RE-on-IServices

September 28, 2015

Appendix Overview

This appendix explains how to set up RE-on-IServices. RE-on-IServices is an extension of Remote Expert that uses the I-Services platform. RE-on-IServices uses the Interactive Experience Client (IEC) as a video endpoint to make Session Initiation Protocol (SIP) calls from a kiosk.

Topics in this appendix include:

RE-on-IServices Overview

RE-on-IServices is an extended feature provided by the Remote Expert Manager (REM) that will enable a customer to interact with a remote agent via Cisco Contact Center on the I-Services platform. RE-on-IServices consists of the RE-Kiosk template and miniREIC.

1. RE-Kiosk template: A sample HTML web application, which provides interactive contents.
2. miniREIC: A JavaScript library that can be used by any HTML-based web application to utilize the capabilities of Remote Expert. This library currently supports Direct Connect (DC), which can be initiated in READ or manually started if using eREAD after a SIP call is established via REM.

In order for the SIP client to work, the IEC will need to be configured in the Cisco Unified Communication Manager (CUCM) and then configured on the REM.

Hardware Required

- Kiosk Side:
  - Cisco Interactive Experience Client (IEC)
  - Cisco Precision HD camera
  - Touchscreen
  - Microphone
  - External speaker if the touchscreen does not have a built-in speaker

Cisco IEC Setup on the CUCM

The Cisco IEC 4600 Series device is set up on the CUCM.

Step 1 Log into your CUCM using an account with administrator privileges. In the CUCM main page, select **Cisco Unified Communications Manager**.

Step 2 In the Cisco Unified CM Administration page, enter the proper credentials. Click the **Login** button.

Step 3 From the Device drop-down menu, choose **Phone**.

Step 4 All the devices registered through the CUCM will be listed. Click **Add New**.

Step 5 From the Phone Type drop-down menu, choose **Third-party SIP Device (Advanced)**. Click **Next**.

Step 6 Within the Device Information area, enter the information detailed in the table below. Click **Save**.

Table C-1 IEC Device Information

Field	Value
MAC Address	MAC address of the IEC
Description	Use a description that easily identifies the phone **Note** This field automatically pulls the value entered in the MAC Address field but this field can be modified.
Device Pool	Default
Phone Button Template	Third-party SIP Device (Advanced)

Note The IEC device's MAC address is located on the label on the back of the device.

Step 7 In order for the IEC device to be activated, it must be associated with a User Profile. From the User Management drop-down menu, choose **End User**.

Step 8 Click **Add New** and enter the information provided in the table below. Click **Save**.

Table C-2 End User Information

Field	Value
User ID	A unique ID to identify the user. ID should only use numerical values. User ID should be same as the directory number (DN) of IEC SIP Client. Also, DN should be unique in CUCM.
Password	A unique password to secure the account
Confirm Password	Re-enter the unique password
Last Name	A name used to identify the IEC SIP client

You will be redirected to a page where you can find the status of your User Profile creation. If all fields have been entered properly the status will show the "Add Successful" message.

Step 9 Associate a Directory Number (DN) to the newly created IEC SIP client profile. Select the desired IEC, by choosing **Phone** from the Device drop-down menu and then clicking the **Find** button.

Step 10 On the Phone Configuration screen, choose **Line [1] – Add a new DN** within the Association Information area.

Step 11 Enter a number in the Directory Number field, which must be the same value as the User ID that you entered earlier. Also enter values for the Description, Alerting Name, and ASCII Alerting Name fields. Click **Save**.

Step 12 Since the IEC SIP client can only handle one call at a time, you need to disable multiple call capability in CUCM. On the Directory Number Configuration page, find the Multiple Call/Call Waiting Setting section as shown in the figure below. Make sure that both Maximum Number of Calls and Busy Trigger fields are set to **1**.

Step 13 To link the DN to a desired user, go to the bottom of page and click **Associate End Users**.

The user list screen appears.

Step 14 Click **Find**. Check the check box next to the user that you would like to associate the IEC directory number. Click **Close**.

