

## Implementing Role Level Security in OBIEE

By

Artur Bakhtriger

&

Kris Vadlamudi

## Authentication Options

**Authentication** is the process by which a system uses a user ID and password to verify that a user has the necessary permissions

**Authorization** on the other hand allows us to control what data user sees

The Oracle BI Server authenticates each connection request it receives.

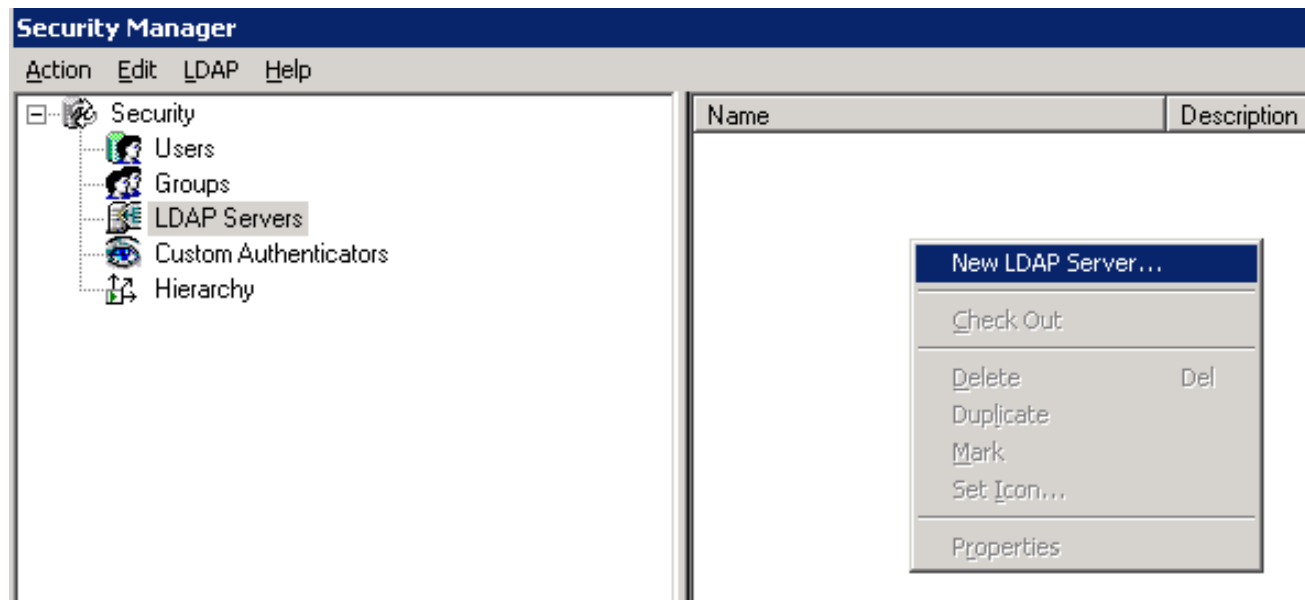
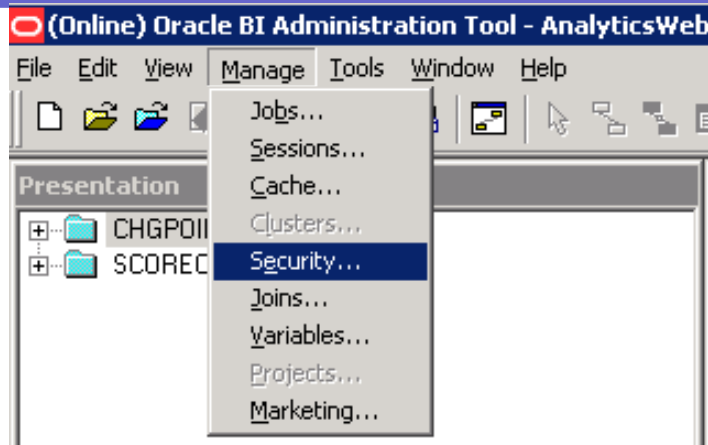
The Oracle BI Server supports the following authentication types:

- **LDAP Authentication**
- External Table Authentication
- Database Authentication
- Repository Authentication

