Novell®

BorderManager™

Authentication Service

Planning

BorderManager™
Authentication Service
DIRECTORY-ENABLED RADIUS SOFTWARE

Novell®

disclaimer

Novell, Inc. makes no representations or warranties with respect to the contents or use of this documentation, and specifically disclaims any express or implied warranties of merchantability or fitness for any particular purpose. Further, Novell, Inc. reserves the right to revise this publication and to make changes to its content, at any time, without obligation to notify any person or entity of such revisions or changes.

Further, Novell, Inc. makes no representations or warranties with respect to any software, and specifically disclaims any express or implied warranties of merchantability or fitness for any particular purpose. Further, Novell, Inc. reserves the right to make changes to any and all parts of Novell software, at any time, without any obligation to notify any person or entity of such changes.

trademarks

Novell, Inc. has attempted to supply trademark information about company names, products, and services mentioned in this manual. The following list of trademarks was derived from various sources.

Novell and NetWare are registered trademarks of Novell, Inc. in the United States and other countries. BorderManager, NDS, and Novell BorderManager are trademarks of Novell, Inc.

Adobe is a registered trademark of Adobe Systems Incorporated.

Adobe Acrobat is a registered trademark of Adobe Systems Incorporated.

Netscape Navigator is a registered trademark of Netscape Communications Corporation.

Windows and Windows NT are registered trademarks and Windows 95 is a trademark of Microsoft Corporation.

Novell, Inc.
122 East 1700 South
Provo, UT 84606
U.S.A.

Contents

About This Guide

Introduction

The purpose of this documentation is to describe the concepts of remote user authentication and how to administer Novell® BorderManager™ Authentication Service on your network.

The audience for this documentation is network administrators. This documentation is not intended for users of the network.

chapter 1

Understanding Novell BorderManager Authentication Service

Understanding Remote Authentication

Novell® BorderManager™ Authentication Service enables remote users to dial in to NetWare® networks (version 4.11 or later) and access network information and resources such as files, databases, applications, e-mail, printing, and host/mainframe services. It maintains security by requiring users to authenticate to the NDS™ database using the Remote Authentication Dial-In User Service (RADIUS) network security protocol before they can access these services.

Dialing in as a user to a network that uses BorderManager™ Authentication Service is not much different from dialing in to any other dial-in service, except users use the same account to access NetWare file and print services. You can use any client software that works with your network access server. Many users find it convenient to use the Windows 95* dial-up networking feature. The BorderManager Authentication Service user must know the syntax of the user name:

Service_Name:*NDS_UserName*@*Domain*

In the simplest case, Service_Name and @Domain are not required and NDS_UserName is the common name of the user's object in NDS. NDS_UserName can be entered in distinguished name form or in common name form if you have configured BorderManager Authentication Service to accept common name login. For example, if Joe is an employee in the sales department at Acme, the common name form would be joe and the distinguished name form would be joe.sales.acme.

If a user is configured for more than one dial-in service, the user must add as a prefix to the username the name of the service followed by a

colon (:) when using a service other than the default (for example, ppp:joe selects the PPP service configured for user joe).

If a RADIUS proxy is used to authenticate from a remote RADIUS server, users must append an at-symbol (@) followed by the proxy domain to the username (for example, joe@acme.com).

Related Topics

“Understanding the RADIUS Protocol”
“Understanding RADIUS and NDS”
“Understanding Common Name Logins”
“Understanding Password Policies”
“Understanding RADIUS Proxy”

Understanding the RADIUS Protocol

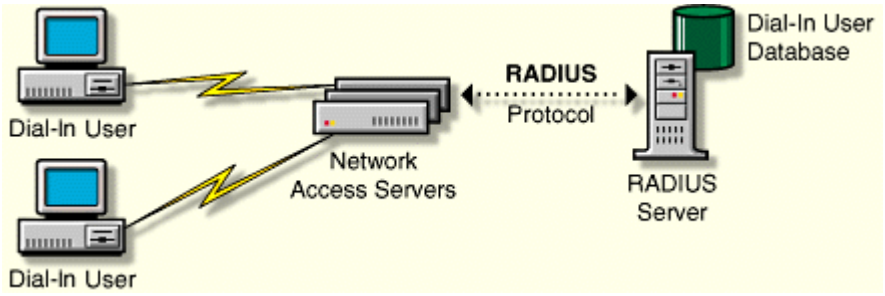
Novell® BorderManager™ Authentication Service implements RADIUS as the network security protocol to authenticate users for dial-in remote access.

A host server running the RADIUS protocol (the RADIUS server) retrieves all dial-in user and authentication information from a central database. A host server running the RADIUS accounting protocol (the RADIUS accounting server) is responsible for logging information about dial-in user connections. The accounting information is typically used for statistical analysis, troubleshooting, and billing.

Dial-in users access the Internet or corporate intranet through network access servers, which handle communication between the users and RADIUS servers. A dial-in user must provide authentication information (typically a username and password). The network access server forwards the information to the RADIUS server using the RADIUS protocol. The RADIUS server authenticates the user by comparing the user request to the user information in the central database. The RADIUS server then returns configuration information necessary for the network access server to deliver the requested service to the dial-in user. A RADIUS server can also communicate with a RADIUS proxy server to authenticate remote users who are not in its local database.

