



Gradient® DCE and DFS for Compaq® Tru64™UNIX®

Release Notes

Software Version 4.2

Notices

Gradient DCE and DFS for Tru64UNIX Release Notes - Software Version 4.2 - Revised May 2002

THIS DOCUMENT AND THE SOFTWARE DESCRIBED HEREIN ARE FURNISHED UNDER A SEPARATE LICENSE AGREEMENT, AND MAY BE USED AND COPIED ONLY IN ACCORDANCE WITH THE TERMS OF SUCH LICENSE AND WITH THE INCLUSION OF THE COPYRIGHT NOTICE BELOW. TITLE TO AND OWNERSHIP OF THE DOCUMENT AND SOFTWARE REMAIN WITH ENTEGRITY SOLUTIONS CORPORATION AND OR ITS LICENSOREES.

The information contained in this document is subject to change without notice.

ENTEGRITY SOLUTIONS MAKES NO WARRANTY OF ANY KIND WITH REGARD TO THE SOFTWARE, DOCUMENTATION AND THIS MATERIAL, INCLUDING BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE.

Entegrity Solutions shall not be liable for errors contained herein, or for any direct or indirect, incidental, special or consequential damages in connection with the furnishing, performance, or use of this material.

Use, duplication or disclosure by the Government is subject to restrictions as set forth in Entegrity's standard commercial license agreement and is commercial computer software and documentation pursuant to Section 12.212 of the FAR and 227.7202 subparagraph (c) (1) (i) of the Rights in Technical Data and Computer Software clause at DFARS 252.227-7013.

Entegrity, Entegrity Solutions, and Gradient are registered trademarks of Entegrity Solutions Corporation. NetCrusader is a trademark of Entegrity Solutions Corporation.

Compaq, TruCluster, and AlphaServer are registered trademarks of Compaq Computer Corporation. Tru64 is a trademark of Compaq Computer Corporation. The the names of other Compaq products referenced herein are trademarks or service marks, or registered trademarks or service marks, of Compaq Computer Corporation.

Kerberos is a trademark of Massachusetts Institute of Technology. UNIX is a registered trademark of The Open Group. The Open Group is a registered trademark of The Open Group. DCE is copyrighted by The Open Group and other parties. Other products mentioned in the document are trademarks or registered trademarks of their respective holders.

Portions of this documentation were derived from materials provided by Entrust Technologies Limited.

Copyright © 1991–2002 The Open Group

Copyright © 2002 Entegrity Solutions Corporation & its subsidiaries.

All Rights Reserved.

Entegrity Solutions Corporation, 2077 Gateway Place, Suite 200, San Jose, CA 95110, USA

Notices ii

Section 1. Introduction 5

Section 2. New Features v4.2 6

- Platforms supported 6
- Updated RPC Interface Specification 6
- SIA 6
- Security 6
- DFS 6
- Internal Nodes 6
- DCE Runtime 7

Section 3. Problems Fixed v4.2 8

- Kerberos Tools 8
- DFS 8

Section 4. Known Problems and Restrictions v4.2 9

- Versions 9
- Applications Need Rebuilding 9
- Internal Nodes Support for Sierra Cluster 9
- getpwuid interface for DCE SIA 9
- DCE SIA must be disabled before deleting DCE runtime 10
- DFS 10
- dced 10
- dcecp: Security with Replica 11

Section 5. Previous Releases 11

- 5.1 New Features (Previous Releases) 11
 - 5.1.1 New Features v4.1 11
 - Tru64 UNIX v5.1 11
 - DFS Support 11
 - RTS, DCE Runtime 11
 - Clusters (Compaq TruCluster and Sierra Cluster) 12
 - KRB5 Library 13
 - Privacy Kit 13
 - 5.1.2 New Features v4.0 13
 - Tru64 UNIX v5.1 13
 - DFS Support 13
- 5.2 Problems Fixed (Previous Releases) 14
 - 5.2.1 Problems Fixed v4.1.4 14
 - Reinstallation Necessary 14
 - cdsadv 14
 - RPC 14

DFS	15
Tru64 and Sierra Cluster: Locks	15
Kernel Assert Failures	15
DFS Kernel pthread routines	16
secd - Security Server	16
5.2.2 Problems Fixed v4.1.3	16
5.2.3 Problems Fixed v4.1.2	17
5.2.4 Problems Fixed v4.1.1	17
5.2.5 Problems Fixed v4.1	17
DFS	17
RTS DCE SIA	18
DCE Runtime	18
CDS Advertiser	18
5.2.6 Problems Fixed v4.0	19
CDS Client Access	19
dcesetup	19
DFS	19
Kerberos Configuration Tool (kcfg)	20
randd (v5.1 systems only)	20
rshd	20
Security Server	20
5.3 Configuration Notes (Previous Releases)	21
5.3.1 Configuration Notes v4.0	21
DFS	21
Kerberos Tools	21
5.4 Known Problems and Restrictions (Previous Releases)	22
5.4.1 Known Problems and Restrictions v4.1.4	22
HP OpenView	22
Cluster: DFS Cache Directory	22
Cluster: Clobbering DFS	22
5.4.2 Known Problems and Restrictions v4.1	23
DFS	23
DMS Dataless Management System	23
Installation	23
Sierra Cluster	23
5.4.3 Known Problems and Restrictions v4.0	23
DFS for Tru64 UNIX v5.1 Was Not Supported	23
DFS Cache Manager Hangs	23
DECnet	24
Error Condition on DCE Client	24
dced	24
Stack Sizes	24
fts command	24
dcecp	25
Split Server Configuration	25
Configuring a Security Server Replica	25
passwd_export Command	25
Kerberos kcfg tool	25
Kerberos rsh tool	26

