Cisco Remote Expert Manager 1.9.2 Troubleshooting and Serviceability Guide

Release 1.9.2

August 21, 2014

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883

Text Part Number: OL-27568-05

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

The following information is for FCC compliance of Class A devices: This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to part 15 of the FCC rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio-frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference, in which case users will be required to correct the interference at their own expense.

Modifications to this product not authorized by Cisco could void the FCC approval and negate your authority to operate the product.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED "AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

CCDE, CCENT, CCSI, Cisco Eos, Cisco HealthPresence, Cisco IronPort, the Cisco logo, Cisco Nurse Connect, Cisco Pulse, Cisco SensorBase, Cisco StackPower, Cisco StadiumVision, Cisco TelePresence, Cisco Unified Computing System, Cisco WebEx, DCE, Flip Channels, Flip for Good, Flip Mino, Flipshare (Design), Flip Ultra, Flip Video, Flip Video (Design), Instant Broadband, and Welcome to the Human Network are trademarks; Changing the Way We Work, Live, Play, and Learn, Cisco Capital, Cisco Capital (Design), Cisco:Financed (Stylized), Cisco Store, Flip Gift Card, and One Million Acts of Green are service marks; and Access Registrar, Aironet, AllTouch, AsyncOS, Bringing the Meeting To You, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, CCVP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Lumin, Cisco Nexus, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Collaboration Without Limitation, Continuum, EtherFast, EtherSwitch, Event Center, Explorer, Follow Me Browsing, GainMaker, iLYNX, IOS, iPhone, IronPort, the IronPort logo, Laser Link, LightStream, Linksys, MeetingPlace, MeetingPlace Chime Sound, MGX, Networkers, Networking Academy, PCNow, PIX, PowerKEY, PowerPanels, PowerTV, PowerTV (Design), PowerVu, Prisma, ProConnect, ROSA, SenderBase, SMARTnet, Spectrum Expert, StackWise, WebEx, and the WebEx logo are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0910R)

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.

Cisco Remote Expert Manager Troubleshooting and Serviceability Guide
© 2014 Cisco Systems, Inc. All rights reserved.

CONTENTS

Preface

Revised: August 21, 2014, OL-27568-05

Note All advertising materials mentioning features or use of this software must display the following acknowledgement: "*This product includes software developed by the University of California, Berkeley and its contributors.*"

Overview

This preface describes the audience, organization, and conventions of this guide for release 1.9.2. It also provides information on related documentation. This preface includes the following sections:

Audience

This guide is intended for customers, partners, and the Advanced Services team who will troubleshoot the hardware and software at the data center, contact center, and branches. It is also intended for administrators who will keep the application up and running.

Purpose

This guide provides the information that you need to troubleshoot and maintain serviceability for the Cisco Remote Expert Manager (REM).

Organization

This guide is organized into the following chapters:

Chapter	Title	Description
1	REM Troubleshooting	Explains how to troubleshoot common problems
2	Serviceability Administration	Assists administrators with maintaining the REM application

Related Documentation

These documents provide additional information about the Cisco Remote Expert Smart solution:

Cisco Remote Expert Manager 1.9.2 Installation Guide

http://www.cisco.com/c/en/us/support/customer-collaboration/remote-expert-manager/products-installation-guides-list.html

Cisco Remote Expert Manager 1.9.2 Port Usage Guide

http://www.cisco.com/c/en/us/support/customer-collaboration/remote-expert-manager/products-installation-guides-list.html

Cisco Remote Expert Manager 1.9.2 Administration Guide

http://www.cisco.com/c/en/us/support/customer-collaboration/remote-expert-manager/products-maintenance-guides-list.html

Cisco Remote Expert Manager 1.9.2 READ, eREAD, and mREAD User Guide

http://www.cisco.com/c/en/us/support/customer-collaboration/remote-expert-manager/products-user-guide-list.html

Cisco Remote Expert Manager 1.9.2 Release Notes

http://www.cisco.com/c/en/us/support/customer-collaboration/remote-expert-manager/products-release-notes-list.html

Cisco Remote Expert Smart Solution 1.9.2 Migration Guide

http://www.cisco.com/c/en/us/support/customer-collaboration/remote-expert-manager/products-installation-guides-list.html

REM Troubleshooting

Revised: August 21, 2014, OL-27568-05

Chapter Overview

This chapter explains how to troubleshoot common problems.

Topics in this chapter include:

Introduction

This document discusses and solves the most common problems that have been reported during testing and also from the field. This document also explains necessary call flow to help you understand the logic to make troubleshooting easier.

Prerequisites

This document assumes that you know the working of Cisco Unified Communication Manager (UCM), Cisco Unified Contact Center Express (UCCX), Cisco Unified Contact Center Enterprise (UCCE), and Cisco TelePresence (TP) video endpoints.

Components Used

This document is not restricted to specific software and hardware versions.

Conventions

Refer to Cisco Technical Tips Conventions for more information on document conventions: http://www.cisco.com/en/US/tech/tk801/tk36/technologies_tech_note09186a0080121ac5.shtml.

Troubleshooting Methodology

In order to isolate the issue and resolve it, it is important to follow a methodology. A high level troubleshooting process flow is a good way to isolate problem components from the overall solution.

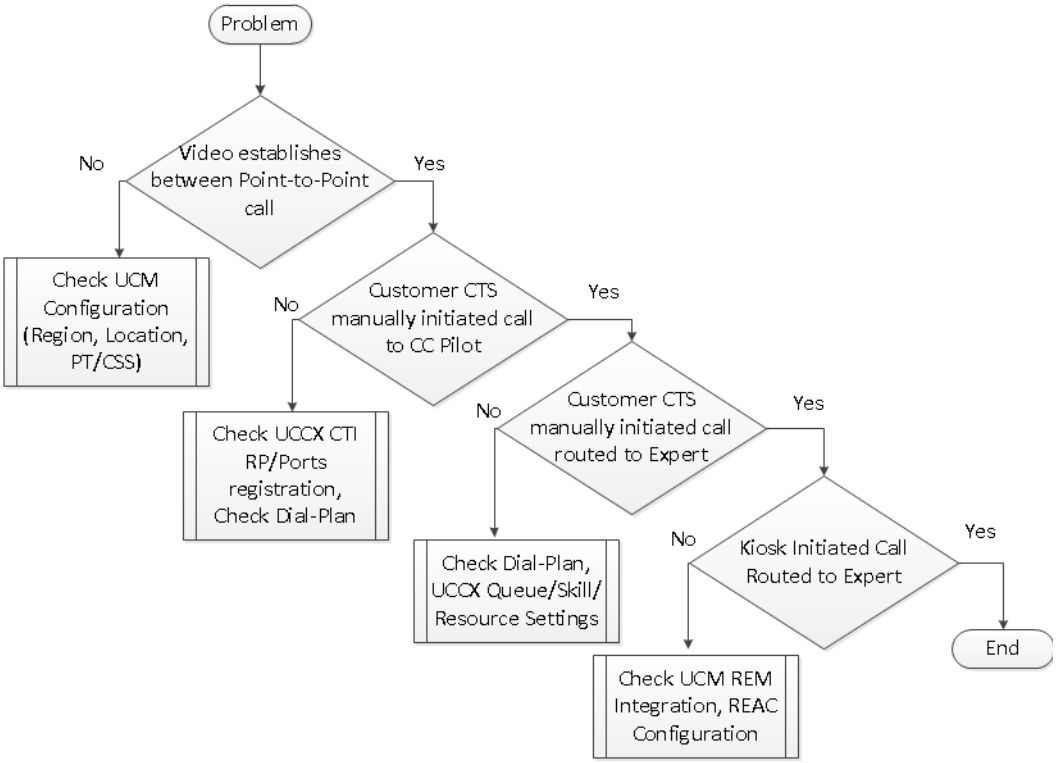
There are mainly three components involved in the Cisco Remote Expert Solution:

1. Unified Communication Manager and its endpoints
2. Unified Contact Center Express and experts
3. Remote Expert Manager and its components

A “Divide and Conquer” troubleshooting approach is suggested in order to isolate the problem component within the solution. For example, without using the customer pod, determine if the other components of the solution are functioning correctly. Is it possible, for example, to manually initiate a call from the branch TP video endpoint and successfully route the call to an expert via Contact Center? If the answer is “no”, then at least part of the problem lies within the CUCM/UCCX/UCCE infrastructure. Correct that problem before determining if REM troubleshooting is necessary.

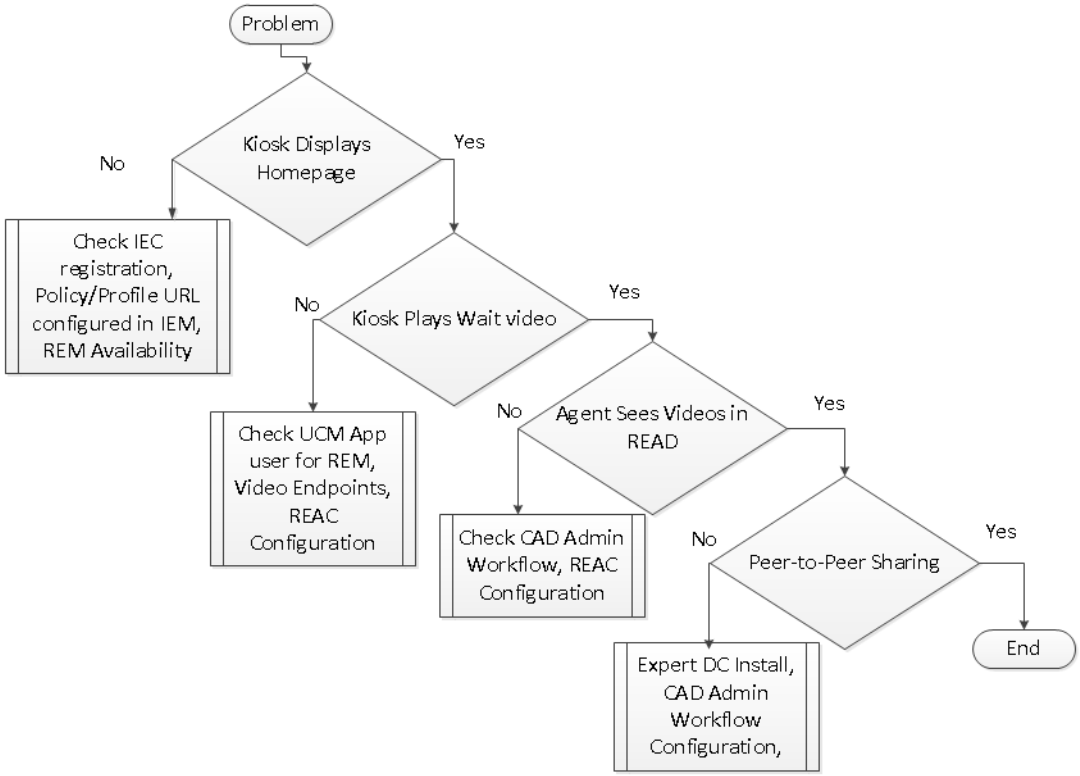
Review the flowchart below to troubleshoot UCM and UCCX/UCCE issues.

Figure 1-1 Troubleshooting Flowchart for UCM and UCCX/UCCE Issues



If customer-side/branch site manually initiated call can be successfully routed to an expert and answered by an expert, but does not work from the customer pod, then it could be a REM-related issue. In that instance, the following flowchart may be helpful.

Figure 1-2 Troubleshooting Flowchart for REM-Related Issues



Possible Errors & Troubleshooting Tips

This section documents errors that customers may encounter and how to fix them.

Table 1-1 Possible Errors and Reasons

Possible Errors	Components Involved	Possible Reasons
Customer pod has no display	Monitor IEC	1. Check whether monitor is working and the power is connected. 2. If monitor was connected after the IEC was booted up, reboot the IEC. 3. Try connecting the monitor to IEC's alternate video port (VGA or HDMI).
IEC displays 'Management failure: Product VEP is not found'	IEC	The IEC has an older version of firmware. Upgrade the IEC's firmware.

Possible Errors	Components Involved	Possible Reasons
IEC displays 'Network Error'	IEC LAN Cable/Switch DHCP Server	If LAN cable was connected after the IEC was booted, reboot the IEC. Check the network connection. If it is DHCP-based, check whether the DHCP server is correctly leasing an IP address to the IEC.
IEC displays 'Kiosk Phone is out of Service'	Customer pod-side video endpoint	Customer pod-side video endpoint is unregistered from the UCM.
IEC reboots in certain cases	REM Customer pod-side video endpoint	The following are some of the scenarios in which reboot is initiated from REM: • Whenever there is a power failure, REM reboots the IEC to identify all peripherals that are connected. • If customer pod-side video endpoint goes down and comes up, REM reboots the IEC. • If the Cobra application is not working normally, REM reboots the IEC.
IEC is not streaming video such as the On Hold Video or a video that was pushed from an expert	RTMP Compliant Streaming Server	1. Check RTMP Compliant Streaming Server is up. 2. If the agent is not registered, the call will not be connected to the agent who then will not be able to load READ. Also, the Kiosk will not move to the connected screen.
Agent Desktop displays 'Checking for Active Session' continually, even after accepting the call	REM Contact Center CAD Admin Workflow	1. Validate Expert configuration in REAC. 2. Verify CAD Workflow settings.

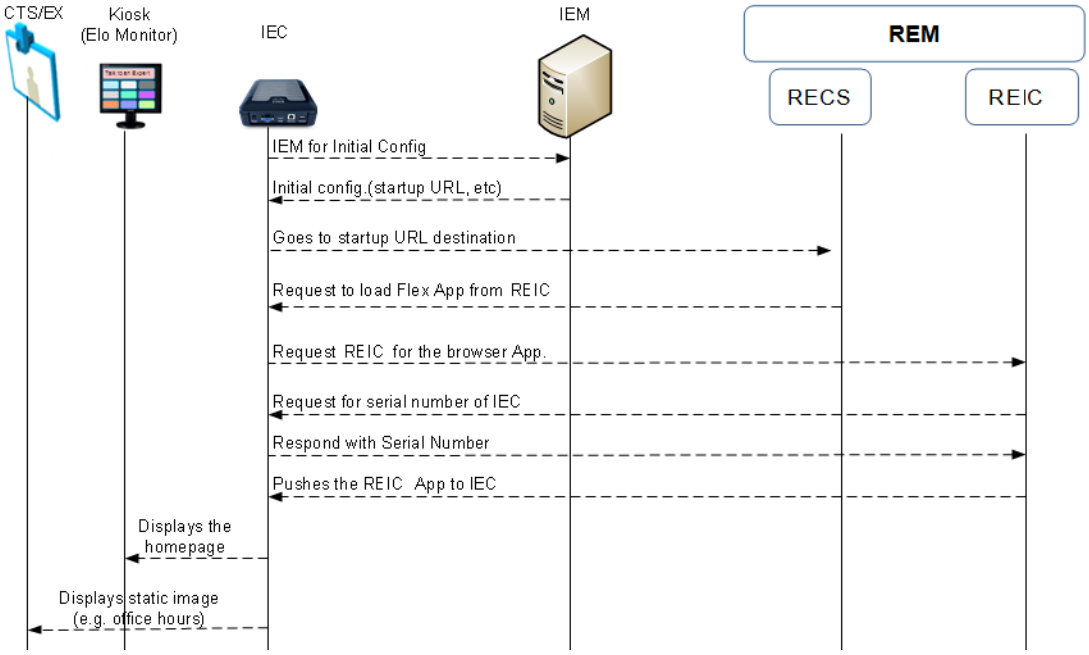
Additional issues and how to solve them are described below.

Unable to Bring Up Kiosk Flex Application on the Customer Pod's Home Page

The call flow that is related to the customer pod's display page is the following:

1. While the IEC boots up, the IEC contacts the IEM for its home page URL (startup URL in the IEM) which is hosted on REM.
2. The IEC goes to the URL destination listed in the startup URL of the IEM's policy.
3. The REM (the destination of the URL) requests the IEC to load the Kiosk Flex application.
4. While requesting to load the Kiosk Flex application, the Kiosk Flex application queries the IEC for its serial number.
5. The IEC responds with its serial number.
6. If the IEC's serial number matches what is configured in the REM, the Kiosk Flex application is loaded into the IEC and the IEC displays the home page with a connect button on the customer pod.
7. The IEC also displays a static image on the TP video endpoint (e.g. office hours).

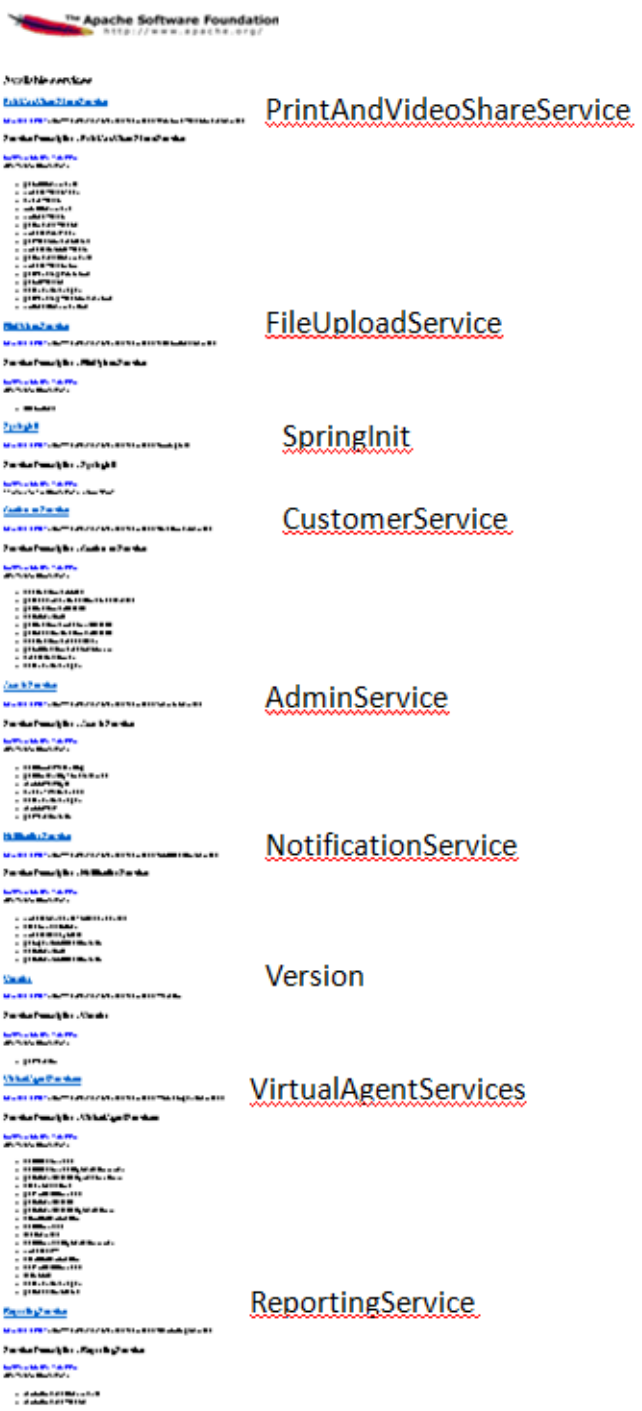
Figure 1-3 Call Flow



If you are unable to bring up the Kiosk Flex application, the following are possible reasons:

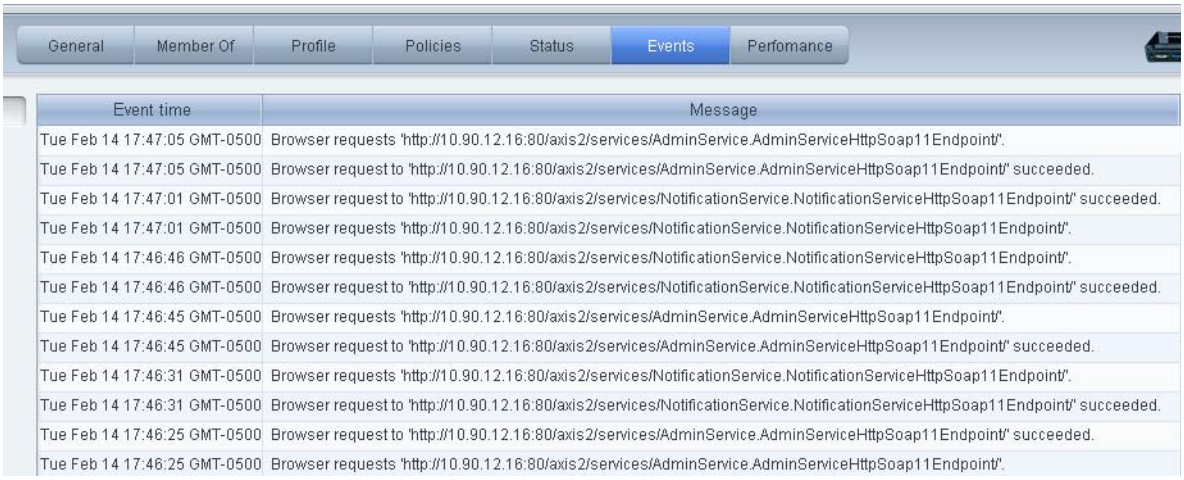
- The IEC was configured with the wrong IEM host information. Verify that the IEM's URL is correct in the IEC and the IEM shows that the IEC is active.
- The URL configured in the IEM is incorrect. First put the default kiosk serial number in rem.properties and run the configuration tool. Then register the kiosk with the default IEC in REAC. Verify that the URL is correct by typing "https://<REM_IP>:8443/reic" in a browser. You should see the same homepage with the connect button on the browser window and be able to click the connect button with a mouse. As a result, a call will try to connect with the video endpoint using the UCCX/UCCE Pilot number.
- The IEC does not have the correct policy applied. Verify that the policy with the REM's URL as the startup URL was applied to the IEC in the IEM.
- The IEC is unable to reach the IEM. This could be a network problem (e.g. Local LAN issue, WAN issue, or cable issue). If the REM's FQDN is used, it could be that DNS server is either incorrectly configured or not reachable. Ping the REM from IEC's console to ensure that it is pingable.
- The LAN connection may not have been up when the IEC was booting up. Reboot the IEC.
- The web service may not be up. Verify that all nine web services are up by entering the URL "https://<REM_IP>:8443/resc/services/listServices".

Figure 1-4 Web Services



- The IEC's serial number is listed incorrectly in the REM. Verify that the REM's Kiosk configuration window is showing the correct serial number of the IEC.
- Check the IEC's event log from IEM for more information. Refer to the "Events Tab in the IEM" section in the Serviceability Administration chapter for detailed information on how to check an IEC's logs.

Figure 1-5 Event Log



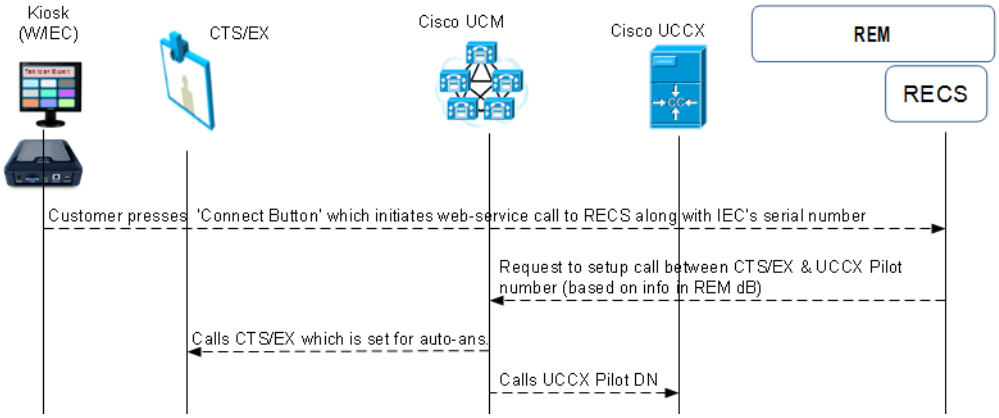
Event time	Message
Tue Feb 14 17:47:05 GMT-0500	Browser requests 'http://10.90.12.16:80/axis2/services/AdminService.AdminServiceHttpSoap11Endpoint/'.
Tue Feb 14 17:47:05 GMT-0500	Browser request to 'http://10.90.12.16:80/axis2/services/AdminService.AdminServiceHttpSoap11Endpoint/' succeeded.
Tue Feb 14 17:47:01 GMT-0500	Browser request to 'http://10.90.12.16:80/axis2/services/NotificationService.NotificationServiceHttpSoap11Endpoint/' succeeded.
Tue Feb 14 17:47:01 GMT-0500	Browser requests 'http://10.90.12.16:80/axis2/services/NotificationService.NotificationServiceHttpSoap11Endpoint/'.
Tue Feb 14 17:46:46 GMT-0500	Browser requests 'http://10.90.12.16:80/axis2/services/NotificationService.NotificationServiceHttpSoap11Endpoint/'.
Tue Feb 14 17:46:46 GMT-0500	Browser request to 'http://10.90.12.16:80/axis2/services/NotificationService.NotificationServiceHttpSoap11Endpoint/' succeeded.
Tue Feb 14 17:46:45 GMT-0500	Browser requests 'http://10.90.12.16:80/axis2/services/AdminService.AdminServiceHttpSoap11Endpoint/'.
Tue Feb 14 17:46:45 GMT-0500	Browser request to 'http://10.90.12.16:80/axis2/services/AdminService.AdminServiceHttpSoap11Endpoint/' succeeded.
Tue Feb 14 17:46:31 GMT-0500	Browser requests 'http://10.90.12.16:80/axis2/services/NotificationService.NotificationServiceHttpSoap11Endpoint/'.
Tue Feb 14 17:46:31 GMT-0500	Browser request to 'http://10.90.12.16:80/axis2/services/NotificationService.NotificationServiceHttpSoap11Endpoint/' succeeded.
Tue Feb 14 17:46:25 GMT-0500	Browser request to 'http://10.90.12.16:80/axis2/services/AdminService.AdminServiceHttpSoap11Endpoint/' succeeded.
Tue Feb 14 17:46:25 GMT-0500	Browser requests 'http://10.90.12.16:80/axis2/services/AdminService.AdminServiceHttpSoap11Endpoint/'.

Unable to Establish Call from Customer Pod ('System Error' Message)

When a customer presses the Connect button, the call flow is the following:

1. The Kiosk application invokes the REM's call connect web service.
2. The REM requests the CUCM to set up a call via JTAPI between the customer pod's video endpoint DN and UCCX/UCCE Pilot DN.
3. The CUCM initiates a call from the customer pod's TP video endpoint to UCCX/UCCE Pilot DN and the call is established.

Figure 1-6 Call Flow



When a call is unable to be established, the following are possible reasons:

Configuration data is incorrect in the REM:

- The TelePresence DN of the customer pod's video endpoint is listed incorrectly in REM. Check the Kiosk configuration in the REAC.
- The IVR Phone number is listed incorrectly in the REM. Check the Expert Type configuration in the REAC.

  - The customer pod's video endpoint is not listed in the CUCM's application user (ragent) control list. Include the customer pod's video endpoint into the REM's control list.
  - The CUCM's application user (ragent) either does not exist or the user's password is not matching the password in the REM configuration.
  - The REM has incorrect CUCM credentials (username, password, IP addresses).
  - The REM may have duplicate entries for the customer pod's video-endpoint (DN).
- Problem with the JTAPI links to either the REM or to UCCX/UCCE:
  - Check that the JTAPI link between REM and CUCM is up and running.
  - Check that the JTAPI link between CUCM and UCCX/UCCE is up and running by checking the CTI Route Point's status in the CUCM administration page.
- Problem with endpoints:
  - The customer pod's video endpoint is not in the active state (e.g. upgrading firmware or rebooting state).
  - The UCCX/UCCE ports are maxed out and hence unable to establish a call with UCCX/UCCE (e.g. UCCX/UCCE getting more calls than it can support).

Customer Pod Displays 'Error: Management Server is not reachable' Message

The message "Management Server is not reachable" indicates that the IEM IP Address is not correct or inaccessible. This message may also appear due to a network problem, a proxy server configuration error, or an incorrect IEM URL. Check if the firewall policy is blocking access.

Figure 1-7 'Management Server is not reachable' Error Message

If the IEM is down but the IEC has accessed the startup URL previously, it will load the startup URL from its cache. In other words, the failure of the IEM does not prevent the IEC from functioning. If any configuration changes are needed, then IEM has to be active for pushing the new policy configurations to the IEC.

Customer Pod Displays 'Startup URL is not configured' Message

Figure 1-8 'Startup URL is not configured' Message

The following are the possible reasons and resolutions for the message "Startup URL is not configured":

- IEC does not have a policy (initial configuration that includes startup URL) enforced in IEM. Verify the IEC has the correct policy applied and the IEC has been rebooted.
- Another possibility is that the IEC is not registered in the IEM, instead it is in standalone mode. Check the IEM to ensure that the proper serial number is added for the IEC.
- If the IEC is not rebooted after configuration changes, reboot the IEC.

IEC Displays 'Cannot register' Message

Figure 1-9 'Cannot register' Message

Click the Show Details button to reveal information about service that is disabled.

Figure 1-10 Details of the 'Cannot register' Issue

This is due to the fact the IEM is not enabled for registration.

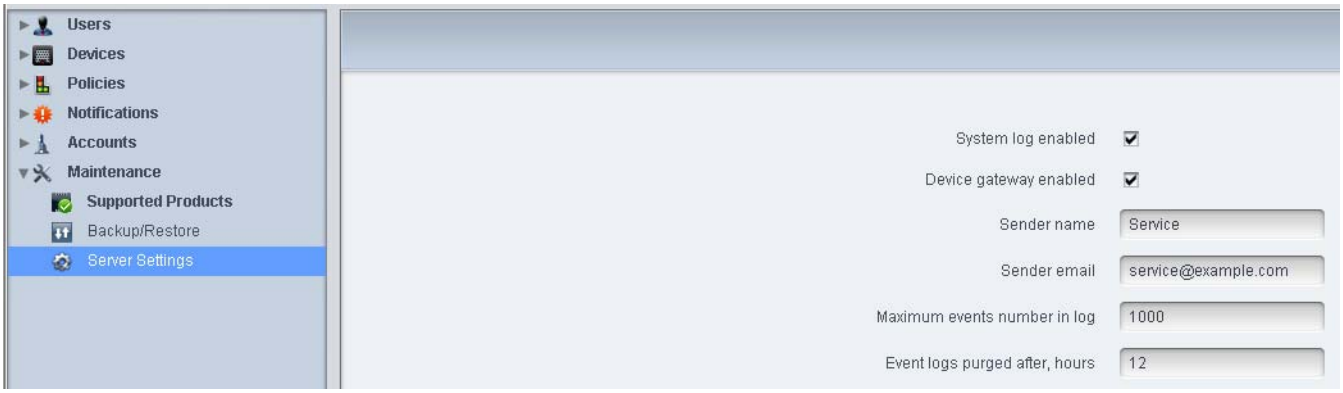
Step 1 Log into the IEM as root/administrator user. Otherwise, users cannot see the Maintenance link. The Maintenance link is not shown to regular users.

Step 2 Click the **Maintenance** link.

Step 3 Click **Server Settings**.

Step 4 Check the **Device gateway enabled** check box.

Figure 1-11 Server Settings Window



Step 5 Click **Apply**.

Customer Pod Touch Screen Function is Not Working Correctly

If the touch screen (customer pod) is not working correctly:

1. Ensure that the USB interface cable is plugged into the IEC and the touch screen.
2. Use the calibration utility to recalibrate the screen.
   a. Press **Ctrl+Alt+S**.
   b. Enter the DMC (Device Maintenance Code).
   c. Click **Calibrator**.
3. Reboot the system if the touch screen USB cable was not connected before boot time.

Customer Pod Displays Virtual Keyboard When Call Connects

When connecting to a remote expert, the touchscreen connected to the IEC displays a virtual keyboard on the customer pod. This is due to an incorrect policy applied to the IEC. Disable the following configuration settings in the policy that is applied to the IEC. If there is no policy applied to the IEC, then these changes should be set in the IEC profile configuration.

Step 1 Log into the IEM.

Step 2 Go to the policy that is applied to the IEC or the IEC's profile.

Step 3 Go to keyboard > virtual > enabled property.

Figure 1-12 Disabled Virtual Keyboard

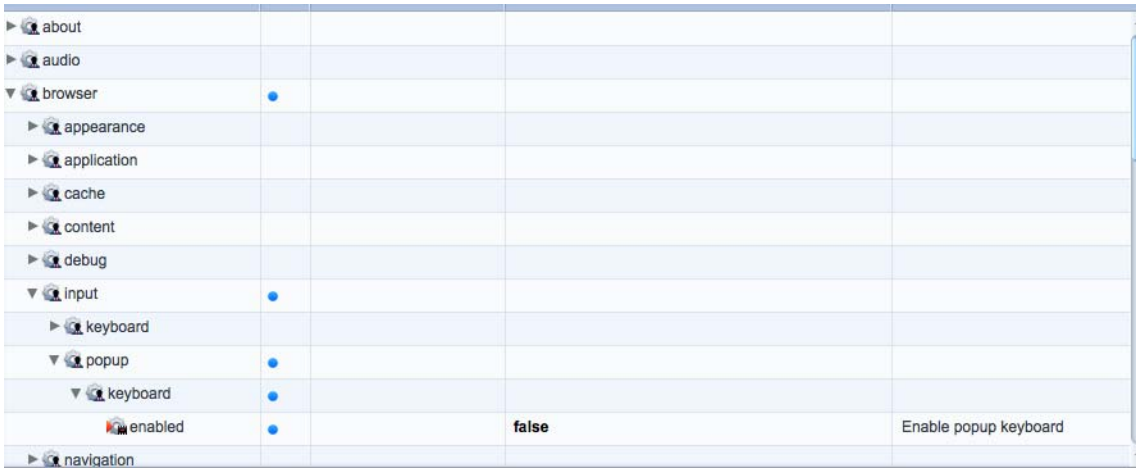
Property		Compatibility	Value	Description
about				
audio				
browser				
clock				
cohttpd				
display				
flashplayer				
hotkeys				
keyboard				
hardware				
virtual				
enabled			false	Enable virtual keyboard
message				

Step 4 Set enabled value to **false**.

