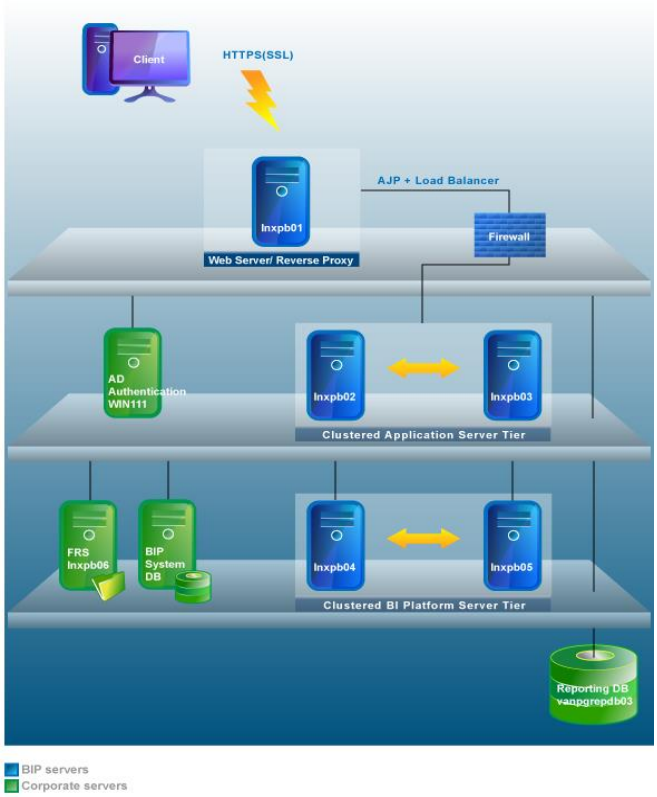
SAP BusinessObjects BI Pattern Books



Pattern Book on Deploying BusinessObjects BI Platform on Linux with Tomcat and Sybase ASE

ABSTRACT

In this pattern, we deploy SAP BusinessObjects BI platform on Linux. This pattern uses one web server, two application servers (Tomcat 7), and two BI platform installations (Red Hat). The CMS database is Sybase ASE and the authentication is Windows AD.

Disclaimer

- This pattern book is for informational purpose only and may not be copied / reproduced without the permission of SAP
- The information provided in this book are based on the SAP BI Pattern Books project for a specific set of patterns / use cases applied within SAP lab environment. Hence, make sure to review and apply the steps / workflows that are applicable to your use cases / patterns, based on your SAP BusinessObjects BI landscape
- Contents of this, or any related document and SAP's strategy and possible future developments, products and or platforms directions and functionality that are discussed in this book all subject to change and may be changed by SAP at any time for any reason without notice. Therefore, read the latest official product guides, release notes to understand the differences and act accordingly

For further comments and questions, email to **SAPEnableBI@sap.com**

Contents

Linux System Landscape Overview 4

Linux Pattern Overview 7

Linux Pattern Prerequisites 8

Linux Pattern Database Overview 10

CMS Database (Linux) 10

Auditing Database (Linux) 13

Linux Pattern Reporting Database 16

File Sharing 16

NFS Configuration 17

Samba Configuration 24

Sybase Middleware 24

BusinessObjects Cluster 30

Setting up BI platform server 1 30

Setting up BI platform server 2 42

Changing the Linux Pattern Cluster Name 56

File Repository Server 57

Application Server 63

Setting up Linux Pattern Application Server 1 63

Setting up Linux Pattern Application Server 2 68

Installing the BIP web tier 72

Configuring the Linux Pattern Application Server cluster 82

Apache 86

Installing Apache with SSL support 86

Configuring the mod_jk connector 93

Configuring Apache using the mod_ssl module 96

Configuring the load balancer 101

Authentication Server 104

Setting up the Active Directory server 104

Setting up the LDAP connector 115

Testing the LDAP authentication 125

Kerberos overview 127
Kerberos and SSO 129
Troubleshooting the Linux Pattern 130
File Sharing Troubleshooting 130
BusinessObjects Cluster Troubleshooting 131
Application Server Troubleshooting 133
Apache Troubleshooting 137
Reference and System Specifications for the Linux Pattern 141
Linux Pattern Acceptance Tests 143
BI launch pad cases 143
Central Management Console cases 144
Web Intelligence cases 145

This pattern is a simple yet real-world example of deploying SAP BusinessObjects BI platform in a company's existing infrastructure. It is robust, scalable, and secure enough to handle a moderate number of user requests.

In our examples, all BI platform machines are running Red Hat Linux version 6.2 with all required patches. This pattern book is also applicable to SUSE.

We will use a number of machines in this pattern and examine the procedures required to set up the Linux pattern in detail from start to finish.

For an overview of the machines in this pattern, see Linux System Landscape Overview.

To follow the pattern, complete the tasks in the order shown in Linux Pattern Overview.

This pattern is for SAP BusinessObjects 4.0 Linux. For previous pattern books, see the following list:

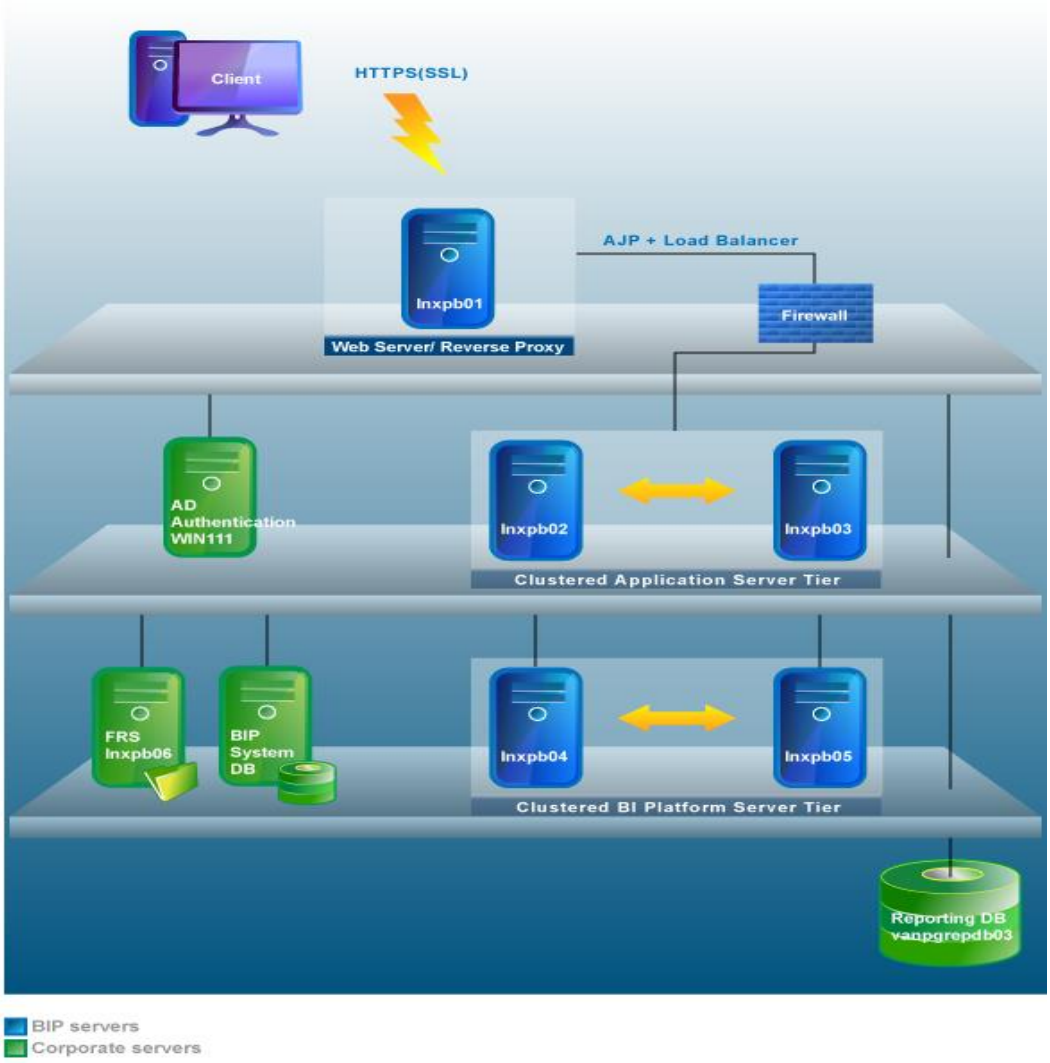
- XI 3.1 Windows
- XI R2 for AIX
- XI R2 for Red Hat
- XI R2 Windows

Linux System Landscape Overview

You use a number of machines in this pattern. The purpose of each machine is described in detail below.

Warning: Do not follow the pattern in the order shown below, as this overview of the system landscape describes the role of each machine in this pattern; it does not describe the order to follow. To follow the pattern, complete the tasks in the order as shown in **BIP on Windows with Mobile and Explorer** pattern book under **Pattern Overview** topic.

The following diagram shows the machines in this pattern and how they connect with one another:



External machine (lnxpb01)

The external machine hosting the web server, reverse proxy server, and load balancer is typically outside the company's external firewall. Customers can access BI platform web applications, such as BI launch pad and the Central Management Console (CMC), from the client machine.

We chose Apache because it is the most commonly used web server on the internet, hosting over 60% of all websites.

Apache 2.2 is the current mainstream release and is the latest supported version of Reverse Proxy Server in BI 4.0 Feature Pack 3.

See Apache for setup details.

Application servers (lnxpb02 and lnxpb03)

The application servers host BI platform web applications, such as BI launch pad and the CMC. For production systems, you should deploy at least two web application servers to handle failover and load balancing.

For this pattern, we chose Tomcat 7.0 for the application server rather than Tomcat 6.0, which is included in the BI platform installation program. Although Tomcat 6.0 is acceptable for production deployments on Linux, we want to show how to deploy BI platform web applications to the company's own application server.

See Application Server for setup details.

Authentication server (WIN111)

All users are authenticated before they can access BI platform. Typically, a company integrates BI platform with its own authentication system such as LDAP or Windows AD. Although BI platform includes its own authentication system by Enterprise authentication, it is not typically used in production deployments because it is less secure than third-party authentication systems.

For this pattern, we chose AD authentication although other third-party systems could also be used.

See Authentication Server for setup details.

Clustered BI platform servers (lnxpb04 and lnxpb05)

BI platform servers handle requests from the application servers, retrieve data from the corporate and system databases, generate BI content, and return the content to the application servers.

This pattern uses a two-machine cluster, in which each machine (lnxpb04 and lnxpb05) hosts all of the BI platform servers. This configuration provides redundancy and some scalability. BI platform web applications detect both BI platform server machines (specifically, they detect all CMS servers in a cluster), and automatically load balance their requests. If one machine fails, the web applications automatically send all requests to the other machine.

For production systems, you should deploy at least two BI platform server machines. If you need to increase scalability, you can deploy more BI platform server machines and deploy only one or two BI platform servers per machine.

See BusinessObjects Cluster for setup details.

File repository server (lnxpb06)

The file repository server (FRS) contains all of the reports and other BI documents that have been created. When a user creates a BI document, the BI platform servers retrieve the data from the company database (Reporting DB), generate the document, and store it in the file repository server. In production environments, you should host the FRS on its own machine because the number of BI documents can grow to a large number.

Because BI documents often contain sensitive information, you should host the FRS on a secure machine. Typically the BI platform administrator does not have access to this machine.

See File Sharing and File Repository Server for setup details.

BI platform system database

BI platform uses a database for its system data, which is called the system database or CMS database. For example, when a user wants to see a report, the CMS checks the system database to find the location of the report. For production systems, you can host the CMS database either on the database included with BI platform or on the company's existing database. Both are recommended for production systems, but companies often use their own databases in order to simplify administration.

We chose to use Sybase ASE because it is a commonly used database in Linux deployments.

See CMS Database (Linux) for setup details.

Reporting database

The reporting database hosts the company’s data. When a user wants to report from, analyze, or view company data, the BI platform servers retrieve data from the company’s database, perform the analysis and formatting, and either serve the result directly to the application layer or store it in the FRS.

See Reporting Database (Linux) for setup details.

Linux Pattern Overview

To deploy this pattern, perform the following workflow steps in the order listed:

To set up ...	Objective
Linux Pattern Prerequisites	A checklist of items to consider before deploying this pattern.
File Sharing	Configure access to a shared file repository location. Instructions for setting up NFS and Samba are provided.
Sybase Middleware	Install and configure the Sybase Client.
BusinessObjects Cluster	Install the BI platform servers on two machines and then cluster them together.
Application Server	Install Tomcat on two machines and then cluster them together.
Apache	Install Apache, configure the modules and load balancer, and purchase a security certificate.
File Repository Server	Set up the file repository server with either Network File System or Samba.
Authentication Server	Set up authentication system with LDAP.

Linux Pattern Prerequisites

Deploying this pattern involves many different systems and dependencies. Below are some of the key elements that will contribute to a successful deployment of this pattern.

Pattern Prerequisite Checklist

Before starting the pattern, ensure you have the following:

Intermediate knowledge of Linux and third-party software used	✔
Installation media downloaded/available	✔
License keys for all software used	✔
Ensured OS compatibility with all software	✔
Operating System Update Utility preconfigured (yum/yast/zypper)	✔
Network access and Internet/Proxy configured	✔
Root/Admin access on machines or System Administrator available	✔
Database access for System (CMS/Auditing) and Reporting databases	✔

Intermediate knowledge of Linux and third-party software used

The pattern lists all of the steps that we used to complete the pattern but does not go into great detail about every command and what it does. We have done our best to document the purpose of each command that we use, but an intermediate to advanced knowledge of the Operating System (OS) and third-party software would be a great asset to the success of your deployment.

Installation media downloaded/available

We do not cover the steps to obtain all the software used in this pattern. You will need to obtain the software from the vendor and make it available somewhere that is accessible within your pattern environment.

License keys for all software used

The license keys used within the pattern are dummy keys and should not be used in your deployment. To avoid delays, obtain the license keys for your software ahead of time.

Ensured OS compatibility with all software

You will want to check the product documentation for the software versions that you are using in your pattern to ensure that they are compatible with the Operating System that you have chosen. In our pattern, we have listed (in most cases) the exact version that we used and ensured compatibility ahead of time. If you use slightly different versions in your environment, be sure to check the product documentation ahead of time.

For more information, see our Product Availability Matrix.

Operating System Update Utility preconfigured (yum/yast/zypper)

It is assumed that your machines have been preconfigured to install updates. The pattern requires a few packages to be verified or installed in certain sections. Verify that you have setup the OS update repositories ahead of time to avoid delays.

Network access and Internet/Proxy configured

The machines will need to be networked and internet access may be required in certain workflows. Ensure all machines in the configuration can access each other and that they can access the internet, if need be.

Root/Admin access on machines or System Administrator available

A number of steps require root access. Depending on your organization, you will either require root access yourself or access to a System Administrator that can carry out the root tasks for you.

Database access for System (CMS/Auditing) and Reporting databases

Depending on your organization, you may need to request access to the database servers that you plan on using in the pattern. For details, see Databases Overview (Linux).

Linux Pattern Database Overview

The following sections examine in detail each database you need in this pattern:

Database	Description
CMS Database (Linux)	Set up the BI platform repository for user, server, folder, document, configuration, and authentication details
Auditing Database (Linux)	Set up the BI platform repository for audit information
Reporting Database (Linux)	Set up and configure databases for reporting

CMS Database (Linux)

The CMS system database is used to store BI platform information, such as user, server, folder, document, configuration, and authentication details. It is maintained by the Central Management Server (CMS), and is sometimes referred to as the system database or repository.

During installation of BI platform you are asked to which database you want to connect. Once you select a database, the setup program creates the tables and views necessary to utilize the database as the system database. During the installation, the default servers, users, groups, and content are added to this database.

For the Linux pattern, a Sybase ASE 15.7 database client and server was used. Before deploying our pattern we requested that a database user and schema be created for our CMS database. The database users will require reading and writing rights, as well as table creation rights on the schema. This pattern reviews the Sybase client configuration in Sybase Middleware.

