

How Filr Works—Overview Guide

Filr 1.1

November 21, 2014

Novell®



Legal Notices

Novell, Inc., makes no representations or warranties with respect to the contents or use of this documentation, and specifically disclaims any express or implied warranties of merchantability or fitness for any particular purpose. Further, Novell, Inc., reserves the right to revise this publication and to make changes to its content, at any time, without obligation to notify any person or entity of such revisions or changes.

Further, Novell, Inc., makes no representations or warranties with respect to any software, and specifically disclaims any express or implied warranties of merchantability or fitness for any particular purpose. Further, Novell, Inc., reserves the right to make changes to any and all parts of Novell software, at any time, without any obligation to notify any person or entity of such changes.

Any products or technical information provided under this Agreement may be subject to U.S. export controls and the trade laws of other countries. You agree to comply with all export control regulations and to obtain any required licenses or classification to export, re-export or import deliverables. You agree not to export or re-export to entities on the current U.S. export exclusion lists or to any embargoed or terrorist countries as specified in the U.S. export laws. You agree to not use deliverables for prohibited nuclear, missile, or chemical biological weaponry end uses. See the [Novell International Trade Services Web page \(http://www.novell.com/info/exports/\)](http://www.novell.com/info/exports/) for more information on exporting Novell software. Novell assumes no responsibility for your failure to obtain any necessary export approvals.

Copyright © 2013 - 2014 Novell, Inc. All rights reserved. No part of this publication may be reproduced, photocopied, stored on a retrieval system, or transmitted without the express written consent of the publisher.

Novell, Inc.
1800 South Novell Place
Provo, UT 84606
U.S.A.
www.novell.com

Online Documentation: To access the latest online documentation for this and other Novell products, see the [Novell Documentation Web page \(http://www.novell.com/documentation/\)](http://www.novell.com/documentation/).

Novell Trademarks

For Novell trademarks, see the [Novell Trademark and Service Mark list \(http://www.novell.com/company/legal/trademarks/tmlist.html\)](http://www.novell.com/company/legal/trademarks/tmlist.html).

Third-Party Materials

All third-party trademarks are the property of their respective owners.

Contents

About This Guide	7
1 Filr Overview	9
1.1 What Is Novell Filr?	9
1.2 Filr Features and Functionality	10
1.3 Why Novell Appliances?	11
2 Setting Up Filr	13
2.1 Getting and Preparing Filr Software	13
2.1.1 Hyper-V	13
2.1.2 VMware	14
2.1.3 Xen	15
2.2 Deploying Filr Appliances	16
2.2.1 Small Filr Deployment Overview	16
2.2.2 Large Filr Deployment Overview	17
2.3 Initial Configuration of Filr Appliances	18
2.3.1 Small Filr Deployment Configuration	18
2.3.2 Large Filr Deployment Configuration	19
2.4 Filr Clustering (Expanding a Deployment)	21
2.5 Integrating Filr Inside Your Network Infrastructure	23
2.5.1 A Small Filr Deployment	23
2.5.2 A Large Filr Deployment	25
2.6 Ports Used in Filr Deployments	26
2.7 There Are No Changes to Existing Servers or Systems	27
3 Filr Administration	29
3.1 Filr Administrative Users	29
3.2 Ganglia Appliance Monitoring	31
3.3 Updating Appliances	32
3.4 Certificate Management in Filr	33
3.5 Filr Site Branding	34
4 Access Rights and Filr	35
4.1 Filr Authentication	35
4.2 Access to Files and Folders Is Controlled by the File System	36
4.3 How Users Get the Required Access Permissions	36
4.3.1 Roles and Net Folders	37
4.3.2 Roles and Shared with Me	37
4.4 Access Through Filr Involves One of Four Possible Roles	37
4.4.1 My Files (Personal Storage)	37
4.4.2 Home Folders	38
4.4.3 Net Folders	38
4.4.4 File Attributes Are Always Honored	39
4.5 Role Requirements Are Rigidly Enforced	40
4.5.1 NSS Example	40
4.5.2 NTFS Example	41

4.6	Rights to Files and Folders.	41
4.6.1	Access Is Always Controlled by the File System.	41
4.7	Sharing Rights	43
4.8	Windows Share Rights.	44
4.9	Access-based Enumeration (Windows)	44
5	Filr Comments	45
6	Filr Email Notifications	47
7	Filr Indexing and Searching	49
7.1	What Is Indexed and When	49
7.2	About Filr Content Indexing	50
8	Filr Licensing	51
9	My Files (Personal Storage)	53
9.1	Understanding My Files	53
9.2	Enabling Personal Storage.	54
9.2.1	Personal Storage for All LDAP Users	54
9.2.2	Personal Storage for Individual Users and/or Groups	55
9.3	Restricting Disk Space Usage	56
9.4	Home Folders Vs. Net Folders.	56
9.5	My Files Sharing Rights	56
10	Net Folders	57
10.1	Overview	57
10.2	Specifying Net Folder Servers	59
10.3	Specifying Net Folders	61
10.4	Net Folder Proxy Users	63
10.4.1	The Functions Facilitated by Net Folder Proxy Users	63
10.4.2	Rights Required for Net Folder Proxy Users	63
10.4.3	Net Folder Proxy User Passwords.	64
10.5	Granting Access to Net Folders	64
11	Protocols and Filr	67
12	Sharing through Filr	69
12.1	Setting Up Sharing	70
12.1.1	System-Level Sharing Must Be Set Up First	70
12.1.2	My Files Sharing Is Automatic	71
12.1.3	Net Folder Sharing Must Be Explicitly Allowed At Two Levels	72
12.2	Understanding Roles and Sharing	73
12.2.1	User Roles and Sharing.	74
12.2.2	Users Can't Grant Share Roles That They Don't Have	74
12.2.3	File System Rights Also Affect the Ability to Assign Share Roles	74
12.3	A Caution Regarding the Re-sharing Feature	75

13 Filr Synchronization	77
13.1 Synchronization Overview	77
13.2 Net Folder Synchronization Detail Overview	80
13.3 Net Folder File Content Indexing Overview	81
14 Network Time and Filr	83
15 Viewing Files as HTML in Filr	85
16 Users and Groups with Filr	87
16.1 Leveraging the Built-in Security of eDirectory and Active Directory	87
16.2 Provisioning Users and Groups	87
16.2.1 User Provisioning Overview.	87
16.2.2 Types of Filr Users.	89
16.2.3 The Role of Groups in Filr	90
16.3 LDAP Proxy User Role and Rights.	90
A Documentation Updates	91

About This Guide

This guide contains high-level overviews of Novell Filr and covers the following topics:

- ♦ Chapter 1, “Filr Overview,” on page 9
- ♦ Chapter 2, “Setting Up Filr,” on page 13
- ♦ Chapter 3, “Filr Administration,” on page 29
- ♦ Chapter 4, “Access Rights and Filr,” on page 35
- ♦ Chapter 5, “Filr Comments,” on page 45
- ♦ Chapter 6, “Filr Email Notifications,” on page 47
- ♦ Chapter 7, “Filr Indexing and Searching,” on page 49
- ♦ Chapter 8, “Filr Licensing,” on page 51
- ♦ Chapter 9, “My Files (Personal Storage),” on page 53
- ♦ Chapter 10, “Net Folders,” on page 57
- ♦ Chapter 11, “Protocols and Filr,” on page 67
- ♦ Chapter 12, “Sharing through Filr,” on page 69
- ♦ Chapter 13, “Filr Synchronization,” on page 77
- ♦ Chapter 14, “Network Time and Filr,” on page 83
- ♦ Chapter 15, “Viewing Files as HTML in Filr,” on page 85
- ♦ Chapter 16, “Users and Groups with Filr,” on page 87
- ♦ Appendix A, “Documentation Updates,” on page 91

Audience

This guide is intended for Novell Filr administrators.

Feedback

Please use the User Comments feature at the bottom of each online documentation page to comment and suggest improvements to this guide and the other documentation included with Novell Filr.

Documentation Updates

The most recent version of this guide is available [here](http://www.novell.com/documentation/novell-filr1/filr1_overvw/data/bookinfo.html) (http://www.novell.com/documentation/novell-filr1/filr1_overvw/data/bookinfo.html) on the Novell Filr Web site.

Additional Documentation

For other Novell Filr documentation, see the [Novell Filr Web site](http://www.novell.com/documentation/novell-filr1/) (<http://www.novell.com/documentation/novell-filr1/>).

1 Filr Overview

Today's workers expect to access work files like they do personal files.

Some of them are moving work files to cloud-based services, which causes their risk managers to lose sleep.

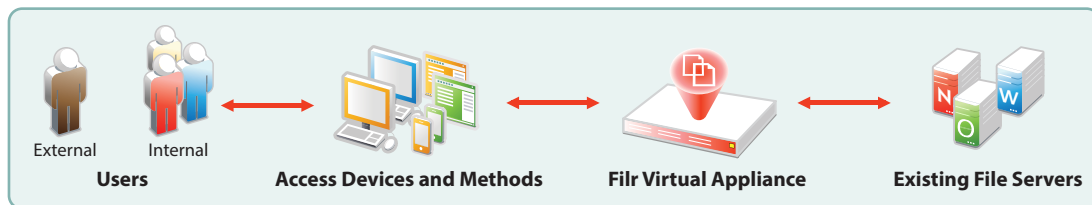
Novell Filr offers modern file access without compromising existing security systems.

- ♦ [Section 1.1, "What Is Novell Filr?," on page 9](#)
- ♦ [Section 1.2, "Filr Features and Functionality," on page 10](#)
- ♦ [Section 1.3, "Why Novell Appliances?," on page 11](#)

1.1 What Is Novell Filr?

Novell Filr provides file access and sharing, and lets users access their home directories and network folders from mobile devices and the Web. Users can also synchronize their files to their PC and Mac computers. They can also share files internally and externally, and comment on files.

Figure 1-1 Mobile Access to Enterprise Data



- ♦ **Users:** Filr lets you control the following:
 - ♦ User authentication inside and outside your organization
 - ♦ Access to organization files and folders that were previously accessible only through mapped drives
 - ♦ Access to personal files and folders in Filr-based storage in addition to traditional Windows, OES, and NetWare home directories
 - ♦ Internal and external sharing of files and folders
- ♦ **Access Devices and Methods:** Filr provides multiple access methods.
 - ♦ A Web (browser-based) application
 - ♦ An app for Apple iOS 6 (and later) personal devices
 - ♦ An app for Android 2.3.X (and later) personal devices
 - ♦ Clients for Windows XP, Windows 7, and Windows 8 workstations
 - ♦ A client for Macintosh OS X 10.7, 10.8, and 10.9 workstations
- ♦ **Filr Virtual Appliance:**
 - ♦ This runs on VMware, Xen, and Hyper-V hypervisors.

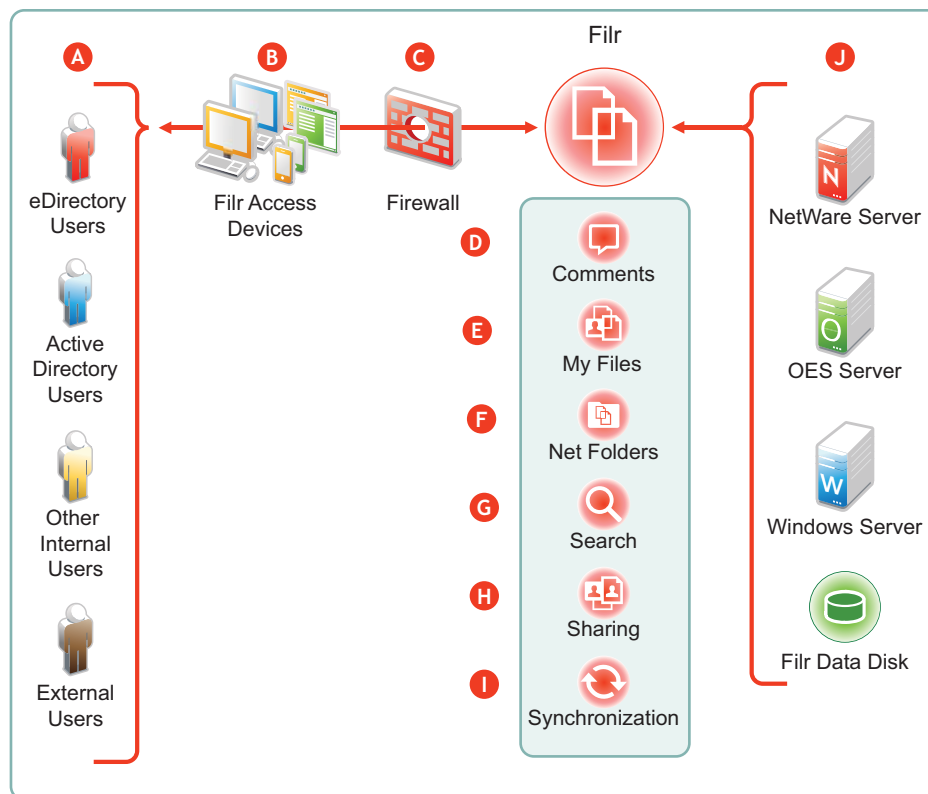
- ♦ It lets users authenticate using their eDirectory and Active Directory usernames and passwords.
- ♦ It provides access to data on NetWare, OES, and Windows servers that use native file protocols (NCP and CIFS).
- ♦ **Existing File Servers:** Are not impacted because Filr does the following:
 - ♦ Requires no changes to file servers
 - ♦ Honors file system trustee rights and attributes

Your Novell and Windows file servers and directory services retain complete control over all file- and folder-related activity.

1.2 Filr Features and Functionality

Figure 1-2 shows Filr's main features in the context of your existing network infrastructure. The table that follows the figure briefly describes each feature and how all of the components shown fit together to provide Filr services.

Figure 1-2 What Filr Provides



Letter	Details
A	<ul style="list-style-type: none"> ♦ eDirectory and Active Directory: You synchronize Filr with eDirectory and Active Directory identity stores through LDAP. See “Synchronizing Users and Groups from an LDAP Directory” in the <i>Novell Filr 1.1 Administration Guide</i>. ♦ Local Users: You can create users on the Filr system independent of any LDAP source. For more information, see “Creating a New Local User” in the <i>Novell Filr 1.1 Administration Guide</i>. ♦ External Users: When a user outside the organization responds to an invitation to share a file or folder, Filr creates a username using the invitation’s email address. When users accept these invitations, they can set their passwords. For more information, see “Sharing Files and Folders” in the <i>Novell Filr 1.1 Web Application User Guide</i>.
B	<p>Filr lets users access files and folders through the following:</p> <ul style="list-style-type: none"> ♦ A Web (browser-based) application ♦ Apps for Apple iOS 6 and later and Android 2.3.X and later ♦ Clients for Windows XP, Windows 7, Windows 8, Macintosh OS X 10.7, 10.8, and 10.9 workstations
C	<p>Filr is designed to work with your security infrastructure. Your firewalls continue to protect your data while Filr provides access to it from practically anywhere. For more information, see “Site Security” in the <i>Novell Filr 1.1 Administration Guide</i>.</p>
D	<p>Filr lets users collaborate by supporting user comments on files and folders. For more information, see “Filr Comments” on page 45.</p>
E	<p>Filr lets users access their personal files and folders on either or both traditional home directories and local Filr storage. For more information, see “My Files (Personal Storage)” on page 53.</p>
F	<p>Filr lets users access your organization’s files and folders that were previously available only through mapped drives. For more information, see “Net Folders” on page 57.</p>
G	<p>Filr lets users search for files and folders that they have rights to access. If indexing is enabled on a folder, they can search within the content of the folder’s files as well. For more information, see “Filr Indexing and Searching” on page 49.</p>
H	<p>Filr lets users share files in Net Folders, and files and folders in My Files, with internal and external users. For more information, see “Sharing through Filr” on page 69.</p>
I	<p>Filr lets you synchronize eDirectory and Active Directory users as well as files and folders according to your organization’s needs. For more information, see “Filr Synchronization” on page 77.</p>
J	<p>Filr provides access to storage on Novell file servers, Windows file servers, and personal storage on the Filr appliance.</p>

1.3 Why Novell Appliances?

Novell appliances simplify the Novell development and delivery model for Filr so that we can provide you with new services more quickly.

Novell appliance benefits include the following:

- ♦ **Simplified Deployment:** Filr appliances are built on specific and tuned operating systems (SLES 11 SP3 in the case of Filr 1.1). This means that you don’t have to install the operating system, select the packages, and so on because everything needed is included and ready to configure and run.

By the same token, packages and services that aren't needed aren't included, and therefore they don't consume system resources.

- ♦ **Simplified Management:** Appliances include the following:
 - ♦ Appliance-specific configuration wizards to configure exactly and only what is required.
 - ♦ Web-based administration tools for changing configurations, adding or provisioning users, and so on, from basically anywhere that you need to be.

2 Setting Up Filr

This section presents high-level overviews of the following setup tasks. For detailed setup information and instructions, see the [Novell Filr 1.1 Installation and Configuration Guide](#).

- [Section 2.1, “Getting and Preparing Filr Software,” on page 13](#)
- [Section 2.2, “Deploying Filr Appliances,” on page 16](#)
- [Section 2.3, “Initial Configuration of Filr Appliances,” on page 18](#)
- [Section 2.4, “Filr Clustering \(Expanding a Deployment\),” on page 21](#)
- [Section 2.5, “Integrating Filr Inside Your Network Infrastructure,” on page 23](#)
- [Section 2.6, “Ports Used in Filr Deployments,” on page 26](#)
- [Section 2.7, “There Are No Changes to Existing Servers or Systems,” on page 27](#)

2.1 Getting and Preparing Filr Software

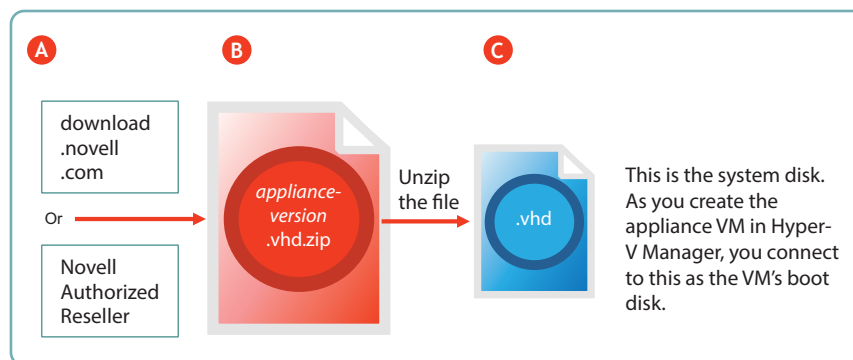
The process of getting and preparing Filr software is straightforward, as illustrated in the following sections.

- [Section 2.1.1, “Hyper-V,” on page 13](#)
- [Section 2.1.2, “VMware,” on page 14](#)
- [Section 2.1.3, “Xen,” on page 15](#)

For more information, see “[Installing the Filr Appliance](#),” “[Installing the Search Index Appliance](#),” and “[Installing the MySQL Database Appliance](#)” in the [Novell Filr 1.1 Installation and Configuration Guide](#).

2.1.1 Hyper-V

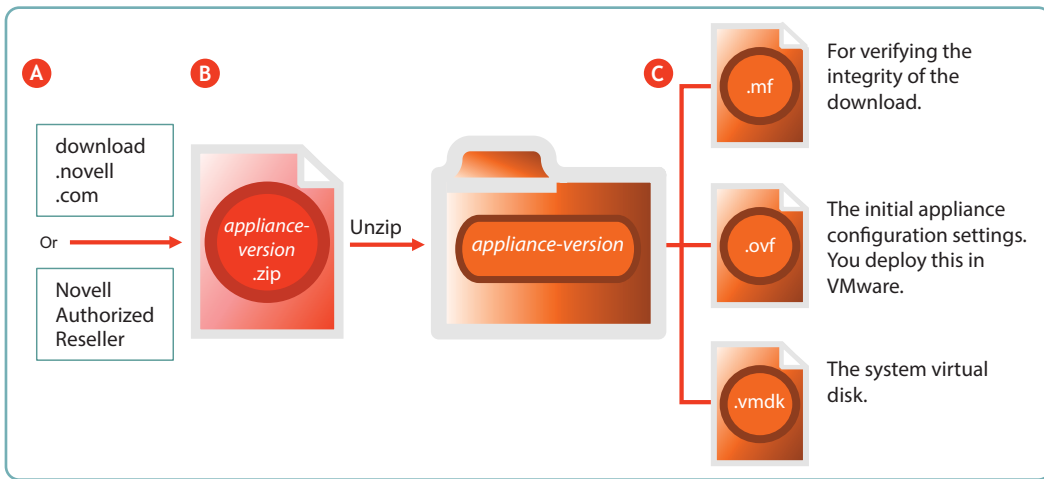
Figure 2-1 Downloading and Preparing Novell Appliances for Hyper-V



Letter	Details
A	You can download the .zip archive files for the Hyper-V build of the three Novell Filr appliances (Filr, Search, and MySQL) directly from the Novell Download Site , or you can obtain them through your Novell Authorized Reseller .
B	Unzip the archive to expose the appliance system disk image. For more information, see “Installing the Filr Appliance,” “Installing the Search Index Appliance,” and “Installing the MySQL Database Appliance” in the Novell Filr 1.1 Installation and Configuration Guide .
C	<p>The .vhd file is a Hyper-V disk image that contains all of the appliance's system files.</p> <p>You connect to this file in Hyper-V Manager by selecting the <i>Use an existing virtual hard disk</i> option.</p> <p>Unlike VMware and Xen, no pre-configured settings file is supplied for the VM. Instead you specify the RAM, network card, additional disks, and so on as instructed in the Novell Filr 1.1 Installation and Configuration Guide.</p>

2.1.2 VMware

Figure 2-2 Downloading and Preparing Novell Appliances for VMware

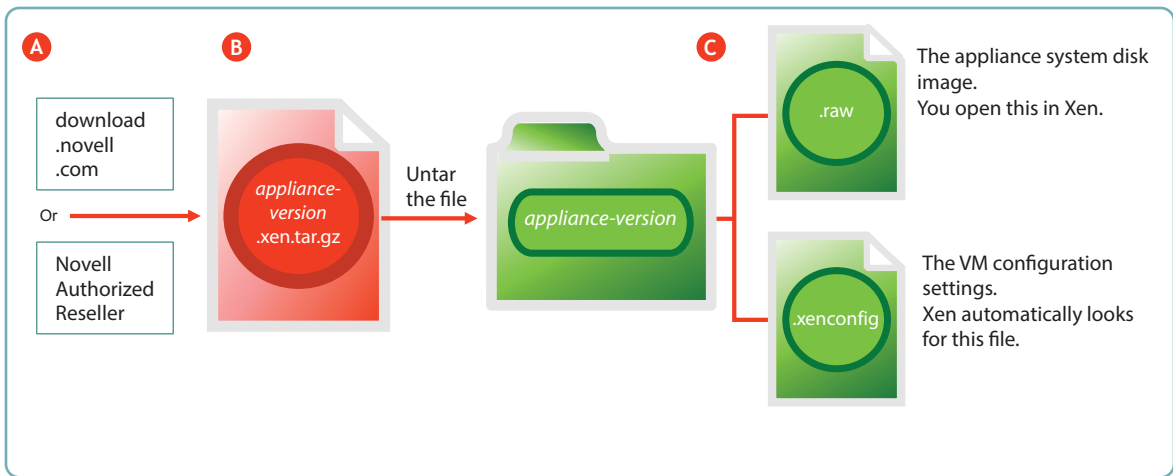


Letter	Details
A	You can download the .zip archive files for the VMware build of the three Novell Filr appliances (Filr, Search, and MySQL) directly from the Novell Download Site , or you can obtain them through your Novell Authorized Reseller .
B	Unzip the archives to expose a folder that contains the three files needed for deployment. For more information, see “Installing the Filr Appliance,” “Installing the Search Index Appliance,” and “Installing the MySQL Database Appliance” in the Novell Filr 1.1 Installation and Configuration Guide .

