Deployment Guide

iFolder 3.9.2

January 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/) for more information on exporting Novell software. Novell assumes no responsibility for your failure to obtain any necessary export approvals.

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).

Novell Trademarks

For Novell trademarks, see the Novell Trademark and Service Mark list (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

Novell iFolder is designed with the basic principle of scalability to support organizational modifications. The Novell *iFolder 3.9.x Deployment Guide* describes how to successfully deploy the following iFolder components in your production environment:

- iFolder Enterprise Server
- iFolder Web Access Server
- iFolder Web Admin Server
- iFolder Client

The cases considered in this guide are not exhaustive. They are intended to be examples that can be mapped to your organizational functions.

Audience

This guide is intended for iFolder administrators.

Feedback

We want to hear your comments and suggestions about this manual and the other documentation included with this product. Please use the User Comments feature at the bottom of each page of the online documentation.

Documentation Updates

For the most recent version of the Novell *iFolder 3.9.x Deployment Guide*, visit the Novell iFolder 3.*x* Documentation.

Additional Documentation

For documentation, see the following:

- *Novell iFolder 3.x documentation*
- *Novell Open Enterprise Server documentation*
- *Novell eDirectory 8.8.x documentation*
- *Novell iManager 2.7.x documentation*
- *Novell Technical Support*

1 Understanding iFolder Deployment

Administration overhead and handling user support calls are major tasks in the Information and Service department of any organization. Deploying a service without proper understanding of the current requirements, the quality of the service, and the projected organizational growth can cause unexpected demands on the system that lead to extra costs to manage the service.

This guide helps you understand the various scenarios in which the Novell iFolder service can be deployed, based on requirements and future expansion plans. It addresses various iFolder deployment scenarios and use cases ranging from simple to complex, targeting small, medium, and enterprise users. You can also request assistance from Novell support personnel to help you implement these deployment scenarios.

1.1 Before You Deploy iFolder

Before you install Novell iFolder, you must plan the setup that is suitable for your enterprise. You should organize the deployment based on your current requirements, the quality of service required, and the projected needs for future growth.

Before you deploy iFolder, consider the following:

1.1.1 Hardware and Software Requirements

Server Hardware Requirements

A Novell iFolder server has the following hardware requirements:

- A server class machine for Open Enterprise Server 11
- A minimum of 2 GB RAM
- 200 GB dedicated storage (200 MB storage per user for 1000 users)
- Minimum 100 Mbps dedicated NIC

This guide follows the OES 11 Linux recommended hardware for server, storage area network (SAN), and clients. This also includes the network requirements.

Server Software Requirements

A Novell iFolder server has the following software requirements:

- Novell Open Enterprise Server 11 with updated Mono patches
- Apache* configured in work mode
- Apache configured for traditional NIC

Client Requirements

The Novell iFolder client supports the following workstation operating systems:

- SUSE Linux Enterprise Desktop (SLED) 10 SP3
- SUSE Linux Enterprise Desktop (SLED) 11 SP1 64-bit
- openSUSE 11.4

  NOTE: The iFolder Linux client requires the Mono framework for Linux and a GNOME desktop for iFolder Nautilus plug-in support.

- Windows XP SP3 32-bit
- Windows Vista SP1
- Windows 7
- Macintosh OS X 32-bit (Intel architecture) v10.5 and later (requires Mono 2.4.2.3). PowerPc architecture is not supported.

1.1.2 Security Considerations

Based on your security requirements, you can create an encrypted iFolder or a normal iFolder. The communication between the iFolder server, clients, Web Admin server, and Web Access server can be set to non-SSL or SSL (secure) or both.

1.1.3 Additional Documentation

For more information, see the following:

- *iFolder 3.9.1 Administration Guide*
  - "Planning iFolder Services"
  - "Prerequisites and Guidelines"
- *iFolder 3.9.1 Cross-Platform User Guide*
  - "Getting Started"
- *Novell iFolder 3.9.2 Security Administration Guide*

1.1.4 Encryption and Key Recovery

For detailed information on encryption and key recovery, refer to the following guides:

- *iFolder 3.9.1 User Guide*
  - "Encryption"
  - "Encryption Policy Settings"
  - "Managing Passphrase for Encrypted iFolders"
- *iFolder 3.9.1 Security Administration Guide*
  - "Creating an Encrypted iFolder"
  - "Creating Strong Password And Passphrase"
  - "Using the Recovery Agent"
  - "Transferring the Encryption Key"

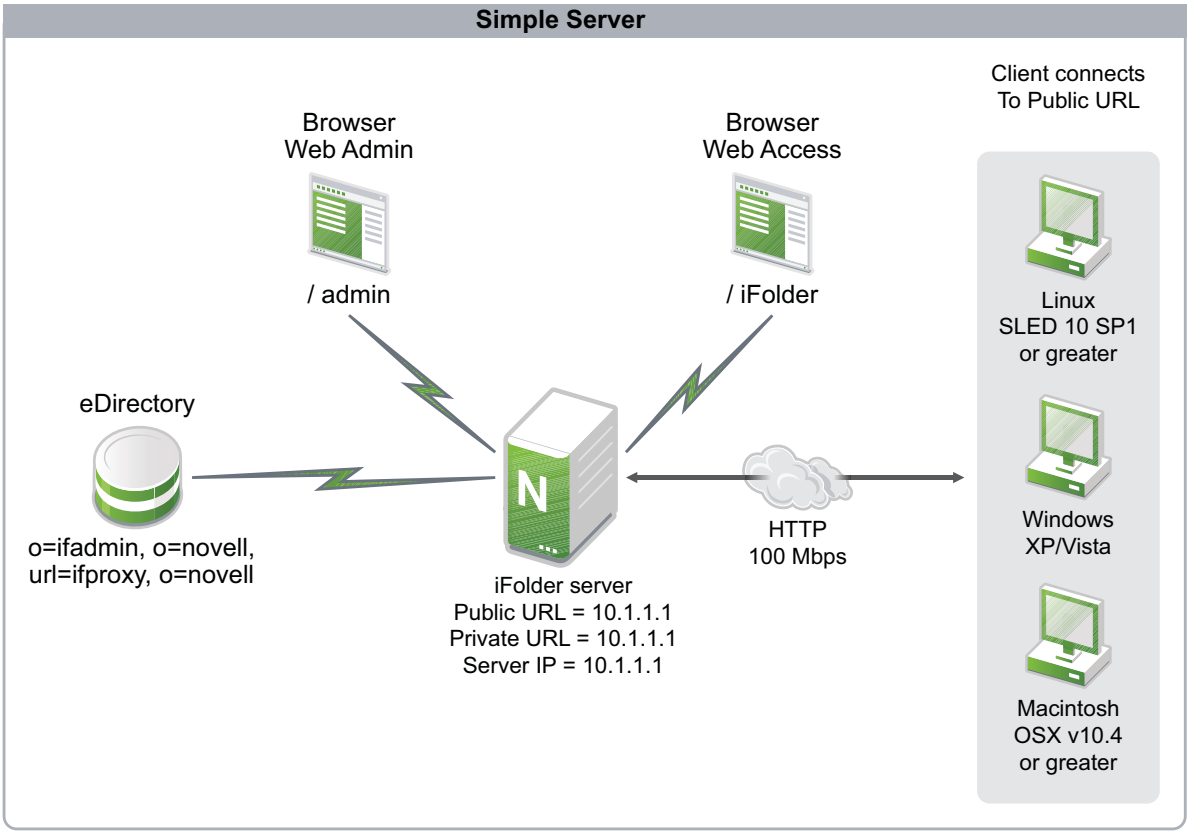
1.2 Using a Deployment Manager

Novell iFolder supports auto-account creation through an XML-based response file. You can use any deployment manager, such as Novell ZENworks, to distribute the response file along with the client to the user machines. After the client is installed, the client startup auto-creates an account when the response file is detected. This is beneficial for large deployments. It also saves time for users and avoids support calls because of account creation errors.

2 Single-Server Deployment

A single-server setup consists of a single server with up to one thousand clients simultaneously connected to it. In such a setup, the iFolder server and the database are located on a single Open Enterprise Server (OES) 11 server, and the client workstations are connected to it. This scenario is illustrated in the following figure.

Figure 2-1 *Single Server*



In a single-server setup, all three iFolder components are installed and configured on the same server. Authentication of users is always LDAP-based. This means that all the users trying to log in and access iFolder data are authenticated with the LDAP server first and then allowed to access iFolder data. All client-to-server communication and communication between server components is done via HTTPS. In this setup, a single server hosts the iFolder server, iFolder Web Access services, and iFolder Web Admin services. Load balancing cannot be performed in this setup and heavy Web Access usage is also not recommended.

The following sections describe the deployment of a single server setup in your environment.

2.1 Key Benefits

The key benefits of a single-server setup are as follows:

- A single-server setup is easy to maintain because operations such as updating patches, upgrading the server, taking a backup, and restoring a backup are limited to a single server.
- Sharing iFolders is faster in a single-server setup as opposed to a multi-server environment. This is because in a single-server setup, users are provisioned to a single server, but in a multi-server environment users are provisioned across multiple servers.
- A single-server setup is beneficial for small setups of 500 to 1000 users. In such a scenario, where all users are provisioned on the same server, the response time is guaranteed. For example, if a server has a dedicated network interface card (NIC) with a minimum of 1 Gbps capacity and each client has a NIC with a minimum capacity of 100 Mbps. With this configuration, a user can upload or download a 1 GB file in less than 5 minutes.

2.2 LDAP Configuration

The LDAP configuration information for a single-server setup is as follows:

- eDirectory, OpenLDAP*, and Active Directory* directory servers are supported.
- Ensure that all users are a part of either a container or a static/dynamic group on the LDAP directory server. During iFolder installation, you must use the same container or group DNs to configure the *Search context* field.
- iFolder supports both secure and non-secure communication with the directory server. You can choose any communication channel that fits your requirements. Ensure that the directory server is listening on standard LDAP ports for secure and non-secure channels.

2.3 Scalability Parameters

The scalability parameters for a single-server deployment are as follows:

- A single-server setup is ideal for small setups of 500 to 1000 users.
- Clients must have a dedicated network interface card (NIC) of 100 Mbps capacity.
- Web-based access must be low, and thick client access must be moderate with up to 500 active connections.
- Data transfer (synchronization of user data) rate must be 10 MB per hour per client.
- The synchronization interval must be 10 minutes.

