DigitalNetworks

Remote Access Security Server Installation Guide

Part Number: IG-DRAS0-00

November 2004

This book describes how to install the Digital Networks Remote Access Security Server software.

www.digitalnetworks.net

Trademarks

The following are third-party trademarks:

Adobe, Acrobat, and Acrobat Exchange are trademarks of Adobe Systems Incorporated.

3Com is a registered trademark of 3Com Corporation.

Cisco is a trademark of Cisco Systems, Inc.

HP is a registered trademark of Hewlett-Packard Corporation.

OpenView is trademark of International Business Machines Corporation.

TME 10 is a registered trademark of Tivoli Systems, Inc.

Windows NT and Internet Explorer are trademarks and Microsoft; Windows, Windows 95, and MS-DOS are registered trademarks of Microsoft Corporation.

Novell and NetWare are registered trademarks and NMS are trademarks of Novell, Inc.

Unicenter is a registered trademark and TNG is a trademark of Computer Associates International, Inc.

Pentium is a registered trademark of Intel Corporation.

Netscape is a registered trademark of Netscape Communications Corporation

Java is a trademark or registered trademark of Sun Microsystems, Inc.

VAX and OpenVMS are trademarks of Compaq Computer Corporation.

All other trademarks and registered trademarks are the property of their respective holders.

Contents

Preface

Chapter 1   Installation

Appendix A   DRAS Server Initialization File

This guide explains how to install the Digital Networks Remote Access Security Server (DRAS) software for the following operating systems:

- Microsoft Windows NT
- Microsoft Windows 9x, 2000 (management utility only)
- OpenVMS
- Tru64 UNIX

Intended Audience

This guide is written for system or network administrators responsible for managing remote access network devices and remote access network connections.

Structure of This Guide

This guide is organized as follows:

Chapter/ Appendix	Title	Description
Chapter 1	Installation	Provides instructions for installing the Digital Networks Remote Access Security Server software on systems that run Microsoft Windows NT, Microsoft Windows 9x, 2000, OpenVMS, or Tru64 UNIX operating systems.
Appendix A	DRAS Server Initialization File	Describes the [Storage], [Server], [Policy], and [Ports] sections of the DRAS Server initialization file.

Conventions

This document uses the following symbol:
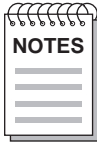
NOTES

***Note** symbol. Calls the reader's attention to any item of information that may be of special importance.*

The following typographical conventions are used:

Convention	Description
italics	Italic text in commands indicates variables for which you must supply a value.
`monospace`	Monospaced text in command examples indicates system output.
boldface	Boldface text in command examples indicates commands that you enter.

Related Documentation

All documentation is located on our web site, see accessing online information.
All documentation also resides on CD (CD-DNAS0-00).

Part Number	Title	Description
IG-DSC04-00	DECserver ConX^4 and ConX^{4P} Installation and User's Guide	Describes how to install, cable and use the ConX^4 and ConX^{4P}.
IG-DSRVW-00	*DECserver 716 and 732 Installation and User's Guide*	Describes how to install, cable and use the DECserver 716 and DECserver 732.
QS-DSRVW-00	*DECserver 716 and 732 Quick Start Card*	Describes how to install, cable and use the DECserver 716 and DECserver 732.
IG-DCSRV-00	*DECserver 90M+ Installation & Users Guide*	Describes how to install, cable and use the DECserver 90M+.
IG-DSRVZ-00	*DECserver 900TM Installation & Users Guide*	Describes how to install, cable and use the DECserver 900TM.
MG-DNAS0-00	*Network Access Software Management Guide*	Provides instructions on how to manage the Network Access Software.
CG-DNAS0-00	*Network Access Software Command Reference Guide*	Lists commands used with the Network Access Server.
PG-DNAS0-00	*Network Access Software Problem Solving Guide*	Describes how to troubleshoot problems while using the Network Access Software.
IG-DNAS0-00	*Network Access Software Installation Guide*	Provides how to install the Network Access Software.
RN-DNAS0-00	*Network Access Software Release Notes*	Documents any release consideration, restrictions, and conditions for the Network Access Software.
IG-DRAS0-00	*Remote Access Security Server Installation Guide*	Provides instructions on how to install the Remote Access Security Server.
MG-DRAS0-00	*Remote Access Security Server Management Guide*	Provides instructions on how to manage the Remote Access Security Server.

