Legal Notices

Information in this document, including URL and other website references, represents the current view of Commvault Systems, Inc. as of the date of publication and is subject to change without notice to you.

Descriptions or references to third party products, services or websites are provided only as a convenience to you and should not be considered an endorsement by Commvault. Commvault makes no representations or warranties, express or implied, as to any third party products, services or websites.

The names of actual companies and products mentioned herein may be the trademarks of their respective owners. Unless otherwise noted, the example companies, organizations, products, domain names, e-mail addresses, logos, people, places, and events depicted herein are fictitious.

Complying with all applicable copyright laws is the responsibility of the user. This document is intended for distribution to and use only by Commvault customers. Use or distribution of this document by any other persons is prohibited without the express written permission of Commvault. Without limiting the rights under copyright, no part of this document may be reproduced, stored in or introduced into a retrieval system, or transmitted in any form or by any means (electronic, mechanical, photocopying, recording, or otherwise), or for any purpose, without the express written permission of Commvault Systems, Inc.

Commvault may have patents, patent applications, trademarks, copyrights, or other intellectual property rights covering subject matter in this document. Except as expressly provided in any written license agreement from Commvault, this document does not give you any license to Commvault’s intellectual property.

COMMVAULT MAKES NO WARRANTIES OF ANY KIND, EXPRESS OR IMPLIED, AS TO THE INFORMATION CONTAINED IN THIS DOCUMENT.
©1999-2017 Commvault Systems, Inc. All rights reserved

Commvault, Commvault and logo, the “C” logo, Commvault Systems, Solving Forward, SIM, Singular Information Management, Commvault Galaxy, Unified Data Management, QiNetix, Quick Recovery, QR, CommNet, GridStor, Vault Tracker, InnerVault, QuickSnap, QSnap, Recovery Director, EA-2016-CS, CommCell, IntelliSnap, ROMS, Simpana OnePass, Commvault Edge and CommValue, are trademarks or registered trademarks of Commvault Systems, Inc. All other third party brands, products, service names, trademarks, or registered service marks are the property of and used to identify the products or services of their respective owners. All specifications are subject to change without notice.

All right, title and intellectual property rights in and to the Manual is owned by Commvault. No rights are granted to you other than a license to use the Manual for your personal use and information. You may not make a copy or derivative work of this Manual. You may not sell, resell, sublicense, rent, loan or lease the Manual to another party, transfer or assign your rights to use the Manual or otherwise exploit or use the Manual for any purpose other than for your personal use and reference. The Manual is provided “AS IS” without a warranty of any kind and the information provided herein is subject to change without notice.
Contents
Legal Notices .......................................................................................................................... 2

Before we begin .................................................................................................................. 4
Module 2 - CommCell® Deployment and Configuration .................................................. 5
  Configure a Distributed Software Cache ........................................................................ 5
Interactive Installation Process and Options .................................................................... 7
  Selecting Installation Type ............................................................................................. 7
  Commserve® Server Specific Installation Options ...................................................... 8
Agent Installation Methods ............................................................................................... 9
  Standard Installation ..................................................................................................... 10
  Push (Remote) Installation ......................................................................................... 12
Module 3 - Data Security and Network Control ............................................................... 14
  Configure Commvault Firewall Proxy server .................................................................. 14
  Configure Firewalls Settings on the Commserve® ...................................................... 16
  Configure the Client or Client Computer Group Level ................................................. 18
Encryption ....................................................................................................................... 20
  Setting Inline Encryption ............................................................................................ 20
  Enabling Encryption on the Client ................................................................................ 21
  Configure Subclient Encryption Options ...................................................................... 22
  Setting Hardware Encryption ...................................................................................... 23
  Setting Copy Based Encryption .................................................................................. 24
  Setting Media Password .............................................................................................. 25
    Setting CommCell® Level Media Password .............................................................. 25
    Setting Storage Policy Level Media Password ......................................................... 26
Extras - Commvault® Tools and Utilities ........................................................................ 27
  Using the Process Manager Tool ................................................................................ 27
  Using the Commserve Recovery Assistant tool .......................................................... 28
  Using the GXTail Tool .................................................................................................. 29
  Using the CVPing option to test network connectivity ............................................... 30
  Using the CVIPInfo tool to get IP configuration information of a machine ............. 30
APPENDIX A: User Guide to Access CVLab environment ............................................. 31
  Accessing and launching the CVLab environment .................................................... 31
  Accessing and using the CommCell® Console ........................................................... 34
Resource Documents ......................................................................................................... 34
Before we begin