2.4 Deployment Scenarios

The following sections describe the deployment scenarios in a single-sever setup:

2.4.1 User Data Backup

Consider a scenario where an organization wants a set of 500 users to be able to back up their desktop data at regular intervals. The organization provides a dedicated LAN link to ensure that 500 users can synchronize the data at the rate of 10 MB per hour. A single-server setup is ideal in such a scenario. Before you use a single-server setup for this scenario, you must consider the following policies:

- "Limiting the Number of iFolders Per User" on page 15
- "Disabling Sharing" on page 15
- "Setting a Disk Quota" on page 15

Limiting the Number of iFolders Per User

In order to maintain the server load at an optimal level, you must limit the number of iFolders that a user can create. Use the Web Admin console to limit the number of iFolders per user in a given iFolder system. You can set this policy at user and system levels. The recommended limit of iFolders per user is 5.

Disabling Sharing

To enable an effective backup and to avoid user data collision, you must disable iFolder sharing. If necessary, you can enable sharing with read-only access. This is useful to maintain the 10 MB per hour data transfer rate at 500 simultaneous connections.

Setting a Disk Quota

The disk quota limit is based on the server capacity. The recommended limit is 4 GB per user. This requirement can be a floating value, so that an average of 4 GB per user is achieved. This means that default settings are used to achieve the requirement.

2.4.2 Document Management

This deployment scenario illustrates the iFolder ability to synchronize documents across various levels in an enterprise. Consider a scenario where a customer in a bank initiates a loan request process by submitting an application form to a bank clerk. As a part of the loan request process, the application form is sent to an official at a higher level for approval.

In this scenario, you can create three iFolders named Submission, Level 1, and Level 2 for the initial submission and for the next levels of approvals. The first two iFolders, Submission and Level 1, can be shared between the clerk and the manager. The Level 2 iFolder can be shared between the manager and the senior manager and made inaccessible to the clerk.

After the initial verification, the clerk can move the loan application form stored in the Submission iFolder to the Level 1 iFolder. The manager accesses the verified loan application form from the Level 1 iFolder for further verification and approval. If the loan request is verified and approved, the manager moves the application form to the Level 2 iFolder for the senior manager's approval.

The various levels of access allow you to use a single-server setup to easily manage the flow of documents in an enterprise.

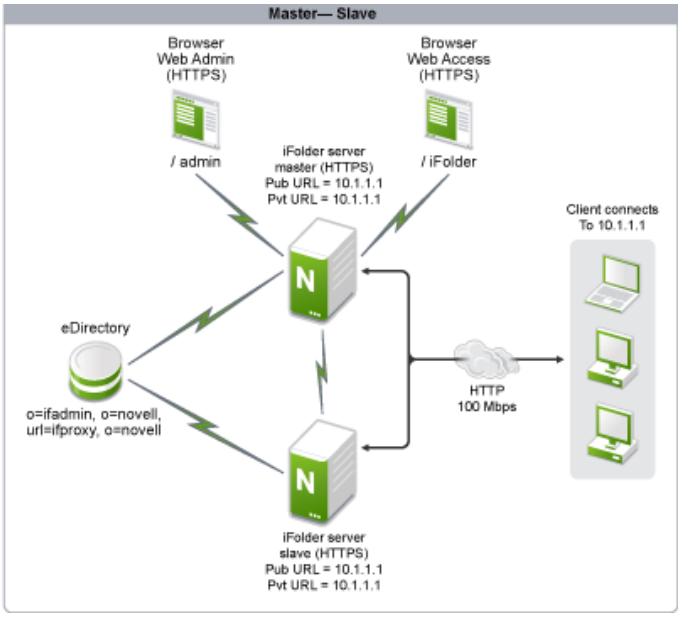
3 Multi-Server (Master-Slave) Deployment

A multi-server setup consists of multiple servers, which can each have more than a thousand simultaneous connections at any point of time. Multi-server configurations are of two types, master-master and master-slave. This section discusses the master-slave setup, and the master-master setup is discussed in Chapter 4, "Multi-Server (Master-Master) Deployment," on page 21.

Multi-server configurations are beneficial for organizations that are expanding their employee strength. This type of setup is also useful for organizations that have their workforce spread across the globe with multiple branches across countries and continents. You can use a multi-server deployment to synchronize and share data across the globe with a predictable response time.

You can convert a single-server system to a multi-server system by connecting an additional server to the main server and creating a master-slave configuration. A multi-server (master-slave) setup is illustrated in the following figure.

Figure 3-1 *Master-Slave*



In this setup, the iFolder server and the iFolder database are located on Open Enterprise Server (OES) 11 servers with client workstations connected to the iFolder server. The iFolder master and slave servers are connected to each other to exchange metadata information. The Web Access and Web Admin consoles of the master server are accessed through a browser. User authentication is done through the eDirectory secure LDAP protocol and all the server-to-server and client-to-server communication is done via HTTPS.

The following sections describe a multi-server (master-slave) iFolder setup:

3.1 Key Benefits

The key benefits of a multi-server (master-slave) setup are as follows:

- Supports a secure communication channel (SSL) to secure the data exchanged on the wire and secures iFolder data stored on the server with the Novell patented encryption and recovery mechanism.
- Ensures scalability with no theoretical limit on the number of servers participating. In addition, each server can have multiple data volumes configured with any limit.
- Guarantees response time because the number of users that are provisioned per server is limited to 1000, so that each user can have a predictable response from the server if the server has a dedicated network interface card (NIC) with a minimum of 1 Gbps capacity and each client has at least a 100 Mbps NIC. With this configuration, the user can upload or download a 1 GB file in less than 5 minutes, which is almost 4 MB per second.
- Enables users across different geographical locations to share data in a secure manner.
- Enables Novell iFolder servers across different geographical locations to be integrated with Business Continuity Clusters (BCC) for data replication and high availability.

3.2 LDAP Configuration

The LDAP configuration information for a multi-server (master-slave) setup is as follows:

- eDirectory, OpenLDAP, and Active Directory directory servers are supported.
- The LDAP Search Context option must be set to an appropriate value for both master and slave in order to optimize LDAP sync time on both servers. The Master LDAP search context specified must either be a superset of all the slave search contexts or a combined list of all slave search contexts as shown in the examples given below:
  - Master context `o=org`, Slave1 context `ou=ku,o=org`, Slave2 context `ou=dl,o=org`
  - Master context `ou=ku,o=org##ou=dl,o=org`, Slave1 context `ou=ku,o=org`, Slave2 context `ou=dl,o=org`
- Ensure that each iFolder server has its own eDirectory replicas so that the authentication happens locally instead of walking the eDirectory tree.
- iFolder supports both secure and non-secure communication with the directory server. You can choose any communication channel that you need. Ensure that the directory server is listening on standard LDAP ports for secure and non-secure channels.

3.3 Scalability Parameters

The scalability parameters for a multi-server (master-slave) deployment are as follows:

- The multi-server (master-slave) deployment is scalable to 1000 users.

  If an exclusive Web Access server is not deployed, the Web Access users are also considered in this scalable parameter. An independent Web Access server can handle 1000 users at any given point in time. If there are more than 1000 Web users connecting at any given point in time, consider the deployment scenario in Chapter 5, "Master-Slave Deployment for a High Web Access Load," on page 25.
- The Enterprise iFolder server must have Web Admin and Web Access capability.
- Web Access usage must be minimal to ensure guaranteed response time.
- Clients must have a dedicated NIC of at least 100 Mbps.
- Web-based access must be low, and thick client access must be moderate with 500 active connections.
- The data transfer (synchronization of user data) rate must be at least 10 MB per hour per client.
- Both SSL and non-SSL communication is supported.
- The synchronization interval must be no more than 10 minutes.
- If the master and slave iFolder servers are in two different geographical locations, individual Web Access servers are beneficial to improve the response time.

3.4 Deployment Scenarios

The following sections discuss the deployment cases in a multi-sever setup. These deployment cases indicate how a multi-server (master-slave) setup can be used for load balancing and data synchronization in an organization where the employee storage requirement is growing in terms of size and frequency of access. In a situation where an organization's employee storage requirement is increasing, an organization needs a reliable response time for users. Also, data synchronization in such a situation needs strict time constraints.

- Section 3.4.1, "Load Balancing," on page 19
- Section 3.4.2, "Data Synchronization," on page 20

3.4.1 Load Balancing

Consider the case of a global manufacturing firm that requires its component plans and drawings to be saved in a secure place. The workforce involved in the manufacturing division of the organization needs this confidential information to be accessed, updated, added, or shared with peers in other departments for various actions to be taken, such as approval of plans.

In this case, you can deploy Novell iFolder in a multi-server setup so that the manufacturing divisions can share the plans and other documents in a secure manner. Because the number of units manufactured might be time-sensitive and limited, the plans and drawings must reach the respective divisions on time, and the operators must be able to retrieve, update, and synchronize them within the required response time. A multi-server configuration is very useful in managing this kind of load in a timely manner.