Letter	Details
C	<p>The <code>.mf</code> file contains an SHA1 digest that VMware uses to verify the integrity of the other two files.</p> <p>The <code>.ovf</code> file contains the virtual appliance's configuration settings. You open and deploy this file in VMware to create the Filr appliance. You modify its settings during the initial deployment phase.</p> <p>The <code>.vmdk</code> file is the virtual appliance's (VA's) system virtual disk and contains all VA system files. It comes ready for the initial start-up and configuration.</p>

2.1.3 Xen

Figure 2-3 Downloading and Preparing Novell Appliances for Xen



Letter	Details
A	You can download the <code>.zip</code> archive files for the Xen build of the three Novell Filr appliances (Filr, Search, and MySQL) directly from the Novell Download Site , or you can obtain them through your Novell Authorized Reseller .
B	Untar the archives to expose a folder that contains the two files needed for deployment. For more information, see " Installing the Filr Appliance ," " Installing the Search Index Appliance ," and " Installing the MySQL Database Appliance " in the Novell Filr 1.1 Installation and Configuration Guide .
C	<p>The <code>.raw</code> file contains the system disk image. You open this file in Xen to begin the deployment process</p> <p>The <code>.xenconfig</code> file contains the virtual appliance's configuration settings. You modify its settings during the initial deployment phase.</p>

2.2 Deploying Filr Appliances

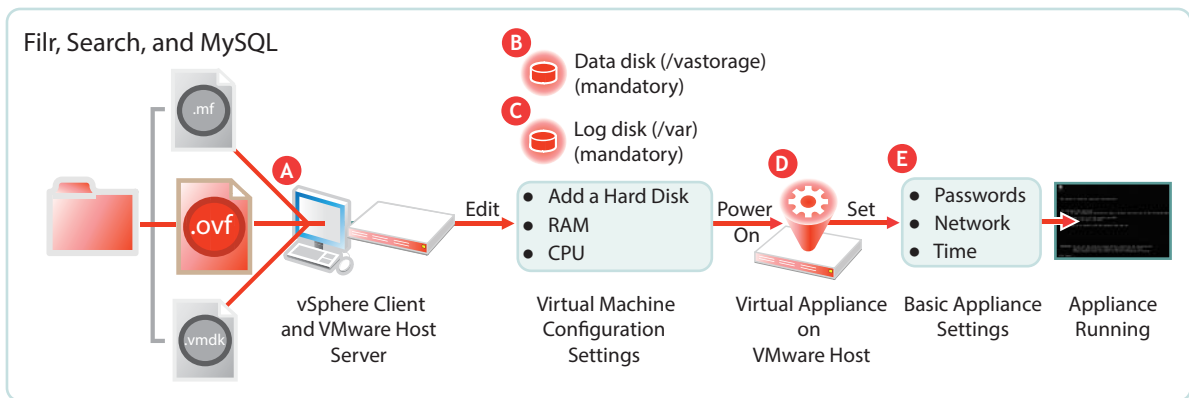
After you have obtained and extracted the appliance software, you need to deploy it on your VMware host server, as illustrated in [Figure 2-4](#) and [Figure 2-5](#) and as explained in the tables that follow them. For more specific information about the different deployment models, see “[Planning the Deployment Type](#)” in the *Novell Filr 1.1 Administration Guide*.

- ♦ [Section 2.2.1, “Small Filr Deployment Overview,”](#) on page 16
- ♦ [Section 2.2.2, “Large Filr Deployment Overview,”](#) on page 17

2.2.1 Small Filr Deployment Overview

NOTE: After initial VM preparation is completed, deploying on Hyper-V and Xen is comparable to the VMware steps illustrated below.

Figure 2-4 A Small Deployment of Filr on VMware



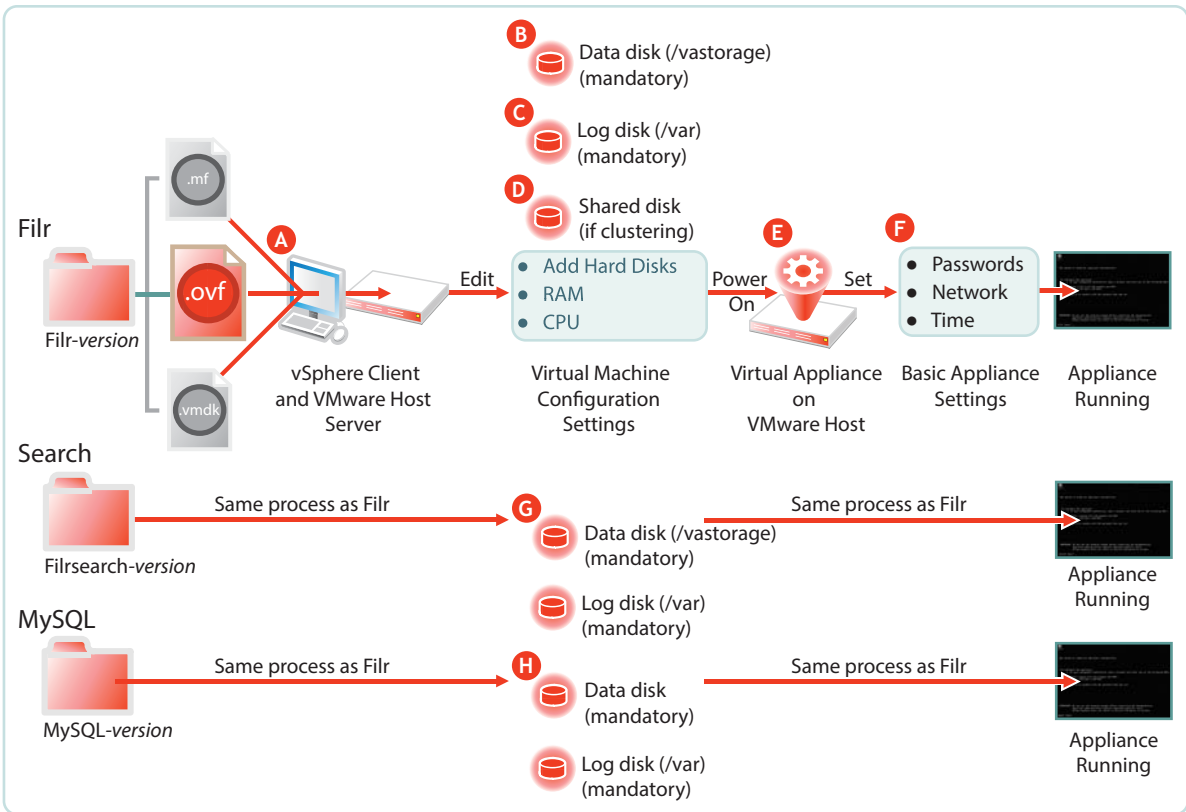
Letter	Details
A	<p>Using the vSphere client, access the VMware host server and deploy the .ovf template file.</p> <p>Specify the hostname and IP address. If possible, the system determines the mask and gateway, and automatically populates those fields.</p> <p>The network interface is bridged by default. Make sure this setting matches the network configuration in your VMware environment.</p>
B	<p>A second disk is needed for the following reasons:</p> <ul style="list-style-type: none"> ♦ Adequate personal storage disk space—personal files are stored here. ♦ Separation of system and data files to facilitate appliance updates—data files are stored here. <p>You might want to also change the RAM allocation and the number of CPUs.</p>
C	<p>A third disk is needed for storing log files, which prevents the system disk from running out of space.</p>
D	<p>Start the appliance.</p>

Letter	Details
E	Specify the appliance's basic configuration, which includes administrative users' passwords, IP address settings, and the time zone and NTP time source. These settings are common to all Novell appliances.

2.2.2 Large Filr Deployment Overview

NOTE: After initial VM preparation is completed, deploying on Hyper-V and Xen is comparable to the VMware steps illustrated below.

Figure 2-5 A Large Deployment of Filr



Letter	Details
A	Using the vSphere client, access the VMware host server and deploy the .ovf template file. Specify the hostname and IP address. If possible, the system determines the mask and gateway, and automatically populates those fields. The network interface is bridged by default. Make sure this setting matches the network configuration in your VMware environment.

Letter	Details
B	<p>A second disk is needed for the following reasons:</p> <ul style="list-style-type: none"> ♦ Adequate personal storage disk space ♦ Separation of system and data files to facilitate appliance updates <p>You might want to also change the RAM allocation and the number of CPUs.</p>
C	<p>A third disk is needed for storing log files, which prevents the system disk from running out of space.</p>
D	<p>If you are clustering the Filr VA, add a shared CIFS or NFS disk to all of the Filr VAs in the cluster to use.</p> <p>This only applies to the Filr VA, not to the Search or MySQL appliances.</p>
E	<p>Start the appliance.</p>
F	<p>Specify the appliance's basic configuration, which includes administrative users' passwords, IP address settings, and the time zone and NTP time source.</p> <p>These settings are common to all Novell appliances.</p>
G	<p>If you are installing separate appliances, you need to deploy at least one and preferably two search appliances as well. The process is very similar to a Filr VA deployment, except that the search appliances don't use shared storage.</p>
H	<p>Installing separate appliances also requires configuring a MySQL or MS SQL database. Deploying the MySQL appliance that comes with Filr is very similar to the process for Filr and the search appliances.</p> <p>If you already have a MySQL or MS SQL database in your organization, you can use it instead of the MySQL appliance that comes with Filr.</p>

2.3 Initial Configuration of Filr Appliances

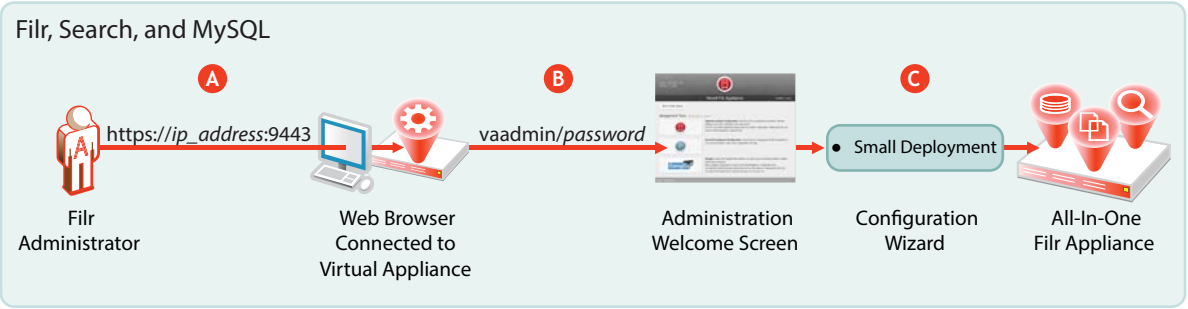
After you have deployed the appliances and set a few basic system settings, such as passwords, you must perform an initial appliance configuration. The process varies, depending on which deployment scenario you are implementing.

- ♦ [Section 2.3.1, “Small Filr Deployment Configuration,” on page 18](#)
- ♦ [Section 2.3.2, “Large Filr Deployment Configuration,” on page 19](#)

2.3.1 Small Filr Deployment Configuration

Starting and configuring an all-in-one Filr appliance is quite straightforward, as illustrated in [Figure 2-6](#) and explained in the table that follows it.

Figure 2-6 Configuring an All-in-One Filr Appliance



Letter	Details
A	Access and configure the Filr appliance through a browser.
B	Log in to the administration console.
C	Run the configuration wizard. When you finish, your all-in-one appliance is running and ready to provide Novell Filr services.

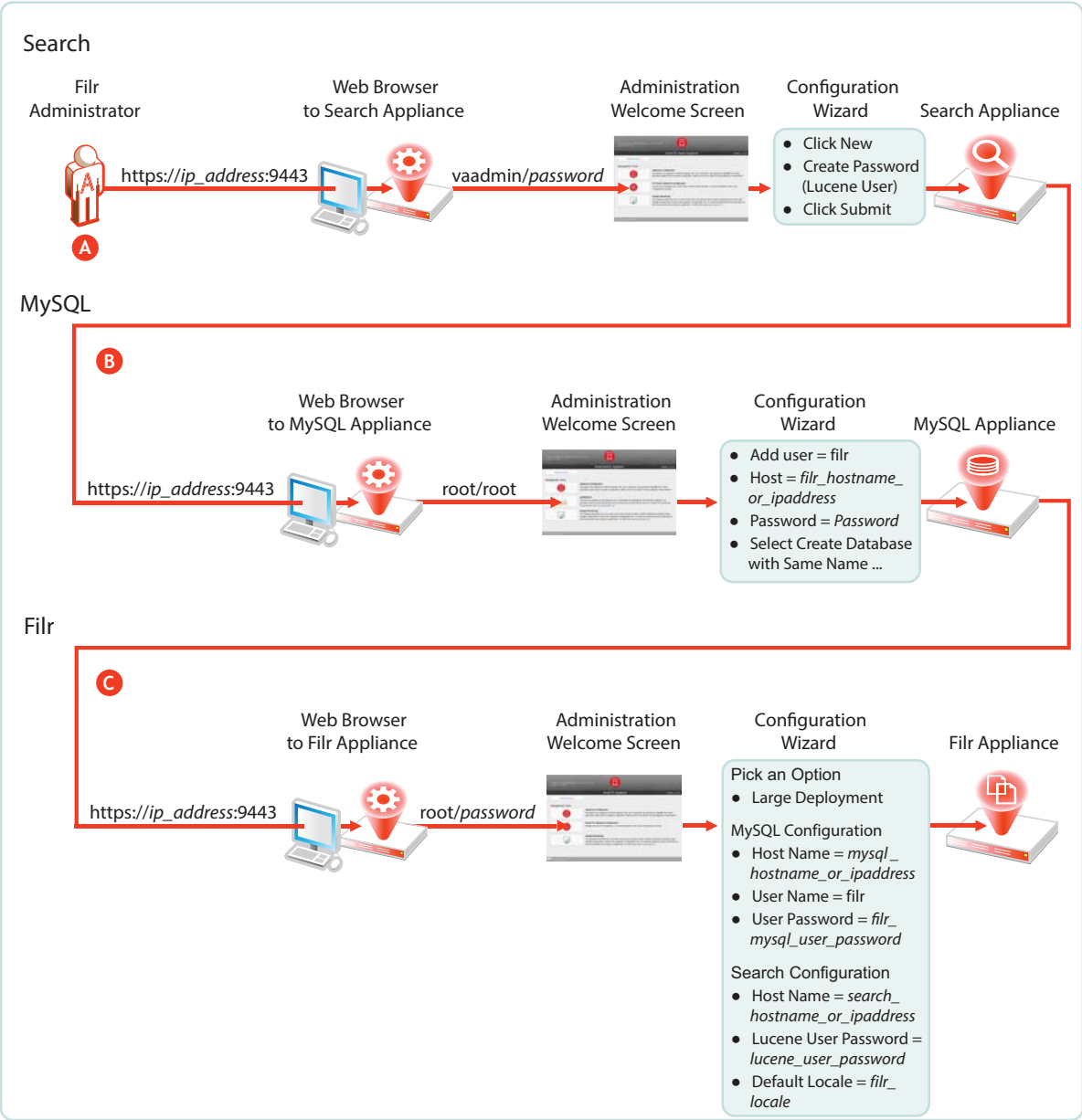
For more information, see “[Configuring a Small Deployment for the First Time](#)” in the *Novell Filr 1.1 Installation and Configuration Guide*.

2.3.2 Large Filr Deployment Configuration

Starting and configuring the appliances for a large deployment is more involved than for a single appliance. However, the process is well documented and also very straightforward, as illustrated in [Figure 2-7](#) and explained in the table that follows it.

Notice that the order of working with the three appliance types is reversed from the order in [Figure 2-5](#) on page 17.

Figure 2-7 Configuring Separate Appliances



Letter	Details
A	<p>First, access and configure the Search appliances through a browser, logging in to the administration console, and running the configuration wizard.</p> <p>When you finish this step, your Search appliances are running and ready to provide indexing services for Filr.</p> <p>For details, see “Installing the Search Index Appliance” in the <i>Novell Filr 1.1 Installation and Configuration Guide</i>.</p>

Letter	Details
B	<p>Second, access and configure the MySQL database appliance through a browser, or configure your database server.</p> <p>If using the MySQL database appliance, use the phpMyAdmin utility to configure the appliance, as instructed in “Installing the MySQL Database Appliance” in the <i>Novell Filr 1.1 Installation and Configuration Guide</i>.</p> <p>When you finish this step, your database appliance is running and ready to provide services to the Filr appliance.</p>
C	<p>Finally, access and configure the Filr appliance through an administrative browser, logging in to the administrative console, and running the configuration wizard.</p> <p>For more information, see “Configuring a Large Deployment for the First Time” in the <i>Novell Filr 1.1 Installation and Configuration Guide</i>.</p> <p>When you finish this step, your virtual appliances are all running and working with each other, providing your network with Filr services.</p>

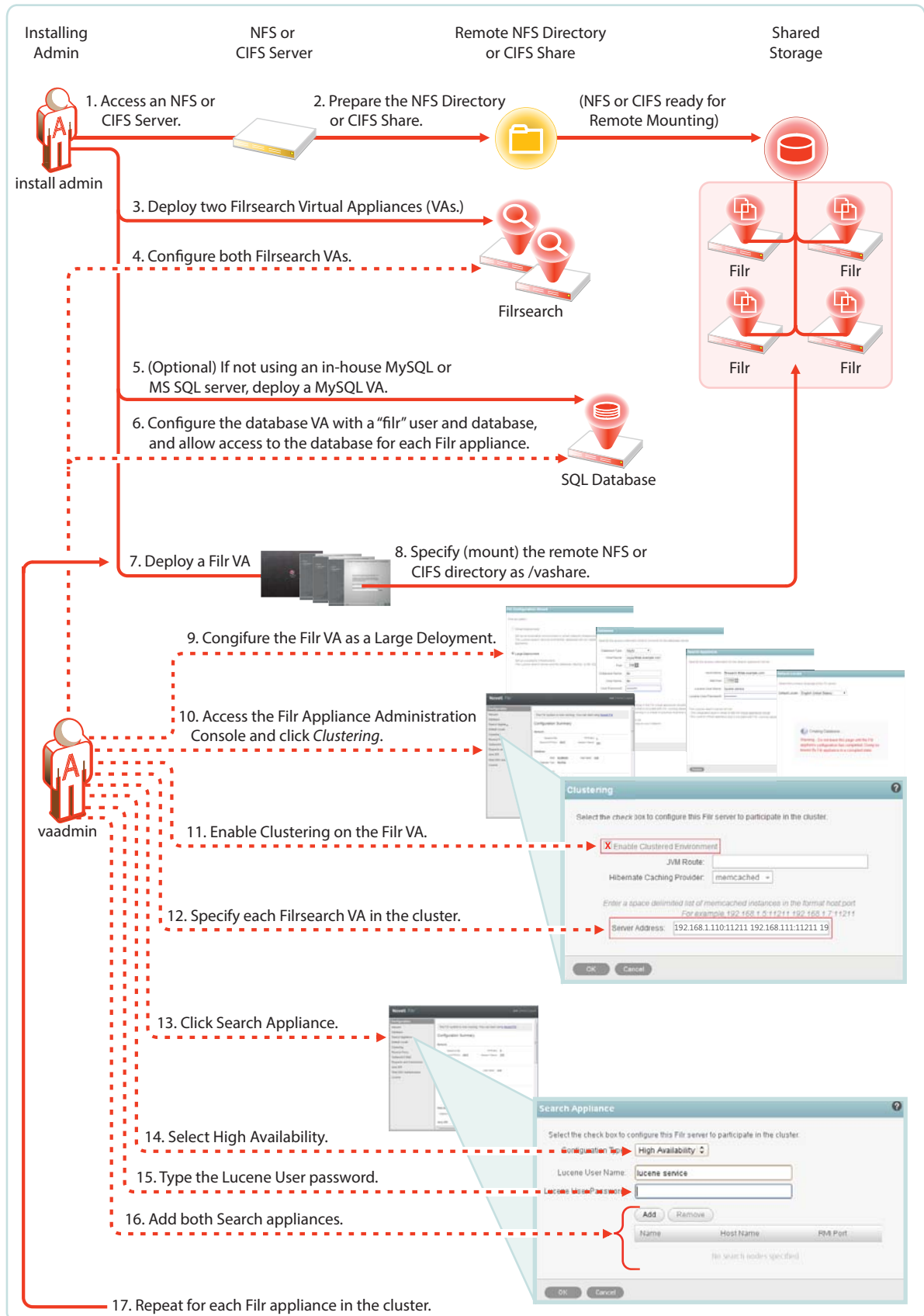
For more information, see “[Creating a Large Deployment](#)” in the *Novell Filr 1.1 Installation and Configuration Guide*.

2.4 Filr Clustering (Expanding a Deployment)

Filr clustering involves two or more Filr VAs sharing the same NFS or CIFS data storage location (/vashare). You can only create a cluster if your Filr appliances were deployed pointing to the same /vashare disk.

Basic steps for setting up Filr clustering are included in [Figure 2-8](#).

Figure 2-8 Clustered Filr VAs



For step-by-step instructions, see “[Setting Up a Large, Expandable \(Clustered\) Deployment](#)” in the *Novell Filr 1.1 Planning and Deployment Best Practices Guide*.

For more information about clustering, see “[Multi-Server \(Clustered\) Deployment](#)” in the *Novell Filr 1.1 Installation and Configuration Guide*.

2.5 Integrating Filr Inside Your Network Infrastructure

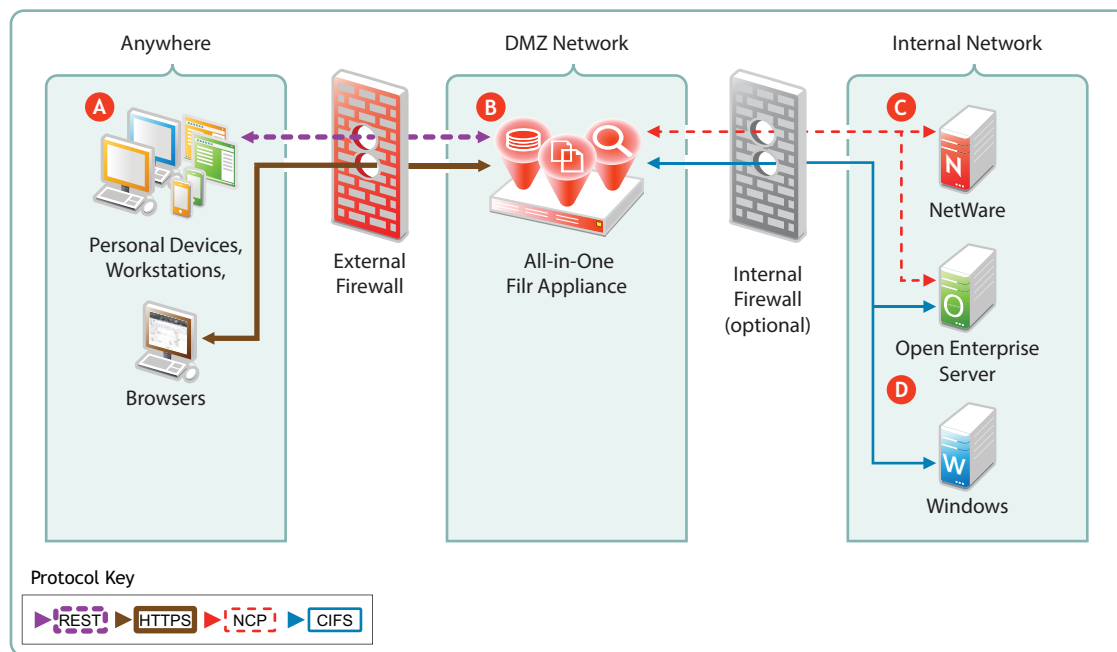
The following examples illustrate two possibilities out of many potential network configurations for deploying Filr.

