Dolby Conferencing Console Version 2.3

Installation Guide

24 April 2020

Notices

Copyright

© 2020 Dolby Laboratories. All rights reserved.

Dolby Laboratories, Inc.
1275 Market Street
San Francisco, CA 94103-1410 USA
Telephone 415-558-0200
Fax 415-645-4000
http://www.dolby.com

Trademarks

Dolby and the double-D symbol are registered trademarks of Dolby Laboratories.

The following are trademarks of Dolby Laboratories:

Dialogue Intelligence™
Dolby®
Dolby Advanced Audio™
Dolby Atmos®
Dolby Audio™
Dolby Cinema®
Dolby Digital Plus™
Dolby Digital Plus Advanced Audio™
Dolby Digital Plus Home Theater™
Dolby Home Theater®
Dolby Theatre®
Dolby Vision®
Dolby Voice®
Feel Every Dimension™
Feel Every Dimension in Dolby™
Feel Every Dimension in Dolby Atmos™
MLP Lossless™
Pro Logic®
Surround EX™

All other trademarks remain the property of their respective owners.

Patents

THIS PRODUCT MAY BE PROTECTED BY PATENTS AND PENDING PATENT APPLICATIONS IN THE UNITED STATES AND ELSEWHERE. FOR MORE INFORMATION, INCLUDING A SPECIFIC LIST OF PATENTS PROTECTING THIS PRODUCT, PLEASE VISIT http://www.dolby.com/patents.

End User Licensing Agreement

END-USER LICENSE AGREEMENT FOR DOLBY SOFTWARE

The following is Dolby’s current version of the End User License Agreement ("EULA"). Dolby may modify this End User License Agreement: (A) immediately in any way which does not reduce or degrade Reseller’s rights or benefits pursuant to the policy or (B) in all other instances, on forty five (45) days written notice; provided, however, that the End User License Agreement in effect at the time of the sale of any Product unit shall continue to govern such Product unit.

This EULA is a legal agreement between you (as an individual hereinafter referred to as "you" or "Customer") and Dolby Laboratories, Inc., a California Corporation, and Dolby International AB, a Swedish company residing in The Netherlands (collectively "Dolby") for the Dolby® software that accompanies this EULA, which includes computer software and may include associated media, printed materials, "online" and electronic documentation (collectively, the "Software"). Dolby may be providing you with the Software pursuant to a separate agreement between you (or a third party such as your employer) and one of Dolby's

licensees (a "Parent Agreement"). In the case of a conflict this EULA takes priority over the Parent Agreement and governs your use of the Software. YOU HEREBY AGREE TO BE BOUND BY THE TERMS OF THIS AGREEMENT BY ACCEPTING THIS AGREEMENT, OR BY INSTALLING, COPYING, OR OTHERWISE USING THE SOFTWARE. IF YOU DO NOT AGREE TO THE TERMS OF THIS AGREEMENT DO NOT INSTALL, COPY, OR USE THE SOFTWARE.

1. LICENSE GRANT. Dolby grants you only those rights expressly granted to you in this EULA provided that you comply with all terms and conditions of this EULA.

   1.1 Software License Grant. Dolby grants you a nonexclusive, revocable, limited, non-transferable license to (a) install and run the Software solely for the purpose of using the Dolby Conference Phone or if applicable, accessing the conferencing service solutions provided under the Parent Agreement and (b) make one copy of the Software solely for backup or archival purposes.

   1.2 Documentation. You may make and use an unlimited number of copies of the documentation, if any, provided that such copies shall be used solely for your own use in association with the Software and are not to be republished nor distributed (in hard copy, electronic or any other form) beyond your premises or to any third party.

   1.3 Beta Materials. The following apply to any Software provided as “pre-release” or “beta:” (a) You shall identify errors, potential improvements, and provide other feedback to Dolby about the pre-release or beta Software as reasonably requested by Dolby, and (b) Dolby reserves the right not to commercially release pre-release or beta Software or, if it does so, to alter prices, features, specifications, capabilities, functions, licensing terms, release dates, and other characteristics of the commercial release.
2. RESERVATION OF RIGHTS AND OWNERSHIP. Dolby reserves all rights not expressly granted to you in this EULA. The Software is protected by copyright, patent and/or other intellectual property laws and treaties and contains trade secrets of Dolby and its suppliers. Dolby and its suppliers own the title, copyright, and other intellectual property rights in the Software. Notwithstanding any statements to the contrary contained in any terms of sale for the Software, the Software is licensed, not sold and Dolby retains ownership of all copies of the Software.
3. LIMITATIONS ON LICENSE. You are expressly prohibited from using the Software in any manner not specifically authorized by Dolby in this EULA. You may not make any copies of the Software except and to the extent necessary for backup and archival purposes. You may not modify, create derivative works, reverse engineer, decompile, or disassemble the Software, except and only to the extent that such activity is expressly permitted by applicable law notwithstanding this limitation. You may not rent, lease, lend or provide commercial hosting services with the Software. You may not delete, fail to reproduce or modify any patent, copyright, trademark or other proprietary rights notices which appear on or in the Software or documentation. No license, right, or interest in any Dolby trademark, trade name or service mark is granted to you pursuant to this EULA.
4. TERMINATION. Without prejudice to any other rights, Dolby may immediately terminate this EULA if you are in material breach of any of the terms or conditions of Sections 1-3 of this EULA which has not been remedied within 14 days of written notice from Dolby to you. In such event, you must immediately cease using the Software and destroy all copies of the Software and all of its component parts.
5. REPRESENTATIONS AND WARRANTIES.

   5.1 You represent, warrant, and covenant that your use of the Software will at all times comply with the terms of this EULA, applicable laws and regulations and that you will not install, use, access, or run the Software for purposes other than using the Dolby Conferencing Console or if applicable, accessing the conferencing services provided under the Parent Agreement.

   5.2 Dolby represents and warrants that (a) it owns or has the right to license the Software and (b) that the Software is complete, correct, effective, and capable of meeting the specifications included in the documentation, if any, provided under the Parent Agreement. Your sole remedy for breach of the foregoing representation in Section 5.2(b) shall be Dolby's commercially reasonable efforts to redeliver the affected Software.

6. DISCLAIMER OF WARRANTIES. EXCEPT AS OTHERWISE SET FORTH ABOVE, DOLBY MAKES NO WARRANTIES REGARDING THE SOFTWARE. FURTHER, TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW, DOLBY AND ITS SUPPLIERS PROVIDE THE SOFTWARE AS IS, AND HEREBY DISCLAIM ALL OTHER WARRANTIES, WHETHER EXPRESS, IMPLIED OR STATUTORY, INCLUDING, BUT NOT LIMITED TO, ALL IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, AND NONINFRINGEMENT, AND ANY WARRANTIES ARISING OUT OF COURSE OF DEALING, USAGE OR TRADE. THERE IS NO WARRANTY THAT THE SOFTWARE WILL OPERATE IN THE COMBINATIONS THAT YOU MAY SELECT FOR USE, THAT THE OPERATION OF THE SOFTWARE WILL BE ERROR-FREE OR UNINTERRUPTED OR THAT ALL SOFTWARE ERRORS WILL BE CORRECTED. NO ADVICE OR INFORMATION, WHETHER ORAL OR WRITTEN, OBTAINED FROM DOLBY OR ELSEWHERE WILL CREATE ANY WARRANTY NOT EXPRESSLY STATED IN THIS AGREEMENT. THE ENTIRE RISK AS TO THE QUALITY, OR ARISING OUT OF THE USE OR PERFORMANCE OF THE SOFTWARE REMAINS WITH YOU.
7. EXCLUSION OF INCIDENTAL, CONSEQUENTIAL AND CERTAIN OTHER DAMAGES. IN NO EVENT WILL DOLBY BE LIABLE TO YOU FOR ANY SPECIAL, INCIDENTAL, INDIRECT, PUNITIVE OR CONSEQUENTIAL DAMAGES (INCLUDING LOSS OF USE, DATA, BUSINESS OR PROFITS) OR FOR THE COST OF PROCURING SUBSTITUTE PRODUCTS OR SERVICES ARISING OUT OF OR IN CONNECTION WITH THIS AGREEMENT OR THE USE OR PERFORMANCE OF THE SOFTWARE, WHETHER SUCH LIABILITY ARISES FROM ANY CLAIM BASED UPON CONTRACT, WARRANTY, TORT (INCLUDING NEGLIGENCE), STRICT LIABILITY OR OTHERWISE, AND WHETHER OR NOT DOLBY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH LOSS OR DAMAGE. YOU AGREE THAT THESE LIMITATIONS WILL SURVIVE AND APPLY EVEN IF ANY LIMITED REMEDY SPECIFIED IN THIS AGREEMENT IS FOUND TO HAVE FAILED OF ITS ESSENTIAL PURPOSE.
8. LIMITATION OF LIABILITY AND REMEDIES. NOTWITHSTANDING ANY DAMAGES THAT YOU MIGHT INCUR FOR ANY REASON WHATSOEVER (INCLUDING, WITHOUT LIMITATION, ALL DAMAGES REFERENCED HEREIN AND ALL DIRECT OR GENERAL DAMAGES IN CONTRACT OR ANYTHING ELSE), THE ENTIRE LIABILITY OF DOLBY AND ANY OF ITS SUPPLIERS UNDER ANY PROVISION OF THIS EULA AND YOUR EXCLUSIVE REMEDY HEREUNDER (OTHER THAN THE LIMITED REMEDY DESCRIBED IN SECTION 5.2 ABOVE) SHALL BE LIMITED TO THE AMOUNT OF USD$10.00 (TEN US DOLLARS). THE FOREGOING LIMITATIONS, EXCLUSIONS AND DISCLAIMERS (INCLUDING SECTIONS 6,7 AND 8) SHALL APPLY TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW, EVEN IF ANY REMEDY SPECIFIED IN THIS AGREEMENT IS FOUND TO HAVE FAILED OF ITS ESSENTIAL PURPOSE.
9. GOVERNING LAW: The validity, interpretation and performance of this Agreement shall be governed by and construed in accordance with the laws, without respect to conflict of laws provisions, and you agree to submit to the jurisdiction of the court, set forth below based on the applicable region where you are located:

Region	Governing law	Court jurisdiction
Countries in the European Economic Area	England	English Courts
All other countries	State of California, USA	State or Federal Courts located in San Francisco, CA
People’s Republic of China	State of California, USA	Arbitration at the Hong Kong International Arbitration Centre in accordance with the UNCITRAL Arbitration Rules ("UNCITRAL Rules"). The arbitration tribunal shall consist of one arbitrator to be appointed according to the UNCITRAL Rules. The language of the arbitration shall be English.

Notwithstanding the foregoing, nothing in this Section 9 shall prevent Dolby from seeking any injunctive or equitable relief by a court of competent jurisdiction that is necessary to protect Dolby's rights or property until such dispute is resolved. This Agreement will be interpreted and construed in accordance with the English language. The parties agree that the provisions of the Uniform Computer Information

Transactions Act ("UCITA") and the U.N. Convention on Contracts for the International Sale of Goods will have no force or effect on these terms and conditions.

10. THIRD PARTY SOFTWARE AND / OR OPEN SOURCE. The Software contains open source components and other third party components, subject to the applicable licensing terms and conditions. From time to time, Dolby may include additional third party software and components subject to third party terms and conditions of use. For more information about these software components, see the following:

- www.dolby.com/us/en/about/warranty-and-maintenance-policies.html
- *Dolby Conferencing Console open source software guide*

Contents

1 Introduction to this guide....8
1.1 About this documentation....9
1.2 Related documentation....9
1.3 Accessing API documentation....9
1.4 Problem reports....10
1.5 Documentation feedback....10

2 Architectural overview....11
2.1 Dolby Conferencing Console....12
2.2 Architecture....12
2.3 Security features....14

3 Requirements....15
3.1 Supported installation types....16
3.2 Minimum hardware specifications....16
3.2.1 Device access service node requirements....17
3.3 Supported operating systems....17
3.4 Supported browsers....17
3.5 Supported devices and device numbers....17
3.6 Network requirements....18
3.6.1 Network ports....18
3.6.2 Network security....18
3.7 Additional requirements and considerations for RPM deployments....19
3.7.1 Single-server RPM deployment requirements....19
3.7.2 Multiple-server RPM deployment requirements....21
3.7.3 Redis server requirements....22
3.7.4 Master node requirements....23
3.7.5 Database server requirements....23
3.7.6 File-storage server requirements....23

4 Installation....24
4.1 Available software packages....25
4.2 Open virtual appliance deployments....25
4.2.1 Installing with the open virtual appliance....25
4.3 RPM deployments on CentOS and RedHat....26
4.3.1 Installing a database....26
4.3.2 Installing and configuring a Redis server....28
4.3.3 Installing with the RPM package on a server....30
4.3.4 Installing with the RPM package on multiple servers....33
4.4 RPM deployments on Amazon Linux....34
4.4.1 Creating an AWS EC2 instance....34
4.4.2 Installing a database....35
4.4.3 Installing and configuring a Redis server....36

4.4.4 Installing with the RPM package on a server....37
4.4.5 Installing Dolby Conferencing Console on multiple AWS servers....39
4.5 Setting up file storage for multiple servers....39
4.6 Accessing file storage server....40
4.7 RPM deployments with redundancy....42
4.7.1 Setting up master node redundancy....42
4.7.2 Installing and configuring a Redis server....44
4.7.3 Setting up device access service node redundancy....46
4.7.4 Setting up database redundancy....47
4.8 Setting up secure access....47
4.8.1 Changing the host name....48
4.8.2 Replacing the default certificate with a new self-signed certificate....48
4.8.3 Replacing the default server certificate with a CA certificate....49
4.8.4 Connecting a device over HTTPS....50
4.8.5 Configuring HTTP and HTTPS access....51
4.8.6 Enabling SSH access on open virtual appliance file installations....52
4.9 Setting the time zone....52

Glossary....54

1

Introduction to this guide

The Dolby Conferencing Console software provides an interface for IT administrators to use in managing Dolby Voice Devices.

