

LDAP Monitor Server Not Failing Over Correctly

Document ID: 40440

- Introduction**
- Before You Begin**
 - Conventions
 - Prerequisites
 - Components Used
- Description**
- Resolution**
- Related Information**

Introduction

This document describes the Lightweight Directory Access Protocol (LDAP), explains how it functions, and details some troubleshooting steps to determine why the LDAP Monitor Server is not failing over.

Before You Begin

Conventions

For more information on document conventions, see the Cisco Technical Tips Conventions.

Prerequisites

Readers of this document should be knowledgeable of the following:

- Cisco Intelligent Contact Management (ICM) functionality
- IP Voice and Networking experience
- Working knowledge of Cisco Agent Desktop

Components Used

The information in this document is based on the software and hardware versions below.

- Cisco ICM version 4.6.2 and later
- Cisco Agent Desktop 3.0 and later
- Microsoft Windows NT Registry Utility

The information presented 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 you are working in a live network, ensure that you understand the potential impact of any command before using it.

Description

The Directory Services server is an LDAP server. All other Cisco Desktop servers register with the Directory Services server at startup. An optional secondary Directory Services server can be installed to provide redundancy for the primary Directory Services server. This secondary Directory Services server must be

installed on a separate machine.

This document assumes you have run through setup from Cisco Agent Desktop, and have configured PG1A to be the primary LDAP server and PG1B to be the secondary (backup) LDAP server. During testing, agents are unable to log into Cisco Agent Desktop when the primary LDAP service (PG1A) is stopped. See the following sample log:

```
18:13:34 11/07/2002 INFO NTSVC The Windows NT service
received a stopmessage from the Windows NT service manager.
18:13:34 11/07/2002 INFO NTSVC The Windows NT service has stopped.
18:13:36 11/07/2002 INFO NTSVC running as NT service..Cisco
Desktop LDAP Monitor
18:13:36 11/07/2002 INFO NTSVC starting NT service...
18:13:36 11/07/2002 MAJOR NTSVC Begin
18:13:36 11/07/2002 MAJOR NTSVC End
18:13:36 11/07/2002 INFO NTSVC The Windows NT service has started.
08:40:00 11/14/2002 INFO NTSVC The Windows NT service received
a shutdown message from the Windows NT service manager.
```

Upon initial setup of Cisco Agent Desktop, you must define which Peripheral hosts the primary LDAP service and which Peripheral hosts the secondary (backup) LDAP service, if configured. Also, it is recommended that you use IP addresses instead of host names in the designated fields to avoid a Domain Name System (DNS) issue.

The secondary Directory Services server (LDAP) provides read access only to its database and it only receives its information from the primary LDAP server.

Note: You do not get true failover redundancy for agents that connect to the secondary Directory Services server with the most current version of Cisco Agent Desktop 4.4 today. However, if a secondary LDAP is configured, agents can log in and receive customer calls.

Resolution

For verifying the configuration and confirming the primary or the secondary LDAP server is running, below are several common things to check.

There are two parts for the Cisco Agent Desktop LDAP solution.

- **LDAP Server**, uses the **slapd.exe** process
- **LDAP monitor service**

The sole function of the **LDAP monitor service** is to start and watch the actual primary **LDAP server** (**slapd.exe** process). If it fails for any reason, it restarts, by design.

Should you want to completely stop the **LDAP server** (**slaped.exe** process), you must stop the **LDAP monitor service** since they are both tied together. This is done by accessing **Start > Programs > Administrative Tools > Services**.

Refer to Figure 1 and Figure 2. You can see what needs to be configured at the agent level along with the registry key at the agent level, which allows you to verify the initial setup.

During the Agent Install Process the Windows dialog box called Directory Services Server Information appears, below

In the Directory Services Server Information dialog box, enter the IP address of the primary Directory Services (LDAP) server, and then click **Next**. If you install a backup (secondary) Directory Services server, enter the IP address of the server where the backup server is installed.

Figure 1: Directory Services Server Information

Directory Services Server Information

Enter the host name or IP address of the computer where the primary Directory Services server will be installed.

