



Oracle Access Manager and RadiantOne Virtual Directory Server (VDS) Integration Implementation Guide

OVERVIEW

Oracle Access Manager is a state-of-the-art solution for both centralized identity management and access control, providing an integrated standards-based solution that delivers; authentication, web single sign-on, access policy creation and enforcement, user self-registration and self-service, delegated administration, reporting, and auditing. **Oracle Access Manager's** unique coupling of access management and identity administration functionality is why it is established as the leading solution for web access management.

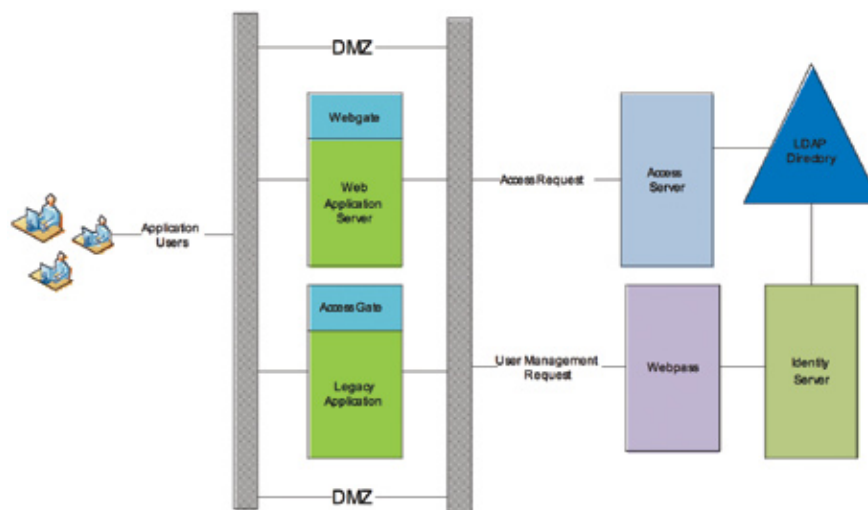
FEATURES

Oracle Access Manager has two major systems: Identity System and Access System.

Identity System allows workflow driven user management and access clearance using administrative, delegated and self-service functions.

The Access System enforces access policies for web resources using WebGate and AccessGate for legacy systems.

Architecture



Continued next page>



Oracle Access Manager and RadiantOne Virtual Directory Server (VDS)

Integration Implementation Guide

LDAP DIRECTORY

Oracle Access Manager uses an LDAP directory for three different types of data and can use the same or a different directory server for each function.

User data: User data consists of user directory entries managed by the Identity System. This data includes the information related to users, groups, locations, and other generic objects managed by the Identity System.

When installing Oracle Access Manager, you need to provide the following information to set up the main directory server profile:

- Directory server where user data is stored
- Bind information; DNS host name, port, user name (bind DN), password
- Searchbase, to identify the node in the directory information tree (DIT) under which this data is stored and the highest possible base for all user data searches
- Master Administrator(s)

Configuration data: Configuration data (Oracle Access Manager Configuration details), are stored in the directory. It can be stored in same, or different directory, as user data. This data includes workflow and configuration information that governs the appearance and functionality of the Identity System and Access System. Configuration data is managed by the Identity System.

Policy data: Policy data consists of definitions and rules that govern access to resources. This data is maintained in the directory server by the Policy Manager. The directory server can be different from the one used to store user and configuration data.

WEBGATE

WebGate is an out-of-the-box access client for enforcing access policy on HTTP-based resources; hence it is the Access System's web Policy Enforcement Point or PEP. The WebGate client runs as a plugin or module on top of most popular web servers and intercepts HTTP requests for web resources and forwards them to the Access Server where access control policies are applied. WebGate is optimized to work on web server environments, streamlined for the HTTP protocol, understand URLs, session cookies, HTTP redirects, secure sessions (HTTPS) and also implement policy caches that improve WebGate's performance and allow for scalability in highly trafficked sites.

ACCESSGATE

The AccessGate is the term used for any Access System client that is not WebGate, so it is the Access System's non-web PEP. Typically it is the implementation of a client using the Access API. AccessGates are leveraged to build the J2EE application server and portal connectors that are available within the Access System, which include BEA WebLogic, IBM WebSphere, and Oracle OC4J. In addition, customers can implement their own Access System clients and develop enforcement points to their custom applications or systems.