This concept is illustrated in Figure 1-1.

Figure 1-1
RADIUS Protocol



The RADIUS protocol is supported by many network access server vendors and is an IETF Proposed Standard (RFC 2138). The RADIUS accounting protocol is also an IETF Proposed Standard (RFC 2139). The key features of the RADIUS protocol are

- Centralized administration
- Client-server model
- Network security
- Support for multiple authentication mechanisms
- User configuration and access control

Centralized Administration

The RADIUS protocol provides a central database to store all dial-in user information. This database can be used by all RADIUS-compatible network access servers.

The RADIUS protocol provides separate log files for system messages and accounting information. You can enable or disable the logging of system messages or accounting information from the server console. Likewise, you can specify the number of days that the log files should be maintained.

Client-Server Model

Network access servers act as clients to RADIUS servers. The network access servers authenticate users through the RADIUS server when users dial in to the network.

RADIUS servers receive user connection requests, authenticate each user, and then return all configuration information necessary for the network access server to deliver the requested service to each user.

A RADIUS server can also act as a proxy client to other RADIUS servers.

Network Security

Transactions between the network access server and the RADIUS server are protected through a shared RADIUS secret. This shared secret is never sent across the network.

In addition, user passwords are encrypted, making it difficult for outsiders to decipher them.

Support for Multiple Authentication Mechanisms

RADIUS servers support Point-to-Point Protocol (PPP), Password Authentication Protocol (PAP), Challenge Handshake Authentication Protocol (CHAP), and other authentication mechanisms.

BorderManager™ Authentication Service maintains these usernames and passwords in the NDS™ database. BorderManager Authentication Service supports NDS-based user passwords for User objects in a Directory tree. Separate passwords are required for other password protocols.

User Configuration and Access Control

The network access server configures a user’s connection and access to the network according to information provided by the RADIUS server when the user is authenticated successfully. Using BorderManager Authentication Service, all users in an NDS container object can use the same configuration information or have unique dial-in configuration settings.

Related Topics

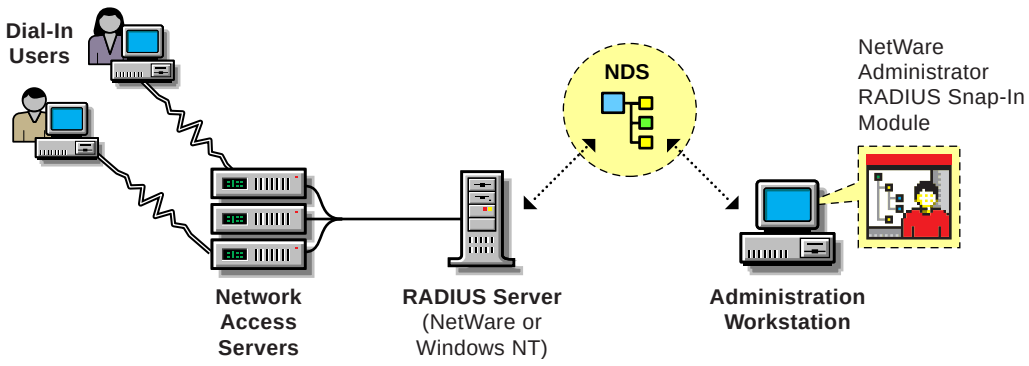
“Understanding RADIUS and NDS”
“Understanding Dial Access Attributes”
“Understanding RADIUS Proxy”
“Understanding RADIUS Accounting”
“Understanding the RADIUS Audit Log”

Understanding RADIUS and NDS

Novell® BorderManager™ Authentication Service enables you to use the NDS™ application as the central database to manage all your dial-in users and services. With the RADIUS server component running on a NetWare® server (version 4.11 or later) or a Windows NT* server (version 4.0 or later), you can centrally monitor and control dial-in authentication and access to network services from the NDS database. From the administration workstation component (running on either Windows 95 or Windows NT), you can centrally manage dial access services for users with the NetWare® Administrator utility. BorderManager™ Authentication Service also enables you to take advantage of all the security, distribution, replication, and administration benefits that NDS has to offer.

This concept is shown in Figure 1-2.

Figure 1-2
BorderManager Authentication Service Configuration



Related Topics

“Planning Dial Access Services”
“Understanding Dial Access Attributes”
“Understanding Password Policies”

Understanding Dial Access Attributes

The RADIUS protocol defines attributes that are used to control dial-in access to the network and user configuration. When the Novell® BorderManager™ Authentication Service server receives a request to authenticate a user, it determines whether the user is authorized to dial in (user exists, account is enabled, dial access is enabled, password is correct, and so on). If the user is authorized, the BorderManager™ Authentication Service server constructs a list of attributes to return to the network access server to configure the user dial-in session.

The list of attributes returned depends on

- The service the user specifies at login
- The attributes specified in the profile associated with the dial access service
  - Container-specific data if the service is defined for a container object instead of a user object
  - Default dial access properties for all users in the selected container
- The type of network access server the user has dialed in to

Related Topics

“Determining Dial Access Attributes”
“Understanding the RADIUS Protocol”

Understanding Common Name Logins

You can configure Novell® BorderManager™ Authentication Service to allow common name logins, as well as distinguished name logins. A

common name is the name displayed in the Directory tree (such as RJONES for the user Richard Jones). A distinguished name is the complete path (or context) from the object to the root of the Directory tree (such as .RJONES.HQ.ACME.US).