Primary

Host Name

IP Address 172 . 17 . 50 . 129

If you intend to install a backup Directory Services the primary Directory Services server must know its network location. Enter the host name or IP address where the backup server will be installed.

Backup

Host Name

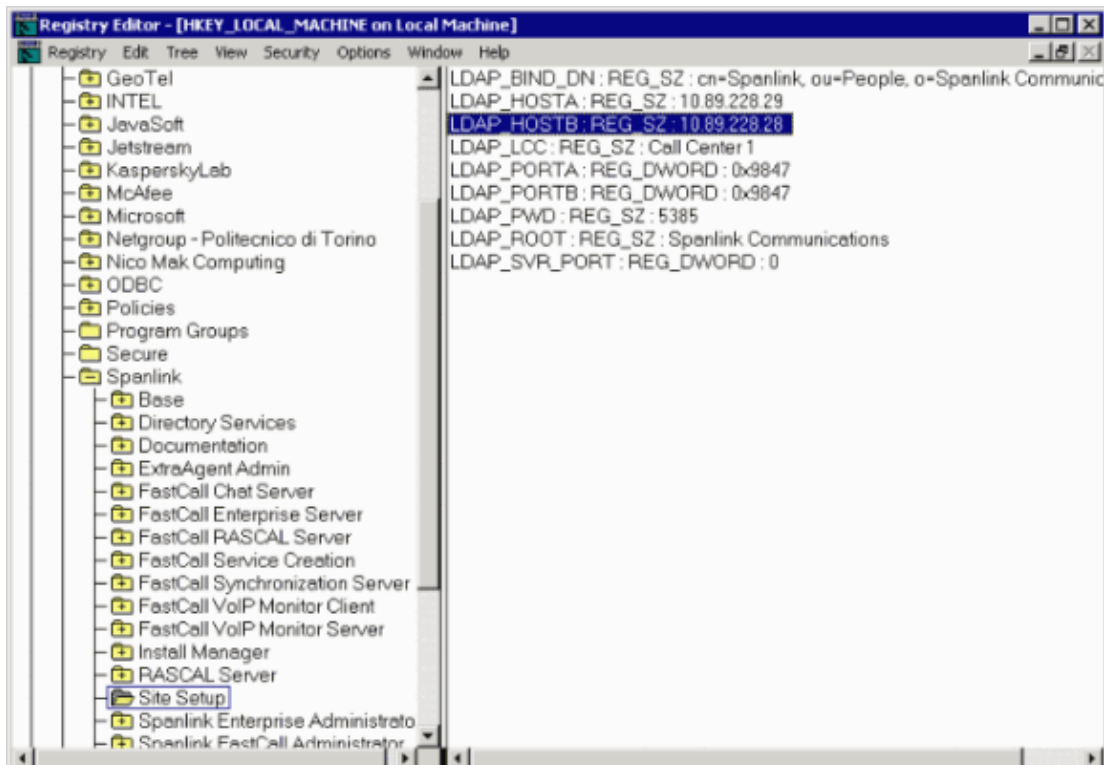
IP Address 0 . 0 . 0 . 0

< Back Next > Cancel Info

The LDAP server agent users are setup in the agent's registry under the following **Site Setup** key:

HKEY_LOCAL_MACHINE/Software/Spanlink/Site Setup

Figure 2: Registry Key



Note: There are values for LDAP_HOSTA and LDAP_HOSTB if a secondary has been setup and configured during installation.

This registry key is what the Cisco Agent Desktop program looks to when it starts. You may consider rerunning setup at the agent level or try modifying the registry key above. Make sure there is an entry in both. Verify the IPs are different and represent the correct primary and backup LDAP servers.

