Configurer ODBC sur ISE 2.3 avec Oracle Database

Contenu

Introduction Conditions préalables **Conditions requises Components Used** Configuration Étape 1. Configuration de base Oracle Étape 2. Configuration de base d'ISE Étape 3. Configurer l'authentification utilisateur Étape 4. Configurer la récupération de groupe Étape 5. Configurer la récupération des attributs Étape 6. Configurer les stratégies d'authentification/d'autorisation Étape 7. Ajouter Oracle ODBC aux séquences de source d'identité Vérification Journaux dynamiques RADIUS Rapport détaillé Dépannage Les informations d'identification incorrectes sont utilisées Nom de base de données incorrect (nom du service) Dépannage des authentifications des utilisateurs **Références**

Introduction

Ce document décrit comment configurer Identity Services Engine (ISE) avec l'authentification Oracle Database for ISE à l'aide d'Open Database Connectivity (ODBC).

L'authentification ODBC (Open Database Connectivity) nécessite ISE pour pouvoir récupérer un mot de passe utilisateur en texte clair. Le mot de passe peut être chiffré dans la base de données, mais doit être déchiffré par la procédure stockée.

Conditions préalables

Conditions requises

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Cisco Identity Services Engine 2.3
- Concepts de base de données et ODBC
- Oracle

Components Used

Les informations contenues dans ce document sont basées sur les versions de matériel et de logiciel suivantes :

- Identity Services Engine 2.3.0.298
- Centos 7
- Base de données Oracle 12.2.0.1.0
- Oracle SQL Developer 4.1.5

Configuration

Note: Considérez les procédures SQL présentées dans ce document comme des exemples. Il ne s'agit pas d'une méthode officielle et recommandée de configuration d'Oracle DB. Assurez-vous que vous comprenez le résultat et l'impact de chaque requête SQL que vous validez.

Étape 1. Configuration de base Oracle

Dans cet exemple, Oracle a été configuré avec les paramètres suivants :

- Nom de la base de données : ORCL
- Nom du service : orcl.vkumov.local
- Port : 1521 (default)
- Compte créé pour ISE avec le nom d'utilisateur ise

Configurez votre base de données Oracle avant de poursuivre.

Étape 2. Configuration de base d'ISE

Créez une source d'identité ODBC à *Administration > Source d'identité externe > ODBC* et testez la connexion :

ODBC List > OracleDB

General	Irce Connection	Stored Procedures	Attributes	Groups
ODBC DB connectio	n details			
* Hostname/IP[:pd	ort] 10.48.26.61			
* Database nar	ne orcl.vkumov.local			
Admin usernar	ne ise	(i)		
Admin passwo	ord •••••			
* Timeo	out 5	Test connection		, j
* Retri	es 1	Connection succ	eeded	^
* Database ty	pe Oracle	Stored Procedur	es	I
	Test Connection	 Plain text passw Plain text passw Plain text passw Check username Fetch groups - N Fetch attributes 	ord authentication - N ord fetching - Not Cor e or machine exists - I lot Configured - Not Configured	lot Configured nfigured Not Configured Close

Note: ISE se connecte à Oracle à l'aide du nom de service. Par conséquent, le champ [nom de base de données] doit être rempli avec le nom de service qui existe dans Oracle, et non avec le nom SID (ou le nom de base de données). En raison du bogue <u>CSCvf06497</u> points (.) ne peut pas être utilisé dans le champ [Nom de la base de données]. Ce bogue est corrigé dans ISE 2.3.

Étape 3. Configurer l'authentification utilisateur

L'authentification ISE vers ODBC utilise des procédures stockées. Il est possible de sélectionner le type de procédures. Dans cet exemple, nous utilisons des jeux d'enregistrements comme retour.

Pour d'autres procédures, reportez-vous au <u>Guide d'administration de Cisco Identity Services</u> Engine, version 2.3

Astuce : Il est possible de renvoyer des paramètres nommés au lieu de resultSet. C'est juste un type de sortie différent, la fonctionnalité est la même.