As an administrator, you can use the Dolby Conferencing Console software to provision devices, assemble them into device pools for ease of management, obtain analytic information about them, and monitor device status on both an individual and group level.

- About this documentation
- Related documentation
- Accessing API documentation
- Problem reports
- Documentation feedback

1.1 About this documentation

IT administrators can use this documentation as a guide for installing the Dolby Conferencing Console software.

We assume that users of this guide are IT administrators or equivalent and are familiar with:

- Basics of computer networking and Linux administration
- IP private branch exchange (PBX) call controls used by your organization
- Conferencing service provider functionality used by your organization

This guide provides details on:

- Installing the Dolby Conferencing Console software either on Linux (natively) or as a virtual appliance
- Using the Dolby Conferencing Console software to manage individual devices or groups of devices

1.2 Related documentation

The documentation for the Dolby Voice product family consists of software documentation, release notes, and guides. Several of these guides are especially useful for users of the Dolby Conferencing Console software.

The describes how to administer Dolby Conferencing Console.

The *Dolby Conferencing Console Open Source Software Guide* describes third-party open-source software that is incorporated into the Dolby Conferencing Console software.

The *Dolby Conference Phone Administrator's Guide* describes how to install and administer the Dolby Conference Phone.

The *Dolby Conference Phone User's Guide* describes how to use the basic and advanced phone features, and how to customize the phone.

The *Dolby Voice Room Quick Start Guide* describes the contents of the Dolby Voice Room package, how to assemble the Dolby Conference Phone, the Dolby Voice Camera, Dolby Voice Hub, and how to connect Dolby Voice Room to the network. The quick start guide is included in the Dolby Voice Room package. It is also available from the Dolby Voice Room support pages.

The *Dolby Voice Room Administrator's Guide* describes how to install and administer the Dolby Voice Room system.

The *Dolby Voice Room Third-Party Software Guide* describes the open source software used in the Dolby Voice Room software.

The *Dolby Voice Product Compatibility Guide* describes the compatibility relationships between the various Dolby Voice Devices.

1.3 Accessing API documentation

You can access application programming interface (API) documentation for the Dolby Conferencing Console software from the user interface.

Procedure

1. From the Dolby Conferencing Console web interface, on the home screen, click the settings button in the upper-right corner.

2. Click the **References** tab.
3. Click the **Web API reference** link and it will open in a new tab.

1.4 Problem reports

When escalating issues to Dolby, please provide answers to these questions.

- Which version of the product is affected?
- When did the problem occur? How often does it occur? Is there any pattern or trend to the occurrence?
- What was the scope of the problem? How many users did it affect? Was there any pattern or trend to the affected users?
- Have you been able to reproduce the problem? If so, please detail how.
- Is there anything that you think might be relevant in the log? Did anything unusual occur? Did the system generate any high-severity log messages? If so, please attach an extract.
- What operating system and version are being used by the user? What browser and version are being used by the client?
- What other observations have you made? Is there anything else you think might assist us in identifying the root cause of the problem?

1.5 Documentation feedback

If you have comments or feedback about this documentation, send us an email at dolbyvoicedocs@dolby.com.

2

Architectural overview

This chapter describes the Dolby Conferencing Console product architecture.

- Dolby Conferencing Console
- Architecture
- Security features

2.1 Dolby Conferencing Console

The Dolby Conferencing Console software allows IT administrators to provision, configure, and administer devices.

Using the Dolby Conferencing Console software, you can:

- Bulk provision and configure devices
- Establish secure network communications between devices and the Dolby Conferencing Console software
- Remotely access device status information, make changes, and restart devices
- Obtain statistical status usage information for devices
- Manage inventory

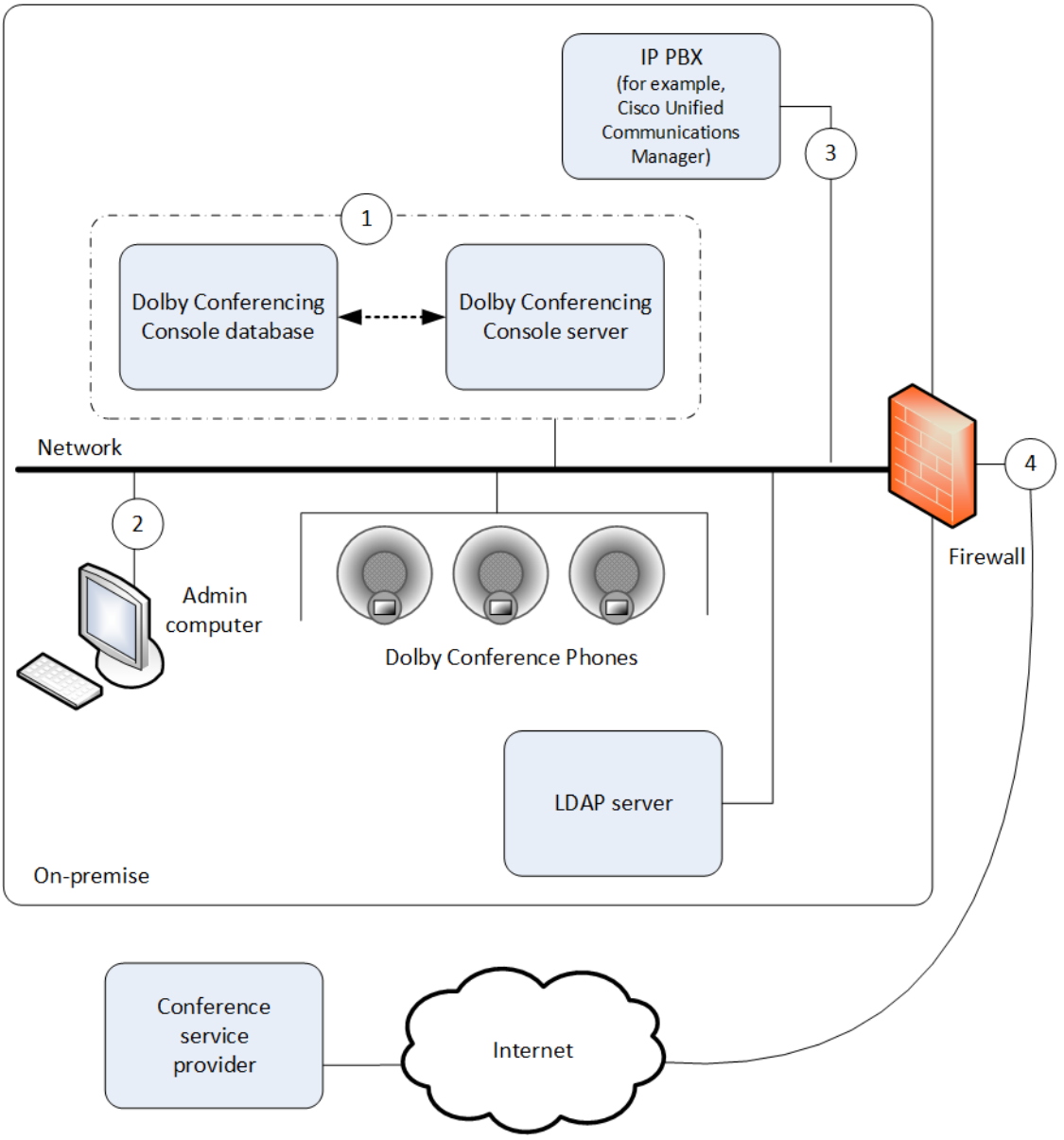
2.2 Architecture

This section provides a high-level overview of how the Dolby Conferencing Console software works with the rest of your network.

The exact architecture of your Dolby Conferencing Console software solution depends on whether you use the open virtual appliance (OVA) file or RPM Package Manager (RPM) method of installation. This high-level diagram shows an open virtual appliance file deployment of the Dolby Conferencing Console software. For information and diagrams of other deployments, see:

- Single-server RPM Package Manager deployment requirements on page 19
- Multiple-server RPM Package Manager deployment requirements on page 21

Figure 1: Open virtual appliance deployment of the Dolby Conferencing Console software



Key:

1. The Dolby Conferencing Console software stores data about devices and their usage to a database for administration. When you perform an open virtual appliance file deployment, the database is automatically created on the same physical or virtual hardware as the Dolby Conferencing Console server (as represented by the dashed line). You do not need create the database separately yourself. However, if you decide to perform an RPM deployment instead, then you will need to create and configure the database yourself.
2. Administrators can manage profiles, pools, and devices from a convenient interface on their computer.
3. The Dolby Conference Phone uses a Session Initiation Protocol (SIP) IP connection to your PBX. Cisco Unified Communications Manager is supported. For information about what other IP PBXs are supported, see the *Dolby Conference Phone administrator's guide* .
4. Secure communication through firewall to the conferencing service.

2.3 Security features

The Dolby Conferencing Console software allows you to secure all components, communications, and devices.

User authentication with Lightweight Directory Access Protocol (LDAP)
You can use LDAP for user authentication. Once configured, LDAP users can log in with their corporate user name and password.

User authentication with SAML
You can use SAML for single sign-on. SAML authentication can be used with any SAML 2.0 identity provider, such as Okta.

Retrieve passwords with Simple Mail Transfer Protocol (SMTP)
You can use SMTP to allow non-LDAP/SAML users to retrieve passwords on their own.

Device access

You can choose to use Hypertext Transfer Protocol (HTTP) or Hypertext Transfer Protocol Secure (HTTPS) from the Dolby Conferencing Console software.

You can use the utility provided in the Dolby Conferencing Console software to generate a self-signed certificate, or you can provide a certificate authority (CA) certificate.

Access password encryption
All Dolby Conferencing Console account passwords are encrypted when stored on the server.

Rogue device access prevention
You can specify device access restrictions for each device pool to help protect against botnets and other threats.

Password fields
Passwords are obfuscated upon entry so that the password values cannot be hijacked.

Network ports
Upon install, the default port 80 allows initial access for the web user interface (UI). Root user access through port 22 (SSH) is disabled.

3

Requirements

This chapter describes the Dolby Conferencing Console supported hardware, software, and installation requirements.

- Supported installation types
- Minimum hardware specifications
- Supported operating systems
- Supported browsers
- Supported devices and device numbers
- Network requirements
- Additional requirements and considerations for RPM deployments

3.1 Supported installation types

Before you install the Dolby Conferencing Console software, review the two types of available installations. Choose the installation that makes the most sense based on your environment and goals.

Open virtual appliance (OVA) installation	RPM installation
The Dolby Conferencing Console software can be installed as a virtual appliance. The Dolby Conferencing Console software is available in the *.ova* file format.	The Dolby Conferencing Console software can be installed as a stand-alone application with RPM, which is a command-line utility. The Dolby Conferencing Console software is available in the *.rpm* file format.
Install the *.ova* file on one of these popular virtual machine (VM) environments: • VMware Workstation Player 5.0 or later • VMware vSphere 5.0 or later • Oracle VM VirtualBox 5.0.10 or later	Install the RPM package on a Linux-based computer or Linux-based virtual machine running one of these operating systems: • CentOS 6.0 and 7.0 • RedHat Enterprise Linux 6 and 7 • Amazon Linux (for Amazon Web Services (AWS)) **Note:** Amazon Linux 2 is not supported

Which installation to use

For trials and small- to medium-scale deployments (less than 500 Dolby Voice Devices), we recommend that you install the Dolby Conferencing Console software on virtual machines by using the *.ova* installation file. This is the simplest installation process and requires 30 minutes or less.

For other deployments, especially those involving more than 500 Dolby Voice Devices and where scalability is important, we recommend that you install the Dolby Conferencing Console software on Linux-based computers by using the RPM package.

3.2 Minimum hardware specifications

The Dolby Conferencing Console software requires a minimum hardware specification on both physical and virtual servers.

The minimum physical or virtual hardware specification for a single-server deployment is:

- Quad-core 64-bit Intel-compatible central processing unit, 2.2 GHz or greater
- 8 GB RAM
- 250 GB hard disk
- 1 Gbps Ethernet interface

For multi-server deployment hardware requirements, see Multiple-server RPM Package Manager deployment requirements on page 21.

For AWS installations, a `t2.xlarge` EC2 instance meets the minimum specification.

A minimum of 1GB of space is required for the */tmp* directory. This is needed for processing firmware files in their uncompressed state.

A minimum of 50GB of space is required for installation and minimal log storage. You need to allocate additional space based on how many log files you want to keep.

Dolby Voice device log files average approximately 2MB - 4MB per hour in a call.

For example, if you have 100 Dolby Voice devices provisioned and your devices average four hours of calls per day, you need to allocate approximately 50GB of space to save 30 day's worth of call logs (100*4MB*4*30 = 48GB).

If you add it to the base DCC disk space requirement of 50GB, you need to allocate a total of 100GB.

Note:

The Dolby Conferencing Console software should be installed on a separate server from the ones being used to run the conferencing service provider and/or the IP PBX call control platform.

