

# Directories, Directory Synchronization and Virtual Directories

*An Oracle White Paper*  
*December 2005*



# Directories, Directory Synchronization and Virtual Directories

## INTRODUCTION

Directory, directory synchronization and virtual directory technologies are essential building blocks for deployment of an identity management strategy. At a superficial level, each technology serves a similar purpose: to provide applications (or end users) with identity and group membership information for resources under management. These resources are most typically users, but can also be other managed resources such as application instances, shared network resources, or application meta-user accounts. While these technologies serve a similar purpose, however, each has its own deployment characteristics. Understanding what these respective technologies do and how and when to deploy them is essential to supporting a manageable environment.

This paper describes the uses of directory, directory synchronization and virtual directory technologies in enterprise environments. Some salient features of each technology are described, and examples of their use in specific deployment situations are described. Finally, this paper gives some guidance on when to deploy these technologies.

## DIRECTORIES, DIRECTORY SYNCHRONIZATION AND VIRTUAL DIRECTORIES

Directory, directory synchronization and virtual directory technologies each has a role in delivering identity management services to the enterprise. Understanding the design centers and trade-offs of these technologies is key to implementing an effective identity management deployment strategy. This section describes each of the technologies, their uses and limitations.

### Directories

Directories are repositories for managing information about users or applications within an organization for a specific purpose. These can include operating system directories such as Windows (NT or ADS), e-mail directories such as Lotus Notes or Microsoft Exchange, application user stores such as those deployed with Oracle E-Business Suite, PeopleSoft, or SAP, as well as general-purpose LDAP directories such as Oracle Internet Directory or Sun Java System Directory Server.

It is important to understand the roles directories, directory synchronization and virtual directories play in an enterprise.

Directories can provide a single, central point of user identity management in service of a community of applications. Furthermore, the identity information managed in a directory can be leveraged by custom-developed and commercial off-the-shelf applications through standard interfaces such as LDAP.

Most enterprises deploy and manage several directory services. The information contained in these directories needs to be consolidated to support most enterprise applications.

Most enterprises end up deploying and maintaining a variety of directories in their environment. Multiple directories emerge for a number of reasons:

- Existing deployments of applications may require their own, dedicated user identity repositories.
- Directories may be deployed to support distinct user communities, for example, intranet versus extranet users, or users in different divisions of the same company.
- Directories may be deployed to support a distinct community of applications (ERP, remote network access, collaboration, etc.)
- Merged or acquired companies may bring their own directories into the enterprise.

There are a number of drawbacks associated with maintaining isolated directories in the enterprise environment. Chief among them:

- Administrators are faced with the challenge of maintaining current user identity information across an assortment of directories and applications.
- End users must deal with multiple user IDs, passwords and administrative interfaces when accessing applications and managing their identity information.
- It is difficult to enforce and monitor compliance with corporate security policies, for example those for password lengths, retry limits, time to live, etc., across heterogeneous user identity stores.
- Finally, deployment of enterprise access services such as single sign-on becomes almost impossible without a single application-level “view” of the identity information.

### **Directory synchronization**

Directory synchronization copies select identities, attributes and group information between identity repositories.

Directory synchronization is one approach to consolidating identity information for enterprise use. Directory synchronization provides a mechanism for copying select identities, attributes and group information between two or more disparate identity repositories according to pre-defined operating rules. Directory synchronization is essential for many enterprise applications, some of which are described below.

#### **Leveraging enterprise identities for a community of applications**

A simple directory synchronization deployment is shown in Figure 1. In this example, an organization has deployed an enterprise directory for managing the identities and credentials for all enterprise users. In addition, the organization has

deployed a handful of special-purpose directories to support different communities of applications, for example, ERP systems, databases and network services. The decision to maintain distinct directories in this case may be motivated by an organizational need for administrative autonomy in these different application environments and/or by special needs of these repositories in supporting their respective application environments.

