Authenticated LDAP Name Lookup for Net Naming

An Oracle White Paper
October 2007

ORACLE

NOTE:

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.

Authenticated LDAP Name Lookup for Net Naming

Note:.... 2
Introduction.... 4
Necessity of Authenticated Name lookups.... 4
Authenticated name lookup feature.... 4
Enabling authenticated name lookup in active directory.... 4
    Setting ACLs on net service names.... 5
Enabling authenticated name lookup in oracle internet directory environment.... 6
    Setting ACLs on net Service Names.... 6
Conclusion.... 6

Authenticated LDAP Name Lookup for Net Naming

INTRODUCTION

Naming method resolves name to a connect descriptor. One of the naming methods is directory-naming method. Directory naming resolves a database service name, Net service name or Net service alias stored in a centralized LDAP-compliant directory server, including Oracle Interne Directory and Microsoft Active Directory. Centralized administration of database services and Net service names makes them easier to add or relocate. Users initiate a connection request by providing a connect string. A connect string includes a username and password, along with a connect identifier. A connect identifier can be the connect descriptor itself or a name that resolves to a connect descriptor

NECESSITY OF AUTHENTICATED NAME LOOKUPS

Necessity of authenticated name lookups

Business rules might require limiting the scope of visibility of database services and Net services in LDAP compliant directory to a set of users depending on user privileges. Oracle Database pre-11g clients always bind anonymously to directory for name lookups.

AUTHENTICATED NAME LOOKUP FEATURE

Oracle Database 11g and later support authenticated binds to directory for name resolution. Authenticated name lookups enable database administrator to control access by way of ACLs to database service and net service names. Database service name, Net services name, machine hosting the service, port number and any other service characteristics are available to privileged users who have access based on ACL settings on service name.

ENABLING AUTHENTICATED NAME LOOKUP IN ACTIVE DIRECTORY ENVIRONMENT

Windows clients that run oracle software can use native windows authentication for making authenticated name lookups. Use the `NAMES.LDAP_AUTHENTICATE_BIND=TRUE` parameter in sqlnet.ora to specify whether the LDAP naming adapter should attempt to authenticate when it connects to the Active Directory to resolve the name in the connect string.

Setting ACLs on net service names in Active Directory

Setting ACLs on net service names

ACLs on net service names in active directory can be set in different ways, including using Active Directory Edit (*ADSI*) and command-line utility *dsacls*.

dsacls.exe command-line tool displays and changes permissions (access control entries) in the access control list (ACL) of objects in Active Directory. Support Tools on the product media includes this command-line tool.

Examples:

To enable anonymous generic read on orcl service, run the following commands:

```
dsacls "CN=OracleContext,OU=Example,O=Com" /G
"anonymous logon":GR
```

```
dsacls "CN=orcl,CN=OracleContext,OU=Example,O=Com"
/G "anonymous logon":GR
```

To enable generic read on orcl service for the user scott in EXAMPLE domain, run the following command:

```
dsacls "CN=orcl, CN=OracleContext,OU=Example,O=Com"
/G example\scott:GR
```

By default, Everyone (users who are authenticated) has read permissions on Net service objects. In order to limit the readability of authenticated users it is recommended to disable read permissions for Everyone.

Example:

```
dsacls "CN=OracleContext,OU=Example,O=Com" /R
"Everyone"
```

To disable anonymous generic read on orcl service, run following command:

```
dsacls "CN=orcl,CN=OracleContext,OU=Example,O=Com"
/R "anonymous logon"
```

To disable generic read on orcl service for the user scott in EXAMPLE domain, run the following command:

dsacls "CN=orcl,CN=OracleContext,OU=Example,O=com" /R example\scott

ENABLING AUTHENTICATED NAME LOOKUP IN ORACLE INTERNET DIRECTORY (OID) ENVIRONMENT

Use the `NAMES.LDAP_AUTHENTICATE_BIND=TRUE` and Oracle Wallet parameters in sqlnet.ora to specify whether the LDAP naming adapter should attempt to authenticate when it connects to the OID to resolve the name in the connect string.

Setting ACLs on net Service Names

ACLs on database service and Net service entry cane be set in many ways including Oracle Internet Directory Administration (OIDADMIN) and ldapmodify command line utility with a ldif file.

Example ldif file that exclusives access rights to user1.

Setting ACLs on net service names in Oracle Internet Directory

```
dn: cn=user1, dc=acme,dc=com
changetype: modify
replace: orclentrylevelaci
orclentrylevelaci: access to entry by
    dn="cn=user1,dc=acme,dc=com" (browse, add,
    delete)
orclentrylevelaci: access to entry by * (none)
```

CONCLUSION

Today's business environments might want to limit availability of database services and net services to authorized users for security reasons. Oracle Database 11g solve it with authenticated name lookup feature. Procedures to use the feature for Oracle Internet Directory and Active Directory environments are described.

Authenticated LDAP Name Lookup for Net Naming
October 2007
Author: Srinivas Pamu
Contributing Author: Kant Patel

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