- ♦ [Section 2.5.1, “A Small Filr Deployment,” on page 23](#)
- ♦ [Section 2.5.2, “A Large Filr Deployment,” on page 25](#)

2.5.1 A Small Filr Deployment

Figure 2-9 illustrates a high-level view of how an all-in-one appliance might be integrated into a small organization’s network. Each letter is explained in the table that follows the figure.

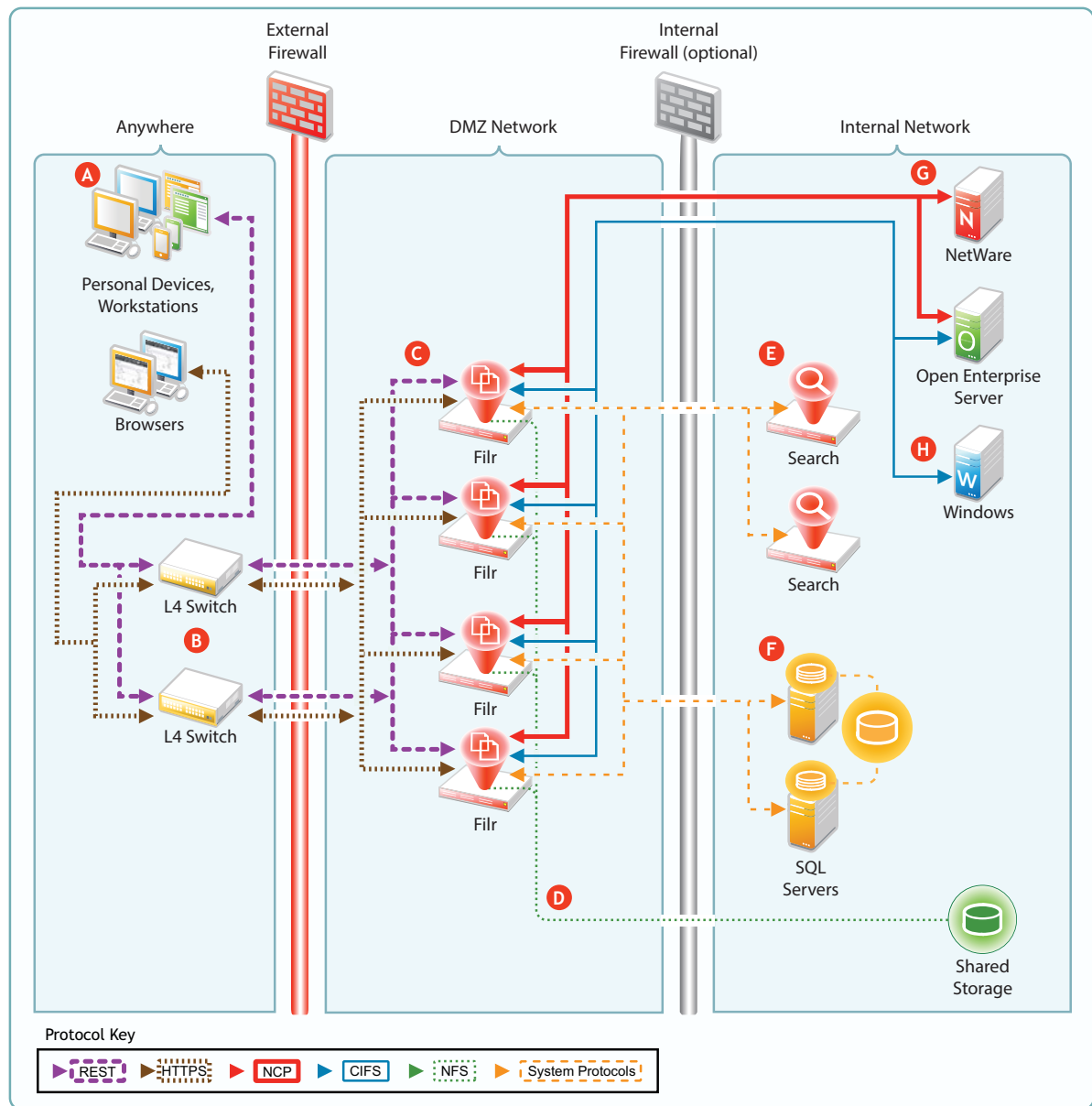
Figure 2-9 Example of a Small Filr Deployment



Letter	Details
A	Filr brings Novell and Windows file services to personal devices, Macintosh and Windows workstations, and Web browsers.
B	Filr is built for fitting in with your security infrastructure and can be deployed in a DMZ network, allowing your organization's data to remain safely inside your internal network.
C	Filr provides full NCP protocol support. Users have access to files stored on both NetWare and Open Enterprise Server file servers.
D	Filr provides full CIFS protocol support to servers providing CIFS file services, such as Windows file servers.

2.5.2 A Large Filr Deployment

Figure 2-10 Example of a Large Filr Deployment



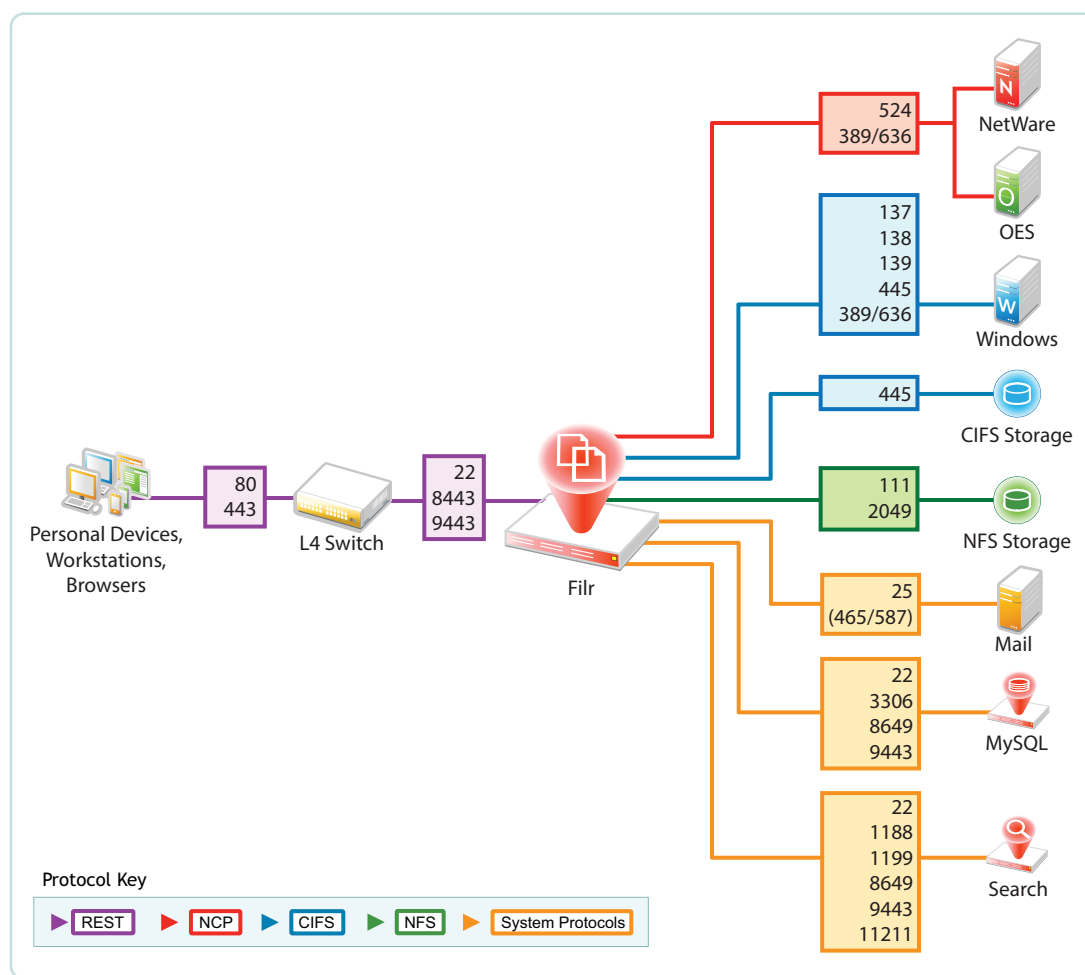
Letter	Details
A	Filr brings Novell and Windows file services to personal devices, Macintosh and Windows workstations, and Web browsers.
B	You can use L4 switches to provide load balancing of REST requests to your Filr appliances. Although not shown, you can, of course, also use software-based load balancers for this.
C	You can deploy Filr appliances inside a front-end DMZ and configure multiple Filr VAs to share NFS- or CIFS-based storage (D), thus providing scalability and high availability.

Letter	Details
D	Shared storage (/vashare) lets you expand your Filr deployment to include multiple Filr VAs (C). Although an exported NFS disk is shown in the illustration, CIFS shares are also supported.
E	You can deploy multiple search appliances in an internal network, each of which maintains indexes of Filr data to provide failover for search and other requests coming through the Filr appliances.
F	Your organization's MySQL or MS SQL servers can be deployed in the internal network and configured to access the same database.
G	As with small deployments, this configuration supports NCP file services.
H	CIFS file services are also supported.

2.6 Ports Used in Filr Deployments

As you configure the firewalls in your deployment, allow traffic on the ports indicated in [Figure 2-11](#), as applicable on your network.

Figure 2-11 Filr Port Usage



2.7 There Are No Changes to Existing Servers or Systems

- ♦ **File Servers:** Filr requires no changes to existing file servers or directory services. There is no new software to install on existing file servers.
- ♦ **File Systems:** There are no changes to existing file systems. File system rights, trustee assignments, storage quotas, and so on are all honored. This is because all file access is controlled by the file systems just as it was before Filr was installed.
- ♦ **Directory Services:** There are no schema extensions or other changes required to existing directory services.

3 Filr Administration

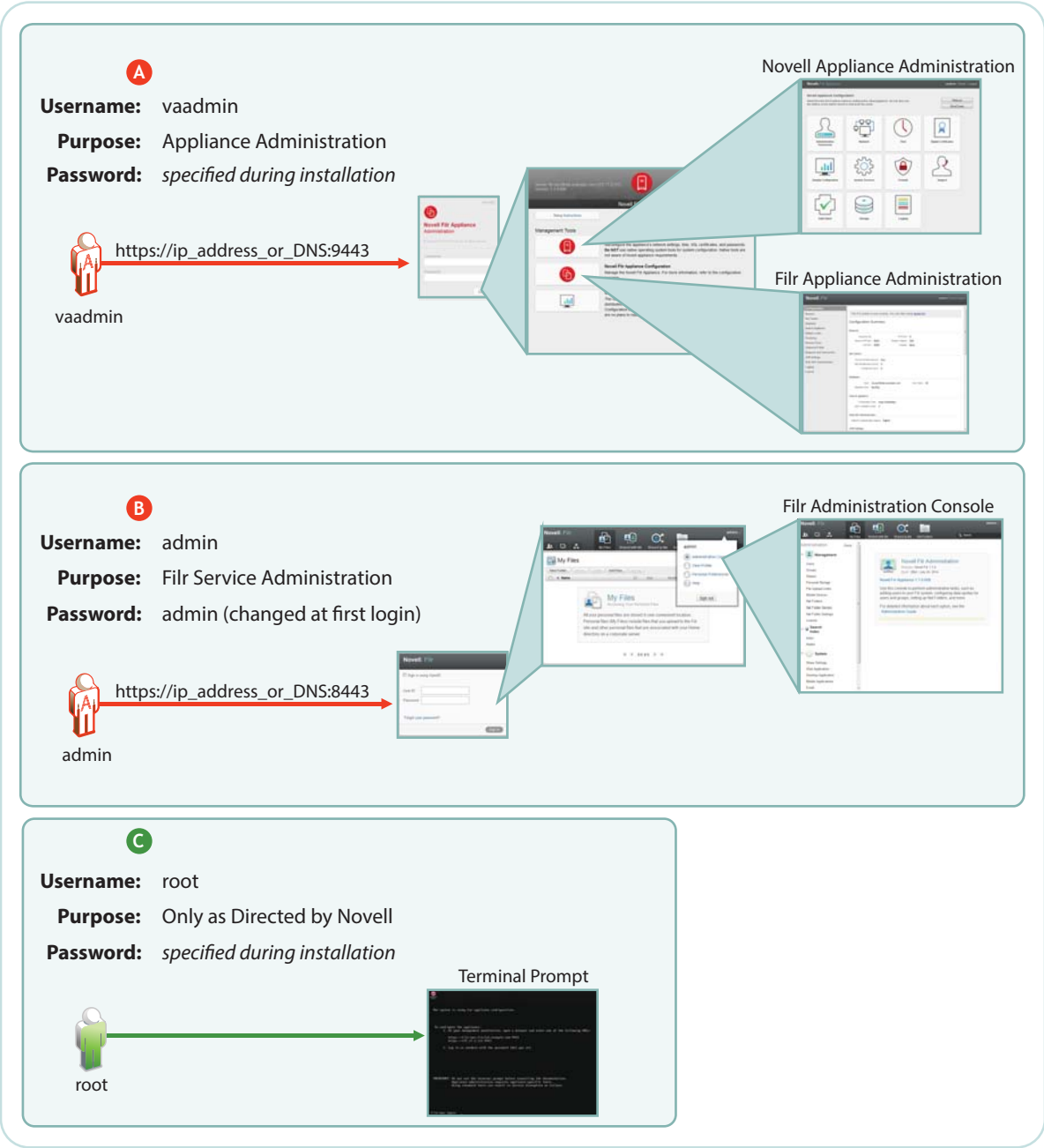
Filr administration is very straightforward as outlined in the following sections.

- ♦ [Section 3.1, “Filr Administrative Users,” on page 29](#)
- ♦ [Section 3.2, “Ganglia Appliance Monitoring,” on page 31](#)
- ♦ [Section 3.3, “Updating Appliances,” on page 32](#)
- ♦ [Section 3.4, “Certificate Management in Filr,” on page 33](#)
- ♦ [Section 3.5, “Filr Site Branding,” on page 34](#)

3.1 Filr Administrative Users

Because Filr is an appliance that is installed and administered in different phases, you install and then administer Filr using two different administrative users to provide separation of duties. Each user utilizes different Web-based administrative tools, as illustrated in [Figure 3-1](#) and explained in the table that follows it.

Figure 3-1 Filr Administrators: Their Purposes, Passwords, and the Interfaces They Use



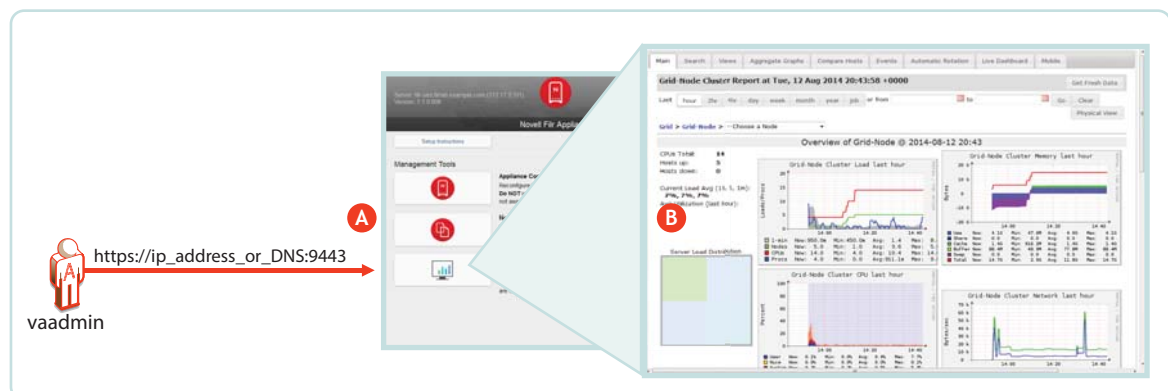
Letter	Details
A	<p>vaadmin takes over the installation process after the initial deployment is finished. It then configures appliance services so that they are fully operational.</p> <p>You use this administrative user whenever appliance settings need to be changed or adjusted. Installing certificates and licenses, adjusting the network configuration, and setting up Filr clustering are just a few of the tasks that you use vaadmin to perform.</p>

Letter	Details
B	<p>After the appliances are fully operational, most of the administrative work is accomplished using the Filr <code>admin</code> user account.</p> <p>The first time you log in, the username/password are <code>admin/admin</code>. You are prompted to change this. See “Changing the Filr Administrator Password” in the <i>Novell Filr 1.1 Administration Guide</i>.</p> <p>You use this administrative user to do the following:</p> <ul style="list-style-type: none"> ◆ Import (synchronize) users and groups from LDAP identity stores ◆ Create additional Filr users ◆ Set up My Files personal storage ◆ Set up Net Folders ◆ Set synchronization schedules ◆ Manage access ◆ Manage quotas ◆ Manage shares
C	<p>Novell Filr and the appliances associated with it are special-purpose virtual machines. They are designed to be configured and managed using the Web-based management consoles (above). Although it is possible to access the appliance using the terminal prompt or through an SSH connection, Novell strongly discourages this practice because it can result in service disruption or more serious problems, including data loss.</p> <p>If you contact Novell Support with a Filr support incident, you might be asked to access the appliance’s terminal prompt as the <code>root</code> user. Otherwise, there are no Filr administrative tasks that involve <code>root</code> or the bash interface.</p>

3.2 Ganglia Appliance Monitoring

By launching the Ganglia monitoring page, as shown in [Figure 3-2](#), you can access various real-time monitoring statistics for all of the Ganglia-enabled machines on your network segment.

Figure 3-2 Ganglia Appliance Monitoring



Letter	Details
A	The <code>vaadmin</code> administrative user has access to Ganglia monitoring, via the Appliance Configuration and Maintenance Web page.
B	<p>At the top of the Ganglia Web page are graphs that represent an aggregation of all of the Ganglia-enabled machines that are being monitored on your network segment.</p> <p>At the bottom of the page are graphs for each machine that is being monitored. By clicking an individual machine's graph, you can get its details. For example, on a Filr appliance you see Filr metrics, <code>/vastorage</code> monitoring, CPU load, disk statistics, memory usage, and all of the standard Ganglia metrics.</p>

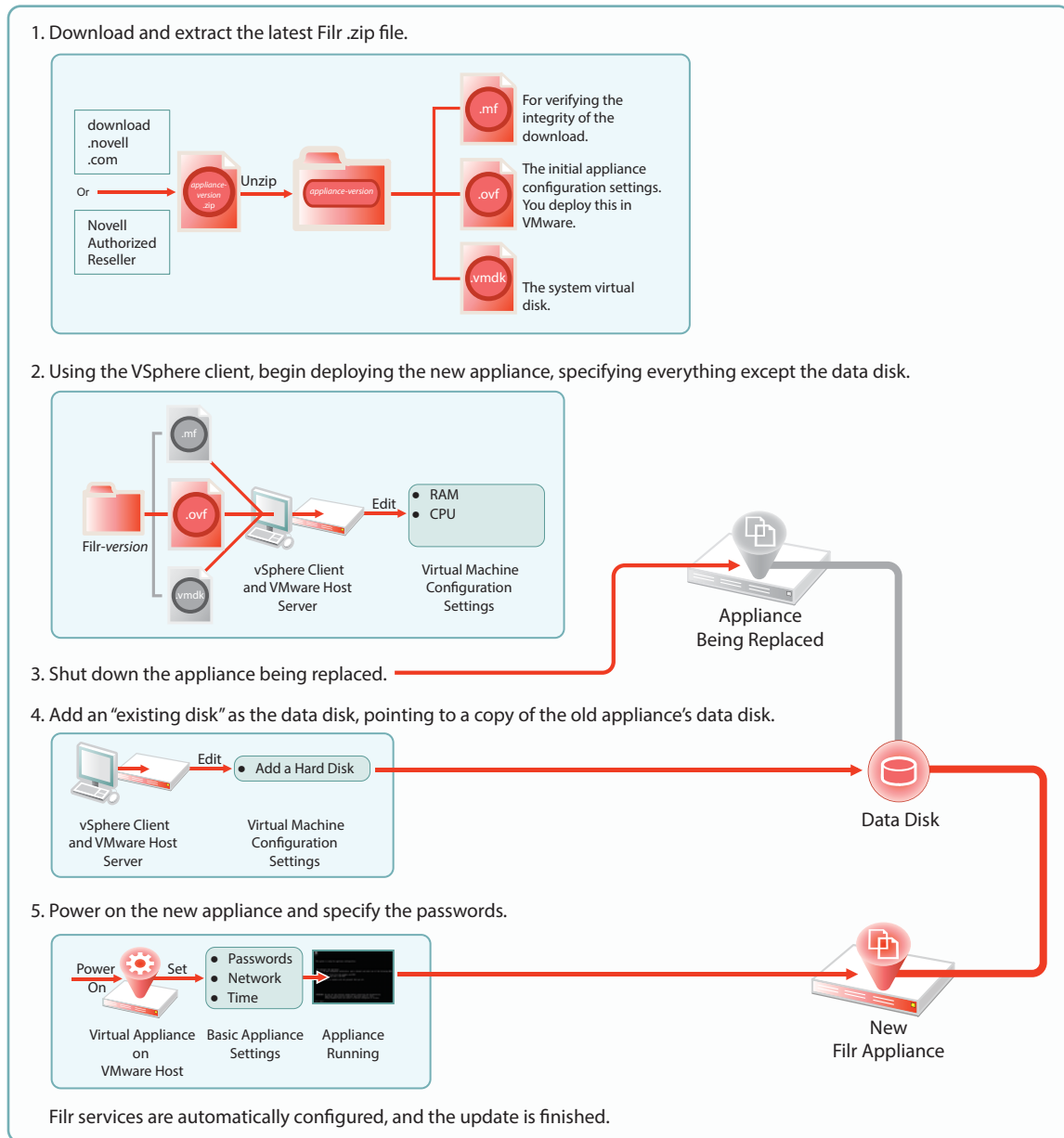
If you want to learn more about using and customizing Ganglia, you might consider investing in publications on the subject, such as the book [Monitoring with Ganglia](#), which was written by developers and others associated with the Ganglia project.

3.3 Updating Appliances

Filr and Search appliances are updated by simply installing a new appliance system disk and linking it to the existing data disk, as illustrated in [Figure 3-3](#).

IMPORTANT: While performing an upgrade, be sure to consult the detailed instructions in “[Upgrading Filr](#)” in the [Novell Filr 1.1 Installation and Configuration Guide](#). A successful upgrade depends on following sub-tasks that are not illustrated here, such as the order in which appliances are shut down and then restarted.

Figure 3-3 Updating a Filr or Search Appliance

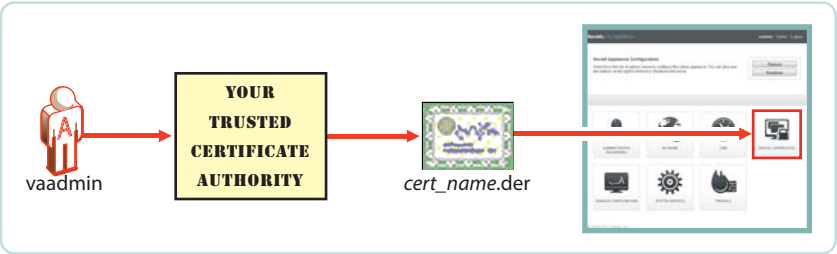


3.4 Certificate Management in Filr

So that your Web client users don't receive security warnings when accessing Filr, we recommend that you configure Filr with a certificate from your CA, as illustrated in [Figure 3-4](#). This will ensure that browsers will trust the Filr appliance as a valid server.

You can also set up Filr as a client to trust other servers. For example, if your LDAP identity store requires SSL communications (LDAPS), you can import the trusted CA certificate from your identity store server.

