DCE and DFS for HP® Tru64® UNIX®

Release Notes

Software Version 4.3.2

Notices

DCE and DFS for Tru64UNIX Release Notes - Software Version 4.3.2 - Revised May 2005

Entegrity Solutions Corporation, 410 Amherst Street, Suite 150, Nashua, NH 03063, USA

Contents

Release Notes

1. Introduction

This set of Release Notes provides release information for DCE and DFS v4.3.2 software for Tru64 UNIX v5.1B machines.

Entegrity DCE version 4.3.2 runs on Tru64™ UNIX® v5.1B through v5.1B-2 (PK4) only.

Entegrity DFS version 4.3.2 runs on Tru64 v5.1B through v5.1B-1 (PK2) only — DFS is not supported on Tru64 5.1B-2 (PK4). If you want to run Entegrity DFS, you should not upgrade to PK4.

If you want to upgrade to PK4, note that you must first uninstall DFS before you can upgrade.

- If you are using Tru64 v5.1A, continue to use Entegrity DCE v4.2.x.
- If you are using Tru64 v5.1, continue to use DCE v4.1.x. (For that release, the product was referred to as NetCrusader/DCE.)

This set of Release Notes contains the following sections:

This document describes new and changed features for the current release, 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 DCE software.

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

2. New Features v4.3.2

There are no new features in this release.

3. Problems Fixed v4.3.2

Kerberos Tools

- Included KRB 2004-002 patch changes which fixes problems with double freeing of data elements.

DCE setup

- Fixed a problem in dcesetup with CDS advertiser shared memory segments where if cdsadv had been killed rather than shut down properly, the old shared memory segment was not removed. After several shutdowns of cdsadv, the allocated shared memory segments would be exhausted and DCE would not start. This has been fixed by correcting the dcesetup script to properly remove both the shared memory segments and semaphores.
- Fixed a problem where the RPC environment variables were not utilized for RPC-only configurations. The dcesetup script has been modified to read the values from the configuration database and properly export the values to the DCE environment.

RPC Library

- Fixed a problem with TCP RPC packets where the reference count was being dropped inadvertently. Under high system loading conditions, this would cause exceptions.
- Incorporated security fix sec_patch_04302004 which fixed a potential buffer overrun.
- Fixed a problem with a call receiver thread waiting indefinitely if the call had been cancelled. Without the fix, the process would either run out of threads that could be allocated or would exceed its quota on memory due to too many threads running (since the threads would never terminate).
- Fixed a problem with previously cancelled and destroyed calls being cancelled under high system loading conditions.
- Fixed a problem with missed RPC call thread cancellations under high load situations.
- Improved the RPC-level debugging messages by adding thread identifiers to the messages.
- Added proper error handling for unexpected RPC call signals that were causing the internal global RPC lock to either remain in a locked state (which hung the image) or to prematurely terminate the image.

- Added proper recovery action for illegal state changes in the RPC state model. The illegal state changes were causing some images to prematurely terminate under incorrect RPC packet data.
- Enabled RPC mutex-level tracing to RPC-level debugging. Also added in recording of the thread that last locked the mutex.
- Fixed a problem where multiple threads were competing for a single RPC address structure.

RPC

- Fixed a problem that caused early program termination when successive BIND packets were received on open RPC connections. The connection is now terminated and the program continues to function as normal.

Evaluation Kit

- Fixed a problem where the kernel would not build if the DFS evaluation kit was installed. The problem was shown as a missing symbol. The symbol reference has been removed.

DCE Login

- Fixed a problem with the handling of null passwords during a login sequence.

Security Server

- Fixed a memory leak in the code used for handling credentials. This leak was caused by faulty code in the ASN.1 compiler.
- Added detailed logging for tracking of request packets and propagation.
- Fixed a problem with inadvertent freeing of preauthentication data.
- Fixed several memory leaks that occurred when sending data to the registry.
- Fixed a problem with freeing an error buffer before it was properly reported.
- Fixed a memory leak with ASN.1 fields in security packets.
- Fixed a problem with a counter in the journaling component.
- Improved messages given when the security server was being terminated.
- Fixed a memory leak with freeing of ACL storage for PGO "add function" calls.
- Fixed several problems with data initialization which caused illegal conditions when memory was reused.
- Fixed several problems with illegal access to a string structure when the pointer was NULL.