The CMS database is a central and critical component of the Business Intelligence platform architecture. A single database server is used in the Linux pattern to host the CMS database, but in a production environment, redundancy and appropriate database recovery policies are necessary.

For more information on the CMS database and other servers within the BI platform, see the BIP 4.0 Administrators Guide.

Warning: Each BI platform environment requires a unique set of users/schemas. If you use an existing schema, the data is overwritten and your existing system is lost.

Below is an example of how you could name your user accounts/schemas. The user name and schema are often the same.

Stage of Deployment	CMS User/Schema Name	Audit User/Schema Name
Development	BI4CMSDEV	BI4AUDDEV
Production	BI4CMSPROD	BI4AUDPROD
Proof of concept (POC)	BI4CMSPOC	BI4AUDPOC
Quality Assurance	BI4CMSQA	BI4AUDQA

Details on the Sybase ASE 15.7 database used for the CMS database in our pattern

Two requirements for Sybase ASE are the following:

1. You must use a Unicode character set.
2. You must set a page size of 8 KB.

CMS Database Overview for our Linux pattern

Version	Sybase ASE 15.7

Database Name	Cms57u05
Character Encoding	UTF-8
Page Size	8KB
Server Name	Cms57u05
Machine	Cmsdb05
Schema	SAPCMS
Username	SAPCMS

For our database server we used the system parameters outlined below. These are not the official recommendations; you should consult with your Database Administrator before making any changes to your database servers.

Data Cache [buffer pool]: Make 250MB memory available

```
EXEC sp_configure 'max memory', 500000
go
EXEC sp_cacheconfig'default data cache', '200.000M'
go
```

Procedure Cache

```
EXEC sp_configure'procedure cache size', 27680
go
```

Lock Granularity

```
EXEC sp_configure 'lock scheme', 0, datarows
go
```

Parallel Processing: set number of engines = number of CPUs

```
EXEC sp_configure 'max online engines', 8
go
EXEC sp_configure 'number of engines at startup', 8
go
```

Number of Connections

```
EXEC sp_configure 'number of remote connections', 100
go
EXEC sp_configure 'number of remote logins', 100
go
EXEC sp_configure 'number of user connections', 100
go
```

Number of tablespaces

```
EXEC sp_configure 'number of devices', 25
go
```

Number of open objects, indexes, and partitions

```
EXEC sp_configure 'open objects', 2000
go
EXEC sp_configure 'open indexes', 4000
go
EXEC sp_configure 'open partitions', 3000
go
```

For more information on tuning your database server, refer to the vendor's documentation. Sybase ASE 15.7 Documentation includes the documentation we used when setting up this pattern.

Auditing Database (Linux)

The Central Management Server (CMS) collects audit information from the other BI platform servers and writes the details to the Auditing Data Store (ADS) or, as it is often called, the

Auditing database. This information enables System Administrators to better manage their BI platform environment and content usage through reporting and analysis of ADS data.

In this pattern, we use the same Sybase ASE 15.7 database server for our CMS and Auditing databases. There is a different user account and schema used specifically for auditing.

Details for the Sybase client configuration are covered in Sybase Middleware.

During the installation of your primary BI platform server you are asked for the connection information for your auditing database. For our pattern, we had our database administrator set up a CMS and Audit user account and schema before we installed the BI platform.

For more information on Auditing setup and configuration, refer to Chapter 20: Auditing in the BI Platform Administrator Guide.

The auditing database user account requires its own schema with create, modify, and delete table rights as well as rights to create stored procedures. The database also needs to be set up to use a Unicode character set such as UTF-8.

Checklist

Before installing the BI platform, ensure the following conditions are met:

The database client is installed and configured for the BI platform user account.	✔
The Auditing database user and schema have been created.	✔
The database is configured to use a Unicode character set (for example, UTF-8).	✔
The Auditing database user has create, modify, and delete rights for tables and stored procedures.	✔

Warning: Each BI platform environment requires a unique set of users/schemas. If you use an existing schema, the data is overwritten and your existing system is lost.

Below is an example of how we recommend you name your user accounts and schemas. The user name and schema are often the same.

Stage of Deployment	CMS User/Schema Name	Audit User/Schema Name
Proof of concept (POC)	BI4CMSPOC	BI4AUDPOC
Development	BI4CMSDEV	BI4AUDDEV

Stage of Deployment	CMS User/Schema Name	Audit User/Schema Name
Quality Assurance	BI4CMSQA	BI4AUDQA
Production	BI4CMSPROD	BI4AUDPROD

You are not asked for the schema name during installation. The installation uses the default specified for the user account.

It is always a good idea to test connecting to the database from the BI platform machine with your CMS and Auditing user account before starting your installation.

Details on the Sybase ASE 15.7 server used for our Auditing database in this pattern

Two requirements for Sybase ASE are the following:

1. You must use a Unicode character set.
2. You must set the page size to 8 KB.

Auditing Database Overview for our Linux pattern

Version	Sybase ASE 15.7
Database Name	Cms57u05
Character Encoding	UTF-8
Page Size	8KB
Server Name	Cms57u05
Machine	Cmsdb05
Schema	SAPAudit
Username	SAPAudit

For more information on tuning your database server, refer to the vendor's documentation. Sybase ASE 15.7 Documentation includes the documentation we used when setting up this pattern.

Linux Pattern Reporting Database

In most companies, there are many different databases that can be used for reporting. We refer to these databases as the Reporting databases.

To report off of these databases, you need to ensure that you have the connection information and a user account to that database that has at least reading rights to the data you want to use. This information is usually obtained from your Database Administrator.

In the Linux pattern described here, we use a Sybase ASE 15.7 Reporting database. This resides on a different server than our CMS and Auditing databases, and must be configured and tested separately.

Information: We generally recommend you not to host the CMS and Auditing databases on the same database server as your Reporting databases. This avoids competition for resources since the CMS and Auditing databases are critical to the health of your system.

Details on the Reporting database used in our Linux pattern

Reporting Database Overview for our Linux pattern

Version	Sybase ASE 15.7
Database Name	TPCU0067
Character Encoding	UTF-8
Page Size	8KB
Server Name	SybaseClient
Machine	Pgrepdb03
Username	Guest

For more information on tuning your reporting database server, refer to the vendor's documentation. Sybase ASE 15.7 Documentation includes the documentation we used when setting up this pattern.

File Sharing

Each clustered BI 4.0 server that hosts the Input / Output File Repository Server (FRS) requires access to a shared file repository location. Most customers utilize an existing storage area network (SAN) or network attached storage (NAS) location.

If you do not have an existing SAN / NAS location to use, you should use a network file system (NFS) or server message block, referred to as Samba, within your Linux pattern.

NFS is preferred in a *NIX-only environment, whereas Samba is a better choice if Windows file sharing is also a requirement.

Information: We recommend that you host your FRS on a separate server, as it may become a single point of failure when hosted on one of your BI 4.0 servers.

For example, if you use lnxpb04 as your NFS server as well as your FRS, and that machine experiences a hardware failure, thenlnxpb05 can no longer use the NFS server to access the files. In our example, we have set up an NFS server on lnxpb06, which is a completely different Linux machine.

We also recommend that your file server use some form of high availability or redundancy to ensure that there is no disruption or loss of data from a disk failure. We do not cover how to do this in this pattern.

The following sections provide more details for each type of configuration:

1. NFS Configuration
2. Samba Configuration

NFS Configuration

There are two parts to the NFS configuration:

1. NFS server configuration
2. NFS client configuration

Below are the steps we used for configuring the NFS Client/Server in our pattern. For more details on configuring NFS, refer to your operating system documentation:

- Red Hat Enterprise Linux 6 - Storage Administration Guide - NFS
- SUSE Linux Enterprise Server 11 SP2 Administration Guide - Chapter 27 - Sharing File Systems with NFS

NFS server configuration

We used the following steps in our pattern to configure the NFS Server:

1. Log into lnxpb06 as root.

2. Ensure the NFS File Server group of packages is installed. Run the following command:

Red Hat
> yum grouplist NFS*
You will see the following output:

```
Loaded plugins: product-id, rhnplugin, security, subscription-manager
Updating certificate-based repositories.
Setting up Group Process
Installed Groups:
NFS file server
Done
```

SUSE

zypper info nfs-kernel-server
You should see output similar to the following. Look for the line **"Installed: Yes"** to ensure the server packages are installed.

```
Loading repository data...
Reading installed packages...

Information for package nfs-kernel-server:

Repository: @System
Name: nfs-kernel-server
Version: 1.2.1-2.6.6
Arch: x86_64
Vendor: SUSE LINUX Products GmbH, Nuernberg, Germany
Support Level: unknown
Installed: Yes
Status: up-to-date
Installed Size: 228.0 KiB
Summary: Support Utilities for Kernel nfsd
Description:
This package contains support for the kernel based NFS server. You can
tune the number of server threads via the sysconfig variable
USE_KERNEL_NFSD_NUMBER. For quota over NFS support, install the quota
package.
```

If the NFS File Server is not installed, run the following command to install it:
Red Hat
> yum groupinstall "NFS file server"

SUSE
> zypper install nfs-kernel-server

3. Once the server is installed, ensure it is running by executing the following command:
Red Hat
> service nfs status
You should see output similar to the following:

```
rpc.svcgssd is stopped

rpc.mountd (pid 1567) is running...

nfsd (pid 1564 1563 1562 1561 1560 1559 1558 1557) is running...

rpc.rquotad (pid 1551) is running...
```

SUSE
> service nfsserver status
You should see output similar to the following:

```
Checking for kernel based NFS server: idmapd running
mountd running
statd running
nfsd running
```

If these services are not running, you can use the following command to start them:
Red Hat
> service nfs start

SUSE
> service nfsserver start

4. Run the following command to create a directory to share:
> mkdir -p /home/nfs/bi43pbfrs

Once the directory is created, create a user account to access this through NFS. By default, NFS uses the root account, which is not ideal for security reasons.

5. Create a user called sapbifrs with the password Sapbifrs*123. Run the following commands:
> useradd -s /bin/bash sapbifrs
> passwd sapbifrs

You are prompted to type the password for the user sapbifrs:

```
Changing password for user sapbifrs.
New password: Sapbifrs*123
Retype new password: Sapbifrs*123
passwd: all authentication tokens updated successfully.
```

6. Grant permissions to this user for our /home/nfs/bi43pbfrs directory by running the following command:
> chown sapbifrs /home/nfs/bi43pbfrs

7. You need the uid and gid of the newly created user to set access permissions in the exports file. Run the following command:
> id sapbifrs

You will see output similar to the following:

```
uid=501(sapbifrs) gid=501(sapbifrs) groups=501(sapbifrs)
```

Information: Your uid and gid will be different. You will use these values in the next step.

Now set up the locations and settings to share. These are referred to as exports and are configured in the /etc/exports file. Modify this file to configure access to the directory being used for this pattern.

8. Add the following line to the /etc/exports file on your NFS server machine. Replace "501" with your own uid and gid.

```
/home/nfs/bi43pbfrs lnxpb*(rw,all_squash,anonuid=501,anongid=501)
```

Warning: The /etc/exports file will need to contain values that pertain to your systems. Ensure you are using the correct host pattern,uid, and gid.

The following table examines each part of the line in more detail:

/home/nfs/bi43pbfrs	Indicates the directory being shared

lnxpb*	Allows any host that begins with "lnxpb" to mount this share
rw	Allows reading and writing rights to this mount
all_squash	Squashes all user accounts that try to mount this share
anonuid	Sets the anonymous user ID used by all accounts that try to mount this share
anongid	Sets the anonymous group ID used by all accounts that try to access this share

9. Run the following command to activate the new share:
 exportfs -a
10. Run the following command to check that the new mount is active:
> showmount -e lnxpb06

Warning: Be sure to substitute your NFS Server hostname for "lnxpb06".
You will see output similar to the following:

```
Export list for lnxpb06:
/home/nfs/bi43pbfrs lnxpb*
```

You have now successfully configured the NFS server.

NFS client configuration

Once you have the NFS server running and configured, mount the NFS share on the client machines. In our pattern, the lnxpb04 and lnxpb05machines are the BI 4.0 server machines, and these two machines need these shares mounted.
For more information on NFS Client configuration, refer to your operating system documentation:

1. Red Hat 6 - Storage Administration Guide - NFS Client Configuration.
2. SUSE Administration Guide - Chapter 27.4 Configuring Clients

To mount the NFS server, complete the following steps:

1. Log into lnxpb04 as **root**.
2. Create the directory to use for the mount point. Run the following command:
   > mkdir -p /opt/sap/bi4/bi43pbfrs
3. Run the following commands to create the user **sapbi** and assign it the password **Sapbi*123**:

> useradd -s /bin/bash -m sapbi
> passwd sapbi

```
Changing password for sapbi.
New Password: Sapbi*123
Reenter New Password: Sapbi*123
Password changed.
```

4. Change ownership of the newly created directory to be **sapbi**. Run the following command:
   > chown sapbi /opt/sap/bi4/bi43pbfrs

5. Run the following command to modify the /etc/fstab file:
   > vi /etc/fstab

6. Add the following line to the end of the fstab file:

```
lnxpb06:/home/nfs/bi43pbfrs /opt/sap/bi4/bi43pbfrs nfs defaults 0 0
```

Information: Ensure that you replace "lnxpb06" with the name of your NFS server.

The following table examines each part of the line in more detail:

lnxpb06	Hostname of the NFS server
/home/nfs/bi43pbfrs	Directory path on the NFS server
/opt/sap/bi4/bi43pbfrs	Mount location on the NFS client
nfs	File system type
defaults	Options for the mount (in this case, the defaults of the NFS server)
0 0	Dump frequency / pass number

7. Run the following command to mount the newly created mount point:
> mount -a

8. Run the following command to check whether the mount is available:
> mount

You will see output similar to the following:

```
…
…
lnxpb06:/home/nfs/bi43pbfrs on /opt/sap/bi4/bi43pbfrs type nfs
(rw,vers=4,addr=10.165.28.122,clientaddr=10.165.28.125)
```

9. Change to the **sapbi** user and ensure you can read and write to that new mount point. Run the following commands:
> su - sapbi
> cd /opt/sap/bi4/bi43pbfrs/
> touch a
> rm a
> ls -alrt

You will see output similar to the following:

```
total 8

drwxr-xr-x. 7 sapbi  root 4096 Mar 20 10:22 .

drwxr-xr-x. 2 nobody root 4096 Mar 20 10:52 .
```

10. Repeat steps 1-9 on the lnxpb05 machine.

11. Create the directories for your input and output files. Run the following command on either lnxpb04 or lnxpb05:
> cd /opt/sap/bi4/bi43pbfrs/
> mkdir frsinput frsoutput
> ls -al

You will see output similar to the following:

```
total 8
drwxrwxr-x. 86 sapbi nobody 4096 Jun 21 15:58 frsinput
drwxrwxr-x. 5 sapbi nobody 4096 Apr 4 19:28 frsoutput
```

Once lnxpb04 and lnxpb05 have these mount points set up, you can point both of your Input/output File Repository Servers to the shared location. This ensures that the

system remains active in the event that one of your file repository servers goes down. We cover this in detail in the File Repository Server section.

You have now successfully mounted the NFS share.

Samba Configuration

Samba configuration is covered in the BusinessObjects XI Release 2 Pattern Book for Linux under the **File Sharing Setup** section.

The steps outlined in the above guide are still valid for a BI 4.0 pattern and can be followed if a Samba share is required for your pattern.

More information on using SAMBA on Red Hat can be found here:

Red Hat Documentation - Chapter 11.5 - Samba Configuration

More information on using SAMBA on SUSE can be found here:

SUSE Documentation - Chapter 26 - Samba

Sybase Middleware

To connect to a Sybase database, the Sybase Middleware Client must be installed on the BI platform servers. The following table provides an overview of the steps we used in our pattern along with a checklist you can use to ensure you follow all of the required steps:

Complete these steps for both the lnxpb04 and lnxpb05 machines.

Sybase Middleware Client Configuration Checklist

Create a Sybase user on the server.	✅
Copy over the installation media for the Sybase client.	✅
Install the Sybase client software.	✅
Add required database server info to the Sybase interfaces file.	✅
Configure the sapbi user for Sybase client access.	✅
Test connectivity to the databases as sapbi.	✅

The following sections examine these tasks in more detail.

