HCL Compass in Azure

Author: Di Lin
Date: November 27, 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 Microsoft Azure cloud services helps transform your organization with the following benefits:

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

Azure provides Windows and Linux virtual machines to build and host the HCL Compass server. Both Azure VMs and HCL Compass web servers support Windows and Linux OS versions. A complete HCL Compass installation using VMs is possible in Azure.

This whitepaper provides general guidance for cloud installation and migration from on-premises ClearQuest or Compass to Azure HCL Compass. It focuses on the additional configuration points beyond usual on-premises lab deployment. These points are caused mainly by Azure VMs have special configuration other than normal OS version, e.g., NSG rules in VNet. Chapter 3 describes the advantages of Azure cloud which include cost saving, 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 Azure, and migrate to the Cloud. It includes procedure and steps for a fresh installation of HCL Compass and migration from ClearQuest to HCL Compass in Azure. The audience must be familiar with HCL Compass installation and its associated configuration and administration.

3. Reasons for deploying HCL Compass in a cloud

This section summarizes reasons for deploying HCL Compass to Azure cloud or moving an existing HCL Compass setup to Azure cloud. The benefits of migration and deployment 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. Savings examples include temperature control, physical security, maintenance services, etc. In Azure Cloud, Azure provides VMs (Virtual Machines) in data centers, host HCL Compass. There is an annotated outline of links that follows the information in the Windows virtual machines in Azure and Linux virtual machines in Azure.

3.2. Scalability

Estimating data center capacity requirements is one of the most difficult tasks. Over-estimation leads to investing capital in unnecessary capacity. Underestimation can end up degrading 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. Azure provides autoscaling, automatically increase or decrease the number of VM instances that run HCL Compass.

3.3 Availability

Azure has the resources and invests in redundant infrastructure, UPS systems, environmental controls, network carriers, power sources, etc. to ensure maximum uptime. Azure provides an easier and cheaper solution compared to an on-premises lab for recovery in the event of disaster, such as a fire or flood destroying a data center. The fast recovery of Azure VM contributes to the high availability of HCL Compass.

4. Plan Your HCL Compass Deployment or Migration in Azure

Give the clear benefits of the Azure services and products explained above, let us now discuss how you can use those capabilities to deploy HCL Compass in Azure.

Determining certain key aspects of HCL Compass deployment provides information deployment is needed to make informed decisions about the use of Azure services. The HCL Compass release note and deployment document provides more information about things you must consider. These include a description of the requirements for deployment.

4.1. HCL Compass Server (Web)

HCL Compass server (web) supported platforms include 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

Azure provides many sizes for virtual machines that can be used for VMs. The recommended type for HCL Compass is in the following table.

Type	Sizes	Description
General purpose	Dsv3, Dv3, Dasv4, Dav4, DSv2, Dv2, Dv4, Dsv4, Ddv4, Ddsv4	Balanced CPU-to-memory ratio.
Memory optimized	Esv3, Ev3, Easv4, Eav4, Ev4, Esv4, Edv4, Edsv4, Mv2, DSv2, Dv2	High memory-to-CPU ratio.

Table 2: Recommended VM type

HCL Compass server requires a minimum 8GB RAM and 80GB hard disk space. Choose the VM type based on RAM requirement according to your organization's usage model. 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. For example, If choosing Ddv4 series and consider Ddv4-series has 7 types with vCPU numbers as 2, 4, 8, 16, 32, 48, 64. Among them, Standard_D4d_v4 is a minimal requirement for HCL Compass deployment and Standard_D8d_v4 is a recommendation for HCL Compass deployment. Any VM size higher above Standard_D8d_v4 is recommended for gaining performance.

4.2. HCL Compass Supported Database Platforms

HCL Compass must use a database to store and retrieve data. The following table explains database type and version supported by HCL Compass 2.0.1. For latest platforms 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

Azure provides Azure SQL for the Azure SQL family of SQL Server database engine products in the cloud: Azure SQL Database, Azure SQL Managed Instance, and SQL Server on Azure VM. It is recommended to deploy SQL Server on an Azure VM to gain its full control. You can also choose to deploy Oracle and DB2 on an Azure VM. On-premises databases can also be used by HCL Compass hosted in Azure. See Chapter 5.6 for performance consideration if the database is on-premises.