3.2.1 Device access service node requirements

Device access service nodes serve a different purpose than the master node. They manage device traffic.

How many device access service nodes you have and where they are on your network depend on these factors:

- For every 3,000 devices, you need one device access service node to handle device traffic. For example, if you have 10,000 devices, you need one master node and four separate, external device access service nodes.
- By default, master nodes have an internal device access service node and will handle all device traffic. However, once you add external device access service nodes for multiple-server deployment, the master node handles very little of the device traffic and the external device access service nodes start handling the traffic instead.
- Because a master node includes an internal device access service node by default, single-server deployments do not require external device access service nodes. In this case, the master node can handle all of the device traffic on its own.
- Multiple-server deployments involve more devices, so additional device access service nodes are required to handle device traffic.
- For multiple-server installations, you install the Dolby Conferencing Console software on multiple hardware instances, but you change mode to das on all device access service nodes except for the master node. This changes those servers from master nodes to device access service nodes.

3.3 Supported operating systems

The Dolby Conferencing Console software is supported on specific versions of Linux.

You can install the Dolby Conferencing Console software on these operating systems:

- CentOS 6.0 and 7.0
- Red Hat Enterprise Linux 6 and 7
- Amazon Linux

Note: Amazon Linux 2 is not supported.

3.4 Supported browsers

Accessing the Dolby Conferencing Console web interface requires a supported web browser.

You can access the Dolby Conferencing Console web interface by using any of these web browsers:

- Apple Safari 11
- Google Chrome 65
- Microsoft Internet Explorer 11
- Mozilla Firefox 59

3.5 Supported devices and device numbers

The Dolby Conferencing Console software supports Dolby Voice Devices.

If you install with open virtual appliance file, up to 500 devices per customer site are supported per each instance of the Dolby Conferencing Console software.

If you install with the RPM package, up to 10,000 devices per customer site are supported when multiple Dolby Conferencing Console nodes are installed.

3.6 Network requirements

The Dolby Conferencing Console software has specific requirements for network services, connectivity, ports, and security.

The minimum network requirements include:

- A Domain Name System (DNS) server
- A Dynamic Host Configuration Protocol (DHCP) server
- HTTP or HTTPS connectivity between the locations where you will deploy the devices

3.6.1 Network ports

Certain network ports allow the Dolby Conferencing Console software to interact with and manage Dolby Voice Devices. They also allow you to remotely access the Dolby Conferencing Console software from administrator computers.

- 22: SSH

  Note:

  For AWS deployments, opening this port is optional, and may be convenient for system administration tasks such as installing software updates.
- 80: HTTP, default network access port for web UI and provisioning
- 443: HTTPS
- 10000: Webmin

Check your network and firewall configurations to make sure that these ports are open.

When you install using the open virtual appliance file, these ports are open on the Dolby Conferencing Console software by default. However, when you install with RPM, the ports are closed by default and the administrator must open them. If the ports remain closed, you will not be able to use the Dolby Conferencing Console software to manage your Dolby Voice Devices.

3.6.2 Network security

We recommend certain network security measures.

Firewalls

Ensure that the standard ports for HTTP (80) and HTTPS (443) are open for incoming connections on the server that hosts the Dolby Conferencing Console software. Run one of these commands as root to enable the required connectivity on the server:

For Redhat 6 and CentOS 6.0

```
iptables -I INPUT -p tcp -m tcp --dport 80 -j ACCEPT
iptables -I INPUT -p tcp -m tcp --dport 443 -j ACCEPT
iptables -I INPUT -p tcp -m tcp --dport 10000 -j ACCEPT
service iptables save
```

For Redhat 7 and CentOS 7.0

```
firewall-cmd --zone=public --add-service http --permanent
firewall-cmd --zone=public --add-service https --permanent
firewall-cmd --zone=public --add-port=10000/tcp --permanent
firewall-cmd --reload
```

Certificates

The Dolby Conferencing Console software includes a default certificate that is available for use upon startup. It is a good idea to set up secure access by creating and using your own certificates.

TLS

Transport Layer Security (TLS) version 1.2 is required if any of the Dolby Voice Devices in your environment are running firmware version 3.1 or later.

To limit Dolby Conferencing Console to TLS version 1.2, add this line to */etc/dcc/web.ini*:

```
ssl_protocols TLSv1.2;
```

3.7 Additional requirements and considerations for RPM deployments

Use the RPM package for medium and large-scale deployments that include up to 10,000 devices.

Before you install the Dolby Conferencing Console software using the RPM package, make sure you can answer some basic questions about the needs of your company and about your environment.

You can use the RPM package in different ways, including single-server and multiple-server deployments, which are described in this document.

You can also take multiple-server deployments one step further by adding redundancy. For information about setting up redundancy, see RPM deployments with redundancy on page 42.

Review all of the information about deployment in this document and then consider your answers to these important questions:

- How many devices will you have (for example, 500 Dolby Voice Devices or less, or up to 10,000 Dolby Voice Devices)?
- Will you perform a single-server deployment or multiple-server deployment?
- On what physical or virtual hardware will you install the Dolby Conferencing Console software?
- For multiple-server deployments, how many external device access service nodes do you need to handle device traffic? What physical or virtual hardware will use for those servers?
- For multiple-server deployments, which server will be the master node? Which servers will be device access service nodes?
- For multiple-server deployments, do you want redundancy?
- Where will your database server be?
- Where will your file storage server be?

To learn more about terms such as master node and device access service, review the Related information.

3.7.1 Single-server RPM deployment requirements

There are specific requirements for deploying Dolby Conferencing Console with the RPM package when using a single virtual or physical server running Dolby Conferencing Console software and its supporting server software packages.

A single-server deployment can support up to 500 devices. You will need:

- At least one administrator computer
- At least one instance of physical or virtual hardware running the Dolby Conferencing Console software. This may be referred to as the Dolby Conferencing Console server or the master node.
- Three supporting software servers:
  - A database server

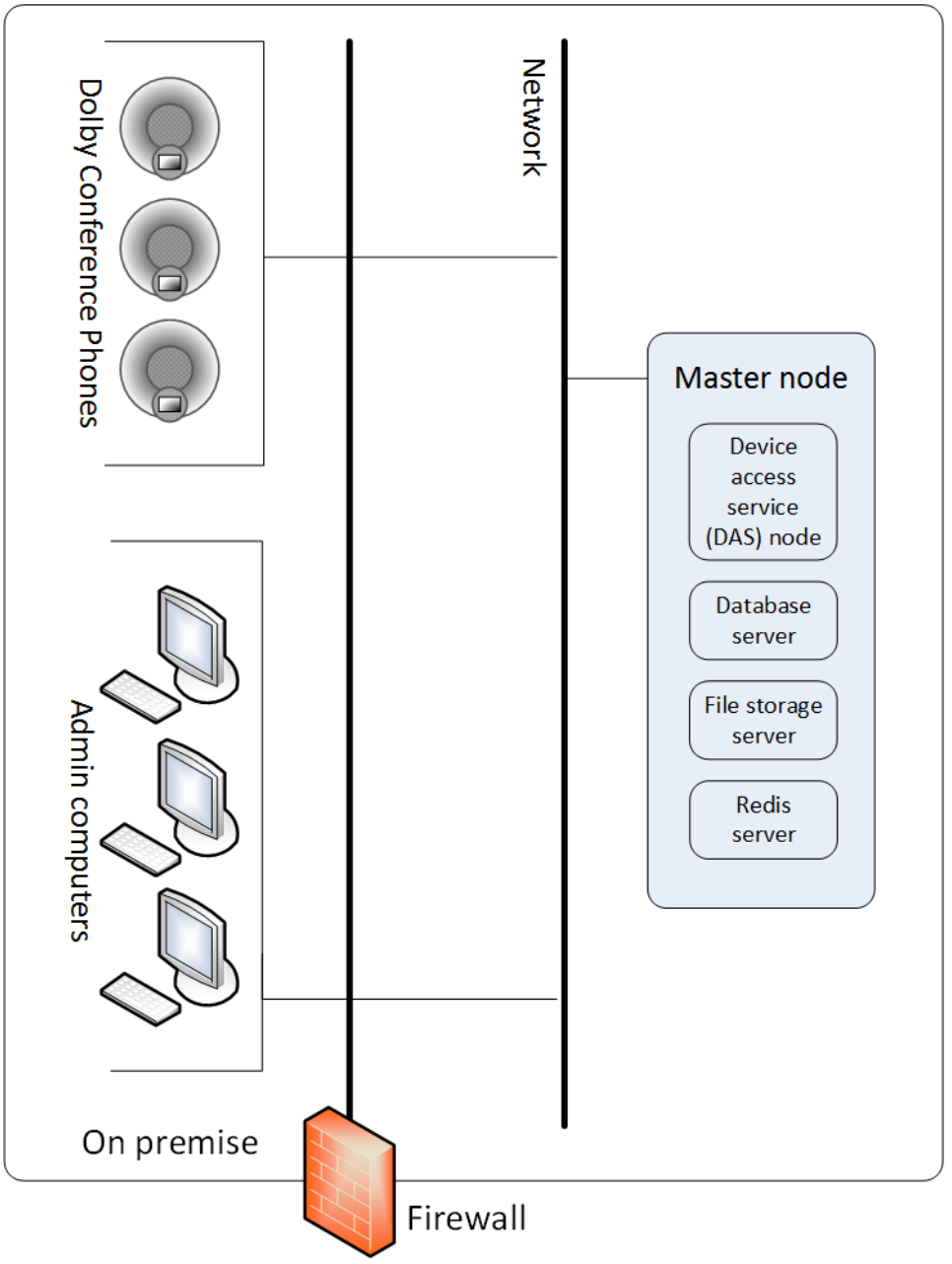
- A file storage server
- A Redis server

These supporting software servers are typically installed on the same physical or virtual hardware as the Dolby Conferencing Console software. However, they may optionally be installed on separate physical or virtual hardware on the local network.

For more information about different types of nodes, see:

- Master node requirements on page 23
- Device access service node requirements on page 17

Figure 2: RPM deployment with a single Dolby Conferencing Console server



3.7.2 Multiple-server RPM deployment requirements

There are specific requirements for deploying the Dolby Conferencing Console software with the RPM package to support 500–10,000 devices when using multiple servers running Dolby Conferencing Console software.

You will need:

- At least one administrator computer.
- One master node: This is an instance of physical or virtual hardware running the Dolby Conferencing Console software with `mode` set to `master`.

  The master node server (and its backup node, if present) must have a dual-core 64-bit Intel-compatible CPU, 2.2 GHz or greater, and at least 4 GB of RAM.
- At least one device access service node, separate from the master node: These are instances of physical or virtual hardware running the Dolby Conferencing Console software with `mode` set to `das`.

  The device access service node servers must have a 64-bit Intel-compatible CPU, 2.2 GHz or greater, and at least 2 GB of RAM.
- One or more database servers: These are completely separate from all instances of physical or virtual hardware running the Dolby Conferencing Console software.

  The database servers must have a quad-core 64-bit Intel-compatible CPU, 2.2 GHz or greater, and at least 8 GB of RAM.
- One Redis server: this component serves as a memory cache and as a point of communication between the solution components.

  The Redis server must have a quad-core 64-bit Intel-compatible CPU, 2.2 GHz or greater, and at least 8 GB of RAM.
- One file-storage server: This must be accessible to all Dolby Conferencing Console nodes (the master node and device access service nodes).

  The file storage server must have a 64-bit Intel-compatible CPU, 2.2 GHz or greater, and at least 2 GB of RAM.

