opentext™

OpenText Filr 23.4

Installation, Deployment, and Upgrade Guide

July 2024

Legal Notice

Copyright 2023-2024 Open Text

The only warranties for products and services of Open Text and its affiliates and licensors (“Open Text”) are as may be set forth in the express warranty statements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty. Open Text shall not be liable for technical or editorial errors or omissions contained herein. The information contained herein is subject to change without notice.

Contents

About This Guide 7

1 Overview 9

2 Planning Is Critical 11

3 Filr System Requirements 13

4 Setting Up Shared Storage 21

5 Downloading and Preparing the Filr Software 25

6 Deploying the Virtual Machines 29

Deploying a VMware VM 29
Deploying a Hyper-V VM 31
Deploying a Xen VM 34
Deploying a Citrix Xen VM 37

7 Starting and Configuring the Filr Appliances 41

8 Creating an Expandable Filr Deployment 47

Setting Up the SQL Database 49
Configuring a PostgreSQL Appliance 50
Configuring a MySQL or MariaDB Server 51
Configuring a Microsoft SQL Server 52
Setting Up Two Filr Search Appliances 53
Setting Up the Filr Appliances 54
Completing the Expandable Filr Deployment 60
Dedicating a Filr Appliance to Indexing and Net Folder Synchronization 63
Using the Dedicated Filr Appliance to Complete the Indexing Setup 64

9 Content Editor 67

Content Editor Requirements 67
System Requirements 67
Other Requirements 68
Virtualization Hypervisor Platform Support 68
Downloading and Installing Content Editor 69
VMWare 69
Hyper-V 70
Xen 73
Citrix Xen 75

Starting and Configuring the Content Editor Appliance . . . 77
Configuring Content Editor Appliance . . . 79
Configuring Content Editor Options in Filr Appliance . . . 80
Content Editor With NetIQ Access Manager For Online Edit Feature . . . 81
Configuring NetIQ Access Manager With Content Editor . . . 81
Allowing Filr to Connect to Content Editor . . . 86
Allowing Content Editor to Connect to the Filr . . . 87
Using the Online Edit Feature . . . 87
Load Balancing . . . 87
Upgrading from Content Editor 1.2.3 to 2.0 . . . 89
Support Matrix . . . 89
Upgrading Content Editor Appliance . . . 90
Before You Upgrade . . . 90
Understanding the Appliance Upgrade Process . . . 91
Downloading and Preparing Software for the Upgrades . . . 92
Copying Each Appliance's /vastorage Disk (Disk 2) . . . 94
Upgrading the VMs . . . 94

Part I Upgrading Filr 101

10 Upgrading from Filr 4.3.1.2 to Filr 5.0 103

Support Matrix . . . 103
Upgrading a Large Filr Deployment . . . 103
Before You Upgrade! . . . 103
Understanding the Appliance Upgrade Process . . . 106
Downloading and Preparing Software for the Upgrades . . . 106
Copying Each Appliance's /vastorage Disk (Disk 2) . . . 109
Upgrading the VMs . . . 109
Deploying the Upgraded (Replacement) VMs . . . 118
Performing Post-Upgrade Tasks . . . 119
Upgrading an All-in-One (Small) Deployment . . . 120
Before You Upgrade! . . . 120
Small Filr Upgrade Process Overview . . . 121
Downloading and Preparing Software . . . 121
Copying Each Appliance's /vastorage Disk (Disk 2) . . . 122
Upgrading the VMs . . . 123
Deploying the Upgraded Filr VM . . . 131
Performing Filr Post-Upgrade Tasks . . . 132

11 Updating Filr through Online Update Channel 133

Updating an All-in-One (Small) Deployment . . . 133
Updating a Large Filr Deployment . . . 134
Recommended Before Updating to Filr 23.4 . . . 134

12 Setting Up Filr Services 135

13 Setting Up Sharing 139

Enabling Users to Share . . . 139
Best Practices for Setting Up Sharing . . . 139

General Order for Setting Up Sharing 140
Enabling Sharing for Specific Net Folders 144
Restricting Sharing Files by Group of Users 144
Do Not Enable Sharing for All Internal Users and All External Users 145
System-Level Sharing Must Be Configured First 145
My Files Sharing Is Automatic 146
Net Folder Sharing Must Be Explicitly Allowed At Two Levels 146

Part II Appendixes **149**

A Access Manager (NAM) and Filr Integration **151**

Overview 151
Configuring Filr Ports 152
Downloading and Installing the Filr Authentication Plugin 152
Configuring the NAM Identity Server 152
Configuring the Identity User Store 153
Creating the Authentication Class 153
Creating the Authentication Method 153
Creating the Authentication Contract 154
Configuring a Reverse-Proxy Single Sign-On Service for Filr 154
Creating a New Reverse Proxy 154
Configuring the Proxy Service 154
Creating Policies 155
Configuring Protected Resources 156
Configuring a Rewriter Profile 158

B All-in-One (Small) Deployment—Creating **161**

C Non-Expandable Deployment—Creating **163**

D SCSI Controller Type—Changing on VMware **165**

E Troubleshooting Filr **167**

Installation Issues 167
Unable to Access a Newly Installed Appliance 167
Upgrade Issues 167
The Upgrade Dialog Box Is Not Displayed during an Upgrade 167
Rolling Back to the Previous Version after an Unsuccessful Upgrade 168

F Filr Limitations **171**

Installation 171
Importing of .ovf and .vmdk Files Fails with VMware vSphere 6.7 Update 2 171
NFS Mount Point Must Not Point to /var on Target Server 171
Upgrade 172
Rolling Upgrades Are Not Supported in a Clustered Environment 172
Appliance 172
VMware Snapshots and Appliance Backup 172
Configuration 172

User Name Character Restrictions for LDAP Synchronization and Login 173
User Names That Are Synchronized from LDAP Are Not Case Sensitive for Filr Login 173
Disabling Web Access Does Not Block Guest Access 173
Unable to Upload Site Branding Image to Filr 173
Distributed File System (DFS) Issues 173
Access Manager Issues 174
Net Folder 175
Active Directory Cross Forest Trust Relationship Is Not Supported 175
Moving or Renaming a File from the File Server Removes Shares 176
Folder Path in Filr Cannot Exceed 48 Levels 176
Modifying the Target Location in a Junction Created On the OES Server Does Not Reflect in the Filr Net Folder Pointing to the Junction 176
Filr Appliance 176
Reporting Issues 177
My Files Storage Directory Is Displayed in Search 177
Sharing Issues 177
Editing an .rtf File Results in an Editing Conflict Error 178
LDAP Synchronization Issues 178
Email Issues 180
Cannot Upload Documents Created with Apple iWork (Pages, Keynote, etc.) or .app Documents to the Filr Web Client 180
Unable to Upload Microsoft OneNote Files to Filr 180
Cannot Extract ZIP File after Downloading on Mac 180
Issues When Downloading Multiple Files with Safari on Mac 181
File Name Should Not Be More Than about 200 Characters 181
WebDAV Issues 181
Cannot Log in to Web Client with Long User ID or Password 182
Display Issues Due to Third-Party Software 182
Cannot View ODP and ODG Files That Contain Charts, Graphs, and Tables When Viewing in HTML Format 182
User Home Directories Are Not Synchronized until Trustee Cache Information is Updated 183
Filr Does Not Support Aliases That Have Been Configured in the LDAP Directory 183
Cannot Use Text Editors Such as Notepad or Wordpad as a Document Editor 183
Must Restart All Appliances after a Network Failure with Microsoft SQL 183
Database Appliance 183
Filr Installation Program Cannot Create the Filr Database in Microsoft SQL When the Database Name Begins with a Number 183
Desktop Application 184
Mobile Apps 184
iOS Devices 184
Windows Device 186
All Mobile Devices 186
Web Application 187
The .bmp Images Appear Blank in the Internet Explorer 187
Password-Protected Files Cannot Be Viewed 187
Enabling a User Account Fails For a Restored User Profile If the User's My Files Storage Folder is Not Restored from the Trash 187
Windows Subsystem For Linux and Filr Client 188

About This Guide

Best Practice Deployments

To create a production-viable, best practice Filr deployment, complete the sections below in the order presented.

- Chapter 1, “Overview,” on page 9
- Chapter 2, “Planning Is Critical,” on page 11
- Chapter 3, “Filr System Requirements,” on page 13
- Chapter 4, “Setting Up Shared Storage,” on page 21
- Chapter 5, “Downloading and Preparing the Filr Software,” on page 25
- Chapter 6, “Deploying the Virtual Machines,” on page 29
- Chapter 7, “Starting and Configuring the Filr Appliances,” on page 41
- Chapter 8, “Creating an Expandable Filr Deployment,” on page 47
- Chapter 9, “Content Editor,” on page 67
- Chapter 10, “Upgrading from Filr 4.3.1.2 to Filr 5.0,” on page 103
- Chapter 12, “Setting Up Filr Services,” on page 135
- Chapter 13, “Setting Up Sharing,” on page 139

Test and Evaluation Deployments

To create an evaluation or test deployment, see the following sections.

- Appendix B, “All-in-One (Small) Deployment—Creating,” on page 161

  and

- Appendix C, “Non-Expandable Deployment—Creating,” on page 163

Upgrade Instructions

To upgrade existing deployments, see

- Chapter I, “Upgrading Filr,” on page 101
- “Upgrading an All-in-One (Small) Deployment” on page 120

Audience

This guide is intended for Filr Administrators.

Feedback

We want to hear your comments and suggestions about this manual and the other documentation included with this product. Please use the **comment on this topic** link at the bottom of each page of the online documentation.

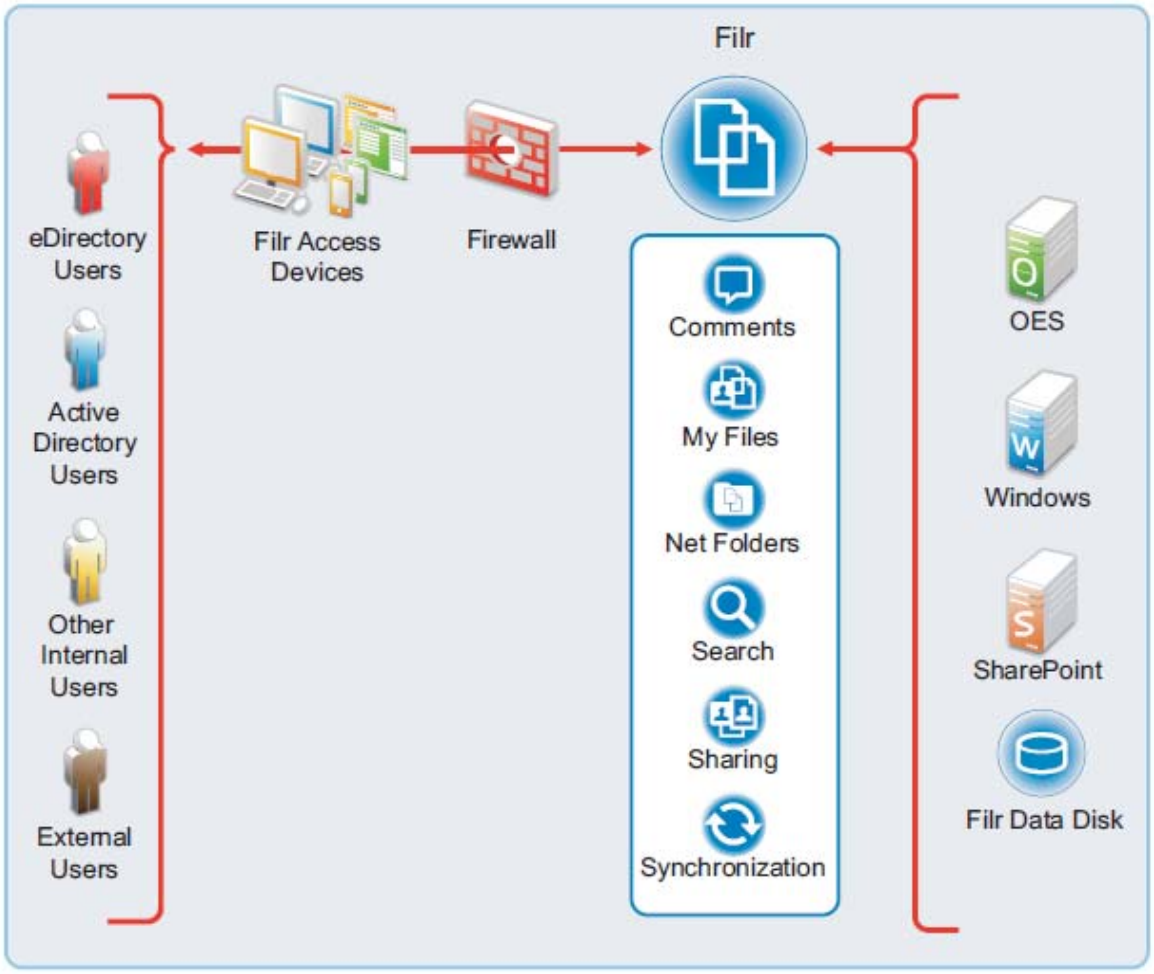
Documentation Updates

For the most recent version of this guide, visit the Filr Documentation web site.

1 Overview

What Is OpenText Filr?

OpenText Filr is an enterprise file sharing tool that leverages your current file server and security infrastructure to provide multi-device access to organizational and personal files.



For more detail about this illustration and for more illustrations and explanations, see the *OpenText Filr 23.4: Understanding How Filr Works*.

What Is “Filr Clustering”?

“Filr clustering” is a term that is sometimes used in the Filr product and means that multiple Filr appliances access a shared storage location, which contains deployment-level configuration settings and data. “Filr clustering” provides a measure of

- Fault tolerance

And

- High availability

“Filr clustering” is not related to Novell Cluster Services.

This guide refers to “Filr-clustered” deployments as “Expandable” deployments.

2 Planning Is Critical

Creating a successful Filr deployment requires that you

1. Involve pertinent stakeholders.
2. Conduct a thorough needs assessment.
3. Plan your deployment based on the needs assessment.

3 Filr System Requirements

The following sections outline platform, version, and other requirements for your expandable Filr deployment.

- "Administrative Workstations and Browsers" on page 13
- "Appliance Disk Space" on page 13
- "Appliance Memory and CPU" on page 14
- "Appliance Shared Storage (/vashare Mount Point) Platforms" on page 13
- "Desktop Platforms (for the Desktop Application)" on page 15
- "Desktop Web Application Access" on page 15
- "File Servers (Backend Storage)" on page 16
- "Filr Software" on page 17
- "IP Addresses" on page 17
- "LDAP Directory Services (Users and Groups)" on page 18
- "Mobile Device Platforms" on page 18
- "SQL Database Server" on page 19
- "Secure Access" on page 19
- "Virtualization Hypervisor Platform" on page 20

Administrative Workstations and Browsers

Table 3-1 *Administrative Workstations and Browsers*

Platform	Browser	Requirement
Windows, Mac, or Linux	Microsoft Edge	Latest version
	Google Chrome	Latest version
	Safari	Latest version

Appliance Disk Space

Planning for disk space varies widely according to organization needs.

For an overview of Filr storage, see "Appliance Storage Illustrated" in the *OpenText Filr 23.4: Understanding How Filr Works*.

Appliance Shared Storage (/vashare Mount Point) Platforms

- Storage Planning Summary

The Filr appliances in an Expandable deployment access a commonly-shared CIFS or NFS storage disk that you will identify and create in Chapter 4, “Setting Up Shared Storage,” on page 21.

Table 3-2 *Shared Storage Platforms (/vashare Mount Point)*

Protocol	Requirement
CIFS	◆ A Windows-based CIFS Share ◆ Any OES based CIFS share (OES 23.4 or later)
NFS	Exported mount point on one of the following: ◆ SLES 15 SP4 NFS on Windows is not supported.

Appliance Memory and CPU

Table 3-3 *Memory and CPU*

Appliance	Recommended
Filr	◆ 20 GB RAM ◆ 12 GB Java Heap ◆ 4 CPUs
Filrsearch	Less than 1,000 Users ◆ 8 GB RAM ◆ 2 GB Memcached ◆ 4 GB Java Heap ◆ 4 CPUs More than 1,000 Users ◆ 16 GB RAM ◆ 3 GB Memcached ◆ 8 GB Java Heap ◆ 4 CPUs
PostgreSQL	Less than 1,000 Users ◆ 8 GB RAM ◆ 2 CPUs More than 1,000 Users ◆ 12 GB RAM ◆ 2 CPUs
Content Editor	◆ 16 GB RAM ◆ 4 CPUs

NOTE: Do not overcommit more memory for the processes than mentioned in the above table, beware that operating system needs considerable amount to free memory to operate.

Desktop Platforms (for the Desktop Application)

For more information about the Filr desktop application, see the following guides:

- **Linux:** *Filr Desktop Application for Linux Guide*
- **Mac:** *Filr Desktop Application for Mac*
- **Windows:** *Filr Desktop Application for Windows Guide*

Table 3-4 *Desktop Platforms (Desktop Application)*

Platform	Versions
Windows	**IMPORTANT:** Always make sure that the latest patches and support packs are installed. ◆ Windows 11 ◆ Windows 10
Mac	**IMPORTANT:** Always make sure that the latest patches and support packs are installed. ◆ Intel - macOS 14 and macOS 13 ◆ ARM64 (in tech preview) - macOS 14 and macOS 13
Linux Platform	◆ Ubuntu 16.04.4 LTS (Xenial Xerus) **NOTE:** Supports Unity graphical desktop environment ◆ SLED 12 SP4 **NOTE:** Filr supports only the default GNOME graphical desktop environment that is shipped with SLED.

Desktop Web Application Access

Three components apply:

- A Browser
- Java
- An Office Application

Table 3-5 *Browsers for Web Application Access*

Platform	Requirement
Linux	Mozilla Firefox
Windows	◆ Microsoft Edge ◆ Mozilla ◆ Firefox ◆ Google Chrome (latest versions)
Mac	◆ Safari ◆ Mozilla ◆ Firefox ◆ Google Chrome

Table 3-6 *Java for Web Application Functionality*

Version	Functionality
Java v11	◆ **Editing files with Edit-in-Place** ◆ **Uploading folders to Filr** If the browser does not support HTML 5, uploading both files and folders requires this version of Java to be installed.

Table 3-7 *Office Application for Edit-in-Place Functionality*

NOTE: OpenOffice and LibreOffice are used synonymously throughout the Filr documentation.	
Linux	◆ OpenOffice.org (latest version) ◆ LibreOffice (latest version)
Windows	◆ LibreOffice (latest version) ◆ OpenOffice (latest version) ◆ MS Office 2016, 2019, and 2022 ◆ MS Office 365
Mac	◆ LibreOffice (latest version) ◆ OpenOffice (latest version) ◆ MS Office 2011 for MAC ◆ MS Office 2013 for MAC ◆ MS Office 365 for MAC

File Servers (Backend Storage)

NOTE: Your organization's file servers provide the backend storage for Net Folders.

If you use Filr only for user personal storage (My Files), then file servers aren't required.

Table 3-8 *File Servers*

Platform	Supported Versions
Windows (Standalone and Clustered environment)	◆ Windows Server 2022 (CIFS) ◆ Windows Server 2019 (CIFS) ◆ Windows Server 2016 (CIFS) Windows native DFS-N and DFS-R with replication are supported
OES (Standalone and Clustered environment)	**IMPORTANT:** You must apply the latest Scheduled Maintenance Update, otherwise the NCP server can fail. ◆ OES 23.4 (NCP and CIFS) ◆ OES 23.4 NSS AD (CIFS) ◆ OES 24.2 (NCP and CIFS) ◆ OES 24.2 NSS AD (CIFS)
Other	In addition to storage that is directly attached to the file servers listed in Net Folders can provide access to files that are being stored on any of the following storage platforms: ◆ NetApp NAS device ◆ EMC ◆ Other Microsoft Active Directory joined NAS devices that support the CIFS protocol. ◆ Storage Area Network (SAN)
SharePoint	◆ 2019

Filr Software

To download and prepare the Filr software, See Chapter 5, “Downloading and Preparing the Filr Software,” on page 25.

IP Addresses

Each appliance requires the following.

Table 3-9 *IP Addresses*

Component	Requirement
IP Address	◆ A static address that is associated with a DNS host name. Example: 192.168.1.61
Network Mask	◆ The appropriate network mask for the IP address. Example: 255.255.255.0
Gateway IP Address	◆ The gateway for the IP address subnet. Example: 192.168.1.254

Component	Requirement
DNS Host Name	◆ The DNS name associated with the IP address. Example: filr-1.myorg.local
DNS IP Address	◆ Up to three IP addresses of DNS servers for the IP address subnet. Example: 192.168.1.1
NTP IP Address or DNS Name	◆ Up to three IP addresses or DNS names of reliable NTP servers used to coordinate time on your organization's network—especially your LDAP directory servers. Example: time.myorg.local When using VMware, it is recommended that you set up NTP in accordance with the VMware best practices guidelines.

LDAP Directory Services (Users and Groups)

Table 3-10 *LDAP Directory Services*

Directory Service	Platform Version
eDirectory	◆ NetIQ eDirectory 9.2.8.x ◆ NettIQ eDirectory 8.8.*x*.*x* For more information, see the NetIQ eDirectory 8.8 Documentation website. ◆ NetIQ eDirectory version 8.8.*x*.*x* on standalone Windows. **IMPORTANT:** eDirectory running on Windows servers with file shares is not supported.
Active Directory	◆ Windows Server 2022 Active Directory with the latest Service Pack ◆ Windows Server 2019 Active Directory with the latest Service Pack ◆ Windows Server 2016 Active Directory with the latest Service Pack

Mobile Device Platforms

IMPORTANT: Accessing Filr through a web browser on a mobile device is not supported. Instead, download the Filr mobile app that is compatible with your mobile device.

For more information about the Filr mobile app, see the OpenText Filr 23.4 Mobile App Quick Start Help.

Table 3-11 *Mobile Devices*

Platform	Supported Versions
iOS Phones and Tablets	◆ iOS 17.x and iOS 16.x The native app is available as a free download in the Apple App Store.
Android Phones and Tablets	◆ Android 8 to 14 The native app is available as a free download in the Google Play App Store.

SQL Database Server

Table 3-12 *SQL Database Server*

Database Type	Supported Versions
PostgreSQL	◆ 15.6
(Standalone and Clustered environment)	◆ 14.3
MySQL	◆ 8.0.34
Microsoft SQL	◆ SQL Server 2022 ◆ SQL Server 2019 ◆ SQL Server 2017 ◆ SQL Server 2016 SP1
MariaDB	◆ 10.11 ◆ 11.1.3

Secure Access

Table 3-13 *Secure Access*

Component	Supported Versions
NetIQ Access Manager	5.0 and 4.5
NetIQ Advance Authentication	6.4.2 and 6.4.1.1. Only the Enterprise Editions are supported.

Virtualization Hypervisor Platform

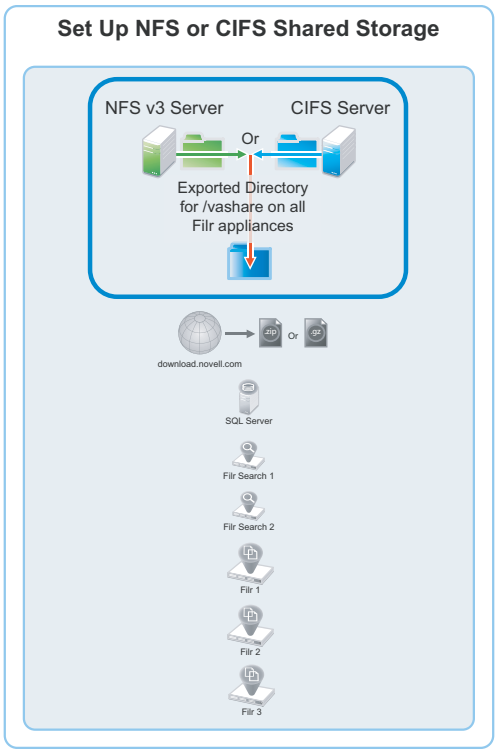
Table 3-14 *Virtualization Hypervisor Platform*

Hypervisor Type	Supported Versions
VMware	◆ One of the following VMware host servers for hosting the appliance VMs. ◆ ESXi 8.0.1 ◆ ESXi 7.0 ◆ ESXi 6.7 For the most up-to-date compatibility matrix of supported VMware host servers, see the *VMware Compatibility Guide* provided by VMware. ◆ VMware vMotion is supported when running Filr on VMware ESXi
Hyper-V	◆ The following platforms ◆ Windows Server 2022 ◆ Windows Server 2019 ◆ Windows Server 2016 ◆ Hyper-V Manager to deploy, set up, and configure the appliances.
Xen	**IMPORTANT:** Apply all Xen and kernel patches before installing. ◆ The server with the Xen packages installed and the Xen bootloader running by default. ◆ SLES 15 SP4 ◆ Virtual Machine Manager to deploy, set up, and configure the appliances.
Citrix Xen	◆ Citrix XenServer 8.2 ◆ Citrix XenServer 7.6 ◆ Citrix XenCenter to deploy, set up, and configure the appliances.

4 Setting Up Shared Storage

Figure 4-1 is the first in a series of illustrations that visually track deployment order.

Figure 4-1 *Export an NFS Directory or Create a CIFS share for the /vashare mount point*



Complete the instructions in the section below:

- “Exporting an NFS Directory for the /vashare Mount Point” on page 21

  Or

- “Creating a CIFS Share for the /vashare Mount Point” on page 22

Exporting an NFS Directory for the /vashare Mount Point

IMPORTANT: Filr does not support remote NFS from a Novell Storage Services (NSS) volume.

If you plan to use a CIFS share for Filr shared storage (/vashare), skip to “Creating a CIFS Share for the /vashare Mount Point” on page 22. Otherwise, export an NFS directory on a Linux server by doing the following:

Table 4-1 *Task 1: Exporting an NFS Directory for /vashare*

Page, Dialog, or Option	Do This
	1 - Verify that the server has adequate disk space.
	1. Make sure that the Linux server that you are targeting has the available disk space you have identified. If necessary, add disk space to the Linux server.
	1. On the Linux server, launch YaST2.
YaST Control Center	1. In the **Network Services** section, click **NFS Server**. The NFS Server Configuration dialog box displays.
NFS Server Configuration	1. Make sure that the NFS Server is set to **Start**, that **Open Port in Firewall** is selected (running firewall required for option), and that **Enable NFSv4** is *not selected* - i.e. NFS v4 is disabled. 2. Click **Next**.
Directories to Export	1. Click **Add Directory**.
YaST2	1. Click **Browse** and choose the directory or share path that has the required disk space. You can add a directory name, such as `/shared` to the path if desired. **IMPORTANT:** The directory path must not be located in the /var directory structure on the NFS server, as explained in "NFS Mount Point Must Not Point to /var on Target Server" on page 171. 2. Click **OK**. As your first Filr appliance is deployed, a directory named `filr` will be created within the directory path you have specified. 3. If you added to the directory path, click **Yes** to confirm directory creation. 4. Leave the asterisk (*) in the **Host Wild Card** field. 5. Click the **Options** field to edit it and change the following options: ◆ `ro` to `rw` (read-only to read-write) ◆ `root_squash` to `no_root_squash`. 6. Click **OK**.
Directories to Export	1. Click **Finish**. 2. Skip to Chapter 5, "Downloading and Preparing the Filr Software," on page 25.

Creating a CIFS Share for the /vashare Mount Point

Table 4-2 *Task 1: Creating a CIFS Share for /vashare*

Page, Dialog, or Option	Do This
	1 - Verify that the Windows server has adequate disk space.

Page, Dialog, or Option	Do This
	1. Make sure that the Windows server that you are targeting has the available disk space you have identified. Beginning with Filr 4.0, CIFS share is configured with SMB2/SMB3 protocol. Versions earlier than SMB2/SMB3 are not supported. 2. Open Windows Explorer
Windows Explorer	1. In Windows Explorer, navigate to the folder that will be the shared storage location (/vashare) for Filr. 2. Right-click the folder, then click **Properties**.
folder Properties	1. Click the **Sharing** tab. 2. Click **Share**.
Filr Sharing	1. Add a user (new or existing) to the list and assign the **Read/Write** permission to the user. **IMPORTANT:** You will need the username and password when you select the CIFS share while deploying the Filr appliances. 2. Click **Share > Done > Close**.
Directories to Export	1. Continue with Chapter 5, “Downloading and Preparing the Filr Software,” on page 25.

Windows Share as /Vashare

By default, encryption is disabled. To enable the encryption, perform the following steps:

For the steps to enable the encryption on the Windows Share, see https://learn.microsoft.com/en-us/windows-server/storage/file-server/smb-security

Perform the following steps to enable encryption on the Filr server:

Open `/etc/fstab`

Change from

```
//server/path /vashare cifs credentials=/etc/opt/novell/base/
.smbcredentials,vers=3.0,rw,nounix,iocharset=utf8,uid=30,gid=478,file_mode
=0777,dir_mode=0777 0 0
```

To

```
//server/path /vashare cifs credentials=/etc/opt/novell/base/
.smbcredentials,vers=3.0,seal,rw,nounix,iocharset=utf8,uid=30,gid=478,file
_mode=0777,dir_mode=0777 0 0
```

OESCIFS Share as /Vashare

By default, encryption is disabled. To enable the encryption, perform the following steps:

On the OES server level, run the command

```
#novcifs --encrypt-data=yes
```

Perform the following steps to enable encryption on the Filr server:

Open the `/etc/fstab`

Change from

```
 //server/path /vashare cifs credentials=/etc/opt/novell/base/
.smbcredentials,vers=3.0,rw,nounix,iocharset=utf8,uid=30,gid=478,file_mode
=0777,dir_mode=0777 0 0
```

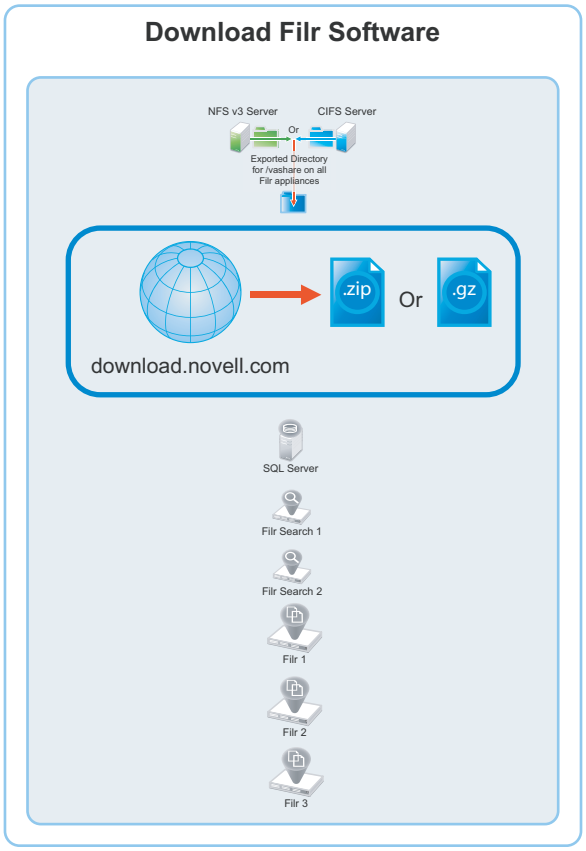
To

```
//server/path /vashare cifs credentials=/etc/opt/novell/base/
.smbcredentials,vers=3.0,seal,rw,nounix,iocharset=utf8,uid=30,gid=478,file
_mode=0777,dir_mode=0777 0 0
```

5 Downloading and Preparing the Filr Software

After planning your deployment and making sure you have the necessary system requirements in place, you are ready to download and prepare the Filr software that applies to your virtualization platform.

Figure 5-1 *Download the Filr Software for your VM platform*



- "VMWare" on page 25
- "Hyper-V" on page 26
- "Xen" on page 26
- "Citrix Xen" on page 27

VMWare

1 Download the Filr software shown below to the location where you plan to host your VMs.

IMPORTANT: Registration with OpenText is required to receive an email with a download link.

Appliance Type	Filename
Filr	`Filr.x86_64-version.ova`
Search	`Filrsearch.x86_64-version.ova`
PostgreSQL	`PostgreSQL-version.ova`

2 Continue with "Deploying a VMware VM" on page 29.

Hyper-V

1 Log in to the Hyper-V host server either locally or from a remote workstation using Remote Desktop.

2 Download the Filr software shown below to the location where you plan to host your VMs.

IMPORTANT: Registration with OpenText is required to receive an email with a download link.

Appliance Type	Filename
Filr	`Filr.x86_64-version.vhdx`
Search	`Filrsearch.x86_64-version.vhdx`
PostgreSQL	`PostgreSQL-version.vhdx`

3 Move the `Filr.x86_64-version.vhdx` archive file to the first Filr appliance-type folder and then copy the archive file to the remaining Filr appliance type folders.

4 Move the `Filrsearch.x86_64-version.vhdx` archive file to the first Filrsearch appliance-type folder and then copy the archive file to the second Filrsearch folder.

5 Continue with "Deploying a Hyper-V VM" on page 31.

Xen

1 Log in to the Xen VM host server either locally or from a remote workstation.

If you are connecting from a remote Linux workstation, use the following command:

```
ssh -X root@host_ip_address
```

The -X in the command in required for the GUI installation program upon which the steps in this section are based.

2 Download the Filr software shown below to the Xen VM host server in the location where you plan to host your VMs.

IMPORTANT: Registration with OpenText is required to receive an email with a download link.

Appliance Type	Filename
Filr	`Filr.x86_64-version.qcow2`
Search	`Filrsearch.x86_64-version.qcow2`
PostgreSQL	`PostgreSQL-version.qcow2`

3 Create two hard disks - In the *`ApplianceType-version`* directory, execute the following commands:

```
qemu-img create -f raw storage1.qcow2 20G
qemu-img create -f raw storage2.qcow2 20G
```

Two hard disks with names storage1 and storage2 are created with 20 GB space.

4 Copy and rename the `ApplianceType` directories until you have one directory for each appliance that you have planned to deploy.

Consider including information in the name that easily identifies the appliance, such as the IP address. For example:

1. Rename the `Filr-version` directory to `Filr-30-192.168.1.61`.
2. Copy the `Filr-30-192.168.1.61` directory and rename it to `Filr-30-192.168.1.62`, and so on until you have the number of Filr appliances you have planned for.
3. In a similar manner, copy and rename the `Filrsearch-version` directory until you have two Filrsearch appliances.
4. If you need a PostgreSQL appliance, follow the same methodology.

IMPORTANT: Do not change the names of the `.qcow2` or `.xenconfig` files within the directories that you have copied and renamed.

5 Continue with "Deploying a Xen VM" on page 34.

Citrix Xen

1 On a workstation with Citrix XenCenter installed, download the Filr software shown below.

IMPORTANT: Registration with OpenText is required to receive an email with a download link.

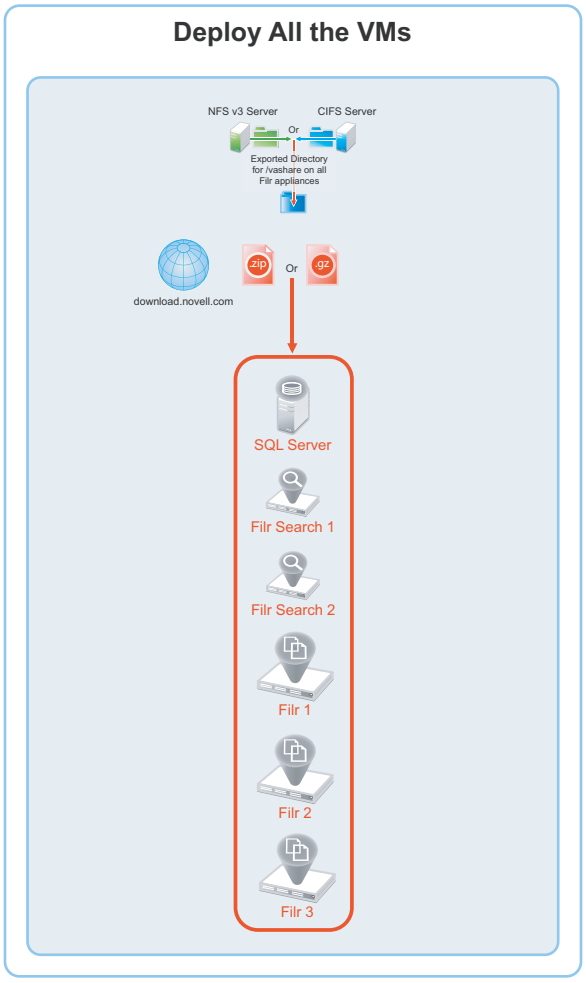
Appliance Type	Filename
Filr	`Filr.x86_64-version.xva`
Search	`Filrsearch.x86_64-version.xva`
PostgreSQL	`PostgreSQL-version.xva`

2 Continue with "Deploying a Citrix Xen VM" on page 37.

6 Deploying the Virtual Machines

After downloading and preparing the Filr software as instructed in Chapter 5, “Downloading and Preparing the Filr Software,” on page 25, complete the instructions in the section for your virtualization platform.