Creating a Sybase user on the server

In this section, you will create a user called **sybase** and then copy and extract the Sybase installation media.

1. Log into lnxpb04 as **root**.
2. Run the following commands as the root user to create a user called **sybase** and set the password to **Sybase*123**:
   > useradd -s /bin/bash sybase
   > passwd Sybase

   Changing password for sybase.
   New Password: **Sybase*123**
   Reenter New Password: **Sybase*123**
   Password changed.

3. Create a directory for the Sybase ASE 15.7 install files:
   > mkdir -p /opt/sybase/ASE15.7/Install
4. Run the following commands to give **sybase** reading rights:
   > chown -R sybase /opt/sybase
   > chmod -R 755 /opt/sybase
5. Copy the Sybase ASE 15.7 installation files to the directory in which you store your media.
   For example,
   > cp /mount/software/Sybase/ASE15.7.gz /opt/sybase/ASE15.7/Install
6. Extract the installation media to that directory:
   > cd /opt/sybase/ASE15.7/Install
   > gunzip ./ASE15.7.gz
7. Run the following commands to switch to the **sybase** user, and change to the Sybase ASE 15.7 install directory:
   > su - sybase
   > cd /opt/sybase/ASE15.7/Install
8. Repeat steps 1-7 on lnxpb05.

You have now successfully created a user for the Sybase Client installation.

Installing Sybase ASE 15.7

In this section, you will install Sybase ASE on both BI platform servers.

The following steps were used in our pattern. For detailed installation instructions, see the Sybase ASE 15.7 Installation Guide for Linux.

1. Log into lnxpb04 as **root**.
2. Run the following command as the newly created sybase user to launch setup.bin from the Sybase installation directory:
   > ./setup.bin
3. Press **Enter** to continue the installation.
4. Enter the path to which you want to install. In our case, we are installing under /opt/sybase, which is the default. We receive a warning because the /opt/sybase directory already exists.
5. Press **Enter** to continue if you are certain it is okay to overwrite the files in this directory.
6. Choose option **3**, then press **Enter**.
   Since we are using the ASE 15.7 Server Enterprise software installer and we need only the Open Client software installed, we will customize our installation.
7. Select the options that ensure only the client, JDBC, ODBC, and Interactive SQL software are installed.
8. Choose the version to install. You will want a full, licensed copy for production environments, but the Developer Edition should suffice for development environments.
9. Read and accept the license agreement.
10. Confirm that the selected options are correct and press **Enter**.
11. Press **Enter** again to install.
12. Choose to enable or disable the option to store ASE passwords, then press **Enter**.
13. If you do not need to set up the Unified Agent, deselect it and then enter **0** to finish.
14. Press **Enter** to exit the installer.
15. Repeat steps 1-14 on lnxpb05.

You have successfully installed Sybase ASE.

In this section, you will add database connection information to the interfaces file.

1. Log into lnxpb04 as sybase.
2. Navigate to the installation directory of the Sybase client. In our example, we run the following command:
   > cd /opt/sybase
3. Run the following command to create or modify a file called interfaces:
   > vi ./interfaces

4. Add the connection information for the CMS, Auditing, and Reporting Database Servers:
   CMS/Auditing Database Server

Adding the Sybase Database Servers to the interfaces file

In this section, you will add database connection information to the interfaces file.

1. Log into lnxpb04 as sybase.
2. Navigate to the installation directory of the Sybase client. In our example, we run the following command:
   > cd /opt/sybase
3. Run the following command to create or modify a file called interfaces:
   > vi ./interfaces
4. Add the connection information for the CMS, Auditing, and Reporting Database Servers:
   CMS/Auditing Database Server

```
cms57u05
    master tcp ether cmsdb05 5001
    query  tcp ether cmsdb05 5001
```

Information: Note that the information for the CMS Database Server connection is the same as the Auditing Database Server. You need to enter the above information only once for the two databases. Each database server still has its own users/schemas setup.

Reporting Database Server
Add the following lines below the CMS/Auditing Database Server entry.

```
fun57u03
    master tcp ether repdb03 5000
    query tcp ether repdb03 5000
```

Note: In our pattern, we used cmsdb05 and repdb03 as our internal server names for the CMS/Auditing and Reporting Databases. Replace these values with your own internal server names for these databases.

Save and close this file.

5. Run the following command:
   > export LC_ALL=en_US.UTF-8

6. Source the SYBASE.sh file for your shell instance to set up the proper environment variables to use isql. Run the following command:
   > . /opt/sybase/SYBASE.sh
7. Test connectivity to the CMS/Auditing database by running the following command:
   > isql -S cms57u05 -U SAPCMS
8. Enter the password when prompted, and then type the following:
   1> select @@version
   2> go

   You will see output similar to the following:

```
-----------------------------------------------------------------
Adaptive Server Enterprise/15.7.0/EBF 19495 SMP /P/x86_64/Enterprise
Linux/ase157/2820/64-bit/FBO/Fri Sep 16 00:54:35 2011
(1 row affected)
```

9. Test the same workflow with the Reporting database using fun57u03 instead of cms57u05:
   > isql -S fun57u05 -U SAPREPORTING
10. Enter the password when prompted, and then type the following:
    1> select @@version
    2> go
    You will see output similar to the following:

```
-----------------------------------------------------------------
Adaptive Server Enterprise/15.7.0/EBF 19495 SMP /P/x86_64/Enterprise
Linux/ase157/2820/64-bit/FBO/Fri Sep 16 00:54:35 2011
(1 row affected)
```

11. Add any other databases into this interfaces file, such as additional reporting databases.
12. Repeat steps 1-11 on lnxpb05.

You have successfully added the Sybase Database Servers to the interfaces file.

Configuring the sapbi user for Sybase Client access

In this section, you will modify the .bash_profile file to configure **sapbi** for Sybase Client access.

For more information on prerequisites for the Sybase Database, see section **3.2.2 Extra requirements for Sybase** of the UNIX Business Intelligence Platform Installation Guide.

1. Log into lnxpb04 as **sapbi**.
2. Run the following command to edit the .bash_profile file:
   > vi ~/.bash_profile

3. Add the following line to the end of the file:

```
. /opt/sybase/SYBASE.sh
```

4. Log off and log back in as sapbi to reload the profile.

5. Run the following command to ensure that the SYBASE environment variables are now sourced upon loging in:
   > env |grep SYBASE

   You will see output similar to the following:

```
SYBASE_JRE6_64=/opt/sybase/shared/JRE-6_0_24_64BIT
SYBASE_JRE6_32=/opt/sybase/shared/JRE-6_0_24_32BIT
SYBASE_JRE6=/opt/sybase/shared/JRE-6_0_24_64BIT
SYBASE_UA=/opt/sybase/UAF-2_5
SYBASE_OCS=OCS-15_0
SYBASE=/opt/sybase
SYBASE_PLATFORM=linux
```

6. Repeat steps 1-5 on lnxpb05.

You have successfully configured the sapbi user for Sybase Client access.

Testing connectivity to the Sybase servers

In this section, you will verify connectivity to the databases.

1. Log into lnxpb04 as sapbi.
2. Run the following command to test that the **sapbi** user has connectivity to the CMS/Auditing database:
   > isql -S cms57u05 -U SAPCMS
3. Enter the password when prompted, and then type the following:
   1> select @@version

2> go
You will see output similar to the following:

```
-----------------------------------------------------------------
Adaptive Server Enterprise/15.7.0/EBF 19495 SMP /P/x86_64/Enterprise
Linux/ase157/2820/64-bit/FBO/Fri Sep 16 00:54:35 2011
(1 row affected)
```

4. Run the following command to test that the **sapbi** user has connectivity to the Reporting database:
   > isql -S fun57u03 -U SAPREPORTING
5. Enter the password when prompted, and then type the following:
   1> select @@version
   2> go

   You will see output similar to the following:

```
-----------------------------------------------------------------
Adaptive Server Enterprise/15.7.0/EBF 19495 SMP /P/x86_64/Enterprise
Linux/ase157/2820/64-bit/FBO/Fri Sep 16 00:54:35 2011
(1 row affected)
```

6. Repeat steps 1-5 on lnxpb05.
   If you see something similar to the above, then you have proper connectivity to the databases.

You have successfully tested connectivity to the Sybase servers and set up the Sybase middleware.

BusinessObjects Cluster

To set up the BusinessObjects cluster, you install the BI platform servers on two machines and cluster them together. The following topics provide step-by-step instructions for setting up the cluster:

- Setting up BI platform server 1
- Setting up BI platform server 2
- Changing the Linux Pattern Cluster Name

Setting up BI platform server 1

Installing BI platform

We will start by installing the BI platform server on machine lnxpb04. This is our primary node in the cluster.

1. Log into lnxpb04 as **root**.

2. Run the following commands to create the directory /opt/sap/bi4 and give the bi4 directory full rights (read, write, and execute rights):
   > mkdir -p /opt/sap/bi4
   > chown sapbi /opt/sap/bi4
   > chmod 755 -R /opt/sap/bi4
3. **For Red Hat Only**
4. **Information:** Red Hat has a few required packages that might not be installed or updated by default on your machine. The commands in this step ensure they are updated in your Red Hat environment.

   You must ensure that the yum tool is configured correctly to run these commands. If you do not have the yum tool configured, contact your Red Hat Administrator.

   Run the following commands to install the binaries required for the BI platform installation to work:
   > yum install glibc.i686
   > yum install libstdc++.i686
   > yum install compat-libstdc++-33-3.2.3-69.el6.i686
   > yum install compat-libstdc++-33.i686
   > yum install compat-libstdc++-33-3.x86_64
   > yum install libX11-1.3-2.el6.i686
5. Run the following command to change to the **sapbi** user:
   > su - sapbi
6. Run the following commands to create the directory /home/sapbi/install and give the install directory full rights:
   > mkdir -p /home/sapbi/install
   > chmod 755 /home/sapbi/install
7. Load, mount, or download the BI platform installation media to your computer and copy it to the install directory. You can download the software from SAP Software Download Center.

   Information: The downloaded package is a multi-spanning RAR archive. Please use SAP Note 886535 for instructions on how to properly extract it on Linux.
7. Run the following commands to set the locale settings to US English and UTF-8.
   > export LANG=en_US.utf8
   > export LC_ALL=en_US.utf8
8. Run the setup command from the install directory:
   > cd /home/sapbi/install
   > ./setup.sh

Proceed through the installer, using the following screenshots as reference.

9. Press **Enter**.

```
Setup Language
Please choose a setup language


 1  -   English
 2  -   French
 3  -   German
 4  -   Russian
 5  -   Turkish
 6  -   Simplified Chinese
 7  -   Traditional Chinese
 8  -   Japanese
 9  -   Korean
10  -   Czech
11  -   Danish
12  -   Spanish
13  -   Finnish
14  -   Hungarian
15  -   Italian

Press [Tab] to move to the next field, [Ctrl-X] to quit, or [Enter] to continue.
```

10. Set the **Destination Folder** to /opt/sap/bi4, then press **Enter**.

```
Specify the Destination Folder
The destination folder is where the product will be installed. Please enter the full pat
h.

Destination Folder
[/opt/sap/bi4                                                    ]



Press [Tab] to move to the next field, [Ctrl-B] to go back, [Ctrl-X] to quit, or [Enter]
 to continue.
```

11. Confirm the necessary prerequisites have been met, then press **Enter**.
The installation program checks for required components and conditions. Since DB2 is not being installed and all other prerequisites are successful, there is nothing else to do here.

```
Prerequisite check
Summary of any missing critical or optional prerequisites.


Failed: Integrated database - home directory (Optional)
        Information: DB2 requires 755 permissions to be set in the user's home
directory.  Please set the permissions if you wish to install the integrated DB2
database.
Failed: Integrated database - user and group (Optional)
        Information: The user group naming fails one of DB2's restrictions or
insufficient kernel parameters.  Please go to
http://publib.boulder.ibm.com/infocenter/db2luw/v9r7 and search 'User ID
restrictions' or 'Kernel parameters' for details.
Succeeded: Information Platform Services not installed (Critical)
Succeeded: Operating system patch level (Optional)
Succeeded: BI platform server 4.x not present (Critical)
Succeeded: Integrated database - directories (Optional)
Succeeded: Integrated database - gunzip (Optional)
Succeeded: Disk space in /tmp (Critical)

Press [Tab] to move to the next field, [Ctrl-X] to quit, or [Enter] to continue.
```

12. Acknowledge the warning, then press **Enter**.

```
Welcome to the installation wizard for SAP BusinessObjects BI platform 4.0


WARNING: This program is protected by copyright law and international treaties.


Unauthorized reproduction or distribution of this program, or any portion of it,
may result in severe civil and criminal penalities, and will be prosecuted to the
maximum extent possible under law.









Press [Tab] to move to the next field, [Ctrl-B] to go back, [Ctrl-X] to quit, or [Enter]
 to continue.
```

13. Read the license agreement, then press **Enter**.

```
License Agreement
You must agree to the licensing conditions to proceed.


SOTFWARE LICENSE AGREEMENT




IMPORTANT-READ CAREFULLY: THIS IS A LEGAL AGREEMENT BETWEEN YOU AND SAP FOR THE SAP
SOFTWARE ACCOMPANYING THIS AGREEMENT, WHICH MAY INCLUDE COMPUTER SOFTWARE,
ASSOCIATED MEDIA, PRINTED MATERIALS AND ONLINE OR ELECTRONIC DOCUMENTATION
(âSOFTWAREâ
           READ, ACKNOWLEDGE AND ACCEPT THE TERMS AND CONDITIONS OF THE SOFTWARE LICENSE

AGREEMENT THAT FOLLOWS (âAGREEMENTâ
                                 OF THE AGREEMENT, YOU MAY RETURN, WITHIN THIRTY (30)
DAYS OF PURCHASE, THE SOFTWARE
TO THE PLACE YOU OBTAINED IT FOR A FULL REFUND.
Press <ENTER> to accept, <CTRL-X> to not accept
```

14. Enter the **Product Keycode**, then press **Enter**.

```
User Information
Please type your product key to proceed.


Product Keycode:
[00000-0000000-0000000-0000000-00                          ]



Press [Tab] to move to the next field, [Ctrl-B] to go back, [Ctrl-X] to quit, or [Enter]
 to continue.
```

15. Leave the English language pack selected, then press **Enter**.

```
Choose Language Packs
A language pack allows a user to interact with the product in a specific language.


[X]  English
[ ]  Simplified Chinese
[ ]  Japanese
[ ]  Czech
[ ]  Norwegian
[ ]  Spanish
[ ]  Hungarian
[ ]  Finnish
[ ]  German
[ ]  Korean
[ ]  Traditional Chinese
[ ]  Dutch
[ ]  Russian
[ ]  Swedish
[ ]  Thai

Press [Space] or [X] to select or deselect a language pack. Press [Ctrl-B] to go back, [
Ctrl-X] to quit, or [Enter] to continue.
```

16. Choose **User install**, then press **Enter**.

```
Select a user install or a system install
System install requires root access to run initialization scripts after install


 1  -   User install - regular SAP BusinessObjects BI platform installation
 2  -   System install - user install plus system initialization scripts

Press [Tab] to move to the next field, [Ctrl-B] to go back, [Ctrl-X] to quit, or [Enter]
 to continue.
```

17. Choose **Custom / Expand**, then press **Enter**.
18. Uncheck the **WebTier** feature, then press **Enter**.

```
Select Features
Select the features that you want to install.

-[~] Instances
  +[ ] WebTier
  +[X] Servers
  +[X] Administrator Tools
  +[~] Database Access
   [X] Samples

Press [Space] to expand the feature tree, or [X] to select or deselect a feature.  Press
 [Ctrl-B] to go back, [Ctrl-X] to quit, or [Enter] to continue.
```

19. Choose **Start a new SAP BusinessObjects BI platform deployment**, then press **Enter**.

```
Expand Installation
Decide whether to start a new SAP BusinessObjects BI platform deployment, or expand an e
xisting one.

 1  -   Start a new SAP BusinessObjects BI platform deployment
 2  -   Expand an existing SAP BusinessObjects BI platform deployment. (Requires a
        remotely installed CMS)

Press [Tab] to move to the next field, [Ctrl-B] to go back, [Ctrl-X] to quit, or [Enter]
 to continue.
```