Kerberos 5 and Kerberos 5 Compliant Utilities	26
CDS	26
Example Programs	26
Public Key Storage Server Does Not Support Security Replicas	26
PKI Components Disabled	26
Thread Stack Overflow Not Reported	27
Use STDERR Instead of STDOUT with dcesetup	27
SIA	27
Change in Reported Zero Divide Exception	27
5.5 Corrections to Documentation (Previous Releases)	28
5.5.1 Corrections to Documentation v4.1	28
5.5.2 Corrections to Documentation v4.0	28
Section 6. Obtaining Technical Support	29
Section 7. Contacting Entegrity Solution	29

Release Notes

1. Introduction

If using Tru64™ UNIX® v5.1A, use Gradient® DCE v4.2.

If using version 5.1, continue to use NetCrusader/DCE 4.1.x. (Note the name change from NetCrusader to Gradient.) Separate documentation is provided for the two product lines. The Release Notes for Gradient DCE v4.2 list the changes in patches 4.1.1, 4.1.2, 4.1.3, and 4.1.4.

The Release Notes contain the following sections:

1. Introduction
2. New Features v4.2
3. Problems Fixed v4.2
4. Known Problems and Restrictions v4.2
5. Previous Releases
6. Obtaining Technical Support
7. Contacting Entegrity Solution

These Release Notes provide release information for Gradient DCE v4.2 software for Tru64 UNIX v5.1A machines.

This document describes new and changed features of Gradient DCE v4.2, as well as corrections to known problems, known problems and restrictions, and corrections to documentation. Similar historical information for v4.1 and v4.0 is provided. Entegrity Solutions® recommends that you read this document before installing and using Gradient DCE software.

NOTE: The products named Gradient DCE, NetCrusader/DCE v3.1 (and higher), Digital® DCE v3.1, and Compaq® DCE v3.1 provide essentially the same features; however, only Gradient DCE, and NetCrusader/DCE function on the Tru64 UNIX v5.x operating system. Although other company names may be referred to within this document (Digital, Compaq, or Gradient Technologies), this DCE product is now produced and supported by Entegrity Solutions® Corporation.

2. New Features v4.2

Platforms supported

Gradient DCE v4.2 runs only on:

	DCE Client	DFS Client	Servers
Tru64 UNIX v5.1A	X	X	X
TruCluster® 5.1A	X		
Sierra Cluster (SC) v2.4	X	X	

Updated RPC Interface Specification

In the prior version, 4.1.4, the RPC runtime library was changed, which required that all images that use the DCE RPC be rebuilt. Therefore, applications need up-to-date versions and need to be rebuilt. See [Known Problems and Restrictions: Applications Need Rebuilding](#).

SIA

DCE SIA was redesigned to:

- Add a mechanism to determine if dced is running and to perform DCE SIA functions, with minimal overhead.
- The DCE SIA entry calls in the `/etc/sia/matrix.conf` file are now enabled/disabled only during initial configuration and at configuration changes. Previously, the DCE SIA entries were added/removed every time DCE was started or stopped, and at configuration changes. All cluster members now use the same matrix.conf file whether or not DCE is operating.
- The CDSL on the `/etc/sia` directory was removed.

Security

The password strength daemon (**pwd_strengthd**) is now included as part of the DCE runtime kit.

DFS

The **tkm_adjust** program is now part of the DFS kit. The program monitors and adjusts token manager settings for DFS servers.

Internal Nodes

Support for Sierra Cluster Internal Nodes is disabled, pending validation with the Compaq Engineering group.

DCE Runtime

The RPC environment variables are now stored in the DCE services file. This eliminates the manual changing of the dcesetup file to support custom configurations.

The following RPC environment variables are supported:

- `RPC_SUPPORTED_NETADDRS`
- `RPC_UNSUPPORTED_NETIFS`
- `RPC_RESTRICTED_PORTS`

To use this new feature:

- 1 Open the file, `/opt/dcelocal/dce_services.db`
- 2 Add the environment variable followed by an equals sign (=) followed by the desired value(s)

Examples for each of the environment variables follow:

- `RPC_SUPPORTED_NETADDRS` — Network addresses to use for RPC communication.

To export and use 10.20.0.100 and 16.96.200.231 as network addresses for RPC communication, place the following line in the DCE services file, with a colon separated list:

```
RPC_SUPPORTED_NETADDRS=10. 20. 0. 100: 16. 96. 200. 231
```

- `RPC_UNSUPPORTED_NETIFS` — Network interface names that should not be used for RPC communication.

To not use the mc0 and tu1 interfaces, place the following line in the DCE services file, with a colon separated list:

```
RPC_UNSUPPORTED_NETIFS=mc0: tu1
```

- `RPC_RESTRICTED_PORTS` — To restrict the creation of ports used for RPC communication.

The value of the environment variable is defined by the following grammar:

```
<entry> [COLON <entry>]*
<entry> : <protseq_name> LEFT_BRACKET <ranges> RIGHT_BRACKET
<ranges> : <range> [COMMA <range>]*
<range> : <endpoint-low> HYPHEN <endpoint-high>
```

To limit the range of ports used for TCP/IP communications to ports 5000 through 5110, and 5500 through 5521, and UDP/IP communications to ports 6500 through 7000, place the following line in the DCE services file:

```
RPC_RESTRICTED_PORTS=ncacn_ip_tcp[5000-5110, 5500-5521]:ncadg_ip_udp[6500-7000]
```

NOTE: These settings will only affect DCE Runtime Services. To have other applications use these restrictions, the environment variable(s) must be exported prior to running those applications.