Step 15 Click **Save**, **Apply Config**, and **Reset**.

Step 16 Select the desired IEC, by choosing **Phone** from the Device drop-down menu and then clicking the **Find** button. Within the Protocol Specific Information area, go to the Digest User drop-down menu and choose the User ID previously created.

Step 17 Click **Save**, **Apply Config**, and **Reset**.

This Cisco IEC 4600 Series device is now registered on the CUCM.

Configuring a SIP Policy in the IEM

Once the IEC has been registered on the CUCM, a policy must be created on the IEM to enable the SIP feature in the REIC. The policy contains details about SIP.

The following steps explain how to create a policy and enter the call manager information on the IEM.

Note Each IEC SIP client should have its own SIP policy because the User ID of each IEC SIP client is unique to the CUCM and REM. Alternatively, you could create a general policy (e.g. SIP-General), which only contains the sip.domain, sip.transport, and sip.target values. Apply this general SIP policy to all IEC SIP clients that would run the RE-on-IServices application. Then for each IEC SIP client, configure sip.username and sip.password in the device's profile.

Step 1 Log into the Cisco IEM using the Account and Username under which the IEC is registered.

Step 2 Create a new policy for a specific IEC (e.g. SIP_SanJose_Kiosk1).

Step 3 Click the Policy tab within the new policy.

Step 4 Go to the application data property.

Step 5 Click the value field.

Step 6 In the Application data editor, click **+**.

Step 7 Click key:value.

Step 8 Enter **sip.domain** in the key field.

Step 9 In the value field, enter the IP address of the CUCM.

Step 10 Enter the remaining keys and values detailed in the table below.

Table C-3 Application Data Property Keys and Values

Key	Value
sip.domain	IP address of the CUCM
sip.username	User ID that was created in the CUCM
sip.password	Password associated with the above username
sip.transport	udp
sip.target	IVR number created in Cisco Contact Center for experts

Note It is important to enter all values in lowercase characters. If you enter "UDP" instead of "udp", the call will not work.

Step 11 Click **Ok**.

Step 12 Click **Apply**.

RE-on-IServices Configuration

There are five components for RE-on-IServices:

1. RE-on-IServices environment

2. miniREIC supporting files
3. I-Services template
4. SIP and DC call flow
5. HA proxy server

Set Up the RE-on-IServices Environment

To set up the RE-on-IServices environment, you will need the following:

- Three (3) servers to be fully functional, namely the REM server, a Reverse Proxy server, and a Content server.
- The IEC with firmware 5.48.62 or above.
- An application that is developed to be used as a "RE-on-IServices" template. This application is based on the I-Services platform template. This application should include the following features:
  - SIP widget
  - Direct Connect widget
  - Navigation buttons that each have a unique URL with self-contained images
  - Video playback

Note Video playback is NOT the same feature as video streaming from the agent's CAD. The video streaming functionality in CAD is NOT available with RE-on-IServices.

  - Accessibility option

Note This will be implemented in the next release.