20. Choose Sybase for the existing CMS database type, then press Enter.

```
Select existing CMS Database Type
Specify the database type to use for the CMS repository.


 1  -   MySQL
 2  -   IBM DB2
 3  -   Oracle
 4  -   MaxDB
 5  -   Sybase




Press [Tab] to move to the next field, [Ctrl-B] to go back, [Ctrl-X] to quit, or [Enter]
 to continue.
```

21. Choose **Sybase** for the existing Auditing database type, then press **Enter**.

```
Select existing Auditing Database Type
Specify the database to use for the Auditing database.  Select No Auditing database to c
onfigure auditing at a later time.

 1  -   MySQL
 2  -   IBM DB2
 3  -   Oracle
 4  -   MaxDB
 5  -   Sybase
 6  -   No Auditing database




Press [Tab] to move to the next field, [Ctrl-B] to go back, [Ctrl-X] to quit, or [Enter]
 to continue.
```

22. Type in the SIA **Node Name** and **SIA Port** number, then press **Enter**.

```
Configure Server Intelligence Agent (SIA)
Enter a name and port number for the SIA node.


Node Name
[SIANAME                                                    ]
SIA Port
[6410  ]



Press [Tab] to move to the next field, [Ctrl-B] to go back, [Ctrl-X] to quit, or [Enter] to continue.
```

23. Type in the **CMS Port** number, then press **Enter**.

```
Configure Central Management Server (CMS)
Enter a port number for the CMS


CMS Port
[6400  ]



Press [Tab] to move to the next field, [Ctrl-B] to go back, [Ctrl-X] to quit, or [Enter]
 to continue.
```

24. Enter a **Password** for the Administrator and a value for the **Cluster Key**, then press **Enter**.

```
Configure CMS Account
Specify the new password for the CMS Administrator account, and a value for the CMS Clus
ter Key.

Administrator Account Password:
[**********                                                    ]
Confirm Password:
[**********                                                    ]
Cluster Key:
[**********                                                    ]
Confirm Cluster Key:
[**********                                                    ]

Press [Tab] to move to the next field, [Ctrl-B] to go back, [Ctrl-X] to quit, or [Enter]
 to continue.
```

25. Enter the Sybase **Username** and **Password** for the BOE_CMS database, then press **Enter**.

```
Configure CMS Repository Database - Sybase
Enter details for the database to use for storing CMS information.

Sybase Service Name
[SERVICENAME                                                   ]
Username
[USER                                                          ]
Password
[********                                                      ]
Reset existing database (1 = yes, 0 = no)
[1]

Press [Tab] to move to the next field, [Ctrl-B] to go back, [Ctrl-X] to quit, or [Enter] to continue.
```

26. Enter the Sybase Username and Password for the BOE_AUDIT database, then press **Enter**

```
Configure Auditing Database - Sybase
Enter details for the database to use for storing Auditing information.


Sybase Service Name
[SERVICENAME                                          ]
Username
[USER                                                 ]
Password
[********                                             ]



Press [Tab] to move to the next field, [Ctrl-B] to go back, [Ctrl-X] to quit, or [Enter] to continue.
```

27. Choose **Yes** to start the servers after the installation, then press **Enter**.

```
Choose to start or stop servers
Start the servers after installation?


 1  -   Yes
 2  -   No



Press [Tab] to move to the next field, [Ctrl-B] to go back, [Ctrl-X] to quit, or [Enter] to continue.
```

28. Enter the **HTTP Listening Port**, then press **Enter**.

```
Configure HTTP Listening Port
Enter the HTTP listening port for connecting to WACS and/or RESTful Web Services.


HTTP Listening Port
[6405 ]



Press [Tab] to move to the next field, [Ctrl-B] to go back, [Ctrl-X] to quit, or [Enter] to continue.
```

29. Enter the **Repository Port number** and **Repository User Password** for the Subversion, then press **Enter**.

```
Configure Subversion
Subversion will be installed and used as the version control system for version management. Provide the por
t and user name for Subversion.

Repository Port
[3690  ]
Repository User Password
[**********                                        ]
Confirm Password
[**********                                        ]

Press [Tab] to move to the next field, [Ctrl-B] to go back, [Ctrl-X] to quit, or [Enter] to continue.
```

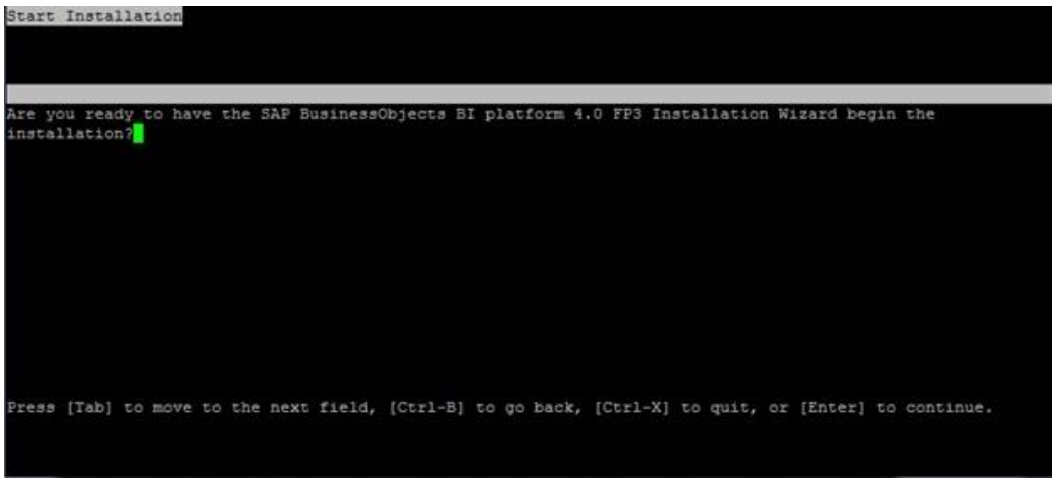
30. Choose **Do not configure connectivity for SMD Agent,** then press **Enter.**

```
Configure Connectivity Solution Manager Diagnostics (SMD) Agent.
Enable connectivity to SMD Agent.

 1  -   Do not configure connectivity to SMD Agent.
 2  -   Configure connectivity to SMD Agent. You will be prompted for information.

Press [Tab] to move to the next field, [Ctrl-B] to go back, [Ctrl-X] to quit, or [Enter] to continue.
```

31. Choose **Do not integrate connectivity to Introscope Enterprise Manager,** then press **Enter.**

```
Introscope Integration
Enable connectivity to Introscope Enterprise Manager.

 1  -   Do not integrate connectivity to Introscope Enterprise Manager.
 2  -   Integrate connectivity to Introscope Enterprise Manager. You will be prompted for information.

Press [Tab] to move to the next field, [Ctrl-B] to go back, [Ctrl-X] to quit, or [Enter] to continue.
```

32. Press **Enter** to start the installation.



Setting up BI platform server 2

Installing BI platform

The pre-installation steps for setting up the second BI platform server are the same as steps 1-8 from Setting up BI platform server 1. The only difference is that the machine name becomes lnxpb05. The installation steps are slightly different though and should be followed carefully.

Warning: Before following the instructions below, ensure that the CMS is running on lnxpb04. See "Verifying that the BI platform server is up and running" in Setting up BI platform server 1 for details.

1. Log into lnxpb05 as **root**.
2. Run the following commands to create the directory /opt/sap/bi4 and give the bi4 directory full rights (read, write, and execute rights):
   > mkdir -p /opt/sap/bi4
   > chown sapbi /opt/sap/bi4
   > chmod 755 -R /opt/sap/bi4
3. **For Red Hat Only**

   Information: Red Hat has a few required packages that might not be installed or updated by default on your machine. The commands in this step ensure they are updated in your Red Hat environment.

   You must ensure that the yum tool is configured correctly to run these commands. If you do not have the yum tool configured, contact your Red Hat Administrator.

Run the following commands to install the binaries required for the BI platform installation to work:

> yum install glibc.i686

> yum install libstdc++.i686

> yum install compat-libstdc++-33-3.2.3-69.el6.i686

> yum install compat-libstdc++-33.i686

4. Run the following command to change to the **sapbi** user:

   > su - sapbi

5. Run the following commands to create the directory /home/sapbi/install and give the install directory full rights:

   > mkdir -p /home/sapbi/install

   > chmod 777 /home/sapbi/install

6. Load, mount, or download the BI platform installation media to your computer and copy it to the install directory. You can download the software from SAP Software Download Center.

   Information: The downloaded package is a multi-spanning RAR archive. Please use SAP Note 886535 for instructions on how to properly extract it on Linux.

7. Run the following commands to set up the locale settings to US English and UTF-8:

   > export LANG=en_US.utf8

   > export LC_ALL=en_US.utf8

8. Run the setup command from the install directory:

   > cd /home/sapbi/install

   > ./setup.sh

   Proceed through the installer, using the following screenshots as reference.

9. Press **Enter**.

```
Setup Language
Please choose a setup language


 1  -   English
 2  -   French
 3  -   German
 4  -   Russian
 5  -   Turkish
 6  -   Simplified Chinese
 7  -   Traditional Chinese
 8  -   Japanese
 9  -   Korean
10  -   Czech
11  -   Danish
12  -   Spanish
13  -   Finnish
14  -   Hungarian
15  -   Italian

Press [Tab] to move to the next field, [Ctrl-X] to quit, or [Enter] to continue.
```

10. Set the **Destination Folder** to /opt/sap/bi4, then press **Enter**.

```
Specify the Destination Folder
The destination folder is where the product will be installed. Please enter the full pat
h.

Destination Folder
[/opt/sap/bi4                                                    ]



Press [Tab] to move to the next field, [Ctrl-B] to go back, [Ctrl-X] to quit, or [Enter]
 to continue.
```

11. Confirm the necessary prerequisites have been met, then press **Enter**.
The installation program checks for required components and conditions. Since

DB2 is not being installed and all other prerequisites are successful, there is nothing else to do here.

```
Prerequisite check
Summary of any missing critical or optional prerequisites.


Failed: Integrated database - home directory (Optional)
        Information: DB2 requires 755 permissions to be set in the user's
home directory.  Please set the permissions if you wish to install the
integrated DB2 database.
Failed: Integrated database - user and group (Optional)
        Information: The user group naming fails one of DB2's restrictions
or insufficient kernel parameters.  Please go to
http://publib.boulder.ibm.com/infocenter/db2luw/v9r7 and search 'User ID
restrictions' or 'Kernel parameters' for details.
Succeeded: Information Platform Services not installed (Critical)
Succeeded: Operating system patch level (Optional)
Succeeded: BI platform server 4.x not present (Critical)
Succeeded: Integrated database - directories (Optional)
Succeeded: Integrated database - gunzip (Optional)
Succeeded: Disk space in /tmp (Critical)

Press [Tab] to move to the next field, [Ctrl-X] to quit, or [Enter] to continue.
```

12. Acknowledge the warning, then press **Enter**.

```
Welcome to the installation wizard for SAP BusinessObjects BI platform 4.0


WARNING: This program is protected by copyright law and international treaties.


Unauthorized reproduction or distribution of this program, or any portion of it, may
result in severe civil and criminal penalities, and will be prosecuted to the maximum
extent possible under law.


Press [Tab] to move to the next field, [Ctrl-B] to go back, [Ctrl-X] to quit, or [Enter] to con
tinue.
```

13. Read over the license agreement, then press **Enter**.

```
License Agreement
You must agree to the licensing conditions to proceed.

SOFTWARE LICENSE AGREEMENT



IMPORTANT-READ CAREFULLY: THIS IS A LEGAL AGREEMENT BETWEEN YOU AND SAP FOR THE SAP
SOFTWARE ACCOMPANYING THIS AGREEMENT, WHICH MAY INCLUDE COMPUTER SOFTWARE, ASSOCIATED
MEDIA, PRINTED MATERIALS AND ONLINE OR ELECTRONIC DOCUMENTATION (âSOFTWAREâ
                                                                  CONTINUING WITH THE
INSTALLATION OF THE SOFTWARE, YOU MUST READ, ACKNOWLEDGE AND ACCEPT
THE TERMS AND CONDITIONS OF THE SOFTWARE LICENSE AGREEMENT THAT FOLLOWS (âAGREEMENTâ
                                                                        YOU DO NOT
ACCEPT THE TERMS AND CONDITIONS OF THE AGREEMENT, YOU MAY RETURN, WITHIN THIRTY
(30) DAYS OF PURCHASE, THE SOFTWARE TO THE PLACE YOU OBTAINED IT FOR A FULL REFUND.


1.  GRANT OF LICENSE. SAP grants you a nonexclusive and limited license to use the
Software products and functionalities for which you have paid the applicable fees solely
```

14. Enter the **Product Keycode**, then press **Enter**.

```
User Information
Please type your product key to proceed.

Product Keycode:
[00000-0000000-0000000-0000000-00                          ]



Press [Tab] to move to the next field, [Ctrl-B] to go back, [Ctrl-X] to quit, or [Enter]
 to continue.
```

15. Leave the English language pack selected, then press **Enter**.

```
Choose Language Packs
A language pack allows a user to interact with the product in a specific language.


[X]  English
[ ]  Polish
[ ]  German
[ ]  Hungarian
[ ]  Simplified Chinese
[ ]  Norwegian
[ ]  Swedish
[ ]  Korean
[ ]  Romanian
[ ]  Dutch
[ ]  Danish
[ ]  Traditional Chinese
[ ]  French
[ ]  Japanese
[ ]  Thai
[ ]  Czech
[ ]  Turkish
[ ]  Spanish

Press [Space] or [X] to select or deselect a language pack. Press [Ctrl-B] to go back, [Ctrl-X]
 to quit, or [Enter] to continue.
```

16. Choose **User install**, then press **Enter**.

```
Select a user install or a system install
System install requires root access to run initialization scripts after install


 1  -   User install - regular SAP BusinessObjects BI platform installation
 2  -   System install - user install plus system initialization scripts



Press [Tab] to move to the next field, [Ctrl-B] to go back, [Ctrl-X] to quit, or [Enter] to con
tinue.
```

17. Choose **Custom / Expand**, then press **Enter**.

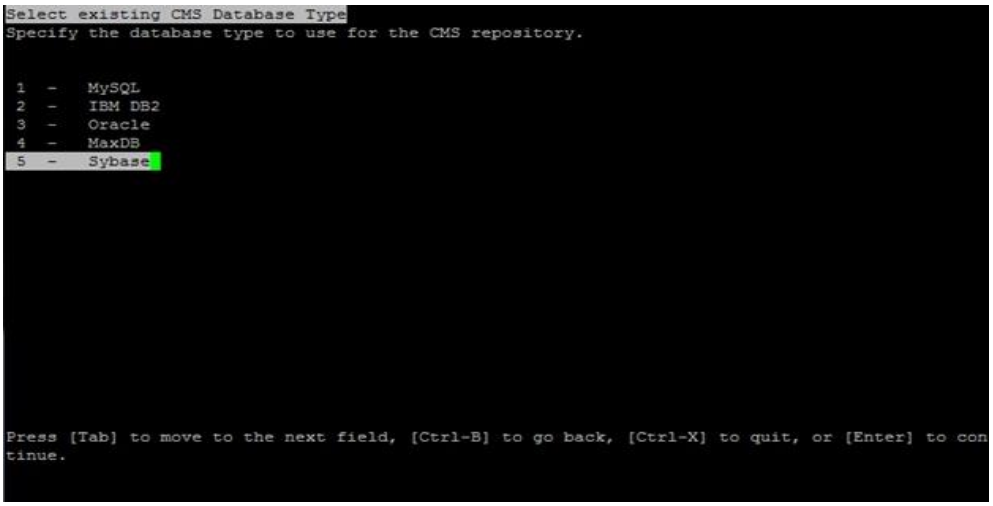
18. Uncheck the **WebTier** and **Subversion** features, then press **Enter**

```
Select Features
Select the features that you want to install.


-[~] Instances
  +[ ] WebTier
  -[~] Servers
    -[~] Platform Services
       [X] Central Management Server
       [X] File Repository Services (FRS)
           Integrated Database
       [X] Event Service
       [X] System Landscape Data Supplier
       [X] Web Application Container Server
       [X] Platform Processing Services
       [X] Platform Scheduling Services
       [X] RESTful Web Service
       [X] Insight to Action Service
       [ ] Subversion
    +[X] Connectivity Services
    +[X] Data Federator Service
    +[X] Analysis Services

Press [Space] to expand the feature tree, or [X] to select or deselect a feature.  Press [Ctrl-
B] to go back, [Ctrl-X] to quit, or [Enter] to continue.
```

