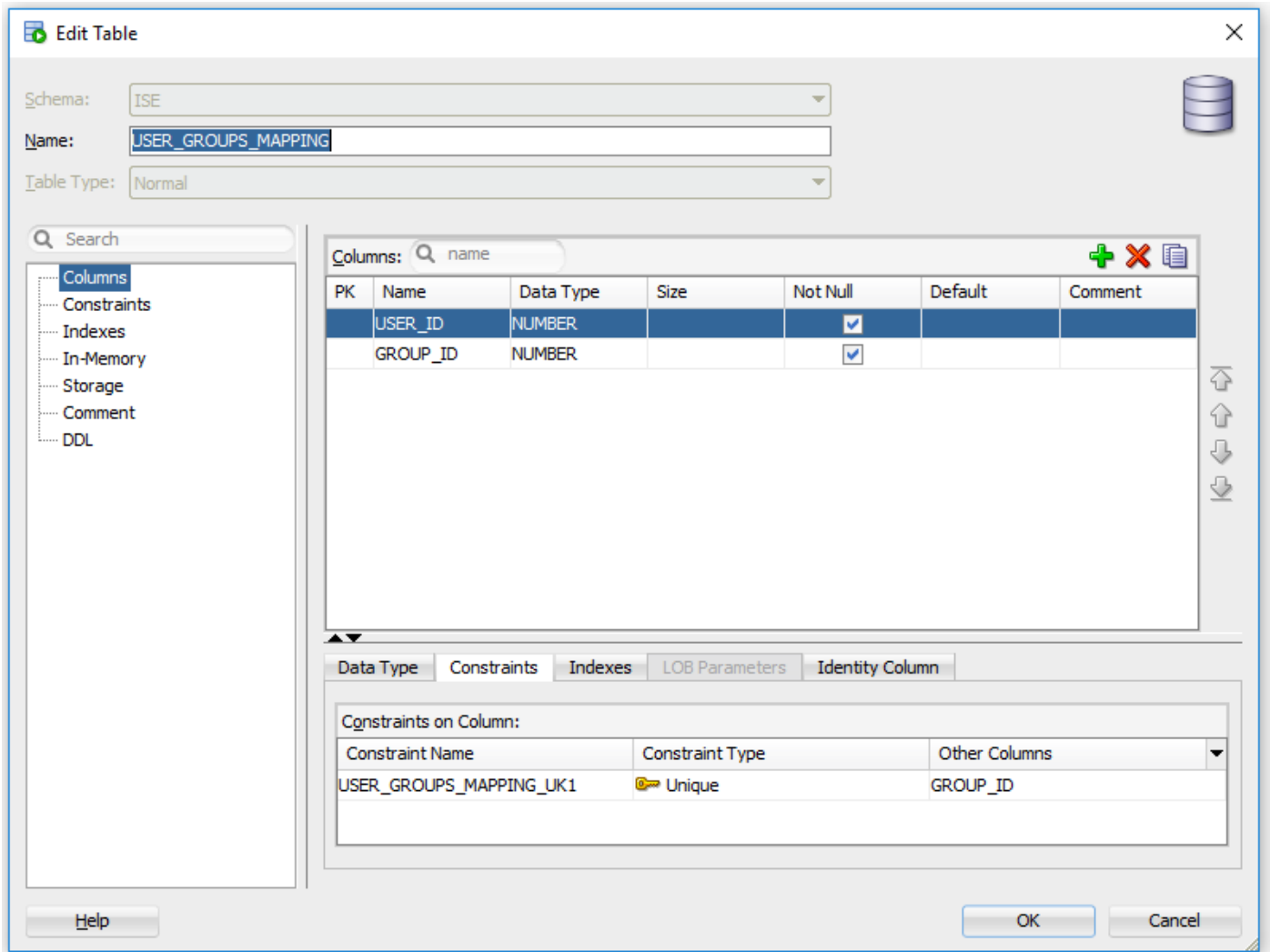
```


-- 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;
```

从GUI :





2. 添加组和映射，因此阿丽斯和突然移动属于组队用户，并且admin属于组队管理员

```
-- 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. 创建一个组检索程序。它返回所有组，如果用户名是“*”

