

Fixing Problems with DC Directory

Document ID: 30002

Introduction

Prerequisites

- Requirements
- Components Used
- Conventions

Problem

Solutions

- Installation
- Reconfiguration
 - Reconfigure DC Directory on the Cisco CallManager Publisher (Database More than 100 Mb)
 - Reconfigure DC Directory on the Cisco CallManager Publisher (Database Less than 100 Mb)
 - Reconfigure DC Directory on the CRA/CRS Server

Modify the UserID in Cisco CallManager using DC Directory

Problem – Unable to Delete a User from the DC Directory

Solution

Error: No free connection control blocks – connection refused.

Solution

Error 1096: The AvDSAD does not have a domain controller for the domain and could not get one from Active Directory.

Solution

Related Information

Introduction

This document explains how to resolve directory replication problems between DC Directory server services that run on Cisco CallManager servers involved in a cluster.

This procedure is valid for Cisco CallManager servers that run versions 3.0(5a) through 3.3.x.

Note: The DC Directory scripts (1.0.7) mentioned in this document are used only with Cisco CallManager 3.0(5a) through 3.3(2c).

Note: For Cisco CallManager 3.3(3) and later, the directory schema version has changed. Therefore, the scripts are already included in Cisco CallManager 3.3(3) and later and you do not need to download them. If you run Cisco CallManager 3.3(3) or later, refer to the procedure in the Reconfiguration section.

This list describes the symptoms associated with this problem:

- The Cisco CallManager publisher server has correct user data. However, one or more Cisco CallManager subscriber servers either do not have user data, or the user data is out of date with the database of the publisher.
- The DC Directory service on the Cisco CallManager publisher server takes a long time to start-up (appears to stall or hang on start-up).
- DC Directory replication errors are logged to the Cisco CallManager publisher and/or subscriber server(s) in the Application Event Viewer.

- An examination of C:\dcdsrvr\run\dcx500\dcx500.out shows duplicate and/or invalid replication agreements.

Note: The logging of DC Directory message DC Directory Server has been QUIESCED in the application log of the Cisco CallManager Publisher during the backup with BARS is normal. The **Quiesced** implies that the DC Directory cannot get enough resources from the server because some other process currently controls most of the resources. Basically, Cisco CallManager pauses the DC Directory service until it completes what it is doing. So while a task is performed on the Publisher server that requires a lot of resources, this error can be normal.

Prerequisites

Requirements

There are no specific requirements for this document.

Components Used

The information in this document is based on these software and hardware versions:

- Cisco CallManager 3.0(5a) through 3.3(2c) on all servers in the cluster.
- An embedded DC Directory server is used as the directory store for all servers in the cluster.

The information in this document was created from devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, ensure that you understand the potential impact of any command.

Conventions

Refer to the Cisco Technical Tips Conventions for more information on document conventions.

Problem

The presence of invalid replication agreements causes the DC Directory database (files in C:\dcdsrvr\run\dcx500\database) to grow extremely large (over 100 MB). This causes the DC Directory to take a large amount of time to shutdown and start-up. These duplicate and invalid agreements are caused due to one of these reasons:

1. The customer reinstalls the Cisco Customer Response Application (CRA) server (or a Cisco CallManager subscriber) one or more times (each reinstall of the CRA server/Cisco CallManager server causes the publisher to have a new replication agreement to the subscriber).
2. A CRA server (or a Cisco CallManager subscriber) already exists, and is decommissioned without the performance of the DC Directory reconfiguration procedure in the Cisco CallManager cluster.

Note: When a directory node is removed from a Cisco CallManager cluster, the DC Directory replication agreements to the removed subscriber are *not* automatically cleaned up.

3. The **avvid_scfg** command is manually run on the subscriber more than once (for instance, a partial DC Directory reconfiguration procedure is attempted).



Warning: Never perform a partial DC Directory reconfiguration procedure, (for example, never run **avvid_scfg** if it is not preceded by **cleandsa** on the publisher and the CRA server, and/or

Cisco CallManager subscriber).

The root cause of the growth of the database to such large sizes is that DC Directory tries to save the state for each and every replication operation that it fails to perform. Over a period, this saved state information for the invalid replication agreements causes the database to grow to several hundred MBs.

Do not confuse DC Directory replication with SQLServer replication. They are two completely independent processes.

If you perform a reinstallation of a Cisco CallManager subscriber or CRA server 2.2(4) and earlier, or CRA server 3.0(1), you *must* perform the DC Directory reconfiguration procedure on *all* of the nodes in the cluster. This includes the standalone CRA servers. Start with the DC Directory publisher.

Solutions

While you perform these tasks, you must be:

- Directly at the console of the Media Convergence Server (MCS) servers, connected through a Keyboard/Video/Mouse (KVM) switch.

OR

- Connected via Telnet to the servers.