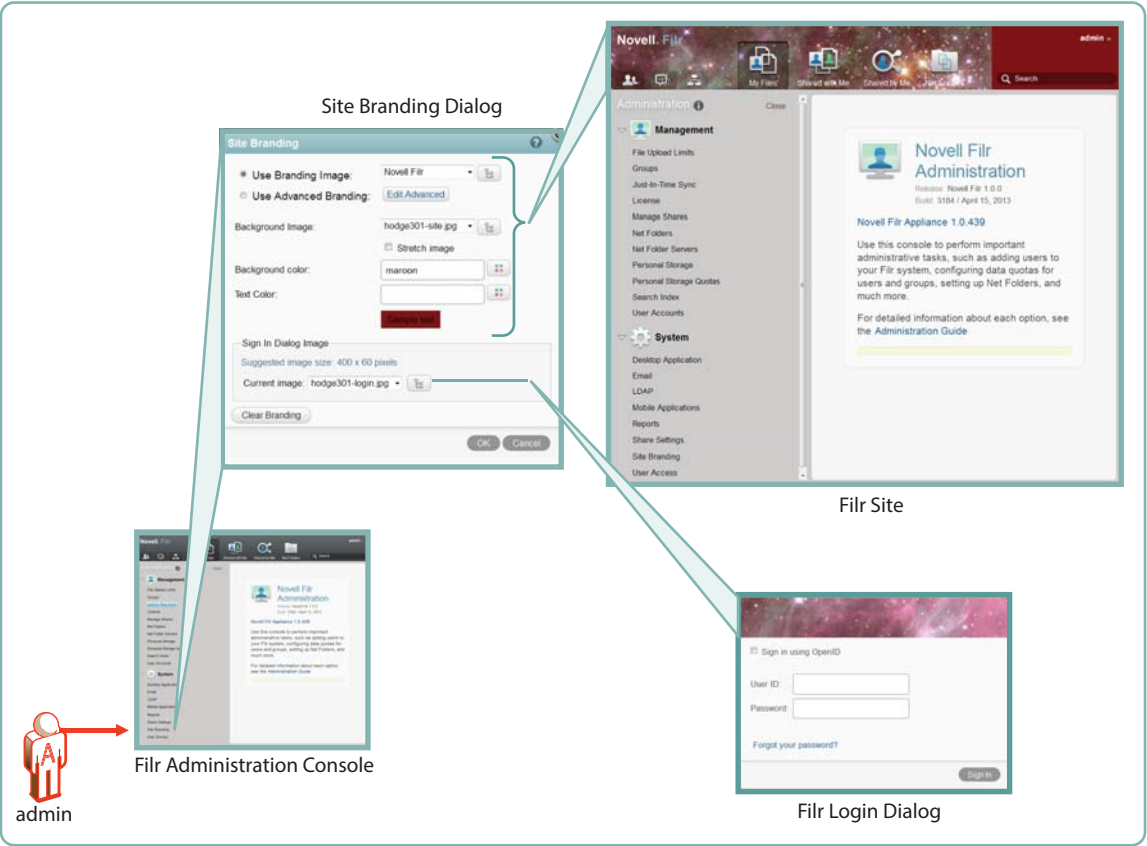
Figure 3-4 Importing a CA certificate



3.5 Filr Site Branding

You can customize the colors and images displayed on the Filr site and the login dialog box, as illustrated in Figure 3-5. Customizations are retained when Filr is upgraded. For more information, see “Setting Up Site Branding” in the *Novell Filr 1.1 Administration Guide*.

Figure 3-5 Branding Filr



4 Access Rights and Filr

Filr administrators need to have a good understanding of how Filr leverages the file system and other rights that are already in place, and also how user rights to use Filr functionality are determined.

- ♦ [Section 4.1, “Filr Authentication,” on page 35](#)
- ♦ [Section 4.2, “Access to Files and Folders Is Controlled by the File System,” on page 36](#)
- ♦ [Section 4.3, “How Users Get the Required Access Permissions,” on page 36](#)
- ♦ [Section 4.4, “Access Through Filr Involves One of Four Possible Roles,” on page 37](#)
- ♦ [Section 4.5, “Role Requirements Are Rigidly Enforced,” on page 40](#)
- ♦ [Section 4.6, “Rights to Files and Folders,” on page 41](#)
- ♦ [Section 4.7, “Sharing Rights,” on page 43](#)
- ♦ [Section 4.8, “Windows Share Rights,” on page 44](#)
- ♦ [Section 4.9, “Access-based Enumeration \(Windows\),” on page 44](#)

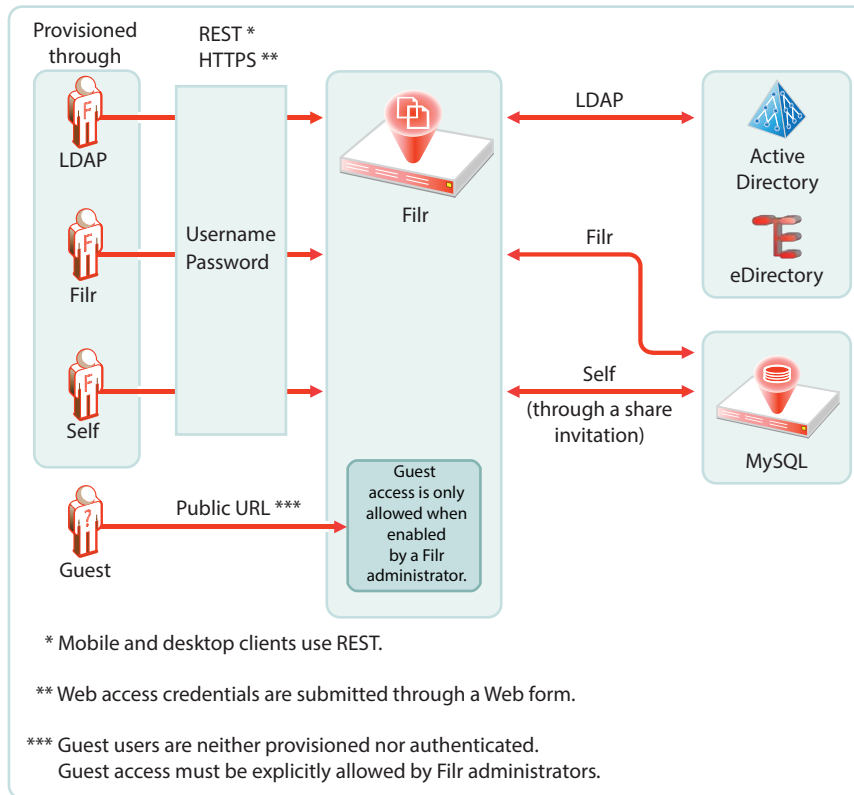
4.1 Filr Authentication

Filr clients for mobile devices and workstations use a REST protocol for Filr authentication. Inside the protocol are the user-supplied credentials. Filr validates these against the identity source (LDAP or local).

Web access is through a Web form that lets Filr take the credentials supplied and validate them as with REST.

This is illustrated in [Figure 4-1](#).

Figure 4-1 User Authentication in Filr



4.2 Access to Files and Folders Is Controlled by the File System

The NSS and NTFS file systems on OES, NetWare, and Windows servers always control access to the files and folders they contain. Users seeking access through a file browser, such as Windows explorer, must generally have the required permissions on the file systems to gain access.

This is absolutely true when accessing files and folders through Filr. You cannot gain more access through Filr than the underlying file system allows.

Filr sharing is no exception. [Shared access through Filr](#) depends on the Net Folder proxy user having the required file system rights.

4.3 How Users Get the Required Access Permissions

From a Filr perspective, users can get the required permissions to access files and folders in one of three ways:

- ♦ **Directly:** Users are assigned permissions to the files and folders.
- ♦ **Group Membership:** Users inherit permissions to the files and folders through membership in a group that has been assigned the permissions.
- ♦ **Net Folder Proxy User:** Users receive and accept Filr share invitations. They can then access the shared files and folders through the assigned Net Folder proxy users that have the required file system rights.

4.3.1 Roles and Net Folders

User roles relative to Net Folders are not assigned. They are automatically derived from users' permissions on [NSS](#) and [NTFS](#) file systems.

As explained in [How Users Get the Required Access Permissions](#), file system permissions can be directly assigned or inherited through group membership.

4.3.2 Roles and Shared with Me

User roles relative to Shares are assigned by the user sending the invitation.

Users sending invitations can only assign roles up to the level that they have.

Users receiving and accepting share invitations might or might not have direct rights on the file system, but that is irrelevant. Individual user rights do not affect Shared with Me functionality. Instead, Net Folder proxy users interface with the file system for everyone who is functioning in a sharing role.

If users access a folder through Shared with Me to which they also have file system rights, their functionality within Shared with Me is defined by the sharing role they were granted with the share invitation, even though that role might provide more or fewer access privileges than they would have through their Net Folder connection to the same folder.

4.4 Access Through Filr Involves One of Four Possible Roles

Depending on the rights that users have on the file system (see [How Users Get the Required Access Permissions](#)), Filr lets users function in one of four roles, as outlined in [Table 4-1](#).

Table 4-1 *Filr Roles and the Rights That They Represent*

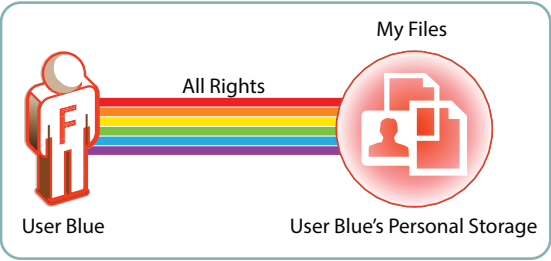
Role	Rights
None	No rights
Viewer	Read and Visibility rights
Editor	Read, Visibility, and Write rights
Contributor	Read, Visibility, and Write rights
	Create, Delete, Rename, Move, and Copy the contents of the folder

4.4.1 My Files (Personal Storage)

Users automatically have all access rights to the Filr-based personal storage assigned to them.

To be available to users, personal storage must be administratively enabled because it is turned off by default.

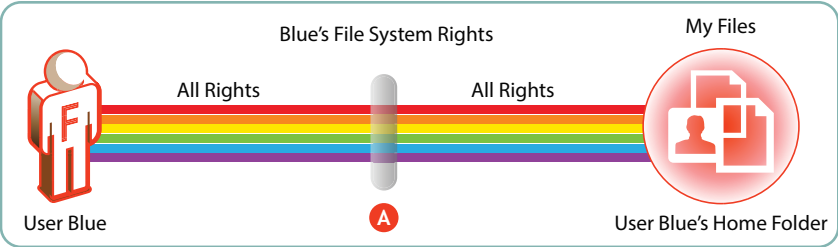
Figure 4-2 Filr users have all rights to their personal storage through My Files



For more information regarding My Files, see [Chapter 9, “My Files \(Personal Storage\),”](#) on page 53.

4.4.2 Home Folders

Users should have all rights to their server-based home folders.

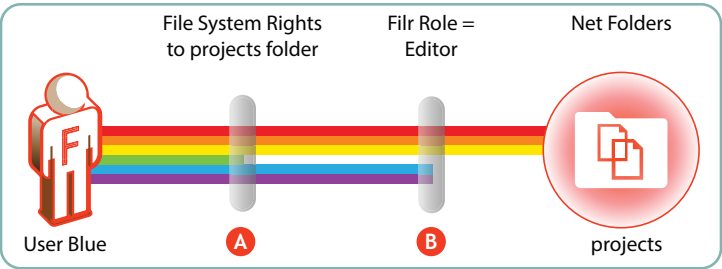


Letter	Details
A	<p>Although it is certainly possible that an administrator might choose to limit the file system rights to a home folder, that would seem to defeat the whole purpose behind providing home directories in the first place.</p> <p>Of course, rights restrictions are completely separate from limiting the available file storage space.</p> <p>In all cases, if there are file system restrictions, Filr always honors them.</p>

4.4.3 Net Folders

Users who are granted access to a Net Folder are not restricted by Filr. The file system of the target folder retains complete access control. The level of rights that users have through Filr depends on the role they have, as explained in, “[Access Through Filr Involves One of Four Possible Roles \(page 37\).](#)”

Figure 4-3 Users' effective rights to Net Folders are controlled by the file system where the Net Folder resides and the Filr role that these rights qualify them for

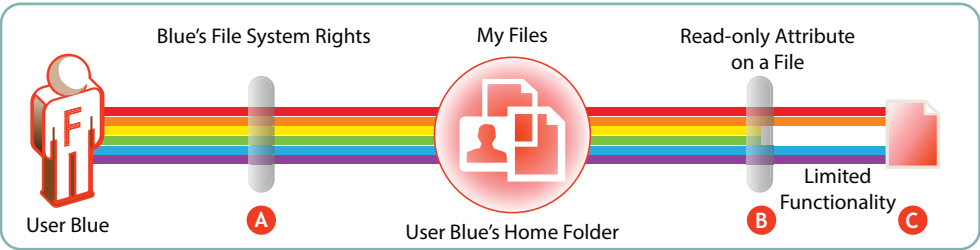


Letter	Details
A	User Blue is granted all rights to the NSS-based <code>projects</code> folder, except the <code>Erase</code> right (green bar).
B	Because User Blue doesn't have the <code>Erase</code> right, Filr assigns the Editor role. This means that even though Blue has <code>Create</code> (blue) and <code>Modify</code> (purple) rights on the file system, and could exercise them through a file browser, such as Windows Explorer, Filr functionality is limited to editing files within the <code>projects</code> folder.

For more information, see [Section 10.5, “Granting Access to Net Folders,”](#) on page 64.

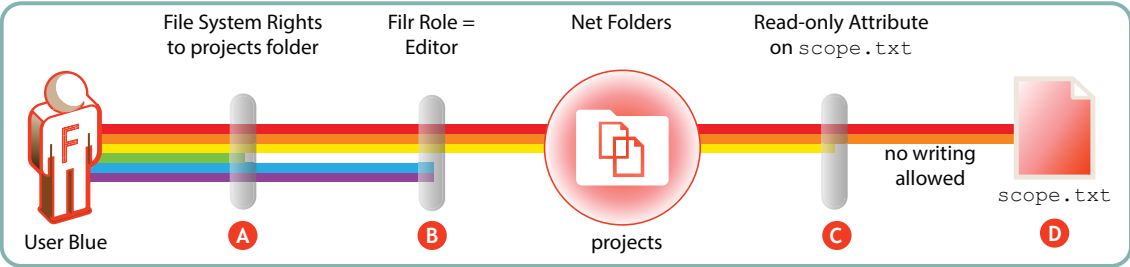
4.4.4 File Attributes Are Always Honored

Figure 4-4 File attributes affect functionality in home folders



Letter	Details
A	User Blue is granted all rights to an NSS-based home folder.
B	User Blue applies the Read-only attribute to one of the files in the home folder to ensure that it doesn't get modified by mistake.
C	A few weeks later, Blue opens the file and tries to change it. The file system doesn't allow this because of the file's Read-only attribute. Of course, Blue could remove the attribute using a file browser, such as Windows Explorer, and then modify the file. Filr always honors the file system. As long as the file is Read-only, it cannot be modified through Filr.

Figure 4-5 File attributes also affect functionality in Net Folders



Letter	Details
A	As shown in Figure 4-3 on page 39 , Blue doesn't have Erase rights on the <code>projects</code> folder.
B	Therefore, Blue only qualifies for the Filr Editor role.
C	The project leader maintains strict control of the <code>scope.txt</code> file by using the Read-only attribute.
D	This means that, even though Blue is an Editor in the <code>projects</code> folder, the <code>scope.txt</code> file is off-limits for making any changes.

4.5 Role Requirements Are Rigidly Enforced

On NSS and NTFS it is possible to define customized permissions. For example, you can create a directory in which users can create files even though they have no permission to view them afterward.

Customized permissions do not apply to Filr.

The NSS and NTFS requirements set forth in [Table 4-2](#) and [Table 4-3](#) are very rigid.

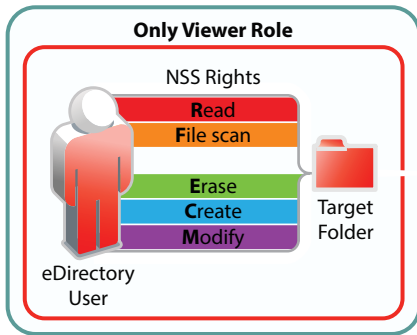
If any permissions are missing for a given role, Filr defaults to a more restrictive role. Additionally, if each and every permission required for the Viewer role is not present, then Filr grants no role to the user, as illustrated in the following sections.

- ♦ [Section 4.5.1, “NSS Example,” on page 40](#)
- ♦ [Section 4.5.2, “NTFS Example,” on page 41](#)

4.5.1 NSS Example

[Figure 4-6](#) shows that if the NSS `write` right is missing, the user can only function as a viewer, even though all of the Contributor-specific rights are present.

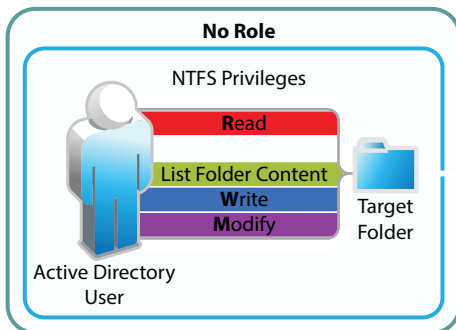
Figure 4-6 Missing Write right limits to only Viewer role



4.5.2 NTFS Example

Figure [Figure 4-7](#) shows that for NTFS, if the `Read & Execute` privilege is missing, the user has no Filr role, even though all of the other permissions are present.

Figure 4-7 Missing Read & Execute privilege prevents access through Filr



4.6 Rights to Files and Folders

Filr users must [have the required rights](#) to access files and folders through Filr.

- ♦ [Section 4.6.1, "Access Is Always Controlled by the File System," on page 41](#)

4.6.1 Access Is Always Controlled by the File System

As already explained, [access through Filr involves one of four possible roles](#).

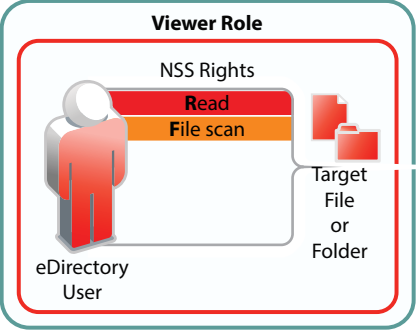
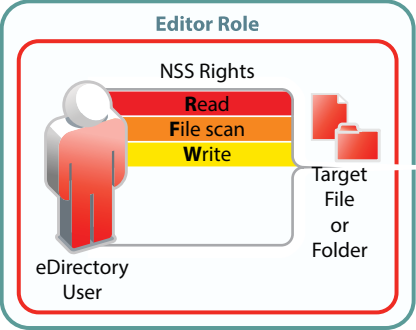
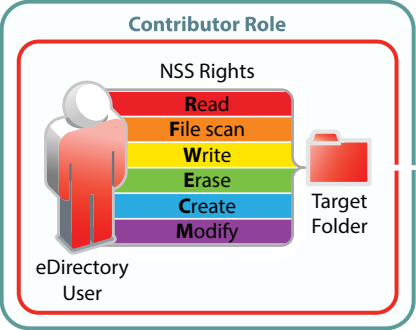
For users to have Viewer, Editor, or Contributor rights through Filr, they must have the minimum rights that those roles require, as outlined and illustrated in the following sections.

- ♦ ["Filr Roles and NSS File System Trustee Rights" on page 41](#)
- ♦ ["Filr Roles and NTFS Permissions" on page 42](#)

Filr Roles and NSS File System Trustee Rights

For eDirectory users to function in Filr roles, they must have the NSS rights illustrated and explained in [Table 4-2](#).

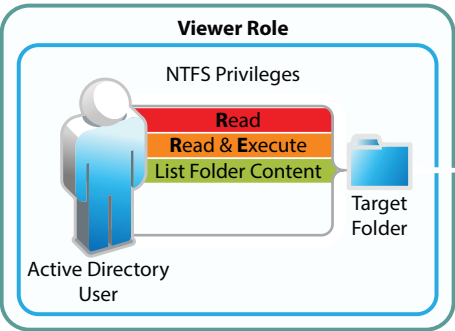
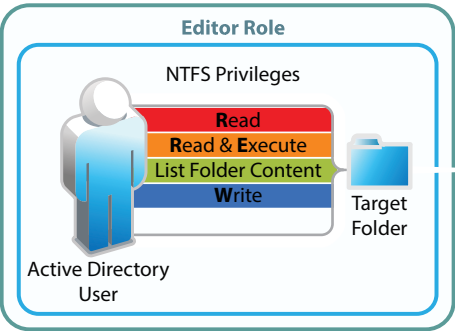
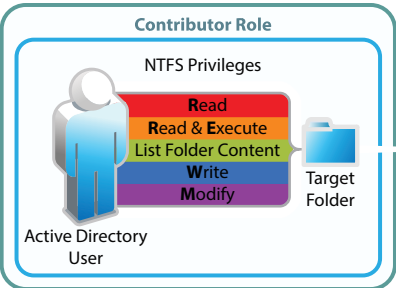
Table 4-2 NSS File System Rights Required for Filr Roles

Role and Minimum NSS Rights Required	Comments
<div><p>Viewer Role</p></div>	<p>Read and File Scan are the minimum file system trustee rights that users must have to view files and folders.</p>
<div><p>Editor Role</p></div>	<p>If the Write file system trustee right is added to Read and File Scan, users can then modify file content.</p>
<div><p>Contributor Role</p></div>	<p>To perform contributor functions, users must either have all file system trustee rights to the file or folder (except for Access Control) or the Supervisor right to the file or folder.</p> <p>You might ask why Access Control isn't listed. That is because it has no effect.</p> <p>Although users can provide access for other users through Filr sharing, that functionality is enabled by the file system rights of Net Folder proxy users.</p> <p>Filr shared access is independent of any file system rights that users have or do not have.</p>

Filr Roles and NTFS Permissions

For Active Directory users to function in Filr roles, they must have the NTFS file system permissions illustrated and explained in [Table 4-3](#).

Table 4-3 NTFS Permissions Required for Filr Roles

Role and Minimum NTFS Permissions Required	Comments
 <p>The diagram shows an 'Active Directory User' icon on the left. A bracket labeled 'NTFS Privileges' points to a stack of three permission boxes: 'Read' (red), 'Read & Execute' (orange), and 'List Folder Content' (green). An arrow points from this stack to a 'Target Folder' icon on the right.</p>	Read, Read & Execute, and List Folder Content are the minimum basic permissions that users must have in order to view files and folders. The default special permissions associated with these basic permissions are also required.
 <p>The diagram shows an 'Active Directory User' icon on the left. A bracket labeled 'NTFS Privileges' points to a stack of four permission boxes: 'Read' (red), 'Read & Execute' (orange), 'List Folder Content' (green), and 'Write' (blue). An arrow points from this stack to a 'Target Folder' icon on the right.</p>	If the basic Write permission is added, users can then modify file content. The default special permissions associated with these basic permissions are also required.
 <p>The diagram shows an 'Active Directory User' icon on the left. A bracket labeled 'NTFS Privileges' points to a stack of five permission boxes: 'Read' (red), 'Read & Execute' (orange), 'List Folder Content' (green), 'Write' (blue), and 'Modify' (purple). An arrow points from this stack to a 'Target Folder' icon on the right.</p>	To perform contributor functions, users must either have the basic Modify permission added, or they must have the basic Full Control permission. The default special permissions associated with these basic permissions are also required.

4.7 Sharing Rights

In contrast to file and folder rights, which are controlled by the file system, Filr controls all My Files and Net Folder sharing.

For more information about sharing, how it is managed, and how it works, see [Chapter 12, “Sharing through Filr,”](#) on page 69.

4.8 Windows Share Rights

Windows Shares are leveraged by Filr to create [Net Folders](#). It might seem logical, therefore, that the rights settings exposed on the *Sharing* tab in Windows would affect Filr functionality. That is not the case.

Setting Windows Share rights on a Windows Share has no effect on Filr. This is in keeping with the best practice recommendation from Microsoft that Share rights not be used to grant or control file access.

