-- create users that will illustrate row access

use role useradmin;

create or replace user USER\_A password='abc123'

default\_role = SYSADMIN

must\_change\_password = TRUE;

create or replace user USER\_B password='abc123'

default\_role = SYSADMIN

must\_change\_password = TRUE;

use role securityadmin;

grant role sysadmin to user USER\_A;

grant role sysadmin to user USER\_B;

grant role accountadmin to user USER\_A;

grant role accountadmin to user USER\_B;

-- create example tables and populate with data

use role sysadmin;

use schema usecase\_Db.usecase\_schema;

create or replace table aba\_doctor(name varchar(100) primary key, username varchar(100));

create or replace table aba\_patient(name varchar(100) primary key, telephone varchar(20));

create or replace table aba\_patient\_record(record\_id number(10,0) primary key,

patient\_name varchar(100), record\_date date, record\_text varchar(1000));

create or replace table aba\_doctor\_patient(doctor\_name varchar(100), patient\_name varchar(100));

USE WAREHOUSE DKWHXS;

insert into aba\_doctor(name, username) values ('Chris','USER\_B'), ('Angela', 'USER\_A');

select \* from aba\_doctor;

insert into aba\_patient(telephone, name) values ('123-456-789', 'David'),

('123-456-789', 'Darla'), ('123-456-789', 'Dorris'),

('123-456-789', 'Daniel'), ('123-456-789', 'Dorothy'), ('123-456-789', 'Devon'), ('123-456-789', 'Darius');

select \* from aba\_patient;

insert into aba\_patient\_record(record\_id, patient\_name, record\_date, record\_text)

values(1, 'David', to\_date('1/1/2022', 'MM/DD/YYYY'), 'record text 1'),

(2, 'David', to\_date('1/1/2022', 'MM/DD/YYYY'), 'record text 2'),

(3, 'Daniel', to\_date('1/2/2022', 'MM/DD/YYYY'), 'record text 3'),

(4, 'Dorris', to\_date('1/3/2022', 'MM/DD/YYYY'), 'record text 4'),

(5, 'Devon', to\_date('1/4/2022', 'MM/DD/YYYY'), 'record text 5'),

(6, 'Darius', to\_date('1/5/2022', 'MM/DD/YYYY'), 'record text 6'),

(7, 'Darla', to\_date('1/6/2022', 'MM/DD/YYYY'), 'record text 7'),

(8, 'Darla', to\_date('1/7/2022', 'MM/DD/YYYY'), 'record text 8'),

(9, 'Dorothy', to\_date('1/8/2022', 'MM/DD/YYYY'), 'record text 9'),

(10, 'Dorothy', to\_date('1/9/2022', 'MM/DD/YYYY'), 'record text 10'),

(11, 'David', to\_date('1/9/2022', 'MM/DD/YYYY'), 'record text 11');

select \* From aba\_patient\_record;

insert into aba\_doctor\_patient(doctor\_name, patient\_name)

values('Chris', 'David'),('Chris', 'Daniel'),('Angela', 'Dorris'),('Chris', 'Devon'),

('Chris', 'Darius'),('Angela', 'Darla'),('Angela', 'Dorothy');

select \* from aba\_doctor\_patient

ORDER BY DOCTOR\_NAME;

-- create integrated view over doctors, patients and records

/\*use role accountadmin;

drop view aba\_doctor\_patient\_record\_dv;

use role sysadmin;

\*/

create or replace view aba\_doctor\_patient\_record\_dv as

select

d.name doctor\_name,

d.username username,

p.name patient\_name,

p.telephone patient\_phone,

pr.record\_date,

pr.record\_text

from

aba\_doctor d,

aba\_patient p,

aba\_patient\_record pr,

aba\_doctor\_patient dp

where

d.name = dp.doctor\_name

and p.name = dp.patient\_name

and pr.patient\_name = p.name

order by pr.record\_date, pr.patient\_name

;

select \* from aba\_doctor\_patient\_record\_dv

ORDER BY DOCTOR\_NAME;

select \* from aba\_doctor;

select \* from aba\_patient;

USE ROLE ACCOUNTADMIN;

select \* from aba\_patient\_record;

select \* from aba\_doctor\_patient

ORDER BY DOCTOR\_NAME;

select \* from aba\_doctor\_patient\_record\_dv

order by doctor\_name;

USE ROLE ACCOUNTADMIN;

DROP row access policy aba\_doc\_patient\_policy;

USE ROLE SYSADMIN;

-- create row access policy that tests a patient name against entries in the aba\_doctor\_patient table

create or replace row access policy aba\_doc\_patient\_policy as (v\_patient varchar(100)) returns boolean ->

current\_role() = 'ACCOUNTADMIN'

or

exists (

select 1 from aba\_doctor\_patient dp, aba\_doctor d

where dp.doctor\_name = d.name

and d.username = current\_user()

and dp.patient\_name = v\_patient

)

;

select \* from aba\_doctor\_patient dp, aba\_doctor d

where dp.doctor\_name = d.name

ORDER BY USERNAME;

--and d.username = current\_user()

--and dp.patient\_name = v\_patient;

-- apply that policy to the aba\_patient\_record table

alter table aba\_patient\_record add row access policy aba\_doc\_patient\_policy on (patient\_name);

-- Test the policy for ACCOUTADMIN role

use role ACCOUNTADMIN;

select \* from aba\_patient\_record;

-- test that the policy works with the view that references the aba\_patient\_record table

-- policy is checked for any access to the table regardless of query source

select \* from aba\_doctor\_patient\_record\_dv;

-- Test the policy for SYSADMIN role

use role sysadmin;

select \* from aba\_patient\_record;

-- test that the policy works with the view that references the aba\_patient\_record table

-- policy is checked for any access to the table regardless of query source

select \* from aba\_doctor\_patient\_record\_dv;

-- log in as USER\_B - should show only male patients assigned to Chris

use role sysadmin;

select \* from aba\_patient\_record;

-- test that the "admin" switch works in the policy

use role accountadmin;

select \* from aba\_doctor\_patient\_record\_dv;

-- login as USER\_A and check

use role sysadmin;

select \* from aba\_doctor\_patient\_record\_dv;

-- switch doctor for Patient Dorothy

select \* from aba\_doctor\_patient

where patient\_name = 'Dorothy';

update aba\_doctor\_patient set doctor\_name = 'Chris' where patient\_name = 'Dorothy';

-- Chris should now be able to see Dorothy's record

USE ROLE ACCOUNTADMIN;

select \* from aba\_doctor\_patient\_record\_dv

order by doctor\_name,patient\_name;