Figure 6-1 *Deploy All VMs*



- “Deploying a VMware VM” on page 29
- “Deploying a Hyper-V VM” on page 31
- “Deploying a Xen VM” on page 34
- “Deploying a Citrix Xen VM” on page 37

Deploying a VMware VM

Complete the steps in Table 6-1 for each appliance that you have planned:

Table 6-1 *Deploying a VMware VM*

Page, Dialog, or Option	Do This
	1 - Identifying the appliance.
	1. Choose an appliance to deploy. **IMPORTANT:** Your Filr deployment must be set up in the order specified in Chapter 8, "Creating an Expandable Filr Deployment," on page 47. 2. It is recommended to deploy the PostgreSQL appliance behind the firewall. 3. The Search appliance runs Memcached service to enable clustering. To secure Memcached, it is strongly recommended to deploy the Search appliance behind the firewall. Port 11211 is used by the Memcached service. For more information on securing Memcached, see Securing Memcached in the OpenText Filr 23.4: Administrative UI Reference.
	2 - Launching the Web browser, naming the VM, and choosing the datastore.
Web Browser	1. On a Web browser, enter the URL for the VMware server and login with the root credentials. 2. Right-click on the **Virtual Machines** and click **Create/register VM**.
Select creation type	Select **Deploy a virtual machine from an OVF or OVA** file, then click **Next**.
Select OVF and VMDK files	Specify the name for the virtual machine. For example, Demo-VM. Upload the ovf and vmdk files of Filr, and click **Next**.
Select Storage	Select a storage repository where the disk images for the imported VMs will be placed. Review the datastore details, and select an appropriate disk format from the available options. Retain all the other default settings, and click **Next**.
Deployment options	Do not select **Power on automatically** (so that the VM can be powered on after adding the disks), and click **Next**.
Ready to complete	Review the screen and click **Finish** to successfully deploy the Filr Appliance. The boot disk is created and the appliance is deployed.
	3 - Editing the VM settings.
	Right-click the VM you just deployed and select **Edit Settings**. The Virtual Machine Properties dialog displays.
Virtual Machine Properties	Filr VMware VMs ship with **Memory** and **CPU** settings that are appliance-type appropriate in most circumstances. You can adjust them at this point if desired, or you can adjust them later if required for performance tuning purposes. If you increase or decrease server memory for a Filr or Filrsearch appliance, you should also modify the Java heap size, as described in "Changing JVM Configuration Settings" in the *OpenText Filr 23.4: Administrative UI Reference*.
	4 - Adding and configuring disk 2 (/vastorage) and disk 3 (/var)

Page, Dialog, or Option	Do This
Virtual Hardware	1. Click **Add hard disk** > **New standard hard disk**. This adds second hard disk. 2. Click **Add hard disk** > **New standard hard disk.** This adds the third hard disk. Click **Save** to successfully add the hard disks.
	Repeat the steps in this table until all of your planned appliances have been deployed, then continue with Chapter 7, "Starting and Configuring the Filr Appliances," on page 41.

Deploying a Hyper-V VM

Complete the steps in Table 6-2 for each appliance:

Table 6-2 *Deploying a Hyper-V VM*

Page, Dialog, or Option	Do This
	1 - Identifying the appliance.
	1. Choose an appliance to deploy. **IMPORTANT:** Your Filr deployment must be set up in the order specified in Chapter 8, "Creating an Expandable Filr Deployment," on page 47. 2. It is recommended to deploy the PostgreSQL appliance behind the firewall. 3. The Search appliance runs Memcached service to enable clustering. To secure Memcached, it is strongly recommended to deploy the Search appliance behind the firewall. Port 11211 is used by the Memcached service. For more information on securing Memcached, see Securing Memcached in the OpenText Filr 23.4: Administrative UI Reference.
	2 - Open Hyper-V Manager.
Hyper-V Host Server	1. Open the Hyper-V Manager.
	3 - Create a new VM.
Hyper-V Manager	1. In the left pane, right-click the server where you have planned to create the new virtual machine, then click **New** > **Virtual Machine**. The New Virtual Machine Wizard displays. 2. Click **Next**.
Specify Name and Location	1. Specify the appliance name and select the folder that you created in "VMWare" on page 25. 2. Click **Next**.

Page, Dialog, or Option	Do This
Specify Generation	1. Make sure that **Generation 1** is selected. 2. Click **Next**.
	4 - Specify memory
Assign Memory	1. In the **Startup RAM** field, specify the amount of memory (in MB) that you have planned for this VM. 2. Click **Next**.
	5 - Assign network adapter
Configure Networking	1. On the Configure Networking page, select the networking card for this VM. 2. Click **Next**.
	6 - Identify the system disk
Connect Virtual Hard Disk	1. Select **Use an existing virtual hard disk**. 2. Browse to and select the `.vhd` file in the folder you created for this appliance. 3. Click **Open**. 4. Click **Next**.
Summary	1. Click **Finish**. The VM is created and appears in the list of Virtual Machines.
	7 - Specify processors
Hyper-V Manager	1. In Hyper-V Manager, right-click the VM that you just created. 2. Click **Settings**.
Processor	1. Click **Processor**. 2. In the **Number of virtual processors** field, specify the number of processors. 3. Click **Next**.
	8 - Add hard disk 2 (/vastorage).
Settings for *VM* on *Host Server*	1. Under **Hardware,** select **IDE Controller 1** 2. Click **Hard Drive**. 3. Click **Add**. A Hard Drive entry is added below the controller.
Hard Drive	1. Under **Media,** select **Virtual hard disk**. 2. Click **New**.
New Virtual Hard Disk Wizard	1. Click **Next**.
Choose Disk Format	1. Select **VHD**. 2. Click **Next**.

Page, Dialog, or Option	Do This
Choose Disk Type	1. On the Choose Disk Type page, select **Fixed size** 2. Click **Next**.
Specify Name and Location	1. Specify the following: ◆ **Name:** A descriptive name for the virtual disk. For example, `Filr-1-Disk-2`. ◆ **Location:** Specify the location where you want the virtual disk to be located. 2. Click **Next.**
Configure Disk	1. Select **Create a new blank virtual hard disk**. 2. **Size:** Specify the amount for disk 2 on this appliance. 3. Click **Next.**
Summary	1. Review the summary information. 2. Click **Finish**
	9 - Add hard disk 3 (/var).
Hyper-V Manager	1. In Hyper-V Manager, right-click the VM that you just created. 2. Click **Settings**.
Settings for *VM* on *Host Server*	1. Under **Hardware,** select **SCSI Controller**. **NOTE:** Ensure that the SCSI controller number is unique for every hard disk. 2. Click **HardDrive**. 3. Click **Add**. A Hard Drive entry is added below the controller.
Hard Drive	1. Under **Media,** select **Virtual hard disk**. 2. Click **New**.
New Virtual Hard Disk Wizard	1. Click **Next**.
Choose Disk Format	1. Select **VHD**. 2. Click **Next**.
Choose Disk Type	1. On the Choose Disk Type page, select **Fixed size** 2. Click **Next**.
Specify Name and Location	1. Specify the following: ◆ **Name:** A descriptive name for the virtual disk. For example, `Filr-1-Disk-3`. ◆ **Location:** Specify the location where you want the virtual disk to be located. 2. Click **Next.**

Page, Dialog, or Option	Do This
Configure Disk	1. Select **Create a new blank virtual hard disk**. 2. **Size:** Specify the amount for disk 3 on this appliance. 3. Click **Next.**
Summary	1. Review the summary information. 2. Click **Finish > OK**
	10 - (Optional) Add a Network Adapter You can add a network adapter if your Filr deployment accesses a separate network for one or more of the following reasons: ◆ Appliance administration. ◆ NFS mount or CIFS access to the /vashare mount point. ◆ Security of Memcached. **IMPORTANT:** Bonding or teaming NICs is not supported with Filr.
Hyper-V Manager	1. In Hyper-V Manager, right-click the virtual machine for which you want to create an additional NIC, then click **Settings**.
Settings for *VM* on *Host Server*	1. Under **Hardware,** select **Add Hardware**.
Add Hardware	1. Click **Network Adapter**. 2. Click **Add**. A Network Adapter entry is added to the hardware list.
Network Adapter	1. Under **Virtual Switch**, select the secondary network associated with the Filr installation. 2. Specify any other required settings for the new network adapter. 3. Click **OK**.
Hyper-V Manager	1. Repeat the steps in this table until all of your planned appliances have been deployed, then continue with Chapter 7, “Starting and Configuring the Filr Appliances,” on page 41.

Deploying a Xen VM

Complete the steps in Table 6-3 for each appliance that you planned:

Table 6-3 *Deploying a Xen VM*

Page, Dialog, or Option	Do This
	1 - Before you deploy the first Xen VM.
	1. If you have not already done so, before you begin this process, you must set up shared storage for your Filr appliances by either: ◆ Exporting an NFS directory or ◆ Creating a CIFS share Complete the instructions in Section 4, "Setting Up Shared Storage," on page 21.
	2 - Identifying the appliance.
	1. Choose an appliance. **IMPORTANT:** Your Filr deployment must be set up in the order specified in Chapter 8, "Creating an Expandable Filr Deployment," on page 47. 2. It is recommended to deploy the PostgreSQL appliance behind the firewall. 3. The Search appliance runs Memcached service to enable clustering. To secure Memcached, it is strongly recommended to deploy the Search appliance behind the firewall. Port 11211 is used by the Memcached service. For more information on securing Memcached, see Securing Memcached in the OpenText Filr 23.4: Administrative UI Reference.
	3 - Launch the installer.
Terminal prompt on Xen VM Host Server	1. Run the following command to launch the GUI configuration menu: `virt-manager` **NOTE:** The `vm-install` command is deprecated from SLES 12 releases.
Create a new virtual machine	1. Click **File** > **New Virtual Machine**. The **Create a new virtual machine** wizard is displayed. 2. Select **Import existing disk image**. 3. Click **Forward**.
Storage path and Operating System	1. Browse and select the existing disk image. 2. Select **SUSE Linux Enterprise Server 12 SP4**. 3. Click **Forward**.

Page, Dialog, or Option	Do This
Choose Memory and CPU settings	1. Set the amount of memory (in MB) to match that of the VM you are upgrading. 2. Specify the **CPUs** to match the number of the VM you are upgrading. 3. Click **Forward**.
	4 - Name the VM.
Name of Virtual Machine	1. Specify the name of the appliance. 2. Select **Customize configuration before install**. 3. Click **Finish**.
	5 - Configure Disk 2 (/vastorage)
Hardware	1. Click **Add Hardware** at the bottom left of the screen. 2. Select the option **Select or create custom storage**. 3. Navigate to the contents of the folder for the appliance you are creating. 4. Select the `.qcow2` file (Step 3 on page 27) that you had created. 5. Click **Open** > **Finish**.
	6 - Configure Disk 3 (/var)
	1. Click **Add Hardware** at the bottom left of the screen. 2. Select the option **Select or create custom storage**. 3. Navigate to the contents of the folder for the appliance you are creating. 4. Select the `.qcow2` file (Step 3 on page 27) that you had created. 5. Click **Open** > **Finish**.
	7 - (Optional) Add a Network Adapter You can add a network adapter if your Filr deployment accesses a separate network for one or more of the following reasons: ◆ Appliance administration. ◆ NFS mount or CIFS access to the /vashare mount point. ◆ Security of Memcached. **IMPORTANT:** Bonding or teaming NICs is not supported with Filr.
Summary	1. Click **Network Adapters**.
Network Adapters	1. Click **New**.
Virtual Network Adapter	1. Specify the settings for the adapter. 2. Click **Apply**.
Network Adapters	1. Click **Apply**.

Page, Dialog, or Option	Do This
Summary	1. Click **OK**. The virtual machine is created, the appliance starts, and the configuration process begins. 2. Go to "4 - Accept the license and specify the keyboard layout." on page 42, then return to Table 6-3 on page 35 to deploy your next appliance.

Deploying a Citrix Xen VM

Complete the steps in Table 6-4 for each appliance:

Table 6-4 *Deploying a Citrix Xen VM*

Page, Dialog, or Option	Do This
	1 - Identify the appliance to deploy.
	1. Choose an appliance to deploy. **IMPORTANT:** Your Filr deployment must be set up in the order specified in Chapter 8, "Creating an Expandable Filr Deployment," on page 47. 2. It is recommended to deploy the PostgreSQL appliance behind the firewall. 3. The Search appliance runs Memcached service to enable clustering. To secure Memcached, it is strongly recommended to deploy the Search appliance behind the firewall. Port 11211 is used by the Memcached service. For more information on securing Memcached, see Securing Memcached in the OpenText Filr 23.4: Administrative UI Reference.
	2 - Launch XenCenter.
Management Workstation	1. Start XenCenter.
XenCenter	1. Connect to the Citrix XenServer where you have planned to deploy Filr. 2. Right-click the server and select **Import**.
	3 - Import the system disk
Locate the File you want to import	1. Browse to and select the `.xva` file on your management workstation for the appliance type that you are deploying. 2. Click **Open**. 3. Click **Next**.
Select the location where the imported VM will be placed	1. Select the XenServer. 2. Click **Next**.
Select target storage	1. Select the storage repository for the VM. 2. Click **Import**.

Page, Dialog, or Option	Do This
	4 - Select the network adapter
Select network to connect VM	1. Select the virtual network adapter. 2. Click **Next**.
Review the import settings	1. Deselect **Start VM(s) after import**. 2. Click **Finish**. **IMPORTANT:** Depending on network latency and other factors, it can take a while to import the system disk.
	5 - Specify Memory
	1. If you need to adjust the memory, select the newly created VM in the left pane. 2. Click the **Memory** tab. 3. Click **Edit**, change the setting, and click **OK**.
	6 - Specify Processors
	1. If you need to adjust the CPUs, right-click the newly created VM in the left pane. 2. Select **Properties**. 3. Click **CPU**, change the setting, and click **OK**.
	7 - Add Disk 2 (/vastorage)
	1. With the newly created VM selected in the left pane, click the **Storage** tab.
Virtual Disks	1. Click **Add...**.
Add Virtual Disk	1. Type a disk name that reflects the appliance name and that this is disk 2. For example, Filr-1-disk-2. 2. Specify the **Size**. 3. Click **Add**.
	8 - Add Disk 3 (/var)
Virtual Disks	1. Click **Add...**.
Add Virtual Disk	1. Type a disk name that reflects the appliance name and that this is disk 3. For example, Filr-1-disk-3. 2. Specify the **Size**. 3. Click **Add**.

Page, Dialog, or Option	Do This
	9 - (Optional) Add a Network Adapter You can add a network adapter if your Filr deployment accesses a separate network for one or more of the following reasons: ◆ Appliance administration. ◆ NFS mount or CIFS access to the /vashare mount point. ◆ Security of Memcached. **IMPORTANT:** Bonding or teaming NICs is not supported with Filr.
	1. With the newly created VM selected in the left pane, click the **Networking** tab. 2. Select the secondary network associated with the Filr installation..
XenCenter	1. Repeat the steps in this table until all of your planned appliances have been deployed, then continue with Chapter 7, “Starting and Configuring the Filr Appliances,” on page 41.

7 Starting and Configuring the Filr Appliances

Access Manager (NAM) and Filr Integration: You can configure NetIQ Access Manager (NAM) to act as Proxy service for a Filr site. To integrate Filr with NAM, you must configure the NetIQ Access Manager Identity Server, the Access Gateway, and configure protected resources for a Filr server. For more information, see Appendix A, “Access Manager (NAM) and Filr Integration,” on page 151.

After the VMs are deployed with the necessary disks added and other settings adjusted according to your plans, it is time to start and configure the appliance software on each appliance. When this step is completed, all of the appliances will be running and ready to be deployed as an integrated Filr infrastructure.

Figure 7-1 *Starting and Configuring the Appliances*

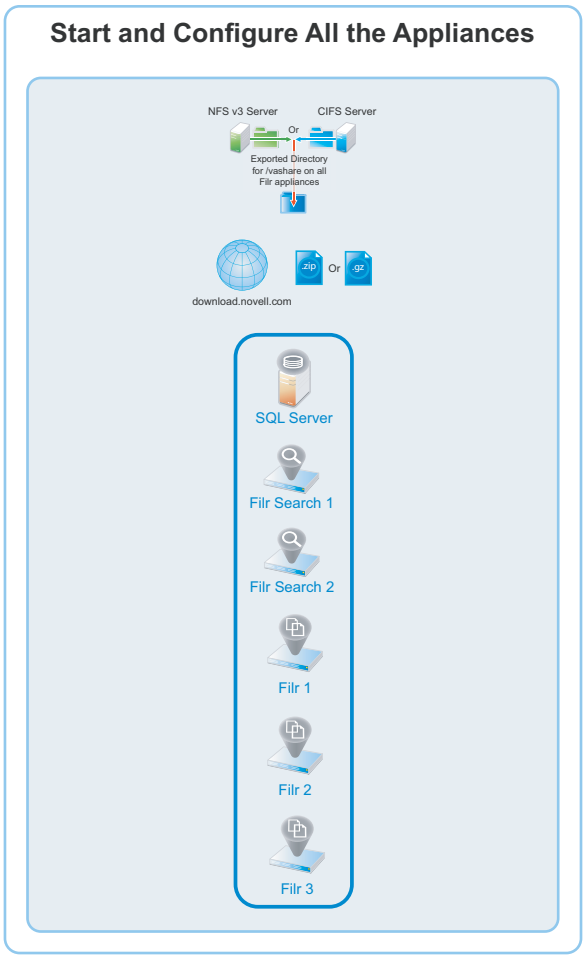


Table 7-1 *Starting and Configuring the Appliances*

Page, Dialog, or Option	Do This
	NOTE: For Xen, after you have completed the instructions in "Deploying a Xen VM" on page 34, skip to "4 - Accept the license and specify the keyboard layout." in this table.
	1 - Before you deploy the first VM.
	1. If you have not already done so, before you begin this process, you must set up shared storage for your Filr appliances by either: ◆ Exporting an NFS directory or ◆ Creating a CIFS share Complete the instructions in Section 4, "Setting Up Shared Storage," on page 21 before continuing.
	2 - Select an appliance.
	1. Choose one of the appliances that you deployed in Chapter 6, "Deploying the Virtual Machines," on page 29. **IMPORTANT:** You must set up your Filr deployment in the order specified in Chapter 8, "Creating an Expandable Filr Deployment," on page 47.
	3 - Start the appliance.
	1. After you have downloaded the Filr software and configured your appliances, you must start and configure each appliance in turn. ◆ **VMware:** In VmWare, power on the first appliance, then click the **Console** tab. ◆ **Hyper-V:** In Hyper-V Manager, right-click the VM and select **Start**. ◆ **Citrix Xen:** In XenCenter, right-click the appliance and select **Start**.
	4 - Accept the license and specify the keyboard layout.
	1. After the appliance boots, the License Agreement screen displays.
License Agreement	1. Select your preferred keyboard layout in the **Keyboard Language** drop-down. 2. (Optional) use the **License Language** drop-down to change the license language. 3. (Optional) use the **Keyboard Language** drop-down to change the keyboard layout. 4. Accept the license agreement.

Page, Dialog, or Option	Do This
Passwords and Time Zone	1. On the configuration page, specify the following information: **IMPORTANT:** Keep a confidential record of the passwords you set for the root and vaadmin users below. **Root password and confirmation:** The root password provides root access to the appliance terminal prompt. Do not access appliances as the root user unless specifically requested by Filr support personnel. **Vaadmin password and confirmation:** The preferred user for accessing the appliance as requested by Filr support personnel. Consider using a different password for each appliance for enhanced security. **NTP Server:** The IP address or DNS name of the reliable external Network Time Protocol (NTP) server for your network. Example: time.example.com. For the best results, set up NTP in accordance with the VMware best practices guidelines (http://kb.vmware.com/selfservice/microsites/search.do?language=en_US&cmd=displayKC&externalId=1006427). **Region:** Your local region. **Time Zone:** The time zone of all file servers that Filr will provide access to. 2. Click **Next**.
Network Settings	1. Specify the following: **Hostname:** The fully qualified DNS host name associated with the appliance's static IP address. Example: myFilr.mynetwork.example.com. **IP Address:** The static IP address for the appliance. Example: 172.17.2.3. **Network Mask:** The network mask associated with the appliance's IP address. Example: 255.255.255.0. **Gateway:** The IP address of the gateway on the subnet where your Filr virtual appliance is located. Example: 172.17.2.254. **IMPORTANT:** Filr appliances do not tolerate latency and should be installed in the same subnet or a near-subnet. **DNS Servers:** The IP address of a primary DNS server for your network. Example: 172.17.1.1. **Domain Search:** The domain that is associated with the Filr host name. 2. Click **Next**.

Page, Dialog, or Option	Do This
Additional LAN Card Configuration	1. (Conditional) If you configured multiple network adapters for this appliance, select from the following options, then click **Next**: ◆ **Do Not Configure:** Select this option to configure this network at a later time as described in "Changing Network Settings" in the *OpenText Filr 23.4: Administrative UI Reference*. ◆ **DHCP Dynamic Address:** Select this option to have an IP address assigned dynamically on the secondary network. ◆ **Statically Assigned IP Address:** Select this option to assign a static IP address on the secondary network. Then specify the IP address, network mask, and host name.
Data Store Location	1. Hard Disk 2 is automatically detected and the disk designation is displayed in the hard drive drop-down. Accept the defaults for the other options on this page by clicking **Next**. **WARNING:** If you have not already created additional disks 2 and 3 for each of your VMs, power off the virtual machine and make sure you have the required disk space in place for your deployment before proceeding. Otherwise, there is a substantial risk that your deployment will not meet your organization's needs.
Data Log Location	1. Hard Disk 3 is automatically detected and the disk designation is displayed in the hard drive drop-down. Accept the defaults for the other options on this page by clicking **Next**.
Shared Storage NFS Location	Referring to the work you did in "Exporting an NFS Directory for the /vashare Mount Point" on page 21, do the following: 1. For the **NFS Server Hostname** field, click **Browse** and select the NFS server that you identified. 2. For the **Remote Directory** field, click **Browse** and select the directory that you exported. 3. Click **Configure**. 4. Go to "Configuring Password, Time, and Network Settings" on page 45.
Shared Storage CIFS Location	Referring to the work you did in "Creating a CIFS Share for the /vashare Mount Point" on page 22, do the following: 1. Type the UNC path to the share that you created. 2. Type the user name of the CIFS user that you identified or created. 3. Type the password of the CIFS user. 4. Click **Configure**.

Page, Dialog, or Option	Do This
Configuring Password, Time, and Network Settings	1. The settings you have specified are configured, storage is verified, and the appliance starts. Continue as indicated for your deployment type: **Expandable Deployment:** Repeat the above steps starting with "2 - Select an appliance." on page 42 until all of your appliances are started, configured, and running. Then go to Chapter 8, "Creating an Expandable Filr Deployment," on page 47. **All-in-one (Small) Deployment:** Return to Appendix B, "All-in-One (Small) Deployment—Creating," on page 161. **Non-expandable Deployment:** Repeat the above steps starting with "2 - Select an appliance." on page 42 until all of your appliances are started, configured, and running. Then return to Appendix C, "Non-Expandable Deployment—Creating," on page 163.

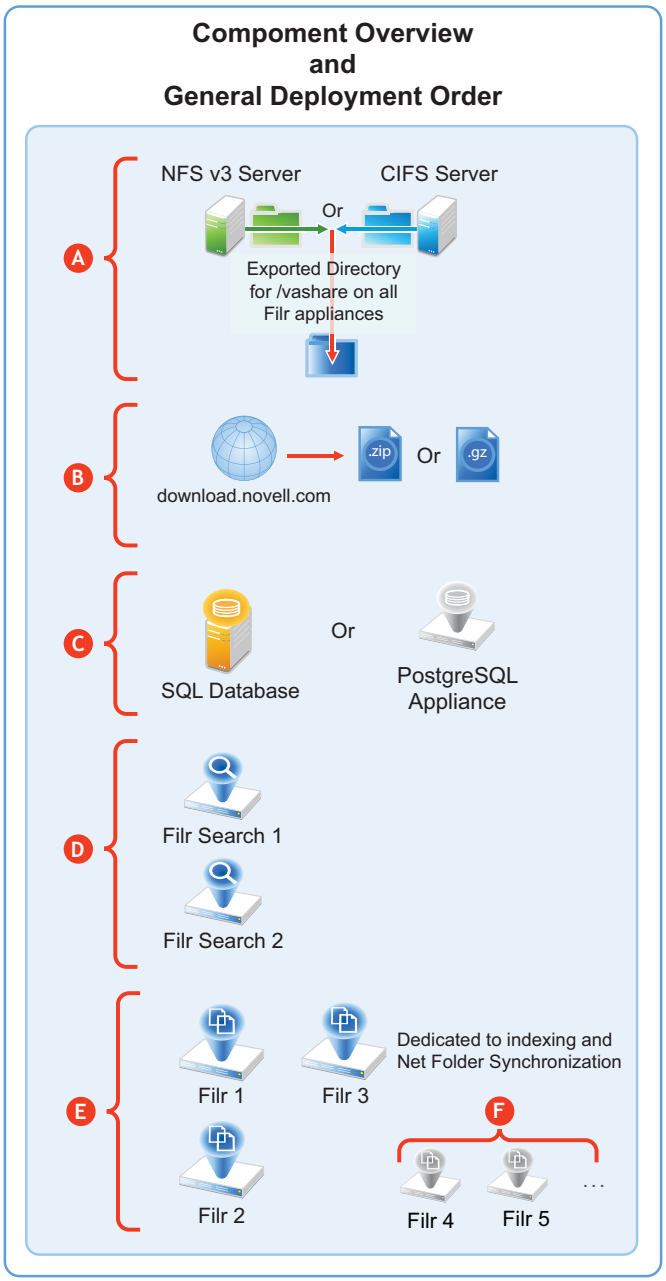
8 Creating an Expandable Filr Deployment

Figure 8-1 illustrates the general order for deploying Filr components. Letters reference brief component/process descriptions in the table that follows.

The first process (shared storage) was completed in Chapter 4, “Setting Up Shared Storage,” on page 21 and illustrated in Figure 4-1 on page 21.

The illustrations that follow are to help you track deployment progress.

Figure 8-1 *Creating an Expandable Deployment*



Letter	Details
A	**Exported NFS Directory or CIFS Share:** All of the Filr appliances in an expandable deployment share this directory, which stores ◆ Mutually accessed configuration files ◆ Personal storage ◆ Temporary files used by upload and conversion processes ◆ HTML renderings

Letter	Details
B	**Filr Software:** You download Filr software that you then deploy as a boot/system disk on your VM host server.
C	**SQL Database:** Each Filr appliance in an expandable deployment accesses the same SQL database. If available, an SQL server should be used, but if that is not an option, the PostgreSQL appliance can be deployed in its place.
D	**Filrsearch Appliances:** OpenText best practices require that each Filr cluster be configured with two Filrsearch appliances.
E	**Filr Appliances:** By definition, a Filr cluster must contain at least two Filr appliances. OpenText recommends three Filr appliances with the third appliance dedicated to Net Folder synchronization and maintaining the search index.
F	**Additional Filr Appliances:** More Filr appliances can be included as the service load increases.

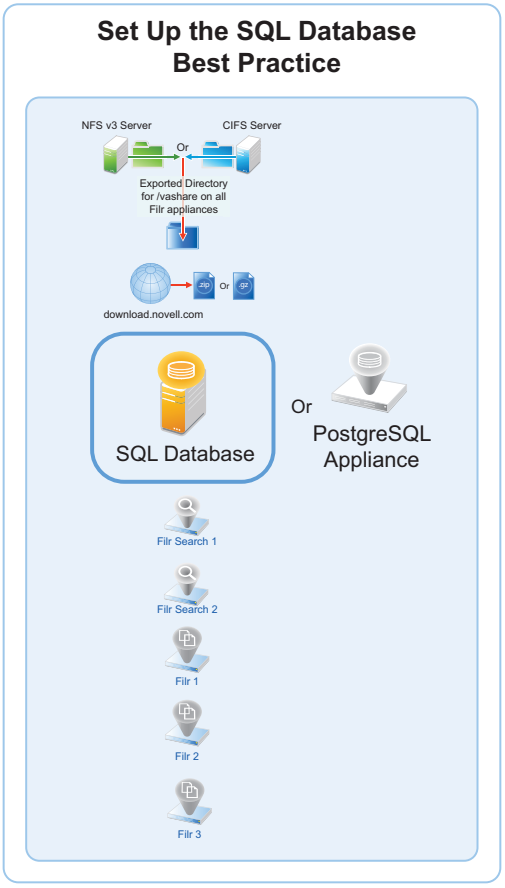
To create an expandable Filr deployment, complete the following sections in the order presented.

- "Setting Up the SQL Database" on page 49
- "Setting Up Two Filr Search Appliances" on page 53
- "Setting Up the Filr Appliances" on page 54
- "Completing the Expandable Filr Deployment" on page 60
- "Dedicating a Filr Appliance to Indexing and Net Folder Synchronization" on page 63
- "Using the Dedicated Filr Appliance to Complete the Indexing Setup" on page 64

Setting Up the SQL Database

Figure 8-3 illustrates that an SQL database is the second component deployed (after shared storage) when creating an expandable Filr deployment.

Figure 8-2 *Set Up an SQL Database*



IMPORTANT: OpenText recommends using an existing SQL database if one is available.

Prepare your in-house SQL server by completing the steps in one of the following sections:

- “Configuring a PostgreSQL Appliance” on page 50
- “Configuring a MySQL or MariaDB Server” on page 51
- “Configuring a Microsoft SQL Server” on page 52

Configuring a PostgreSQL Appliance

- “Deploying a PostgreSQL Appliance” on page 50
- “Creating User Roles for Accessing PostgreSQL Appliance” on page 51
- “Creating Database for Connecting to Filr” on page 51

Deploying a PostgreSQL Appliance

1. Deploy the PostgreSQL Appliance similar to the Filr Appliance. The binary is available on the sld.microfocus.com location.
2. Specify `<postgresqlappliance_IP or hostname>:9443` to access the PostgreSQL Appliance as the vaadmin user.

3 Under **PostgreSQL Appliance Tools**, click **Configure PostgreSQL**.

4 Specify a password for the "`postgres`" user, then click **OK**.

Creating User Roles for Accessing PostgreSQL Appliance

This user is used when connecting Filr to PostgreSQL in 9443 console.

1 Under **PostgreSQL Appliance Tools**, click **phpPgAdmin**.

2 Click **PostgreSQL**, then specify the **Username** as "`postgres`" and password that you specified in Step 4 on page 51.

3 Click **Roles > Create role**.

4 Specify all the required details to create a user. Ensure to select the options: **Create DB?** and **Can login?** and click **Create**.

Creating Database for Connecting to Filr

This database is used to connect to Filr.

1 Click **Databases** > **Create database**.

2 The **Name** should be same as the user you created in Step 4 on page 51.

3 In the **Template** field, select **template0**, then continue with defaults and click **Create**.

4 (Optional) Create one more database, if you want to connect to Filr with a database with a different name than the user.

Configuring a MySQL or MariaDB Server

This section describes configuring MySQL or MariaDB server by using the Filr configuration wizard. It is recommended not to manually create the Filr database on your MySQL or MariaDB server.

The MySQL database mentioned in this section is an existing database and not a Filr default database. From Filr 4, the default database is PostgreSQL.

Table 8-1 *Configuring MySQL or MariaDB for Filr*

File	Do This
	1 - Edit the configuration file.

File	Do This

MySQL or MariaDB server > `/etc/my.cnf` file	1. Edit the file as follows:
	`[client]`
	`default-character-set = utf8`
	`[mysqld]`
	`character-set-server = utf8`
	`max_connections = 900`
	`transaction-isolation = READ-COMMITTED`
	`expire_logs_days = 7`
	The `expire_logs_days` setting is optional, but is recommended because it cleans up `mysql-bin-*` files.
	Unless this is done regularly, the files will consume significant disk space in the `vastorage` directory.
	2. Uncomment the InnoDB tables section.
	3. Increase the buffer pool size to approximately 60 percent of the amount of RAM that has been allocated to the dedicated server.
	For example, a dedicated server with 4 GB of RAM should have a buffer pool size of 2560 MB, as follows:
	`innodb_buffer_pool_size = 2560M`
	4. Identify or create a user account with sufficient rights to create and manage the Filr database.

	Continue with "Setting Up Two Filr Search Appliances" on page 53.

Configuring a Microsoft SQL Server

IMPORTANT: Do not create the Filr database on your MS SQL server manually.

Let the Filr configuration wizard create the database to ensure the correct configuration.

Table 8-2 *Configuring Microsoft SQL Server for Filr*

File	Do This
	1 - Configure the server.
Server management console	1. Enable remote access to the Microsoft SQL database server. 2. Open port 1433 on the Windows firewall where the database server is running. 3. Identify or create a user account that is configured with **SQL Server Authentication** and has sufficient rights to create and manage the Filr database. **IMPORTANT:** Filr supports only **SQL Server Authentication**. Windows Authentication and Windows Domain User Authentication to Microsoft SQL are not supported.

File	Do This

Server management console	1. Run the following queries against the database:
	`ALTER DATABASE database-name SET READ_COMMITTED_SNAPSHOT ON`
	`ALTER DATABASE database-name COLLATE Latin1_General_CI_AS_KS_WS`
	2. Continue with "Setting Up Two Filr Search Appliances" on page 53.

Setting Up Two Filr Search Appliances

Filr best practices require that every expandable deployment have two Filrsearch appliances. There are no advantages to having more than two.

Best practices allow for operating Filr with one search appliance, but only under special circumstances, such as when reindexing is required. One appliance continues to service user requests while the other is focused on rebuilding the search index.

Figure 8-3 shows that two Filr Search appliances are the third and fourth components deployed in an expandable deployment.

Figure 8-3 *Set up Two Filr Search Appliances*

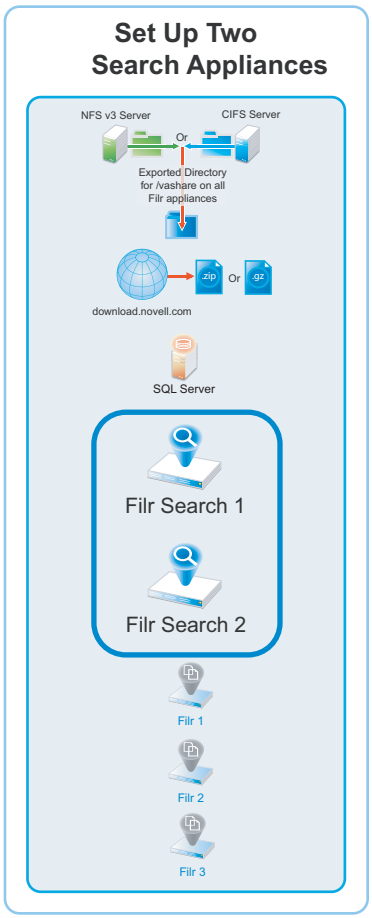


Table 8-3 *Setting Up the Filrsearch Appliances*

Page, Dialog, or Option	Do This
	1. Open a management browser on your administrative workstation and access the Port 9443 Administration Utility on the first Filrsearch appliance using the following URL: `https://filrsearch_IP_Address:9443` Where *IP_Address* is the IP address of the first Filrsearch appliance.
Filr Search Appliance Sign In	1. Log in as the `vaadmin` user with the password that you set for the appliance in "Vaadmin password and confirmation:" on page 43.
Filr Search Tools	1. Click the **Configuration** button  to launch the **Filr Search Configuration Wizard**.
Filr Search Configuration Wizard	1. Click **Next**. 2. Type and confirm a password for the Lucene Service User (use the same password for both appliances). Make a note of the password for later. 3. Click **Finish**.
Search Settings	1. Scroll down and click **Submit > OK**.
	1. Repeat the steps in this table for the second Filrsearch appliance, then close the browser. 2. Continue with "Setting Up the Filr Appliances" on page 54

Setting Up the Filr Appliances

Figure 8-4 illustrates that the Filr appliances are deployed after all other components are in place.