Please follow the instructions below to access the CVLab environment:

- Login to your Education Advantage Profile from https://ea.commvault.com, to access your course materials and virtual lab environment.
- For information regarding logging into the Virtual Lab Environment please refer to Appendix A.
- FYI: Module 1 has no formal labs so we start with Module 2 on the next page.

Accessing and using the CommCell® Console on the Commserve:

To access the CommCell console click the launcher icon in the Windows Task bar.

Use the following credentials to log in to the CommCell console:
- Username: admin
- Password: admin

Note: password is all lowercase. Click OK.
Module 2 - CommCell® Deployment and Configuration

For step-by-step instructions for installing Commvault components, go to:


Configure a Distributed Software Cache

1. In the CommCell® Console’s ribbon bar select Tools | Add/Remove Software | Software Cache Configuration.

2. Select the Remote Software Cache tab and click Add.

3. In the Configure Remote Software Cache dialog box:
   a. For Computer select EA-2016-MA
   b. Click Add/Remove Clients.
   c. From the “Available Clients/Client Groups” list, select Laptop Clients, then click Include >. (This adds the client group to the Selected Clients/Client Groups window.)
   d. Click OK.
   e. Click OK to exit the “Configure Remote Software Cache” dialog box.
f. Click OK to exit the “Add/Remove Software Configuration” dialog box.

4. In the CommCell® Console’s ribbon bar, select Tools | Add/Remove Software | Download Software.
   a. In the Download and Sync Cache Options dialog box | General tab, select Service Pack and Hotfixes.
   b. In the Options tab, select Download and Sync.
   c. In the Job Initiation tab select Schedule and then Configure.

5. Select Monthly.

6. For the Schedule Name type: Monthly Download and Sync.

7. For the Start Time enter: 4:00PM.

8. Set the schedule to run on the First Sunday.

9. Click OK to exit the scheduler.

10. Click OK to exit the Download and Sync Cache Options.
Interactive Installation Process and Options

Note: the following section is for reference purposes. Some of these installations may not be supported in the CVLab environment.

Selecting Installation Type

Interactive installation provides the following installation types:

- Standard installation can be used to install software on a local machine.
- Custom package installation is used to create smaller distributable installation packages to be deployed on remote machines.
- Decoupled installation can be used to install Commvault® agents on machines without connectivity to the EA-2016-CS® server.
- Restore Only agents can be installed on machines without allocating licenses. These can receive restores but cannot be used for backups (unless reactivated).
Commserve® Server Specific Installation Options

1. Enter CommServe software installation location
2. Enter SQL software installation location
3. Enter CommServe database location
4. Enter location for CommServe metadata DR backup (export phase)
Agent Installation Methods

Commvault® client agents can be deployed using several methods:

- Push installation can be used to push Commvault agents to one or more remote machines.
- Standard installation can be used to install software on a local machine.
- Custom package installation is used to create smaller distributable installation packages to be deployed on remote machines.
- Decoupled installation can be used to install Commvault agents on machines without connectivity to the CommServe® server.
- Restore Only agents can be installed on machines without allocating licenses. These can receive restores but cannot be used for backups (unless reactivated).