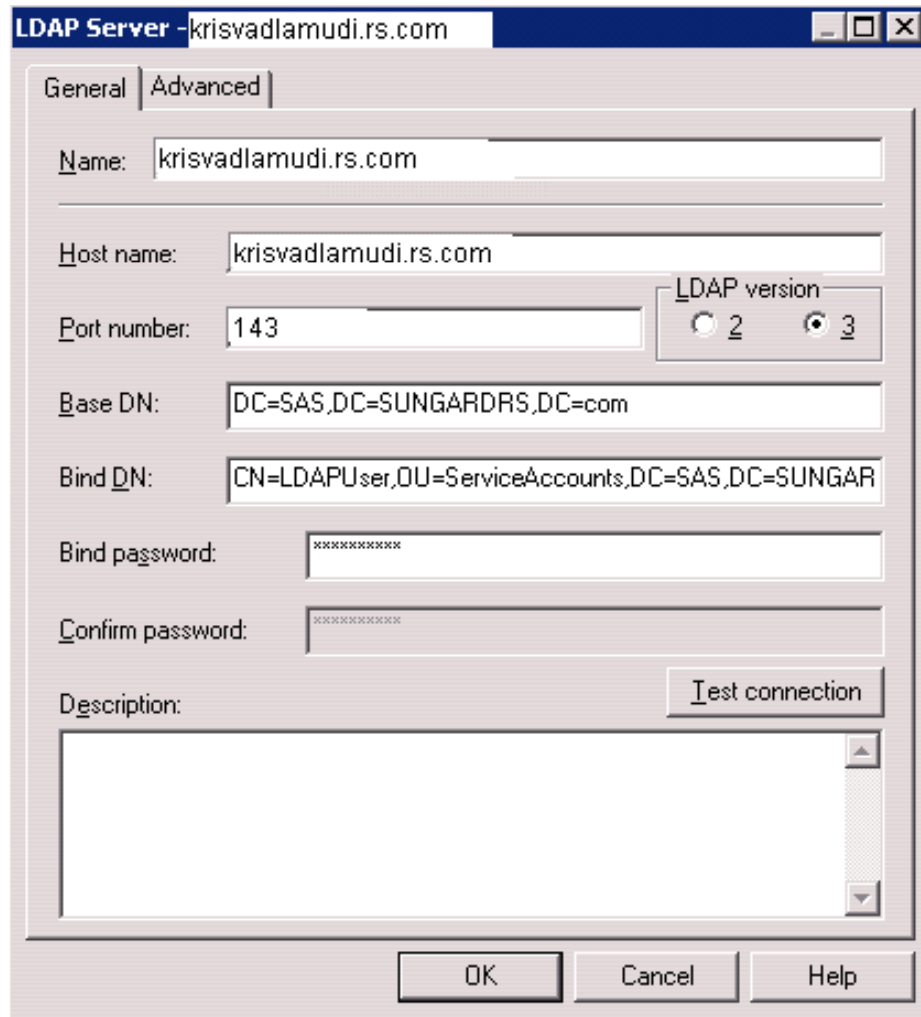
LDAP, Lightweight Directory Access Protocol, is an Internet protocol that email and other programs use to look up information from a server

## Setting up LDAP (*Lightweight Directory Access Protocol*) in OBIEE

In order to configure LDAP server in the Repository we need to register the LDAP server first



## Enter the details of LDAP server



The screenshot shows a dialog box titled "LDAP Server - krisvadlamudi.rs.com". It has two tabs: "General" (selected) and "Advanced". The fields are as follows:

- Name:** krisvadlamudi.rs.com
- Host name:** krisvadlamudi.rs.com
- Port number:** 143
- LDAP version:** Radio buttons for 2 and 3, with 3 selected.
- Base DN:** DC=SAS,DC=SUNGARDRS,DC=com
- Bind DN:** CN=LDAPUser,OU=ServiceAccounts,DC=SAS,DC=SUNGAR
- Bind password:** [masked with asterisks]
- Confirm password:** [masked with asterisks]
- Description:** [empty text area]
- Buttons:** OK, Cancel, Help, and a "Test connection" button.