4.3. HCL Compass full-text search

HCL Compass's 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 (cqweb) server on the same VM. Optionally you can choose to install HCL Compass full-text search feature on another VM which type can follow ***Error! Reference source not found.***. You should deploy the full-text search VM in the same sub-net of HCL Compass database in Azure to achieve a better search performance. If HCL Compass full-text search VM is in Azure, but the database is located on-premises, ensure the low network latency between the two for the best performance.

4.4. HCL Compass Clients

There are two main ways to access and manipulate HCL Compass data. One way to access the HCL Compass Web Client which relies on the 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 4: Supported Browsers

The other way is to use the eclipse based HCL Compass client to access the database directly. Azure has port control policy on NSGs, so this procedure shall not be widely used in Azure deployment.

5. Azure Deployment Considerations

Before starting the deployment of HCL Compass, set up the basic network between Azure and your on-premises lab. It must include a seamless (high bandwidth and low latency) connection between HCL Compass server and on-premises machines if applicable. Since almost all the ports on an VM are closed by default, the following discussion focuses 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 5: Pre-requisite Software

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

Table 6: Requisite database software

The base images and the licenses for HCL Compass requisite software can be obtained through HCL focal.

5.2. Windows OS

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

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

Table 7: Inbound Rule for Databases

<SSL port> means, the SSL port is configured while enabling the SSL connection on the database. The database listens on the SSL port and the connection between HCL Compass and the database is secure. For Oracle server, the SSL port is normally configured as 2484. For DB2 VM, the SSL port is the ssl_svcename configuration parameter (which can be retrieved by 'get dbm cfg' command). For Microsoft SQL Server, the SSL port is as the same as the 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 8: <IP/IP block> Setting Examples

10.134.14.38/32, which is the exact HCL Compass server IP, allows the only connection from the HCL Compass server to the port on database. No connection initiated from any other machines is not allowed.

5.3. Linux OS

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

1. Log into the Linux VM after obtaining the .pem file.
   following the related guide to log into RHEL server, ensure that "azureuser" is the username associated with that key. Following the login, enter **sudo su -** before continuing with the following operations.
2. Install the GUI related package on the HCL Compass Linux VM. Choose the 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 the system file has the correct content with the 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 Linux VM .
   If the connection fails, you may have to add the VNC port into whitelist of firewall and Azure console with the following:
   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, there is an optional configuration that turns off firewall. The following commands for stopping and disabling firewall must not be applied for the production HCL Compass web server.
      Enter **systemctl stop firewalld**
      Enter **systemctl disable firewalld**

b. In the Azure VM console of the HCL Compass Linux VM, 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 Linux VM	5901	TCP	<IP/IP block>

Table 9: Inbound Rule for HCL Compass Linux VM

<IP/IP block> refers to an IP address block and See *Table 8: <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 following sample /root/.vnc/xstartup file 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 Azure 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 VM	<12043> OR <12060>	TCP	<IP>/<IP Block>
HCL Compass VM	<12443> OR <12080>	TCP	<IP>/<IP Block>

Table 10: Inbound Rule for HCL Compass VM

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)://< Azure_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 8: <IP/IP block> Setting Examples.* It is recommended to use <administrative_machine_IP>/32.

If the database server is in Azure, to manage schema repositories and user databases, it is recommended to deploy the HCL Compass administration tool in Azure. Allow the tool to access the ports of the database specified in *Table 7: 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 will take a longer time to complete, depending on the network latency.

5.5. HCL Compass web and thick client

It is recommended that the end user access HCL Compass Web by browser.

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

Table 11: Inbound Rule for HCL Compass VM

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 8: <IP/IP block> Setting Examples.* It is recommended to use 10.0.0.0/8 if the IP of this HCL Compass VM starts with 10.

The thick (eclipse based or windows MFS based) clients are not recommended to be widely used in Azure because of Azure NSGs control. If administrator(s) want to manage HCL Compass database and schema by HCL Compass eclipse designer, maintenance tool and user administration tool, open the corresponding ports in *Table 7: Inbound Rule for Databases* from administrative machines to HCL Compass database.

5.6. Performance

Azure VMs behave efficiently during lab trial performance testing. There is no performance downgrade or performance issues observed. However, login and querying performance are impacted by the network latency between HCL Compass server and database. The login time will increase if the database is deployed on-premises lab. So, deploying the database on-premises is not recommended for performance reasons.