- Fixed a problem with the registry database structure where data was not being set to NULL when it being allocated or reallocated. This was causing a minor corruption in the database.
- Added returning the error code if the server properties cannot be retreived due to file or disk problems on the server's system.
- Fixed a problem where the PGO structure was not being properly initialized which caused some incorrect fetches of data.
- Fixed a problem when the cursor had reached the end of the list when trying to look up attributes using the UUID as the index.
- Fixed a memory leak with ACL when an invalid cursor was being used.
- Fixed a problem with nonexpansion of the cell name when converting registry names from global to local names.
- Fixed a problem where the type was not initialized when resolving paths in the registry which could cause an incorrect error to be returned.

DFS

- Added kernel-level thread tracing for better kernel logging.

4. Known Problems and Restrictions v4.3.2

Problems listed under Previous Releases may apply to the current release, unless a correction is noted.

There are no additional known problems and restrictions at this time.

5. Previous Releases

5.1 New Features in Previous Releases

5.1.1 New Features v4.3.1

Active Directory Extension

The Active Directory® extension for the DCE Security Server delivers single sign-on capabilities enabling DCE principles to log in to a Microsoft® Windows® Active Directory Domain using their DCE usernames and passwords; they can use the domain's resources even when their account is managed by a DCE cell. The ticket obtained with the login is compliant with Kerberos RFC 1510. Entegrity is the only vendor to offer SSO capability between DCE and Microsoft Windows.

This feature is sold separately. To enable it, you need a license file, which you must place in the **/opt/dcelocal/bin** directory on the Security Server machine(s).

5.1.2 New Features v4.3

Operating System Support

This release supports the Tru64™ UNIX® v5.1B release

5.1.3 New Features v4.2.2

dcesiad

The new daemon, *dcesiad*, performs all of the DCE work needed by the SIA API calls. The new libdcesiad.so library has been rewritten to be single threaded.This was done due to issues with single threaded system daemons and applications. It is further explained in Problems Fixed: *DCE SIA*.

Platforms supported

DCE v4.2.2 runs only on:

	DCE Client	DFS Client	Servers
Tru64 UNIX v5.1A	X	X	X
Tru64 UNIX v5.1A PatchKit2	X	X	X
TruCluster® 5.1A	X		
TruCluster® 5.1A PatchKit2	X		

	DCE Client	DFS Client	Servers
Sierra Cluster (SC) v2.5	X	X	

5.1.4 New Features v4.2.1

No new features were introduced in v4.2.1.

5.1.5 New Features v4.2

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

Platforms supported

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 the *Applications Need Rebuilding* item in Known Problems and Restrictions, later in this document.