**Host name.** The name of your LDAP server.

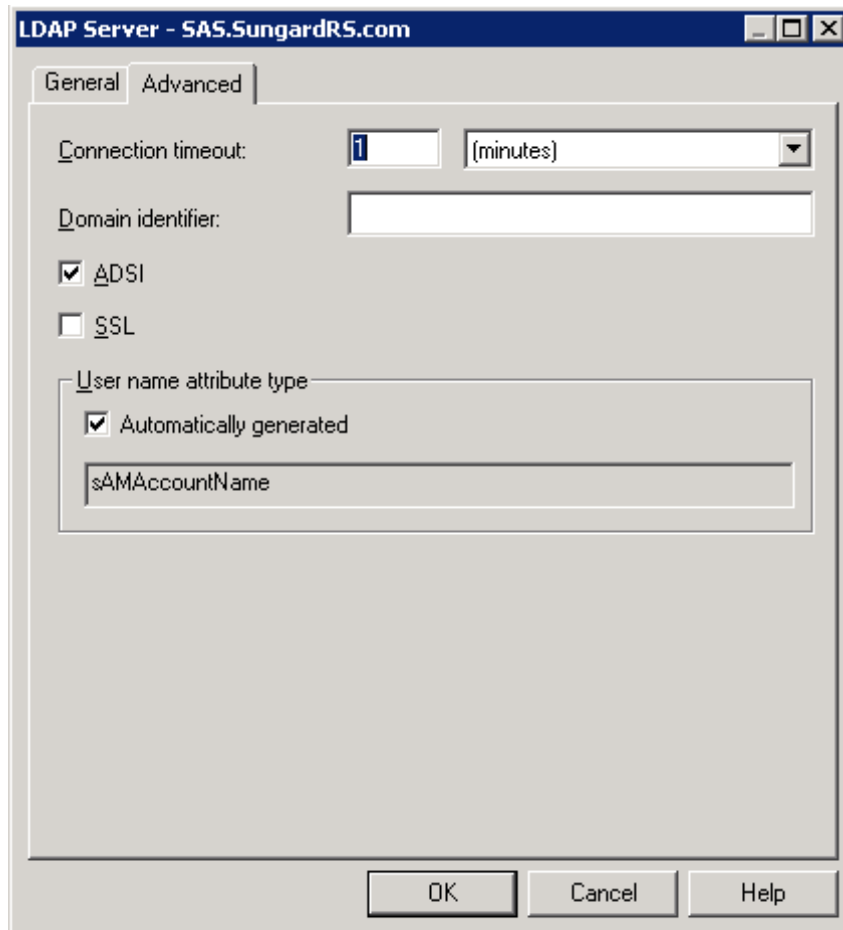
**Port number.** The default LDAP port is 389.

**LDAP version.** LDAP 2 or LDAP 3 (versions).

The default is LDAP 3.

**Base DN.** The base distinguished name (DN) identifies the starting point of the authentication search. For example, if you want to search all of the entries under the o=Oracle.com subtree of the directory, o=Oracle.com is the base DN.

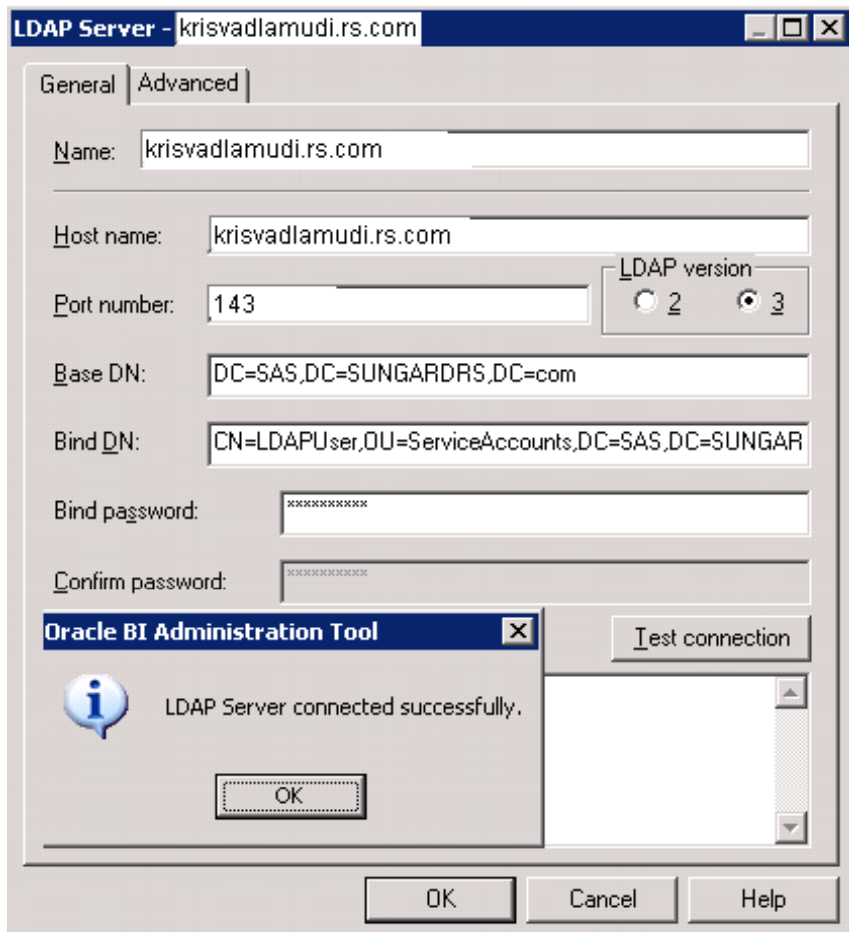
**Bind DN and Bind Password.** The optional DN and its associated user password that are required to bind to the LDAP server.