ACCESS SERVER

Access Manager's Access Server is a standalone software server that enforces access policies on web and non-web resources, so it is the Access System's Policy Decision Point or PDP. The Access Server can be deployed in a single instance, or as part of a clustered implementation to support load balancing and failover. Load-balancing and failover of the Access Server is built in and does not require the deployment of external load-balancers. The Access Server provides dynamic policy evaluation as users access resources, as well as authentication, authorization, and auditing services. The Access System is a scalable server, which provides configurable caching of both user and policy information to significantly improve the performance of access policy evaluation.

POLICY MANAGER AND ACCESS SYSTEM CONSOLE

Access Manager's Policy Manager is a browser-based graphical tool for configuring resources to be protected and well as creating and managing access policies. It is the Access System's Policy Management Authority or



Oracle Access Manager and RadiantOne Virtual Directory Server (VDS)

Integration Implementation Guide

PMA. The Policy Manager provides the login interface for the Access System, communicates with the directory server to manage policy data, and communicates with the Access Server over the Oracle Access Protocol to update the Access Server cache when policies are modified. A screen shot of the policy administration interface of the Policy Manager is shown in figure 1. Master Access Administrators and Delegated Access Administrators use the Policy Manager to:

- Create and manage policy domains that consist of:
 - Resource types to protect
 - Authentication, authorization, and audit rules
 - Policies (exceptions)
 - Administrative rights
- Add resources to policy domains
- Test access policy enforcement

WEBPASS

A WebPass is a web server plug-in that passes information back and forth between the web server and the Identity Server over the Oracle Identity Protocol (formerly Netpoint or COREid Identity Protocol). WebPass is the presentation tier of the Identity System. By default, WebPass renders its content as HTML so that it can be accessed through a browser. But in addition, it provides a Web Service interface, known as IdentityXML, which SOAP-based clients can leverage to programmatically interact with the Identity System. The idea behind IdentityXML is that it allows the integration of business logic governing identity administration process to be available and easily integrated with existing applications in a SOA environment.

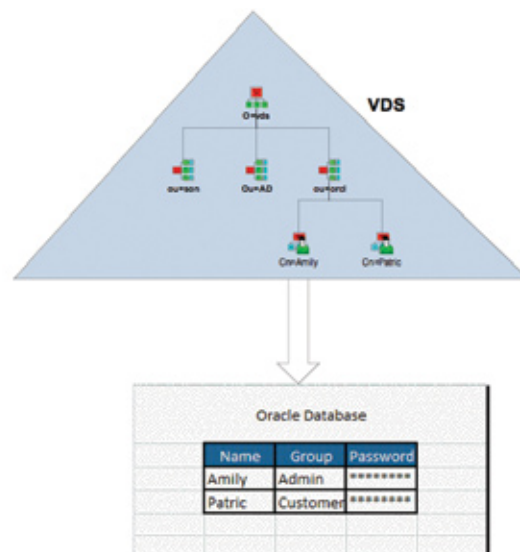
IDENTITY SERVER

The Identity Server manages identity information about users, groups, organizations, and other objects. The Identity Server performs three main functions:

- Reads and writes to your LDAP directory server across a network connection
- Stores user information on a directory server and keeps the directory current
- Processes all requests related to user, group, and organization identification

LIMITATIONS AND SOLUTIONS

- **RDBMS as User store:** Oracle Access Manager is not able to manage or enforce access control on applications which have a user base in RDBMS tables. Most organizations have user data in one or more databases. For example, most popular CRM tools store customer information in RDBMS tables and application are authenticating customers by querying these databases.



The RadiantOne Virtual Directory Server (VDS) can create LDAP objects from Database tables, able to be queried using LDAP. Implementing VDS as the User Data Store in Oracle Access Manager extends functionality of Oracle Access Manager in managing database users.

- **Multiple user directories:** In an era of a dynamic business world, every organization has to be ready with major organizational changes like acquisitions, mergers and spin-offs. In most scenarios, a single user directory cannot meet all identity requirement of the organization. Legislation compliance is forcing organizations to manage users in multiple directories based on locations.

Oracle Access Manager provides disjoint search functionality to manage multiple user directories using a single Identity system. The limitation of this approach is that it requires a separate Identity System admin to manage each user and separate workflow configuration for each directory server.

RadiantOne VDS can aggregate all directory servers under one federated namespace. It significantly reduces cost of having multiple administrators and duplication of maintenance.