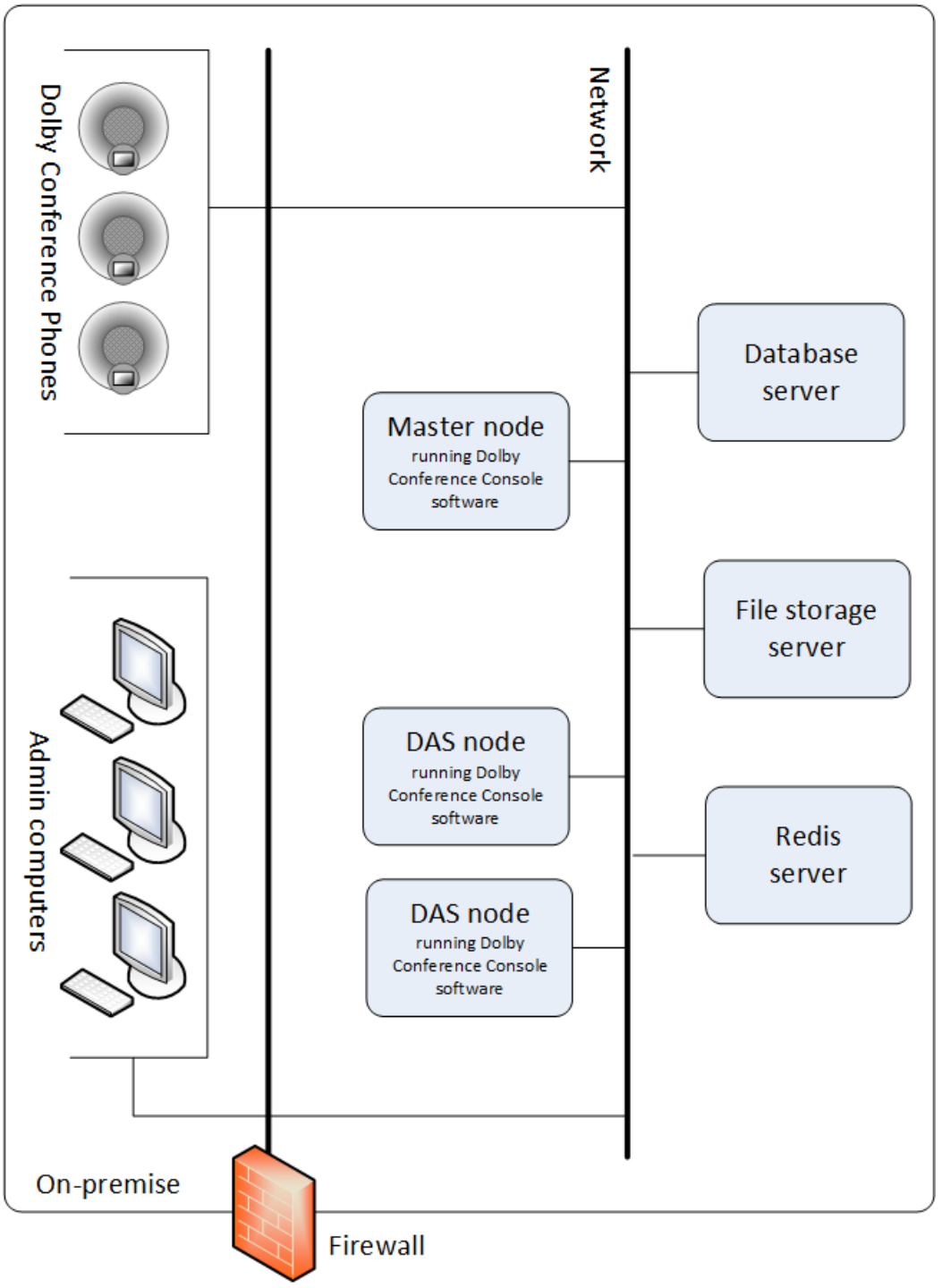
All of the physical and virtual servers must meet these hardware requirements, in addition to the requirements stated above:

- 250 GB hard disk
- 1 Gbps Ethernet interface

For more information about different types of nodes, see:

- Master node requirements on page 23
- Device access service node requirements on page 17

Figure 3: RPM deployment with multiple Dolby Conferencing Console servers



3.7.3 Redis server requirements

The Dolby Conferencing Console requires a Redis server to serve as a memory cache and a point of communication between multiple components.

Before you set up a Redis server for Dolby Conferencing Console, determine which version of Redis you require based on the number of devices at your site.

CentOS version 6.0 includes Redis version 2.4 in the Extra Packages for Enterprise Linux (EPEL) repository by default. This version of Redis can support up to 6,000 devices. However, if you have more than 6,000 devices, Redis version 3.0 is required because it can support up to 10,000 devices.

If you have more than 6,000 devices, you have these options:

- Use CentOS version 6.0 and then upgrade to Redis version 3.0.
- Use CentOS version 7.0, which comes with Redis version 3.0.

The Redis server can use CentOS, Ubuntu, RedHat, or Debian as its operating system.

3.7.4 Master node requirements

The master node manages communications between the Dolby Conferencing Console server (master node), device access service nodes, database servers, and file-storage server.

- Only one active master node is required per deployment. This applies to both single-server and multiple-server deployments.
- The master node is an instance of physical or virtual hardware running the Dolby Conferencing Console software with mode set to `master`. When you install the Dolby Conferencing Console software with the RPM package, the hardware is set this way by default.

3.7.5 Database server requirements

Both single-server and multiple-server installations require a database server. For high availability, you may need multiple database servers.

The procedures for setting up the database are slightly different, depending on the type of installation you choose:

- For single-server installations, the database server can be on the same physical or virtual hardware as the Dolby Conferencing Console server. However, this is not a requirement. You can choose to use a separate database server that is somewhere else on the network.
- For multiple-server installations, the database server must be completely separate from the Dolby Conferencing Console server.
- For multiple-server installations where the database server is not colocated in the same master node and any device access service nodes, confirm that the connection between the Dolby Conferencing Console server and the database is functioning. If you use a database on another host, add the DB_HOST variable to */etc/dcc/settings.ini* and confirm that port 5432 is reachable on DB_HOST.
- For single-server installations, the database server does not have to be separate from the file-storage server.

3.7.6 File-storage server requirements

Both single-server and multiple-server installations require a file-storage server. Only one file-storage server is required per deployment.

- For single-server installations, the file-storage server can be on the same physical or virtual hardware as the Dolby Conferencing Console server. However, this is not a requirement. You can choose to use a separate file-storage server that is somewhere else on the network.
- For multiple-server installations, you must use a file-storage server that is accessible to all Dolby Conferencing Console nodes (the master node and any device access service nodes).

4

Installation

You have several options for installing the Dolby Conferencing Console software and setting up the system. Read through this chapter, and choose the options that best suit your needs.

- Available software packages
- Open virtual appliance deployments
- RPM deployments on CentOS and RedHat
- RPM deployments on Amazon Linux
- Setting up file storage for multiple servers
- Accessing file storage server
- RPM deployments with redundancy
- Setting up secure access
- Setting the time zone

4.1 Available software packages

Dolby Conferencing Console software packages are available for download from http://download.dolbyvoice.com.

These software packages are available:

- *dcc-2.3.0.*.ova* (for open virtual appliance file installations)
- *dcc-2.3.0.*-1.el6.x86_64.rpm* (for Linux RPM installations on RedHat/CentOS 6)
- *dcc-2.3.0.*-1.el7.x86_64.rpm* (for Linux RPM installations on RedHat/CentOS 7)
- *dcc-2.3.0.*-1.amzn.x86_64.rpm* (for AWS installations)

Note: AWS version 2 is currently not supported.

After installation, we recommend that you periodically check with your provider for updates.

4.2 Open virtual appliance deployments

For trials and small-scale deployments (less than 500 Dolby Voice Devices), we recommend that you install the Dolby Conferencing Console software on virtual machines using the open virtual appliance file. This is the simplest installation process and requires 30 minutes or less.

Keep in mind:

- The open virtual appliance file is used to create a new virtual machine on your computer, and contains a complete installation of the Dolby Conferencing Console software.
- The new virtual machine (the guest system) for the Dolby Conferencing Console software is based on a Linux operating system (the guest operating system).

Note:

The default Linux password for the `root` account on the virtual machine is `dolby`. The default account for the Dolby Conferencing Console software is `admin`, with the password `admin`.

We recommend that you change these passwords after installing the virtual machine. If you are working with an already-installed virtual machine, keep in mind that a colleague may have already changed one or both passwords.

4.2.1 Installing with the open virtual appliance

Before you begin, make sure you know which virtual machine application you want to use.

About this task

Note: This topic assumes that you know how to use third-party virtual machine applications such as VMware Workstation Player 5.0 or later, VMware vSphere 5.0 or later, and Oracle VM VirtualBox 5.0.10 or later. These are applications that install and run virtual machines. Specific directions about how to use these applications is beyond the scope of this document.

Procedure

1. If needed, install a virtual machine application on your computer.
2. Click the *.ova* file (*dcc-2.3.0.ova*) to open it with your virtual machine application.

   The *.ova* file is a virtual appliance or appliance. The virtual machine application imports it.

   For example, if you use Oracle VM VirtualBox:

   - When you open the file, the **Appliance settings** screen appears.
   - You can see that **Virtual System I** is named **DCC-2.3.0**.

3. Follow the onscreen prompts to import the Dolby Conferencing Console software.

   For example, if you use Oracle VM VirtualBox, after you click the **Import** button, there is a new virtual machine named **DCC-2.3.0** on your computer.
4. Configure the virtual machine.
   a) Choose the imported virtual machine.
   b) Click **Settings** > **System**.
   c) Change the base memory to 8192 media block (MB) under the **Motherboard** tab.
   d) Change the number of processors to 4 under the **Processor** tab.
   e) Click **OK** to save your changes.
5. Start the Dolby Conferencing Console virtual machine.
6. On the virtual machine, from the command line, log in to the Dolby Conferencing Console software with the default user name (`root`) and password (`dolby`).

   Note: User names and passwords are case sensitive. We recommend that you change the password from the default as soon as possible for security reasons.
7. Use the `ifconfig` command to obtain the IP address of the Dolby Conferencing Console server.

   For example:

```
dcc login: root
Password: dolby
[root@dcc ~]# ifconfig
eth0    Link encap:Ethernet HWaddr 08:00:27:02:85:00 HW Address HWaddr
08:00:27:02:85:00
        inet addr: 10.112.100.167  Bcast 10.112.101.255  Mask: 255.255.254.0
```

8. From an Internet browser, perform these steps to open the Dolby Conferencing Console UI:
   a) Enter the IP address of the Dolby Conferencing Console software (from the previous step).
   b) Log in with the default user name (`admin`) and password (`admin`).

   Note: User names and passwords are case sensitive. We recommend that you change the password from the default as soon as possible for security reasons.

4.3 RPM deployments on CentOS and RedHat

This section provides detailed instructions on how to deploy RPM on CentOS 6.0/7.0 and RedHat 6/7.

Single and multiple-server RPM deployments require installing the RPM on one or more servers, installing a database, and setting up file storage.

Before you begin, read Additional requirements and considerations for RPM deployments on page 19 and determine which type of deployment is appropriate for you. That section includes specific information and diagrams about how these types of deployments will be configured on your network.

You will need the Linux root or “superuser” password to perform the procedures in this section. For RPM deployments, Dolby software never sets your `root` password; consult the other system administrators in your organization to learn the password.

4.3.1 Installing a database

Before you install the Dolby Conferencing Console software with the RPM package, install a database to handle the data.

Procedure

1. Run these commands as root user and use **`yum`** to install the database:

On CentOS 6.0 or RedHat 6:

```
sudo /bin/bash
yum install -y https://download.postgresql.org/pub/repos/yum/reporpms/EL-6-x86_64/
pgdg-redhat-repo-latest.noarch.rpm
yum install -y postgresql96-server
service postgresql-9.6 initdb
service postgresql-9.6 start
```

On CentOS 7.0 or RedHat 7:

```
sudo /bin/bash
yum install -y https://download.postgresql.org/pub/repos/yum/reporpms/EL-7-x86_64/
pgdg-redhat-repo-latest.noarch.rpm
yum install -y postgresql96-server
/usr/pgsql-9.6/bin/postgresql96-setup initdb
systemctl start postgresql-9.6.service
```

2. Create the database with full access granted to the Dolby Conferencing Console software:

```
# su postgres -c psql
postgres=# CREATE DATABASE dcc;
postgres=# CREATE USER dcc WITH PASSWORD 'secret';
postgres=# GRANT ALL PRIVILEGES ON DATABASE dcc to dcc;
postgres=# \q
```

Note: 'Secret' is only a placeholder until you create the password. The password can be anything you choose.

3. (Mandatory for multiple-server deployments) Open port 5432 to allow the Dolby Conferencing Console server to communicate with the database, and then check the status of the firewall by entering these commands:
For CentOS 6.0 or RedHat 6:

```
iptables -I INPUT -p tcp -m tcp --dport 5432 -j ACCEPT
service iptables save
service iptables status
```

For CentOS 7.0 or RedHat 7:

```
firewall-cmd --zone=public --add-port=5432/tcp --permanent
firewall-cmd --reload
```

4. Allow the database to listen to any remote servers (such as the Dolby Conferencing Console server) instead of the default `localhost` and increase the maximum number of database threads allowed.
   a) Modify the *postgresql.conf* file.
   For CentOS 6.0 or RedHat 6:

   ```
   /var/lib/pgsql/9.6/data/postgresql.conf
   ```

   For CentOS 7.0 or RedHat 7:

   ```
   /var/lib/pgsql/9.6/data/postgresql.conf
   ```

   b) Uncomment `listen_addresses`.
   c) Change`localhost` to `listen_addresses`.

   ```
   'localhost' change to listen_addresses = '*'
   ```

   d) Change `max_connections` from 100 to 300. For example:

   ```
   max_connections = 300
   ```

5. Modify the *pg_hba.conf* for CentOS 6.0 or RedHat 6: */var/lib/pgsql/9.6/data/pg_hba.conf* or for CentOS 7.0 or RedHat 7: */var/lib/pgsql/9.6/data/pg_hba.conf* to allow remote servers (such as the Dolby Conferencing

Console server) to access the dcc user and dcc database created in step 2. Use authentication method md5. For example, if you want to allow access to the address range 10.0.0.0/8 :

```
# IPv4 local connections:
host     all     all     127.0.0.1/32    ident
host     dcc     dcc     10.0.0.0/8      md5
```

Note:

In this example, PostgreSQL is not installed on the master node.

6. If you made any changes to the PostgreSQL configuration in steps 4 or 5, restart the database service with this command:
For CentOS 6.0 or RedHat 6:

```
service postgresql-9.6 restart
```

For CentOS 7.0 or RedHat 7:

```
systemctl restart postgresql-9.6.service
```

7. Configure postgresql to start automatically when the system reboots.
For CentOS 6.0 or RedHat 6:

```
chkconfig postgresql-9.6 on
```

For CentOS 7.0 or RedHat 7:

```
systemctl enable postgresql-9.6.service
```

4.3.2 Installing and configuring a Redis server

Single-server and multiple-server RPM deployments require a Redis server. Install and configure the Redis server before you install Dolby Conferencing Console software on any servers.

Prerequisites

Review Redis server requirements on page 22 and determine which version of Redis you require based on the number of devices at your site. Redis version 3.0 which is included with CentOS 7.0 and later, is required if you have more than 6,000 devices.