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 HP (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]
```

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.

5.1.6 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 (HP (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 must 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.

5.1.7 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 in Previous Releases

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

5.2.1 Problems Fixed v4.3.1

RPC

- The security patches released on 07-Aug-2003 and 16-Sep-2003 are included. For more information, see the following Entegrity Support Web page:

  http://support.entegrity.com/private/patches/dce/rpcattacks.shtml
- Various runtime initialization issues have been fixed
- Fixed a problem where if an RPC call was cancelled then RPC threads were not cancelled. The threads are now properly cancelled. Note that this problem and the following problem would cause images to grow and would eventually result in a core dump.
- Fixed a problem where if an RPC call failed during the connection to the remote server, then the RPC threads were not cancelled. Now when the connection failure is detected, the threads are properly cancelled.
- Fixed a problem where an association was being reused by a server and the connection was not properly reset. The connection is now reset when the server reuses a previously existing association if there are no other current outstanding calls on the association.
- Fixed an issue where a call would deallocate an input buffer and packets were received at a later time. The deallocation pointer was set to point to a NULL routine and the buffer length to zero, which caused further usage of the call structure's buffer to be ignored.

- Fixed an issue where the association state engine would enter an illegal state, which would cause servers (including dced) to terminate prematurely. Altered the state transition table to change the processing of this event.
- Fixed an issue where the handling of illegal state transitions in the RPC state engine would terminate the image. Now the state engine logs a message, the association is properly shut down, and the image continues to operate.
- Added additional trace messages.

DCE Library

- The following routines have been removed from **libdce.so** since they are already included in the standard C library:
  - snprintf
  - vsnprintf
- Fixed an issue where an insufficient amount of memory was being allocated to store DCE credentials. The proper amount of memory is now allocated.
- Fixed an issue in the sec_login interface where an incorrect status could have been returned from a routine. This is now corrected.

Security Server

Added additional trace messages.

DFS

The minimum token limit setting is now properly checked in the client token manager.

Installation Kit

The DCE kit can now be installed if the DCE Toolkit has already been installed. Previous versions required that you uninstall the DCE Toolkit prior to installing a new DCE kit.

Evaluation Kit

- When licensing files are nonexistent or invalid, messages are now printed. Previously, **dcesetup** would report an invalid configuration and terminate.
- Evaluation license files are now required for DFS clients and servers.

5.2.2 Problems Fixed v4.3

Memory Leak Fixes

Fixes to memory leaks in secd and dced have been added to this kit.

5.2.3 Problems Fixed v4.2.2

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

DCE SIA

The DCE SIA Library has been re-implemented to correct interaction problems with system daemons and other single threaded programs. Some daemons, such as envmond, would cause a core dump during system startup if DCE SIA was enabled. Other daemons and applications (rshd) would go into a compute loop. The problem was caused by the incorrect handling of stacks during the dlopen in the Tru64 5.x SIA implementation, working with the threads library.

To provide the required DCE and KRB5 functionality, it was necessary to implement a new daemon called dcesiad. This daemon performs all of the DCE work needed by the SIA API calls. The new **libdcesiad.so** library is single threaded. The dcesetup show command will list the daemon in the pid list.

DFS

Several items in the DFS kernel component were fixed. These items had caused system crashes and hangs under certain conditions on AlphaServer Sierra Cluster systems. The following is a list of problems that were corrected.

- Lock mode 4 violation in the cm_putpage routine during the flushing of UBC buffers. For AlphaServer SC systems, the user must obtain a patch for vfs.mod from Hewlett Packard. Use this in addition to the dcedfs.mod file in this kit.
- Unauthenticated message on the console log.
- Wrong user message on the console log.
- System hang-up due to a call from the kernel to users space to obtain credentials that then made a kernel call to obtain a new vnode.
- System crashed when reference count was set to an invalid value.

dfsbind

The DFS bind image would go into a catatonic state under certain conditions. The problem was being caused by not releasing a lock. The lock is now properly released.

Installation/Configuration

- When members were added in a cluster, they would obtain the DCE and DFS configuration for member zero, the wrong member. Now the hostname is checked against the host listed in the DCE host configuration file. If the hostname does not match, then the script removes the DCE and DFS configuration files for the new cluster member. The new cluster member will then have to be configured for DCE and, if desired, for DFS.
- When the DCE runtime kit is removed on configurations that have the Kerberos services enabled, these services will be temporarily disabled. When the DCE runtime kit is reinstalled the Kerberos services will be enabled. During the time that the kit is uninstalled, the Kerberos services will not be activated. This prevents problems where telnet clients did not work when the Kerberos telnet service was enabled.

Security Server

- Fixed a memory leak within the security server that could have stopped it's execution when traversing through the security database.
- Fixed where secd would attempt to look up login activity for an account without checking the operating state of the security registry server. Now secd checks on the state of the server before attempting the account lookup, and proceeds only if the master or replica server is in service.
- Fixed the security registry server where entries were propagated for deleted members. Incorrect PGO member structures were being propagated for deleted members. The use of correct PGO structures corrected this.

dced

Fixed where the security server had exported bindings that a client could not use because of transport restrictions (as in DECnet). Within the pe_update thread, the server bindings were placed into an array and then written out to the file. When the binding list was reduced, some of the bindings were set to NULL. The write routine tried to write them anyway causing an exception. Now, bindings set to NULL will not be written.

cdsadv

Fixed a CDS caching issue where a CDS cache file of several hundred megabytes was being produced. The CDS Advertiser had calculated a cache size that was too big. A typical CDS cache file, is:

/var/dcelocal/var/adm/directory/cds/cds_cache.0000000000.

Using new APIs addressed the problem.

NOTE: A warning message will be displayed the first time DCE is started up after the new kit is installed. The message indicates that the CDS cache size was adjusted from a previous value. This message is expected and should only occur once.

5.2.4 Problems Fixed in v4.2.1

dcecp principal show

Corrected a problem with the **dcecp principal show** command. This problem was occurring on some systems when the **principal show** command was executed more than once and was producing a "No more entries" error message.

The problem occurred because a registry cursor was not being reset before making a call to look up a principal's group membership. It worked the first time because the structure allocated for the member cursor was being set to 0 by the C library. But on subsequent calls, the cursor was not zero and more than likely was pointing to the old cursor, which was set to the end of the list thus producing the "No more entries" error message. The registry cursor is now being reset before the lookup call.

dcecp -c account show

Fixed a problem where using the **dcecp-c account show** command returned the error message, "registry object not found." It had occurred because either the original account creator or the last changer of the account were no longer in the registry.

When the registry data could not be found, the error was produced. The UUID was still in the account record in the registry. The change code now checks for this specific error and then converts the account record UUID into a string.

This UUID string is now displayed in place of the account name for either the missing account creator or last changer or both, depending on which one is no longer a valid account. **libdcecp**, needed for this operation, was rebuilt.

dcesetup: RPC Environment Variables

Fixed a problem where **dcesetup** had failed to export environment variables correctly, resulting in unwanted network addresses in the local endpoint map (dced) and the CDS namespace. The variables are now read from the DCE configuration file, **/opt/dcelocal/dce_services.db**, and exported correctly.