Accessing Online Information

Documentation Comments

Digital Networks prides itself on responding to customer needs. To continue serving you, we need your comments. If you find errors in a document or want to make comments, please E-mail your comments to:

TechnicalSupport@digitalnetworks.net

Support Services

To locate product-specific information and warranty information, refer to the following Digital Networks web sites:

www.digitalnetworks.net

To contact us by mail:

Digital Networks
20 N. Wentworth Avenue
Londonderry, NH 03053

To contact us by phone:

U.S. and Canada (603) 216-6000
Europe +44 (0) 1256-855-600

Installation

Overview

In This Chapter

This chapter provides instructions about installing the Digital Networks Remote Access Security (DRAS) software on systems that run Microsoft Windows NT or Windows 9x, 2000 operating systems.

Software Components

The following table lists the software components that the DRAS installation procedure installs:

For This Operating System:	The Procedure Installs:
Microsoft Windows NT	DRAS Server software and the DRAS Manager (the management utility)
Microsoft Windows 9x, 2000	DRAS Manager (the mangement utility)
OpenVMS	DRAS Server software and the unsupported command line manager utility
Tru64 UNIX	DRAS Server software

Release Notes

Each installation kit contains release notes. The release notes contain additional technical information that is not currently in the documentation. Please read the release notes before you install the DRAS software.

Microsoft Windows NT and Windows 9x, 2000 Installation

Preparing for Installation

The following table lists the prerequisites for installing the DRAS software on a Microsoft Windows NT or Windows 9x, 2000 system:

For This:	You Need This for the DRAS Server:	And This for the DRAS Manager:
Operating system	Windows NT Version 3.51, 4.0, or higher	Either of the following: • Windows NT Version 3.51, 4.0, or higher • Windows 9x, 2000
Memory	32 MB	32 MB
Disk space for files	Database files can vary depending on activity. See the Release Notes or README.TXT file for details.	Database files and user cache size can vary depending on activity. See the Release Notes or README.TXT file for details.
System setup	TCP/IP stack installed and running.	TCP/IP stack installed and running.

Special Note About DHCP Clients

Do not install the DRAS Server software on a Windows NT system that is a DHCP (Dynamic Host Configuration Protocol) client. A DHCP server can assign a different IP address to the DHCP client each time the client requests an IP address. This can cause problems with accessing the DRAS Server.

Installing the Software

To install the software, do the following:

Step	Action
1	Insert the DRAS installation CD into your CD-ROM drive and run the appropriate SETUP.EXE file using the Program Manager or the Start menu: • If installing on a Windows NT or Windows 9x, 2000 Intel system, run \DRAS\WINNT\I386\SETUP.EXE. • If installing on a Windows NT Alpha system, run \DRAS\WINNT\ALPHA\SETUP.EXE. **Example**: Use the following path to install the DRAS software on a Windows NT Intel system in which drive D is the CD-ROM drive. D:\DRAS\WINNT\I386\SETUP.EXE If this is a new installation or if you want to install DRAS into a different directory, reboot your system before proceeding.
2	To initialize your DRAS Server's database, go to the DRAS installation directory and run the setupDb command line utility from a console window. Enter your management station's Internet address and its secret when prompted. The installation procedure creates a database that contains: • An administration group object named Admin. • A users group object named Users. • An administrator user object. The procedure prompts you to enter a user name and password. • A client object for a management station. • Authentication objects for the standard authentication methods.

Installing DRAS as an NT Service

After installing the DRAS software, install DRAS as an NT service. Use the following command in the NT console window:

c:\> **Drassrv install**

Starting the DRAS Server

After you install the DRAS Server as an NT service, do the following to start a DRAS Server at any time:

Step	Action
1	Open the Control Panel.
2	Run the Services application.
3	Select Remote Access Security from the displayed list.
4	Click Start to start the DRAS service.

Modifying Startup Parameters

When you install DRAS as an NT service, the startup type is set to manual. Use the Services application to modify the DRAS startup parameters if you want DRAS to start automatically each time the system boots.