Step 5 Go to browser > input > popup > keyboard > enabled property.

Step 6 Set enabled value to **false**.

Figure 1-13 Disabled Popup Keyboard



Step 7 Save the policy by clicking the **Apply** button.

Step 8 Reboot the IEC to activate the policy on it.

Customer Pod Displays 'Server is down' Message

Figure 1-14 'Server is down' Message

There are multiple possible reasons for this error message:

1. Check the IEC's Policy or Profile settings in the IEM with respect to startup URL configuration.
1. Check REM-UCM JTAPI configuration (application username/password in UCM and REM).
2. The REM's tomcat service may be down.
3. The most likely reason for this error message is that the REM's service is not up and running. A successful REM installation should show nine services listed. To list those services, go to https://<REM_IP>:8443/resc/services/listServices where "<REM_IP>" is the IP address of the REM.

   If you see only one service as shown below, you need to check resc.log. Check that the JTAPI link between the REM and UCM is up and running. If the link is not up and running, the UCM username and password that is listed in the rem.properties file are not what is configured in UCM application user page.

Figure 1-15 Only One Active Service

Try the following to resolve the issue:

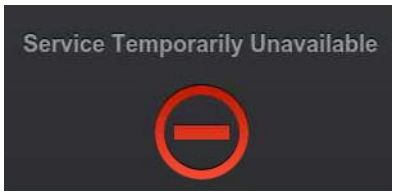
1. Restart the Tomcat service. See the *Cisco Remote Expert Manager 1.9.2 Installation Guide* for instructions.
2. Look for the message 'bad login' in the resc.log.

```
[root@localhost ~]# grep --color 'bad login' /var/rem/resc/logs/resc.log
2012-06-08 22:33:44,442 ERROR [pool-2-thread-1]
org.apache.axis2.deployment.ServiceDeployer - The VirtualAgentServices.aar
service, which is not valid, caused Error creating bean with name
'virtualAgentService' defined in class path resource [applicationContext.xml]:
Cannot resolve reference to bean 'callService' while setting bean property
'callService'; nested exception is
org.springframework.beans.factory.BeanCreationException: Error creating bean with
name 'callService' defined in class path resource [applicationContext.xml]:
Instantiation of bean failed; nested exception is
org.springframework.beans.BeanInstantiationException: Could not instantiate bean
class [com.cisco.big.call.CallService]
: Constructor threw exception; nested exception is
com.cisco.jtapi.PlatformExceptionImpl: Unable to create provider -- bad login or
password.
```

If it is a bad login or password error, correct the JTAPI username and password either in the rem.properties file or in the UCM application configuration page. If the rem.properties file is modified to correct this username and password issue, execute the IAS. See the *Cisco Remote Expert Manager 1.9.2 Installation Guide* for instructions.

Customer Pod Displays 'Service Temporarily Unavailable' Message

Figure 1-16 'Service Temporarily Unavailable' Message



This error occurs when the IEC cannot pull the home page from the REM because the startup URL configured in the IEM is not reachable or the REM server or services are down.

To resolve this error:

- Verify the REM is up and functioning by checking this URL on a browser: https://<REM_IP>:8443/reic where "<REM_IP>" is the IP address of the REM.
- Check the IEC's event log in the IEM. In the sample displayed below, the IEC's access to the startup URL failed. Verify the IP address of the REM as configured in the IEM policy that is applied to the IEC or the IEC's profile.

Figure 1-17 An IEC's Logs in the IEM

Customer Pod Displays 'Kiosk is not registered' Message

Figure 1-18 'Kiosk is not registered' Message

If the customer pod does not display the 'Connect homepage' message but instead displays the 'Kiosk is not registered' message, the reason for this error is due to the fact that REAC does not have an entry for this IEC in its Kiosk menu page. Add the IEC to the REAC. If it is already added, verify that the IEC's serial number is correct.

The resc.log file will display this issue as 'unique serialNumber':

```
[root@localhost ~]#grep --color 'unique serialNumber:' /var/rem/resc/logs/resc.log
```

Figure 1-19 'unique serialnumber' Output

```
[root@localhost ~]# grep --color 'unique serialNumber:' /var/rem/resc/logs/resc.log
2012-06-07 21:26:35,062 INFO  [http-bio-80-exec-7] com.cisco.big.va.services.VirtualAgentServices - Received getKioskDetails unique serialNumber: 656015330015
2012-06-07 21:26:35,069 INFO  [http-bio-80-exec-1] com.cisco.big.va.services.VirtualAgentServices - Received getKioskDetails unique serialNumber: 656015330015
2012-06-07 21:27:44,839 INFO  [http-bio-80-exec-15] com.cisco.big.va.services.VirtualAgentServices - Received getKioskDetails unique serialNumber: 656015330015
2012-06-07 21:27:45,068 INFO  [http-bio-80-exec-7] com.cisco.big.va.services.VirtualAgentServices - Received getKioskDetails unique serialNumber: 656015330015
```

When the IEC is added or updated with the correct serial number, the resc.log should display 'kiosk: <serialnumber> is alive' as shown below.

Figure 1-20 Serial Number is Alive Output

```
[root@localhost ~]# grep --color '656015330015 is alive' /var/rem/resc/logs/resc.log
2012-06-07 21:41:30,479 INFO  [http-bio-80-exec-36] com.cisco.big.admin.service.AdminService - Kiosk:656015330015 is alive
2012-06-07 21:41:50,520 INFO  [http-bio-80-exec-36] com.cisco.big.admin.service.AdminService - Kiosk:656015330015 is alive
2012-06-07 21:42:10,526 INFO  [http-bio-80-exec-36] com.cisco.big.admin.service.AdminService - Kiosk:656015330015 is alive
2012-06-07 21:42:30,562 INFO  [http-bio-80-exec-51] com.cisco.big.admin.service.AdminService - Kiosk:656015330015 is alive
2012-06-07 21:42:50,560 INFO  [http-bio-80-exec-58] com.cisco.big.admin.service.AdminService - Kiosk:656015330015 is alive
2012-06-07 21:43:10,566 INFO  [http-bio-80-exec-54] com.cisco.big.admin.service.AdminService - Kiosk:656015330015 is alive
2012-06-07 21:43:30,601 INFO  [http-bio-80-exec-58] com.cisco.big.admin.service.AdminService - Kiosk:656015330015 is alive
2012-06-07 21:43:50,654 INFO  [http-bio-80-exec-58] com.cisco.big.admin.service.AdminService - Kiosk:656015330015 is alive
2012-06-07 21:44:10,690 INFO  [http-bio-80-exec-58] com.cisco.big.admin.service.AdminService - Kiosk:656015330015 is alive
```

Connected Peripherals are Not Detected by the IEC

Peripherals such as a printer, scanner, keyboard, or mouse must be connected to the IEC before it is booted up in order for the IEC to detect them. If you connect a peripheral after the IEC has booted up, reboot the IEC to detect that peripheral.

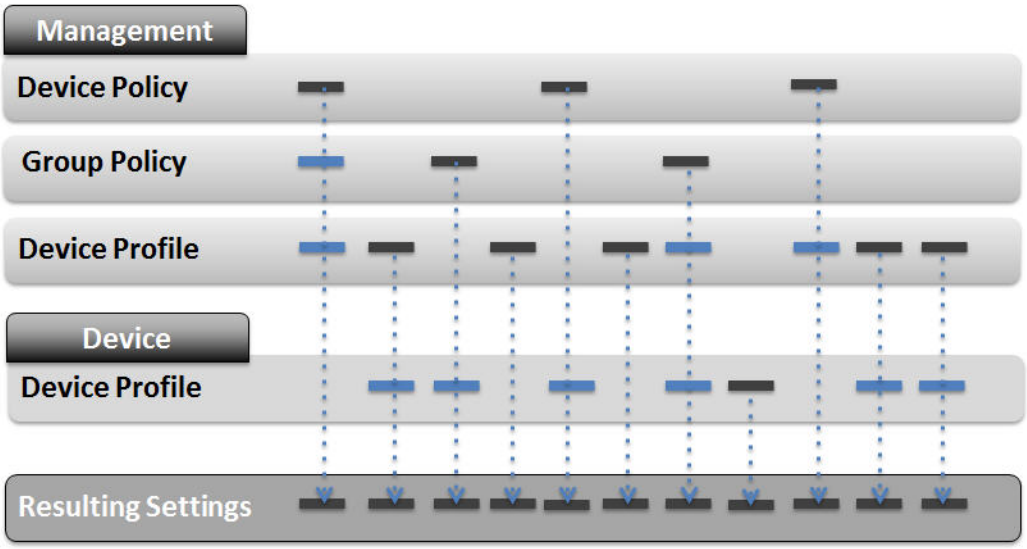
IEC is Not Reflecting the Applied Policy

After applying the policy, IEC needs to be rebooted to have the policy enforced. Also check the IEM to ensure that the IEC has the proper policy applied to it.

IEC's Profile Configuration is Not Active

If there is a policy assigned to the IEC, its configuration take precedence over the IEC's profile configuration. If the IEC's profile configuration is required instead, remove the applied policy.

Figure 1-21 Profile and Policy Hierarchy for IECs



Customer Pod Displays 'System is not available, Please try after some time' Message

If the customer pod displays the 'System is not available, Please try after some time' message, it could be due to the video endpoint at the customer pod is not in the UCM's REM application user's control list.

```
[root@localhost ~]# grep --color 'not in provider' /var/rem/resc/logs/resc.log
com.cisco.jtapi.InvalidArgumentExceptionImpl: Address 2512 is not in provider's
domain.
```

To resolve this issue, go to the UCM application user configuration that is used by the REM in its rem.properties file. Add the video endpoint (in this example, DN:2512) into its control list.

Use the Unix "less" command to view and search the resc.log file for RE call issues. Within the "less" command, search for the following strings to find call issues:

- 'Making a Call connect via Jtapi' is the resc.log entry indicating a new RE session attempt.
- 'ObserverThread' are resc.log entries containing ObserverThread that correspond to the client pod video endpoint initiating and participating in the RE session.
- 'AgentObserver' are resc.log entries containing AgentObserver that correspond to the expert pod's video endpoint participating in the RE session.

The following command shows which the DNs that successfully got connected in the past:

```
[root@localhost ~]# grep --color 'CallConnected' /var/rem/resc/logs/resc.log
```

The result of the command is the following output:

```
2012-06-07 22:15:25,632 INFO
[ObserverThread(com.cisco.big.call.BIGObserver@6f221448)]
com.cisco.big.call.BIGObserver - CallConnected2512
2012-06-07 22:15:25,634 INFO
[ObserverThread(com.cisco.big.call.BIGObserver@6f221448)]
com.cisco.big.call.BIGObserver - CallConnected1134
```

```
2012-06-07 22:15:43,017 INFO
[ObserverThread(com.cisco.big.call.BIGObserver@6f221448)]
com.cisco.big.call.BIGObserver - CallConnected2504
2012-06-072:22:24,026 INFO  [ObserverThread(com.cisco.big.call.BIGObserver@1539d980)]
com.cisco.big.call.BIGObserver - CallConnected2512
```

Customer Pod Displays 'Expert not available' Message

Whenever the IEC is rebooted or powered up, the REM will check reachability to the IEC's local video endpoint that is configured in the REAC's Kiosk menu page. If the IEC's video endpoint is not pingable from the REM, the REM instructs the IEC to display 'Expert not available'.

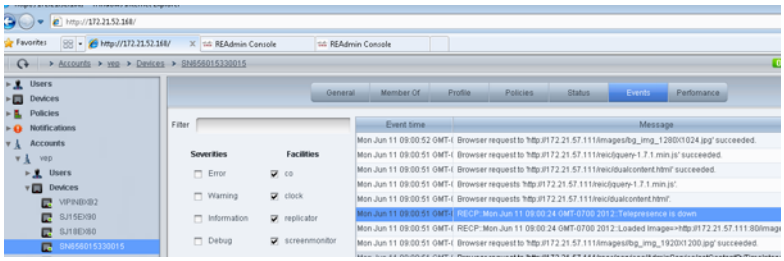
This may also happen when the REM or REAC's Kiosk page has multiple instances of the same IEC.

If you check the resc.log, you will see following error messages:

```
[root@localhost ~]#grep --color 'is not reachable' /var/rem/resc/logs/resc.log

WARN [http-bio-80-exec-60] com.cisco.big.admin.util.VepManagementUtil - ------ ****
CTS for kiosk: 656015330015 is not reachable 4 ****
WARN  [http-bio-80-exec-60] com.cisco.big.admin.util.VepManagementUtil - ------ ****
CTS for kiosk: 656015330015 is not reachable 5 ****
WARN  [http-bio-80-exec-60] com.cisco.big.admin.util.VepManagementUtil - **** ---- CTS
for kiosk:656015330015 is dead. after 5 tries
```

A similar message will also be logged in the IEC's Event screen in the IEM as shown below.

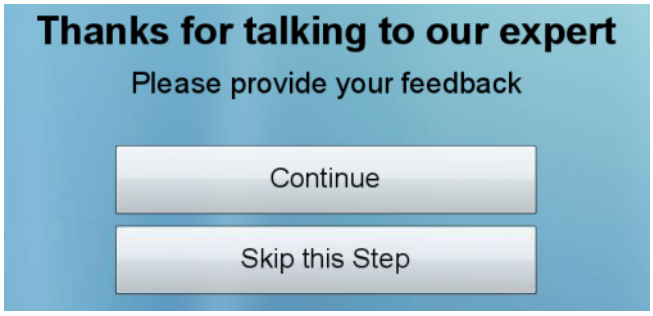
Figure 1-22 IEM's Event Screen for an IEC



Customer Pod Displays Request to Provide Feedback After Pressing the Connect Button

If the customer pod displays a screen requesting the customer to provide feedback about the session after the customer presses the Connect button, the wrong CC Pilot DN was configured or the DN is not working. Contact Center could also be possibly down or busy or the UCM-Contact Center integration has issues.

Figure 1-23 Screen Requesting Customer Feedback



Check the resc.log for Called Address:Unknown:

```
[ObserverThread(com.cisco.big.call.BIGObserver@5b7127)] com.cisco.big.call.BIGObserver
- BIGObserver - Curent Called Address:Unknown
INFO  [ObserverThread(com.cisco.big.call.BIGObserver@5b7127)]
com.cisco.big.call.BIGObserver - BIGObserver - Curent Calling Address:2512
INFO  [http-bio-80-exec-73] com.cisco.big.call.CallService - Time taken for Call
Connect: 4
INFO  [ObserverThread(com.cisco.big.call.BIGObserver@5b7127)]
com.cisco.big.call.BIGObserver - Setting the session to status 2
INFO  [ObserverThread(com.cisco.big.call.BIGObserver@5b7127)]
com.cisco.big.call.BIGObserver - Call disconnected
```

Customer Pod Does Not Display the Home Page

There are several possible reasons why the customer pod does not display the Home page:

- The IEC does not have the policy with the startup URL pointing to the REM applied to it. Apply that policy to the IEC in the IEM.
- If IEC does not have a policy but using its profile in the IEM for the startup URL, verify that the startup URL in the profile is pointing to the REM.

Note Use of policies is the preferred method for configuring IEC properties.

- Verify that the IEC has been added to the REAC's Kiosk menu.
- If the IEC was updated recently but not rebooted, the IEC needs to be rebooted.
- Check if REM Server is reachable and web services are accessible.

Once you have fixed the above issue, verify that the content in the Home page is correct by following these steps:

Step 1 Check which images will load in the IEC by going to the following link: https://<REM_IP>:8443/resc/services/VirtualAgentServices/getKioskDetailsBySerialNum?serialNumber=<Serial Number>. For example, the following link is displayed in the figure below: https://172.21.63.41:8443/resc/services/VirtualAgentServices/getKioskDetailsBySerialNum?serialNumber=656015330015

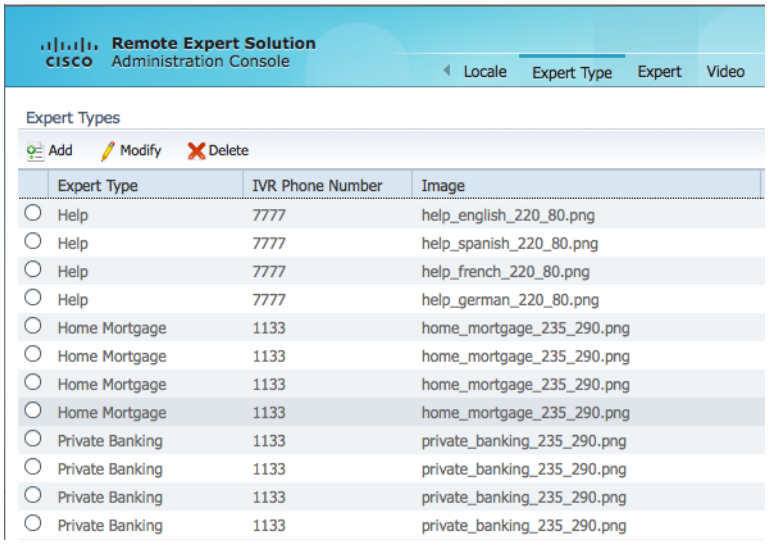
Figure 1-24 Link that Shows Which Images Will Load in the IEC


```
http://172.21.63.41/resc/services/VirtualAgentServices/getKioskDetailsBySerialNum?serialNumber= - Windows Internet Explorer
http://172.21.63.41/resc/services/VirtualAgentServices/getKioskDetailsBySerialNum?serialNumber=656015330015
Favorites   http://172.21.52.168/   http://172.21.63.41/resc...   REAdmin Console

- <ns:getKioskDetailsBySerialNumResponse xmlns:ns="http://services.va.big.cisco.com">
  - <ns:return xmlns:ax29="http://event.big.cisco.com/xsd" xmlns:ax27="http://dao.va.big.cisco.
      xmlns:ax23="http://tp.call.big.cisco.com/xsd" xmlns:ax24="http://util.java/xsd" xmlns:ax21:
      xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" xsi:type="ax213:KioskDetailsW
      <ax21:errorCode>0</ax21:errorCode>
      <ax21:errorMsg xsi:nil="true" />
      <ax21:statusCode>SUCCESS</ax21:statusCode>
      <ax213:appServerHostname>sjEX60</ax213:appServerHostname>
      <ax213:customerId xsi:nil="true" />
    - <ax213:experts xsi:type="ax213:ExpertTypeWS">
        <ax213:id>12</ax213:id>
        <ax213:imgURL>http://172.21.63.41:80/images//btn_commercial_lending_238_291.pnc
        <ax213:ivr_pn>1133</ax213:ivr_pn>
        <ax213:typeName>decorator</ax213:typeName>
      </ax213:experts>
    - <ax213:experts xsi:type="ax213:ExpertTypeWS">
        <ax213:id>13</ax213:id>
        <ax213:imgURL>http://172.21.63.41:80/images//btn_home_mortgage_238_291.png</a
        <ax213:ivr_pn>1133</ax213:ivr_pn>
        <ax213:typeName>decorator</ax213:typeName>
      </ax213:experts>
    - <ax213:experts xsi:type="ax213:ExpertTypeWS">
        <ax213:id>14</ax213:id>
        <ax213:imgURL>http://172.21.63.41:80/images//btn_private_banking_238_291.png</a
        <ax213:ivr_pn>1133</ax213:ivr_pn>
        <ax213:typeName>decorator</ax213:typeName>
      </ax213:experts>
    - <ax213:experts xsi:type="ax213:ExpertTypeWS">
        <ax213:id>18</ax213:id>
        <ax213:imgURL>http://172.21.63.41:80/images//btn_help.png</ax213:imgURL>
        <ax213:ivr_pn>1133</ax213:ivr_pn>
        <ax213:typeName>help</ax213:typeName>
      </ax213:experts>
    - <ax213:experts xsi:type="ax213:ExpertTypeWS">
        <ax213:id>20</ax213:id>
        <ax213:imgURL>http://172.21.63.41:80/images//btn_problem_resolution_238_291.png
        <ax213:ivr_pn>1133</ax213:ivr_pn>
        <ax213:typeName>decorator</ax213:typeName>
      </ax213:experts>
    - <ax213:experts xsi:type="ax213:ExpertTypeWS">
        <ax213:id>21</ax213:id>
        <ax213:imgURL>http://172.21.63.41:80/images//btn_retirement_savings_239_291.png
        <ax213:ivr_pn>1133</ax213:ivr_pn>
```


The PNG files in the figure above are the ones that actually display on the customer pod.

Step 2 Those PNG files displayed above are in fact mapped to specific Contact Center Pilot DNs, Expert Types are grouped together and the IVR (DN) number can be modified altogether for an Expert Type group.

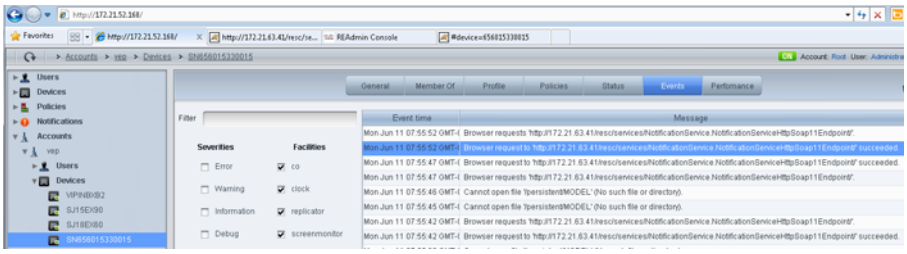
Figure 1-25 PNG Files Mapped to Different DNs



Expert Type	IVR Phone Number	Image
Help	7777	help_english_220_80.png
Help	7777	help_spanish_220_80.png
Help	7777	help_french_220_80.png
Help	7777	help_german_220_80.png
Home Mortgage	1133	home_mortgage_235_290.png
Home Mortgage	1133	home_mortgage_235_290.png
Home Mortgage	1133	home_mortgage_235_290.png
Home Mortgage	1133	home_mortgage_235_290.png
Private Banking	1133	private_banking_235_290.png
Private Banking	1133	private_banking_235_290.png
Private Banking	1133	private_banking_235_290.png
Private Banking	1133	private_banking_235_290.png

Step 3 Check the IEC's event log in the IEM to see if the request from the IEC was successful.

Figure 1-26 Successful Request in the IEC's Event Log



Note The IP address used in the request is also in its response. This would help to identify the REM IP address used by the IEC in its request.

IEC Reboots Twice

In certain circumstances, such as during a power failure at the branch, the IEC reboots twice. This is expected because the IEC was designed to only detect those peripherals that are connected to it when it is rebooted. In a power failure scenario, the TP video endpoint takes longer time to reboot compared to the IEC. As a result, the IEC does not detect the TP video endpoint connected to its HDMI port. In order to circumvent this issue, IEC reboots again after it finds the TP video endpoint is reachable.

The following resc.log shows that the REM rebooted the IEC:

```
2012-06-11 16:45:40,326 INFO  [http-bio-80-exec-144]
com.cisco.big.common.util.CommandExec - reboot
[root:localhost ~]$ echo "RE_CHANNEL_TERM";
RE_CHANNEL_TERM
[root:localhost ~]$
```

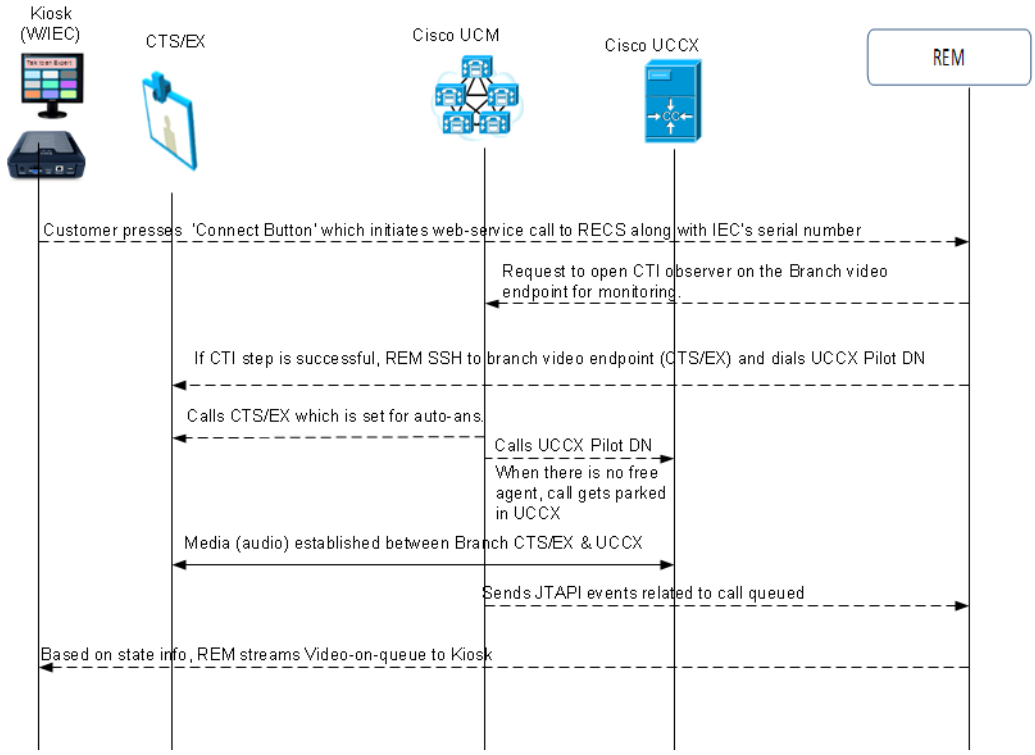
```
Broadcast message from root@localhost (pts/2) (Mon Jun 11 09:45:28 2012):

The system is going down for reboot NOW!
```

Unable to See Wait Video While Call is in the Queue

The Wait Video that is streamed when the call is in a queue is handled by REM. The call flow when a customer call is being queued is as follows:

1. When there is no expert available, the UCCX/UCCE puts the call in a queue.
2. Based on the JTAPI event, the RECS requests the media server (Adobe) to stream a pre-configured video file to the IEC.

Figure 1-27 Call Flow When Call is in the Queue



Possible reasons for the Wait video not playing are:

- The Wait video has not been added in the REM. Go to /opt/apache-tomcat-7.0.23/webapps/reic/assets/video and ensure that the Wait video has been added.
- If a particular video has been provided as the Wait video for an expert type in REAC and still does not play, check the following:
  - The video format provided in REAC in the Video tab is correct (https or rtmp format).
  - The video filename in REAC is the same as that given in the Adobe server (Folder Path: Adobe > webroot > vod > filename).

Unable to See On-Hold Video While Call is On Hold

The On-Hold video is handled by the external media server such as Adobe Media Server (AMS). There are two deployment models: customers can install AMS on a different server or customers can install AMS and REM on the same server.

Possible reasons for the On-Hold video not playing are:

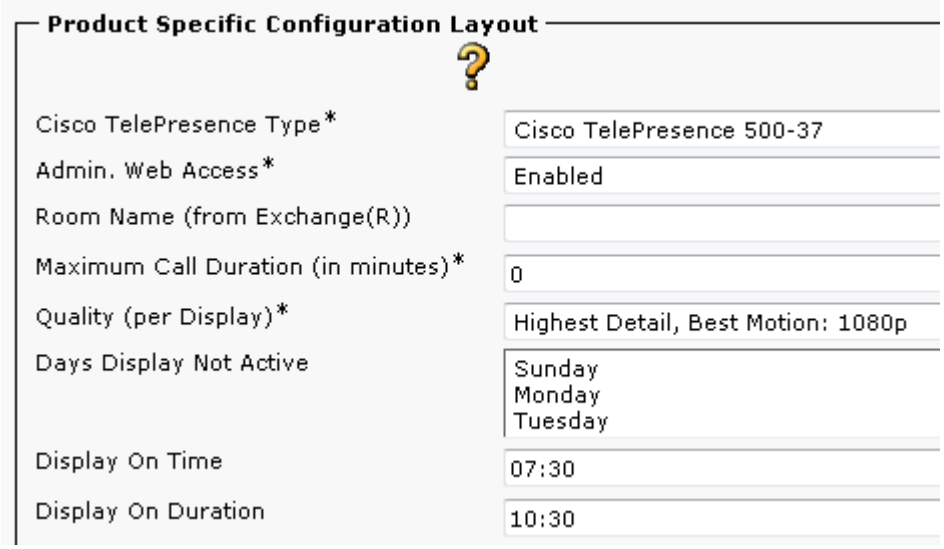
- The Adobe server does not have the requested media file. Check the REAC Video tab to ensure that the file's URL is provided in the correct format.
- The file is not present in the Adobe media server location (Folder Path: Adobe > webroot > vod > filename). Check if the filename provided in the REAC is the same as that stated in this location.
- Only filenames of types .flv, .f4v, .mp4 and .mov are supported. Video clips are streamed via the rtmp protocol. Only filenames and formats of these types would play if provided as the On-Hold video. Convert the video format or change the filename if necessary.

Unable to Bring Up Static Graphic Page in TP (During Non-TP Calls)

The IEC can display a static image or stream a video file to the TP video endpoint when it is not being used. If this feature is not working, a configuration mismatch is the likely cause.

Step 1 Verify the TP video endpoint device configuration in UCM is correct and make sure that the 'Days Display Not Active', 'Display On Time', and 'Display on Duration' settings are correctly configured.

Figure 1-28 TP Device Configuration



Step 2 Verify the REM's Content configuration page has correct image file names and hours.

Figure 1-29 REAC's Content Page

Step 3 Go to the following URL: https://<REM_IP>:8443/reic/dualcontent.html

This URL response should display the graphics that supposed to show up at the current time.

Step 4 Verify in the IEM that the IEC shows dual images (one image for the customer pod and the other image is for TP video endpoint when it is not on a call). Click **Devices** in the left pane and then click the Show Screenshot icon located at the top of the center pane.

If the dual images show up in the IEM, then the issue is probably with the TP video endpoint.

Figure 1-30 Show Screenshot Feature of the IEM

Unable to Upload and Update Images to REM

The static graphic images and video files can be uploaded to the REM from REAC. However, such uploading fails from certain browsers. Only use supported browsers while accessing the REAC.

READ is Not Showing Up

When the expert answers the call, the READ will be displayed in the Cisco Agent Desktop's integrated browser. If it does not, the following are possible reasons:

- UCCX/UCCE does not have a Premium Package license. The CAD needs the Premium Package license.
- Cisco Agent Workflow is not correctly configured. Verify that the Cisco Agent Workflow is correctly configured to bring up the READ from the REM server.

Note The configuration parameters in the HTTP Action Setup are case sensitive so ensure that the values entered into fields are correct.

- The webservices are not running. This link should show nine active services: https://<REM_IP>:8443/resc/services/listServices.

- Verify each of the call events.dation of READ. For different call event states, the expert's desktop will display different web pages.

  Note Replace <rem_server_ip> with the actual IP address and replace <agent_dn> with the actual user ID.

  - Not Ready: https://<rem_server_ip>:8443/read/Common.jsp?agentDn=<agent_dn>&state=0&request=welcome
  - Ready: https://<rem_server_ip>:8443/read/Common.jsp?agentDn=<agent_dn>&state=1&request=welcome
  - Ringing: https://<rem_server_ip>:8443/read/desktoppage?agentDn=<agent_dn>&calling=<ivr_queue_id>
  - Dropped: https://<rem_server_ip>:8443/read/Common.jsp?agentDn=<agent_dn>&request=disconnect
  - Logout: https://<rem_server_ip>:8443/read/Common.jsp?request=logout

Video Call is Not Established Between Different Types of TelePresence Video Endpoints

When an expert is available, the customer call that has been queued in UCCX/UCCE will be redirected to the available expert's video endpoint. If the video endpoints used between the customer and the expert are of different types (i.e. one is an EX90 and the other is a C40), there could be interoperability issues associated with MTP.

UCM-based MTP does not support video and if the end-to-call uses MTP resources, the resulting call will be an audio call. There are two workarounds:

1. Remove MTP resources being used in such calls between customer-side video endpoint and expert's video endpoint.
2. If MTP is needed for some other reasons, use IOS-based MTP with pass-through configuration. IOS-based pass-through feature supports video calls getting established.

Experts are not Getting Registered in REAC

While registering experts in REAC, if the registration fails and shows both nodes (in a dual node setup) in red, do the following:

Step 1 Go to the console of the VM in VMWare VSphere.

Step 2 Type the command `system-config-network`.

Step 3 Go to the option **Edit DNS Configuration**.

Step 4 Check if the Hostname is different in both these VMs. The Hostname must be unique for each VM. If it is the same name, change the Hostname in one of the VMs.

Step 5 Validate the UCM configuration.

Step 6 Restart the network by typing the command `/etc/init.d/network restart`.