  - RSS feed

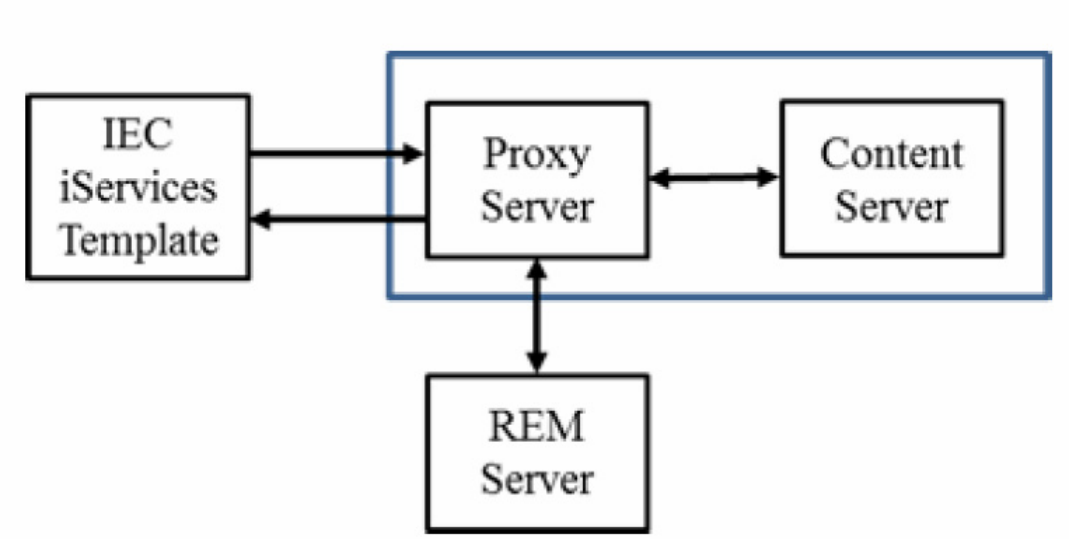
Note This feature is partially supported in this release.

Server Deployment

As mentioned above, RE-on-IServices requires three servers to be fully functional: the REM server, a Reverse Proxy server, and a Content server.

Although there are many ways to set up those three servers to enable RE-on-IServices to work, it is better to have the Reverse Proxy and Content servers on the same host server for system performance. The REM could be either a single node or HA setup. If this recommended deployment model is used, the work flow should look like the figure below.

Figure C-1 Recommended Server Deployment Model



Note All commands below are based on CentOS (6.4). The settings of components use default configurations. If you use a different operation system, please refer to that OS's user guide to get more details.

Note The VM hosting Reverse Proxy and Content servers are referred to as the "proxy server" in the following step set.

Steps to Set Up the RE-on-IServices Environment

Follow these steps to set up the RE-on-IServices environment:

Step 1 Create a new VM for Reverse Proxy and Content servers.

Step 2 Install Apache and PHP on the proxy server and verify its installation:

Note The Apache version should be version 2.2.22 or higher. The PHP version should be version 5.3.10-1 or higher.

a. Obtain the tested PHP file (phpinfo.php) from the code drop FTP site.

b. Upload the file to the /var/www/html folder in the proxy server.

c. Open a browser, and go to **https://<proxy server IP>:443/phpinfo.php**. You should see the PHP information if it was installed properly.

Step 3 Once Apache and PHP are up and running, configure Apache as the Reverse Proxy:

a. If the Apache service is running, stop the service by issuing the following command:

```
service httpd stop
```

b. Edit the Apache configuration file by issuing the following command:

```
vi /etc/httpd/conf/httpd.conf
```

c. Uncomment the following lines in the file to enable proxy modules:

```
LoadModule proxy_module modules/mod_proxy.so
LoadModule proxy_http_module modules/mod_proxy_http.so
```

d. Change the port for Reverse Proxy by finding the Listen line and changing its value to **81**.

e. Add the following lines to the bottom of file:

```
#For RE on iServices
SSLProxyEngine on
ProxyRequests Off
ProxyPass /resc https://172.25.26.141:8443/resc
ProxyPassReverse /resc https://172.25.26.141:8443/resc

<Location "/resc">
Order allow,deny
Allow from all
</Location>
```

f. Save the file and exit the vi editor.

Step 4 Create a new folder called “reOnIservices” under the /var/www/html directory to host the RE-on-IServices application.

Step 5 Unzip the RE-on-Iservices.zip file to the /var/www/html/reOnIservices directory. It should create a sub-folders called “v1”.