3.4.2 Data Synchronization

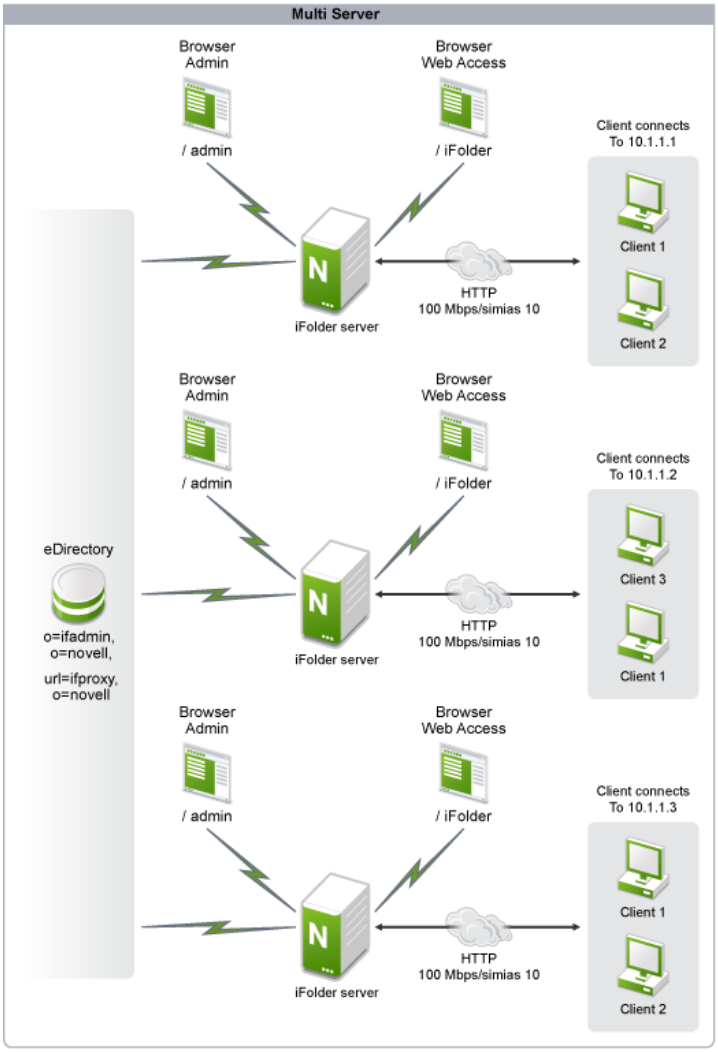
Consider an example where a company is organizing an event to showcase its products on the same day in different geographical locations. Representatives of the company are at the different locations for the event with their presentations, spreadsheets, and Flash* videos. The presentation material needs to be replicated across different locations. Because the presentation material might need last-minute changes, it needs to be synchronized in real time. In such a scenario, an iFolder multi-server (master-slave) deployment can offer real-time data synchronization capabilities.

4 Multi-Server (Master-Master) Deployment

A multi-server (master-master) setup consists of multiple domains that are created so that master servers can communicate to each other. A master-master setup is particularly useful for organizations that have multiple independent departments that do not need to communicate with each other. Also, this setup is beneficial for organizations that have offices in different geographical locations where each location needs its own domain.

A multi-server (master-master) setup is illustrated in the following figure. In this setup, all three servers host the iFolder server, Web Access console, and Web Admin console. Each of these servers is independent from the others and serve an independent set of clients. The clients or users connected to these servers can view and share iFolders with users of the same server only. User authentication is done through the eDirectory secure LDAP protocol.

Figure 4-1 *Multi Server*



The following sections describe the multi-server (master-master) iFolder setup.

- Section 4.1, “Key Benefits,” on page 23
- Section 4.2, “LDAP Configuration,” on page 23
- Section 4.3, “Scalability Parameters,” on page 23
- Section 4.4, “Deployment Scenarios,” on page 23

4.1 Key Benefits

The key benefits of a multi-server (master-master) setup are as follows:

- The master-master setup is useful in cases where you want to set up two separate servers for two separate and unrelated sets of users. This setup is similar to two separate single-server setups.
- The master-master setup limits sharing to a set of related users.
- This configuration is most suitable when an organization has more than one identity pool.
- In an organization with a single identity tree, this configuration allows a particular domain to be part of the Business Continuity Clusters (BCC) for data replication and high availability.

4.2 LDAP Configuration

The LDAP configuration information for a multi-server (master-master) setup is as follows:

- eDirectory, OpenLDAP, and Active Directory directory servers are supported.
- Each master server must be configured to a particular container or a group (static or dynamic). These sets of users cannot share the iFolder with other master servers.
- Ensure that all users are part of either a container or a static/dynamic group. During iFolder installation, you must use the same container or group DNs to configure the search context field.
- iFolder supports both secure and non-secure communication with the directory server. You can choose any communication channel that you need. Ensure that the directory server is listening on standard LDAP ports for secure and non-secure channels.

4.3 Scalability Parameters

The scalability parameters for a multi-server (master-master) deployment are as follows:

- Scalable to 1000 simultaneous connections per master.

  If a slave is included, see Section 3.3, “Scalability Parameters,” on page 19 in Chapter 3, “Multi-Server (Master-Slave) Deployment,” on page 17
- Each master server can store up to a terabyte of data.
- The synchronization interval must be 5 minutes.

4.4 Deployment Scenarios

A multi-server (master-master) setup is particularly beneficial for enterprises that have multiple lines of businesses spread across different geographical locations. The following sections discuss the deployment scenarios for a multi-sever (master-master) setup:

4.4.1 Functional Grouping

Consider the example of a global consulting firm that provides consultancy services on information management, construction services, and automobile manufacturing. The employees of a particular consulting do not need to communicate with employees of other groups because the nature of the work in each consulting group might be entirely different.

In this case you can deploy the iFolder in master-master setup, based on the storage need, frequency of access, and nature of access. Also, if heavy Web access is expected for a particular domain, then a separate Web Access server can be configured.

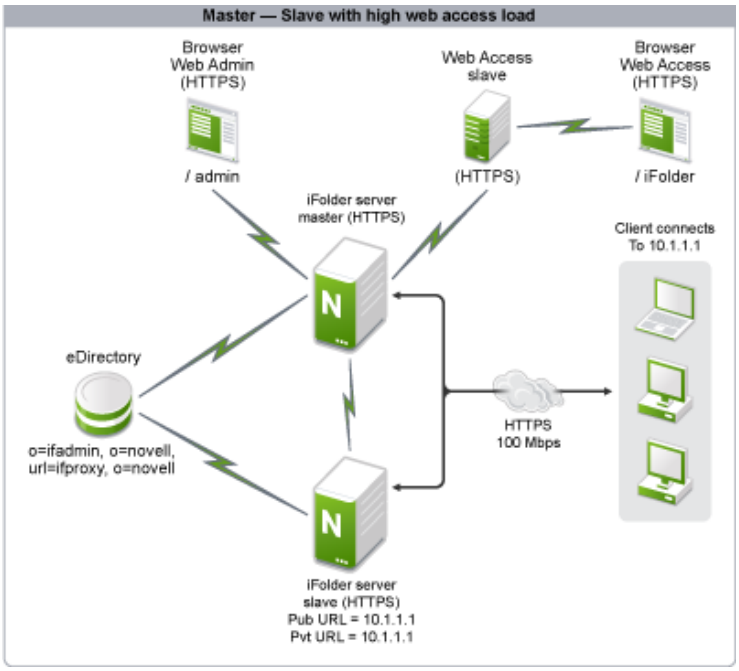
4.4.2 Specialized Services

Using master-master setup, specialized services can be also be provided for a particular domain. For instance, a particular domain can use BCC to enhance the response time, have a unique set of policies, and use an individual Web Access server to support the users on the move.

5 Master-Slave Deployment for a High Web Access Load

In a master-slave deployment with a high Web Access load, the setup consists of a master server, a slave server, and a slave server dedicated to Web Access. In this setup, the iFolder server and the database are typically located on the master and slave servers, and the client workstations are connected to the iFolder server. This setup also uses a dedicated iFolder Web Access server to serve and prioritize a high number of iFolder Web Access client requests. This scenario is illustrated in the following figure:

Figure 5-1 *Master-Slave with High Web Access Usage*



This setup is useful in organizations where employees tend to access confidential documents by using cell phones or mobile devices. This deployment helps you securely share confidential information such as organization documents, presentations, Flash videos, sales and marketing data, and spreadsheets. A dedicated setup is required if there are thousands of mobile users.

The following sections describe a master-slave deployment with a high Web Access load.

5.1 Key Benefits

The key benefits of a master-slave setup with a high Web Access load are as follows:

- An organization that has a high Web-based data access load can deploy this setup. In this case, the Web Access application is set up on a separate physical server. This server serves all the user Web requests and reduces the load of iFolder server that serves the back-end data. All the user requests are received by the Web Access server, which can be a publicly accessible server. The actual iFolder server is deployed within the organization firewall.
- All communication to the Web Access server can be SSL-enabled.The communication between the Web Access server and the iFolder server can also be SSL-enabled if a secure channel is required between these servers.
- The number of hits per second to the Web Access server through a browser is based on the server processing capability and the network link. A Novell iFolder Web Access server does not limit the number of hits because it runs behind Apache and Apache governs the processing capability. The recommended number of hits per second is around 1000, which means 1000 simultaneous connections from users can exist at any time.
- The hits to the Web Access server do not need to translate to requests to the iFolder server. The iFolder server capability is about 1000 simultaneous requests in a medium server class machine. If the H/W is higher, this capability can be increased.
- Multiple Web Access servers can be configured in a multi-server iFolder setup, which means that each iFolder server (master or slave) can have its own Web Access server.

5.2 LDAP Configuration

The LDAP configuration information for a master-slave deployment with a high Web Access load is as follows:

- The eDirectory, OpenLDAP, and Active Directory directory servers are supported.
- Each master server must be configured to a particular container or a group (static or dynamic). These sets of users cannot share the iFolder with other master servers.
- Ensure that all users are part of either a container or a static/dynamic group. During iFolder installation, you must use the same container or group DNs to configure the search context field.
- iFolder supports both secure and non-secure communication with the directory server. You can choose any communication channel that you need. Ensure that the directory server is listening on standard LDAP ports for secure and non-secure channels.

5.3 Scalability Parameters

The scalability parameters for a master-slave deployment with a high Web Access load are as follows:

- Organizational strength can be up to x1000 users, where x is the number of iFolder servers.
- An independent Web Access server can handle up to 1000 users at any given point in time. If more than 1000 Web users connect at any given point in time, an independent Web Access server can be deployed per iFolder server to handle more load.
- Clients must have a dedicated NIC of at least 100 Mbps.
- Moderate thick client access with 500 active connections is supported.

- The data transfer (synchronization of user data) rate must be 10 MB per hour per client.
- The synchronization interval must be 10 minutes for thick clients.
- Both SSL and non-SSL communication is supported.
- Heavy Web access is supported with a data transfer rate of 60 MB per hour per client.

5.4 Deployment Scenarios

The following sections discuss deployment scenarios in a master-slave deployment with a high Web Access load:

- Section 5.4.1, "Web Access," on page 27
- Section 5.4.2, "Online Application Submission," on page 27

5.4.1 Web Access

Consider an example of a consulting firm that provides various services to its clients by presenting products or solutions, performing customer product analysis in spreadsheets, or recording customer scenarios. In addition, a majority of the workforce of this firm is always on the move.