Remember, Filr Sharing is only enabled through the Net Folder proxy user and the file system privileges assigned to it.

4.9 Access-based Enumeration (Windows)

Access-based Enumeration settings on an NTFS file system have no effect on Filr.

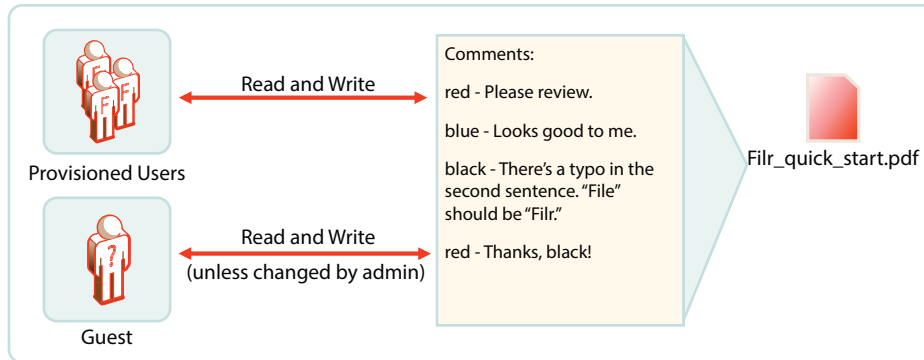
For example, a Windows administrator might disable Access-based Enumeration so that the files in a shared folder always display in Windows Explorer no matter what the user's rights.

The administrator might then expect that users would also be able to see the files through Filr. That is not the case. Disabling Access-based Enumeration has no effect on Filr. Only those users who have all of the NTFS permissions required for the Viewer role (Read, Read & Execute, and List Folder Content) can see the files.

5 Filr Comments

Comments are linked to the files that are commented on. All users, including Guest, have Read and Write access to comments on the files and folders that they are allowed to see. If there is a risk of Guest users logging inappropriate comments, rights can be changed to Read Only, as indicated in [Figure 5-1](#).

Figure 5-1 Who Can Log Comments in Filr

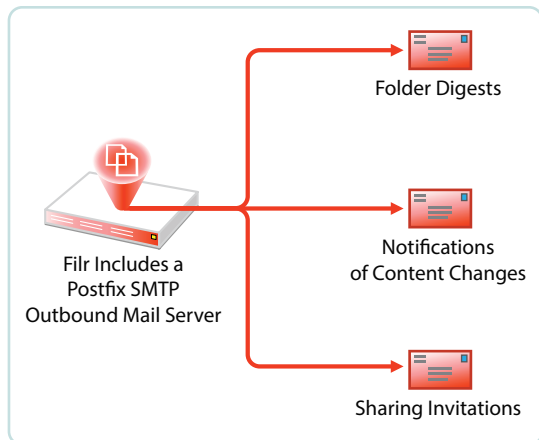


For more information about Filr comments, see ["Comments"](#) in the [Novell Filr 1.1 Administration Guide](#).

6 Filr Email Notifications

Filr includes a Postfix mail server for outbound email notifications, as illustrated in [Figure 6-1](#).

Figure 6-1 *Filr Outbound Email Functionality*



Although the default mail server should work well for most Filr installations, you can configure Filr to use your outbound SMTP mail server. For more information, see “[Changing Outbound Email Configuration Settings](#)” in the *[Novell Filr 1.1 Administration Guide](#)*.

7 Filr Indexing and Searching

All Filr searching involves the Index server (Lucene). Everything that is searchable is in the index, including users and groups. All synchronized files and folders have their metadata synchronized automatically, so that their basic information (in contrast with actual content) is searchable.

- ♦ [Section 7.1, “What Is Indexed and When,” on page 49](#)
- ♦ [Section 7.2, “About Filr Content Indexing,” on page 50](#)

7.1 What Is Indexed and When

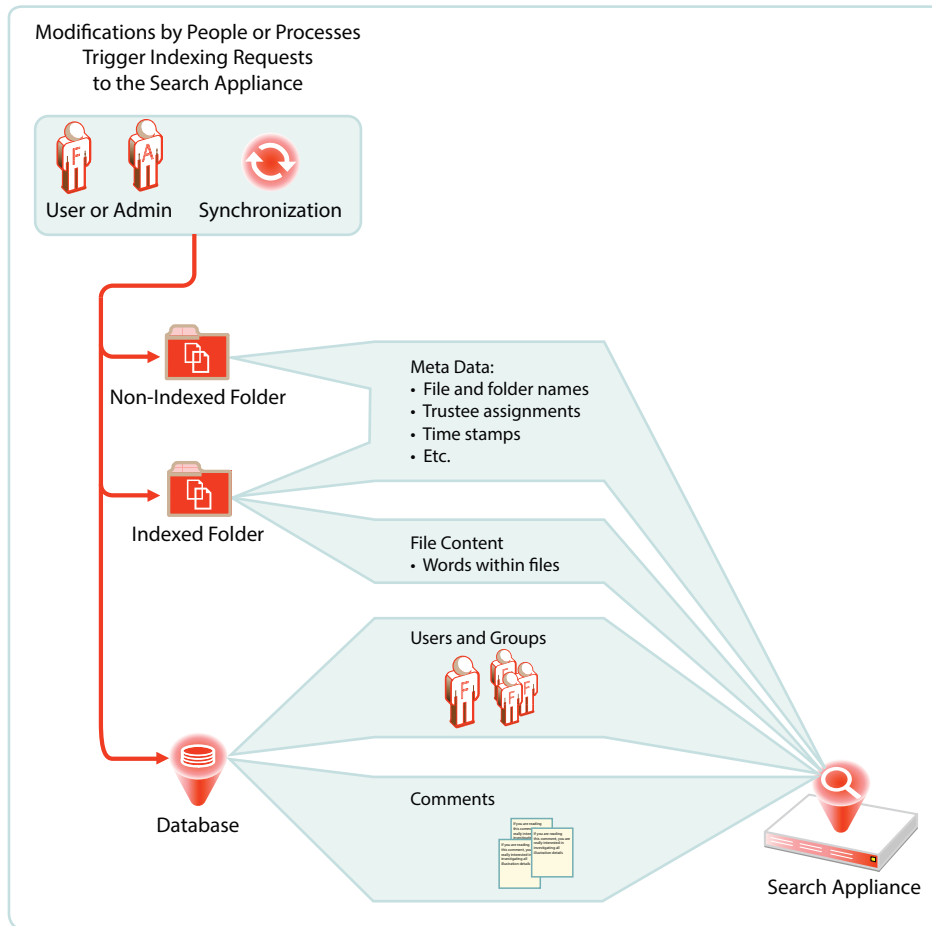
As illustrated in [Figure 7-1](#), indexing occurs each time that data is modified. Index triggers include the following:

- ♦ Modifications made by a user or administrator
- ♦ Synchronization of files and folders

When a folder is indexed, the only files re-indexed are those whose time stamps or hash sums have changed since the last index was performed.

- ♦ Synchronization of users and groups

Figure 7-1 When Indexing Occurs



7.2 About Filr Content Indexing

Only files that live in Net Folders that are specifically enabled for indexing have their content indexed.

Files in home folders and personal storage are always indexed.

After the files have been synchronized to Filr, the indexing process can begin.

IMPORTANT: Content indexing is performed as a background process. Depending on the number of files that need to be indexed, it can take several hours or even days before all of the content is indexed and searchable in the Filr system. Therefore, it is important to consider which files need to have their content be searchable.

For an overview of when indexing occurs in conjunction with Net Folder synchronization, see [Section 13.2, “Net Folder Synchronization Detail Overview,”](#) on page 80.

For more information about Filr indexing, see “[Managing the Lucene Index](#)” in the *Novell Filr 1.1 Administration Guide*.

8 Filr Licensing

Filr comes with a 60-day evaluation license pre-installed. You must install a full license in order for Filr to continue functioning beyond the 60-day evaluation period.

For instructions on viewing and installing Filr licenses, see “[Viewing and Updating the Filr License](#)” in the [Novell Filr 1.1 Administration Guide](#)..

9 My Files (Personal Storage)

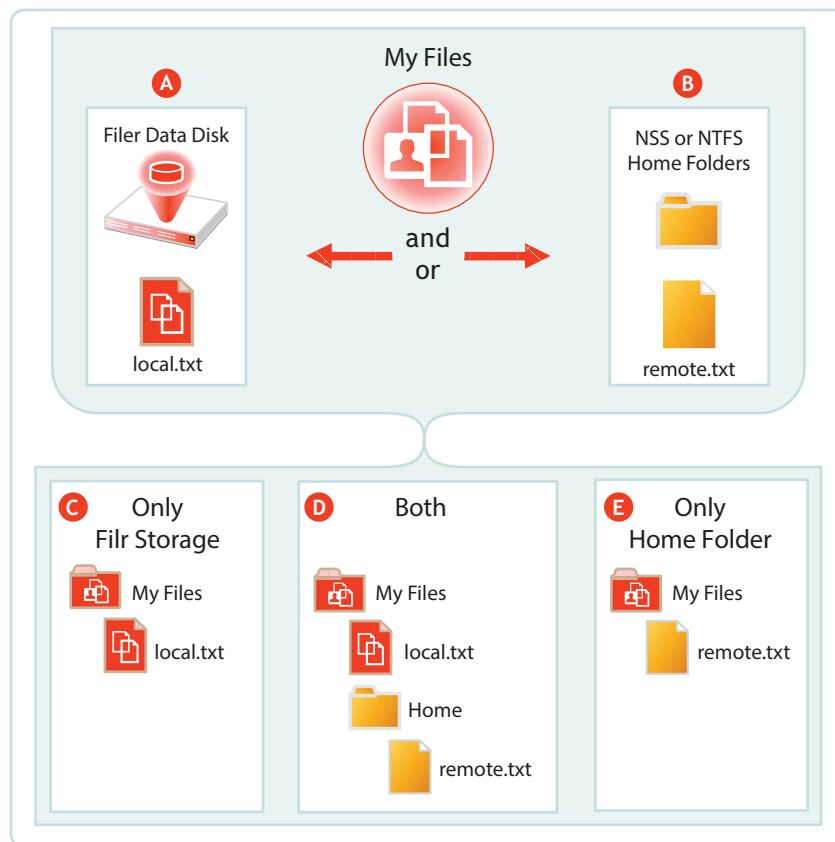
Many organizations let their network users store personal files on organization file servers. Filr supports this practice through My Files, which can include access to personal storage on Filr as well as to traditional home directories.

- ♦ [Section 9.1, “Understanding My Files,” on page 53](#)
- ♦ [Section 9.2, “Enabling Personal Storage,” on page 54](#)
- ♦ [Section 9.3, “Restricting Disk Space Usage,” on page 56](#)
- ♦ [Section 9.4, “Home Folders Vs. Net Folders,” on page 56](#)
- ♦ [Section 9.5, “My Files Sharing Rights,” on page 56](#)

9.1 Understanding My Files

My Files is an optional personal storage area that you can make available to your Filr users. It can include two possible data storage locations, as illustrated in [Figure 9-1](#) and explained in the table that follows it.

Figure 9-1 *My Files’ Possible Storage Locations*



Letter	Details
A	If you enable personal storage for users as outlined in Figure 9-2 on page 55 , then Filr automatically creates a personal storage directory on its data disk.
B	If your LDAP users have home directory attributes associated with them in the identity store (eDirectory or Active Directory), then when their users accounts are synced, Filr creates special Net Folders that link to their home directories.
C	If you have enabled personal storage for users who do not have home directories as described on the previous row, then those users see only what is stored in the Filr data store in their <i>My Files</i> .
D	If you have enabled personal storage for users, and those users also have home directories associated with them in the identity store, they see what is stored in the Filr data store and a folder named <i>Home</i> under <i>My Files</i> . The <i>Home</i> folder provides a distinction between files and folders in the Filr data store and those in Home directories on the file server.
E	If you haven't enabled personal storage, but your users have home directories, then the files and folders in their home directory display as direct entries within <i>My Files</i> .
NOTE: Of course, if you don't enable personal storage, and users don't have home directories, then their <i>My Files</i> is empty and not usable.	

9.2 Enabling Personal Storage

Personal storage can be enabled for all users on the Filr system or on individual users and/or groups level, as fits your organization's needs and illustrated in the following sections.

- [Section 9.2.1, "Personal Storage for All LDAP Users," on page 54](#)
- [Section 9.2.2, "Personal Storage for Individual Users and/or Groups," on page 55](#)

9.2.1 Personal Storage for All LDAP Users

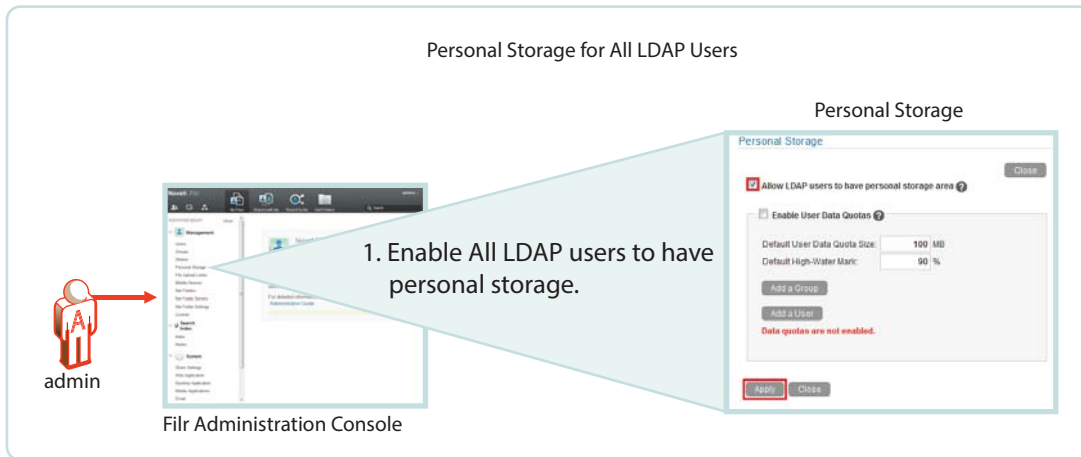
If personal storage is enabled, then space is allocated to users for personal storage. [Figure 9-2](#) illustrates how to enable personal storage for all of the LDAP users on the Filr site.

After enabling personal storage for everyone, you can then use the *Users > More and/or Groups > More* menu to disable or modify personal storage settings for individual users and/or groups.

Alternatively, you can choose to not use this dialog at all, but rather enable personal storage for only specific users or groups by using the *Users > More and/or Groups > More* menu.

For an overview of personal storage disk space quotas, see [Section 9.3, "Restricting Disk Space Usage," on page 56](#).

Figure 9-2 Enabling Personal Storage for All Users



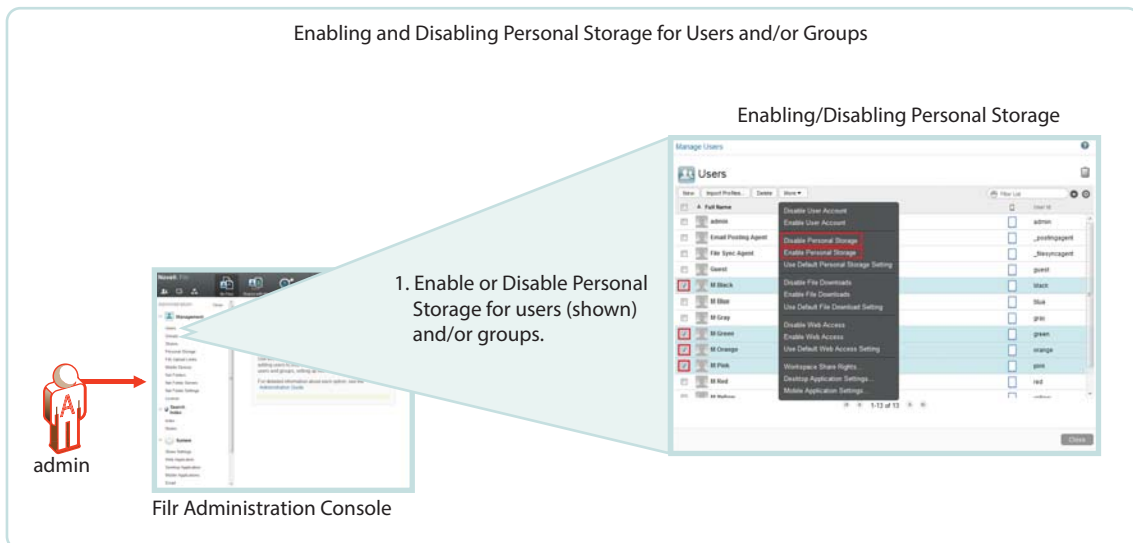
9.2.2 Personal Storage for Individual Users and/or Groups

In Filr 1.0 you had to enable personal storage globally before adjusting the individual personal storage settings.

Filr 1.1 doesn't require the global setting but lets you directly enable personal storage for individual users and/or groups as illustrated in [Figure 9-3](#).

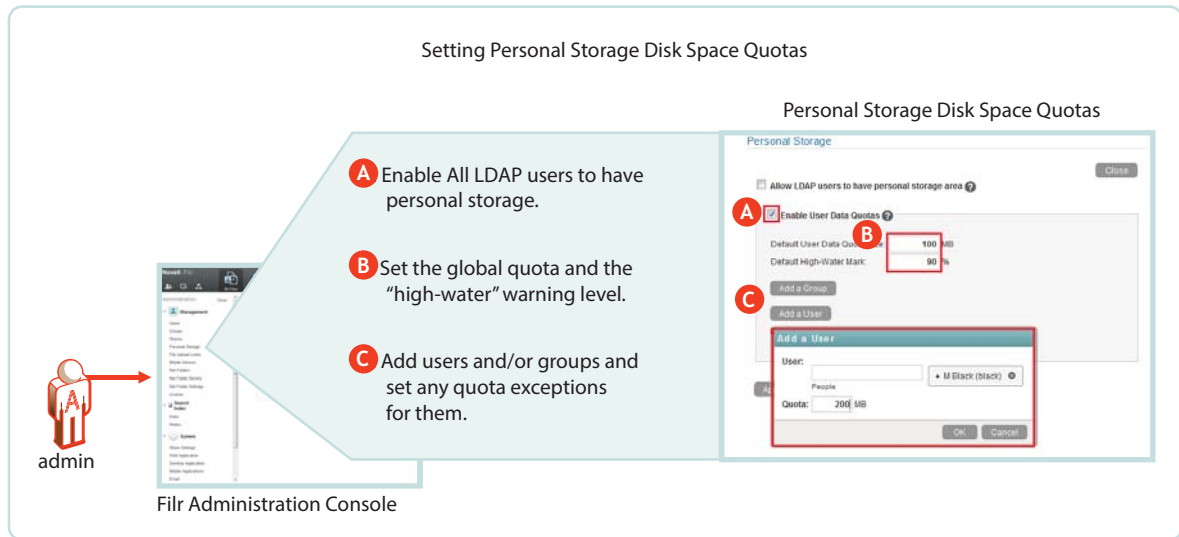
For an overview of personal storage disk space quotas, see [Section 9.3, "Restricting Disk Space Usage,"](#) on page 56.

Figure 9-3 Setting Default and Individual Storage Quotas



9.3 Restricting Disk Space Usage

Figure 9-4 Enabling Personal Storage for All Users



9.4 Home Folders Vs. Net Folders

A home folder is a special kind of Net Folder that is included in *My Files*.

Home folders allow for the sharing of files and sub-folders, while Net Folders only allow for the sharing of files, not sub-folders.

	Home Folders	Net Folders
File-server-based	Yes	Yes
Focus	Individual users	Groups or teams of users
Appear under Net Folders icon	No	Yes
Appear under My Files icon	Yes	No
Indexing	Metadata and content by default	Metadata by default; content if enabled
Sharing granularity	Files and sub-folders	Files only

9.5 My Files Sharing Rights

See [Section 12.1.2, “My Files Sharing Is Automatic,”](#) on page 71.

10 Net Folders

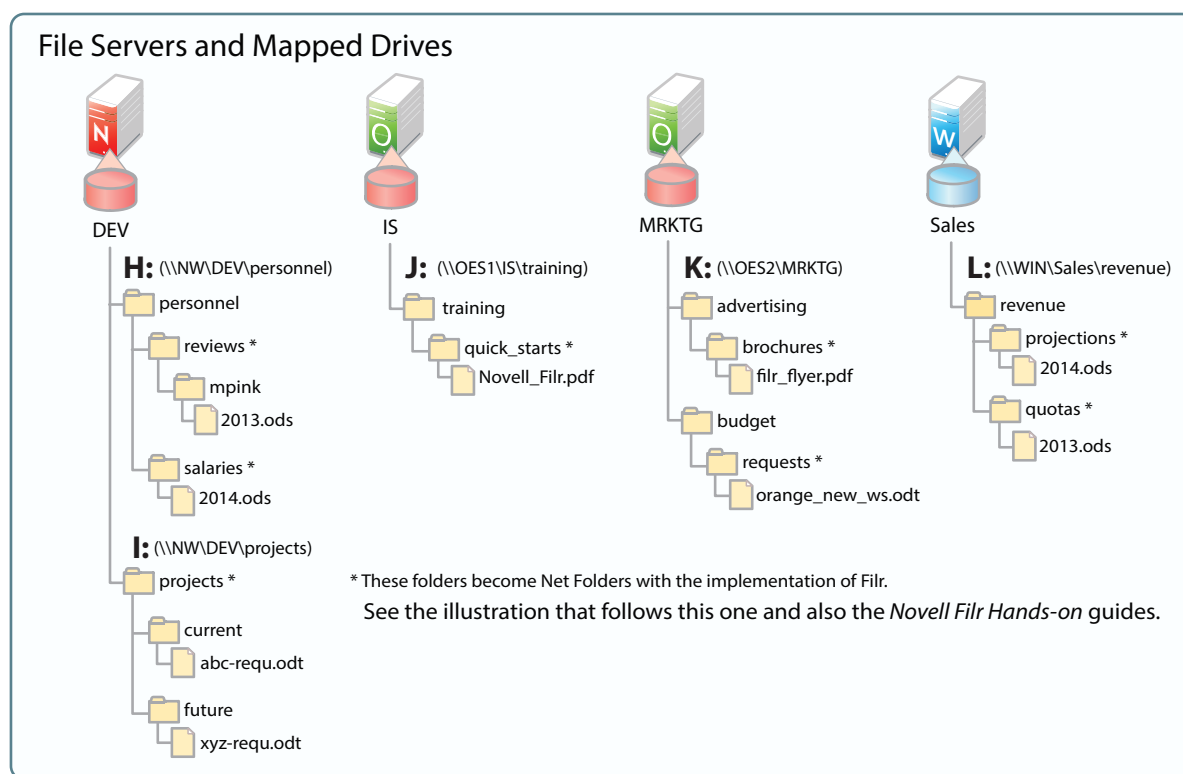
Filr introduces a new way of accessing file server data—Net Folders—a new file access method that shares some similarities with Novell's long-standing concept of mapped network drives.

- ♦ [Section 10.1, “Overview,” on page 57](#)
- ♦ [Section 10.2, “Specifying Net Folder Servers,” on page 59](#)
- ♦ [Section 10.3, “Specifying Net Folders,” on page 61](#)
- ♦ [Section 10.4, “Net Folder Proxy Users,” on page 63](#)
- ♦ [Section 10.5, “Granting Access to Net Folders,” on page 64](#)

10.1 Overview

To understand Net Folders, it is useful to see the similarities and differences between them and the mapped drives that you probably have on your current network. [Figure 10-1](#) and [Figure 10-2](#) illustrate such a comparison.