Starting the DRAS Manager

To start the DRAS Manager, click on the DRAS Manager icon in your DRAS program group. Refer to the *Remote Access Security Server Management Guide* for details about using the DRAS Manager or see the DRAS Manager's online help.

Environment Variables

The installation procedure defines the following environment variables:

Variable	Description
DRAS_DIR	Defines the full path where the DRAS Server stores its database files. **Default Path**: \DRAS
DRAS_CALLOUT	Defines the full path where the DRAS callout DLL files reside. **Default Path**: \DRAS

Using HOST Authentication on Windows NT Domain Controllers

If you install the DRAS Server on a Windows NT server that is a primary domain controller, you must change the account of any local user that is authenticated by HOST authentication:

Step	Action
1	From the Programs menu, select Administrative Tools and then User Manager.
2	Click User and then New Local Group... from the menu.
3	Create a new group named "DRAS Users".
4	Click Policies and then User Rights from the menu.
5	Select "Log on locally" from the drop-down list box.
6	Add the right to the DRAS Users group.
7	Select the user accounts from which you will interactively run the DRAS Server and add them as members of the DRAS Users group.

See the *Remote Access Security Server Management Guide* for more information about HOST authentication.

Running DRAS in Console Trace Mode on Windows NT

To perform host authentication on Windows NT while running in interactive trace mode, you must use an account with the privilege to act as part of the operating system:

Step	Action
1	From the Programs menu, select Administrative Tools and then User Manager.
2	Click User and then New Local Group... from the menu.
3	Create a new group named "DRAS Server".
4	Click Polices and then User Rights from the menu.
5	Check the Show Advanced User Rights check box.
6	Select "Act as part of the operating system" from the drop-down list box.
7	Add the right to the DRAS Server group.

Step	Action
8	Select the user accounts from which you will interactively run the DRAS Server and add them as members of the DRAS Server group.
9	Log out and then log on to enable the new privileges.

Running the DRAS Server in Debug Trace Mode

You can run the DRAS Server from the console in debug trace mode. The trace often provides sufficient information to solve authentication and remote management connection problems. You can also verify that the server is able to start and initialize. To run trace mode:

Step	Action
1	Stop the server if it is running as a service.
2	Make sure the environment variable DRAS_DIR points to the location of the DRAS database files.
3	Go to the DRAS installation directory.
4	Start the server using the following command: > **drassrv console 5**

You can view more detailed trace information using a trace level of 6, 7, or 998.

Files Installed on Windows NT Systems

The following table lists the files that the installation procedure installs:

File Name	Description
Files in \DRAS	
README.TXT	Release Notes
DRASSRV.EXE	DRAS Server executable
DRASMAN.EXE	DRAS Manager executable
DRASMAN.HLP	DRAS Manager online help
DRASRC.DLL	DRAS Manager Windows resources

File Name	Description
DRASCOAR.DLL	Accounting database interface
DRASCOUR.DLL	User and server database interface
DRASCOSP.DLL	Static password authentication module
DRASCOWW.DLL	WatchWord authentication module
DRASCOCH.DLL	CHAP authentication module
DRASCODS.DLL	Defender authentication module
DRASCOHP.DLL	Host password authentication module
DRASCOSD.DLL	SecurID authentication module
DRASCOSK.DLL	OTP authentication module
SETUPDB.EXE	SetupDb utility
DRAS.INI	Initialization file
Files in %SystemRoot%\System32	
ADVAPI32.DLL	API for NT system services
GRID32.OCX	Access Hour grid control
MFC40.DLL	Microsoft Foundation Class library, Version 4.0
MFC42.DLL	Microsoft Foundation Class library, Version 4.2
MSVCRT.DLL	Microsoft Visual C++ Run Time library
MSVCIRT.DLL	Microsoft Visual C++ library
OLEPRO32.DLL	Specific OLE grid control
REGSVR32.EXE	Creates entries in the Windows Registration Database

Files Installed on Windows 9x, 2000 Systems

The following table lists the files that the installation procedure installs:

File Name	Description
Files in \DRAS	
README.TXT	Release Notes
DRASMAN.EXE	DRAS Manager executable
DRASMAN.HLP	DRAS Manager online help
DRASRC.DLL	DRAS Manager Windows resources
DRASCOAR.DLL	Accounting database interface
DRASCOUR.DLL	User and server database interface
DRASCOSP.DLL	Static password authentication module
DRASCOWW.DLL	WatchWord authentication module
DRASCOCH.DLL	CHAP authentication module
DRASCODS.DLL	Defender authentication module
DRASCOHP.DLL	Host password authentication module
DRASCOSD.DLL	SecurID authentication module
DRASCOSK.DLL	OTP authentication module
SETUPDB.EXE	SetupDb utility
DRAS.INI	Initialization file
Files in %SystemRoot%\System32	
ADVAPI32.DLL	API for NT system services
GRID32.OCX	Access Hour grid control
MFC40.DLL	Microsoft Foundation Class library, Version 4.0
MFC42.DLL	Microsoft Foundation Class library, Version 4.2
MSVCRT.DLL	Microsoft Visual C++ Run Time library
MSVCIRT.DLL	Microsoft Visual C++ library
OLEPRO32.DLL	Specific OLE grid control
REGSVR32.EXE	Creates entries in the Windows Registration Database

Deinstallation

To remove the DRAS software, do the following:

Step	Action
1	Bring up the Control Panel.
2	Click Add/Remove Programs.
3	Click Digital Networks Remote Access Security Server from the list of programs.
4	Click the Add/Remove... button to remove the software.

OpenVMS Installation

Before You Install

The following table lists the prerequisites required for installing the DRAS software on an OpenVMS system:

For This:	You Need This on VAX Systems:	And This on Alpha Systems:
Operating System	OpenVMS 6.2 or higher	OpenVMS 6.2 or higher
Minimum disk space	1000 blocks	1700 blocks

Management

To manage the DRAS server on an OpenVMS system, install the DRAS Manager on a Windows NT or Windows 9x, 2000 system.

Installing the Software

To install the DRAS software on an OpenVMS system, do the following:

Step	Action
1	Log in to the SYSTEM account.
2	Insert the CD into your CD-ROM drive and mount it using the following command: **$ MOUNT ddcu: DNAS0nn /MEDIA=CD** The *ddcu:* variable is the CD-ROM drive. When you mount the CD-ROM drive, you can access the [DRAS.OPENVMS] directory that contains the DRAS kit for OpenVMS.
3	If you previously installed the DRAS software, terminate any active DRAS servers. Enter the following: **$ @SYS$MANAGER:DRAS$SHUTDOWN**
4	Run the VMSINSTAL procedure: **$ @SYS$UPDATE:VMSINSTAL DRAS0*nn* ddcu: OPTIONS N** where ***nn*** is the current version number
5	Follow the instructions that the DRAS installation procedure provides.

Initial Database

During installation, the procedure prompts you to enter information it needs to create the initial DRAS server database. The installation procedure populates the database with:

- An administration group object (default name is ADMIN).

- A users group object (default name is USERS).

- An administrator user object (default name is SYSTEM). The installation procedure prompts you to enter a password.

- Authentication objects for the standard authentication methods.

- A client object for a management station.

You can select the default names for these objects or enter different ones during the installation.

Logicals

The installation procedure defines the following logicals:

Logical	Description
DRAS$DIR	DRAS$DIR Defines the full path where the DRAS server stores its database files. **Default Path**: SYS$COMMON:[SYSEXE]
DRAS$COxx	DRAS$COxx Defines the full path where the DRAS callout images reside. **Default Path**: SYS$COMMON:[SYSLIB]

Starting the DRAS Server

Type the following at the DCL prompt:

@SYS$STARTUP:DRAS$STARTUP

Running the DRAS Server in Debug Trace Mode

You can run the DRAS server from the console in debug trace mode. The trace often provides sufficient information to solve authentication and remote management connection problems. You can also verify that the server is able to start and initialize.

To run trace mode:

Step	Action
1	Stop the server if it is running as a detached process.
2	Make sure the logical name DRAS$DIR resolves to the location of the server database files.
3	Define DRAS$TRACE_LEVEL as 5.
4	Start the server using the following command: **> $ MCR DRAS$SERVER**

You can view more detailed trace information using a trace level of 6, 7, or 998.

