Testing

Testing Overview

System testing is a part of the installation, upgrade, and ongoing maintenance of a Unified CCE solution. Testing requirements and processes vary from customer to customer. Therefore, specific steps for executing tests are not included in this document.

For installations, testing must ensure all aspects of contact center operation before going live.

For upgrades, at the beginning of each maintenance window, consider running preupgrade tests to establish a benchmark. The benchmark is used when you run the postupgrade tests. Postupgrade tests are necessary for each maintenance window to ensure continued contact center operation throughout the entire upgrade process, which can span multiple maintenance windows.

If you require assistance with Unified CCE solution testing, work with your Cisco representative.

Contact centers need established tests plans and processes for all aspects of contact center operation. Have the plans, tools, and processes in place to test your contact center.

Testing Tasks

Verify Upgrade to Cisco Unified Customer Voice Portal

After upgrading Unified CVP, verify the following:

Procedure

Step 1 Verify that error messages did not display during the upgrade process.

Step 2 Check the upgrade logs for error messages.

Step 3 Ensure that the Unified CVP Operations, Administration, Monitoring and Provisioning (OAMP) Web interface is available for use.

Step 4 Use the diagnostic page at http://<CVPHOST>:8000/cvp/diag to verify the status of the Unified CVP system.

Step 5 Use the Operations Console (**System** > **Control Center**, Device Pool tab) to verify that the upgraded Unified CVP Call Servers, Unified CVP VXML Server and Unified CVP Reporting Server show a status of "Up".

Step 6 Use the Operations Console (**Device Management** > **Unified CVP Call Server**, General tab for selected Call Server) to verify that the Device Version reflects the correct upgraded version.

Step 7 Verify that the appropriate voice prompt is heard when the call is made.

Step 8 Ensure that the Unified CVP license is properly installed.

Verify IOS Gateway Upgrade

After upgrading IOS gateways, verify the following:

Procedure

Step 1 At the Cisco IOS exec level, execute the following CLI commands:

- To check that the upgraded IOS target image is running:

  show version

- To verify that the boot system is configured to boot the correct image:

  show running-config

- To verify that configuration done previously is not lost:

  show running-config

- To verify that the ISDN connection status is at MULTIFRAME_ESTABLISHED:

  show isdn status

- To verify that configured interfaces are in up/up state:

  show ip interface brief

- To verify manually placed incoming calls:

  show isdn history

- To verify IP routing from branch site to a data center:

  ping or **traceroute**

- To verify IP routing from one branch site to another branch site:

  ping or **traceroute**

Step 2 Ensure that the following devices are configured and registered correctly: Gatekeeper, trunks, and CTI Route Point.

Step 3 Ensure that all MGCP end points (FXS, FXO, PRI, T1 CAS and BRI) are properly registered with Unified Communications Manager.

Step 4 Manually spot check calls as appropriate from the PSTN vis SIP Gateways.

Step 5 Verify that a PSTN user who places an inbound call from the PSTN to a Unified IP Phone in a Unified Communications Manager cluster through gateways and puts the call on hold can hear Music-on-Hold (MOH) and can also finally resume the call.

Verify Upgrade to Cisco IOS-Based Transcoders and Conference Bridges

After upgrading Cisco IOS-based transcoders and conference bridges, verify the following:

Procedure

Step 1 Check if the complete configuration before the upgrade still exists.

Step 2 Check if all DSPs are registered and are functioning normally.

Step 3 Check if there are no error messages in the buffer log or console.

Step 4 Check if no dump file is created in the flash memory.

Step 5 To verify that the configuration is not lost, type the “show running-config” command.

Step 6 To verify that the interfaces are in up state, type the “show ip interface brief” command.

Step 7 Verify IOS Transcoding is working with G711 codec configure for one device while G729 codec is configured on another device.

Verify Upgrade to Cisco Unified CCE Router and Logger

After upgrading the Cisco Unified CCE Router and Logger, verify the following:

Procedure

Step 1 Verify basic operations such as the following:

- Setup logs indicate no errors or failure conditions (icmsetup.txt and ICMInstall.txt, located in the \Temp directory of the disk on which the application was installed).
- All components can “ping” public and private IP addresses as applicable.
- Schema upgrade is successful for all databases and there is no loss of data integrity or data.
- All component services start correctly without generating errors.
- Firewalls and other security measures do not block the ability to access Microsoft SQL Server and to run third-party software components, like VNC or PCAnywhere.
- Ccagent is in service and connected to any Peripheral Gateways located in Side A.
- Recovery process not required, no activity other than process start-up.
- Configuration information is passed to the Router by the Logger. Replication process begins when the Historical Database Server comes online.
- Replication process begins with no errors. (Use the Windows Event Viewer to view Windows Event logs).
- The Router is in a synchronized state. (Use the Diagnostic Framework Portico, under **ListProcesses**, verify that the status of ccagent and mdsproc is "InSvc".)

