HCL Compass in AWS

Author: Di Lin
Date: September 30, 2020
Contact: d.lin@hcl.com

Contents

1. INTRODUCTION

HCL® Compass® is the next generation of IBM® Rational® ClearQuest®. Creating an HCL Compass server or migrating an existing ClearQuest server to HCL Compass server in Amazon Web Services (AWS) Cloud helps transform your organization with the following benefits:

- Lower costs
- Increased agility
- Enables reliable and global delivery

AWS provides EC2 (Amazon Elastic Compute Cloud) instances as the servers in Amazon's data centers which can be used to build and host the HCL Compass server. Both AWS EC2 instances and HCL Compass web server support Windows and Linux OS versions. So, a complete HCL Compass installation using EC2 instances is possible in AWS.

This whitepaper provides general guidance for cloud installation and migration from on-premises ClearQuest to AWS HCL Compass. It focuses on the additional configuration points beyond usual on-premises lab deployment. These points are caused mainly by AWS EC2 instances have special configuration other than normal OS version, e.g. port control and security groups. Chapter 3 describes the advantages of AWS cloud which include saving cost, flexible scalability, and high availability. Chapter 5 describes the considerations for deploying HCL Compass functions and features. Chapter 6 describes the migration process. Finally, Chapter 7 describes the sample deployment scenarios.

2. Audience

This whitepaper helps the administrators of HCL Compass deploy HCL Compass to AWS, and administrators of ClearQuest migrate to the Cloud. It includes strategy for a fresh installation of HCL Compass and migration from ClearQuest to HCL Compass in AWS. The administrator must be familiar with HCL Compass installation and ClearQuest configuration and administration.

3. Reasons for deploying HCL Compass in a cloud

This section summarizes reasons for deploying HCL Compass in cloud or moving an existing HCL Compass setup to cloud. The reasons include reducing capital expenditure, decreasing ongoing cost, improving scalability and availability, and attaining improvements in security and compliance.

3.1. Cost effectiveness

Virtual resources remove the capital expense of procuring and maintaining equipment as well as the expense of maintaining an on-premises data center, for example, cooling, physical security, janitorial services, etc. In AWS Cloud, AWS provides EC2 (Amazon Elastic Compute Cloud) instances as the servers in Amazon's data centers, to build and host HCL Compass. There is an annotated outline of links that follows the information in the Amazon Elastic Compute Cloud document and provides some annotations and links to other information in the AWS Documentation.

3.2. Scalability

Estimating data center capacity requirements is one of the most difficult tasks. Over-estimation leads the sinking capital into capacity you do not need. Underestimate, and you end up crippling the business’s ability to respond to an opportunity.

Cloud computing resources (compute, cloud storage, and network bandwidth) can be scaled up, down, or off to meet your current needs. AWS provides elastic computing, which automatically expands compute and storage to fit HCL Compass capacity requirements.

3.3. Availability

AWS has the resources to invest in redundant infrastructure, UPS systems, environmental controls, network carriers, power sources, etc. to ensure maximum uptime. AWS provides easier and cheaper solution than on-premises lab for recovery in the event of disaster, such as a fire or flood destroying a data center. The fast recovery of AWS EC2 instance and RDS service contribute to the high availability of HCL Compass.

4. Plan Your HCL Compass Deployment or Migration in AWS

Given, some of the AWS services and products explained in the above topics, let us now discuss about how you can use those capabilities to deploy HCL Compass in AWS.

Determining key aspects of HCL Compass deployment provides information that is useful in making decisions about the use of AWS services. The HCL Compass release note and deployment document provides more information about things you should consider including a description of the requirements for deployment.

4.1. HCL Compass Server (Web)

HCL Compass server (web) supported platform includes 64bit Windows and Linux as mentioned in the following table.

OS	HCL Compass 2.0.0 Platforms
Windows	Windows 10 Enterprise (x86_64) all updates Windows Server 2016 Windows Server 2019
Linux	RHEL 7.4 + (x86_64) RHEL 8.0 (x86_64)

Table 1: Supported Platforms

The following table explains recommended EC2 instance types based on lab trial. '*.xlarge' is a minimal requirement for HCL Compass deployment. '*.2xlarge' is a common recommendation for HCL Compass deployment. Any instance above '*.2xlarge' is recommended to use for gaining a higher performance. AWS supports all kinds of EC2 instance types, such as compute Optimized instances, memory optimized instances, accelerated computing instances, and storage optimized instances. For more details, see Amazon EC2 Instance Types. HCL Compass server requires a minimum 8GB RAM and 80GB hard disk space. Choose EC2 instance type carefully based RAM requirement according to your organization scale. RAM can differ for each customer workload (number of queries run, complexity of queries), record types, row width (number and size of fields), concurrent use access, longer session timeouts, use of reporting, etc.

Instance	vCPU*	Memory (GiB)	Instance Storage (GiB)	Network Bandwidth (Gbps)
t3.xlarge	4	16	EBS-Only	Up to 5
t3.2xlarge	8	32	EBS-Only	Up to 5
m6g.xlarge	4	16	EBS-Only	Up to 10
m6g.2xlarge	8	32	EBS-Only	Up to 10

m5.xlarge	4	16	EBS-Only	Up to 10
m5.2xlarge	8	32	EBS-Only	Up to 10

Table 2: Recommended EC2 Instance Type

* Each vCPU is a thread of either an Intel Xeon core or an AMD EPYC core, except for M6g instances, A1 instances, T2 instances, and m3.medium. vCPU and RAM are non-shareable in AWS. You can specify a custom number of vCPUs during launching this instance type. For more details on valid vCPU counts and how to start using this feature, visit the Optimize CPUs documentation page here. You can consult with AWS service team to identify how to match on-premises server configuration into AWS resources.

4.2. HCL Compass Supported Database Platforms

HCL Compass must work with a database to store and display data. The following table explains database type and version supported by HCL Compass 2.0.0. For latest platform supported by HCL Compass future releases, see HCL official site.

Database	Version
Microsoft SQL Server	2017
Oracle	12cR2, 18c, 19c
DB2	11.5

Table 3: Supported Databases

Amazon Relational Database Service (Amazon RDS) is available on several database instance types and provides you with six familiar database engines to choose from. Among them, HCL Compass can integrate with Amazon RDS Oracle database. Furthermore, you can choose to deploy databases on an AWS EC2 instance so that you can gain full control of the databases. Also, on-premises databases can work with HCL Compass in AWS. See Chapter 5.6 for performance consideration if the database is on-premises. The following table explains supported configurations.

Database	Amazon RDS-Supported	EC2 Instance-Supported	On-premises-Supported
Microsoft SQL Server	No	Yes	Yes
Oracle	Yes	Yes	Yes
DB2	No	Yes	Yes

Table 4: Supported AWS RDS Matrix

4.3. HCL Compass full-text search

HCL Compass full-text search feature has a separate WebSphere application server that handles indexing and search services for Compass databases. In most of the cases, HCL Compass full-text search feature is installed together with HCL Compass web server on the same instance. Optionally you can choose to install HCL Compass full-text search feature on another instance which type can follow *Table 2: Recommended EC2 Instance* Type. Deploy HCL Compass full-text search instance in the same sub-net of HCL Compass database in AWS to gain a better search performance. If HCL Compass full-text search instance is in AWS, but database is located on-premises, ensure the low network latency between HCL Compass full-text search instance and database for performance consideration.