Figure 8-4 *The Filr Appliances Are Set Up Last*

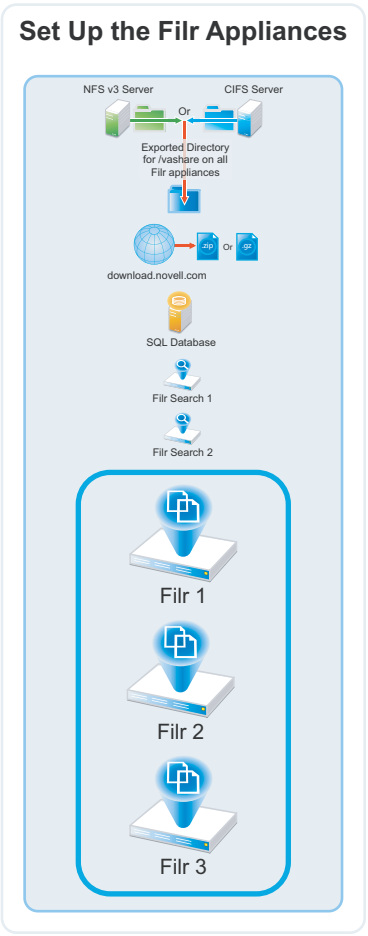


Table 8-4 *Logging in and Starting the Configuration Wizard*

Page, Dialog, or Option	Do This
	1. Open a management browser on your administrative workstation and access the Port 9443 Administration Utility on the first Filr appliance using the following URL: `https://filr_IP_Address:9443` Where *IP_Address* is the IP address of the first Filr appliance.
Filr Appliance Sign In	1. Log in as the `vaadmin` user with the password that you set for the appliance in "Vaadmin password and confirmation:" on page 43.
Filr Appliance Tools	1. Click the Configuration icon  to launch the **Filr Configuration Wizard**.
Filr Configuration Wizard	1. **Large Deployment** is automatically selected. Click **Next**.

Figure 8-5 *Each Filr Appliance Needs the Database Connection Information*

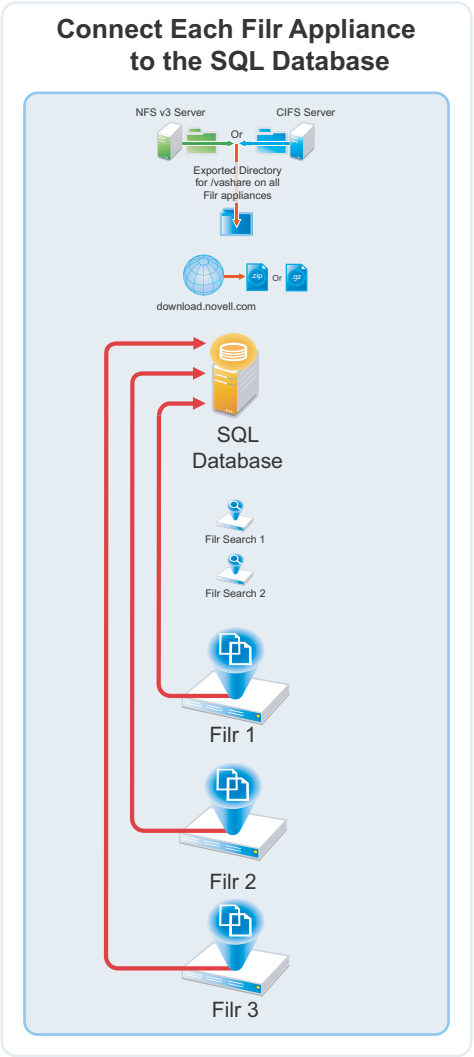


Table 8-5 *Configuring each Filr to connect to the SQL Database*

Page, Dialog, or Option	Do This
Database	1. Specify the following configuration options for the database: **Database Type:** Select the type of database that you prepared in "Setting Up the SQL Database" on page 49. **Host Name:** The host name or IP address of the database server. **Port:** The wizard selects the standard port for the database type. If your server communicates using a non-standard port, adjust the number accordingly **Database Name:** The name of the database you want the wizard to create (first appliance) and then connect to (subsequent appliances). **User Name:** The administrative user name you identified in "Setting Up the SQL Database" on page 49. **Password:** The administrative user's password. 2. Click **Next**.

Figure 8-6 *Initially, Each Filr Appliance Is Configured to Work with One Filr Search Appliance*

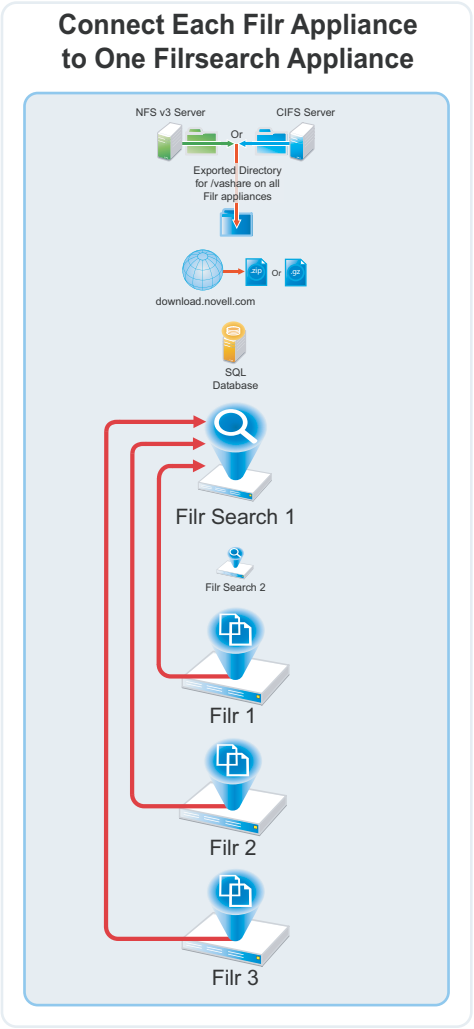


Table 8-6 *Specify the First Search Appliance, Locale, and Admin user*

Page, Dialog, or Option	Do This
Search Appliance	1. Specify the first Filrsearch appliance's DNS name and Lucene password, then click **Finish**. **IMPORTANT:** If you specify the IP address, it must be resolvable to the DNS hostname of the search appliance. 2. Click **Next**.
Default Locale	1. Select a **Default Locale**. 2. If desired, specify a name other than `admin` for appliance administration on port 8443. 3. Click **Finish**. **IMPORTANT:** Wait for the appliance to start before closing the tab or navigating away from the page. 4. When the "Congratulations!" message displays, return to Table 8-4 and deploy the next Filr appliance. 5. After all of the Filr appliances are deployed, continue with "Completing the Expandable Filr Deployment."

Completing the Expandable Filr Deployment

Figure 8-7 *When One Filr Appliance Is Configured for "Filr Clustering," All of Them Are*

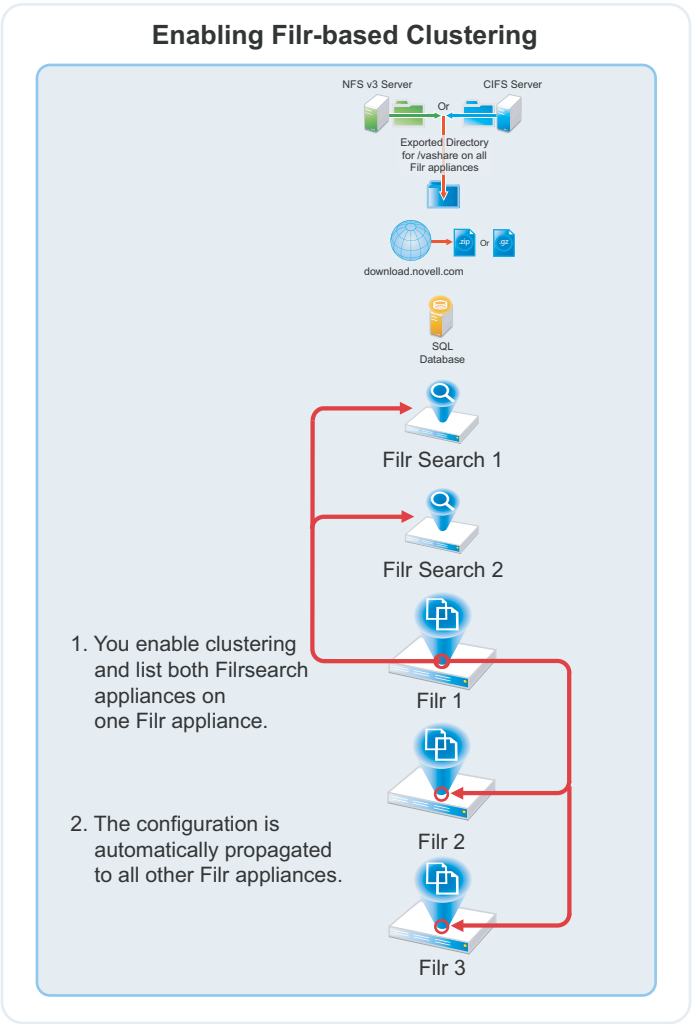


Table 8-7 *Enabling Filr-based Clustering*

Page, Dialog, or Option	Do This
Configuration Summary	1. In the Configuration panel, click **Clustering**.
Clustering	1. Select **Enable Clustered Environment**. 2. The **JVM Route** field is used only if you are setting up Apache load balancing, and is used to uniquely identify this appliance. In many cases, the hostname (automatically supplied) will suffice, but you can customize it if needed. 3. In the **Server Address** field, make sure that both Filrsearch appliances in your deployment are listed. Separate the appliances with a space. Use either IP addresses or fully-qualified hostnames to identify the appliances. 4. Click **OK**. 5. Click **Reconfigure Filr Server**. The Filr appliance is reconfigured and restarted. Subsequently, the configuration is shared by each Filr appliance through the `/vashare` mount point.

Figure 8-8 *The Filr Appliances Are Individually Configured to Use Both Filrsearch Appliances*

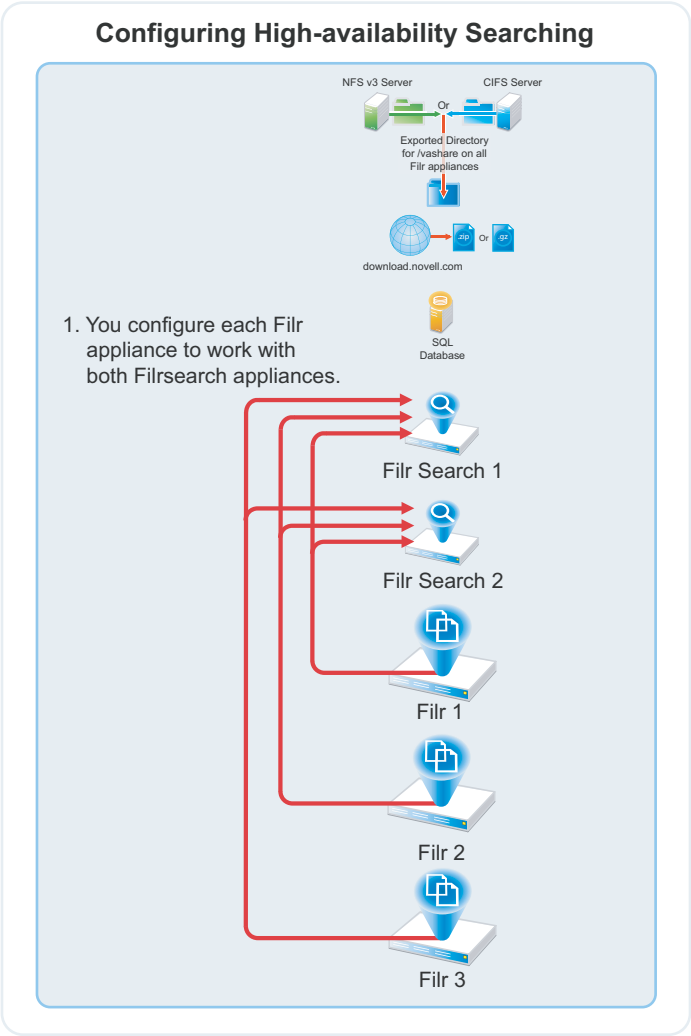


Table 8-8 *Configuring High-availability Searching*

Page, Dialog, or Option	Do This
Configuration Summary	1. In the Configuration panel, click **Search Appliance**.
Search Appliance	1. Click the **Configuration Type** drop-down list and select **High Availability**. 2. Type the Lucene service password that you set in Table 8-3 on page 54. 3. Notice that the Filrsearch appliance you configured for this Filr appliance is listed under Name. Click **Add**.
New Search Node	1. In the **Name:** field, type an arbitrary name for the second appliance. 2. In the **Host Name:** field, type the DNS host name of the other Filrsearch appliance. 3. Click **OK**.
Search Appliance	1. Click **OK**.

Page, Dialog, or Option	Do This
Configuration	1. Click **Reconfigure Filr Server**. The appliance is reconfigured and restarted. However, in contrast with the process in Table 8-7, the Search Appliance configuration is not propagated to the other Filr appliances. 2. In the upper-right corner, click **Log out**.
	1. Log in to the next Filr appliance and repeat the steps in this table. 2. When all of the Filr appliances have been configured for high-availability searching, continue with Dedicating a Filr Appliance to Indexing and Net Folder Synchronization.

Dedicating a Filr Appliance to Indexing and Net Folder Synchronization

As a best practice, OpenText recommends dedicating one Filr appliance to Indexing and Net Folder Synchronization, which are very resource-intensive tasks.

Do the following:

- **Allow Net Folder Synchronization on only the dedicated appliance:** Disable Net Folder Synchronization on all other Filr appliances as follows:
  1. Access the Port 9443 administration console.
  2. Click **Net Folders**.
  3. De-select **Allow Synchronization**.
  4. Repeat on all other Filr appliances except the one you are dedicating to Net Folder Synchronization.

     Now when a Full synchronization occurs (either as a result of a scheduled or manual synchronization), the Filr appliance that you set aside is the one that handles the load.

  NOTE: Just-in-time synchronization (JITS) is unaffected and takes place on whichever Filr appliance receives the user request that triggers JITS.

- **Use Load Balancing to isolate the dedicated appliance from user requests:** When you set up load balancing, don't include the dedicated Filr appliance in the round-robin rotation.
- **Rebuild the search index using the dedicated appliance:** Follow the steps in the next section.

  Thereafter, the dedicated appliance will handle all of the re-indexing workload.

Using the Dedicated Filr Appliance to Complete the Indexing Setup

Table 8-9 *Index with the Dedicated Appliance*

Page, Dialog, or Option	Do This
	1. Open a management browser on your administrative workstation and access the Port 8443 Administration Utility on the *Dedicated Filr Appliance* using the following URL: `https://dedicated_filr_IP_Address:8443` Where *IP_Address* is the IP address of the dedicated Filr appliance.
Filr Sign In Dialog	1. Log in as user `admin` with password `admin`, or with the alternate administrator name/password if you specified one for this appliance in Table 8-6 on page 59. 2. When prompted, change the user password.
Product Improvement (first login only)	1. Click **OK**.
Filr Main Window (Web access)	1. Click the Admin user name in the upper-right corner. 2. Select **Administration Console**.
Administration Console	1. Click **Index** in the left frame.

Page, Dialog, or Option	Do This
Search Index	**IMPORTANT:** If you have users across multiple zones, ensure to perform reindexing on every zone. 1. Take the first search index node out of service to rebuild it while the other is still running. Set this node as "**Write Only**". For information about how to take a node out of service, see Maintaining Your High Availability Lucene Index in the OpenText Filr 23.4: Maintenance Best Practices Guide. 2. Select **Re-Index Everything** in the **Search Index** section of the Administration Console. 3. After the first search index node is rebuilt, put it back into service. Set the node as "**Read and Write**". For information about how to take a node out of service, see Maintaining Your High Availability Lucene Index in the OpenText Filr 23.4: Maintenance Best Practices Guide. 4. Repeat Step 1 to Step 3 for any additional search index node. To view when indexing is complete, keep the **Search Index** dialog box open to see the status. Alternatively, a message is displayed in either of the appserver.log files stating that reindexing is complete. 5. To ensure that the rebuild was successful, verify that the following messages appear in the appserver.log file: `Completed indexing of tree with xxx binders. Time taken for indexing is xxx.xxx msAdministrative reindexing completed on binders [1]` For information about how to access the appserver.log file, see Accessing Filr System Log Files in the OpenText Filr 23.4: Administrative UI Reference.
Indexing has finished!	1. Click **Close**.
Administration Console	1. Click **Nodes** in the left frame.
Search Nodes	1. Change the **User Mode Access** option for the second Filrsearch appliance to **Read and Write**. 2. Click **Apply > Close**. The dedicated Filr appliance will now handle all of the re-indexing workload.

9 Content Editor

The Content Editor (CE) Appliance enables collaborative editing for Filr users. The functionalities are:

- Available with Filr Advanced Edition.
- Available with the Filr Web UI, desktop clients and mobile.
- Multiple files (around 100 files) can be concurrently edited by multiple users.
- Supports collaborative edits for all major file types such as Microsoft and LibreOffice. documents, spreadsheet, and and similar formats.
- Files are edited online and no native application is required to edit the files. There is no need to move or download the files.
- Policies to block copy, print, and download of the content.
- Available for all files under My Files, Shared With Me, Shared By Me, and Net Folder areas.

A separate appliance is required as collaborative editing is a resource intensive task.

- "Content Editor Requirements" on page 67
- "Downloading and Installing Content Editor" on page 69
- "Starting and Configuring the Content Editor Appliance" on page 77
- "Configuring Content Editor Options in Filr Appliance" on page 80
- "Content Editor With NetIQ Access Manager For Online Edit Feature" on page 81
- "Load Balancing" on page 87
- "Upgrading from Content Editor 1.2.3 to 2.0" on page 89

Content Editor Requirements

- "System Requirements" on page 67
- "Other Requirements" on page 68
- "Virtualization Hypervisor Platform Support" on page 68

System Requirements

- CPU: 4
- RAM: 16 GB
- IP address details for the appliance:
  - Static IP address
  - Network mask
  - Gateway IP address

    - Host name associated with the IP address
    - IP address of a DNS server
- NTP server - IP address or host name
- Primary Hard Disk: 20 GB
- Hard Disk 1: 20 GB (minimum)
- Hard Disk 2: 20 GB (minimum)

Other Requirements

- A valid CA certificate is required on the Content Editor Appliance and Filr Appliance for this feature to work with all the Filr clients.

Virtualization Hypervisor Platform Support

Table 9-1 *Virtualization Hypervisor Platform*

Hypervisor Type	Supported Versions

VMware	• One of the following VMware host servers for hosting the appliance VMs.
	  ◦ ESXi 7.0
	  ◦ ESXi 6.7 with the latest update
	For the most up-to-date compatibility matrix of supported VMware host servers, see the *VMware Compatibility Guide* (http://www.vmware.com/resources/compatibility/search.php?deviceCategory=software&testConfig=16) provided by VMware.
	• VMware vMotion is supported when running Content Editor on VMware ESXi

Hyper-V	• The following platforms
	  ◦ Windows Server 2016
	  ◦ Windows Server 2012 R2
	• Hyper-V Manager to deploy, set up, and configure the appliances.

Xen	**IMPORTANT:** Apply all Xen and kernel patches before installing. • The server with the Xen packages installed and the Xen bootloader running by default. ◦ SLES 15 SP4 • Virtual Machine Manager to deploy, set up, and configure the appliances.
Citrix Xen	• Citrix XenServer 7.6 • Citrix XenServer 7.0 • Citrix XenCenter to deploy, set up, and configure the appliances.

Downloading and Installing Content Editor

- "VMWare" on page 69
- "Hyper-V" on page 70
- "Xen" on page 73
- "Citrix Xen" on page 75

VMWare

After making sure you have the necessary system requirements in place, you are ready to download and prepare the CE software that applies to your virtualization platform.

	1 - Downloading Content Editor Software 1. Download the Content Editor software (`ContentEditor.x86_64.2022-09-13.53.ova`.zip) from the Micro Focus Customer Center or from the trial download page. The key and zip files will be available under the Filr 23.4 Advanced Edition. 2. Extract the `.ova.zip` file on your management workstation.
	2 - Launching the Web browser, naming the VM, and choosing the datastore.
Web Browser	1. On a Web browser, enter the URL for the VMware server and login with the root credentials. 2. Right-click on the **Virtual Machines** and click **Create/register VM**.
Select creation type	Select **Deploy a virtual machine from an OVF or OVA** file, then click **Next**.
Select OVF and VMDK files	Specify the name for the virtual machine. For example, Demo-VM. Upload the ovf and vmdk files of Content Editor, and click **Next**.
Select Storage	Select a storage repository where the disk images for the imported VMs will be placed. Review the datastore details, and select an appropriate disk format from the available options. Retain all the other default settings, and click **Next**.
Deployment options	Do not select **Power on automatically** (so that the VM can be powered on after adding the disks), and click **Next**.
Ready to complete	Review the screen and click **Finish** to successfully deploy the Content Editor Appliance. The boot disk is created and the appliance is deployed.
	3 - Editing the VM settings. Right-click the VM you just deployed and select **Edit Settings**. The Virtual Machine Properties dialog displays.
Virtual Machine Properties	Content Editor VMware VMs ship with **Memory** and **CPU** settings that are appliance-type appropriate in most circumstances. You can adjust them at this point if desired, or you can adjust them later if required for performance tuning purposes.

	4 - Adding and configuring disk 2 (/vastorage) and disk 3 (/var)
Virtual Hardware	1. Click **Add hard disk** > **New standard hard disk**. This adds second hard disk. 2. Click **Add hard disk** > **New standard hard disk.** This adds the third hard disk. Click **Save** to successfully add the hard disks. On successful deploying the appliance, continue with "Starting and Configuring the Content Editor Appliance" on page 77.

Hyper-V

After making sure you have the necessary system requirements in place, you are ready to download and prepare the CE software that applies to your virtualization platform.

Page, Dialog, or Option	Do This
	1 - Downloading Content Editor Software.
Hyper-V Host Server	1. Download the Content Editor software (`ContentEditor.x86_64-1.0.0.40.vhdx.zip`) from the Micro Focus Customer Center or from the trial download page. The key and zip files will be available under the Filr 23.4 Advanced Edition. 2. Extract `*.vhdx.zip` file on your management workstation.
	2 - Create a new VM.
Hyper-V Manager	1. Log in to the Hyper-V host server either locally or from a remote workstation using Remote Desktop. 2. In the left pane, right-click the server where you have planned to create the new virtual machine, then click **New** > **Virtual Machine**. The New Virtual Machine Wizard displays. 3. Click **Next**.
Specify Name and Location	1. Specify the appliance name. 2. Click **Next**.
Specify Generation	1. Ensure that **Generation 1** is selected. 2. Click **Next**.
	3 - Specify memory
Assign Memory	1. In the **Startup RAM** field, specify the amount of memory (in MB) that you have planned for this VM. 2. Click **Next**.
	5 - Assign network adapter
Configure Networking	1. On the Configure Networking page, select the networking card for this VM. 2. Click **Next**.

Page, Dialog, or Option	Do This
	6 - Identify the system disk
Connect Virtual Hard Disk	1. Select **Use an existing virtual hard disk**. 2. Browse to and select the `ContentEditor.x86_64-1.0.0.*.vhdx` file of this appliance. 3. Click **Open**. 4. Click **Next**.
Summary	1. Click **Finish**. The VM is created and appears in the list of Virtual Machines.
	7 - Specify processors
Hyper-V Manager	1. In Hyper-V Manager, right-click the VM that you just created. 2. Click **Settings**.
Processor	1. Click **Processor**. 2. In the **Number of virtual processors** field, specify the number of processors. 3. Click **Next**.
	8 - Add hard disk 2 (/vastorage).
Settings for *VM* on *Host Server*	1. Under **Hardware,** select **IDE Controller** *. 2. Click **Hard Drive**. 3. Click **Add**. A Hard Drive entry is added below the controller.
Hard Drive	1. Under **Media,** select **Virtual hard disk**. 2. Click **New**.
New Virtual Hard Disk Wizard	1. Click **Next**.
Choose Disk Format	1. Select **VHDX**. 2. Click **Next**.
Choose Disk Type	1. On the Choose Disk Type page, select **Fixed size**. 2. Click **Next**.
Specify Name and Location	1. Specify the following: ◆ **Name:** A descriptive name for the virtual disk. For example, `CE-Disk-2`. ◆ **Location:** Specify the location where you want the virtual disk to be located. 2. Click **Next.**
Configure Disk	1. Select **Create a new blank virtual hard disk**. 2. **Size:** Specify the size for Disk 2 on this appliance. 3. Click **Next.**

Page, Dialog, or Option	Do This
Summary	1. Review the summary information. 2. Click **Finish**
	9 - Add hard disk 3 (/var).
Hyper-V Manager	1. In Hyper-V Manager, right-click the VM that you just created. 2. Click **Settings**.
Settings for *VM* on *Host Server*	1. Under **Hardware,** select **IDE Controller** * or SCSI Controller. **NOTE:** Ensure that the SCSI controller number is unique for every hard disk. 2. Click **HardDrive**. 3. Click **Add**. A Hard Drive entry is added below the controller.
Hard Drive	1. Under **Media,** select **Virtual hard disk**. 2. Click **New**.
New Virtual Hard Disk Wizard	1. Click **Next**.
Choose Disk Format	1. Select **VHDX**. 2. Click **Next**.
Choose Disk Type	1. On the Choose Disk Type page, select **Fixed size** 2. Click **Next**.
Specify Name and Location	1. Specify the following: ◆ **Name:** A descriptive name for the virtual disk. For example, `CE-Disk-3`. ◆ **Location:** Specify the location where you want the virtual disk to be located. 2. Click **Next.**
Configure Disk	1. Select **Create a new blank virtual hard disk**. 2. **Size:** Specify the amount for disk 3 on this appliance. 3. Click **Next.**
Summary	1. Review the summary information. 2. Click **Finish > OK**

Page, Dialog, or Option	Do This
	10 - (Optional) Add a Network Adapter You can add a network adapter if your Content Editor deployment accesses a separate network for one or more of the following reasons: ◆ Appliance administration. ◆ NFS mount or CIFS access to the /vashare mount point. ◆ Security of Memcached. **IMPORTANT:** Bonding or teaming NICs is not supported with Content Editor.
Hyper-V Manager	1. In Hyper-V Manager, right-click the virtual machine for which you want to create an additional NIC, then click **Settings**.
Settings for *VM* on *Host Server*	1. Under **Hardware,** select **Add Hardware**.
Add Hardware	1. Click **Network Adapter**. 2. Click **Add**. A Network Adapter entry is added to the hardware list.
Network Adapter	1. Under **Virtual Switch**, select the secondary network associated with the Content Editor installation. 2. Specify any other required settings for the new network adapter. 3. Click **OK**. On successful deploying the appliance, continue with "Starting and Configuring the Content Editor Appliance" on page 77.

Xen

After making sure you have the necessary system requirements in place, you are ready to download and prepare the CE software that applies to your virtualization platform.

Page, Dialog, or Option	Do This
	1 - Downloading the Content Editor Software 1. Download the Content Editor software (`ContentEditor.x86_64-1.0.0.40.xen.zip`) from the Micro Focus Customer Center or from the trial download page. The key and zip files will be available under the Filr 23.4 Advanced Edition. 2. Extract `.xen.zip` file in the directory where you downloaded it. **3 - Launch the installer.**

Page, Dialog, or Option	Do This
Terminal prompt on Xen VM Host Server	1. Run the following command to launch the GUI configuration menu: `virt-manager` **NOTE:** The `vm-install` command is deprecated from SLES 12 releases.
Create a new virtual machine	1. Click **File** > **New Virtual Machine**. The **Create a new virtual machine** wizard is displayed. 2. Select **Import existing disk image**. 3. Click **Forward**.
Storage path and Operating System	1. Browse and select the existing disk image. 2. Select **SUSE Linux Enterprise Server 12 SP4**. 3. Click **Forward**.
Choose Memory and CPU settings	1. Set the amount of memory (in MB) to match that of the VM you are upgrading. 2. Specify the **CPUs** to match the number of the VM you are upgrading. 3. Click **Forward**.
	4 - Name the VM.
Name of Virtual Machine	1. Specify the name of the appliance. 2. Select **Customize configuration before install**. 3. Click **Finish**.
	5 - Configure Disk 2 (/vastorage)
Hardware	1. Click **Add Hardware** at the bottom left of the screen. 2. Select the option **Select or create custom storage**. 3. Navigate to the contents of the folder for the appliance you are creating. 4. Select the `.qcow2` file. 5. Click **Open** > **Finish**.
	6 - Configure Disk 3 (/var)
	1. Click **Add Hardware** at the bottom left of the screen. 2. Select the option **Select or create custom storage**. 3. Navigate to the contents of the folder for the appliance you are creating. 4. Select the `.qcow2` file. 5. Click **Open** > **Finish**.

Page, Dialog, or Option	Do This
	7 - (Optional) Add a Network Adapter You can add a network adapter if your Content Editor deployment accesses a separate network for one or more of the following reasons: ◆ Appliance administration. ◆ NFS mount or CIFS access to the /vashare mount point. ◆ Security of Memcached. **IMPORTANT:** Bonding or teaming NICs is not supported with Content Editor.
Summary	1. Click **Network Adapters**.
Network Adapters	1. Click **New**.
Virtual Network Adapter	1. Specify the settings for the adapter. 2. Click **Apply**.
Network Adapters	1. Click **Apply**.
Summary	On successful deploying the appliance, continue with "Starting and Configuring the Content Editor Appliance" on page 77.

Citrix Xen

After making sure you have the necessary system requirements in place, you are ready to download and prepare the CE software that applies to your virtualization platform.

Page, Dialog, or Option	Do This
	1 - Identify the appliance to deploy. 1. On a workstation with Citrix XenCenter installed, download the Content Editor software (`ContentEditor.x86_64-0.0.40.xva.zip`) from the Micro Focus Customer Center. The key and zip files will be available under the Filr 23.4 Advanced Edition. 2. Extract `.xva.zip` file in the directory where you downloaded it.
	2 - Launch XenCenter.
Management Workstation	1. Start XenCenter.
XenCenter	1. Connect to the Citrix XenServer where you have planned to deploy Content Editor. 2. Right-click the server and select **Import**.
	3 - Import the system disk

Page, Dialog, or Option	Do This
Locate the File you want to import	1. Browse to and select the `.xva` file on your management workstation for the appliance type that you are deploying. 2. Click **Open**. 3. Click **Next**.
Select the location where the imported VM will be placed	1. Select the XenServer. 2. Click **Next**.
Select target storage	1. Select the storage repository for the VM. 2. Click **Import**.
	4 - Select the network adapter
Select network to connect VM	1. Select the virtual network adapter. 2. Click **Next**.
Review the import settings	1. Deselect **Start VM(s) after import**. 2. Click **Finish**. **IMPORTANT:** Depending on network latency and other factors, it can take a while to import the system disk.
	5 - Specify Memory
	1. If you need to adjust the memory, select the newly created VM in the left pane. 2. Click the **Memory** tab. 3. Click **Edit**, change the setting, and click **OK**.
	6 - Specify Processors
	1. If you need to adjust the CPUs, right-click the newly created VM in the left pane. 2. Select **Properties**. 3. Click **CPU**, change the setting, and click **OK**.
	7 - Add Disk 2 (/vastorage)
	1. With the newly created VM selected in the left pane, click the **Storage** tab.
Virtual Disks	1. Click **Add...**.
Add Virtual Disk	1. Type a disk name that reflects the appliance name and that this is disk 2. For example, CE-1-disk-2. 2. Specify the **Size**. 3. Click **Add**.
	8 - Add Disk 3 (/var)
Virtual Disks	1. Click **Add...**.

Page, Dialog, or Option	Do This
Add Virtual Disk	1. Type a disk name that reflects the appliance name and that this is disk 3. For example, CE-1-disk-3. 2. Specify the **Size**. 3. Click **Add**. **9 - (Optional) Add a Network Adapter** You can add a network adapter if your Content Editor deployment accesses a separate network for one or more of the following reasons: ◆ Appliance administration. ◆ NFS mount or CIFS access to the /vashare mount point. ◆ Security of Memcached. **IMPORTANT:** Bonding or teaming NICs is not supported with Content Editor. 1. With the newly created VM selected in the left pane, click the **Networking** tab. 2. Select the secondary network associated with the Content Editor installation.
XenCenter	On successful deploying the appliance, continue with "Starting and Configuring the Content Editor Appliance" on page 77.

Starting and Configuring the Content Editor Appliance

Table 9-2 *Starting and Configuring the Appliances*

Page, Dialog, or Option	Do This
	1 - Start the appliance. 1. After you have configured your appliance, you must start and configure each appliance in turn. ◆ **VMware:** In VmWare, power on the first appliance, then click the **Console** tab. ◆ **Hyper-V:** In Hyper-V Manager, right-click the VM and select **Start**. ◆ **Citrix Xen:** In XenCenter, right-click the appliance and select **Start**. **2 - Accept the license and specify the keyboard layout.** 1. After the appliance boots, the License Agreement screen displays.
License Agreement	1. Select your preferred keyboard layout in the **Keyboard Language** drop-down. 2. (Optional) use the **License Language** drop-down to change the license language. 3. (Optional) use the **Keyboard Language** drop-down to change the keyboard layout. 4. Accept the license agreement. **3 - Setting Password and Network Details**

Page, Dialog, or Option	Do This
Passwords and Time Zone	1. On the configuration page, specify the following information: **IMPORTANT:** Keep a confidential record of the passwords you set for the root and vaadmin users below. **Root password and confirmation:** The root password provides root access to the appliance terminal prompt. Do not access appliances as the root user unless specifically requested by Filr support personnel. **Vaadmin password and confirmation:** The preferred user for accessing the appliance as requested by Filr support personnel. Consider using a different password for each appliance for enhanced security. **NTP Server:** The IP address or DNS name of the reliable external Network Time Protocol (NTP) server for your network. Example: time.example.com. For the best results, set up NTP in accordance with the VMware best practices guidelines (http://kb.vmware.com/selfservice/microsites/search.do?language=en_US&cmd=displayKC&externalId=1006427). **Region:** Your local region. **Time Zone:** The time zone of all file servers that Filr will provide access to. 2. Click **Next**.
Network Settings	1. Specify the following: **Hostname:** The fully qualified DNS host name associated with the appliance's static IP address. Example: myFilr.mynetwork.example.com. **IP Address:** The static IP address for the appliance. Example: 172.17.2.3. **Network Mask:** The network mask associated with the appliance's IP address. Example: 255.255.255.0. **Gateway:** The IP address of the gateway on the subnet where your Filr virtual appliance is located. Example: 172.17.2.254. **IMPORTANT:** Content Editor appliance does not tolerate latency and should be installed in the same subnet or a near-subnet. **DNS Servers:** The IP address of a primary DNS server for your network. Example: 172.17.1.1. **Domain Search:** The domain that is associated with the Filr host name. 2. Click **Next**.

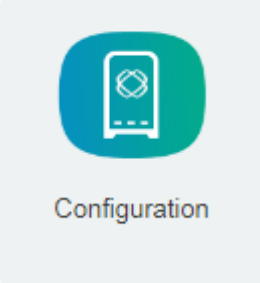
Page, Dialog, or Option	Do This
Data Store Location	1. Hard Disk 2 is automatically detected and the disk designation is displayed in the hard drive drop-down. Accept the defaults for the other options on this page by clicking **Next**. **WARNING:** If you have not already created additional disks 2 and 3 for each of your VMs, power off the virtual machine and make sure you have the required disk space in place for your deployment before proceeding. Otherwise, there is a substantial risk that your deployment will not meet your organization's needs.
Data Store Location	1. Hard Disk 3 is automatically detected and the disk designation is displayed in the hard drive drop-down. Accept the defaults for the other options on this page by clicking **Next**.
Configuring Password, Time, and Network Settings	1. The settings you have specified are configured, storage is verified, and the appliance starts.

Configuring Content Editor Appliance

Specify the vaadmin or root user password to manage virtual-machine-level settings and Content Editor service configuration.

Path: https://content_editor_appliance_ip_or_dns:9443

After installing a Content Editor appliance, configure it with the DNS hostnames of each Filr appliance that you want to be able to connect to it.



Path: Port 9443 Appliance Console > Content Editor Appliance Tools > Configuration icon

Table 9-3 *Allowed Hosts Dialog*

Field, Option, or Button	Information and/or Action
Allowed Hosts	1. To allow Filr appliances to access the appliance's editing services, type their DNS hostnames, one per line. 2. Click Submit. The hosts you enter are listed in the left panel.
Submit button	Click this to add the typed DNS hostnames to the list of allowed hosts.
Cancel button	Click this to cancel any changes and return to the Home panel.