**Next in the Advanced tab, based on the kind of LDAP server you have and its configuration, make the necessary changes.**

**For Microsoft ADSI (Active Directory Service Interface), choose ADSI and for all others leave it unchecked. Most of the times, Username attribute would be automatically generated. For Microsoft ADSI It is sAMAccountName; for most of the LDAP servers it is uid or cn. Check with your network security group/administrator on what is the username attribute for your LDAP server. Make a note of the user name attribute you will need it later.**

Click the Test Connection to test the connectivity

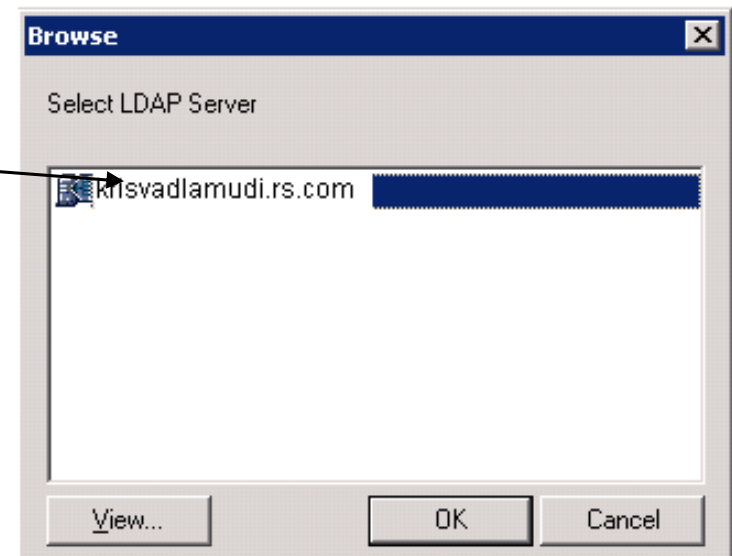
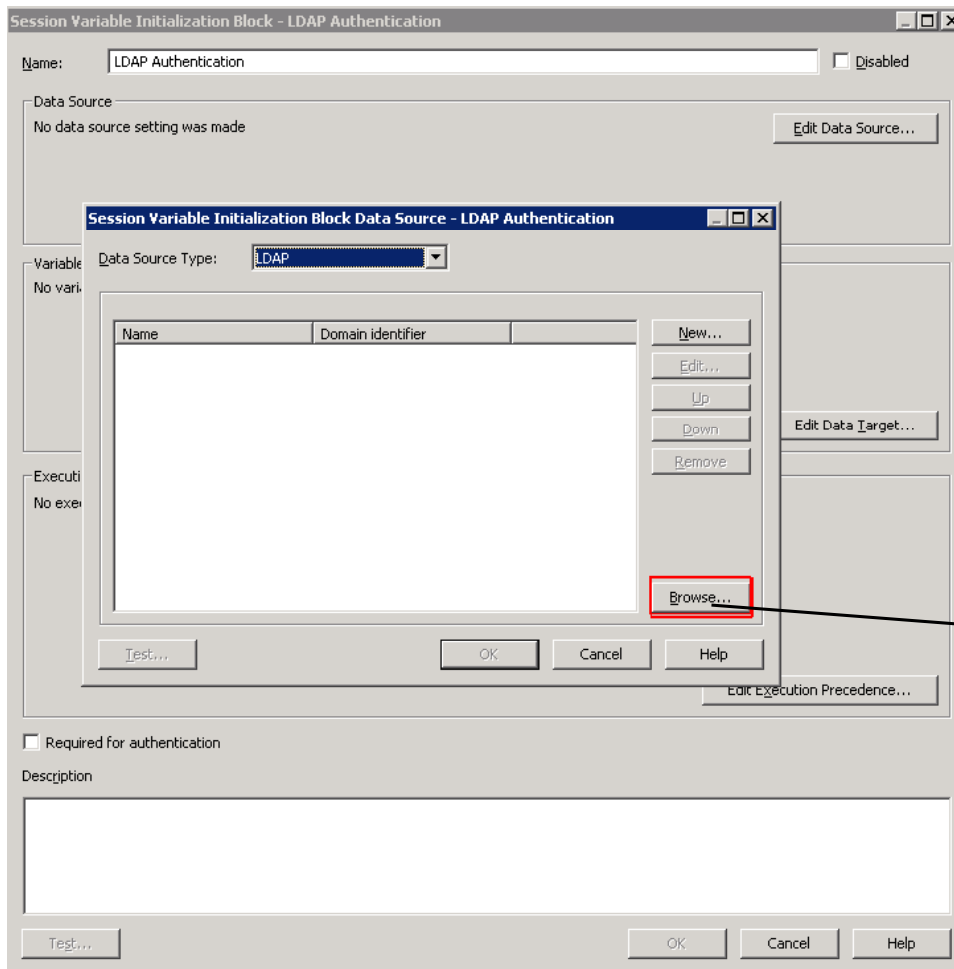