(See the *NetCrusader/DCE Product Guide* Section 10.4 for illustrations of setting up the environment variables.)

The following steps describe one example of how to initially configure a machine into the cell and prevent addresses associated with a specific network interface from being utilized for DCE RPC operations.

1. Open the **/opt/dcelocal/dce_services.db** file and insert the entry for the network interface you do not want to export, entering:

   RPC_UNSUPPORTED_NETIFS=*tu1*, where *tu1* is the name of the unsupported network interface.

2. Run **dcesetup config** now and select [y] when you are asked if you would like to unconfigure.

3. After configuration is complete, check the **/opt/dcelocal/dce_services.db** file to make sure that your RPC_UPSUPPORTED_NETIFS entry still exists. **dcesetup** leaves it there, with other entries generated during the configuration.

To test that environment variables were exported correctly, you can use the commands **dcecp -c rpccp show mapping**, and **cdscp show cell.**

DCE SIA

- A problem was occurring that caused the event monitoring daemon (**evmd**) to produce a core dump when DCE SIA was enabled. The problem was being caused by an incorrect checking of the return code, from the socket receive call to the dced daemon. The return code was negative from the socket operation but the assigned result variable was an unsigned integer. The test on the result for -1, which indicated an error, failed; so a buffer was copied of 0xffffffff in size which caused a SEGV. The proper checking of the return code has been put into the code and the problem is fixed.
- For many of the system interfaces (getpw*, getgrp* and so on.), the interface could be called when DCE was in the start-up mode causing some problems. Checks were added for all DCE SIA interface routines to check whether DCE was ready to accept calls. The calls now fail if DCE is not ready to process the requests.
- At some point during the start-up sequence, there was a possibility that the socket interface to the getpw* and getgrp* routines would hang in a receive state. When this happened, both the calling program and dced would sit and wait for the other to send data. A timeout was added on both socket interfaces that will be activated if a response has not been received within 10 seconds. The socket will then shut down and continue to accept the next call.
- There was a problem with the socket interface when an inbound call was received to the dced getpw* and getrgrp* socket interfaces. The recv call would return an error and then the receiver loop would attempt to send an error message back to the caller. The problem was that the caller had

closed the socket and then the dced socket listener thread would toss an exception, the thread would terminate, and then no additional DCE SIA calls would function. Proper error detection and handling is now in the code to prevent this situation.

- An error message occasionally appeared on clustered systems when the DCE SIA services were being enabled or disabled. The message indicated that the **/etc/auth/system/default_DCE_temp** file was missing. This was due to multiple machines operating on the same temporary file. The scripts have been modified to use a member-specific temporary file.
- There was an installation problem of the DCE runtime kit when it was installed on machines where X11 was not installed and DCE SIA was enabled. There was a complaint about the nonexistence of the xdm-config file. This problem has been resolved.

RPC

- Intermittent RPC delays, primarily during file close operations, were occurring with the kernel RPC used for DFS. This problem appears to be a bug within the single-threaded RPC implementation in the kernel. The kernel level RPC implementation was reverted to multiple threading with a minor performance degradation.
- There are several fixes applied to the kernel RPC debug routines. These fixes now allow the kernel RPC components to be traced using the **dfstrace** tool.
- There were some kernel RPC multithreading timer issues that have been resolved.

Kerberos Tools

- The **kcfg** tool that was used to configure the Kerberos tools did not remove temporary files before exiting. The tool now deletes all temporary files used.
- The **rsh** program incorrectly sent all output to the stderr stream. Output is now directed to the proper output stream.
- The **rsh** program has been rebuilt without debug messages.

DFS

- On some DFS server machines, a panic was seen when trying to shut down the machine. The problem occurred when the DFS root filesystem was being unmounted. The kernel unmount routine now properly checks for the root DFS filesystem before releasing the mount point.

- A problem existed in the token revocation routine that was causing loops within the DFS components that would cause system hangs and panics. This problem was being caused by improper parameters being sent to a routine to free the local cache blocks. The correct parameters are now passed into the routine, resulting in the hangs and panics not reappearing.
- The system would crash when DFS was in the kernel but not configured, and a cache manager **(cm)** was issued. The kernel cache manager command processing routine now properly checks to see if DFS is initialized before executing the command. If the **cm** command is issued when DFS is not configured then an error message indicating invalid parameters will be displayed.
- A problem occurred when the server crashed and token recovery was started. The client application would hang forever. This has been fixed.
- Fixed a deadlock in token code where a connection was reset that would cause several threads to prevent each other from recovering. They would continually mark a server as bad.
- All of the known DFS recursion errors which can cause deadlocks or panics have been fixed.
- File deletion failures, using the **rm** command, were reported. This problem was occurring due to the **dfsd** kernel processes not being able to obtain the machine credentials. The problem was related to the file partition that contained the DCE credential files reaching maximum capacity.
- Internal to the RPC code, a routine made a call to the fcntl routine using the wrong parameters for kernel calls. This condition was being caused by datagram connections that were being forced to a closed state. The condition was seen on the server but could have easily appeared on the client side as well. The code has been corrected to pass in the proper parameters to the fcntl kernel function.

dfsbind

- There was a hang related to **dfsbind** going into a catatonic state. This was being caused by incorrect locking of the dfsbind data structures. This problem has been resolved.

A problem occurred when dfsd kernel processes could not obtain self credentials via **dfsbind** from the dced daemon. This problem occurred within a bind routine where local credentials could not be obtained from the creds cache. This problem occurred because the file partition that contained the DCE credential files had reached maximum capacity.

5.2.5 Problems Fixed v4.2

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

DFS

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

5.2.6 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.

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

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.

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.

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.

5.2.7 Problems Fixed v4.1.3

rsh

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 must obtain a new version of Tru64 rshd from HP (Compaq) when they make it available. The existing Tru64 version of rshd also had the same problems.

5.2.8 Problems Fixed v4.1.2

SIA

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	matrix.conf.preDCE	matrix.conf.preDCE
Yes	OSFC2_matrix.conf	OSFC2_matrix.conf
Yes	bsd_matrix.conf	bsd_matrix.conf
No	bsd_matrix.conf	bsd_matrix.conf
No	<none of the above>	.proto..matrix.conf

5.2.9 Problems Fixed v4.1.1

Installing Cluster

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

5.2.10 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

- TheTru64 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.

5.2.11 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 from 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 in Previous Releases

The following were known problems and restrictions at the times of their respective releases. Many list workarounds. Problems listed under Previous Releases may apply to the current release, unless a correction is noted.

5.4.1 Known Problems and Restrictions v4.3.1

Security Server

- Under certain conditions with large registries, secd will prematurely terminate without leaving a core file.
- Under certain conditions with large registries, the propagation will not propagate some changes to the replica(s). However, these changes will be propagated when the replica is restarted.

5.4.2 Known Problems and Restrictions v4.3

DFS Panic When Clobbering DCE Configuration

A system panic can occur when you are clobbering the machine's DCE configuration if you have just clobbered the DFS configuration. The panic occurs when a DFS directory is being read by the system. During the DFS clobber, the cache files have been deleted and the DFS directory cannot be read. This causes the panic message shown below.