Configuring Content Editor Options in Filr Appliance

Path: Port 8443 Filr Administration Console **> System > Content Editor**

Before you configure the Content Editor options, you must do the following:

- Deploy a Content Editor appliance.
- Configure the Content Editor appliance with the DNS hostnames of each Filr appliance that you want to be able to connect to it.

Table 9-4 *Using the Content Editor Configuration dialog*

Field, Option, or Button	Information and/or Action
Enable Content Editor	1. Select this to enable collaborative editing for Filr users. 2. Specify the configuration information for the following fields.
◆ **Server URL**	◆ The access URL (IP address or DNS hostnames of the Content Editor appliance.
◆ **Test connection**	◆ Click this to test the connection between Filr and the Content Editor appliance.
Content Editor Policies:	◆ Set the policies that will be applicable to the user when performing collaborative edit. ◆ When a user is editing the file and if changes are made to the policy, then the file has to be reloaded for the changes to take effect.
◆ **Disable copy**	◆ Content from the document cannot be copied to any other document.
◆ **Disable print and download**	◆ The file getting edited cannot be printed or downloaded to your local workstation.

Field, Option, or Button	Information and/or Action
◆ **Disable Watermark**	◆ By default, this option is enabled. When this option is enabled, watermark is displayed across the document. Email id or name of the user is displayed as watermark. The watermark is also displayed on printing the document. **NOTE:** This option is available with CE 1.0.1 version onwards.

Now the Collaborative Editing functionality is ready to use on all Filr Clients and Web UI.

Content Editor With NetIQ Access Manager For Online Edit Feature

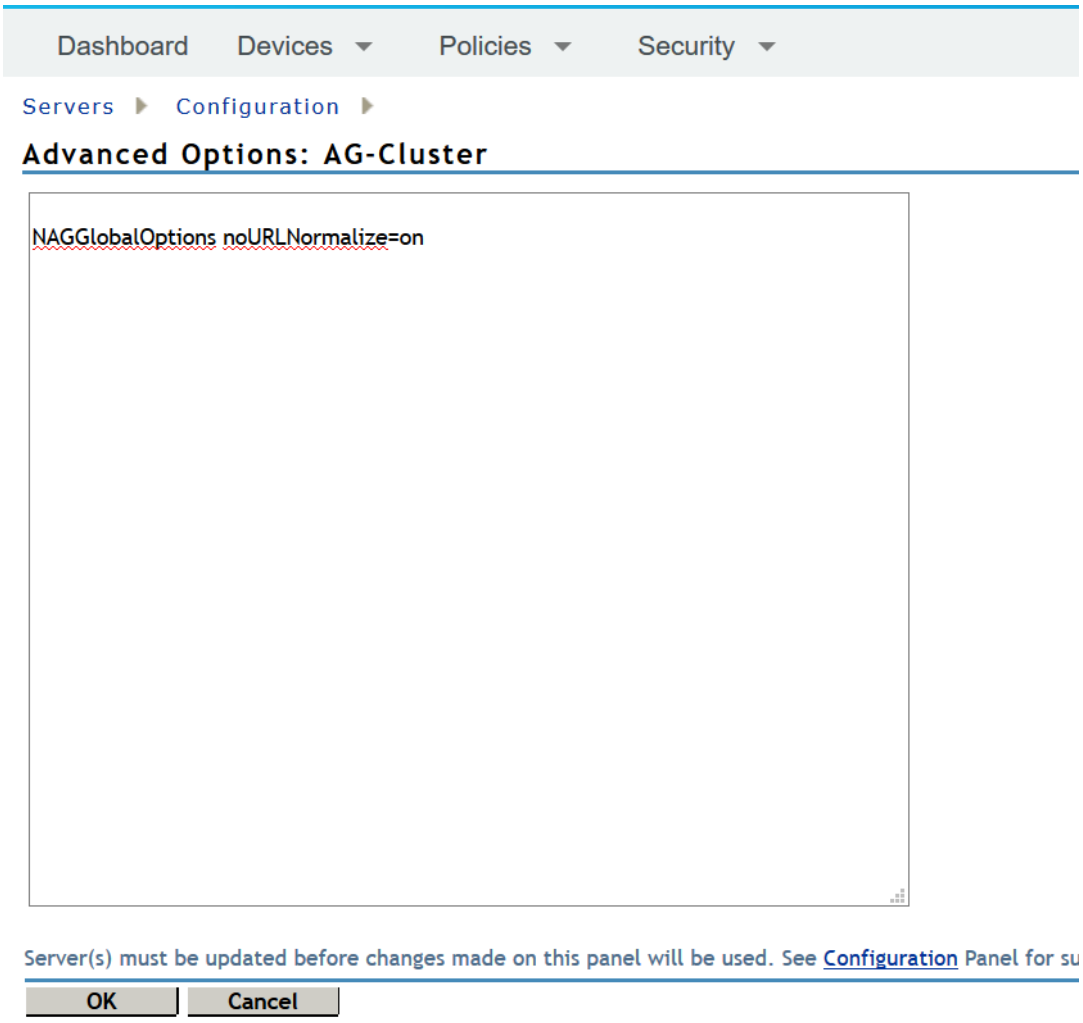
- "Configuring NetIQ Access Manager With Content Editor" on page 81
- "Allowing Filr to Connect to Content Editor" on page 86
- "Allowing Content Editor to Connect to the Filr" on page 87
- "Using the Online Edit Feature" on page 87

You can configure NetIQ Access Manager (NAM) to act as Reverse Proxy service for CE site when using the **Online-Edit** option. This helps you provide the ease of single sign-on and establish a trusted relationship with the Access Gateway. Using CE in conjunction with NetIQ Access Manager adds enterprise-level security to your Filr system.

When a user performs Online Edit on a file, the Online Edit session (Filr) communicates to CE Via NAM.

Configuring NetIQ Access Manager With Content Editor

1. Log in to the NAM Administration Console.
2. Click **Devices** > **Access Gateways** > **AG-Cluster.**
   - **2a** Under **Content Settings**, click **Advanced Options**.
   - **2b** In the **Advanced Options** window, add `NAGGlobalOptions noURLNormalize=on`.



Add this option to ensure that CE works with NAM.

2c Click **OK**.

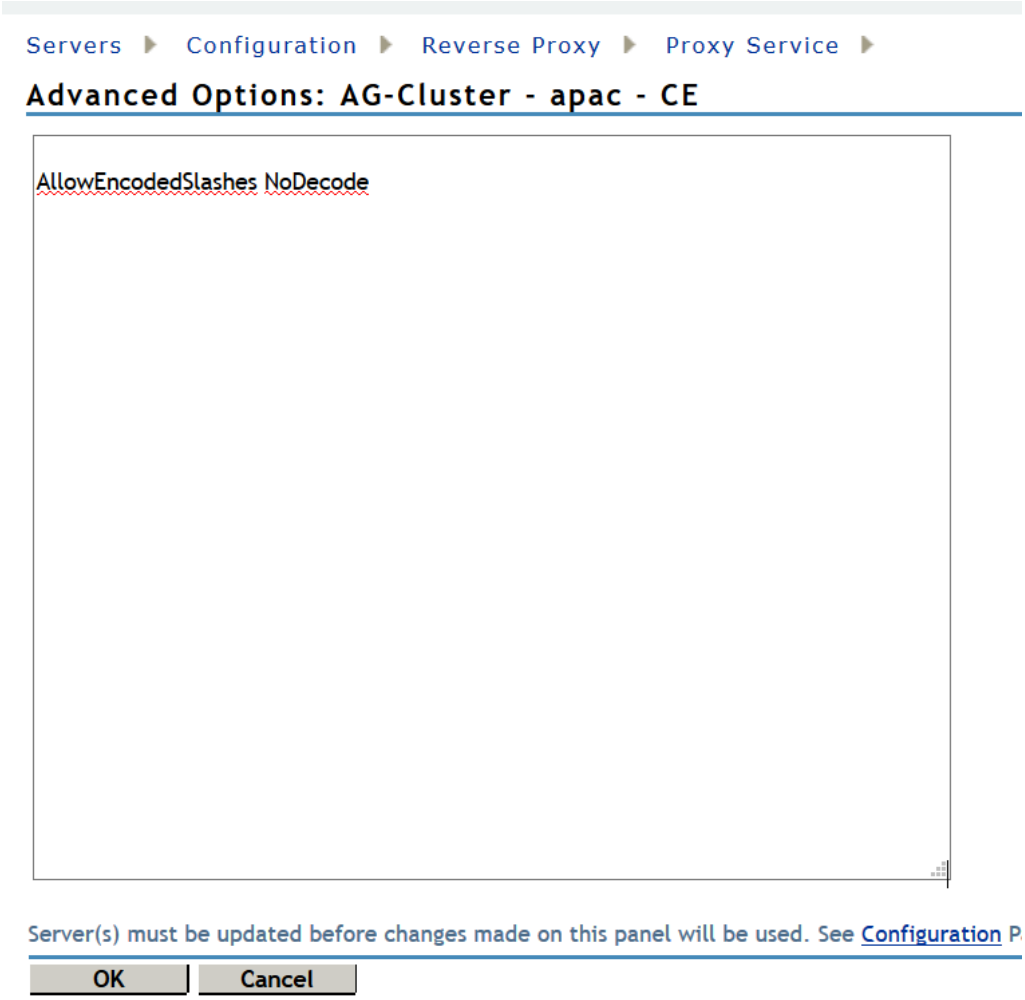
3 Click **Devices** > **Access Gateways** > **AG-Cluster** > *<Name of the Reverse Proxy>* that you have created.

4 Under the **Proxy Service List** create a new proxy service for CE. For example, CE_edit

5 Select the proxy service (CE_edit) that you created in Step 4.

5a In the **Reverse Proxy Service** > **Proxy Service**, select **Advanced Options**.

5a1 In the **Advanced Options**, specify `AllowEncodedSlashes NoDecode`.



This option ensures that files can be downloaded with CE.

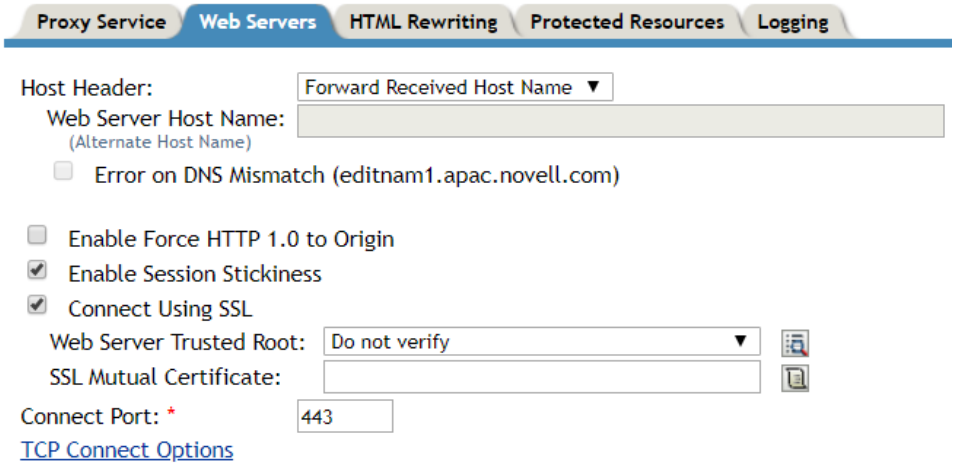
5a2 Click **OK**.

5b Click **Web Servers**.

5b1 Enable the option **Connect Using SSL**.

- **Web Server Trusted Root:** Select **Do not verify**.

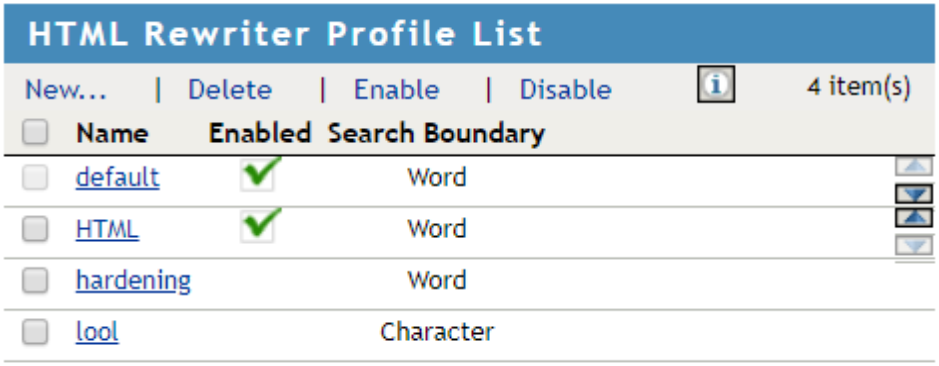
- **Connect Port:** Specify the value 443.



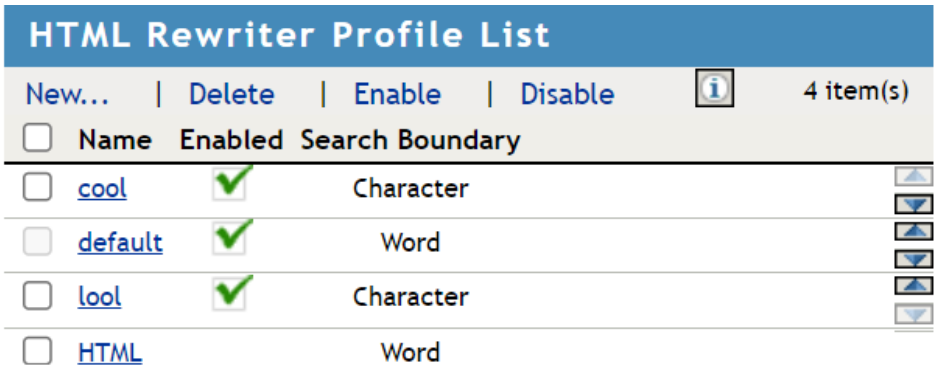
5b2 Click **OK**.

5c Click **HTML Rewriting**. The HTML rewriter profile was created for Filr, the same profile is used for CE.

For the versions earlier than CE 23.2, use the following configuration:



For the CE 23.2 and later versions, use the following configuration:



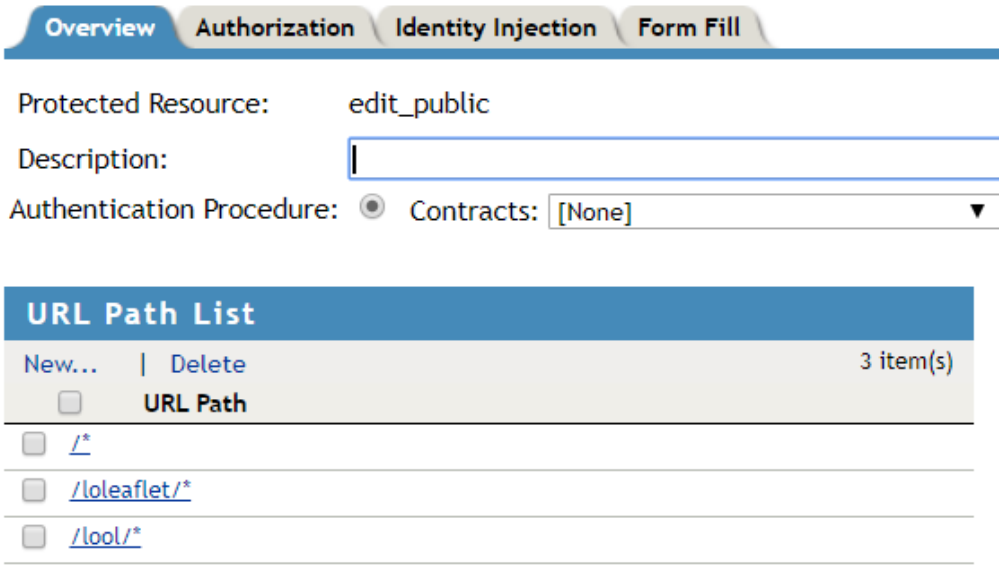
5d Click **Protected Resources**.

5d1 Create a new protected resource. For example, edit_public.

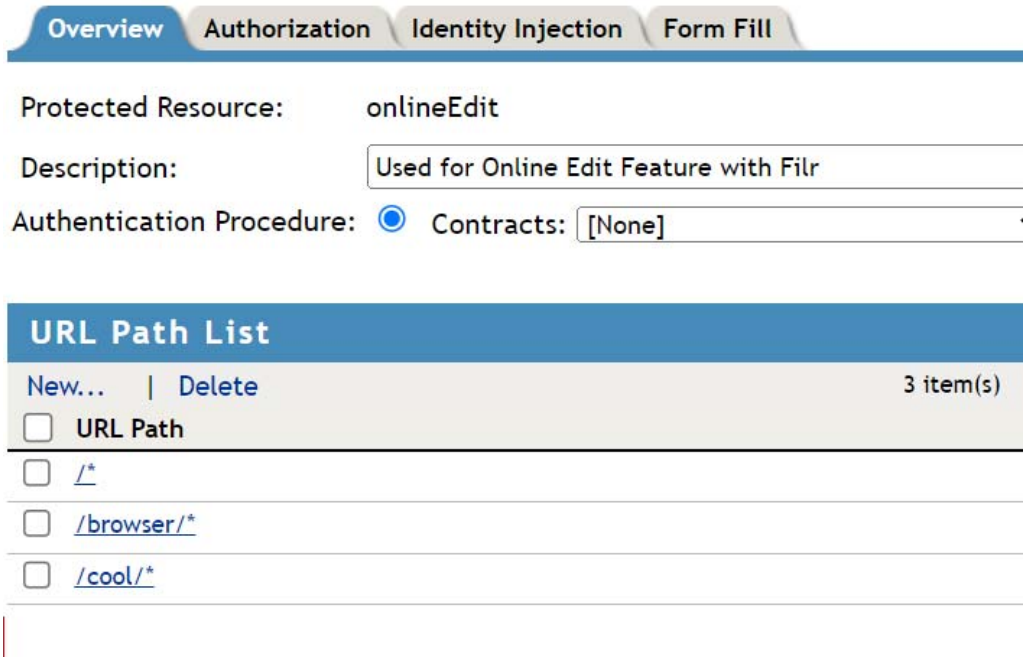
5d2 Enter the description.

5d3 Select Authentication Procedure as `Contracts: None`.

5d4 For the versions earlier than CE 23.2, in the URL Path list, add two new paths. For example, /loleaflet/* and /lool/*.



For the CE 23.2 and later versions, in the URL Path list, add two new paths. For example, /browser/* and /cool/*.



5d5 Click **OK**.

5e Click **Logging**.

5e1 Select **Enable Logging**.



5e2 Click **OK**.

6 To apply all your changes, click **Devices** > **Access Gateways**, then click **Update All**.

Allowing Filr to Connect to Content Editor

Perform the following steps, to add the DNS hostname of the CE appliance that was configured in NAM.

1. **Login to Filr:** https://*filr_appliance_ip_or_dns*:8443/.
2. To access the Administration Console, click on **Username > Administration Console**.
3. Under **System** > **Content Editor**, specify the **Server URL** as the NAM hostname for CE.

   This is the **Published DNS name** that you have configured for CE on the NAM server.

Allowing Content Editor to Connect to the Filr

This works with the Filr 4 and later servers.

Perform the following steps, to add the DNS hostname of the Filr appliance that was configured in NAM.

1. **Login to CE:** https://*content_editor_appliance_ip_or_dns*:9443/.
2. In the **Allowed Hosts** field, specify the NAM hostname for Filr.

   This is the **Published DNS name** that you have configured for Filr on the NAM server.

Using the Online Edit Feature

When a user performs Online Edit on a file, the Online Edit session (Filr) communicates to CE via NAM. The URL of the Online Edit session is shown accessing via NAM for CE.

Load Balancing

The Content Editor Appliance is configured by using HAProxy for load balancing. Load balancing refers to efficiently distributing incoming network traffic across a group of backend servers, also known as a server farm or server pool.

For collaborative editing to function correctly, you need to ensure that all the users editing the same document are served by the same Content Editor Appliance. Using the `WOPI` protocol, the https URL includes a unique identifier (`WOPISrc`) for use with this document. Thus load balancing can be done by using `WOPISrc` – ensuring that all URLs that contain the same `WOPISrc` are sent to the same Content Editor Appliance.

The browser reaches the proxy with the HTTPS protocol. The proxy terminates the HTTPS connection and passes traffic to backends via HTTP.

NOTE: For load balancing to work, all the nodes must run the same version of Content Editor Appliance. You cannot upgrade the Content Editor with one node and continue with the older version on another node.

For versions earlier than CE 23.2, in the Content Editor's config file, in `/var/opt/novell/contenteditor/loolwsd/loolwsd.xml`, or in the command line which starts `loolwsd` daemon, disable SSL and enable SSL termination.

For versions CE 23.2 and later, in the Content Editor's config file, in `/etc/coolwsd/coolwsd.xml`, or in the command line which starts `coolwsd` daemon, disable SSL and enable SSL termination.

The SSL termination option in the config file enables integration of Content Editor with SSL termination proxies, which handle incoming SSL connections, decrypt the SSL and pass on the unencrypted request to the server. In this setup only the proxy server has to have proper SSL settings, the Content Editor server is hidden behind it, and Content Editor communicates unencrypted with the proxy.

Load Balancing for versions earlier than CE 23.2

```
frontend loolwsd
       bind *:443 ssl crt /path/to/your/certificate_and_key.pem
       mode http
       default_backend loolwsd

backend loolwsd
      timeout tunnel 3600s
      mode http
      balance url_param WOPISrc check_post
      hash-type consistent
      server loolwsd01 127.0.0.1:9993
      server loolwsd02 127.0.0.1:9994
```

Sample configuration for Load Balancing with HAProxy

Add the following blocks to `haproxy.cfg`:

```
Frontend loolwsd
bind *:443 ssl crt /Path to your certificate_and_key.pem
http-request set-header X-HAProxy-loolwsd %[url_param(WOPISrc)]
mode http
default_backend loolwsd

backend loolwsd
timeout tunnel 3600s
mode http
balance hdr(X-HAProxy-loolwsd)
server lool1 <CE Server 1 IP>:9980
server lool2 <CE Server 2 IP>:9980
server lool3 <CE Server 3 IP>:9980
server loolN <CE Server N IP>:9980
```

Here CE server 1, 2 and 3 are different CE nodes.

Load Balancing for CE 23.2 and above versions

```
frontend coolwsd
bind *:443 ssl crt /path/to/your/certificate_and_key.pem
mode http
default_backend coolwsd

backend coolwsd
timeout tunnel 3600s
mode http
balance url_param WOPISrc check_post
hash-type consistent
server coolwsd01 127.0.0.1:9993
server coolwsd02 127.0.0.1:9994
```

Start Docker containers as described above, with `-p 127.0.0.1:9993:9980` and `-p 127.0.0.1:9994:9980`.

Sample configuration for Load Balancing with HAProxy

Add the following blocks to `haproxy.cfg`:

```
Frontend loolwsd
bind *:443 ssl crt /Path to your certificate_and_key.pem
balance balance url_param WOPISrc check_post
mode http
default_backend coolwsd
backend coolwsd
timeout tunnel 3600s
mode http
balance hdr(X-HAProxy-loolwsd)
server cool1 <CE Server 1 IP>:9980
server cool2 <CE Server 2 IP>:9980
server cool3 <CE Server 3 IP>:9980
server coolN <CE Server N IP>:9980
```

Here CE server 1, 2 and 3 are different CE nodes.

NOTE: If users are not able to perform an Online Edit when Filr is configured with AAF and CE is configured with Ha-Proxy Load Balancer, then add `enable.content.editor.check=false` to `/opt/novell/filr/apache-tomcat/webapps/ssf/WEB-INF/classes/config/ssf-ext.properties` and restart the Filr service.

Upgrading from Content Editor 1.2.3 to 2.0

Review the following sections before you upgrade your Content Editor Appliance 1.2.3 setup to Content Editor 2.0:

- "Support Matrix" on page 89
- "Upgrading Content Editor Appliance" on page 90
- "Understanding the Appliance Upgrade Process" on page 91
- "Downloading and Preparing Software for the Upgrades" on page 92
- "Copying Each Appliance's /vastorage Disk (Disk 2)" on page 94
- "Upgrading the VMs" on page 94

Support Matrix

Make sure that all the CE appliances are running version 1.2.3 with the latest patches applied.

Upgrading Content Editor Appliance

Before upgrading Content Editor Appliance, you must ensure certain requirements are met. See "Before You Upgrade!" on page 103 and then complete the instructions in the following sections in order:

Before You Upgrade

Failure to comply with the following critical points could result in a non-functional CE system.

Critical Point	Details
◆ Review the Release Notes and Limitations	◆ Check the Release Notes for any upgrade issues and "Upgrade" on page 172 before you start the upgrade process.
◆ Ensure that the VM host has enough unformatted disk space.	◆ The VM host server must have enough unallocated disk space to contain the following disks for each appliance. This is only temporary because after the upgrade completes, old appliances can be deleted and their disk space reclaimed. ◆ **System Disk (/):** This is created automatically as you deploy the downloaded software. Size is 50 GB per appliance. ◆ **Disk 2 (/vastorage):** You make a copy of each old appliance's Disk. Size needed equals the total size of all disks to be copied. ◆ **Each Disk 3 (/var):** You create this disk for each appliance in conjunction with the upgrade process. Size recommendation for Filr is 4 GB plus 3 times the RAM allocation for each appliance being upgraded. **NOTE:** The existing `/vashare` mount point is used by the upgraded Filr appliances. No new disk space is required for upgrading.
◆ Make sure that existing appliances are running version 1.2.3 with the latest patches.	◆ Make sure that all appliances are running version 1.2.3 with the latest patches applied. ◆ The earlier version of CE must be upgraded to CE 1.2.3 for upgrading to CE 2.0.
◆ Remove all VMware Snapshots	◆ Before copying Disk 2, make sure to remove all VMware snapshots so that the `/vastorage` disk has the correct disk file and latest configuration settings.
◆ Make sure that upgraded appliances meet the system requirements.	◆ See "System Requirements" on page 67.
◆ Do not attempt unsupported path migrations.	◆ **No Cross-platform:** You cannot upgrade from one virtualization platform to another. You can only upgrade VMware to VMware, and so forth. ◆ **No Mixed Versions:** All of the CE appliances in an expandable deployment must be upgraded to the same version.

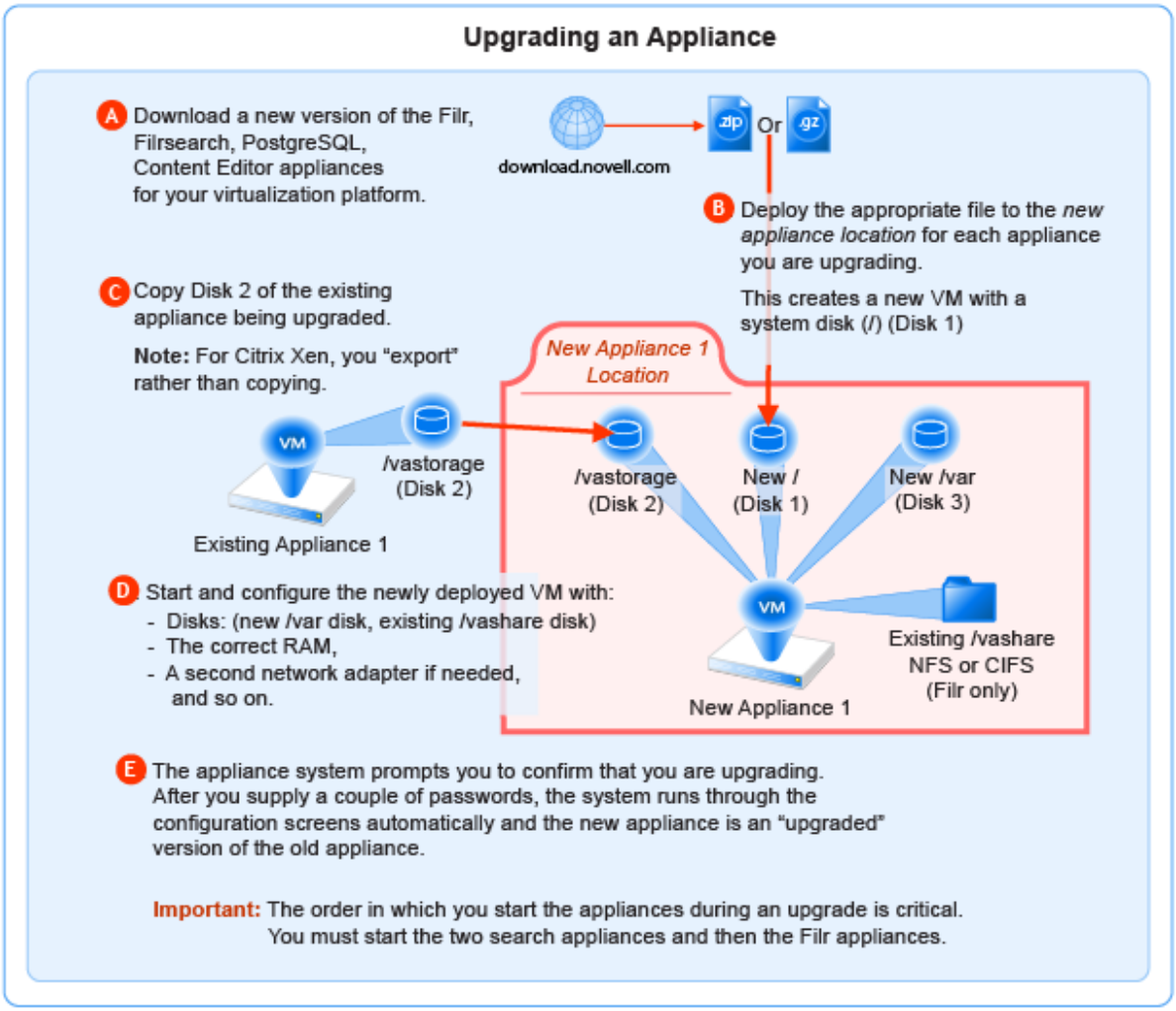
Critical Point	Details
◆ Plan when to upgrade.	Schedule the upgrade for a block of time that is least disruptive from a production standpoint. 2. Notify Filr users about the upgrade.

After ensuring that you have met the prerequisites and cautions above, complete the instructions in the following sections in order.

Understanding the Appliance Upgrade Process

The process of upgrading OpenText appliances is illustrated in Figure 10-1 on page 106.

Figure 9-1 *Overview of the Appliance Upgrade Process*



NOTE: ◆If you are using PostgreSQL DB shipped with Filr, then the order in which you start the appliances during an upgrade has to be

1. PostgreSQL
2. Lucene (Search Appliances)

3. Content Editor
4. Filr Appliance

- If you are using an external database, the order in which you start the appliances during an upgrade is critical. You must start the two search appliances and then the Filr appliances

Downloading and Preparing Software for the Upgrades

Download and prepare the software for your virtualization platform as described in the following sections:

VMWare

1 Download the CE software shown below to your management workstation.

IMPORTANT: Registration with OpenText is required to receive an email with a software-download link.

Appliance Type	Filename
Content Editor	`ContentEditor.x86_64.2022-09-13.53.ova.zip`

2 Extract each `.ova.zip` file on your management workstation until an *`ApplianceType-version`* folder appears.

3 Launch the vSphere Client and navigate to the datastore where you plan to host the upgraded VMs.

4 Create a folder for each appliance that you plan to upgrade.

Name each folder with a name that is easily associated with (but not the same as) the VM name of the associated appliance being upgraded.

5 Continue with "Copying Each Appliance's /vastorage Disk (Disk 2)" on page 109.

Hyper-V

1 Log in to the Hyper-V host server either locally or from a remote workstation using Remote Desktop.

2 Download the CE software shown below to the location where you plan to host your upgraded VMs.

IMPORTANT: Registration with OpenText is required to receive an email with a software-download link.

Appliance Type	Filename
Content Editor	`ContentEditor.x86_64.2022-09-13.53.vhdx.zip`

3 Extract each `.vhdx.zip` file in the directory where you downloaded it until an *`ApplianceType-version`*`.vhdx archive file` appears.

4 Create a new directory for each virtual machine you are upgrading.

As a best practice, name these directories with names that are easily associated with, but not the same as the VM name of each appliance being upgraded.

5 Move the `ce-`*`version`*`.vhdx` archive file to the first CE appliance-type folder and then copy the file to the remaining CE appliance type folders.

6 Continue with "Copying Each Appliance's /vastorage Disk (Disk 2)" on page 109.

Xen

1 Log in to the Xen VM host server either locally or from a remote workstation.

If you are connecting from a remote Linux workstation, use the following command:

`ssh -X root@`*`host_ip_address`*

The -X in the command in required for the GUI installation program upon which the steps in this section are based.

2 Download the CE software shown below to the Xen VM host server in the location where you plan to host your upgraded VMs.

IMPORTANT: Registration with OpenText is required to receive an email with a download link.

Appliance Type	Filename
Content Editor	`ContentEditor.x86_64.2022-09-13.53.qcow.zip`

3 Copy and rename the *`ApplianceType-version`* directories until you have one directory for each appliance that you are upgrading.

IMPORTANT: Only change the directory names.

Do not change the names of the `.qcow2` or `.xenconfig` files within the directories that you have copied and renamed.

For example:

1. Rename the CE-*`version`* directory to `CE-1-30-192.168.1.61`.
2. Copy the `CE-1-30-192.168.1.61` directory and rename it to `CE-1-30-192.168.1.62`, and so on until you have a directory for each appliance you are upgrading.

4 Continue with "Copying Each Appliance's /vastorage Disk (Disk 2)" on page 109.

Citrix Xen

1 On a workstation with Citrix XenCenter installed, download the CE software shown below.

IMPORTANT: Registration with OpenText is required to receive an email with a download link.

Appliance Type	Filename
Content Editor	`ContentEditor.x86_64.2022-09-13.53.xva.zip`

2 Extract each `.xva` file on your management workstation until an *`ApplianceType-version`* folder appears.

3 Continue with "Copying Each Appliance's /vastorage Disk (Disk 2)" on page 109.

Copying Each Appliance's /vastorage Disk (Disk 2)

IMPORTANT: ◆VMware requires shutting down an appliance before copying a disk.

This doesn't mean that the entire service must be down while disk copying takes place.

If you have a Filr-clustered deployment, you can minimize service interruption by shutting down one Filr or Filrsearch appliance, copying the disk, restarting the appliance and continuing with the next appliance.

- On Citrix Xen you "export" rather than copying Disk 2.

Copying each appliance's disk is at the heart of the upgrade process because it uses the corresponding "old" appliance's configuration settings on Disk 2 to create an upgraded version of the appliance with minimal input on your part.

Disk copying can take a while, depending on disk size and the VM host environment.

Therefore, we recommend keeping service downtime to a minimum by making the copies while the Filr system is still running.

1 Using the tools provided by your hypervisor, copy the /vastorage (second disk) to its associated folder or directory that you created for your upgraded appliances in "Downloading and Preparing Software for the Upgrades" on page 92.

Upgrading the VMs

- "Shutting Down the Appliances" on page 94
- "Upgrading VMware VMs" on page 95
- "Upgrading Hyper-V VMs" on page 96
- "Upgrading and Deploying Xen VMs" on page 98

Shutting Down the Appliances

1 Shut down all of your existing appliances in the shut down order that you identified earlier:

2 Continue with the instructions for your VM platform:

- VMware
- Hypter-V

- Xen
- Citrix Xen

Upgrading VMware VMs

Complete the steps in Table 10-1 for each appliance that you are upgrading

Table 9-5 *Upgrading a VMware VM*

Page, Dialog, or Option	Do This
	1 - Launching the vSphere Client.
	1. On your management workstation, start the vSphere Client.
vSphere Client	**2 - Deploying the OVA Template and naming the VM.**
	1. Click **File** > **Deploy OVA Template**.
Deploy OVA Template	1. Click **Browse**.
Open	1. For the appliance type you are deploying, navigate to the contents of the folder that you downloaded and extracted in "Downloading and Preparing Software for the Upgrades" on page 92. 2. Select and open the.ova file.
Deploy OVA Template	1. Name the appliance with the same name of the folder that you created for this upgraded appliance in Step 4 on page 107. 2. Click **Next**. 3. Choose the datastore and folder were you copied the appliance's Disk 2. 4. Click **Next** to accept the default for the disk format. 5. Do not select **Power on after deployment**. 6. Click **Finish**. The boot disk is created and the appliance is deployed as specified to this point.
	3 - Editing the VM settings.
vSphere Client	1. In the vSphere Client, right-click the VM you just deployed and select **Edit Settings**. The Virtual Machine Properties dialog displays.
Virtual Machine Properties	1. Set the **Memory** and **CPU** settings to match the appliance you are replacing, or increase them as planned.
	4 - Configuring Disk 2 (/vastorage)
Virtual Machine Properties	1. Click **Add**.