Step 6 Edit the RE-on-IServices application configuration by issuing the following command:

```
vi /var/www/html/reOnIservices/v1/reic/js/reic.json
```

The content of the reic.json file is:

```
{
"poolingInterval" : "3000",
“sessionPoolingInterval”: "1000",
"isDCEnable": "true",
"rescURL" : "<proxy server IP>: <Port>"
}
```

Step 7 Restart Apache by issuing the following command:

```
service httpd start
```

Step 8 Create a policy for RE-on-IServices in the IEM. Refer to the “Create and Apply a Policy for REM in the IEM” section in Chapter 1 for instructions. Ensure the following has been completed:

a. Provide proper SIP information in the application data property of the policy applied to the IEC.

b. In the browser property, disable web cache (browser > cache > web > enabled = **false)** and set the web cache mode to “Prefer network” (browser > cache > web > mode = **Prefer network**).

c. In the browser property, disable network failover (browser > network > failover > enabled = **false**), network timeout (browser > network > timeout > enabled = **false**), and watchdog (browser > watchdog > enabled = **false**).

d. In the browser property, configure the startup URL as:

https://<proxy server IP>:8443/reOnIservices/v1/index.html

e. Reboot the IEC after applying the new policy to the IEC.

miniREIC Supporting Files

There are three components required to initiate an RE instance:

1. reic-mini-< RE version >.js: This is the minified JavaScript file which makes the handshake with REM server for all feature collaboration. At this time of preparing this document, the library currently supports the DC feature only.

Note miniREIC takes advantage of jquery for all DOM manipulation so it requires importing the jQuery (jquery-2.0.3.min.js) separately before importing the reic-mini-<RE version>.js.

2. reic.json: Create a folder called “reic” under the root directory of the web application and place this reic.json file in the reic directory. The content of the reic.json file is the following:

```
{
"poolingInterval" : "3000",
"sessionPoolingInterval": "1000",
"isDCEnable": "true",
"rescURL" : "<proxy server IP>: <Port>"
}
```

Table C-4 reic.json File Properties

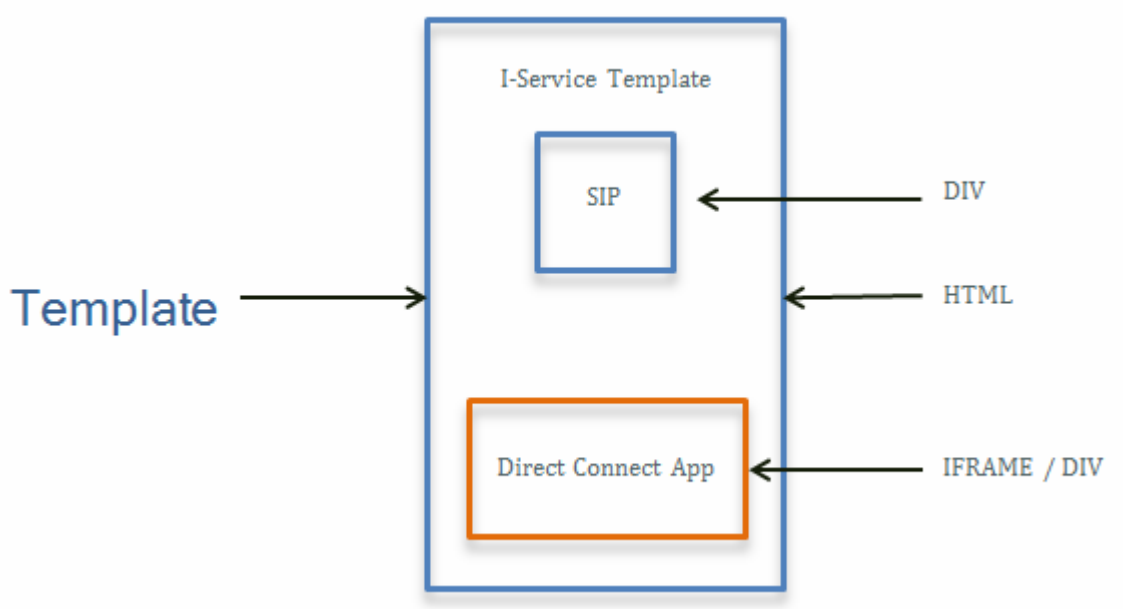
Property	Description
sessionPoolingInterval	Adjust the pooling interval that makes requests to the RE server. The default value is 3 seconds.
poolingInterval	Interval to detect the SIP call connection
isDCEnable	‘true’ enables Direct Connect and ‘false’ disables it
rescURL	REM URL (this is mostly a proxy URL since the REM URL is configured in the proxy server)

3. reic.css

The miniREIC library files can be found in the standard miniREIC template. The reic-mini-< RE Version >.js, reic.json, and reic.css files are built into the template.