Now we need to create an Init Block for the Authentication

The screenshot displays the Oracle BI Administration Tool interface. The top window, titled "(Online) Oracle BI Administration Tool - AnalyticsWeb", has a menu bar with "File", "Edit", "View", "Manage", "Tools", "Window", and "Help". The "Manage" menu is open, showing options: "Jobs...", "Sessions...", "Cache...", "Clusters...", "Security...", "Joins...", "Variables..." (highlighted), "Projects...", and "Marketing...".

Below the main window is the "Variable Manager" dialog box. It has a menu bar with "Action", "Edit", and "Help". On the left is a tree view showing the hierarchy: "Repository" (expanded) contains "Initialization Blocks" and "Variables" (expanded). "Variables" contains "Dynamic" and "Static". "Session" (expanded) contains "Initialization Blocks" (highlighted), "Variables" (expanded), "System", "Security", and "Non-System".


The main area of the Variable Manager is a table with two columns: "Name" and "Initialization string". A context menu is open over the table, listing actions: "New Initialization Block..." (highlighted), "Check Out", "Delete" (with "Del" as a shortcut), "Duplicate", "Mark", "Set Icon...", and "Properties".



Session Variable Initialization Block - LDAP Authentication

Name:   Disabled

Data Source Edit Data Source...

Name	Domain identifier
 krisvadlamudi.rs.com	

Variable Target  
No variable target setting was made

**Session Variable Initialization Block Variable Target - LDAP Authenticati...**

Variables

Variable	Default Initializer	LDAP variable
----------	---------------------	---------------

Row-wise initialization  
 Use caching

OK Cancel Help

Edit Data Target...

Execution Precedence...

Cancel Help

**System Session Variable - USER**

Name:

Enable any user to set the value


Security Sensitive

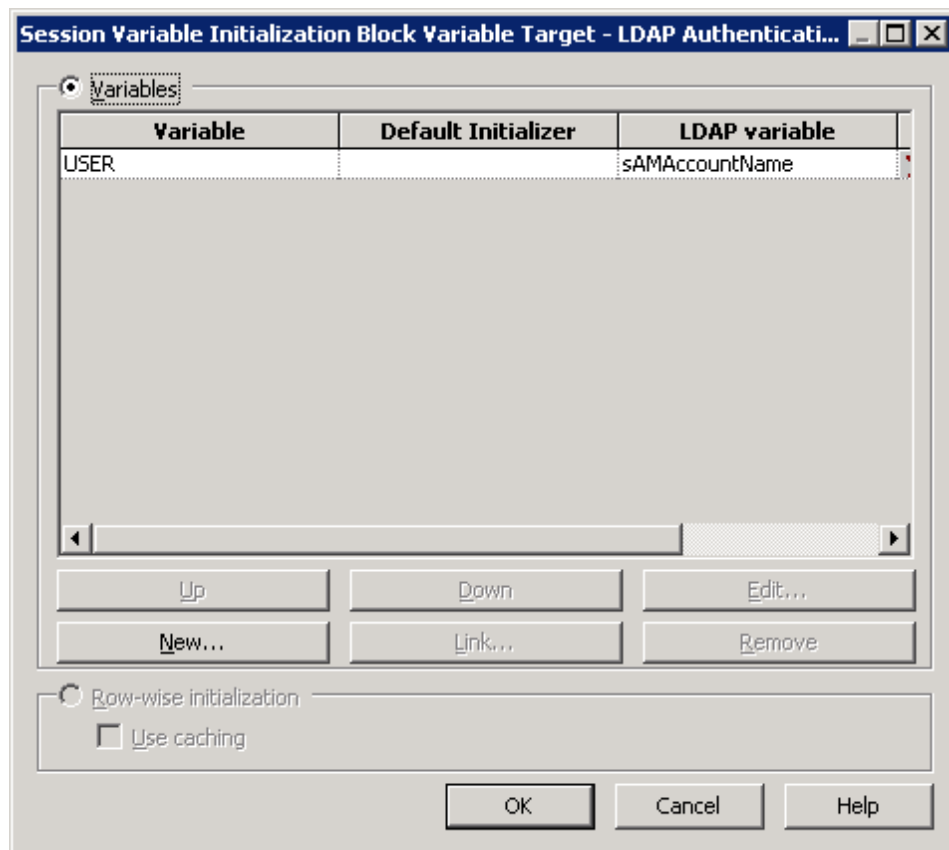
Initialization Block:

Default Initializer:

Description

**Oracle BI Administration Tool**

 USER session variable has a special purpose. Are you sure you want to use this name?




Next enter the LDAP variable for username. sAMAccountName in the case of ADSI as configured in the LDAP.


**Session Variable Initialization Block - LDAP Authentication**

Name:   Disabled

Data Source

Name	Domain identifier
 krisvadamudi.rs.com	

Variable Target

Name	Default Initializer
 USER	

Execution Precedence

No execution precedence setting was made

Required for authentication

Description

## Create a new Init Block for the Group

**Session Variable Initialization Block - Group**

Name:   Disabled

Data Source

Connection Pool:

Data base: Oracle 10g R2/11g (Initialization string inherited from Default)

```
SELECT 'GROUP' "GROUP", b.responsibility_name FROM FND_USER_RESP_GROUPS a,  
FND_RESPONSIBILITY_VL b, FND_USER u WHERE a.user_id = u.user_id AND a.responsibility_id
```

Variable Target

Row-wise initialization

Execution Precedence

Name	Initialization string	Data Source
LDAP Authentication	USER=sAMAccountName	SAS.SungardRS.com