4.4. HCL Compass Clients

There are two ways to access the data in the database. One way to access the HCL Compass Web Client is through an HCL Compass server. The following table displays supported browsers and versions. It is recommended to use Google Chrome and Mozilla Firefox to access HCL Compass Web.

Browsers	Version
Google Chrome	37 and future versions, releases and fix packs
Microsoft Edge	20 and future versions, releases and fix packs
Microsoft Internet Explorer	11 and future fix packs
Mozilla Firefox	54 and future fix packs
Mozilla Firefox ESR	38 and future versions, releases and fix packs

Table 5: Supported Browsers

The other way is to use HCL Compass eclipse client to access the database directly. Because AWS has strict port control policy on security group, this way shall not be widely used in AWS deployment.

5. AWS Deployment Considerations

Before starting the deployment of HCL Compass, set up the basic network through Amazon VPC. It must include the seamless (high bandwidth and low latency) connection between HCL Compass server and on-premises machines if any component is deployed in on-premises lab or clients are accessing from the on-premises lab. Since almost all the ports on an EC2 instance are closed by default, the following discussions of considerations focus on opening ports. Ensure those ports are not disabled by any firewall between Azure network and your on-premises lab. It also describes issues faced during lab trial.

5.1. Requisite Software

The following are the software pre-requisites and requisites to install and deploy HCL Compass.

Software	Version	Purpose
IBM Installation Manager	1.8.6 and future fixpacks	Download location
IBM HTTP Server	8.5.5.* and 9.0.0.5/above	Optional during installation. Installation guide.
IBM WebSphere Application Server	8.5.5.* and 9.0.0.5/above	Mandatory during installation. Download location
IBM WebSphere Application Server Supplements	8.5.5.* and 9.0.0.5/above	Optional during installation. Download Location
Licensing	Flexera	Hosted on Flexera. Refer to the software order acknowledgment letter for instructions on how to access the HCL License & Delivery Portal.
Java	OpenJDK8U 64bit	Mandatory during installation https://adoptopenjdk.net/

Table 6: Pre-requisite Software

Database	Microsoft SQL Server	2017
Database	Oracle	12cR2, 18c
Database	DB2	11.5

Table 7: Requisite database software

The base images can only be obtained through Passport Advantage site and consult HCL focal to get the licenses for HCL Compass requisite software.

5.2. Windows OS

After installing HCL Compass successfully using the installation guide, related ports of each database vendor must be opened before creating a schema repository. Configure the inbound rules on the deployed database side (for example, the RDS of Oracle, the EC2 instance that hosts SQL Server, or the EC2 instance that hosts DB2 as explained in the following table.

Database Server	Ports	Protocol	Source
Oracle RDS	1521/<SSL port>	TCP	<IP/IP block>
Microsoft SQL Server EC2 Instance	1433	TCP	<IP/IP block>
DB2 EC2 Instance	50000/<SSL port>	TCP	<IP/IP block>

Table 8: Inbound Rule for Databases

<SSL port> means, the SSL port is configured while enabling the SSL connection on the database. Database listens on the SSL port and the connection between HCL Compass and database is secured. For Oracle RDS, SSL port is normally configured as 2484. For DB2 EC2 instance, SSL port is the ssl_svcename configuration parameter which can be retrieved by 'get dbm cfg' command. For Microsoft SQL Server, SSL port is as the same as non-SSL port which is 1433.

<IP/IP block> refers to an IP address block and the IP must be related to HCL Compass Server IP. For example,

IP/IP block	Subnet Mast	IP block ranging
10.0.0.0/8	255.0.0.0	10.0.0.0-10.255.255.255
10.134.0.0/16	255.255.0.0	10.134.0.0-10.134.255.255
10.134.14.0/24	255.255.255.0	10.134.14.0-10.134.14.255
10.134.14.38/32	255.255.255.255	10.134.14.38

Table 9: <IP/IP block> Setting Examples

10.134.14.38/32, which is the exact HCL Compass server IP, allows the only connection from HCL Compass server to the port on database. And no other connection initiated from any other machines is allowed.

5.3. Linux OS

Remote display of RHEL's desktop is a must to install IBM WebSphere Application Server. But EC2 instances cannot be connected remotely with a GUI display after launching. So, the first step is to install requisite software to launch VNC server. The following example steps are provided on RHEL 7.6.

1. Log into Linux instance after obtaining the .pem file.
   When following related guide to log into RHEL server, Ensure that ec2-user is the username associated with that key. Then after login, enter **sudo su -** before continuing the following operations.
2. Install GUI related package on the HCL Compass EC2 Linux instance. Choose vnc server package based on your requirement.
   Enter **yum groupinstall 'Server with GUI'**

Enter **yum install -y pixman pixman-devel libXfont**
Enter **yum -y install tigervnc-server**

After installation, check this system file has correct content by the following command.

[root@ip-10-123-12-12 .vnc]# cat /etc/sysconfig/vncservers
# THIS FILE HAS BEEN REPLACED BY /lib/systemd/system/vncserver@.service
VNCSERVERS="1:root"

3. Using <IP>:1 in VNC Viewer, connect to VNC server of the HCL Compass EC2 Linux instance.
   If the connection failed, perform the following setting to make VNC connect OK.
   a. Add the VNC port into whitelist of firewall
      Enter **iptables -I INPUT -p tcp --dport 5901 -j ACCEPT**
      If testing a server of HCL Compass, an optional configuration turns off firewall. The following commands for stopping and disabling firewall must not be applied for productive HCL Compass web server.
      Enter **systemctl stop firewalld**
      Enter **systemctl disable firewalld**

   b. In AWS EC2 console of the HCL Compass EC2 Linux instance, open the VNC port 5901 and the source should be your access machine's IP. A sample inbound rule is explained in the following table.

Server	Ports	Protocol	Source
HCL Compass EC2 Linux Instance	5901	TCP	<IP/IP block>

Table 10: Inbound Rule for HCL Compass EC2 Linux Instance

<IP/IP block> refers to an IP address block and See *Table 9: <IP/IP block> Setting* Examples for the definition .

After connecting to VNC IP:1, if the screen does not display correctly, such as a grey screen, the sample /root/.vnc/xstartup file given in the following can be a possible solution:

```
#!/bin/sh
[ -x /etc/vnc/xstartup ] && exec /etc/vnc/xstartup
[ -r $HOME/.Xresources ] && xrdb $HOME/.Xresources
xsetroot -solid grey
vncconfig -iconic &
x-terminal-emulator -geometry 80x24+10+10 -ls -title "$VNCDESKTOP Desktop" &
x-window-manager &
gnome-panel &
gnome-settings-daemon &
metacity &
nautilus &
```

4. If deploying HCL Compass on RHEL 8.0 and above, Ensure the following lib is installed.
   yum -y install libnsl
   If using SQL server database with Linux HCL Compass, Ensure the following rpm is installed.
   rpm -i --nodeps msodbcsql17-17.4.2.1-1.x86_64.rpm

5.4. HCL Compass Administration

Administering HCL Compass Administrators are typically responsible for installing the software, creating a release area, and installing fix packs. Administrators also create and manage schema repositories and user databases, configuring Lightweight Directory Access Protocol (LDAP) user authentication, managing user accounts, and setting up HCL Compass Web. There is no significant difference between the administration of HCL Compass in AWS and an on-premises HCL Compass. To allow the administrative machine to access to the HCL Compass web administrative ports, the HCL Compass web server needs to open ports listed as follows:

Server	Ports	Protocol	Source
HCL Compass EC2 Instance	<12043> OR <12060>	TCP	<IP>/<IP Block>
HCL Compass EC2 Instance	<12443> OR <12080>	TCP	<IP>/<IP Block>

Table 11: Inbound Rule for HCL Compass EC2 Instance

The port 12043 is the default port of cqwebprofile console management https connection. The port 12060 is the default port of cqwebprofile console management http connection. Open either one to connect to cqwebprofile console management url which is https(http)://< AWS_HCL_Compass_IP>:<12043|12060>/ibm/console.