```
panic (cpu 0): readdir open
```

The panic occurs in the cm_readdir routine within the DFS code in the kernel.

There are two possible workarounds. Either method works.

Workaround 1

8 Clobber the DFS configuration.

9 Reboot immediately after the DFS configuration has been deleted.

10 After rebooting, clobber the DCE configuration.

Workaround 2

1 Clobber the DCE configuration.

2 Clobber the DFS configuration.

3 Reboot the system.

The panic in the DFS code is a "safeguard" panic, so that if the DFS cache files get accidently deleted from the system, the panic occurs since DFS would not be able to function properly. If this occurs, then DFS needs to be configured to properly restore the cache files.

DECNet Support

DECnet support has been removed from this release.

DCE Toolkit

The DCE toolkit 2.3 Beta has been removed from this kit. If you are interested in obtaining the 3.0 version, contact Entegrity Solutions DCE Sales at DCESales@entegrity.com.

5.4.3 Known Problems and Restrictions v4.2.2

Problems listed under Previous Releases may apply to the current release, unless a correction is noted.

DFS

If the DFS cache manager (in the kernel) is not able to write to the disk cache, then a system panic will occur. This problem occurs when the partition that contains the DFS cache is full, so the DFS cache cannot be written.

The work-around is to place the DFS cache onto a separate partition that is large enough to contain the configured cache size.

5.4.4 Known Problems and Restrictions v4.2.1

DCE SIA

(Corrected in version 4.2.2.)

The DCE SIA library, **libdcesiad.so**, has been written using the pthreads library. This causes some calling applications, including system tools and daemons, to core dump when making system calls to obtain security information. We are looking at this problem and have removed all thread calls and exception handling from the library but due to the nature of some of the required DCE security interfaces, all threading issues could not be resolved. We are still investigating the removal of threads from the library, which may result in a reimplementation of library routines.

DFS

Testing has revealed the following problems, not yet resolved.

Occasional RPC “who are you” messages followed by “set auth binding failed” messages on consoles. These are sometimes, though infrequently, followed by a message to say the client has disconnected from the server. When this occurs, the client will successfully reconnect.

“ubc_invalidate returns: -1” messages. These are debug messages from DFS that occur during token revocation when removing UBC pages. The source of these errors is being investigated. As of now, they appear benign.

It is possible for certain DFS vnode operations to recursively call into DFS again. These can cause kernel stack invalid panics or dfs deadlocks. All of the vnode operations that have caused problems have been fixed by insertion of a per-thread sentinel. The remaining operations will be fixed in a subsequent kit for completeness.

envmond may cause a core dump. Entegrity and Compaq (now a subsidiary of HP) are pursuing this issue. If it occurs, you must obtain a copy of **libtcl.so** from the Compaq/HP support group and place it in **/usr/share/sysman/lib/tcl8.2/** as follows.