Required for authentication

Description

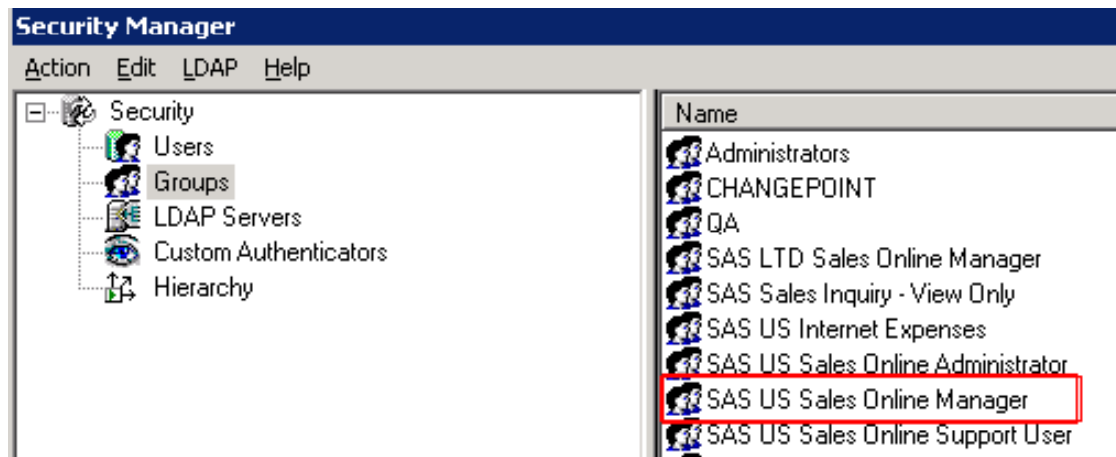
Here we get the Responsibility for that User from Oracle APPS

```
SELECT 'GROUP' "GROUP", b.responsibility_name
FROM apps.fnd_user_resp_groups a,
     apps.fnd_responsibility_vl b,
     apps.fnd_user u
WHERE a.user_id = u.user_id
     AND a.responsibility_id = b.responsibility_id
     AND a.responsibility_application_id = b.application_id
     AND SYSDATE BETWEEN a.start_date AND NVL (a.end_date, SYSDATE + 1)
     AND b.end_date IS NULL
     AND u.end_date IS NULL
     AND ( LOWER (b.responsibility_name) LIKE '%sales%'
         OR b.responsibility_name = 'SAS US Internet Expenses'
       )
     AND LOWER (u.user_name) = LOWER (':USER')
ORDER BY b.responsibility_name, u.user_name
```

This Query will return all the Subordinates for the User who logged in

```
SELECT distinct 'SUBORDINATE_ID', resource_id FROM
TABLE(SG_OBIEE_SALESREPS_SECURITY.get_peers_rs_id(':USER'))
```

## Create a Groups needed for the Security



**Session Variable Initialization Block - SUBORDINATE\_ID**

Name:   Disabled

Data Source


Connection Pool:

Data base: Oracle 10g R2/11g (Initialization string inherited from Default)

Variable Target

Row-wise initialization

Execution Precedence

Name	Initialization string
 Group	SELECT 'GROUP' "GROUP", b.responsibility_name FROM FND_USER_RESP_GROUPS a, FND_RES

Required for authentication

Description

```

CREATE OR REPLACE PACKAGE DSSD.SG_OBIEE_SALESREPS_SECURITY
IS
    type sg_rsrc_rec is record ( resource_ID number );
    type sg_rsrc_tab is table of sg_rsrc_rec ;
    FUNCTION GET_RESOURCE_ID(OBIEE_USER_Name varchar2)
        RETURN SG_OBIEE_SALESREPS_SECURITY.sg_rsrc_tab PIPELINED ;
    FUNCTION GET_PEERS_RS_ID (OBIEE_USER_Name varchar2)
        RETURN SG_OBIEE_SALESREPS_SECURITY.sg_rsrc_tab PIPELINED ;
    PROCEDURE PRINT_RESOURCE_ID (OBIEE_USER_Name varchar2);
    PROCEDURE PRINT_PEERS_RESOURCE_ID(OBIEE_USER_Name varchar2);
END SG_OBIEE_SALESREPS_SECURITY ;
/

```

```

FUNCTION GET_PEERS_RS_ID(OBIEE_USER_Name in varchar2)
    RETURN SG_OBIEE_SALESREPS_SECURITY.sg_rsrc_tab PIPELINED
IS

```

```
FOR y IN 1..v_parent_group_tab.COUNT LOOP

    FOR i IN c5_SalesReps( v_parent_group_tab(y))
    LOOP
        rec_out.resource_id := i.resource_id;
        PIPE ROW (rec_out);
    END LOOP;
END LOOP ;
RETURN;
```

This Filter is to restrict the row returned

Logical Table Source - DSS\_SCORECARD\_QUOTA\_ATTN\_SUM

General | Column Mapping | Content

Aggregation content, group by: Logical Level

Show mapped     Show unmapped    More...