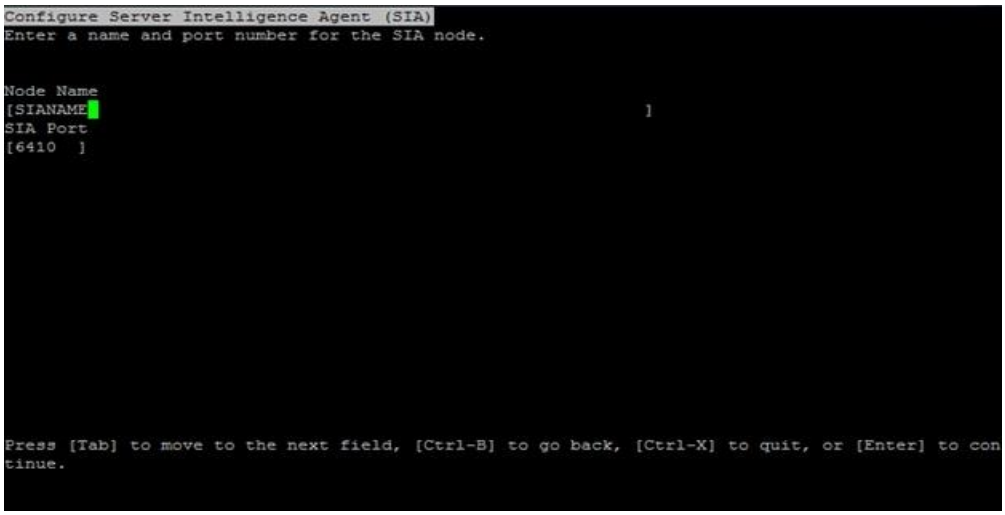
19. Choose **Expand an existing SAP BusinessObjects BI platform deployment**, then press **Enter**.

```
Expand Installation
Decide whether to start a new SAP BusinessObjects BI platform deployment, or expand an existing
 one.

 1  -   Start a new SAP BusinessObjects BI platform deployment
 2  -   Expand an existing SAP BusinessObjects BI platform deployment. (Requires a remotely
        installed CMS)

Press [Tab] to move to the next field, [Ctrl-B] to go back, [Ctrl-X] to quit, or [Enter] to con
tinue.
```

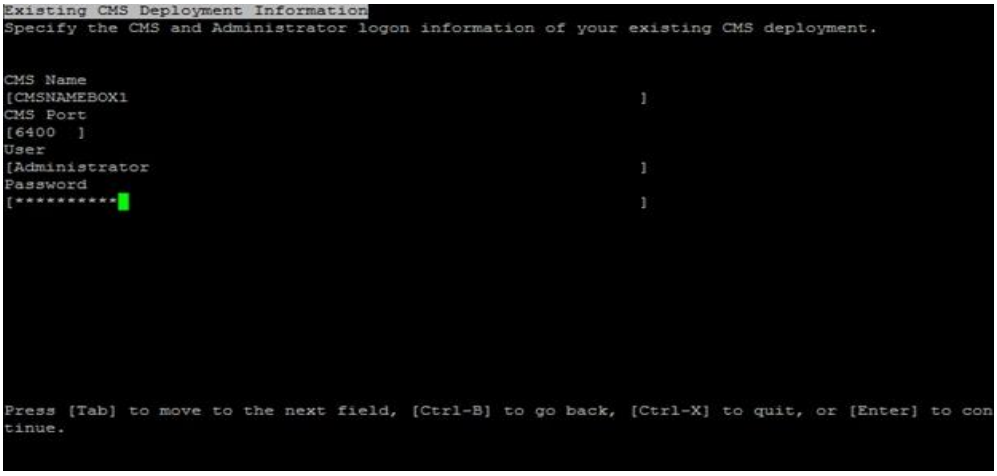
20. Choose **Sybase** for CMS DB, then press **Enter**.
Notice there is no option for choosing an existing Auditing database type when doing an expanded installation.



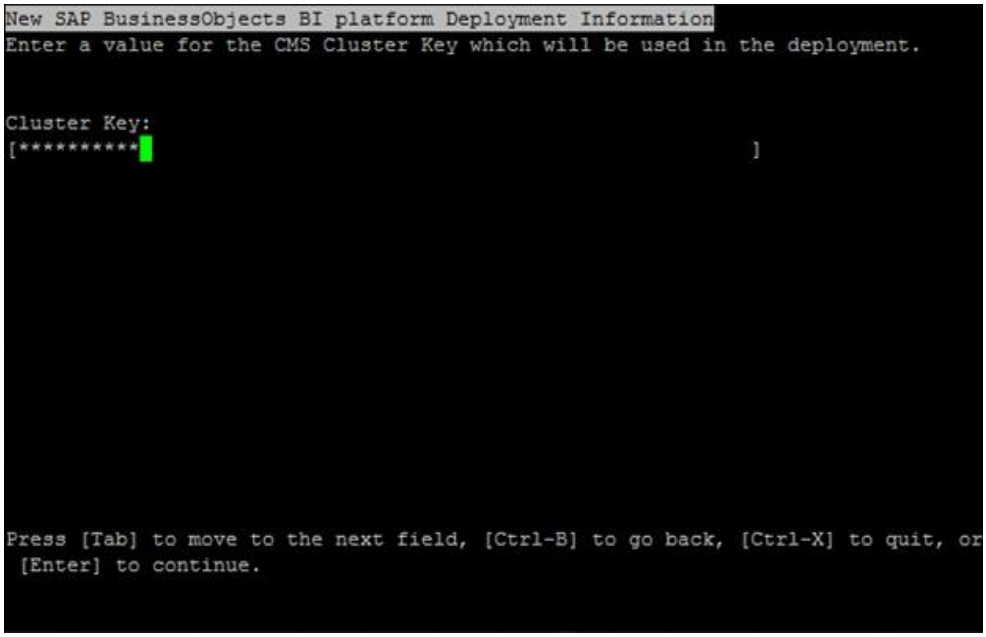
21. Enter the SIA **Node Name** and **SIA Port** number, then press **Enter**.



22. Enter the **CMS Name**, the **CMS Port** number, and the Administrator's **Password**, then press **Enter**.



23. Enter the Cluster Key that you specified in [Setting up BI platform server 1](), then press Enter.



24. Enter the **CMS Port** number, then press **Enter**.

```
Configure Central Management Server (CMS)
Enter a port number for the CMS


CMS Port
[6400 ]



Press [Tab] to move to the next field, [Ctrl-B] to go back, [Ctrl-X] to quit, or
 [Enter] to continue.
```

25. Enter the Sybase **Username** and **Password**, then press **Enter**.

```
Configure CMS Repository Database - Sybase
Enter details for the database to use for storing CMS information.


Sybase Service Name
[SERVICENAME                                                    ]
Username
[USER                                                           ]
Password
[**********                                                     ]



Press [Tab] to move to the next field, [Ctrl-B] to go back, [Ctrl-X] to quit, or
 [Enter] to continue.
```

26. Choose **Yes** to start servers after installation, then press **Enter**.

```
Choose to start or stop servers
Start the servers after installation?

 1  -   Yes
 2  -   No

Press [Tab] to move to the next field, [Ctrl-B] to go back, [Ctrl-X] to quit, or
 [Enter] to continue.
```

27. Enter the **HTTP Listening Port**, then press **Enter**.

```
Configure HTTP Listening Port
Enter the HTTP listening port for connecting to WACS and/or RESTful Web Services
.

HTTP Listening Port
[6405 ]

Press [Tab] to move to the next field, [Ctrl-B] to go back, [Ctrl-X] to quit, or
 [Enter] to continue.
```

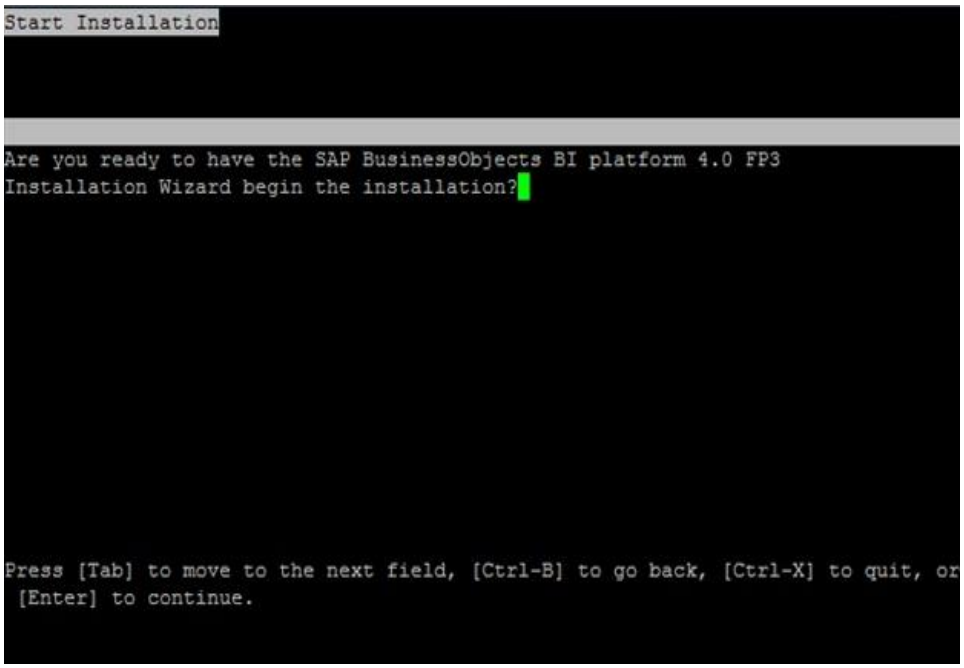
28. Choose **Do not configure connectivity for SMD Agent**, then press **Enter**.

```
Configure Connectivity Solution Manager Diagnostics (SMD) Agent.
Enable connectivity to SMD Agent.

 1  -   Do not configure connectivity to SMD Agent.
 2  -   Configure connectivity to SMD Agent. You will be prompted for
        information.

Press [Tab] to move to the next field, [Ctrl-B] to go back, [Ctrl-X] to quit, or
 [Enter] to continue.
```

29. Choose **Do not integrate connectivity to Introscope Enterprise Manager**, then press **Enter**.

```
Introscope Integration
Enable connectivity to Introscope Enterprise Manager.

 1  -   Do not integrate connectivity to Introscope Enterprise Manager.
 2  -   Integrate connectivity to Introscope Enterprise Manager. You will be
        prompted for information.

Press [Tab] to move to the next field, [Ctrl-B] to go back, [Ctrl-X] to quit, or
 [Enter] to continue.
```

30. Press **Enter** to start the installation.



You have successfully set up BI platform server 2.

Verifying the BI platform server is up and running

In this section, you will verify if the installation was successful.

1. Navigate to the directory you installed to:
   > cd /opt/sap/bi4/sap_bobj

2. Run the following command to see if the cms process is running:
   > ps -ef |grep boe_cmsd
   You will see output similar to the following:

```
sapbi 22599 22559 3 12:54 pts/0 00:01:43
/opt/sap/bi4/sap_bobj/enterprise_xi40/linux_x64//boe_cmsd -loggingPath
/opt/sap/bi4/sap_bobj/logging/ -port 6400 -restart -dbinfo
/opt/sap/bi4/sap_bobj/enterprise_xi40/linux_x64/_boe_SAPBI43B.dbinfo -
noauditor -autoboot -fg -name SAPBI43B.cms -pidfile
/opt/sap/bi4/sap_bobj/serverpids/SAPBI43B_SAPBI43B.CentralManagementServ
er.pid
```

3. If the boe_cmsd process is running, run the following command to logon to the CMS and display a list of the servers:
   > ./ccm.sh -display -username Administrator -password Pattern123

You should see output similar to the following, indicating that the installation was successful:

```
Creating session manager...
Logging onto CMS...
Creating infostore...
Sending query to get all server objects on the local machine...
Checking server status...
Server Name: SAPBI43B.CentralManagementServer
    State: Running
    Enabled: Enabled
    Host Name: vantgvmlnxpb05
    PID: 22599
    Description: Central Management Server
...
...
```

Changing the Linux Pattern Cluster Name

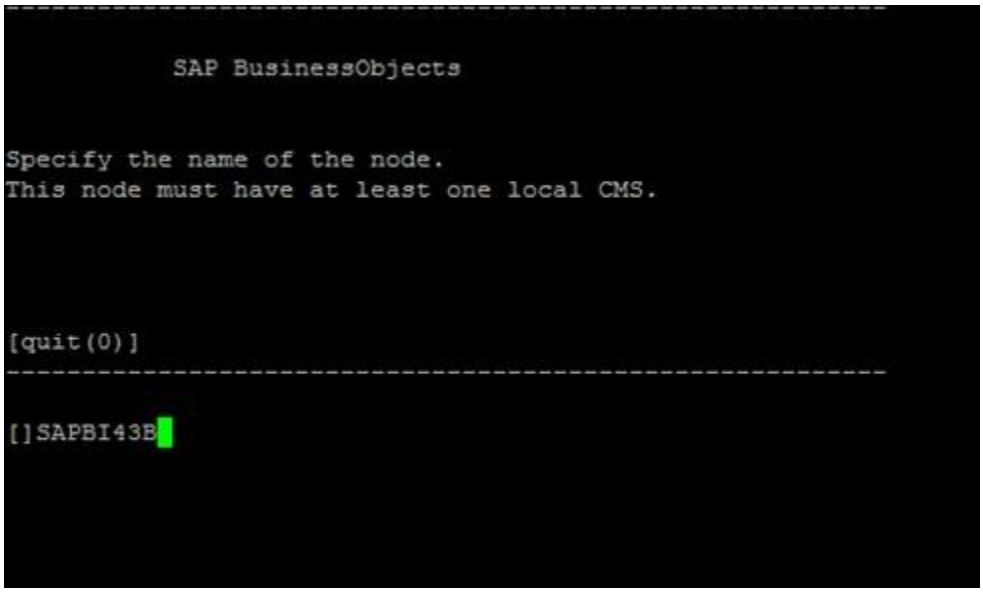
These steps can be performed on any server where the CMS is running. In our environment, the CMS is running on lnxpb04 and lnxpb05. Sincelnxpb04 is my primary server in the cluster, I am going to change the cluster name on the lnxpb05 machine, then verify the name change.

Changing the cluster name

In this section, you will stop the servers and change the cluster name.

1. Log into lnxpb05 as **sapbi**.
2. Run the following command to navigate to the sap_bobj directory:
   > cd /opt/sap/bi4/sap_bobj/
3. Run the following command to stop the SIA servers:
   > ./stopservers
4. Run the following command:
   > ./cmsdbsetup.sh

5. Enter the SIA server name you set up for lnxpb05 in Setting up BI platform server 2 and press **Enter**.
   In our example, we enter SAPBI43B.



File Repository Server

A clustered BI platform environment requires the Input and Output File Repository Servers to use a common file share location for the servers within the cluster.

There are many options for file sharing between Linux machines. Two of the most popular ways are

Network File System (NFS) and (Samba). NFS is more common when the file share will remain in a Linux environment. Samba is mainly used for sharing files within a mixed Linux/Windows environment.

We use NFS within this pattern and also provide some resources on how to use Samba if you wanted to go down that road instead.

By now, you should already have your 2 BI platform servers up and running along with your Application Server (Tomcat) and Web Server (Apache). These are prerequisites for this sections so if you don't have these up, please revisit those sections to complete the setup of those components.