1. Créez la table avec les informations d'identification des utilisateurs. Assurez-vous de définir les paramètres d'identité sur la **clé primaire.**

```
_____
-- DDL for Table USERS
_____
 CREATE TABLE "ISE". "USERS"
  ("USER_ID" NUMBER(*,0) GENERATED ALWAYS AS IDENTITY MINVALUE 1 MAXVALUE
NOSCALE ,
"USERNAME" VARCHAR2(120 BYTE),
"PASSWORD" VARCHAR2(120 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 USERS_PK
_____
 CREATE UNIQUE INDEX "ISE"."USERS_PK" ON "ISE"."USERS" ("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 USERS
_____
 ALTER TABLE "ISE"."USERS" MODIFY ("USER_ID" NOT NULL ENABLE);
 ALTER TABLE "ISE"."USERS" MODIFY ("USERNAME" NOT NULL ENABLE);
 ALTER TABLE "ISE"."USERS" MODIFY ("PASSWORD" NOT NULL ENABLE);
 ALTER TABLE "ISE"."USERS" ADD CONSTRAINT "USERS_PK" PRIMARY KEY ("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;
```

Ou à partir de l'interface graphique de SQL Developer :

🐻 Create Tab	le							×
<u>S</u> chema: I <u>N</u> ame: U Table Type: N	SE SERS Iormal				• 			✓ Advanced
Q Search		<u>C</u> olu	mns: Q name)				+ × 🗈
Columns		PK	Name	Data Type	Size	Not Null	Default	Comment
Todeves	s	8	USER_ID	12 INT		Image: A start of the start	<identity colu<="" td=""><td></td></identity>	
Indexes	,		USERNAME	VARCHAR2	120	~		
Storage			PASSWORD	VARCHAR2	120	~		$\overline{\mathbf{O}}$
DDL		Dat	a Type Constr	aints Indexes	LOB Parameter	s Identity Co	olumn	
		⊙ s C <u>o</u> lu	Simple Comp	olex <u>V</u> irtual		•		
		Si <u>z</u> e	: 120] <u>u</u>	nits: <pre></pre>	d>
Help							ОК	Cancel

2. Ajouter des utilisateurs

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. Créer une procédure pour l'authentification par mot de passe en texte brut (utilisée pour PAP, méthode interne EAP-GTC, 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;
```

4. Créer une procédure pour l'extraction du mot de passe en texte brut (utilisée pour CHAP, MSCHAPv1/v2, EAP-MD5, LEAP, méthode interne EAP-MSCHAPv2, 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. Créer une procédure pour vérifier qu'il existe un nom d'utilisateur ou une machine (utilisée pour MAB, reconnexion rapide de PEAP, EAP-FAST et 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. Configurer les procédures sur ISE et enregistrer

ODBC List > OracleDB

ODBC Identity Source

	General	Connection	Stored Procedures	Attributes	Groups
	Store	d procedure type	Returns recordset	-	
P	lain text passwo	ord authentication	ISEAUTH_R	i	\oplus
	Plain text p	assword fetching	ISEFETCH_R	(j.	\oplus
Ch	eck username	or machine exists	ISELOOKUP_R	(i)	\oplus
		Fetch groups		(i)	\oplus
		Fetch attributes		<i>i</i>	\oplus
8	Search for MAC	Address in format	XX-XX-XX-XX-XX-XX	• (j)	

7. Revenir à l'onglet Connexion et cliquer sur le bouton Tester la connexion



Étape 4. Configurer la récupération de groupe

1. Créer des tables contenant des groupes d'utilisateurs et d'autres tables utilisées pour le mappage de plusieurs à plusieurs

-- DDL for Table GROUPS CREATE TABLE "ISE"."GROUPS" ("GROUP_ID" NUMBER(*,0) GENERATED ALWAYS AS IDENTITY MINVALUE 1 MAXVALUE 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;

Àpartir de l'interface utilisateur graphique :

🔂 Edit Table								×
Schema: ISE Name: GROUPS Table Type: Normal					▼ 			
Q Search	Colu	mns: Q name)				4 X	
Columns	PK	Name	Data Type	Size	Not Null	Default	Comment	-
- Indexes	*	GROUP_ID	12 NUMBER		✓	<identity colu<="" td=""><td></td><td></td></identity>		
- In-Memory	_	GROUP_NAME	VARCHAR2	255	Image: A start of the start			
- Storage		DESCRIPTION	CLOB					
	Dat Cor	a Type Constr Instraints on Colum	aints Indexes	LOB Para	ameters Identity Co	umn		
	Co	nstraint Name		Constraint	Туре	Other Columns		-
	GRO	DUPS_PK		😽 Primary	Key			
Help						ОК	c	ancel

🔂 Edit Table								×
Schema: ISE Name: USER_GROUPS_MAPPIN Table Type: Normal	G				•			
Q Search	<u>C</u> olu	mns: Q name					+ ×	
Columns	PK	Name	Data Type	Size	Not Null	Default	Comment	
Indexes		USER_ID	NUMBER		Image:			
In-Memory		GROUP_ID	NUMBER		~			_
Comment DDL	Dat	a Type Constra	aints Indexe	LOB Paran	neters Identity Co	umn		
	Co	nstraints on Colum	n:					
	Co	nstraint Name		Constraint Ty	/pe	Other Columns		-
	USE	R_GROUPS_MAPP	PING_UK1	Omique 🕬		GROUP_ID		
Help						ОК		Cancel

2. Ajoutez des groupes et des mappages de sorte que **alice** et **bob** appartiennent au groupe **Utilisateurs** et administrateur appartiennent au groupe **Administrateurs**

-- 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. Créez une procédure de récupération de groupe. Il renvoie tous les groupes si le nom d'utilisateur est "* "