Azure Monitoring maximizes the availability and performance of HCL Compass in Azure by delivering a comprehensive solution for collecting, analyzing, and acting on telemetry from cloud and on-premises environments. It helps you understand how HCL Compass is performing in Azure and proactively identifies issues affecting them and the resources they depend on. Azure Network Watcher is a packet capture tool and NSG flows logs provider, to diagnose problems with traffic filtering and routing, and to monitor connections. Those two services can be used to gauge the health of the various servers and clients running in Azure. 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 relevant ports.

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

Table 12: Inbound Rule for HCL Compass and RQM VMs

The port 443 is the default port for IBM HTTP Server after configuring the web server plugin into IBM WebSphere Application server cqwebprofile. This port is recommended to be used for OSLC usage as well. 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

Azure load balancer operates at layer four of the Open Systems Interconnection (OSI) model. Load Balancer distributes inbound flows that arrive at the load balancer's front end to backend pool instances. These flows are according to configured load balancing rules and health probes. The backend pool instances can be back up HCL Compass VM in a virtual machine scale set. With Standard Load Balancer, you can scale HCL Compass with highly available services. Load balancer supports both inbound and outbound scenarios. Load balancer provides low latency and high throughput and scales up to millions of flows for all TCP and UDP packets. Contact Azure support for how to configure Azure load balancing efficiently.

If a load balancer is required between on-premises lab and Azure, IBM HTTP server simple load balancing is another option. Verify the following checklist for the load balancer to run successfully. If any issues arise during the configuration, contact WAS Support for assistance. The following steps can be applied for any servers needing configuration into the load balancer group. Assume IP1 is the IP of Azure VM 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.
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 and ensure session affinity is configured properly.
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 the 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, clear the browser cache and access https://<IP1>/cqweb. The first time, it shows the login page of IP1. Refresh to access https://<IP1>/cqweb again, now it shows 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 Azure VMs.

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

End user can access https://<Azure_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, the end user can access and log into https://<Azure_HCL_Compass_IP>/cqweb. If cqweb cannot be launched successfully, follow Configuring the web server plug-in for Secure Sockets Layer to copy the keystore and 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 the 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 SSL configuration
    a) Setup SSL configuration on Oracle server in Azure VM following Oracle related guide. If running into issue, contact your Oracle server DBA.

b) Export the certificate from wallet configured in Oracle server and transfer this certificate to Azure HCL Compass VM.

c) Install the Oracle client which is equal or higher version compared to the Azure Oracle server version. For example, if Azure Oracle has a DB engine version as oracle 18c, choose oracle client oracle 18c or 19c. Ensure Azure HCL Compass VM can access the Azure Oracle server 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 truststore.cer exported from Azure Oracle server.

   prompt>.\orapki.bat wallet add -wallet C:/Users/Administrator/Desktop/ssl_wallet -trusted_cert -cert C:/Users/Administrator/Downloads/truststore.cer -auto_login_only