For each agent installation method, specific common settings can be selected based on preconfigured settings in the CommCell® environment:

- Client Computer Group
- Subclient policy
- Storage policy
- Global filters

Additional configuration settings are also required, which are determined at the time of installation:

- CommServe® server name
- Agent installation folder path
- Job results folder path
Standard Installation

1. From your CVLab Launchpad window, verify that the **EA-2016-SERV** virtual machine is running.
2. Click on the icon to connect to the **EA-2016-SERV** VM.
3. Login to the **EA-2016-SERV** system using the following credentials:
   a. Username: *company\student*
   b. Password: *student*
4. Click on the Windows Start icon to open the Start Menu. Then select the Windows File Explorer and navigate down the folders using the path `\\EA-2016-CS\softwarecache\CVMedia\11.0.0\Windows` to double-click **Setup.exe**.
5. The Commvault® Setup wizard appears. Check the box next to “I Agree” to accept terms in the license agreement and click “>” to continue.
6. From the Installation Type screen, select the radio button for “Install packages on this computer” then click “>” to continue.
7. From the Select Packages screen, select **Microsoft Windows** on the left of the screen, then click the boxes next to “File System Core” and **File System**. Click “>” to continue.
8. Review settings for the Installation Path screen, then click “>” to continue.
9. Accept the default settings for the next screens and the installation will begin.
10. When the **Firewall Configuration** screen appears, review the choices, keep the defaults and click “>” to continue.
11. Review the populated responses for Client Name and Host Name fields on the Client Computer Information screen. Click “>” to continue.

12. In the Commserve Information screen, enter EA-2016-CS.company.com and click “>” to continue.

13. In the Client Certificate screen, keep the defaults and click “>” to continue.

14. In the Commserve Authentication screen, enter the following:
   a. Username: Admin
   b. Password: admin

**Note: Require Authentication for Agent Installation is now checked by default.

15. Click “>” to continue.

16. In the Additional Configuration screen select the following from the dropdown menu:
   a. Client Group: <leave blank>
   b. Storage Policy: Basic Disk
   c. Subclient Policy: <leave blank>

17. Click “>” to continue. After the software has been installed click “Finish” to close the install screen.

   Return to the EA-2016-CS Server, From the CommCell® Browser, expand Client Computers to view the EA-2016-SERV client.

18. If the client does not appear, select View | Refresh from the ribbon bar. Return to Client Computer section and view the new client.
Push (Remote) Installation

1. From the EA-2016-CS virtual machine, log on to the CommCell Console. (If not already logged in)

2. On the Ribbon Bar click the Tools tab. From the available icons click the Add/Remove Software icon which opens a sub menu. From the dropdown menu, Click Install Software.

3. Once the Install Wizard appears. Click Next.

4. In the Select the computer’s operating system screen, select Windows, then click Next.

5. In the Select how to discover the computers for installing the software screen, select Manually select computers, then click Next to continue.

6. In the Enter the host names of the computers screen, select Import From Active Directory.
   a. Select the domain Company from the Domain Name drop-down list.
   b. Click OK to close and continue.
   c. From the Discovered Computers screen, select EA-2016-SERV.company.com and click Add.
   d. In the “Enter the host names of the computers” screen, note the newly selected server and click Next.

7. In the Select Software Cache screen, accept the defaults and click Next.

8. On the Enter Account Information screen, using an account that has permissions to install software on this server, enter the following:
   a. User Name: company\student
   b. Password: student
c. Confirm the password

9. Click **Next** to continue.

10. In the Select Package(s) to Install screen, select **MediaAgent** located in the Server section. (A previous lab installed the File System Agent).

11. Click **Next** to continue.

12. In the **Enter Recommended Settings for the selected Software** screen, select **Basic Disk** from the drop-down menu for “Storage Policy To Use” section. (The system will add additional specialty subclients under the File System Agent for DDB and V2 Indexing and these will need a Storage Policy.)