The port 12443 is the default port of cqwebprofile https protocol. The port 12080 is the default port of cqwebprofile http protocol. Open either one to connect to HCL Compass web.

<IP>/<IP Block> refers to Table 9: <IP/IP block> Setting Examples. It is recommended to use <administrative_machine_IP>/32.

If the database server is in AWS, to manage schema repositories and user databases, it is recommended to deploy the HCL Compass administration tool in AWS. Allow the tool to access the ports of the database specified in Table 8: Inbound Rule for Database. If the database server is on-premises, it is recommended to deploy the HCL Compass administration tool on-premises. If the database server and HCL Compass administration tool are not located in the same sub-LAN, administration operation takes a longer time to complete which is depended on the network latency.

5.5. HCL Compass web and thick client

End user is recommended to access HCL Compass Web by browser.

Server	Ports	Protocol	Source
HCL Compass EC2 Instance	<443> OR <80>	TCP	<IP>/<IP Block>
HCL Compass EC2 Instance	<12443> OR <12080>	TCP	<IP>/<IP Block>

Table 12: Inbound Rule for HCL Compass EC2 Instance

If 443 port is opened and IBM HTTP server plugin is configured successfully, then opening port 12443 is optional.

The port 443 is the default port for https protocol. The port 80 is the default port for http protocol.

<IP>/<IP Block> refers to Table 9: <IP/IP block> Setting Examples/. It is recommended to use 10.0.0.0/8 if the IP of this HCL Compass EC2 instance starts with 10.

Thick client is not recommended to be widely used in AWS because of AWS port control policy. If administrators wants to manage HCL Compass database and schema by HCL Compass eclipse designer, maintenance tool and user administration tool, open the corresponding ports in *Table 8: Inbound Rule for* Databases from administrative machines to HCL Compass database.

5.6. Performance

AWS EC2 t2 type instance behaves efficiently during lab trial performance testing. There is no performance downgrade or performance issue observed. But the time for login and querying are impacted by the network latency between HCL Compass server and database. The login time will increase if database is deployed on-premises lab because of network latency. So, deploying database in on-premises lab is not recommended in the consideration of performance.

AWS Monitoring provides a number of services including details described in Linux Monitoring and Windows Monitoring. It can be used to gauge the health of the various servers and clients running in AWS. It can provide notifications if various configured thresholds are exceeded. See here for details on "Monitoring HCL Compass Web Server".

5.7. OSLC Integration

Before Configuring HCL Compass Web server for cross-server communication, see the following table for opening the ports.

Server	Ports	Protocol	Source
HCL Compass EC2 Instance	<443> OR <12443>	TCP	<RQM IP>/32
RQM EC2 Instance	<9443>	TCP	<HCL Compass IP>/32

Table 13: Inbound Rule for HCL Compass EC2 and RQM EC2 Instances

The port 443 is the default port for IBM HTTP Server after configuring web server plugin into IBM WebSphere Application server cqwebprofile. This port is recommended to be used in OSLC integration. If there is no web server plugin configured, use the default port 12443 of cqwebprofile.

The port 9443 is the default port for RQM https protocol.

5.8. Load Balancing

AWS provides load balancing service called Elastic Load Balancing. Elastic Load Balancing distributes incoming application or network traffic across multiple targets, such as Amazon EC2 instances, containers, and IP addresses, in multiple Availability Zones. Elastic Load Balancing scales your load balancer as traffic to your application changes over time. It can automatically scale to the vast majority of workloads. Elastic Load Balancing supports three types of load balancers: Application Load Balancers, Network Load Balancers, and Classic Load Balancers. Application Load Balancers is recommended for HCL Compass web. You can configure ALB listener rules to route requests to HCL Compass web. The rules support path-based routing, host-based routing, and redirecting requests from one URL to another. Contact AWS support for how to configure AWS load balancing efficiently.

If a load balancer is required between on-premises lab and AWS, IBM HTTP server simple load balancing is another option. Verify the following checklist for load balancer to run successfully. If any issues during the configuration, contact WAS Support for assistance. The following steps can be applied to any servers which needs to be configured into the load balancer group. Assume IP1 is the IP of AWS EC2 instance installed with HCL Compass web server and IP2 is the IP of on-premises server installed with HCL Compass web server.

1. Following chapter 5.9 step ② to configure https://<IP1>/cqweb and https://<IP2>/cqweb accessible.
2. Ensure IP1 can access the port 12443 of IP2, which means on IP1 https://<IP2>:12433/cqweb can be opened successfully.
3. Ensure IP2 can access the port 12443 of IP1, which means on IP2 https://<IP1>:12443/cqweb can be opened successfully.
4. Configuring simple load balancing across multiple application server profiles (V9.0.5.X).

5. Configure a unique HTTP session clone ID for each application server for IP1 and IP2 inside V9.0.5.X.
6. After merging C:\Program Files (x86)\IBM\WebSphere\Plugins\config\plugin-cfg.xml of IP1 and IP2 following the steps inside V9.0.5.X, the keyring and stash file of IP1 must be shipped to IP2. Also, the keyring and stash file of IP2 must be shipped to IP1. After shipping. Ensure the location is correct for the merged plugin-cfg.xml.
7. In merged plugin-cfg.xml, the Hostname shall be changed from localhost to IP1 according to the server clone ID has been configured in step5. The following is one part of a sample plugin-cfg.xml after merging and updating manually.

```
<Server CloneID="<IP1_CloneID>" ConnectTimeout="0"
        ExtendedHandshake="false" MaxConnections="-1"
        Name="dfltNode_server1_1" ServerIOTimeout="900" WaitForContinue="false">
        <Transport ConnectionTTL="28" Hostname="<IP1>"
          Port="12080" Protocol="http"/>
        <Transport ConnectionTTL="28" Hostname="<IP1>"
          Port="12443" Protocol="https">
          <Property Name="keyring" Value="C:\Program Files (x86)\IBM\WebSphere\Plugins\config\webserver2\plugin-key.kdb"/>
          <Property Name="stashfile" Value="C:\Program Files (x86)\IBM\WebSphere\Plugins\config\webserver2\plugin-key.sth"/>
        </Transport>
      </Server>
```