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

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

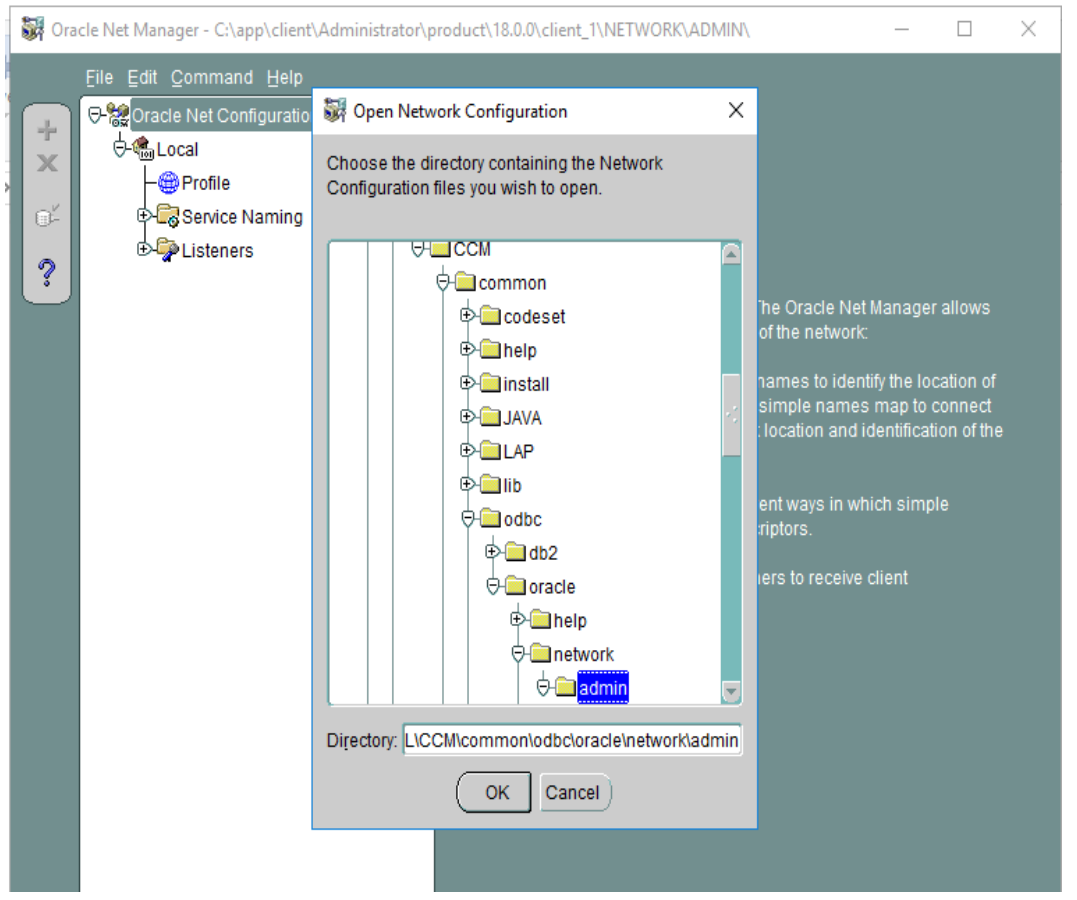

Figure 1: Select Network Configuration file

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

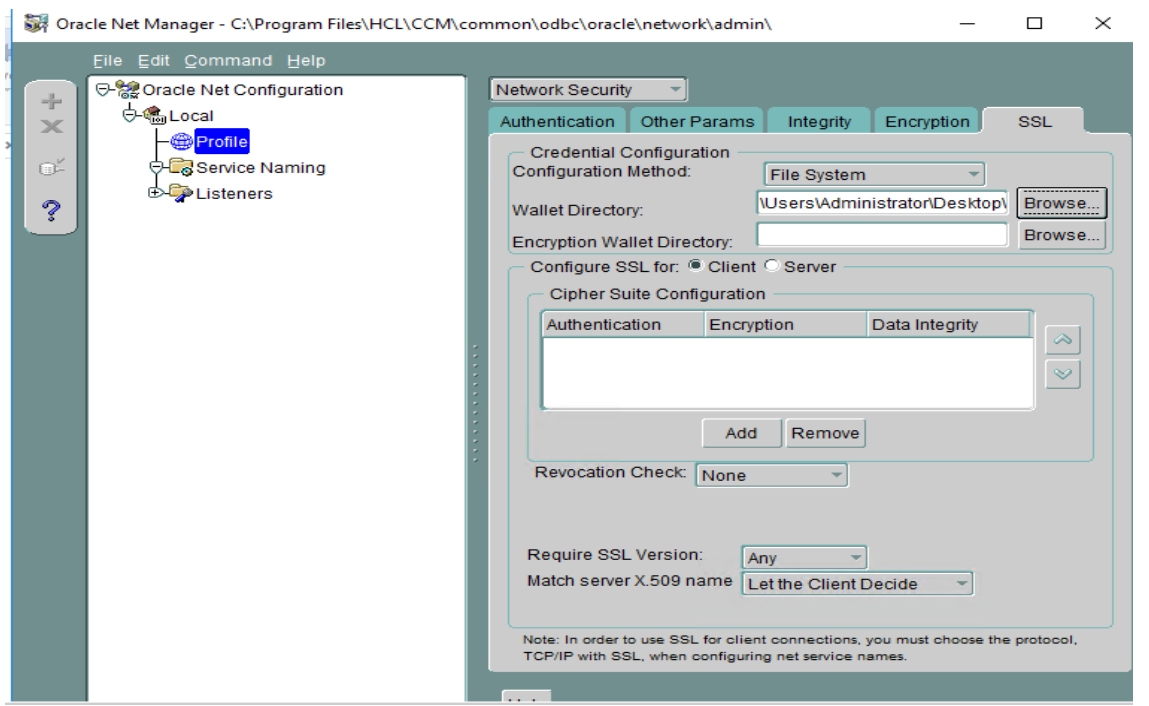

Figure 2: Input Wallet location

i) Create a service naming with net service name as <orcl>, TCP/IP with SSL, hostname of Azure Oracle server, Port Number as 