13. Click **Next** to continue

14. Review **Installer Flags** options for **Enter Additional Install Options** screen and click **Next** to continue.

15. Review the additional choices from the **Optional Settings** screen and click **Next**.

16. On the **Firewall Configuration** screen, click **Next** to accept the default settings and continue.

17. In the **Please Select When To Run The Job** screen, select **Immediate** and click **Next**.

18. Review the **Summary** screen, then click **Finish** and the task will be submitted to the Job Manager.

19. Monitor the job in the Job Controller window. Double click the job to open the Job Details window and select the **Client Status** tab. When the job completes, expand **Storage Resources | MediaAgents** to verify the install.

20. If the MediaAgent does not appear, select **View | Refresh** from the ribbon bar.
Module 3 - Data Security and Network Control

Configure Commvault Firewall Proxy server

1. In the CommCell® Browser, expand Client Computers.
2. Right-click on the Proxy client | Properties.
3. In the Client Computer Properties for Proxy dialog box, click Network.
4. On the Firewall Configuration tab, check the box to enable Configure Firewall Settings.
5. Select the Advanced radio button and review the warning message. Click OK.
6. In the Incoming Connections sub-tab, click Add.
7. In the Connections to (Proxy) pop-up box:
   a. Select From: Laptop Clients
   b. Select State: RESTRICTED
   c. Click OK. The selected information appears in the Incoming Connections list.
   d. Repeat steps 6, 7a, b and c. but this time “Select from” the EA-2016-CS and again for EA-2016-MA.
8. There are no additional Incoming Ports or Outgoing Routes to select for the Proxy. Communication is inbound traffic only.
9. From the Options tab select, “This computer is in DMZ and will work as a proxy”. 
10. Click **OK** to save the **Network Properties for Client: Proxy** configuration window.

11. Click **OK** to close the Proxy properties dialog box.
Configure Firewall Settings on the Commserve®

1. In the CommCell® Browser select **EA-2016-CS** (top of the Entities tree); right-click and select **Properties**.
2. From the **CommCell Properties** dialog box, select the **Firewall Configuration** tab.
3. Check the box to enable **Configure Firewall Settings**.
4. In the Incoming Connections sub-tab click **Add**.
5. In the “Connections to (EA-2016-CS)” pop-up box:
   a. Select From: **Laptop Clients**
   b. Select State: **Blocked**
   c. Click **OK**. Laptop Clients appears in the Incoming Connections list.
6. In the Incoming Ports sub-tab ensure the “Listen for tunnel connections on port:” is set to **8403**. Port 8403 is registered to Commvault but you can select any available port.
7. In the Outgoing Routes sub-tab, select **Add**.
   a. For Remote Group/Client select **Laptop Clients**.
   b. Set the Route Type to **Via Proxy**.
c. In the Proxy Settings section, ensure the “Remote Proxy:” option is set to Proxy. If it is not, set it to Proxy.

d. Click OK. Laptop Clients will appear in the Outgoing Routes list.

8. To view the Summary Tab you must exit this window and return, click OK to exit the Properties Page.

9. Expand Client Computers in the CommCell Browser, select the EA-2016-MA client, right click and select Properties.

10. Click the Network button and select the Summary tab to examine the settings.

11. Click Cancel to exit the network settings and click Cancel to close the client properties.

12. After the firewall settings are configured you must apply the settings to Clients and Media Agents. To do this, right-click on EA-2016-CS at the top of the CommCell Browser window.

13. Select All Tasks | Push Firewall configuration.


15. An information dialog box appears stating the “Push Firewall Configuration submitted successfully for client [EA-2016-CS]”. Click OK.

---

**Best Practice for your environment:** Configure the EA-2016-CS® firewall using Client Computer Groups. This keeps firewall configuration requirements to the minimum and facilitates a dynamic client environment.
Configure the Client or Client Computer Group Level