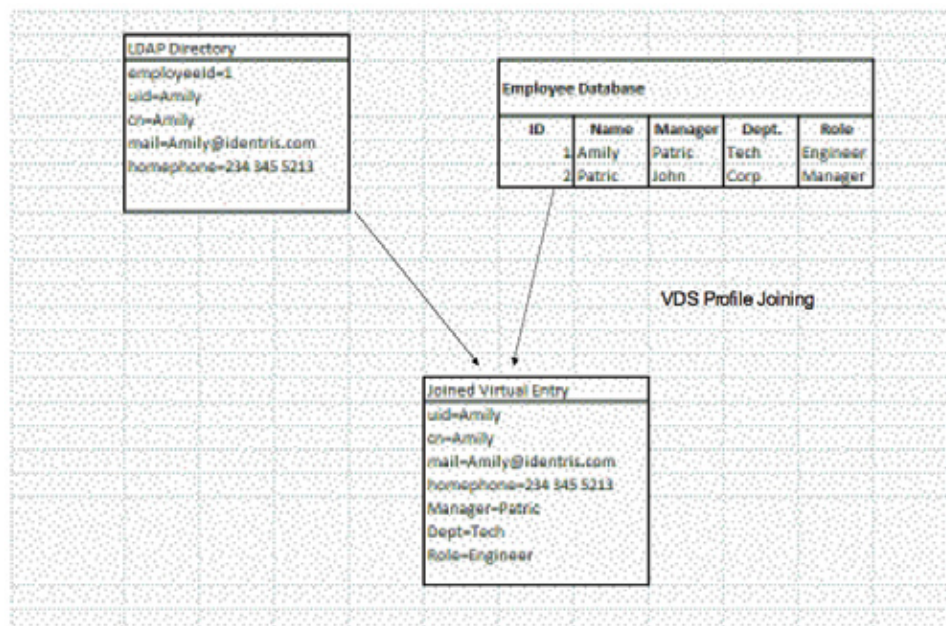
- **Split user profiles:** In any organizational environment, it is difficult to have a single user directory with 100% accurate information. In most of the organization, different departments maintain different information. HR maintains employee designation, department, manager, etc while IT maintains employee credentials.

In addition to authentication/authorization credentials, in many scenarios Oracle Access Manager requires accurate information of users like their department and designation.



Oracle Access Manager and RadiantOne Virtual Directory Server (VDS)

Integration Implementation Guide



RadiantOne VDS aggregates user information by joining multiple data sources, based on common attribute values, and makes them available as an LDAP object. Oracle Access Manager with RadiantOne VDS can also manage this information across multiple sources.

Product Configuration

Configure RadiantOne for use with Oracle Access Manager in following easy steps.

- 1) Extend schemas user information
- 2) Extract schema from user data stores
- 3) Map user information from each source
- 4) Build a virtual DIT of the user store
- 5) Aggregate all virtual DITs into a single federated namespace
- 6) Set RadiantOne VDS as the user directory in Oracle Access Manager



Oracle Access Manager and RadiantOne Virtual Directory Server (VDS)

Integration Implementation Guide

Step 1. Update schema in all underlying stores used for User identity and in VDS

Addition to access control, Oracle Access Manager also provides support for user management, group management and Organization management functionality. In order to use the full capability, it is required to extend schema of backend identity stores for the mandatory attributes of Oracle Access Manager.

The files required for ldap schema extension are located in:

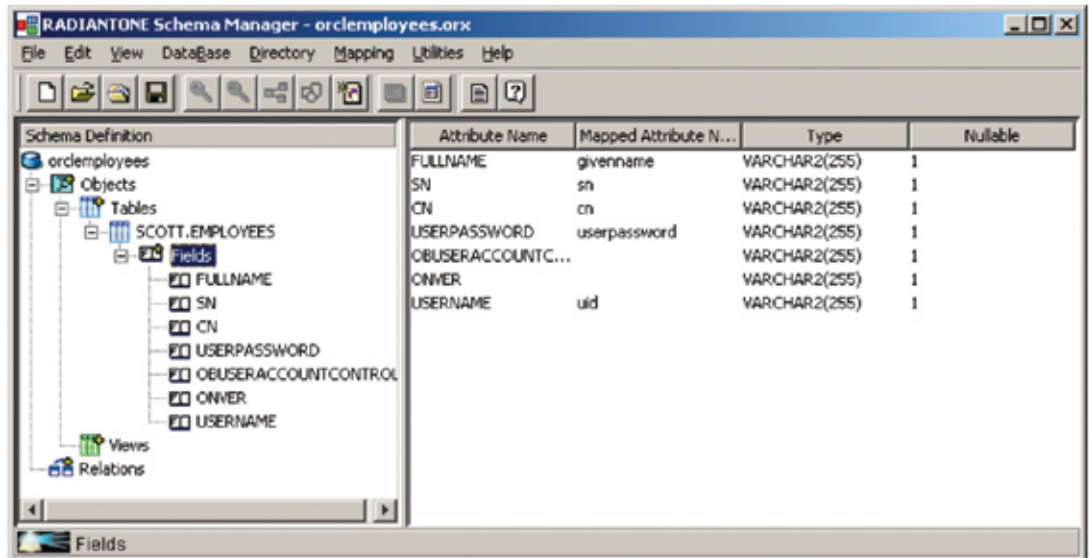
IdentityServer_install_dir\identity\oblix\tools\DNConversionToolkit\oblix\tools\DataAnyWhere\OblixUserSchema*.ldif

For extending table structure to store oracle access manager related data, Please refer to Oracle Documentation at:

http://download-uk.oracle.com/docs/cd/B28196_01/idmanage.1014/b25353/vde.htm#CDEJBIHD

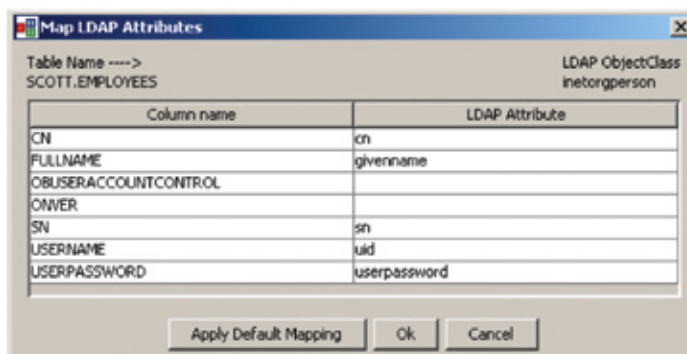
Step 2. Extract schema from User data stores

The RadiantOne Schema Manager connects to the user store and inventories different objects and attributes. The RadiantOne Schema Manager captures the metadata that will contribute to the virtual directory. Any data source that can be reached through ODBC, JDBC, LDAP V2 or V3, SOAP or any Java API can be extracted using Schema Manager. Upon capture, the schema extractor wizard encodes the schema in XML. After the schema is extracted, you can manage/modify the metadata by setting up the mapping for objectclasses and attributes, declaring keys, and relation between objects. The diagram below shows extracted schema from Oracle Database.



Step 3. Map Objects and Attributes to a common format for Oracle Access Manager.

Oracle Access Manager expects the virtual directory to expose inetOrgPerson and group object for identity management and enforcing access policy. Hence all native object classes and attributes needs to be mapped with either of these object types. In this example, the common object class will be inetorgperson. The object and attribute mapping is accomplished using the RadiantOne Schema Manager. The picture below depicts the Schema Manager interface and how the attributes will appear after they are mapped.