Note If the hostname has changed, restart Tomcat for REM to function properly.

REIC (Cobra Browser) Hangs

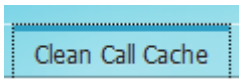
When the REIC hangs or goes into a limbo state due to some reason, use the following command to clear cache: https://<Virtual IP>:8443/resc/services/AdminService/cleanCallCache

Session Hangs

The administrator can clean the call cache of kiosks if a session hangs. When a session hangs, a new call cannot be initiated to or from the customer pod. By cleaning the call cache, the session's status in the Session tab is changed to "Completed", which then allows the customer pod to start or receive a new call.

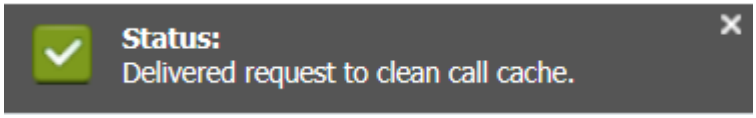
Step 1 Click the **Clean Call Cache** tab.

Figure 1-31 Clean Call Cache Tab



A Status box appears in the lower right corner of the screen indicating that the call cache was cleaned.

Figure 1-32 Clean Call Cache Status Message



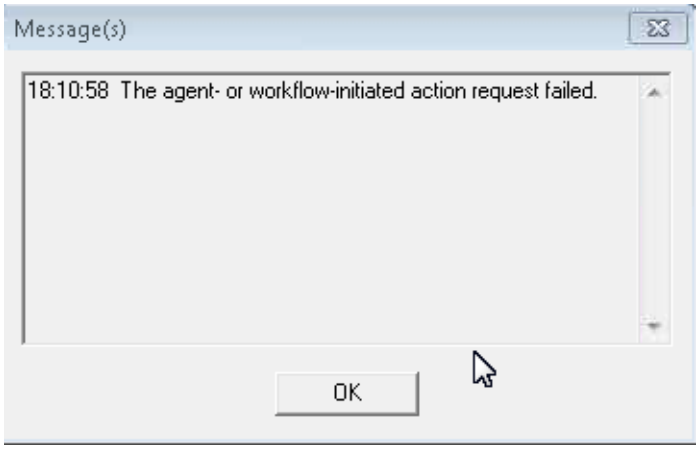
REM Error Message

If you see the error message "Address <DN> is not in provider's domain", the device whose Directory Number (DN) is <DN> is not in the control-list of application user (ragent) in CUCM's configuration. Add the device in the CUCM under the appropriate Application User.

EX90 Firmware Error Message

If you see the error message "The agent or workflow-initiated action request failed", update the EX90 firmware to TC6.1.

Figure 1-33 Error Message



Troubleshooting Guidelines for IEC as Video Endpoint

If the IEC is being used as the video endpoint as opposed to a Cisco TelePresence unit such as the EX-60, you may encounter the following issues related to the SIP configuration.

SIP Video Call is Not Established Between IEC Video Endpoint and Agent

If the call cannot be made or received, verify the following was configured correctly in the IEM:

- The format of the CUCM phone is: **sip.target** or **sip.target1**
- The value of the CUCM phone is the directory number in CUCM.
- The format of the CUCM username is: **sip.username**
- The value of the CUCM username is the username in CUCM.
- The format of the CUCM password is: **sip.password**
- The value of the CUCM password is the CUCM password.
- The format of the CUCM domain is: **sip.domain**
- The value of the CUCM domain is the IP address of the CUCM.
- The format of the CUCM protocol is: **sip.transport**
- The value of the CUCM protocol is: **udp**

Note Ensure that all of the above formats and values are in lowercase.

Troubleshooting Guidelines for Remote Expert Applications Running on VMware

Performance indicators from within the virtual machines are still valid. For the UC applications that support it, use RTMT or the perfmon data for analysis of the performance of the UC application. Data from these tools provides view of the guest performance such as disk, CPU, memory, etc.

Move to the VMware infrastructure when there is a need to get the perspective from the ESXi host. Use the vSphere Client to view data.

- If vCenter is available, historical data is available through the client.
- If vCenter is not available, live data from the host is available through the client.

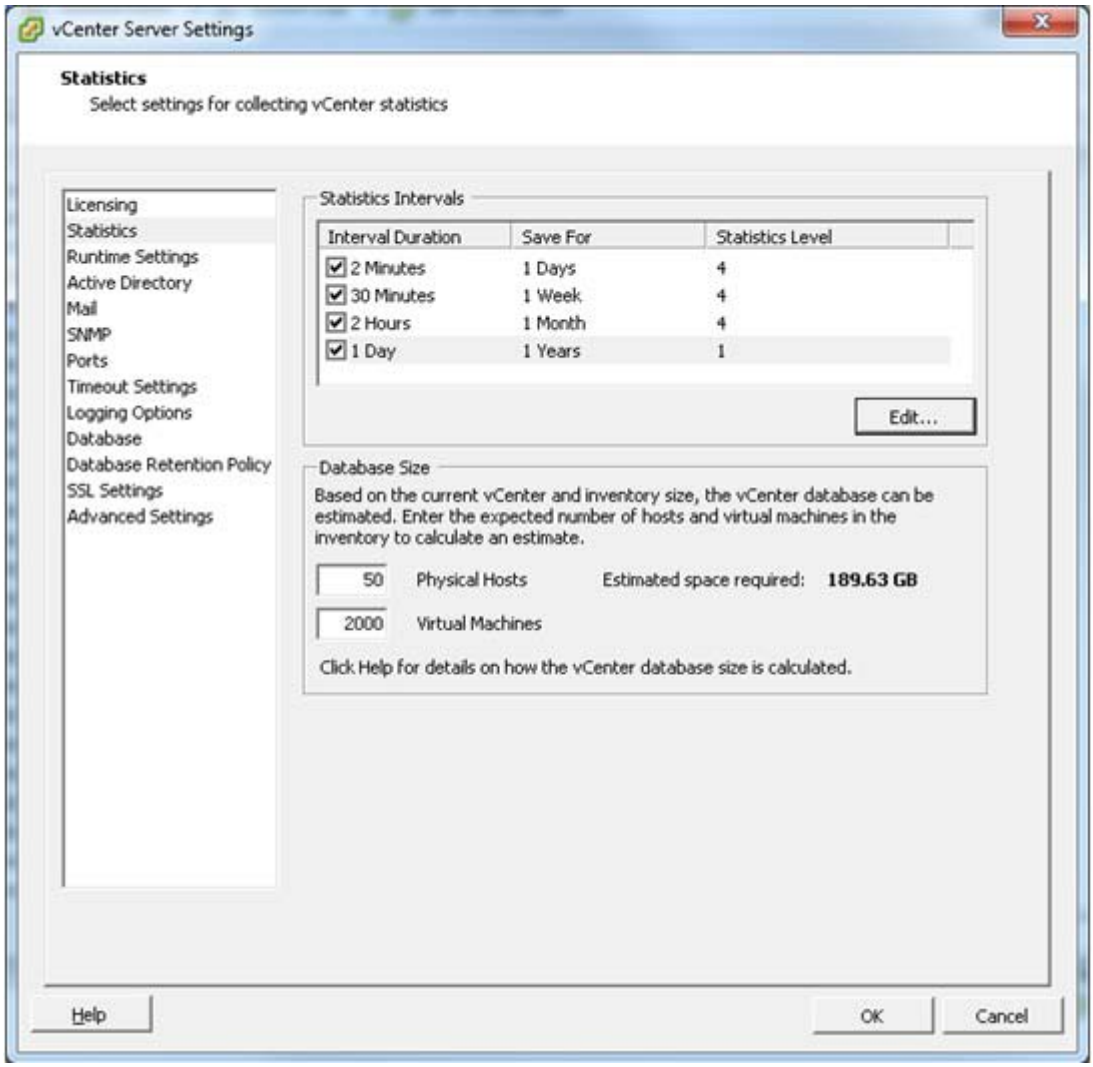
vCenter Settings

Just like some of the UC applications, vCenter can be configured to save more performance data. The more historical data saved, the bigger disk space needed by the database used by vCenter.

Note This is one of the main areas where you need vCenter rather than going directly to the ESXi host for performance data. vCenter can save historical data that the ESXi host does not keep.

The configurations to change the amount historical data saved by vCenter is located in the vSphere client under Administration > Server Settings. For each interval duration, the duration that the statics will be saved for (days, weeks, months, or years) and the statistics level can be set. The statistic levels range from 1 to 4 with level 4 containing the most data. Look at the data size estimates to make sure there is enough space to keep all of the statistics.

Figure 1-34 Statistic Settings in vCenter



VMware Performance Indicators

The following table lists the performance indicators to monitor and view from a VMware perspective when a virtual machine's performance is not optimal. Most counters are from the ESXi host, which can give a perspective of VM interactions and overall host and data store utilization.

Table 1-2 VMware Performance Indicators

Performance Area	Object	Counter	Acceptable Range
CPU	Host	Usage	less than 80%
CPU	Virtual Machine	Ready	less than 3%
Memory	Host	Consumed	general trend is stable

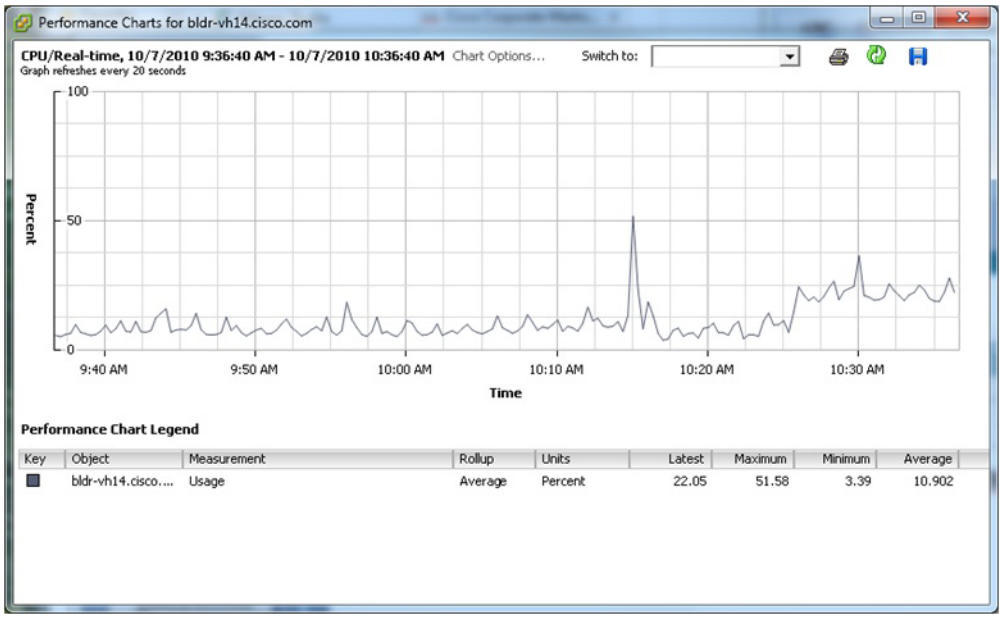
Performance Area	Object	Counter	Acceptable Range
Memory	Host	Balloon/Swap used	0 kb
Disk	Specific datastore	Kernel command latency	less than 3ms
Disk	Specific datastore	Physical device command latency	less than 20ms
Disk	Specific datastore	Average commands issued per second	less than LUN capacity
Network	Host	Receive packets dropped / Transmit packets dropped	0 packets

CPU Troubleshooting

High CPU usage could be due to a small number of VMs using all of the resources or too many VMs running on the host. IF there are too many VMs running on the host, see if CPU reservations are in use (see oversubscription section). To isolate a CPU issue for a particular VM, consider moving it to another ESXi host.

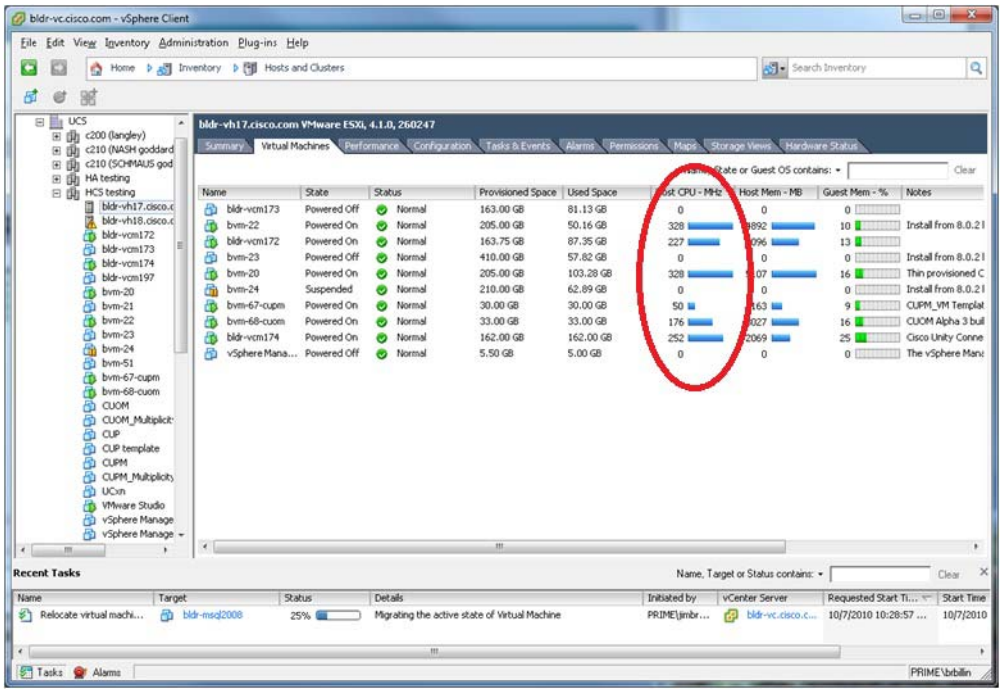
To view the CPU performance indicators, go to the ESXi host's performance tab and select the advanced button. Under chart options, select CPU, timeframe, and then only the host (not individual cores) to view overall CPU usage on the host.

Figure 1-43 Performance Chart



Each virtual machine CPU usage can also be seen from the Virtual Machines tab on the host.

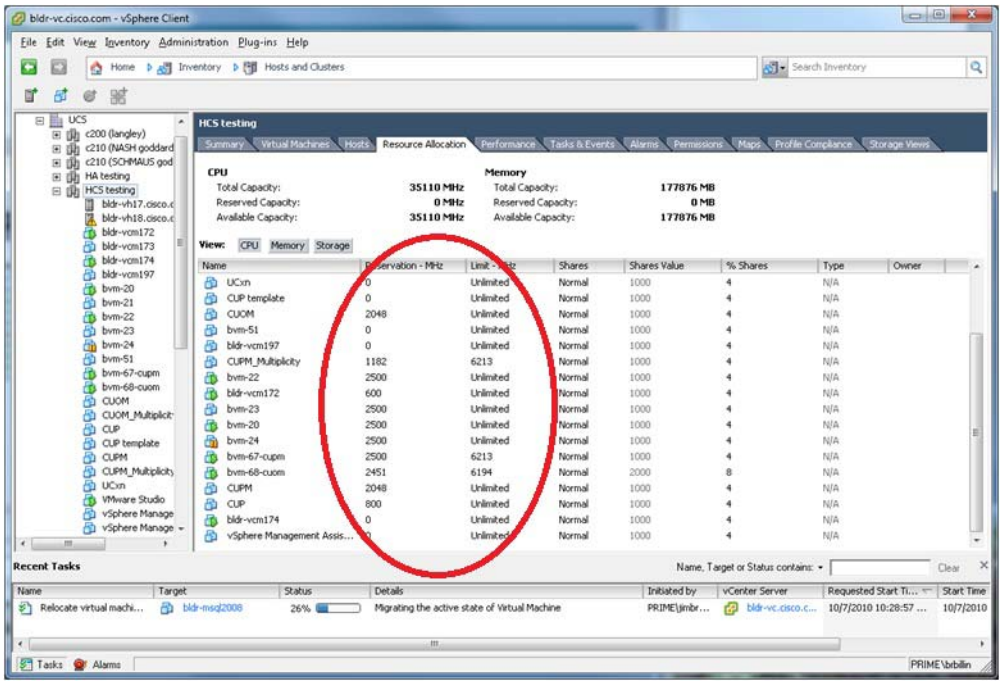
Figure 1-44 Virtual Machines Tab on the Host



To get a view of the reservations set by all of the VMs, use the Resource Allocation tab of the cluster.

Note This is only available via vCenter.

Figure 1-45 Resource Allocation Tab



Memory Troubleshooting

The guidelines do not support memory sharing between VMs. To verify, the swapping and ballooning counters should be set to zero. If a given VM does not have enough memory and there are not memory issues on the specific host, consider increasing the VM's memory.

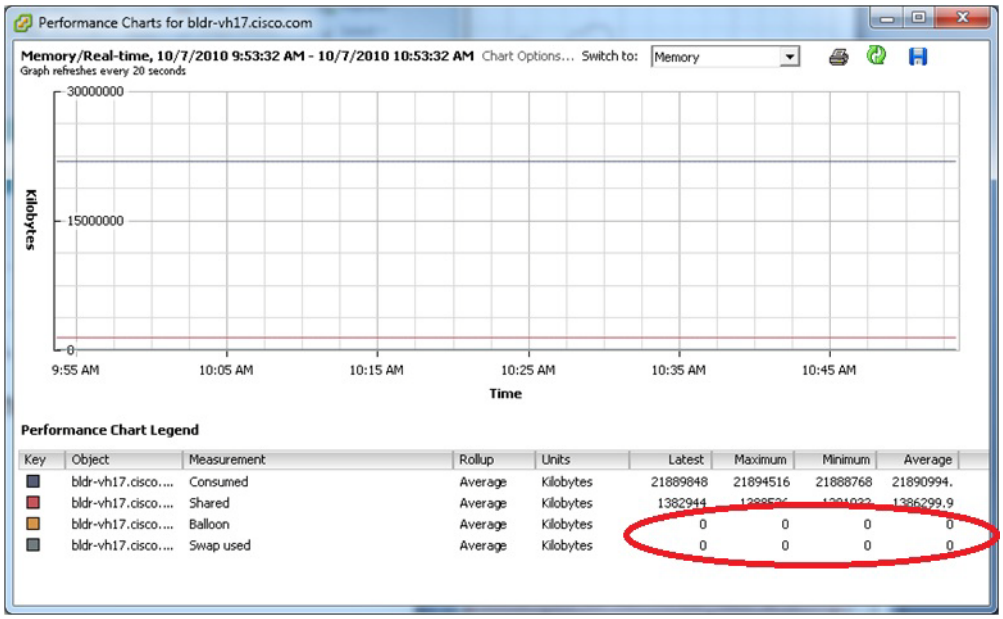
To view the memory performance indicators, go to the ESXi host's performance tab and select the advanced button.

Under chart options, select memory and timeframe, and then select the following counters:

- Used memory
- Swap used
- Balloon

Used memory can be used to look at general trends. Swap and balloon should always be “0”, otherwise memory sharing is being used, which should not be the case.

Figure 1-46 Memory in the Performance Chart



Disk Troubleshooting

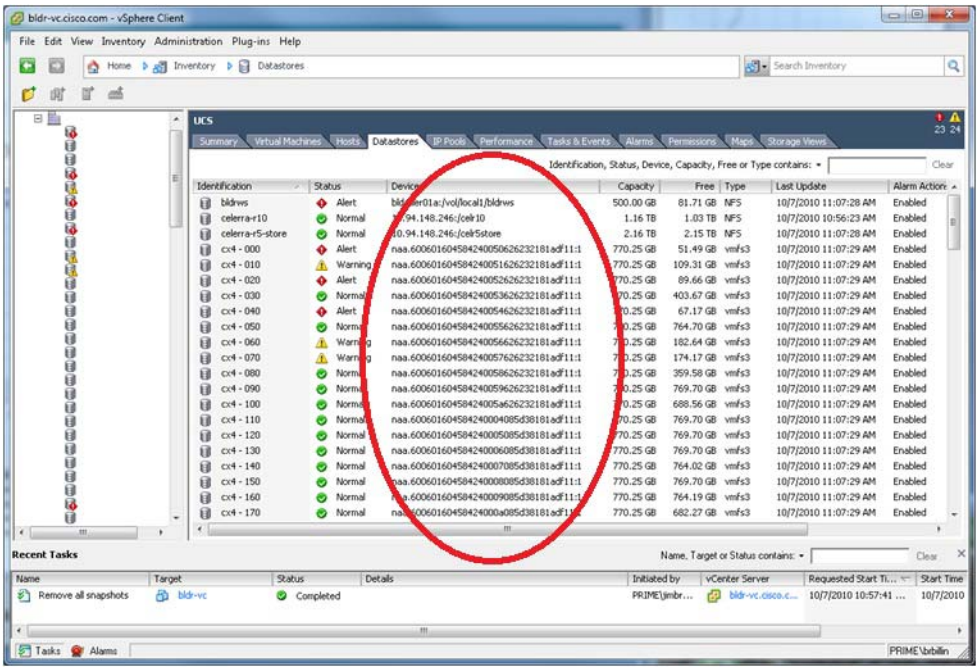
Bad disk performance often shows up as high CPU usage. IOPS data can provide information on how hard the application and VM is working the disks. Specific activities can cause spikes in IOPS such as upgrades and database maintenance. If VMs running on the same datastore are all doing these activities at the same time, the disks might not be able to keep up. IOPS data can be seen from vCenter or the SAN. Disk latency (response time) is a good indicator of disk performance.

Step 1 To view the disk performance indicators, go to the ESXi host's performance tab.

Step 2 Choose the **advanced** button.

Step 3 Choose the appropriate datastore, which can be found on the datastore page.

Figure 1-47 Datastore Page in vCenter



Step 4 Under chart options, select **disk** and **timeframe**.

Step 5 Choose the following counters:

- **Physical device command latency**
- **Kernel command latency**
- **Average commands issued per second**

The kernel counter should not be greater than 2-3ms. The physical device counter should not be greater than 15-20 ms. The 'Average commands issued per second' counter can be used if IOPS are not available from the SAN. IOPS should be considered if it looks like datastore is overload. This IOPS data is viewable from the host and each VM.

Note For NFS datastores, the physical and kernel latency data is not available. Starting in VMware 4.0 update 2 and beyond the esxtop command can be used to view NFS counters and in particular the guest latency. The guest latency is a summation of the physical device and kernel latencies.

Figure 1-48 Disk Latency Performance Chart

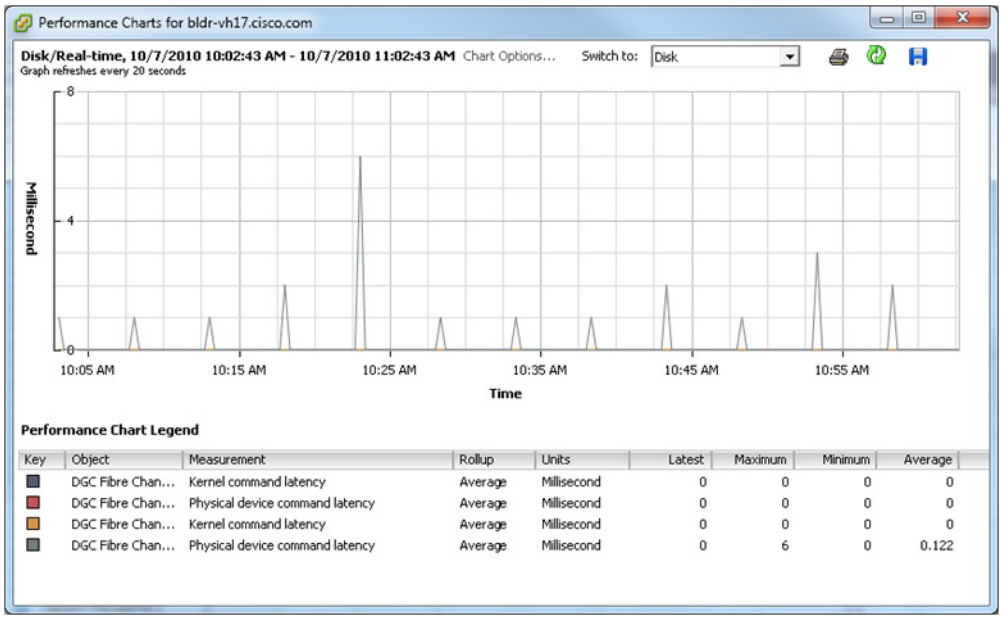
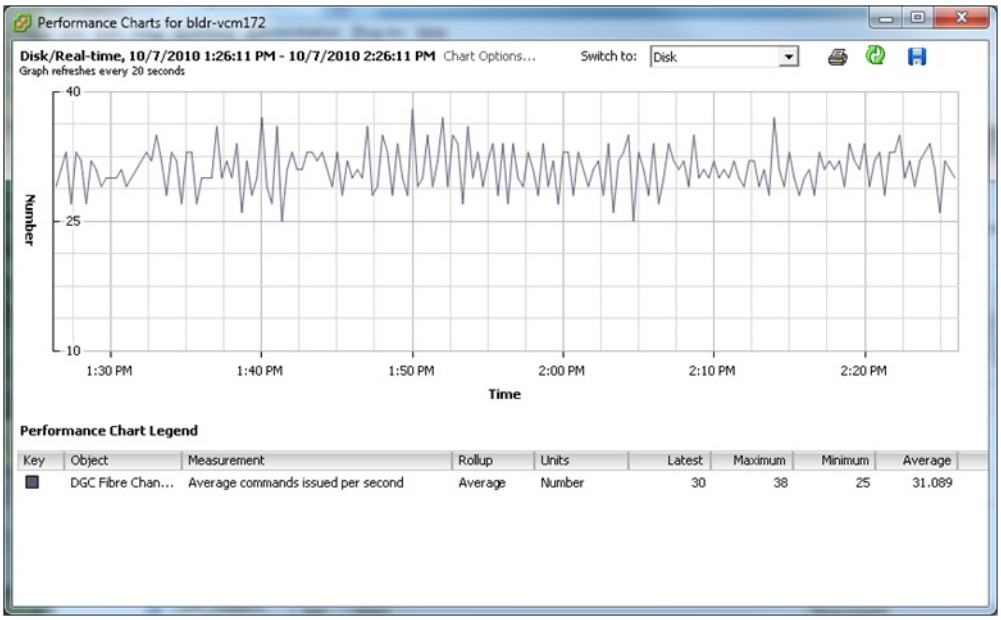


Figure 1-49 Disk IOPS Chart

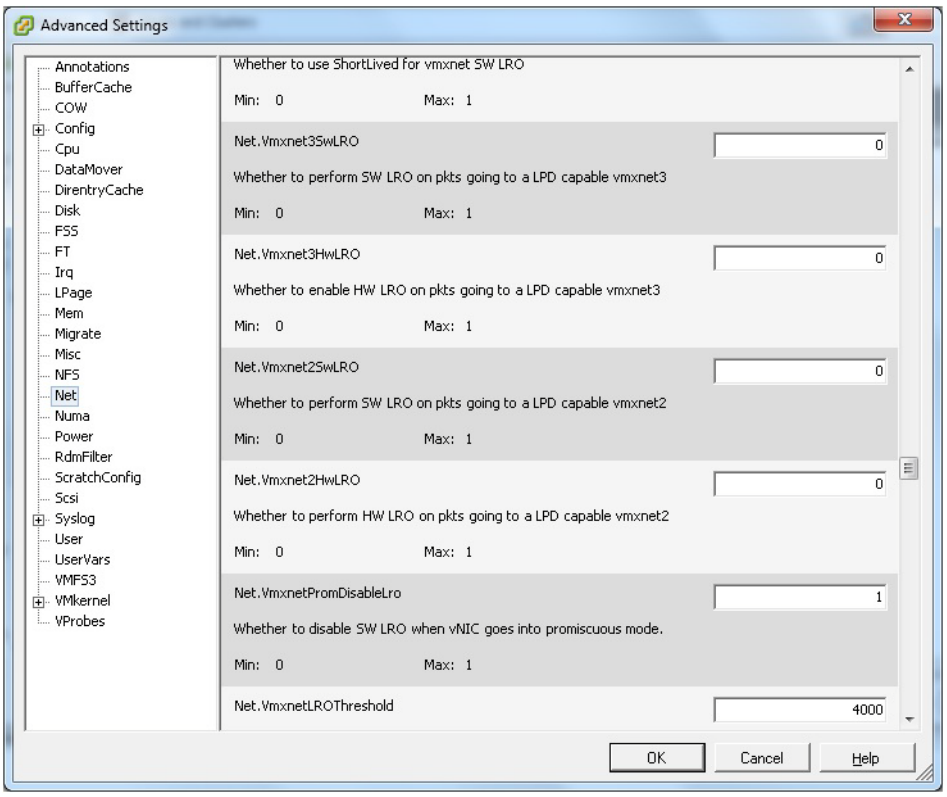


Network Troubleshooting

Generally, network performance issues can be seen by dropped packets. If dropped packets are seen from an ESXi host, the network infrastructure should be investigated for the issue, which might include a virtualized switch (Nexus 1000V). In ESXi 4.1, issues have been seen with large file transfers (e.g. SFTP/FTP transfers). For this issue, the Large Receive Offload options need to be disabled on the ESXi host. This setting is found on the host's Configuration tab > Advanced Settings > Net.*.

Note There are several LRO settings on this page and all of them need to be disabled. If a VM has been cloned and uses static MAC addresses, verify there are not duplicate MAC addresses in the network.

Figure 1-50 LRO Settings



To view the network performance indicators, follow these steps:

Step 1 Go to the ESXi host's performance tab.

Step 2 Choose the **advanced** button.

Step 3 Under chart options, select **Network** and **timeframe**.

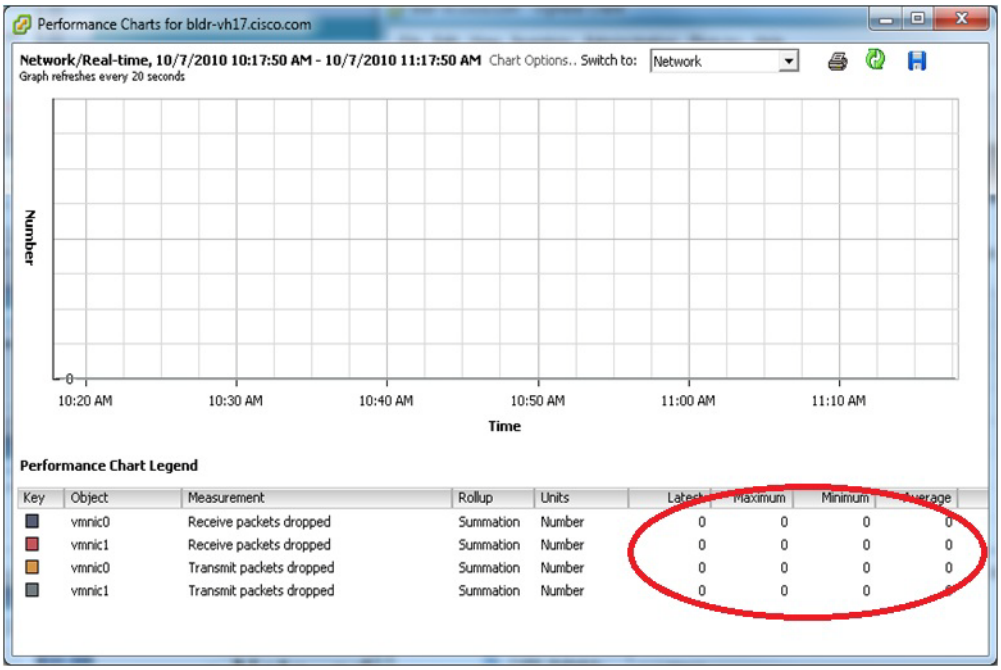
Step 4 Choose the following counters:

- **Receive packets dropped**
- **Transmit packets dropped**

The main thing to check is that no packets are getting dropped in the network.

Note Advanced network debugging and configuration can be done on Nexus 1000v if used, which requires vCenter.

Figure 1-51 Number of Packets Dropped



CPU Oversubscription Implications on Performance

Some deployments allow CPU oversubscription, which is the sharing of CPU cores between VMs. In this case, a few more data points need to be considered. First, look to see if CPU reservations are set for the VM. Cisco has recommended CPU reservations while using CPU oversubscription for some applications which are part of the official OVA. Second, look at the CPU ready time (i.e. how long a VM is waiting to run on a core). This counter can be converted into a percentage. General guidelines are to keep the percentage below 6% and then anything above 3% should be monitored for desired response times.