1. In the CommCell® Browser, expand **Client Computer Groups**.
2. Right-click on **Laptop Clients** | **Properties**.
3. In the Client Group Properties, click the **Network** button and select the **Firewall Configuration** tab.
4. From the **Firewall Configuration** tab, select the box to enable **Configure Firewall Settings**. Ensure the **Basic** radio button is selected.
5. In the **Commserve Connectivity** tab select the following:
   a. “This Computer is” – “Always outside of Commserve network”.
   b. “When connecting from outside” – select **Use remote proxy** and select **Proxy** from the drop-down list.
6. In the MediaAgent Connectivity sub-tab select:
   a. “This Computer is” – “Always outside of MediaAgent Network”.
   b. “When connecting from outside” - select the **Use remote proxy** and select **Proxy** from the drop-down list.
7. Click **OK** to save the firewall configuration and click **OK** to close the properties window.
8. Right-click on the Laptop Clients group | All Tasks | Push Firewall configuration. A warning dialog box appears. Click Continue. (A window will appear with a failed attempt to push the configuration – this is due to no systems being members of the Laptop Clients group.)

9. Click OK to acknowledge the warning window.

---

**Best Practice:** When possible, use the Basic Configuration option for external client and computers. Use Advanced Configuration for Proxy and EA-2016-CS® settings.
Encryption

Commvault® offers three methods to encrypt data:

- Inline encryption - encrypts data during the backup job. Inline encryption is software based.
- Offline encryption - encrypts backup data during auxiliary copy jobs. Offline encryption is software based.
- Hardware encryption - uses LTO4 or above tape drives. Hardware encryption is performed on the drive itself.

The following chart illustrates how encryption can be used with Commvault® software and advantages / disadvantages of each method.

<table>
<thead>
<tr>
<th>Type</th>
<th>Where Encryption is Performed</th>
<th>How it is Enabled / Disabled</th>
<th>Advantages</th>
<th>Disadvantages</th>
</tr>
</thead>
<tbody>
<tr>
<td>In-Line</td>
<td>Client or Media Agent</td>
<td>Enabled on the client, activated on individual subclients. From V11, can also be activated at the storage policy primary copy.</td>
<td>Allows encryption over network and choice of encryption algorithm</td>
<td>Software based utilizes CPU &amp; memory of client or MediaAgent</td>
</tr>
<tr>
<td>Off-line</td>
<td>MediaAgent</td>
<td>Turned on/off at storage policy secondary copy</td>
<td>Does not affect primary backup windows and provides choice of encryption algorithm</td>
<td>Software based utilizes CPU &amp; memory on MediaAgent</td>
</tr>
<tr>
<td>Hardware</td>
<td>LTO4 or higher drive with encryption support</td>
<td>Turned on/off at storage policy copy</td>
<td>Hardware based faster encryption &amp; no load on client or MediaAgent</td>
<td>Requires supported hardware for backups and restores</td>
</tr>
</tbody>
</table>

Setting Inline Encryption

Inline encryption is configured in either of two areas:

1. Client Advanced Properties enables encryption and provides choice of algorithm, then can be activated on individual subclients; or
2. Subclient properties provides options to Enable on Media, Network or both (default); or Disable.
Enabling Encryption on the Client

1. In the CommCell® Browser, expand **Client Computers**.
2. Right-click on **EA-2016-CS client** | **Properties**.
3. In the Client Computer Properties for EA-2016-CS dialog box, click **Advanced**.
4. Select the **Encryption** tab and check the **Encrypt Data with the following settings** button.
5. In the **Cypher** drop-down box select **AES(Rijndael)**.
6. In the **Key Length** drop-down box, select **256**.
7. Click **OK** to save changes to the Advanced Properties.
8. Click **OK** to close the Properties page.
Configure Subclient Encryption Options

1. In the CommCell® Browser, expand Client Computers | EA-2016-CS | File System |defaultBackupSet.
2. Right-click on the Default subclient | Properties.
3. Click the Advanced button.
4. In the Encryption tab ensure the default encryption option is set to “Network and Media (Agent Side)”. If it is not, change the settings to “Network and Media (Agent Side)”.
5. Click OK to exit the “Advanced Subclient Properties” page.
6. Click OK again to exit the Main Properties page.
Setting Hardware Encryption