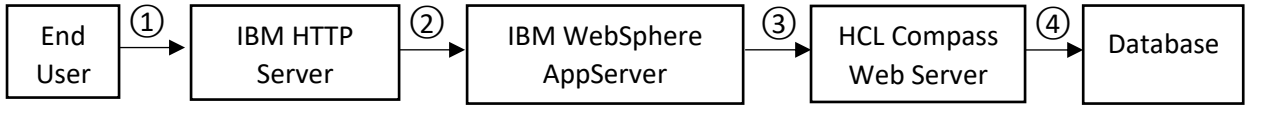
And another sample as the following:

```
<Server CloneID="<IP2_CloneID>" ConnectTimeout="0"
        ExtendedHandshake="false" MaxConnections="-1"
        Name="dfltNode_server1_0" ServerIOTimeout="900" WaitForContinue="false">
        <Transport ConnectionTTL="28" Hostname="<IP2>"
          Port="12080" Protocol="http"/>
        <Transport ConnectionTTL="28" Hostname="<IP2>"
          Port="12443" Protocol="https">
          <Property Name="keyring" Value="C:\Program Files (x86)\IBM\WebSphere\Plugins\config\webserver1\plugin-key.kdb"/>
          <Property Name="stashfile" Value="C:\Program Files (x86)\IBM\WebSphere\Plugins\config\webserver1\plugin-key.sth"/>
        </Transport>
      </Server>
```

8. After plugin-cfg.xml is placed and updated correctly, restart IBM HTTP Server and IBM WebSphere Server on both IP1 and IP2 for the load balancing to work.
9. To confirm load balancing is configured successfully, Clearing browser cache and access https://<IP1>/cqweb. First time, it is showing the login page of IP1. Refresh to access https://<IP1>/cqweb again, it is showing the login page of IP2.

5.9. SSL Enablement

HCL Compass supports several ways to enhance the security of transportation. The following diagram shows the four points where the security can be enhanced. IBM HTTP Server and/or IBM WebSphere Application Server can be configured after the installation. All the following steps are performed on AWS EC2 instances or RDS.



① Connection between End users and HCL Compass server can be secured.

End user can access https://<AWS_HCL_Compass_IP>/ after IBM HTTP Server is installed and started.

② Connection between IBM HTTP server and IBM WebSphere Application Server can be secured.

After Configuring a web plug-in for IBM HTTP Server and Configuring secure connections between IBM HTTP server and IBM WebSphere Application Server, End user can access and log into https://<AWS_HCL_Compass_IP>/cqweb. If cqweb cannot be launched successfully, following Configuring the web server plug-in for Secure Sockets Layer to copy the keystore and to stash files to a managed web server.

③ IBM WebSphere Application Server can be secured.

After ① and ② has been setup successfully, the transportation between End user and HCL Compass Web has been encrypted by SSL.

Additionally, to comply with the US government SP 800-131 security standard, you can configure the WebSphere® Application Server which hosts Compass to support the Transport Layer Security (TLS) 1.2 protocol.

④ Connection between HCL Compass Web server and database can be secured.

Compass provides the support of three database vendors as SQL server, Oracle, DB2 server. All of them can be setup with an SSL connection.

a. Oracle RDS SSL configuration

a) Setup SSL configuration on AWS RDS Oracle instance following AWS guide.
b) Download the root certificate that works for all AWS Regions and check the file is in the Download directory. Currently the certificated is named as rds-ca-2019-root.pem and it might change in the future but can always be downloaded in AWS official site.
c) Install Oracle client which is equal or higher version compared to the AWS Oracle RDS DB engine version. For example, if AWS Oracle RDS has a DB engine version as oracle 18c, choose oracle client oracle 18c or 19c. The installed machine can access the AWS RDS Oracle 1521 port.

   Note: Choose The installation type of oracle client as Administrator.

d) Create a wallet.

```
prompt> cd C:\app\client\Administrator\product\18.0.0\client_1\bin
prompt> .\orapki.bat wallet create -wallet C:/Users/Administrator/Desktop/ssl_wallet -auto_login_only
```

e) Add root cert of AWS.

```
prompt>.\orapki.bat wallet add -wallet C:/Users/Administrator/Desktop/ssl_wallet -trusted_cert -cert
C:/Users/Administrator/Downloads/rds-ca-2019-root.pem -auto_login_only
```

f) Create folder network/admin under C:\Program Files\HCL\CCM\common\odbc\oracle.

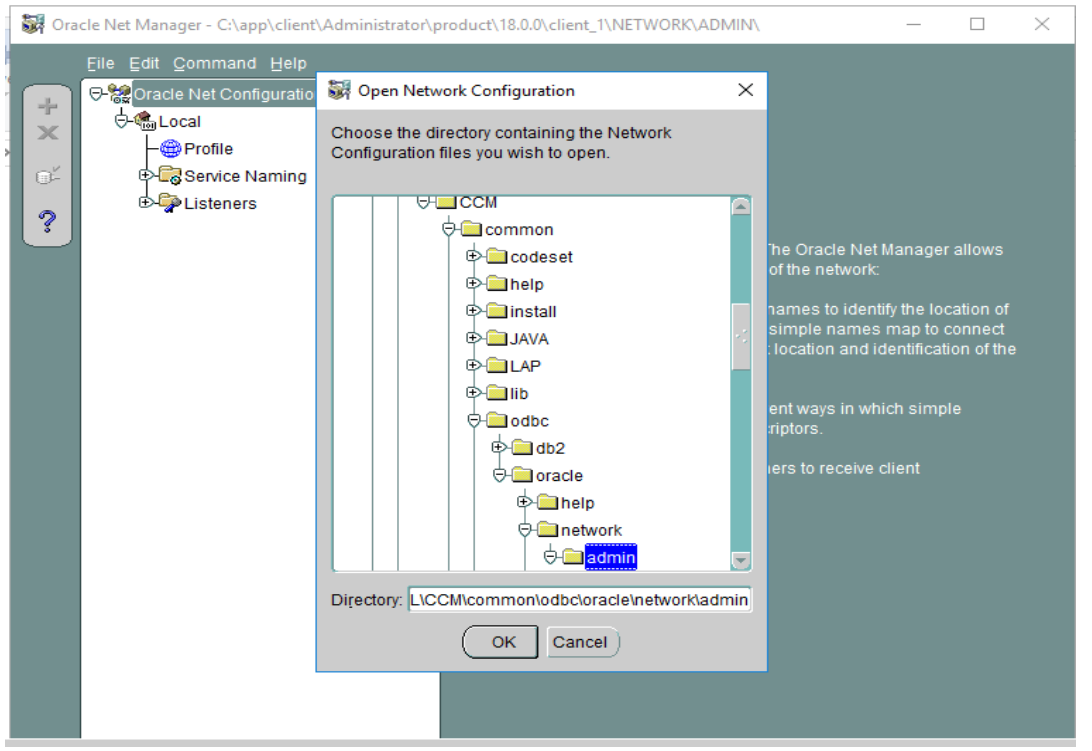


Figure 1: Select Network Configuration file

g) Open Oracle Net Manager, Select File->Open Network Configuration and select C:\Program Files\HCL\CCM\common\odbc\oracle\network\admin, Click Ok.

h) Select Profile->Network Security->SSLCheck configure SSL for client and input wallet location in step d.

