Using the RAD-Series Server with Microsoft® Active Directory

This article will describe how to configure the Interlink Networks RAD-Series server to authenticate users against a Microsoft Active Directory Server.

INTRODUCTION TO ACTIVE DIRECTORY

Active Directory is the data repository used by Windows 2000 and Windows XP domain controllers. It provides a single point of management for Windows-based user accounts, clients, servers, and applications. Data is stored in a hierarchical, object oriented, fashion. Objects are used to represent network resources (users, printers, servers, etc.), and containers are used to group related objects together. Every object and container is uniquely identified by its dn property.

User Containment

In a typical Active Directory deployment, the top most container is the domain being administered. The objects in this container relevant to configuring the RAD-Series server include the following: users, security groups, and organizational units (departments). Users can be stored directly in the domain container or in an organizational unit container.

As an example, lets say an Active Directory contains a domain called acme.com, and that this domain contains two departments: accounting and engineering. The dn of the accounting department would be

```
dn: ou=accounting,dc=acme,dc=com
```

The dn of the engineering department would be

```
dn: ou=engineering,dc=acme,dc=com
```

Continuing the example, lets say the engineering department has a user called Barbara Jansen. The dn of that user would be

```
dn: cn=Barbara Jansen,ou=engineering,dc=acme,dc=com
```

In most deployments, the administrative user for a domain is not contained in an organizational unit. Instead, it is contained in a generic container named Users. Thus, the administrator for the domain acme.com would have a dn of

```
dn: cn=Administrator,cn=Users,dc=acme,dc=com
```

The Windows 2000 Management Console or the ldifde.exe utility, both provided by Microsoft can be used to determine the dn of a user or container.

User Properties

User objects contain many properties that are used by the Windows 2000 and Windows XP operating systems. Of these properties, the only one that is relevant for configuring the RAD-Series server is sAMAccountName. This property represents the login id for a user.

Continuing the example from above, lets say the user Barbara Jansen had login id of bjansen. The sAMAccountName property for this user would be

```
sAMAccountName: bjansen
```

Like the dn property, the Windows 2000 Management Console or ldifde.exe utility can be used to determine the sAMAccountName of a user.

CONFIGURING THE RAD-SERIES SERVER

The RAD-Series server communicates with an Active Directory Server via LDAP (lightweight directory access protocol). Configuring this communication involves setting up a ProLDAP entry in the RAD-Series server's authfile.

The following is an example of a ProLDAP entry that has been setup to access the Active Directory deployment described above.

```
engin.acme.com      PROLDAP     "realm for acme engineers"
{
   Directory   “ACME Domain Controller”
   {
         Host        192.168.3.9
         Port        389
         Administrator   "cn=Administrator,cn=Users,dc=acme,dc=com"
         Password    "dmpassword"
         SearchBase  "ou=engineering,dc=acme,dc=com
         Filter      sAMAccountName
         Authenticate    auto
   }
}
```

The `Host` and `Port` parameters indicate the TCP attributes that should be used to communicate with the Active Directory Server.

The `Administrator` parameter is the dn of an Active Directory administrator; an Active Directory administrator is any user with read, write, and create permissions to the Active Directory. These permissions can be changed with the Windows 2000 Management Console.

The `Password` parameter is the password of the Active Directory administrator. This is the same password that the administrator would use to login on to a network computer.

The `SearchBase` parameter indicates what portion of the Active Directory will be searched. In this example, only users in the engineering department will be searched. If this parameter were set to dc=acme,dc=com, all users in the domain acme.com would be searched, no matter what department they were in.

The `Filter` parameter is the property that will be used to perform the user search. Setting this value to sAMAccountName allows users to use the same userid no matter if they are logging in via Radius or directly into a network computer. Other parameters can be used in place of sAMAccountName, but that would mean users would have a different userid when logging in via Radius.

The `Authenticate` parameter must be set to auto, bind and search are not supported with Active Directory.

With this configuration, the user Barbara Jansen would login via Radius using a userid/realm combination of bjansen@engin.acme.com. Her password would be the same as if she was logging on to a network computer.