Procedure

1. From the computer or virtual machine that you will use as your Redis server, enter these commands to install Redis:
For CentOS 6.0 or RedHat 6:

```
wget http://dl.fedoraproject.org/pub/epel/epel-release-latest-6.noarch.rpm
rpm -Uvh epel-release-latest-6.noarch.rpm
yum install -y redis
```

Note:

If you encounter difficulties installing the *epel-release* package, see this page for suggestions:

http://www.tecmint.com/how-to-enable-epel-repository-for-rhel-centos-6-5/

For CentOS 7.0 or RedHat 7:

```
yum install https://download.fedoraproject.org/pub/epel/epel-release-
latest-7.noarch.rpm
yum install -y redis
```

2. Perform one of these steps:

- For CentOS 6.0 or RedHat 6, edit the `/etc/sysctl.conf` file.
- For CentOS 7.0 or RedHat 7, create and edit the `/etc/sysctl.d/99-dcc.conf` file.

3. Append these `sysctl` parameters to tune the node for high network load.

```
fs.file-max=188146
net.core.somaxconn=8192
net.netfilter.nf_conntrack_max=131072
```

4. After you edit the **`sysctl`** parameters, enter this command to apply the changes:
   For CentOS 6.0 or RedHat 6:

```
sysctl -p
```

   For CentOS 7.0 or RedHat 7:

```
sysctl --system
```

   You may encounter the following error:

```
error: "net.netfilter.nf_conntrack_max" is an unknown key
```

   This error means that your system administrator has not installed the `nf_conntrack` module on this host. You can ignore this error if you do not anticipate high network load. Otherwise, contact your system administrator to install the `nf_conntrack` module. You can still proceed with next step of installation.

5. Edit the */etc/redis.conf* file, and add the following line:

```
maxclients 20000
```

6. Edit the */etc/redis.conf* file, and make one of the following changes:

   - For a single node Dolby Conferencing Console deployment, uncomment the `bind 127.0.0.1` line in the */etc/redis.conf* file.
   - For a multiple node Dolby Conferencing Console deployment, uncomment the `bind 127.0.0.1` line in the */etc/redis.conf* file and modify it to `bind IP_address` , where *`IP_address`* is the IP address associated with the interface (for example, `eth0` , bond `0` , and so on) that is used for communication between the nodes of the Dolby Conferencing Console cluster.

   Note:

   For a multiple node Dolby Conferencing Console deployment, if you specify `bind 0.0.0.0`, it will open the Redis server to all interfaces and introduce a security risk if the Redis host is reachable via the Internet. See the bind description in the *redis.conf* file for more details.

7. Edit and set the Redis server limits configuration.

   Note: If the Redis server limits configuration file is not present, create the file.

   On CentOS 6.0 or RedHat 6, edit the */etc/security/limits.d/95-redis.conf* file, and set the limit.

```
redis soft nofile 32000
redis hard nofile 32000
```

   On CentOS 7.0 or RedHat 7, edit the */etc/systemd/system/redis.service.d/limit.conf* file, and set the limit.

```
LimitNOFILE=32000
```

8. Enter one of these commands to open the Redis server port on your firewall and check the status of the firewall:

For CentOS 6.0 or RedHat 6:

```
iptables -I INPUT -p tcp --dport 6379 -i eth0 -j ACCEPT
service iptables save
service iptables status
```

For CentOS 7.0 or RedHat 7:

```
firewall-cmd --zone=public --add-port=6379/tcp --permanent
firewall-cmd --reload
firewall-cmd --list-all
```

9. Configure Redis to start automatically when the system reboots.
   For CentOS 6.0 or RedHat 6:

```
chkconfig redis on
```

   For CentOS 7.0 or RedHat 7:

```
systemctl enable redis
```

10. Start the Redis server:
    For CentOS 6.0 or RedHat 6:

```
service redis start
```

    For CentOS 7.0 or RedHat 7:

```
systemctl start redis
```

11. For Redis versions 2.6 and later, verify that the `maxclients` value is set to `20000`:

```
redis-cli -h redis-ipaddress config get maxclients
```

    If you do not receive a `maxclient` output perform these steps:

    - Check the Redis server limits configuration
    - Reduce the `maxclients` value
    - Restart the Redis server
    - Re-check the `maxclients` value

12. Verify that Redis is configured to start automatically:
    For CentOS 6.0 or RedHat 6:

```
chkconfig --list redis
```

```
redis 0:off 1:off 2:on 3:on 4:on 5:on 6:off
```

    For CentOS 7.0 or RedHat 7:

```
systemctl is-enabled redis
```

```
enabled
```

4.3.3 Installing with the RPM package on a server

You can install the Dolby Conferencing Console software with the RPM package on Linux-based computers or Linux-based virtual machines.

Prerequisites

Do not proceed unless you have already installed a database (see Installing a database on page 26) and set up a Redis server (see Installing and configuring a Redis server on page 28).

Procedure

1. From a Linux-based computer or Linux-based virtual machine, use the **su** command to log in as superuser. Enter this command:

```
$ su
```

2. Set up Network Time Protocol (NTP) on the server, and sync it with your company NTP server or any public NTP server:
   a) Enter `yum install ntpdate`.
   b) Enter `ntpdate company_NTP_server` or `ntpdate time.nist.gov`.
3. (Optional) Install the PostgreSQL RPM if the database was installed on a different server,
   For CentOS 6.0 or RedHat 6

```
yum install -y https://download.postgresql.org/pub/repos/yum/reporpms/EL-6-x86_64/
pgdg-redhat-repo-latest.noarch.rpm
```

   For CentOS 7.0 or RedHat 7

```
yum install -y https://download.postgresql.org/pub/repos/yum/reporpms/EL-7-x86_64/
pgdg-redhat-repo-latest.noarch.rpm
```

4. Download the RPM package file to the server.
5. Use the **yum** command to install the Dolby Conferencing Console software. Enter this command:

```
yum install dcc-version-arch.rpm
```

   This list explains what values to enter based on this example:

   - *version*: The version of the Dolby Conferencing Console software.
   - *arch*: For CentOS 6.0 or RedHat 6: `1.el6.x86_64` or For CentOS 7.0 or RedHat 7: `1.el7.x86_64`

   Note: Both the Dolby Conferencing Console software and *postgresql-libs* (a dependency) will be installed.
6. (Optional) In the Dolby Conferencing Console web server, create and sign an Secure Sockets Layer (SSL) certificate and store the results in */etc/dcc/web-cert.key* and */etc/dcc/web-cert.pem*.

   You perform this step only when replacing the default certificate with a CA certificate as described in Replacing the default server certificate with a CA certificate on page 49.
7. (Required for single-server installations) Ensure that connections between the Dolby Conferencing Console server and the database are functioning by checking the listed entries in these files, and ensuring that your firewall allows for these port connections:

```
/etc/dcc/settings.ini
[database]
DB_USER=dcc
DB_NAME=dcc
DB_PASSWORD=secret
DB_HOST=database.company.com
DB_HOST
```

```
/etc/dcc/web.ini
HTTP port: 80; HTTPS port: 443 HW Address HWaddr 08:00:27:02:85:00
```

   Note: To check connectivity, the PostgreSQL client is required.

   You can use this command to check connectivity:

```
psql -U dcc -h database.company.com -p 5432
```

Note: Confirm that both HTTP port 80 and HTTPS port 443 are open; otherwise, you will not be able to log in from a web browser. For more information, see Network security on page 18.

8. From the Dolby Conferencing Console server, edit `/etc/dcc/settings.ini` file and enter these directives to define the connection between the Dolby Conferencing Console server and the Redis server.

   For multi-server installations, repeat this step on each device access service and master node.

   Sample configuration:

   ```
   [database]
   DB_USER=dcc
   DB_NAME=dcc
   DB_PASSWORD=secret
   DB_HOST=database.company.com
   ```

   Note: This is the password you created during the database installation.

   ```
   [redis]
   HOST=10.2.0.1
   DB=5
   PASSWORD=password
   PORT=6379
   ```

   This list explains what values to enter based on this example:

   HOST
   The host name of the Redis server. The default value is `localhost`.

   PORT
   The Redis server port number (default: 6379).

   DB
   The Redis database number: Required for multiple-server installations if there are other Redis consumers not using Dolby Conferencing Console. The value must be a number equal or greater than zero and that does not include decimals.

   PASSWORD
   Required only if the Redis server is password protected. If you use the AWS platform, the Redis server is not accessible to the outside world unless you explicitly grant access. If the Redis server is on a separate physical or virtual server and you do not use the AWS platform, we recommend that you configure a Redis server password.

9. Use the **`service`** command to start the Dolby Conferencing Console software. For example, enter this command:
   For CentOS 6.0 or RedHat 6:

   ```
   service dcc start
   ```

   For CentOS 7.0 or RedHat 7:

   ```
   systemctl start dcc
   ```

10. Enter one of these commands to obtain the IP address of the Dolby Conferencing Console:

    - For CentOS 6.0 or RedHat 6 the command is **`ifconfig`**:

      ```
      dcc login: root
      [root@dcc ~]# ifconfig
      eth0    Link encap:Ethernet  HWaddr 08:00:27:02:85:00
              inet addr: 10.112.100.167  Bcast 10.112.101.255  Mask: 255.255.254.0
      ```

- For CentOS 7.0 or RedHat 7 the command is **`ip addr`**:

```
dcc login: root
[root@dcc ~]# ip addr
...
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP qlen
1000
    link/ether 08:00:27:87:f0:d2 brd ff:ff:ff:ff:ff:ff
    inet 10.120.100.173/23 brd 10.120.101.255 scope global eth0
       valid_lft forever preferred_lft forever
    inet6 fe80::a00:27ff:fe87:f0d2/64 scope link
       valid_lft forever preferred_lft forever
```

11. Configure the firewall to allow HTTP connections.
    For CentOS 6.0 or RedHat 6:

```
iptables -I INPUT -p tcp --dport 80 -i eth0 -j ACCEPT
service iptables save
```

    For CentOS 7.0 or RedHat 7:

```
firewall-cmd --zone=public --add-service http --permanent
firewall-cmd --reload
```

12. Configure the firewall to allow HTTPS connections.
    For CentOS 6.0 or RedHat 6:

```
iptables -I INPUT -p tcp --dport 443 -i eth0 -j ACCEPT
service iptables save
```

    For CentOS 7.0 or RedHat 7:

```
firewall-cmd --zone=public --add-service https --permanent
firewall-cmd --reload
```

13. From an Internet browser, enter the IP address and then perform these steps from the Dolby Conferencing Console UI:
    a) Log in with the default user name (`admin`) and password (`admin`).
    b) If desired, change your password (recommended).

4.3.4 Installing with the RPM package on multiple servers

Installing the Dolby Conferencing Console software with the RPM package on multiple servers is the same as installing it on one server, but with some additional steps.

Procedure

1. Install the Dolby Conferencing Console software on multiple servers.
   For more information, see Installing with the RPM package on a server on page 30.
2. Decide which server will be your master node and which will be device access service nodes.
   For more information, see Master node requirements on page 23 and Device access service node requirements on page 17.
3. Set up a file server.
   For more information, see Setting up file storage for multiple servers on page 39.
4. On each server that you want to use as a device access service node, perform these steps:
   a) Go to the */etc/sysconfig/dcc* file, and set the `MODE` variable to `das`.
   b) Restart the server using this command:

```
service dcc restart
```

c) Confirm that port 8001 is open on each device access service node, so that the master node can access them with these commands:

For CentOS 6.0 or RedHat 6:

```
iptables -I INPUT -p tcp -m tcp --dport 8001 -j ACCEPT
service iptables save
service iptables status
```

For CentOS 7.0 or RedHat 7:

```
firewall-cmd --zone=public --add-port=8001/tcp –permanent
firewall-cmd --reload
firewall-cmd --list-all
```

5. On the remaining server that you are using as the master node, edit */etc/dcc/das-nodes.ini* as described here. You must list all of your device access service nodes so that they are available to the master node.

   Note: If you want redundancy, perform this step for the backup master node as well. The active master and backup master nodes must have the same configuration for redundancy to work.

   Sample configuration:

   ```
   /etc/dcc/das-nodes.ini
   ```

   ```
                          # the upstream for DAS nodes
   upstream das {
       # List of all DAS nodes in nginx "upstream" compatible format
       server 10.0.0.101:8001 weight=10;
       server 10.0.0.102:8001 weight=10;
       server 10.0.0.103:8001 weight=10;
       # !!! DO NOT DELETE THIS LINE !!!
       server unix:/var/run/dcc/das.sock;
   }
   ```

4.4 RPM deployments on Amazon Linux

This section provides detailed instructions on how to install all of the components of Dolby Conferencing Console on a single Amazon Linux `t2.xlarge` EC2 instance. This type of installation supports up to 1,000 devices.

Single and multiple-server RPM deployments require installing the RPM on one or more servers, installing a database, and setting up file storage.

Before you begin, read Additional requirements and considerations for RPM deployments on page 19 and determine which type of deployment is appropriate for you. That section includes specific information and diagrams about how these types of deployments will be configured on your network.

You will need the Linux root or “superuser” password to perform the procedures in this section. For RPM deployments, Dolby software never sets your `root` password; consult the other system administrators in your organization to learn the password.

4.4.1 Creating an AWS EC2 instance

Procedure

1. Spawn an Amazon Linux EC2 instance with ports 22, 80, 443 open for inbound connections.
2. Use **`ssh`** to log in to the instance.