Figure 1-52 Reservation Page

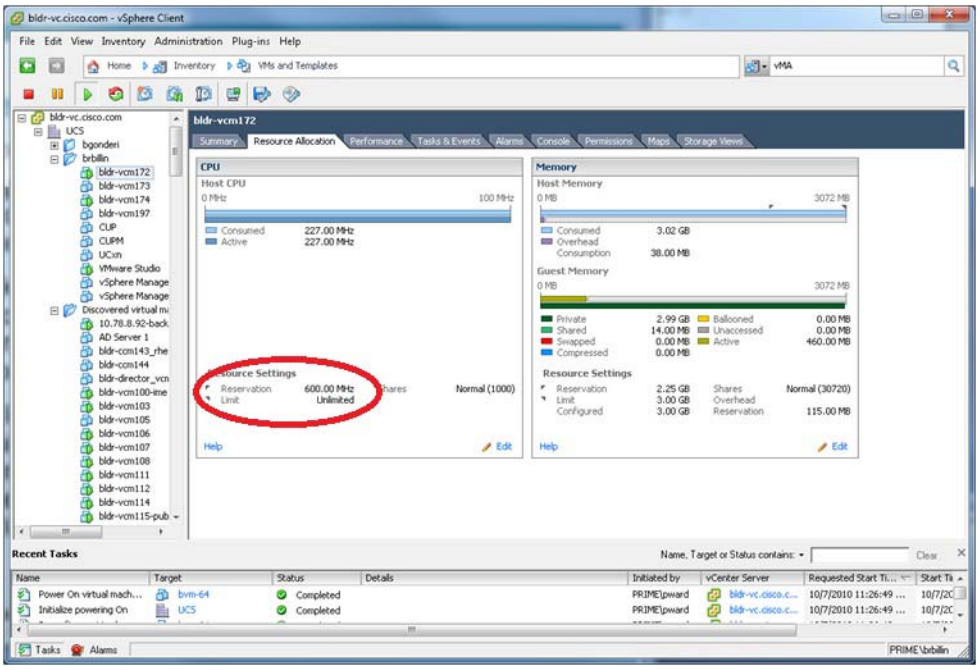
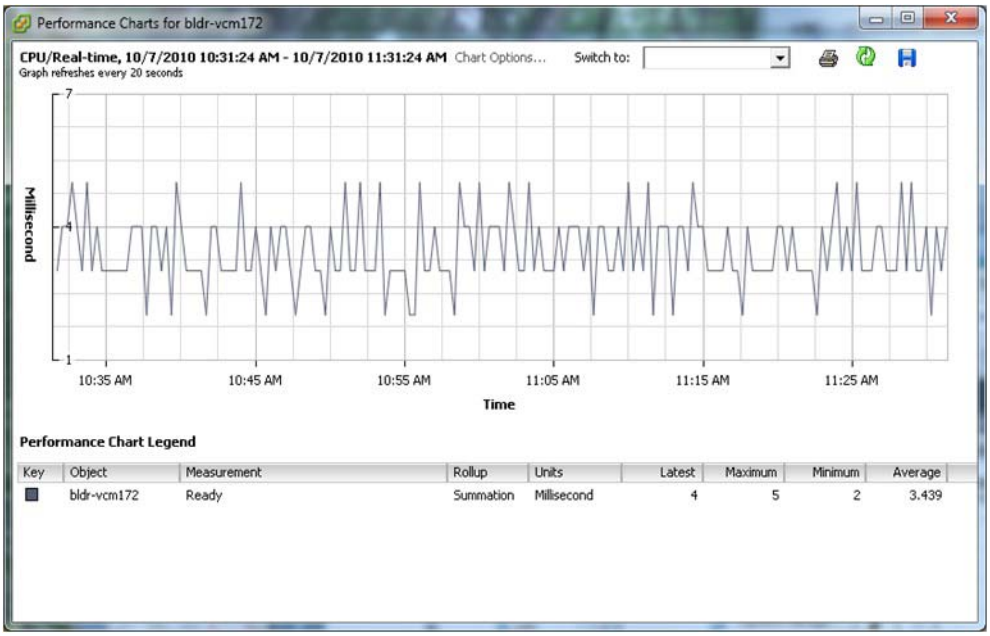


Figure 1-53 Ready Time Performance Chart



Other Considerations

On the C-series UCS servers there have been issues with the write cache battery backup. If this battery is not operating correctly, performance will suffer. Use a tool like WBEM Command Line Interface (wbemcli) to verify the battery is okay. The following output is an example of using the wbemcli:

```
wbemcli ei -noverify 'https://root:<password>@<ESXi Host
IP>:5989/root/cimv2:VMware_HHRCBattery'
```

Go to the following link to learn more about troubleshooting virtualized environments:

http://docwiki.cisco.com/wiki/Troubleshooting_and_Performance_Monitoring_Virtualized_Environments

Information to Help with Troubleshooting

RE Event and RESC Logs

RE Event logs can help with troubleshooting issues. Follow these steps:

Step 1 Download the RE Event log from REAC.

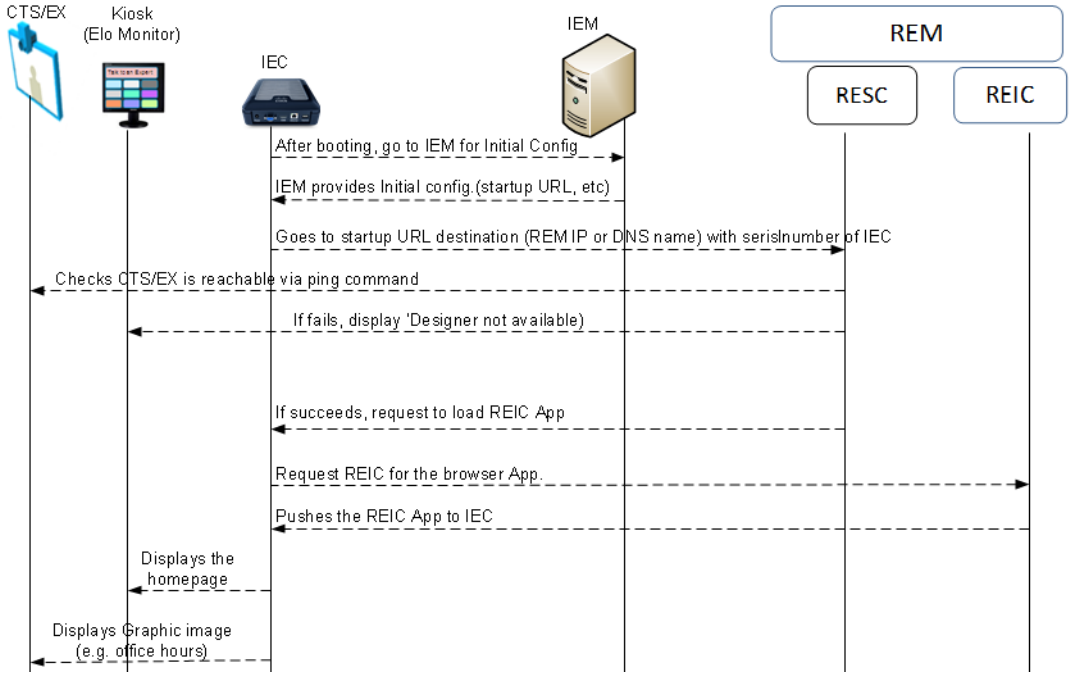
Step 2 Review the exception message column to determine if the desired operation threw an exception.

Step 3 If the root cause cannot be identified in the RE Event log, then download the resc log from REAC.

Step 4 Scan the resc log file for detailed information.

Normal IEC Bootup Sequence

Figure 1-54 IEC Bootup Sequence



The following happens during the IEC bootup sequence:

1. REM receives initial notification as indicated by “Received getKioskNotificationInfo : 656015330015”:

```
[http-bio-80-exec-44] com.cisco.big.scheduler.services.NotificationService - Received
getKioskNotificationInfo : 656015330015
[http-bio-80-exec-44] com.cisco.big.scheduler.services.NotificationService - Return
getKioskNotificationInfo
[org.springframework.scheduling.quartz.SchedulerFactoryBean#0_Worker-3]
com.cisco.big.scheduler.job.SchedulingJob - SchedulingJob invoked
[org.springframework.scheduling.quartz.SchedulerFactoryBean#0_Worker-3]
com.cisco.big.scheduler.job.SchedulingJob - SchedulingJob executed successfully
[org.springframework.scheduling.quartz.SchedulerFactoryBean#0_Worker-1]
com.cisco.big.scheduler.job.SchedulingJob - SchedulingJob invoked
[org.springframework.scheduling.quartz.SchedulerFactoryBean#0_Worker-1]
com.cisco.big.scheduler.job.SchedulingJob - SchedulingJob executed successfully
[http-bio-80-exec-37] com.cisco.big.va.services.VirtualAgentServices - Received
getKioskDetails unique serialNumber: 656015330015
[http-bio-80-exec-37] com.cisco.big.va.dao.KioskDAO -
[com.cisco.big.va.pojo.domain.Locale@57d04f0a]
[http-bio-80-exec-41] com.cisco.big.va.services.VirtualAgentServices - Received
getKioskDetails unique serialNumber: 656015330015
[http-bio-80-exec-41] com.cisco.big.va.dao.KioskDAO -
[com.cisco.big.va.pojo.domain.Locale@6555121a]
[http-bio-80-exec-44] com.cisco.big.admin.service.AdminService -
getContentByTimeInterval: Time :09-06-2012 05:18:23
[http-bio-80-exec-44] com.cisco.big.admin.service.AdminService - Parsed Date :Sat Jun
09 05:18:23 GMT+00:00 2012
```

2. REM instructs to load dual content image:

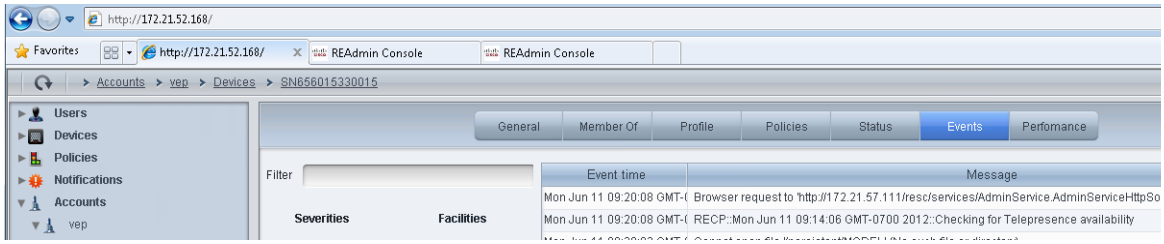
```
[http-bio-80-exec-44] com.cisco.big.va.dao.ContentDAO - Return DC Value
:http://172.21.57.111:80/images//bg_img_1920X1200.jpg
[http-bio-80-exec-37] com.cisco.big.admin.service.AdminService - reportPostIECReboot
invoked for KioskId :656015330015
```

3. REM routinely checks TP video endpoint reachability:

```
WARN [http-bio-80-exec-60] com.cisco.big.admin.util.VepManagementUtil - ------ ****
CTS for Kiosk: 656015330015 is not reachable 4 ****
WARN  [http-bio-80-exec-60] com.cisco.big.admin.util.VepManagementUtil - ------ ****
CTS for Kiosk: 656015330015 is not reachable 5 ****
WARN  [http-bio-80-exec-60] com.cisco.big.admin.util.VepManagementUtil - **** ---- CTS
for Kiosk:656015330015 is dead. after 5 tries
```

These logs will only be created when the IEC's local TP video endpoint is not reachable. If the TP video endpoint is reachable, then no such logs are created. However the routine checking of TP reachability logs will be available in IEC's event log in IEM.

Figure 1-55 IEC's Event Log

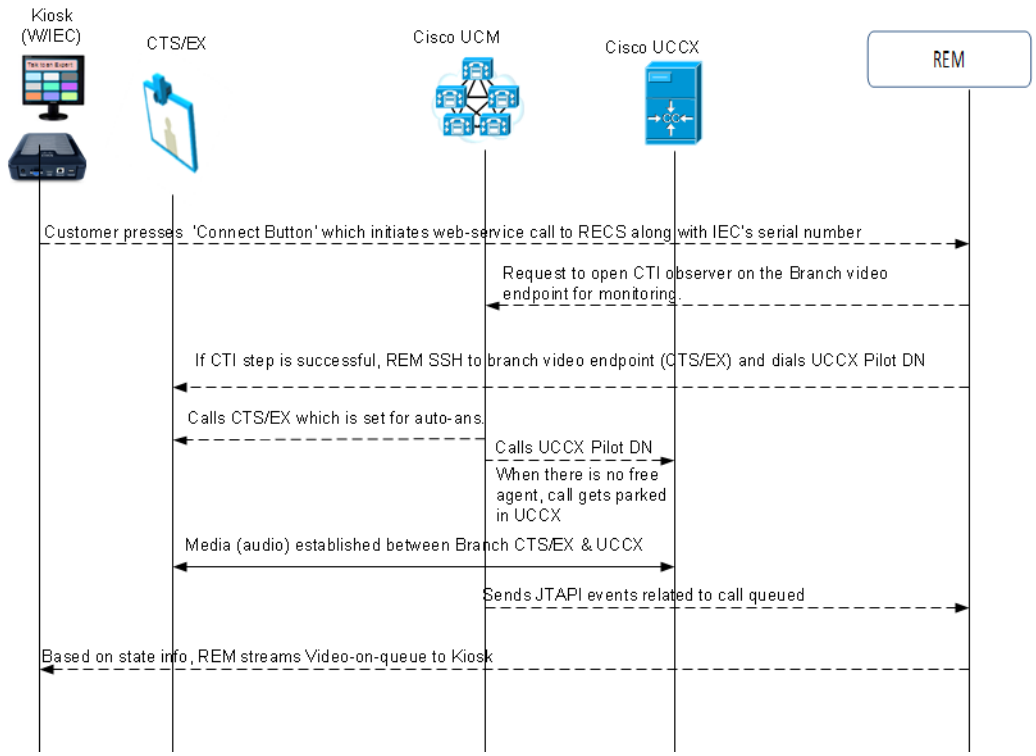


4. REM regularly monitors for aliveness of IEC, in particular the Cobra Application:

```
[http-bio-80-exec-46] com.cisco.big.admin.service.AdminService - Checking for
aliveness :656015330015 time:Sat Jun 09 12:19:11 GMT+00:00 2012
[http-bio-80-exec-46] com.cisco.big.admin.service.AdminService - Kiosk:656015330015 is
alive
```

Normal Call Flow and its Associated resc.log

Figure 1-56 Call Flow



In the scenario below, the customer presses the Connect button on the customer pod to have an immersive virtual collaboration with an expert and the following values are used:

- Customer pod IEC's serial number: 656015330015
- Customer-side EX90 video endpoint DN: 2512
- Contact Center Pilot DN: 1134
- Expert's DN: 2504
- Log file: resc.log

1. REM receives Call-Connect request after the customer pressed the Connect button on the customer pod indicated by "getKioskNotificationInfo: 656015330015" in the first line of the following output:

```
[http-bio-80-exec-87] com.cisco.big.scheduler.services.NotificationService - Received
getKioskNotificationInfo: 656015330015
[http-bio-80-exec-87] com.cisco.big.scheduler.services.NotificationService - Return
getKioskNotificationInfo
[pool-17-thread-2] com.cisco.big.call.CallService - CallConnectTimeout Call not
established yet....
[pool-17-thread-2] com.cisco.big.call.CallService - ExpertType namedecoratorEWT : 10
[pool-17-thread-4] com.cisco.big.call.CallService - CallConnectTimeout Call not
established yet....
[pool-17-thread-4] com.cisco.big.call.CallService - ExpertType namedecoratorEWT : 10
[http-bio-80-exec-87] com.cisco.big.va.services.VirtualAgentServices - Call Connect
Request : Kiosk Serial : 656015330015 ExpertType :
```

2. REM gets the DN of the customer pod-side video endpoint REAC/REM indicated by “Address in service event for:2512” in the first line of the following output:

```
[ObserverThread(com.cisco.big.call.BIGObserver@403bfa49)]
com.cisco.big.call.BIGObserver - Address in service event for :2512
[http-bio-80-exec-87] com.cisco.big.call.CallService - Time taken to check if Address
is in service: 0
```

3. REM able to start JTAPI Monitoring on 2512:

```
[http-bio-80-exec-87] com.cisco.big.call.CallService - Is Address in service: true
[http-bio-80-exec-87] com.cisco.big.call.CallService - Time taken to check if call is
present: 1002
[http-bio-80-exec-87] com.cisco.big.call.CallService - Is call Present: false
[http-bio-80-exec-87] com.cisco.big.call.BIGObserver - Starting an SSH connection to
CTS to execute call Startcommand
[http-bio-80-exec-86] com.cisco.big.scheduler.services.NotificationService - Received
getKioskNotificationInfo: 656015330015
[http-bio-80-exec-86] com.cisco.big.scheduler.services.NotificationService - Return
getKioskNotificationInfo
[pool-17-thread-2] com.cisco.big.call.CallService - CallConnectTimeout Call not
established yet....
[pool-17-thread-2] com.cisco.big.call.CallService - ExpertType namedecoratorEWT : 10
```

4. REM connects to customer pod-side endpoint via SSH indicated by “Starting an SSH connection to 10.17.161.51” in the first line of the following output:

```
[http-bio-80-exec-87] com.cisco.big.call.tp.SSHCommandExecutor - Starting an SSH
connection to 10.17.161.51
[http-bio-80-exec-87] com.cisco.big.call.tp.SSHCommandExecutor - Starting Pre
condition Check
[http-bio-80-exec-87] com.cisco.big.call.tp.SSHCommandExecutor - Initializing
PreCommandExecutionMatchString
[http-bio-80-exec-87] com.cisco.big.call.tp.SSHCommandExecutor - available: 0
[http-bio-80-exec-87] com.cisco.big.call.tp.SSHCommandExecutor - totalReadTimeout:
25000
[http-bio-80-exec-87] com.cisco.big.call.tp.SSHCommandExecutor - sleepReadtime: 2000
[http-bio-80-exec-87] com.cisco.big.call.tp.SSHCommandExecutor - available: 95
[http-bio-80-exec-87] com.cisco.big.call.tp.SSHCommandExecutor - readBytes: 95
[http-bio-80-exec-87] com.cisco.big.call.tp.SSHCommandExecutor - Welcome
to.0.290141Alpha3
```

5. REM successfully connected to video endpoint via SSH indicated by “Completed preCommandExecutionMatchString” in the second line of the following output:

```
R [http-bio-80-exec-87] com.cisco.big.call.tp.SSHCommandExecutor -
ProcessBytesAndMatchString executed successfully for Command: callConnect
[http-bio-80-exec-87] com.cisco.big.call.tp.SSHCommandExecutor - Completed
preCommandExecutionMatchString
```

6. REM dials Contact Center Pilot DN (1134) indicated by “Executing xcommand dial number: 1134”in the first line of the following output:

```
[http-bio-80-exec-87] com.cisco.big.call.tp.SSHCommandExecutor - Executing xcommand
dial number: 1134
[http-bio-80-exec-87] com.cisco.big.call.tp.SSHCommandExecutor - Starting Post
condition Check
[http-bio-80-exec-87] com.cisco.big.call.tp.SSHCommandExecutor - Initializing
PreCommandExecutionMatchString
[http-bio-80-exec-87] com.cisco.big.call.tp.SSHCommandExecutor - available: 0
[http-bio-80-exec-87] com.cisco.big.call.tp.SSHCommandExecutor - totalReadTimeout:
23000
[http-bio-80-exec-87] com.cisco.big.call.tp.SSHCommandExecutor - sleepReadtime: 2000
```

```
[pool-17-thread-4] com.cisco.big.call.CallService - CallConnectTimeout Call not
established yet....
[pool-17-thread-4] com.cisco.big.call.CallService - ExpertType namedecoratorEWT : 10
[http-bio-80-exec-86] com.cisco.big.admin.service.AdminService - Checking for
aliveness :656015330015 time:Fri Jun 08 14:39:25 GMT+00:00 2012
[http-bio-80-exec-86] com.cisco.big.admin.service.AdminService - Kiosk:656015330015 is
alive
[http-bio-80-exec-87] com.cisco.big.call.tp.SSHCommandExecutor - available: 108
[http-bio-80-exec-87] com.cisco.big.call.tp.SSHCommandExecutor - readBytes: 108
[http-bio-80-exec-87] com.cisco.big.call.tp.SSHCommandExecutor - xcommand dial number:
1134
[http-bio-80-exec-87] com.cisco.big.call.tp.SSHCommandExecutor -
ProcessBytesAndMatchString executed successfully for Command: callConnect
[http-bio-80-exec-87] com.cisco.big.call.tp.SSHCommandExecutor - Completed
PostCommandExecutionMatchString
[http-bio-80-exec-87] com.cisco.big.call.BIGObserver - Time taken to execute SSH
command on CTS: 4
```

7. REM shows call connected between DN 2512 and 1134 indicated by “1134” in the first line, “2512” in the second line, and “CallConnected1134” in the third line of the following output:

```
[ObserverThread(com.cisco.big.call.BIGObserver@403bfa49)]
com.cisco.big.call.BIGObserver - BIGObserver - Curent Called Address:1134
[ObserverThread(com.cisco.big.call.BIGObserver@403bfa49)]
com.cisco.big.call.BIGObserver - BIGObserver - Curent Calling Address:2512
[ObserverThread(com.cisco.big.call.BIGObserver@403bfa49)]
com.cisco.big.call.BIGObserver - CallConnected1134
[ObserverThread(com.cisco.big.call.BIGObserver@403bfa49)]
com.cisco.big.call.BIGObserver - class com.cisco.jtapi.ConnCreatedEvImpl
[ObserverThread(com.cisco.big.call.BIGObserver@403bfa49)]
com.cisco.big.call.BIGObserver - BIGObserver - Curent Called Address:2504
[ObserverThread(com.cisco.big.call.BIGObserver@403bfa49)]
com.cisco.big.call.BIGObserver - BIGObserver - Curent Calling Address:2512
[ObserverThread(com.cisco.big.call.BIGObserver@403bfa49)]
com.cisco.big.call.BIGObserver - class com.cisco.jtapi.ConnConnectedEvImpl
```

8. REM finds call is not connected to expert (queued call):

```
[pool-17-thread-2] com.cisco.big.call.CallService - CallConnectTimeout Call not
established yet....
[pool-17-thread-2] com.cisco.big.call.CallService - ExpertType namedecoratorEWT : 10
[pool-17-thread-4] com.cisco.big.call.CallService - CallConnectTimeout Call not
established yet....
[pool-17-thread-4] com.cisco.big.call.CallService - ExpertType namedecoratorEWT : 10
pool-17-thread-6] com.cisco.big.call.CallService - CallConnectTimeout Call not
established yet...
```

9. REM shows call connected to the expert (DN:2504) indicated by “2504” in the first line, “2512” in the second line, and “CallConnected2504” in the third line of the following output:

```
[ObserverThread(com.cisco.big.call.BIGObserver@403bfa49)]
com.cisco.big.call.BIGObserver - BIGObserver - Curent Called Address:2504
[ObserverThread(com.cisco.big.call.BIGObserver@403bfa49)]
com.cisco.big.call.BIGObserver - BIGObserver - Curent Calling Address:2512
[ObserverThread(com.cisco.big.call.BIGObserver@403bfa49)]
com.cisco.big.call.BIGObserver - CallConnected2504
```

10. REM detects call is on hold by expert indicated by “2504 In manageOnHold” in the last line of the following output:

```
[ObserverThread(com.cisco.big.call.cm.observer.AgentObserver@5e6276e5)].AgentObserver
-  Agent Observer - DN: 2504
[ObserverThread(com.cisco.big.call.cm.observer.AgentObserver@5e6276e5)]
com.cisco.big.call.cm.observer.AgentObserver - Event :
```

```
[ObserverThread(com.cisco.big.call.cm.observer.AgentObserver@5e6276e5)]
com.cisco.big.call.cm.observer.AgentObserver - 2504 Call:2512 --> 2504
[ObserverThread(com.cisco.big.call.cm.observer.AgentObserver@5e6276e5)]
com.cisco.big.call.cm.observer.AgentObserver - 2504 Call Id:9245
[ObserverThread(com.cisco.big.call.cm.observer.AgentObserver@5e6276e5)]
com.cisco.big.call.cm.observer.AgentObserver - 2504 In manageOnHold
```

11. REM detects call is resumed by expert indicated by “2504 In manageTalking” in the third line of the following output:

```
[ObserverThread(com.cisco.big.call.cm.observer.AgentObserver@5e6276e5)]
com.cisco.big.call.cm.observer.AgentObserver - 2504 Call:2512 --> 2504
[ObserverThread(com.cisco.big.call.cm.observer.AgentObserver@5e6276e5)]
com.cisco.big.call.cm.observer.AgentObserver - 2504 Call Id:9245
[ObserverThread(com.cisco.big.call.cm.observer.AgentObserver@5e6276e5)]
com.cisco.big.call.cm.observer.AgentObserver - 2504 In manageTalking
[ObserverThread(com.cisco.big.call.cm.observer.AgentObserver@5e6276e5)]
com.cisco.big.call.cm.observer.BaseObserver - Session reference not
[ObserverThread(com.cisco.big.call.cm.observer.AgentObserver@5e6276e5)]
com.cisco.big.call.cm.observer.AgentObserver - List of Session on Agent
```

12. REM detects call is disconnected indicated by “Call disconnected” in the last line of the following output:

```
[ObserverThread(com.cisco.big.call.BIGObserver@403bfa49)]
com.cisco.big.call.BIGObserver - class com.cisco.jtapi.ConnDisconnectedEvImpl
[ObserverThread(com.cisco.big.call.BIGObserver@403bfa49)]
com.cisco.big.call.BIGObserver - class com.cisco.jtapi.ConnDisconnectedEvImpl
[ObserverThread(com.cisco.big.call.BIGObserver@403bfa49)]
com.cisco.big.call.BIGObserver - BIGObserver - Curent Called Address:2504
[ObserverThread(com.cisco.big.call.BIGObserver@403bfa49)]
com.cisco.big.call.BIGObserver - BIGObserver - Curent Calling Address:2512
[ObserverThread(com.cisco.big.call.BIGObserver@403bfa49)]
com.cisco.big.call.BIGObserver - class com.cisco.jtapi.TermConnDroppedEvImpl
[ObserverThread(com.cisco.big.call.BIGObserver@403bfa49)]
com.cisco.big.call.BIGObserver - BIGObserver - Curent Called Address:2504
[ObserverThread(com.cisco.big.call.BIGObserver@403bfa49)]
com.cisco.big.call.BIGObserver - BIGObserver - Curent Calling Address:2512
[ObserverThread(com.cisco.big.call.BIGObserver@403bfa49)]
com.cisco.big.call.BIGObserver - class com.cisco.jtapi.ConnDisconnectedEvImpl
[ObserverThread(com.cisco.big.call.BIGObserver@403bfa49)]
com.cisco.big.call.BIGObserver - BIGObserver - Curent Called Address:2504
[ObserverThread(com.cisco.big.call.BIGObserver@403bfa49)]
com.cisco.big.call.BIGObserver - BIGObserver - Curent Calling Address:2512
[ObserverThread(com.cisco.big.call.BIGObserver@403bfa49)]
com.cisco.big.call.BIGObserver - Setting the session to status 2
[ObserverThread(com.cisco.big.call.BIGObserver@403bfa49)]
com.cisco.big.call.BIGObserver - Call disconnected
```

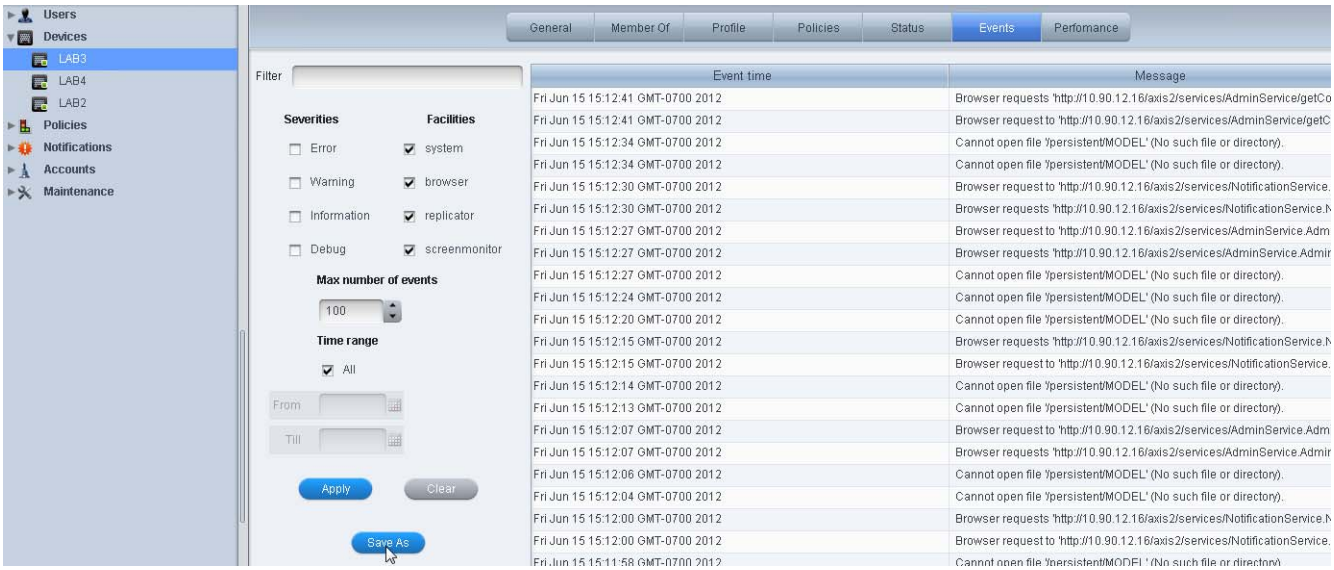
Trace Files for TAC

There are normally two log files that are needed by the Cisco TAC team to troubleshoot REM related issues:

1. resc.log file
2. IEC’s event log from the IEM

Go to the IEC’s event screen, select all the check boxes under facility (by default it is all selected), and then press the **Save as** button. When the local workstation’s Windows Explorer window opens, save the log file to the local disk.

Figure 1-57 IEC's Event Log in the IEM



CHAPTER 2

Serviceability Administration

Revised: August 21, 2014, OL-27568-05

Chapter Overview

This chapter is intended for service engineers and server administrators who are accountable for keeping the REM up and running to its complete usability and performance. The scope of this chapter is restricted to topics that assist administrators with maintaining the REM application. This chapter also explains how to backup and restore the REM.

Topics in this chapter include:

Serviceability Overview

Serviceability administration provides descriptions and procedures for the following functionality:

- Supports daily management of REM applications
- Schedules monitoring and maintenance of the each component
- Captures events for troubleshooting and provides alert/error message definitions
- Saves trace information to various log files for troubleshooting
- Monitors the disk usage of the log partition on a server

Monitoring

Monitoring involves keeping track of various errors and warning being thrown by various components of the REM. It involves checking the state or health of all REM components for availability and appropriate functioning of all solution features.

There are various errors and alerts that are thrown by REM which needs to be resolved to keep the REM up and running.

Errors and Alerts from REAC

The tables below document the errors and alerts that could be thrown by the Remote Expert Admin Console (REAC) application and shown on the user interface (UI).