We setup the FRS in our cluster by following the below checklist:

Move files from original FRS location on BIP Servers to shared location	✅
Start up BIP Servers and disable all services	✅
Update Input/Output FRS Services on BIP Servers to the shared location	✅
Enable BIP Server services	✅

Moving files from original FRS location on BIP servers to shared location

Please ensure that the steps in the section NFS Configuration have been carried out before continuing.

1. Log into lnxpb04 as the sapbi user
2. Ensure your NFS mount point is available by running the following command:
   > mount |grep bi43pbfrs

   You should see output similar to the following:

   ```
   vantgvmlnxpb01:/home/nfs/bi43pbfrs on /opt/sap/bi4/bi43pbfrs type nfs
   (rw,vers=4,addr=10.165.28.122,clientaddr=10.165.28.125)
   ```

3. Once the mount has been set up, run the following command to navigate to the sap_bobj directory:
   > cd /opt/sap/bi4/sap_bobj
4. Run the following command to stop your SIA servers:
   > ./stopservers
5. Run the following command to navigate to your default input FRS directory:
   > cd /opt/sap/bi4/sap_bobj/data/frsinput/
6. Run the following command to copy all of the files and folders in the input FRS directory to the mounted drive:
   > cp -r * /opt/sap/bi4/bi43pbfrs/frsinput
7. Run the following command to navigate to the output FRS directory:
   > cd /opt/sap/bi4/sap_bobj/data/frsoutput/
8. Run the following command to copy all of the files and folders in the output FRS directory to the mounted drive:
   > cp -r * /opt/sap/bi4/bi43pbfrs/frsoutput

9. Repeat steps 1-8 on lnxpb05.

Information: In most cases, only one of your servers will have content within these directories but in the odd chance that one of your servers did failover to the backup FRS, it is best to copy the content from both servers over to the new location.

Now that you have copied all of the content into the shared input and output FRS directories, start up the SIA servers (both servers)

10. Run the following command to navigate to the sap_bobj folder:
    > cd /opt/sap/bi4/sap_bobj/
11. Run the following command to start up the SIA servers:
    > ./startservers
    You have successfully copied the content of the input and output FRS directories.
12. This next step ensures that no further files are written to the old FRS locations while we are making the changes within the Central Management Console (CMC). From either server, run the following commands:
    > cd /opt/sap/bi4/sap_bobj/
    > ./ccm.sh -disable all -username Administrator -password Pattern123

    You should see output similar to the following:

```
Creating session manager...
Logging onto CMS...
Creating infostore...
Sending query to get all server objects on the local machine...
Checking server status...
SAPBI43A.CentralManagementServer has been disabled.
SAPBI43A.AdaptiveProcessingServer has been disabled.
...
...
Committing changes to infostore...
```

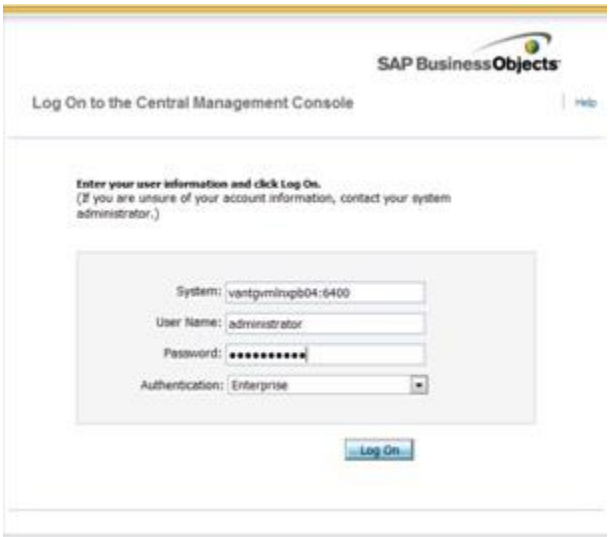
13. Repeat steps 10-12 for lnxpb05.

We can now carry out our steps in the CMC without worrying about more files being written to the old FRS locations.

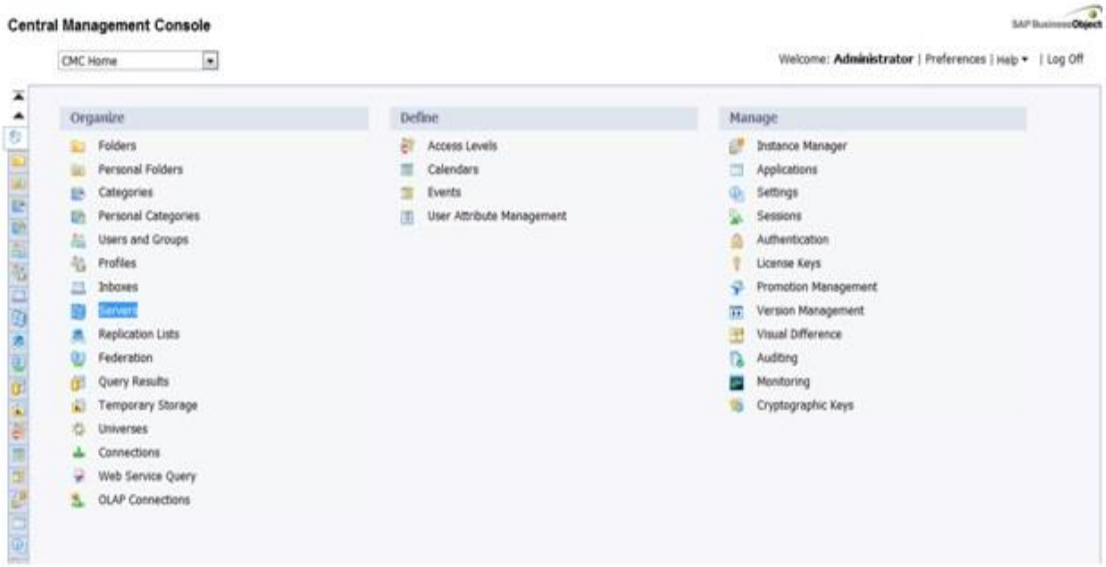
Updating Input/Output FRS services on BIP servers to the shared location

Now that the physical files have been moved to the new location, it is important for us to update the services on the BIP servers.

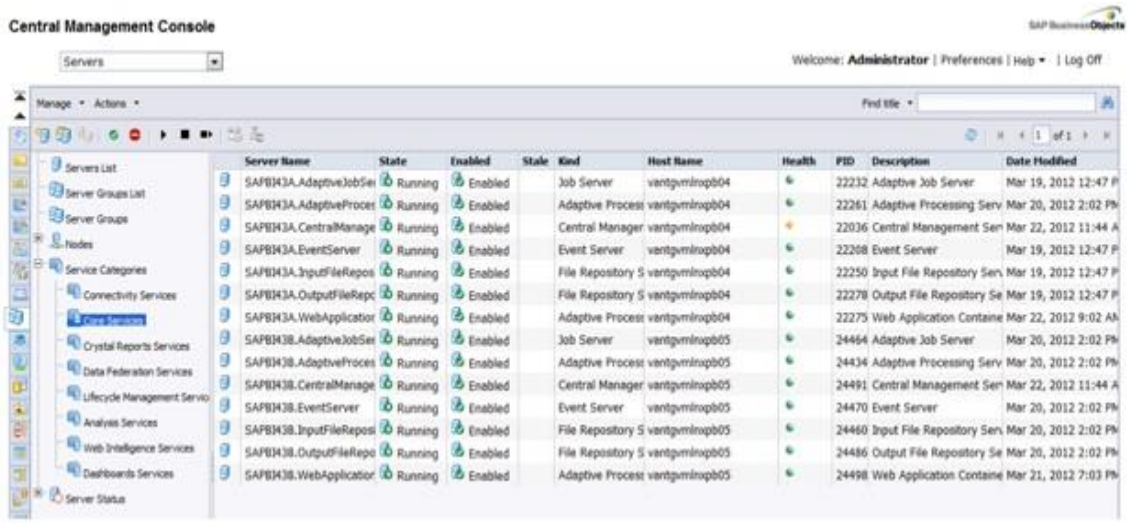
1. Log onto the Central Management Console as **Administrator**.



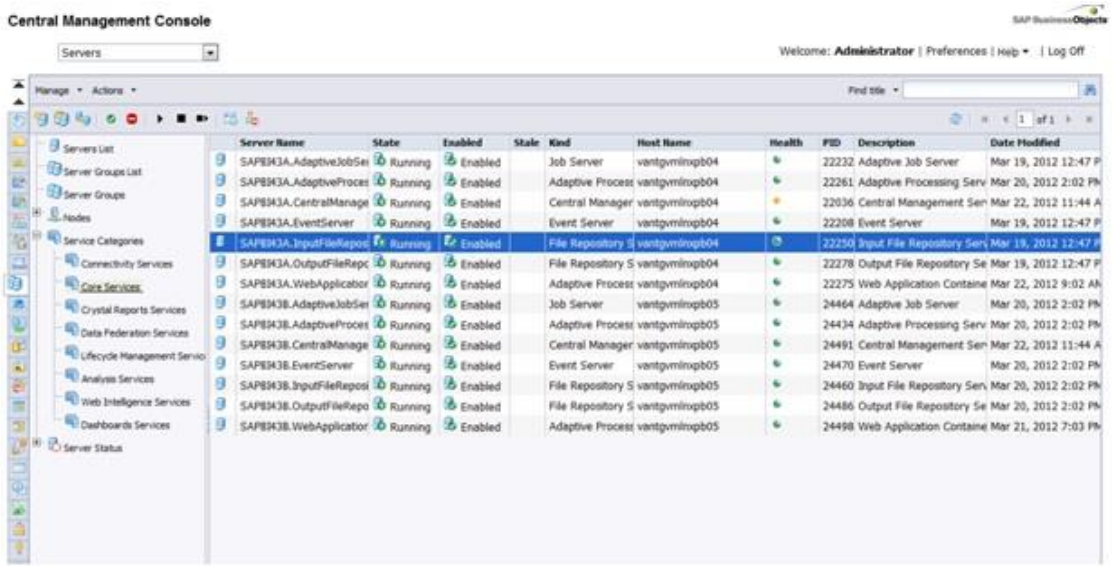
2. Click **Servers**.



3. Click **Core Services**.



4. Double-click **SAPBI43A.InputFileRepository**.



5. Under the "Input Filestore Service" section, enter the following text in the File Store Directory field:
/opt/sap/bi4/bi43pbfrs/frsinput

Input Filestore Service

Use Configuration Template

File Store Directory:	/opt/sap/bi4/bi43pbfrs/frsinput
Temporary Directory:	%DefaultInputFRSDir%/temp
Maximum Idle Time (minutes):	10
Maximum Retries for File Access:	1

Restore System Defaults

Set Configuration Template

6. Enter the following text in the Temporary Directory field:
   /opt/sap/bi4/bi43pbfrs/frsinput/temp

Input Filestore Service

Use Configuration Template

File Store Directory:	/opt/sap/bi4/bi43pbfrs/frsinput
Temporary Directory:	/opt/sap/bi4/bi43pbfrs/frsinput/tem
Maximum Idle Time (minutes):	10
Maximum Retries for File Access:	1

Restore System Defaults

Set Configuration Template

Click **Save and Close**.

7. Repeat steps 4 to 6 for **SAPBI43B.InputFileRepository**.

8. Repeat steps 4 to 6 for
   the **SAPBI43A.OutputFileRepository** and **SAPBI43B.OutputFileRepository** service
   s as well. Ensure that the following root path is used:
   /opt/sap/bi4/bi43pbfrs/frsoutput
9. Restart each of the modified servers to for the changes to take effect.
10. Enable all servers from within the CMC or with the following command line
    in lnxpb04 or lnxpb05:
    > ./ccm.sh -enable all -username Administrator -password Pattern123

You have successfully updated the input and output FRS in the CMC.

Setup with Samba

See the sections **To set up Samba on Linux servers** and **To create a Windows-shared folder and a new user** in the BusinessObjects XI Release 2 Pattern Book for Linux to set up the file repositories on a Red Hat server using Samba.

Application Server

In this pattern, we set up two application server instances running Tomcat 7.0.25 and cluster them for session replication and failover. The Application Server instances use Java 1.6.0_31 as the JDK.

The following topics provide step-by-step instructions on setting up the application servers:

- Setting up Linux Pattern Application Server 1
- Setting up Linux Pattern Application Server 2
- Installing the BIP web tier
- Configuring the Linux Pattern Application Server cluster

Setting up Linux Pattern Application Server 1

Tomcat is an open-source web server and servlet container developed by the Apache Software Foundation. At the time of this writing, the latest major release of Tomcat is version 7. New features in Tomcat 7 include security improvements that prevent cross-site scripting attacks and session fixation, as well as improved memory leak detection and prevention.

A complete write up of Tomcat 7 and its new features are described in Top 7 Features in Tomcat 7: The New and the Improved.

You will set up the first application server on lnxpb02.

1. Log into lnxpb02 as **root** to fulfill the prerequisites of the Tomcat installation.
2. Create a directory to store the Java SDK needed to run Tomcat. Run the following command:
   > mkdir -p /software/java
3. Download the latest version of Java 6 to /software/java from the Java SE Downloads website. Select **Accept License** Agreement and then choose the Linux x64 (RPM) version to download. In our case, we downloaded jdk-6u31-linux-x64-rpm.bin.

   Information: In this pattern, we are using version 1.6.0_31 of Java 6. Replace this version number with your own version of Java 6.

4. Change to the java directory and install the JDK. Run the following commands:
   > cd /software/java

> chmod 755 jdk-6u31-linux-x64-rpm.bin
> ./jdk-6u31-linux-x64-rpm.bin

The Java SDK installs to /usr/java/jdk1.6.0_31 where jdk1.6.0_31 represents the version installed.

5. Create a directory to store the Tomcat binary. Run the following command:
   > mkdir -p /software/tomcat7025
6. On the Tomcat 7 download site, under "Binary Distributions", download the latest tar.gz version of Tomcat 7 and save it to thetomcat7025 directory. Downloading the binary release saves the additional effort of compiling the source code.

   Information: In this pattern, we are using version 7.0.25 of Tomcat 7. Replace this version number with your own version of Tomcat 7.

7. Run the following command to verify that the package is correct:
   > cd /software/tomcat7025
   > md5sum apache-tomcat-7.0.25.tar.gz

   You will see the following output:

   ```
   2aa59d23555d641b20efad4aed86b693 apache-tomcat-7.0.25.tar.gz
   ```

8. Compare the published md5 checksum on the Tomcat site.

   You can find the checksum for the latest versions here. Click the latest version number, and then click **bin**. You can find the latest md5 checksum by accessing the md5 link next to the binary download.

   For example, the checksum for version 7.0.25 is found here:

   http://www.apache.org/dist/tomcat/tomcat-7/v7.0.25/bin/apache-tomcat-7.0.25.tar.gz.md5

   Note that this link does not work because version 7.0.25 is no longer the latest version. However, the checksum for the latest version has a similar path.

   On the Tomcat site, we see this line:

   ```
   From tomcat site: 2aa59d23555d641b20efad4aed86b693 *apache-tomcat-7.0.25.tar.gz
   ```

The checksum matches, so the download is valid.

9. Extract the tarball to the install directory under /opt. Run the following command:
   > tar -xvf apache-tomcat-7.0.25.tar.gz -C /opt
10. Create a user called **tomcat** with the password **Tomcat*123** by running the following commands:
   > useradd -s /bin/bash -m tomcat
   > passwd tomcat

Changing password for user tomcat. New password: **Tomcat*123** Retype new password: **Tomcat*123** passwd: all authentication tokens updated successfully.

