Agilent

Agilent OpenLab Server and OpenLab ECM XT Scalable System

Installation Guide

Notices

Document Identification

DocNo D0013948
May 2022

Copyright

Agilent Technologies, Inc.
5301 Stevens Creek Blvd.
Santa Clara, CA 95051

Software Revision

This guide is valid for the 2.7 revision of Agilent OpenLab Server and OpenLab ECM XT until superseded.

Warranty

The material contained in this document is provided "as is," and is subject to being changed, without notice, in future editions. Further, to the maximum extent permitted by applicable law, Agilent disclaims all warranties, either express or implied, with regard to this manual and any information contained herein, including but not limited to the implied warranties of merchantability and fitness for a particular purpose. Agilent shall not be liable for errors or for incidental or consequential damages in connection with the furnishing, use, or performance of this document or of any information contained herein. Should Agilent and the user have a separate written agreement with warranty terms covering the material in this document that conflict with these terms, the warranty terms in the separate agreement shall control.

Technology Licenses

The hardware and/or software described in this document are furnished under a license and may be used or copied only in accordance with the terms of such license.

Restricted Rights Legend

U.S. Government Restricted Rights. Software and technical data rights granted to the federal government include only those rights customarily provided to end user customers. Agilent provides this customary commercial license in Software and technical data pursuant to FAR 12.211 (Technical Data) and 12.212 (Computer Software) and, for the Department of Defense, DFARS 252.227-7015 (Technical Data - Commercial Items) and DFARS 227.7202-3 (Rights in Commercial Computer Software or Computer Software Documentation).

Safety Notices

CAUTION

A **CAUTION** notice denotes a hazard. It calls attention to an operating procedure, practice, or the like that, if not correctly performed or adhered to, could result in damage to the product or loss of important data. Do not proceed beyond a **CAUTION** notice until the indicated conditions are fully understood and met.

WARNING

A WARNING notice denotes a hazard. It calls attention to an operating procedure, practice, or the like that, if not correctly performed or adhered to, could result in personal injury or death. Do not proceed beyond a WARNING notice until the indicated conditions are fully understood and met.

Content

1 Installation Workflow

The following chart summarizes the installation workflow for a scalable installation.

Step	Substeps/Notes
1 **"Prerequisite Systems Setup"** on page 7	**a** Install database server **b** Set up file server **c** Set up shared internal certificate folder/directory **d** Install and configure load balancer
2 **"Install the OpenLab Server/ECM XT server"** on page 13 **a** Install primary OpenLab Server/ECM XT server **b** Install second and third OpenLab Server/ECM XT servers.	**a** Installer Step 1 **b** Installer Step 2 **c** Installer Step 3 **d** Shared certificate setup **e** Installer Step 4 **f** Update properties and config file **g** Tune AlfrescoTomcat JVM **h** Configure in Control Panel
3 **"Install and configure the OpenLab Index server"** on page 16	**a** Installer Step 1 **b** Installer Step 2 **c** Installer Step 3 **d** Installer Step 4 **e** Tune AlfrescoTomcat JVM **f** Disable OpenLab Shared Services **g** Reboot
4 **"Configure a Virtual FQDN as the Content Management storage location"** on page 17	
5 **"Bring up the Scalable System"** on page 19	
6 **"Configure Redundant License Servers for the Scalable System"** on page 20	
7 Install AICs	See CDS documentation.
8 Install Clients	See CDS documentation.

2 Install and Configure a New System

To confirm that you have the correct hardware and software to support your chosen system, review the *Agilent OpenLab Server and OpenLab ECM XT Hardware and Software Requirements Guide*. You can open this document from the Planning page of the OpenLab Server/ECM XT Installer (setup.exe). It is also located in the documentation folder on the installation media at setup\docs\EN. Localized versions are available on SubscribeNet.

To configure an existing system, see **"Reconfigure an Existing OpenLab Server/ECM XT System"** on page 25.

To configure a remote database server, see the section "Configuring a Remote Database Server" in the OpenLab Server and OpenLab ECM XT Installation Guide.

Prerequisite Systems Setup

To configure an OpenLab Server/ECM XT scalable system, install these servers: OpenLab Server/ECM XT servers, OpenLab Index Server, Database server, and Windows file server or NAS. In addition, the load balancer must be prepared.

The following information is required before doing the server setup:

- **A Windows domain user**: Used as the service account for OpenLab Server/ECM XT servers and the OpenLab Index server in the scalable system. This user must be a member of the local administrators group for each OpenLab server and must be assigned the “Log on as a Service” permission on each OpenLab server.
- **A Windows domain user**: Used as user for OpenLab Server/ECM XT installation. This user must be a member of local administrators group for all OpenLab servers. It could be the same user as the service account or a different user.
- **Virtual IP address**: IP for the scalable Content Management system.
- **Virtual FQDN**: Fully qualified domain name for the scalable Content Management system that is assigned to the Virtual IP address.
- **Virtual FQDN SSL certificate**: A SSL certificate issued to the **Virtual FQDN** of the load balancer enabling trusted communication via port 443. Please see your load balancer manual on how to request and install a SSL certificate. You can request the SSL certificate from commercial vendors or your company’s Certificate Authority/Private Key infrastructure.
- **ICMP**: All OpenLab servers must permit inbound ping requests from any other server of the Scalable System.

Database Server

Please follow the instructions in the installation guide for the Database server installation.

After the database server is installed, it must be configured to allow the remote access from the OpenLab Server/ECM XT servers and the Index server.

1. Open the database connection port in Windows Firewall to allow the access from the OpenLab Server/ECM XT servers and the Index server.
2. Configure the Database server to allow the remote access request from the OpenLab Server/ECM XT servers and Index Server.
3. If there are many instruments, tune the maximum concurrent processes allowed. Use **Table 1** for the Agilent recommended value of a system to support 300 logical instruments.

Table 1. Maximum concurrent processes value set to support 300 logical instruments

Database server type	Maximum concurrent processes
Oracle	600
PostgreSQL	400
Microsoft	Default value

Set up the shared storage in Windows file server

A shared storage is set for keeping OpenLab Server/ECM XT content. The shared storage is secured by only allowing access from the planned Windows domain user, which is the service account for the OpenLab Server/ECM XT servers and the Index server.

To set a shared storage folder on the Server:

1. Log into the Windows file server as the Windows domain user, who is the member of the local administrators group.
2. Create a shared storage folder.
3. Right-click the shared storage folder and select **Properties**.
4. Select the **Sharing** tab.
5. Click **Share**.

6 Add the planned windows domain user account (the service account) and give Read/Write permission.
7 Open **Server Manager**.
8 Select **File and Storage Services > Shares**.
9 Right-click the shared storage set and select **Properties**.
10 Select **Settings**.
11 Select **Enable access-based enumeration**.
12 Uncheck **Allow caching of share**.
13 Click **OK**.