Performance of these specific tasks while you are connected through a Terminal Services Client connection has not been fully tested, and can produce unexpected results. Cisco recommends that you schedule a downtime in order to run the procedure. The two steps involved are:

1. Installation
2. Reconfiguration

Installation

Complete these steps for installation:

1. Download **DCDScripts.1-0-7.exe** from the Cisco CallManager Version 3.2 (registered customers only) website. Only download these scripts if you run Cisco CallManager versions *prior* to 3.3. There is no need to download scripts on versions 3.3 and later as they are included and found in the c:\dvdsrvr\bin folder. If you install and run the DCDScripts.1-0-7.exe file on newer versions of Cisco CallManager, this causes the system to fail.
2. Copy and run **DCDScripts.1-0-7.exe** on *all* the nodes in the Cisco CallManager cluster, and on the CRA/CRS application servers. Accept the default settings when you are prompted to do so, and click **Unzip**.

Note: Make sure that you run the scripts during off-peak hours in order to avoid high CPU utilization.

Reconfiguration

There are two possible scenarios when you go to reconfigure your DC Directory after installation:

1. When the DC Directory database is larger than 100 Mb, refer to the Reconfigure DC Directory on the Cisco CallManager Publisher (Database Greater than 100 Mb) solution in this document.

2. When the DC Directory database is less than 100 Mb, refer to the Reconfigure DC Directory on the Cisco CallManager Publisher (Database Less than 100 Mb) solution in this document.

Reconfigure DC Directory on the Cisco CallManager Publisher (Database More than 100 Mb)

These steps ensure that your user data in DC Directory on the publisher Cisco CallManager server is backed up in case of a failure during these steps. These steps also help when the DC Directory database is larger than 100 Mb (C:\dcdsrvr\run\dcx500\database).

Note: You must disable the Cisco Security Agent (CSA) service before you install, uninstall, or upgrade any software (including the operating system), on Cisco CallManager. You must disable the agent by using the method that is described in Disabling and Reenabling the Cisco Security Agent Service. Ensure that the service does not become re-enabled at any time during the installation or upgrade. Failure to do so can cause problems with the installation or upgrade. After the software installation or upgrade, you must re-enable CSA before it starts to monitor the Cisco Unified CallManager server again.

1. Back up your current directory information. Use either the MCS backup utility, or run the **dcbackdib /y backup C:\dcdsrvr\backup** command from a DOS command prompt.

Note: The C:\dcdsrvr\backup folder *must* exist before you run the **dcbackdib /y backup C:\dcdsrvr\backup** command.

2. On the publisher server, while logged in as the Administrator, open a command prompt. In order to do so, select **Start > Run**, and enter **cmd**.
3. Type the **avvid_migrate_save.cmd servername password** command, and press any key when prompted.

The output of this command looks similar to this output:

```
C:\>avvid_migrate_save jayas-w2k ciscocisco
A subdirectory or file C:\dcdsrvr\log already exists.

*****
*
* -- CISCO User Preferences Support -- *
*
*****

A subdirectory or file C:\dcdsrvr\suspense already exists.

Run the perl script avvid_migrate_save.pl
A subdirectory or file C:\dcdsrvr\log already exists.
A subdirectory or file C:\dcdsrvr\run\DCX500\config\Migration-Backup
already exists.
Saving User Information...
Saving Profile Information...
Saving Apps20 Information...
Saving Admin Information...
Saving PA node Information...
Saving E911 node Information...
Saving systemProfile...
Saving MITRA data...
Saving Groups data...

C:\>
```

4. Stop the DC Directory Service. Enter **net stop dcdirectory** from the command prompt.
5. Run **cleandsa.cmd** or **deletedib.cmd**, if **cleandsa.cmd** reports that it is not supported.
6. Run **avvid_migrate_cfg.exe**.

(Usage **avvid_migrate_cfg** *password*)

7. Run **avvid_migrate_restore.cmd**.

(Usage **avvid_migrate_restore** *Server Name DCDpassword*)

8. Run **reconfig_cluster.cmd**.

(Usage **reconfig_cluster** *DCDAdminPassword*)

This command establishes replication agreements to all Cisco CallManager subscribers. You do not need to perform any tasks on any of the Cisco CallManager subscribers.

Reconfigure DC Directory on the Cisco CallManager Publisher (Database Less than 100 Mb)

Complete these step in order to reconfigure DC Directory in the Cisco CallManager publisher when the DC Directory database is less than 100 Mb (C:\dcdsrvr\run\dcx500\database).

Run **reconfig_cluster.cmd**.

This command establishes replication agreements to all Cisco CallManager subscriber servers. You do not need to perform any additional steps on any of the Cisco CallManager subscribers.

Reconfigure DC Directory on the CRA/CRS Server

Complete these steps in order to reconfigure the DC Directory on the CRA/CRS server:

1. Stop the DC Directory service.
2. Run **cleandsa.cmd** or **deletedib.cmd** if **cleandsa.cmd** reports that it is not supported.
3. Run **avvid_scfg.cmd**.