You can configure common name logins by specifying a list of lookup contexts (locations of an object within the Directory tree) in the Dial Access System object. The RADIUS server searches in these locations for any user who logs in without using a distinguished name. This feature is most useful if each User object in your Directory tree has been assigned a unique common name. Users who have names that are not unique must enter their distinguished names when logging in.

Refer to the BorderManager™ Authentication Service help for information about specific configuration procedures.

Related Topics

“Understanding Remote Authentication”
“Understanding RADIUS and NDS”

Understanding Password Policies

When you create a Dial Access System object, you must specify the password policy. Novell® BorderManager™ Authentication Service supports two options:

- Use Novell Directory Services Passwords
- Use Separate Dial Access Passwords

Use Novell Directory Services Passwords

When this option is selected, the NDS™ password (the same one used for NetWare® file and print services) is used to authenticate dial-in access. This means that users are not required to remember or change additional passwords.

Use Separate Dial Access Passwords

Separate passwords are encrypted in NDS in such a way that only an authenticated RADIUS server can easily decrypt them. There are two reasons for using separate dial access passwords:

- The Challenge Handshake Authentication Protocol (CHAP) algorithm requires the RADIUS server to have access to the clear-text password. NDS passwords are not available in clear text, so they cannot be used in conjunction with CHAP.
- The RADIUS protocol causes the password to be visible in clear text to the network access server and all RADIUS servers that process the authentication request (such as proxy RADIUS servers and the authenticating RADIUS server). You might not want your NDS password to appear as clear text in these systems if they are not administered by you.

Related Topics

“Understanding Remote Authentication”

“Understanding RADIUS and NDS”

Understanding RADIUS Proxy

A Novell® BorderManager™ Authentication Service server can be configured to receive authentication requests from another RADIUS server (the RADIUS proxy) or to act as a RADIUS proxy and send authentication requests to another RADIUS server.

Users who log in without a domain or a domain that has been configured to use the local NDS tree will be authenticated by your RADIUS server. Users who log in with another domain name will have their RADIUS communications sent to the RADIUS server for their domain. A user can specify the target domain at login time by appending the username with an @ followed by the domain name.

The syntax is similar to the Internet e-mail address syntax; however, the domain name is not restricted to Domain Name System (DNS), although DNS names might be convenient to use. For example, Jane, an employee of Acme, would be authenticated by the company’s RADIUS server by entering her username as jane@acme.com.

Related Topics

“Planning RADIUS Proxy”
“Understanding the RADIUS Protocol”
“Understanding RADIUS and NDS”
“Understanding Common Name Logins”

Understanding RADIUS Accounting

The RADIUS accounting server is responsible for logging information about dial-in user connections. The accounting information is typically used for statistical analysis, troubleshooting, and billing.

The RADIUS accounting server is typically implemented as a separate process of the RADIUS authentication server. The RADIUS accounting server listens on User Data Protocol (UDP) port number 1813. When an accounting packet is received from a RADIUS client (such as a network access server), the RADIUS accounting server logs the information in an ASCII text file and returns an acknowledgment to the RADIUS client.

When a user session begins, an accounting request packet containing connection information about a dial-in user (such as the type of service being delivered) is generated by a RADIUS client (such as a network access server) and sent to the RADIUS accounting server to be logged. When a user session ends, another accounting request packet containing the type of service delivered and any optional statistics is generated and sent to the RADIUS accounting server.

Related Topics

“Maintaining RADIUS Accounting”
“Understanding the RADIUS Protocol”

Understanding the RADIUS Audit Log

The RADIUS audit log is a disk file that contains the system messages that are displayed in the RADIUS status display console. The RADIUS audit log is typically used for troubleshooting.

The RADIUS audit log file contains the same messages that are displayed on the status display (successes or failures). The status display is not required to be open in order for messages to be logged to the system log file.

The naming of the audit log file takes the form

YYYYMMDD.LOG

where *YYYY* represents the year, *MM* represents the month, and *DD* represents the day (such as 19981120.LOG for a audit log file created on November 20, 1998). Naming files using this convention keeps log files to a manageable size and enables you to group system log information by month, week, or day.

By default, Novell® BorderManager™ Authentication Service starts with the RADIUS audit log file enabled. The default location for the RADIUS audit log file is as follows:

- SYS:\ETC\RADIUS\LOG for NetWare® servers (version 4.11 or later)
- C:\NOVELL\RADIUS\LOG for Windows NT servers (version 4.0 or later)

Related Topics

“RADIUS Status Display Options”
“RADIUS Status Messages”

chapter 2

Planning Novell BorderManager Authentication Service

Planning Dial Access Services

You must create the following NDS™ objects in your Directory tree to set up dial access services with Novell® BorderManager™ Authentication Service:

- Dial Access System object
- Dial Access Profile object

After these objects are created, you can modify the following NDS objects in your Directory tree to manage dial access services with BorderManager™ Authentication Service:

- Organization and Organizational Unit container objects
- User object

Dial Access System Object

You must create a Dial Access System object in your Directory tree to manage common configuration tasks for a collection of RADIUS servers working together. The information stored in this object consists of

- Client configuration—Enables you to define IP addresses for network access servers and shared secrets among the RADIUS servers and the various network access servers.
- Proxy targets—Enable you to configure other RADIUS servers to which you want to forward RADIUS requests.
- Password policy—Enables you to define the password policy for the Dial Access System object.