Dimension	Logical Level	
Sales Reps Dim		X
Scorecard DW Data Dict Dim		X
Time Dim		X

Fragmentation content:

This source should be combined with other sources at this level

Use this "WHERE" clause" filter to limit rows returned (exclude the "WHERE"):

```
sgdssd.""DSSD.DSS_SCORECARD_QUOTA_ATTN_SUM.RESOURCE_RECORD_ID =  
VALUEOF(NQ_SESSION."SUBORDINATE_ID")
```

Select distinct values

OK    Cancel    Help


When a user logs in, he sees the Dashboard that is assigned to his Group

ORACLE Interactive Dashboards SCORECARD

SCORECARD Welcome, kris.vadlamudi! Dashboards -- More Products ▾

Performance Retention Quota Forecast KPI

LEVEL 4:  LEVEL 3:  LEVEL 2:  LEVEL 1:  LEVEL 0:  AE:  As Of: 1/31/2009

 [Performance Data Dictionary](#)

Please select each level and click "Go"

## My Account

Make changes to your account information.

Finished

Cancel

### General

Display Name kris.vadlamudi

User ID kris.vadlamudi

### Preferences

Default Dashboard Default

Locale (location) English - United States

User Interface Language English

Time Zone Default

[Change Password](#)

### Delivery Options

Configure devices and delivery profiles for Oracle BI Delivers.

#### Devices

Email Phone Pager Handheld Other

Default	Device Name
No devices of this category are defined.	
<a href="#">Add Email Device</a>	

#### Delivery Profiles

Active	Profile Name
No delivery profiles are defined.	

[Add Delivery Profile](#)

#### Group Membership

This list shows the groups to which you belong.

Authenticated Users  
SAS US Sales Online Manager

## This is the SQL that is being sent to the OBIEE Server from the Presentation Server

```
SELECT DISTINCT t44767.level4_full_name AS c1, t44767.level3_full_name AS c2,
  t44767.level2_full_name AS c3, t44767.level1_full_name AS c4,
  t44767.level0_full_name AS c5,
  t44767.resource_full_name AS c6,
  t44767.l_month_end_date AS c7
FROM dss_scorecard_quota_attn_sum t44767
WHERE ( t44767.l_month_end_date =
      TO_DATE ('2009-01-31', 'YYYY-MM-DD')
      AND t44767.resource_full_name = '(NOT SELECTED)'
      AND t44767.level0_full_name = '(NOT SELECTED)'
      AND t44767.level1_full_name = '(NOT SELECTED)'
      AND t44767.level2_full_name = '(NOT SELECTED)'
      AND t44767.level3_full_name = '(NOT SELECTED)'
      AND t44767.resource_record_id IN
        (4575,
         100000180,
         100000183,
         100000188,
         100000189,
         100000201,
         100000202,
         100000203,
         100000204,
         100000206,
         100000207,
         100000209,
         100000260,
         100000280,
         100000281,
         100000283,
        )
      )
ORDER BY c1, c2, c3, c4, c5, c6, c7
```

There might be some LDAP users who are not in Oracle Apps – so need to have a Table to Look up for the actual User name for the LDAP Account name

```
SELECT 'GROUP' "GROUP", b.responsibility_name
FROM fnd_user_resp_groups a, fnd_responsibility_vl b, fnd_user u
WHERE a.user_id = u.user_id
AND a.responsibility_id = b.responsibility_id
AND a.responsibility_application_id = b.application_id
AND SYSDATE BETWEEN a.start_date AND NVL (a.end_date, SYSDATE + 1)
AND b.end_date IS NULL
AND u.end_date IS NULL
AND ( LOWER (b.responsibility_name) LIKE '%sales%'
OR b.responsibility_name = 'SAS US Internet Expenses'
)
AND LOWER (u.user_name) = LOWER (':USER')
UNION
SELECT 'GROUP' "GROUP", b.responsibility_name
FROM fnd_user_resp_groups a, fnd_responsibility_vl b, fnd_user u
WHERE a.user_id = u.user_id
AND a.responsibility_id = b.responsibility_id
AND a.responsibility_application_id = b.application_id
AND SYSDATE BETWEEN a.start_date AND NVL (a.end_date, SYSDATE + 1)
AND b.end_date IS NULL
AND u.end_date IS NULL
AND ( LOWER (b.responsibility_name) LIKE '%sales%'
OR b.responsibility_name = 'SAS US Internet Expenses'
)
AND (u.user_name) IN (SELECT UPPER (apps_user)
FROM dss_ldap2apps_user_xref
```

DSS_LDAP2APPS_USER_XREF	
LDAP_USER	APPS_USER
idep	Jhonny Dep
bspears	Britney Spears
Jtravaolta	John Travolta



Q & A