3. Problems Fixed v4.2

Problems fixed in previous patches and releases are described in *Section 5.2*.

Kerberos Tools

The Kerberos versions of `ftpd` and `telnetd` now display the proper name for the operating system and DCE. This indicates whether the Tru64 or the Kerberos version of the tool is being executed.

When a connection is made:

- The Kerberos telnet daemon now displays "Gradient DCE Kerberos Telnet for Compaq Tru64 UNIX".
- The Kerberos ftp daemon now displays "FTP Server (Gradient DCE Kerberos FTP for Compaq Tru64 UNIX)".

DFS

dfssetup now properly handles errors when configuring DFS servers that have incorrect device names.

4. Known Problems and Restrictions v4.2

Versions

The 4.2 kit will run only on Tru64 v5.1A, not earlier versions.

Applications Need Rebuilding

Third party DCE based applications or software, such as Hewlett Packard OpenView, that require DCE components, must be up-to-date with this version, and be rebuilt. Versions released in 2002, should have indications that they run on DCE 4.1.4 and 4.2. (There is a backward compatible version of DCE available for the transitional version, 4.1.4, but there are not backward compatible versions for later versions, v4.1.5 upwards, and v4.2.x).

In version, 4.1.4, we corrected a potential problem with internal RPC structures, that could have caused problems with RPC transmission of data. The RPC runtime library was changed, which required that all images that use RPC be rebuilt.

Rebuild all images (including the stub/client code) that depend on DCE, using the DCE 4.1.4 or 4.2 ADK (depending on the version being used).

Internal Nodes Support for Sierra Cluster

Internal nodes support is disabled, pending validation with the Compaq Sierra Engineering Group.

getpwuid interface for DCE SIA

The getpwuid interface of DCE SIA does not work properly with the Tru64 5.1A operating system.

- If DCE SIA is enabled, the dtgreet process will cause a core dump on a standalone system when the system is booted.
- If DCE SIA is enabled on a Sierra Cluster 2.4 system then the system will hang.

Workaround:

This problem can be removed by replacing one line in the **/etc/sia/matrix.conf** file after DCE SIA has been enabled and before the system is rebooted.

(If you forget to change the file and reboot, then you will have to boot the system in single user mode and make the change.)

Change

```
si_ad_getpwuid=(DCE, libdcesiad.so) (BSD, libc.so)
```

to

```
si_ad_getpwuid=(BSD, libc.so)
```

This may cause a problem if groups are defined in the DCE registry that are not in the **/etc/groups** file on the local system.

Entegrity is working closely with the CompaqTru64 Engineering group to resolve this problem.

DCE SIA must be disabled before deleting DCE runtime

Disable DCE SIA before deleting the DCE runtime kit.

If DCE SIA is enabled while you attempt to delete the kit, the following message will be displayed:

```
The DCE SIA library is in the /etc/sia/matrix.conf file.  
Removing the DCE runtime kit with DCE SIA enabled will  
cause the system to behave improperly or hang.
```

```
Please disable DCE SIA by using dcesetup prior to deleting  
the DCE runtime kit.
```

```
The DCE runtime kit will not be deleted.
```

Reenable DCE SIA after the DCE runtime kit is reinstalled.

DFS

For DFS on Sierra Clusters, the DFS cache must be on a locally mounted filesystem.

There is a performance-related problem that occurs with RPC calls from the DFS components within the kernel. This problem is being worked on and will be resolved in a future patch.

dced

dced Daemon Consumes Large Memory Amounts

For configurations with security servers that export DECnet bindings, the dced daemon consumes large memory amounts. This occurs due to a problem in the pe_site update thread that periodically updates the security server binding list in the **/opt/dcelocal/etc/security/pe_site** file. The DECnet bindings are not properly handled and cause a problem with call threads.

Workaround

For **applicable** client configurations, place the following in the **/opt/dcelocal/dce_services.db** file:

```
disable pe_site_update
```

This will disable the thread.

If security servers are added, then the pe_site file should be manually updated with the new binding information.

dcecp: Security with Replica

If the following command sequence is executed, an error is generated:

```
dcecp
```

```
principal show <ajg>
```

This works the first time but not on subsequent events.

Error: No more matching entries even though the principal exists.

Workaround

Use rgy_edit as follows:

- 1 rgy_edit
- 2 do p
- 3 view ajg -f
- 4 view tpb -f

5. Previous Releases

5.1 New Features (Previous Releases)

5.1.1 New Features v4.1

This section describes new and changed features for NetCrusader/DCE v4.1.

Tru64 UNIX v5.1

Tru64 UNIX v5.1 is now a supported operating system. TruCluster 5.1 and Sierra Cluster v2.0 configurations are now supported.

DFS Support

DFS is supported on Tru64 UNIX v5.1 machines and on Sierra Cluster v2.0 configurations. DFS is not supported on TruCluster v5.1.

RTS, DCE Runtime

- Runtime supports more than four network interfaces.
- dce_login now supports -f switch so forwardable credentials can be created. This facilitates the use of Kerberos tools.
- SIA (Security Integrated Architecture) mechanism now supports creation of forwardable credentials.