- Dial Access System object password—Enables you to restrict access to authorized users.
- Lookup contexts—Enables contexts to be searched when the common name portion of the username is received in an authentication request.

Typically, you need only one Dial Access System object in your Directory tree.

You can easily assign rights to an NDS object using NetWare® Administrator. For example, you can assign Browse and Read rights from NetWare Administrator by dragging the Dial Access System object over an Organizational Unit object near the root of an NDS tree.

Refer to *Novell BorderManager Authentication Service Installation and Setup* for information about setting up a Dial Access System object.

Dial Access Profile Object

You must create at least one Dial Access Profile object in your Directory tree to define common services used by many dial-in users. The Dial Access Profile object contains a list of RADIUS dial access attributes that specify the configuration for creating a specific service.

You can define as many profiles as you require to define different services. For example, you can create a PPP profile that enables users to dial in and access the Internet. You can also create a Telnet profile that enables users to connect to a local host using a terminal or terminal emulator. You can specify dial access profiles in the User object that can override settings in the Dial Access Profile object.

Refer to *Novell BorderManager Authentication Service Installation and Setup* for information about setting up a Dial Access Profile object.

Organization and Organizational Unit Container Objects

You can specify common dial access properties for all users in Organization or Organizational Unit container objects. The Dial Access Service page of an Organization or Organizational Unit allows you to

- Enable dial access services for all users

- Select the Dial Access System object for all users
- Configure dial access services that can be used by all users in a container

For example, if your organization has several departments that want to allow remote users to access your corporate network, you could use BorderManager™ Authentication Service to manage users who authenticate with the RADIUS protocol. Each department could specify rights to applications, file and print services, and dial-in configuration information. However, multiple departments could be managed by the same network administrator without the requirement to maintain multiple databases.

Specifying dial access properties in the Dial Access Service page for an Organization or Organizational Unit container object has the following benefits:

- Configuring all users in an Organization or Organizational unit to have the same dial-in rights simplifies administration over per-user administration.
- Configuring users in different containers with different access rights enhances security.

The dial access properties that you define for an Organization or Organizational Unit container object apply to every user in the selected container object (but not to users in organizational units that are at a lower level in the Directory tree).

User Object

You can override the dial access properties of an Organization or Organizational Unit container object by modifying the Dial Access Services page of a User object. This allows you to specify unique dial access properties for any User object in your Directory tree.

The User Dial Access Services page allows you to

- Enable a user for dial access services
- Select the appropriate Dial Access System object for a user

- Set a dial access password for a user (if you use separate passwords for dial-in users)
- Configure (or define) dial-in services for a user (such as enabling a user to select one or more Dial Access Profile objects and associate user-specific settings for each)
- Select a default dial access service if a user is configured for more than one

Refer to *Novell BorderManager Authentication Service Installation and Setup* for information about enabling a User object for dial access services.

Related Topics

“Determining Dial Access Attributes”
“Planning RADIUS Proxy”
“Adding NDS Container Administration”

Determining Dial Access Attributes

You can configure RADIUS dial access attributes for a Dial Access Profile object, an Organization or Organizational Unit container object, and a User object. The effective dial access attributes are determined as follows:

- Dial Access Profile objects are used to control defined services used by many users.
- The Organization/Organizational Unit Dial Access Services pages provide a way to define default dial access properties for all users in the selected container (but not for users in organizational units that are at a lower level in the Directory tree).
- User object attributes are used to supplement or modify profiles for data that is user-dependent.

For example, you might have a PPP Dial Access Profile object defined for all users, a default Dial Access System object defined for all users in an Organizational Unit container object, and a unique IP address defined in each User object.

A remote user specifies a Dial Access Profile by adding a prefix to the username with the name of the service. For example, user RJONES has two Dial Access Profiles: PPP and Telnet. If the user logs in as TELNET:RJONES, the user will receive the Telnet service.

User-specific attributes supplement the attributes specified in the Dial Access Profile, except when an attribute that can appear only once is specified. In that case, the user-specific attribute takes precedence. For example, you create a PPP Dial Access Profile for your users that specifies a Virtual Private Network (VPN) connection (tunnel) to your corporate network. The default tunnel termination point is directed to your corporate headquarters in Chicago, but your eastern region sales representative has a user-specific tunnel termination point directed to the tunnel to your eastern office.

The RADIUS server filters out attributes that do not apply to the network access server that has requested access for a user. For example, if a RADIUS server responds to a Shiva network access server, only generic RADIUS dial access attributes and Shiva-specific attributes will be returned to the network access server. Attributes for other vendor-specific features that appear in the Dial Access Profile will not be returned. In this way, one Dial Access Profile can contain vendor-specific attributes for a variety of vendors.