Step 4. Build Virtual Directory trees from the Data stores

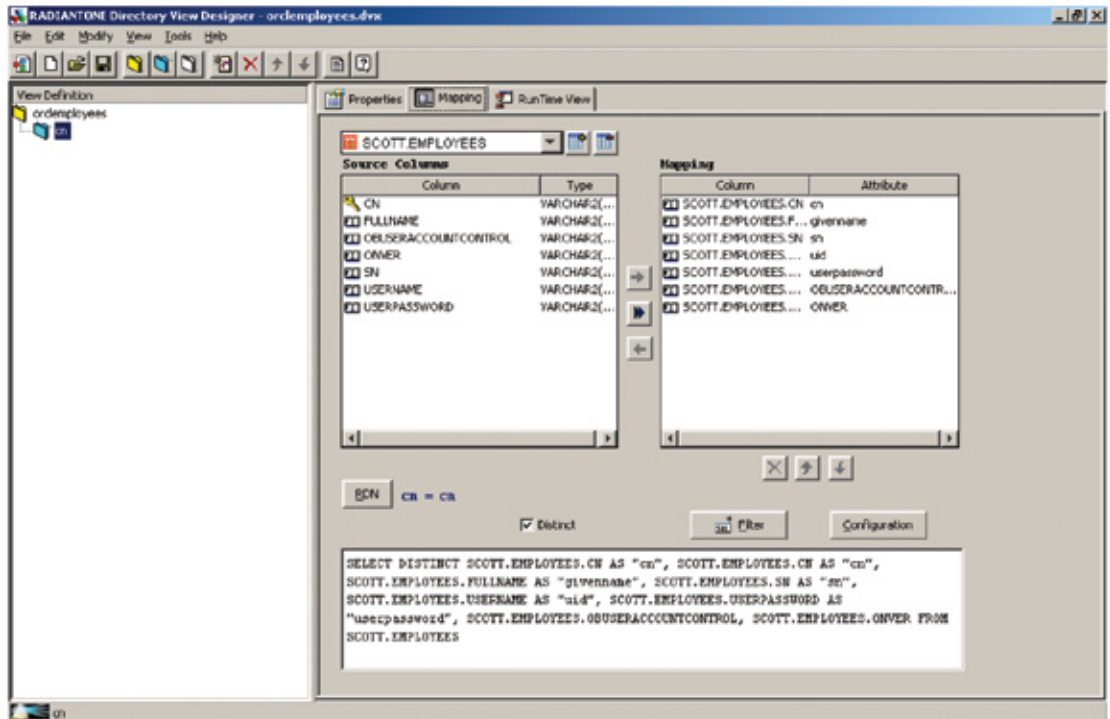
Use the RadiantOne View Designer to leverage the metadata captured with the schema manager to create custom virtual DITs. Using View Designer, it is possible to combine multiple virtual DITs to form one federated tree, or join multiple metadata to form join and split profiles.

Every virtual directory view (DIT) will specify which attributes to expose to Oracle Access Manager. The picture below displays the attribute from database that will be available (uid, cn, givenname)



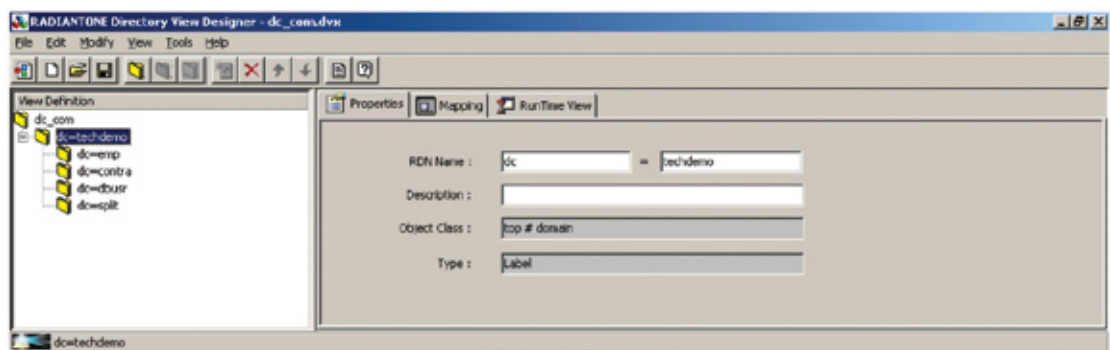
Oracle Access Manager and RadiantOne Virtual Directory Server (VDS)

Integration Implementation Guide



Step 5. Aggregate Virtual Directory trees to build a common namespace

After configuring the virtual DIT for each data store, a final virtual directory tree will be designed to aggregate the trees that were created from each source, so that all of them appear as a single tree. Below is a picture depicting the aggregation in RadiantOne View Designer.