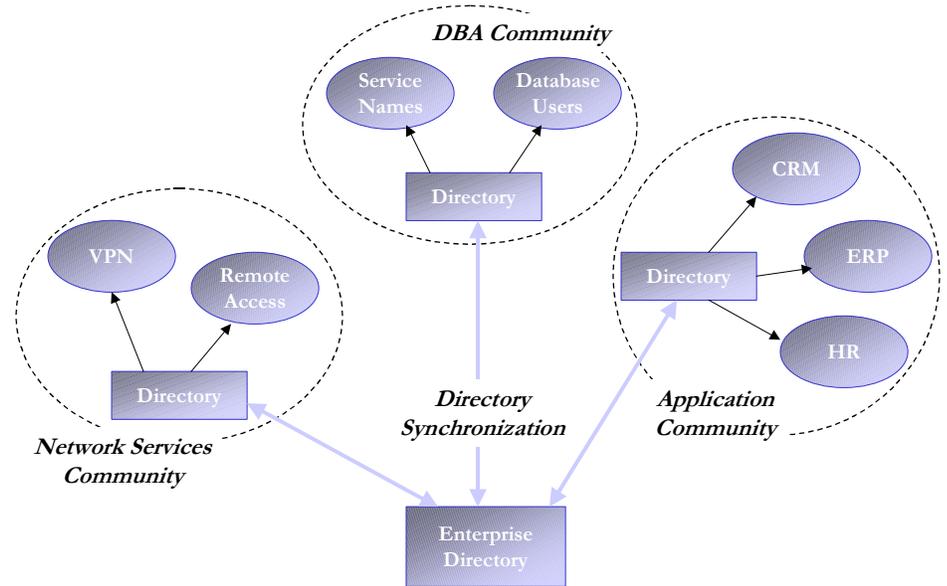


Figure 1: A simple directory synchronization deployment.

In this case, directory synchronization allows the various application communities to leverage the enterprise directory for user identities and credentials. As a result, users are able to access these applications with their enterprise user IDs and authentication credentials, freeing the application administrators from having to manage this information in the process.

#### Using the HR system to drive user provisioning

A second application of directory synchronization we will consider is using the corporate HR system (or systems) to automatically drive user provisioning. This is shown in Figure 2. In this example, directory synchronization is used to feed information directly from the “employee” table of an enterprise HR system into the enterprise directory service. The user identity thus created is available to connected applications, and may also be further leveraged to trigger an automated application provisioning workflow. This approach to user management can shorten the time new employees need to wait before they are provisioned to various enterprise applications. It can also minimize errors associated with the provisioning process. Finally, information about changes in employee status such as job responsibility

Directory synchronization can be used to drive the automatic provisioning of user identities from an HR system.

changes, terminations, etc., can be instantly reflected and leveraged in the enterprise application directory.

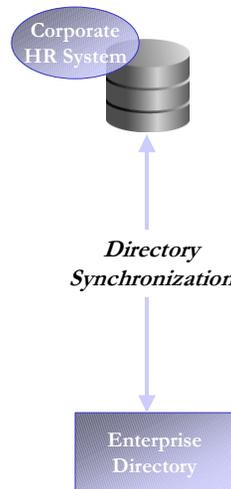


Figure 2: Directory feed from a corporate HR system.

#### Deploying enterprise meta-directories

Finally, directory synchronization can be leveraged to deploy enterprise meta-directories as shown in Figure 3. With a meta-directory, user identity information from a variety of sources is aggregated and made available in a central directory service to a variety of enterprise applications. Furthermore, changes made to identity information either in the central directory or in one of the connected repositories is reconciled according to pre-defined rules.

While most enterprises deploy some level of directory synchronization, deployment of a comprehensive meta-directory is a daunting prospect for most. One issue with meta-directories is the design and deployment of the system itself, and keeping the various components up to date through constant new system deployments and upgrades. A second issue is that it tends to force a “one size fits all” directory constraint on new applications deployed to leverage the enterprise meta-directory. The truth is that enterprise applications vary widely in their performance, administrative and metadata requirements, and these can be difficult to accommodate with a single enterprise directory. Finally and perhaps foremost, the process of deploying a meta-directory forces an enterprise to wrestle with a number of issues around identity data management and representation, as well as “political” issues of data and system ownership. These factors combined can be almost insurmountable obstacles to the realization of an enterprise’s meta-directory vision.