Files Installed

The OpenVMS installation kit contains executable images for OpenVMS Alpha and OpenVMS VAX systems. During installation, the procedure installs the correct files for the system on which you are installing the software.

The following table lists the files that the installation procedure installs:

File Name	Description
Files in DRAS$DIR	
DRAS$CONFIG.INI	Initialization file
Files in SYS$COMMON:[SYSMGR]	
DRAS$SYSTARTUP.COM	DRAS$SYSTARTUP.COM Secondary startup command procedure
DRAS$REGISTER_COS.COM	DRAS$REGISTER_COS.COM Authentication method registration procedure
DRAS$RUN.COM	DRAS$RUN.COM Secondary startup command procedure
DRAS$SHUTDOWN.COM	DRAS$SHUTDOWN.COM DRAS server shutdown command procedure
Files in SYS$COMMON:[SYSHLP]	
DRAS0nn.RELEASE_NOTES	Release Notes

File Name	Description
Files in SYS$COMMON:[SYSEXE]	
DRAS$SERVER.EXE	DRAS server executable
DRAS$MANAGER.EXE	Management utility executable
DRAS$CONFIG.INI	Initialization file
Files in SYS$COMMON:[SYSLIB]	
DRAS$COARSHR.EXE	Accounting database interface
DRAS$COCHSHR.EXE	CHAP authentication module
DRAS$COSPSHR.EXE	Static password authentication module
DRAS$COURSHR.EXE	User and server database interface
DRAS$COWWSHR.EXE	WatchWord authentication module
DRAS$COHPSHR.EXE	Host password authentication module
DRAS$COSDSHR.EXE	SecurID authentication module
DRAS$CODSSHR.EXE	Defender authentication module
DRAS$COSKSHR.EXE	OTP authentication module
Files in SYS$COMMON:[SYS$STARTUP]	
DRAS$STARTUP.COM	DRAS startup command procedure
Files in SYS$SYSROOT:[SYSTEXT]	
DRAS$IVP.COM	DRAS Installation Verification

True UNIX Installation

Introduction

To manage the DRAS server on a Tru64 UNIX system, install the DRAS Manager on a Windows NT or Windows 9x, 2000 system.

Installing the Software

To install the DRAS software on a Tru64 UNIX system (Version 3.2 or higher), do the following:

Step	Action
1	Log in as root or super user, and go to the root directory.
2	Insert your CD into your CD-ROM drive and mount it using the following command: **% mount -rt cdfs -o noversion,rrip /dev /dir** The */dev* variable is the CD-ROM drive, the /dir variable is the kit directory name. The rrip option instructs the operating system to use the Rock Ridge extensions on the CD-ROM. If you omit the rrip option, you cannot install DRAS. The DRAS directory of the CD-ROM includes OVMS, WINNT and Tru64_UNIX directories. (This is because the CD-ROM is in ISO-9660 format). The Tru64_UNIX directory contains a dras0nn_install directory (where nn is the version number) which the setld command uses to install DRAS.
3	Access the CD-ROM mounted directory: **# cd /dev/DRAS/Tru64_UNIX/dras0*nn*-install** where ***nn*** is the current version number
4	Install the kit by entering the following command: **# setld -l .**

Step	Action
5	Enter the management station's Internet address and its secret when prompted. The installation procedure creates a database that contains: • An administration group object (default name is Admin). • A users group object (default name is Users). • An administrator user object. The procedure prompts you to enter a user name and password. • A client object for a management station. • Authentication objects for the standard authentication methods. You can select the default names for these objects or enter different ones during the configuration.
6	If necessary, install the libcxx.so shareable object library. DRAS for Tru64 UNIX uses the libcxx.so shareable object library that is shipped with the operating system, which may not be installed on your system. On Tru64 UNIX V3.n systems, libcxx.so is in the optional subset CXXSHRDA30n. On Tru64 UNIX V4.0 systems, libcxx.so is in the mandatory subset OSFBASE400 (CXXSHRDA130 on DEC OSF/1 Version 1.3 systems and CXXSHRDA131 on Version 2.0 systems).