Table 2-1 Generic REAC Errors

Error/Alert	Description	Solution
Unable to contact the web server. Please check web server status.	Occurs when the REM server is down	Bring the REM server up by using the TUI: Main Menu > Services Control > Application Server > b) Start Service
An internal error occurred	Occurs during Kiosk restart if RESC has encountered an internal error	Check the RESC log file for the specific error condition by using the TUI: Main Menu > Troubleshooting > Logs > Remote Expert Logs > a) RESC Logs: resc.log
Unable to connect to REM Server	Occurs during Kiosk restart when REAC is unable to connect to RESC (if RESC is deployed on a separate server)	1. Bring the REM server up by using the TUI: Main Menu > Services Control > Application Server > b) Start Service 2. Check the RESC IP by using the TUI: Main Menu > REM Server Administration > b) Edit REM Properties > REM Core Properties
Unable to restart kiosk	Occurs during Kiosk restart if REM has failed to restart due to issues on the server	1. Check the Kiosk settings > IEC Serial Number 2. Perform the same operation again 3. Restart IEC from IEM 4. Restart IEC manually
Illegal input provided	Occurs during Kiosk restart if Kiosk has been deleted from REM	Check the REAC log file for the specific error condition by using the TUI: Main Menu > Troubleshooting > Logs > Remote Expert Logs > d) REAC Logs: reac.log
Unable to connect to Kiosk	Occurs during Kiosk restart when REM server is unable to make connection to the IEM	Verify if the IEM IP address is correct in the REM Properties file by using the TUI: Main Menu > REM Server Administration > b) Edit REM Properties
HTTP (500): The server reported an Error	The server has encountered an internal error, which prevented it from fulfilling the request	1. Check REAC log file for the specific error condition by using the TUI: Main Menu > Troubleshooting > Logs > Remote Expert Logs > d) REAC Logs: reac.log 2. Check RESC log file for the specific error condition by using the TUI: Main Menu > Troubleshooting > Logs > Remote Expert Logs > a) RESC Logs: resc.log

Error/Alert	Description	Solution

An error occurred during File Transfer	The server has encountered an internal error, which prevented it from fulfilling the request	1. Check RESC IP by using the TUI: Main Menu > REM Server Administration > b) Edit REM Properties > REM Core Properties
		2. Check the following parameters in REAC PROPERTIES by using the TUI: Main Menu > REM Server Administration > Edit REM Templates > a) REAC Properties:
		`remote_server_ip=$*[RESC_IP]*`
		`remote_server_uname=ENC($*[RESC_SERVER_USER]*)`
		`remote_server_pwd=ENC($*[RESC_SERVER_PASSW]*)`

Unable to synchronize resources across cluster nodes	Occurs during file transfer when handshaking between the two nodes fails	1. Refer to the JTAPI Issues section of this chapter to fix the issue 2. Upload the file from REAC again

Table 2-2 Remote Service Call Errors

Error/Alert	Description	Solution
Remote call to xxxx failed	Occurs when REAC is unable to communicate to REM server	1. Check REAC log file for the specific error condition by using the TUI: Main Menu > Troubleshooting > Logs > Remote Expert Logs > d) REAC Logs: reac.log 2. Verify if RESC services are available by invoking "https://<REM_IP>:8443/resc/services/listServices"
Remote call to xxxx returned an empty response	Occurs when REM server sends invalid response	Check RESC log file for the specific error condition by using the TUI: Main Menu > Troubleshooting > Logs > Remote Expert Logs > a) RESC Logs: resc.log

Table 2-3 Cluster Management Errors

Error/Alert	Description	Solution
The requested operation cannot be executed due to incomplete configuration	Occurs if the REM server details and DB details are missing in REM configuration file	1. Verify the values of $*[NODE_IP_1]* and $*[DATABASE_1]* in the REM Properties file by using the TUI: Main Menu > REM Server Administration > b) Edit REM Properties 2. Use the TUI: Main Menu > REM Server Administration > c) Run Configuration Tool
The selected operation failed	Occurs if there is an error while activating the DB	Check the REAC log file for the specific error condition by using the TUI: Main Menu > Troubleshooting > Logs > Remote Expert Logs > d) REAC Logs: reac.log
The selected node "{0}" is not found	Occurs if the REM server details and DB details are missing in REM configuration file	1. Verify the values of $*[NODE_IP_1]* and $*[DATABASE_1]* in REM Properties location by using the TUI: Main Menu > REM Server Administration > b) Edit REM Properties 2. Use the TUI: Main Menu > REM Server Administration > c) Run Configuration Tool

Errors and Alerts from READ

The errors generated by the READ application can be grouped in two scenarios:

1. Direct Connect (DC) errors in the READ application
2. Errors or alerts from the READ application

Table 2-4 Direct Connect Errors

Error/Alert	Description	Solution
DC pops up in READ and after clicking on the Start sharing button but it remains in the Waiting state	The 'cv_service_url' in DirectConnect.exe.config is incorrect. File direction C:\CSI\DirectConnect\bin\DirectConnect is incorrect	1) Fix 'cv_service_url' to point to the correct REM IP address 2) Restart the DC Server from the desktop
	The Expert is not registered in REM	Verify in the Expert tab in REAC that the expert is added
	DC license has expired. The error displayed in error.log available at C:\CSI\DirectConnect\Server\tomcat\logs\error.log is the following: `2012-04-13 11:46:47,584 ERROR [/] Exception sending context initialized event to listener instance of class pureweb.servlet.ContextListener java.lang.RuntimeException: com.reprisesoftware.rlm.RlmException: License has expired (-3) at pureweb.servlet.ContextListener.contextInitialized(ContextListener.java:88) ~[ContextListener.class:na]`	Renew DC license

Table 2-5 READ Errors

Error/Alert	Description	Solution
READ not initialized	Occurs when READ is unable to contact RESC	Verify if services of RESC are available by invoking "https://<REM_IP>:8443/resc/services/listServices"
Previous collaboration request is still in progress	Occurs if trying to start a READ module when the current one is still in progress	In READ, check job status if Document Camera, Scan, Signature Capture, or DirectConnect are running before trying to start another module
Checking for an active session…	Occurs if CAD Admin has incorrect values	Refer to the *CAD Administration Guide*
Communication Failure: Please contact Administrator	Occurs if the REM server goes down during the session	Bring the REM server up by using the TUI: Main Menu > Services Control > Application Server > b) Start Service

Error/Alert	Description	Solution
404 error in document sharing panel for local file upload	Unable to fetch the url of the uploaded file	Check if the 'docstore.url' or 'docstore.path' parameter is configured properly in READ properties by using the TUI: Main Menu > REM Server Administration > Edit REM Templates > f) READ properties
No route to host	Occurs when printing a local file	Check if the 'webservice.url' parameter is missing in READ properties by using the TUI: Main Menu > REM Server Administration > Edit REM Templates > f) READ properties

Errors and Alerts from REIC

There are different types of error pages used in REIC. All the error codes with detailed description are tabulated below. A message specific to particular error code is displayed on the REIC screen. If there is no message associated with the error code, REIC displays the error code itself on the touch screen collaboration panel.

Table 2-6 REIC Errors

Error/Alert	Description	Solution
System is not available, Please try after some time	Occurs due to below reasons: 1. If TP details (TP Directory Number or TP Type) is incorrect 2. TP MAC address is not added in CUCM> Application user 3. IVR Phone Number is incorrect	1. Verify the TP details in REAC > Kiosk 2. Add the TP MAC address in CUCM >Application user 3. Check IVR Phone Number in REAC > Expert Type
Kiosk phone is out of service	Occurs if connection within the Kiosk phone is not available	1. Verify the values of CUCM in REM Properties by using the TUI: Main Menu > REM Server Administration > b) Edit REM Properties 2. Kiosk phone is not reachable. Please check the connection status.
Sorry, there is already an active call to an Expert. Please try again after the current call ends	Occurs when an expert is engaged in another call	Make sure that the current call ends on the TP and try again after some time
Locale File does not exist	Occurs if the file is missing in the system	Make sure Message Bundle is added in REAC > Locale

Error/Alert	Description	Solution
Kiosk serial number is not configured, cannot start a call	Occurs when Kiosk serial number is not configured properly	Verify the IEC Serial Number in REAC > Kiosk
Selected Locale is not associated to any expert type. Please contact admin	Occurs if the locale associated to the kiosk is not associated with any expert type	Associate the Expert Type with locale in REAC > Expert Type
Agents are not available currently. Please try after sometime	Occurs when all agents are busy	Try again after a period of time
Expert not Available	Occurs when 1. TP is down 2. TP IP address in REAC > Kiosk is incorrect	1. Power on the TP and restart IEC from the IEM 2. Edit TP details (TP IP address in REAC > Kiosk)
Server is down	REM server is down	Bring the REM server up by using the TUI: Main Menu > Services Control > Application Server > b) Start Service
Kiosk is not registered	Occurs if the particular device number is not added in REAC	Make sure this kiosk is added in REAC > Kiosk
SYSTEM ERROR Below are probable reasons for this error. Please contact admin • RESC is not running	Occurs during the loading of Kiosk home page	1. Verify if services of RESC are available by invoking "https://<REM_IP>:8443/resc/services/listServices" 2. Verify the values of CUCM in REM Properties by using the TUI: Main Menu > REM Server Administration > b) Edit REM Properties 3. Restart the REM server by using the TUI: Main Menu > Services Control > Application Server > c) Stop Service > b) Start Service
Improper loading of REIC	1. Occurs if the value of $*[RESC_IP]* in rem.properties is incorrect 2. Expert type is not configured properly in REAC 3. If Startup URL in IEM is incorrect	1. Check RESC IP by using the TUI: Main Menu > REM Server Administration > b) Edit REM Properties > REM Core Properties 2. Check Expert type in REAC > Expert Type 3. Check Startup URL in the IEM
REIC hangs	Occurs if there are un-terminated sessions	Terminate sessions in REAC > Clean Call Cache

Error/Alert	Description	Solution
REIC is showing Cobra browser page with message “Startup URL is not configured.”	Occurs if the policy is missing in IEM	Check if the IEM has correct policy assigned to this Kiosk
REIC is showing “Service Temporarily Unavailable”	Occurs if the Startup URL in IEM is incorrect or REM server is unable to make connection to the IEM	1. Verify if the IEM IP address is correct in REM Properties by using the TUI: Main Menu > REM Server Administration > b) Edit REM Properties 2. Verify correct Startup URL in the IEM policy

REM Server (RESC) Errors

- In order to check if RESC is running properly, run this URL in the browser: https://<REM_IP>:8443/resc/services/AdminService/getVersionInfo
- If RESC is deployed or running properly then you will see the result shown in the figure below.

Figure 2-1 RESC is Running Properly

```
– <ns:getVersionInfoResponse>
    <ns:return>REM-1.9.0-7</ns:return>
  </ns:getVersionInfoResponse>
```

- If RESC is not deployed or running properly, then you will see the result shown in the figure below.

Figure 2-2 RESC is Not Running Properly

```
– <soapenv:Reason>
  – <soapenv:Text xml:lang="en-US">
      The service cannot be found for the endpoint reference (EPR) /resc/services/AdminService/getVersionInfo
    </soapenv:Text>
  </soapenv:Reason>
```

Refer to the “Call Related Errors” section of this chapter to troubleshoot these issues.

Log Monitoring

The log files for all the REM components are tabulated below.

Table 2-7 Log Files

Component Name	Log File Location
RESC	TUI: Main Menu > Troubleshooting > Logs > Remote Expert Logs > a) RESC Logs: resc.log
REAC	TUI: Main Menu > Troubleshooting > Logs > Remote Expert Logs > a) REAC Logs: reac.log
REIC	Refer to the "Events Tab in the IEM" for REIC log location
READ	TUI: Main Menu > Troubleshooting > Logs > Remote Expert Logs > a) READ Logs: read.log

Look into the respective log files mentioned above if there are any errors in any of the REM components.

Events Tab in the IEM

The IEM allows you to do the following:

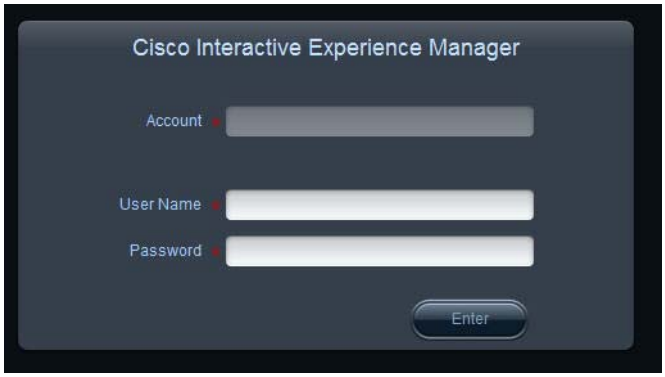
- View all the IECs registered with the IEM
- Check the REIC logs

To perform the above tasks, follow these steps:

Step 1 Enter http://<IEM_IP> in a browser.

Step 2 Enter the credentials and click **Enter**.

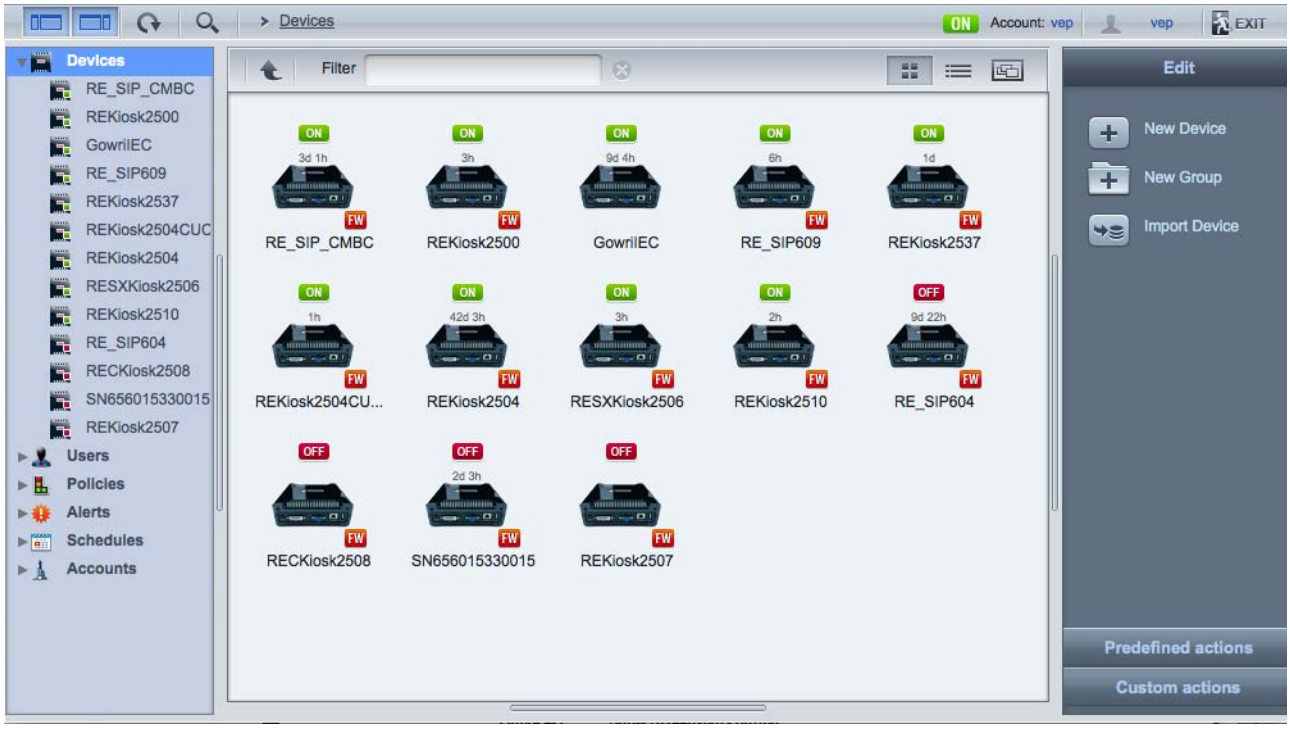
Figure 2-3 IEM Login Window



Step 3 Click **Devices** on the left navigation pane.

All the IECs registered with the IEM in your account are visible in both the left and center panes.

Figure 2-4 Devices

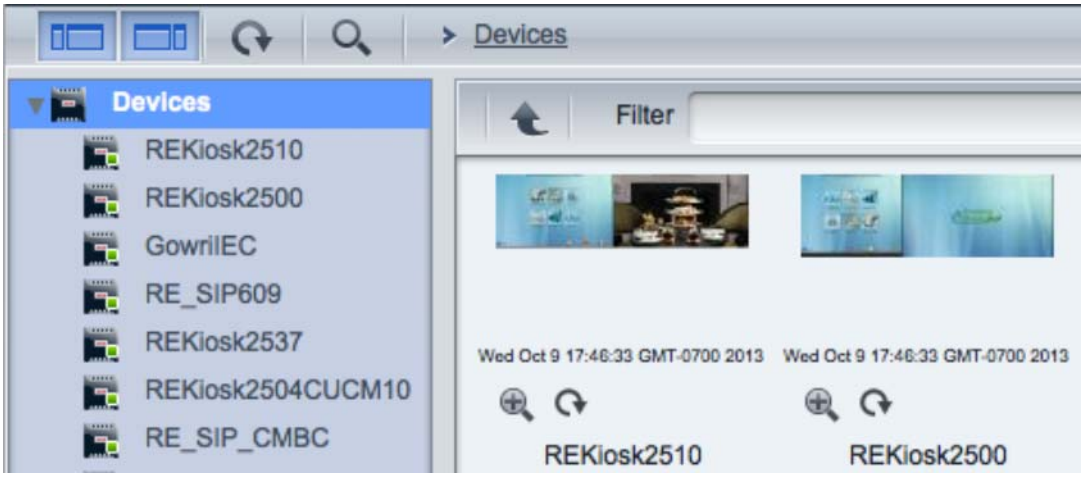


Step 4 Click the **Show screenshots** button on the top right corner of the display view to view the screenshot of each of the IECs registered with the IEM.

Figure 2-5 Show Screenshots Button

The screenshots are pulled from the last time that the IECs were polled by the IEM.

Figure 2-6 Screenshot View

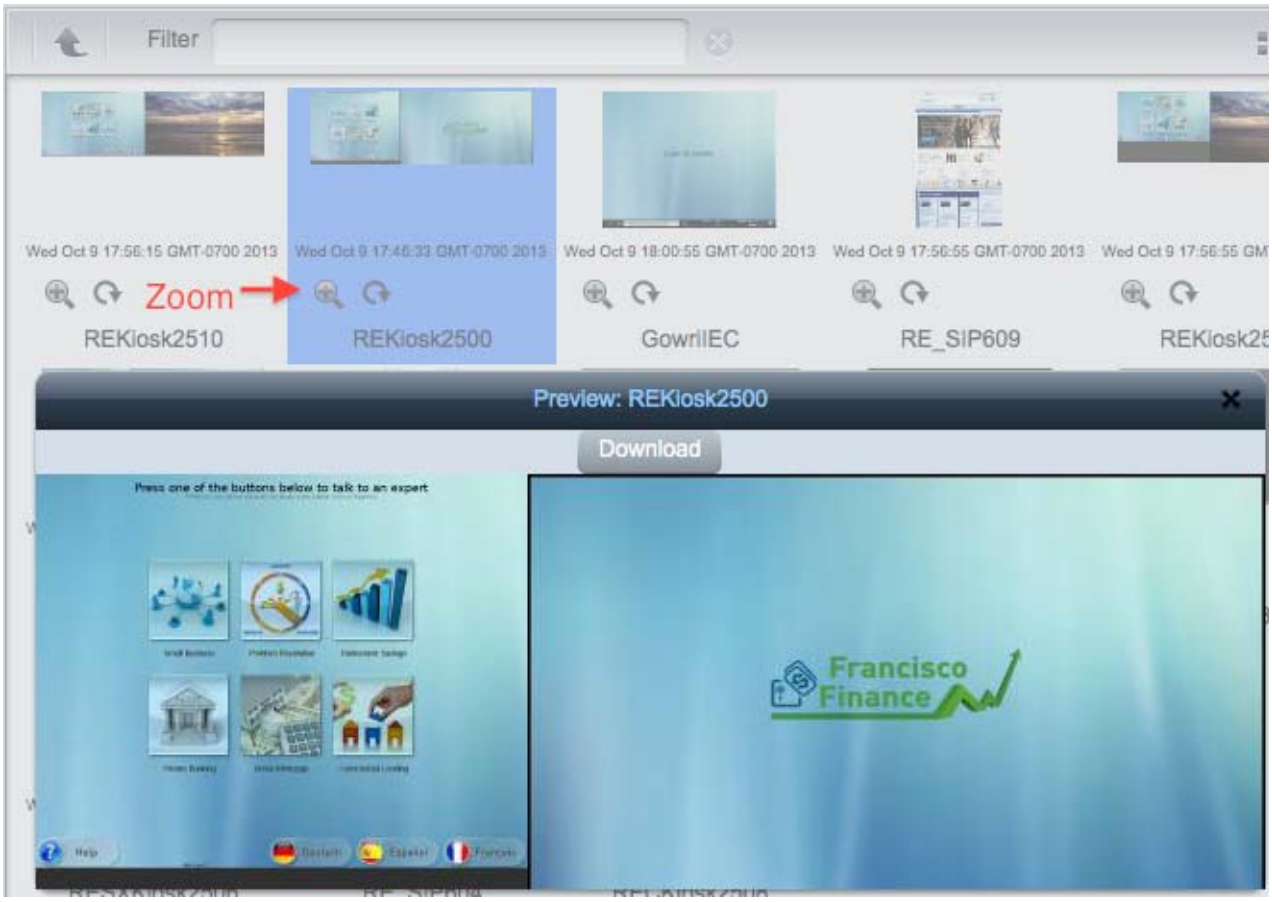


The REIC displays the welcome screen and the dual content TelePresence screen.

Step 5 Default polling time for each IEC image is 10 minutes. The most recent image for the specific IEC can be obtained by clicking the **Refresh** button beneath the IEC's screenshot.

Step 6 In order to enlarge the screenshot of the IEC, click the **Zoom** button beneath the IEC's screenshot.

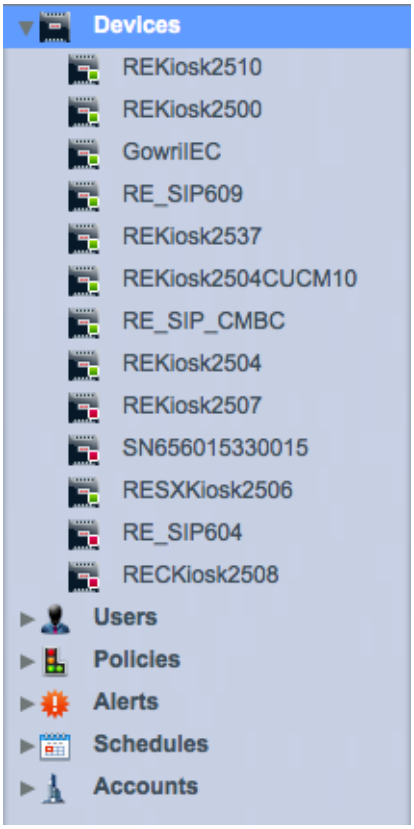
Figure 2-7 Enlarged Screenshot



Now you will check the logs in the IEM.

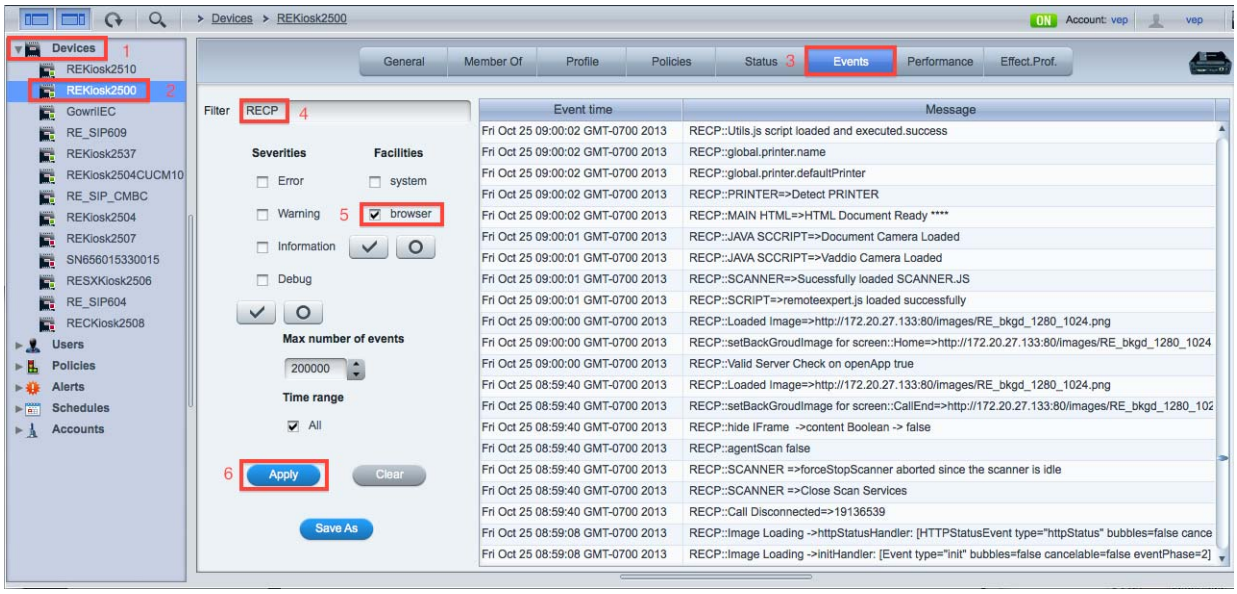
Step 7 In the Devices menu (left pane), choose the IEC by double-clicking on the icon for that particular IEC.

Figure 2-8 Devices Menu



Step 8 Click the **Events** tab.

Figure 2-9 Events Tab



Step 9 You can filter the logs related to REIC by checking the **browser** check box in the Facilities list. Click **Apply**.

Call Related Errors

When call is initiated from REIC, all call flow related information is generated in the database.

The different flows of a call both successful and failed are:

- Call Connect
- Call Hold
- Call Resume
- Call Transfer
- Call Conference
- Call Disconnect

The duration of each event can also be seen in the queries.

All the call related errors for each failed event are listed in the resc.log under the $REM_HOME/resc/logs directory.

The following are examples of how system administrators can search for the errors using Unix commands:

1. The error for a particular event can be extracted from the resc.log located under the $REM_HOME/resc/logs directory. Go to the logs folder within the $REM_HOME directory by executing the command: **`cd $REM_HOME/resc/logs/`**
2. Use the **`grep`** command to find all Call Connect related errors.
3. To search for errors at a specified time, use the command **`vi <log_name>|grep <time>`**. For example, **`cat resc.log|grep 00:53:18`**

Figure 2-10 Errors that Occurred at a Specified Time

```
[root@local1-8temp logs]# vi resc.log| grep 00:53:18
Vim: Warning: Output is not to a terminal
2012-06-15 00:53:18,240 INFO  [http-bio-80-exec-77] com.cisco.big.scheduler.serv
2012-06-15 00:53:18,244 INFO  [http-bio-80-exec-77] com.cisco.big.scheduler.serv
2012-06-15 00:53:18,413 INFO  [http-bio-80-exec-84] com.cisco.big.scheduler.serv
2012-06-15 00:53:18,417 INFO  [http-bio-80-exec-84] com.cisco.big.scheduler.serv
2012-06-15 00:53:18,240 INFO  [http-bio-80-exec-77] com.cisco.big.scheduler.serv
```

4. To search for errors that occurred on a particular device, use the command **`vi <log_name>|grep <device>`** and enter the IEC or TP serial number. For example, **`cat resc.log|grep 656015030030`**

Figure 2-11 Errors that Occurred for a Specific Device

```
[root@local1-8temp logs]# vi resc.log|grep 656015320030
Vim: Warning: Output is not to a terminal
2012-06-15 00:53:18,240 INFO  [http-bio-80-exec-77] com.cisco.big.scheduler.services.NotificationService - Received getKioskNotificationInfo : 65601532
2012-06-15 00:53:21,533 INFO  [http-bio-80-exec-77] com.cisco.big.admin.service.AdminService - Checking for aliveness :656015320030 time:Fri Jun 15 00:
GMT+00:00 2012
2012-06-15 00:53:21,537 INFO  [http-bio-80-exec-77] com.cisco.big.admin.service.AdminService - Kiosk:656015320030 is alive
2012-06-15 00:53:23,274 INFO  [http-bio-80-exec-77] com.cisco.big.scheduler.services.NotificationService - Received getKioskNotificationInfo : 65601532
2012-06-15 00:53:28,275 INFO  [http-bio-80-exec-77] com.cisco.big.scheduler.services.NotificationService - Received getKioskNotificationInfo : 65601532
2012-06-15 00:53:33,280 INFO  [http-bio-80-exec-85] com.cisco.big.scheduler.services.NotificationService - Received getKioskNotificationInfo : 65601532
2012-06-15 00:53:38,318 INFO  [http-bio-80-exec-85] com.cisco.big.scheduler.services.NotificationService - Received getKioskNotificationInfo : 65601532
2012-06-15 00:53:41,572 INFO  [http-bio-80-exec-85] com.cisco.big.admin.service.AdminService - Checking for aliveness :656015320030 time:Fri Jun 15 00:
```

5. To search for call related errors that occurred, use the command **`vi <log_name>|grep <string>`**. to fetch all the lines containing the string “call”. For example, **`cat resc.log|grep -i call`**

Figure 2-12 Call Related Errors

```
[root@big-va log]# cat catalina.out |grep "call"
[INFO] Destroying singletons in org.springframework.beans.factory.support.DefaultListableBeanFactory@1e6f0ef: defining beans [applicationContext,entityManage
rFactory,virtualAgentService,customerService,fileupload,printAndVideoShareService,adminService,cobraWatchDog,reportingService,notificationService,notificati
nManager,scheduleExtractor,ctsReportingAPIExtractorImpl,notReadyStateHandler,callDisconnectEventHandler,eventManager,callService,sessionDAO,customerDAO,kiosk
DAO,expertDAO,schedulerDAO,contentDAO,eventDAO,org.springframework.beans.factory.config.PropertyPlaceholderConfigurer#0,org.springframework.orm.jpa.support.
ersistenceAnnotationBeanPostProcessor#0,dataSource,transactionManager,org.springframework.aop.config.internalAutoProxyCreator,org.springframework.transactio
.annotation.AnnotationTransactionAttributeSource#0,org.springframework.transaction.interceptor.TransactionInterceptor#0,org.springframework.transaction.conf
g.internalTransactionAdvisor,myTxManager,tpCallConnect,cts500CommandFactory,ctsEXCommandFactory,purgeJob,cobraRestartJob,scheduleJob,scheduleSyncJob,purgeTr
gger,schedulerTrigger,ctsTrigger,cobraRestartTrigger,org.springframework.scheduling.quartz.SchedulerFactoryBean#0,calleventhandler]; root of factory hierarc
y
[INFO] Pre-instantiating singletons in org.springframework.beans.factory.support.DefaultListableBeanFactory@1731334: defining beans [applicationContext,enti
yManagerFactory,virtualAgentService,customerService,fileupload,printAndVideoShareService,adminService,cobraWatchDog,reportingService,notificationService,not
ficationManager,scheduleExtractor,ctsReportingAPIExtractorImpl,notReadyStateHandler,callDisconnectEventHandler,eventManager,callService,sessionDAO,customerD
O,kioskDAO,expertDAO,schedulerDAO,contentDAO,eventDAO,org.springframework.beans.factory.config.PropertyPlaceholderConfigurer#0,org.springframework.orm.jpa.s
pport.PersistenceAnnotationBeanPostProcessor#0,dataSource,transactionManager,org.springframework.aop.config.internalAutoProxyCreator,org.springframework.tra
saction.annotation.AnnotationTransactionAttributeSource#0,org.springframework.transaction.interceptor.TransactionInterceptor#0,org.springframework.transacti
n.config.internalTransactionAdvisor,myTxManager,tpCallConnect,cts500CommandFactory,ctsEXCommandFactory,purgeJob,cobraRestartJob,scheduleJob,scheduleSyncJob,
urgeTrigger,schedulerTrigger,ctsTrigger,cobraRestartTrigger,org.springframework.scheduling.quartz.SchedulerFactoryBean#0,calleventhandler]; root of factory
ierarchy
com.cisco.jtapi.InvalidStateExceptionImpl: Did not meet pre-conditions -- call must be ACTIVE and at least one TerminalConnection must be Active
        at com.cisco.big.call.BIGObserver.drop(BIGObserver.java:202)
        at com.cisco.big.call.CallService.createCall(CallService.java:197)
        at com.cisco.big.va.services.VirtualAgentServices.callConnectBySerialNumber(VirtualAgentServices.java:251)
[ERROR] com.cisco.jtapi.InvalidStateExceptionImpl: Did not meet pre-conditions -- call must be ACTIVE and at least one TerminalConnection must be Active
com.cisco.jtapi.InvalidStateExceptionImpl: Did not meet pre-conditions -- call must be ACTIVE and at least one TerminalConnection must be Active
        at com.cisco.big.call.BIGObserver.drop(BIGObserver.java:202)
        at com.cisco.big.call.CallService.createCall(CallService.java:197)
        at com.cisco.big.va.services.VirtualAgentServices.callConnectBySerialNumber(VirtualAgentServices.java:251)
[ERROR] com.cisco.jtapi.InvalidStateExceptionImpl: Did not meet pre-conditions -- call must be ACTIVE and at least one TerminalConnection must be Active
```

JTAPI Issues

Agent Registration When Done From REAC Shows a Red Status

1. Check if the correct CUCM IP and credentials were provided when the REM was setup.
2. For a call connection to work properly, the JTAPI adapter should be configured correctly.
   a. The IP address and TP details should be configured properly to initiate the call.
   b. To receive the call, the agent DN must be configured in REAC. The registration status of the agent DN is available in the Expert tab of REAC. Refer to the *Cisco Remote Expert Manager 1.9.2 Administration Guid*e for instructions on how to configure the agent DN.

If the above parameters are not configured properly then log messages are logged in the resc.log file under $REM_HOME/resc/logs.

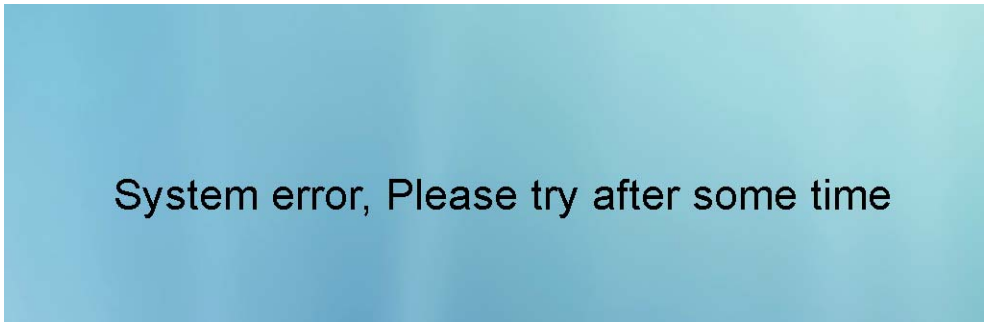
To check if incorrect CUCM IP or credentials have been setup, check for the error in the resc.log. Check the IP address of CUCM in the rem.properties using the TUI. Go to Main Menu > REM Server Administration > Edit REM Properties.