Refer to *Novell BorderManager Authentication Service Installation and Setup* for information about setting up dial access attributes for a Dial Access System object, Dial Access Profile object, or User object.

Related Topics

“Planning Dial Access Services”

“Adding NDS Container Administration”

Planning RADIUS Proxy

The RADIUS server provided with Novell® BorderManager™ Authentication Service can act as both a conventional RADIUS server and a RADIUS proxy server at the same time.

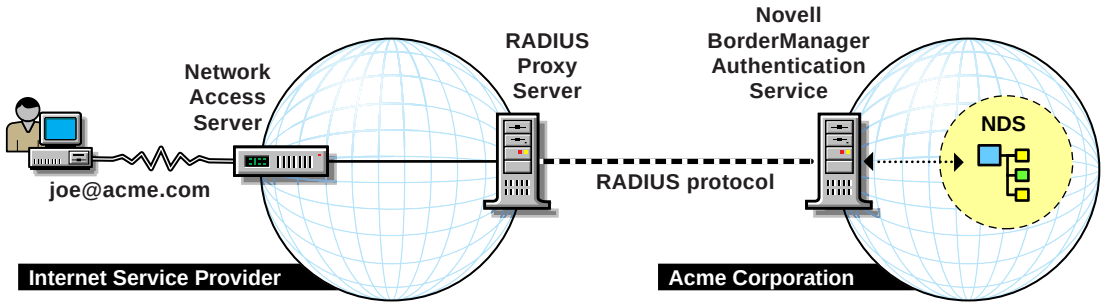
You can use RADIUS proxy to outsource the management of dial-in hardware to an Internet Service Provider (ISP) while you manage the

users in your NDS™ tree. This benefit provides you with the flexibility to manage dial-in users without the investment in dial-in hardware.

Using RADIUS proxy, a remote user (such as jane@acme.com) dials in to an ISP network. The user's access request (user ID and password) is forwarded to a RADIUS proxy server on the ISP network. The ISP RADIUS proxy server forwards the access request to your company's RADIUS server. The RADIUS server then checks the information in the access request and either accepts or rejects the request. If the RADIUS server accepts the request, it returns configuration information specifying the type of connection service (such as PPP or Telnet) to deliver to the user.

This concept is shown in Figure 2-1

Figure 2-1
RADIUS Proxy



To set up a RADIUS proxy, you must first configure a RADIUS proxy server to act as a RADIUS client. Your RADIUS server can also be configured to act as a RADIUS proxy server in a proxy chain if you configure other RADIUS servers as proxy targets.

You can configure a chain of multiple RADIUS proxy servers from which access requests are forwarded. The last RADIUS server in a chain of proxies must have a proxy target that causes the domain name to authenticate to <THIS NDS TREE> or the local IP address the RADIUS server.

Example 1—Separate Dial Access System Objects

There are separate Dial Access System objects for two RADIUS servers: RAD1 that serves the domain acme.com and RAD2 that serves the domain comp.com.

The proxy configuration for RAD1 is as follows:

Domain	Proxy Target
acme.com	IP address of RAD1 or <THIS NDS TREE>
comp.com	IP address of RAD2

The proxy configuration for RAD2 is as follows:

Domain	Proxy Target
acme.com	IP address of RAD1
comp.com	IP address of RAD2 or <THIS NDS TREE>

Example 2—Shared Dial Access System Object

There is a single Dial Access System object for two RADIUS servers: RAD1 that serves the domain acme.com and RAD2 that serves the domain comp.com. The proxy target <THIS NDS TREE> is not used.

The proxy configuration for RAD1 is as follows:

Domain	Proxy Target
acme.com	IP address of RAD1
comp.com	IP address of RAD2

The proxy configuration for RAD2 is as follows:

Domain	Proxy Target
acme.com	IP address of RAD1
comp.com	IP address of RAD2

Related Topics

“Understanding RADIUS Proxy”
“Planning Dial Access Services”
“Adding RADIUS Proxy”

chapter 3

Managing Novell BorderManager Authentication Service

Novell® BorderManager™ Authentication Service is ready for use after you have installed the software and set up the default configuration. You can customize BorderManager™ Authentication Service to your network requirements with the tasks in the following table.

Task	Topic
Configuring dial-in access for all users in an NDS™ Organization or Organizational Unit object	“Adding NDS Container Administration”
Configuring dial-in access from an Internet Service Provider (ISP)	“Adding RADIUS Proxy”
Configuring a RADIUS accounting server	“Maintaining RADIUS Accounting”

Adding NDS Container Administration

You can specify common dial access properties for all users in Organization or Organizational Unit container objects. You use the Dial Access Service page of an Organization or Organizational Unit to

- Enable dial access services for all users
- Select the Dial Access System object for all users
- Configure dial access services that can be used by all users in a container

Adding Dial Access Services for Users in an NDS Container Object

To enable dial access services for users in a container object, complete the following steps:

1. **From the administration workstation, run NetWare® Administrator.**
2. **Select the container object (Organization or Organizational Unit) for which you want to enable dial access for users.**
3. **Select Dial Access Services.**

   The Dial Access Services property page appears.
4. **Check Dial Access.**
5. **Select a Dial Access System object.**
6. **If desired, select additional configured services and attributes.**
7. **Click OK twice.**

Related Topics

“Planning Dial Access Services”
“Determining Dial Access Attributes”

Adding RADIUS Proxy

To set up RADIUS proxy, you must perform the following tasks from NetWare® Administrator:

- Configure a RADIUS server as a proxy client
- Specify a RADIUS proxy server as a proxy target

Configuring a RADIUS Client

To configure a RADIUS client, complete the following steps:

1. **From the administration workstation, run NetWare Administrator.**

2. **Select a Dial Access System object that you already created.**

   The Dial Access System dialog box appears.