Environment Variables

The DRASD start/stop script defines the following environment variables:

Variable	Description
DRAS_DIR	Defines the full path where the DRAS server stores its database files. **Default Path**: /usr/opt/dras/database
DRAS_CALLOUT	Defines the full path where the DRAS callout images reside. **Default Path**: /usr/opt/dras/callout
DRAS-TRACE_LEVEL	Defines the trace level when the DRAS server is running. **Default Path**: 5

Starting the DRAS Server as a Console

Do the following to start the DRAS server as a console:

Step	Action
1	Log in as root or user with permission to access the DRAS server database.
2	Enter the following command: **# DRASD console**

The DRAS server starts when you reboot the system.

Starting the DRAS Server as a Daemon

Do the following to start the DRAS server as a daemon:

Step	Action
1	Log in as root or user with permission to access the DRAS server database.
2	Enter the following command: **# DRASD start**

The DRAS server starts when you reboot the system.

Running the DRAS Server in Debug Trace Mode

You can run the DRAS server from the console in debug trace mode. The trace often provides sufficient information to solve authentication and remote management connection problems. You can also verify that the server is able to start and initialize.

To run trace mode:

Step	Action
1	Stop the server if it is running as a daemon.
2	Make sure the environment variable DRAS_DIR points to the location of the server database files.
3	Start the server using the following command: **> # DRASD console** The DRAS_TRACE_LEVEL environment variable contains the trace level and the default 5.

You can view more detailed trace information using a trace level of 6, 7, or 998.

Stopping the DRAS Server

Do the following to stop the DRAS server:

Step	Action
1	Log in as root or user with permission to access the DRAS server database.
2	Enter the following command: **# DRASD stop**

Files Installed

The following table lists the files that the installation procedure installs:

File Name	Description
Files in /usr/opt/dras	
dras0nn.links (see Note)	Installation/deinstallation script
dras0nn.release_notes (where nn is the current version number)	Release Notes
Files in /usr/opt/dras/bin/	

File Name	Description
drasserver	Server executable
setupdb	SetupDb utility
DRASD	Start/stop script
Files in /usr/opt/dras/callout	
drascoar.so	Accounting database interface
drascour.so	User and server database interface
drascosp.so	Static password authentication module
drascoww.so	WatchWord authentication module
drascoch.so	CHAP authentication module
drascohp.so	Host password authentication module
drascosd.so	SecurID authentication module
drascosk.so	OTP authentication module
drascods.so	Defender authentication module
Files in /usr/opt/dras/database	
drasconfig.ini	Initialization file

Notes About the Directory Structure

Keep the following in mind:

- All files in /usr/opt/dras/bin are soft-linked into /usr/sbin, which is the standard system executables directory.

- All shareable objects (.so files) are soft-linked into /usr/shlib, which is the default share library search path.

- Database files are located in /usr/opt/dras/database.

Deinstallation

To remove the DRAS software, do the following:

Step	Action
1	Log in as root or super user.
2	Deinstall the software by entering the following command: **# setld -d DRAS0***nn* where ***nn*** is the current version number

Postinstallation

Introduction

Ensure that your RADIUS clients are configured properly for RADIUS and IP operations. See the documentation for your clients for details.

Configuring Access Server Units

To configure the access server unit, use access server console commands or the access server Manager. See the *Network Access Software Management Guide* or the *Network Access Software Installation Guide* for more information. The following table illustrates how to create a basic RADIUS configuration using the access server console commands:

Step	Action
1	Define an authentication realm using the same DRAS Server name for both the authentication and accounting host. Use the following command syntax: Local> **CHANGE RADIUS REALM realm-name SECRET "secret_string" AUTHENTICATION HOST ACCOUNTING HOST radius_host** **Example**: Local> **CHANGE RADIUS REALM SISKO SECRET "OBRIEN" AUTHENTICATION HOST ACCOUNTING HOST OBRIEN.MMG.ORG.COM**
2	Set one or all ports to use the new authentication realm. Use one of the following command syntaxes: Local> **DEFINE PORT ALL AUTHENTICATION ENABLED** Local> **DEFINE PORT port-number AUTHENTICATION ENABLED**
3	Verify the realm setting. Use the following command syntax: Local> **SHOW RADIUS**
4	Log in to the selected port using RADIUS authentication. Use the following command syntax (user names and passwords are case sensitive): Username> username@realm-name Password> password **Before Logging In**: Define the appropriate user accounts in the DRAS Server database. See the *Remote Access Security Server Management Guide* or the DRAS Manager online help for details.
5	Verify the port authorization settings. Use the following command syntax: Local> **SHOW PORT AUTHORIZATION**

Registering Access Server Clients

Register access server clients by their network IP addresses, even if the access servers are registered on a name server. An access server identifies itself in a RADIUS packet using the NAS-IP-Address attribute. The DRAS Server does not translate the IP address to a host name.