1. In the CommCell® Browser, expand Policies | Storage Policies | Basic Tape.
2. Right-click on the Primary copy | Properties.
3. Select the Data Paths tab | Commvault SL8500 4 data path
4. Click the Properties button at the bottom of the window.
5. Check the “Use Hardware Encryption” check box.
6. A Confirmation window will appear, read the message and click OK to continue.
7. Click OK to save the encryption settings.
8. Click OK to close the Storage Policy Copy page.
Setting Copy Based Encryption

1. In the CommCell® Browser, expand **Policies | Storage Policies | Dedupe Disk**.
2. Right-click on **Dedupe Disk | All Tasks | Create New Copy**.
3. Select/Enter the following information for the new secondary copy:
   a. **General tab**:
      i. Copy Name: **Tape Compliance Copy**
      ii. Library: **Commvault SL8500 4**
      iii. MediaAgent: **EA-2016-CS**
      iv. Drive Pool: **DrivePool(EA-2016-CS)x**
      v. Scratch Pool: **Default Scratch**
   b. **Advanced tab**:
      i. In the **Data Encryption** section click the radio button for **"Re-encrypt data using selected cipher"**.
      ii. In the **Data Encryption Algorithm** section select **"AES (Rijndael)"** for the Cipher and **256** for the Key Length.
4. Click **OK** to create the secondary encrypted copy.
Setting Media Password

The media password is used when cataloging tapes using the Media Explorer Tool. If encryption keys are placed on the media, the Media Explorer Tool prompts for the password during the tape catalog operation.

Setting CommCell® Level Media Password

1. From the Home tab of the CommCell® ribbon, select Control Panel.
2. In the CommCell section, click System and select the Change Password tab.
3. Check the box “Change Media Password”.
4. In the “Enter New Media Password” and “Confirm New Media Password” text fields, type StrongPassword.
5. In the Enter Old Media Password text box, leave it blank as no prior password has been set.
6. Click OK and then close the Control Panel.
Setting Storage Policy Level Media Password

1. In the CommCell® Browser, expand **Policies** | **Storage Policies**.
2. Right-click **CommserveDR** | **Properties**.
3. Select the **Advanced** tab and check the box to "Enable Storage Policy Level Media Password".
4. Check the box next to "Change Media Password".
5. In the "Enter New Media Password" and "Confirm New Media Password" text fields, type **CustomPassword**.
6. In the Enter Old Media Password text box, leave it **blank** as no prior password has been set.
7. Click **OK** to create the new Media Password and exit the properties page.
Extras - Commvault® Tools and Utilities

Using the Process Manager Tool

1. On the EA-2016-CS® host, click on the Process Manager icon from the Windows Taskbar.

   You can optionally click the Windows start button (lower left corner) which brings up the Windows Start desktop. From that view, click on the circled down arrow, to display the applications for the system. Look for the Commvault apps and select Process Manager.

2. Select the Services tab which displays Base Services, EA-2016-CS Services, MediaAgent Services, Replication Service, VSS Provider Service, Workflow, and Web Console services.

3. Right-click the Commvault Replication Service and click Restart.

4. Select the General tab. View the various parameters shown.

5. Select the Processes Tab. Each column can be sorted by selecting the column header. Select the Name header to sort the column in alphabetical order.

6. Right-click on the JobMgr process and note options in the drop-down box.

7. Select the Logging tab. Logging levels can be edited from this window.
Working with Commvault Technical Support, the system administrator can modify the logging level, maximum log file size, maximum number of log files, and setting the debugging wait time. These settings should only be modified while under the supervision of a Commvault Technical Support representative.

8. Close the Process Manager Tool.

Using the Commserve Recovery Assistant tool

1. Using Windows Explorer, navigate to \EA\-2016-MA\CSDR. Copy the most recent SET folder to the EA-2016-CS "Downloads" folder in Windows Explorer.