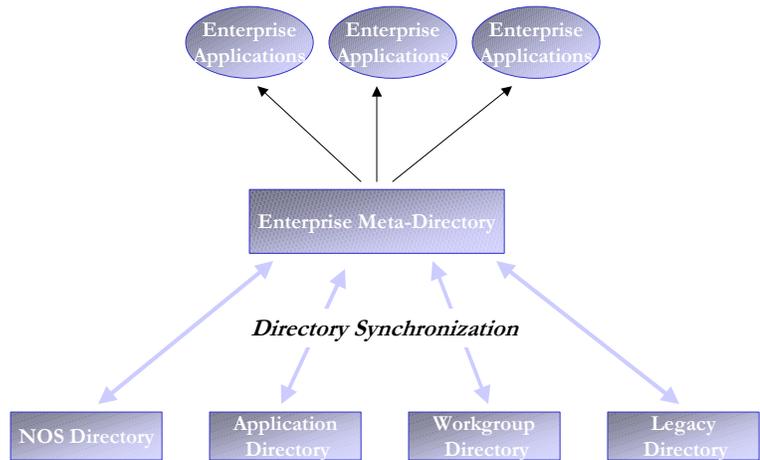


Figure 3: Enterprise meta-directory deployment.

### Virtual directories

"The connectivity provided is generally less intrusive and does not require that changes be made to the underlying source...which often makes virtual directory deployments more politically palatable than more involved meta-directory deployments."

#### The Burton Group

Virtual directories utilize the mapping abilities of meta-directories, without actually creating a central “join” repository of directory information. As such, virtual directories bypass the complexity of dealing with dataflow between directories. When an application requests directory data from a virtual directory, that data is retrieved, assembled and delivered to the application in real time. With virtual directories there is only one source of information for any particular data record (or directory-tree).

Virtual directories can be leveraged to deliver enterprise services, such as application single sign-on, with minimum disruption to an existing administrative environment. Such a deployment is shown in Figure 4. In this example, enterprise user identities and credentials are independently managed in a handful of directory services, perhaps reflecting users in autonomous business units of the same company. Deploying an enterprise access management service in combination with a virtual directory allows this company to provide transparent access to shared enterprise applications to all users. Moreover, each business unit can maintain administrative autonomy over its own users, as well as continue to control access to its own applications. Advantages of the virtual directory approach in this instance include:

- The organization is able to deploy enterprise access management services without disruptions or changes to existing administrative environment.
- There is no need to deploy and maintain a central service to store directory information.

- For each user, his or her identity information is managed in one place, minimizing potential for confusion and ensuring that the application view is always up to date.

## EFFECTIVELY LEVERAGING DIRECTORY, DIRECTORY SYNCHRONIZATION AND VIRTUAL DIRECTORY TECHNOLOGIES

"Anytime you're considering spending money to customize an application so that it can use your directory, you should look at virtual directory technology." (Quote from customer, The Boeing Company)

ComputerWorld

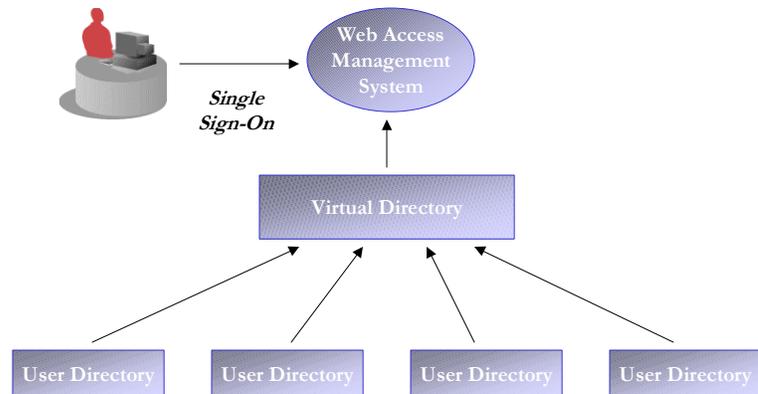


Figure 4: Virtual directory deployment.

All of these technologies, directory, directory synchronization and virtual directory, can and should be leveraged by enterprises managing application deployments. Some examples where directory synchronization technology is suitable include:

- Enterprises that have an enterprise source of truth for identities, and are seeking to leverage that information in administratively isolated application environments, should consider directory synchronization. This can allow these application environments to leverage this information to provide user login through a centrally managed user identity and credential.
- Organizations seeking to drive user provisioning from corporate HR system(s) should consider directory synchronization for this purpose.

On the other hand, certain deployments tend to be ideal for virtual directory technology. For example:

- Organizations seeking to quickly deploy an enterprise access service such as web single sign-on or remote access can leverage virtual directory technology to provide a real-time view of enterprise identity information to these services with minimal impact to the way this information is managed. This allows enterprises to deploy these services quickly without having to deal with the political issues of data ownership and representation.

