

MeetingPlace Server infocap Tool

Document ID: 48257

- Introduction
- Prerequisites
 - Requirements
 - Components Used
 - Conventions
- The infocap Tool
- Related Information

Introduction

This document presents an examination of the **infocap** tool on the Cisco MeetingPlace server.

Prerequisites

Requirements

There are no specific requirements for this document.

Components Used

The information in this document is based on Cisco MeetingPlace server software versions 4.1.3 and later.

The information in this document was created from the 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, make sure that you understand the potential impact of any command.

Conventions

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

The infocap Tool

The **infocap** tool was developed to standardize information capture and streamline information gathering for cases. It is a Unix script that was written to grab the necessary information for a case in one session. The **infocap** command accepts one or two switches. The switches are:

```
-b [mmddhhmm] for the beginning month, day, hour, and minute in 24 hour time  
-e [mmddhhmm] for the ending month, day, hour, minute in 24 hour time
```

In this example, the **infocap** command captures information from 1:00 p.m. to 1:15 p.m. on May 10th.

```
infocap -b05101300 -e05101315
```

When you issue this command on a Cisco MeetingPlace server running version 4.3.x and above, an option is given to gather gateway logs. For example:

```
Malone:csc$ infocap
```

```

Usage: infocap -b[mmddhhmm] -e[mmddhhmm]
Malone:csc$ infocap -b02261400
infocap for the capture of escalation information.

This might take a minute or two. Please stand by...
Do you need Gateways Logs (Y or N):
Y
enter gateway unit (10 - 15):
10
Which drive (c, d, e ... etc) would you like to search for Dr Wason Log?
C

```

Only select Y (yes) if experiencing a gateway issue, because the logs can be extremely large.

The script saves the output in a file called caselog in the usr/users/csc directory. This directory is the home for the Customer Service Center (CSC) user. Every time the **infocap** command is issued, the caselog file is appended, not replaced. This means that caselog contains a history of every time that the **infocap** command was issued. Each separate instance is separated from the others with a timestamp. This looks like:

```

*****
**  NEW FILE
*****

Wed May 10 11:53:02 PDT 2000

```

This makes it easy to do searches for specific instances of **infocap**.

Each command within the **infocap** tool is separated with a header to make it easy to find specific information. Each header starts with a row of stars followed by a row with two stars and the name of the command. Finally there is one more row of stars. After that there is a space and the output of that command. This is a list of the titles within the caselog:

```

NEW FILE
SIMSHOW
HWCONFIG
GWSTATUS
SPANSTAT -s and SPANSTAT -cl
ERRORLOG
History of restarts
This is where the cores are...
cm_alt.log before last restart...
Is there an OhNoo?
VIEWEXLOG
CPTRACE -C
CPTRACE -v
CPTRACE -S

```

All of these are common commands that are used every day. The **swstatus** command is not on the list because it is just a subset of the **simshow** command. The **errorlog** command is a subset of the **viewexlog** command, but the **viewexlog** command is also attached as it runs with the **-s info -l** tags and provides more information on alarms. For cores and OhNoos, the **infocap** tool shows only the location or the existence of these files. It is still up to the Network Consulting Engineer to use FTP to transfer these files back to the support center.

The **infocap** tool detects the difference between a network server, a conference server, and a stand-alone server. It then determines which commands are relevant. For example, because there is no telephony in a network server, the **spanstat** command does not provide any useful information. Likewise, a conference server does not communicate to the gateway System Integrity Manager (SIM) so the **gwstatus** command is not issued. As such, in a network environment it is important to issue the **infocap** command from each of the servers in the system to get a complete picture of what was going on during the problem.

On systems without **infocap**, this utility can be downloaded to a server as long as the server is running Cisco MeetingPlace version 4.0.x or later. To do this, use FTP to transfer the file to the /lat/techbin directory, and then issue the **chmod 555 infocap** command. The current uncompressed checksum (cksum) for this script is 1864586414 2885 infocap.

Related Information

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

[Contacts & Feedback](#) | [Help](#) | [Site Map](#)

© 2008 – 2009 Cisco Systems, Inc. All rights reserved. [Terms & Conditions](#) | [Privacy Statement](#) | [Cookie Policy](#) | [Trademarks of Cisco Systems, Inc.](#)

Updated: Jan 31, 2006

Document ID: 48257