Figure 2-13 Incorrect CUCM IP Address in resc.log

```
        ... 31 more
Caused by: org.springframework.beans.factory.BeanCreationException: Error creating bean with name 'callService' defined in class path resource [applicationC
ntext.xml]: Instantiation of bean failed; nested exception is org.springframework.beans.BeanInstantiationException: Could not instantiate bean class [com.ci
co.big.call.CallService]: Constructor threw exception; nested exception is com.cisco.jtapi.PlatformExceptionImpl: Unable to create provider -- No route to h
st
        at org.springframework.beans.factory.support.AbstractAutowireCapableBeanFactory.instantiateBean(AbstractAutowireCapableBeanFactory.java:965)
        at org.springframework.beans.factory.support.AbstractAutowireCapableBeanFactory.createBeanInstance(AbstractAutowireCapableBeanFactory.java:911)
        at org.springframework.beans.factory.support.AbstractAutowireCapableBeanFactory.doCreateBean(AbstractAutowireCapableBeanFactory.java:485)
        at org.springframework.beans.factory.support.AbstractAutowireCapableBeanFactory.createBean(AbstractAutowireCapableBeanFactory.java:456)
        at org.springframework.beans.factory.support.AbstractBeanFactory$1.getObject(AbstractBeanFactory.java:291)
        at org.springframework.beans.factory.support.DefaultSingletonBeanRegistry.getSingleton(DefaultSingletonBeanRegistry.java:222)
        at org.springframework.beans.factory.support.AbstractBeanFactory.doGetBean(AbstractBeanFactory.java:288)
        at org.springframework.beans.factory.support.AbstractBeanFactory.getBean(AbstractBeanFactory.java:190)
        at org.springframework.beans.factory.support.BeanDefinitionValueResolver.resolveReference(BeanDefinitionValueResolver.java:322)
        ... 46 more
Caused by: org.springframework.beans.BeanInstantiationException: Could not instantiate bean class [com.cisco.big.call.CallService]: Constructor threw except
on; nested exception is com.cisco.jtapi.PlatformExceptionImpl: Unable to create provider -- No route to host
        at org.springframework.beans.BeanUtils.instantiateClass(BeanUtils.java:141)
        at org.springframework.beans.factory.support.[illegible]y.java:74)
        at org.springframework.beans.factory.support.AbstractAutowireCapableBeanFactory.instantiateBean(AbstractAutowireCapableBeanFactory.java:958)
        ... 54 more
```

REIC Displays the Error Message "System error, please try after some time"

Figure 2-14 REIC System Error Message



If the REIC displays the error message "System error, please try after some time", the TP details (TP DN or TP type) in REAC are incorrect. To fix this issue, refer to the *Cisco Remote Expert Manager 1.9.2 Administration Guid*e to configure SSH in REAC.

Customer Pod Displays "Expert not Available" Message

The customer pod displays the "Expert not Available" error message when the video endpoint IP Address is incorrect. As a result, the Virtual Agent Services failed to function properly. To fix this issue, refer to the *Cisco Remote Expert Manager 1.9.2 Administration Guid*e to configure SSH host name in REAC.

Customer Pod Displays "Kiosk phone is out of service" Message

If the customer pod displays the "Kiosk phone is out of service", the video endpoint IP phone terminals are not registered in CUCM.

Figure 2-15 "Kiosk phone is out of service" Message

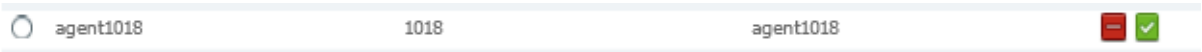
Figure 2-16 IP Phone Terminals Not Registered in CUCM

```
2012-06-21 01:30:24,918 INFO  [http-bio-80-exec-6] com.cisco.big.call.CallService - Time taken to check if Address is in service: 2001
2012-06-21 01:30:24,919 INFO  [http-bio-80-exec-6] com.cisco.big.call.CallService - Is Address in service: false
2012-06-21 01:30:24,919 INFO  [http-bio-80-exec-6] com.cisco.big.call.CallService - Address is not in Service: 1002
2012-06-21 01:30:38,511 INFO  [http-bio-80-exec-23] com.cisco.big.va.services.VirtualAgentServices - Received getKioskDetails unique serialNumber: 6560153200
30
2012-06-21 01:30:38,521 INFO  [http-bio-80-exec-23] com.cisco.big.va.dao.KioskDAO - [com.cisco.big.va.pojo.domain.Locale@380d519a, com.cisco.big.va.pojo.doma
in.Locale@6fc6ce97]
2012-06-21 01:30:38,530 INFO  [http-bio-80-exec-22] com.cisco.big.va.services.VirtualAgentServices - Received getKioskDetails unique serialNumber: 6560153200
```

Expert Registration Issue

The expert registration on one of the nodes or both is shown as red. This occurs when the REM database is not in sync.

Figure 2-17 Expert Registration Showing One Node as Red



To correct this issue, perform database synchronization and re-start Postgres on the node where the expert registration has failed by following these steps:

Step 1 SSH into REM via the TUI.

Step 2 In the Main Menu, select **c) Services Control**.

Step 3 In the Services Control menu, select **c) Database Server**.

Step 4 In the Database Server menu, select **c) Stop Service** and follow the on-screen instructions.

Step 5 In the Database Server menu, select **a) Start Service** and follow the on-screen instructions.

Step 6 Go to REAC and click the **DB Cluster** tab.

Step 7 Choose the DB node and click the **Activate** button.

Rsync Command Failure

An rsync command failure occurs when a RSA fingerprinting issue happens (e.g. it goes out of sync). This occurs during a file transfer when handshaking between the two nodes fail.

```
@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@
@ WARNING: REMOTE HOST IDENTIFICATION HAS CHANGED! @
@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@
IT IS POSSIBLE THAT SOMEONE IS DOING SOMETHING NASTY!
Someone could be eavesdropping on you right now (man-in-the-middle attack)!
```

```
It is also possible that the RSA host key has just been changed.
The fingerprint for the RSA key sent by the remote host is
30:2b:2c:e4:34:7d:3f:88:05:50:09:5b:5e:13:1f:fc.
Please contact your system administrator.
Add correct host key in /root/.ssh/known_hosts to get rid of this message.
Offending key in /root/.ssh/known_hosts:1
RSA host key for 10.76.8.192 has changed and you have requested strict checking.
Host key verification failed.
```

To fix this solution, remove the known host keys from all the other nodes in the REM HA cluster and set up the rsync utility again by following these steps:

Step 1 SSH into REM via the TAC account.

Step 2 Execute the following commands:

```
sudo cp /root/.ssh/known_hosts /root/.ssh/known_hosts.bak
sudo vi /root/.ssh/known_hosts
```

Step 3 In the VI editor, delete all entries.

Step 4 Save the file and exit the VI editor.

REM Node Failure

REM node failure occurs when the sequence of REM node restoration is incorrect:

- Incorrect approach of shutting down the nodes: If Node 1 (Database 1 has outdated data), which is the first node to go down, is started first then followed by the startup of Node 2, the online recovery will sync the data from Database 1 (outdated) to Database 2 (updated). With this sequence, you will lose the updated data which was available in Database 2 though both nodes will have synched up data. No operational issue will be experienced but any change to Node 2 when Node 1 was down is lost.
- Correct approach of shutting down the nodes: The correct approach of shutting down the nodes to ensure no data loss is to first start the database that is the last to go down (Database 2 in this case) since it will have extra data. Once Node 2 is up, then start Node 1.

After both nodes are running, online-recovery (i.e. click the Activate button for the nodes in the DB Cluster tab of REAC) will sync (copy) data from Node 2: Database 2 to Node1: Database 1. This will ensure that both the nodes have updated data and no data is lost.

Communication Failure

Communication failure occurs when the communication between two nodes has failed due to a network issue. In the following text, you can observe the following in the haz.log.

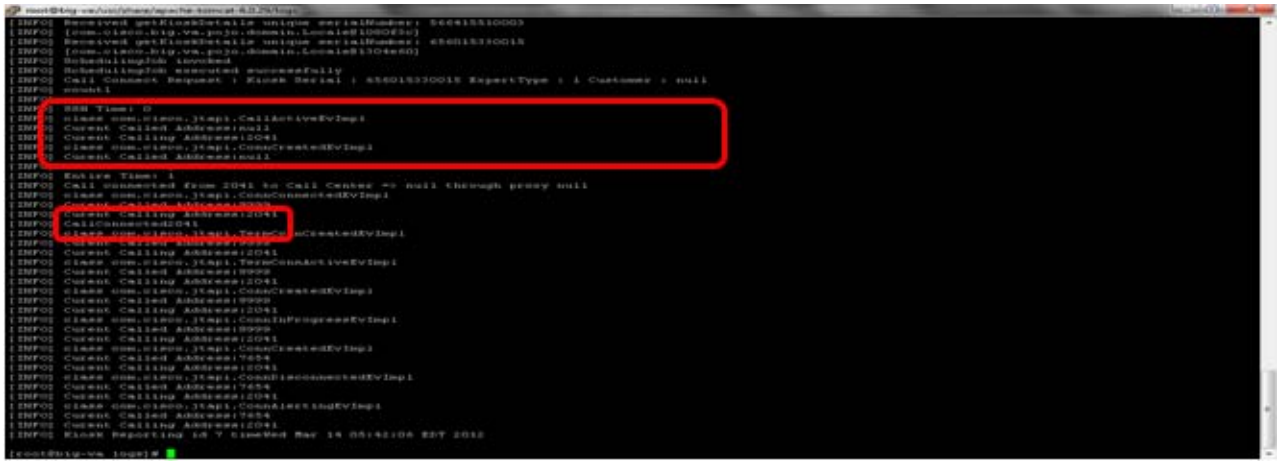
```
2013-02-07 09:38:58,646 INFO  [hz._hzInstance_1_dev.ServiceThread]
com.hazelcast.cluster.ClusterManager - [192.168.2.4]:5701 [dev]
Members [1] {
        Member [192.168.2.4]:5701 this
}
2013-02-07 09:38:58,650 DEBUG [hz._hzInstance_1_dev.ServiceThread]
com.hazelcast.impl.ListenerManager - [192.168.2.4]:5701 [dev] AddListenerOperation
from Address[192.168.2.4]:5701, local=true  key:null op:REMOVE_LISTENER
```

```
2013-02-07 09:38:59,637 DEBUG [hz._hzInstance_1_dev.cached.thread-5]
com.hazelcast.impl.SplitBrainHandler - [192.168.2.4]:5701 [dev] Searching for other
clusters.
2013-02-07 09:38:59,637 DEBUG [hz._hzInstance_1_dev.cached.thread-5]
com.hazelcast.impl.TcpIpJoiner - [192.168.2.4]:5701 [dev] Address[192.168.2.3]:5701 is
local? False
2013-02-07 09:38:59,637 DEBUG [hz._hzInstance_1_dev.cached.thread-5]
com.hazelcast.impl.TcpIpJoiner - [192.168.2.4]:5701 [dev] Address[192.168.2.4]:5701 is
local? true
2013-02-07 09:38:59,637 DEBUG [hz._hzInstance_1_dev.cached.thread-5]
com.hazelcast.impl.TcpIpJoiner - [192.168.2.4]:5701 [dev] Address[192.168.2.4]:5701 is
connecting to Address[192.168.2.3]:5701
2013-02-07 09:38:59,638 DEBUG [hz._hzInstance_1_dev.cached.thread-4]
com.hazelcast.nio.SocketConnector - [192.168.2.4]:5701 [dev] Starting to connect to
Address[192.168.2.3]:5701
2013-02-07 09:38:59,638 DEBUG [hz._hzInstance_1_dev.cached.thread-4]
com.hazelcast.nio.SocketConnector - [192.168.2.4]:5701 [dev] Connecting to
/192.168.2.3:5701, timeout: 0, bind-any: true
2013-02-07 09:38:59,638 DEBUG [hz._hzInstance_1_dev.cached.thread-4]
com.hazelcast.nio.SocketConnector - [192.168.2.4]:5701 [dev] Could not connect to:
/192.168.2.3:5701. Reason: ConnectException[Connection refused]
2013-02-07 09:38:59,638 DEBUG [hz._hzInstance_1_dev.cached.thread-4]
com.hazelcast.nio.SocketConnector - [192.168.2.4]:5701 [dev] Connection refused
java.net.ConnectException: Connection refused
        at sun.nio.ch.Net.connect(Native Method)
        at sun.nio.ch.SocketChannelImpl.connect(Unknown Source)
        at com.hazelcast.nio.SocketConnector.tryToConnect(SocketConnector.java:106)
        at com.hazelcast.nio.SocketConnector.run(SocketConnector.java:55)
        at java.util.concurrent.ThreadPoolExecutor$Worker.runTask(Unknown Source)
```

Call Start

The log in the figure shows that the call starts successfully from the customer.

Figure 2-18 Call Start in the Log



Call Connect

The following log shows that the call from the customer is connected successfully to the agent.

```
2013-02-07 09:36:31,153 INFO
[ObserverThread(com.cisco.big.call.cm.observer.AgentObserver@3cdf672a)]
com.cisco.big.sm.impl.SessionManager - Session Activated :21594114
2013-02-07 09:36:31,153 INFO
[ObserverThread(com.cisco.big.call.cm.observer.AgentObserver@3cdf672a)]
com.cisco.big.call.cm.observer.AgentObserver - 1004Adding GCID :2600
2013-02-07 09:36:31,158 INFO
[ObserverThread(com.cisco.big.call.cm.observer.AgentObserver@3cdf672a)]
com.cisco.big.call.cm.observer.BaseObserver - Lock Acquired
2013-02-07 09:36:31,158 INFO
[ObserverThread(com.cisco.big.call.cm.observer.AgentObserver@3cdf672a)]
com.cisco.big.call.cm.observer.AgentObserver - 1004Session added to Agent and Lock
tried
```

Call Disconnect

The following log shows that the call is disconnected successfully.

```
2013-02-07 09:11:05,996 INFO
[ObserverThread(com.cisco.big.call.cm.observer.AgentObserver@7ab2f62)]
com.cisco.big.call.cm.observer.AgentObserver - 1005 Event : CallObservationEndedEv
2013-02-07 09:11:05,996 INFO
[ObserverThread(com.cisco.big.call.cm.observer.AgentObserver@7ab2f62)]
com.cisco.big.call.cm.observer.AgentObserver - 1005 Call:1036 --> 1005 Call Id :2591
2013-02-07 09:11:05,996 INFO
[ObserverThread(com.cisco.big.call.cm.observer.AgentObserver@7ab2f62)]
com.cisco.big.call.cm.observer.AgentObserver - 1005 Call Key:1036
```

Call Hold and Release from Hold

The following log shows that the call is placed on hold and is released from hold successfully.

```
2013-02-07 09:13:12,037 INFO
[ObserverThread(com.cisco.big.call.cm.observer.AgentObserver@3612afd8)]
com.cisco.big.sm.impl.SessionManager - Session onHoldSession :21594113
2013-02-07 09:13:12,037 INFO
[ObserverThread(com.cisco.big.call.cm.observer.AgentObserver@3612afd8)]
com.cisco.big.call.cm.observer.AgentObserver - Call Put on Hold

2013-02-07 09:14:11,849 INFO
[ObserverThread(com.cisco.big.call.cm.observer.AgentObserver@3612afd8)]
com.cisco.big.sm.impl.SessionManager - Session resumeSession :21594113
2013-02-07 09:14:11,849 INFO
[ObserverThread(com.cisco.big.call.cm.observer.AgentObserver@3612afd8)]
com.cisco.big.call.cm.observer.AgentObserver - 1005Call Put on Talking
```

Call Transfer

The following log shows that the call is transferred successfully.

```
2013-02-07 09:33:41,836 INFO
[ObserverThread(com.cisco.big.call.cm.observer.AgentObserver@75775dde)]
com.cisco.big.call.cm.observer.sequencehandler.CallTransferEventHandler - 1004Transfer
Sequence Handler Event : CallObservationEndedEv
2013-02-07 09:33:41,836 INFO
[ObserverThread(com.cisco.big.call.cm.observer.AgentObserver@75775dde)]
com.cisco.big.call.cm.observer.sequencehandler.CallTransferEventHandler – 1004
```

```
2013-02-07 09:33:41,836 INFO
[ObserverThread(com.cisco.big.call.cm.observer.AgentObserver@75775dde)]
com.cisco.big.call.cm.observer.AgentObserver - --------------- Agent Observer - DN:
1004 --------------------
2013-02-07 09:33:41,836 INFO
[ObserverThread(com.cisco.big.call.cm.observer.AgentObserver@75775dde)]
com.cisco.big.call.cm.observer.AgentObserver - 1004 Event : CiscoTransferEndEv
2013-02-07 09:33:41,836 INFO
[ObserverThread(com.cisco.big.call.cm.observer.AgentObserver@75775dde)]
com.cisco.big.call.cm.observer.AgentObserver - 1004 Call:1036 --> 1005 Call Id :2593
2013-02-07 09:33:41,836 INFO
[ObserverThread(com.cisco.big.call.cm.observer.AgentObserver@75775dde)]
com.cisco.big.call.cm.observer.AgentObserver - 1004Connections :1036 1005
2013-02-07 09:33:41,851 INFO
[ObserverThread(com.cisco.big.call.cm.observer.AgentObserver@75775dde)]
com.cisco.big.call.cm.observer.AgentObserver - 1004 Call Key:1036
2013-02-07 09:33:41,851 INFO
[ObserverThread(com.cisco.big.call.cm.observer.AgentObserver@75775dde)]
com.cisco.big.call.cm.observer.AgentObserver - 1004Sequence Handler exists
2013-02-07 09:33:41,851 INFO
[ObserverThread(com.cisco.big.call.cm.observer.AgentObserver@75775dde)]
com.cisco.big.call.cm.observer.sequencehandler.CallTransferEventHandler -
1004---------------- Transfer Sequence Destruction Handler ----------------
2013-02-07 09:33:41,851 INFO
[ObserverThread(com.cisco.big.call.cm.observer.AgentObserver@75775dde)]
com.cisco.big.call.cm.observer.sequencehandler.CallTransferEventHandler - 1004Detected
Parts: Transfer Dn :1005 Kiosk dn :null
2013-02-07 09:33:41,863 INFO
[ObserverThread(com.cisco.big.call.cm.observer.AgentObserver@75775dde)]
com.cisco.big.call.cm.observer.sequencehandler.CallTransferEventHandler - Kiosk Dn
Assigned
```

Call Conference

The following log shows that the call is successfully added to a conference call.

```
2013-02-07 09:31:01,637 INFO
[ObserverThread(com.cisco.big.call.cm.observer.AgentObserver@75775dde)]
com.cisco.big.call.cm.observer.AgentObserver - --------------- Agent Observer - DN:
1004
2013-02-07 09:31:01,637 INFO
[ObserverThread(com.cisco.big.call.cm.observer.AgentObserver@75775dde)]
com.cisco.big.call.cm.observer.AgentObserver - 1004 Event : CiscoConferenceEndEv
2013-02-07 09:31:01,637 INFO
[ObserverThread(com.cisco.big.call.cm.observer.AgentObserver@75775dde)]
com.cisco.big.call.cm.observer.AgentObserver - 1004 Call:1005 --> Unknown Call Id
:2593
2013-02-07 09:31:01,637 INFO
[ObserverThread(com.cisco.big.call.cm.observer.AgentObserver@75775dde)]
com.cisco.big.call.cm.observer.AgentObserver - 1004Connections :1036 1004 1005
2013-02-07 09:31:01,642 INFO
[ObserverThread(com.cisco.big.call.cm.observer.AgentObserver@75775dde)]
com.cisco.big.call.cm.observer.AgentObserver - 1004 Call Key:null
2013-02-07 09:31:01,642 INFO
[ObserverThread(com.cisco.big.call.cm.observer.AgentObserver@75775dde)]
com.cisco.big.call.cm.observer.AgentObserver - 1004Sequence Handler exists
2013-02-07 09:31:01,642 INFO
[ObserverThread(com.cisco.big.call.cm.observer.AgentObserver@75775dde)]
com.cisco.big.call.cm.observer.sequencehandler.CallConferenceEventHandler -  Received
handleDestructionEvent
```

```
2013-02-07 09:31:01,642 INFO
[ObserverThread(com.cisco.big.call.cm.observer.AgentObserver@75775dde)]
com.cisco.big.call.cm.observer.sequencehandler.CallConferenceEventHandler -
Destroying this handler
2013-02-07 09:31:01,642 INFO
[ObserverThread(com.cisco.big.call.cm.observer.AgentObserver@75775dde)]
com.cisco.big.call.cm.observer.sequencehandler.CallConferenceEventHandler -
1004---------------- Conference Sequence Destruction Handler
2013-02-07 09:31:01,642 INFO
[ObserverThread(com.cisco.big.call.cm.observer.AgentObserver@75775dde)]
com.cisco.big.call.cm.observer.sequencehandler.CallConferenceEventHandler - 1004
Detected Parts: Target DN :1005 Kiosk DN :1036
```

Web Service

The web service correctly loads if the configurations for web service in rem.properties are correct. The contents of rem.properties are the following:

```
$*[REM_VIRTUAL_IP]*= Virtual IP denotes the Cisco ACE Load Balancer Virtual IP. In case of
Single Node provide the same IP as that of $*[RESC_IP]*
$*[RESC_IP]*= Provide the IP address of REM

# For a Call Flow via CCX set the below property to true
$*[IS_CCX]*=True, if the call flow is via UCCX. False, if the call flow is via UCCE

# For a Call Flow via CVP set the below property to true
$*[IS_CVP]*=False,   if the call flow is via UCCX. True, if the call flow is via UCCE

#CUCM Credentials
$*[CUCM_HOST]*= Provide CUCM Host name or IP address.It can have multiple addresses
separated by comma, if you have CUCM HA setup

# ================================- HA Properties -==================================
$*[Total_Nodes_In_Cluster]*=1 if you have single node; 2 if you have REM HA
# REM Server IP & database details
$*[NODE_IP_1]*=same as RESC_IP if it is for a single node; private IP of node 1 if it is
for a HA setup
…
…
$*[NODE_IP_2]*= ignore this one if it is for a single node; private IP of node 2 if it is
for a HA setup
# RSYNC true in clustered setup, false in single node setup
$*[RSYNC_ENABLED]*=false if it is for a single node; true if it is for a REM HA

# REIC Customer logo and background image can be configured using below properties file
$*[REIC_BIG_CUSTOMER_LOGO]*=This is required to customize the kiosk screen. Refer REIC UI
configuration
$*[REIC_SMALL_CUSTOMER_LOGO]*= This is required to customize the kiosk screen. Refer REIC
UI configuration
$*[REIC_BACKGROUND_IMAGE]*= This is required to customize the kiosk screen. Refer REIC UI
configuration
$*[EXPERT_TYPE_WIDTH]*= This is required to customize the kiosk screen. Refer REIC UI
configuration
$*[REIC_SCREEN_MODULE]*=null is for regular RE; keyboard is for keypad support; magstripe
is for card reader
$*[EXTENSION_MOBILITY]*=false is for regular RE; true is for Connected Justice
```

Warning **Providing incorrect REAC credentials will result in a file transfer error.**

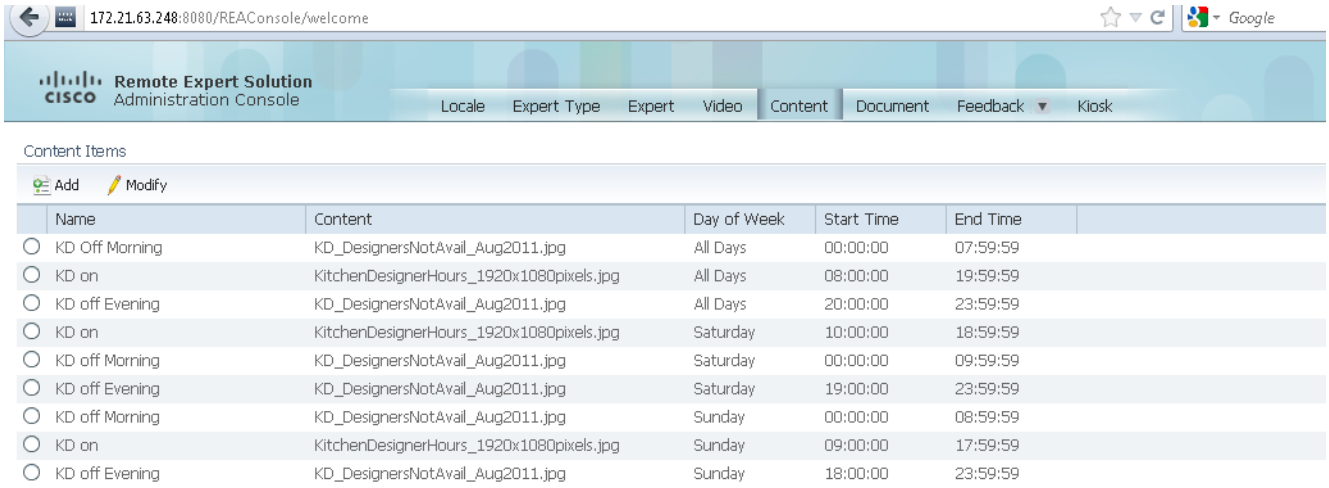
Warning **Providing incorrect CUCM credentials will result in a call connect error due to a JTAPI issue.**

Dual Content Issue

Refer to the "Events Tab in the IEM" section to monitor whether dual content is displaying properly in the secondary screen attached to the IEC. If dual content is not loaded, follow the below steps to troubleshoot the issue.

Step 1 Check if the dual screen image and time are configured properly in the REAC. (Refer to the *Cisco Remote Expert Manager 1.9.2 Administration Guide*.)

Figure 2-19 Content Screen in the REAC



Name	Content	Day of Week	Start Time	End Time
KD Off Morning	KD_DesignersNotAvail_Aug2011.jpg	All Days	00:00:00	07:59:59
KD on	KitchenDesignerHours_1920x1080pixels.jpg	All Days	08:00:00	19:59:59
KD off Evening	KD_DesignersNotAvail_Aug2011.jpg	All Days	20:00:00	23:59:59
KD on	KitchenDesignerHours_1920x1080pixels.jpg	Saturday	10:00:00	18:59:59
KD off Morning	KD_DesignersNotAvail_Aug2011.jpg	Saturday	00:00:00	09:59:59
KD off Evening	KD_DesignersNotAvail_Aug2011.jpg	Saturday	19:00:00	23:59:59
KD off Morning	KD_DesignersNotAvail_Aug2011.jpg	Sunday	00:00:00	08:59:59
KD on	KitchenDesignerHours_1920x1080pixels.jpg	Sunday	09:00:00	17:59:59
KD off Evening	KD_DesignersNotAvail_Aug2011.jpg	Sunday	18:00:00	23:59:59

Step 2 Enter https://<REM_IP>:8443/resc/services/AdminService/getContentByTimeInterval?time=< dd-MM-yyyy HH:mm:ss> in a browser (e.g. https://10.76.8.171:8443/resc/services/AdminService/getContentByTimeInterval?time=22-06-2012 09:52:00).

Step 3 Verify that the status code indicates "SUCCESS".

Figure 2-20 Status Code


```
− <ns:getContentByTimeIntervalResponse>
  − <ns:return xsi:type="ax267:AdminServiceResponse">
      <ax265:errorCode>0</ax265:errorCode>
      <ax265:errorMsg xsi:nil="true"/>
      <ax265:statusCode>SUCCESS</ax265:statusCode>
    − <ax267:contentItems xsi:type="ax269:ContentItemWS">
        <ax269:groupId>1</ax269:groupId>
        <ax269:groupName xsi:nil="true"/>
        <ax269:height>0</ax269:height>
        <ax269:itemName>DUAL CONTENT TEST</ax269:itemName>
        <ax269:value>http://10.76.8.171:80/images//bg_img_1920X1200.jpg</ax269:value>
        <ax269:width>0</ax269:width>
      </ax267:contentItems>
    </ns:return>
  </ns:getContentByTimeIntervalResponse>
```

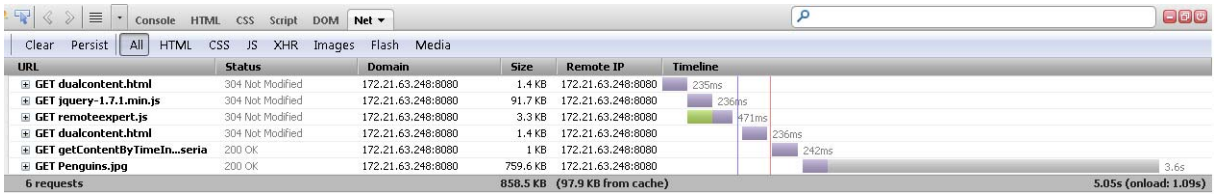

Step 4 Enter https://<REM_IP>:8443/reic/dualcontent.html in the Firefox browser.

Step 5 Check whether the image loads.

Figure 2-21 Image Loaded in the Browser

Note You can use the Firebug tool in Firefox to track the flow in loading the dual content URL.

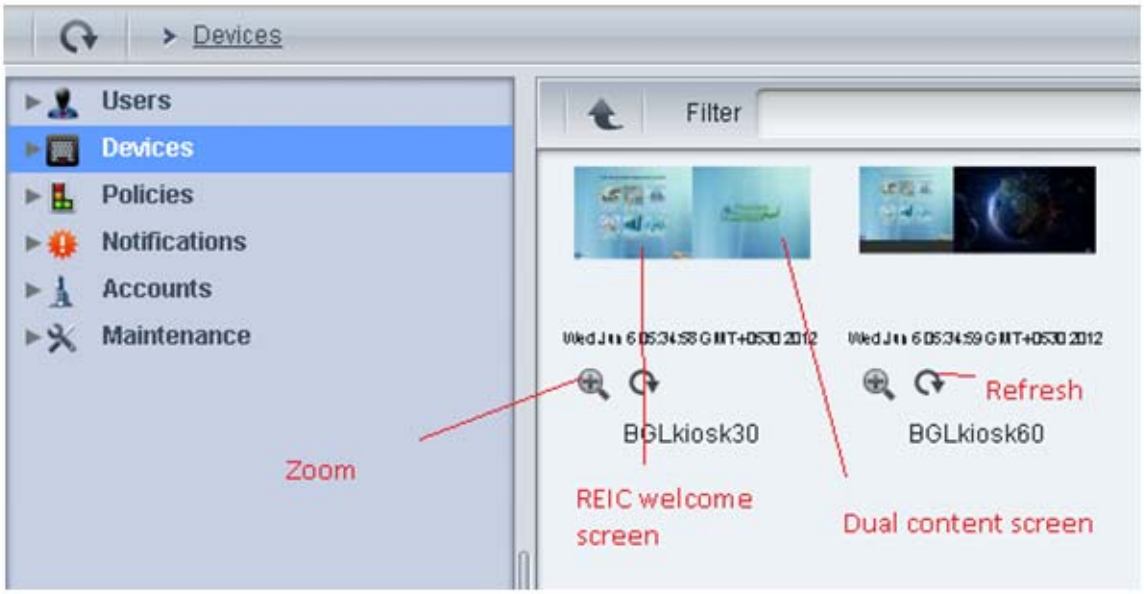
Figure 2-22 Firebug Tool in Firefox



Step 6 If the image loaded in the browser, go to the IEM and choose the IEC in question.

Step 7 Look at the screenshot of the IEC. The REIC application screen and the dual screen image should be displayed in the IEC screenshot pane.

Figure 2-23 Screenshot View of the IEC



Failure of RESC Web (API) Services

Sometimes after the reboot of the REM VM, services provided by the REM Server fail to start due to delay in setting up of the $REM_HOME environment variable path.

In order to circumvent the above problem, perform the following steps after the REM VM server is rebooted:

Step 1 Run the main.sh file from the bash shell using the following command:
`#.$REM_HOME/tools/ias/scripts/main.sh`

Step 2 Check whether all the services are up and running by accessing the list of services provided by the RESC server by navigating to the following URL:
https://<REM_IP>:8443/resc/services/AdminService/getVersionInfo

Step 3 If web services are running properly, then you will see the result show in the figure below.

Figure 2-24 Web Services Result

```
  <?xml version="1.0"?>
- <ns:getVersionInfoResponse xmlns:ns="http://service.admin.big.cisco.com">
      <ns:return>REM-1.8.0-27</ns:return>
  </ns:getVersionInfoResponse>
```

Verifying VM Settings

Installation of a virtual machine is done using the vShpere client. The REM VM setup requires some of the settings to be configured and maintained, such as time zone setup, master configuration setup, NTP and SMTP server configuration, etc. For installation of the VM, refer to the *Cisco Remote Expert Manager 1.9.2 Installation Guide*.

To troubleshoot time-related errors (e.g. dual content is not working or file timestamp mismatch), REM components configuration-related errors, connectivity errors, or mail-related errors, review the following topics.

Master Configuration

The master configuration file contains all the required settings that are required to get the system up and running. At the time of installation of the REM ISO, some basic inputs are required to be configured before the environment could be prepared for the successful execution of the various REM applications (i.e. REIC, RESC, READ, and REAC) and third-party services like Postgres and Tomcat.

All the variables or inputs required are enlisted in the Master template which needs to be populated beforehand or by the administrator at the time of installation. The Master template is located at $REM_HOME/tools/ias/templates/rem.properties. Refer to the *Cisco Remote Expert Manager 1.9.2 Installation Guide*.

NTP

NTP setup is part of the REM ISO installation. NTP synchronizes the clock of the local server with the NTP server. This is required for synchronization of files with timestamps. All NTP-related settings can be found in /etc/ntp.conf.

If you plan to use internal NTP servers, follow the below steps. Otherwise, you may skip this step.

Step 1 Using the TUI, choose **a) System Settings** in the Main Menu.

Step 2 In the System Settings menu, choose **b) Date and Time Settings**.

Step 3 In the Date and Time Settings, choose **a) Setup NTP Source**.

Step 4 A VI window will open. Replace the IPs or hostname of your NTP servers in the following entries. If you only use one or two NTP servers, comment out the unused entries by adding # at the beginning of lines.

```
server 0.rhel.pool.ntp.org
server 1.rhel.pool.ntp.org
server 2.rhel.pool.ntp.org
```

Step 5 Save and exit the VI.