3. **Select the Clients property page to configure the RADIUS server of the ISP as a proxy client.**

4. **Select Add to add a RADIUS client.**

   The Configure Client dialog box appears.

   4a. Enter the IP address of the RADIUS server of the proxy RADIUS server (such as an ISP RADIUS server) in the Client Address field.

   4b. Select a client type (default: Generic RADIUS).

   Do not select Generic RADIUS as a client type if you require vendor-specific attributes. You must select a specific vendor to obtain those attributes that it supports.

   4c. Enter the RADIUS secret. Reenter the secret.

   The secret should be a random string of 20 to 30 alphanumeric characters. The secret protects the authentication information sent across the network.

   4d. Check Add Another Client if you want to add another ISP RADIUS server after you create this one. Leave this check box unchecked if this is the last (or only) RADIUS client you will create.

   4e. Click OK twice.

Specifying a Proxy Target

To specify a proxy target, complete the following steps:

1. **Select Proxy Targets to specify a RADIUS proxy target.**
2. **Select Add to add a proxy target.**

   The Configure Proxy Target dialog box appears.

   2a. Enter the domain name of the proxy target.

   2b. Select a proxy target from the list or enter its IP address. Select <This NDS Tree> if the proxy target is the last RADIUS server in the proxy chain.

   2c. Enter the RADIUS secret. Reenter the secret.

   The secret should be a random string of 20 to 30 alphanumeric characters. The secret protects the authentication information sent across the network.

   2d. Check Add Another Proxy Target if you want to add another proxy target after you created this one. Leave the check box unchecked if this is the last (or only) proxy target that you will create.

   2e. Click OK twice.

Related Topics

“Understanding RADIUS Proxy”
“Planning RADIUS Proxy”

Maintaining RADIUS Accounting

By default, Novell® BorderManager™ Authentication Service starts with the authentication server and accounting server enabled. The default settings for the accounting server are as follows:

- Files are located in the following directories:
  - SYS:\ETC\RADIUS\ACCT for NetWare® servers (version 4.11 or later)

- C:\NOVELL\RADIUS\ACCT for Windows NT servers (version 4.0 or later)

- UDP port for RADIUS accounting is 1813.
- File format for RADIUS accounting is comma-delimited text.
- Rollover period for RADIUS accounting files is daily.

You can change the default values from the command line of a NetWare server or a Windows NT server.

The naming of the accounting log file takes the form

YYYYMMDD.DAT

where *YYYY* represents the year, *MM* represents the month, and *DD* represents the day (such as 19981120.DAT for an accounting log file created on November 20, 1998). Naming files using this convention keeps log files to a manageable size and enables you to group accounting information by month, week, or day.

Changing RADIUS Server Options from NetWare

To change RADIUS server options from the NetWare server command line, complete the following steps:

Procedure

1. **If BorderManager Authentication Service is running, type the following command from the system console:**

   UNLOAD RADIUS

2. **Enter the following command from the system console:**

   LOAD RADIUS
   [name = <Dial Access System distinguished name>]
   [password = <Dial Access System password>]
   [acctPath = <RADIUS accounting directory>]
   [acctPort= <UDP port for RADIUS accounting>]
   [fileFormat = [standard|comma]]
   [rollOver = [daily|weekly|monthly]]
   [serverType = [accounting|authentication]]

3. **Select BorderManager Authentication Service as the window to view.**

4. **Enter the distinguished name of the Dial Access System object (if you did not specify it on the command line).**

5. **Enter the dial access password for the Dial Access System object you specified (if you did not specify it on the command line).**

Changing RADIUS Server Options from Windows NT

To change RADIUS server options from the Windows NT server command line, complete the following steps:

1. **Select Settings from the Start menu.**

2. **Select Control Panel.**

3. **Select Services.**

4. **Select BorderManager Authentication Service from the Services list.**

5. **Click Stop if BorderManager Authentication Service is running.**

6. **Click Startup.**

7. **Enter a username to be used with BorderManager Authentication Service in the Log On As field.**

8. **Enter a valid password.**

9. **Select Automatic from the Startup Type list.**

10. **Enter any of the following options in the Startup Parameters field:**

```
[name = <Dial Access System distinguished name>]
[password = <Dial Access System password.]
[acctPath = <RADIUS accounting directory>]
[acctPort = <UDP port for RADIUS accounting>]
[fileFormat = [standard|comma] ]
```

```
[rollOver = [daily|weekly|monthly] ]
[serverType = [accounting|authentication] ]
```

11. **Click Start.**

Related Topics

“Understanding RADIUS Accounting”
“Understanding the RADIUS Protocol”
“Command Line Options”

appendix A RADIUS Status Messages

The Novell® BorderManager™ Authentication Service status display provides status messages that are helpful in troubleshooting user access problems. You can display the status display in the following ways:

- From the NetWare® (version 4.11 or later) server console, enter the following commands to control the status display:

```
RADIUS display {on|off}
RADIUS display {+|-} {failure|success}
RADIUS SystemLog {on|off}
RADIUS SystemLog <file_location>
RADIUS SystemLogSize <new_size>
RADIUS SystemLogPolicy [daily|weekly|<days>]
RADIUS LogStatus
```

- From the Windows NT server, select the System Log tab page in the Service Control Manager.