In such a situation, you can deploy a master-slave deployment to effectively meet the needs of the employees. The employees can use iFolder over the Internet to securely access the organization's presentations about various solutions and products that the customer is interested in. The sales or marketing representatives of the firm can download the presentations and spreadsheets through iFolder Web Access and do online presentations.

The sales or marketing representatives can also modify presentations and upload them to the iFolder, then share the iFolder with offsite representatives for evaluation, or they can distribute the modified presentations to other sales or marketing representatives across the globe. Novell iFolder effectively synchronizes these information units among company representatives so that everyone has access to the latest information.

5.4.2 Online Application Submission

Consider the case of a banking organization that is planning to provide online banking services to its customers. The online banking features could include all types of application submission procedures, so that the customer can visit the online bank instead of going to the actual bank location.

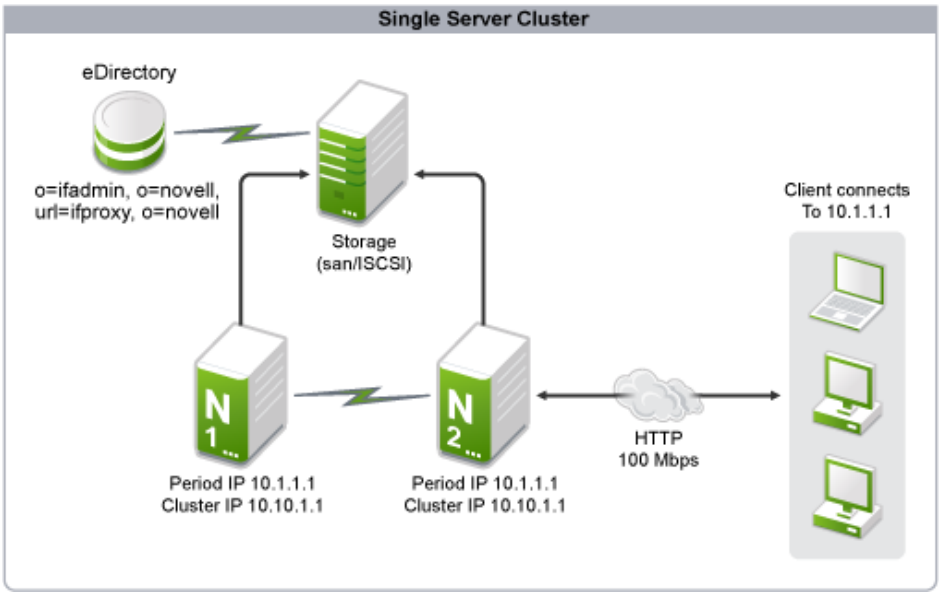
One such application submission procedure is the loan application. For every customer, the bank can allocate an iFolder and the customer can receive documents, update them, and upload them again to the iFolder for the bank's verification.

The document exchange procedure can be fully automated so the data between the bank and the customer is always in sync and the customers get a real-time experience wherever they are. This effectively replaces the form-based submission procedure. Using iFolder, the customer can download the document, fill in the form at leisure, and upload it to his or her own iFolder, which synchronizes with the bank's iFolder, and the bank representative gets the updated document that can be printed or processed further.

6 Single-Server Cluster Deployment

Cluster-enabling the Novell iFolder service enables the iFolder server to be highly available at any time. If your organization is deploying only one iFolder server for the iFolder service, you should enable a server cluster. This scenario is illustrated in the following figure.

Figure 6-1 *Single-Server Cluster*



Open Enterprise Server (OES) 11 provides iFolder service migration scripts that are based on Novell Cluster Services, for automatic service migration from one node to another (failover) and for re-migration to the actual node when the node recovers from failure (failback).

This configuration ensures that the iFolder service is always available during unforeseen node failures in a cluster environment.

The following sections describe a single-server cluster deployment.

6.1 Planning

6.1.1 iFolder Configuration

In the Web Admin console, ensure that all volumes that are enabled for iFolder are present in the shared storage used by the Cluster node. For more information on creating and configuring additional volumes for iFolder, see “Manage the Data store.” in the *Novell iFolder 3.9.2 Administration Guide*.

6.2 Key Benefits

The key benefits of a single-server cluster setup are as follows:

- This type of setup is beneficial to organizations that require high data availability.
- The number of hits per second to the iFolder server through a browser and thick client is based on the server processing capability and the network link.
- The Novell iFolder server does not limit the number of hits, because it runs behind Apache and Apache governs the processing capability.

6.3 LDAP Configuration

The LDAP configuration information for a single cluster setup is as follows:

- iFolder supports the eDirectory, OpenLDAP, and Active Directory directory servers.
- iFolder supports both secure and non-secure communication with directory server. You can choose any communication channel that you need. Ensure that the directory server is listening on standard LDAP ports for secure and non-secure channels.
- Ensure that each iFolder node has its own eDirectory replicas so that the authentication is done locally instead of walking the eDirectory tree.

6.4 Scalability Parameters

The scalability parameters for a single cluster setup are as follows:

- Clients must have a dedicated network interface card (NIC) of 100 Mbps capacity.
- Web-based access must be low and thick client access must be moderate with 500 active connections.
- The data transfer (synchronization of user data) rate must be 10 MB per hour per client.
- The synchronization interval must be 10 minutes.

6.5 Deployment Scenarios

6.5.1 Document Collaboration

A BPO (Business Process Outsourcing) organization that specializes in product documentation needs a solution for storing the documents in a common repository in which multiple users have their own document sets to be updated.

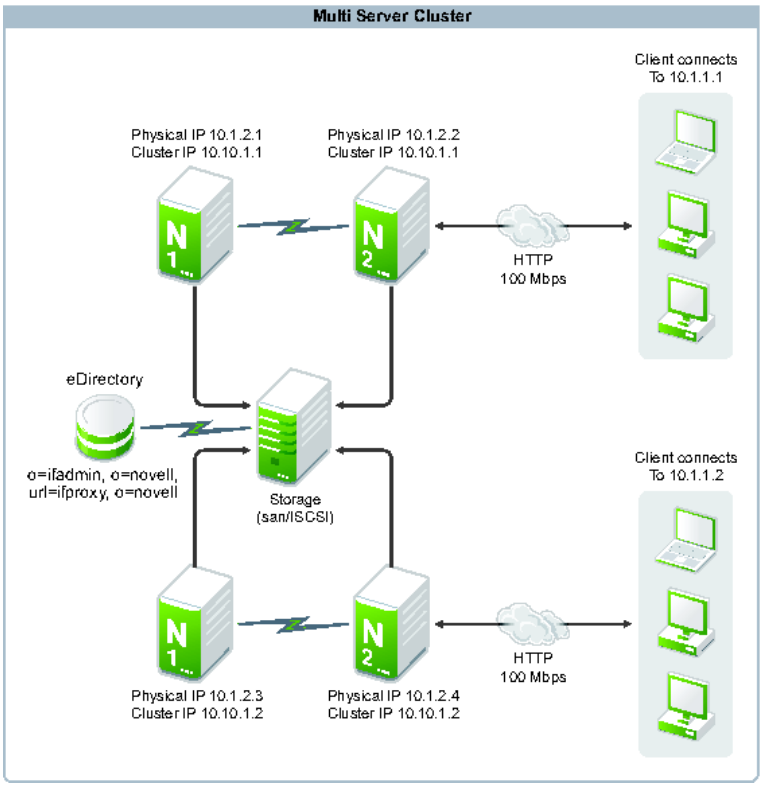
In this scenario, the server must always be online and the file service must be available at all times. Novell iFolder provides an excellent solution for the user to work on the local copy and to update the central iFolder server with the latest document copy at regular intervals. Because updating the document is delta-based, very little data is transferred across the wire.

A single-server cluster enables users to have their documents in sync with others and also ensures that the latest version of a document is available on the server. This protects user data from an unanticipated crash of the local system. The organization consumes less bandwidth by uploading only deltas and ensuring that users work only on a local copy. A single-server cluster with iFolder enables the organization to be continuously productive and provides a very good document collaboration environment.

7 Multi-Server Master-Slave Deployment in a Cluster

In a multi-server cluster scenario, the setup consists of multiple servers with up to 1000 simultaneous connections at a time. The iFolder server and the database are located on a single Open Enterprise Server (OES) 11 server with client workstations connected to it.

Figure 7-1 *Multi-Server Cluster*



In a multi-server setup, one master and multiple slaves participate in a single iFolder domain. Thousands of users communicate with the domain and each server services a different set of users. Multiple servers are involved for users who share iFolders across the organization.

Cluster-enabling a multi-server setup involves multiple iFolder servers in different clusters so that the master and slave do not end up in the same node during failover/failback operations. If a single cluster is used for multi-server iFolder service, then during iFolder configuration, you must ensure that each slave resource uses a mutually exclusive set of cluster nodes to perform failover or failback, in order to avoid any collisions with either the master server or other slave servers.

The following sections describe the multi-server cluster setup.

7.1 Configuration

7.1.1 iFolder Configuration

When you configure the master or slave stores, ensure that the file system resources are online on the respective iFolder server nodes and are mutually exclusive.

7.1.2 Web Admin Server Configuration

The Web Admin server can be part of the master server resource and does not need to be a separate cluster node.

7.1.3 Web Access Server Configuration

Ensure that multiple Web Access servers are configured in a multi-server environment. For every three iFolder servers, you must configure a Web Access server.

7.2 Key Benefits

The key benefits of a multi-server cluster setup are as follows:

- This type of setup is beneficial to organizations in which users or storage requirements change frequently.
- This setup is useful to organizations that require high data availability. Every iFolder server must be cluster-enabled for high data availability. However, Web Admin and Web Access do not need to be cluster-enabled.

7.3 LDAP Configuration

The LDAP configuration information for a multi-server cluster setup is as follows:

- iFolder supports the eDirectory, OpenLDAP, and Active Directory directory servers.