(Usage **reconfig_cluster** *DCDAdminPassword*)

Note: If the network has a single Cisco CallManager server with or without co-located CRA/CRS, you need to run **reconfig_cluster.cmd**. In this case *do not* run the steps listed for the Cisco CRA/CRS server.

Note: If you upgrade, reinstall, or add a new Cisco CallManager server 3.2(2c) or earlier, or CRA 2.2(4) or earlier, and CRA 3.0(1), you *must* copy and run **DCDScripts.1-0-7.exe** as described in the Installation section.

Modify the UserID in Cisco CallManager using DC Directory

The userID is used to identify each user in Cisco CallManager. By default, Cisco CallManager does not allow you to change the userID. If required, you can change it using the DC Directory Administrator with these steps.

1. Login to the **DC Directory Administrator** from **Start > Programs > DC Directory Administrator**.
2. Click **Users**.

The list of users appears on the right side of the window. Double-click on the user for which the userID should be modified.

3. Go to the E-mail tab and click **Modify**.
4. Change the userID specified against the **Internet** value, then click **Apply** and **OK**.

Complete these steps to verify whether the userID is changed.

1. Go to the Cisco CallManager Administration page.
2. Select **User > Add a New User**.
3. Click **Basic Search** with the new userID and verify whether the userID has changed.

Problem – Unable to Delete a User from the DC Directory

When a user tries to delete a user in DC Directory, this error message is received:

```
Could not delete user. UserID = "<username>"
```

Solution

This issue can occur if the DC Directory service has been stopped. In order to resolve the issue, restart the **DC Directory Server** service from **Start > Programs > Administrative Tools > Services**. You are then able to delete the user.

Note: You can use pattern match as well as exact match in order to search for department name. Use pattern match, such as wildcard based symbols like ?,-,*,%, if department name has blank spaces.

Error: No free connection control blocks – connection refused.

This DC Directory error message appears on the event viewer:

```
Event Type:      Warning
Event Source:    DCDirectory
Event Category:  Configuration
Event ID:        9415
Date:            1/30/2009
Time:            11:10:31 AM
User:            N/A
Computer:        QPUB
Description:
(BASE IL NEW CONNECT(47) Proc 88, Sev 14)
    No free connection control blocks - connection refused. This
    indicates that the maximum number of simultaneous TCP/IP
    connections has been reached, and further connection
    attempts will fail until one of the existing connections
    has been closed.
    Socket ID                D4859209
    Component                 LDAP
    Number of CBs configured  504
```

Solution

From version 3 and later, DC Directory uses the KeepAlive socket option in order to detect dead connections. However, if the KeepAlive signal is delayed at least one millisecond, it generates the error since some connections are not released on time and the system can reach the limit for just a very small moment. This behavior also causes clients behind firewalls to continue to open new connections when the firewall times out idle connections. In addition, when the clients are rebooted, old connections are not torn down on the server side, which causes DC Directory to exceed its maximum limit of allowed LDAP connections of 500 over time.

The practical effects of these open connections is small, and they do not cause any operational effects. They cause a minute overhead on the Operating System and count towards the configured limit on inbound LDAP connections.

If you do not experience any effect in your Cisco CallManager, this behavior does not represent a problem. As mentioned earlier, this kind of error can provoke behaviors, such as problems for users to login to DCD or IPCC. If that is the case, you see the error repeat hundreds of times.

If you detect that your system is affected by this error, these DC Directory/LDAP connections can be forced shut. In order to do this, stop and restart the DC–Directory server, under Services. Refer to CallManager Cannot Open the DC Directory for steps to restart the DC–Directory Server.

Error 1096: The AvDSAD does not have a domain controller for the domain and could not get one from Active Directory.

This error message appears on the event viewer:

```
Event Type:      Error
Event Source:    CiscoUnity_DSAD
Event Category: Warning
Event ID:        1096
Date:            08/05/2009
Time:            4:09:19 PM
User:            N/A
Description:
Computer:        CLUSTER8-UNITY
Description:
```

The AvDSAD does not have a domain controller for the domain, and could not get one from Active Directory. Ensure that a domain controller exists for this domain, that no DNS issues exist, and that The Cisco Unity service that monitors Active Directory (AvDSAD) account has the proper rights.

Solution

In order to remove this error, open the DC/GC tool and perform a Force Reconnect. In some cases, DCGC reconnect tool displays a blank domain. In this case, complete these steps in order to delete that DC from the database and then perform a Force Reconnect.

1. Choose **Start > Programs > SQL > Enterprise Manager**.
2. Expand **local > Database > UnityDb > Tables**.
3. Right-click **ADDomain > Open Table > Return all rows**.
4. Delete the entry for the blank domain.
5. Open the DCGC tool and perform a Force Reconnect with the DC.

Related Information

- **Voice Technology Support**
 - **Voice and Unified Communications Product Support**
 - **Recommended Reading: Troubleshooting Cisco IP Telephony**
 - **Technical Support & Documentation – Cisco Systems**
-