When a BorderManager™ Authentication Service server is started, the status window displays only messages for authentication failures. Descriptions of failure messages are listed in the following categories:

- Access Rejected Messages
- Messages Dropped Messages
- Other Messages

Each message is listed with the possible causes.

Access Rejected Messages

No such user

Possible causes:

- User object does not exist.
- Lookup context does not exist.
- User entered the username incorrectly (distinguished name syntax error).
- Dial Access System does not have Browse and Read rights to the User object.

No such profile

Possible cause is that the Dial Access System object does not have Browse and Read rights to the Dial Access Profile object.

User not enabled for RADIUS login

Possible causes:

- Dial access is disabled on the User object.
- Dial access is disabled on the container object for a User object using the container setting.
- Dial Access System object does not have Browse and Read rights to the User object or container object.

Invalid password

Possible causes:

- User entered the wrong password.
- Shared secret does not match between the network access server and the RADIUS server. The shared secret is case-sensitive.
- Client workstation attempted to authenticate using CHAP but the password policy was set to use an NDS™ password (CHAP authentication requires a separate dial access password).

No such proxy target

Possible cause is that no entry exists in the proxy target page for the domain that the user entered.

No such service tag

Possible cause is that no service is defined for the User or container object that matches the service tag entered by the user.

Proxy rejected

Possible cause is that the target RADIUS server rejected the authentication request. Consult the output of the final RADIUS server in the proxy chain to determine the problem.

Login disabled

Possible cause is that the user NDS account has been disabled on the login restriction page.

Password expired

Possible cause is that the NDS password has expired.

User not a member of dial access system

Possible causes:

- Dial Access System object does not have Browse and Read rights to the User object or container object.
- Dial Access System object has not been specified for the User or container object.
- User or container object has been configured to use a different Dial Access System object.

Message Dropped Messages

Unknown RADIUS client

Possible cause is that no entry exists in the Dial Access System client table for the RADIUS client that issued the access request.

Proxy loop detected

Possible cause is that the chain of proxy RADIUS servers has been configured in a loop. A loop is an invalid configuration. Check your proxy target configuration to ensure that no loops occur.

Other Messages

RADIUS Error -150

Insufficient Memory

Possible cause is that a system error has occurred (sufficient memory was not available to satisfy the current memory allocation request).

RADIUS Error -307

Missing NDS™ Replica

Possible cause is that the NDS replica that the RADIUS server is using failed.

RADIUS Error -801

Insufficient Buffer

Possible cause is an internal failure (the system allocated a buffer of insufficient size).

RADIUS Error -802

Invalid Request

Possible cause is that an invalid request was received.

RADIUS Error -803

No Such Attribute

Possible causes:

- A requested RADIUS attribute was not found.

- An invalid attribute was detected in an incoming RADIUS message.

RADIUS Error -804

Invalid Data

Possible cause is that malformed data was detected in the NDS directory.

RADIUS Error -805

Invalid Transport

Possible cause is that the host system is not configured properly for TCP/IP.

RADIUS Error -806

Invalid Signature

Possible cause is that the signature on a proxy reply message is invalid.

RADIUS Error -807

Invalid Data Version

Possible cause is that unknown data was found in the NDS directory.

RADIUS Error -808

Proxy Loop Detected

Possible cause is that the chain of proxy RADIUS servers has been configured in a loop. A loop is an invalid configuration. Check your proxy target configuration to ensure that no loops occur.

RADIUS Error -809

Invalid Parameter

Possible cause is that an invalid parameter value was specified.

appendix B Command Line Options

You can specify options for Novell® BorderManager™ Authentication Service on the command line of a NetWare® server (version 4.11 or later) or when starting BorderManager™ Authentication Service as a Windows NT service (version 4.0 or later).

NetWare Command Line Options

The command line syntax for loading Novell® BorderManager™ Authentication Service on a NetWare® server is as follows.

```
LOAD RADIUS
[name = <Dial Access System distinguished name>]
[password = <Dial Access System password>]
[threads = <number of threads>]
[port = <UDP port number for RADIUS>]
[acctPath = <RADIUS accounting directory>]
[acctPort= <UDP port for RADIUS accounting>]
[fileFormat = [standard|comma] ]
[rollOver = [daily|weekly|monthly] ]
[serverType = [accounting|authentication] ]
```

All parameters are optional. The values you specify override the default values.

If you do not specify the name or password on the command line, you will be prompted to provide a name and password at startup. Names can be specified as relative distinguished names, distinguished names, or partial distinguished names. Both typed and typeless names are supported. Refer to the NDS™ documentation for details on specifying names.