- While configuring the iFolder server, use the *LDAP Search Context* option in YaST to ensure that the master LDAP search group you specify is the superset of all the slaves. You can specify all the slave search contexts, separated by commas. For example, o=org is the master LDAP search group, and ou=KAR and ou=DL are the slave LDAP search groups. In this case, the slave LDAP search groups should be the subset of the master LDAP search group. You can either specify o=org as the LDAP search context or specify ou=KAR, ou=DL. In the latter case, slaves have a specific search context or group containing users who can exclusively access the slave server and store the data.
- Ensure that each iFolder server has its own eDirectory replicas so that the authentication happens locally instead of walking the eDirectory tree.
- iFolder supports both secure and non-secure communication with the directory server. You can choose any communication channel that you need. Ensure that the directory server is listening on standard LDAP ports for secure and non-secure channels.

7.4 Scalability Parameters

The scalability parameters for a multi-server cluster deployment are as follows:

- Scalable to 1000 simultaneous connections per master.

  If a slave is included, see Section 3.3, “Scalability Parameters,” on page 19 in Chapter 3, “Multi-Server (Master-Slave) Deployment,” on page 17
- Over a million users can be provisioned in each master.
- Each master server can store up to a terabyte of data.
- The synchronization interval must be 5 minutes.

7.5 Deployment Scenarios

A multi-sever setup in a cluster environment is beneficial where high availability is needed and high volatility is expected. The following deployment cases discuss how a multi-server (master-slave) setup can be used for load balancing and data synchronization in an organization where requirements are expected to increase for employee count, frequency of access, and high availability.

- Section 7.5.1, “Business Services with High Volatility,” on page 35

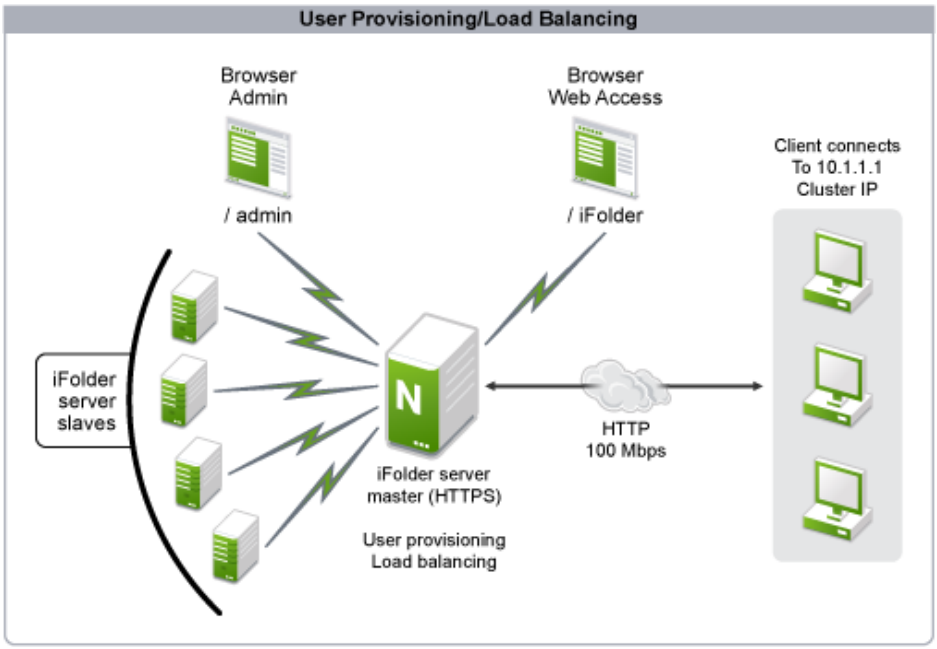
7.5.1 Business Services with High Volatility

Consider a stock brokerage firm that has 10000 users and 100 relationship managers. The firm's primary requirement is to have immediate data availability with a good response time. Over a period of time, the number of users in the firm might increase. Under the current setup, the storage can be increased dynamically, but the response time will continuously decline. With an iFolder cluster, the physical server upgrade can be less painful with no downtime. Also, if the business grows at a particular location and declines at another location, users can be migrated to another iFolder server and the servers can be consolidated.

8 Using an iFolder Master Server as a Load Balancer

Organizations that need to distribute an equal number of users across iFolder servers need user load balancing support. User load balancing ensures an equal amount of connections per server and balanced data transfer across servers.

Figure 8-1 *Load Balancer*



Organizations that need automatic user management should provision the users soon after iFolder server deployment. This is necessary in large organizations where user management is difficult and provisioning existing users requires considerable administrative overhead. With the load balancing option, the users are provisioned to the server that has fewer users provisioned so that the number of users across the deployed iFolder servers is equalized.

This configuration ensures that the response time for every user is good and the number of connections per server is not excessive. If some super users have large data sets, this setup does not guarantee data load-balancing, but only guarantees user count balancing across available servers.

The following sections describe the deployment of an iFolder master server as a load balancer.

8.1 Key Benefits

The users are equally distributed across servers. This ensures that the load on servers is approximately the same.

8.2 LDAP Configuration

The LDAP configuration information for deploying an iFolder master server as a load balancer is as follows:

- eDirectory, OpenLDAP, and Active Directory directory servers are supported.
- While configuring the iFolder server, use the *LDAP Search Context* option in YaST to ensure that the master LDAP search group you specify is the superset of all the slaves. You can specify all the slave search contexts, separated by commas. For example, o=org is the master LDAP search group, and ou=KAR and ou=DL are the slave LDAP search groups. In this case, the slave LDAP search groups should be the subset of the master LDAP search group. You can either specify o=org as the LDAP search context or specify ou=KAR, ou=DL. In the latter case, slaves have a specific search context or group containing users who can exclusively access the slave server and store the data.
- Ensure that each iFolder server has its own eDirectory replicas so that the authentication happens locally instead of walking the eDirectory tree.
- iFolder supports both secure and non-secure communication with the directory server. You can choose any communication channel that you need. Ensure that the directory server is listening on standard LDAP ports for secure and non-secure channels.

8.3 Scalability Parameters

The scalability parameters for an iFolder master server as a load balancer are as follows:

- Every slave server is scalable to 1000 users.
- Both SSL and non-SSL communication is supported.
- The synchronization interval must be 5 minutes.
- The master server must have a relatively smaller load than a slave server.

8.4 Deployment Scenarios

- Section 8.4.1, “Information Management,” on page 39
- Section 8.4.2, “Load Balancing,” on page 39

8.4.1 Information Management

Consider an example of an organization that has about 100,000 employees in 10 different locations within a city and 10 different cities in a country. This organization wants to deploy Novell iFolder for information management (storing, retrieving, and sharing) across cities. You want to make sure that management overhead for the 100,000 users in this scenario does not become excessive.

In this case, the administrator can use iFolder to specify a group of users and servers for a city. iFolder automatically distributes the group of users to the servers specified for the city. In just 10 operations, 100,000 users can be provisioned and user-balanced according to their the cities. Now, the 100,000 users can create, store, retrieve, and share data among other peers and also create confidential iFolders that are encrypted. The group of users within a city must be specified so that a user is not accidentally provisioned to a server that is in a different city, which might cause more remote traffic and low response time.

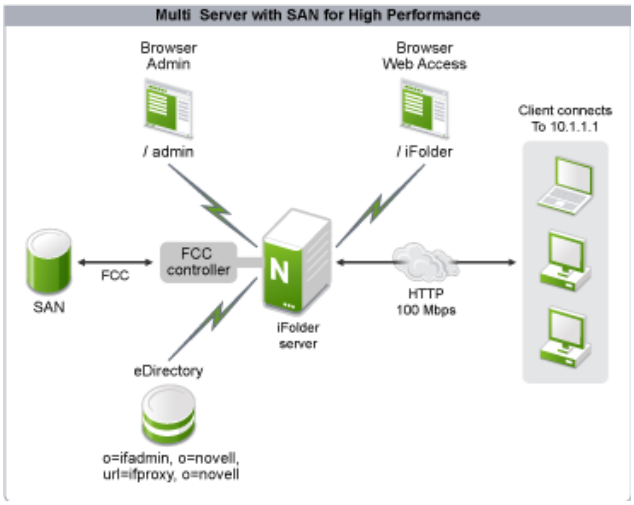
8.4.2 Load Balancing

Consider an organization with multiple branches operating in a city that has a network set up in such a way that the response time across any branch is constant. Given this case, Novell iFolder can be deployed with auto-user provisioning without specifying a particular user group. The iFolder server automatically load-balances the users across the servers. Because the response time across any branch is constant, the user can be provisioned to any of the servers in the branch and still get a constant response from the iFolder server.

9 Using Fibre Channel to Deploy iFolder in a Storage Area Network

Many organizations are providing round-the-clock operations and high-availability services to their users. Integration with Novell Cluster Services helps these organizations to deploy Novell iFolder behind cluster-enabled servers either through a Fibre Channel SAN (storage area network) or through iSCSI.

Figure 9-1 *Deployment using SAN and FC*



If a SAN can meet your organization requirements, you can use Fibre Channel to deploy iFolder in a SAN environment. This setup provides very good response (high performance low-latency data transfers) for data requests (I/O) for iFolder users. If your deployment needs heavy data transfer between users and the servers, you can also use the SAN with a Fibre Channel setup.

Organizations involved in multi-media invest in SANs for storage scalability and high- performance data transfer rates. Implementing Novell iFolder in this scenario enables users to transfer data to and from different users in a fast and reliable manner. Because iFolder performs a delta synchronization of data, the data transfer is minimized and performance is increased. The users do not need to use file system protocols (CIFS/AFP/NFS) to access or share files.

The following sections describe the deployment in SAN environment through Fibre Channel.

9.1 iFolder Configuration

Ensure that you configure the iFolder store in the SAN storage.

9.2 Web Admin and Web Access Server Configuration

Because the storage is SAN with Fibre Channel, data retrieval is faster and more requests can be processed. This in turn increases the CPU load factor as the number of data synchronization requests grow. For optimal performance, you should have separate Web Access and Web Admin servers.

9.3 Planning

To ensure that all servers are behind SAN and that cluster failover/failback is implemented, you must deploy 2*n* servers, where *n* is the number of iFolder servers the organization is planning to deploy in a multi-server environment. In this case, all the servers share the same storage array, with different partitions enabling the cluster to be effective. This means that every iFolder server has a backup node to support failover and failback and to provide high availability.

If hardware is a constraint, Apache virtual hosts can be leveraged, so that during a failover, the slave runs along with another slave in virtual host mode behind Apache. The only drawback is performance, because the Apache server must service twice the server load and number of user requests, which is not recommended unless the deployment has comparatively few user requests.

