

IPCC/ICM Server Best Practices Checklist

Document ID: 89948

Introduction

Prerequisites

- Requirements
- Components Used
- Conventions

Checklist

- ICM Configuration
- Network Configuration
- Network Interface Cards (NIC) Settings
- Third Party Configuration and Settings
- Tracing Recommendations

Related Information

Introduction

The purpose of this checklist is to eliminate known issues that lead to call processing problems for the Cisco Unified Contact Center (UCC) and Cisco Unified Intelligent Contact Management (ICM) products. Complete this checklist and provide the information to the Cisco Technical Assistance Center (TAC).

Prerequisites

Requirements

Cisco recommends that you have knowledge of these topics:

- Cisco ICM Enterprise and Hosted Editions
- Cisco UCC Enterprise and Hosted Editions
- Cisco Customer Response Solutions (CRS)
- Cisco Customer Voice Portal (CVP), formerly known as Cisco Internet Service Node (ISN)
- Cisco CallManager
- Microsoft Windows

Components Used

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

- Cisco ICM/UCC version 4.6.2 and later
- Microsoft Windows 2000
- Microsoft Windows 2003

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.

Checklist

ICM Configuration

Review the items in this checklist:

1. What software version(s) is used?
2. Are there any ICM configuration changes?
3. If yes, what changes?
4. Are these changes confirmed by the ICM Administrators?
5. Does the dumpcfg Administration Tool capture any configuration changes?
6. If yes, provide this information to TAC with this checklist.

Network Configuration

Review the items in this checklist:

1. Are there any network infrastructure changes?
2. If yes, what changes?
3. Are these changes confirmed by network Administrators?

Complete these baseline steps in order to troubleshoot the network:

1. Request an up-to-date, accurate network diagram that shows all the switches, routers and circuits.
2. Provide the output from the Trace Route Utility (tracert) from Host 1 to Host 2, which includes private and private-high addresses, as well as the reverse from Host 2 to Host 1. Perform the tracert "by name" if you use names in the setup in order to verify the hostname-to-IP address resolution is proper.
3. Provide the show tech-support output from all the private network switches and IP routers.
4. In the show tech-support output, verify that the Quality of Service (QoS) is properly enabled as described in Solution Reference Network Design (SRND).

Network Interface Cards (NIC) Settings

Complete these steps:

1. Verify that all of the NIC settings and switch ports are coded appropriately in order to avoid duplex mismatch errors. One of these settings must used:
 - ◆ 100 Mb NIC set both the NIC and the switch to 100/Full.
 - ◆ 100 Mb switch set both the NIC and the switch to 100 Mb.
 - ◆ 100 Mb NIC and 100 Mb switch set both the NIC and the switch to 100/Full.
 - ◆ Gigabit NIC and Gigabit switch ensure that both are set to Auto/Auto.
 - ◆ Avaya ensure that the NIC speed matches that of the MAP-D.
2. Verify that the NIC Binding Order is set correctly in order to be Visible on top of Private.
3. Verify that NIC teaming is disabled.

Refer to this document for more information on the completion of these tasks:

Third Party Configuration and Settings

Complete these steps:

1. Verify that Hyper-Threading is disabled for Windows 2000 servers. Refer to Field Notice: FN-62518 – Media Convergence Servers with Hyperthreading Enabled May Experience Call Processing Failures for more information.
2. If the server runs Windows 2003, verify that the TCP/IP SACK Patch is applied. Refer to Field Notice: FN – 62508 – Unified Contact Center Enterprise/Hosted, Unified ICM Enterprise/Hosted TCP/IP Private Path Network Failure – Windows Server 2003 SP1 for more information.
3. Determine if Network Associates VirusScan or another Anti-Virus software is in use. If it is in use, verify it is configured properly:
 - ◆ On-Access scanning must be enabled for inbound files only.
 - ◆ Drive scanning must take place weekly, during an off-peak time outside of normal business hours.
 - ◆ The HST and EMS files must be excluded.Refer to Security Best Practices for Cisco Intelligent Contact Management Software Release 6.0(0) for more information.
4. Determine if any Third Party software applications run on any IPCC system components and verify that they are not the root cause of the system instability. Refer to Cisco Customer Contact Software Policy for use of Third-Party Software and Security Updates for more information.
5. Verify the Logger Database settings:
 - ◆ Verify that the Logger database is sized appropriately.
 - ◆ Determine on which partition the SQL server files reside.
 - ◆ Determine how much memory is dedicated for the SQL server and whether it is dynamic or fixed.Refer to Cisco ICM Enterprise Edition Release 6.0(0) Administration Guide for more information.
6. Verify that all of the hardware meets the Bill of Material. Refer to these documents for more information:
 - ◆ Cisco Intelligent Contact Management Software Release 7.0 (0) SR1 – SR4 & 7.1 (x) Bill of Materials
 - ◆ Cisco Intelligent Contact Management Software Release 6.0(0) Bill of Materials
7. Verify that the EMSDisplaytoScreen feature for all ICM processes is set to zero through the registry, and minimize all of the process windows in order to prevent excessive memory usage by the ICM process windows. Refer to Turning up Tracing for more information.
8. Verify that clock synchronization best practices are used in order to ensure that all devices are synchronized. Refer to Cisco IP Telephony Clock Synchronization: Best Practices for more information.

Tracing Recommendations

If these steps do not resolve the problem, it can be necessary to apply tracing in order to further troubleshoot the issue. Refer to these basic guidelines in order to troubleshoot the problem:

- ICM Tracing Contact Cisco TAC for specific tracing levels for ICM processes.
- IPCC Tracing Refer to Recommended Tracing Levels for Troubleshooting IPCC Issues.
- CVP Tracing Refer to Recommended Trace Levels for CVP/ISN.
- CRS Tracing Refer to CRS Quick Tracing Guide for Version 3.x and 4.0.x or Setting up, Viewing

and Collecting Cisco IPCC Express Traces.

Related Information

- [Cisco Support Tools 2.0 Data Sheet](#)
 - [Technical Support & Documentation – 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: May 11, 2008

Document ID: 89948