4.4.2 Installing a database

Before you install the Dolby Conferencing Console software with the RPM package, install a database to handle the data.

Procedure

1. Run these commands as root user and use **yum** to install the database:

```
sudo /bin/bash
yum install -y postgresql96-server
service postgresql96 initdb
service postgresql96 start
```

2. Create the database with full access granted to the Dolby Conferencing Console software:

```
# su postgres -c psql
postgres=# CREATE DATABASE dcc;
postgres=# CREATE USER dcc WITH PASSWORD 'secret';
postgres=# GRANT ALL PRIVILEGES ON DATABASE dcc to dcc;
postgres=# \q
```

   Note: Secret is only a placeholder until you create the password. The password can be anything you choose.

3. (Mandatory for multiple-server deployments) Open port 5432 to allow the Dolby Conferencing Console server to communicate with the database, and then check the status of the firewall by entering these commands:

```
iptables -I INPUT -p tcp -m tcp --dport 5432 -j ACCEPT
service iptables save
service iptables status
```

4. Allow the database to listen to any remote servers (such as the Dolby Conferencing Console server) instead of the default `localhost` and increase the maximum number of database threads allowed.
   a) Modify the */var/lib/pgsql96/data/postgresql.conf* file.
   b) Uncomment `listen_addresses`
   c) Change`localhost` to `"*" listen_addresses = 'localhost' change to listen_addresses = '*'`.
   d) Change `max_connections` from 100 to 300. For example:

```
max_connections = 300
```

5. Modify the */var/lib/pgsql96/data/pg_hba.conf* to allow remote servers (such as the Dolby Conferencing Console server) to access the dcc user and dcc database created in step 2. Use authentication method `md5`. For example, if you want to allow access to the address range `10.0.0.0/8` :

```
# IPv4 local connections:
host     all     all     127.0.0.1/32    ident
host     dcc     dcc     10.0.0.0/8      md5
```

   Note:

   In this example, PostgreSQL is not installed on the master node.

6. If you made any changes to the PostgreSQL configuration in steps 4, 5, or 6, restart the database service with this command:

```
service postgresql96 restart
```

7. Configure postgresql to start automatically when the system reboots.

```
chkconfig postgresql96 on
```

4.4.3 Installing and configuring a Redis server

Single-server and multiple-server RPM deployments require a Redis server. Install and configure the Redis server before you install Dolby Conferencing Console software on any servers.

Prerequisites

Review Redis server requirements on page 22 and determine which version of Redis you require based on the number of devices at your site. Redis version 3.0 is required if you have more than 6,000 devices.

Procedure

1. From the EC2 instance that you will use as your Redis server, enter these commands to install Redis:

```
yum-config-manager --enable epel
yum install -y epel-release
yum install -y redis
```

2. Edit the `/etc/sysctl.conf`
3. Append these `sysctl` parameters to tune the node for high network load.

```
fs.file-max=188146
net.core.somaxconn=8192
net.netfilter.nf_conntrack_max=131072
```

4. After you edit the **`sysctl`** parameters, enter this command to apply the changes:

```
sysctl -p
```

You may encounter the following error:

```
error: "net.netfilter.nf_conntrack_max" is an unknown key
```

This error means that your system administrator has not installed the `nf_conntrack` module on this host. You can ignore this error if you do not anticipate high network load. Otherwise, contact your system administrator to install the `nf_conntrack` module. You can still proceed with next step of installation.

5. Edit the */etc/redis.conf* file, and add the following line:

```
maxclients 20000
```

6. Edit the */etc/redis.conf* file, and make one of the following changes:
   - For a single node Dolby Conferencing Console deployment, uncomment the `bind 127.0.0.1` line in the */etc/redis.conf* file.
   - For a multiple node Dolby Conferencing Console deployment, uncomment the `bind 127.0.0.1` line in the */etc/redis.conf* file and modify it to `bind IP_address`, where *`IP_address`* is the IP address associated with the interface (for example, `eth0`, bond `0`, and so on) that is used for communication between the nodes of the Dolby Conferencing Console cluster.

   Note:

   For a multiple node Dolby Conferencing Console deployment, if you specify `bind 0.0.0.0`, it will open the Redis server to all interfaces and introduce a security risk if the Redis host is reachable via the Internet. See the bind description in the *redis.conf* file for more details.
7. Edit and set the Redis server limits configuration.

Note: If the Redis server limits configuration file is not present, create the file.

```
/etc/security/limits.d/95-redis.conf
```

```
redis soft nofile 32000
redis hard nofile 32000
```

8. Enter one of these commands to open the Redis server port on your firewall and check the status of the firewall:

```
iptables -I INPUT -p tcp --dport 6379 -i eth0 -j ACCEPT
service iptables save
service iptables status
```

9. Configure Redis to start automatically when the system reboots.

```
chkconfig redis on
```

10. Start the Redis server:

```
service redis start
```

11. For Redis versions 2.6 and later, verify that the `maxclients` value is set to `20000`:

```
redis-cli -h redis-ipaddress config get maxclients
```

If you do not receive a `maxclient` output perform these steps:

- Check the Redis server limits configuration
- Reduce the `maxclients` value
- Restart the Redis server
- Re-check the `maxclients` value

12. Verify that Redis is configured to start automatically:

```
chkconfig --list redis
```

```
redis 0:off   1:off   2:on    3:on    4:on    5:on    6:off
```

4.4.4 Installing with the RPM package on a server

You can install the Dolby Conferencing Console software with the RPM package on Linux-based computers or Linux-based virtual machines.

Prerequisites

Do not proceed unless you have already installed a database (see Installing a database on page 35) and set up a Redis server (see Installing and configuring a Redis server on page 36).

Procedure

1. Set up NTP on the server, and sync it with your company NTP server or any public NTP server:
   a) Enter `yum install ntpdate`.
   b) Enter `ntpdate company_NTP_server` or `ntpdate time.nist.gov`.
2. Download and install these packages:
   a) Download the Dolby Conferencing Console RPM for AWS.
      - http://download.dolbyvoice.com/dcc/xmlsec1-1.2.20-1.x86_64.rpm
      - http://download.dolbyvoice.com/dcc/xmlsec1-openssl-1.2.20-1.x86_64.rpm

You can use curl or wget to download the RPM package.

```
wget url_from_release_email
curl -O url_from_release_email
```

You can also upload the package to the AWS host.

b) Download these two prerequisite packages to the same folder as the Dolby Conferencing Console RPM package on the instance. These required packages are not included in Amazon Linux: http://download.dolbyvoice.com/dcc/xmlsec1-1.2.20-1.x86_64.rpm

c) Install the three packages, working from the directory into which they have been downloaded:

```
sudo yum install xmlsec1-openssl-1.2.20-1.x86_64.rpm xmlsec1-1.2.20-1.x86_64.rpm
dcc-2.3.0.*.amzn.x86_64.rpm
```

3. (Optional) Install the PostgreSQL RPM if the database was installed on a different server,

```
yum install -y https://download.postgresql.org/pub/repos/yum/reporpms/EL-6-x86_64/
pgdg-redhat-repo-latest.noarch.rpm
```

4. (Optional) In the Dolby Conferencing Console web server, create and sign an SSL certificate and store the results in */etc/dcc/web-cert.key* and */etc/dcc/web-cert.pem*.

   You perform this step only when replacing the default certificate with a CA certificate as described in Replacing the default server certificate with a CA certificate on page 49.

5. Ensure that connections between the Dolby Conferencing Console server and the database are functioning by checking the listed entries in these files, and ensuring that your firewall allows for these port connections:

```
/etc/dcc/settings.ini
[database]
DB_USER=dcc
DB_NAME=dcc
DB_PASSWORD=secret
DB_HOST=database.company.com
DB_HOST
```

```
/etc/dcc/web.ini
HTTP port: 80; HTTPS port: 443 HW Address HWaddr 08:00:27:02:85:00
```

   Note: To check connectivity, the PostgreSQL client is required.

   If you need to install the PostgreSQL client, use this command:

```
yum install -y postgresql
```

   After the PostgreSQL client is installed, you can then use this command to check connectivity:

```
psql -U dcc -h database.company.com -p 5432
```

   Note: Confirm that both HTTP port 80 and HTTPS port 443 are open; otherwise, you will not be able to log in from a web browser. For more information, see Network security on page 18.

6. From the Dolby Conferencing Console server, edit `/etc/dcc/settings.ini` file and enter these directives to define the connection between the Dolby Conferencing Console server and the Redis server.

   For multi-server installations, repeat this step on each device access service and master node.

Sample configuration:

```
[database]
DB_USER=dcc
DB_NAME=dcc
DB_PASSWORD=secret
DB_HOST=database.company.com
```

Note: This is the password you created during the database installation.

```
[redis]
HOST=10.2.0.1
DB=5
PASSWORD=password
PORT=6379
```

This list explains what values to enter based on this example:

HOST
The host name of the Redis server. The default value is `localhost`.

PORT
The Redis server port number (default: 6379).

DB
The Redis database number: Required for multiple-server installations if there are other Redis consumers not using Dolby Conferencing Console. The value must be a number equal or greater than zero and that does not include decimals.

PASSWORD
Required only if the Redis server is password protected. If you use the AWS platform, the Redis server is not accessible to the outside world unless you explicitly grant access. If the Redis server is on a separate physical or virtual server and you do not use the AWS platform, we recommend that you configure a Redis server password.

7. Use the **`service`** command to start the Dolby Conferencing Console software. For example, enter this command:

```
yum install -y postgresql96
```

4.4.5 Installing Dolby Conferencing Console on multiple AWS servers

You can install the Dolby Conferencing Console software and its supporting servers on multiple Amazon instances. This configuration can support up to 10,000 devices (optionally with redundancy to prevent service disruptions or performance problems).

About this task

Follow the instructions in these sections, making any necessary changes for the AWS platform:

- RPM Package Manager deployments on Amazon Linux on page 34
- Setting up database redundancy on page 47

Note: Make sure that the AWS security group used by each server has inbound rules that allow access to each port opened in the firewall.

4.5 Setting up file storage for multiple servers

A file-storage server is required for all RPM installations (both single-server and multiple-server installations).

Prerequisites
Before you begin, review requirements for file-storage servers at File-storage server requirements on page 23.

Procedure

1. Install file-storage programs on the server with this command:

```
yum install nfs-utils nfs-utils-lib
```

2. Run these scripts:

```
chkconfig nfs on
service rpcbind start
service nfs start
```

3. Export the desired share directory and make it available to all the Dolby Conferencing Console nodes, both master nodes and DAS nodes.
   To share the /home directory on the file-storage server, append these lines to */etc/exports*. Assume that `10.203.131.179` is the active master node, that `10.203.131.180` is the redundancy master node and `10.203.131.181` and `10.203.131.181` are DAS nodes.

```
/home 10.203.131.179(rw,async,no_root_squash,no_subtree_check)
/home 10.203.131.180(rw,async,no_root_squash,no_subtree_check)
/home 10.203.131.181(rw,async,no_root_squash,no_subtree_check)
/home 10.203.131.182(rw,async,no_root_squash,no_subtree_check)
```

4. Run this command to export:

```
exportfs -a
```

5. Open the firewall (**`iptables`**) for the file-storage server port 2049 with this command:
   Example for Redhat 6CentOS 6.0:

```
iptables -I INPUT -p tcp -m tcp --dport 2049 -j ACCEPT
```

   Save `iptables`, and check the status of the firewall with these commands:

```
service iptables save
service iptables status
```

   Example for Redhat 7 CentOS 7.0:

```
firewall-cmd --zone=public --add-port=2049/tcp --permanent
firewall-cmd --reload
firewall-cmd --list-all
```

4.6 Accessing file storage server

Both single-server and multiple-server installations require access to a file-storage server. Only one file-storage server is required for each deployment. For more information on creating a file storage server see Setting up file storage for multiple servers on page 39.

About this task
For single-server installations, the file-storage server can be on the same physical or virtual hardware as the Dolby Conferencing Console server. However, this is not a requirement. You can choose to use a separate file-storage server that is somewhere else on the network.

For multiple-server installations, you must use a file-storage server that is accessible to all Dolby Conferencing Console nodes (the master node and any device access service nodes).