For SUSE Only

In SUSE, a group with the same name is not automatically created when a user is added. We need to manually create the **tomcat** group and add our **tomcat** user to it by running the following commands:
> groupadd tomcat
> usermod -g tomcat tomcat

We can then check that the **tomcat** user is part of the **tomcat** group by running the following command:
> id tomcat

You will see output similar to the following:

uid=1004(tomcat) gid=1000(tomcat) groups=16(dialout),33(video),1000(tomcat)

11. Set the **tomcat** user as the owner and secure non-root access. Run the following commands:
   > chown -R tomcat /opt/apache-tomcat-7.0.25
   > chgrp -R tomcat /opt/apache-tomcat-7.0.25
   > chmod -R 755 /opt/apache-tomcat-7.0.25
12. Set the JAVA_HOME and CATALINA_HOME variables for the tomcat user. Run the following command:
   > vi /home/tomcat/.bash_profile

   Add the following information to the profile:

```
JAVA_HOME=/usr/java/jdk1.6.0_31
export JAVA_HOME
CATALINA_HOME=/opt/apache-tomcat-7.0.25
export CATALINA_HOME
PATH=$JAVA_HOME/bin:$PATH:$HOME/bin
export PATH
```

13. Switch to **tomcat** to test that Tomcat starts. Run the following commands:
    > su - tomcat
    > cd /opt/apache-tomcat-7.0.25/bin
    > ./startup.sh
14. Switch back to **root** to confirm the process is running and listening on TCP port 8080, which is the default port. Run the following commands:
    > su - root
    > cat /etc/services | grep -i 8080

    We see that the TCP port 8080 is registered under the **webcache** service:
    webcache 8080/tcp http-alt # WWW caching service
    webcache 8080/udp http-alt # WWW caching service
15. Run the following command to confirm that the process is listening correctly:
    > netstat -p -l | grep -i java
    You should see output similar to the following:

    tcp 0 0 **:webcache *:** LISTEN 16198/java

16. Run the following command to create a script to run Tomcat as a service:
    > cd /etc/init.d
    > vi tomcat7
    Add the following text to the script:

```
#!/bin/bash
#description: Tomcat Start Stop Restart
#processname: java
#chkconfig: 234 20 80
#source tomcat profile containing JAVA_HOME and
CATALINA_HOME env
. /home/tomcat/.bash_profile
case $1 in
start)
su - tomcat -c "sh $CATALINA_HOME/bin/startup.sh"
;;
```

```
stop)
su - tomcat -c "sh $CATALINA_HOME/bin/shutdown.sh"
;;
restart)
su - tomcat -c "sh $CATALINA_HOME/bin/shutdown.sh"
su - tomcat -c "sh $CATALINA_HOME/bin/startup.sh"
;;
esac
exit 0
```

This is a simple script that switches to the **tomcat** user and calls the startup process. Other scripts are widely available on the internet.

17. Run the following command to allow executing permissions on the script:
    > chmod 755 tomcat7
18. Run the following commands to configure the tomcat7 script to start upon machine boot:
    > chkconfig --add tomcat7
    > chkconfig --level 234 tomcat7 on
    > chkconfig --list tomcat7

    You will see the following output:

    ```
    tomcat7 0:off 1:off 2:on 3:on 4:on 5:off 6:off
    ```

19. Restart the service and confirm it is executing as the **tomcat** user. Run the following commands:
    > su - tomcat
    > service tomcat7 restart
    > ps -ef | grep java

    You will see output similar to the following:

    ```
    tomcat 16618 1 6 07:26 ? 00:00:03 /usr/java/jdk1.6.0_31/bin/java -Djava.util.logging.config.file=/opt/apache-tomcat-7.0.25/conf/logging.properties -Djava.util.logging.manager=org.apache.juli.ClassLoaderLogManager -Djava.endorsed.dirs=/opt/apache-tomcat-7.0.25/endorsed -classpath /opt/apache-tomcat-7.0.25/bin/bootstrap.jar:/opt/apache-tomcat-7.0.25/bin/tomcat-juli.jar -Dcatalina.base=/opt/apache-tomcat-7.0.25 -Dcatalina.home=/opt/apache-tomcat-7.0.25 -Djava.io.tmpdir=/opt/apache-tomcat-7.0.25/temp org.apache.catalina.startup.Bootstrap start
    ```

20. Test to see if we can get to the Apache Tomcat homepage.

You have successfully set up Application Server 1.

Setting up Linux Pattern Application Server 2

Setting up the second application server requires following the same steps from Setting up Application Server 1 (Linux). The only difference is that the machine name becomes lnxpb03.

1. Log into lnxpb03 as **root** to fulfill the prerequisites for the Tomcat installation.
2. Create a directory to store the Java SDK needed to run Tomcat. Run the following command:
   > mkdir -p /software/java
3. Download the latest version of Java 6 to /software/java from the Java SE Downloads website. Select **Accept License Agreement** and then choose the Linux x64 (RPM) version to download. In our case, we downloaded: jdk-6u31-linux-x64-rpm.bin.

   Information: In this pattern, we are using version 1.6.0_31 of Java 6. Replace this version number with your own version of Java 6.

4. Change to the java directory and install the JDK. Run the following commands:
   > cd /software/java
   > chmod 755 jdk-6u31-linux-x64-rpm.bin
   > ./jdk-6u31-linux-x64-rpm.bin

   The Java SDK installs to /usr/java/jdk1.6.0_31 where jdk1.6.0_31 represents the version installed.
5. Create a directory to store the Tomcat binary. Run the following command:
   > mkdir -p /software/tomcat7025
6. On the Tomcat 7 download site, under "Binary Distributions", download the latest tar.gz version of Tomcat 7 and save it to the tomcat7025 directory. Downloading the binary release saves the additional effort of compiling the source code.

   Information: In this pattern, we are using version 7.0.25 of Tomcat 7. Replace this version number with your own version of Tomcat 7.

7. Run the following command to verify that the package is correct:

   > cd /software/tomcat7025

   > md5sum apache-tomcat-7.0.25.tar.gz

   You will see the following output:

   ```
   2aa59d23555d641b20efad4aed86b693 apache-tomcat-7.0.25.tar.gz
   ```

8. Compare the published md5 checksum on the Tomcat site.

   You can find the checksum for the latest versions here. Click the latest version number, and then click **bin**. You can find the latest md5 checksum by accessing the md5 link next to the binary download.

   For example, the checksum for version 7.0.25 is found here:

   http://www.apache.org/dist/tomcat/tomcat-7/v7.0.25/bin/apache-tomcat-7.0.25.tar.gz.md5

   Note that this link does not work because version 7.0.25 is no longer the latest version. However, the checksum for the latest version has have a similar path.

   On the Tomcat site, we notice this line:

From tomcat site: 2aa59d23555d641b20efad4aed86b693 *apache-tomcat-7.0.25.tar.gz

   The checksum matches, so the download is valid.

9. Extract the tarball to the install directory under /opt. Run the following command:
   > tar -xvf apache-tomcat-7.0.25.tar.gz -C /opt

10. Create a user called **tomcat** with the password **Tomcat*123** by running the following commands:
    > useradd -s /bin/bash -m tomcat
    > passwd tomcat

Changing password for user tomcat. New password: **Tomcat*123** Retype new password: **Tomcat*123** passwd: all authentication tokens updated successfully.

    For SUSE Only
    In SUSE, a group with the same name is not automatically created when a user is added. We need to manually create the **tomcat** group and add our **tomcat** user to it by running the following commands:
    > groupadd tomcat
    > usermod -g tomcat tomcat

    We can then check that the **tomcat** user is part of the **tomcat** group by running the following command:

> id tomcat

You will see output similar to the following:

```
uid=1004(tomcat) gid=1000(tomcat)
groups=16(dialout),33(video),1000(tomcat)
```

11. Set the tomcat user as the owner and secure non-root access. Run the following commands:
    > chown -R tomcat /opt/apache-tomcat-7.0.25
    > chgrp -R tomcat /opt/apache-tomcat-7.0.25
    > chmod -R 755 /opt/apache-tomcat-7.0.25
12. Set the JAVA_HOME and CATALINA_HOME variables for the **tomcat** user. Run the following command:
    > vi /home/tomcat/.bash_profile

    Add the following information to the profile:

```
JAVA_HOME=/usr/java/jdk1.6.0_31
export JAVA_HOME
CATALINA_HOME=/opt/apache-tomcat-7.0.25
export CATALINA_HOME
PATH=$JAVA_HOME/bin:$PATH:$HOME/bin

export PATH
```

13. Switch to **tomcat** to test that Tomcat starts. Run the following commands:
    > su - tomcat
    > cd /opt/apache-tomcat-7.0.25/bin
    > ./startup.sh
14. Switch back to root to confirm the process is running and listening on TCP port 8080, which is the default port. Run the following commands:

    > su - root

    > cat /etc/services | grep -i 8080

    We see that the TCP port 8080 is registered under the webcache service:

    webcache 8080/tcp http-alt # WWW caching service

    webcache 8080/udp http-alt # WWW caching service

15. Run the following command to confirm that the process is listening correctly:
> netstat -p -l | grep -i java

You should see output similar to the following:

```
tcp 0 0 :webcache *: LISTEN 16198/java
```

16. Run the following command to create a script to run Tomcat as a service:
> cd /etc/init.d
> vi tomcat7

Add the following text to the script:

```
#!/bin/bash
#description: Tomcat Start Stop Restart
#processname: java
#chkconfig: 234 20 80
#source tomcat profile containing JAVA_HOME and
CATALINA_HOME env
. /home/tomcat/.bash_profile
case $1 in
start)
su - tomcat -c "sh $CATALINA_HOME/bin/startup.sh"
;;
stop)
su - tomcat -c "sh $CATALINA_HOME/bin/shutdown.sh"
;;
restart)
su - tomcat -c "sh $CATALINA_HOME/bin/shutdown.sh"
su - tomcat -c "sh $CATALINA_HOME/bin/startup.sh"
;;
esac
exit 0
```

This is a simple script that switches to the **tomcat** user and calls the startup process. Other scripts are widely available on the internet.

17. Run the following command to allow executing permissions on the script:
> chmod 755 tomcat7

18. Run the following commands to configure the tomcat7 script to start upon machine boot:
> chkconfig --add tomcat7
> chkconfig --level 234 tomcat7 on
> chkconfig --list tomcat7

You will see the following output:

```
tomcat7 0:off 1:off 2:on 3:on 4:on 5:off 6:off
```

19. Restart the service and confirm it is executing as **tomcat** user. Run the following commands:
> su - tomcat
> service tomcat7 restart
> ps -ef | grep java

You will see output similar to the following:

```
tomcat 16618 1 6 07:26 ? 00:00:03 /usr/java/jdk1.6.0_31/bin/java -Djava.util.logging.config.file=/opt/apache-tomcat-7.0.25/conf/logging.properties -Djava.util.logging.manager=org.apache.juli.ClassLoaderLogManager -Djava.endorsed.dirs=/opt/apache-tomcat-7.0.25/endorsed -classpath /opt/apache-tomcat-7.0.25/bin/bootstrap.jar:/opt/apache-tomcat-7.0.25/bin/tomcat-juli.jar -Dcatalina.base=/opt/apache-tomcat-7.0.25 -Dcatalina.home=/opt/apache-tomcat-7.0.25 -Djava.io.tmpdir=/opt/apache-tomcat-7.0.25/temp org.apache.catalina.startup.Bootstrap start
```

20. Test to see if we can get to Apache Tomcat homepage.

You have successfully set up Application Server 2.

Installing the BIP web tier

By installing the BIP web tier on each application server machine, we ensure that the WDeploy tool is available to build the SAP web applications on each server individually. Furthermore, this allows you to apply SAP patches directly to the machine to that ensure web applications are patched correctly.

It is also possible to deploy the web applications without installing the BIP web tier. Complete instructions can be found in the Web Application Deployment Guide for Unix (BI 4.0 FP03). Use this document as a reference throughout the remainder of this section.

1. Log into lnxpb02 as **tomcat**.

   Next, you will need to update the Tomcat heap size per the requirements on page 24 of the Web Application Deployment Guide.

It is recommended that you change the heap size and maximum perm size settings of your JVM to the following:
-Xms128m -Xmx2048m -XX:MaxPermSize=512m

For example, if you are using Tomcat, your modified settings would look like this:
JAVA_OPTS="-Xms128m -Xmx2048m -XX:MaxPermSize=512m"

The Tomcat 7 documentation suggests you set the heap size through the environment variable CATALINA_OPTS instead.

```
#CATALINA_OPTS (Optional) Java runtime options
used when the "start",
# "run" or "debug" command is executed.
# Include here and not in JAVA_OPTS all options,
that should
# only be used by Tomcat itself, not by the stop
process,
# the version command etc.
# Examples are heap size, GC logging, JMX ports
etc.
```

We will update the Tomcat heap size using CATALINA_OPTS.

2. Modify the catalina startup script to set the correct heap size. Run the following commands:
   > cd /opt/apache-tomcat-7.0.25/bin
   > cp catalina.sh catalina.sh.bak
   > vi catalina.sh
3. Locate the following line:

```
# OS specific support. $var_must_be set to either true or false.
```

Insert the updated CATALINA_OPTS line immediately above it:
CATALINA_OPTS="-Xms128m -Xmx2048m -XX:MaxPermSize=512m"
The section should now look like this:

```
CATALINA_OPTS="-Xms128m -Xmx2048m -XX:MaxPermSize=512m"
# OS specific support. $var _must_ be set to either true or false.
```

4. In the same file (catalina.sh), echo CATALINA_OPTS during the startup process to confirm that it has been set correctly. Enter the following to search for the correct section:
   /Using CATALINA_HOME
   Insert the following line:
   echo "Using CATALINA_OPTS: $CATALINA_OPTS"
   Save and exit the file.
5. Restart Tomcat and confirm that the max heap size is set correctly. Run the following command:
   > service tomcat7 restart

   Information: Depending on your Linux version, you may have to run this command as the root user. Here is a simple command to do this without having to open a new shell:
   > su - -c "service tomcat7 restart"

```
[tomcat@vantgvmlnxpb02 ~]$ service tomcat7 restart
Password:
Using CATALINA_BASE:   /opt/apache-tomcat-7.0.25
Using CATALINA_HOME:   /opt/apache-tomcat-7.0.25
Using CATALINA_OPTS:   -Xms128m -Xmx2048m -XX:MaxPermSize=512m
Using CATALINA_TMPDIR: /opt/apache-tomcat-7.0.25/temp
Using JRE_HOME:        /usr/java/jdk1.6.0_31
Using CLASSPATH:       /opt/apache-tomcat-7.0.25/bin/bootstrap.jar:/opt/apache-t
omcat-7.0.25/bin/tomcat-juli.jar
```

6. Confirm the heap size also shows up on the command line of the process. Run the following command:

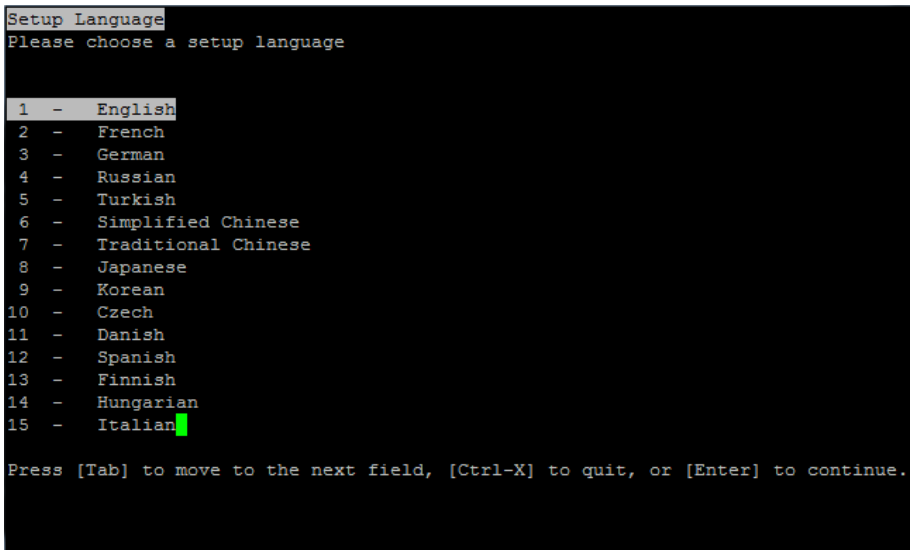
   > ps -ef | grep -i java

```
[tomcat@vantgvmlnxpb02 ~]$ ps -ef | grep java
tomcat   14379     1 10 11:26 ?        00:00:09 /usr/java/jdk1.6.0_31/bin/java -
Djava.util.logging.config.file=/opt/apache-tomcat-7.0.25/conf/logging.properties
 -Dlog4j.debug -Djava.util.logging.manager=org.apache.juli.ClassLoaderLogManager
 -Xms128m -Xmx2048m -XX:MaxPermSize=512m -Djava.endorsed.dirs=/opt/apache-tomcat
-7.0.25/endorsed -classpath /opt/apache-tomcat-7.0.25/bin/bootstrap.jar:/opt/apa
che-tomcat-7.0.25/bin/tomcat-juli.jar -Dcatalina.base=/opt/apache-tomcat-7.0.25
-Dcatalina.home=/opt/apache-tomcat-7.0.25 -Djava.io.tmpdir=/opt/apache-tomcat-7.
0.25/temp org.apache.catalina.startup.Bootstrap start
```

7. **For Red Hat Only**
   Install the required packages for running the BIP installation. Run the following commands:
   > su - root
   > yum install glibc-2.12-1.47.el6_2.5.i686
   > yum install compat-libstdc++-33-3.2.3-69.el6.i686
8. The next step assumes you have already downloaded the SAP BusinessObjects BI Plaform 4.0 FP03 installation media to the machine. Visit the SAP Software Download Center to download the media if you have not done so already. Store them in the user home directory.