2. Navigate to c:\ Program Files\CommVault\ContentStore\Base.

3. Double-click to run CSRecoveryAssistant.exe.

4. In the CommServe Recovery Assistant box, select “Recovery” for operation type for DB Restore. Click Next.

5. From the next screen, next to the "Enter the path to the database dump folder:" entry box, click the Browse button and select the path: C:\Users\Student\Downloads\Set_xxx. This should now show the path in the window to the CommserveDR backup data that was previously copied. Click Next.

6. In the next screen, the "Enter the path to extract the database files:" entry box should be automatically populated with the database path. You can use this box to set an alternate database location (If you have changed it during the Commserve recovery).

7. On the Next window, check the summary of options you selected and click the Start Recovery button.
8. In the next recovery window, when all of the routines are marked with a green checkmark the recovery is completed. Click **Next**.

9. Click **Next** on the license screen, and when the recovery completion screen comes up, click **Finish**.

10. Open the **Process Manager** tool and start all services from the **Services tab**.

11. Log back into the CommCell® console to verify that the Database recovery was successful.

**Using the GXTail Tool**

1. On the EA-2016-CS® host, launch **Windows Explorer**. Navigate to the **C:\Program Files\Commvault\Content Store\Base** directory.

2. Double-click on **GxTail.exe**.

3. From the GxTail tool, select **File** and **Open**.

4. For the path enter **c:\Program Files\Commvault\Content Store\Log Files**.

5. Select **JobManager.log** and click **Open**.

6. View the various information in the log file such as the Process ID, Thread ID, Job ID, Process Subroutine and Job Description.

7. After viewing some of the other log files in the Program Files\Commvault\Content Store\Log Files directory, close the **GXTail** program.
Using the CVPing option to test network connectivity

1. In Windows Explorer, while holding down the Shift key, right-click the Commvault Base folder and select Open command window here.

2. Type `cvping` and press Enter. This lists the options available for the CVPing utility.

3. Type `cvping EA-2016-SERV.company.com` and press Enter. This verifies basic communication using the client hostname.

4. Type `cvping EA-2016-SERV.company.com --port 8402` and press Enter. This verifies communication for the client using port 8402.

5. Type `cvping 172.19.178.42` and press Enter. This verifies communication using the client IP address.

Using the CVIPInfo tool to get IP configuration information of a machine

1. While still in the Command Prompt window, type `cvipinfo` and press Enter. This lists the options available for the CVIPinfo utility.

2. Type `cvipinfo ipv4` and press Enter. This shows IPv4 connection information for the local host.

3. Type `cvipinfo ipv6` and press Enter. This shows IPv6 connection information for the local host.

4. Type `cvipinfo ipv4 EA-2016-SERV.company.com` and press Enter. This shows IPv4 connection information for the remote EA-2016-SERV client.
APPENDIX A: User Guide to Access CVLab environment

CommVault® Education Services
https://ea.commvault.com

Accessing and launching the CVLab environment

Go to:
https://ea.commvault.com

Log in using your Education Advantage credentials.

If you don’t know your password click the “Forgot your password” link.
In My Education Advantage, select the Courses Scheduled tab.

Locate the CVLab launcher icon:
- If the CVLab is being provided as part of a course, locate the course.
- If the CVLab has been purchased as a standalone component, locate the CommVault Virtual Lab – OnDemand course.
Click the link to launch the lab environment.

Click on the launcher button.
If a pop-up window prompts ‘Do you want to open or save…’ click Open.

Otherwise, click on the downloaded .rdp file to open the virtual machine.

If a remote desktop connection pop-up box prompts to connect to the remote computer, click Connect.

The remote desktop connection will start.

Remote connection log in credentials:
- Username: company\student
- Password: student

Note: password is all lowercase.

Click OK.
Accessing and using the CommCell® Console

To access the CommCell console click the launcher icon in the Windows Task bar.

Use the following credentials to log in to the CommCell console:

- Username: admin
- Password: admin

Note: password is all lowercase.

Click OK.

Resource Documents

Depending on the course chosen, various resource documents will be available:

- Activity Guide
- Course Guide

Return to Lab Steps