Page, Dialog, or Option	Do This
Add Hardware	1. Select **Hard Disk**, click **Next** and select **Use an existing Virtual disk**. 2. Click **Next > Browse**, then navigate to and select the copy of Disk 2 that you made for this appliance. 3. Click **Next > Next > Finish**.
	5 - Adding and Configuring Disk 3 (/var)
Virtual Machine Properties	1. Click **Add**.
Add Hardware	1. Select **Hard Disk**. 2. Click **Next > Next**. 3. Adjust the **Disk Size** to the same size as disk 3 (/var) on the appliance you are replacing. 4. Under **Disk Provisioning**, select either: ◆ **Thick Provision Eager Zeroed** or ◆ **Support clustering features such as Fault Tolerance** Depending on the VMware version that you are running. 5. Under **Location**, select **Specify a datastore or Datastore cluster** 6. Click **Browse**. 7. Select the datastore and folder for this appliance. 8. Click **OK**. 9. Click **Next**. 10. Under the **Virtual Device Node** section, select **SCSI**. 11. Click **Next**. 12. Click **Finish**.
Virtual Machine Properties	1. Click **Add**.
Add Hardware	1. Select **Ethernet Adapter**. 2. Click **Next**. 3. Under **Network Connection**, select the secondary network associated with the CE installation. 4. Click **Next > Finish > OK**.
vSphere Client	1. Repeat the steps in this table from 2 - Deploying OVA Template until all of your planned appliances have been deployed, then continue with "Deploying the Upgraded (Replacement) VMs" on page 118.

Upgrading Hyper-V VMs

Complete the steps in Table 10-2 for each appliance that you are upgrading.

Table 9-6 *Upgrading a Hyper-V VM*

Page, Dialog, or Option	Do This
	1 - Open Hyper-V Manager.
Hyper-V Host Server	1. Open the Hyper-V Manager.
	2 - Create a new VM.
Hyper-V Manager	1. In the left pane, right-click the server where you have planned to create the new virtual machine, then click **New** > **Virtual Machine**. The New Virtual Machine Wizard displays. 2. Click **Next**.
Specify Name and Location	1. Name the appliance with the name of the directory that you created for it in Step 4 on page 107. 2. Click **Next**.
Specify Generation	1. Make sure that **Generation 1** is selected. 2. Click **Next**.
	3 - Specify memory
Assign Memory	1. In the **Startup RAM** field, specify the same amount of memory (in MB) of the appliance that you are replacing, or increase the memory as planned. 2. Click **Next**.
	4 - Assign network adapter
Configure Networking	1. On the Configure Networking page, select the networking card for this VM. 2. Click **Next**.
	6 - Identify the system disk
Connect Virtual Hard Disk	1. Select **Use an existing virtual hard disk**. 2. Browse to and select the `.vhd` that you created for this appliance. 3. Click **Open**. 4. Click **Next**.
Summary	1. Click **Finish**. The VM is created and appears in the list of Virtual Machines.
	7 - Specify processors
Hyper-V Manager	1. In Hyper-V Manager, right-click the VM that you just created. 2. Click **Settings**.

Page, Dialog, or Option	Do This
Processor	1. Click **Processor**. 2. In the **Number of virtual processors** field, specify the number of processors for this VM. 3. Click **Next**.
	8 - Use existing copy of hard Disk 2 (/vastorage).
Settings for *VM* on *Host Server*	1. Add the copy you made of Disk 2 to this VM. 2. When you have added the disk, review the VM summary information and click **Finish**.
	9 - Add hard Disk 3 (/var).
Hyper-V Manager	1. In Hyper-V Manager, right-click the VM that you just created. 2. Click **Settings**. 3. Create a new blank virtual disk the same size as disk 3 on the appliance you are upgrading.
Summary	1. Review the summary information. 2. Click **Finish > OK**
Hyper-V Manager	**11 - Repeat until all VMs have upgraded copies** 1. Repeat the steps in this table until all of your planned appliances have been deployed, then continue with "Deploying the Upgraded (Replacement) VMs" on page 118.

Upgrading and Deploying Xen VMs

IMPORTANT: Unlike the other virtualization platforms, which you power on and deploy separately from the upgrade process, upgraded Xen VMs power on automatically when the upgrade process completes. You must then deploy the appliance before continuing with the next one.

Therefore, it is critical that you make sure to follow the deployment order that you identified earlier.

Complete the steps in Table 10-3 for each appliance that you are upgrading and deploying.

Table 9-7 *Upgrading and Deploying a Xen VM*

Page, Dialog, or Option	Do This
	1 - Launch the installer.
Terminal prompt on Xen VM Host Server	1. Run the following command to launch the GUI configuration menu: `virt-manager` **NOTE:** The `vm-install` command is deprecated from SLES 12 releases.

Page, Dialog, or Option	Do This
Create a new virtual machine	1. Click **File** > **New Virtual Machine**. The **Create a new virtual machine** wizard is displayed. 2. Select **Import existing disk image**. 3. Click **Forward**.
Storage path and Operating System	1. Browse and select the existing disk image. 2. Select **SUSE Linux Enterprise Server 12 SP4**. 3. Click **Forward**.
Choose Memory and CPU settings	1. Set the amount of memory (in MB) to match that of the VM you are upgrading. 2. Specify the **CPUs** to match the number of the VM you are upgrading. 3. Click **Forward**.
	2 - Name the VM.
Name of Virtual Machine	1. Specify the name of the appliance. 2. Select **Customize configuration before install**. 3. Click **Finish**.
	3 - Configure Disk 2 (/vastorage)
Hardware	1. Click **Add Hardware** at the bottom left of the screen. 2. Select the option **Select or create custom storage**. 3. Add the copy you made of Disk 2 to this VM. Select the `.qcow2` file. 4. Click **Open** > **Finish**.
	4 - Add and Configure a new Disk 3 (/var)
	1. Click **Add Hardware** at the bottom left of the screen. 2. Select the option **Select or create custom storage**. 3. Navigate to the contents of the folder for the appliance you are creating. 4. Select the `.qcow2` file. 5. Click **Open** > **Finish**.
Summary	1. Click **Network Adapters**.
Network Adapters	1. Click **New**.
Virtual Network Adapter	1. Specify the settings for the adapter. 2. Click **Apply**.
Network Adapters	1. Click **Apply**.

Page, Dialog, or Option	Do This
Summary	1. Click **OK**. The virtual machine is created, the appliance starts, and the configuration process begins.
Console	**6 - Deploy the Appliance** : 1. Access the appliance's console. 2. When prompted, enter the root and vaadmin passwords for the appliance being replaced. The upgrade process proceeds automatically. 3. When the appliance displays the final screen in the console window, open your management browser and log in to the appliance on port 9443 as the vaadmin user.
Port 9443 Admin Console	1. Depending on the appliance type you are upgrading, check the following: a. Click the CE configuration icon. b. Ensure that all of the settings are in place as expected (for example, - previously configured hostnames should be present). For more information see "Configuring Content Editor Options in Filr Appliance" on page 80
	7 - Upgrade the Next Appliance: 1. Return to the top of the table and repeat the process for the next appliance in your list.

Upgrading Filr

You can upgrade your Filr setup from Filr 4.3.1.2 to Filr 5.0.

The following chapter is covered in this section.

- Chapter 10, “Upgrading from Filr 4.3.1.2 to Filr 5.0,” on page 103
- Chapter 11, “Updating Filr through Online Update Channel,” on page 133

10 Upgrading from Filr 4.3.1.2 to Filr 5.0

Review the following sections before you upgrade your Filr 4.3.1.2 setup to Filr 5.0:

- "Support Matrix" on page 103
- "Upgrading a Large Filr Deployment" on page 103
- "Upgrading an All-in-One (Small) Deployment" on page 120

Support Matrix

You must update to the latest 4.3.x patch version before upgrading to 5.0.

	Source Version	Status
Server	4.3.x with latest patch	Supported
	4.3 or earlier versions	Not Supported. Upgrade to 4.3.x
Client	4.3.x	Supported
	4.3 or earlier versions	Not Supported. Upgrade to 4.3.x

Upgrading a Large Filr Deployment

Before upgrading a Filr deployment, you must ensure certain requirements are met. See "Before You Upgrade!" on page 103 and then complete the instructions in the following sections in order:

- "Understanding the Appliance Upgrade Process" on page 106
- "Downloading and Preparing Software for the Upgrades" on page 106
- "Copying Each Appliance's /vastorage Disk (Disk 2)" on page 109
- "Upgrading the VMs" on page 109
- "Deploying the Upgraded (Replacement) VMs" on page 118
- "Performing Post-Upgrade Tasks" on page 119

Before You Upgrade!

Failure to comply with the following critical points could result in a non-functional Filr system.

Critical Point	Details
• Review the Release Notes and Limitations	• Check the Release Notes for any upgrade issues and "Upgrade" on page 172 before you start the upgrade process.

Critical Point	Details
◆ Plan the upgrade order and follow it.	◆ You must upgrade the appliances in order of dependency upon each other. 1. **Shut Down Order:** Prepare a list of your appliances that defines the correct shut down order: ◆ **Filr:** All Filr appliances must be shut down first. ◆ **Filrsearch:** Next, you shut down the Filrsearch appliances. 2. **PostgreSQL:** If you are using PostgreSQL appliance (shipped with Filr), then ensure it is running. 3. **Deployment Order:** Prepare a second list of that defines the correct upgrade and deployment order: ◆ **Filrsearch:** You must upgrade and deploy the Filrsearch appliances before the Filr appliances. ◆ **Filr:** When the upgraded Filrsearch appliances are up and running, upgrade and deploy the first Filr appliance. Then upgrade and deploy the additional Filr appliances. 4. If there are things you need to remember about individual appliances, include those reminders in the appropriate list. 5. Use the shut down list as you complete the steps in "Upgrading the VMs." 6. Use the upgrade list as you complete the steps in "Deploying the Upgraded (Replacement) VMs."
◆ Ensure that the VM host has enough unformatted disk space.	◆ The VM host server must have enough unallocated disk space to contain the following disks for each appliance. This is only temporary because after the upgrade completes, old appliances can be deleted and their disk space reclaimed. ◆ **System Disk (/):** This is created automatically as you deploy the downloaded software. Size is 50 GB per appliance. ◆ **Disk 2 (/vastorage):** You make a copy of each old appliance's Disk. Size needed equals the total size of all disks to be copied. ◆ **Each Disk 3 (/var):** You create this disk for each appliance in conjunction with the upgrade process. Size recommendation for Filr is 4 GB plus 3 times the RAM allocation for each appliance being upgraded. **NOTE:** The existing `/vashare` mount point is used by the upgraded Filr appliances. No new disk space is required for upgrading.

Critical Point	Details
◆ Make sure that existing appliances are running version 4.3.1.2 with the latest patches.	◆ Make sure that all appliances are running version 4.3.1.2 with the latest patches applied. See Managing Field Test Patches in the Filr 5.0 Administrative UI Reference. ◆ The earlier version of Filr must be upgraded to Filr 4.3.1.2 for upgrading to Filr 5.0. ◆ If the existing appliances are running version is 4.3.1.1, then before upgrade, you will be prompted to enter the CIFS vashare details.
◆ Remove all VMware Snapshots	◆ Before copying Disk 2, make sure to remove all VMware snapshots so that the `/vastorage` disk has the correct disk file and latest configuration settings.
◆ Make sure that upgraded appliances meet the system requirements.	◆ See Chapter 3, "Filr System Requirements," on page 13.
◆ Do not attempt unsupported path migrations.	◆ **No Cross-platform:** You cannot upgrade from one virtualization platform to another. You can only upgrade VMware to VMware, and so forth. ◆ **No Mixed Versions:** All of the Filr and Filrsearch appliances in an expandable deployment must be upgraded to the same version. ◆ **No Cross-Deployment-Types:** You can only upgrade small to small, non-expandable to non-expandable, or expandable to expandable. If you have a small or non-expandable deployment, and you need an expandable deployment, you must either install a new system or contact OpenText Consulting to assist you with the migration.
◆ Appliances with two network adapters.	◆ You should manually add the additional network card on successfully upgrading the appliance.
◆ Plan when to upgrade.	◆ Filr services must be offline during the upgrade. 1. Schedule the upgrade for a block of time that is least disruptive from a production standpoint. 2. Notify Filr users about the upgrade.

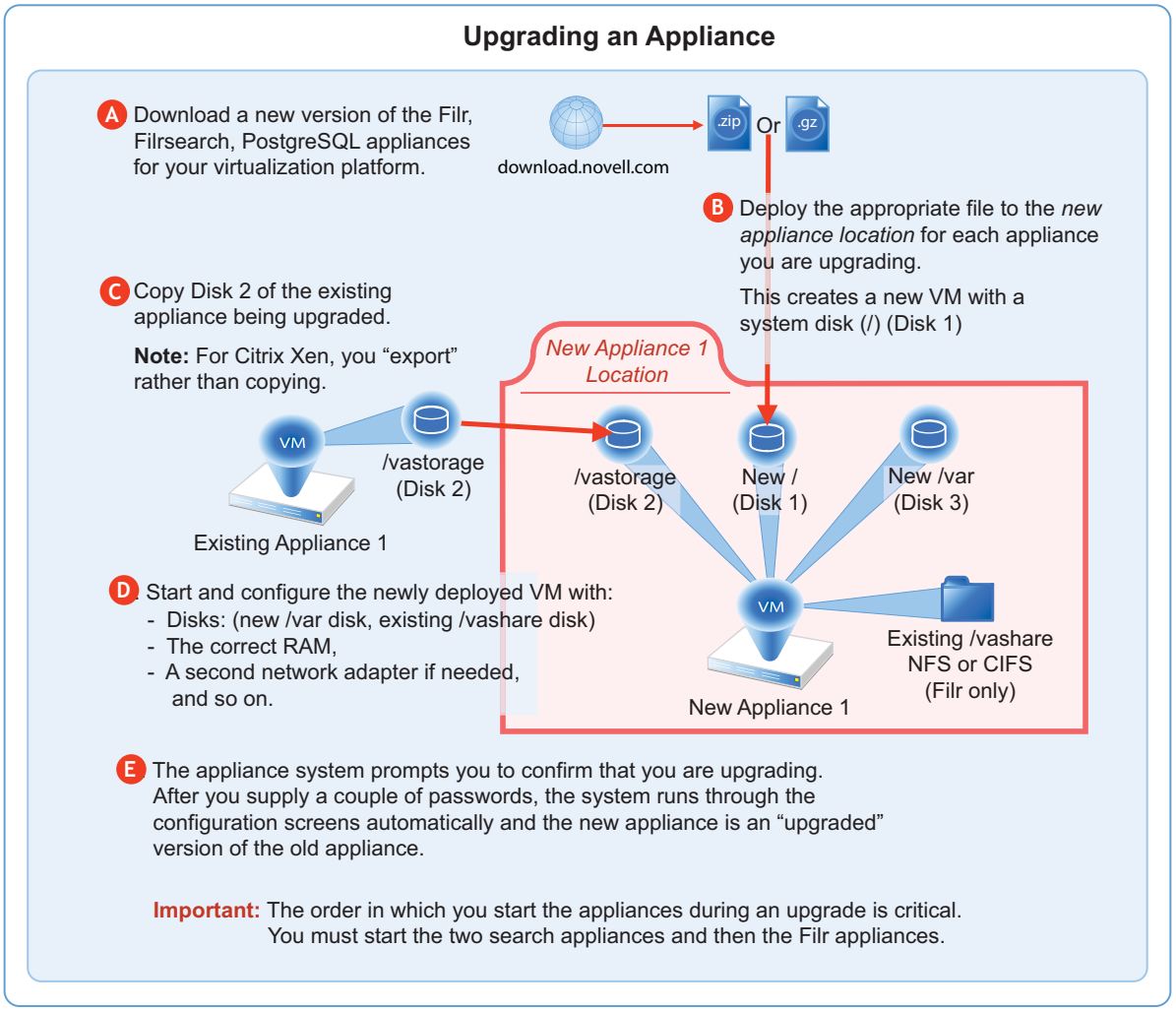
After ensuring that you have met the prerequisites and cautions above, complete the instructions in the following sections in order.

- "Understanding the Appliance Upgrade Process" on page 106
- "Downloading and Preparing Software for the Upgrades" on page 106
- "Copying Each Appliance's /vastorage Disk (Disk 2)" on page 109
- "Upgrading the VMs" on page 109
- "Deploying the Upgraded (Replacement) VMs" on page 118
- "Performing Post-Upgrade Tasks" on page 119

Understanding the Appliance Upgrade Process

The process of upgrading OpenText appliances is illustrated in Figure 10-1 on page 106.

Figure 10-1 *Overview of the Appliance Upgrade Process*



NOTE: ◆If you are using PostgreSQL DB shipped with Filr, then the order in which you start the appliances during an upgrade has to be

1. PostgreSQL
2. Lucene (Search Appliances)
3. Filr Appliances

◆ If you are using an external database, the order in which you start the appliances during an upgrade is critical. You must start the two search appliances and then the Filr appliances.

Downloading and Preparing Software for the Upgrades

Download and prepare the software for your virtualization platform as described in the following sections:

VMWare

1 Download the Filr software shown below to your management workstation.

IMPORTANT: Registration with OpenText is required to receive an email with a software-download link.

Appliance Type	Filename
Filr	`Filr.x86_64-version.ova.zip`
Search	`Filrsearch.x86_64-version.ova.zip`
PostgreSQL	`PostgreSQL-version.ova.zip`

2 Extract each `.ova.zip` file on your management workstation until an *`ApplianceType-version`* folder appears.

3 Launch the vSphere Client and navigate to the datastore where you plan to host the upgraded VMs.

4 Create a folder for each appliance that you plan to upgrade.

Name each folder with a name that is easily associated with (but not the same as) the VM name of the associated appliance being upgraded.

5 Continue with "Copying Each Appliance's /vastorage Disk (Disk 2)" on page 109.

Hyper-V

1 Log in to the Hyper-V host server either locally or from a remote workstation using Remote Desktop.

2 Download the Filr software shown below to the location where you plan to host your upgraded VMs.

IMPORTANT: Registration with OpenText is required to receive an email with a software-download link.

Appliance Type	Filename
Filr	`Filr.x86_64-version.vhdx.zip`
Search	`Filrsearch.x86_64-version.vhdx.zip`
PostgreSQL	`PostgreSQL-version.vhdx.zip`

3 Extract each `.vhdx.zip` file in the directory where you downloaded it until an *`ApplianceType-version`*`.vhdx archive file` appears.

4 Create a new directory for each virtual machine you are upgrading.

As a best practice, name these directories with names that are easily associated with, but not the same as the VM name of each appliance being upgraded.

5 Move the *`filr-version`*`.vhdx` archive file to the first Filr appliance-type folder and then copy the file to the remaining Filr appliance type folders.

6 Move the *filr*search-*version*.vhdx archive file to the first Filrsearch appliance-type folder and then copy the file to the second Filrsearch folder.

7 Continue with "Copying Each Appliance's /vastorage Disk (Disk 2)" on page 109.

Xen

1 Log in to the Xen VM host server either locally or from a remote workstation.

If you are connecting from a remote Linux workstation, use the following command:

```
ssh -X root@host_ip_address
```

The -X in the command in required for the GUI installation program upon which the steps in this section are based.

2 Download the Filr software shown below to the Xen VM host server in the location where you plan to host your upgraded VMs.

IMPORTANT: Registration with OpenText is required to receive an email with a download link.

NOTE: Begining with Filr 5.0, any .tar.gz files will not be shipped. Instead, the images will be provided.

Appliance Type	Filename
Filr	Filr.x86_64-*version*.xen.qcow2
Search	Filrsearch.x86_64-*version*.xen.qcow2
PostgreSQL	PostgreSQL-*version*.xen.qcow2

3 Copy and rename the *ApplianceType-version* directories until you have one directory for each appliance that you are upgrading.

IMPORTANT: Only change the directory names.

Do not change the names of the `.qcow2` or `.xenconfig` files within the directories that you have copied and renamed.

For example:

1. Rename the Filr-*version* directory to `filr-1-30-192.168.1.61`.
2. Copy the `filr-1-30-192.168.1.61` directory and rename it to `filr-1-30-192.168.1.62`, and so on until you have a directory for each appliance you are upgrading.
3. In a similar manner, copy and rename the Filrsearch-*version* directory until you have two Filrsearch appliances.

4 Continue with "Copying Each Appliance's /vastorage Disk (Disk 2)" on page 109.

Citrix Xen

1 On a workstation with Citrix XenCenter installed, download the Filr software shown below.

IMPORTANT: Registration with OpenText is required to receive an email with a download link.

Appliance Type	Filename
Filr	`Filr.x86_64-version.xva.xva`
Search	`Filrsearch.x86_64-version.xva.xva`
PostgreSQL	`PostgreSQL-version.xva.xva`

2 Extract each `.xva` file on your management workstation until an *`ApplianceType-version`* folder appears.

3 Continue with "Copying Each Appliance's /vastorage Disk (Disk 2)" on page 109.

Copying Each Appliance's /vastorage Disk (Disk 2)

IMPORTANT: ◆VMware requires shutting down an appliance before copying a disk.

This doesn't mean that the entire service must be down while disk copying takes place.

If you have a Filr-clustered deployment, you can minimize service interruption by shutting down one Filr or Filrsearch appliance, copying the disk, restarting the appliance and continuing with the next appliance.

- On Citrix Xen you "export" rather than copying Disk 2.

Copying each appliance's disk is at the heart of the upgrade process because it uses the corresponding "old" appliance's configuration settings on Disk 2 to create an upgraded version of the appliance with minimal input on your part.

Disk copying can take a while, depending on disk size and the VM host environment.

Therefore, we recommend keeping service downtime to a minimum by making the copies while the Filr system is still running.

1 Using the tools provided by your hypervisor, copy the /vastorage (second disk) to its associated folder or directory that you created for your upgraded appliances in "Downloading and Preparing Software for the Upgrades" on page 92.

Upgrading the VMs

- "Shutting Down the Appliances" on page 110
- "Upgrading VMware VMs" on page 110
- "Upgrading Hyper-V VMs" on page 112
- "Upgrading and Deploying Xen VMs" on page 114
- "Upgrading Citrix Xen VMs" on page 117

Shutting Down the Appliances

1. Shut down all of your existing appliances in the shut down order that you identified earlier:
2. Continue with the instructions for your VM platform:
   - VMware
   - Hypter-V
   - Xen
   - Citrix Xen

Upgrading VMware VMs

Complete the steps in Table 10-1 for each appliance that you are upgrading

Table 10-1 *Upgrading a VMware VM*

Page, Dialog, or Option	Do This
	1 - Launching the vSphere Client.
	1. On your management workstation, start the vSphere Client.
vSphere Client	**2 - Deploying the OVA Template and naming the VM.**
	1. Click **File** > **Deploy OVA Template**.
Deploy OVA Template	1. Click **Browse**.
Open	1. For the appliance type you are deploying, navigate to the contents of the folder that you downloaded and extracted in "Downloading and Preparing Software for the Upgrades" on page 92. 2. Select and open the.ova file.
Deploy OVA Template	1. Name the appliance with the same name of the folder that you created for this upgraded appliance in Step 4 on page 107. 2. Click **Next**. 3. Choose the datastore and folder were you copied the appliance's Disk 2. 4. Click **Next** to accept the default for the disk format. 5. Do not select **Power on after deployment**. 6. Click **Finish**. The boot disk is created and the appliance is deployed as specified to this point.
	3 - Editing the VM settings.
vSphere Client	1. In the vSphere Client, right-click the VM you just deployed and select **Edit Settings**. The Virtual Machine Properties dialog displays.
Virtual Machine Properties	1. Set the **Memory** and **CPU** settings to match the appliance you are replacing, or increase them as planned.

Page, Dialog, or Option	Do This
	4 - Configuring Disk 2 (/vastorage)
Virtual Machine Properties	1. Click **Add**.
Add Hardware	1. Select **Hard Disk**, click **Next** and select **Use an existing Virtual disk**. 2. Click **Next > Browse**, then navigate to and select the copy of Disk 2 that you made for this appliance. 3. Click **Next > Next > Finish**.
	5 - Adding and Configuring Disk 3 (/var)
Virtual Machine Properties	1. Click **Add**.
Add Hardware	1. Select **Hard Disk**. 2. Click **Next > Next**. 3. Adjust the **Disk Size** to the same size as disk 3 (/var) on the appliance you are replacing. 4. Under **Disk Provisioning**, select either: ◆ **Thick Provision Eager Zeroed** or ◆ **Support clustering features such as Fault Tolerance** Depending on the VMware version that you are running. 5. Under **Location**, select **Specify a datastore or Datastore cluster** 6. Click **Browse**. 7. Select the datastore and folder for this appliance. 8. Click **OK**. 9. Click **Next**. 10. Under the **Virtual Device Node** section, select **SCSI**. 11. Click **Next**. 12. Click **Finish**. 13. If you need to add network adapters, continue with 6 - (Optional) Adding a Network Adapter. Otherwise, click **OK**, return to "2 - Deploying the OVA Template and naming the VM." on page 110, and deploy the next appliance that you have planned for When all of your planned appliances have been deployed, continue with "Deploying the Upgraded (Replacement) VMs" on page 118.

Page, Dialog, or Option	Do This
	6 - (Optional) Adding a Network Adapter You can add a network adapter if your Filr deployment accesses a separate network for one or more of the following reasons: ◆ Appliance administration. ◆ NFS mount or CIFS access to the /vashare mount point. ◆ Security of Memcached. **IMPORTANT:** Bonding or teaming NICs is not supported with Filr.
Virtual Machine Properties	1. Click **Add**.
Add Hardware	1. Select **Ethernet Adapter**. 2. Click **Next**. 3. Under **Network Connection**, select the secondary network associated with the Filr installation. 4. Click **Next > Finish > OK**.
vSphere Client	1. Repeat the steps in this table from 2 - Deploying OVA Template until all of your planned appliances have been deployed, then continue with "Deploying the Upgraded (Replacement) VMs" on page 118.

Upgrading Hyper-V VMs

Complete the steps in Table 10-2 for each appliance that you are upgrading.

Table 10-2 *Upgrading a Hyper-V VM*

Page, Dialog, or Option	Do This
	1 - Open Hyper-V Manager.
Hyper-V Host Server	1. Open the Hyper-V Manager.
	2 - Create a new VM.
Hyper-V Manager	1. In the left pane, right-click the server where you have planned to create the new virtual machine, then click **New** > **Virtual Machine**. The New Virtual Machine Wizard displays. 2. Click **Next**.
Specify Name and Location	1. Name the appliance with the name of the directory that you created for it in Step 4 on page 107. 2. Click **Next**.
Specify Generation	1. Make sure that **Generation 1** is selected. 2. Click **Next**.

Page, Dialog, or Option	Do This
	3 - Specify memory
Assign Memory	1. In the **Startup RAM** field, specify the same amount of memory (in MB) of the appliance that you are replacing, or increase the memory as planned. 2. Click **Next**.
	4 - Assign network adapter
Configure Networking	1. On the Configure Networking page, select the networking card for this VM. 2. Click **Next**.
	6 - Identify the system disk
Connect Virtual Hard Disk	1. Select **Use an existing virtual hard disk**. 2. Browse to and select the `.vhd` that you created for this appliance. 3. Click **Open**. 4. Click **Next**.
Summary	1. Click **Finish**. The VM is created and appears in the list of Virtual Machines.
	7 - Specify processors
Hyper-V Manager	1. In Hyper-V Manager, right-click the VM that you just created. 2. Click **Settings**.
Processor	1. Click **Processor**. 2. In the **Number of virtual processors** field, specify the number of processors for this VM. 3. Click **Next**.
	8 - Use existing copy of hard Disk 2 (/vastorage).
Settings for *VM* on *Host Server*	1. Add the copy you made of Disk 2 to this VM. 2. When you have added the disk, review the VM summary information and click **Finish**.
	9 - Add hard Disk 3 (/var).
Hyper-V Manager	1. In Hyper-V Manager, right-click the VM that you just created. 2. Click **Settings**. 3. Create a new blank virtual disk the same size as disk 3 on the appliance you are upgrading.
Summary	1. Review the summary information. 2. Click **Finish > OK**

Page, Dialog, or Option	Do This
	10 - (Optional) Add a Network Adapter 1. If the appliance you are upgrading has a secondary network adapter, add that now.
Hyper-V Manager	**11 - Repeat until all VMs have upgraded copies** 1. Repeat the steps in this table until all of your planned appliances have been deployed, then continue with "Deploying the Upgraded (Replacement) VMs" on page 118.

Upgrading and Deploying Xen VMs

IMPORTANT: Unlike the other virtualization platforms, which you power on and deploy separately from the upgrade process, upgraded Xen VMs power on automatically when the upgrade process completes. You must then deploy the appliance before continuing with the next one.

Therefore, it is critical that you make sure to follow the deployment order that you identified earlier.

Complete the steps in Table 10-3 for each appliance that you are upgrading and deploying.

Table 10-3 *Upgrading and Deploying a Xen VM*

Page, Dialog, or Option	Do This
	1 - Launch the installer.
Terminal prompt on Xen VM Host Server	1. Run the following command to launch the GUI configuration menu: `virt-manager` **NOTE:** The `vm-install` command is deprecated from SLES 12 releases.
Create a new virtual machine	1. Click **File** > **New Virtual Machine**. The **Create a new virtual machine** wizard is displayed. 2. Select **Import existing disk image**. 3. Click **Forward**.
Storage path and Operating System	1. Browse and select the existing disk image. 2. Select **SUSE Linux Enterprise Server 12 SP4**. 3. Click **Forward**.
Choose Memory and CPU settings	1. Set the amount of memory (in MB) to match that of the VM you are upgrading. 2. Specify the **CPUs** to match the number of the VM you are upgrading. 3. Click **Forward**.

Page, Dialog, or Option	Do This
	2 - Name the VM.
Name of Virtual Machine	1. Specify the name of the appliance. 2. Select **Customize configuration before install**. 3. Click **Finish**.
	3 - Configure Disk 2 (/vastorage)
Hardware	1. Click **Add Hardware** at the bottom left of the screen. 2. Select the option **Select or create custom storage**. 3. Add the copy you made of Disk 2 to this VM. Select the `.qcow2` file. 4. Click **Open** > **Finish**.
	4 - Add and Configure a new Disk 3 (/var)
	1. Click **Add Hardware** at the bottom left of the screen. 2. Select the option **Select or create custom storage**. 3. Navigate to the contents of the folder for the appliance you are creating. 4. Select the `.qcow2` file. 5. Click **Open** > **Finish**.
	5 - (Optional) Add a Network Adapter You can add a network adapter if your Filr deployment accesses a separate network for one or more of the following reasons: ◆ Appliance administration. ◆ NFS mount or CIFS access to the /vashare mount point. ◆ Security of Memcached. **IMPORTANT:** Bonding or teaming NICs is not supported with Filr.
Summary	1. Click **Network Adapters**.
Network Adapters	1. Click **New**.
Virtual Network Adapter	1. Specify the settings for the adapter. 2. Click **Apply**.
Network Adapters	1. Click **Apply**.
Summary	1. Click **OK**. The virtual machine is created, the appliance starts, and the configuration process begins.

Page, Dialog, or Option	Do This
Console	**6 - Deploy the Appliance** 1. Access the appliance's console. 2. When prompted, enter the root and vaadmin passwords for the appliance being replaced. The upgrade process proceeds automatically. 3. When the appliance displays the final screen in the console window, open your management browser and log in to the appliance on port 9443 as the vaadmin user.
Port 9443 Admin Console	1. Depending on the appliance type you are upgrading, check the following: ◆ **Filrsearch:** 1. Click the Filrsearch configuration icon. 2. Ensure that all of the settings are in place as expected. 3. If the configuration wizard displays, there was a problem with the configuration. 4. Resolve the configuration issues, then click Finish to reconfigure the system. ◆ **Filr:** 1. Click the Filr configuration icon. 2. Ensure that all of the settings are in place as expected. 3. If the configuration wizard displays, there was a problem with the configuration. 4. Resolve the configuration issues, then click Finish to reconfigure the system. Common configuration issues include: ◆ If your system is not using DNS, the most likely problem is unresolvable DNS names and missing /etc/hosts entries. ◆ If the appliance doesn't have access to the database, ensure that all of the settings are as expected.
	7 - Upgrade the Next Appliance 1. Return to the top of the table and repeat the process for the next appliance in your list. When all of your appliances are running, continue with "Performing Post-Upgrade Tasks."

Upgrading Citrix Xen VMs

Table 10-4 *Upgrading a Citrix Xen VM*

Page, Dialog, or Option	Do This
	1 - Launch XenCenter.
Management Workstation	1. Start XenCenter.
XenCenter	1. Connect to the Citrix XenServer where you are deploy the upgraded appliances. 2. Right-click the server and select **Import**.
	2 - Import the system disk
Locate the File you want to import	1. Browse to and select the `.xva` file on your management workstation for the appliance that you are upgrading. 2. Click **Open**. 3. Click **Next**.
Select the location where the imported VM will be placed	1. Select the XenServer. 2. Click **Next**.
Select target storage	1. Select the storage repository for the VM. 2. Click **Import**.
	3 - Select the network adapter
Select network to connect VM	1. Select the virtual network adapter. 2. Click **Next**.
Review the import settings	1. Deselect **Start VM(s) after import**. 2. Click **Finish**. **IMPORTANT:** Depending on network latency and other factors, it can take a while to import the system disk.
	4 - Specify Memory
	1. If you need to adjust the memory to the amount of memory, select the newly created VM in the left pane. 2. Click the **Memory** tab. 3. Click **Edit**, change the setting, and click **OK**.
	5 - Specify Processors
	1. If you need to adjust the CPUs, right-click the newly created VM in the left pane. 2. Select **Properties**. 3. Click **CPU**, change the setting, and click **OK**.
	6 - Link to Disk 2 (/vastorage)

Page, Dialog, or Option	Do This
	1. With the newly created VM selected in the left pane, add the copy of Disk 2 for this appliance.
	8 - Add Disk 3 (/var)
Virtual Disks	1. Click **Add...**.
Add Virtual Disk	1. Type a disk name that reflects the appliance name and that this is disk 3. For example, Filr-1-disk-3. 2. Change the **Size** field value to match that of the appliance you are replacing. 3. Click **Add**.
	9 - (Optional) Add a Network Adapter You can add a network adapter if your Filr deployment accesses a separate network for one or more of the following reasons: ◆ Appliance administration. ◆ NFS mount or CIFS access to the /vashare mount point. ◆ Security of Memcached. **IMPORTANT:** Bonding or teaming NICs is not supported with Filr.
	1. With the newly created VM selected in the left pane, click the **Networking** tab. 2. Select the secondary network associated with the Filr installation..
XenCenter	1. Repeat the steps in this table until all of your planned appliances have been upgraded, then continue with "Deploying the Upgraded (Replacement) VMs" on page 118.

Deploying the Upgraded (Replacement) VMs

IMPORTANT: ◆Make sure that you deploy (Start and configure) your appliances one at a time.

Attempting to start and configure multiple upgraded appliances at the same time causes timing, synchronization, and other problems.

- Also make sure that you deploy the appliances in the deployment order that you identified earlier:
  1. Filrsearch
  2. Filr

1 Power on the first (or next) appliance in your deployment order list.

2 Access the appliance's console.

3 When prompted, enter the root and vaadmin passwords for the appliance being replaced.

The upgrade process proceeds automatically.

4 When the appliance displays the final screen in the console window, open your management browser and log in to the appliance on port 9443 as the vaadmin user.

5 Depending on the appliance type you are upgrading, check the following:

Filrsearch	Filr
1. Click the Filrsearch configuration icon. 2. Ensure that all of the settings are in place as expected. 3. If the configuration wizard displays, there was a problem with the configuration. Resolve the configuration issues, then click **Finish** to reconfigure the system.	1. Click the Filr configuration icon. 2. Ensure that all of the settings are in place as expected. 3. If the configuration wizard displays, there was a problem with the configuration. Resolve the configuration issues, then click **Finish** to reconfigure the system. Common configuration issues include: ◆ If your system is not using DNS, the most likely problem is unresolvable DNS names and missing `/etc/hosts` entries. ◆ If the appliance doesn't have access to the database, ensure that all of the settings are as expected.

