

CRPL (CICR Replication) Fails after Upgrade from Cisco Unified ICM Hosted Edition to ICM 7.0 with Access Error Code 9986

Document ID: 70536

Contents

Introduction

Prerequisites

- Requirements
- Components Used
- Conventions

CICM Replication

Events Seen within ICM / EMS Log Files Relevant to the CICR Replication Fault / Error Code 9986

Workaround

Defect Report Opened Against setup.exe Related to this Issue

Related Information

Introduction

When you upgrade the Cisco Unified Intelligent Contact Manager (ICM) Hosted Edition to ICM 7.0 and later, the CICR replication process (CRPL) does not have the proper rights and permissions in order to make configuration updates to the customer instances without the manual changes outlined within Active Directory. This document outlines the manual changes.

Note: The associations that are outlined within this document do not automatically occur with the installation and setup of ICM. These associations must be setup manually. Refer to Cisco bug ID CSCse55800 (registered customers only) for more information.

Prerequisites

Requirements

Cisco recommends that you have knowledge of these topics:

- Active Directory (AD) concepts
- Basic functionality of the CRPL

Components Used

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

- Cisco Unified ICM Hosted Edition Release 7.0(0) and later
- Microsoft AD

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.

CICM Replication

Customer ICM (CICM) replication within a Hosted ICM environment is a process that replicates configuration items from the Network Applications Manager (NAM) level to the CICM level (specifically dialed numbers and labels) without the need for an administrator to manually add the items in both places.

Events Seen within ICM / EMS Log Files Relevant to the CICR Replication Fault / Error Code 9986

The CRPL failure represented in these Event Management System (EMS) log segments is indicative of not having all the proper mappings. Mappings for the service logon account(s) of the NAM loggers, associated with the service security group of the specific customer instance(s), are missing.

Events from February 20, 2006:

```
11:51:51 lb-crpl Trace: Connecting to Cicr <customer Instance>
11:51:51 lb-crpl Trace: AwRtClient Client started at Mon Feb 20 11:51:51 2006
11:51:51 lb-crpl Trace: Real Time Feed activated from preferred side of
central controller.
11:51:51 lb-crpl Trace: Config Change message received, last update
key 406154682083.000000, last update time 877761033
11:51:51 lb-crpl Real-time Client cannot connect to database using
ServerName: geocustdist1b, UserName , SqlCode 3.
11:51:51 lb-crpl Session to local database could not be opened. Aborting...
11:51:51 lb-crpl Session to local database could not be opened. Aborting...
11:51:51 lb-crpl Trace: Connection to Cicr <customer Instance> Failed:
Initialize UpdateCC returned error code -9986: Session to local database
could not be opened.
```

Events from February 20, 2006:

```
11:51:51 dis-uaw Trace: New trace client: cicrreplication(upcc) on pipe 0x270.
11:51:51 dis-uaw Trace: [client: cicrreplication(upcc)] Real-time Client
cannot connect to database using ServerName: geocustdist1b, UserName , SqlCode 3.
11:51:51 dis-uaw Trace: [client: cicrreplication(upcc)] Session to local
database could not be opened. Aborting...
11:51:51 dis-uaw Trace: Info: Trace client on pipe 0x270 disconnected.
Last API Error [109]: Unknown status code 109. GetLastError() after
FormatMessage() returned 317
```

