

Use the dumpcfg Administration Tool to Track ICM Configuration Changes

Document ID: 69985

Contents

Introduction

Prerequisites

- Requirements

- Components Used

- Conventions

Background Information

Dump the Config_Message_Log

Related Information

Introduction

This document describes the dumpcfg utility program, which is a database administration tool. The main function of the dumpcfg tool is to dump the Config_Message_Log table of the Logger database and display the table in a meaningful format. The Config_Message_Log table keeps track of configuration changes in an IP Contact Center (IPCC) Enterprise environment.

Prerequisites

Requirements

Cisco recommends that you have knowledge of these topics:

- Cisco Intelligent Contact Management (ICM)
- Cisco IPCC

Components Used

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

- Cisco IPCC Enterprise Edition

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

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

Background Information

The ICM system keeps track of insertions, deletions and updates in the configuration database. The system retains this configuration history in a database table named Config_Message_Log.

Config_Message_Log is a database system table that stores configuration messages. Config_Message_Log contains these elements:

1. **RecoveryKey:** RecoveryKey is a value that the ICM software uses internally to track virtual time. This key can be converted to a twelve-digit configuration sequence number, which increments by one for each new record.
2. **LogOperation:** LogOperation indicates the type of configuration change. "Add" and "Update" are examples for LogOperation.
3. **TableName:** TableName represents the name of the table that the configuration change affects.
4. **DateTime:** DateTime indicates the date and time when a set of messages was logged.
5. **ConfigMessage:** ConfigMessage lists all configuration messages in a transaction.

Dump the Config_Message_Log

The Config_Message_Log table is rather cryptic in the native state. Therefore, in order to understand the Config_Message_Log table, you need to extract the data, and convert the data into a readable and meaningful format. The dumpcfg utility can process the data and display the information in this list:

- Who performed what operation
- When did a change occur
- Which program made the change

In order to view the details in the Config_Message_Log table, you can run the dumpcfg utility program. The audit trail of configuration changes appears. You can run the dumpcfg utility against the Logger database. Here is the syntax for this utility:

```
dumpcfg <database>[@server] <low recovery key> [high recovery key]
```

In this syntax:

- *< database >* represents the case-sensitive name of the Logger database, for example, lab60_sideA.
- *@server* represents the hostname of the ICM Admin Workstation (AW) or Logger.

Note: If you run the command at the server in question, substitute the @server with '@' character.

- *< low recovery key >* and *[high recovery key]* represent a configuration sequence number (the RecoveryKey field in the Config_Message_Log table). In order to track all changes, ICM increments this configuration sequence number (see pink rectangles in Figure 1).

Run this command to produce a complete dump of these changes:

```
dumpcfg lab60_sideA@. 0
```

Set the value of lowRecoveryKey to zero (0), and drop the highRecoveryKey (see arrow A in Figure 1).

Figure 1 displays the partial output of the dumpcfg program.

In order to run dumpcfg and store the output in an ASCII text file named **dumpcfg-output.txt**, run the command with this syntax:

```
dumpcfg lab60_sideA@. 0 > dumpcfg-output.txt
```