Network Configuration

Step 1 To set up the network, SSH into REM via TUI.

Step 2 In the Main Menu, type **a** to choose the System Settings menu.

Step 3 In the System Settings menu, type **a** to choose Network Settings.

Step 4 In the Network Settings menu, type **a** to choose Setup Network Information.

Step 5 In the Setup Network Information screen, press any key to continue.

Step 6 Configure for either Single Node or REM HA setup.

a. Single Node:

1. Within the Select Action screen, choose **Edit Devices.**
2. Select **eth0** to configure. Press the Enter key.
3. Uncheck the **Use DHCP** check box.
4. Enter the desired IP addresses for the Static IP address, Netmask IP address, and Default gateway IP address fields. Select **Ok**.
5. Choose **Save** and press the Enter key.
6. Choose **Edit DNS Configuration**.
7. Enter the Hostname, Primary DNS, Secondary DNS, Tertiary DNS, and Search fields. Select **Ok**.
8. Select **Save and Quit.**
9. Go back to the Main Menu.
10. To restart network service, select **c) Services Control** in the Main Menu. Then choose **a) Networking** in the Services Control menu. Finally, choose **a) Restart networking** in the Networking menu.

    If network is set up properly, you should see a message similar to “Updating REM DB with IP Address: 172.20.20.20”.

b. REM HA (Dual Node):

1. Choose **Edit Devices.**
2. Select **eth0** to configure. Press the Enter key.
3. Uncheck the **Use DHCP** check box.
4. Enter a public IP address in the Static IP address, Netmask IP address, and Default gateway IP address fields. Select **Ok**.
5. Select **eth1** to configure. Press the Enter key.
6. Uncheck the **Use DHCP** check box.

7. Enter a private IP address (e.g. 192.168.10.100) in the Static IP address field. In the Netmask IP address field, enter **255.255.255.0**. Leave the Default gateway IP address field empty. Select **Ok**.
8. Choose **Save** and press the Enter key.
9. Choose **Edit DNS Configuration** and enter the Hostname. Leave the Primary DNS, Secondary DNS, Tertiary DNS, and Search fields empty. Select **Ok**.

Note Each node should be given a unique hostname.

10. Select **Save and Quit.**
11. Go back to the Main Menu.
12. To restart network service, select **c) Services Control** in the Main Menu. Then choose **a) Networking** in the Services Control menu. Finally, choose **a) Restart networking** in the Networking menu.
13. If network is set up properly, you should see a message similar to "Updating REM DB with IP Address: 172.20.20.20".
14. Repeat substeps 1-13 for the second node.

Step 7 To verify if the network is configured properly:

a. In the Main Menu, type **a** to choose the System Settings menu.
b. In the System Settings menu, type **d** to choose System Information.

You should see something similar to what is shown in the figure below.

Figure 2-25 Network Details

```
-------------------------------------------------------------------------------
                        Network Details
eth0      Link encap:Ethernet  HWaddr 00:50:56:A2:46:77
          inet addr:172.25.26.116  Bcast:172.25.26.255  Mask:255.255.255.0
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:686669 errors:0 dropped:0 overruns:0 frame:0
          TX packets:470537 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:144578430 (137.8 MiB)  TX bytes:442637935 (422.1 MiB)

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          UP LOOPBACK RUNNING  MTU:16436  Metric:1
          RX packets:938151 errors:0 dropped:0 overruns:0 frame:0
          TX packets:938151 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:781337338 (745.1 MiB)  TX bytes:781337338 (745.1 MiB)
```

Note If the IP address needs to be changed later, you may need to follow this section to reconfigure your network.

Effect on Database

First, make sure that you SSH to REM via the TAC account. Execute the below commands on the Shell prompt of REM server to check the REM DB Details:

Step 1 On the Shell prompt of the REM server, execute **/etc/init.d/postgresql-<version> status** to check Postgres status.

Figure 2-26 Check Postgres Status

```
[root@locREM_HA_1 ~]# /etc/init.d/postgresql-9.1 status
 (pid  14576) is running...
```

Step 2 Log into the node where REM DB is running.

Step 3 At the DB prompt of the REM server, execute the following:

[REM1-9]$ sudo su -l postgres

-bash-3.2$ psql postgres

Figure 2-27 REM DB Console

```
[root@locREM_HA_1 ~]# psql -Upostgres -hlocalhost REM_DB;
Password for user postgres:
psql (9.1.5)
Type "help" for help.

REM_DB=#
```

Step 4 Check the list of tables available in REM_DB.

Step 5 At the DB prompt, execute **\d** to list the REM database tables.

Figure 2-28 List REM Database Tables

```
REM_DB=# \d
```

Step 6 To take a database schema backup, enter **pg_dump -Upostgres -hlocalhost --schema-only -f <location/of/backup.sql> REM_DB**.

Figure 2-29 Schema Backup

```
[root@locREM_HA_1 ~]# pg_dump -Upostgres -hlocalhost --schema-only -f /tmp/remdb.sql REM_DB
Password:
```

Step 7 To take a database data backup, enter p**g_dump -Upostgres -hlocalhost --data-only -f <location/of/backup.sql> REM_DB**.

Figure 2-30 Data Backup

```
[root@locREM_HA_1 ~]# pg_dump -Upostgres -hlocalhost --data-only -f /tmp/remdata
Password:
```

Step 8 Restore the schema from the sql file by entering the **psql -Upostgres -hlocalhost -d REM_DB -f <location/of/dumpfile.sql>** command.

Figure 2-31 Restoring the Schema

```
[root@locREM_HA_1 ~]# psql -Upostgres -hlocalhost -d REM_DB -f /tmp/remdb.sql
Password for user postgres:
```

Step 9 Log into the database.

Step 10 Execute the **\i <location/of/backup.sql>** command to restore the data from the sql dump file.

Figure 2-32 Restore Data

```
[root@locREM_HA_1 ~]# psql -Upostgres -hlocalhost REM_DB;
Password for user postgres:
psql (9.1.5)
Type "help" for help.

REM_DB=# \i /tmp/remdata.sql
SET
SET
```

Step 11 Drop the database using the **DB dropdb -Upostgres -hlocalhost REM_DB** command.

Step 12 Create the database using the **createdb -Upostgres -hlocalhost 'REM_DB'** command.

Step 13 Check the list of data available in the table.

Step 14 At the DB prompt, execute **Select * from <table_name>**.

Step 15 To logout from REM database, enter **\q** at the REM_DB prompt.

Figure 2-33 Logout from REM Database

```
REM_DB=# \q
[root@locREM_HA_1 ~]#
```

Document

After adding the document from REAC, the document will be added in the database with creation date (in the doc_table it is called 'added_date'). If time zone is not configured properly, it is very difficult to maintain the database.

Figure 2-34 Documents Table in the Database

id bigint	added_by character varying(255)	added_date timestamp without time zone	category character varying(255)	description text	doc_name character varying(255)	doc_type character varying(255)	doc_url character varying(255)	islocal boolean	ispublic boolean	modified_date timestamp without time
19300	1005	2013-01-29 13:31:44.868			Genesyss.txt	txt	http://10.76.8.83:8	t	f	2013-01-29 13:31:44.
19824	agent1004	2013-01-30 06:23:40.526			test - Copy.txt	txt	http://10.76.8.83:8	t	f	2013-01-30 06:23:40.
20381	agent1031	2013-01-30 08:04:17.006			test - Copy.txt	txt	http://10.76.8.83:8	t	f	2013-01-30 08:04:17.

Call Session

When customer touches an expert type button on the REIC, a call is initiated. This call will come to the remote expert desk. After answering the call, a session has been established. This call session information can be found in the session table of the database.

Figure 2-35 Session Table in the Database

id bigint	estimate_wait_time bigint	session_end bigint	session_start bigint	status integer	customer bigint	expert_type bigint	kiosk bigint	on_hold_vid bigint	schedule bigint	transaction_data text
21594	10	1360232106	13602297868	2		1	19005	19202048		
19529	10	1359526540	13595264522	2		1	19464	19202048		
21692	10	1360312915	13603110217	2		1	19005	19202048		

Note The session information contains the time when the session was generated. This information is generated from RESC. If the time zone is not configured properly, then this call start time will not be correct compared to the local time where the server is located. If that is the case, it is very difficult to inspect the time when the session was generated.

Video

All the videos added by REAC are added into the REM database. The video is added to the database with the time when it was added to the REAC. For maintaining the database time zone, the VM should be configured properly.

Figure 2-36 Videos Table in the Database

id bigint	addedby character varying(255)	category character varying(255)	description text	isonholdvid boolean	thumbnail_name character varying(255)	time timestamp without time zone	vid_name character varying(255)	vid_type character varying(255)	vid_url character varying(255
20742		footbal	footvball	f	http://10.76.8.83:8				http://10.76.8.217
20742		patio	patio	f	http://10.76.8.83:8				rtmp://10.76.8.217
19922		video	video	f	http://10.76.8.83:8				http://10.76.8.217
19202		videol	bvicdoe	t	http://10.76.8.83:8				rtmp://10.76.8.217

REM Events

When a call is initiated from the REIC, all the call related information such as call connect, call on hold, or call disconnect are visible in the database.

Figure 2-37 REM Call Status Table in the Database

id bigint	artifact_id bigint	description character varying(255)	end_time timestamp without time zone	event_type character varying(255)	exception_msg text	kiosk_id bigint	session_id bigint	start_time timestamp without time zone	status character varying(255)
19038		Call Connect Reques	2013-01-29 13:10:37.44	CallConnect	com.cisco.jts	1900544	19070976	2013-01-29 13:10:20.797	Success
19038		Call Connect Reques	2013-01-29 13:13:05.055	CallConnect	com.cisco.jts	1900544	19070977	2013-01-29 13:12:48.515	Success

The start time for each call status is also added to the database. An incorrectly configured time zone affects this time.

Log Files

Time zone affects the generation of log files. Logs are generated with current time and date in the log files. The following figures show the log files for various REM components.

Figure 2-38 Tomcat Catilana Log

```
Loading messages from basepath [/usr/share/apache-tomcat-6.0.29/conf/reaconsole/messages/]
Mar 5, 2012 10:02:07 AM org.springframework.web.servlet.FrameworkServlet initServletBean
INFO: FrameworkServlet 'Spring Servlet': initialization started
Mar 5, 2012 10:02:07 AM org.springframework.context.support.AbstractApplicationContext prepareRefresh
INFO: Refreshing WebApplicationContext for namespace 'Spring Servlet-servlet': startup date [Mon Mar 05 10:02:07 UT
Mar 5, 2012 10:02:07 AM org.springframework.beans.factory.xml.XmlBeanDefinitionReader loadBeanDefinitions
INFO: Loading XML bean definitions from ServletContext resource [/WEB-INF/spring/applicationContext.xml]
Mar 5, 2012 10:02:08 AM org.springframework.beans.factory.xml.XmlBeanDefinitionReader loadBeanDefinitions
INFO: Loading XML bean definitions from ServletContext resource [/WEB-INF/spring/db-config.xml]
Mar 5, 2012 10:02:08 AM org.springframework.core.io.support.PropertiesLoaderSupport loadProperties
INFO: Loading properties file from URL [file:////usr/share/apache-tomcat-6.0.29/conf/reaconsole/config/db_config.pr
Mar 5, 2012 10:02:08 AM org.springframework.beans.factory.support.DefaultListableBeanFactory preInstantiateSingleto
INFO: Pre-instantiating singletons in org.springframework.beans.factory.support.DefaultListableBeanFactory@1384a6a:
Mar 5, 2012 10:02:09 AM org.springframework.orm.hibernate3.LocalSessionFactoryBean buildSessionFactory
INFO: Building new Hibernate SessionFactory
10:02:09 REAdmin Console WARN  com.jolbox.bonecp.BoneCPConfig - Max Connections < 1. Setting to 20
Mar 5, 2012 10:02:10 AM org.springframework.web.servlet.handler.AbstractUrlHandlerMapping registerHandler
INFO: Mapped URL path [/locale/view] onto handler 'localeController'
Mar 5, 2012 10:02:10 AM org.springframework.web.servlet.handler.AbstractUrlHandlerMapping registerHandler
INFO: Mapped URL path [/locale/view.*] onto handler 'localeController'
```

Figure 2-39 REAC Log

```
13:13:58 c.c.r.a.w.RemoteExpertContextListener INFO  - Initializing [Remote Expert Administration Console] context
13:13:58 c.c.r.a.w.RemoteExpertContextListener DEBUG - REACONSOLE_HOME [/usr/share/apache-tomcat-6.0.29/conf/reaconsole]
13:13:58 c.c.r.a.w.RemoteExpertContextListener INFO  - Context [Remote Expert Administration Console] initialized
14:22:52 c.c.r.a.w.RemoteExpertContextListener INFO  - Context [Remote Expert Administration Console] shutting down
14:26:55 c.c.r.a.w.RemoteExpertContextListener INFO  - Initializing [Remote Expert Administration Console] context
14:26:55 c.c.r.a.w.RemoteExpertContextListener DEBUG - REACONSOLE_HOME [/usr/share/apache-tomcat-6.0.29/conf/reaconsole]
14:26:55 c.c.r.a.w.RemoteExpertContextListener INFO  - Context [Remote Expert Administration Console] initialized
07:58:30 c.c.r.a.w.RemoteExpertContextListener INFO  - Context [Remote Expert Administration Console] shutting down
08:08:17 c.c.r.a.w.RemoteExpertContextListener INFO  - Initializing [Remote Expert Administration Console] context
08:08:18 c.c.r.a.w.RemoteExpertContextListener DEBUG - REACONSOLE_HOME [/usr/share/apache-tomcat-6.0.29/conf/reaconsole]
08:08:18 c.c.r.a.w.RemoteExpertContextListener INFO  - Context [Remote Expert Administration Console] initialized
```

Figure 2-40 READ Log

```
2011-12-19 14:40:45,373 INFO  [http-8080-1] com.cisco.re.servlet.REActionServlet - EXIT: ActionServlet.doPost()
2011-12-19 14:40:45,373 INFO  [http-8080-1] com.cisco.re.servlet.REActionServlet - EXIT: REActionServlet.doGet()
2011-12-19 14:41:00,311 INFO  [http-8080-1] com.cisco.re.servlet.REActionServlet - ENTER: REActionServlet.doGet()
2011-12-19 14:41:00,311 INFO  [http-8080-1] com.cisco.re.servlet.REActionServlet - ENTER: REActionServlet.doPost()
2011-12-19 14:41:00,311 INFO  [http-8080-1] com.cisco.re.servlet.REActionServlet - ENTER: ActionServlet.processActionRequest()
2011-12-19 14:41:00,311 INFO  [http-8080-1] com.cisco.re.servlet.REActionServlet - Action :17
2011-12-19 14:41:00,311 INFO  [http-8080-1] com.cisco.re.service.impl.NotificationServiceImpl - getAllNotifications(): invoked
2011-12-19 14:41:00,322 INFO  [http-8080-1] com.cisco.re.service.impl.NotificationServiceImpl - getAllNotifications(): returned
2011-12-19 14:41:00,322 INFO  [http-8080-1] com.cisco.re.servlet.REActionServlet - EXIT: ActionServlet.processActionRequest()
2011-12-19 14:41:00,322 INFO  [http-8080-1] com.cisco.re.servlet.REActionServlet - EXIT: ActionServlet.doPost()
2011-12-19 14:41:00,322 INFO  [http-8080-1] com.cisco.re.servlet.REActionServlet - EXIT: REActionServlet.doGet()
```

Figure 2-41 REM Backup Log

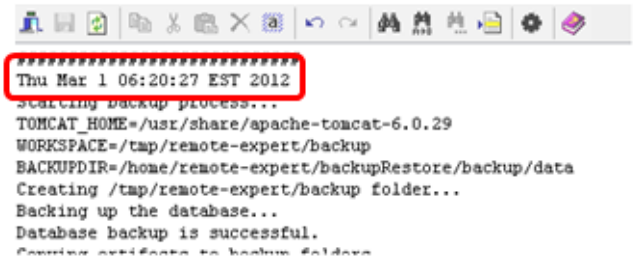
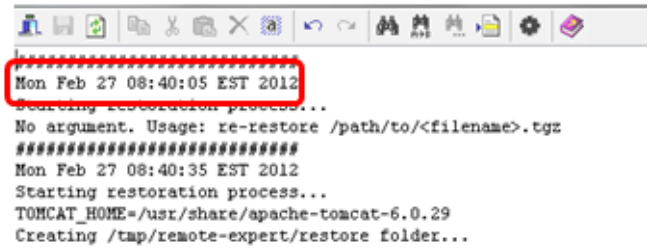


Figure 2-42 REM Restore Log



TUI Troubleshooting Tools

This section explains how to use the Troubleshooting tools in the TUI that is accessed by a SSH client.

Ping

Use the Ping utility to verify that the REM servers are up. This is particularly useful for HA where there are four IP addresses that should be verified.

Step 1 In the Main menu, type **e** to access the Troubleshooting menu.

Figure 2-43 Main Menu

```
-----------------------------------------------------------------

Main Menu

                Please choose one of the following menu options:

                          a) System Settings
                          b) System Accounts
                          c) Services Control
                          d) REM Server Administration
                          e) Troubleshooting
                          X) Exit
```

Step 2 In the Troubleshooting menu, type **a** to ping a host.

Figure 2-44 Troubleshooting Menu

```
-------------------------------------------------------------------------------

Main Menu > Troubleshooting

                Please choose one of the following menu options:

                          a) Ping a host
                          b) Logs
                          c) Generate Diagnostics Archive
                R or < or ,) Return to prior menu
```

Step 3 Enter the IP address of the REM server.

Figure 2-45 Ping

```
-------------------------------------------------------------------------------
                        Ping A Host
                        Enter hostname or IP address to ping or just press <ENTER>
ck to the main menu
Enter hostname (or press <ENTER> to cancel):
```

The host will be pinged and the results are displayed.

Step 4 When finished, press any key to return to the previous menu.

System, RE, and Application Server Logs

There are a number of logs that are generated that can help you with troubleshooting issues.

- System logs: These are basically hardware-related logs including system console messages, authentication and authorization logs, and driver messages.
- Remote Expert logs: The majority of logs that you will use are located in this menu which includes logs for all the REM components (REAC, READ, RESC), IAS tool, and Report Generation tool as well as logs for Backup and Restore.
- Application Server logs: These are the Tomcat and Postgres logs.

Step 1 In the Troubleshooting menu, type **b** to access logs.

Figure 2-46 Troubleshooting Menu

```
--------------------------------------------------------------------------------


Main Menu > Troubleshooting

                Please choose one of the following menu options:

                          a) Ping a host
                          b) Logs
                          c) Generate Diagnostics Archive
                R or < or ,) Return to prior menu

```

Step 2 Choose a log menu: **System**, **Remote Expert**, or **Application Server**.

Figure 2-47 Logs Menu

```
--------------------------------------------------------------------------------


Main Menu > Troubleshooting > Logs

                Please choose one of the following menu options:

                          a) System logs
                          b) Remote Expert Logs
                          c) Remote Expert Application Server Logs
                R or < or ,) Return to prior menu

```

- If you chose the System logs, you will see the menu in the figure below. Type a letter corresponding to the log that you want to view.

Figure 2-48 System Logs Menu

```
--------------------------------------------------------------------------------

Main Menu > Troubleshooting > Logs > System logs

                Please choose one of the following menu options:

                          a) System Console Messages: /var/log/messages
                          b) Authentication/Authorization Logs: /var/log/secure
                          c) Driver Messages: dmesg
                R or < or ,) Return to prior menu
```

- If you chose the Remote Expert logs, you will see the menu shown in the figure below. Type a letter corresponding to the log that you want to view.

Figure 2-49 Remote Expert Logs Menu

```
--------------------------------------------------------------------------------

Main Menu > Troubleshooting > Logs > Remote Expert Logs

                Please choose one of the following menu options:

                          a) RESC Logs: resc.log
                          b) RESC Logs: haz.log
                          c) RESC API Logs: CiscoJtapi.log
                          d) REAC Logs: reac.log
                          e) READ Logs: read.log
                          f) IAS Tool Logs
                          g) Backup Logs
                          h) Backup Schedule Logs
                          i) Restore Logs
                          j) REM DB Upgrade Log
                          k) REM Template Upgrade Log
                          l) REM ISO Upgrade Log
                R or < or ,) Return to prior menu
```

- If you chose the Application Server logs, you will see the menu shown in the figure below. Type a letter corresponding to the log that you want to view.

Figure 2-50 Remote Expert Application Server Logs Menu

```
--------------------------------------------------------------------------------

Main Menu > Troubleshooting > Logs > Remote Expert Application Server Logs

                Please choose one of the following menu options:

                         a) Catalina Startup Log: catalina.out
                         b) Catalina Error Log: catalina.err
                         c) Catalina Log: catalina.2014-06-05.log
                         d) Host Manager Log: host-manager.2014-06-05.log
                         e) Manager Log: manager.2014-06-05.log
                         f) Localhost Log: localhost.2014-06-05.log
                         g) Localhost Access Log: localhost_access.2014-06-05.log
                R or < or ,) Return to prior menu
```

Note For security reasons, the TUI will disconnect after three minutes of no activity on the part of the administrator. If the administrator wants to view log activity for more than three minutes, the administrator needs to interact with the TUI in some way such as press the Enter key in order to keep a connection.

Step 3 Press **ESC :q!** to stop watching a log.

Step 4 When finished, press the **R**, **<**, or **,** key to return to the previous menu.

Troubleshooting Tools in REAC

The Download Logs tab in REAC contains lists of logs that can be used for troubleshooting issues:

1. Admin Console: Contains the reac.log from this REAC
2. Agent Desktop: Contains the read.log from READ
3. Session Manager: Contains the resc.log from the RESC
4. RE Events: Capture RE events during a specified time
5. Tomcat: Contains the catalina log for the Tomcat service

Refer to the “Downloading Logs” section of the *Cisco Remote Expert Manager 1.9.2 Administration Guide* for instructions on how to download those logs.

Backup and Restore

Backup and Restore Overview

The backup tool automatically takes a backup of various REM assets such as IAS templates (for all REM component configurations), videos, images, documents and the database from the primary REM server at a scheduled time and stores the backup archive in a secondary REM server or remote FTP/SFTP location.

The restore tool is used to restore the REM server to the last working state using the backup archive in case the REM server goes down.

Any Linux-based system can be used for the backup and restore server.

Note The SSH port (22) must be open.

Single and Dual Node Backups

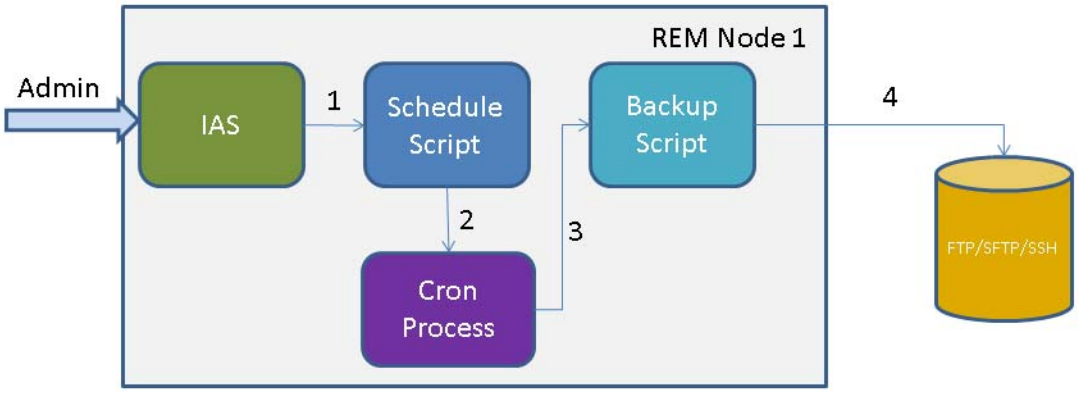
In this section are high level block diagrams for the backups of single node and dual node REM servers.

Single Node Backup

The figure below shows the steps for a single node backup. It assumes that the administrator has logged into REM and accessed the IAS tool and Tomcat, PostgreSQL and SSH are running on the REM server. The backup is taken from the REM node and stored in the remote FTP/SFTP/SSH server.

1. The IAS tool triggers schedule script located in the Backup utility.
2. The schedule script adds job scheduling parameters related to the backup and starts the Cron process.
3. The Cron process executes the backup script at the configured interval.
4. The backup script backs up the data and sends the backup archive to a remote FTP/SFTP server or a remote SSH server (Linux machine).

Figure 2-51 Single Node Backup

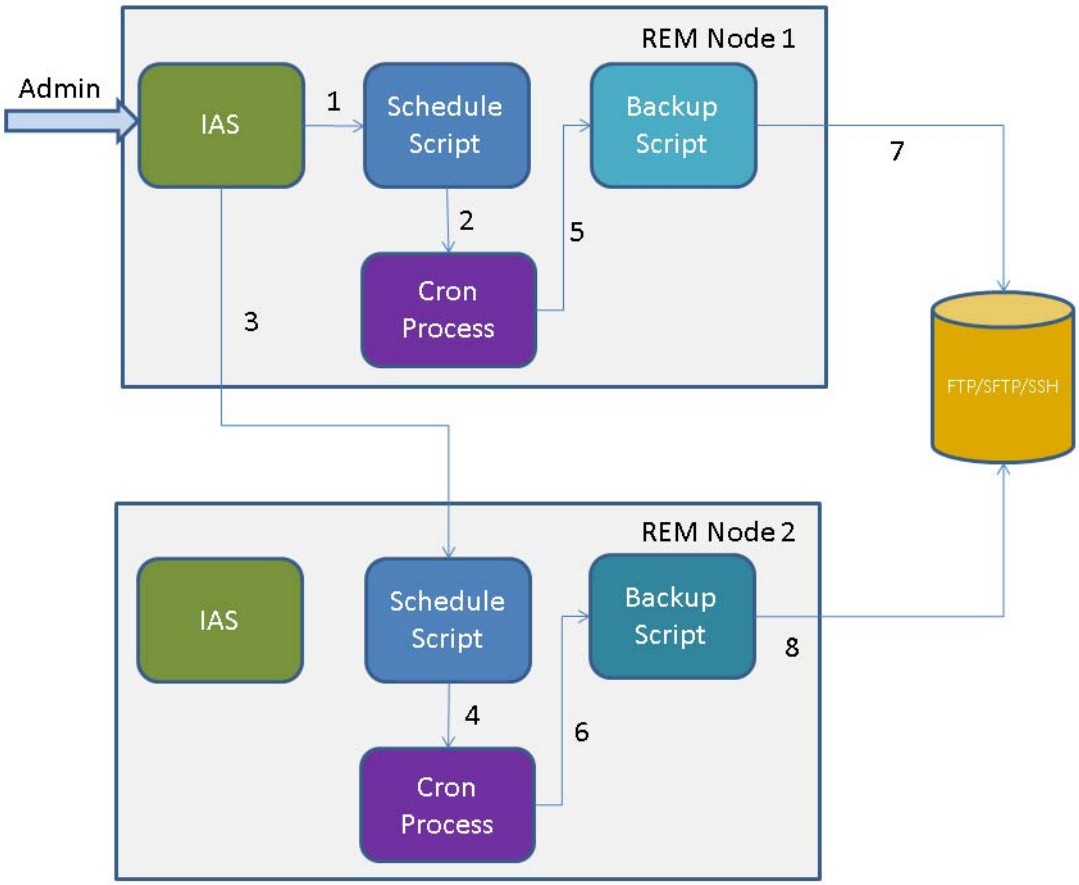


Dual Node Backup

The figure below shows the steps for a dual node backup. It assumes that the administrator has logged into REM and accessed the IAS tool and Tomcat, PostgreSQL and SSH are running on both REM servers. The backup files are created from both REM nodes and stored in the remote FTP/SFTP/SSH server.

1. The IAS tool triggers the schedule script located in the Backup utility in the primary REM server.
2. The schedule script adds job scheduling parameters related to the backup and starts the Cron process in the primary server.
3. The IAS tool triggers the schedule script located in the Backup utility in the secondary server.
4. The schedule script adds job scheduling parameters related to the backup and starts the Cron process in the secondary server.
5. The Cron process executes the backup script at the configured interval in the primary server.
6. The Cron process executes the backup script at the configured interval in the secondary server.
7. The backup script backs up the data from the primary server and sends the backup archive to a remote FTP/SFTP server or a remote SSH server (Linux machine).
8. The backup script backs up the data from the secondary server and sends the backup archive to a remote FTP/SFTP server or a remote SSH server (Linux machine).

Figure 2-52 Dual Node Backup



Different Scenarios in Backup and Restore Processes

Back Up Process

Following are the different scenarios incorporated in the backup process:

1. PostgreSQL service status: The backup process checks whether the PostgreSQL service is running. If it is not running then the PostgreSQL service is started automatically. This check is mandatory to create the PostgreSQL database backup.
2. Log file existence: Log files are used to track the backup process. When executing the backup process, it checks if there are log files in the log directory. If there are no log files, then it is assumed that the backup process is executing for the first time and it creates the log file in the specified directory.
3. Artifacts existence: Artifacts are the different REM components such as template files for configurations, images, videos, etc. If any of the artifacts to be backed up are missing in the primary REM server, then the backup process logs error messages in the log file and continues.
4. Remote copying: If there is an error in storing backup archive remotely, then the backup process logs errors with appropriate error messages in the log file.

5. Backup archive rotation: The backup archive rotation is done in the remote storage server to keep the most recent backup archives. In case an error occurs in backup file rotation, (for details refer to the "Log File Rotation" section of this chapter) the backup process logs errors in the backup log file.

If email notification is enabled for backup and restore, an email notification is sent to the system administrator regarding the last backup status. In case of an error in the last backup, an email is sent with appropriate error messages so that system administrator can debug the issue to find the root cause.

For details on different error messages used in the tool refer to the "Error Messages" section of this chapter.

Note If there is a problem in the database backup, the backup process terminates. After creation of the entire backup, the backup process creates an archive with the .tgz extension. If there is a failure in creating a backup archive, the backup process is terminated instantly. Restoration activity cannot be performed in this case.

Restore Process

Following are the different scenarios incorporated in the restore process:

1. PostgreSQL service status: The restore process checks whether the PostgreSQL service is running in the REM server. If it is not running, then the PostgreSQL service is started automatically. This check is mandatory to restore the database.
2. Tomcat service status: During the restoration of artifacts, the restore process checks whether the Tomcat service is running. If it is running, then it stops the service. This check is required because the Tomcat service may use some configuration files of REM components at the same time that the restore process is overwriting them.
3. Directory structure: If there is something wrong in the directory structure of the artifacts path during restoration of artifacts, then the restore process logs errors in a log file located in the log directory.
4. Database restoration: If there is an error in the database restoration, then the restore process logs that error in the log file.

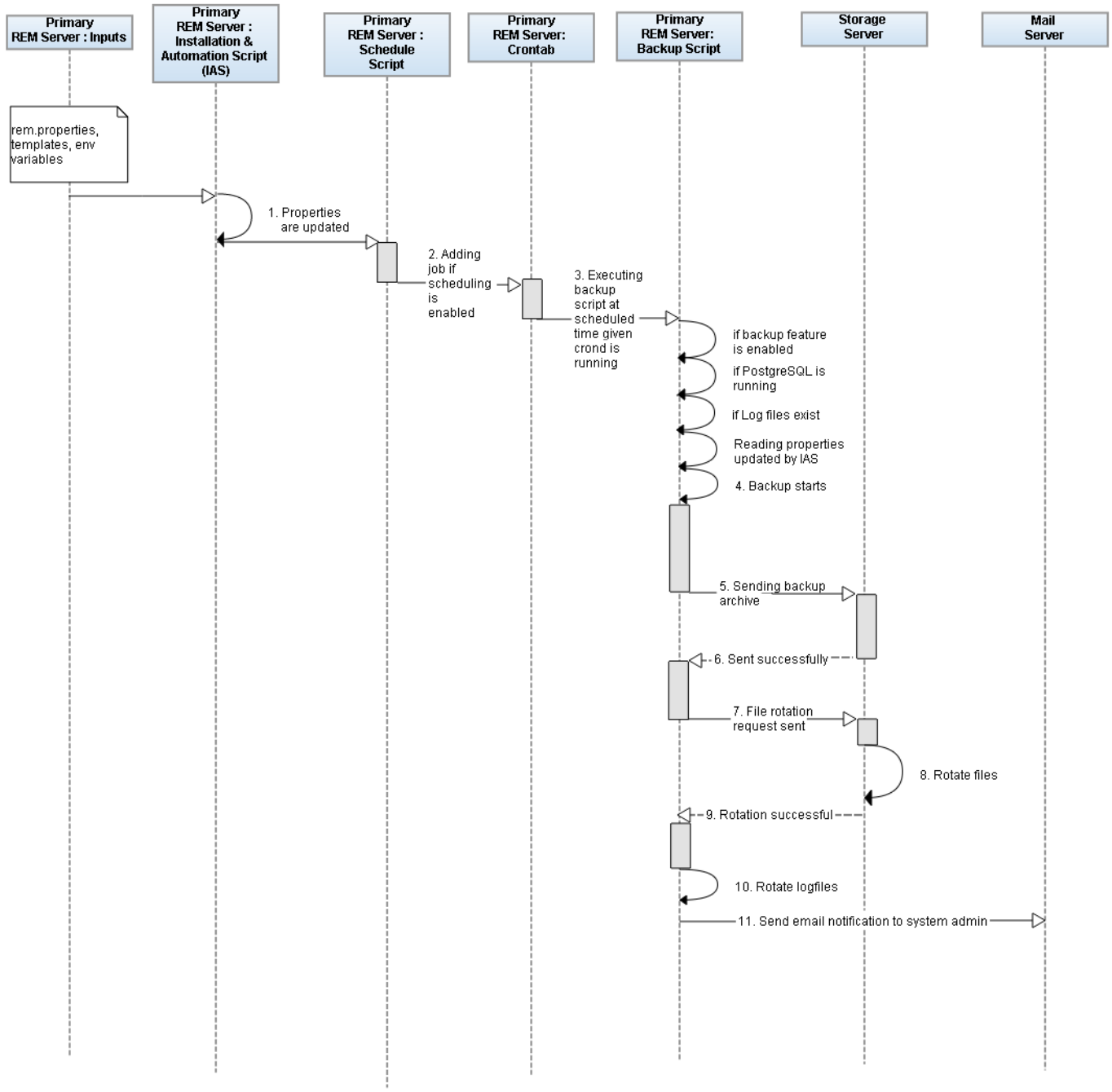
Note The restore process continues to restore the REM server irrespective of failure of one of the artifacts restoration. Restoration terminates if there is failure in restoring the database since the REM does not work with an invalid database. After restoration, the Tomcat service is started automatically by the restore script.