6 When the appliance is running, deploy the next appliance.

7 When all of your appliances are running, continue with "Performing Post-Upgrade Tasks."

Performing Post-Upgrade Tasks

After upgrading to a new version of Filr, you should perform the following tasks to ensure a fully functional Filr system:

- "Install Your New Filr License" on page 119
- "Java Heap" on page 119

Install Your New Filr License

The newly upgraded Filr appliances have a 60-day evaluation license installed. The evaluation license is expired in most cases since it considers the day of deployment as the day when it was installed with the earlier version.

To prevent a service interruption, you must install your new license by following the instructions in "Installing/Updating the Filr License" in the *OpenText Filr 23.4: Administrative UI Reference*.

Java Heap

For optimal performance of Filr appliance, the minimum Java heap space should be 12 GB. After upgrading the appliance, the Java heap space is overwritten with the value that was set for the earlier Filr appliance. If new value is less, then ensure to update it to 12 GB or greater.

Upgrading an All-in-One (Small) Deployment

Before upgrading a Filr deployment, you must ensure certain requirements are met. See "Before You Upgrade!" on page 120 and then complete the instructions in the following sections in order:

- "Small Filr Upgrade Process Overview" on page 121
- "Downloading and Preparing Software" on page 121
- "Copying Each Appliance's /vastorage Disk (Disk 2)" on page 122
- "Upgrading the VMs" on page 123
- "Deploying the Upgraded Filr VM" on page 131
- "Performing Filr Post-Upgrade Tasks" on page 132

Before You Upgrade!

Failure to comply with the following critical points could result in a non-functional Filr system.

- **Review the Release Notes:** Check "Upgrade Filr" before you start the upgrade process.
- **Ensure that the VM host has enough unformatted disk space:**
  - **System Disk (/):** A 50 GB disk is created automatically.
  - **Disk 2 (/vastorage):** You make a copy of the appliance's Disk 2.
  - **Each Disk 3 (/var):** You create this disk. The recommended size is 4 GB plus 3 times the appliance's RAM allocation.
- **Check the version:** Make sure that the existing appliance is running version 4.3.x with the latest patches applied.
- **Remove VMware Snapshots:** Before copying Disk 2, make sure to remove all VMware snapshots so that the `/vastorage` disk has the correct disk file and latest configuration settings.
- **Filr Database User Name Changed:** If the earlier Filr database was configured with an user name other than '`filr`', the upgrade fails. Ensure to reconfigure the earlier Filr appliance with Filr database user name as '`filr`' before performing upgrade.
- **If the appliance has two network adapters:** You should manually add them after upgrading the appliance.

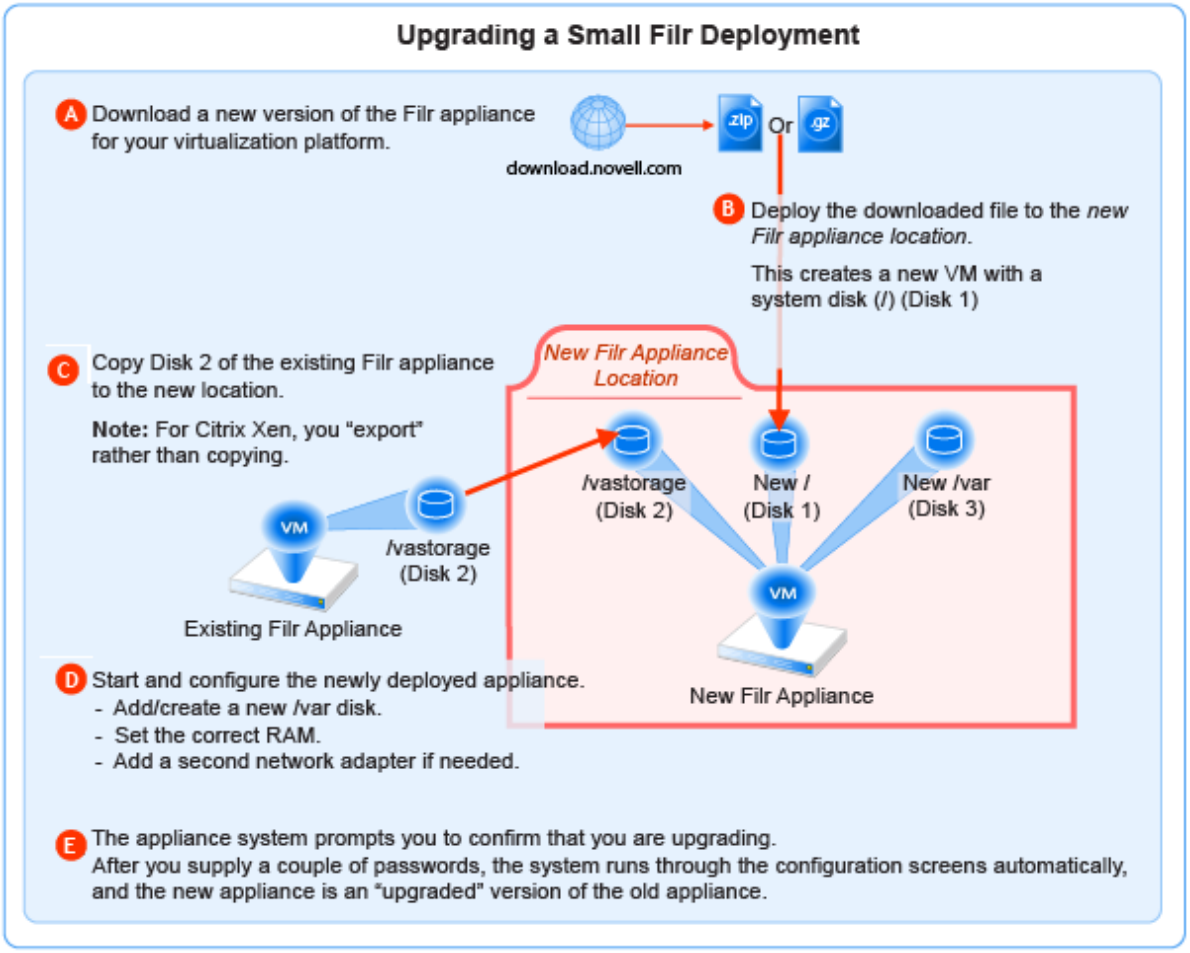
After ensuring that you have met the prerequisites and cautions above, complete the instructions in the following sections in order.

- "Small Filr Upgrade Process Overview" on page 121
- "Downloading and Preparing Software" on page 121
- "Copying Each Appliance's /vastorage Disk (Disk 2)" on page 122
- "Upgrading the VMs" on page 123
- "Deploying the Upgraded Filr VM" on page 131
- "Performing Filr Post-Upgrade Tasks" on page 132

Small Filr Upgrade Process Overview

If you have upgraded a small Filr deployment before, the following reminder might be all you need.

Figure 10-2 *Overview of the Small Filr Appliance Upgrade Process*



Downloading and Preparing Software

Download and prepare the software for your virtualization platform as described in the following sections:

VMWare

1 Download the Filr appliance software to your management workstation.

IMPORTANT: Registration with OpenText is required to receive an email with a software-download link.

---

2 Extract the `.ova.zip` file on your management workstation until a `Filr-`*`version`* folder appears.

3 Launch VMware and navigate to the datastore where you plan to host the upgraded VM.

4 Create a folder for the new appliance with a name that is easily associated with (but not the same as) the VM name of the appliance being upgraded.

Hyper-V

1 Log in to the Hyper-V host server either locally or from a remote workstation using Remote Desktop.

2 Download the Filr appliance software to the location where you plan to host your upgraded VMs.

IMPORTANT: Registration with OpenText is required to receive an email with a software-download link.

---

3 Extract the `.vhdx.zip` file in the directory where you downloaded it until an `Filr-`*`version`*`.vhdx archive file` appears.

4 Create a directory for the new appliance with a name that is easily associated with, but not the same as the VM name of the appliance being upgraded.

5 Move the *`Filr-version`*`.vhdx` archive file to the folder you just created.

Xen

1 Log in to the Xen VM host server either locally or from a remote workstation.

If you are connecting from a remote Linux workstation, use the following command:

```
ssh -X root@host_ip_address
```

The -X in the command in required for the GUI installation program upon which the steps in this section are based.

2 Download the Filr appliance software to the Xen VM host server in the location where you plan to host your upgraded VM.

IMPORTANT: Registration with OpenText is required to receive an email with a download link.

Citrix Xen

1 On a workstation with Citrix XenCenter installed, download the Filr appliance software.

IMPORTANT: Registration with OpenText is required to receive an email with a download link.

---

2 Extract `.xvz` file on your management workstation until a *`Filr-version`* folder appears.

Copying Each Appliance's /vastorage Disk (Disk 2)

IMPORTANT: ◆VMware requires shutting down an appliance before copying a disk.

This means that Filr services will be down while disk copying takes place.

- On Citrix Xen you “export” rather than copying Disk 2.

---

1 Using the tools provided by your hypervisor, copy the /vastorage (second disk) to its associated folder or directory that you created for your upgraded appliances in “Downloading and Preparing Software” on page 121.

Upgrading the VMs

- “Shutting Down the Appliance” on page 123
- “Upgrading a Filr VMware VM” on page 123
- “Upgrading a Filr Hyper-V VM” on page 126
- “Upgrading and Deploying a Filr Xen VM” on page 127
- “Upgrading Citrix Xen VMs” on page 129

Shutting Down the Appliance

1 Shut down the Filr appliance using the Port 9443 Appliance Console.

2 Continue with the instructions for your VM platform:

- Upgrading a Filr VMware VM
- Upgrading a Filr Hyper-V VM
- Upgrading and Deploying a Filr Xen VM
- Upgrading Citrix Xen VMs

Upgrading a Filr VMware VM

Complete the steps in Table 10-5.

Table 10-5 *Upgrading the Filr VMware VM*

Page, Dialog, or Option	Do This
	1 - Launching the Web browser. 1. On a Web browser, enter the URL for the VMware server and login with the root credentials.

Page, Dialog, or Option	Do This
	2 - Deploying the OVA Template and naming the VM.
	1. Right-click on the **Virtual Machines** and click **Create/register VM**. 2. Select **Deploy a virtual machine from an OVA** file, then click **Next**. 3. Name the appliance with the same name of the folder that you created for this upgraded appliance in Step 4 on page 122. 4. Upload the **ova** and **vmdk** files that you downloaded and extracted in Step 4 on page 122. 5. Click **Next**. 6. Choose the datastore and folder were you copied the appliance's Disk 2. 7. Click **Next** to accept the default for the disk format. 8. Do not select **Power on after deployment**. 9. Click **Finish**. The boot disk is created and the appliance is deployed as specified to this point.
	3 - Editing the VM settings.
vSphere Client	1. In the vSphere Client, right-click the VM and select **Edit Settings**. The Virtual Machine Properties dialog displays.
Virtual Machine Properties	1. Set the **Memory** and **CPU** settings to match the appliance you are replacing, or increase them as planned.
	4 - Configuring Disk 2 (/vastorage)
Virtual Machine Properties	1. Click **Add**.
Add Hardware	1. Select **Hard Disk**, click **Next** and select **Use an existing Virtual disk**. 2. Click **Next > Browse**, then navigate to and select the copy of disk 2 that you made for this appliance. 3. Click **Next > Next > Finish**.
	5 - Adding and Configuring Disk 3 (/var)
Virtual Machine Properties	1. Click **Add**.

Page, Dialog, or Option	Do This
Add Hardware	1. Select **Hard Disk**. 2. Click **Next > Next**. 3. Adjust the **Disk Size** to the same size as disk 3 (/var) on the appliance you are replacing. 4. Under **Disk Provisioning**, select either: ◆ **Thick Provision Eager Zeroed** or ◆ **Support clustering features such as Fault Tolerance** Depending on the VMware version that you are running. 5. Under **Location**, select **Specify a datastore or Datastore cluster** 6. Click **Browse**. 7. Select the datastore and folder for this appliance. 8. Click **OK**. 9. Click **Next**. 10. Under the **Virtual Device Node** section, select **SCSI**. **NOTE:** Ensure that the SCSI controller number is same as what you had used during installing Filr. 11. Click **Next**. 12. Click **Finish**. 13. If you need to add network adapters, continue with 6 - (Optional) Adding a Network Adapter. Otherwise, click **OK** and skip to continue with "Deploying the Upgraded Filr VM" on page 131.
	6 - (Optional) Adding a Network Adapter You can add a network adapter if your Filr deployment accesses a separate network for one or more of the following reasons: ◆ Appliance administration. ◆ Security of Memcached. **IMPORTANT:** Bonding or teaming NICs is not supported with Filr.
Virtual Machine Properties	1. Click **Add**.
Add Hardware	1. Select **Ethernet Adapter**. 2. Click **Next**. 3. Under **Network Connection**, select the secondary network associated with the Filr installation. 4. Click **Next > Finish > OK**.
vSphere Client	1. Continue with "Deploying the Upgraded Filr VM" on page 131.

Upgrading a Filr Hyper-V VM

Complete the steps in Table 10-6.

Table 10-6 *Upgrading a Filr Hyper-V VM*

Page, Dialog, or Option	Do This
	1 - Open Hyper-V Manager.
Hyper-V Host Server	1. Open the Hyper-V Manager.
	2 - Create a new VM.
Hyper-V Manager	1. In the left pane, right-click the server where you have planned to create the new virtual machine, then click **New** > **Virtual Machine**. The New Virtual Machine Wizard displays. 2. Click **Next**.
Specify Name and Location	1. Name the appliance with the name of the directory that you created for it in Step 4 on page 122. 2. Click **Next**.
Specify Generation	1. Make sure that **Generation 1** is selected. 2. Click **Next**.
	3 - Specify memory
Assign Memory	1. In the **Startup RAM** field, specify the same amount of memory (in MB) of the appliance that you are replacing, or increase the memory as planned. 2. Click **Next**.
	4 - Assign network adapter
Configure Networking	1. On the Configure Networking page, select the networking card for this VM. 2. Click **Next**.
	6 - Identify the system disk
Connect Virtual Hard Disk	1. Select **Use an existing virtual hard disk**. 2. Browse to and select the `.vhd` file in the folder you created for this appliance. 3. Click **Open**. 4. Click **Next**.
Summary	1. Click **Finish**. The VM is created and appears in the list of Virtual Machines.
	7 - Specify processors

Page, Dialog, or Option	Do This
Hyper-V Manager	1. In Hyper-V Manager, right-click the VM that you just created. 2. Click **Settings**.
Processor	1. Click **Processor**. 2. In the **Number of virtual processors** field, specify the number of processors for the VM. 3. Click **Next**.
	8 - Use existing copy of hard Disk 2 (/vastorage).
Settings for *VM* on *Host Server*	1. Add the copy you made of disk 2 to this VM. 2. When you have added the disk, review the VM summary information and click **Finish**.
	9 - Add hard Disk 3 (/var).
Hyper-V Manager	1. In Hyper-V Manager, right-click the VM that you just created. 2. Click **Settings**. 3. Create a new blank virtual disk the same size as disk 3 on the appliance you are upgrading.
Summary	1. Review the summary information. 2. Click **Finish > OK**
	10 - (Optional) Add a Network Adapter 1. If the appliance you are upgrading has a secondary network adapter, add that now.
Hyper-V Manager	**11 - Deploy the upgraded appliance** 1. Continue with "Deploying the Upgraded Filr VM" on page 131.

Upgrading and Deploying a Filr Xen VM

Complete the steps in Table 10-7.

Table 10-7 *Upgrading and Deploying a Filr Xen VM*

Page, Dialog, or Option	Do This
	1 - Launch the installer.
Terminal prompt on Xen VM Host Server	1. Run the following command to launch the GUI configuration menu: `virt-manager` **NOTE:** The `vm-install` command is deprecated from SLES 12 releases.

Page, Dialog, or Option	Do This
Create a new virtual machine	1. Click **File** > **New Virtual Machine**. The **Create a new virtual machine** wizard is displayed. 2. Select **Import existing disk image**. 3. Click **Forward**.
Storage path and Operating System	1. Browse and select the existing disk image. 2. Select **SUSE Linux Enterprise Server 12 SP4**. 3. Click **Forward**.
Choose Memory and CPU settings	1. Set the amount of memory (in MB) to match that of the VM you are upgrading. 2. Specify the **CPUs** to match the number of the VM you are upgrading. 3. Click **Forward**.
	2 - Name the VM.
Name of Virtual Machine	1. Specify the name of the appliance. 2. Select **Customize configuration before install**. 3. Click **Finish**.
	3 - Configure Disk 2 (/vastorage)
Hardware	1. Click **Add Hardware** at the bottom left of the screen. 2. Select the option **Select or create custom storage**. 3. Navigate to the contents of the folder for the appliance you are creating. 4. Select the `.qcow2` file. 5. Click **Open** > **Finish**.
	4- Configure Disk 3 (/var)
	1. Click **Add Hardware** at the bottom left of the screen. 2. Select the option **Select or create custom storage**. 3. Navigate to the contents of the folder for the appliance you are creating. 4. Select the `.qcow2` file. 5. Click **Open** > **Finish**.
	5 - (Optional) Add a Network Adapter You can add a network adapter if your Filr deployment accesses a separate network for one or more of the following reasons: ◆ Appliance administration. ◆ Security of Memcached. **IMPORTANT:** Bonding or teaming NICs is not supported with Filr.

Page, Dialog, or Option	Do This
Summary	1. Click **Network Adapters**.
Network Adapters	1. Click **New**.
Virtual Network Adapter	1. Specify the settings for the adapter. 2. Click **Apply**.
Network Adapters	1. Click **Apply**.
Summary	1. Click **OK**. The virtual machine is created, the appliance starts, and the configuration process begins.
Console	**6 - Deploy the Appliance** 1. Access the appliance's console. 2. When prompted, enter the root and vaadmin passwords for the appliance. The upgrade process proceeds automatically. 3. When the appliance displays the final screen in the console window, open your management browser and log in to the appliance on port 9443 as the vaadmin user.
Port 9443 Admin Console	1. Check the following: ◆ **Filr:** ◆ Click the Filr configuration icon. ◆ Ensure that all of the settings are in place as expected. ◆ If the configuration wizard displays, there was a problem with the configuration. ◆ Resolve the configuration issues, then click Finish to reconfigure the system. Common configuration issues include: ◆ If your system is not using DNS, the most likely problem is unresolvable DNS names and missing /etc/hosts entries. ◆ If the appliance doesn't have access to the database, ensure that all of the settings are as expected. 2. When the appliance is running, continue with "Performing Filr Post-Upgrade Tasks."

Upgrading Citrix Xen VMs

Complete the steps in Table 10-8.

Table 10-8 *Upgrading a Citrix Xen VM*

Page, Dialog, or Option	Do This
	1 - Launch XenCenter.
Management Workstation	1. Start XenCenter.
XenCenter	1. Connect to the Citrix XenServer where you planned to deploy Filr. 2. Right-click the server and select **Import**.
	2 - Import the system disk
Locate the File you want to import	1. Browse to and select the `.xva` file on your management workstation. 2. Click **Open**. 3. Click **Next**.
Select the location where the imported VM will be placed	1. Select the XenServer. 2. Click **Next**.
Select target storage	1. Select the storage repository for the VM that you used in Step 2 on page 122. 2. Click **Import**.
	3 - Select the network adapter
Select network to connect VM	1. Select the virtual network adapter. 2. Click **Next**.
Review the import settings	1. Deselect **Start VM(s) after import**. 2. Click **Finish**. **IMPORTANT:** Depending on network latency and other factors, it can take a while to import the system disk.
	4 - Specify Memory
	1. If you need to adjust the memory to the amount of memory, select the newly created VM in the left pane. 2. Click the **Memory** tab. 3. Click **Edit**, change the setting, and click **OK**.
	5 - Specify Processors
	1. If you need to adjust the CPUs, right-click the newly created VM in the left pane. 2. Select **Properties**. 3. Click **CPU**, change the setting, and click **OK**.
	6 - Link to Disk 2 (/vastorage)
	1. With the newly created VM selected in the left pane, add the copy of disk 2 for this appliance.
	8 - Add Disk 3 (/var)

Page, Dialog, or Option	Do This
Virtual Disks	1. Click **Add...**.
Add Virtual Disk	1. Type a disk name that reflects the appliance name and that this is disk 3. For example, Filr-1-disk-3. 2. Change the **Size** field value to match that of the appliance you are replacing. 3. Click **Add**.
	9 - (Optional) Add a Network Adapter You can add a network adapter if your Filr deployment accesses a separate network for one or more of the following reasons: ◆ Appliance administration. ◆ Security of Memcached. **IMPORTANT:** Bonding or teaming NICs is not supported with Filr.
	1. With the newly created VM selected in the left pane, click the **Networking** tab. 2. Select the secondary network associated with the Filr installation..
XenCenter	1. Continue with "Deploying the Upgraded Filr VM" on page 131.

Deploying the Upgraded Filr VM

1. Power on the appliance.
2. Access the appliance's console.
3. When prompted, enter the root and vaadmin passwords for the appliance.

   The upgrade process proceeds automatically.
4. When the appliance displays the final screen in the console window, open your management browser and log in to the appliance on port 9443 as the vaadmin user.
5. Check the following:
   - **PosgtgreSQL :**
     - Click the phpPgAdmin icon.
     - Verify that the database is populated as expected.
   - **Filr:**
     - Click the Filr configuration icon.
     - Ensure that all of the settings are in place as expected.
     - If the configuration wizard displays, there was a problem with the configuration.
     - Resolve the configuration issues, then click Finish to reconfigure the system.

Common configuration issues include:

- If your system is not using DNS, the most likely problem is unresolvable DNS names and missing /etc/hosts entries.
- If the appliance doesn't have access to the database, ensure that all of the settings are as expected.

6 When the appliance is running, continue with "Performing Post-Upgrade Tasks."

Performing Filr Post-Upgrade Tasks

After upgrading to a new version of Filr, you should perform the following tasks to ensure a fully functional Filr system:

- "Install Your New Filr License" on page 132
- "Java Heap" on page 132

Install Your New Filr License

Upgraded Filr appliances have a 60-day evaluation license installed. The evaluation license is expired in most of the cases because it considers the day of deployment as the day when it was installed with the earlier version.

To prevent a service interruption, you must install your new license by following the instructions in "Installing/Updating the Filr License" in the *OpenText Filr 23.4: Administrative UI Reference*.

Java Heap

For optimal performance of Filr appliance, the minimum Java heap space should be 12 GB. After upgrading the appliance, the Java heap space is overwritten with the value that was set for the earlier Filr appliance. If new value is less, then ensure to update it to 12 GB or greater.

11 Updating Filr through Online Update Channel

Filr 23.4 is available as an online update to Filr 5.0, PostgreSQL 2.0, and Filr Search 5.0 appliances or later. Note the following:

- **No Separate Hypervisor-specific Downloads:** The virtual machine configurations are not impacted.

For information about using the Online Update feature, see "Using the Online Update dialog" in the *OpenText Filr 23.4: Administrative UI Reference*.

IMPORTANT: ◆Ensure that the required server certificates are valid and not expired. If the certificates are expired, update them accordingly.

- We recommend that you schedule Online updates only for updating non-interactive patches on Filr Appliance.
- If you change the IP address of the proxy server that is configured on the Filr Appliances, then you must update the proxy server configuration on the Filr Appliances before registering and applying the online updates:
  1. On the Filr Appliance, use the Yast Proxy Management tool to reconfigure the proxy server.
  2. Launch a new terminal.
  3. Run the following command to restart the datamodel services:

     ```
     rcvabase-datamodel restart
     ```
  4. Run the following command to restart the jetty services:

     ```
     rcvabase-jetty restart
     ```

Review the following sections:

- "Updating an All-in-One (Small) Deployment" on page 133
- "Updating a Large Filr Deployment" on page 134

Updating an All-in-One (Small) Deployment

1. Ensure that the version of the Filr appliance is 5.0 or later.
2. Log in to the Filr Appliance Configuration Console (`https://appliance_ip_or_dns:9443`) as vaadmin.
3. Click **Online Update**.
4. In the Patches drop-down option, select **Needed Patches** and ensure that the latest patch update is listed.
5. Click **Update Now**.

6 Click **OK**.

A progress bar displays the status of the update. After the update completes, select the **Installed Patches** option in the drop-down and verify that the latest patch is listed there.

Updating a Large Filr Deployment

- "Recommended Before Updating to Filr 23.4" on page 134

Recommended Before Updating to Filr 23.4

- Stop the Filr service
- Update the Filr Search appliances with latest patches
- Update the PostgreSQL appliance with latest patches

Perform the following steps on every Filr appliance in the cluster:

1 Ensure that the version of the Filr appliance is 5.0 or later.

2 Log in to the Filr Appliance Configuration Console (`https://appliance_ip_or_dns:9443`) as vaadmin.

3 Click **Online Update**.

4 In the Patches drop-down option, select **Needed Patches** and ensure that the Enable update to Filr 23.4 is listed.

5 Click **Update Now**.

6 Click **OK**.

A progress bar displays the status of the update. After the update completes, select the **Installed Patches** option in the drop-down and verify that the latest patch is listed there.

12 Setting Up Filr Services

Complete the following steps to prepare your Filr site and make it available to users.

1. Using the Port 9443 > License dialog, install the same valid license on each Filr appliance in your system.
2. Change any Filr infrastructure configuration settings that require restarting Filr.

   This prevents interrupting Filr services after users begin accessing Filr services.

Notifications	1. (Optional) Using the Port 9443 > Configuration > Outbound E-mail dialog, configure your system for integration with an external email system. 2. Using the Port 8443 > System > E-Mail dialog, review the default notification settings and make any required configuration changes.

Networking Support	1. Review the settings in the Port 9443 > Firewall dialog and make sure that the port and firewall settings on your network are configured to support Filr services. 2. If you are enabling port redirection so that users don't need to include :8443 in Filr requests, configure that now. **Path:** Port 9443 Appliance Console > **Configuration > Network** 3. If you are using NetIQ Access Manager. **Path:** Port 9443 Appliance Console > **Configuration > Reverse Proxy**

3. Add users and groups to your Filr site and set up the LDAP synchronization processes.

Users and Groups (LDAP and Non)	1. Configure your Filr system to connect to an existing LDAP source, such as eDirectory or Active Directory, to control user access to the system. **Path:** Port 8443 Filr Admin Console > **System > LDAP** 2. Manually create any non-LDAP users and groups that need access to Filr services. For more information, see "Filr Admin Created Users and Groups:" in *OpenText Filr 23.4: Understanding How Filr Works* and "the New User button" in the *OpenText Filr 23.4: Administrative UI Reference*.
LDAP Synchronization	1. Configure the Filr system to synchronize with your LDAP servers. For assistance, see "LDAP Servers and Synchronization" in the *OpenText Filr 23.4: Administrative UI Reference*.

4 If you want users to be able to share through Filr, you must enable sharing for the Filr system.

System-Level Sharing Settings	1. Configure the system-level share settings. For more information about allowing users to share documents within Filr, see "Managing Sharing, License Terms, and Comments" in the *OpenText Filr 23.4: Administrative UI Reference*.

5 if you want users to be able to upload personal files and folders directly to the Filr site, you must enable personal storage.

Personal Storage	1. Configure Personal Storage. For more information about allowing users to share documents within Filr, see "Enabling Personal Storage for Users and Groups" in the *OpenText Filr 23.4: Administrative UI Reference*.

For more information about personal storage, as well as how personal storage relates to users' Home folders, see "Enabling Personal Storage for Users and Groups" in the *OpenText Filr 23.4: Administrative UI Reference*.

6 Configure Home Net Folder servers.

Net Folder Servers	1. Configure Home Net Folder servers. For more information, see "Creating and Managing Net Folder Servers" in the *OpenText Filr 23.4: Administrative UI Reference*.

If the search context of your LDAP synchronization contains an OES or Windows server that has a Home folder attribute associated with at least one user, a Net Folder Server is ready to be configured immediately after running the LDAP synchronization process. You need to consider the amount of data in users' Home folder directories when performing an LDAP synchronization.

The following points are critical to successful Home NF Server creation and the synchronization of access privileges.

- **Import Both Groups and Users:** If you import only LDAP users and not the groups they belong to, then file system group permissions won't map to Filr group permissions when Net Folders are created.
- **Register User Profiles Automatically (default):** If you deselect this option, then users won't be created until after they log in. This causes the following issues:
  - You must wait until users log in to their home folders before you can configure the proxy users and passwords for any HOME Net Folder Servers.
  - Net Folder access permissions that key off user-based file system permissions will not be set or updated during Net Folder Synchronizations.
- **Register Group Profiles Automatically (default):** If you deselect this option, groups will not be created and Net Folder access permissions that key off group-based file system permissions will not be set or updated during Net Folder Synchronizations.

7 Configure Net Folder Servers.

Net Folder Servers Home Folder Net Folder Servers Net Folder Server Synchronization	1. Configure the other Net Folder servers. For more information, see "Creating and Managing Net Folder Servers" in the *OpenText Filr 23.4: Administrative UI Reference*.

8 Configure Net Folders.

Net Folders Net Folder Sharing Settings Net Folder Global Settings Net Folder Synchronization	1. Configure the Net Folders settings. For more information, see "Managing Net Folders" in the *OpenText Filr 23.4: Administrative UI Reference*.

Net Folders in Filr provide access to files on your corporate OES, Windows, file servers by synchronizing file metadata. In essence, a Net Folder is simply a pointer or a reference to a specific folder on a specific file server.

Filr can be configured to index the content of Net Folders to make the content searchable.

For more information about Net Folders, see "Managing Net Folders" the *OpenText Filr 23.4: Administrative UI Reference*.

9 Enable additional Filr Users for Administrative Access.

Administrative Access	1. Configure users for administrative access to Filr. For more information, see "Assigning and Managing Port 8443 Direct Administrators" in the *OpenText Filr 23.4: Administrative UI Reference*.

10 (Optional) Allow access to the Filr site through NetIQ Access Manager.

For more information about using NetIQ Access Manager with Filr, see Chapter A, "Access Manager (NAM) and Filr Integration," on page 151.

IMPORTANT: When you use NetIQ Access Manager with Filr, external users cannot access your Filr site. This means that the following features are not functional:

- Users are not able to share with external users.
- Users cannot make items accessible to the public.

  This means that public users cannot access the Filr site as the Guest user. For more information about the Guest user, see "Guest Users:" in *OpenText Filr 23.4: Understanding How Filr Works*.

For more information about external users in Filr, see "External, Self-Provisioned Users:" in *OpenText Filr 23.4: Understanding How Filr Works*.

11 Configure mobile device access to the Filr site, as described in "Mobile Device Access—Default Settings" in the *OpenText Filr 23.4: Administrative UI Reference*.

12 Configure the Filr desktop application to access files from the Filr site.

For more information about configuring the Filr desktop application.

IMPORTANT: For optimal performance of the Filr system when using the Filr desktop application, consider the following:

- Users should not configure the Filr desktop application to synchronize more than 1,000 total files, or to synchronize individual files that are larger than 1 GB to their workstations. For information about how users can configure the Filr desktop application to synchronize files to their workstations, see the *OpenText Filr 23.2 Desktop Application Guide for Windows* and the *OpenText Filr 23.2 Desktop Application Guide for Mac*.

13 Configure Filr to support WebDAV on a Windows 7 environment, as described in "WebDAV Support" in the *OpenText Filr 23.4: Maintenance Best Practices Guide*.

14 If your Filr site needs to support multiple languages, configure the site as described in "UI Language" in the *OpenText Filr 23.4: Administrative UI Reference*.

15 After you have completed all of the topics in this list that are relevant to your Filr environment, you can invite users to use the Filr site.

13 Setting Up Sharing

Before users can share, they must have sharing enabled for them at the Filr system level, either individually or as a member of a group.

After that, sharing of My Files is enabled by default, but sharing in Net Folders requires additional steps.

Use the following sections as a guide through the process of setting up sharing.

- "Enabling Users to Share" on page 139
- "Do Not Enable Sharing for All Internal Users and All External Users" on page 145
- "System-Level Sharing Must Be Configured First" on page 145
- "My Files Sharing Is Automatic" on page 146
- "Net Folder Sharing Must Be Explicitly Allowed At Two Levels" on page 146

Enabling Users to Share

- "Best Practices for Setting Up Sharing" on page 139
- "General Order for Setting Up Sharing" on page 140
- "Enabling Sharing for Specific Net Folders" on page 144
- "Restricting Sharing Files by Group of Users" on page 144

Best Practices for Setting Up Sharing

- **Enable Sharing for the Filr System:** You must enable the sharing feature before any sharing can take place on the Filr system.

  As a best practice, enable sharing in an unrestricted way for those users and groups that will be allowed to share.

- **If Needed, Restrict My Files Sharing:** Enabling sharing automatically lets all users share files in their My Files area, including in their Home folder and in personal storage.

  You can restrict My Files sharing on a per-user basis if desired.

- **Carefully Restrict Net Folder Sharing:** Net Folder sharing must be explicitly allowed for each Net Folder.

  IMPORTANT: Make sure that only those who need to share a Net Folder's contents are granted sharing rights on that Net Folder.

  For example, Group A is granted rights to share files in Net Folder A. User A (a member of Group A) then shares a file with User B (a member of Group B). Because the file contains sensitive information, User A doesn't grant User B permission to reshare the file.

As long as User B doesn't have rights to share files in Net Folder A, there is no problem.

However, if Group B also has permission to share Net Folder A's files, then User B can reshare the file even though User A assumed otherwise.

General Order for Setting Up Sharing

When you set up sharing for your Filr site, complete the necessary steps in the following order:

1. Set up sharing for the entire Filr site (as described in "Enabling Sharing in Filr" on page 140).
2. Configure sharing for individual users (as described in "Restricting Personal Storage Sharing" on page 143).

   After you have enabled sharing for the entire Filr system, you can fine-tune share rights throughout the site on the user level.

   For example, if you want only a few groups of users to be allowed to share with external users, you first need to enable sharing to external users at the site level. After you have enabled it at the site level, you can then remove this ability from the users who you do not want to have this ability.
3. Set up sharing for specific Net Folders (as described in "Enabling Sharing for Specific Net Folders" on page 144).

   Users who are given share rights on a specific Net Folder are able to share files within that Net Folder that they have rights to at least view on the file system.

Enabling Sharing in Filr

After you set up sharing for the entire Filr site, all users by default are granted rights to share files in the My Files area (this includes files in the Home folder and files in personal storage), with the site-wide access rights that you specify. If you want only certain users to be allowed to share files from their My Files area, you must enable sharing for the entire site as described in this section. Then you must restrict sharing privileges at the user level, as described in "Restricting Personal Storage Sharing" on page 143.

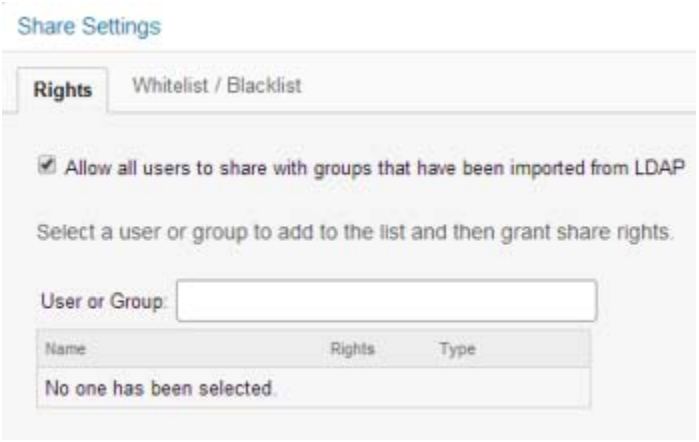
1. Log in to the Filr site as the Filr administrator.
   - **1a** Launch a web browser.
   - **1b** Specify one of the following URLs, depending on whether you are using a secure SSL connection:

     `http://Filr_hostname:8080`
     `https://Filr_hostname:8443`

     Replace *`Filr_hostname`* with the hostname or fully qualified domain name of the Filr server that you have set up in DNS.

     Depending on how you have configured your Filr system, you might not be required to enter the port number in the URL. If you are using NetIQ Access Manager, the Filr login screen is not used.
2. Click the **admin** link in the upper-right corner of the page, then click the **Administration Console** icon .
3. Under **System**, click **Share Settings**.

The Share Settings page is displayed.



4 Select **Allow all users to share with groups that have been imported from LDAP** to enable users to share with LDAP groups.

If you select this option, groups that were imported from the LDAP directory are displayed in the **Share with** field when users are sharing an item. All users in the LDAP group then have access to the item that was shared.