```
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
```

```

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 ;

```

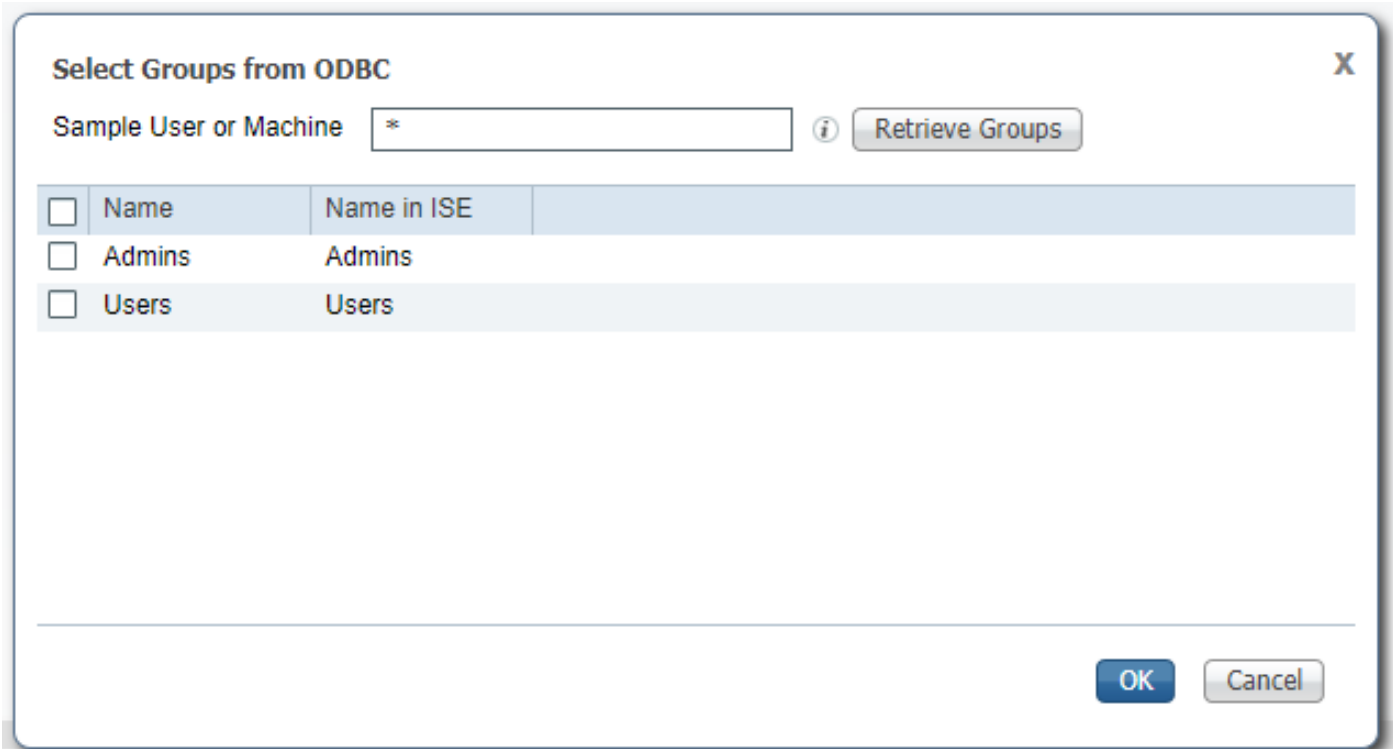
4. 映射它拿来组

[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	

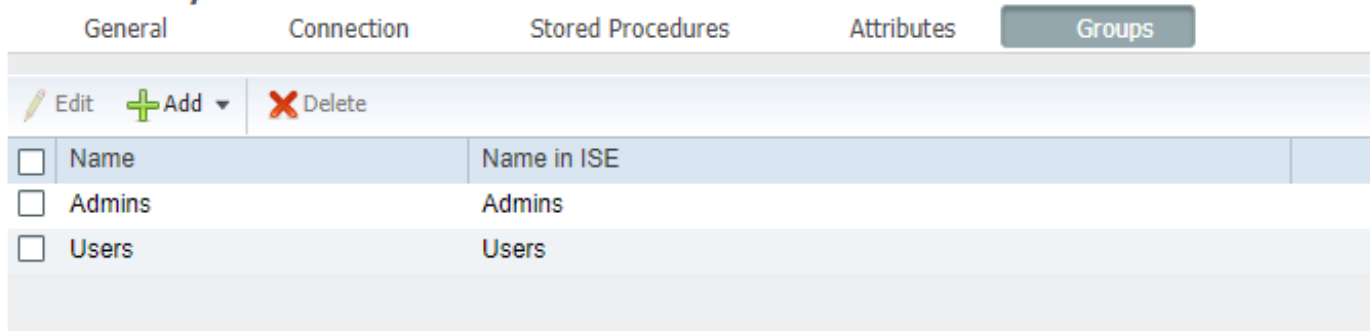