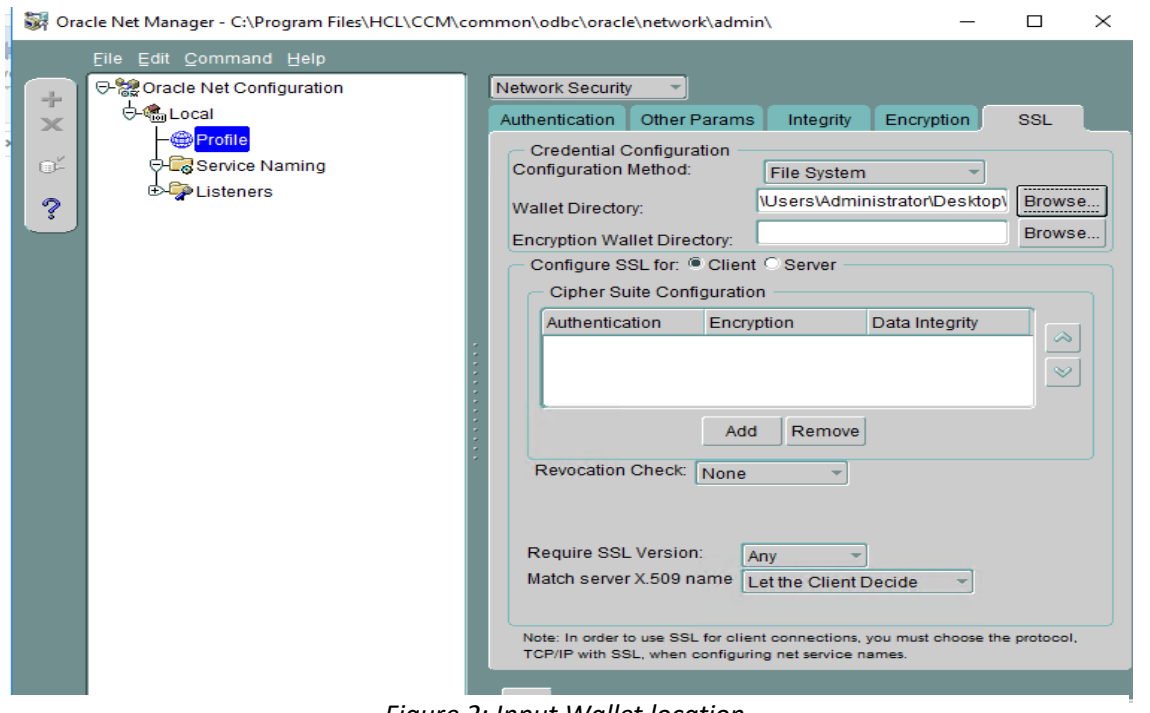


Figure 2: Input Wallet location

i) Create a service naming with net service name as <ORCL>, TCP/IP with SSL, hostname of AWS RDS Oracle, Port Number as 2484, Service Name as <ORCL>. Service Name should be the SID provided by AWS RDS instance and it is set to ORCL usually.

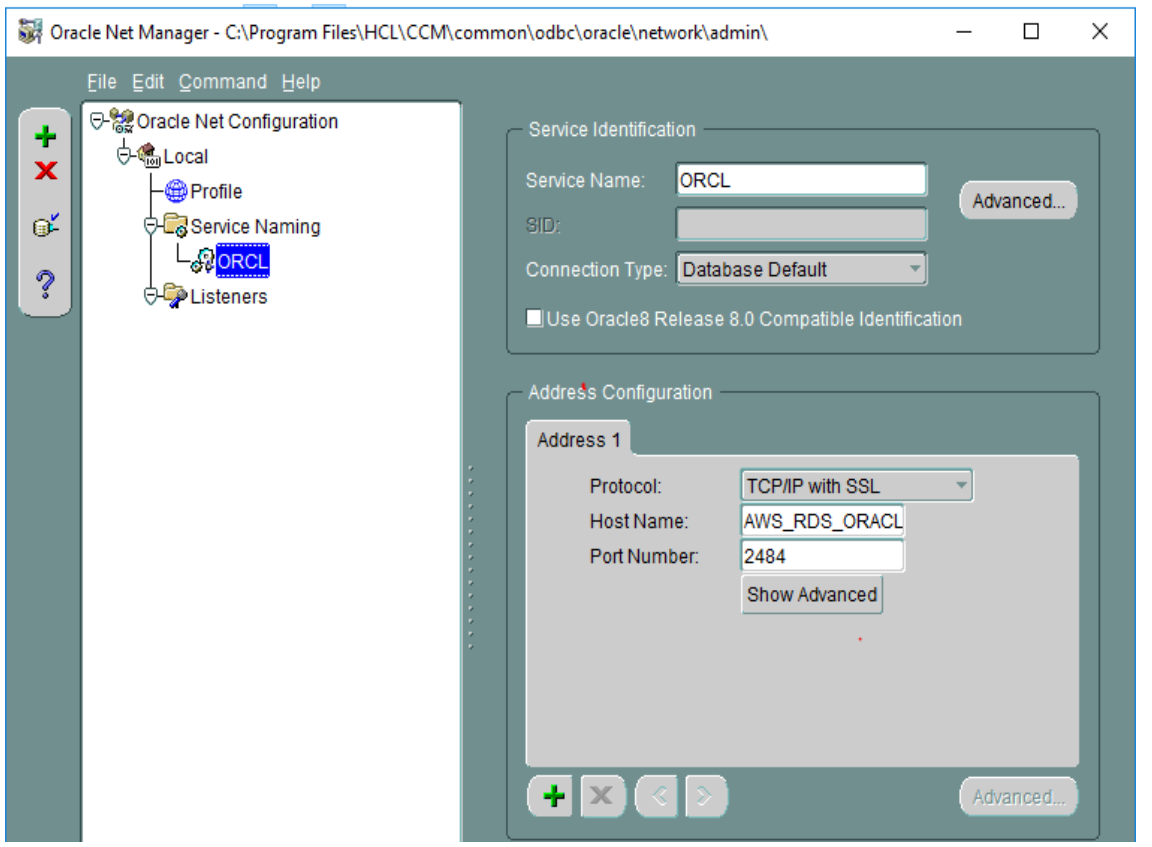


Figure 4: Create SSL orcl connection

j) Save network configuration.

k) In the command line administrative mode, run the following command to update master database connect option.

installutil relocateschemarepo -dbset <dbset> <admin> <admin_password> ORACLE <AWS_RDS_Oracle_HOSTNAME> <orcl> <master_dbo_login> <master_dbo_password> <master_rw_login> <master_rw_password> <master_ro_login> <master_ro_password> "TNS_SERVICE_NAME=ORCL;"

Then run the following command to update user database connect option.

installutil relocateuserdb -dbset <dbset> <admin> <admin_password> <user_dbname> ORACLE <AWS_RDS_Oracle_HOSTNAME> <orcl> <user_dbo_login> <user_dbo_password> <user_rw_login> <user_rw_password> "TNS_SERVICE_NAME=ORCL;"

Note:

TNS_SERVICE_NAME as ORCL is the net service name created in step I. Change it to the value if the net service name has been created as another name but not ORCL.

AWS RDS cannot turn off the non-SSL port 1521. To turn it off, remove all the security groups which allows access to port 1521.

l) If HCL Compass is deployed on Linux instance, step b~k needs to be done on Linux instance accordingly. After all the steps are finished successfully, run the following command to add dbset with connect option.