To enable SIA forwardable credential creation put the following into the /**opt/dcelocal/dce_services.db** file:

enable SIA forward

This change will take place on the next restart of DCE services.

- Added enhanced log messages to the SIA library. To enable logging of SIA messages, perform the following steps:

touch **/opt/dcelocal/var/adm/security/sialog** file

enable SIA forward

The sialog file will contain the output from the SIA DCE logging.

- Creates new directory during installation,
/opt/dcelocal/var/security/keytabs is required by Sierra Clusters v2.0 and is used by its prun in clustered configurations.
- The random number generator daemon (randd) is now disabled for RPC only configurations. The randd daemon is used for the security interfaces, and is not needed for RPC only configurations.

Clusters (Compaq TruCluster and Sierra Cluster)

- Several directories and files need to be member-specific on a TruCluster installation. The following need to be member-specific:

/opt/dcelocal
/krb5
/etc/sia
/etc/krb5.conf

The installation scripts generate Context Dependent Sensitive Links. These CDSLs are symbolic pointers, indicating a member specific configuration in a cluster. Each member (or node or machine) is a DCE client, so in a cluster directory there are member specific pointers.

- V4.1 supports generating forward credentials for DCE-enabled SIA, to provide consistent credentials between cluster members.
- dcesetup is cluster aware.

Dcesetup allows for one time DCE client configuration of all cluster members, as DCE clients using the same configuration information.

For Sierra Clusters, only cluster members that share the same sub-cluster and CFS file system can be configured at the same time. One will have to run dcesetup for each of the subclusters.

- dfssetup is cluster aware.

Dfssetup allows for one time DFS client configuration of all cluster members, as DFS clients using the same configuration information.

For Sierra Clusters, only cluster members that share the same sub-cluster and CFS file system can be configured at the same time. One will have to run dfssetup for each of the subclusters.

KRB5 Library

A new library provides the KRB5 public functions. It will only work with Tru64 5.1, not 5.0 or earlier versions.

The new library is called: **libdcekrb5.so**

Users will need to modify their makefiles to use the new library. The name given does not conflict with other public KRB5 libraries.

Privacy Kit

The Privacy Kit is now part of the Base Kit.

5.1.2 New Features v4.0

This section describes new and changed features for the Previous Release, NetCrusader/DCE v4.0.

Tru64 UNIX v5.1

Tru64 UNIX v5.1 is now a supported operating system.

DFS Support

DFS could work with, but was not supported, on Tru64 UNIX v5.0 and v5.0a.

5.2 Problems Fixed (Previous Releases)

Problems fixed in previous releases are listed in this section, the most recent first.

5.2.1 Problems Fixed v4.1.4

Reinstalling this kit also implements all the changes in the previous patches 4.1.1, 4.1.2 and 4.1.3.

Reinstallation Necessary

Since the DCE runtime was rebuilt, a complete reinstallation is necessary, to obtain the new images and libraries. It is not necessary to reinstall the man pages for DCE, DFS, or the ADK.

To reinstall, follow these steps on the command line:

- 1 Copy the kit, **dce414.tar**, to some location (NOT /tmp)
- 2 # tar -xvf
- 3 # cd output
- 4 # setld -i | grep DCE | grep “_ _installed”

This will give you a list of the installed DCE and DFS kits.

- 5 # setld -d <kits> except man pages
- 6 # setld -l to reinstall the kits

When the DFS binary is installed, the kernel will be rebuilt.

Copy the new kernel to /vmunix.

Be sure the new vmunix is approximately 20MB. If it is only around 15MB, then the DFS option was not built into the kernel.

If this happens, follow the steps in the *Installation and Configuration Guide Section 1.12*.

- 7 If the kernel does not rebuild, follow the steps in the *Installation and Configuration Guide section 1.12*.

cdsadv

Problems were encountered on machines with memory greater than 2 GB. The cdsadv code incorrectly reported back a negative cache size and caused the daemon to core dump.

RPC

We corrected a potential problem with internal RPC structures, that could have caused problems with RPC transmission of data. The RPC runtime library was changed, which required that all images that use RPC be rebuilt.

DFS

- **dfsbind** sometimes failed because threads did not work correctly in the kernel, due to problems with the DFS kernel locking and threads routines. We rewrote the internal DFS locking and threads routines to be threadsafe.
- When an executable image was changed on one machine, other machines would execute the prior version, due to a problem within the token revocation routine. We added code to invalidate the Universal Buffer Cache (ubc) when the token from the server gets revoked. Now all clients run the current, not the cached, executable image.

These three changes above, in RPC and DFS, fixed defects 6608, and 7453 - 7456.

Tru64 and Sierra Cluster: Locks

Fixed a problem where errors were reported that locks were being released when they had not been locked. The problem was related to an inadvertent re-initialization of a DFS kernel lock.

Kernel Assert Failures

Sierra Cluster File System - Revocation

Fixed a CFS recovery lock problem. The Cluster File System (CFS) calls through the Universal Buffer Cache (UBC) ops functions to the DFS cache manager `cm_putpage` function. This could in turn call back into CFS to store code to disk. This produced a recovery lock assertion and executables were not updated.

Other assertions produced include:

- Other locks held (Tru64 and DFS)
- Internal stack corruption

Issues addressed include:

- CFS to DFS to CFS lock issue
- Recursion of trying to free the same block repeatedly

This corrected problems 27224CA, 27388CA and 27393CA.

Tru64 Systems other than Sierra Cluster

Fixed a lock problem. The File System calls, through the UBC to the DFS Vnode which generates a lock thread. The process stopped in a recursive loop and could not get past the lock to write back to the file system.