Workaround

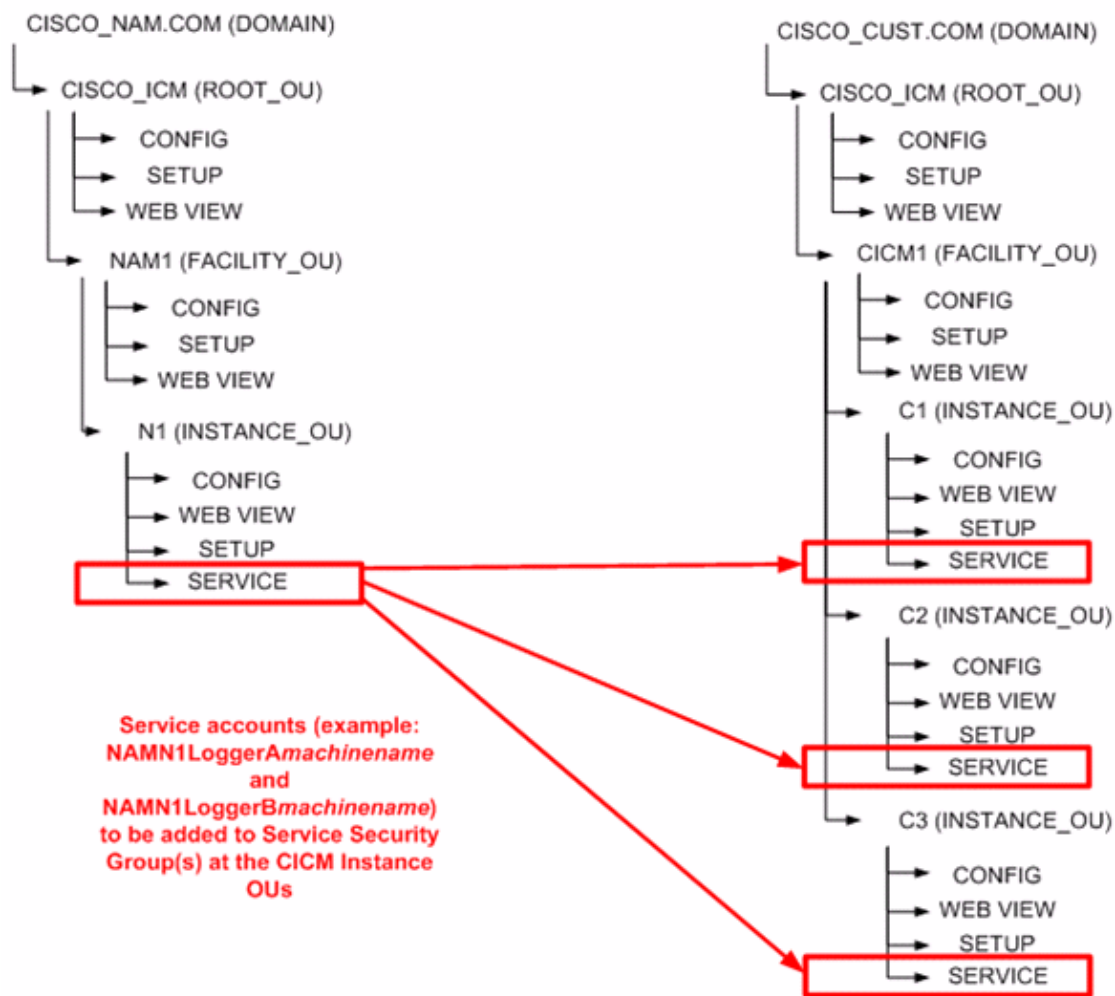
Through Active Directory Users and Computers, add the NAM logger A and B side service accounts (NAMN1LoggerAmachinename and NAMN1LoggerBmachinename) to the service security group of the specific customer instance at the CICM level. This must be done through Active Directory Users and Computers, and not the ICM Domain Manager tool.

Complete these steps:

1. Choose **Start > Program Files > Administrative Tools > Active Directory Users and Computers** on the Domain Controller.
2. Highlight the NAM instance at the Instance OU level in order to determine the name of the NAM instance service account.

3. In the diagram, the example is the N1 instance and the service security group is NAM1_N1_Service. Highlight and right-click this service group and choose **Properties**. Go to the **Member** tab and make a note of the logger service accounts called **NAMN1LoggerAmachinename** and **NAMN1LoggerBmachinename**.
4. Navigate to the CICM Customer Instance and highlight the **Instance OU**.
5. You see a Service security group within the right pane of the interface.
6. Highlight and right-click this service group and choose **Properties**.
7. Go to the Members tab and complete these steps:
 - a. Click **Add**.
 - b. Select the NAM domain.
 - c. Add the service accounts of the NAM loggers that you made note of in step 3.

This diagram is one example of what a typical hosted domain structure could look like. The groups that are relevant to this solution are highlighted.



Note: The workaround procedure in this document is not a one-time fix. Each time the ICM setup is run, the configuration group accounts are automatically reset. Therefore, this procedure must be repeated each time the setup is run.

Defect Report Opened Against setup.exe Related to this Issue

This issue is outlined in Cisco bug ID CSCse55800 (registered customers only) . Cisco bug ID CSCse55800 provides individuals who have a valid CCO ID with the official description and release notes for this issue, including the workaround steps noted in this document.

Related Information

- **Upgrade Guide Cisco ICM/IPCC Enterprise & Hosted Editions**
 - **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: Oct 11, 2006

Document ID: 70536
