An Oracle White Paper
March 2009

Integrating Microsoft SharePoint Server With Oracle Virtual Directory
Disclaimer

The following is intended to outline our general product direction. It is intended for information purposes only, and may not be incorporated into any contract. It is not a commitment to deliver any material, code, or functionality, and should not be relied upon in making purchasing decisions. The development, release, and timing of any features or functionality described for Oracle's products remains at the sole discretion of Oracle.
Introduction

In many organizations that are considering deploying Microsoft SharePoint they face a challenge of needing to leverage identities stored in either multiple Active Directory servers or identities stored in non-LDAP stores.

Oracle Virtual Directory provides a solution to this challenge.

This is because Oracle Virtual Directory enables organizations to aggregate identity information without needing to consolidate.

The benefits of Oracle Virtual Directory:

- Provides single point of truth for identity-enabled applications
- Clients can access OVD via LDAP, Web Services and SQL
- OVD can connect to data from a variety of sources including LDAP, relational databases and Web Services

The benefits of SharePoint and Oracle Virtual Directory Integration are:

- Allow a single SharePoint instance to use multiple Active Directory domains
- Allow SharePoint to use identity information stored in non-Active Directory based identity stores including databases
- Allow SharePoint to use identity information that is split between Active Directory and non-Active Directory data stores including databases

Example use cases enabled by Oracle Virtual Directory with SharePoint:

- Allow a SharePoint workspace to be used by two different business units who each maintain their own AD domain
• Allow users to authenticate to SharePoint with Windows credentials but control access based on job codes maintained in a HR database

Process Overview

The integration process is very similar to any typical OVD deployment. What this package provides items that can be used for a typical deployment to reduce the time needed to deploy an OVD-SharePoint solution.

The process steps are:
• Install SharePoint and Oracle Virtual Directory
• Configure OVD to connect to identity stores
• Configure SharePoint's LDAP provider to connect to OVD

OVD Configuration

• Create a Local Store Adapter (LSA) to store the static base tree value (for example dc=mydomain,dc=com)
• Populate the LSA with the static entry data
• Add adapters with ROOT values configured to be branches under the base tree (such as ou=staff,dc=mydomain,dc=com)
• For any AD LDAP adapters -- add the ObjectClass mapper plug-in and map the cn attribute to the samaccountname attribute. This is because SharePoint will attempt to lookup the username in the cn attribute instead of the AD standard samaccountname attribute.
• If using OVD to connect SharePoint to OID – the Proxied Page Size parameter needs to be set to 10.

Microsoft SharePoint Configuration

The integration with Oracle Virtual Directory requires a version of SharePoint that works with the SharePoint LDAP Membership provider. This provider is developed and supported by Microsoft.

Create a new zone in SharePoint for the web application (portal) that's is going to use OVD. Use the option "Extend an existing Web Application"
• Change the authentication method for the application and choose Forms Authentication (Applications->Authentication Providers->New Zone). Make sure you use **LdapMembership** for Membership Provider and **LdapRole** for Role Management. These are the names used in the web.config below.

• Modify the web.config file for the web application in the new zone and also for the Central Administration site. Add the following entries:

• Between the key `<PeoplePickerWildcards>` on both files

```xml
<PeoplePickerWildcards>
    <add key="LdapMembership" value="*" />
    <add key="LdapRole" value="*" />  
</PeoplePickerWildcards>
```

• Between the key `<system.web>` on the Web Application web.config. Replace OVDHOST, OVDPORT, USERSEARCHBASE, and GROUPSEARCHBASE for the respective values. Restart the Application

```xml
<membership defaultProvider="LdapMembership">
    <providers>
        <add server="OVDHOST" port="OVDPORT" useSSL="false"
             userDNAttribute="distinguishedName" userNameAttribute="cn"
             userContainer="USERSEARCHBASE" userObjectClass="person"
             userFilter="(ObjectClass=person)" scope="Subtree"
             otherRequiredUserAttributes="sn,givenname,cn" name="LdapMembership"
    </providers>
</membership>
```

```xml
<roleManager defaultProvider="LdapRole" enabled="true" cacheRolesInCookie="false"
             cookieName=".PeopleDCRole">
    <providers>
        <add name="LdapRole" type="Microsoft.Office.Server.Security.LDAPRoleProvider,
             Microsoft.Office.Server, Version=12.0.0.0, Culture=neutral,
             PublicKeyToken=71E9BCE111E9429C" server="OVDHOST" port="OVDPORT" useSSL="false"
             groupContainer="GROUPSEARCHBASE" groupNameAttribute="cn"
             groupMemberAttribute="Member" userNameAttribute="cn" dnAttribute="distinguishedname"
             groupFilter="(ObjectClass=group)" scope="Subtree" />
```
</providers>
</roleManager>

- Restart the Applications (iisreset)

- Assign a new administrator to the new App/Zone. (Application Management->Policy for Web Applications->Choose app and new zone). Choose a user as the admin. Users should show up as {dapmembership:user id}. If users or groups can’t be searched something is bad in the web.config file.

- Try to login to the Web App in the new zone, it should ask for credentials with a Form.

- Permissions can be added to users and groups in SharePoint as normally.