Prompt>./cqreg add_dbset -v oracle -d <service_name> -s <AWS_RDS_Oracle_HOSTNAME> -u <username> -p <password> -dbset <ORACLESSL> -co "EXTRA_PARAMS='TNS_SERVICE_NAME=ORCL; '"

b. DB2 SSL Configuration

a) The following steps are summarized based on lab trial and the official link. The detailed steps might change based on different DB2 server version. If running into issue, contact your DB2 server DBA.

b) Create kdb On DB2 EC2 instance.

```
prompt>cd cd C:\Program Files\IBM\gsk8\bin
prompt>gsk8capicmd_64.exe -keydb -create -db "mydbserver.kdb" -pw "mypassword" -stash
```

c) Create self-signed certificate and pick up a supported signer algorithm. If there is official certificate, this step can be skipped.

```
prompt>gsk8capicmd_64.exe -cert -create -db "mydbserver.kdb" -pw "mypassword" -label "myselfsigned" -dn
"C=US,ST=Washington,L=Seattle,O=Amazon.com,OU=RDS,CN=<AWS_DB2_HOSTNAME>" -size 2048 -sigalg
SHA256_WITH_RSA
```

d) Update db2 setup with kdb and sth and ssl port information on DB2 EC2 instance. Enter db2 command line Processor and execute the following commands.

```
prompt>update dbm cfg using SSL_SVR_KEYDB "C:\Program Files\IBM\gsk8\bin\mydbserver.kdb"
prompt>update dbm cfg using SSL_SVR_STASH "C:\Program Files\IBM\gsk8\bin\mydbserver.sth"
prompt>update dbm cfg using SSL_SVR_LABEL myselfsigned
prompt>update dbm cfg using ssl_svcename  50602
```

e) Turn on SSL switch of DB2 EC2 instance.
Enter DB2 command window

```
prompt>cd C:\Program Files\IBM\SQLLIB\BIN
prompt>db2set -i DB2 DB2COMM=SSL
```

f) Restart DB2 EC2 instance.

```
prompt>cd C:\Program Files\IBM\SQLLIB\BIN
prompt>db2stop force
prompt>db2start
```

m) In the command line administrative mode, run the following command to update master database connect option. The path of certification can be set as a UNC path which can be accessible globally by other machines without downloading the certification.

```
installutil relocateschemarepo -dbset <dbset> <admin> <admin_password>  DB2  <AWS_DB2_HOSTNAME>
<master_database> <master_dbo_login> <master_dbo_password> <master_rw_login> <master_rw_password>
<master_ro_login> <master_ro_password>
"PORT=50602;EXTRA_PARAMS_WINDOWS='Security=SSL;SSLClientKeystoredb=C:\mydbserver.kdb;SSLClientKeystash=C:\mydbserver.sth;';"
```

If HCL Compass is deployed on Linux instance, the connect option should be replaced as the following.

```
PORT=50602;EXTRA_PARAMS_WINDOWS='Security=SSL;SSLClientKeystoredb=C:\mydbserver.kdb;SSLClientKeystash=C:\mydbserver.sth;';EXTRA_PARAMS_UNIX='Security=SSL;SSLClientKeystoredb=/root/mydbserver.kdb;SSLClientKeystash=/root/mydbserver.sth;'
```

Then run the following command to update user database connect option.

```
installutil relocateuserdb -dbset <dbset> <admin> <admin_password> <user_dbname> DB2 <AWS_DB2_HOSTNAME>
<user_database>  <user_dbo_login> <user_dbo_password> <user_rw_login> <user_rw_password>
"PORT=50602;EXTRA_PARAMS_WINDOWS='Security=SSL;SSLClientKeystoredb=C:\mydbserver.kdb;SSLClientKeystash=C:\mydbserver.sth;'"
```

If HCL Compass is deployed on Linux instance, the connect option should be replaced as the following.

PORT=50602;EXTRA_PARAMS_WINDOWS='Security=SSL;SSLClientKeystoredb=C:\mydbserver.kdb;SSLClientKeystash=C:\mydbserver.sth;';EXTRA_PARAMS_UNIX='Security=SSL;SSLClientKeystoredb=/root/mydbserver.kdb;SSLClientKeystash=/root/mydbserver.sth;'

g) If HCL Compass is deployed on Linux instance, add dbset with the following command and specified connect option and make sure the certificate is shipped to Linux instance and placed at the location specified in connect option.

prompt>./cqreg add_dbset -v db2 -d <table_name > -s <AWS_DB2_HOSTNAME> -u <username> -p <pwd> -dbset <DB2SSL> -co "PORT=50602;EXTRA_PARAMS_WINDOWS='Security=SSL;SSLClientKeystoredb=C:\mydbserver.kdb;SSLClientKeystash=C:\mydbserver.sth;';EXTRA_PARAMS_UNIX='Security=SSL;SSLClientKeystoredb=/root/mydbserver.kdb;SSLClientKeystash=/root/mydbserver.sth;'"

c. SQL Server SSL Configuration

a) Prepare the SQL server key. It can be generated by IIS tool.
Prompt>cd C:\Program Files (x86)\IIS Resources\SelfSSL
Prompt> selfssl.exe /N:CN=<AWS_SQL_Server_HOSTNAME> /K:1024 /V:7 /S:1 /P:442 /T

b) Configure SQL server SSL configuration following the link.
Note: The configuration details might change based on different SQL server version. If running into issue, contact your SQL server DBA.

h) In the command line administrative mode, run the following command to update master database connect option.
'TrustServerCertificate=true' can be skipped in deploying in a productive environment to enhance the security.

installutil relocateschemarepo -dbset <dbset> <admin> <admin_password> SQL_SERVER <AWS_SQL_Server_HOSTNAME> <master_database> <master_dbo_login> <master_dbo_password> <master_rw_login> <master_rw_password> <master_ro_login> <master_ro_password> "EXTRA_PARAMS='Encrypt=true;TrustServerCertificate=true;'"

If HCL Compass is deployed on Linux instance, the connect option should be replaced as the following.

EXTRA_PARAMS_UNIX='Encrypt=yes;TrustServerCertificate=yes;';EXTRA_PARAMS_WINDOWS='Encrypt=true;TrustServerCertificate=true;'

Then run the following command to update user database connect option.

installutil relocateuserdb -dbset <dbset> <admin> <admin_password> <user_dbname> SQL_SERVER <AWS_SQL_Server_HOSTNAME> <user_database> <user_dbo_login> <user_dbo_password> <user_rw_login> <user_rw_password> "EXTRA_PARAMS='Encrypt=true;TrustServerCertificate=true;'"

If HCL Compass is deployed on Linux instance, the connect option should be replaced as the following.

EXTRA_PARAMS_UNIX='Encrypt=yes;TrustServerCertificate=yes;';EXTRA_PARAMS_WINDOWS='Encrypt=true;TrustServerCertificate=true;'

c) If HCL Compass is deployed on Linux instance, Add dbset with the following command and specified connect option.

prompt>./cqreg add_dbset -v ss -d <table_name > -s <AWS_SQL_server_HOSTNAME> -u <username> -p <pwd> -dbset <SQLSSL> -co "
EXTRA_PARAMS_UNIX='Encrypt=yes;TrustServerCertificate=yes;';EXTRA_PARAMS_WINDOWS='Encrypt=true;TrustServerCertificate=true;'"

5.10. SSO external server

If deploying SSO authentication server in an AWS EC2 instance, perform the following steps to open ports. After setting up SSO server following the guide, opening the port described in the following table.