Procedure

1. (Optional for single-server installations) Set the file-storage client on the Dolby Conferencing Console server to access the remote file-storage server.
2. Configure the file-storage client (in this case, it is the Dolby Conferencing Console master node or device access service node) with this command:

```
yum install nfs-utils nfs-utils-lib
```

3. Mount */var/lib/dcc/files* with this command. Assume that */home* is the directory you need to access on the file-storage server.

```
mount nfs.company.com:/home /var/lib/dcc/files
```

4. Confirm that the mount is configured with the **`df -h`** command:

   Sample output:

```
[root@dcc ~]# df -h
Filesystem     Size Used Avail Use%
Mounted on /dev/mapper/vg_dsvddmspf1-lv_root

18G 2.1G 15G 13% / tmpfs
939M 76K 939M 1% /dev/shm /dev/sda1
477M 33M 419M 8% /boot
nfs.company.com:/home 45G 1.9G 41G 5% /var/lib/dcc/files
```

5. Modify the */etc/fstab* to have a persistent shared mount drive after the server reboots with the command:

```
nfs.company.com:/home /var/lib/dcc/files nfs defaults 0 0
```

   Sample configuration:

```
/etc/fstab

#
# /etc/fstab
# Created by anaconda on Thu Oct 29 12:51:12 2015
#
# Accessible filesystems, by reference, are maintained under '/dev/disk'
# See man pages fstab(5), findfs(8), mount(8) and/or blkid(8) for more info
#

/dev/mapper/vg_dsvddmspf2-lv_root /                       ext4    defaults        1 1
UUID=83c2a6d9-85e6-40bf-acf2-2e64da6c23f2 /boot                   ext4    defaults
    1 2
/dev/mapper/vg_dsvddmspf2-lv_swap swap                    swap    defaults        0 0
tmpfs                   /dev/shm                tmpfs   defaults        0 0
devpts                  /dev/pts                devpts  gid=5,mode=620  0 0
sysfs                   /sys                    sysfs   defaults        0 0
proc                    /proc                   proc    defaults        0 0
nfs.company.com:/home    /var/lib/dcc/files     nfs     defaults        0 0
```

6. Change owner of */var/lib/dcc/files* to dcc instead of root with the **chown** command:

```
[root@dsv-ddmspf-1 ~]# chown -R dcc:dcc /var/lib/dcc/files

[root@dcc ~]# ls -lat /var/lib/dcc/files
total 16
drwxr-xr-x. 2 nobody nobody 4096 Jan 7 17:02 uploads
drwxr-xr-x. 4 nobody nobody 4096 Jan 7 16:31 .
drwxr-xr-x. 2 nobody nobody 4096 Jan 7 16:19
fw drwxrwxr-x. 3 dcc dcc 4096 Jan 7 15:26 ..
[root@dcc ~]#
```

7. Start the NFS server.

```
service nfs start
```

4.7 RPM deployments with redundancy

With large-scale deployments (1,000 devices or more), redundancy ensures that users do not experience service disruptions or performance problems.

Set up the Dolby Conferencing Console software with these components: master nodes, device access service nodes, and database nodes. For each type of node, create both an active and a backup version. These are identical (or redundant), but if a master fails, the backup becomes the new active node.

4.7.1 Setting up master node redundancy

You can set up redundant nodes by using failover software (**`keepalived`**).

Prerequisites

Do not proceed unless you have already completed these prerequisite tasks:

- Set up the Dolby Conferencing Console software with the following components: master node, database node, and network file storage mounted to `/var/lib/dcc/files` on the master node.
- Create a backup master node with the same configuration as the active master node.

About this task

The information here is for example only; the actual IP addresses you use should be different:

- The IP address of the active master node is 10.112.100.230.
- The IP address of the backup node is 10.112.100.231.
- The IP address (virtual IP address) of the Dolby Conferencing Console server (*dcc.ourcompany.com*) is 10.112.100.233.

Procedure

1. On both the active and backup master nodes, install **`keepalived`**.

```
yum install keepalived
```

2. On both the active and backup master nodes, edit `/etc/sysconfig/dcc` and uncomment these lines:

```
DCC_DAS_WORKERS = 16
DCC_TASKQUEUE_WORKERS = 8
     (Two workers are recommended for every 3,000 devices.)
DCC_WEBSOCKETS_WORKERS = 4
     (One worker is required for every 3,000 devices.)
```

3. Perform one of these steps:
   - For Redhat 6, edit the `/etc/sysctl.conf` file.
   - For Redhat 7, create and edit the `/etc/sysctl.d/99-dcc.conf` file.
4. Append these `sysctl` parameters to tune the node for high network load.

```
fs.file-max=188146
net.core.somaxconn=8192
net.netfilter.nf_conntrack_max=131072
```

5. If needed, configure your firewall so that Virtual Router Redundancy Protocol (VRRP) is allowed through, and confirm the change.
   Example for Redhat 6 CentOS 6.0:

```
iptables -I INPUT -p 112 -i eth0 -j ACCEPT
service iptables save
service iptables status
```

Example for Redhat 7 CentOS 7.0:

```
firewall-cmd --add-rich-rule='rule protocol value="vrrp" accept' --permanent
firewall-cmd --reload
firewall-cmd --list-all
```

6. On the active master node, back up the default *keepalived.conf* configuration file and configure a new file. Then enable and start keepalived.

   The command for backing up keepalived.conf is `mv /etc/keepalived/keepalived.conf /etc/keepalived/keepalived.conf_default`.

```
cat > /etc/keepalived/keepalived.conf <<__EOF__
! Configuration File for keepalived
global_defs {
    router_id DCC_ASP
}
vrrp_instance DCC {
    state MASTER
    interface eth0
    virtual_router_id 51
    priority 101
    advert_int 1
    notify /usr/bin/dcc-keepalived-notify.sh
    authentication {
        auth_type PASS
        auth_pass longandwindingroad
    }
    virtual_ipaddress {
    10.112.100.233
    }
}
__EOF__
service keepalived start
chkconfig keepalived on
```

   Note: Replace correct interface name in the keepalived.conf file.

7. Repeat the previous step on the backup node, but make sure that the backup priority value is less than the active master priority value.
   For example, if the active master has a priority value of 101, then the backup master node must have a priority value of 100 or less.

```
cat > /etc/keepalived/keepalived.conf <<__EOF__
! Configuration File for keepalived
global_defs {
   router_id DCC_ASP
}
vrrp_instance DCC {
    state MASTER
    interface eth0
    virtual_router_id 51
    priority 100
    advert_int 1
    notify /usr/bin/dcc-keepalived-notify.sh
    authentication {
        auth_type PASS
        auth_pass longandwindingroad
    }
    virtual_ipaddress {
        10.112.100.233
    }
}
__EOF__
service keepalived start
chkconfig keepalived on
```

   Note: Replace correct interface name in the keepalived.conf file.

8. Confirm that the device access service nodes listed in the */etc/dcc/das-nodes.ini* file on both the active and backup master nodes match.

   Note: For redundancy to work, the active and backup master nodes need have the same configuration. For more information, including a sample configuration of the */etc/dcc/das-nodes.ini* file, see step 4 in Installing with the RPM Package Manager package on multiple servers on page 33.

9. Confirm that the Dolby Conferencing Console server is available at the `virtual_ipaddress` configured in these steps (for example, 10.112.100.233).
10. Test your failover by shutting down the active master node. Confirm that the Dolby Conferencing Console server is available on the same IP address (you may need to log in again).
11. Review the `logrotate` settings in */etc/logrotate.d/dcc* and update them, if needed. By default, the logs are rotated on a daily basis.

    For example, if a rotated log file gets too large when rotated on a daily basis, add the size trigger for those logs.

```
/var/log/dcc/nginx-*.log {
        size 750M
        missingok
        rotate 10
        notifempty
        sharedscripts
        nodateext
        postrotate
            /etc/init.d/dcc logrotate
        endscript
}
```

4.7.2 Installing and configuring a Redis server

Single-server and multiple-server RPM deployments require a Redis server. Install and configure the Redis server before you install Dolby Conferencing Console software on any servers.

Prerequisites

Review Redis server requirements on page 22 and determine which version of Redis you require based on the number of devices at your site. Redis version 3.0 which is included with CentOS 7.0 and later, is required if you have more than 6,000 devices.

Procedure

1. From the computer or virtual machine with CentOS that you will use as your Redis server, enter these commands to install Redis:
   For Redhat 6:

```
wget http://dl.fedoraproject.org/pub/epel/epel-release-latest-6.noarch.rpm
rpm -Uvh epel-release-latest-6.noarch.rpm yum install -y redis
```

   Note:

   If you encounter difficulties installing the *epel-release* package, see this page for suggestions:

   http://www.tecmint.com/how-to-enable-epel-repository-for-rhel-centos-6-5/

   For Redhat 7:

```
yum install https://download.fedoraproject.org/pub/epel/epel-release-
latest-7.noarch.rpm
yum install -y redis
```

2. Perform one of these steps:

- For Redhat 6, edit the `/etc/sysctl.conf` file.
- For Redhat 7, create and edit the `/etc/sysctl.d/99-dcc.conf` file.

3. Append these `sysctl` parameters to tune the node for high network load.

```
fs.file-max=188146
net.core.somaxconn=8192
net.netfilter.nf_conntrack_max=131072
```

4. After you edit the **`sysctl`** parameters, enter this command to apply the changes:
For Redhat 6:

```
sysctl -p
```

For Redhat 7:

```
sysctl --system
```

You may encounter the following error:

```
error: "net.netfilter.nf_conntrack_max" is an unknown key
```

This error means that your system administrator has not installed the `nf_conntrack` module on this host. You can ignore this error if you do not anticipate high network load. Otherwise, contact your system administrator to install the `nf_conntrack` module. You can still proceed with next step of installation.

5. Edit the */etc/redis.conf* file, and add the following line:

```
maxclients 20000
```

6. Edit the */etc/redis.conf* file, and make one of the following changes:

- For a single node Dolby Conferencing Console deployment, uncomment the `bind 127.0.0.1` line in the */etc/redis.conf* file.
- For a multiple node Dolby Conferencing Console deployment, uncomment the `bind 127.0.0.1` line in the */etc/redis.conf* file and modify it to `bind IP_address`, where *`IP_address`* is the IP address associated with the interface (for example, `eth0`, bond `0`, and so on) that is used for communication between the nodes of the Dolby Conferencing Console cluster.

Note:

For a multiple node Dolby Conferencing Console deployment, if you specify `bind 0.0.0.0`, it will open the Redis server to all interfaces and introduce a security risk if the Redis host is reachable via the Internet. See the bind description in the *redis.conf* file for more details.

7. Edit and set the Redis server limits configuration.

Note: If the Redis server limits configuration file is not present, create the file.

For example, on Community Enterprise Operating System 6.x., edit the */etc/security/limits.d/95-redis.conf* file, and set the limit.

```
redis soft nofile 32000
redis hard nofile 32000
```

For example, on Community Enterprise Operating System 7.x., edit the */etc/systemd/system/redis.service.d/limit.conf* file, and set the limit.

```
LimitNOFILE=32000
```

8. Enter one of these commands to open the Redis server port on your firewall and check the status of the firewall:

For Redhat 6:

```
iptables -I INPUT -p tcp --dport 6379 -i eth0 -j ACCEPT
service iptables save
service iptables status
```

For Redhat 7:

```
firewall-cmd --zone=public --add-port=6379/tcp --permanent
    firewall-cmd --reload
    firewall-cmd --list-all
```

9. Configure Redis to start automatically when the system reboots.
   For Redhat 6:

   ```
   chkconfig redis on
   ```

   For Redhat 7:

   ```
   systemctl enable redis
   ```

10. Start the Redis server:
    For Redhat 6:

    ```
    service redis start
    ```

    For Redhat 7:

    ```
    systemctl start redis
    ```

11. For Redis versions 2.6 and later, verify that the `maxclients` value is set to `20000`:

    ```
    redis-cli -h redis-ipaddress config get maxclients
    ```

    If you do not receive a `maxclient` output perform these steps:

    - Check the Redis server limits configuration
    - Reduce the `maxclients` value
    - Restart the Redis server
    - Re-check the `maxclients` value

12. Configure Dolby Conferencing Console to start automatically when the system reboots:

    For example, on CentOS:

    ```
    chkconfig dcc on
    ```

13. Verify that Redis is configured to start automatically:

    ```
    chkconfig --list redis
    ```

    ```
    redis           0:off   1:off   2:on    3:on    4:on    5:on    6:off
    ```

4.7.3 Setting up device access service node redundancy

device access service redundancy is achieved simply by having more device access service nodes than are required to handle traffic.

About this task

When a device access service node goes down, `nginx` on the active master node detects this condition and stops sending traffic to it, and then periodically checks the device access service node state. Once the node is back up, `nginx` starts sending requests to it again.

Sample configuration:

```
/etc/dcc/das-nodes.ini
# the upstream for DAS nodes
upstream das {
    # List of all DAS nodes in nginx "upstream" compatible format
    server 10.0.0.101:8001 weight=10;
    server 10.0.0.102:8001 weight=10;
    server 10.0.0.103:8001 weight=10;
    # !!! DO NOT DELETE THIS LINE !!!
    server unix:/var/run/dcc/das.sock;
}
```

Procedure

1. To run the Dolby Conferencing Console software as a device access service node, edit */etc/sysconfig/dcc* and set `MODE = das` and `DCC_DAS_WORKERS = 32`.
2. On each device access service node, confirm that port 8001 is open so that the active and backup master nodes can access them with these commands:
   Example for Redhat 6CentOS 6.0:

   ```
   iptables -I INPUT -p tcp -m tcp --dport 8001 -j ACCEPT
   service iptables save
   service iptables status
   ```

   Example for Redhat 7 CentOS 7.0:

   ```
   firewall-cmd --zone=public --add-port=8001/tcp --permanent
   firewall-cmd --reload
   firewall-cmd --list-all
   ```

3. Perform one of these steps:
   - For Redhat 6, edit the `/etc/sysctl.conf` file.
   - For Redhat 7, create and edit the `/etc/sysctl.d/99-dcc.conf` file.
4. Append these `sysctl` parameters to tune the node for high network load.

   ```
   fs.file-max=188146
   net.core.somaxconn=8192
   net.netfilter.nf_conntrack_max=131072
   ```

4.7.4 Setting up database redundancy

You can use any solution for high-availability PostgreSQL setup.

For example, you can use a combination of the **`pgpool`** and **`repmgr`** tools described in Set up a redundant PostgreSQL database with repmgr and pgpool. In this case, all nodes should point to the **`pgpool`** machine as a database server. In case of active master node failure, **`pgpool`** will detect this condition and switch all database traffic to standby mode.