2484, Service Name as <ORCL>. Service Name should be the SID setup on Azure Oracle server, and it is set to ORCL usually.

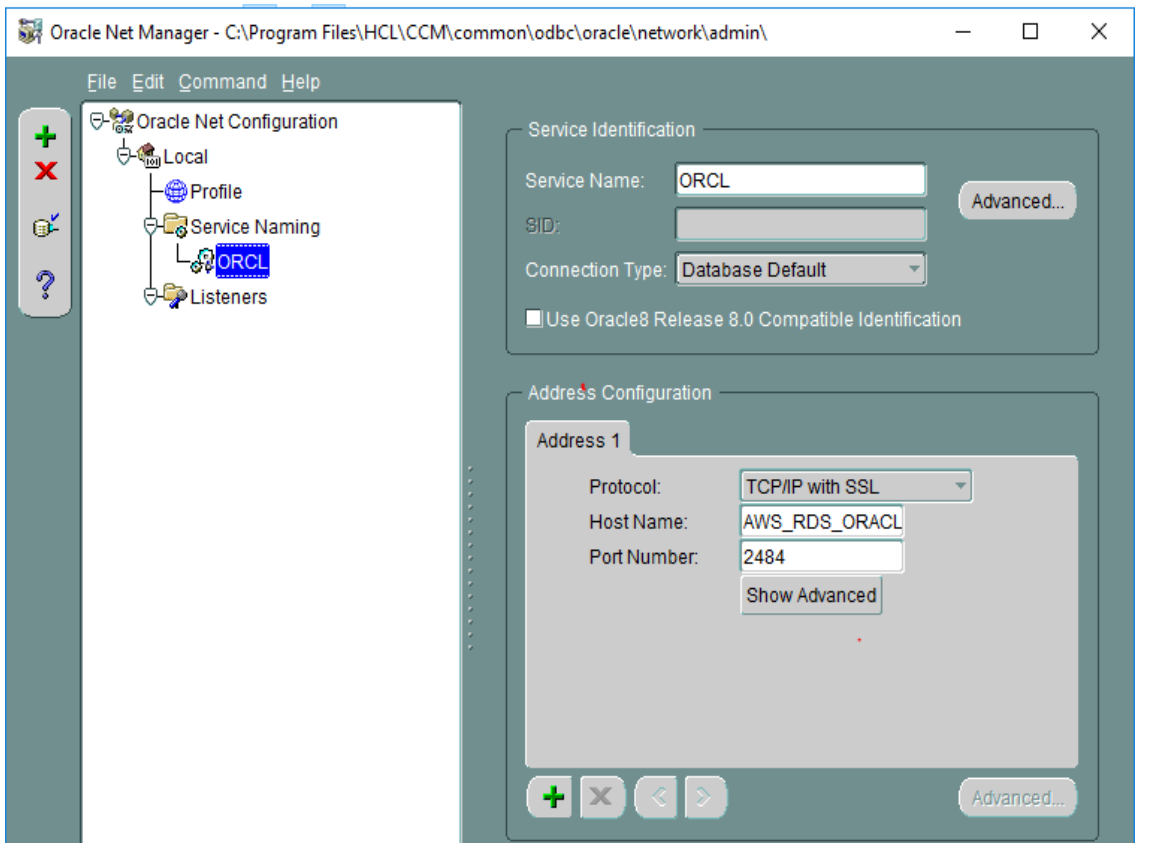

Figure 3: Create SSL orcl connection

j) Save network configuration.

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

```
installutil relocateschemarepo -dbset <dbset> <admin>
<admin_password>  ORACLE  <Azure_Oracle_Server_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 options.