The file server can be set on different operating systems or on a NAS that supports storage sharing using SMB protocol.

Set up shared internal certificate store in Windows file server

A shared internal certificate store is used for keeping OpenLab Server/ECM XT internal certificates. The shared store is secured by allowing only the access (both read and write permission) from the planned Windows domain user, which is the service account for the OpenLab Server/ECM XT servers, the Index server, and possibly the Windows domain user who runs the installation.

To set a shared internal certificate store on the Server:

1 Log into the Windows file server as the Windows domain user, who is the member of the local administrators group.
2 Create a shared internal certificate store folder.
3 Right-click the shared storage folder and select **Properties**.
4 Select the **Sharing** tab.
5 Click **Share**.
6 Add the planned Windows domain user account (the service account) and the planned Windows domain user account (the user who runs the installation), give both accounts the Read/Write permission.
7 Open **Server Manager**.
8 Select **File and Storage Services > Shares**.
9 Right-click the shared internal certificate store folder and select **Properties**.

10 Select **Settings**.

11 Select **Enable access-based enumeration**.

12 Uncheck **Allow caching of share**.

13 Click **OK**.

Configure the load balancer

The load balancer can be either a hardware load balancer or a software load balancer that has IP and path-based routing load-balancing capabilities and supports session persistence. It needs to be physically located in the same subnet as the OpenLab Server/ECM XT servers and needs to connect to the same network switch as where the OpenLab Server/ECM XT servers are connected.

Configure the load balancer to distribute the traffic from OpenLab AICs or OpenLab clients to the OpenLab Server/ECM XT servers.

Depending on your load balancer manufacturer, wildcard characters (*) may be required to forward all traffic containing the path */openlab/* to the primary OpenLab Server/ECM XT server. **Table 2** provides the recommended configurations including * as a wildcard.

NOTE

If you are using an Nginx Load Balancer, see **"Appendix A: Installation and Configuration of Nginx Load Balancer"** on page 36 for additional information on how to install and configure it.

Table 2. Recommended configuration in load balancer

Service name	Port/Paths	Service type	Virtual IP	Configuration	Distribute traffic to
FTP	21	Layer7-FTP	Virtual IP of the scalable CM system	FTP PASV port range: 11100-11150 Session timeout: 0 (never timeout) Enable Keepalive Probes: Yes	All OpenLab Server/ECM XT servers. Only needed if FTP is active on the individual server
HTTPS	443	Layer7-HTTPS	Virtual IP of the scalable CM system	Path-based routing port Persistence: Client IP Session timeout: 0 (never timeout) Enable Keepalive Probes: Yes SSL Offloading/ Acceleration: Select the signed Load Balancer certificate SSL Termination/ Reencryption: Yes	Configure path-based/URL-based routes for this port.
OLSS	/Agilent/OpenLab/* /openlab/* /testservices/*	Path-based routing/URL-based routing	N/A	Activate "Ignore case sensitivity"	Primary OpenLab Server/ECM XT server
Content Management	/*	Path-based routing/URL-based routing	N/A	Persistence: Client IP Persistence Time: 1 day Session timeout: 0 (never timeout) Enable Keepalive Probes: Yes	All OpenLab Server/ECM XT servers
OLSS-RESTServices	6625	TCP-Proxy	Virtual IP of the scalable CM system	Session timeout: 0 (never time out) Enable Keepalive Probes: Yes	Primary OpenLab Server/ECM XT server
OLSS-License	6570	TCP-Proxy	Virtual IP of the scalable CM system	Session timeout: 0 (never time out) Enable Keepalive Probes: Yes	Primary OpenLab Server/ECM XT server

Table 2. Recommended configuration in load balancer

Service name	Port/Paths	Service type	Virtual IP	Configuration	Distribute traffic to
OLSS-License1	8090, 8098, 8099	TCP-Proxy	Virtual IP of the scalable CM system	Session timeout: 0 (never time out) Enable Keepalive Probes: Yes	Primary OpenLab Server/ECM XT server
OLSS-License2	one port of 27000–27009 (Default: 27009)	TCP-Proxy	Virtual IP of the scalable CM system	Session timeout: 0 (never time out) Enable Keepalive Probes: Yes	Primary OpenLab Server/ECM XT server

NOTE

All previous configurations are based on the Nginx version 1.20.2 software load balancer. The configurations can be used for both hardware and software load balancers. Please adjust the settings based on your load balancer.

For server monitoring or health check, configure the load balancer to perform health check using the following HTTPS URL:

https://<server>/alfresco/s/api/healthCheck?format=html.

The health check will return Status code 200 if successful. Certain load balancers/proxies may require additional pattern checking in the HTTP response. Please specify '<body>200</body>' as the pattern to be checked.

Installation and Configuration of OpenLab Servers in the Scalable System

Each OpenLab Server/ECM XT server in the scalable system must be part of the same Windows domain. These servers have the same hardware configuration and are installed with same configuration.

NOTE

The following installation procedure is given with the default installation folder **C:\Program Files (x86)\Agilent Technologies**.

Install the OpenLab Server/ECM XT server

Use the OpenLab Installer to install the three OpenLab Server/ECM XT servers required as part of the scalable system.

1. Run the Installer Step 1, and follow the instructions to install all prerequisite software.
2. Run the Installer Step 2:
   - If installing the first OpenLab Server/ECM XT server, choose the remote Database server, and select **Create new database for Server/ECM XT**. Follow the instructions to finish this step. Record the information that you set in this step.
   - If installing a second or third server with PostgreSQL database, continue to step 3. Otherwise, choose the remote Database server, and select **Connect to existing database**. Record the information that you set in this step.
3. Run the Installer Step 3, and follow the instructions to install the OpenLab software components.

4 Execute the PowerShell script **config-cluster.ps1** in the "C:\Program Files (x86)\Agilent Technologies\Certificate Service\Bin" folder from each OpenLab Server/ECM XT server using the UNC path of the shared internal certificate store:

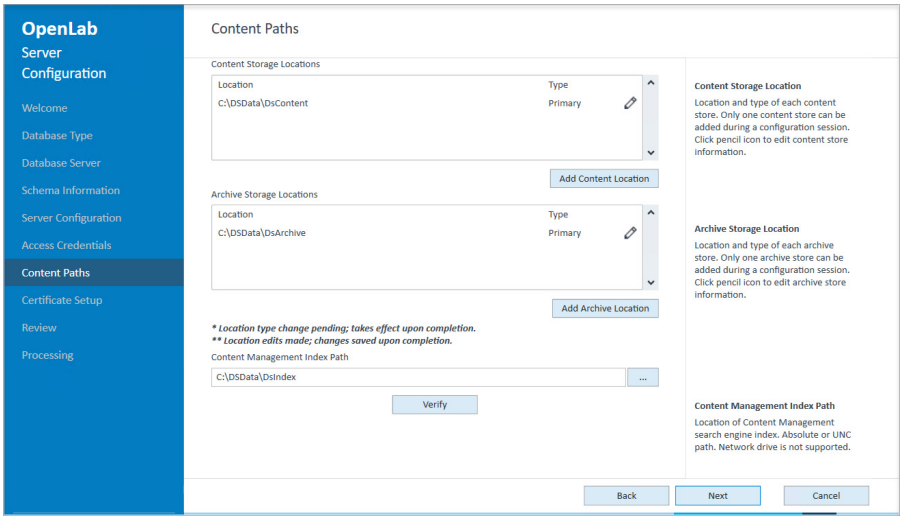
a
```
>cd "C:\Program Files (x86)\Agilent Technologies\Certificate Service\Bin"
```

b
```
>./config-cluster.ps1
-shareName "\\FileServer\SharedCertificateStore"
-serviceAccountName "domain\ServiceUserName"
-serviceAccountPassword "ServiceUserPassword"
```

Once the command runs successfully, data will be generated in the shared internal certificate store and corresponding services will be restarted.

5 Run the Installer Step 4, and follow the instructions to finish the configuration.

- On the **Server Configuration** screen, select **Content Management only**.
- On the **Access Credential** screen, use the planned Windows domain user as the service account.
- On the **Content Paths** screen,
  - Edit the content storage location to use the UNC path of the shared storage location for the Content Storage Locations.
  - Use the fully qualified domain name of the Index server as the Index host name. The Index Server Computer must be running, and ICMP Echo Request must be allowed.
  - Edit the archive storage location to use the UNC path of the shared storage location for the Archive Storage Locations.



6 If you are installing an ECM XT system, add a new aos.baseUrlOverwrite property to the C:\Program Files (x86)\Agilent Technologies\OpenLAB Data Store\tomcat\shared\classes\alfresco-global.properties file. See the following example and replace <fully-qualified-domain-name> with the fully qualified domain name of your load balancer.

   aos.baseUrlOverwrite=https://<Virtual FQDN>/alfresco/aos

   This will ensure that the "Edit in Microsoft Office" link in Content Management uses the load balancer's fully qualified domain name when accessing Office documents.

7 Using the administrative notepad, open “C:\Program Files (x86)\Agilent Technologies\OpenLAB Data Store\tomcat\shared\classes\alfresco\web-extension\share-config-custom.xml” and add |https://<Virtual FQDN>.* as the last entry to assertReferer and assertOrigin sections. See **“Allow load balancer’s URL to work with OpenLab Server/ECM XT Server”** on page 22.

8 Update the memory required by the AlfrescoTomcat JVM per the instructions in the *Agilent OpenLab Server/ECM XT Installation Guide*. For example, for an OpenLab Server/ECM XT server with 24 GB memory, set the JVM size to 16g.

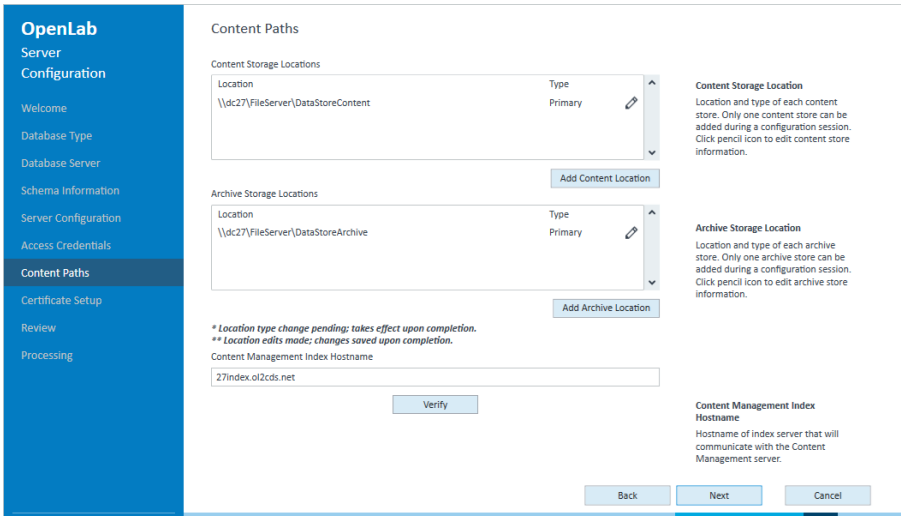
9 Open OpenLab Control Panel and change the default password.

10 Repeat **step 1**–**step 8** for each OpenLab Server/ECM XT server.

Install and configure the OpenLab Index server

To add an OpenLab Index Server to the scalable system, perform the following steps using the OpenLab Installer.

1. Run the Installer Step 1, and follow the instructions to install all prerequisite software.
2. If using a PostgreSQL database, continue to step 3. Otherwise, run the Installer Step 2. Choose the remote Database server, and select **Connect to existing database**. Follow the instructions to finish this step. Record the information that you set in this step.
3. Run the Installer Step 3, and follow the instructions to install OpenLab software components.
4. Run the Installer Step 4, and follow the instructions to finish the configuration.
   - On the **Server Configuration** screen, select **Index and Search only**. Enter the FQDN of the primary OpenLab Server/ECM XT server and verify the connection.
   - On the **Access Credential** screen, use the planned Windows domain user as the service account.
   - On the **Content Paths** screen,
     - Edit the content storage location to use the UNC path of the shared storage location for the Content Storage Locations.
     - Use the local drive of the OpenLab Index server for the Content Management Index Path.
     - Edit the archive storage location to use the UNC path of the shared storage location for the Archive Storage Locations.



5 On the **Certificate Setup** screen, select **Use internal certificate from Content Management host**.

6 Update the memory required by AlfrescoTomcat JVM and the SearchService JVM per the OpenLab Server/ECM XT installation guide. For example, for an OpenLab Index server with 32 GB memory, set the JVM for the Search Service to 16g. Set the AlfrescoTomcat JVM to 8g.

7 Stop and disable the OpenLab Shared Services service from Windows Services.

Configure a Virtual FQDN as the Content Management storage location

In the scalable system topology, there is one primary OpenLab Server/ECM XT server, which was already designated during the OpenLab Index server and load balancer setup.

1 Log into the primary **OpenLab Server/ECM XT** server.

2 Open the **OpenLab Control Panel**.

3 Select **System Configuration > Edit System Settings**.

4 Select **Content Management** for the storage location.

5 Select **Change Server**.

6 Put the Virtual FQDN (typically, the configured FQDN of the load balancer) for the OpenLab Server/ECM XT scalable system as the only Content Management server URL: https://<Virtual FQDN>.

7 Select **Activate**. An information window stating that Content Management successfully activated pops up.

8 Select **OK**.

9 Select **Next**.

10 Select **Apply**, and then **OK** to change the system configuration.

All servers in the scalable system must be restarted. See the steps in **"Bring up the Scalable System"** on page 19.