- Database space allocation and % used are reported correctly. (Use the dumplog utility to view the hlgr and rcv processes on the Logger server. The trace messages display the percentage of available free space and the log space of the database at 30-second intervals. Verify this using Microsoft SQL Management Studio to view the Logger database properties.)

Step 2 Use the Windows Event Viewer on each server to check that no exceptions, errors, or unexpected events have occurred. Select **Administrative Tools** > **Event Viewer**, then expand **Windows Logs** and review the Application and System logs.

Step 3 Verify that configuration changes can be made and are passed to the Logger and AW databases.

Step 4 Ensure that basic calls and call functionality such as transfers, conferences, call treatment and queuing are working properly.

Verify Upgrade to Cisco Real Time Administration Workstation, Historical Database Server

After upgrading the Real Time AW/HDS software, verify the following:

Procedure

Step 1 Use the Windows Event Viewer on each server to check that no exceptions, errors, or unexpected events have occurred. Select **Administrative Tools** > **Event Viewer**, then expand **Windows Logs** and review the Application and System logs.

Step 2 After Side A Central Controller components have been upgraded, verify basic operations such as the following:

- Setup logs indicate no errors or failure conditions (icmsetup.txt and ICMInstall.txt located in the \Temp directory of the disk on which the application was installed).
- All components can “ping” public and private IP addresses as applicable.
- Schema upgrade is successful for all databases and there is no loss of data integrity or data.
- All component services start correctly without generating errors.
- All general activities such as the ability to access SQL server and to run third-party software components like VNC or PCAnywhere, etc. are not stopped by any security application.
- Rtsvr, the process that provides real time data from the Router to the AW database, is connected to the primary Administrative Workstation. (Open the Configuration Manager tool on Administration & Data server. If the tool opens without any errors, the feed is active. Additionally, use the Dumplog utility to view the uaw process. The uaw trace message shows "Waiting for new work…".)
- Configuration information is passed to the router by the Logger. Replication process begins when the Historical Database Server comes online.
- Real Time Administrative Workstation indicates that it is ready.
- Replication process begins with no errors. (use the Windows Event Viewer to view Windows Event logs).
- Authorized users are able to use the Configuration Manager on the Real Time Administrative Workstation.
- Authorized users are able to log into Cisco Unified Intelligence Center and can access both public and private reports and that all previously existing reports are still available.
- Previous settings for users are still valid when any application is opened.
- The “Validate All” script yields the same results after the upgrade as prior to the upgrade.

Note All existing scripts can be opened and edited and new scripts can be created.

- Database space allocation and % used are reported correctly. (Use the dumplog utility to view the hlgr and rcv processes on the Logger server. The trace messages display the percentage of available free space and the log space of the database at 30 second intervals. Verify this using Microsoft SQL Management Studio to view the Logger database properties.)
- Diagnostic Framework Portico can acquire logs, capture registry information, and schedule collection of logs.
- Verify that configuration changes are possible.

Verify Upgrade to Peripheral Gateways

After upgrading the peripheral gateways, verify the following:

Procedure

Step 1 Use the Windows Event Viewer on each server to check that no exceptions, errors, or unexpected events have occurred. Select **Administrative Tools** > **Event Viewer**, then expand **Windows Logs** and review the Application and System logs.

Step 2 Ensure that real time and historical data is sent to the Router and AW database.

Step 3 Ensure that basic calls and call functionality (such as transfers, conferences, call treatment and queuing) are working properly.

Step 4 Ensure that the peripheral is running properly on the upgraded gateway by verifying call flows, CTI desktops, Outbound Option, and other applications.

Verify Redundancy

After you upgrade both sides of all redundant components, verify the following:

Procedure

Step 1 Stop each active component.

Step 2 Ensure that the backup component assumes an active state and that the system operation switches to the backup component with no loss of functionality.

Verify Upgrade to Cisco Unified Communications Manager

After upgrading Unified Communications Manager, verify the following:

Procedure

Step 1 Verify that no error messages have occurred during the upgrade process.

Step 2 Check the upgrade log file for any errors.

Step 3 Start all first node and subsequent node servers.

Step 4 Verify that there is no replication failure between the first node and subsequent node servers.

Step 5 Verify that SIP and SCCP IP Phones are registered with Unified Communications Manager.

Step 6 Ensure that the following devices are configured correctly: gatekeeper, trunks, and CTI route points.

Step 7 Ensure that the media resources (conference bridges, MTP and transcoders) are configured correctly by checking their status.

Step 8 Verify if the end users are able to connect to their CTI managers.

Step 9 Check if the license usage is correct as reported in the License Unit Report.

Step 10 Check if services on all servers in the cluster are up.

Step 11 Perform the Unified Communications Manager first node and subsequent node process verification using the following Real Time Monitoring Tool feature verification process:

a) Verify if Multiple Route Patterns and Route Lists are configured and working properly.
b) Verify if Extension Mobility is configured and working properly.
c) Verify if Unified IP Phone Services are configured and working properly.