The default context is set to the current bindery context. After BorderManager™ Authentication Service has been loaded, it sets the default context to the Dial Access System name context.

Strings with embedded spaces must be contained in quotation marks. In addition, a quoted parameter must be preceded with a space.

The valid values for the number of threads range between 1 and 127. The default number of threads is 5, which should be satisfactory in most cases.

The default User Datagram Protocol (UDP) port number is 1645 (the most commonly used). However, a new UDP port number (1812) has been assigned by the Internet Engineering Task Force (IETF) for RADIUS services.

The default path for the RADIUS accounting files is SYS:\ETC\RADIUS\ACCT.

The RADIUS accounting server is typically implemented as a separate process of the RADIUS authentication server. The RADIUS accounting server listens on UDP port number 1813. When an accounting packet is received from a RADIUS client (such as a network access server), the RADIUS accounting server logs the information in an ASCII text file and returns an acknowledgment to the RADIUS client.

The default RADIUS accounting file format is comma-delimited text (standard ASCII file format is optional).

The default period before a RADIUS accounting file is rolled over is daily (weekly and monthly are optional).

By default, the BorderManager Authentication Service software runs both the authentication server and the accounting server when you do not specify the ServerType option on the command line (running just the authentication server or the accounting server is optional).

Windows NT Command Line Options

The following command line options can be specified when Novell® BorderManager™ Authentication Service is loaded from the Startup Parameters field in the Services control panel of a Windows NT server:

```
[name = <Dial Access System distinguished name>]
[password = <Dial Access System password>]
[threads = <number of threads>]
[port = <UDP port number for RADIUS>]
```

```
[acctPath = <RADIUS accounting directory>]
[acctPort = <UDP port for RADIUS accounting>]
[fileFormat = [standard|comma] ]
[rollOver = [daily|weekly|monthly] ]
[serverType = [accounting|authentication] ]
```

All parameters are optional The values you specify override the default values.

If you do not specify the name or password on the command line, you will be prompted to provide a name and password at startup. Names can be specified as relative distinguished names, distinguished names, or partial distinguished names. Both typed and typeless names are supported. Refer to the NDS™ documentation for details on specifying names.

The default context is set to the current bindery context. After BorderManager Authentication Service has been loaded, it sets the default context to the Dial Access System name context.

Strings with embedded spaces must be contained in quotation marks. In addition, a quoted parameter must be preceded with a space.

The valid values for the number of threads range between 1 and 127. The default number of threads is 5, which should be satisfactory in most cases.

The default User Datagram Protocol (UDP) port number is 1645 (the most commonly used). However, a new UDP port number (1812) has been assigned by the Internet Engineering Task Force (IETF) for RADIUS services.

The default path for the RADIUS accounting files is C:\NOVELL\RADIUS\ACCT.

The RADIUS accounting server is typically implemented as a separate process of the RADIUS authentication server. The RADIUS accounting server listens on UDP port number 1813. When an accounting packet is received from a RADIUS client (such as a network access server), the RADIUS accounting server logs the information in an ASCII text file and returns an acknowledgment to the RADIUS client.

The default RADIUS accounting file format is comma-delimited text (standard ASCII file format is optional).

The default period before a RADIUS accounting file is rolled over is daily (weekly and monthly are optional).

By default, the BorderManager Authentication Service software runs both the authentication server and the accounting server when you do not specify the ServerType option on the command line (running just the authentication server or the accounting server is optional).

RADIUS Status Display Options

A separate display now displays RADIUS status messages for NetWare® servers. You can enter the following RADIUS commands from the RADIUS server console to control the status display:

RADIUS display {on|off}	Turns the status display on or off
RADIUS display {+|-} {failure|success}	Displays failures or successes

At startup, the status display displays messages for authentication successes and failures. When configuring Novell® BorderManager™ Authentication Service, you might find it useful to display messages for just authentication failures by entering the following command from the NetWare server console:

```
RADIUS display -success
```

The RADIUS audit log is a disk file that contains the system messages that are displayed in the RADIUS status display console. The RADIUS audit log is typically used for troubleshooting.

You can enter the following RADIUS commands from the RADIUS server console to control the audit log file:

RADIUS SystemLog {on|off}	Turns the RADIUS audit log file on or off
RADIUS SystemLogInterval <Interval>	Specifies the number of days that the RADIUS audit log file should be maintained (zero disables logging)

RADIUS LogStatus	Displays the current settings for the RADIUS audit log file

The RADIUS audit log file contains the system messages that are displayed on the status display (successes or failures). The status display is not required to be open in order for messages to be logged to the audit log file.

The RADIUS server maintains an audit log file for the number of days specified as the log interval (starting at the time that logging started). After the specified interval, the RADIUS server deletes the first file that is older than the starting date.

For example, if the log interval is set to 7 days and the logging started on January 22, 1998, the RADIUS server will delete the audit log file for January 22, 1998, on January 29, 1998, and create the file 19980129.log.

If the log interval is reduced, the RADIUS server reduces the number of audit log files. The RADIUS server also checks and deletes older files every time it is loaded, as well as when the date changes at midnight.