Enabling Users and Groups for Net Folder Sharing

1 To enable sharing for all internal users on the Filr site, go to the **User or Group** field, begin typing `All Internal Users`, then select it when it appears in the drop-down list.

or

To enable sharing on a per-user or per-group basis, go to the **Select user/group** field, begin typing the name of the user or group for whom you want to grant share rights, then select the name when it appears in the drop-down list.

The Edit Share Rights dialog box is displayed. Select from the following options:

Re-share items: When users share a file or folder, they can give the users they are sharing with the ability to re-share the file or folder. The user receiving the share can share the file only if that user has been given administrative rights to share the file or folder.

IMPORTANT: When selecting this option, be aware that if one user's access rights to an item are removed, it does not remove the access rights of the user with whom the item was re-shared.

For example, suppose User A shares an item with User B and grants re-share rights. User B then shares the item with User C. If User A revokes User B's access rights to the item, User C continues to have access to the shared item.

Share with Internal users: Allows users to share items with internal users.

Share with "All Internal Users" group: Allows users to perform a mass share to all internal users by sharing with the `All Internal Users` group.

Share with External users: Allows users to share items with users external to the organization.

Users external to the organization receive an email notification with a link to the shared item, and they can then log in to the Filr site.

Share with Public: Allows users to make items publicly available. This means that anyone with the correct URL to the shared item can access the shared item without logging in to the Filr site.

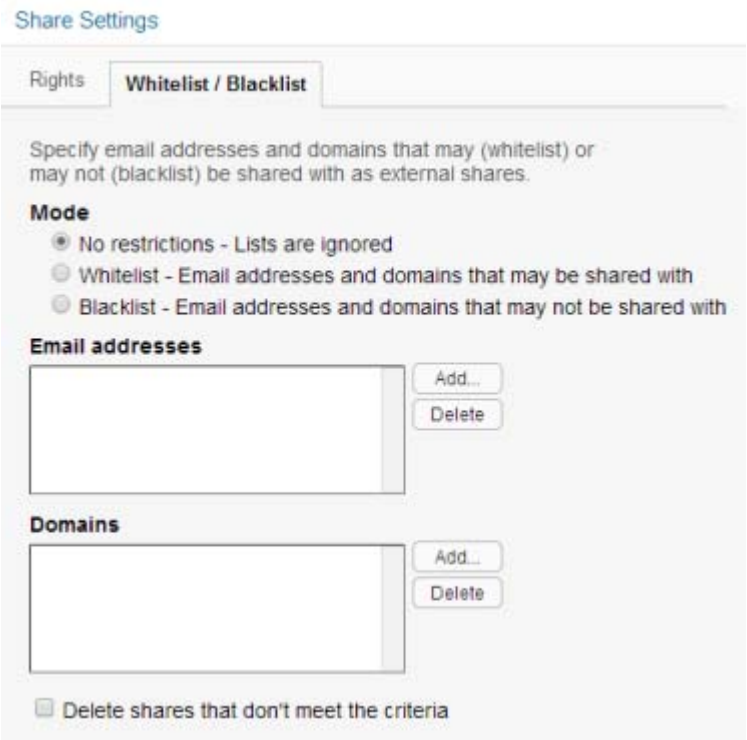
In addition to selecting this option, you also need to enable Guest access to the Filr site if you want to allow users to share items with the public. For information about how to enable Guest access to the Filr site, see

Share using File Link: Allows users to share a link to a file in Filr. Any user with the link can then access the file. However, the file is not displayed in the Public area, so users must have direct access to the link in order to access the file.

NOTE: If you select this option, users can share a link of the Filr file even with email addresses that are listed in the **Blacklist** field.

---

2 (Optional) Click the **Whitelist / Blacklist** tab to configure which email addresses and domains users can share with when sharing externally.



The following options are available when configuring a whitelist or blacklist for sharing:

No restrictions: Select this option to disregard any email addresses or domains that might already exist in the **Email addresses** and **Domains** fields. Selecting this option means that users can share with any email address.

Whitelist: Select this option to allow sharing only with email addresses and domains that have been specified in the **Email addresses** and **Domains** fields.

Email addresses: Click **Add**, specify the email address that you want to add to the whitelist or blacklist, then click **OK**.

Blacklist: Select this option to disallow sharing with any email addresses and domains that have been specified in the **Email addresses** and **Domains** fields.

Repeat this process to add multiple email address.

NOTE: If a user has **Share using File Link** rights, the user can share links of Filr files even with the blacklisted email addresses.

Domains: Click Add, specify the domain that you want to add to the whitelist or blacklist (for example, `yahoo.com`), then click **OK**.

Repeat this process to add multiple domains.

Delete shares that don't meet the criteria: Select this option to delete all existing shares in the Filr system that do not match the criteria you set.

For example, if you selected **Blacklist** and then specified **yahoo.com** in the **Domains** field, selecting this option would delete all Filr shares made to Yahoo email addresses.

3 Click **OK**.

Restricting Personal Storage Sharing

After you have enabled sharing of files for the entire Filr system (as described in "Enabling Sharing in Filr" on page 140), you can restrict shared-access right granting on an individual-user basis.

You cannot grant individual users more rights than are currently defined for the site-wide setting.

To restrict share rights for specific users:

1 Log in to the Filr site as the Filr administrator.

1a Launch a web browser.

1b Specify one of the following URLs, depending on whether you are using a secure SSL connection:

`http://Filr_hostname:8080`
`https://Filr_hostname:8443`

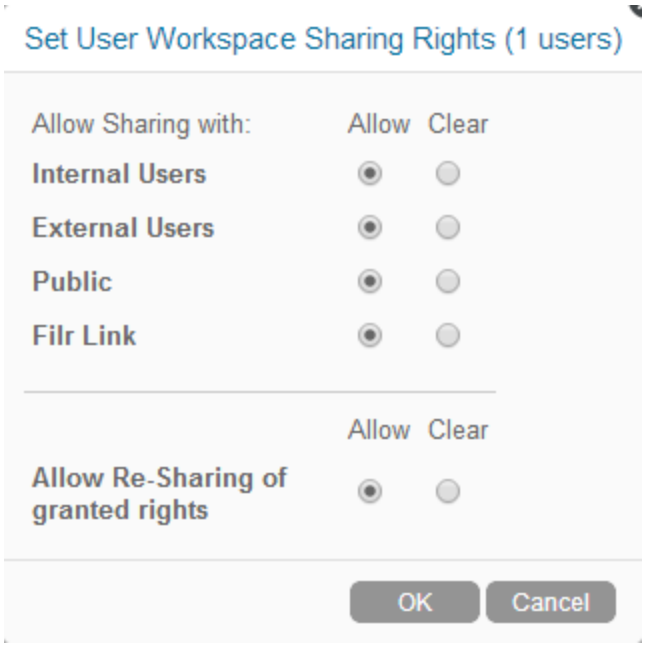
Replace *`Filr_hostname`* with the hostname or fully qualified domain name of the Filr server that you have set up in DNS.

Depending on how you have configured your Filr system, you might not be required to enter the port number in the URL. If you are using NetIQ Access Manager, the Filr login screen is not used.

2 Click the **admin** link in the upper-right corner of the page, then click the **Administration Console** icon .

3 Under **Management**, click **Users**.

4 Select the users whose sharing rights you want to manage, then click **More** > **Workspace Share Rights**.



5 Select the radio button in the **Clear** column next to the sharing right that you want to remove from the user or group, then click **OK**.

or

If you have already removed a share right and you want to add it again, select the radio button in the **Allow** column next to the sharing right that you want to add to the user or group, then click **OK**.

Enabling Sharing for Specific Net Folders

1 Ensure that you have configured sharing as described in "Enabling Sharing in Filr" on page 140.

2 Configure sharing for the Net Folder as described in).

Restricting Sharing Files by Group of Users

You can restrict a group of users from sharing files to others.

1 Stop the Filr service.

```
rcfilr stop
```

2 Add the following two lines to the `/opt/novell/filr/apache-tomcat/webapps/ssf/WEB-INF/classes/config/ssf-ext.properties` file:

Syntax:

- `enable.sharing.exception=true`
- `enable.sharing.exception.list=<GroupName>`

  GroupName is the name of the group that you do not want to have the ability to share the files.

3 Start the Filr service.

```
rcfilr start
```

Do Not Enable Sharing for All Internal Users and All External Users

Prior to the release of Filr 2.0, the documentation stated that enabling sharing for `All Internal Users` and `All External Users` was an acceptable method of enabling sharing on the system.

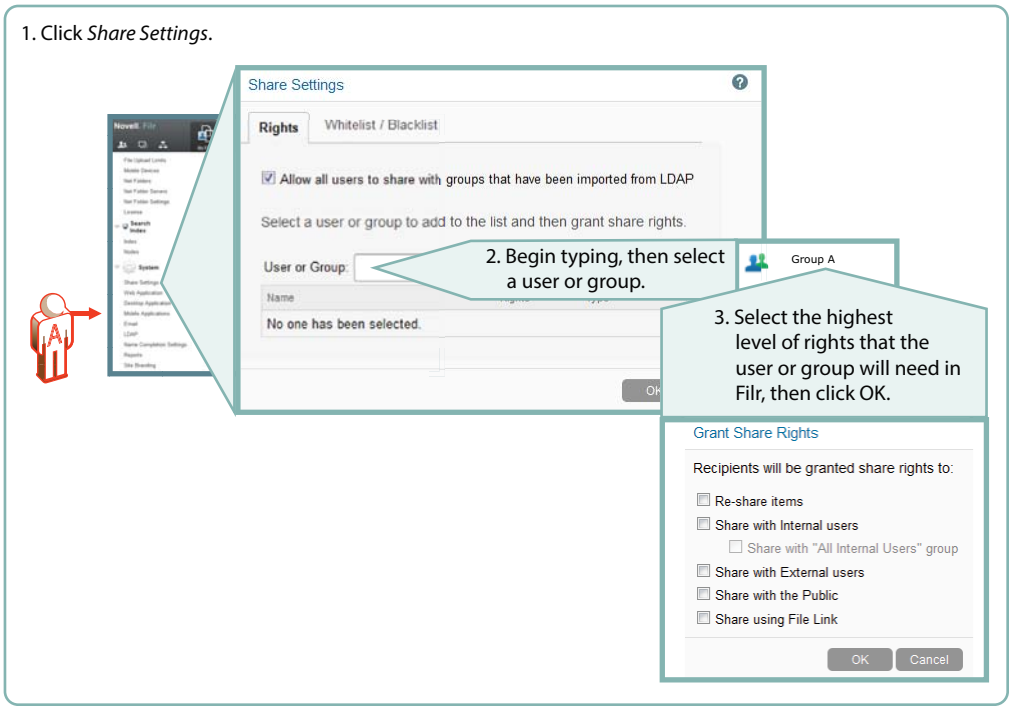
Unfortunately, this shortcut results in significant system overhead and often leads to serious performance degradation.

We strongly recommend that you enabling sharing only for specific users and/or groups, as outlined in the sections that follow.

System-Level Sharing Must Be Configured First

The first step in allowing Filr sharing to take place is to list the users and groups who are allowed to share in the Share Settings dialog. When you add the user or group, you also specify the upper limits of possible sharing rights for them. You can further restrict the rights, but you can't expand them beyond this limit.

Figure 13-1 *Setting Up System-Level Sharing Rights*

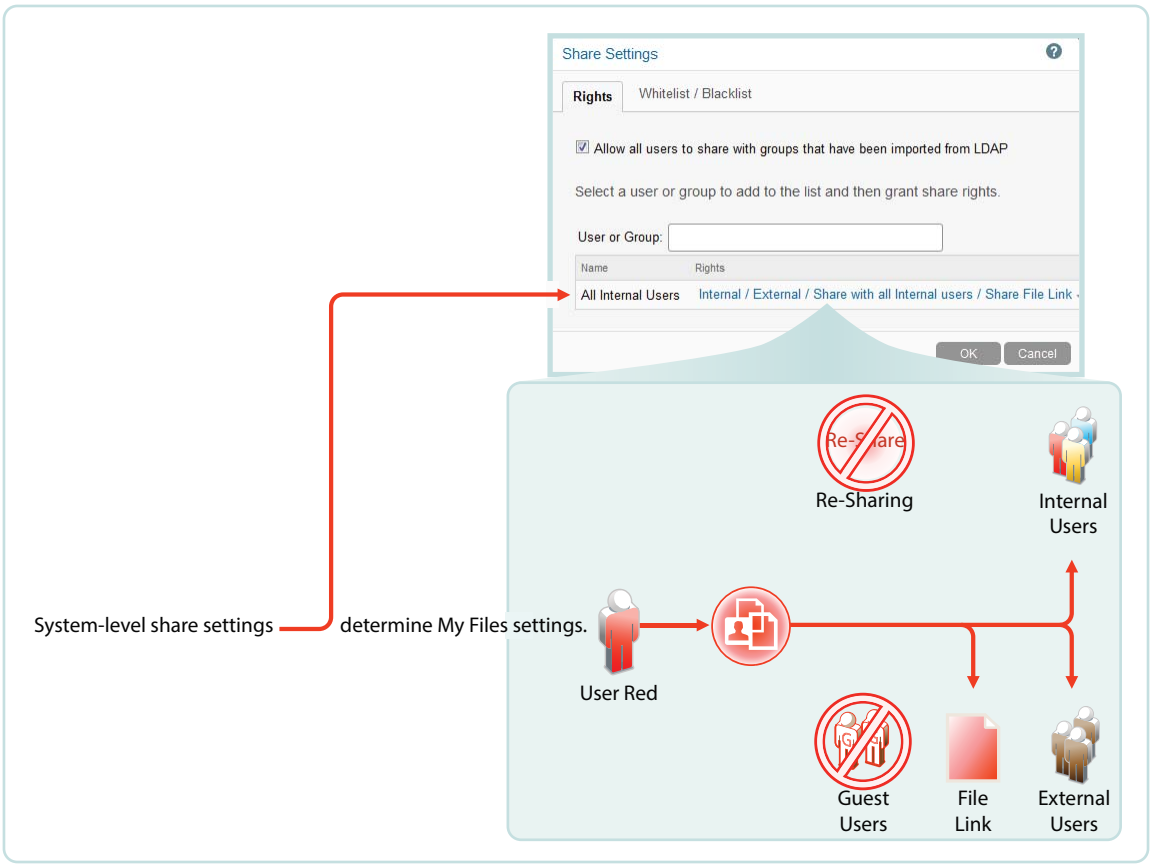


My Files Sharing Is Automatic

After sharing is enabled at the system level for users individually or as members of groups, then if those users have personal storage enabled, they can share their files and folders within the limitations set for the system.

Administrators can disable sharing of files and folders in My Files on an individual user basis.

Figure 13-2 *My Files Share Settings*



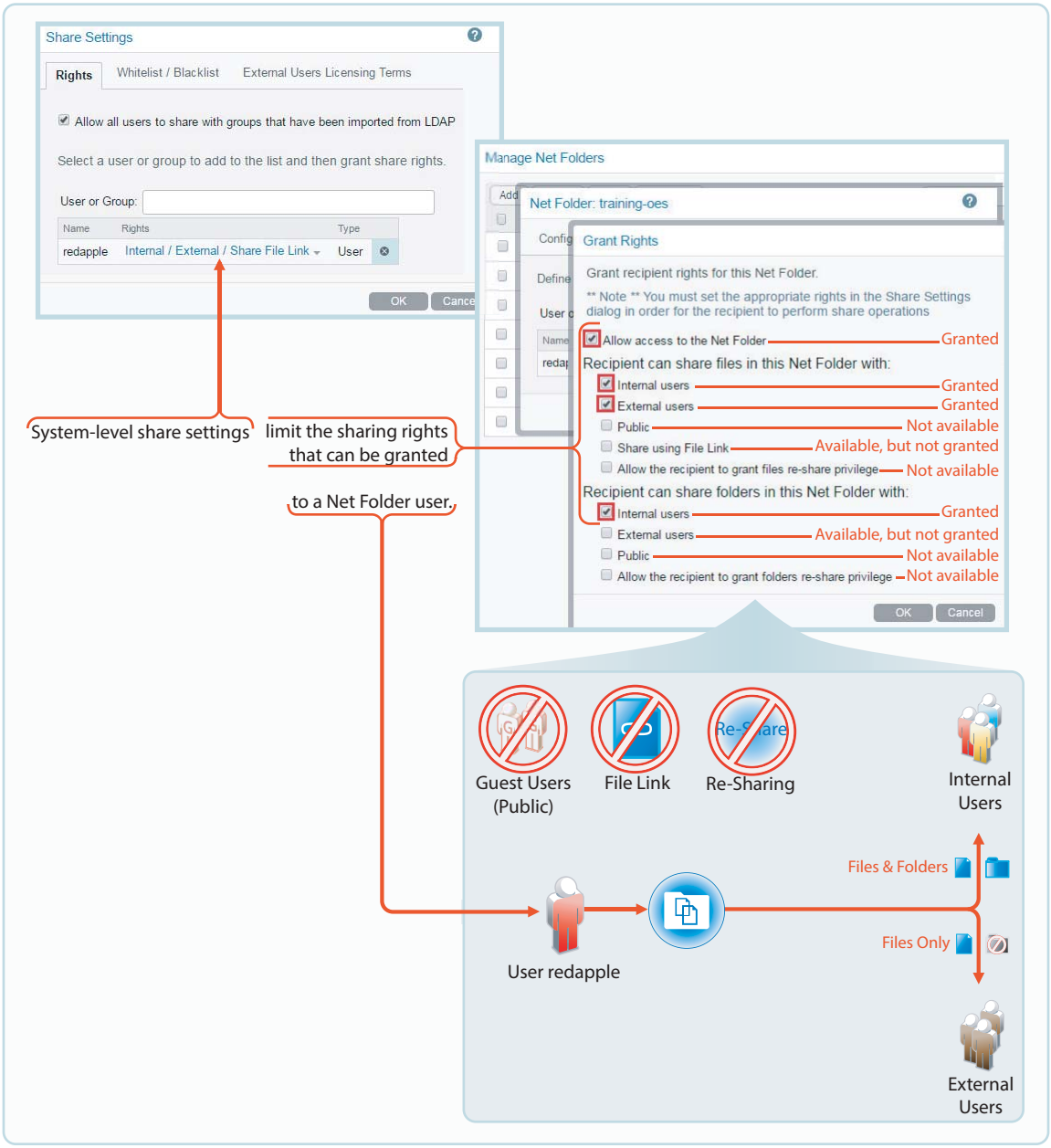
Net Folder Sharing Must Be Explicitly Allowed At Two Levels

Before the users or groups listed in the Share Settings dialog can share files and folders in their assigned Net Folders, they must have sharing enabled on those Net Folders.

When enabling Net Folder access for a user or group, a Filr administrator can only assign up to the maximum sharing rights that are set at the system level.

In Figure 13-3, user red can only be assigned sharing rights that are allowed at the system level.

Figure 13-3 *An Example of Net Folder Sharing*



Appendixes

The following:

- Appendix A, “Access Manager (NAM) and Filr Integration,” on page 151
- Appendix B, “All-in-One (Small) Deployment—Creating,” on page 161
- Appendix C, “Non-Expandable Deployment—Creating,” on page 163
- Appendix D, “SCSI Controller Type—Changing on VMware,” on page 165
- Appendix E, “Troubleshooting Filr,” on page 167
- Appendix F, “Filr Limitations,” on page 171

A Access Manager (NAM) and Filr Integration

You can configure NetIQ Access Manager (NAM) to act as Proxy service for a Filr site. This helps you provide the ease of single sign-on and establish a trusted relationship with the Access Gateway. Using Filr in conjunction with NetIQ Access Manager adds enterprise-level security to your Filr system.

NOTE: Guest users cannot access Filr through NAM.

Review the following sections:

- "Overview" on page 151
- "Configuring Filr Ports" on page 152
- "Downloading and Installing the Filr Authentication Plugin" on page 152
- "Configuring the NAM Identity Server" on page 152
- "Configuring a Reverse-Proxy Single Sign-On Service for Filr" on page 154

Also, for information on configuring NAM with Content Editor, see the "Content Editor With NetIQ Access Manager For Online Edit Feature" on page 81

Overview

To integrate Filr with NAM, you must configure the NetIQ Access Manager Identity Server, the Access Gateway, and configure protected resources for a Filr server.

The integration of Filr with NAM allows both LDAP and non-LDAP (local and external) users to log in to Filr through Web client, Desktop and Mobile clients through NAM.

To integrate Filr with NAM for non-LDAP users, you must create new classes, methods, and contracts in NAM. For LDAP users, you can either use the predefined NAM classes, methods, and contracts, or create new ones. If you have both LDAP and non-LDAP users, then you can create a new class, method, and contract to support the authentication for both LDAP and non-LDAP users.

Filr introduces a new authentication plugin to enable both LDAP and non-LDAP (local and external) users to log in to Filr through NAM. To download and install the authentication plugin, see "Downloading and Installing the Filr Authentication Plugin" on page 152.

For information about NetIQ Access Manager, see the Access Manager Documentation website.

Configuring Filr Ports

Use the following port configuration when NetIQ Access Manager is fronting your Filr system:

- HTTP Port: 80
- Secure HTTP Port: 443

You must configure the port on the **Reverse Proxy** and **Network** page of the Port 9443 Appliance Console. For more information, see "Reverse Proxy Configuration Settings" and "Network Configuration" in the *OpenText Filr 23.4: Administrative UI Reference*.

Downloading and Installing the Filr Authentication Plugin

To enable Filr users to access the Filr services through NetIQ Access Manager (NAM), Filr provides an authentication plugin that you must download and install on the NAM server that you want to use as a proxy server.

To download and install the plugin:

1. Open a browser on your administrative workstation and access the Port 9443 Appliance Console on the first Filr appliance using the following URL:

   `https://Filr_IP_Address:9443`

   Where *Filr_IP_Address* is the IP address of the Filr appliance.
2. Click the **Configuration**  and then click **Reverse Proxy**.
3. In the NetIQ Access Manager Integration section, click **Filr Plugin for NAM** to download the `FilrAuthClass.jar` file.
4. Copy the `FilrAuthClass.jar` file to the following locations on the NAM server:
   - **Linux:** `/opt/novell/nids/lib/webapp/WEB-INF/lib`
   - **Windows:** `C:\Program Files (x86)\Novell\Tomcat\webapps\nidp\WEB-INF\classes`
5. Run the following commands to restart the Identity Server and the Access Gateway:
   - **Identity Server:** `/etc/init.d/novell-idp restart`
   - **Access Gateway:** `/etc/init.d/novell-mag restart`

Configuring the NAM Identity Server

- "Configuring the Identity User Store" on page 153
- "Creating the Authentication Class" on page 153
- "Creating the Authentication Method" on page 153
- "Creating the Authentication Contract" on page 154

Configuring the Identity User Store

Configure an identity user store to which the Filr users should authenticate. See "Configuring Identity User Stores" in the NetIQ Access Manager Administration Guide.

Creating the Authentication Class

Authentication classes let you define ways of obtaining end-user credentials.

Perform the following steps to create a class:

1. Log in to the NAM Administration Console.
2. Click **Devices** > **Identity Server** > **Servers > Edit > Local > Classes**.
3. Click **New** to launch the Create Authentication Class wizard, then fill in the following fields:
   - **Display name:** Specify a name for the class.
   - **Java class:** Select **Other**.
   - **Java class path:** Specify `com.novell.nam.authentication.FilrAuthClass`.
4. Click **Next** and then click **New** to add the following properties for the class:
   - **Property Name:** Specify `FilrWsURL`.
   - **Property Value:** Specify the HTTP or HTTPS URL of the Filr server in the format: `http(s)://IP_Address_of_Filr_Server:port_number`.
5. Continue with Creating the Authentication Method.

Creating the Authentication Method

Authentication methods let you associate authentication classes with user stores.

1. Log in to the NAM Administration Console.
2. click **Devices** > **Identity Server** > **Servers > Edit > Local > Methods**.
3. Click **New** to launch the Create Authentication Method wizard, then fill in the following fields:
   - **Display name:** Specify a name for the method.
   - **Class:** Specify the name of the class that you created in Creating the Authentication Class.
   - **Identifies User:** Ensure that this option is selected.
   - **User stores:** Add user stores to search. You can select from the list of all the user stores you have set up. If you have several user stores, the system searches through them based on the order specified here. If a user store is not moved to the User stores list, users in that user store cannot use this method for authentication.
4. Continue with Creating the Authentication Contract.

Creating the Authentication Contract

Authentication contracts define how authentication occurs. Perform the following steps to create a new contract with the authentication method you created in Creating the Authentication Method.

1. Log in to the NAM Administration Console.
2. click **Devices** > **Identity Server** > **Servers** > **Edit** > **Local** > **Contracts**.
3. Click **New** to launch the Create Authentication Method Wizard, then fill in the following fields:
   - **Display name:** Specify a name for the contract.
   - **Methods:** Add the authentication methods that you created before from the list of the available methods.
4. To save the configuration changes, click **Devices** > **Identity Servers**, then click **Update All**.
5. Continue with "Configuring a Reverse-Proxy Single Sign-On Service for Filr" on page 154.

Configuring a Reverse-Proxy Single Sign-On Service for Filr

The Access Gateway can be configured as a reverse proxy server that provides single sign-on to Filr and restricts access to the Filr server by securely providing credential information for authenticated users.

To configure a reverse-proxy single sign-on service for Filr, complete the following tasks:

- "Creating a New Reverse Proxy" on page 154
- "Configuring the Proxy Service" on page 154
- "Creating Policies" on page 155
- "Configuring Protected Resources" on page 156
- "Configuring a Rewriter Profile" on page 158

Creating a New Reverse Proxy

You must ensure that the Reverse Proxy that you use for integrating NAM with Filr listens on the default HTTP (port 80) and HTTPS (port 443) ports.

Before you can configure the proxy service, you need to create a new reverse proxy. See "Configuring a Reverse Proxy" in the NetIQ Access Manager Administration Guide.

Configuring the Proxy Service

1. In the NAM Administration Console, click **Devices** > **Access Gateways** > **Edit**, then click the name of the reverse proxy that you created in "Creating a New Reverse Proxy" on page 154.
2. In the **Reverse Proxy List**, click **New** and then fill in the following fields:

   Proxy Service Name: Specify a display name for the proxy service.

   Published DNS Name: Specify the publicly-available DNS name for accessing your Filr site. This DNS name must resolve to the IP address you set up as the listening address. For example, `filr.doc.provo.microfocus.com`.

Web Server IP Address: Specify the IP address of the Filr server.

Host Header: Select **Forward Received Host Name**.

Web Server Host Name: Because of your selection in the **Host Header** field, this option is dimmed.

3 Click **OK**.

4 Click the newly added proxy service, then select the **Web Servers** tab.

5 Change the **Connect Port** to the default HTTP or HTTPS Filr web service port.

6 Click **OK**.

7 Continue with "Creating Policies" on page 155.

Creating Policies

You need to create two policies: LDAP Identity Injection and X-Forwarded-Proto:

- "Creating the LDAP Identity Injection Policy" on page 155
- "Creating the X-Forwarded-Proto HTTP Header Policy" on page 156

Creating the LDAP Identity Injection Policy

1 In the NAM Administration Console, click **Policies > Policies**.

2 Select the policy container, then click **New**.

3 Specify `ldap_auth` as the name for the policy, select **Access Gateway: Identity Injection** for the type, then click **OK**.

4 (Optional) Specify a description for the injection policy. This is useful if you plan to create multiple policies to be used by multiple resources.

5 In the **Actions** section, click **New**, then select **Inject into Authentication Header**.

6 Fill in the following fields:

User Name: If users are provisioned with `cn` or `uid` attributes, select **Credential Profile**, then select **LDAP Credentials:LDAP User Name**. In the **Refresh Data Every** drop-down, select **Session**.

Password: Select **Credential Profile**, then select **LDAP Credentials:LDAP Password**.

7 Leave the default value for the **Multi-Value Separator**, which is comma.

8 Click **OK**.

9 To save the policy, click **OK**, then click **Apply Changes**.

For more information on creating such a policy, see "Configuring an Authentication Header Policy" in the *NetIQ Access Manager Administration Guide*.

Creating the X-Forwarded-Proto HTTP Header Policy

If your network provides HTTPS (secure) connections between browsers and NAM but HTTP (insecure) connections between NAM and Filr, we strongly recommend creating an X-Forwarded-Proto HTTP Header Policy as a best practice.

1. In the NAM Administration Console, click **Policies > Policies**.
2. Select the policy container, then click **New**.
3. Specify `x-forward` as the name for the policy, select **Access Gateway: Identity Injection** for the type, then click **OK**.
4. (Optional) Specify a description for the injection policy. This is useful if you plan to create multiple policies to be used by multiple resources.
5. In the **Actions** section, click **New**, then select **Inject into Custom Header**.
6. Fill in the following fields:

   Custom Header Name: Specify `X-Forwarded-Proto` as the name.

   Value: Select **String Constant** in the drop-down, then specify `https`.
7. Leave the other settings at the defaults.
8. Click **OK**.
9. To save the policy, click **OK**, then click **Apply Changes**.

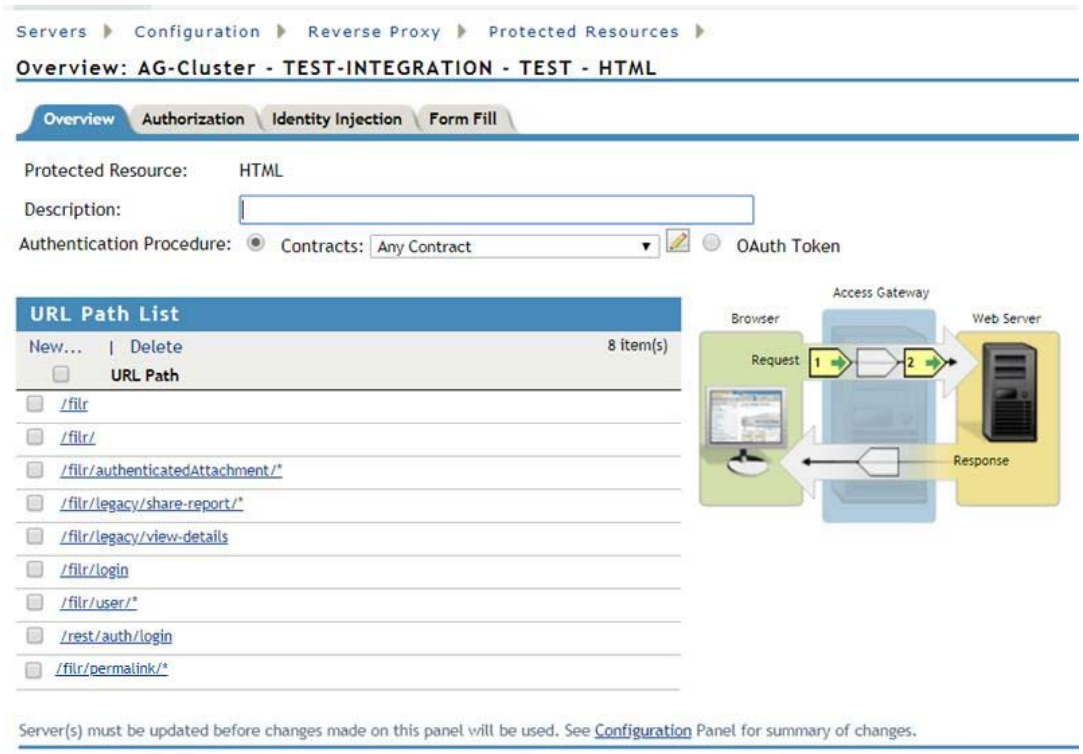
   For more information on creating such a policy, see “Configuring an Authentication Header Policy” in the *NetIQ Access Manager Administration Guide*.

Configuring Protected Resources

You must create two protected resources: a protected resource for HTML content and a public protected resource for web services.

1. Create a protected resource for HTML content:
   - **1a** In the **Protected Resource List**, click **New.** Specify a name, then click **OK**.
   - **1b** (Optional) Specify a description for the protected resource. You can use it to briefly describe the purpose for protecting this resource.
   - **1c** In the **Authentication Procedure**, select **Contracts** and specify the value that uses the FilrAuth method.
   - **1d** In the **URL Path List**, add the following paths for HTML content:

     ```
     /filr
     /filr/
     /filr/authenticatedAttachment/*
     /filr/legacy/share-report/*
     /filr/legacy/view-details
     /filr/login
     /filr/user/*
     /rest/auth/login
     /filr/permalink/*
     ```



1e Click **OK**.

2 Create a public protected resource for Web Services:

2a In the **Protected Resource** List, click **New**. Specify `public` for the name, then click **OK**.

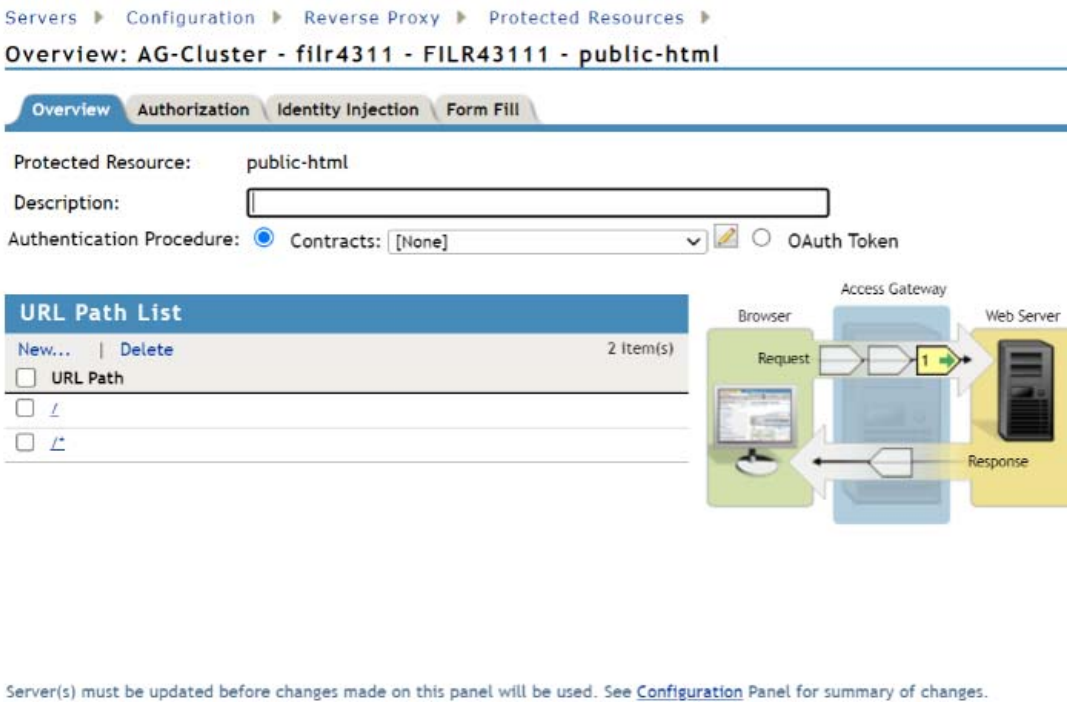
2b (Optional) Specify a description for the protected resource. You can use it to briefly describe the purpose for protecting this resource.

2c In the **Authentication Procedure**, select **Contracts** and specify the value as **None**.

2d Click **OK**.

2e In the **URL Path List**, add the following paths for public content:

```
/
/*
```



2f Click **OK**.

3 Assign the X-Forwarded-Proto Header policy to both protected resources that you created:

3a Click **Access Gateways** > **Edit** > **[Name of Reverse Proxy]** > **[Name of Proxy Service]** > **Protected Resources**.

3b For each Filr protected resource, click the **Identity Injection** link, select the **x-forwarded** policy that you created, click **Enable**, then click **OK**.

3c Click **OK.**

4 Assign the Identity Injection policy to the HTML protected resource that you created.

4a Click **Access Gateways** > **Edit** > **[Name of Reverse Proxy]** > **[Name of Proxy Service]** > **Protected Resources**.

4b For each Filr protected resource, click the **Identity Injection** link, select the **ldap_auth** policy that you created, click **Enable**, then click **OK**.

4c Click **OK.**

5 In the **Protected Resource List**, ensure that the protected resources that you created are enabled.

6 To apply your changes, click **Devices** > **Access Gateways**, then click **Update All**.

Configuring a Rewriter Profile

1 Click **Devices** > **Access Gateways** > **Edit** > **[Name of Reverse Proxy]** > **[Name of Proxy Service]** > **HTML Rewriting**.