4.8 Setting up secure access

The Dolby Conferencing Console software uses HTTPS for secure web UI access and secure provisioning. This is an overview of the procedures involved in setting up secure access for your system.

Assign a server host name

This allows devices and the IT administrators to connect to the Dolby Conferencing Console software using a host name as opposed to an IP address. See Changing the host name on page 48.

Replace the default certificate

The Dolby Conferencing Console software package contains a default self-signed certificate using the common name dcc. For a higher level of security, you should replace this with either a self-signed

certificate or a certificate authority (CA) certificate. See Replacing the default certificate with a new self-signed certificate on page 48 and Replacing the default server certificate with a CA certificate on page 49.

Connect a device to the Dolby Conferencing Console software using HTTPS

You can connect a Dolby Voice Device to your Dolby Conferencing Console securely. See Connecting a device over Hypertext Transfer Protocol Secure on page 50.

Note: You can accept the server certificate at the device during the first-time provisioning stage, or later through a user-interface menu.

Once you have configured secure access, you can use HTTPS to connect to the Dolby Conferencing Console web interface. Enter *https://hostname* in the browser to connect securely.

Note:

When a self-signed certificate is in use, most browsers display a warning, You can simply ignore this warning and log in to Dolby Conferencing Console.

4.8.1 Changing the host name

You can change the server host name for the Dolby Conferencing Console server. This allows devices and IT administrators to access the Dolby Conferencing Console software by using a convenient and easy-to-remember name instead of an IP address.

About this task

To change the server host name, set up the Dolby Conferencing Console host name and populate the DNS records.

Procedure

1. Log in to the Dolby Conferencing Console software as the root user.
2. Perform one of these steps:
   - For Redhat 6 CentOS 6.0:

     Edit the */etc/sysconfig/network* file, and change the value of the HOSTNAME field from the default, dcc, to the desired name.
   - For Redhat 7CentOS 7.0:

     Use the hostnamectl command to change the host name:

     ```
     hostnamectl set-hostname my_dcc
     ```

     Where my_dcc is your server host name.
3. Edit the */etc/sysconfig/network-scripts/ifcfg-eth0* file, and add the line DHCP_HOSTNAME="my_dcc", where *my_dcc* is your server host name.
4. Restart the network service by using this command:

   ```
   service network restart
   ```

4.8.2 Replacing the default certificate with a new self-signed certificate

Use this procedure to replace the default certificate with a self-signed certificate.

Procedure

1. On the server that hosts your Dolby Conferencing Console software, log in as the root user.

2. Open a console, and enter this command to open the certificate utility:

```
/usr/bin/dcc-generate-self-signed-cert
```

The certificate utility sends certificate parameter requests to the console.

3. Respond to these console requests.

Option	Description
Country name (two-letter code)	Two-letter code for country
State or province name (full name)	State or province name for your organization
Locality name (city)	City name for your organization
Organization name	Name of your company
Organization unit name	Name of your team or division within the company
Common name	The fully qualified domain name (FQDN) for your server (for example, `dcc.your-company.net`) **Important:** This name must match the host name used when you connect a device over HTTPS. See Connecting a device over Hypertext Transfer Protocol Secure on page 50.
Email address	An administrator email address (your valid email address)
Challenge password	Optional extra password

Results

After you have entered the desired information, the utility generates a certificate. The certificate is then ready for use.

4.8.3 Replacing the default server certificate with a CA certificate

Some organizations prefer to use CA signed certificates for their SSL web servers. The Dolby Conferencing Console software supports CA signed certificates.

About this task

On the server that hosts your Dolby Conferencing Console software, log in as the root user.

Procedure

1. Generate the certificate key, using the preferred data encryption standard (DES) for your organization. For example:

```
openssl genrsa -des3 -out /tmp/web-cert.key 2048
```

2. Generate a certificate signing request (CSR):

```
openssl req -new -key /tmp/web-cert.key -out /tmp/web-cert.csr -sha256
```

`openssl` sends certificate parameter requests to the console.

3. Respond to these console requests:

Option	Description
Pass phrase for `web-cert.key`	Must be blank

Option	Description
Pass phrase for `web-cert.key`	Must be blank
Country name (two-letter code)	Two-letter code for country
State or province name (full name)	State or province name for your organization
Locality name (city)	City name for your organization
Organization name	Name of your company
Organization unit name	Name of your team or division within the company
Common name	The fully qualified domain name for your server (for example, `dcc.your-company.net`) **Important:** This name must match the host name used when you connect a device over HTTPS. See Connecting a device over Hypertext Transfer Protocol Secure on page 50.
Email address	An administrator email address (your valid email address)
Challenge password	Optional extra password

Once you have finished the entries, `openssl` generates a certificate.

4. Retrieve the CSR file at */tmp/web-cert.csr*.
5. Use **`scp`** to copy the file to a remote Linux server at this server address:

```
scp /tmp/web-cert.csr user@server.address:remoteDirectory
```

6. Submit the file ending in *.csr* to a commercial SSL provider for signing.
7. After you receive the signed certificate, upload it to Dolby Conferencing Console.

```
scp user@server.address:/remoteDirectory/web-cert.pem /tmp/
```

8. Replace the server certificate located at */etc/dcc-web-cert.pem*.

```
mv /tmp/web-cert.pem /etc/dcc/web-cert.pem
mv /tmp/web-cert.key /etc/dcc/web-cert.key
```

9. Fix the owner/group for the file:

```
chown dcc:dcc /etc/dcc/web-cert.*
```

10. Restart the server:

```
service dcc restart
```

4.8.4 Connecting a device over HTTPS

You can connect a Dolby Voice Device to your Dolby Conferencing Console securely over HTTPS.

About this task

When you plug in a device and it powers up for the first time, it launches an out-of-box wizard. This wizard requests some basic information for its network connection, along with information about a provisioning server.

When you use the Dolby Conferencing Console software as a provisioning server, you are prompted to accept the server identity (server certificate). Verify the server certificate information, and then accept it.

Note: Without an accepted server identity, a Dolby Voice Device is not able to connect to the Dolby Conferencing Console server, and it displays a warning on the home screen.

Procedure

1. Plug in the device.
   A configuration screen begins a setup wizard. Follow the wizard until you get to the **Provisioning Configuration** screen.
2. For provisioning type, select **static**.
3. For protocol type, select **https**.
4. For host name, enter the fully qualified host name (for example, *dcc.your-company.net*).

   Important: This server host name must match the common name used when you replace the default certificate with a CA certificate or a new self-signed certificate.
5. If the Dolby Conferencing Console software is configured to restrict access to the server, enter the user name and password as requested.

What to do next
If the Dolby Conference Phone is not able to connect to the Dolby Conferencing Console software over HTTPS, the device displays a red warning icon on the Dolby Conference Phone home screen. Change the device provisioning server settings under the administrative settings menu.

1. Log in to the device using the default Dolby Conference Phone administrator password *1739*.
2. Tap the **Settings** menu, then tap **Provisioning Server** and **Accept server identity**.
3. When server certificate information displays, confirm all of the data by scrolling to the bottom and then tapping **Confirm**.

   The device reboots and picks up the changes. It then reconnects to the Dolby Conferencing Console software over HTTPS.

Steps 1-3 describe the manual setup process. Alternatively, you can set the Dolby Conference Phone so that it detects the Dolby Conferencing Console address, and then you can avoid entering the address manually.

For example, in the DHCP server, use **option 66** for the Dolby Conference Phone to automatically connect to the Dolby Conferencing Console software. In option 66, enter *https://dcc.yourcompany.net* , where *dcc* is your Dolby Conferencing Console host name.

Note: If you performed steps 1-3, you do not need to enter the company name in option 66. For more information, see the *Dolby Conference Phone Administrator's Guide*.

4.8.5 Configuring HTTP and HTTPS access

You can increase security by disabling HTTP access on port 80. You can optionally allow HTTPS access.

Procedure

1. Disable HTTP port 80.

   The HTTP port (80) can be disabled completely to increase security for Dolby Conferencing Console.

   a) Make the */etc/dcc/web.ini* file writable:

   ```
   chmod +w /etc/dcc/web.ini
   ```

   b) Delete the first line from that file where it enables port 80.

   c) Restart the Dolby Conferencing Console software:

   ```
   service dcc restart
   ```

d) Make the */etc/dcc/web.ini* file read only again:

```
chmod -w /etc/dcc/web.ini
```

2. (Optional) Enable HTTPS access through the server firewall.

   In some cases, it is possible that the firewall has disabled port 443 access. To open port 443 for HTTPS access and check the status of the firewall, use these commands:

   Example for Redhat 6 and CentOS 6.0:

```
iptables -I INPUT -p tcp -m tcp --dport 443 -j ACCEPT
service iptables save
service iptables status
```

   Example for Redhat 7 and CentOS 7.0:

```
firewall-cmd --zone=public --add-service https --permanent
firewall-cmd --reload
firewall-cmd --list-all
```

4.8.6 Enabling SSH access on open virtual appliance file installations

SSH access is disabled by default on open virtual appliance file installations. You can optionally enable SSH access.

About this task

On open virtual appliance file installations, perform these steps to enable root user access through port 22 (SSH) by editing the **sshd_config** file:

Procedure

1. Enter this command:

```
vi /etc/ssh/sshd_config
```

2. Change `PermitRootLogin no` to `PermitRootLogin yes`.
3. Save the file.
4. Restart **sshd** with this command:

```
service sshd restart
```

4.9 Setting the time zone

Use the Linux command line on the Dolby Conferencing Console server to update the symbolic link for */etc/localtime* to match your local time.

Prerequisites

To set the time zone, you need to know the Linux `root` password for the server. For open virtual appliance file deployments, the default `root` password is `dolby`. We recommend that you change the default password; a colleague may have already done so for your server. For RPM installations, Dolby software never sets your `root` password; consult the other system administrators in your organization to learn the password.

Procedure

1. Log in as `root`, and locate the correct time zone file under */usr/share/zoneinfo*.

2. Save a copy of the old symbolic link at */etc/localtime*, and then update the link to reflect your time zone.

```
cp /etc/localtime /root/old.timezone
rm /etc/localtime
ln -s /usr/share/zoneinfo/my_zone /etc/localtime
```

3. Restart the Dolby Conferencing Console server:

```
service dcc restart
```

4. Repeat these steps on each server.

Glossary

API
Application programming interface. A set of functions that can be used to access the functions of an operating system or other type of software.

AWS
Amazon Web Services. The Amazon cloud computing services platform.

CentOS
Community Enterprise Operating System.

device access service
A server or node on a network that manages device traffic for the Dolby Conferencing Console.

DHCP
Dynamic Host Configuration Protocol.

DNS
Domain Name System. An Internet service that translates Internet domain and host names to IP addresses and conversely. DNS automatically converts between the name entered in a web browser and the IP addresses of the web server hosting the site whose URL is entered in the web browser.

HTTP
Hypertext Transfer Protocol. An application protocol for hypermedia information systems, and the foundation for data communication for the World Wide Web.

HTTPS
Hypertext Transfer Protocol Secure. An application protocol for secure communication over a network and the Internet that provides authentication of websites and keeps user information private.

IP
Internet Protocol.

IP address
Internet Protocol address. A numerical identifier assigned to a device that is a member of a network that uses the IP for communication.

LDAP
Lightweight Directory Access Protocol. An application protocol for querying or modifying items in corporate directories that allows sharing of information about users, devices, and applications on a network.

MAC
Multiply-accumulate. In digital signal processing, the multiply-accumulate operation is a common step that computes the product of two numbers and adds that product to an accumulator.

MAC address
Media access control address. A unique identifier assigned to a network interface for communications on a network. MAC addresses are typically assigned by the network interface manufacturer.

MIB
Management information base. A type of communications network management database.

NTP
Network Time Protocol. A network protocol for clock synchronization on computers.

OVA file
A single Open Virtualization Format (OVF) file packaged together with all of its supporting files. Also known as open virtual applications.

OVF
Open Virtualization Format. File format for the packaging and distribution of software to be run in a virtual machine.

PBX
Private branch exchange. A phone system that is delivered as a hosted service.

PEM
Privacy-Enhanced Electronic Mail. A file format for security certificates in email communication.

RPM
RPM Package Manager. A system for managing Linux software installation packages.

SIP
Session Initiation Protocol. An application-layer communications protocol used for signaling and controlling communications sessions.

SMTP
Simple Mail Transfer Protocol. An Internet standard for sending and receiving emails.

SNMP
Simple Network Management Protocol. A protocol for managing IP network devices

SSH
Secure Shell protocol. An encrypted network protocol for secure data communication, remote command-line login, remote command execution, and other secure network services between two networked computers.

SSL
Secure Sockets Layer . A security protocol that works at a socket level.

STARTTLS
An extension to plain text communication protocols (such as Simple Mail Transfer Protocol [SMTP] and Lightweight Directory Access Procotol [LDAP] services) that changes a plain text connection to an encrypted (Transport Layer Security [TLS] or Secure Socket Layer [SSL]) connection instead of using a separate port for encrypted communication.

TLS
Transport Layer Security. A cryptographic protocol designed to provide communications security over a computer network.

UDP
User Datagram Protocol. A communications protocol that uses no handshaking dialogues to establish a connection with the remote host. UDP is a member of the IP suite.

UI
User interface.

Dolby Laboratories, Inc. 1275 Market Street, San Francisco, CA 94103-1410 USA.
© Dolby Laboratories. All rights reserved. Dolby and the double-D symbol are registered trademarks of Dolby Laboratories. All other trademarks remain the property of their respective owners.


DOLBY
VOICE