Server	Ports	Protocol	Source
SSO OIDC EC2 Instance	<9447>	TCP	<IP>/<IP Block>
SSO SAML EC2 Instance	<8001>	TCP	<IP>/<IP Block>

Table 14: Inbound Rule for SSO EC2 Instance

<9447> and <8001> are the example ports for SSO OIDC server and SAML server. Port needs to be switched to the SSO authentication service provided URL which is also specified in the configuration file. For example, identify the following values in the SSO setup configuration files, ssoconfig_oidc_ex.txt or ssoconfig_saml2_ex.txt.

SSO_OIDC_IDP_URL=https://test.domain.company.com:9447/oidc/

SSO_SAML2_IDP_URL=https://www.domain.company.com:8001/isam/sps/saml20idp/saml20

<IP>/<IP Block> refers to *Table 9: <IP/IP block> Setting* Examples. It is recommend to use 10.0.0.0/8 if SSO EC2 instance IP starts with 10.

SSO can also be used to limit the access to HCL Compass Web, e.g., a non-organization Email id cannot pass the authorization. For example, if using Okta as SSO server, refer to SSO working with Okta and Okta help center to create a new access policy for HCL Compass Web.

5.11. LDAP authentication server

HCL Compass offers two methods of user authentication. You can use traditional HCL Compass authentication or use the industry standard Lightweight Directory Access Protocol (LDAP) to authenticate using an LDAP directory server. With HCL Compass authentication, a user types a username and password to log on, and HCL Compass verifies that they match a username and password stored in the HCL Compass database set (schema repository).

With LDAP authentication, a user types a username and password in the same HCL Compass login window and HCL Compass checks an LDAP directory for a matching user record. HCL Compass supports environments where multiple LDAP configurations can be used to authenticate.

HCL Compass supports the following LDAP servers that support LDAP protocol Version 3:

- IBM® Lotus® Domino® LDAP Server
- IBM Tivoli® Directory Server
- Microsoft™ Active Directory Server
- Novell eDirectory Server
- Oracle Java™ System Directory Server

AWS LDAP service is based on AWS IAM user against AWS serverless services. HCL Compass must be deployed in AWS with an EC2 instance which is a server process. So, HCL Compass does not work with AWS LDAP service. HCL Compass works with LDAP installed on an AWS EC2 instance. After the installation of LDAP server, opening the port which LDAP server is listening on. For example, if LDAP server is IBM Tivoli Directory server, use the values displayed in the following table to open port. After opening port, see the guide of setting up LDAP authentication for how to enable the LDAP authentication.

Server	Ports	Protocol	Source
LDAP EC2 Instance	<636>	TCP	<HCL_Compass_IP>/32

Table 15: Inbound Rule for LDAP EC2 Instance

<636> is the default secure port of IBM Tivoli Directory server. It is recommended to use LDAP server with SSL configured.

5.12. HCL Compass MultiSite

You can use HCL Compass MultiSite software to replicate a database across multiple sites and to update those copies of the database, also known as replicas, at scheduled intervals. HCL Compass MultiSite is mainly used to support people in different geographies and to support geographically distributed development. It is also beneficial for enhanced disaster recovery preparedness, for example synchronization between sites in AWS and on-premises. There is no difference between configuring HCL Compass MultiSite in AWS and on-premises. Since this feature was not covered during writing this white paper of HCL Compass 2.0.0, the official support of HCL Compass MultiSite in AWS will be announced in the future.

5.13. EmailRelay consideration

EmailRelay should be configured after applying EmailPlus package v2.1 into master schema. EmailPlus should be used with SMTP Relay mode because it supports authentication and SSL encryption of email transport. SMTPS (SSL) port must be opened on Email server to allow secured access from HCL Compass web server. EmailRelay runs as a service in Webshpere profile (cqwebprofile) and listens on the port configured in EmailPlus package. Open this port in the following table to allow all the clients send email request to this port. Related guide could be referred during the configuration.

Server	Ports	Protocol	Source
Compass EC2	<36001>	TCP	<IP>/<IP Block>

Table 16: Inbound Rule for Compass EC2

<IP>/<IP Block> is recommended to be setup as 10.0.0.0/8 if Compass EC2 IP is started with 10.

5.14. License server

Click the link for details on how to configure HCL Licensing. There is no difference between AWS and on-premises lab for configuring license if the EC2 instance is connected to HCL licensing server.

6. AWS Migration Considerations

6.1. HCL Compass server migration

HCL Compass 2.0.0 historical versions include HCL Traxiem and IBM Rational ClearQuest. ClearQuest has been widely deployed since last over twenty years. Official document of migration from ClearQuest to HCL Compass 2.0.0 is located here. It has a full coverage list of migration points of HCL Compass Web Server. The migration steps are not impacted by the location of source server and target server. In another words, the migration from on-premises ClearQuest to AWS HCL Compass is as same as the migration from on-premises ClearQuest to on-premises AWS HCL Compass. After migration, follow the considerations in Chapter 5 to setup HCL Compass correctly.

6.2. Database server migration

If you need to migrate on-premises Database into AWS , HCL Compass provides scripts to migrate the data. It can migrate the data between different database vendor type, such as from DB2 to Oracle. Use convertschemarepo and convertuserdb to copy master and use database into AWS RDS Oracle along with updating the connection information in the original database.

Refer here for the usage of convertschemarepo. For example, Use the following command to copy the data of dbset master schema which is located on-premises lab into the table places of to_master_dbo_login in AWS RDS Oracle.

installutil convertschemarepo -dbset <dbset> <admin> <adminpassword> ORACLE <AWS_RDS_Oracle_IP> <orcl> <master_dbo_login> <master_dbo_password> <master_rw_login> <master_rw_password> <master_ro_login> <master_ro_password> connect_options "LOB_TYPE=CLOB"

Refer here for the usage of convertuserdb. For example, Use the following command to copy the data of user database of dbset which is located on-premises lab into the table places of to_user_dbo_login in AWS RDS Oracle.

installutil convertuserdb -dbset <dbset> <admin> <adminpassword> <user_dbname > ORACLE <AWS_RDS_Oracle_IP> <orcl> <user_dbo_login> <user_dbo_password> <user_rw_login> <user_rw_password> connect_options "LOB_TYPE=CLOB"

Additionally, AWS Database Migration Service helps you migrate databases to AWS quickly and securely. After migrating the data using AWS database migration service, update the connection information in the original database with relocateschemarepo and relocateuserdb commands. Refer here for the usage of relocateschemarepo and relocateuserdb commands.

installutil relocateschemarepo -dbset <dbset > <admin> <adminpassword> ORACLE <AWS_RDS_Oracle_IP> <orcl> <master_dbo_login> <master_dbo_password> <master_rw_login> <master_rw_password> <master_ro_login> <master_ro_password> connect_options "LOB_TYPE=CLOB"

installutil relocateuserdb -dbset <dbset> <admin> <adminpassword> <user_dbname > ORACLE <AWS_RDS_Oracle_IP> <orcl> <user_dbo_login> <user_dbo_password> <user_rw_login> <user_rw_password> connect_options "LOB_TYPE=CLOB"

7. Sample Usage Scenarios

7.1. Scenario 1: HCL Compass and Database in AWS

Customer has deployed HCL Compass and database both in AWS. AWS lab and on-premises lab are connected seamlessly. On-premises end user can use HCL Compass Web successfully.