Troubleshooting Management Connection Failures

The following is a checklist to help determine why an attempt to create a management link between a workstation running the DRAS Manager and a remote system running a DRAS Server may fail.

Step	Action
1	Verify that the remote DRAS Server is running.
2	Verify that the management station is registered correctly as a client in the DRAS Server database. The management station name must be either the full system and domain name, or the client's IP address. You can use the domain name if your client is registered in a domain naming system. Otherwise, use the client's IP address as the name. The database must also contain the correct client secret for the management station and the client must be enabled. To check the client registration, use the DRAS Manager to examine the "Local Database" entry for the client.
3	Verify that the remote management user is registered correctly in the DRAS Server database. A user that requests a remote management connection must be registered in the DRAS Server database with Administrator privilege. The Administrator privilege is assigned to a group and applies to each user that is a member of the group. The user must have PASSWORD authentication selected. Make sure that the user is enabled and the password has not expired. Note that case sensitivity can cause problems, particularly with cross-platform connections.

DRAS Server Initialization File

Overview

In This Appendix

This appendix describes the following sections of the DRAS Server initialization file:

- [Storage] Section
- [Server] Section
- [Policy] Section
- [Ports] Section

Initialization File Description

File Names

The DRAS installation procedure installs a server initialization file in the same directory where you install the DRAS data files. For OpenVMS systems, this is the location that the DRAS$DIR logical name defines. On all other platforms, this is the directory that the DRAS_DIR environment variable defines.

The following table lists the initialization file name for each software platform:

Platform	Initialization File Name
Tru64 UNIX	drasconfig.ini
OpenVMS	DRAS$CONFIG.INI
Windows NT and Windows 9x,me,2000	DRAS.INI

Initialization File Example

The following example shows the initialization file from a Tru64 UNIX system. The following sections explain each part of the example.

Tru64 UNIX drasconfig.ini File

The following example shows a DRAS initialization file for a system running the Tru64 UNIX operating system. This file specifies the default values.

! Tru64 UNIX drasconfig.ini file

[storage]

userdb=/usr/opt/dras/database/drasusers

usercallout=/usr/opt/dras/callout/drascour.so

serverdb=/usr/opt/dras/database/drasdb

servercallout=/usr/opt/dras/callout/drascour.so

accountingdb=/usr/opt/dras/database/drasaccounting

accountingcallout=/usr/opt/dras/callout/drascoar.so

[server]

RadiusThreads=3

AccountingThreads=3

MaxConsecutiveRejects=5

[policy]

NoLoginSession=Continue

NoFramedSession=Continue

NoCallbackNumber=Continue

BlankPassword=Reject

NoAuthentication=Reject

[ports]

Radius=1645

Accounting=1646

Management=1645

[Storage] Section

Description

The entries in the [Storage] section specify the location of the DRAS data files (excluding the initialization file).

Entry Descriptions

The following table describes the entries in the [Storage] section:

Entry	Default Value	Description
userdb	• OpenVMS: DRAS$DIR:DRAS$USERS.DAT • Windows NT: %DRAS_DIR%DRASUSRS.* • Tru64 UNIX: %DRAS_DIR%drasusers.*	Defines the location of the DRAS user database.
usercallout	• OpenVMS: DRAS$COUR • Windows NT: %DRAS_CALLOUT%DRASCOUR.DLL • Tru64 UNIX: %DRAS_CALLOUT%cmancour.so	Defines the location of the user database interface routines. For Windows NT and Tru64 UNIX: If the DRAS_CALLOUT environment variable has no definition, the DRAS software looks for the images in the directory to which DRAS_DIR points.
serverdb	• OpenVMS: DRAS$DIR:DRAS$DB.DAT • Windows NT: %DRAS_DIR%DRASDB.* • Tru64 UNIX: %DRAS_DIR%drasdb.*	Defines the location of the server database.
servercallout	• OpenVMS: DRAS$COUR • Windows NT: %DRAS_CALLOUT%DRASCOUR.DLL • Tru64 UNIX: %DRAS_CALLOUT%drascour.so	Defines the location of the server database interface routines. For Windows NT and Tru64 UNIX: If the DRAS_CALLOUT environment variable has no definition, the DRAS software looks for the images in the directory to which DRAS_DIR points.