```
mv /usr/share/sysman/lib/tcl8.2/libtcl.so
/usr/share/sysman/lib/tcl8.2/libtcl.so.dist
mv /tmp/libtcl.so.nothreads /usr/share/sysman/lib/tcl8.2/libtcl.so
```

DO NOT apply this file unless you encounter problems. It contains a temporary workaround only.

5.4.5 Known Problems and Restrictions v4.2

Versions

The 4.2 kit will run only onTru64 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 HP (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

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

to

```
siad_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 HP (Compaq) Tru64 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.

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 Hewlett Packard.

dcecp: Security with Replica

(Corrected in version 4.2.1)

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

5.4.6 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
```

5.4.7 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.

5.4.8 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 HP/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.

Entegrity 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_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/bi**n 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 v4.0

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. Documentation Notes

This set of Release Notes provides release information for DCE and DFS v4.3.2 software for Tru64 UNIX v5.1B machines.

Separate documentation is provided for 4.1.x and 4.2.x. The Release Notes for DCE v4.2.x lists the changes in patches 4.1.1, 4.1.2, 4.1.3, and 4.1.4. Changes after 4.1.5 are paralleled in versions after 4.2.1.

7. Obtaining Technical Support

If you purchased your Gradient product directly from Entegrity 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.entegrity.com**. The web site also contains online forms for easy registration.

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

8. Contacting Entegrity Solutions

Contact	Address	Phone/Fax/Email
Entegrity Product and Sales Information	Entegrity Solutions Corporation 410 Amherst Street, Suite 150 Nashua, NH 03063 USA	Email: sales@entegrity.com Web: www.entegrity.com Tel: +1-603-882-1306 ext.2700 Toll Free (US): 1-800-525-4343 ext. 2700 Fax: +1-603-882-6092
Technical Support	Entegrity Solutions Corporation 410 Amherst Street, Suite 150 Nashua, NH 03063 USA	Email: support@entegrity.com Web: support.entegrity.com Tel: +1-603-882-1306 ext. 2702 Toll Free (US): 1-888-368-3555 ext. 2702 Fax: +1-603-882-6092
Documentation Comments and Suggestions		Email: docs@entegrity.com
Other Inquiries	Entegrity Solutions Corporation 410 Amherst Street, Suite 150 Nashua, NH 03063 USA	Email: info@entegrity.com Web: www.entegrity.com Tel: +1-603-882-1306 Toll Free (US): 1-800-525-4343 Fax: +1-603-882-6092

The contact information in this table may change. For the most up-to-date information, see our contact page on the Entegrity Solutions web site: http://www.entegrity.com/corporate/offices.shtml.