Sequence Diagrams

In this section are sequence diagrams for backup and restore processes.

Backup Sequence Diagram

Figure 2-53 Backup Sequence Diagram



The above sequence diagram includes the update of the properties file by the REM configurator and automatic backup script execution. Before doing the backup, all the properties files used by the backup script must be updated by the IAS (Installation and Automation Script) tool. Backup scheduling is done using Crontab, an utility to schedule jobs in UNIX-like operating systems. In the backup process, the

backup archive is generated in the primary REM server and the archive is sent to the secondary REM server or a FTP/SFTP server (storage server). After storing the backup archive, another script is invoked in the secondary server by the backup script for backup archive rotation. This is required to keep the last modified backup archives in the storage server.

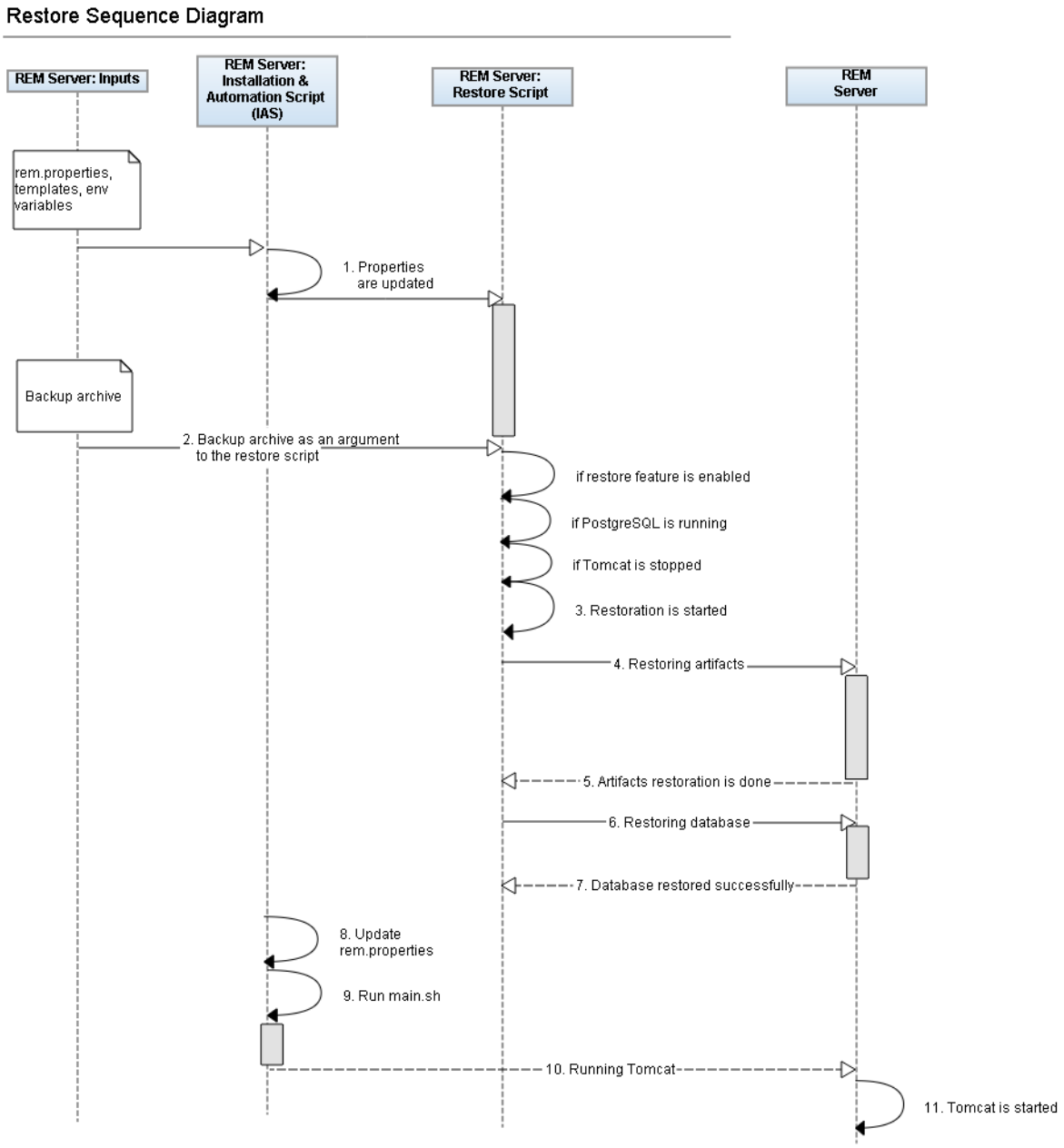
After each backup process, an email notification is sent to the system administrator containing information about the last backup. If the last backup is successful, a success message is sent to the system administrator. If the last backup is not successful, appropriate error messages are sent to the system administrator.

The flows in the above sequence diagram are:

1. The IAS tool reads rem.properties, templates and environment (env) variables and updates the configuration files for the backup process by executing 'main.sh'.
2. The script for scheduling backup (discussed in the "Scheduling" section of this chapter) is invoked in the primary REM server by the system administrator. It adds the job parameters for automatic backup in Crontab if scheduling is enabled by the REM configurator.
3. Executing the backup script at the configured time interval using Crontab if the Crond process, a daemon process for scheduling used by Crontab, is running in the REM server.
4. Before backing up the data in the primary REM server, the backup script checks and validates the pre-conditions. The backup starts if the backup feature is enabled by the REM configurator and the PostgreSQL service is running.
5. After creating the backup archive, the script sends the backup archive to a REM server or a remote FTP/SFTP server (storage server).
6. The remote server sends an acknowledgement to the primary REM server that the archive was sent successfully.
7. A request for file rotation is sent to the storage server.
8. Backup archives files are rotated in the storage server.
9. The storage server sends an acknowledgement to the primary REM server that file rotation was successful.
10. Log files in the primary server are rotated after each backup process.
11. Backup script sends an email notification after each backup process with appropriate messages to the system administrator.

Restore Sequence Diagram

Figure 2-54 Restore Sequence Diagram



If the REM server goes down, the restoration process uses the backup archive located in the storage server to restore the REM server.

In the above sequence diagram, the different flows are:

1. The IAS tool reads rem.properties, templates and environment (env) variable and updates the configurations file for the restore process.

2. The restore script takes the backup archive name with its full path (e.g., $REM_HOME/tools/backup/data/rem_Aug-29-2012_02-13-32_10.76.8.178.tgz) as an argument.
3. The restore script checks the pre-conditions. The restoration starts if the restore feature is enabled by the REM configurator, PostgreSQL is running, and the Tomcat service has stopped.
4. All the REM artifacts are restored to the proper location in the REM server.
5. REM server acknowledges the script that artifacts restoration is done. If an error in artifacts restoration occurs, appropriate error messages are displayed on the console.
6. The script restores the PostgreSQL database in the REM node.
7. The REM node acknowledges that the database was restored successfully.
8. The rem.propeties (master template) is updated.
9. The command `main.sh` is executed in the IAS tool is executed.
10. The IAS tool starts Tomcat in the REM node.
11. Tomcat service is started in the REM server.

Artifacts

The following is terminology used for artifacts:

- REM_HOME = Base installation folder path containing necessary configuration setting for REM application (e.g., REM_HOME = /var/rem)
- tomcat_home = Absolute path of apache tomcat (e.g., tomcat_home = /opt/apache-tomcat-6.0.29)

The backup archive contains the following list of artifacts:

1. REM database
2. REIC assets that contain Wait videos for REIC located under <tomcat_home>/webapps/reic/assets
3. Locale properties for REIC located under <tomcat_home>/webapps/reic/resources
4. Images for the REIC application located under <tomcat_home>/webapps/images
5. Properties related to Connected Justice (CJ) located under <REM_HOME>/cj/conf/segments
6. Template configuration files for REIC located under <REM_HOME>/tools/ias/templates/reic
7. Template configuration files for RESC located under <REM_HOME>/tools/ias/templates/resc
8. Template configuration files for REAC located under <REM_HOME>/tools/ias/templates/reac
9. Template configuration files for READ located under <REM_HOME>/tools/ias/templates/read
10. Template configuration files for CJ located under <REM_HOME>/tools/ias/templates/cj
11. Master template for REM (<REM_HOME>/tools/ias/templates/rem.properties)
12. All the documents which are shared with customers located under <tomcat_home>/webapps/docstore

Location of Backup and Restore Tools

Scripts

The following scripts for the backup process are located under $REM_HOME/tools/backup/scripts/:

- backup (main script for backup)
- schedule (for scheduling backup)
- logrotation (for log file rotation)

The script for the restore process is located under $REM_HOME/tools/restore/scripts/:

- restore (main script for restore)

Properties File

The backup process uses the following properties file located under $REM_HOME/tools/backup/conf/:

- backup.properties
- schedule.properties
- logrotate.properties

The restore process uses the following property file located under $REM_HOME/tools/restore/conf/:

- restore.properties

Log Files

System administrators can use the log files to track previous processes - both backup or restore.

The backup.log file is generated under $REM_HOME/tools/backup/logs/ during the backup process. The restore.log file is generated under $REM_HOME/tools/restore/logs/ during the restore process.

Third Party Libraries

All the third party libraries for the backup process are located under $REM_HOME/tools/backup/lib. There are no third-party libraries used by the restore process.

Binaries

The binaries (rem-backup.jar) for the backup process are located under $REM_HOME/tools/backup/dist. There are no binaries for the restore process.

Pre-Conditions for Restoration

Restoration can be done in either a single node or a dual node setup.

Single Node Setup

The following are the minimum set of requirements for restoration to be done successfully for a single node setup:

- The node should have all the REM components (REAC, READ, RESC and REIC) and IEP Licensing service deployed
- Database schema

Dual Node Setup

The following are the minimum set of requirements for restoration to be done successfully for a dual node setup:

- Primary and secondary REM servers should be synchronized by time zone
- Both REM servers should have the same REM components (REAC, READ, RESC and REIC) and IEP Licensing service deployed
- Both servers should have the same database schema
- All the artifacts path should be same in both machines

Enabling or Disabling Backup and Restore Tool

The backup and restore tool can be enabled or disabled by the REM configurator (IAS tool) during installation of the REM ISO. The flag which is used for enabling or disabling is located under the following properties and updated by the IAS tool during REM ISO installation:

- backup.properties
- logrotate.properties
- restore.properties

In the rem.properties file, set the flag to **True** to enable the feature or **False** to disable the feature. The flag is the FEATURE_ENABLE property:

```
#To enable backup and restore for this release make it ‘True' and
make it 'False' to disable this feature
$*[FEATURE_ENABLE]*=
```

Execute Scripts

This section explains the procedure to back up the various artifacts (database, template configuration files, assets and images) from the REM servers and then restore the REM servers.

Creating the Backup

All properties related to the backup process must be configured in the rem.properties file during REM ISO installation. For details on how to update rem.properties and create properties file for backup refer to IAS documentation.

In the steps below, you will update the properties used for backup. These must be updated before executing the IAS tool.

Step 1 Configure the rem.properties file. All properties related to backup process are typically configured in the rem.properties file during REM ISO installation but they can be modified later.

a. Open the rem.properties file.

b. To enable backup and restore, change the FEATURE_ENABLE property to **true**.

c. In the ARCHIVE_IDENTIFIER property, enter the IP address or hostname of the server from where the file will be backed up. This value will be appended to the backup file name so its origins can be easily identified by the administrator. In the figure below, the backup file name is indicated in red. The name contains “rem”, the system-generated date (Oct-17-2013) and time (15-51-31) of the backup, and the IP address of the server (172.25.26.116) from where the backup was taken.

Figure 2-55 Example of REM Backup File Name

```
[root@REM190-5-v3 ~]# cd /home/admin/
[root@REM190-5-v3 ~]# ls
old  rem_Oct-17-2013_15-51-31_172.25.26.116.tgz
[root@REM190-5-v3 ~]#
```

Note Do not modify the BACKUPDIR property. It is used for Cisco internal testing purposes only.

d. SSH is the only mode currently supported so enter **ssh** for the MODE property.

e. In the SERVER_ADDRESS property, enter the IP address of the remote archiving server where the backup file will be sent.

f. For the SERVER_BACKUP_PATH property, enter the path as to where the backup files should be stored on the remote archiving server.

Figure 2-56 Backup and Restore Properties

```
# ------------------------------------- Backup Restore Properties --------------------------
#To enable backup and restore for this release make it 'true' or make it 'false' to disable t
is feature
$*[FEATURE_ENABLE]*=true

#The name appended to the backup archive created.
#It should contain information regarding the backup server. E.g., name can be ip address of t
ckup server or hostname.
#This property is used to track the backup archive source server
$*[ARCHIVE_IDENTIFIER]*=172.25.26.142

#Backup archive location in storage server
$*[BACKUPDIR]*=/var/rem/tools/backup/data

#Backup related properties
#Backup mode. Use "ftp" to store backup archive in a remote FTP server or "ssh" to store in t
H server
$*[MODE]*=ssh

#Server credentials
$*[SERVER_ADDRESS]*=10.76.8.179
$*[SERVER_USERNAME]*=OAAFYjESfENtIh3kFntUrg==
$*[SERVER_PASSWORD]*=t/JMJWuQX+i1J7IxvIpGzEm1eNO1qgHa

#Full path to location on remote server where backups will be stored
$*[SERVER_BACKUP_PATH]*=/home/cisco/backup

#No of backup archives to be stored in storage server (FTP or SSH)
$*[NO_BACKUP_FILES]*=1

#Database name
-- INSERT --                                                          128,1          72
```

g. Configure the frequency of backups by entering the time and day that the backup should occur. This will create a Cron job inside the system.

   You can modify the backup frequency by changing the values of the property.

   The default is everyday at 6:30 p.m. which is configured as follows:

   - MIN=**30**
   - HOUR=**18**
   - DAY=*
   - MONTH=*
   - WEEKDAY=*

   Note For job scheduling, an asterisk (*) can be used to indicate that every instance (i.e. every hour, every weekday, etc.) of the particular time period will be used.

   If you want to backup on the 15th of every month instead, for example, enter **15** for the DAY property. If you want to backup on Fridays only, enter **5** for the WEEKDAY property.

Figure 2-57 Frequency of Backups

```
#The values can not be blank. User can enter multiple values seperated by commas.
#E.g, 30 18 * * *  (each day at 6:30 PM)
#* * * * * (every min)
#0 0 1,5,10 * * (midnight on 1st,5th & 10th of month)
#*/2 * * * * (Every 2 min)

#Configure min (between 0-59)
$*[MIN]*=30

#Configure hour (between 0-23, 0=midnight)
$*[HOUR]*=18

#Configure day (between 1-31)
$*[DAY]*=*

#Configure month (between 1-12)
$*[MONTH]*=*

#Configure day of week (0-6, 0=Sunday)
$*[WEEKDAY]*=*
```

h. If you want e-mail alerts for status of backups, change the MAIL_ENABLED property to **true** and then populate the SMTP server name, sender's mail ID, and recipients mail ID.

Figure 2-58 Mail Alert

```
#Mail alert related properties
#Enable mail alert
$*[MAIL_ENABLED]*=true

#SMTP server name
$*[SMTP]*=outbound.cisco.com

#Senders mail id
$*[FROM]*=rem_admin@cisco.com

#Recipients mail id
$*[TO]*=rem@cisco.com

#Google API License Key
$*[GOOGLE_KEY]*=AIzaSyChKRrMUqKo6u2dUO2eXG1xZ91rJp3v6fo
-- INSERT --
```

i. After you make all the changes to the rem.properties file, you need to save it by pressing **SHIFT :** and then entering **wq**.

j. Follow the instructions in the "Execute IAS" section of the *Cisco Remote Expert Manager 1.9.2 Installation Guide* to run the configuration tool and encrypt the passwords.

Step 2 Configure the backup.properties file:

a. Navigate to the backup.properties file by using the following commands:

```
#cd $REM_HOME/tools/ias/templates/backup
#vi backup.properties.template
```

b. Configure the following properties:

Note Replace the brackets with the actual values. For example, replace <path to the temp location where backup folder was created> with /tmp/rem/backup.

- tomcat_home= <path to the installation of Tomcat server>
- workspace= <path to the temp location where backup folder was created>
- backupdir= <backup archive location in storage server>
- succsub=**Backup was successful!**
- failsub= **Backup has failed!**

```
#Absolute path to the installation of Tomcat server
tomcat_home=

# Absolute path to the temp location where backup folder are created
workspace=
#(E.g., /tmp/rem/backup)
#Backup archive location in storage server
backupdir=
#(E.g., /var/rem/tools/backup/data)
```

```
#Configure the subject of the mail message in case backup is
successful (must be quoted if it contains spaces)
succsub=

#Configure the subject of the mail message in case backup is
unsuccessful (must be quoted if it contains spaces)
failsub=
```

c. Save the file.

Step 3 Update the logrotate.properties file for file rotation:

a. Open the logrotate.properties file located under $REM_HOME/tools/backup/conf/.

b. Configure the properties in the file with the following values:

- feature_enable=**True**
- rotate=**2**
- size=**4k**

c. Save the file.

d. Execute the logrotation script located under $REM_HOME/tools/backup/scripts/ for adding parameters to /etc/logrotate.conf (in UNIX) for log file rotation by entering the command: **`./logrotation`**

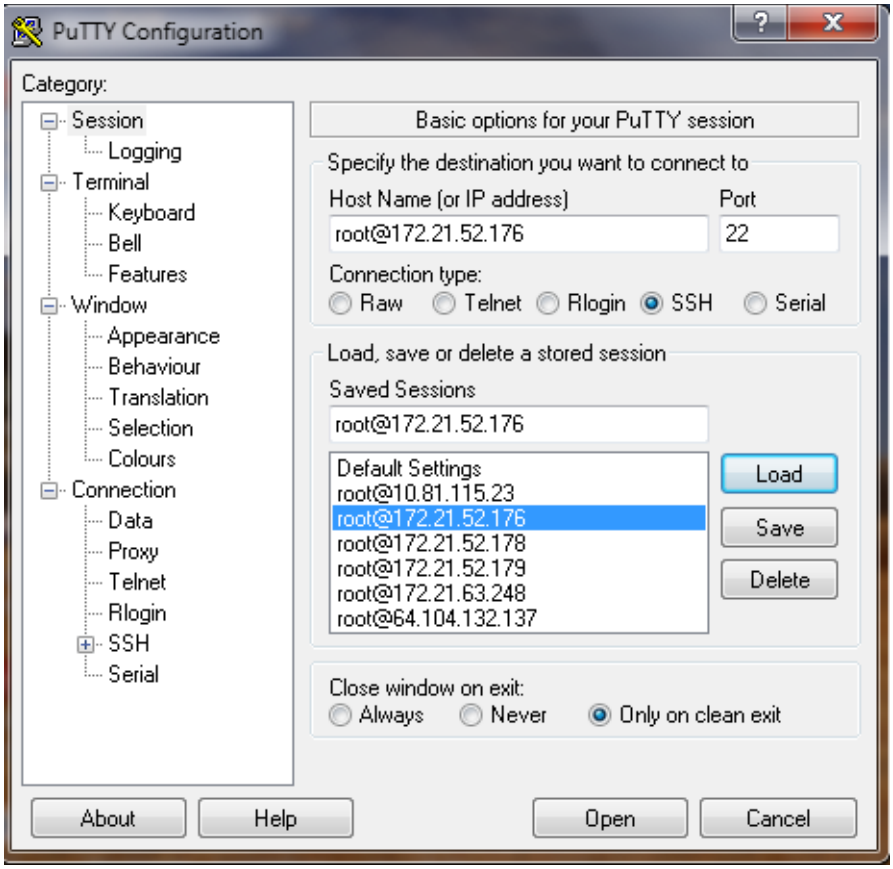
Note This step is necessary because the backup script uses log file rotation after backing up all the REM components each time. More details on log file rotation can be found in the "Log File Rotation" section of this chapter.

Now follow the steps below to create the backup.

Step 4 Log into the Primary REM Server through SSH.

Windows users: Download putty from http://www.putty.org/.

Figure 2-59 Putty Access



Linux Users:

a. Execute the following command to login to the REM server: **`#ssh <user>@<host>`** (e.g. **`ssh root@172.21.52.176`**)

b. Enter the password to log in.

Step 5 Execute the script to create the backup.

```
#cd $REM_HOME/tools/backup/scripts/
#./backup
```

Note The script can be executed from any directory by providing the full path (e.g. $REM_HOME/tools/backup/scripts/backup). On executing the backup script, the data and logs directories are created under $REM_HOME/tools/backup. The backup process creates an archive with the .tgz extension and the name appended with date, time, and REM server information from where the backup is created. It is stored in a REM server under the $REM_HOME/tools/backup/data directory (e.g.

$REM_HOME/tools/backup/data/rem_Aug-29-2012_02-13-32_10.76.8.178.tgz) or a remote FTP/SFTP server. A log file for backup activity is generated under the $REM_HOME/tools/backup/logs/ directory after each backup process. Log file rotation is performed in the same directory. For details on log file rotation please refer to the "Log File Rotation" section of this chapter. For details on scheduling the backup and automation of backup refer to the "Scheduling" section of this chapter.

Restoring the REM Server

This is the process of restoring the REM server in a single node or a dual node setup using the backup archive.

Pre-conditions: The required environment (e.g., OS, PostgreSQL and Tomcat) and application binaries are installed on the secondary server. To perform the above, please refer to the *Cisco Remote Expert Manager 1.9.2 Installation Guide*.

First, you will need to update the rem.properties file during REM ISO installation and before executing the IAS tool.

Follow these steps to restore the REM server:

Step 1 Configure the FEATURE_ENABLE property in the rem.properties file to enable restoration:

```
#To enable backup and restore for this release make it 'True' and
make it 'False' to disable this feature
$*[FEATURE_ENABLE]*=
```

Step 2 Configure the restore.properties file:

a. Navigate to the restore.properties file by using the following commands:

```
#cd $REM_HOME/tools/ias/templates/restore
#vi restore.properties.template
```

b. Configure the following properties:

Note Replace the brackets with the actual values. For example, replace <path to the temp location where backup folder was created> with /tmp/rem/backup.

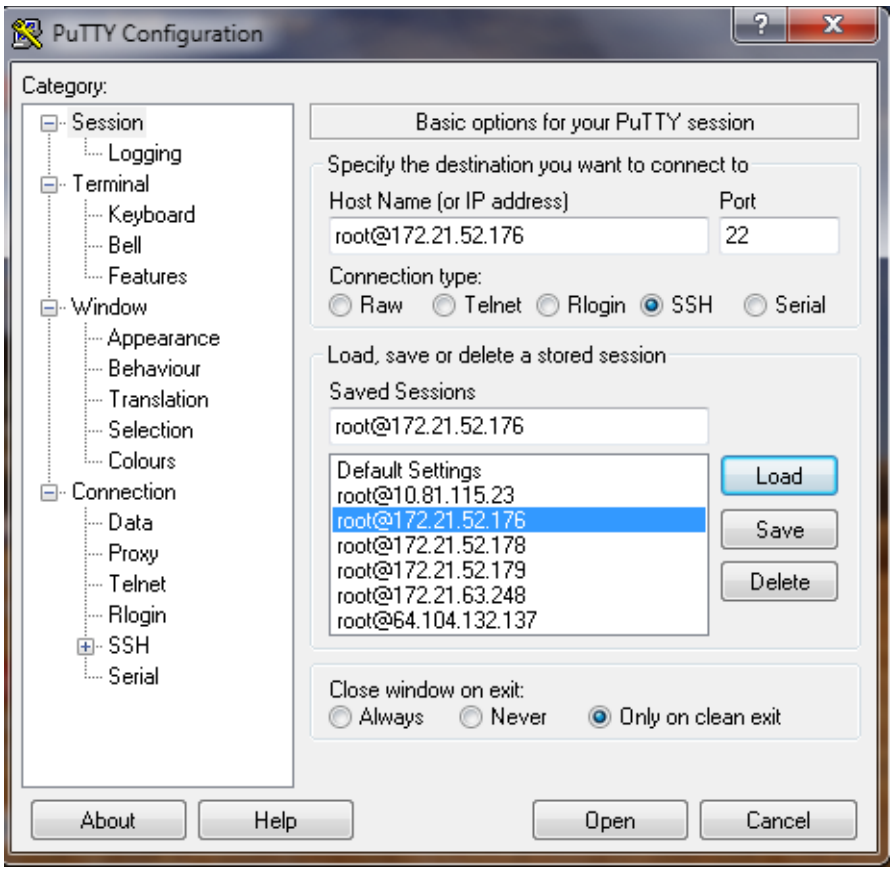
- tomcat_home= <path to the installation of Tomcat server>
- workspace= <path to the temp location where backup folder is extracted from archive>

```
#Absolute path to the installation of Tomcat server
tomcat_home=

#Absolute path to the temp location where backup folder are extracted
from archive
workspace=
```

Step 3 Log into the REM server where restoration has to be done using SSH.

- Windows users: Download putty from http://www.putty.org/.

Figure 2-60 Putty Access for Secondary Server



- Linux Users:

a. Execute the following command to login to the REM server: **`#ssh <user>@<host>`** (e.g. **`ssh root@172.21.52.176`**)

b. Enter the password to log in.

Step 4 Execute the script to restore the backup archive.

Pass the argument to run the restore script backup archive location with the filename by entering the following commands:

```
#cd /var/rem/tools/restore/scripts/
#./restore </path/to/backup_archive_name>
```

Note Replace `</path/to/backup_archive_name>` with the actual path. For example, **`#./restore $REM_HOME/tools/backup/data/rem_Aug-29-2012_02-13-32_10.76.8.178.tgz.`** The script can be executed from any directory by providing the full path (e.g., $REM_HOME/tools/restore/scripts/restore </path/to/backup_archive_name>).

Caveats

- Restore is required on demand if the REM server goes down due to system failure.
- In dual node setup, restoration must be done in both REM nodes to prevent data inconsistency.
- Both REM nodes must be in the same time zone.
- After restoration, file integrity should be checked in both REM nodes using the md5 checksum. If the checksum is mismatched, then restoration has to be executed again.

Error Messages

The following table contains all the error messages generated in backup and restore processes. These messages are logged in backup and restore log files respectively during the processes. If error messages are logged during a backup process, the messages are sent to the system administrator's email account. For restoration errors, all the error messages appear in the console.

Table 2-8 Backup Error Messages

Condition when the alert will be triggered	Alert type (Success/ Warning/ Error)	Alert message	Error Code	Configuration needs to be checked to resolve the issue
Artifacts are not backed up successfully!	Error	Cannot copy: No such file or directory	BR001	Check artifacts location in primary server
Database backup is failed!	Error		BR002	Check DB properties in backup.properties
Sending backup archive to ssh server<server_address> is failed!	Error	Authentication to <server address> is failed!	BR003	Check server_username and server_password in backup.properties
		Connection to <server address> is failed!	BR004	Check server_address in backup.properties
Login credentials are incorrect for FTP server!			BR005	Check server properties in backup.properties

Condition when the alert will be triggered	Alert type (Success/ Warning/ Error)	Alert message	Error Code	Configuration needs to be checked to resolve the issue
File upload is failed to < server_address >!			BR006	Check server properties in backup.properties
FTP server refused connection			BR007	Check server_address in backup.properties
Backup directory creation is failed in FTP server!			BR008	Check backup directory property in backup.properties file
File rotation is failed!			BR009	Check server related properties and no_backup_files in backup.properties file
Number of backup files cannot be negative			BR010	Check no_backup_files in backup.properties
Number of backup files cannot be zero			BR011	Check no_backup_files in backup.properties
Number of backup files should be a number			BR012	Check no_backup_files in backup.properties
Configured number of backup files is not correct			BR013	Check no_backup_files in backup.properties
Backup archive creation is failed!			BR014	
Backup is done with errors	Warning			Check log file to find the root cause

Table 2-9 Restore Process Error Messages

Condition when the alert will be triggered	Alert type (Success/ Warning/ Error)	Alert message	Error Code	Configuration needs to be checked to resolve the issue
Artifacts are not restored properly!	Error		BR015	Check artifacts path in REM server
Database restoration is failed!	Error		BR016	Check DB in restore.properties

Scheduling

Backups can be scheduled so that they are automatically performed at set intervals. The Crontab utility is used to schedule backups.

During REM ISO installation, the IAS tool triggers schedule script located under $REM_HOME/tools/backup/scripts/ in REM node for single node as well as dual node setups. If backup is enabled, it adds the job to Crontab and starts the Cron job in the REM servers automatically.

Step 1 Update the following parameters in rem.properties located under $REM_HOME/tools/ias/templates/ in the IAS tool. (For details refer to IAS documentation.)

Note The following properties need to be updated in both REM servers if there is a dual node setup.

```
#Configuring job scheduling parameters
#To configure the schedule user has to configure the following
parameters. User can use * as a value of any of these parameters.
#An asterisk (*) is used to indicate that every instance (i.e. every
hour, every weekday, etc.) of the particular time period will be
used.
#The values can not be blank. User can enter multiple values
separated by commas.
#E.g, 30 18 * * *  (each day at 6:30 PM)
#* * * * * (every min)
#0 0 1,5,10 * * (midnight on 1st,5th & 10th of month)
#*/2 * * * * (Every 2 min)
#Configure min (between 0-59)
$*[MIN]*=
#Configure hour (between 0-23, 0=midnight)
$*[HOUR]*=
#Configure day (between 1-31)
$*[DAY]*=
#Configure month (between 1-12)
$*[MONTH]*=
#Configure day of week (0-6, 0=Sunday)
$*[WEEKDAY]*=
```

Step 2 Execute **`main.sh`** located under $REM_HOME/tools/ias/scripts.

Note The log of the scheduling activity can be found in $REM_HOME/tools/backup/logs/schedule.log. It is recommended that backup scheduling should be done when the network load is low. It is not suggested to schedule backup during working hours.

Backup Archive Rotation

Backup archives are rotated after each backup in the backup storage server (SSH/FTP/SFTP server) to keep the most recently created backup archives. If the last backup archive is corrupted, then the system administrator has the option to choose another archive. File names include dates so that the administrator can choose a backup archive that was created on a particular day to restore the REM server to that date.

The NO_BACKUP_FILES property must be updated in the rem.properties file during REM ISO installation to indicate the number of backup files that should be stored in the backup server.

```
#No of backup files to be stored in backup server
$*[NO_BACKUP_FILES]*=
```

File rotation is done whenever a new backup archive is stored under $REM_HOME/tools/backup/data/ in case of the REM server (SSH) or FTP server.

All the logs related to the backup archive rotation can be found in $REM_HOME /tools/backup/logs/backup.log.

Log File Rotation

Logrotate is the default application used to rotate all application or process log files, which is provided by the UNIX operating system. For backup, it is backup.log file. Logrotate allows automatic truncation, rotation, compression, removal, and mailing of log files.

If a log file grows too large, it must be truncated and rotated. All this is done more efficiently by the logrotate application.

In the backup and restore process, the logrotate application is used to rotate the backup.log if it exceeds the user-specified size.

You must configure the rotate and size properties in the logrotate.properties file located under $REM_HOME/tools/backup/conf/:

```
#Number of log files to be rotated
rotate=


#Truncate the log file if it has size greater than the size specified
here
#If size is followed by M, the size is assumed to be in megabytes or
if k is used, the size is in kilobytes
size=
```

Execute the logrotation script located under $REM_HOME/tools/backup/scripts using following command to configure logrotate.conf using above properties for log file rotation:

```
#cd '$REM_HOME/tools/backup/scripts'
#./logrotation
```

The logrotate application is automatically executed by the backup script after creating the backup archive.

For example, consider the case where rotate=2 and size=1M. After rotating and truncating the backup.log file, the $REM_HOME/tools/backup/logs folder may contain the following files:

- backup.log
- backup.log.1
- backup.log.2, etc.

The backup.log file contains the most recent back up logs. The backup.log.1 file contains the logs which are older than the backup.log file. The backup.log.2 file contains the logs which are older than those in backup.log.1.

Note The script for logrotation must be executed before executing the backup script.