Entry	Default Value	Description
accountingdb	• OpenVMS: • DRAS$DIR:DRAS$ACCOUNTING.DAT • Windows NT: • %DRAS_DIR%DRASACCT.DAT • Tru64 UNIX: • %DRAS_DIR%drasaccounting.dat	Defines the location of the accounting database interface routines.

accounting callout	• OpenVMS: DRAS$COAR
	• Windows NT:
	  %DRAS_CALLOUT%DRASCOAR.DLL
	• Tru64 UNIX:
	  %DRAS_CALLOUT%drascoar.so
		Defines the location of the server database interface routines.
		For Windows NT and Tru64 UNIX: If the DRAS_CALLOUT environment variable has no definition, the DRAS software looks for the images in the directory to which DRAS_DIR points.

[Server] Section

Description

The entries in the [Server] section control the DRAS Server operation.

Entry Descriptions

The following table describes the entries in the [Server] section:

Entry	Default Value	Description
RadiusThreads	3	Defines the number of worker threads that the server creates to handle RADIUS requests.
AccountingThreads	3	Defines the number of worker threads that the server creates to handle RADIUS accounting requests.
MaxConsecutiveRejects	5	Defines the number of consecutive access rejects allowed for a user before the DRAS Server disables the user object.

[Policy] Section

Description

The entries in the [Policy] section determine whether the DRAS Server rejects a user's request for access when it cannot find expected information in the user database.

Policy Entry Values

Policy entries have a value of Reject or Continue:

- A policy entry value of Reject indicates that the DRAS Server controls acceptance or rejection of a user's access request.

- A policy entry value of Continue indicates that the RADIUS client controls acceptance or rejection of a user's access request.

Entry Descriptions

The following table describes the entries in the [Policy] section:

Entry	Default Value	Description
BlankPassword	Reject	Defines the policy for access requests that contain a blank or null password. **Recommendation**: Allowing users to be authenticated without a password is a security risk. Therefore, It is recommended that you set this policy to Reject. **Note**: Setting this policy to Reject does not affect users who have an authentication method that allows them to supply a blank password. In this case, the authentication method usually supplies an alternate challenge. An example of this is WatchWord authentication.
NoAuthentication	Reject	Defines the policy for access requests from users for whom no authentication method is set. **Recommendation**: Allowing a user access to the network without authentication is a security risk. Therefore, It is recommended that you set this policy to Reject.
NoCallbackNumber	Continue	Defines the policy for a user whose entry in the user database includes a service type of Callback, but not the expected session definitions.

Entry	Default Value	Description
NoFramedSession	Continue	Defines the policy for a user whose entry in the user database includes a service type of Framed, but not the expected session definitions.
NoLoginSession	Continue	Defines the policy for a user whose entry in the user database includes a service type of Login, but not the expected session definitions.

[Ports] Section

Description

The entries in the [Ports] section indicate the UDP ports on which the DRAS Server listens for RADIUS and RADIUS-Accounting packets.

Entry Descriptions

The following table describes the entries in the [Ports] section:

Entry	Default Value	Description
RADIUS	1645	The UDP port on which the DRAS Server listens for RADIUS packets. The default value is the value that the RADIUS Draft Specification defines. To ensure compatibility with RADIUS clients, It is recommended that you do not change this value.
RADIUS Accounting	1646	The UDP port on which the DRAS Server listens on for RADIUS-Accounting packets. The default value is the RADIUS port number plus one. To ensure compatibility with other RADIUS clients, It is recommended that you use caution if you change this value.
Management	1645	The TCP port on which the DRAS Server listens for remote management connections. To ensure compatibility with other RADIUS clients, It is recommended that you use caution if you change this value.