Bring up the Scalable System

To bring up the scalable system, perform the following steps:

1. Shut down the **Index Server** and all the **OpenLab Server/ECM XT** servers.
2. Reboot the OpenLab Server/ECM XT servers in the following order:
   - **a** Primary OpenLab Server/ECM XT server
   - **b** Second OpenLab Server/ECM XT server
   - **c** Third OpenLab Server/ECM XT server
   - **d** Index Server
3. Wait for a few minutes, then check **Repository Server Clustering** in the OpenLab Server/ECM XT Admin Console. All OpenLab Server/ECM XT servers should be listed as cluster members.

   The Index Server will be listed as "Connected Non-clustered Server."

NOTE

When starting up a scalable environment, start the nodes in a scalable system in a rolling start, such that each node is fully started before the next is started. This prevents any resource/load concurrency conflicts.

Configure Redundant License Servers for the Scalable System

To provide licensing redundancy, the three OpenLab Server/ECM XT servers will act as license servers. The application only supports three redundant license servers.

Obtain MAC addresses

Using the Get MAC Address tool, gather the MAC addresses for each of the three OpenLab Server/ECM XT server machines.

Generate license files

- Enter the three server names and MAC addresses into SubscribeNet, and generate a license file for the three servers.
- View the license file to verify that port 27009 is specified for each of the three servers.

Configure servers for licensing

For each of the three OpenLab Server/ECM XT servers in the system:

1. Copy the license file into **C:\Program Files (x86)\Agilent Technologies\OpenLab Services\Licensing\Flexera\licenses\AGTOL**.
2. Copy the **C:\Program Files (x86)\Agilent Technologies\OpenLab Services\Licensing\Flexera\conf\server.xml.cluster** file to the Desktop.
3. On the Desktop, rename **server.xml.cluster** to **server.xml**.

4 Edit the server.xml file on the Desktop. Find the following and change the server names from *server1, server2,* and *server3* to the names of servers in the scalable system. Default port numbers are shown. The port you designate should match the port defined in the load balancer.

```
<redundantGroup primaryIsMaster="false" timeout="0">
  <member hostName="server1" port="27009"/>
  <member hostName="server2" port="27009"/>
  <member hostName="server3" port="27009"/>
</redundantGroup>
```

5 In **C:\Program Files (x86)\Agilent Technologies\OpenLab Services\Licensing\Flexera\conf**, rename **server.xml** to **server.xml.single**.

6 Copy the **server.xml** file from the Desktop to **C:\Program Files (x86)\Agilent Technologies\OpenLab Services\Licensing\Flexera\conf**.

NOTE

For licensing to function correctly and the license servers to work, all three Agilent OpenLab License Server services must be running simultaneously at least once after startup. In a failover situation, at least two of the three Agilent OpenLab License Server services must be running.

Configure licensing in OpenLab Control Panel

To configure licensing in Control Panel:

1 Open OpenLab Control Panel on the primary OpenLab Server/ECM XT server.

2 Select **Administration** > **Licenses** > **Change Server**.

3 Enter the names of the three servers in your system, separated by semicolons (;).

4 Click **Ping** to verify that the names are entered correct, and click **OK**.

5 Verify that the names of the three servers in your system are shown in the main view for Licenses. Separate the server names by semicolons.

6 Restart the Scalable System

Allow load balancer's URL to work with OpenLab Server/ECM XT Server

There is a Cross-Site Request Forgery (CSRF) Filter that protects the OpenLab Server/ECM XT server against CSRF security attacks. Under default installation, the CSRF Filter setting is found inside C:\Program Files (x86)\Agilent Technologies\OpenLAB Data Store\tomcat\shared\classes\alfresco\web-extension\share-config-custom.xml.

CAUTION

Running Step 4 sets all settings in the share-config-custom.xml file to default values. If you manually update the share-config-custom.xml file, you must apply the changes again after you run Step 4.

For security reasons, by default, the installation will only allow URLs of localhost or local server name as referrer or origin to access OpenLab Server/ECM XT server. The following is an example of a CSRF Filter setting where you can see one list for the allowed referrers and another list for the allowed origins including the <Virtual FQDN>. The URLs are separated by pipes "|" and each URL has a version for HTTP and HTTPS:

```
<config evaluator="string-compare" condition="CSRFPolicy"
replace="true">
  <filter>
    <rule>
      <action name="assertReferer">
        <param name="referer">https://localhost/.*|http://
        localhost/.*|http://your-local-server-name.*
        |https://your-local-server-name.*|https://<Virtual FQDN>.*
        </param>
      </action>
      <action name="assertOrigin">
        <param name="origin">https://localhost|http://
        localhost|http://your-local-server-name.*
        |https://your-local-server-name.*|https://<Virtual FQDN>.*
        </param>
      </action>
    </rule>
  </filter>
</config
```

To allow the load balancer's URL to work with the OpenLab Server/ECM XT server, use this procedure.

1 Check if the list of URLs contains **|https://<Virtual FQDN>.***.

If not, add them to the end of the existing URLs.

If yes, check if they are correct. For example, in a cloud environment such as AWS, you may need to add **aws.yourdoman.net** to the URLs so they become **your-loadbalancer-fqdn.aws.yourdomain.net**. Make sure the URLs are separated by pipes "|" (see the previous example).

Do not delete other existing URLs. Make sure you include the dot asterisk regular expression pattern (.*) after your URLs to also allow any URLs that contain any trailing characters zero or more times following the load balancer's fully qualified domain name (FQDN).

2 Repeat the previous step for each OpenLab Server/ECM XT server in your scalable system cluster. You will need to restart Alfresco Tomcat for your change to take effect. These steps are not required for the Index server as it is not accessed by the load balancer.

3 The configuration from step 1 will be overwritten each time the Configuration Utility is carried out to apply changes to the server. Make sure to create a backup of your server's share-config-custom.xml file in advance.

3 Secure the System

The Scalable System is already secured by the Load Balancer configuration using SSL certificate for port 443 communication.

4 Reconfigure an Existing OpenLab Server/ECM XT System

Reconfiguring an existing OpenLab Server/ECM XT system to expand to a scalable topology involves many of the same steps as installing a new scalable system. This section outlines the steps needed to reconfigure an existing OpenLab Server/ECM XT system to become an OpenLab scalable system.