Integrating miniREIC into the I-Services Template

Figure C-2 Integration Design Overview



To initiate miniREIC, follow these steps:

Step 1 To include the reic-mini-< RE Version >.js file in the web page, place the following tag in the HEAD section of the web page:

<!-- RE ON I-Service START-->

<scripttype="text/javascript"src="js/reic1.9.0.js"></script>

<!-- RE ON I-Service END -->

Note Import jQuery separately prior to importing the reic-mini-< RE Version >.js file.

Step 2 Create a tag with id set to “reicContainer” and assigned to it. Place the following tag in the BODY section of the webpage:

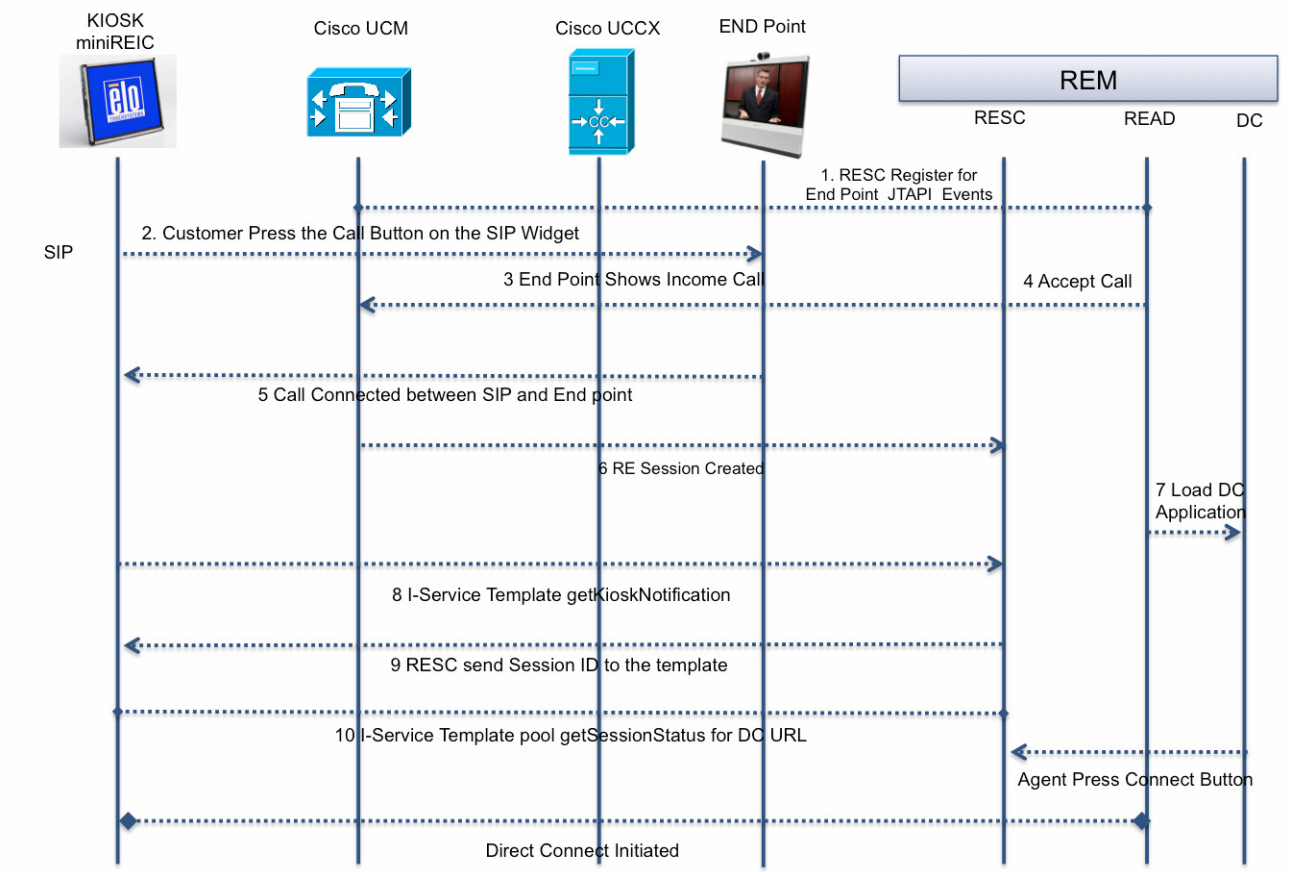
** **

Step 3 Link a reic style sheet for styling and positioning:

<link rel="stylesheet" href="css/reic.css"/>

SIP and DC Call Flow

Figure C-3 RE-on-IServices Call Flow