9.4 Key Benefits

The key benefits of deploying the iFolder server in Fibre Channel or iSCSI are as follows:

- This type of setup is beneficial in organizations that require high data availability and faster response time.
- The number of hits per second to the iFolder server through a browser and thick client is based on the server processing capability and the network link. A Novell iFolder server does not limit the number of hits because it runs behind Apache.
- A smaller backup window enables high data availability to the clients.

9.5 Scalability Parameters

The scalability parameters for deploying the iFolder server in fibre channel or iSCSI are as follows:

- The server is scalable to 1000 users.
- Data storage can scale to several terabytes of data.
- The data transfer (synchronization of user data) rate can be 50 MB per hour per client.

9.6 Deployment Scenarios

This section covers the following:

- Section 9.6.1, “Case 1,” on page 43
- Section 9.6.2, “Case 2,” on page 43

9.6.1 Case 1

An ISP has a portal providing users with disk space to store their data at a central location for continuous access. The users pay for the service, so they expect the ISP to provide round-the-clock service, because the users across the globe expect access to their data anytime. The ISP can deploy this iFolder solution to ensure high availability and for faster access. The ISP must deploy the setup behind a Fibre Channel SAN with 1:1 server node backup for each iFolder server. This enables the setup to perform a faster failover if a particular node is going down for maintenance or for some other reason.

High performance is delivered by using Fibre Channel and the failover is not noticeable. Also, because the data store is faster, the simultaneous user data transfer is high compared to other deployments because the main usage of this setup is to store and share data.

9.6.2 Case 2

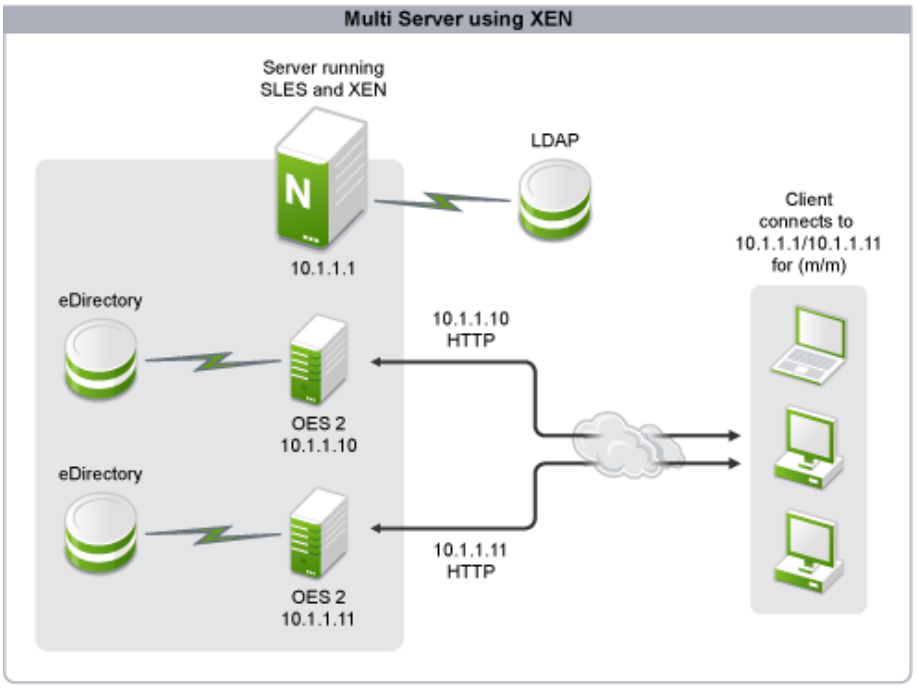
Backup of user data is a major task for administrators, especially for organizations that work around the clock, because the administrators do not get a window of time for backing up user data. iFolder deployment provides an almost real-time backup solution, where the user data is backed up and the delta is synchronized with a latency of five minutes. At any given point, if a failure occurs, the user data is available with a risk of losing only the last five minutes of data.

Using this deployment, you can formulate a backup strategy where the administrator doesn't need to find time to perform a backup, and can recover data in real time. This deployment employs Novell Cluster Services and a high speed SAN with a Fibre Channel controller to provide good response time for the data that is synchronized.

10 Using Xen to Deploy iFolder as a Virtual Service

Hardware consolidation and virtualization is implemented in most organizations to reduce operational costs, and Xen plays an important role in virtualizing multiple servers on a high-capacity physical server. Virtualized servers provide the same services as a physical server and their operation is very transparent to the end user. You must configure the Novell iFolder service on a virtual server for deployment in virtualized environments.

Figure 10-1 *Multi-Server Using Xen*



The following sections describe using Xen to deploy iFolder as a virtual service.

- Section 10.1, “Key Benefits,” on page 46
- Section 10.2, “LDAP Configuration,” on page 46
- Section 10.3, “Deployment Scenarios,” on page 47

10.1 Key Benefits

The key benefits of deploying iFolder as a virtual service are as follows:

- With Novell iFolder configured on a virtual server either in single-server mode or multi-server mode, the capability and capacity of the iFolder server remains the same. Using Xen or any other virtualized environment, each virtual host can be used as an iFolder server consuming a common storage, yet providing load balancing between the hosts. If each host can afford a dedicated network resource, the performance of the host increases because Novell iFolder is dependent on wired communication for most of its operations.
- A virtualized environment helps in reducing the number of physical resources and helps improve management. When the iFolder servers are deployed in a virtual environment, you can handle multiple Web Administration consoles with ease and with lower maintenance overhead. Users transparently get the performance and scalability expected from the physical servers.
- Novell iFolder deployment in a virtual environment ensures that multiple services run on a single physical resource with a dedicated virtual guest server for each service. Given this, an iFolder multi-server setup can run on a single physical server with multiple virtual hosts. The entire multi-server setup can run on a single physical resource. This reduces cost and time to deploy.
- If each virtual guest is treated as a single server, see Chapter 2, “Single-Server Deployment,” on page 13. If a multi-server setup is used for the virtual guests, see Chapter 3, “Multi-Server (Master-Slave) Deployment,” on page 17 and Chapter 4, “Multi-Server (Master-Master) Deployment,” on page 21. If a cluster is set up on the virtual guest, see Chapter 6, “Single-Server Cluster Deployment,” on page 29.

10.2 LDAP Configuration

The LDAP configuration information for using Xen to deploy iFolder as a virtual service is as follows:

- eDirectory, OpenLDAP, and Active Directory directory servers are supported.
- While configuring the iFolder server, use the *LDAP Search Context* option in YaST to ensure that the master LDAP search group you specify is the superset of all the slaves. You can specify all the slave search contexts, separated by commas. For example, o=org is the master LDAP search group, and ou=KAR and ou=DL are the slave LDAP search groups. In this case, the slave LDAP search groups should be the subset of the master LDAP search group. You can either specify o=org as the LDAP search context or specify ou=KAR, ou=DL. In the latter case, slaves have a specific search context or group containing users who can exclusively access the slave server and store the data.
- Ensure that each iFolder server has its own eDirectory replicas so that the authentication happens locally instead of walking the eDirectory tree.
- iFolder supports both secure and non-secure communication with the directory server. You can choose any communication channel that you need. Ensure that the directory server is listening on standard LDAP ports for secure and non-secure channels.

10.3 Deployment Scenarios

Consider the example of an organizational unit that has several smaller subgroups, with each subgroup having different data storage and collaboration requirements. For example, one subgroup has 100 users, and they all collaborate with each other every day. The storage requirement of this subgroup is low because they collaborate regularly with each other.

In contrast, consider another subgroup with 200 users who are involved in financial transactions that require their data to be maintained in a secure manner. The storage requirement of this subgroup might be high, but the users in the group might not need to collaborate with each other.

Although both the subgroups are part of the same organization and work in the same geography, their iFolder policy needs are different. From the administrative perspective, it is simpler if a master-slave iFolder server is deployed and the employee count is low. For this deployment scenario, the iFolder services can be deployed over Xen to maximize the underlying hardware.

11 NAT-Based Configuration

Organizations utilize Network Address Translation (NAT) to secure server access and identity. This helps users access all services through a single public IP address.

11.1 Planning

This type of setup benefits organizations that do not want to expose the Open Enterprise Server (OES) 11 servers to the external network, so they have a common router that routes the information to the servers. The router ensures that the servers are not exposed to the external network and that they are safeguarded from attacks. A single public IP address can be used for all the services that are provided through multiple physical servers.

11.2 Key Benefits

The key benefits of deploying a NAT-based configuration are as follows:

- It saves IP addresses by having one IP address represent a group of computers.
- The iFolder server is safeguarded because the users are inside the NAT network.
- If a Web Access server is needed, it can be configured outside the NAT network for external users.

11.3 Scalability Parameters

Even though this provides an additional layer of access control and security, it does not affect the scalability of the application. Depending upon the type of setup you deploy, refer to the scalability parameters section in the respective chapters. For example, if you deploy a single-server setup, see Section 2.3, “Scalability Parameters,” on page 14.

11.4 Deployment Scenarios

Consider the example of a small organization that needs to set up multiple iFolder servers for data sharing and backup, and it has a limited number of IP addresses that are available for public use. The organization is not planning to expose all the iFolder servers to the external network even though firewall and traffic filters like ZoneAlarm* can be deployed. Also, the organization is not ready to bear the additional costs of deploying firewall and traffic filtering software.

The routers available in the market come with built-in traffic filtering and maintain a database of known attacks. This helps the organizations track and avoid security threats and attacks.

To configure an iFolder server with NAT, you must ensure that the users can access the iFolder server via the router even though the server has a NAT address. This also means that the Web Access and the Web Admin console must be able to work outside the NAT network, because the users might sometimes be in a public domain and might need access to their iFolder data. The Novell iFolder server's public URL must be set to the router's DNS address, so that Web Access, Web Admin, and the clients can access the iFolder server inside the NAT network from the external network.

12 Using Router Port Forwarding and Mod Proxy

Your organization does not always need to expose the iFolder data servers to the Internet in order to enable users to access information through the firewall. Instead, you can use a port forwarding mechanism and mod proxy as a means to handle requests from external users without directly exposing the iFolder data servers.