```
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. Mapper à des groupes de récupération

ODBC List > OracleDB

ODBC Identity Source

General	Connection	Stored Procedures	Attributes	Groups
Sto	ored procedure type	Returns recordset	*	
Plain text pass	word authentication	ISEAUTH_R	<i>i</i>	\oplus
Plain tex	t password fetching	ISEFETCH_R	<i>i</i>	\oplus
Check usernam	e or machine exists	ISELOOKUP_R	()	\oplus
	Fetch groups	ISEGROUPSH	<i>i</i>	Ð
	Fetch attributes			\oplus
Search for MA	AC Address in format	XX-XX-XX-XX-XX-XX	• (i)	

5. Récupérer les groupes et les ajouter à la source d'identité ODBC

Select Groups from ODBC							
Sample User or Mach	ine * (i) Retrieve Groups						
Name	Name in ISE						
Admins	Admins						
Users	Users						
	OK Cancel						

Sélectionnez les groupes requis et cliquez sur OK. Ils s'afficheront dans l'onglet Groupes.

ODBC List > OracleDB	ODBC List > OracleDB									
ODBC Identity Source										
General	Connection	Stored Procedures	Attributes	Groups						
🖉 Edit 🕂 Add 👻 🏅	🗙 Delete									
Name		Name in ISE								
Admins		Admins								
Users		Users								

Étape 5. Configurer la récupération des attributs

1. Afin de simplifier cet exemple, une table plate est utilisée pour les attributs

```
-- 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;

Àpartir de l'interface utilisateur graphique :

🔂 Edit Table								×
Schema: ISE Name: ATTRIBUTES					•			
Table Type: Normal					-			
Q Search	Columns	, Q name						<u>a</u>
Columns	PK N	lame	Data Type	Size	Not Null	Default	Comment	
Indexes	🏆 US	ER_ID	NUMBER		V			
In-Memory	😽 AT	TR_NAME	VARCHAR2	255	~			
Storage	VA	LUE	VARCHAR2	255				
	Data Ty	ype Constra	aints Indexes	LOB Parameters	Identity Colu	ımn		2
	Constra	aints on Colum	n:					
	Constr	raint Name		Constraint Type		Other Columns		-
	ATTRIB	UTES_FK1		🚰 Foreign Key				
	ATTRIB	BUTES_PK		🏹 Primary Key		ATTR_NAME		
Help						ОК	Ca	ancel

2. Créer des attributs pour les utilisateurs

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. Créez une procédure. Comme avec la récupération de groupes, il retournera tous les attributs distincts si le nom d'utilisateur est "* "