```
installutil relocateuserdb -dbset <dbset> <admin> <admin_password>
<user_dbname > ORACLE <Azure_Oracle_Server_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.

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

```
Prompt>./cqreg add_dbset -v oracle -d <service_name> -s
<Azure_Oracle_VM_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 version. If running into issue, contact your DB2 DBA.

b) Create a kdb On Azure DB2 VM.

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

c) Create a self-signed certificate and pick up a supported signer algorithm. If there is an 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=Azure.com,OU=DB2,CN=<Azure_DB
2_HOSTNAME>" -size 2048 -sigalg SHA256_WITH_RSA
```

d) Update the db2 setup with kdb, sth, and the ssl port information on the Azure DB2 VM. Enter the 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 the SSL switch of Azure DB2 VM.
Enter the DB2 command window.

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

f) Restart the Azure DB2 VM.

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

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

```
installutil relocateschemarepo -dbset <dbset> <admin>
<admin_password>  DB2  <Azure_DB2_HOSTNAME>
```

<master_database> <master_dbo_login> <master_dbo_password> <master_rw_login> <master_rw_password> <master_ro_login> <master_ro_password> <connect_options>

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

installutil relocateuserdb -dbset <dbset> <admin> <admin_password> <user_dbname> DB2 <Azure_DB2_HOSTNAME> <user_database> <user_dbo_login> <user_dbo_password> <user_rw_login> <user_rw_password> <connect_options>

If HCL Compass is deployed on a Windows VM, set the connect_options with the following:

"PORT=50602;EXTRA_PARAMS='Security=SSL;SSLClientKeystoredb=C:\mydbserver.kdb;SSLClientKeystash=C:\mydbserver.sth;';"

If HCL Compass is deployed on a Linux VM, set the connect_options with 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;'"

Note:

The path of certification can be set as a UNC path which can be accessed globally by other machines without downloading the certification.

h) If HCL Compass is deployed on a Linux VM, add the dbset with the following command containing the connect options specified in step g). Ensure the certificate is shipped to the Linux VM and placed at the location specified in connect options.

prompt>./cqreg add_dbset -v db2 -d <table_name > -s <Azure_DB2_HOSTNAME> -u <username> -p <pwd> -dbset <DB2SSL> -co <connect_options>

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=<Azure_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.

c) In the command line administrative mode, run the following command to update master database connect options. 'TrustServerCertificate=true' can be skipped in production deployment to enhance security.

installutil relocateschemarepo -dbset <dbset> <admin> <admin_password> SQL_SERVER <Azure_SQL_Server_HOSTNAME> <master_database> <master_dbo_login> <master_dbo_password>

<master_rw_login> <master_rw_password> <master_ro_login> <master_ro_password> <connect_options>

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

installutil relocateuserdb -dbset <dbset> <admin> <admin_password> <user_dbname> SQL_SERVER <Azure_SQL_Server_HOSTNAME> <user_database> <user_dbo_login> <user_dbo_password> <user_rw_login> <user_rw_password> <connect_options>

If HCL Compass is deployed on a Windows VM, set the connect_options with the following:

"EXTRA_PARAMS='Encrypt=true;TrustServerCertificate=true;'"

If HCL Compass is deployed on a Linux VM, set the connect_options with the following:

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

d) If HCL Compass is deployed on a Linux VM, add the dbset with the following command containing the connect options specified in step c).

prompt>./cqreg add_dbset -v ss -d <table_name > -s <Azure_SQL_server_IP> -u <username> -p <pwd> -dbset <SQLSSL> -co <connect_options>

5.10. SSO external server

If deploying a SSO authentication server in an Azure VM, do the following steps to open ports. After setting up SSO server, follow the guide and open the port described in the following table.

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

Table 4: Inbound Rule for SSO VM

<9447> and <8001> are the example ports for SSO OIDC server and SAML server. The 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 8: <IP/IP block> Setting Examples.* It is recommended to use 10.0.0.0/8 if SSO VM IP starts with 10.

SSO can also be used to limit the access to HCL Compass Web, e.g., a non-organization Email id fails 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 the industry standard Lightweight Directory Access Protocol (LDAP) to authenticate through an LDAP directory server. With the native application authentication, a user types a username and password to log on, and HCL Compass verifies that this matches 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

Azure Active Directory Domain Services provides managed domain services such as domain join, group policy, lightweight directory access protocol (LDAP), and Kerberos / NTLM authentication. Setup and configure secure the LDAP for an Azure Active Directory Domain Services managed domain which HCL Compass VM residents. Then open the port on which the LDAP VM is listening as the following table. After opening the port, see the guide of setting up LDAP authentication enabling the LDAP authentication.