Figure 10-1 File Servers and Mapped Drives

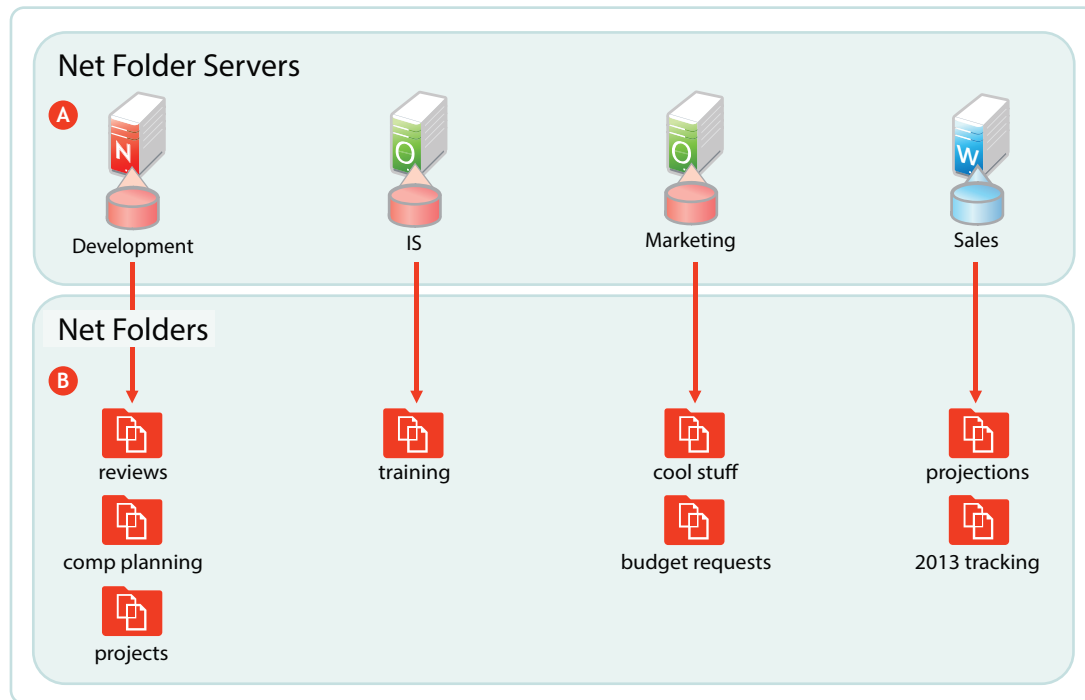


[Figure 10-2](#) shows the same servers as in [Figure 10-1](#), with their volumes defined as Net Folder Servers. Notice that the Net Folder Server names do not need to match the volume names, which can sometimes be rather cryptic.

The asterisk-marked folders in [Figure 10-1](#) are shown as Net Folders here.

As with the Net Folder Server names, some of the Net Folder names in [Figure 10-2](#) are different from the [Figure 10-1](#) volume and folder names that they represent. This illustrates that Net Folder names are not tied to their corresponding actual folder names. Instead, you can name them whatever best communicates their purpose and content to those who access them.

Figure 10-2 Net Folder Servers and Net Folders



Letter Information

- A** A Net Folder Server represents a volume or share on a NetWare, OES, or Windows file server.
- In this example, Net Folder Servers for OES point to the root of an NSS volume on the server, but they can also point to a directory or sub-directory.
- Net Folder Servers for Windows servers point to a Windows share, which is usually defined at a folder level other than at the root of the file system. Therefore, it is common for a Net Folder Server for Windows to point to the same folder as an associated Net Folder does.
- There is usually one Net Folder Server per volume or share, but you can create multiple Net Folder Servers to the same volume or share if needed.
-



A Net Folder is a pointer or reference to a specific folder within a Net Folder Server.

Often there is just one Net Folder for every Net Folder Server, but you can create multiple Net Folders that point to a single Net Folder Server. You can even create multiple Net Folders that point to the same relative path.

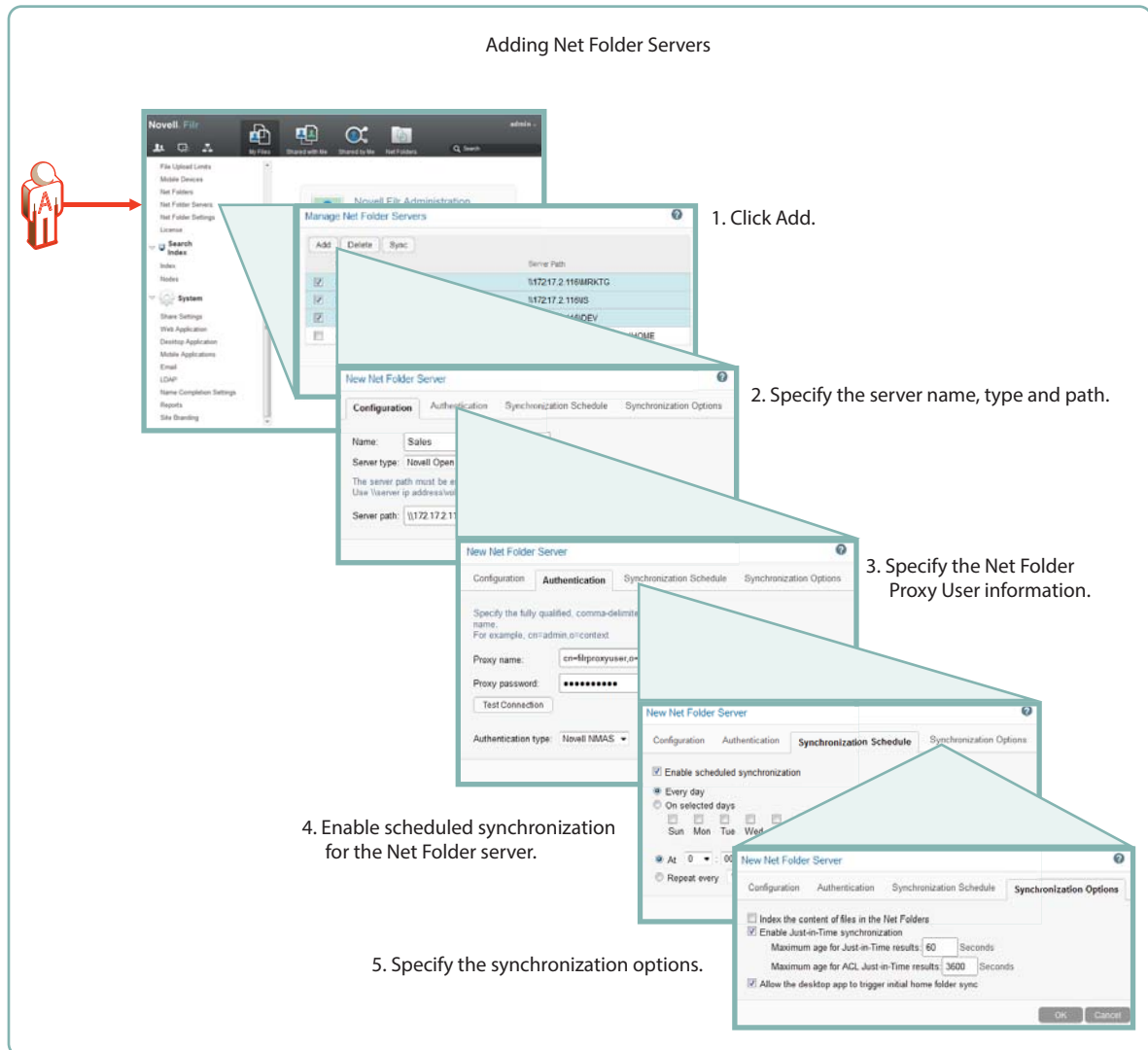
Why might you want to duplicate Net Folders? Possibilities include the following:

- ♦ Different synchronization schedule requirements
 - ♦ Different access rights requirements
 - ♦ Different usage patterns
 - ♦ Different access loads
-

10.2 **Specifying Net Folder Servers**

The first step in creating Net Folder is to set up Net Folder Servers.

Figure 10-3 Net Folder Server Creation



As illustrated in [Figure 10-3](#), adding a Net Folder Server includes the following:

- ♦ **Specifying the Name, Type, and Path**
 - ♦ **Name:** Net Folder users don't see this name, so use a name that makes sense from an administrative perspective. For example, you might include the IP address or DNS name of the server, or you could use a location name, such as `Third_Floor_Server`.
 - ♦ **Type:** Filr 1.1 requires that you select the server type being targeted: Microsoft Windows, Novell OES, or Novell NetWare
 - ♦ **Server Path:** This is the full UNC path to the NSS volume or directory on OES, or to the Windows share on NTFS where your Net Folder is located.
- ♦ **Specifying the Net Folder Proxy User Information**
 - ♦ **Proxy Name:** This is the name of the Net Folder proxy user that provides access to this volume. For more information, see [Section 10.4, "Net Folder Proxy Users,"](#) on page 63.

IMPORTANT: Be sure to follow these guidelines when specifying the proxy user

- ♦ **OES:** Always use a fully qualified name, such as `cn=admin,o=myorganization`.

If you specify only a simple name, such as `admin`, then Filr accesses the Net Folders for the server using CIFS rather than NCP.

When you test the connection, the test succeeds and data synchronizes using CIFS.

Unfortunately, when Filr attempts to determine a user's effective rights, the request fails because that function requires NCP and the simple name doesn't provide enough information to the NCP process.

- ♦ **Windows:** Use `domain\username` as the syntax.

DFS for Windows requires this, and the syntax will always work with Active Directory and Windows.

-
- ♦ **Proxy Password:** This is the password of the Net Folder proxy user. If the password changes in the identity store, it must be updated here.
 - ♦ **Test Connection:** This lets you test the path and the credentials of the proxy user that you have specified.

- ♦ **Enabling Synchronization for the Net Folder Server**

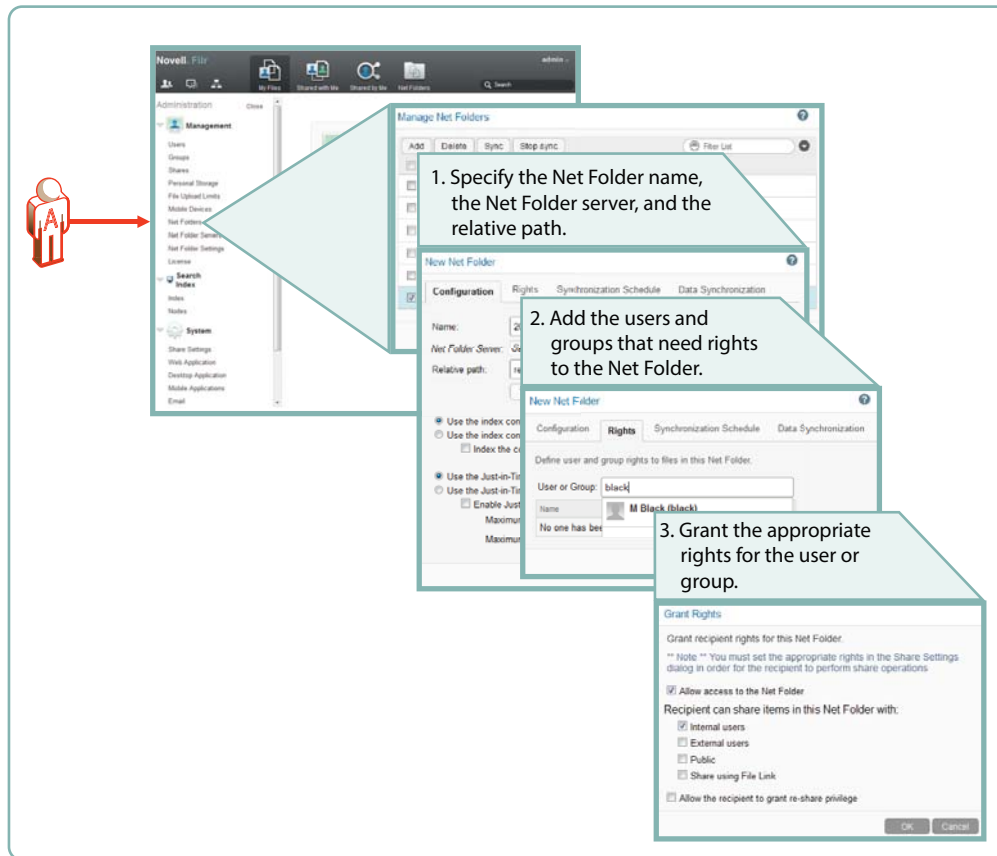
- ♦ **Enable Scheduled Synchronization:** This creates a synchronization schedule for this Net Folder Server. You can then specify when you want the synchronization to occur. Any Net Folders for this server that don't have their own synchronization schedules will be synchronized according to this schedule.
 - ♦ **Specifying the Synchronization Options** This lets you specify whether you want Net Folder contents indexed for searching, whether to enable Just-in-Time synchronization, and whether to allow desktop users to request Net Folder synchronizations.

For more information about Net Folder Server creation, see “[Configuring and Managing Net Folder Servers](#)” in the *Novell Filr 1.1 Administration Guide*.

10.3 Specifying Net Folders

After creating Net Folder Servers, you can create Net Folders for users to access.

Figure 10-4 Net Folder Creation



The minimum tasks required for adding a Net Folder are illustrated in Figure 10-4. Setting a synchronization schedule and specifying the data synchronization options are not specifically called out because they are summarized in Figure 10-3 on page 60.

- ◆ **Specify the Net Folder Information**

- ◆ **Name:** Filr users with rights to the Net Folder see this name, so you should use a name that they will recognize and that will help them to understand what the Net Folder contains.
- ◆ **Net Folder Server:** The Net Folder Servers you have created appear in a drop-down list. You also have the option to create an additional Net Folder Server from within the Net Folder creation dialog.
- ◆ **Relative Path:** This is the path to the folder relative to the UNC path entered for the Net Folder Server. A blank path creates a Net Folder that points to the Net Folder Server's UNC path.
- ◆ **Test Connection:** This lets you verify that you have typed the path correctly.

- ◆ **Add Users and/or Groups**

- ◆ **User or Group:** As you type a user or group name, a list populates from which you can make your selection. When you click the name, the Access Rights dialog displays
- ◆ **Access and Sharing rights:** After you enable access to the Net Folder for the user or group, you can specify sharing privileges as well.

For more information about Net Folder creation, see “[Creating and Managing Net Folders](#)” in the *Novell Filr 1.1 Administration Guide*.

10.4 Net Folder Proxy Users

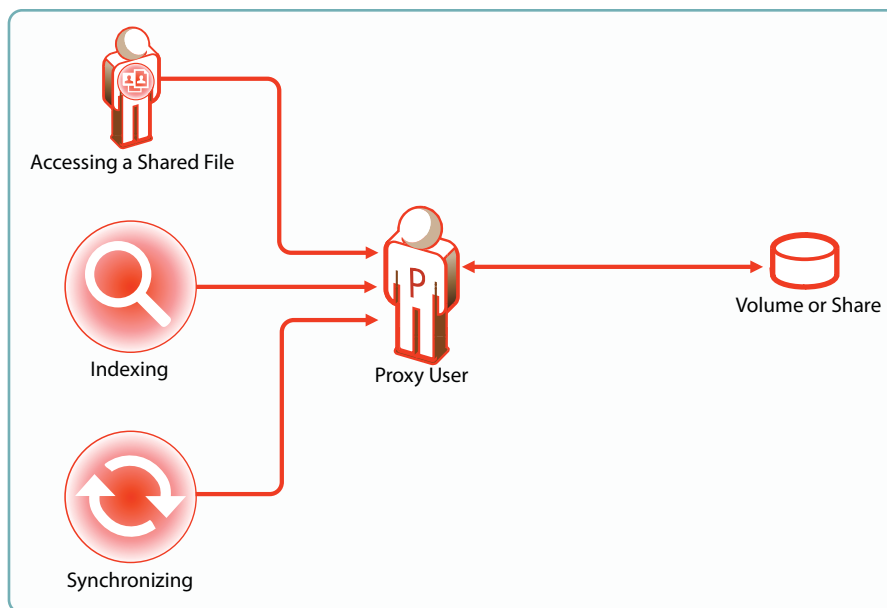
For more information about Net Folder Server proxy users, see “Planning the Net Folder Server Proxy User” in the *Novell Filr 1.1 Administration Guide*.

- ♦ Section 10.4.1, “The Functions Facilitated by Net Folder Proxy Users,” on page 63
- ♦ Section 10.4.2, “Rights Required for Net Folder Proxy Users,” on page 63
- ♦ Section 10.4.3, “Net Folder Proxy User Passwords,” on page 64

10.4.1 The Functions Facilitated by Net Folder Proxy Users

Net Folder proxy users provide Net Folder access for three Filr functions: file sharing, indexing, and synchronization, as illustrated in [Figure 10-5](#).

Figure 10-5 Functions of a Net Folder Proxy User

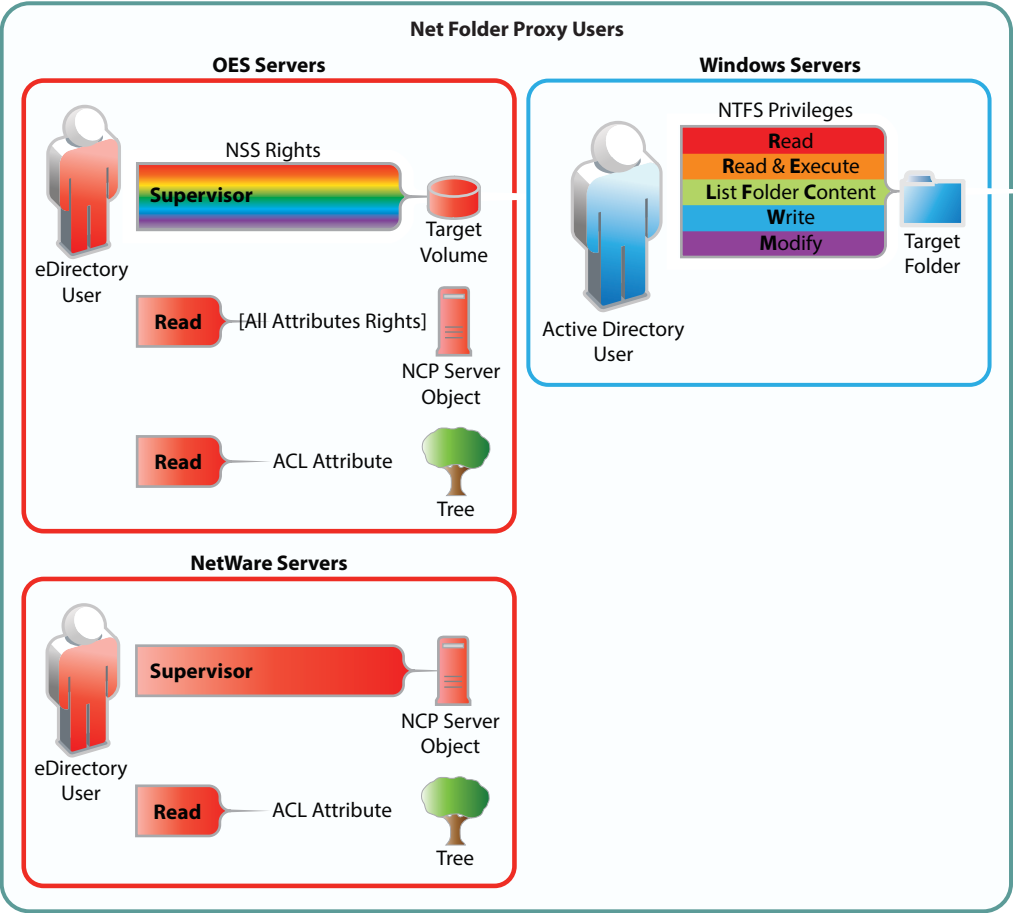


- ♦ Access to shared files always involves the proxy user, even for users who have file system rights to the shared files.
- ♦ Proxy users have no role when users with Net Folder rights access Net Folders directly.

10.4.2 Rights Required for Net Folder Proxy Users

Net Folder proxy users must have the rights shown in [Figure 10-6](#).

Figure 10-6 Proxy User Rights Summary

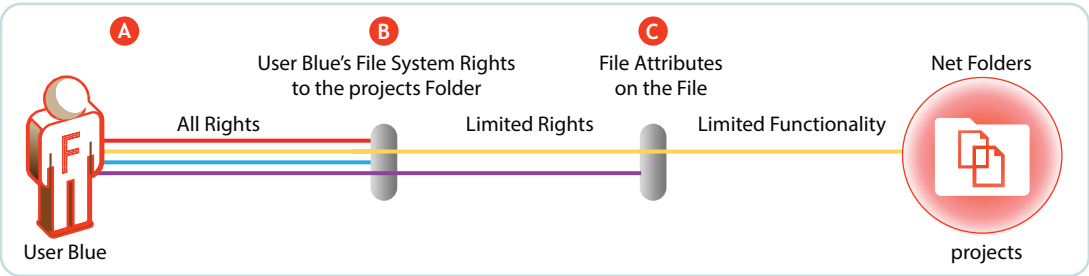


10.4.3 Net Folder Proxy User Passwords

If the proxy user password changes in the LDAP identity store, it must also be changed in the Net Folder Server configuration dialog.

10.5 Granting Access to Net Folders

Figure 10-7 Net Folder Access Involves Filr and the File System



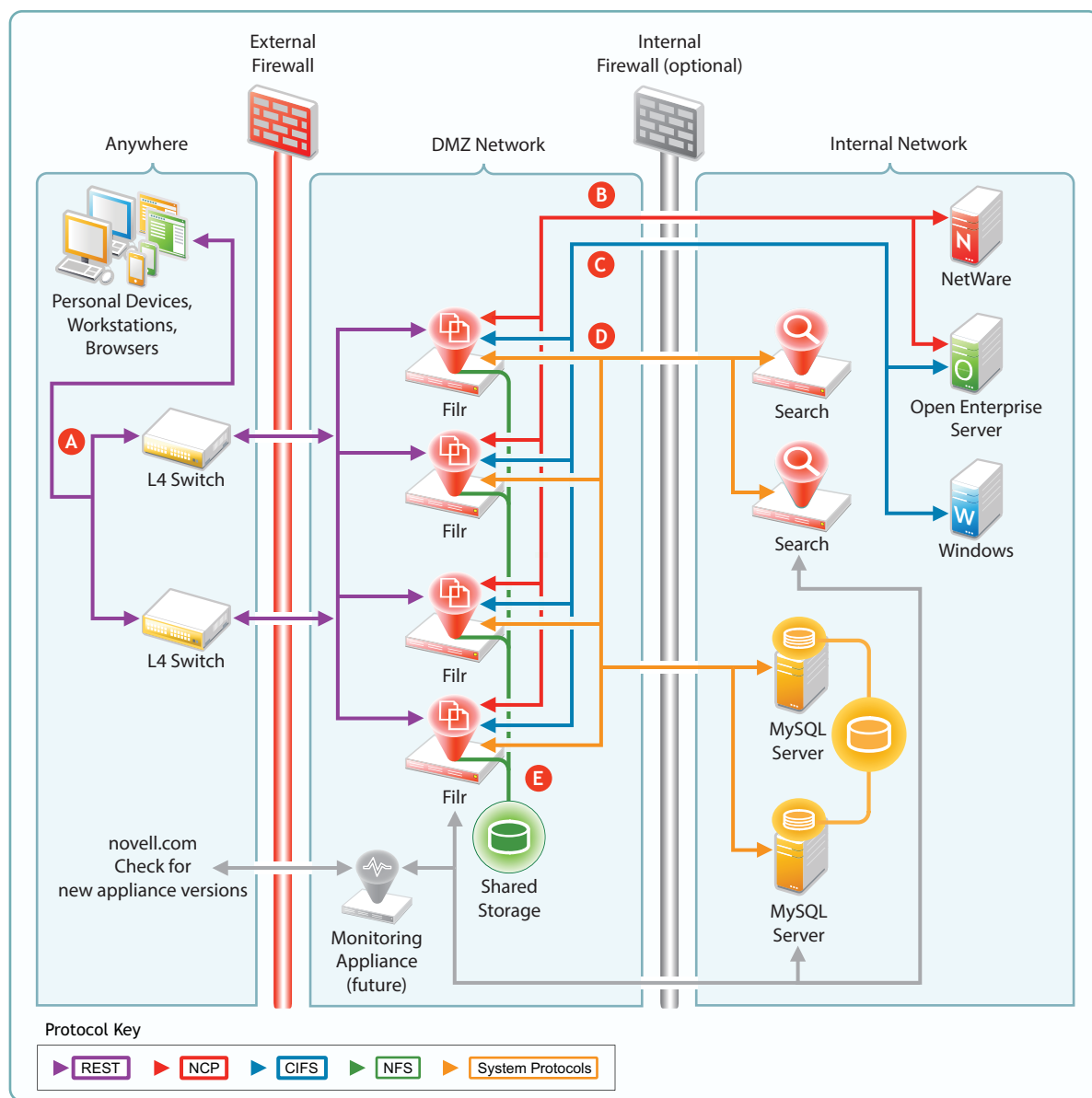
Letter	Explanation
A	When you grant a user access to a Net Folder, either individually or as a member of the group by using the Rights tab (see the explanation for Figure 10-4), then from a Filr perspective, the user has all rights to that folder. However, the file system is the access master controller.
B	The user must have file system trustee rights that allow the file to be viewed and accessed. For example, if the user has Read, Write, and File Scan rights to a file on an NSS volume, then the file is not only visible, but can, in theory, be modified. However, there's one more part to the access equation.
C	Files can have attributes that prevent them from being modified, such as Read Only. They might also be hidden, in which case they would not be visible to the Filr user.