Continued next page>

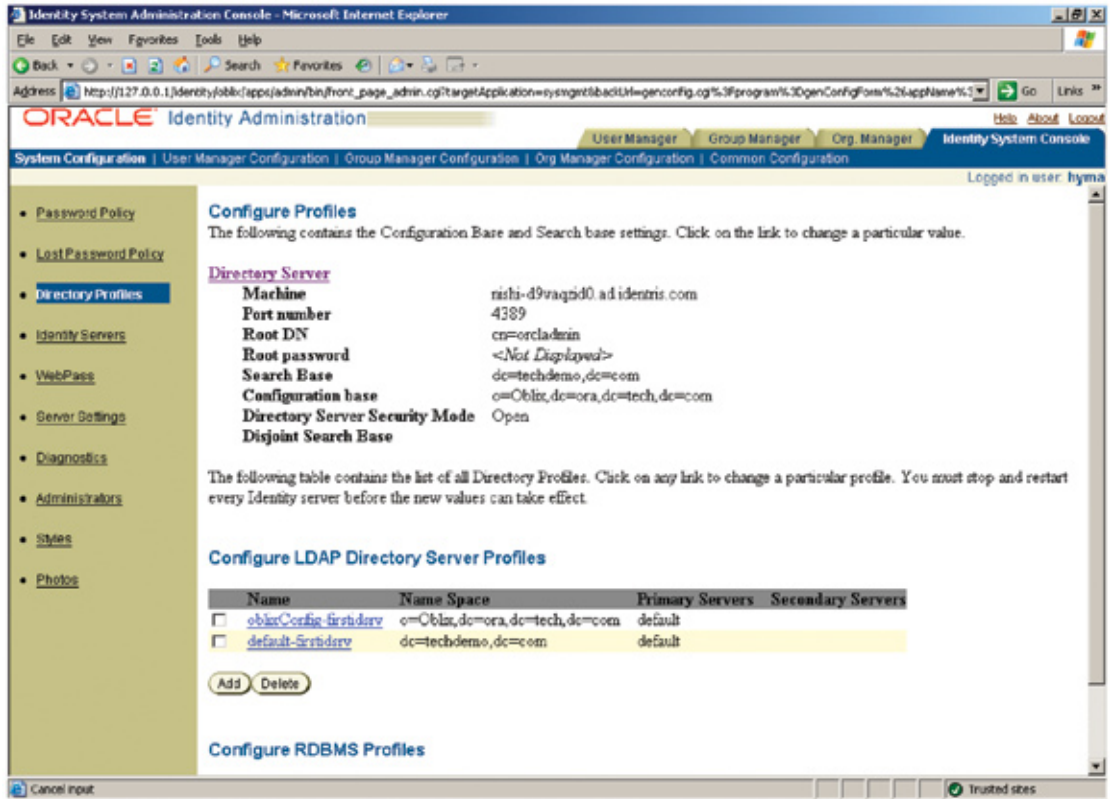


Oracle Access Manager and RadiantOne Virtual Directory Server (VDS)

Integration Implementation Guide

Step 6. Configure a user directory for Oracle Access Manager based on RadiantOne VDS

In Oracle Access Manager, the User Directory can be defined at the time of installation or at run time. With VDS integration, it is required to provide directory the admin user and password to the oracle access manager so it can access all branches of the virtual tree. The aggregated virtual directory tree (dv=virtual tree) is specified as the root for user and group search base.



The screenshot shows the Oracle Identity Administration console in a Microsoft Internet Explorer browser. The page title is "ORACLE Identity Administration". The navigation menu includes "System Configuration", "User Manager Configuration", "Group Manager Configuration", "Org Manager Configuration", and "Common Configuration". The "System Configuration" section is active, and the "Directory Profiles" link is selected in the left-hand menu.

The main content area is titled "Configure Profiles" and contains the following information:

Configure Profiles
The following contains the Configuration Base and Search base settings. Click on the link to change a particular value.

Directory Server

Machine	nishi-d9vaqnd0.ad.identris.com
Port number	4389
Root DN	cn=orcladmin
Root password	<Not Displayed>
Search Base	dc=techdemo,dc=com
Configuration base	o=Oblix,dc=ora,dc=tech,dc=com
Directory Server Security Mode	Open
Disjoint Search Base	

The following table contains the list of all Directory Profiles. Click on any link to change a particular profile. You must stop and restart every Identity server before the new values can take effect.

Configure LDAP Directory Server Profiles

Name	Name Space	Primary Servers	Secondary Servers
<input type="checkbox"/> oblixConfig-firstdirsv	o=Oblix,dc=ora,dc=tech,dc=com	default	
<input type="checkbox"/> default-Serverdirsv	dc=techdemo,dc=com	default	

Buttons: Add Delete

Configure RDBMS Profiles

CONCLUSION

Oracle Access Manager with RadiantOne VDS becomes the most flexible Identity and Access Management solution on the market. RadiantOne VDS is solving problems which are currently known as major limitations in Oracle Access Manager.