Assertions include locked, kernel stack violation, and DCE/DFS assert panics.

This corrected problems 27388CA and 27397CA

DFS Kernel pthread routines

Fixed a race condition in a pthread wait routine.

Where a signal to unlock a mutex came in too soon, before a sleep signal was in effect, it caused a race condition. Now the signal arrives after the sleep signal is activated.

Errors listed included: dfs:auth helper not running; DCE errors: DFS, dfsbind; DCE Hang; set auth binding failed, running unauthenticated, LS command hanging, and Node hangs upon login following user/password.

This corrected problems 27197CA, 27242CA, 27350CA and 27390CA

secd - Security Server

A problem was found in configurations with a master and one or more replica security servers. When a principal was removed from a group, the master server crashed and would not properly restart. This was being caused by mapping the change log item to an improper structure when the security change log was being propagated to replica servers. The log item is now mapped to the correct structure and the problem has been corrected.

5.2.2 Problems Fixed v4.1.3

Fixed two problems that occurred when using the Kerberos version of rsh (Restricted Shell).

- The rsh command no longer times out (appears to hang) without completion of the requested command, when running as root. (problem report 27190CA)
- Intermittent data loss, while running rsh, was corrected.

The patch kit replaces rsh and rshd files for:

- NetCrusader/DCE 4.0 for Tru64 5.0 and 5.0a and
- NetCrusader/DCE 4.1 for Tru64 5.1.

It does not apply to version 3.1 or other versions not listed.

NOTE: You will need to obtain a new version of Tru64 rshd from Compaq when they make it available. The existing Tru64 version of rshd also had the same problems.

5.2.3 Problems Fixed v4.1.2

When DCE SIA was disabled, the removal script would sometimes leave the `/etc/sia/matrix.conf` file linked to a nonexistent file (`/etc/sia/bsd_matrix.conf`). Now the insert and remove scripts ensure that the `matrix.conf` file is correctly linked.

The `sec_remove_dce_entires.sh` and `sec_insert_dce_entries.sh` shell scripts have been modified to check for the existence of prior `matrix.conf` files before setting the value of `/etc/sia/matrix.conf`.

The insertion script now copies the current `matrix.conf` file to `matrix.conf.preDCE`.

The removal script now performs the following steps and the new scheme is as follows:

The following items are checked in order. The first match sets the new `matrix.conf` file.

C2 Active	Old matrix.conf file	New matrix.conf file
N/A	<code>matrix.conf.preDCE</code>	<code>matrix.conf.preDCE</code>
Yes	<code>OSFC2_matrix.conf</code>	<code>OSFC2_matrix.conf</code>
Yes	<code>bsd_matrix.conf</code>	<code>bsd_matrix.conf</code>
No	<code>bsd_matrix.conf</code>	<code>bsd_matrix.conf</code>
No	<none of the above>	<code>.proto..matrix.conf</code>

5.2.4 Problems Fixed v4.1.1

Fixed where the cluster install script did not create `cdsl` for `/etc/sia` and `/etc/krb5.conf`.

5.2.5 Problems Fixed v4.1

This section describes problems fixed in NetCrusader/DCE v4.1.

DFS

- In the TruCluster environment, a lock of the time variable caused a system crash. This no longer happens.
- A DFS crash due to a credential pointer not being set has been remedied.
- Kernels now configure properly, with or without specifying the DFS option while building the kernel.

RTS DCE SIA

- The Tru64 version of rsh and Kerberized-rsh programs hung during execution if DCE SIA was enabled. This problem was being caused by a problem with vfork in the C library, where the child process did not inherit properly the parent's process information. The Kerberized -rsh tool has been modified to use fork, and now works properly with DCE SIA enabled.

To use rsh with DCE SIA enabled, use the Kerberized version of rsh found in the **/opt/dcelocal/bin** directory.

- On a multihomed host or a host where the hostname did not match the network name, there was a problem with the Kerberized daemons (rsh, rlogind) that would reject incoming requests. This was partially fixed. Incoming client requests should use the name of the machine as it was configured into the DCE cell, i.e. host name.

Configure these machines using the external network name of the machine in the DCE cell.

- There was a problem with disabling of the DCE SIA mechanism during a system shutdown on machines that did not have an X11 interface running. When the system was rebooted, DCE SIA would still be enabled and the cdsadv daemon would hang while trying to fork and check for existing interfaces via a socket with the dced daemon. The problem was caused by an error in the sec_remove_dce_entries.sh script file. This problem has been fixed.

DCE Runtime

In RPC only configurations, dced would not start and a "Yellow Zone" stack overflow message was reported in the dced.log file. This was an intermittent problem on some systems. The problem was due to an insufficient stack size in the bootstrap_mgmt thread where dced was initializing interfaces. The stack size for this thread has been doubled and the problem is now fixed.

CDS Advertiser

The CDS advertiser daemon (cdsadv) was hanging during some start up sequences. The hang was occurring in DCE cell configurations with one or more CDS replicas. The problem was being caused by a down or unreachable CDS replica. During this time, the internal CDS reader got into a hung state when the command to check for cdsadv daemon was executed. This problem has been fixed.

5.2.6 Problems Fixed v4.0

This section describes problems fixed in NetCrusader/DCE v4.0.