```
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 TF;
    return resultSet;
  end;
END ;
```

4. Mapper les attributs de récupération

ODBC List > OracleDB

ODBC Identity Source

General	Connection	Stored Procedures	Attribu	tes		Groups
Stor	ed procedure type	Returns recordset	•			
Plain text passw	ord authentication	ISEAUTH_R		i	\oplus	
Plain text	password fetching	ISEFETCH_R			\oplus	
Check username	or machine exists	ISELOOKUP_R		i	\oplus	
-	Eatab groups			1	-	
	Fetch groups	ISEGROUPSH				
	Fetch attributes	ISEATTRSH		i	\oplus	
Search for MAC	C Address in format	XX-XX-XX-XX-XX-XX		• •		

5. Récupérer les attributs

Select Attributes f	rom ODBC			x
Sample User or Mac	hine *		(i) Retrieve Attributes	
Name	Туре	Default Value	Name in ISE	
SecurityLevel	STRING	0	SecurityLevel	
			ОК Са	ncel

Sélectionnez les attributs et cliquez sur OK.

Étape 6. Configurer les stratégies d'authentification/d'autorisation

Dans cet exemple, les stratégies d'autorisation simples suivantes ont été configurées :

\odot	Allow admin network access	4	OracleDB ExternalGroups EQUALS Admins	× PermitAccess	+	Select from list	- +	1	٥
Ø	SecurityLevel too low	£;	OracleDB SecurityLevel EQUALS 5	EnyAccess	+	Select from list	• +	0	٥
\odot	Allow users network access	40	OracleDB ExternalGroups EQUALS Users	× PermitAccess	+	Select from list	· +	2	٥

Les utilisateurs avec **SecurityLevel = 5** seront refusés.

Étape 7. Ajouter Oracle ODBC aux séquences de source d'identité

Accédez à *Administration > Identity Management > Identity Source Sequences,* sélectionnez votre séquence et ajoutez ODBC à la séquence :

Identity Source Sequences List > All_User_ID_Stores

Identity Source Sequence

Identity Source Sequence

* Name All_User_ID_Stores
Description A built-in Identity Sequence to include all User Identity Stores

Certificate Based Authentication

Select Certificate Authentication Profile Preloaded_Certificate_P 💌

Authentication Search List

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

Available

Selected

Internal Endpoints		> <	Internal Users All_AD_Join_Points Guest Users OracleDB		⊼ ∧
	÷	» «		+	✓✓

Advanced Search List Settings

If a selected identity store cannot be accessed for authentication

- O 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



Enregistrez-le.

Vérification

Vous devriez maintenant être en mesure d'authentifier les utilisateurs par rapport à ODBC et de récupérer leurs groupes et attributs.

Journaux dynamiques RADIUS

Effectuez certaines authentifications et accédez à Operations > RADIUS > Live Logs

	Time	Status	Details	Repeat	Identity	Endpoint ID	Endpoint P	Authenticat	Authorizati	Authorizati	IP Address		Network Device
×		٠			Identity	Endpoint ID	Endpoint Prof	Authentication	Authorization	Authorization	IP Address	٠	Network Device
	Aug 08, 2017 04:31:32.545 PM	٥	0		badUser	92:77:F1:E4:D2:53		Default >> D	Default				SWITCH
	Aug 08, 2017 04:31:32.465 PM	0	0	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	S	0		admin	61:AD:77:0F:DF:CF		Default >> D	Default >> A	PermitAccess			SWITCH
	Aug 08, 2017 04:31:32.365 PM	0	0	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	S	0		bob	FC:F4:97:F2:F5:4F		Default >> D	Default >> A	PermitAccess			SWITCH
	Aug 08, 2017 04:31:32.237 PM	٥	Q		alice	42:27:B1:C6:F9:A4		Default >> D	Default >> S	DenyAccess			SWITCH

Comme vous pouvez le voir, l'utilisateur Alice a **SecurityLevel = 5,** d'où le rejet de l'accès.

Rapport détaillé

Cliquez sur **Rapport détaillé** dans la colonne **Détails** pour la session intéressante afin de vérifier le flux.

Rapport détaillé pour l'utilisateur Alice (rejeté en raison d'un niveau de sécurité faible) :