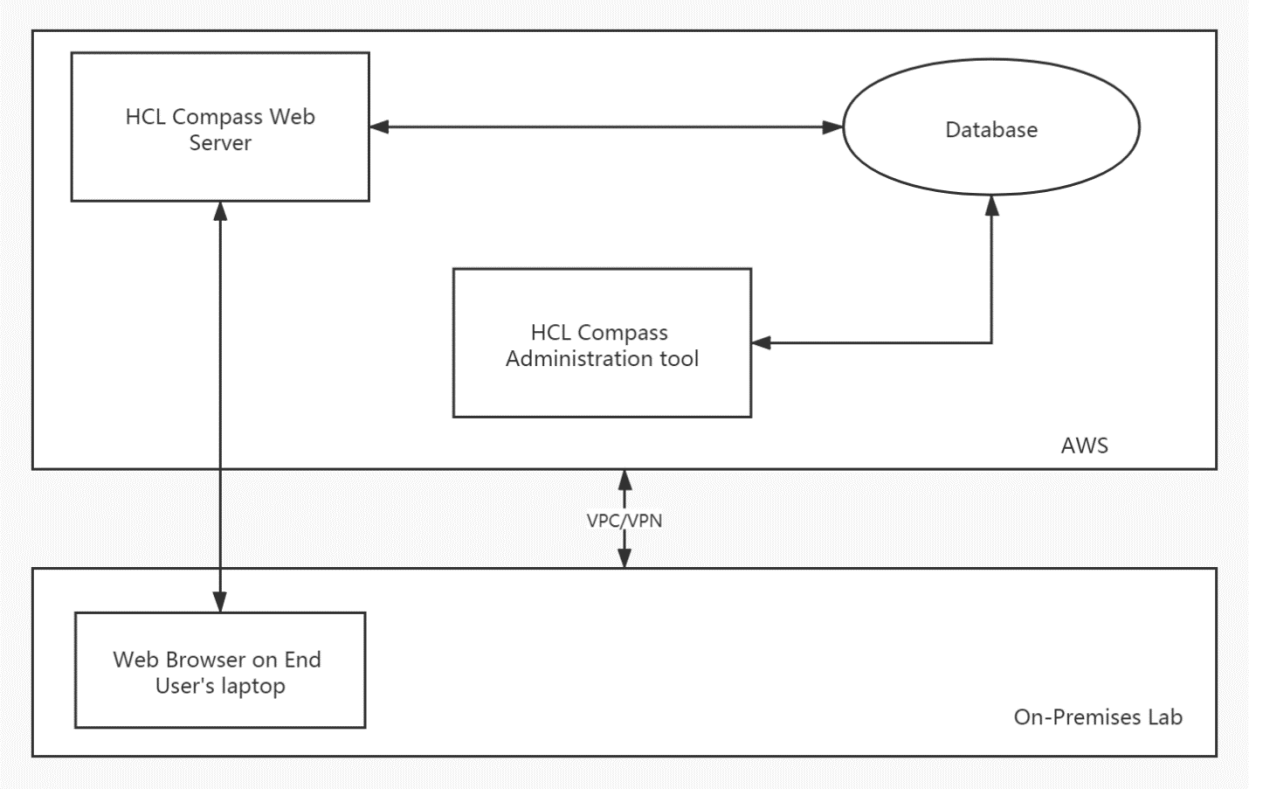


Figure 5: Scenario 1: HCL Compass and Database server in AWS

7.2. Scenario 2: HCL Compass in AWS and Database On-premises

Customer has deployed HCL Compass in AWS and database on-premises. AWS lab and on-premises lab are connected seamlessly (high bandwidth and low latency). On-premises end user can use HCL Compass web or connect to the database directly with HCL Compass Thick client. The significant difference with the scenario 1 is that the database data might get back to HCL Compass web server with longer time because of network latency. So, the scenario 2 is not recommended in productive deployment based on performance consideration if connection is not seamless.

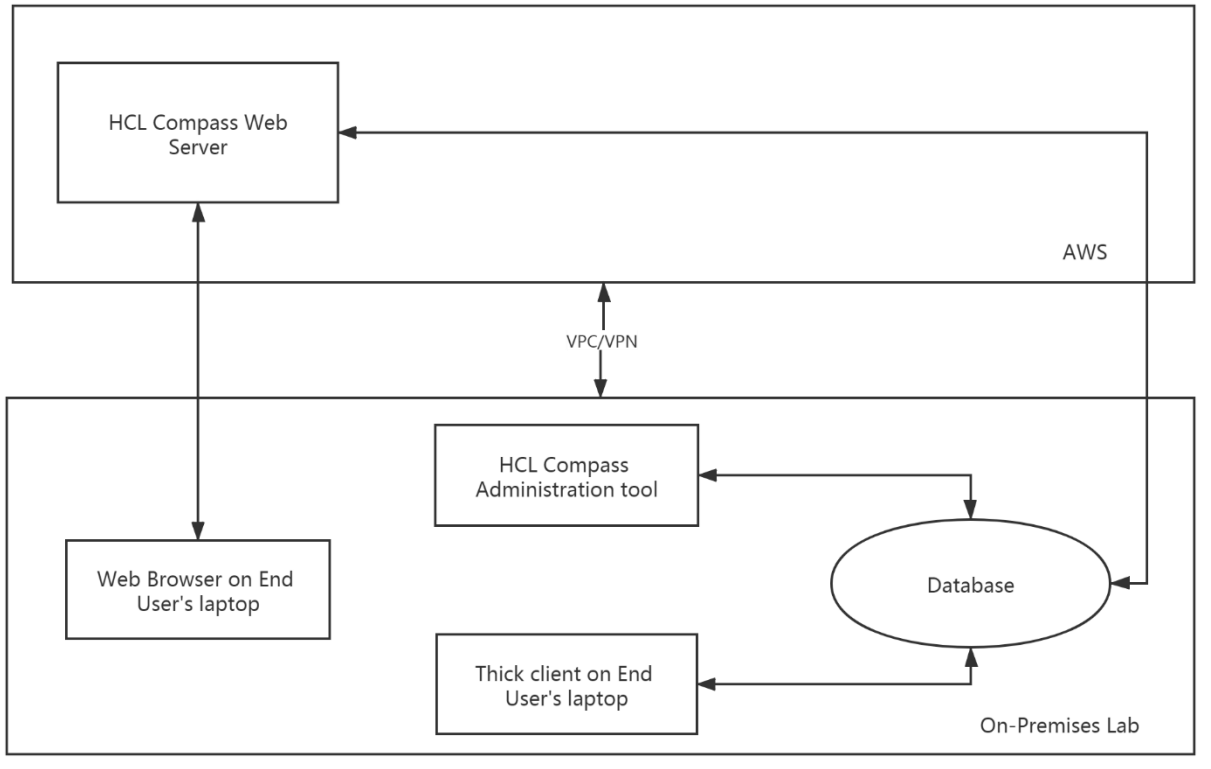


Figure 6: Scenario 2: HCL Compass in AWS and Database on-Premises

8. References and More Information

AWS Website – The main AWS website from which everything AWS related can be found.

AWS Documentation – The AWS documentation website for user guides, developer guides, etc.

General Virtualization Considerations (pt 1) – Some general things to consider when virtualizing HCL Compass (or any application).

General Virtualization Considerations (pt 2) – Some (relatively old) performance measurements for HCL Compass running in a VMWare environment.

What is Cloud Computing – AWS information on cloud computing in general.