For more information about Net Folders, see “[Setting Up Net Folders](#)” in the *Novell Filr 1.1 Administration Guide*.

11 Protocols and Filr

The components in a Filr deployment use a number of different protocols to communicate and provide Filr services, as shown in [Figure 11-1](#). The optional internal firewall is shown to facilitate the illustration of a separate (and also optional) DMZ network.

Figure 11-1 Protocols Used in Filr Installations



Letter	Details
A	Workstations and devices running Filr software access Filr using REST protocols that facilitate authentication and other access requests. Browsers use HTTPS to communicate with Filr.
B	Filr communicates with Novell file servers using NetWare Core Protocol (NCP) requests.
C	Filr communicates with Windows servers using the Common Internet File System (CIFS) protocol.
D	Other system protocols handle communication between Filr and the MySQL and Search appliances.

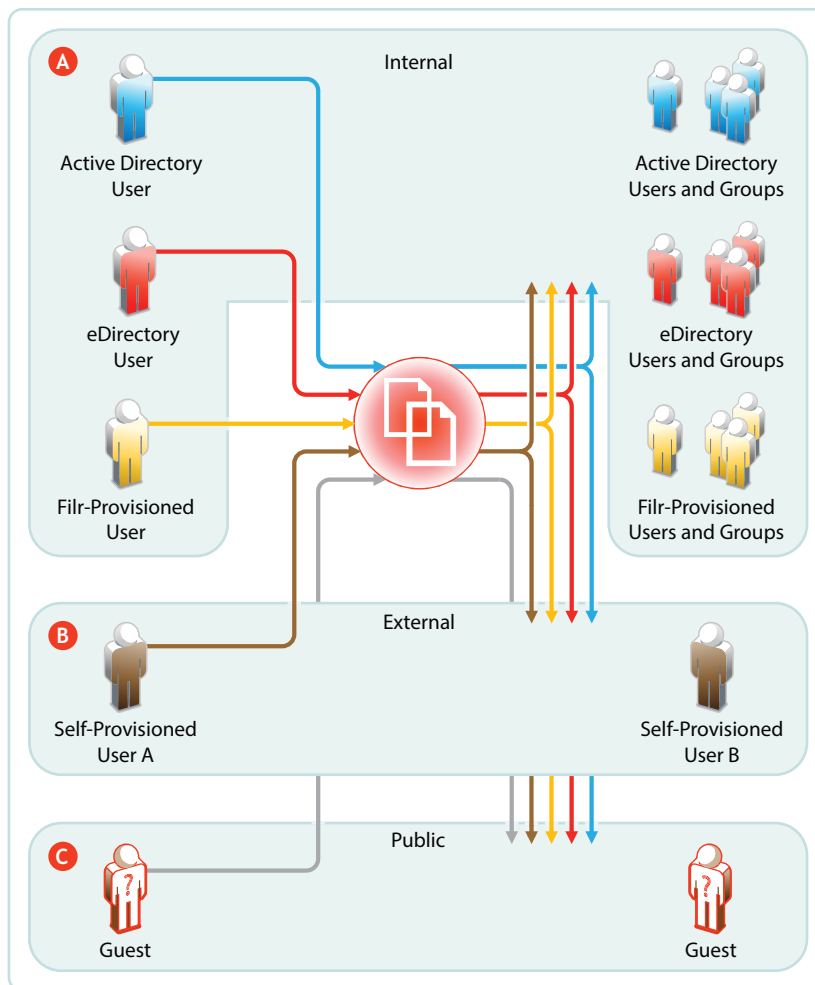
12 Sharing through Filr

Sharing lets users grant other users (internal or external) access to files that they own. If allowed, users can also share files that they have received share invitations for.

Figure 12-1 presents a high-level overview of the sharing functionality available in Filr. The sections that follow provide more detail.

- ♦ [Section 12.1, “Setting Up Sharing,” on page 70](#)
- ♦ [Section 12.2, “Understanding Roles and Sharing,” on page 73](#)
- ♦ [Section 12.3, “A Caution Regarding the Re-sharing Feature,” on page 75](#)

Figure 12-1 *Sharing through Filr*



Letter	Explanation
A	<p>Depending on the sharing privileges they are granted, internal users can share and collaborate with each other, with external users who have been invited to self-provision into the Filr system, and with the public. If re-sharing items is allowed, those who receive share invitations can also share.</p> <p>This means that eDirectory users can share files with Active Directory users and groups, that the reverse is also true, and that both of them can invite external partners or others to join the Filr system for collaboration and other purposes.</p>
B	<p>When External Sharing is enabled in Filr, external users who receive share invitations can self-provision into the Filr system and collaborate with internal and external users, using the Comments feature.</p> <p>If Filr is configured to allow it, external users can also share with internal users, with each other, and with the public.</p>
C	<p>If Filr is configured to allow public sharing, and if a file is shared publicly through a system-generated URL, then anyone with that URL can access the file as a guest user and share it with any other user, including other public users. This re-sharing is not a function of Filr but a function of sharing the URL through email, social networking, and so on.</p>

12.1 Setting Up Sharing

Before any sharing can happen, it must first be enabled at the Filr system level. After that, the system-level settings define the upper limit of sharing that can be enabled at lower levels.

After sharing is enabled for the system, sharing of My Files is automatically available up to the limits granted at the system level. Sharing files from Net Folders must be enabled on an individual Net Folder basis.

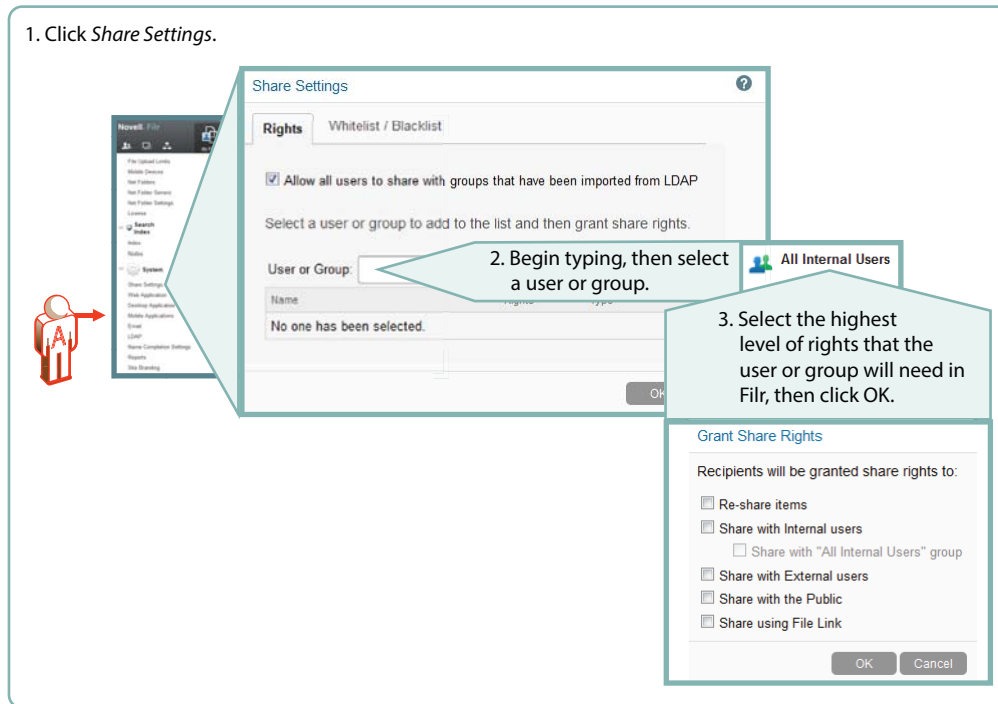
12.1.1 System-Level Sharing Must Be Set Up First

The Filr Administrative Console provides access the Share Settings dialog. Some Filr administrators prefer to enable sharing and set its upper limits on an individual-user and individual-group basis. Others prefer to enable sharing at a global level by leveraging the `All Internal Users` and `All External Users` groups.

In the first case, My Files sharing will be limited to only those users and groups that have sharing enabled at the system level. In the second case, all internal and external users will have My Files sharing enabled.

In both cases, Net Folder sharing must be configured for each Net Folder individually.

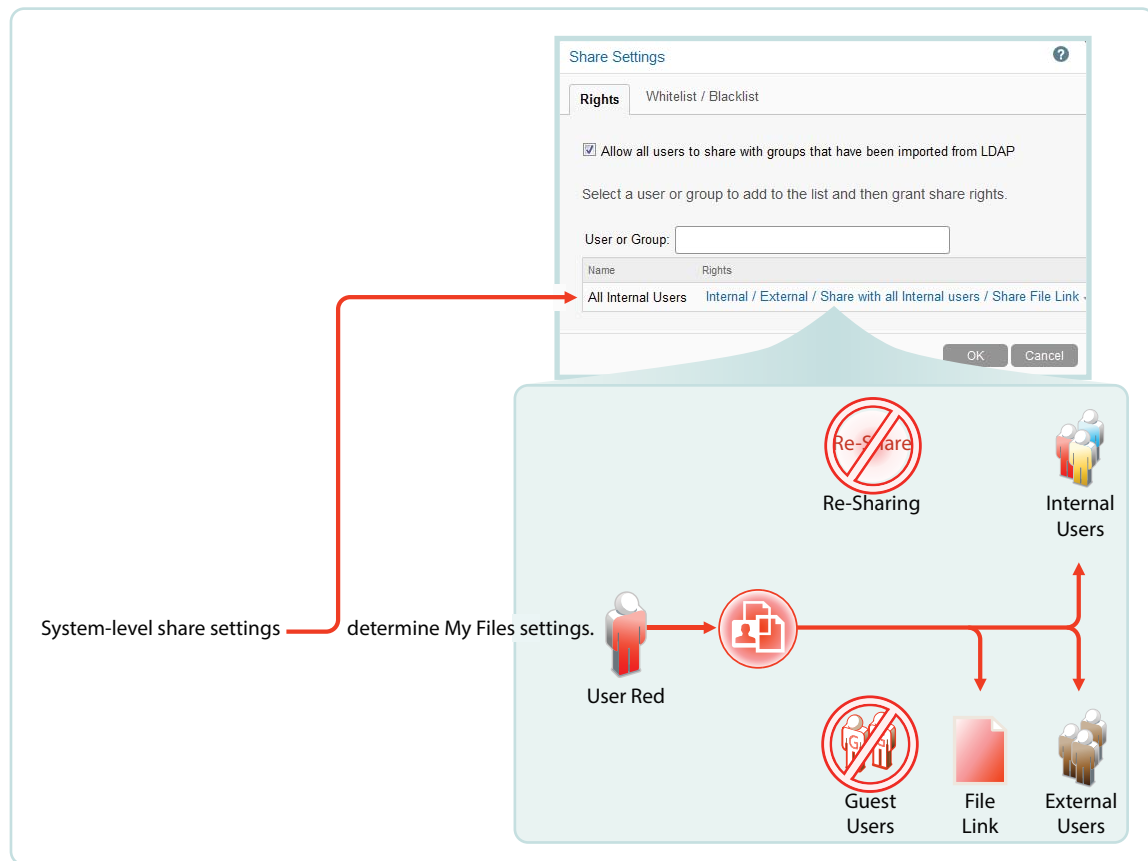
Figure 12-2 Setting Up System-Level Sharing Rights



12.1.2 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.

Figure 12-3 My Files Share Settings



12.1.3 Net Folder Sharing Must Be Explicitly Allowed At Two Levels

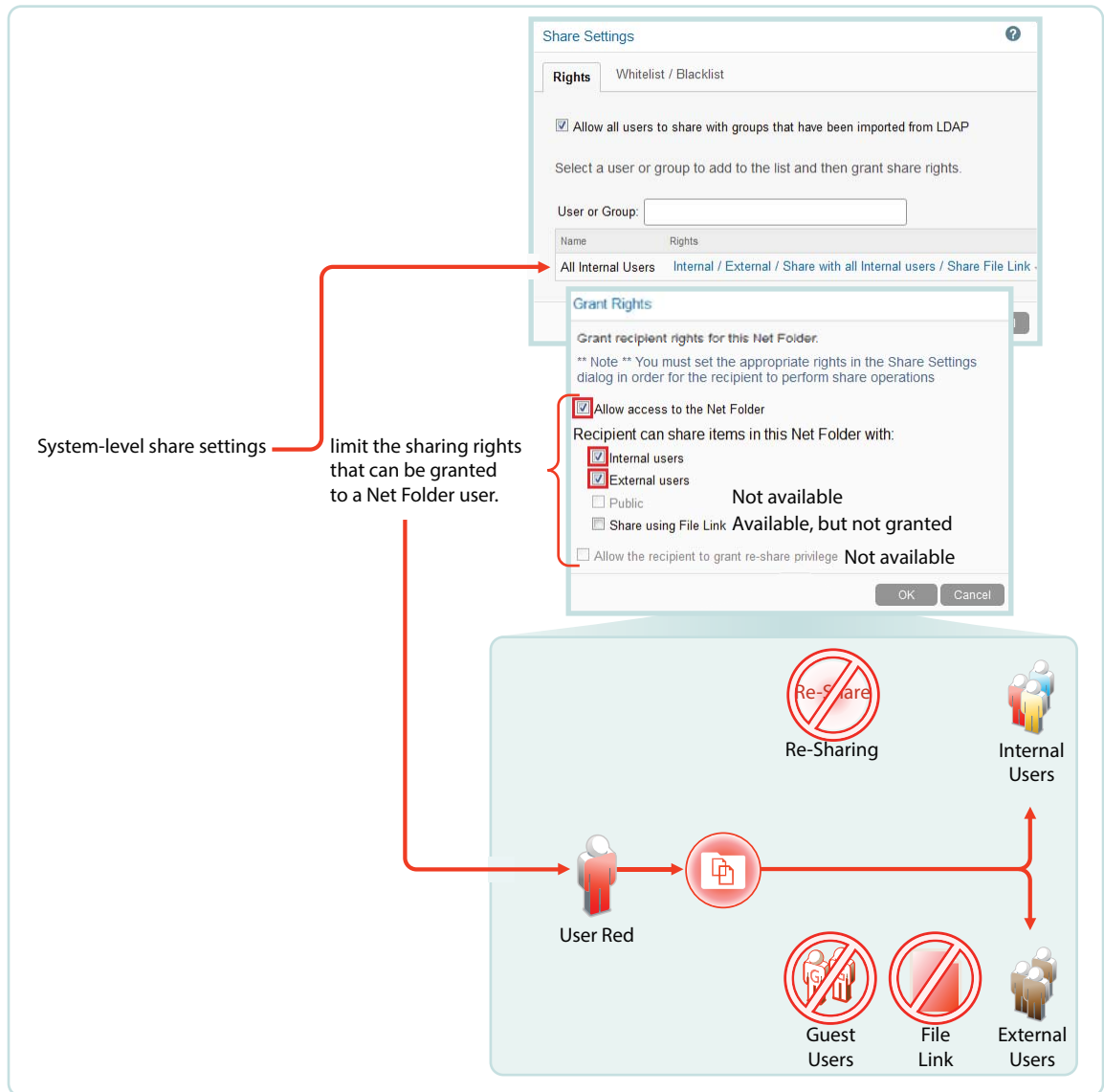
Sharing must be enabled and maximum sharing rights specified at the system level for users individually or as members of groups.

Next, before the users or groups can share files in their assigned Net Folders, they must have sharing enabled and rights assigned 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 12-4](#), user red can only be assigned sharing rights that are allowed at the system level.

Figure 12-4 An Example of Net Folder Sharing



12.2 Understanding Roles and Sharing

Users can share both files and folders in their *My Files* area, but *Net Folders* restrict sharing to only files.

When users send share invitations, they must designate the role that they want the user receiving the share to have for the file they are sharing. For more information about user roles, see [Section 4.4, “Access Through Filr Involves One of Four Possible Roles,”](#) on page 37.

The following are a few foundational concepts that Filr administrators should understand regarding user roles and sharing.

- ♦ [Section 12.2.1, “User Roles and Sharing,”](#) on page 74
- ♦ [Section 12.2.2, “Users Can’t Grant Share Roles That They Don’t Have,”](#) on page 74
- ♦ [Section 12.2.3, “File System Rights Also Affect the Ability to Assign Share Roles,”](#) on page 74

12.2.1 User Roles and Sharing

When users receive share invitations, they also receive one of three user roles: Viewer, Editor, or Contributor. For more information, see [Section 4.4, “Access Through Filr Involves One of Four Possible Roles,” on page 37](#).

Users who receive and accept share invitations can then access shared files through the proxy user assigned to the Net Folder where the file lives.

If multiple users share the same item with a single user, the user receiving the share has the highest role that was shared. For example, if User B shares a file with User A and grants User A Viewer rights to the file, and then User C shares the same file with User A and grants Editor rights to the file, User A has Editor rights to the file.

12.2.2 Users Can’t Grant Share Roles That They Don’t Have

Users with Contributor rights on folders can grant Viewer, Editor, and Contributor rights to other users as Filr system share and Net Folder share settings allow.

On the other hand, Users with Viewer rights on folders can only grant Viewer rights to other users with whom they are allowed to share.

12.2.3 File System Rights Also Affect the Ability to Assign Share Roles

Sharing of files and directories involves an additional layer that provides access and manages what those who are granted rights to share files can actually do.

For users to grant Viewer, Editor, or Contributor rights to another user, they must have the minimum rights that those roles require, as outlined in the following tables.

Table 12-1 NSS File System Rights Required for Assigning Filr Roles

Role	Minimum NSS Rights Required	Comments
Viewer	Read (R), File Scan (F)	These are the minimum file system trustee rights that users must have to view files and folders.
Editor	Read (R), Write (W), File Scan (F)	If the Write file system trustee right is added to Read and File Scan, users can then modify file content.

Role	Minimum NSS Rights Required	Comments
Contributor	Read (R), Write (W), Erase (E), Create (C), Modify, File Scan (F) or Supervisor	To perform contributor functions, users must either have all file system trustee rights to the file or folder (except for Access Control) or the Supervisor right to the file or folder. The presence or absence of Access Control has no meaning in Filr because Filr cannot modify file system trustee rights. A Filr user with the Access Control right on the file system cannot grant <i>file system</i> access to another user through Filr. It is true that Filr users with sufficient Filr permissions can <i>share</i> access to files and folders with other users, but this is a Filr function that leverages the file system rights of Net Folder proxy users. Access to shared files and folders is independent of any file system rights that individual users have or do not have.

Table 12-2 NTFS Permissions Required for Assigning Filr Roles

Role	Minimum NTFS Permissions Required	Comments
Viewer	Read, Read & Execute, List Folder Content	These are the minimum basic permissions that users must have in order to view files and folders. The default special permissions associated with these basic permissions are also required.
Editor	Read, Read & Execute, List Folder Content, Write	If the basic Write permission is added, users can then modify file content. The default special permissions associated with these basic permissions are also required.
Contributor	Read, Read & Execute, List Folder Content, Write, Modify or Full Control	To perform contributor functions, users must either have the basic Modify permission added or they must have the basic Full Control permission. The default special permissions associated with these basic permissions are also required.

12.3 A Caution Regarding the Re-sharing Feature

Use caution when enabling file re-sharing. Removing one user's access rights to an item does not remove the access rights of other users 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 file with User C. Even if User A revokes User B's access rights to the item, User C continues to have access to the shared item.

13 Filr Synchronization

The synchronization of users, groups, files, and folders, along with the associated ACL rights, file contents, and so on, is central to Filr services. This section provides a high-level overview of the various synchronization processes in Filr 1.1.

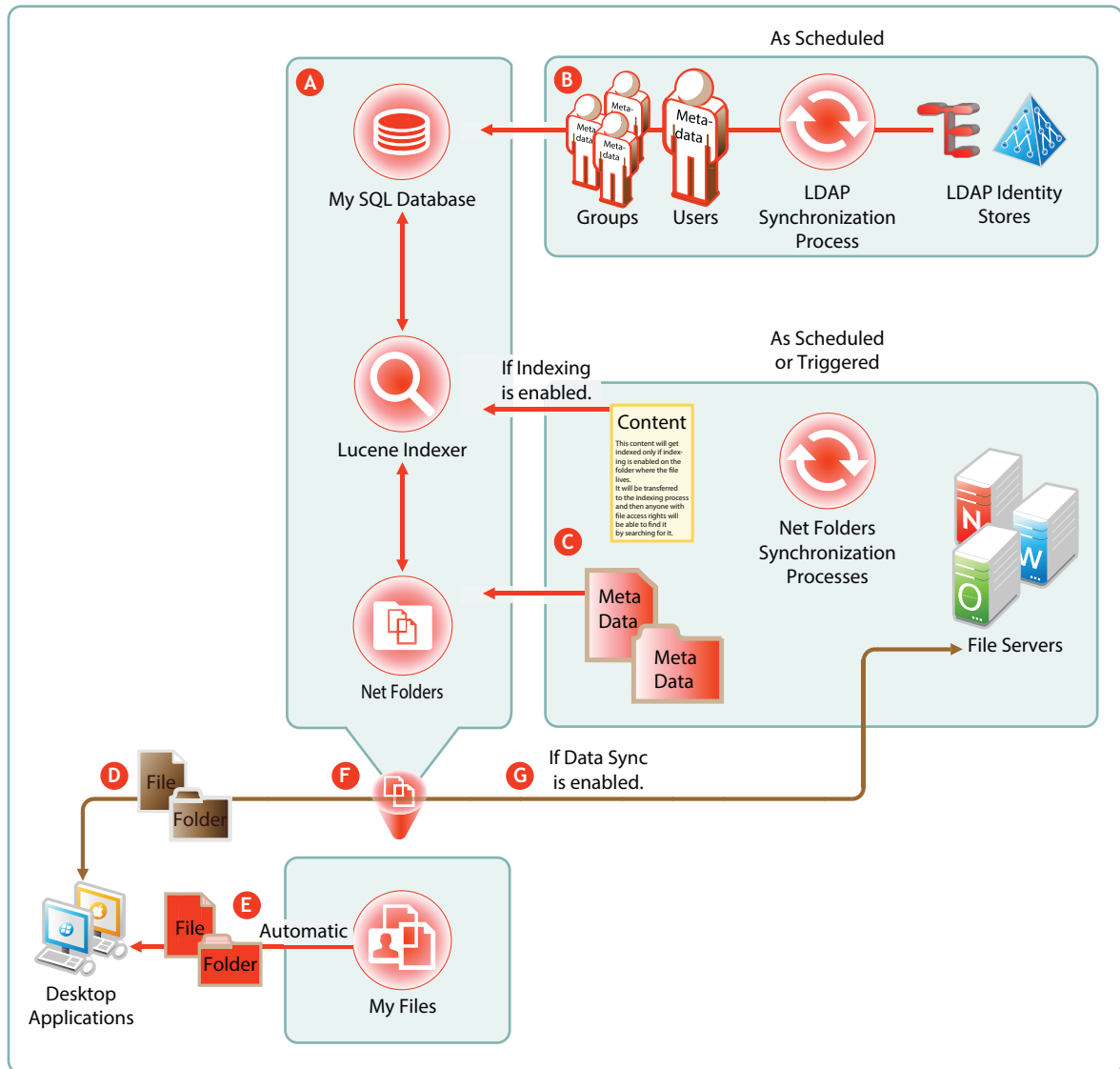
- ♦ [Section 13.1, “Synchronization Overview,” on page 77](#)
- ♦ [Section 13.2, “Net Folder Synchronization Detail Overview,” on page 80](#)
- ♦ [Section 13.3, “Net Folder File Content Indexing Overview,” on page 81](#)

13.1 Synchronization Overview

[Figure 13-1](#) illustrates at a high level the information and content that get synchronized in Filr. The table that follows the figure describes some of the results and implications of the processes that take place.