2 In **HTML Rewriter Profile List**, click **New**.

3 Specify a name for the profile, select **Word** as the search boundary, then click **OK**.

4 In the **And Document Content-Type Header Is** section, click **New**, then specify the following type:

```
application/rss+xml
```

5 In the **Variable or Attribute Name to Search for Is** section, click **New**, then specify the following as the variable to search for:

```
value
```

6 Click **OK**.

7 In the Protected Resource List, ensure that the protected resources you created are enabled.

8 To apply your changes, click **Devices** > **Access Gateways**, then click **Update All**.

B All-in-One (Small) Deployment—Creating

To create an all-in-one deployment, you install one Filr appliance. By default Filr also includes the PostgreSQL database and Filrsearch functions.

Ensuring All-in-One Suitability

With few exceptions, small deployments are only suitable for proof-of-concept deployments, which, by definition, do not require extensive planning.

The OpenText best practice recommendation is always an expandable deployment, which is the focus of this guide.

All-in-One System Requirements

Most of the requirements in Chapter 3, “Filr System Requirements,” on page 13 apply to small deployments.

However, minimum RAM and CPU recommendations are increased to handle the database and search functions running in addition to Filr.

- 20 GB of RAM
- 4 CPUs

60% of the RAM should be dedicated to the Java heap.

For information about adjusting the Java heap settings, see “Changing JVM Configuration Settings” in the *OpenText Filr 23.4: Administrative UI Reference*.

All-in-One Deployment

To deploy an all-in-one Filr appliance, complete the instructions in the following sections:

Table B-1

Section	Additional Information
Chapter 5, “Downloading and Preparing the Filr Software,” on page 25	You only need to download the Filr software for your virtualization platform.
Chapter 6, “Deploying the Virtual Machines,” on page 29	Follow the instructions in the section for your virtualization platform.
Chapter 7, “Starting and Configuring the Filr Appliances,” on page 41	Follow the instructions in the referenced section, then continue with

Setting Up an All-in-One (small) Filr Appliance

Table B-2 *Logging in and Setting Up a Small Filr Appliance*

Page, Dialog, or Option	Do This
	1. Open a management browser on your administrative workstation and access the Port 9443 Administration Utility on the Filr appliance using the following URL: `https://filr_IP_Address:9443` Where *IP_Address* is the IP address of the Filr appliance.
Filr Appliance Sign In	1. Log in as the `vaadmin` user with the password that you set for the appliance in "Vaadmin password and confirmation:" on page 43.
Filr Appliance Tools	1. Click the Configuration icon  to launch the **Filr Configuration Wizard**.
Filr Configuration Wizard	1. Click **Next**.
Database	1. Type and confirm a password for the filr user in the PostgreSQL database.
Default Locale	1. Select your Locale from the dropdown list. 2. Change the **Administrator User ID** if you want to. The User ID that you enter is also the password for the initial login for the Port 8443 administration console. 3. Click **Finish**. 4. Do not close or exit the browser page until the warning message disappears.

C Non-Expandable Deployment—Creating

The steps required to create a non-expandable Filr deployment are almost identical to those for an expandable deployment.

Do the following:

1. Begin with Chapter 2, “Planning Is Critical,” on page 11 and complete all of the instructions that apply to your virtualization platform and plans.
2. Skip Chapter 4, “Setting Up Shared Storage,” on page 21.
3. Follow the instructions in the remaining sections as they apply.

D SCSI Controller Type—Changing on VMware

To change the SCSI controller type on a VMware-based appliance to **VMware Paravirtual**:

1. Finish the installation and power on the Filr system.
2. Ensure that the Filr system is running. (Log in as the Filr administrator, create a user, and log in as that user.)
3. Shut down each appliance in the Filr system. (For information about how to safely shut down an appliance, see "Shutting Down and Restarting the Appliance" in the *OpenText Filr 23.4: Administrative UI Reference*.)
4. In VMware, change the controller to **VMware Paravirtual**.
5. Power on each appliance in the Filr system.

E Troubleshooting Filr

- "Installation Issues" on page 167
- "Upgrade Issues" on page 167

Installation Issues

Unable to Access a Newly Installed Appliance

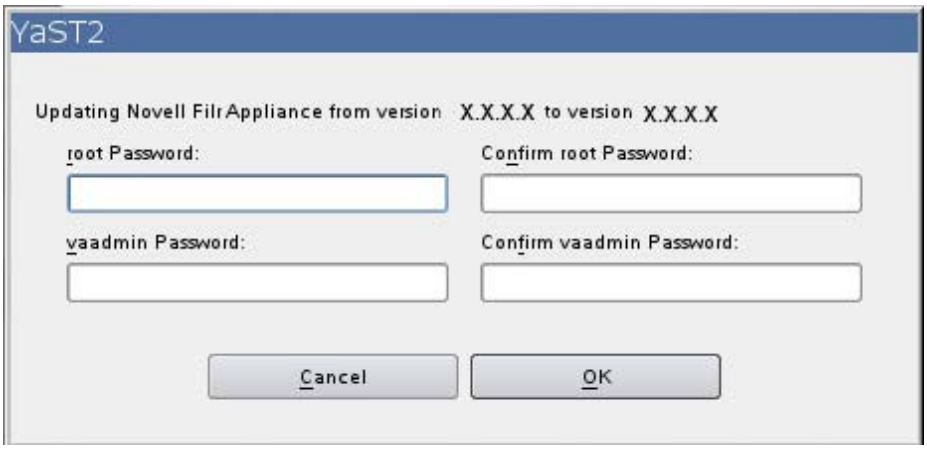
If you are unable to access a newly installed appliance and you need to change appliance settings, such as the IP address, use the VACONFIG utility from the Filr command prompt.

For more information, see "Using VACONFIG to Modify Network Information" in the *OpenText Filr 23.4: Maintenance Best Practices Guide*.

Upgrade Issues

The Upgrade Dialog Box Is Not Displayed during an Upgrade

The following dialog box should be displayed when powering on the new appliance.



If it is not displayed, the data storage location was not successfully copied or attached to the new Filr system. Begin the upgrade process again and ensure that you have configured the new Filr system to point to the data storage location of the source Filr system.

Rolling Back to the Previous Version after an Unsuccessful Upgrade

You can roll the Filr system back to the previous version if the upgrade is unsuccessful.

- "Rolling Back a Small or Non-Clustered Filr System" on page 168
- "Rolling Back a Clustered Filr System" on page 168

Rolling Back a Small or Non-Clustered Filr System

You should have created a copy of the data storage location (/vastorage) to be used in the new Filr system (as described in "Copying Each Appliance's /vastorage Disk (Disk 2)" on page 109).

If you experience complications when upgrading the Filr system, your existing Filr system is still intact and you are able to power it on at any time.

Rolling Back a Clustered Filr System

A clustered Filr system (multiple Filr appliances) consists of not only a data storage location (`/vastorage`), but also shared storage (`/vashare`).

- "Rolling Back the Data Storage Location (/vastorage)" on page 168
- "Rolling Back the Shared Storage Location (/vashare)" on page 168

Rolling Back the Data Storage Location (/vastorage)

You should have created a copy of the data storage location (`/vastorage`) to be used in the new Filr system (as described in "Copying Each Appliance's /vastorage Disk (Disk 2)" on page 109).

If you experience complications when upgrading the Filr system, the data storage location of your existing Filr system is still intact.

Rolling Back the Shared Storage Location (/vashare)

After an unsuccessful upgrade, you can roll back the shared storage location (`/vashare`) to the previous version by reconfiguring clustering on the Filr server:

1. On the Filr appliance that you are rolling back to, log in as the Filr administrator.

   `https://ip_address:9443`

   Replace **ip_address** with the IP address of your Filr appliance.
2. Sign in to the Filr appliance using the `vaadmin` user and the password that you set during installation.

   The Filr Appliance landing page is displayed.
3. Click the **Filr Server Configuration**  icon.
4. Click **Clustering**.

5 In the **Server Address** field, add the port number to the server address of each search index appliance.

For example, change `172.17.2.2` to `172.17.2.2:11211`

F Filr Limitations

- “Installation” on page 171
- “Upgrade” on page 172
- “Appliance” on page 172
- “Configuration” on page 172
- “Net Folder” on page 175
- “Filr Appliance” on page 176
- “Database Appliance” on page 183
- “Desktop Application” on page 184
- “Mobile Apps” on page 184
- “Web Application” on page 187
- “Windows Subsystem For Linux and Filr Client” on page 188

Installation

- “Importing of .ovf and .vmdk Files Fails with VMware vSphere 6.7 Update 2” on page 171
- “NFS Mount Point Must Not Point to /var on Target Server” on page 171

Importing of .ovf and .vmdk Files Fails with VMware vSphere 6.7 Update 2

Import of `.ovf` and `.vmdk` files fails when using VMware vSphere 6.7 Update 2. This issue is planned to be fixed by VMware in their upcoming updates. A workaround is available to resolve this issue in the TID 7023863 https://support.microfocus.com/kb/doc.php?id=7023863.

NFS Mount Point Must Not Point to /var on Target Server

Large installations require shared NFS or CIFS storage for the `/vastorage` mount point on the Filr server.

If you are using NFS, you must not target the `/var` mount point or a child directory within it. Doing so will cause `/vastorage` to fail to mount when the Filr appliance reboots. (See TID 7017379.)

Upgrade

- "Rolling Upgrades Are Not Supported in a Clustered Environment" on page 172

Rolling Upgrades Are Not Supported in a Clustered Environment

Rolling upgrades (upgrading one Filr or search index server while another continues to serve clients) are not supported when upgrading Filr in a clustered environment.

You must shut down all Filr and search index appliances before you begin the upgrade process. Then restart the appliances after the upgrade is complete.

This issue does not affect small or non-clustered large installations.

For information about how to upgrade Filr, see "Upgrading a Large Filr Deployment" in the *OpenText Filr 23.4: Installation, Deployment, and Upgrade Guide*.

Appliance

- "VMware Snapshots and Appliance Backup" on page 172

VMware Snapshots and Appliance Backup

Do not use VMware snapshots as a backup method for Filr. Doing so inhibits your ability to upgrade Filr in the future.

If you do use snapshots, you must remove them before upgrading to a new version of Filr.

For more detailed information about how to back up various Filr components, see "Backing Up Filr Data" in the *OpenText Filr 23.4: Maintenance Best Practices Guide*.

Configuration

- "User Name Character Restrictions for LDAP Synchronization and Login" on page 173
- "User Names That Are Synchronized from LDAP Are Not Case Sensitive for Filr Login" on page 173
- "Disabling Web Access Does Not Block Guest Access" on page 173
- "Unable to Upload Site Branding Image to Filr" on page 173
- "Distributed File System (DFS) Issues" on page 173
- "Access Manager Issues" on page 174

User Name Character Restrictions for LDAP Synchronization and Login

LDAP user names must contain only valid alphanumeric characters 0 - 9 and upper-case and lower-case letters (A-Z). User names that contain ASCII characters and special characters (for example, / \ * ? " < > : |) cannot be used as Filr user names. If your LDAP directory includes user names with these characters, they synchronize to Filr, but the associated users cannot log in.

These characters cannot be used in a Filr user name because a Filr user name becomes the user's workspace title, and the workspace title becomes an element of the hierarchical path that leads to the workspace. These characters are not legal characters in Linux and Windows pathnames.

User Names That Are Synchronized from LDAP Are Not Case Sensitive for Filr Login

User names that are synchronized from an LDAP directory are not case sensitive when users log in to the Filr system.

Local user accounts (user accounts that are created in Filr and not synchronized from an LDAP directory) are case sensitive. Login credentials for local user accounts are stored in the MySQL database.

Disabling Web Access Does Not Block Guest Access

If both **Allow Guest Access** and **Disable Web Access** are selected on the Web Application page of the Administration Console, then **Enter as Guest** is displayed on the initial Web Access Login dialog and Guest users can see publicly available files and folders.

If you choose to disable the web access, you should ensure that the guest access is not enabled.

Unable to Upload Site Branding Image to Filr

If a user with administrator privileges chooses to upload image that has to be used in the site branding to Filr, the image fails to upload.

To upload site branding image to Filr, you must login as the built-in Filr administrator (admin).

Distributed File System (DFS) Issues

- "Access Based Enumeration Is Not Supported When Using DFS Namespace" on page 173
- "NSS AD DFS Junction Visibility Requires Net Folder Rights Cache Refreshing" on page 174
- "Unable to Access Data on a DFS Junction In an OES Server Cluster Environment" on page 174

Access Based Enumeration Is Not Supported When Using DFS Namespace

Filr doesn't support Microsoft's Access Based Enumeration (ABE) when the backend Windows server uses the Distributed File System (DFS) namespace.

NSS AD DFS Junction Visibility Requires Net Folder Rights Cache Refreshing

If you have a remote DFS junction on an OES 2015 server that is running NSS for AD, you must ensure that the **Refresh Cached Rights** interval under **Net Folder Settings** in the Filr administration console is not set to 0 minutes (meaning that it's disabled). Otherwise, Filr users will not be able to access files and folders under the DFS target through Filr and the owner of all the files and folders under the target will be displayed as `File Sync Agent` in Filr.

Unable to Access Data on a DFS Junction In an OES Server Cluster Environment

When the Filr server encounters issue accessing data on a DFS junction in an OES cluster environment, the following error displays:

```
ConvertXplatErrToFAMTErr xplat status: 0xc7e90503
```

To fix this problem, ensure that the VLDB service is up and running. For more information about the VLDB service, see OES Documentation.

Access Manager Issues

- "Unable to Log Into Filr as a Guest User When Filr is Fronted by Access Manager" on page 174
- "Unable to Edit a File Using the Edit-in-Place Functionality When Filr is Fronted by Access Manager" on page 174
- "Logout Does Not Happen When Filr Is Accessed Directly and Is Fronted by Access Manager" on page 175
- "External User confirmation Link Displays the Filr login page Even When Filr Is Fronted by Access Manager" on page 175
- "Cannot Use Multiple Identity Injection Policies Simultaneously" on page 175

Unable to Log Into Filr as a Guest User When Filr is Fronted by Access Manager

Currently, you cannot use a guest user account to log into Filr that is fronted by Access Manager.

Unable to Edit a File Using the Edit-in-Place Functionality When Filr is Fronted by Access Manager

If you attempt to edit a file using the edit-in-place functionality when Filr is fronted by Access Manager, the file fails to open.

To workaround this issue, do the following:

1. Log in to the Access Manager server.
2. Navigate to **Devices** > **Access Gateways** > ***[Name of the Access Gateway Server]*** > **Edit** > **Advanced Options**.

3 Set the advanced option `NAGGlobalOptions AllowMSWebDavMiniRedir` to on.

4 To apply your changes, click **Devices** > **Access Gateways**, then click **Update All**.

Logout Does Not Happen When Filr Is Accessed Directly and Is Fronted by Access Manager

When Filr is fronted by NetIQ Access Manager, only the Filr administrator is able to access Filr directly. When Filr is accessed directly in this configuration, simultaneous logout for the Filr system is not successful.

After the Filr administrator logs in directly to Filr (and Filr is configured with Access Manager), all browser sessions should be immediately closed to ensure logout.

External User confirmation Link Displays the Filr login page Even When Filr Is Fronted by Access Manager

After using the registration link for self-provisioning your user account on the Filr server that is fronted by Access Manager, clicking the same confirmation link again directs you the Filr login page instead of NAM login page.

Cannot Use Multiple Identity Injection Policies Simultaneously

When NetIQ Access Manager is configured to front Filr, you cannot use multiple identity injection policies simultaneously.

Net Folder

- "Active Directory Cross Forest Trust Relationship Is Not Supported" on page 175
- "Moving or Renaming a File from the File Server Removes Shares" on page 176
- "Folder Path in Filr Cannot Exceed 48 Levels" on page 176
- "Modifying the Target Location in a Junction Created On the OES Server Does Not Reflect in the Filr Net Folder Pointing to the Junction" on page 176

Active Directory Cross Forest Trust Relationship Is Not Supported

Cross Forest Trust relationships in Active Directory are not supported in Filr.

Moving or Renaming a File from the File Server Removes Shares

If a user moves or renames a file directly from the file server (instead of using a Filr client to do the move or rename), any shares that are associated with that file in Filr are removed. This means that users who gained access to a file via a share in Filr no longer have access to the file if the file was moved or renamed from the file server. Additionally, the file is not displayed in users' Shared by Me and Shared with Me views.

If this situation occurs, files must be re-shared in Filr.

Folder Path in Filr Cannot Exceed 48 Levels

When folders on the file system are synchronized to a Net Folder, the folder path in Filr cannot exceed 48 levels deep (nested sub-folders). The file synchronization code will reject any sub-folder whose depth will cause the corresponding Filr folder path to exceed the sub-folder limit of 48.

When the Filr system encounters the limit of 48 folder levels, the sync code returns the following message and the folder is not created:

```
The folder xxx has reached the allowed path maximum depth. Its sub-folders
will not be added in the system.
```

Modifying the Target Location in a Junction Created On the OES Server Does Not Reflect in the Filr Net Folder Pointing to the Junction

Create a junction on the OES Server and then create a net folder in Filr pointing to this junction. On changing the target location in this junction, the net folder still continues to point to the older target location in the junction. Consequently, the contents of the net folder continues to be the files and folders in the older target location.

To view the contents of the new target location in the net folder, run the following command to restart famtd.

```
rcnovell-famtd restart
```

Filr Appliance

- "Reporting Issues" on page 177
- "My Files Storage Directory Is Displayed in Search" on page 177
- "Sharing Issues" on page 177
- "Editing an .rtf File Results in an Editing Conflict Error" on page 178
- "LDAP Synchronization Issues" on page 178
- "Email Issues" on page 180
- "Cannot Upload Documents Created with Apple iWork (Pages, Keynote, etc.) or .app Documents to the Filr Web Client" on page 180
- "Unable to Upload Microsoft OneNote Files to Filr" on page 180
- "Cannot Extract ZIP File after Downloading on Mac" on page 180
- "Issues When Downloading Multiple Files with Safari on Mac" on page 181
- "File Name Should Not Be More Than about 200 Characters" on page 181
- "WebDAV Issues" on page 181
- "Cannot Log in to Web Client with Long User ID or Password" on page 182
- "Display Issues Due to Third-Party Software" on page 182
- "Cannot View ODP and ODG Files That Contain Charts, Graphs, and Tables When Viewing in HTML Format" on page 182

- "User Home Directories Are Not Synchronized until Trustee Cache Information is Updated" on page 183
- "Filr Does Not Support Aliases That Have Been Configured in the LDAP Directory" on page 183
- "Cannot Use Text Editors Such as Notepad or Wordpad as a Document Editor" on page 183
- "Must Restart All Appliances after a Network Failure with Microsoft SQL" on page 183

Reporting Issues

- "License Report Issues" on page 177

License Report Issues

The License Report currently counts Administrator, Guest, and three internal users (`_emailPostingAgent`, `_jobProcessingAgent`, and `_synchronizationAgent`) as local users. The Administrator counts as an active user, but the other four local users do not count against your Filr license usage.

For information about how to generate a license report, see "License Report" in the *OpenText Filr 23.4: Administrative UI Reference*.

My Files Storage Directory Is Displayed in Search

When Personal Storage is disabled and Home folders have not been configured, users can find a directory called My Files Storage when clicking in the global Search field and pressing the Spacebar. This is normally a hidden directory, but can it be displayed under these special circumstances.

When you click **My Files Storage**, it can take you to either your My Files area or to the profile of another user (depending on where you are when you do the search).

Sharing Issues

- "External User Share Invitation Link and Confirmation Link Are Valid Only Once" on page 178
- "Files Shared with Users In Share Point Does Not Appear in Shared with Me or Shared by Me Areas in Filr" on page 178

External User Share Invitation Link and Confirmation Link Are Valid Only Once

When a file is shared with an external user, the user receives an invitation email with a link to register self and then a confirmation email with a link to sign in and access the shared items. The user cannot use these links to access the file post they have registered and confirmed the registration. To access the file again, they must log in to the site where the file is shared with them. For this, the external users must note the hostname of the site from which they accessed the file for the first time by clicking the **Sign in and access shared items** link in the confirmation email.

Files Shared with Users In Share Point Does Not Appear in Shared with Me or Shared by Me Areas in Filr

When users share files on Share Point servers, the files do not appear in the **Shared by Me** or **Shared with Me** folders. However, the users with whom the files were shared can see the shared files if they are in Net Folders and if the users have access to the Net Folders.

Editing an .rtf File Results in an Editing Conflict Error

After editing an `.rtf` file from Filr in a text editor (such as Microsoft Word), saving the file results in a message indicating that the file has been changed by another author. In this case, select the option to combine your changes with the other author's changes, then click **OK**.

Changes that you make to the file are saved to Filr as expected.

LDAP Synchronization Issues

- "Issues with Initial Synchronization of Filr Users" on page 178
- "Sub-Groups Are Not Included in Group Membership during the Initial Synchronization" on page 179
- "Issues with Renaming and Moving Users in Your LDAP Directory" on page 179
- "Users Cannot Log in to the Filr Mobile App or Desktop Application with New Name or Password after Changed in LDAP" on page 179
- "Duplicate User ID Import Attempts Are Logged but Not Reported" on page 179

Issues with Initial Synchronization of Filr Users

The LDAP value of the attribute you specify for the LDAP configuration setting **LDAP attribute for the Filr account name** must be unique throughout your LDAP directory. For example, if you specify `cn`, all users in the LDAP directory might not have a unique value.

To resolve this issue, use an attribute whose value is always unique across all containers, such as `emailAddress`.

Sub-Groups Are Not Included in Group Membership during the Initial Synchronization

When synchronizing groups that contain sub-groups to Filr from an LDAP directory, the sub-groups are not included in their parent group's membership during the initial synchronization.

Perform an additional LDAP synchronization to ensure that group membership contains all expected sub-groups.

Issues with Renaming and Moving Users in Your LDAP Directory

In order to rename or move users in your LDAP directory, ensure that you have specified a value for the setting **LDAP attribute that uniquely identifies a user or group**, as described in "LDAP Servers and Synchronization" in the *OpenText Filr 23.4: Administrative UI Reference*. If a value is not specified for this setting, renaming or moving users in your LDAP directory might result in new users being created in Filr or in the existing user account being deleted.

Users Cannot Log in to the Filr Mobile App or Desktop Application with New Name or Password after Changed in LDAP

After a user is renamed in the LDAP directory or after a user's password is changed in the LDAP directory, the user must use the old user name or password when logging in to the Filr mobile app or the Filr desktop application until one of the following occurs:

- An LDAP synchronization is run
- The user logs in to the web client using the new user name or password

A user can use the old or new user name or password when logging in to Filr from the web client.

Duplicate User ID Import Attempts Are Logged but Not Reported

If you attempt to import an LDAP user that has the same User ID as a previously imported user, the import fails and is logged, but the failure is not reported in the administrative GUI. The import error is logged in `/opt/novell/filr/apache-tomcat/logs/appserver.log`.

Subsequently, only the first user imported is able to log in. Other users with the same User ID are not able to log in, but they are given no indication as to why the login request failed. Failed login attempts are logged in `/opt/novell/filr/apache-tomcat/logs/appserver.log`.

Email Issues

- "Test Connection Fails without User Name and Password Even When Authentication Is Not Required" on page 180

Test Connection Fails without User Name and Password Even When Authentication Is Not Required

When configuring Filr to use an external outbound mail system (such as Novell GroupWise), the **Test Connection** button fails when no user name and password is specified, even when the **Authentication required** option is not selected.

For information about how to configure Filr to use an external outbound mail system, see "Configuring an Email Service for Filr to Use" in the *OpenText Filr 23.4: Administrative UI Reference*.

Cannot Upload Documents Created with Apple iWork (Pages, Keynote, etc.) or .app Documents to the Filr Web Client

When uploading a document that was created with one of the following types of files, you get an error indicating that the file or folder cannot be uploaded when attempting to upload to the Filr web client:

- iWork document (such as a Pages, Keynote, or Numbers document)
- Mac application file (a document with the `.app` extension)

The Filr web client is not able to upload these types of documents because the document architecture for these documents more closely resembles a folder, and you cannot upload folders using the Filr web client.

You can upload these types of documents to Filr by using the Filr desktop application or the Filr mobile app.

For information about how to upload documents using the desktop application or mobile app, see the *Filr Desktop Application for Windows Guide* (https://www.novell.com/documentation/filr-3/filr-desktop/data/bookinfo.html), the *Filr Desktop Application for Mac Guide*, and the *Filr Mobile App Quick Start* (https://www.novell.com/documentation/filr-3/filr-qs-mobile/data/filr-qs-mobile.html).

Unable to Upload Microsoft OneNote Files to Filr

If a user chooses to upload `.one` file, the file fails to upload even if the Filr administrator has whitelisted the `.one` file.

Cannot Extract ZIP File after Downloading on Mac

After downloading a single file or multiple files as a `.zip` file.), the file can be extracted only when using third-party tools such as iZip Unarchiver.

This issue is due to the fact that OS X does not currently handle ZIP64, the technology that is used to create the `.zip` file.

Issues When Downloading Multiple Files with Safari on Mac

If you are experiencing issues when downloading multiple files when using Safari on Mac, ensure that the option **Open “safe” files after downloading** is not selected.

1. Click **Safari** > **Preferences**.
2. On the General tab, ensure that **Open “safe” files after downloading** is not selected.

File Name Should Not Be More Than about 200 Characters

The exact maximum file name length depends on the configuration of the Filr server, but generally it is about 200 characters. If file names are too long, files cannot be added to Filr.

WebDAV Issues

- "Cannot Edit a File through WebDAV (Edit-in-Place) When the User Password Contains a Space" on page 181
- "Cannot Rename a File When Editing through WebDAV (Edit-in-Place)" on page 181
- "WebDAV Limitations on Mac" on page 181

Cannot Edit a File through WebDAV (Edit-in-Place) When the User Password Contains a Space

If you try to edit a file through WebDAV, when your user password contains a space, the authentication fails.

To edit files through WebDAV, ensure that your user password does not contain a space.

Cannot Rename a File When Editing through WebDAV (Edit-in-Place)

When using Edit-in-Place functionality to edit a file, you cannot click **Save As** and rename the file. Doing so results in an upload error, and changes to the file are not synchronized to Filr.

WebDAV Limitations on Mac

When you use WebDAV functionality in a Mac environment, you encounter the following limitations:

- **Limitations When Editing Files on Mac through WebDAV** Edit-in-Place functionality is not supported on a Mac when you use Microsoft Office as your document editor. To use Edit-in-Place functionality on a Mac, you must use OpenOffice or LibreOffice as your document editor.
- **Cannot Edit a File through WebDAV (Edit-in-Place) When Using LibreOffice on a Mac** If you are accessing Filr from a Mac and using LibreOffice as your document editor, you cannot edit files through WebDAV using Edit-in-Place functionality.

  If you are using Apache to front the Filr system, users are able to edit files through WebDAV when accessing Filr from a Mac and using LibreOffice as the document editor.
- **Using WebDAV to Access the Filr folder (via Mac Finder) Is Read Only** When using WebDAV to access the Filr desktop application Filr folder via Mac Finder, access is Read Only.
- **Cannot Edit a File through WebDAV (Edit-in-Place) When Using Safari 7.*x* with OS X 10.9.*x***

  When accessing Filr with Safari 7.*x* and OS X 10.9.*x*, using Edit-in-Place functionality to edit a file, results in an error and you are not able to edit the file.

  To configure Safari 7.*x* and OS X 10.9.*x* to support the Filr Edit-in-Place feature and to support adding files to folders when using a browser that does not support HTML 5:

  1. With Filr open, in Safari, click **Menu** > **Preferences**.
  2. Click the **Security** tab, then click **Manage Website Settings**.
  3. Select **Java**, then click the drop-down arrow next to the Filr URL and select **Run in Unsafe Mode**.
  4. Click **Done**.

Cannot Log in to Web Client with Long User ID or Password

Users cannot log in to the Filr web client if the user ID exceeds 128 characters or the password exceeds 64 characters.

Display Issues Due to Third-Party Software

- "Filr Is Not Displayed Correctly When the Ask Toolbar Is Installed on Chrome" on page 182

Filr Is Not Displayed Correctly When the Ask Toolbar Is Installed on Chrome

When the Ask toolbar is installed on a Chrome browser, it inhibits users from being able to view all of the Filr masthead. The Ask toolbar is not a Chrome-sanctioned toolbar and should not be installed on a Chrome browser.

Cannot View ODP and ODG Files That Contain Charts, Graphs, and Tables When Viewing in HTML Format

ODP and ODG files that contain charts, graphs, or tables are not displayed when viewing files by using the HTML view, as described in the following situations:

- When viewing the file in a browser
- When viewing a file from the Filr mobile app and clicking **Generate Online Preview**

User Home Directories Are Not Synchronized until Trustee Cache Information is Updated

When you add a user to your LDAP directory, the user's Home directory in Filr is not displayed immediately after running the LDAP synchronization.

You must wait for the trustee cache information to be refreshed on the file system before Home directory information is displayed in Filr. (The default rights cache refresh interval is every 5 minutes. You can modify this interval as described in "Just-in-Time Synchronization" in the *OpenText Filr 23.4: Administrative UI Reference*.)

Filr Does Not Support Aliases That Have Been Configured in the LDAP Directory

If your users have aliases associated with their user account in the LDAP directory, the alias is not synchronized to Filr during the LDAP synchronization. This means that users are not able to log in to Filr with their alias.

Cannot Use Text Editors Such as Notepad or Wordpad as a Document Editor

Filr allows you to change the default application that is used for editing files. However, you cannot use text editors such as Notepad or Wordpad as the default document editor for editing files because these applications do not support WebDAV.

Must Restart All Appliances after a Network Failure with Microsoft SQL

If your Filr deployment includes a Microsoft SQL database, and if your network fails, you must restart all of the appliances in your Filr deployment to restore Filr services.

Database Appliance

- "Filr Installation Program Cannot Create the Filr Database in Microsoft SQL When the Database Name Begins with a Number" on page 183

Filr Installation Program Cannot Create the Filr Database in Microsoft SQL When the Database Name Begins with a Number

In the configuration wizard when configuring a large deployment, the database name that you specify in the **Database Name** field cannot begin with a number when using a Microsoft SQL database. If the name does begin with a number, the configuration wizard does not allow the database to be created. For example, `1Filr` is not accepted, but `Filr1` is.

Desktop Application

For a list of issues related to the Filr desktop application (for Windows, Mac, and Linux clients), see the *Filr Desktop Application ReleaseNotes*.

Mobile Apps

For information about how to install and run the Filr mobile app, see the *Filr Mobile App Quick Start*.

Following are known issues in the Filr mobile app:

- "iOS Devices" on page 184
- "Windows Device" on page 186
- "All Mobile Devices" on page 186

iOS Devices

- "Files App" on page 184
- "Unable to Preview Some Files on an iOS Device" on page 184
- "Activity View Display on a iOS 11 Device Does Not Honor the AppConnect Apps or Whitelist Settings" on page 185
- "Filr Menu Options Not Listed After Logging In To Filr on an iOS Device That Has MobileIron Configured" on page 185
- "iOS App Extensions Are Restricted When Applications Are Whitelisted" on page 185

Files App

- An error may occur while performing the Filr file operations by using Files App. To resolve the issue, try again.
- The download icon continues to remain even after downloading the file to your iOS device.
- On installing Filr, unable to login through file provider extension. To resolve this issue, in the Files app edit section, toggle the switch off and then on for the Filr app.

Unable to Preview Some Files on an iOS Device

On an iOS device, you cannot preview some files such as `.odt`, `.odp`, and `.dwg` if the Filr server uses a self-signed certificate.

Ensure that the Filr server uses a valid SSL certificate that is signed by a well-known certificate authority (CA).

Activity View Display on a iOS 11 Device Does Not Honor the AppConnect Apps or Whitelist Settings

The Activity View Display that displays on an iOS 11 device with MobileIron configured when you tap the **Actions** icon does not honor the Mobileiron **AppConnect apps** or **Whitelist** settings and lists all applications and extensions. Even if you tap an application or extension that is not listed in **AppConnect apps** or **Whitelist**.settings, files get shared to such blocked applications and extensions.

However, the Filr **Open In** option below the Activity View Display honors the Mobileiron **AppConnect apps** or **Whitelist** settings.

Filr Menu Options Not Listed After Logging In To Filr on an iOS Device That Has MobileIron Configured

When you log into Filr from an iOS device with MobileIron configured, the Filr menu options are not displayed on tapping the **Actions** icon  if the Mobileiron **Allow open in** setting is set to either **AppConnect apps** or **Whitelist**.

To workaround this issue, you must create or modify the AppConnect app configuration and add the following key-value pair to the app-specific configuration section:

- **Key:** `MI_AC_DISABLE_OPEN_IN_ENFORCEMENT`
- **Value:** YES

iOS App Extensions Are Restricted When Applications Are Whitelisted

The iOS App Extensions and sharing through AirDrop is restricted when the applications are added to whitelist.

For example, when Google drive is added to whitelist (com.google.Drive), then sharing of files through the extensions such as AirDrop, Drive, Save to Files, and so on is restricted. The files can only be shared through applications such as Import with Drive or Copy to Drive.

Windows Device

Windows Phone Users See an Authentication Error When Filr Has a Self-Signed Certificate

If Filr is configured with a self-signed certificate, Windows Phone users see an authentication error when attempting to access Filr by using the Windows Filr mobile app.

You can resolve this issue in either of the following ways:

- (Recommended) Configure Filr to use an official certificate in the *OpenText Filr 23.4: Maintenance Best Practices Guide*.
- Send a copy of the self-signed certificate via email to each Windows Phone in your system. Users must then open the email and click the certificate attachment. After users click the attachment, the self-signed certificate is installed on the phone. When the certificate is installed, users are able to log in to the Filr app without seeing the authentication error.

All Mobile Devices

- "Files in Downloads Area Are Not Synchronized with Just-in-Time Synchronization" on page 186
- "Files from the Home Folder in the Downloads Area Are Removed after Personal Storage Is Enabled" on page 186
- "Files from Net Folders Are Removed from the Downloads Area after Being Renamed or Moved" on page 187
- "Email Addresses in Share Dialog Cannot Contain Extended Characters" on page 187

Files in Downloads Area Are Not Synchronized with Just-in-Time Synchronization

Accessing a file from the **Downloads** area from the mobile app does not trigger Just-in-Time synchronization.

If you have configured only Just-in-Time synchronization (scheduled synchronization is not enabled), files that are located in a Net Folder that have been added to the **Downloads** area on the mobile app are not automatically updated with changes made from the file system. The file is updated in the **Downloads** area only after a user uses one of the Filr clients to browse to the Net Folder that contains the file.

Files from the Home Folder in the Downloads Area Are Removed after Personal Storage Is Enabled

If users have added files from their Home folder to the Downloads area on the mobile app, and then the Filr administrator enables personal storage (as described in "Enabling Personal Storage for Users and Groups" in the in the *OpenText Filr 23.4: Administrative UI Reference*), files from the Home folder are removed from the Downloads area on the mobile app.

Files from Net Folders Are Removed from the Downloads Area after Being Renamed or Moved

If users have added files from a Net Folder to the Downloads area on the mobile app, and then the file is renamed or moved on the OES or Windows file system, the file is removed from the Downloads area on the mobile app.

Email Addresses in Share Dialog Cannot Contain Extended Characters

When specifying an email address in the Share dialog, if the email address contains extended characters (such as an apostrophe), an error message is displayed indicating that the item cannot be shared with the specified user.

Web Application

- "The .bmp Images Appear Blank in the Internet Explorer" on page 187
- "Password-Protected Files Cannot Be Viewed" on page 187
- "Enabling a User Account Fails For a Restored User Profile If the User's My Files Storage Folder is Not Restored from the Trash" on page 187

The .bmp Images Appear Blank in the Internet Explorer

If you upload a .bmp image for custom branding for the Filr Web UI, then the branded image appears as blank on launching the GUI in Internet Explorer. The branded image is available in all the other browsers.

Password-Protected Files Cannot Be Viewed

Files that have been password-protected in the application where they were created cannot be viewed in Filr.

Enabling a User Account Fails For a Restored User Profile If the User's My Files Storage Folder is Not Restored from the Trash

If you choose to enable a user account whose user profile is restored from the trash but the `My Files Storage` folder of the user is still trashed, the following error displays:

`User` `could not be enabled because the 'My Files Storage' folder is in the trash`.

Before enabling the user account, you must ensure that the user account is completely restored from the trash. To restore the user account completely from trash, you must restore both the user profile and the `My Files Storage` for the user from the trash.

Windows Subsystem For Linux and Filr Client

Filr client is currently not supported with the Windows Subsystem for Linux (WSL) feature. Uninstall the Filr client before enabling your Windows machine for Linux. Failing to do so might cause your system to crash.