Server	Ports	Protocol	Source
Secure LDAP external IP	<636>	TCP	<HCL_Compass_IP>/32

Table 14: Inbound Rule for LDAP VM

<636> is the default secure port of secure LDAP service. 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 Azure and on-premises. There is no difference between configuring HCL Compass MultiSite in Azure and on-premises. Since this feature was not covered

during authoring of this white paper, official support of HCL Compass MultiSite in Azure will be announced in the future.

5.13. EmailRelay consideration

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

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

Table 15: Inbound Rule for Compass VM

<IP>/<IP Block> is recommended to be setup as 10.0.0.0/8 if Compass VM 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 Azure and on-premises lab for configuring license if the VM is connected to HCL licensing server.

6. Azure Migration Considerations

6.1. HCL Compass server migration

HCL Compass is the next generation of IBM Rational ClearQuest. ClearQuest has been widely deployed since last over twenty years. Official document of migration from ClearQuest to HCL Compass 2.0.1 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 Azure HCL Compass is as same as the migration from on-premises ClearQuest to on-premises Azure 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 Azure, 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 Azure Oracle server 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 Azure Oracle server.

installutil convertschemarepo -dbset <dbset> <admin> <adminpassword> ORACLE <Azure_Oracle_Server_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 Azure Oracle server.

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

Additionally, Azure Database Migration Service helps you migrate databases to Azure quickly and securely. After migrating the data using Azure 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 <Azure_Oracle_Server_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 <Azure_Oracle_Server_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 Azure

The customer has deployed HCL Compass and its database both in Azure. Azure lab and on-premises lab are connected seamlessly. The on-premises end user can use HCL Compass Web successfully.