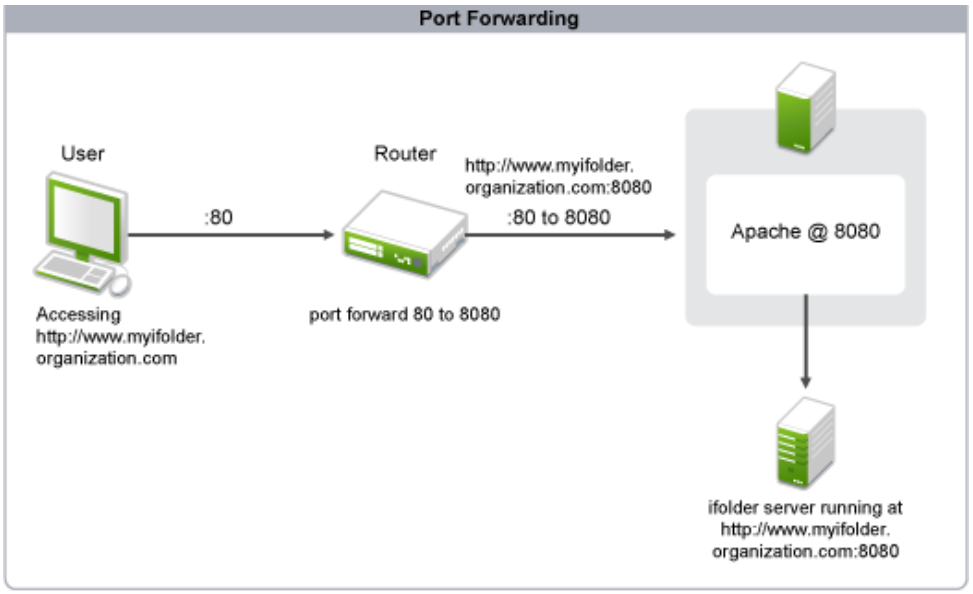
12.1 Port Forwarding

An Apache Web server by default uses port 80 for non-secure connections and port 443 for secure connections. You are not required to use these ports, but certain applications might need them for connections. In this scenario, you can use the port forwarding mechanism.

The port forwarding ability is provided by the router that handles an organization’s incoming connections. For instance, a router can be configured to route all information in port 80443 to port 443 internally, which enables users to use port 80443 for iFolder service. This helps you segregate the information coming to ports 443 and 80443 so that application-based statistics can be developed.

The figure given below illustrates how the port forwarding mechanism can be used to forward requests from a restricted port (port 80) to an unrestricted port (8080).

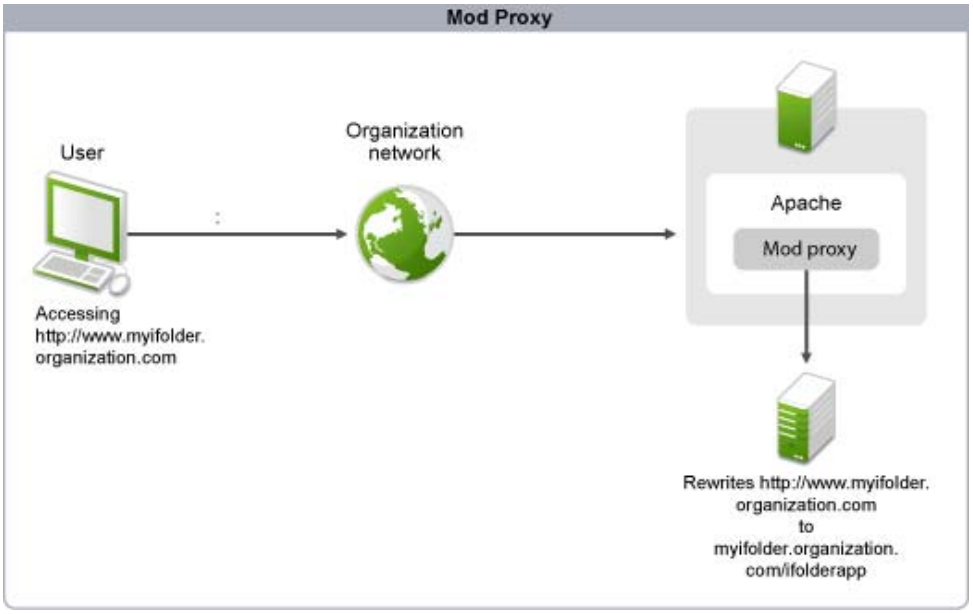
Figure 12-1 *Port Forwarding*



12.2 Mod Proxy

Mod proxy is a module used by the Apache server to implement proxying capabilities. It handles all the queries directed to it and forwards only the services that are configured to use iFolder. Mod proxy can be used when an iFolder server is maintained internal to an organization as an application server and is not exposed to the external network. The figure given below illustrates how mod proxy can act as a gateway to the requests directed from the external network by obtaining the required information from the internal iFolder application server.

Figure 12-2 *Mod Proxy*

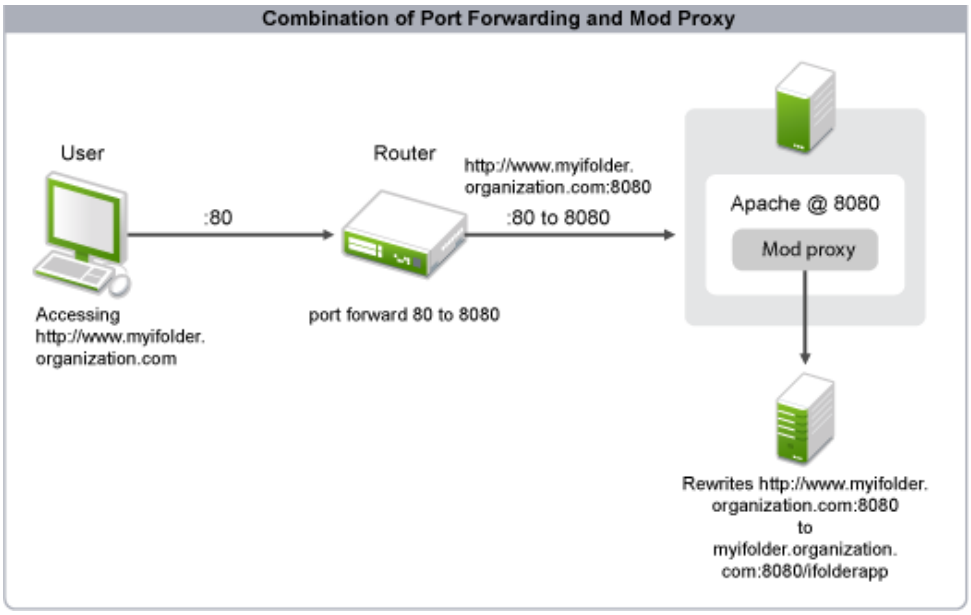


12.3 Port Forwarding and Mod Proxy

Consider an example where myifolder.organization.com/ifolderapp is an internal ifolder application server and external users need to access this server using the URL www.myifolder.organization.com. In this scenario, mod proxy can enable the external users to access the internal iFolder application server by rewriting the external URL < a href = http://myifolder.organization.com/ifolderapp> foobar to < a href = http://www.myifolder.organization.com"> foobar . This enables external users to access the internal iFolder application server without directly exposing the server.

The following figure illustrates how the port forwarding mechanism can be used in conjunction with mod proxy to handle requests from external users.

Figure 12-3 *Port Forwarding and Mod Proxy*



The following sections describe port forwarding and mod proxy.

12.4 Key Benefits

One of the key benefits of port forwarding is that it can also be used within a single machine. Port forwarding is necessary for a standalone computer if any of the following conditions are true:

- The computer is using a shared IP address.
- The Windows Internet Connection Sharing option is enabled and a NAT-enabled router is being used.

12.5 Scalability Parameters

Even though this provides an additional layer of access control and security, it does not affect the scalability of the application. Depending upon the type of setup you deploy, refer to the scalability parameters section in the respective chapters. For example, if you deploy a single server setup, see Section 2.3, "Scalability Parameters," on page 14

12.6 Deployment Scenarios

Consider the Acme organization, which provides several financial application services that are hosted via the Web. As part of a subscription, Acme also provides storage space for its customers to store their financial data reports in an encrypted iFolder.

Acme decides to maintain a consistent view of its Web applications, so that they are easier to manage. Therefore, Acme hosts all its Web applications under the `FINAPPS` directory. For instance, the insurance services are accessible via *https://acme.com/APPS/Insurance*, and the investments services are accessible via *https://acme.com/APPS/Investments*. However, these URLs expose the applications to potential hackers. Also, for additional security, Acme administrators do not want the HTTP default port to have direct access to the Web applications, so they need a proxy for the URL as well as a port forwarding solution.

This can be addressed by port forwarding and proxy addressing. Port forwarding for the Apache services can be performed by the router and the URL redirection can be done by Apache supported mod proxy. Mod proxy has multiple configurations. For more information on mod proxy, refer to the mod proxy configuration information at the Apache Module mod proxy Web site (http://httpd.apache.org/docs/2.0/mod/mod_proxy.html).

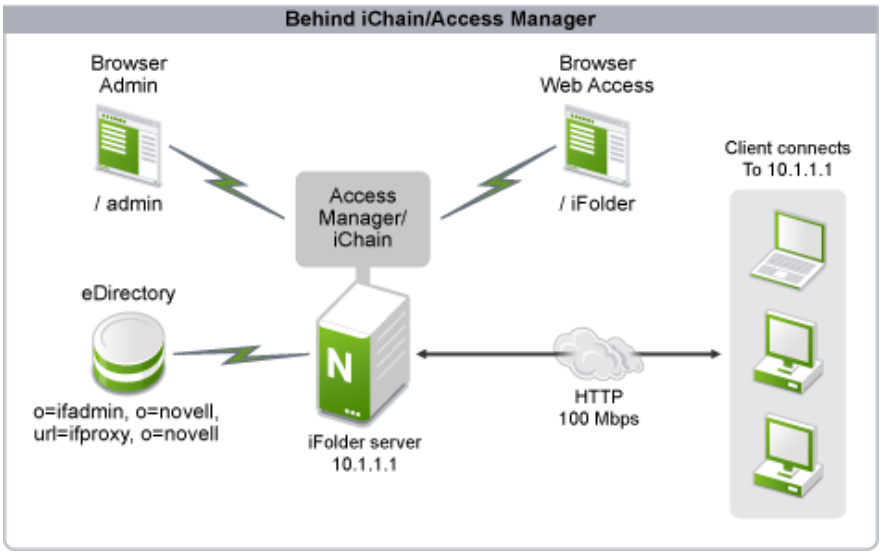
13 Deploying iFolder behind Access Manager or iChain

Novell iFolder provides secure access to the data via SSL. However, this channel uses the public network if the user accesses the data from a public Internet kiosk. Nevertheless, your business must be accessible to employees, customers, and partners, regardless of location or time of day. Novell Access Manager solves this challenge by helping you maximize access without limiting security or control. It integrates seamless security from Novell, which lowers risk and facilitates more agile customer and partner relationships. It simplifies and safeguards online asset-sharing, giving you a new way to control access to Web-based and traditional business applications. Trusted users gain secure authentication and access to portals, Web-based content, and enterprise applications. Also, IT administrators gain centralized policy-based management of authentication and access privileges for Web-based environments and enterprise applications.