1. Setup a load balancer according to **"Configure the load balancer"** on page 10.
2. Stop all Agilent OpenLab Services on the existing OpenLab Server/ECM XT server.
3. Install a Database server, if one does not exist. Follow the steps in **"Database Server"** on page 8.
4. Migrate the existing DataStore and SharedServices databases to the new database server.
5. Set up a File server, if one does not exist. Follow the steps in **"Set up the shared storage in Windows file server"** on page 8.
6. Migrate the existing DataStoreContent and DataStoreArchive to the File server.
7. Execute the PowerShell script **config-cluster.ps1** in the "C:\Program Files (x86)\Agilent Technologies\Certificate Service\Bin" folder from the existing OpenLab Server/ECM XT server using the UNC path of the shared internal certificate store:

   a. `>cd "C:\Program Files (x86)\Agilent Technologies\Certificate Service\Bin"`

   b. `>./config-cluster.ps1 -shareName "\\FileServer\SharedCertificateStore" -serviceAccountName "domain\ServiceUserName" -serviceAccountPassword "ServiceUserPassword"`

   Once the command runs successfully, data will be generated in the shared internal certificate store and corresponding services will be restarted.
8. Reconfigure the existing OpenLab Server/ECM XT server to be a Content Management only server.
   a. Run the OpenLab Server Configuration Utility.
   b. Reconfigure the server.

- On the **Server Configuration** screen, select **Content Management only**.
- On the **Content Paths** screen,
  - Edit the content storage location to use the UNC path of the shared storage location for the Content Management path.
  - Use the Fully Qualified Domain Name of the Index server as the Index host name.
  - Edit the archive storage location to use the UNC path of the shared storage location for the Archive Storage Locations.
- On the **Certificate Setup** screen, select to use the Agilent OpenLab internal certificate.
- Using the administrative notepad, open "C:\Program Files (x86)\Agilent Technologies\OpenLAB Data Store\tomcat\shared\classes\alfresco\web-extension\share-config-custom.xml" and add |https://<Virtual FQDN>.* as the last entry to assertReferer and assertOrigin sections. See **"Allow load balancer's URL to work with OpenLab Server/ECM XT Server"** on page 22.

9 Install two new OpenLab Server/ECM XT servers using the steps in **"Install the OpenLab Server/ECM XT server"** on page 13.

10 Move the index files to the index server.

a On the reconfigured OpenLab Server/ECM XT server, locate the DataStoreIndex location by clicking the **Server Configuration** shortcut in the Agilent Technologies program group.

b Move the Index files to the desired location on the index server. This location must meet the requirements described in the *Agilent OpenLab Server and OpenLab ECM XT Hardware and Software Requirements Guide*.

11 Install the Index Server using the steps in **"Install the OpenLab Server/ECM XT server"** on page 13.

12 Follow the steps in **"Configure a Virtual FQDN as the Content Management storage location"** on page 17 to configure the Content Management Storage location.

13 Follow the steps in **"Bring up the Scalable System"** on page 19 to start the system.

14 Follow the steps in **"Configure Redundant License Servers for the Scalable System"** on page 20 to regenerate the license file and apply the license to the servers.

5 Administration

Switch Primary OpenLab Server/ECM XT Server

The following reconfigurations are required to change the primary OpenLab Server/ECM XT server:

1. Disconnect all OpenLab AICs and Clients.
2. Stop all Agilent OpenLab services, which can alter data on your current primary OpenLab Server/ECM XT server. Backup related services should not be stopped.
3. Back up the Data Repository PostgreSQL database on your current primary OpenLab Server/ECM XT server.
4. Restore the Data Repository PostgreSQL database backup to your new primary OpenLab Server/ECM XT server.
5. Optional: When using Agilent OpenLab CopyTo Server feature on your current primary server, change the “Log On As” property of the service to your Service User Account on your new primary OpenLab Server/ECM XT server. Otherwise, access to the CopyTo report destinations may not be possible.
6. Set one of the other active OpenLab Server/ECM XT servers as the primary OpenLab Server/ECM XT server by executing the Server Configuration Utility on the Index server, and enter the new primary OpenLab Server/ECM XT server FQDN on the **Server Configuration** screen.
7. Update the configuration in the load balancer to ensure that the traffic is distributed to the new primary OpenLab Server/ECM XT server.
8. Repeat the steps in **“Bring up the Scalable System”** on page 19.
9. Verify that the primary OpenLab Server/ECM XT server is part of the system as an online cluster member in the Content Management Admin Console.

Remove an OpenLab Server/ECM XT Server from the Scalable System

If an OpenLab Server/ECM XT server is no longer available, the server can be removed from the scalable system. Use the following steps to remove the server from the system.

1. From one of the active OpenLab Server/ECM XT server that will remain on the system, log into the Content Management Admin Console.
2. Select **Repository Server Clustering**. The failed OpenLab Content Management Server is displayed in the list of Offline Cluster Members.

NOTE

If the failed server also acts as the primary OpenLab Server/ECM XT server, then switch the primary server role to a different machine.

NOTE

If you want to remove the offline cluster members, please call Agilent Support.

Restore an OpenLab Server/ECM XT server to the Scalable System

To restore or replace a removed or failed OpenLab Server/ECM XT server, you must install and configure the server as you would install a new OpenLab Server/ECM XT server. If you still have a valid system image of your installed and configured server, it might be possible to restore the image to the server and reboot the server to work as part of the scalable system. The server will automatically become a member in the OpenLab Server/ECM XT scalable system.

Be aware that previously installed updates must be installed to a recovered system if the other OpenLab Server/ECM XT servers are on the respective update. Restore your backup of the Data Repository on your primary OpenLab Server/ECM XT server if the failed server was your primary server.

Add a New OpenLab Server/ECM XT Server to the Scalable System

To add a new OpenLab Server/ECM XT server to the scalable system:

1. As three OpenLab Server/ECM XT servers are the maximum on a scalable system, either the second or third OpenLab Server/ECM XT server must be removed from the system prior to adding a new node to the scalable system.
2. Follow the steps in **"Install the OpenLab Server/ECM XT server"** on page 13 to set up the additional OpenLab Server/ECM XT server. Remember to select the **Connect to existing database** option.
3. If the new server is also supposed to be the primary OpenLab Server/ECM XT server follow all the steps in the**"Install the OpenLab Server/ECM XT server"** on page 13 to configure the new server, and point the remaining Index server to it.
4. Follow the steps in **"Configure Redundant License Servers for the Scalable System"** on page 20 to regenerate the license file and re-apply the license to servers.
5. Follow the steps in **"Configure the load balancer"** on page 10 to update the load balancer configuration to include the new OpenLab Server/ECM XT server.

Centralized Printing and Sample Scheduler

Customers intending to use Centralized Printing or Sample Scheduler in a scalable system must ensure that the primary OpenLab Server/ECM XT server is configured in accordance with the respective feature/application.

The Centralized Printing preparations listed in the OpenLab CDS Client AIC guide must be applied to the primary server to allow for Centralized Printing to be operational in a scalable system as all Centralized Printing traffic is directed to the primary server by the load balancer.

Sample scheduler utilizes by default the Data Repository instance on the primary server and the load balancer redirects all Sample Scheduler related traffic to the primary web server as well. Therefor apply all changes on the primary OpenLab Server/ECM XT server.