5. 拿来组并且添加他们到ODBC身份来源



select需要组并且点击OK键，他们将出现在组选项

[ODBC List > OracleDB](#)

ODBC Identity Source



步骤5.配置属性检索

1. 为了简化此示例，一张平面的表使用属性

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

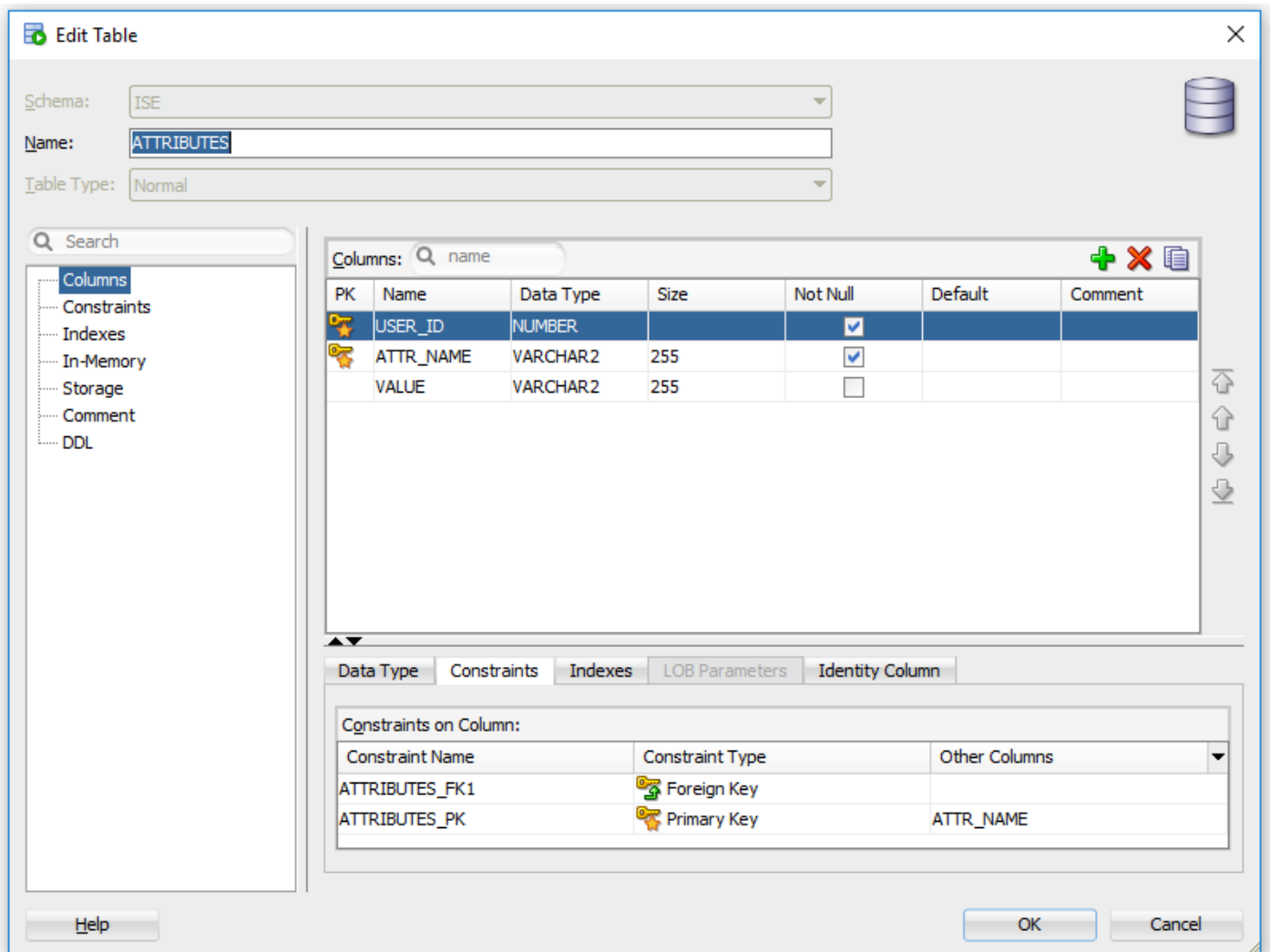
-- DDL for Index ATTRIBUTES_PK