CDS Client Access

Due to a marginal stack size, calls to obtain values from CDS would occasionally result in the call hanging. The stack size has been increased.

dcesetup

- The dcesetup script had some syntax errors that prevented the using of disable capability for randd and the pe_site update thread. The script has been corrected.
- The DCE services and configuration files were being displayed on Tru64 5.0a and higher systems. The dcesetup script has been fixed to send the output to the null device so that the contents are no longer displayed on the screen.
- An error message was being generated on Tru64 5.1 systems during the configuration of KRB services. See *Kerberos Configuration Tool (kcfg)* for more information.
- A timing problem existed on faster machines (500MHz and higher) that caused the dcesetup script to not recognize that the security client had been started. A delay was added between starting the client and checking for its activation.
- A problem existed if the KRB5 tools were configured after client or cell configuration. The problem was due to the nonexistence of sec-admin credentials. A call was made to perform a dce_login to obtain the proper credentials.

DFS

An internal symbol, inet_addr, in the kernel RPC and DFS code caused a symbol collision when trying to build a DFS enabled kernel on Tru64 v5.0 Cluster. A duplicate routine was provided in the **/usr/opt/TCR500/sys/ics_11_tcp.mod** file. The name of the routine was changed to the dce_inet_addr name.

Kerberos Configuration Tool (kcfg)

- The kcfg tool used by dcesetup generated an error message from the `.../rca/internal_binding.c:2664` file. This problem has been fixed by providing the correct binding handle to the `sec_rgy_close` routine.
- The kcfg tool generated an error message from the kill command during configuration of KRB services on Tru64 v5.1 machines. The error message was generated due to an invalid `grep` command when trying to restart the initd daemon. The problem was caused by a change in the naming of forked programs in the `ps` command. A change was made to the program to properly construct the command to send the HUP command to the inetd process after the Kerberos configuration is completed. This enables the Kerberos remote daemons to be properly executed.

randd (v5.1 systems only)

Due to a change in the naming of forked processes, the randd daemon would get started multiple times during the configuration process. This problem has been fixed by altering the way the randd daemon is detected.

rshd

- If SIA was enabled, the rshd daemon would hang during the forking the child process. This problem was caused by an incorrect ordering of calls to the `sia_session_release` and the `geteuid` routines. The order of the calls has been switched and rshd now properly forks the child process.
- Due to missing code in the rshd source file, error messages were not properly sent back to the client's programs. This problem is now fixed and error messages are properly delivered to the client.

Security Server

The dcesetup script appeared to hang when trying to create a security replica on a machine. This happened on machines that were reconfigured into a different cell. The hang occurred because the `/etc/krb5.conf` file was not properly updated. The value for `default_realm` needed to be corrected to have the value of the new DCE cell. This would fix the problem.

5.3 Configuration Notes (Previous Releases)

5.3.1 Configuration Notes v4.0

This section describes additional information to be aware of during configuration.

DFS

The value of the **@SYS** variable was changed from **alpha_OSF1** to **alpha_tru64_v500**. This value now (version 4.0) reflects the version of the operating system. (changed to **alpha_tru64_510** in the current version: 4.1)

Kerberos Tools

A user must have forwardable credentials and use the **-f** switch on **rlogin** and **rsh** to obtain credentials on the remote machine. After logging into DCE, a user needs to obtain forwardable credentials by executing **kinit -f** and providing their password. When the tool is used, the user must provide **-f** as the first parameter and DCE credentials will be obtained when the program is executed.

5.4 Known Problems and Restrictions (Previous Releases)

The following were known problems and restrictions at the times of their respective releases. Many list workarounds.

5.4.1 Known Problems and Restrictions v4.1.4

HP OpenView

Prior versions of HP Open View do not work with this version.

If you are using HP OpenView, you need to obtain the latest build from Entegrity support, **dce414_64bit_if.tar**.

Cluster: DFS Cache Directory

The DFS cache directory **MUST** be placed into a local mounted file system. This is not a concern for standalone machines. However, for cluster machines it is, so the user will have to make sure before configuring DFS in the cluster. The **dfssetup** script will verify that the requested DFS cache directory is a local mounted file system.

While configuring, choose between the defaults:

standalone: **/opt/dcelocal/var/adm/dfs/cache.**
cluster: **/local/dfscache.**

dfssetup now enforces that the DFS cache directory is mounted on a local filesystem for cluster configurations. If the cache directory is not a local filesystem, then DFS will not start when the machine is booted and the following message will be issued:

```
DFS client cache is at <disk cache directory>
```

```
The DFS cache MUST be on a locally mounted filesystem for a cluster configuration. You must reconfigure the client.
```

```
DFS will not be started.
```

Cluster: Clobbering DFS

For cluster configurations, the DFS startup/shutdown scripts are not removed when a single member's DFS configuration is clobbered. This was causing a problem where other cluster members would not start DFS on startup.

If the DFS client configuration is clobbered on a cluster member, the following message is printed:

```
To remove DFS startup/shutdown files for the cluster, run the following commands. Note, that if you are clobbering only some of the cluster members, then issuing these commands will prevent DFS from starting on the other cluster members.
```

```
rm -f /sbin/init.d/dfsstartup  
rm -f /sbin/rc3.d/S67dfs  
rm -f /sbin/init.d/dfsshutdown  
rm -f /sbin/rc0.d/K00dfs  
rm -f /sbin/rc2.d/K00dfs
```

5.4.2 Known Problems and Restrictions v4.1

This section describes problems known in NetCrusader/DCE version 4.1.

DFS

Occasionally, dfsd will hang, causing the system to significantly slow down. The problem is caused by a write lock on a file node in the dfsd

DMS Dataless Management System

Though DMS works with a non-clustered environment, it is not supported in a clustered environment.