6 Upgrade Scalable System

Before upgrading the scalable system, make sure your infrastructure (including operating systems) is supported by OpenLab Server/ECM XT. Familiarize yourself with all prerequisites for the new OpenLab Server/ECM XT version.

Due to the reduction of ports with OpenLab CDS 2.7 and the usage of path-based routing and load balancing instead of port-based routing and load balancing, it is important to update your load balancer configuration. Port 443 requires special attention and reconfiguration to allow for path-based routing.

After upgrading Scalable System servers, you can use old client/AIC (versions 2.4, 2.5, and 2.6) combinations during migration. The respective required ports of older versions need to remain configured on the load balancer until the migration to OpenLab CDS 2.7 is completed.

Many of the steps outlines below align with the installation of a new scalable system. Contact Agilent support if you intend to switch to a new set of OpenLab Server/ECM XT servers due a change to a later Windows Server version.

Upgrade your existing scalable system license to the current version prior to upgrading using the MAC addresses of the planned OpenLab Server/ECM XT servers.

Use the following procedure to upgrade the OpenLab Server/ECM XT server and the Index server. The procedure must be run separately on each server.

1. Stop Content Management Search service and AlfrescoTomcat service on the Index server.
2. Change the OpenLab Shared Services service startup type from disabled to manual on the Index Server.
3. Stop AlfrescoTomcat, Agilent OpenLab Shared Services, and Agilent OpenLab Automation services, and set the startup type of the services to manual on each OpenLab Server/ECM XT server. Apply the steps in the order tertiary, secondary, and primary OpenLab Server/ECM XT server.

   Upgrade the OpenLab servers one by one in the following order: primary, secondary, tertiary OpenLab Server/ECM XT server followed by the Index server.
4. Start the OpenLab Server/ECM XT installer.

5 Run the installer **Step 1: Install of Upgrade Software Prerequisites**, and follow the prompts to install all prerequisite software.

When upgrading a scalable system, which is connected to an external PostgreSQL database server, make sure the installed PostgreSQL version is supported by OpenLab Server/ECM XT.

6 If upgrading a scalable system connected to an external PostgreSQL server, skip Step 2.

Otherwise, run the installer **Step 2: Create or Update Database Schema**. Choose the same remote Database server as in **Step 1**, and select **Connect to and upgrade existing database for OpenLab Server**.

7 Follow the prompts to finish **Step 2**. Enter the information that you set in this step during the initial installation.

8 Run the installer **Step 3: Install or Update OpenLab Content Management**.

9 The **Review** screen displays the **Installed** and **Min. Required** columns with versions of individual OpenLab Server/ECM XT server and OpenLab Index server components. Click **Upgrade**.

10 Once the upgrade progress reaches 100%, click **Next**.

11 The **Reboot the computer now** option is selected by default. Run Software Verification and check the validity of all installed components. Click **Finish**, and wait for the machine to complete the reboot.

12 Execute the PowerShell script config-cluster.ps1 in the "C:\Program Files (x86)\Agilent Technologies\Certificate Service\Bin" folder from each OpenLab Server/ECM XT server using the UNC path of the shared internal certificate store:

a
```
>cd ":\Program Files (x86)\Agilent Technologies\Certificate Service\Bin"
```

b
```
>./config-cluster.ps1
-shareName "\\FileServer\SharedCertificateStore"
-serviceAccountName "domain\ServiceUserName"
-serviceAccountPassword "ServiceUserPassword"
```

Once the command runs successfully, data will be generated in the shared internal certificate store and corresponding services will be restarted.

13 Run the installer **Step 4: Configure OpenLab Content Management**.

14 On the OpenLab Server/ECM XT server, the **Server Configuration** screen displays the **Content Management only** option selected by default. Click **Next**.

On the Index server, the **Server Configuration** screen displays the **Index and Search only** option selected by default. Enter the FQDN of the primary OpenLab Server/ECM XT server and click **Next**.

15 On the **Access Credentials** screen, the configuration of the service account from the previous installation is displayed. Keep the default configuration and click **Verify**. Then, click **Next**.

16 On the **Content Paths** screen, the configuration of the **Content Storage Location**, **Archive Storage Location**, and **Content Management Index Hostname** from the previous installation is displayed. Update the Content Management Index Hostname to the FQDN of the Index server. All storage paths are displayed in UNC path format. Verify that the configuration is correct, and click **Next**.

17 On the **Certificate Setup** screen, select to use the Agilent OpenLab internal certificate.

18 Click **Apply**, and then click **Done**.

19 When prompted, provide the Shared Services administrator credentials, and click **OK**.

20 Using the administrative notepad, open "C:\Program Files (x86)\Agilent Technologies\OpenLAB Data Store\tomcat\shared\classes\alfresco\web-extension\share-config-custom.xml" and add |https://<Virtual FQDN>.* as the last entry to the assertReferer and asserOrigin sections. See **"Allow load balancer's URL to work with OpenLab Server/ECM XT Server"** on page 22.

21 Stop and disable OpenLab Shared Services service on the OpenLab Index server.

22 Reapply the new scalable system license according to **"Configure Redundant License Servers for the Scalable System"** on page 20.

23 Bring up the scalable system.

24 In OpenLab Control Panel, configure the load balancer URL as https://<Virtual FQDN>. See **"Allow load balancer's URL to work with OpenLab Server/ECM XT Server"** on page 22.

7 Appendix A: Installation and Configuration of Nginx Load Balancer

Set Up Nginx Load Balancer on Linux System

Agilent Technologies does not include any of the sources or binaries described below on the install medium. If you plan to use Nginx load balancer, referenced modules, and haproxy, make sure to adhere to their respective owners licensing terms.

Prerequisites

- A Linux system with 8 core CPU, 4 GB memory, and 20 GB HDD
- Connected to the same network of OpenLab Server/ECM XT servers
- Superuser/root privileges to install additional software on load balancer

NOTE

CentOS 8 was used when preparing this document.