1. Since the JTAPI application in CUCM does not support the 3rd party SIP device (such as the IEC SIP client), REM cannot communicate with IEC via a JTAPI link. Instead, the RESC register uses the JTAPI events on agent endpoints to monitor all call statuses for RE-on-IServices SIP calls.
2. The customer presses an Expert Type (i.e. Call) button on the RE-Kiosk template to register and initiate a SIP call to the CUCM.
3. CUCM connects the call to an originated DN (i.e. the agent DN).
4. The agent answers the call.
5. The SIP call is established between the customer and the agent.
6. The RE session is created when the agent accepts the call.
7. The Direct Connect (DC) application loads in READ followed by call connected.

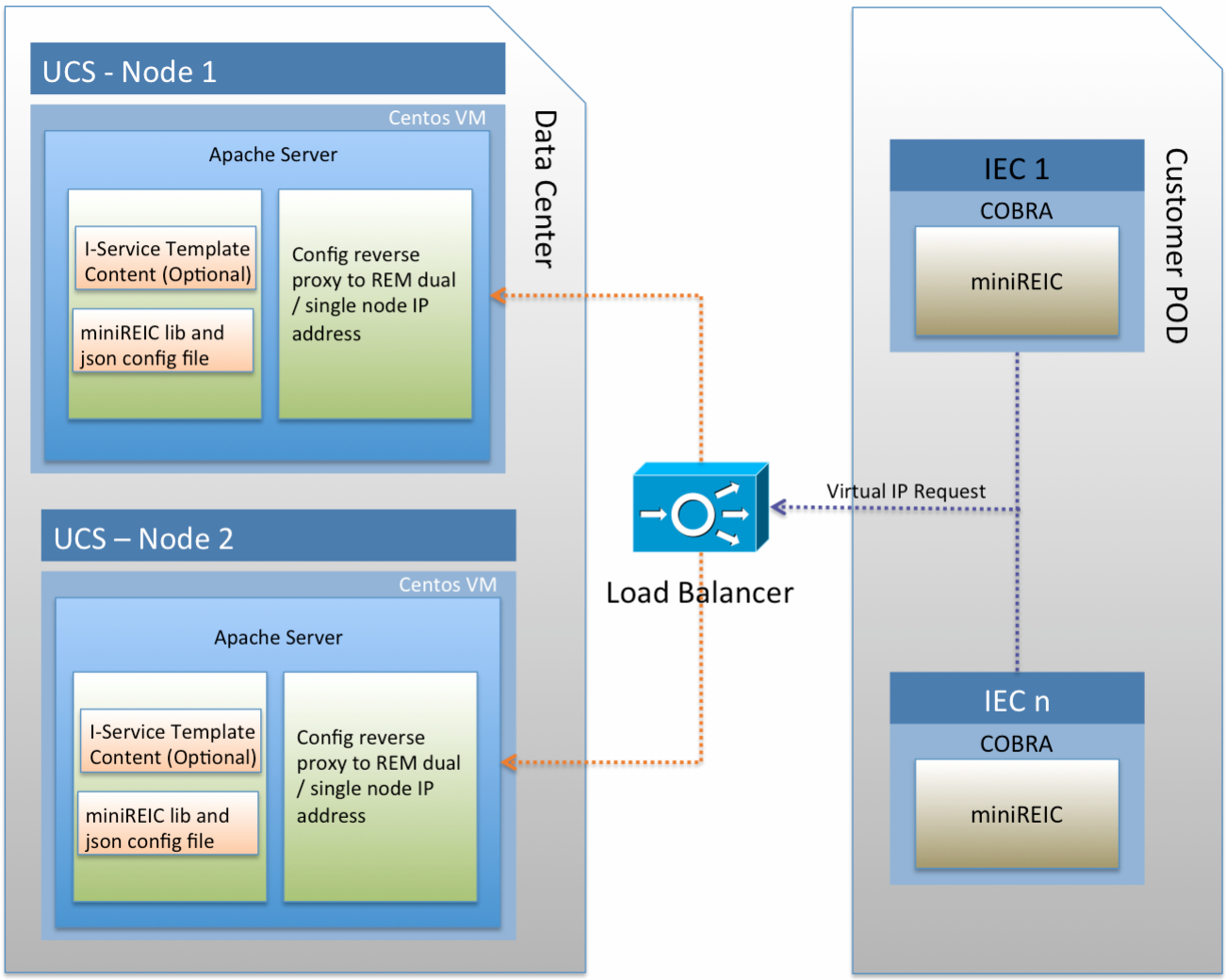
Note If the agent is using eREAD, the DC application will not automatically load. An agent using eREAD will need to manually start the DC application.