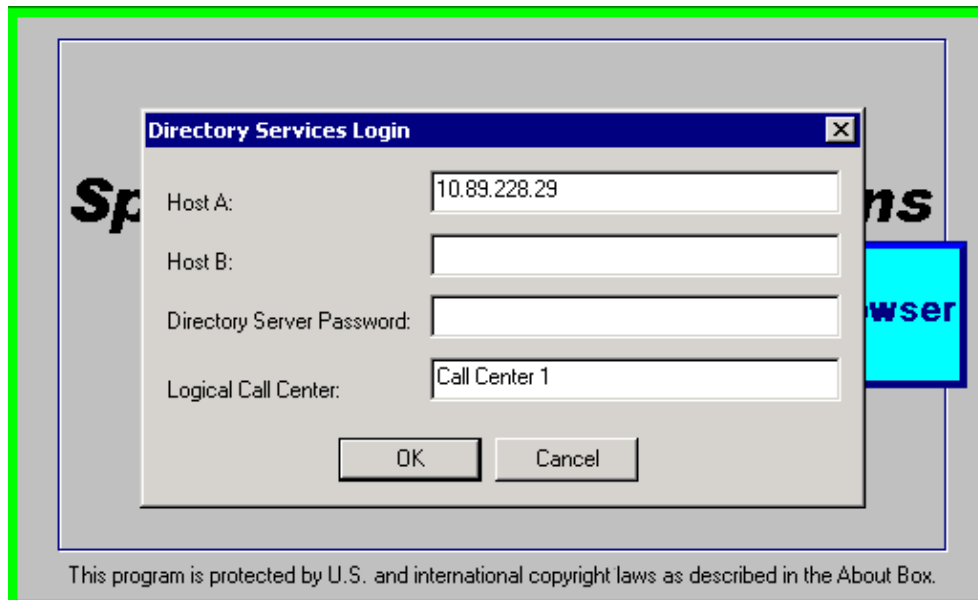
To start **dsbrowser**, take the following steps on the primary and secondary LDAP server:

1. Click **Start > Run**.
2. Enter the following command in the **Open** field.

```
"C:\Program Files\Cisco\Desktop_config\Util\
dsbrowser.exe" /editable
```

3. Click **OK** and the **Directory Services Login** window opens.
4. If the IP address is valid and the Local Call Center name is correct for the primary LDAP server, enter the password and click **OK**.

Figure 3: Directory Services Login



Another way to start **dsbrowser** is to choose **Start > Programs > Cisco > Desktop > Utilities**, open **dsbrowser** and the **Directory Services Login** window opens.

Another file called **replug** located on the primary LDAP server, if there is a secondary LDAP server configured, can be viewed to determine if there are current errors with failovers.

Note: If the **replug** file size is very large (100MG+), this can indicate a problem.

It is the best practice to have all agents point to the primary LDAP service by default.

If agents are unable to log into the LDAP server through Cisco Agent Desktop and the **LDAP monitor service** is running, then try using CTIttest utility. Refer to the Cisco Technical Assistance Center (TAC) to confirm there is a Cisco ICM configuration issue.

At the agent level, there may not be a backup LDAP server configured so that when you stop the **LDAP monitor service**, the primary LDAP server stops as well, due to the inter-relationship, thus agents cannot log in.

Agent level tracing can be set, as noted below, to gather specific agent information:

- Agent Desktop provides the following functionality:

- ◆ Screen POP
- ◆ Call Control
- ◆ View Agent Reports
 - ◇ Stats
 - ◇ Call Logs
 - ◇ Agent State Logs
 - ◇ Call/Chat
 - ◇ Enterprise Data

- Application Name: **fastcall.exe**
- Log File Directory: <Install Dir>\log
- Log file Name: agent[.dbg / .log]

- Config File Directory: <Install Dir>\config
- Config File Name: **fastcalllocal.ini**
- How to increase the debug level for application:
 - ◆ Level = 6 – for call/chat app
 - ◆ Level = 10 – for basic CTI debugging, enterprise traces, fchoker
 - ◆ Level = 11 – for lower level communication between Cisco Agent Desktop and CTI Server
 - ◆ Level = 170–179 – for RASCAL Traces
 - ◆ Level = 3000–3100 – agent state traces
 - ◆ **Level = 4000–4100 – LDAP traces**
 - ◆ Level = 8000 – full blown

Restart desktop after changing debug level.

Note: Use level 4100 to capture LDAP information.

Related Information

- [CTI Test Guide](#)
- [Using CTITest to Troubleshoot IPCC Agent Login Problems](#)
- [Technical Support – Cisco Systems](#)

All contents are Copyright © 1992–2006 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

Updated: Jul 19, 2006

Document ID: 40440