Figure 1 The dumpcfg Utility and Partial Output

```

C:\>dumpcfg lab60_sideA0. 0 ← A

[ 411867067000.0, First, Apr 18 2006 5:01PM ]
msgTransactionID: 12188

[ 411867067001.0, Add, Apr 18 2006 5:01PM ]
PID: 3708
MachineName: HPIPCCHDS
UserDomain: ICM60
UserName: khamb
ProcessName: conicrList(upcc)
SQLServerUserName: dbo

[ 411867067002.0, Add, User_Group, Apr 18 2006 5:01PM ]
ObjectAccessLevel: 0
UserGroupID: 5069
CustomerDefinitionID: 0
UserGroupType: U
ServiceProvider: Y
ReadOnly: N
FeatureSetID: 0
ChangeStamp: 0
UserGroupName: ICM60_test
Description: test

[ 411867067003.0, Add, User_Group_Member, Apr 18 2006 5:01PM ]
ObjectAccessLevel: 0
UserGroupMemberID: 5069
ChangeStamp: 0
UserGroupName: ICM60_test
UserName: ICM60_test

[ 411867067004.0, Last, Apr 18 2006 5:01PM ]
msgTransactionID: 12188

[ 411867067005.0, First, Apr 21 2006 3:39PM ]
msgTransactionID: 12190

[ 411867067006.0, Add, Apr 21 2006 3:39PM ]
PID: 3572
MachineName: HPIPCCHDS
UserDomain: ICM60
UserName: bphi
ProcessName: scripted(upcc)
SQLServerUserName: dbo

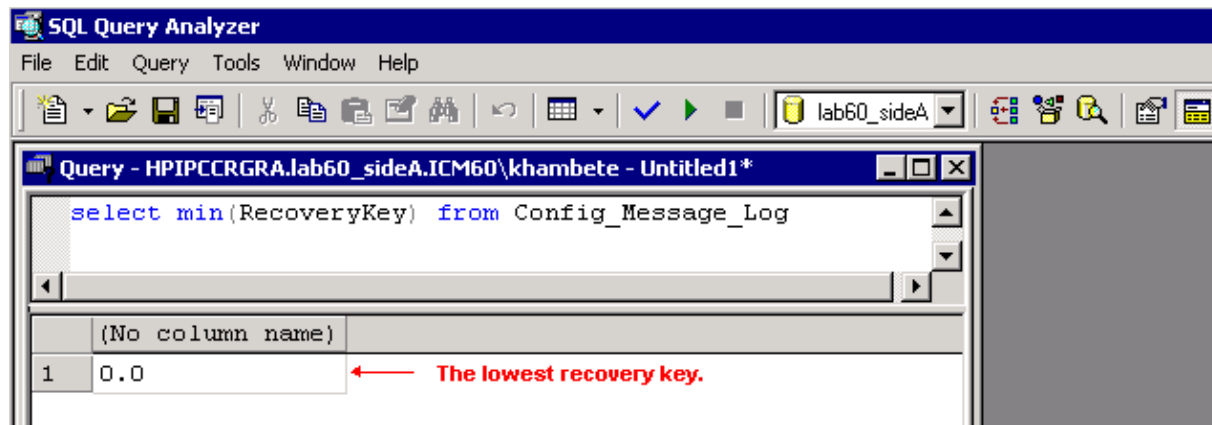
```

You can determine the actual sequence numbers from the configuration in one of these ways:

- Run these SQL commands:
 - ◆ In order to determine the lowest recovery key:

```
select min(RecoveryKey) from Config_Message_Log
```

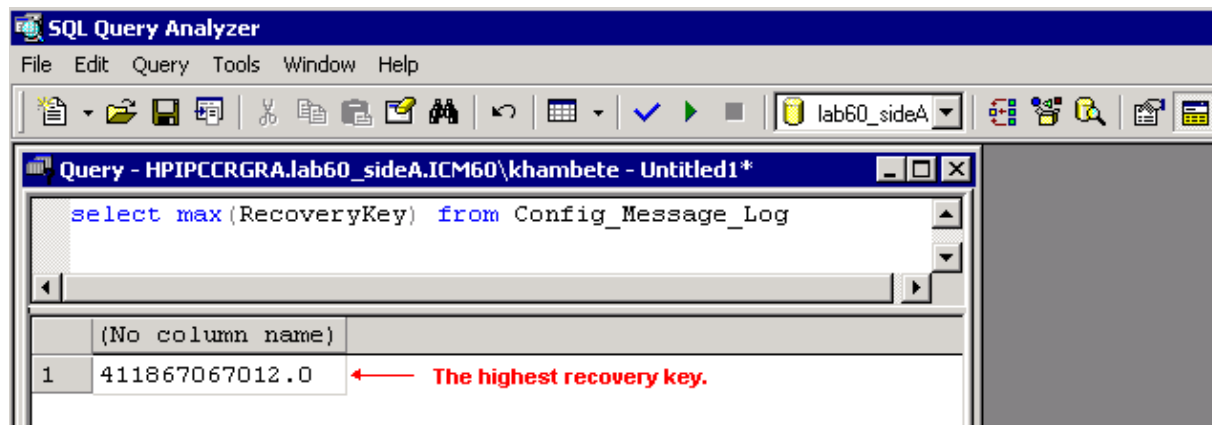
Figure 2 Dump the Lowest Recovery Key



- ◆ In order to determine the highest recovery key:

```
select max(RecoveryKey) from Config_Message_Log
```

Figure 3 Dump the Highest Key



- ◆ In order to specify a DateTime to obtain the changes that occur before or after a certain date or time:

```
select RecoveryKey from Config_Message_Log where  
DateTime >= '4/15/2006 00:00'
```

- Review the logs on the Router or Logger. Whenever you insert, update or delete a configuration or script, the Router or Logger includes the new sequence number in the logs:

```
15:25:35 ra-rtr The config sequence number of 411,969,759,020  
has been broadcast to all distributors.
```

Related Information

- **Technical Support & Documentation – Cisco Systems**

Contacts & Feedback | Help | Site Map

© 2013 – 2014 Cisco Systems, Inc. All rights reserved. Terms & Conditions | Privacy Statement | Cookie Policy | Trademarks of Cisco Systems, Inc.

Updated: Apr 24, 2006

Document ID: 69985