The figure does not illustrate functional details. For example, it does not attempt to show the flow of LDAP metadata and file/folder metadata to Filr services for storage and indexing.

Figure 13-1 What Gets Synchronized



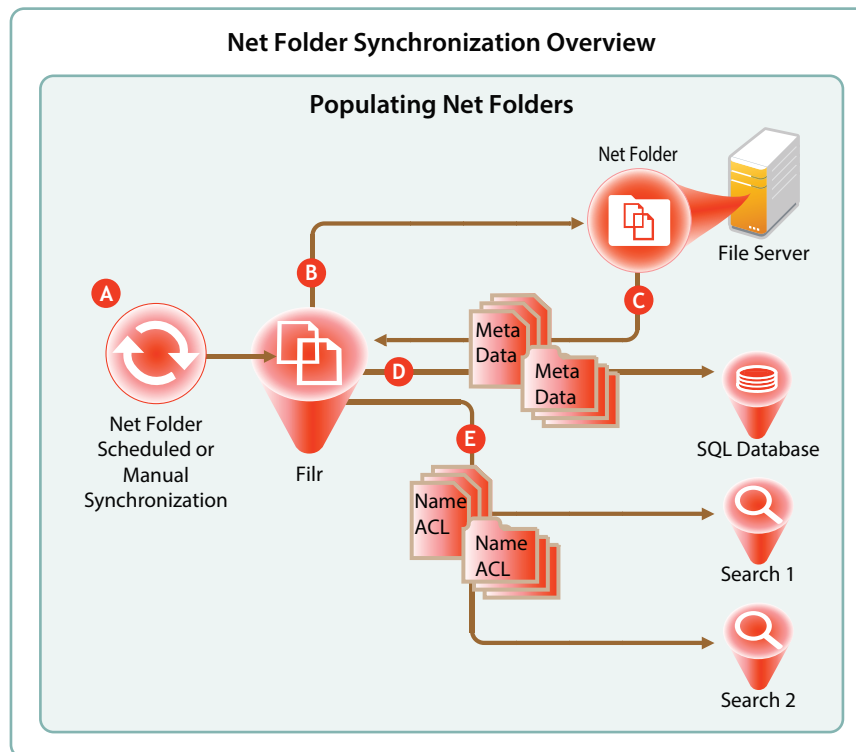
Letter	Details
--------	---------

- | | |
|----------|--|
| A | <p>The MySQL database, the Lucene indexer, and Net Folders work together to provide access to data through Filr. MySQL houses the Filr database.</p> <p>The Lucene indexer indexes all of the LDAP and file storage metadata so that search functionality is available. It also indexes file content for searching in folders that have indexing enabled. (See the note above letter C.)</p> <p>Net Folders provide users who have authenticated with proper credentials, access to files and folders on the network through the file storage metadata that is associated with them.</p> |
|----------|--|

Letter	Details
B	<p>A Filr LDAP synchronization is required when users are added or removed, or when group memberships change in the LDAP identity store.</p> <p>LDAP synchronization is essential to user access to their files and folders. For most organizations, it is usually sufficient to synchronize LDAP once a day. Others require more frequent synchronization to keep Filr abreast of changes in their identity stores.</p>
C	<p>Because file and folder activity on network file servers can be in constant flux, and because synchronization needs vary greatly from server to server, Net Folder synchronization is multi-faceted and very flexible.</p> <p>You can set synchronization schedules for each Net Folder Server. The Net Folders associated with that server are then synchronized according to the general nature of the volume or share where they reside.</p> <p>You can also set synchronization schedules for individual Net Folders that will override the server schedules and synchronize the folders either more or less frequently than the server schedule dictates.</p> <p>You can perform manual synchronizations, which is a very useful feature when creating Net Folders to ensure that desktop application users can download local copies for access.</p> <p>You can enable Just-in-Time Synchronization (JITS) so that each time a folder is accessed from the Web or a mobile device, its content is synchronized with Filr. (The desktop applications do not trigger JITS.)</p>
D	<p>Desktop applications for Windows and Macintosh workstations must download local copies of files and folders before users can access them.</p> <p>Before the files and folders in Net Folders can be downloaded, their metadata must be synchronized with Filr. (See the metadata synchronization process indicated below letter C.)</p> <p>For this reason, many Filr administrators perform a manual synchronization of the meta data when initially setting up a Net Folder. When users access the Net Folder from their desktops, they can immediately start to download the files and folders as expected.</p> <p>For home folders (My Files), the meta data is automatically downloaded so that home folder synchronization to desktop users begins the moment users first access their My Files area.</p> <p>After data is synchronized with the desktops, then as long as the desktops are connected with the network, changes to local copies are immediately synchronized with the file server. If the workstation is disconnected, then when the connection is restored, synchronization is automatic.</p>
E	<p>Files and folders in Filr-based personal storage are automatically synchronized to the workstation's file system.</p>
F	<p>Note that the brown arrow passes through Filr.</p> <p>Net Folder and Home Folder files and folders are not stored in Filr. Instead, Filr simply facilitates the synchronization of the actual files and folders between the file server and the desktop clients.</p>
G	<p>Net Folders are configured by default to allow data synchronization with desktop applications. However, the download functionality can be disabled.</p> <p>If the download functionality is disabled, then desktop application users will not be able to view or access the files and sub-folders in their assigned Net Folders from their workstations. (Unlike Web and mobile access, Desktop applications do not provide Net Folder browsing. Browsing within the desktop applications is limited to local downloaded copies of Net Folder files.)</p> <p>One reason that Filr administrators might disable the download functionality would be to prevent anyone from getting a local copy of sensitive files that must be stored only on the organization's file servers.</p>

13.2 Net Folder Synchronization Detail Overview

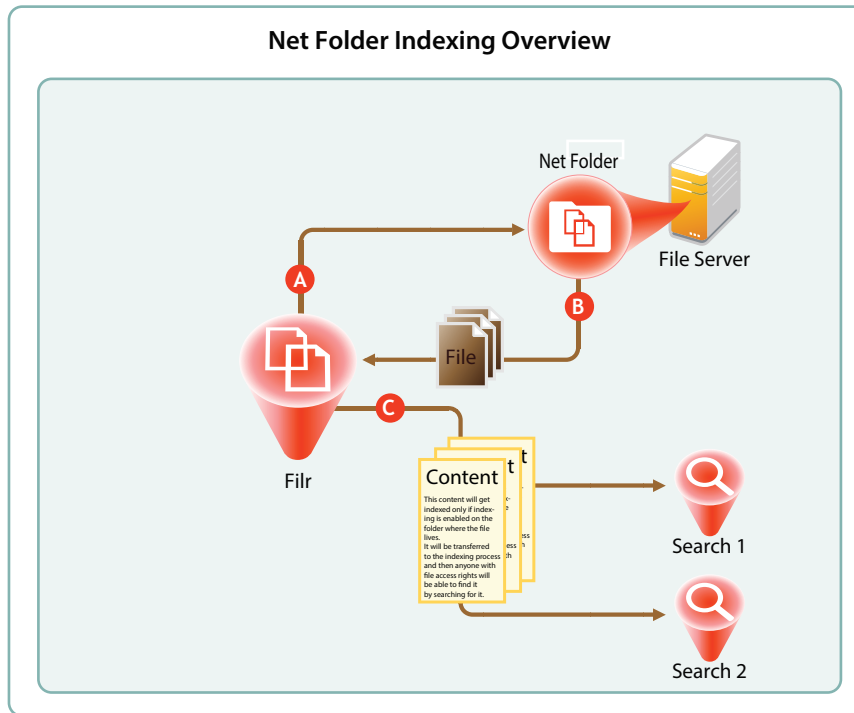
Figure 13-2 Net Folder Synchronization



Letter	Details
A	<p>Full Net Folder synchronizations occur according to individual Net Folder schedules, or if no schedule is defined for the Net Folder, then they occur according to the associated Net Folder Server's synchronization schedule.</p> <p>If no schedule is set, then it falls to Filr administrators to manually synchronize them.</p>
B	<p>When a Net Folder Synchronization is triggered, the Filr appliance connects to the specified Net Folder location on the target file server.</p>
C	<p>Filr then walks the directory structure, collecting meta data (name, size, dates, ACL information, etc.) about each folder and file as it goes.</p>
D	<p>Filr stores the collected meta data in the SQL database.</p>
E	<p>Then Filr sends the folder and file names and ACL information to each Filr Search appliance to be indexed.</p> <p>This makes it possible for users to search for folder and file names, provided that they have sufficient rights on the file system to see them.</p> <p>The majority of Net Folder synchronization work occurs on the File appliance.</p>

13.3 Net Folder File Content Indexing Overview

Figure 13-3 File Content Indexing



Letter	Details
A	For content indexing, Filr first requests copies of all of the files contained in the Net Folder.
B	After a file is copied to the Filr appliance, up to the first 1.1 MB of file content is extracted by Stellent, the technology that provides HTML rendering of file content in Filr.
C	Filr then sends the extracted content to each Search appliance for content indexing. IMPORTANT: Content indexing is powerful and useful functionality. It is also very CPU- and IO-intensive because each file is processed separately. It is therefore important to carefully consider which Net Folders contain files that organization members must be able to search for specific content.

14 Network Time and Filr

Filr 1 appliances and the file servers that they point to should be in the same time zone and they should use the same reliable NTP time source.

Browsers and access devices can be in different time zones than the appliances and servers that they access because all time-stamp-associated actions are handled using UTC. However, if the desktop is not synced to a reliable time source, there could be some confusion. For example, a time stamp on the server might appear to be “in the future” when compared with the time on the desktop.

15 Viewing Files as HTML in Filr

Many files that are accessible through Filr can be viewed as HTML through the same Oracle Outside In technology that is included with Novell Vibe and GroupWise.

To learn more about this technology, see [a PDF document available on Oracle's Web site](#).

16 Users and Groups with Filr

- ♦ [Section 16.1, “Leveraging the Built-in Security of eDirectory and Active Directory,” on page 87](#)
- ♦ [Section 16.2, “Provisioning Users and Groups,” on page 87](#)
- ♦ [Section 16.3, “LDAP Proxy User Role and Rights,” on page 90](#)

16.1 Leveraging the Built-in Security of eDirectory and Active Directory

Novell recommends that you leverage the security features of eDirectory and Active Directory whenever possible.

Both of these directory services have extensive and proven experience with authorization and authentication services. They also provide security features, such as intruder detection, forced complex passwords, password expiration, password history, and so on.

Local user accounts that you create through Filr in the SQL database are certainly not insecure, but neither are they protected by the security features mentioned above.

16.2 Provisioning Users and Groups

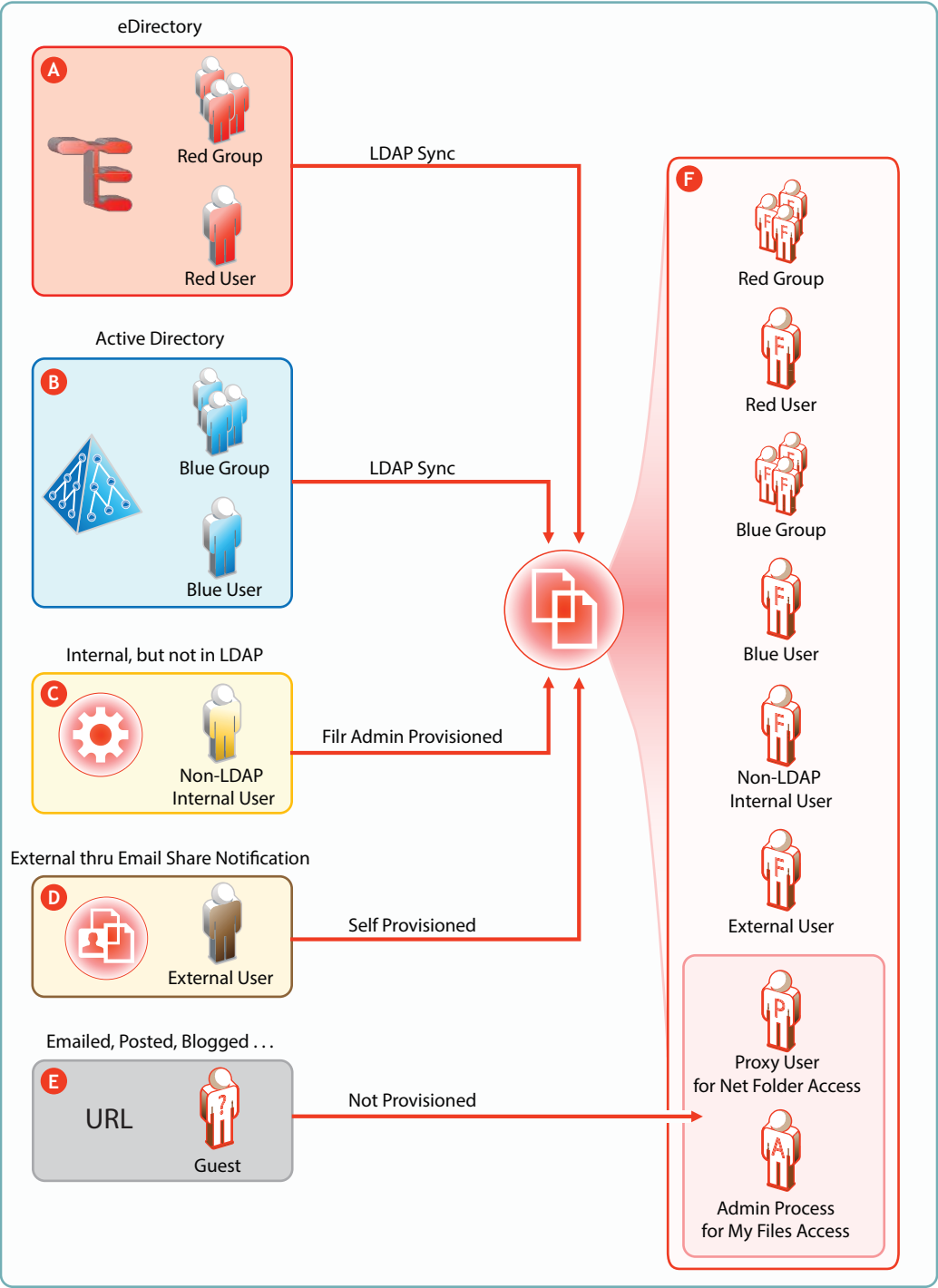
For users to access Filr, they must be provisioned on the Filr system. They can then be assigned [access rights](#).

- ♦ [Section 16.2.1, “User Provisioning Overview,” on page 87](#)
- ♦ [Section 16.2.2, “Types of Filr Users,” on page 89](#)
- ♦ [Section 16.2.3, “The Role of Groups in Filr,” on page 90](#)

16.2.1 User Provisioning Overview

[Figure 16-1](#) provides a high-level overview of the provisioning process that allows users and groups to access an organization’s internal data through Filr.

Figure 16-1 Provisioning Users and Groups



Letter	Details
A	<p>eDirectory users are provisioned on Filr through LDAP/LDAPS synchronization. Synchronization is one-way.</p> <p>Password and other changes on the eDirectory side are handled in Filr without additional configuration.</p> <p>Password and other changes can be made to a user's Filr configuration. However, they are not synchronized back to eDirectory. Instead, they are overwritten by the configuration in eDirectory with each synchronization.</p>
B	<p>Active Directory (AD) users are provisioned on Filr through LDAP/LDAPS synchronization. Synchronization is one-way.</p> <p>Password and other changes on the AD side are handled in Filr without additional configuration.</p> <p>Password and other changes can be made to a user's Filr configuration. However, they are not synchronized back to AD. Instead, they are overwritten by the configuration in AD with each synchronization.</p>
C	<p>Filr administrators can also provision users on the Filr appliance. These are referred to as Local users in the documentation and Filr interfaces.</p>
D	<p>External User accounts are created when share invitations are issued through email from Filr. The users provision themselves with a password, and so on when they log in to Filr.</p>
E	<p>Public users (Guests) aren't provisioned with accounts on Filr. Public users are anonymous to Filr and are allowed access to shared files in Net Folders through the Proxy User assigned to the Net Folder they are accessing. For shared files and folders in My Files, Public users gain access through the Filr admin process.</p>

16.2.2 Types of Filr Users

- ♦ **LDAP Synchronized:** Users and groups can be synchronized from an internal LDAP identity store.

After users and groups are provisioned through an initial synchronization, they have accounts in Filr that correspond to their original identities, but these are only secondary. By leveraging the rights of one or more [LDAP proxy users](#) in the directory, Filr synchronizes regularly to keep authentication credentials current, update changes in home directory and file system rights assignments, and so on.

- ♦ **Filr Admin Created:** Users and groups can be created by Filr administrators.

Admin-created groups are managed as part of the Filr system. They can be assigned personal storage, but access to Net Folders and other users' home directories happens only through Filr-based sharing.

- ♦ **External, Self-Provisioned:** Users can be invited to participate through share invitations.

When they respond to the invitations, they are given the opportunity to self-provision an account on the Filr server.

After they are provisioned, they can then be granted personal storage and other permissions similar to those enjoyed by internal users.

- ♦ **Guest Users:** When Filr administrators allow it, Filr users can share the URLs to files in Net Folders and My Files, making them available to the general public. Those who access files in this way are referred to as "Guest" users. Guest users are not provisioned and anonymous from a Filr perspective.

16.2.3 The Role of Groups in Filr

Users can be assigned rights on Filr as members of groups, including as members of either the `All Internal Users` group or the `All External Users` group, which includes those whose accounts were created as a result of an email share invitation.

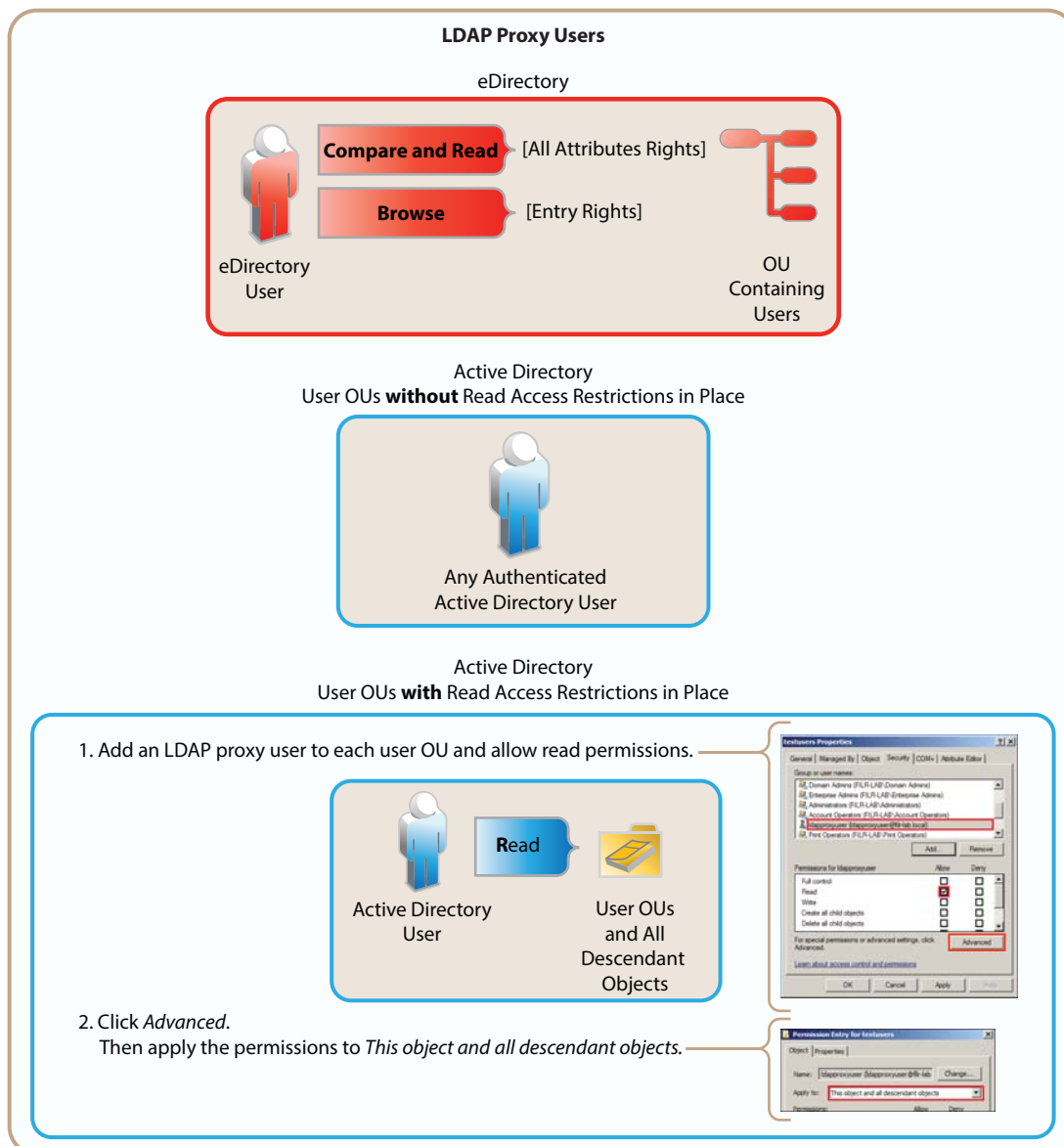
16.3 LDAP Proxy User Role and Rights

Filr synchronizes LDAP users by leveraging proxy users in the targeted LDAP directories that have sufficient rights to read the user and group information required by Filr.

Currently, eDirectory and Active Directory are supported as LDAP identity stores.

The rights required for LDAP synchronization are platform-specific, and for Active Directory they vary depending on whether read access restrictions are in place, as illustrated in [Figure 16-2](#).

Figure 16-2 Rights Required for LDAP Proxy Users



A Documentation Updates

This section summarizes the changes that have been made to this guide since the initial release of Filr 1.1.

12 November 2014

Section	Change
Section 2.6, "Ports Used in Filr Deployments," on page 26	Added port 11211 for search appliances.

10 November 2014

Section	Change
Section 4.3.1, "Roles and Net Folders," on page 37	Corrected two missing links.

3 November 2014

Section	Change
Chapter 13, "Filr Synchronization," on page 77	Corrected technical inaccuracy in explanation of the relationship between Net Folder Synchronization and file content indexing.

23 October 2014

Section	Change
Section 13.2, "Net Folder Synchronization Detail Overview," on page 80	New section.

8 October 2014

Section	Change
Chapter 16, "Users and Groups with Filr," on page 87	Fleshed out the user and group information a bit more. Added a new section about LDAP proxy users .