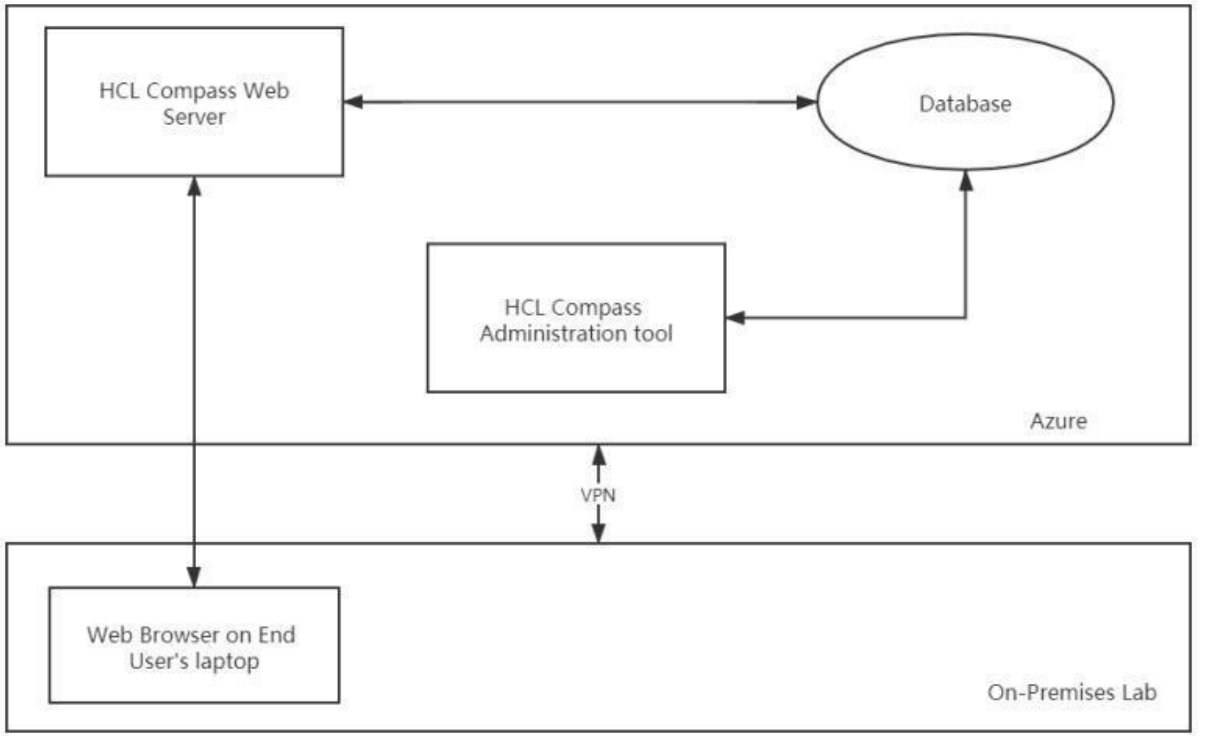

Figure 4: Scenario 1: HCL Compass and Database server in Azure

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

The customer has deployed HCL Compass in Azure and the database on-premises. Azure lab and on-premises lab are connected seamlessly (high bandwidth and low latency). The 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 communicate more slowly with HCL Compass web server because of network latency. So, the scenario 2 is not recommended in production based on performance.

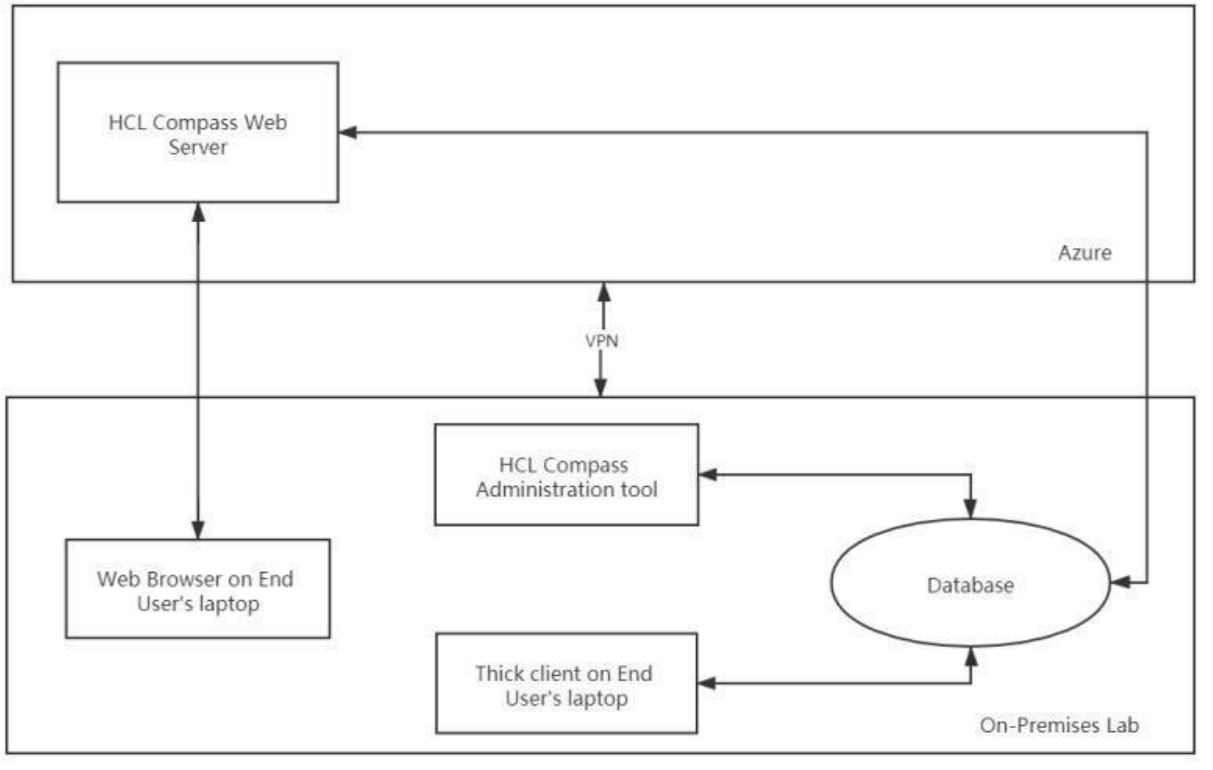

Figure 5: Scenario 2: HCL Compass in AZURE and Database on-Premises

8. References and More Information

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

Azure Documentation – The Azure 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 – Azure information on cloud computing in general.