8. miniREIC initiates getKioskNotification with passing the IEC's serialNumber to the RESC server to obtain the session ID.

9. The RESC returns the session.
10. miniREIC sends the pooling getSessionStatus request to the RESC server to check if DC is initialized or terminated.
11. The agent initiates a DC session in READ or manually starts DC if using eREAD.
12. During the getSessionStatus, pooling from miniREIC detects the DC URL. Then it will create and load the IFRAME and share the collaboration between the agent and the customer. The collaboration is initiated or terminated based on the data available from getSessionStatus.

HA Proxy Server

Figure C-4 Architecture Overview



Configure the HA Proxy Server

Follow the below steps to configure the HA Proxy Server for both Node 1 and Node 2.If the Apache service is running, stop the service by issuing the following command:

```
service httpd stop
```

Step 4 Edit the Apache configuration by issuing the command:

```
vi /etc/httpd/conf/httpd.conf
```

Step 5 Uncomment the following lines in the file to enable proxy modules by adding a "#" in front of the lines:

```
#LoadModule proxy_module modules/mod_proxy.so
#LoadModule proxy_http_module modules/mod_proxy_http.so
```

Step 6 Find the keyword "Listen" and change the value of the port for Reverse Proxy to **81**. The line should look like the following:

```
Listen 81
```

Note By default, the load balancer is configured to listen to port 80. You may set your preferred PORT configuration in the load balancer and then move to the next step.

Step 7 Add the following lines to the bottom of file:

```
#For miniREIC
ProxyRequests Off
ProxyPass /resc <IP Address>/resc
ProxyPassReverse <IP Address>/resc
<Location "/resc">
Order allow,deny
Allow from all
</Location>
```

Step 8 Save the file and exit the vi editor.

Step 9 Start Apache by issuing the command:

```
service httpd start
```

Configure miniREIC to Support HA

To configure miniREIC to support HA, follow these steps:

Step 1 Modify the reic.json file (refer to the "miniREIC Supporting Files" section above).

Step 2 Update the load balancer's virtual IP address in the rescURL property.

```
{
```

```
"poolingInterval" : "3000",
"sessionPoolingInterval" : "1000",
"isDCEnable": "true",
"rescURL" : "<Load Balancer Virtual IP>:<Port>"
}
```