Download the software

1 Log in as root to the load balancer system.

2 Update the system

```
yum -y update
```

3 If FTP application is activated on OpenLab Server/ECM XT servers, install haproxy as the FTP load balancer application.

```
yum -y install haproxy
```

4 Install the extra packages for Enterprise Linux.

```
yum -y install
https://dl.fedoraproject.org/pub/epel/epel-release-latest-8.noarch.rpm
```

5 Download and install nmap.

```
yum install nmap
```

6 Install additional packages required for Nginx compilation.

yum -y install wget tar git gcc make pcre pcre-devel zlib zlib-devel openssl openssl-devel GeoIP GeoIP-devel

7 Go to your planned compile directory, for example, /root.

cd /root

8 Download Nginx.

wget http://nginx.org/download/nginx-1.20.2.tar.gz

9 Download sticky sessions module.

git clone https://bitbucket.org/nginx-goodies/nginx-sticky-module-ng.git
git clone https://github.com/yaoweibin/nginx_upstream_check_module.git

Install Nginx

1 Uncompress the Nginx package.

tar -xvzf nginx-1.20.2.tar.gz

2 Compile Nginx with the sticky session module.

a cd nginx-1.20.2/

b ./configure --prefix=/usr/share/nginx --sbin-path=/usr/sbin/nginx
--conf-path=/etc/nginx/nginx.conf --error-log-path=/var/log/nginx/error.log
--http-log-path=/var/log/nginx/access.log
--http-client-body-temp-path=/var/lib/nginx/tmp/client_body
--http-proxy-temp-path=/var/lib/nginx/tmp/proxy
--http-fastcgi-temp-path=/var/lib/nginx/tmp/fastcgi
--pid-path=/var/run/nginx.pid --lock-path=/var/lock/subsys/nginx
--user=nginx --group=nginx --with-http_gzip_static_module
--with-http_stub_status_module --with-http_ssl_module --with-pcre
--with-file-aio --with-http_realip_module --without-http_scgi_module
--without-http_uwsgi_module --without-http_fastcgi_module
--with-http_geoip_module --with-stream
--add-module=/root/nginx-sticky-module-ng
--add-module=/root/nginx_upstream_check_module

c make

If you are getting an error, make sure that the additionally required packages are installed and that the sticky session modules are present in the directory /root

yum install -y gcc pcre pcre-devel openssl openssl-devel gd gd-devel GeoIP-devel

Repeat step b above, then run **make** again.

d make install

3 Configure the systemd service file to run the Nginx service.

a Create the unit file nginx.service in /etc/systemd/system/
nano /etc/systemd/system/nginx.service

b A template nginx.service file is included on the install medium in \Setup\Tools\Support\Scalable. Copy the following content into nginx.service:

[Unit]

Description=The NGINX HTTP and reverse proxy server

After=syslog.target network-online.target remote-fs.target nss-lookup.target

Wants=network-online.target

[Service]

Type=forking
PIDFile=/run/nginx.pid
ExecStartPre=/usr/sbin/nginx -t
ExecStart=/usr/sbin/nginx
ExecReload=/usr/sbin/nginx -s reload
ExecStop=/bin/kill -s QUIT $MAINPID
PrivateTmp=true

[Install]

WantedBy=multi-user.target

Configuration

1. Configure the FTP port with haproxy (only required if FTP is activated on OpenLab Server/ECM XT servers).
2. Copy the template haproxy configuration file haproxy.cfg from the installation medium folder \Setup\Tools\Support\Scalable to your load balancer directory /etc/haproxy\.
3. Open haproxy.cfg and replace the FQDN and IP address of your CM scalable system node to the server lines in this file. A template haproxy.cfg is included on the install medium in \Setup\Tools\Support\Scalable.

   server **your_CM_server1 your_CM_Server1_IP** check port 21 inter 10s rise 2 fall 2

   server **your_CM_server2 your_CM_Server2_IP** check port 21 inter 10s rise 2 fall 2

   server **your_CM_server3 your_CM_Server3_IP** check port 21 inter 10s rise 2 fall 2
4. Configure Nginx.
   a. Replace the nginx.conf file in etc/nginx/ with the one provided on the installation medium located in directory \Setup\Tools\Support\Scalable.
   b. Create directory /etc/nginx/conf.d

      mkdir /etc/nginx/conf.d
   c. Copy the files http.conf, http-proxy-params.conf, and stream.conf in directory \Setup\Tools\Support\Scalable from the installation medium to directory /etc/nginx/conf.d.
   d. Replace the OpenLab Server/ECM XT server IPs in http.conf with your system's IP addresses or server FQDNs, and replace the server_name value with your load balancer's <Virtual-FQDN>.
   e. Replace the OpenLab Server/ECM XT server IPs in stream.conf with your system IP address or its FQDN.
5. Configure the load balancer firewall.
   a. Add all required ports to the load balancer firewall.

      21, 443, 6625, 6570, 8090, 8098-8099, 11100-11150, 27009

      For example, to add ports 443 and 8098-8099 to the load balancer, execute the following:

```
firewall-cmd --add-port=443/tcp --permanent
firewall-cmd --add-port=8098-8099/tcp --permanent
```

Port 21 and port range 11100-11150 are only required if FTP is activated on OpenLab Server/ECM XT servers.

b Repeat the same command for all remaining ports.

c After adding all the ports to the firewall, reload the firewall to update the ports on the load balancer using the following command:

```
firewall-cmd --reload
```

d Verify all ports have been added to the firewall:

```
firewall-cmd --list-all
```

6 Set up an SSL configuration for Nginx.

a Create the Nginx certificate directory

```
mkdir /etc/nginx/certs
```

b Prepare the load balancer certificate (loadbalancer.crt) containing the initial commercial load balancer certificate (org_loadbalancer.crt) as well as the Root Certificate Authority certificate (RootCA.crt) in the folder /etc/nginx/certs/. In Linux, this can be achieved by using:

```
cat org_loadbalancer.crt RootCA.crt > /etc/nginx/certs/loadbalancer.crt
```

c Copy your corresponding key (loadbalancer.key) to the folder /etc/nginx/certs/loadbalancer.key.

7 Prepare an SSL dhparam file on the load balancer. For example,

```
openssl dhparam -out /etc/nginx/certs/dhparam.pem 2048
```

8 Verify that the certificate, key, and dhparam files are correctly addressed in the http configuration file (/etc/nginx/conf.d/http.conf). For example,

```
ssl_certificate /etc/nginx/certs/loadbalancer.crt;
ssl_certificate_key /etc/nginx/certs/loadbalancer.key;
ssl_dhparam /etc/nginx/certs/dhparam.pem;
ssl_protocols TLSv1.2;
```

NOTE

An Agilent self-signed certificate tool is included with any of the OpenLab Server/ECM XT scalable system nodes after completing the scalable system configuration. Please refer to **"Configure SSL for the Nginx Load Balancer"** on page 44 for more information.

Disable SELinux:

To disable SELinux permanently, do the following (only required if FTP is activated on OpenLab Server/ECM XT server):

1 nano /etc/sysconfig/selinux.

2 Change the SELINUX=enforcing directive to SELINUX=disabled.

To disable SELinux temporarily, use the following command:

setenforce 0

NOTE

Disabling SELinux can reduce security of the installed Linux machine and violate your IT security policy. Make sure to comply with your IT policy. FTP access to Content Management is only required for direct FTP access, not for CDS result uploads and downloads via CDS clients. By default FTP access is disabled on each OpenLab Server / ECM XT server.