Installation

In a Cluster environment, it is recommended that you only install the Run Time Services and Command Reference Manual Pages of the DCE kits. The others might work, but are not fully tested, so are not supported.

Sierra Cluster

Member nodes that do not have external network addresses are not supported.

5.4.3 Known Problems and Restrictions v4.0

This section describes problems known in the previous version, NetCrusader/DCE v4.0.

DFS for Tru64 UNIX v5.1 Was Not Supported

In NC/DCE release NC/DCE v4.0, DFS for Tru64 v5.1 was not supported, due to several internal operating system changes.

In NC/DCE release 4.1, DFS only works on 5.1 machines.

DFS Cache Manager Hangs

Occasionally the DFS cache manager hangs and dfsbind will crash causing a core dump. This problem is being addressed and will be fixed in a subsequent release.

DECnet

When DECnet is installed and configured on a Tru64 v5.1 system, one may get the following error when dced tries to start:

```
2000-12-14-09:00:17.142-05:00I418.531 dced ERROR dhd general main.c 1721 0
x3ffc01b2000
Process (pid 3442) exited with status 0400
```

First, make sure you have the correct version of DECnet installed and configured. If the problem still persists, disable DECnet use from DCE by putting the following into **/opt/dcelocal/bin/dcesetup**:

```
RPC_SUPPORTED_PROTSEQ=ncacn_ip_tcp:ncadg_ip_udp
export RPC_SUPPORTED-PROTSEQ
```

This will eliminate the use of DECnet with DCE.

Error Condition on DCE Client

The following error has been seen while running the machine as a DCE client:

```
cdsclerk (2514) FATAL rpc recv krbclt.c 285
(rpc_krb_get_tkt) Unexpected exception was raised.
```

The client machine's DCE functions still appear to work properly; however, the DTS daemon may hang and require restarting.

dced

If you try to configure DCE before you configure the network on the system, then dced will not start. You will receive the following messages:

```
Init dced
Starting dced...
dced ERROR dhd general main.c 1721
```

If you get this error message, then configure the network first before trying to configure DCE.

Stack Sizes

Due to memory alignment and allocation changes in Tru64 V5.0 and later, problems have been seen with threads due to insufficient stack sizes. Problems that have been seen are "Yellow Zone" stack overflow messages, SEGV exceptions, thread hangs, and thread early termination.

To solve the problem, increase the stack size as needed. This applies to DCE based application programs (not the kernel).

fts command

The system crashes when executing the following **fts** command:

```
fts restart -bosserver -server <bos server>
```

To fix this problem, contact Compaq support to obtain a patch for the `execvp` calls. The problem occurs due to a system crash when a new shell is invoked via one of these calls.

dcecp

The following dcecp commands do not work for this release:

- host configure
- host unconfigure
- cellalias set (disabled)
- cdsalias set (disabled)

Split Server Configuration

Split server configuration using a node running NetCrusader/DCE v4.0 as the Security Server and a node running Transarc or HP DCE V1.3b ECO #2 as the CDS Server is not supported in this release. A DCE Release 1.2.2 system running IBM AIX R1.2.2 cannot be configured in a split cell environment as the Security server if NetCrusader/DCE v4.0 is configured to run the CDS server. This problem will be corrected in a future product release.

Configuring a Security Server Replica

In a mixed version Security server/replica environment, the Security server must be configured at the lowest DCE software revision in use. For example, you cannot configure a Security replica on a DCE for Tru64 UNIX Version 2.x system, if the Security server is running on a NetCrusader/DCE v4.0 system. The Security server must be running the same or lower version of DCE as that running on the Security replica system.

Entropy cannot guarantee that you can configure a security replica on a NetCrusader/DCE v4.0 system when the Security server runs on another vendor's DCE Release 1.2.2 system. Conversely, it may not be possible to configure a security replica on another vendor's DCE Release 1.2.2 system when the Security server runs on a NetCrusader/DCE v4.0 machine. This problem will be corrected in a future product release.

passwd_export Command

When the execution of the **passwd_export** command is interrupted, this process leaves the **/etc/passwd** and the **/etc/group** in an unusable state.

Kerberos kcfg tool

The **/etc/krb5.conf** configuration file does not always get properly reset when a machine is reconfigured into a different cell or into its own cell. The Kerberos tools will return an error message stating that the remote server returns a "Wrong principal in request" error message. You need to manually edit the **/etc/krb5.conf** file to correct the following item:

```
default_t_realm=<current cell>
```

Enter the value of your current cell name after the equal sign with no spaces.

Kerberos rsh tool

Permission denied errors come to various sources. First, the **/opt/dce/bin/rsh** image should reside in the **/usr/bin** directory with permissions of 4755 (note that the system bit is enabled) and the file owner should be **root:bin**. Also, it is suggested that you copy the operating system's version of the program to a safe location. These steps also apply to the other Kerberos client programs such as **rlogin** and **telnet**.

Kerberos 5 and Kerberos 5 Compliant Utilities

- The NetCrusader/DCE v4.0 implementation of Kerberos 5 does not interoperate with generic Kerberos. Therefore, if a generic version of Kerberos is installed on your system, remove it before installing NetCrusader/DCE v4.0. This problem will be corrected in a future product release.
- If you use the operating system's version of the **rlogin** and **rsh** tools without proper DCE credentials, you will receive a Permission Denied error. If you want to use the tools without DCE credentials, instead use **/usr/bin/rlogin** and **/usr/bin/rsh**. This problem will be corrected in a future product release.