Novell iFolder needs some additional configuration if Access Manager or iChain is used to secure the Web application access. Users logging in via Access Manager can use single sign-on so that password management is made simpler.

Because Access Manager interfaces with iFolder, iFolder needs to know certain configuration settings of Access manager to function efficiently. For more information, see Section 13.3, “Additional Configuration,” on page 56.

Figure 13-1 *Deployment Behind Access Manager iChain*



The following sections describe iFolder deployment behind Access Manager or iChain.

- Section 13.1, “Key Benefits,” on page 56
- Section 13.2, “Scalability Parameters,” on page 56

13.1 Key Benefits

The key benefits of iFolder deployment behind Access Manager are as follows:

- Access Manager creates a trusted and secure connection between the user and the iFolder application and iFolder employs an additional layer of security for mobile users to access their data.
- Novell iFolder can also be accessed via the SSL-VPN option of Access Manager for a trusted tunnel connection.
- This setup provides better access control and administration for the administrator to manage the security aspects of an organization.

13.2 Scalability Parameters

Even though this provides an additional layer of access control and security, it does not affect the scalability of the application. Instead, it provides more scalability because both Novell iFolder and Access Manager are highly scalable, providing a multiplier effect.

- This setup is ideal for small organizations of 500 to 1000 users.
- Clients must have a dedicated network interface card (NIC) of 100 Mbps capacity.
- Web-based access must be low and thick client access must be moderate, with 500 active connections.
- The data transfer (synchronization of user data) rate must be 10 MB per hour per client.
- The synchronization interval must be 10 minutes.

13.3 Additional Configuration

During the Web Admin and Web Access setup, the Access Manager or iChain logout URL must be specified for redirection. This helps iFolder ensure that the connection created by the user via Access Manager is cleared properly. This URL can be obtained from the Access Manager or iChain server configuration settings.

For more information on customizing the logout requests, see the "Customizing Logout Requests" section of the Access Manager Administrator guide.

13.4 Deployment Scenarios

Consider the case of a company that has 200 branches with 50000 employees and 100 business partners. All business partners are always on the move and at least 1000 employees are travelling at any given point of time. Every employee and business partner has an identity in the company eDirectory for access control of their respective applications and data. The company uses iFolder to enable users to access their data at any time and anywhere.

Because the company has business partners and some of the business partners might also be competitors, the business partners need more security while they store data in the company repository, but at the same time they need accessibility to data.

In this scenario, the company can install and configure iFolder behind Access Manager to provide stricter access control and security. Novell iFolder is configured to use Access Manager as an access method so that the employees and business partners can use single sign-on as well as a secure connection from the public Internet.

14 Deploying the My Documents Folder as an iFolder

This section helps you deploy Novell iFolder in a scenario where the user's `My Documents` folder is converted to an iFolder. By using the instructions given in this section, you can configure the server and client in different environments with different policy settings. These instructions are not limited to the given environments, so you can also use them for other scenarios.

14.1 Environments

14.1.1 Trusted

The server and the user machines are within the organization firewall. No user is expected to access the system outside the firewall through a Web browser.

14.1.2 Untrusted (User Network Alone)

The server is within the organization firewall. It has a protected public IP interface that the users outside the firewall can use to access the data by using a VPN client or other secure means.

14.1.3 Untrusted

The server is in the public domain, and the users can access the server data from anywhere, including Internet kiosks.

14.2 Server Configuration

14.2.1 General

For the environments discussed in Section 14.1, “Environments,” on page 59, the method to configure SSL options differs with iFolder versions. iFolder 3.6 does not support SSL communication, so you must use it only in a trusted environment. Novell iFolder 3.7 and later versions do support SSL.

Table 14-1 *SSL Recommendations*

Environment	SSL Support
Trusted	Disable SSL to increase performance.
	Deselect the *Configure SSL for iFolder* option in YaST.
Untrusted	Require SSL communication.
	Select the *Configure SSL for iFolder* option in YaST.

In addition to SSL, specifying the public URL is a must in an untrusted environment. Instead of an IP address, set the public URL to the DNS name of the server so that the client uses the DNS name to connect to the server. When the iFolder client uses the DNS name, even if the iFolder client has been moved out to a network outside the firewall, the client can still connect to the server. In this case, the server must be configured to receive the IP requests (both inside and outside the firewall) either directly or indirectly to send or receive through a configured gateway.

14.2.2 Single Server and Multi-Server

In a single-server configuration, 1000 users are serviced at a time, although there is no practical limit on the number of users provisioned to the server. The recommended load on a single server is 4000 provisioned users, with 1000 users serviced at a time. All 4000 users can be connected to the server but only 1000 users are active.

This scalability data is for a single dual-core processor with 4 GB RAM. If the server has more capacity, such as 4 processors with 16 GB RAM, the capacity can be scaled up based on the hardware.

A multi-server setup is best when there is a large number of users or when they are distributed across different locations. Multiple servers let you use load balancing for a large number of users, or if your users are distributed across many locations, you can provision them to the nearest iFolder server to get a better response time. This allows you to scale in an enterprise environment where there are many users who are located in different locations in the same geography and across geographies.

14.2.3 Novell iFolder Configuration

iFolder 3.6 must be used only in a trusted environment because there is no SSL support for it. iFolder 3.7 and later versions provide SSL support that can be disabled during configuration in a trusted environment. In this context, only the initial user login uses SSL to safeguard the credentials regardless of the server-side SSL configuration. See Section 14.2.4, “Novell Web Admin Configuration,” on page 61 for information about the Web Admin Console features that can be used for this deployment.

14.2.4 Novell Web Admin Configuration

The Web Administration console helps you create policies for the system as a whole or at every user/group level. For iFolder 3.7 and later versions, LDAP groups are supported.

Provisioning

For a single-server setup and a multi-server setup within the same location, automatic provisioning is recommended. For multiple locations, LDAP attribute-based provisioning is recommended. There is also a manual provision method in the Web Admin console that can be used to provision users to a specific server against the auto-provisioning algorithm. For more information, see "Provisioning / Reprovisioning Users and LDAP Groups for iFolder " in the *Novell iFolder 3.9.2 Administration Guide*.

Limiting iFolder Count to One

To limit the iFolder count, log in to the Web Admin console as an iFolder administrator. In the *System* page, enable the iFolder limit policy and set it to one. (This policy is available only in iFolder 3.7 and later versions). This ensures that only one iFolder is allowed per user, and in this case, the iFolder is the `My Documents` directory. For more information on policies, see "Viewing and Modifying iFolder System Information" in the *Novell iFolder 3.9.2 Administration Guide*.

Sharing iFolders

You can use the *System* page of the Web Admin console to manage iFolder sharing. By default, iFolder sharing is enabled. If you disable the option, the users cannot share their `My Documents` iFolder with other iFolder users.

File List Exclusion

The file exclusion list ensures that unwanted files are not synchronized to the server from the user copy of the iFolder. For example, you can add `.mp3` in order to disable users from uploading MP3-based music files. Similarly, video files can also be excluded from synchronization, because these files are usually large and consume more bandwidth and disk space.

Passphrase-Based Encryption

For iFolder version 3.6 and later, user passphrase-based encryption of iFolder is permitted. This encryption is independent of the SSL channel for communication. This encryption method ensures that the data is stored securely on the server side. In trusted environments, this might not be needed because this method of iFolder creation encrypts data on the fly and reduces the performance for data synchronization. Also, the data is not delta-synchronized in this mode, so passphrase-based encryption is not recommended for the `My Documents` iFolder in a trusted environment.

14.2.5 Web Access Configuration

The Web Access server must be installed on a dedicated server setup if the number of users expected to use the Web Access console for accessing iFolders is more than 10% of the total number of users.

For better performance in a trusted environment, the Web Access Server should not be configured to use SSL for both server communication and user communication.

In untrusted environments, the Web Access Server must be configured to use SSL for both server and user communication. This ensures greater security.

14.2.6 Converting the My Documents Folder to an iFolder

This setup ensures that every user's `My Documents` folder is marked as iFolder and this is the only iFolder for any given user. This is similar to the iFolder 2.*x* setup where only one iFolder is allowed per user.

In iFolder 3.7 and later versions, you can limit the number of iFolders per user by using the Web Admin console. This ensures that you have control over the number of iFolders and the amount of data that is transferred between the servers and the clients.

- **Administrator:** The administrator should limit the number of iFolders per user (including the `Default iFolder`) to one.
- **User:** Users can use their default iFolder as `My Documents` during account creation and then synchronize.

14.3 Key Benefits

The key benefits of deploying the `My Documents` folder as an iFolder are as follows:

- Having multiple computer configurations is more and more common every day. For instance, users might have one desktop at work, one desktop at home, and have a personal laptop. By converting the `My Documents` folder to an iFolder, it is easier to keep track of a given file.
- This type of deployment is beneficial when a user has different computers at different locations.
- By deploying this setup, you don’t need to create a default iFolder.

14.4 Scalability Parameters

The scalability parameters for deploying the `My Documents` folder as an iFolder are as follows:

- Ensure that the size of the iFolder does not grow beyond the limit specified by the administrator.
- You should avoid storing a large amount of data in an iFolder because data synchronization is evenly distributed among the iFolders on the workstation.