```
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;
```

从GUI :



2. 创建用户的一些属性

```
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. 创建一个程序。同样与组检索，它将返回所有明显的属性，如果用户名是“*”

```
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 ;
```

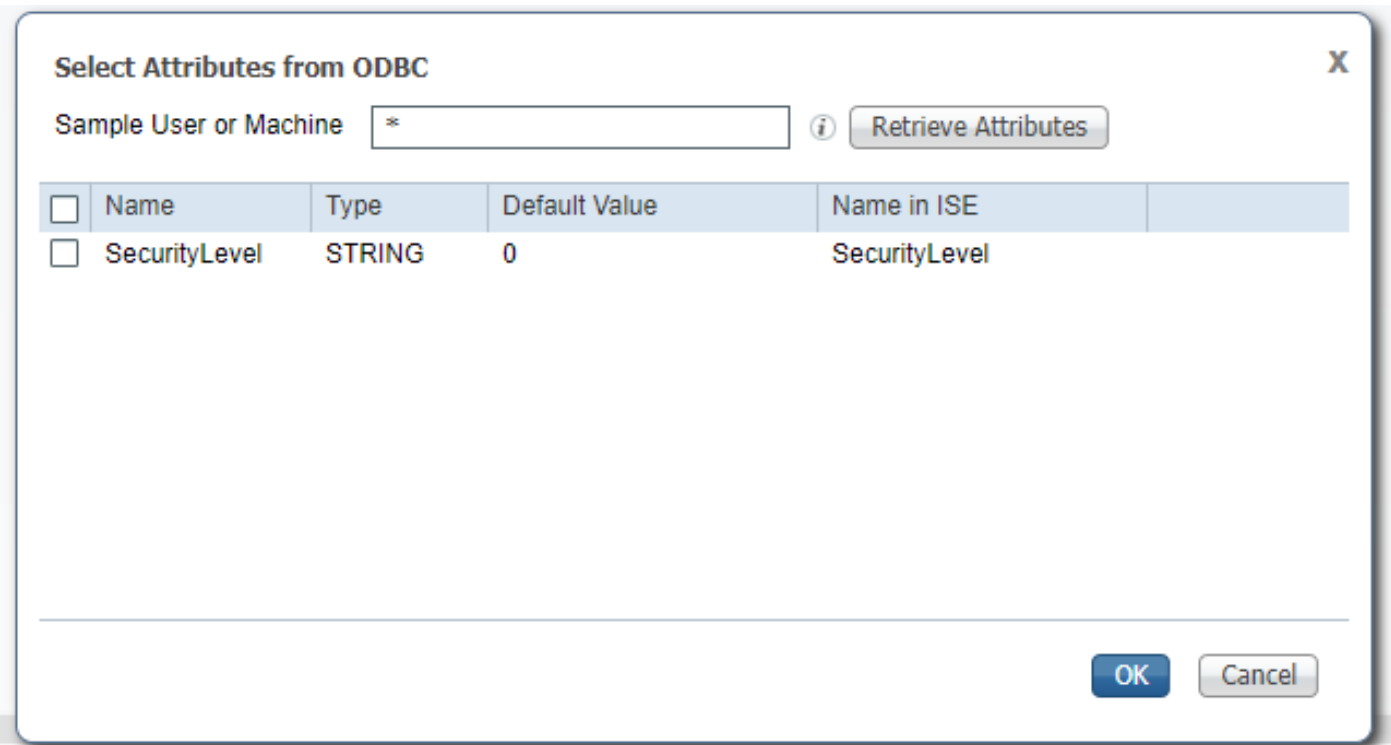
4. 映射它拿来属性

[ODBC List > OracleDB](#)

ODBC Identity Source

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

5. 拿来属性



选择属性并且点击OK键。

步骤6.配置认证/授权策略

在本例中配置了以下简单的授权策略：

<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	⚙

有SecurityLevel的用户= 5将被拒绝。

步骤7.添加Oracle ODBC到身份来源顺序

连接对Administration > 身份管理 > 身份来源顺序，选择您的顺序并且添加ODBC到顺序：

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

保存它。

验证

您应该当前能利用ODBC现在验证用户和检索他们的组和属性。

RADIUS实际日志

进行一些认证并且连接对操作> RADIUS>实际日志

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

正如你看到的用户阿丽斯有SecurityLevel = 5，因此访问被拒绝了。

详细资料报表

点击在Details列的详细资料报表有趣会话的检查流。

用户的阿丽斯(被拒绝的由于详细资料报表低SecurityLevel)：