CDS

The command **dcecp -c clearinghouse disable ./clearinghouse** renders the CDS server "Unable to Communicate." As a Workaround you can recreate the clearinghouse and then issue a **dcecp -c clearinghouse delete** command.

Example Programs

There is no README file associated with the DTS examples.

Public Key Storage Server Does Not Support Security Replicas

The Public Key Storage Server (PKSS) was not designed to support Security Replicas as stated in the non-goals section of the PKSS RFC (RFC 94.0) from The Open Group. The **dcesetup** program does not allow you to configure a PKSS in a client and/or security replica environment.

PKI Components Disabled

The PKI, public key, components have been disabled internally. The **pkss** server can be configured but will not properly operate due to the RSA library being removed from the library.

If you need PKI capability, please contact Entegrity Solutions.

Thread Stack Overflow Not Reported

Calling the **sec_login_valid_from_keytable** routine from a thread (as is commonly done in a server's refresh identity thread) may result in a silent thread stack overflow, a SEGV, and a memory fault (core dump). This problem can be avoided by using the **pthread_attr_setstacksize** routine to increase the thread's stack size.

Increasing the stack size to 65536 bytes corrected the stack overflow problem in our test case.

Use STDERR Instead of STDOUT with dcesetup

The dcesetup utility uses output from dcecp commands to verify that certain interfaces are running. When Serviceability via the routing file is turned on, dcesetup can successfully bring up all the daemons only if STDERR is specified instead of STDOUT.

SIA

- If you have just enabled SIA on the system, reboot the machine as soon as possible. If you attempt an operation that performs a login function, such as **rlogin**, then the machine will crash. Further, you will have to manually recreate the **matrix.conf** file from one of the prototype files in **/etc/sia**.
- DCE SIA on Tru64 UNIX does not properly charge usage against the product license. With DCE SIA enabled, the available license count is decremented when a non-root user logs in, but is not incremented when the user logs out. On a machine without an unlimited user license, the available license count will eventually be consumed. This problem will be fixed in a future release of the Tru64 UNIX operating system. Currently, the following Workarounds are available:
 - Disable DCE SIA before the problem occurs.
 - Reboot the machine whenever the license count is exceeded.
 - Perform all logins as **root**, with a subsequent **su** to the desired user.
 - Obtain an unlimited user license.
- When DCE SIA is used to obtain a local user's group membership list, the list of group uids obtained from the DCE Registry is not processed against the group override file.

Change in Reported Zero Divide Exception

The reported exception for dividing a number by zero has changed due to a change in the operating system reporting mechanism. The following table lists the reported exceptions for dividing by zero.

exc_e_aritherr	0 / 0
exc_c_fltdiv	x / 0 (where x != 0)

5.5 Corrections to Documentation (Previous Releases)

5.5.1 Corrections to Documentation v4.1

This section updates the documentation for the *NetCrusader/DCE v4.1 Installation and Configuration Guide* and for the *NetCrusader/DCE v4.1 Distributed File Service (DFS) Configuration Guide*.

There are no corrections at this time.

5.5.2 Corrections to Documentation v4.0

The following documentation problems have been noted in the DCE manpages:

- Some manpages incorrectly state that the startup scripts are located in **/etc/rc.d**. The correct location for the startup scripts is **/sbin/rc3.d**
- The manpage for **rpc_mgmt_ep_elt_inq_begin** is not displayed correctly.

6. Obtaining Technical Support

If you purchased your Gradient product directly from Entegriety Solutions Corporation or Gradient Technologies, Inc. you are entitled to 30 days of limited technical support beginning on the day the product is expected to arrive.

You may also purchase a support plan that entitles you to additional services. You *must* register prior to receiving this support. For details, refer to the customer support information package that accompanied your shipment or refer to the Technical Support area of <http://support.entegriety.com>. The web site also contains online forms for easy registration.

If you purchased Gradient DCE 4.2 from a reseller, please contact the reseller for information on obtaining technical support.

7. Contacting Entegriety Solution

Contact	Address	Phone/Fax/Email
DCE Product and Sales Information	Entegriety Solutions Corporation 410 Amherst Street, Suite 150 Nashua, NH 03063 USA	Email: DCESales@entegriety.com Web: www.entegriety.com Telephone and Fax: Tel: +1 (508) 624-9600 Tel: (US Only): 1-800-525-4343 Fax: +1 (508) 229-0338
All Other Product and Sales Information Requests	Entegriety Solutions Corporation 2077 Gateway Place, Suite 200 San Jose, CA 95110 USA	Email: info@entegriety.com Web: www.entegriety.com Telephone and Fax: Tel: +1 (408) 487-8600 Tel: (US Only): 1-866-487-8600 Fax: +1 (408) 487-8610
Technical Support	Entegriety Solutions Corporation Technical Support 2 Mount Royal Ave. Marlborough, MA 01752 USA	Tel: +1 (508) 229-0239 Tel: (US Only): 1 (888) 368-3555 Fax: +1 (508) 229-0338 Email: support@entegriety.com http://support.entegriety.com
Documentation Comments and Suggestions		Email: docs@entegriety.com
Other Inquiries	Entegriety Solutions Corporation 2077 Gateway Place, Suite 200 San Jose, CA 95110 USA	Tel: +1 (408) 487-8600 Fax: +1 (408) 487-8610 Email: info@entegriety.com http://www.entegriety.com