Start haproxy service

To start the haproxy service, run the following commands (only required if FTP is activated on OpenLab Server/ECM XT server nodes):

systemctl start haproxy.service

If there is an error returned by systemctl, check the error with the following command:

systemctl status haproxy.service

Start Nginx Service

1 Create the required runtime directories:
mkdir /var/lib/nginx/tmp

2 Create an Nginx user as the system account to execute Nginx service:
useradd -r nginx

3 To start the Nginx service, run the following command:
systemctl start nginx.service

If there is an error returned by systemctl, check the error with the following command:
systemctl status nginx.service

Verification

Open a web browser and enter the load balancer FQDN to the address bar. For example,

Content Management:
https://<Virtual-FQDN>

Agilent OpenLab Shared Services:
https://<Virtual-FQDN>/openlab/olss/v1.0/health

Certificate Service:
https://<Virtual-FQDN>/openlab/certservice/health

Sample Scheduler:
https://<Virtual-FQDN>/openlab/samplescheduler

The Content Management Login page should appear, for the first example, when the load balancer is configured correctly. When using an Agilent self-signed certificate, make sure that the OpenLabRootCA certificate is installed to the machine you are testing from.

Configure SSL for the Nginx Load Balancer

OpenLab CDS 2.7 AICs and clients require a trusted certificate installed on port 443 of the load balancer to ensure secured communication. For an isolated scalable system without internet or enterprise network access and without an own enterprise certificate authority/Private key infrastructure, you can configure the load balancer to use Agilent internal certificates with all the secure listening endpoints. Please contact your Agilent representative to ensure the system runs in a supported configuration.

1. Generate the self-signed certificate package using the Certificate Tool available on any scalable OpenLab Server/ECM XT node hosting a Certificate Service. Certificate Service must be configured for a scalable system before generating the certificate package for the Nginx load balancer.
2. On one of the scalable system nodes, launch an elevated command prompt and traverse to the Certificate Tool's bin folder ({Installation Path}\Agilent Technologies\Certificate Service Tool\Bin).
3. Run the command providing the fully-qualified domain-name of the loadbalancer <Virtual-FQDN> and a location to where the certificate package is to be stored. For example,

   ```
   Agilent.OpenLab.CertService.CertTool.exe GetServerCert -d
   C:\TempFolder\ -c "loadbalancer-name.scs.agilent.com" [-h
   localhost -p 52088]
   ```

   On successful execution of the command, the folder specified in the command will contain the certificate package.
4. Copy the **loadbalancer-name.scs.agilent.com.zip** folder and the **OpenLabRootCA.crt** files to a folder on the Nginx load balancer. Extract the files from the certificate package to the folder which contains **OpenLabRootCA.crt**.

   It should contain a certificate for the machine (loadbalancer-name.scs.agilent.com.crt), the corresponding unencrypted key (loadbalancer-name.scs.agilent.com.keyUnencrypted) and the root CA certificate (OpenLabRootCA.crt).

5 Concatenate the contents of the loadbalancer-name.scs.agilent.com.crt and OpenLabRootCA.crt files and create a new certificate which contains both certificates. On Linux, you can run the command:

```
cat loadbalancer-name.scs.agilent.com.crt
OpenLabRootCA.crt > /etc/nginx/certs/loadbalancer.crt
```

This creates a single certificate file which contains both the certificate for the load-balancer and the Root CA certificate.

6 Copy the **loadbalancer-name.scs.agilent.com.keyUnencrypted** to the /etc/nginx/certs/ folder.

7 Ensure the Nginx load balancer http.conf file in /etc/nginx/conf.d/ has the correct values listed for the load balancer certificate and key file.

```
ssl on;
ssl_certificate /etc/nginx/certs/loadbalancer.crt;
ssl_certificate_key /etc/nginx/certs/loadbalancer-name
  .scs.agilent.com.keyUnencrypted;
server_name loadbalancer-name.scs.agilent.com;
```

8 Once configured, restart Nginx so that the SSL changes are applied.

8 Appendix B: Agilent OpenLab Services Path-Based Routing and Health Queries

Agilent recommends using wildcards for the path-based routing to the primary OpenLab Server/ECM XT server. If this is not possible with your load balancer or within your IT infrastructure, you will find the information for every individual path in the table below. The required routes and paths are marked "all" if they need to be load balanced amongst all OpenLab Server/ECM XT servers.

Service Name	Route/Path	Destination	Health Check Method Reply Pattern
AlfrescoTomcat (ECM XT)	/ /alfresco/ /webhorse/ /_vti_bin/ /datastore/	All (Round Robin)	/alfresco/s/api/health Check?format=html GET 200
Audit Trail Service	/openlab/audit-trail/	Primary	/openlab/audit-trail/health GET
Certificate Service	/openlab/certservice/	Primary	/openlab/certservice/health GET Healthy
Copy To	/openlab/copy-to-server/	Primary	
Data Collection Service	/openlab/dcs/	Primary	/openlab/dcs/health GET Healthy
Distributed Transaction Coordinator	/openlab/distributed- transaction -coordinator/	Primary	/openlab/distributed- transaction-coordinator/ health GET
Electronic Signature Service	/openlab/esignature/	Primary	/openlab/esignature/health GET
Sample Scheduler Webserver	/openlab/samplescheduler/	Primary	/openlab/samplescheduler/ GET

Service Name	Route/Path	Destination	Health Check Method Reply Pattern
Sample Scheduler DB Management Service	/openlab/sched-db-agent/	Primary	/openlab/sched-db-agent/ health GET
Sample Scheduler Orchestrator	/openlab/sched-orchestrator/	Primary	/openlab/sched-orchestrator/health GET
Sample Scheduler Services Controller	/openlab/scheduler-services/	Primary	/openlab/scheduler-services /health GET
Shared Services Rest Service	/openlab/olss/ /Agilent/OpenLab/Diagnostics/ /Agilent/OpenLab/EntityService/ /Agilent/OpenLab/SecurityService/ /Agilent/OpenLab/ActivityLogService/ /Agilent/OpenLab/NotificationService/ /Agilent/OpenLab/ReplicationService/ /Agilent/OpenLAB/Licensing/ /Agilent/OpenLab/SingleSignOn/ /openlab/licensing/	Primary	/openlab/olss/v1.0/health GET {"message":"OK"}
Licensing Support REST Service	/Agilent/OpenLab/LicensingService/	Primary	
Test Services Central Mgmt Service	/openlab/testservicesserver/	Primary	
Test Services REST API	/openlab/ca/ /openlab/testservices/	Primary	
Test Services (QualA) Web UI	/testservices/	Primary	/testservices/ HEAD

9 Appendix C: Support

Sales and Support Assistance

Please check the following web site for your local sales and support contact:

https://www.agilent.com/en/support

Agilent Community

To get answers to your questions, join over 10,000 users in the Agilent Community. Review curated support materials organized by platform technology. Ask questions to industry colleagues and collaborators. Get notifications on new videos, documents, tools, and webinars relevant to your work.

https://community.agilent.com

www.agilent.com

DocNo D0013948
May 2022