"With VDE, the data stayed in the original source, and no extra effort was needed on our part to tell the test application where to find the necessary data, aside from directing it to VDE."

eWeek

- Organizations with a highly decentralized IT infrastructure such as government agencies, holding companies and diversified enterprises typically manage their users at a department or operating business unit level. Users in these environments may primarily access a set of applications unique to that department or business unit during a typical work day, but have an occasional need to access shared applications for tasks such as benefits administration or payroll self-service. These organizations can use virtual directory technology to provide users secure access to these applications without the additional burden of administering their identities.

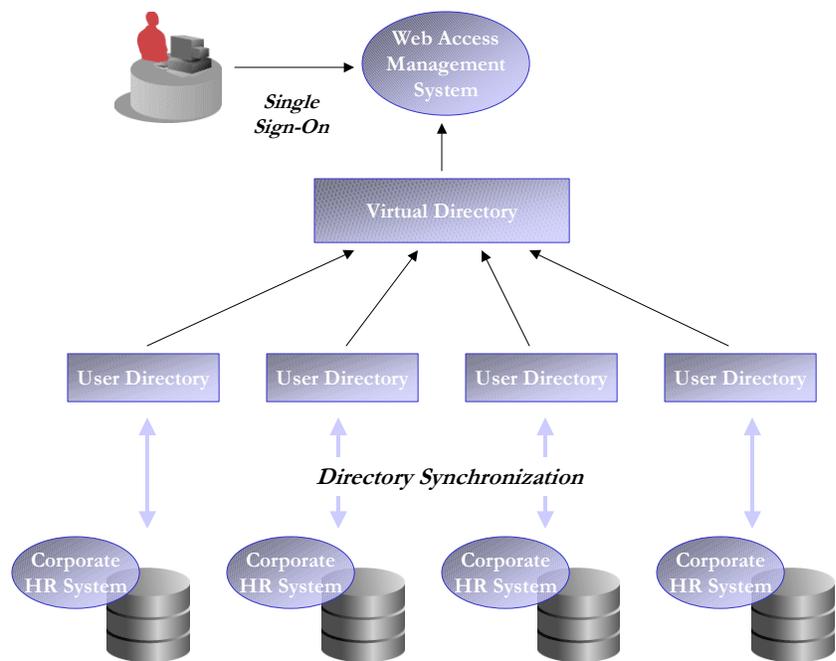


Figure 5: Deployment leveraging virtual directory and directory synchronization.

Finally, it is important to note that in many environments these technologies will be combined. Such an example is shown in Figure 5. Here, users are managed in autonomous directory communities at the departmental or business unit level. Furthermore, each department has its own HR systems for managing its employees. In this example, each department uses directory synchronization technology to feed automatic provisioning of users into the directory service. At the agency or company level, virtual directory technology is used to provide access control to a shared set of applications and/or network services.

## CONCLUSIONS

Directory, directory synchronization and virtual directory technologies are all essential for supporting enterprise application deployments. Each brings a particular set of capabilities, and combined they provide a powerful set of tools for

addressing any identity management requirement. Understanding the design centers and trade-offs of these technologies is key to their effective deployment.

## **ORACLE FUSION MIDDLEWARE**

Directories, Directory Synchronization and Virtual Directories  
December 2005

Oracle Corporation  
World Headquarters  
500 Oracle Parkway  
Redwood Shores, CA 94065  
U.S.A.

Worldwide Inquiries:  
Phone: +1.650.506.7000  
Fax: +1.650.506.7200  
[oracle.com](http://oracle.com)

Copyright © 2005, Oracle. All rights reserved.

This document is provided for information purposes only and the contents hereof are subject to change without notice.

This document is not warranted to be error-free, nor subject to any other warranties or conditions, whether expressed orally or implied in law, including implied warranties and conditions of merchantability or fitness for a particular purpose. We specifically disclaim any liability with respect to this document and no contractual obligations are formed either directly or indirectly by this document. This document may not be reproduced or transmitted in any form or by any means, electronic or mechanical, for any purpose, without our prior written permission.

Oracle, JD Edwards, PeopleSoft, and Retek are registered trademarks of Oracle Corporation and/or its affiliates. Other names may be trademarks of their respective owners.