   Information: The downloaded package is a multi-spanning RAR archive. Please use SAP Note 886535 for instructions on how to properly extract it on Linux.

9. Change to the directory containing the BI Platform 4.0 FP03 installation files and launch the setup. In this case, the install is located in /home/tomcat. Run the following commands:
   > cd /home/tomcat
   > ./setup.sh
   Proceed through the installer, using the following screenshots as a reference.
10. Press Enter.



11. Specify the Destination Folder for the web tier and press Enter. Here we chose a subdirectory called bi4 located in the Tomcat install directory.

```
Specify the Destination Folder
The destination folder is where the product will be installed. Please enter the
full path.

Destination Folder
[/opt/apache-tomcat-7.0.25/bi4                                    ]

Press [Tab] to move to the next field, [Ctrl-B] to go back, [Ctrl-X] to quit, or
 [Enter] to continue.
```

12. Confirm the necessary prerequisites have been met and then press Enter. In a web tier installation, installing a system database is not necessary. Therefore, we can proceed based on the success of the remaining items.

```
Prerequisite check
Summary of any missing critical or optional prerequisites.


Failed: Integrated database - home directory (Optional)
        Information: DB2 requires 755 permissions to be set in the user's
home directory.  Please set the permissions if you wish to install the
integrated DB2 database.
Failed: Integrated database - user and group (Optional)
        Information: The user group naming fails one of DB2's restrictions
or insufficient kernel parameters.  Please go to
http://publib.boulder.ibm.com/infocenter/db2luw/v9r7 and search 'User ID
restrictions' or 'Kernel parameters' for details.
Succeeded: Information Platform Services not installed (Critical)
Succeeded: Operating system patch level (Optional)
Succeeded: BI platform server 4.x not present (Critical)
Succeeded: Integrated database - directories (Optional)
Succeeded: Integrated database - gunzip (Optional)
Succeeded: Disk space in /tmp (Critical)

Press [Tab] to move to the next field, [Ctrl-X] to quit, or [Enter] to continue.
```

13. Acknowledge the warning and then press Enter.

```
Welcome to the installation wizard for SAP BusinessObjects BI platform 4.0



WARNING: This program is protected by copyright law and international
treaties.


Unauthorized reproduction or distribution of this program, or any portion
of it, may result in severe civil and criminal penalities, and will be
prosecuted to the maximum extent possible under law.









Press [Tab] to move to the next field, [Ctrl-B] to go back, [Ctrl-X] to quit, or
 [Enter] to continue.
```

14. Read the license agreement and then press Enter.

```
License Agreement
You must agree to the licensing conditions to proceed.


SOFTWARE LICENSE AGREEMENT




IMPORTANT-READ CAREFULLY: THIS IS A LEGAL AGREEMENT BETWEEN YOU AND SAP FOR
THE SAP SOFTWARE ACCOMPANYING THIS AGREEMENT, WHICH MAY INCLUDE COMPUTER
SOFTWARE, ASSOCIATED MEDIA, PRINTED MATERIALS AND ONLINE OR ELECTRONIC
DOCUMENTATION (âSOFTWAREâ
                          THE SOFTWARE, YOU MUST READ, ACKNOWLEDGE AND ACCEPT THE
 TERMS AND
CONDITIONS OF THE SOFTWARE LICENSE AGREEMENT THAT FOLLOWS (âAGREEMENTâ
                                                                      YOU DO NOT
 ACCEPT THE TERMS AND CONDITIONS OF THE AGREEMENT, YOU MAY
RETURN, WITHIN THIRTY (30) DAYS OF PURCHASE, THE SOFTWARE TO THE PLACE YOU
OBTAINED IT FOR A FULL REFUND.<X> to not accept
```

15. Type in the Product Keycode and then press Enter.

16. Leave the English language pack selected and then press Enter.

```
Choose Language Packs
A language pack allows a user to interact with the product in a specific languag
e.

[X]  English
[ ]  Norwegian
[ ]  Turkish
[ ]  Finnish
[ ]  Italian
[ ]  Hungarian
[ ]  Slovak
[ ]  Korean
[ ]  Portuguese
[ ]  Japanese
[ ]  Traditional Chinese
[ ]  Romanian
[ ]  Spanish
[ ]  Czech
[ ]  Swedish

Press [Space] or [X] to select or deselect a language pack. Press [Ctrl-B] to go
 back, [Ctrl-X] to quit, or [Enter] to continue.
```

17. Select **User install** and then press **Enter**.

```
Select a user install or a system install
System install requires root access to run initialization scripts after install


 1  -   User install - regular SAP BusinessObjects BI platform installation
 2  -   System install - user install plus system initialization scripts

Press [Tab] to move to the next field, [Ctrl-B] to go back, [Ctrl-X] to quit, or
 [Enter] to continue.
```

18. Select **Web Tier** and then press Enter.

```
Choose Install Type
Select one of the options below.


 1  -   Full
 2  -   Custom / Expand
 3  -   Web Tier



Press [Tab] to move to the next field, [Ctrl-B] to go back, [Ctrl-X] to quit, or
 [Enter] to continue.
```

19. Since we are using a preinstalled Java Application Server (Tomcat 7), uncheck the integrated Tomcat 6.0 option. Press Enter.

```
Select Features
Select the features that you want to install.


-[~] Instances
  -[~] WebTier
      [X] Java Web Applications
      [ ] Tomcat 6.0



Press [Space] to expand the feature tree, or [X] to select or deselect a feature
.  Press [Ctrl-B] to go back, [Ctrl-X] to quit, or [Enter] to continue.
```

20. Type lnxpb04 as the CMS Name and provide the CMS Port and administrative credentials. Press Enter.

```
Existing CMS Deployment Information
Specify the CMS and Administrator logon information of your existing CMS deploym
ent.

CMS Name
[vantgvmlnxpb04                                                  ]
CMS Port
[6400  ]
User
[Administrator                                                   ]
Password
[*********                                                       ]



Press [Tab] to move to the next field, [Ctrl-B] to go back, [Ctrl-X] to quit, or
 [Enter] to continue.
```

21. Choose **Do not integrate connectivity to Introscope Enterprise Manager** and then press **Enter**.

```
Introscope Integration
Enable connectivity to Introscope Enterprise Manager.


 1  -   Do not integrate connectivity to Introscope Enterprise Manager.
 2  -   Integrate connectivity to Introscope Enterprise Manager. You will be
        prompted for information.



Press [Tab] to move to the next field, [Ctrl-B] to go back, [Ctrl-X] to quit, or
 [Enter] to continue.
```

22. Press **Enter** to start the installation.

```
Start Installation

Are you ready to have the SAP BusinessObjects BI platform 4.0 FP3
Installation Wizard begin the installation?

Press [Tab] to move to the next field, [Ctrl-B] to go back, [Ctrl-X] to quit, or
 [Enter] to continue.
```

23. Complete the installation to begin the post-installation steps.

```
Post Installation Steps
Post Installation Instructions:

Java web applications and web services have not yet been deployed to a Web
Application Server. Please run the wDeploy tool to deploy the Java web
applications and web services. The WDeploy tool is located in:
/opt/apache-tomcat-7.0.25/bi4//sap_bobj/enterprise_xi40/wdeploy/wdeployGUI.
sh

Define the default viewer URL for OpenDocument. This machine has not been
registered as the default web application server for handling document
viewing requests. If it has not been configured prior to installation, it
may be necessary to register this machine with the CMS as the default web
application server. The OpenDocument properties page can be accessed via
the Central Management Console.

To access the Monitoring Tool in order to run diagnostic tests, logon to
the Central Management Console (CMC), click on the "Monitoring" button, and

Installation is complete. Please press Enter to continue
```

Document Reference: The following steps come from Section 4.5.2 of the Web Application Deployment Guide for Unix. Subsection 4.5.2.3 contains the relevant steps for Tomcat 6 and Tomcat 7.

24. Use the WDeploy tool to build and deploy the BIP web applications. Run the following commands:
    > cd /opt/apache-tomcat-7.0.25/bi4/sap_bobj/enterprise_xi40/wdeploy/conf/
    > cp config.tomcat7 config.tomcat7.bak
    > vi config.tomcat7
25. In the vi editor, modify the as_dir property to reflect the local Tomcat installation.
    Change the default as_dir property. Currently, it looks like this:
    as_dir=C:\Program Files\Apache Software Foundation\Tomcat 7.0
    Modify the property to this:
    as_dir=/opt/apache-tomcat-7.0.25
    Save and close the file.
26. Run the following commands to build the web applications:
    > cd ..
    > ./wdeploy.sh tomcat7 predeployall
    Upon completion, a message should be returned indicating success and the amount of time taken. It should look similar to the following:

    ```
    BUILD SUCCESSFUL
    Total time: 5 minutes 26 seconds
    ```

27. Run the following command to deploy the web applications:
    > ./wdeploy.sh tomcat7 deployonlyall

    Upon completion of this step, you should see a message similar to the following:

    ```
    BUILD SUCCESSFUL
    Total time: 2 minutes 27 seconds
    ```

28. Test the deployment to ensure the web applications have deployed successfully

You have successfully installed the BIP web tier.

Configuring the Linux Pattern Application Server cluster

Tomcat 7 supports clustering 2 or more application servers to provide session replication and failover functionality. In addition, BI platform sessions are serialized, which means the state of a user session can fail over seamlessly to another instance of Tomcat without the users noticing. If a user navigates several levels into the folder hierarchy within BI launch pad, and the application server instance he is connected to crashes, a correctly configured application server cluster should enable him to continue his existing navigation path without being redirected to the login page or to the root folder.

You can find a comprehensive "how-to" for configuring a Tomcat 7 cluster in Clustering/Session Replication HOW-TO.

1. Log into lnxpb02 as **tomcat**.
2. Confirm Multicast is running on the machine. Tomcat uses Multicast to monitor cluster heartbeat. Run the following command:
   > ifconfig

   The output should specifically mention MULTICAST in the properties. For example:

   ```
   eth0 Link encap:Ethernet HWaddr 00:50:56:8E:04:31
   inet addr:10.165.28.124 Bcast:10.165.31.255
   Mask:255.255.252.0
   inet6 addr: fe80::250:56ff:fe8e:431/64 Scope:Link
   UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
   ```

3. Switch to the **root** user and then add a local Multicast route to the network interface eth0. Run the following commands:
   > su - root
   > route add -host 228.0.0.4 dev eth0
4. Switch back to the **tomcat** user and update the server.xml file to enable clustering. Run the following commands:
   > su - tomcat
   > cd /opt/apache-tomcat-7.0.25/conf
   > cp server.xml server.xml.bak
   > vi server.xml
   Search for "Cluster":
   /Cluster
   Locate the following line:

   ```
   <!--
   <Cluster
   className="org.apache.catalina.ha.tcp.SimpleTcpCluster"/>
   -->
   ```

   Replace the line with the following:

   ```
   <Cluster
   className="org.apache.catalina.ha.tcp.SimpleTcp
   Cluster"
   channelSendOptions="8">
   ```

```
<Manager
className="org.apache.catalina.ha.session.Delta
Manager"
expireSessionsOnShutdown="false" notifyListener
sOnReplication="true"/>

<Channel
className="org.apache.catalina.tribes.group.Gro
upChannel">

<Membership
className="org.apache.catalina.tribes.membershi
p.McastService"
address="228.0.0.4" port="45564" frequency="500
" dropTime="3000"/>

<Receiver
className="org.apache.catalina.tribes.transport
.nio.NioReceiver"
address="auto" port="4000" autoBind="100" selec
torTimeout="5000" maxThreads="6"/>

<Sender
className="org.apache.catalina.tribes.transport
.ReplicationTransmitter">

<Transport
className="org.apache.catalina.tribes.transport
.nio.PooledParallelSender"/>

</Sender>

<Interceptor
className="org.apache.catalina.tribes.group.int
erceptors.TcpFailureDetector"/>

<Interceptor
className="org.apache.catalina.tribes.group.int
erceptors.MessageDispatch15Interceptor"/>

</Channel>
```

```
<Valve
className="org.apache.catalina.ha.tcp.ReplicationValve" filter=""/>

<Valve
className="org.apache.catalina.ha.session.JvmRouteBinderValve"/>

<ClusterListener
className="org.apache.catalina.ha.session.JvmRouteSessionIDBinderListener"/>

<ClusterListener
className="org.apache.catalina.ha.session.ClusterSessionListener"/>

</Cluster>
```

This represents the default cluster configuration, which is expected to function properly in almost all cases. Cluster membership is defined by the Multicast address 228.0.0.4 and this value changes between independent clusters if you have several running on the same network. Session replication takes place over TCP/IP and uses port 4000 for communication.
Save and close the file.

5. Restart Tomcat and confirm the cluster is online. Run the following commands:
> service tomcat7 restart
> cat /opt/apache-tomcat-7.0.25/logs/catalina.out | grep -i cluster
You should see output similar to the following:

```
Mar 2, 2012 11:06:18 AM
org.apache.catalina.ha.tcp.SimpleTcpCluster startInternal
INFO: Cluster is about to start
INFO: Setting cluster mcast soTimeout to 500
INFO: Sleeping for 1000 milliseconds to establish cluster
membership, start level:4
INFO: Sleeping for 1000 milliseconds to establish cluster
membership, start level:8
```

6. Repeat steps 1-5 in lnxpb03 as **tomcat**.
   The output from catalina.out should have one additional component when the second cluster member starts. In this case, you should see the member join the cluster as follows:

```
Mar 2, 2012 11:11:39 AM
org.apache.catalina.ha.tcp.SimpleTcpCluster startInternal
INFO: Cluster is about to start
INFO: Setting cluster mcast soTimeout to 500
INFO: Sleeping for 1000 milliseconds to establish cluster
membership, start level:4
>> Mar 2, 2012 11:11:40 AM
org.apache.catalina.ha.tcp.SimpleTcpCluster memberAdded
INFO: Sleeping for 1000 milliseconds to establish cluster
membership, start level:8
```

The Tomcat cluster is now functional.

Apache

The following sections provide step-by-step instructions for the Apache web server setup:

- Installing Apache with SSL support
- Configuring the mod_jk connector
- Configuring Apache using the mod_ssl module
- Configuring the load balancer

Installing Apache with SSL support

1. Log into lnxpb01 as root.
2. Run the following command to create a directory named software on the machine:
   > mkdir /software
3. Download Apache 2.2.22 from the official website by clicking httpd-2.2.22.tar.gz and saving it to the software directory.
4. Download the Apache KEYS file to verify the integrity of the download files and then save it to the software directory.
   See Verifying Apache HTTP Server Releases for details about why this process is important.
5. Download the PGP signature for the httpd-2.2.22 package and save it to the software directory.
6. Run the following command to switch to the software directory:
   > cd /software
7. Run the following command to view all the files and subdirectories in

the software directory:
> ls –al

```
[root@vantgvmlnxpb01 software]# pwd
/software
[root@vantgvmlnxpb01 software]# ls -al
total 7416
drwxrwxr-x.  3 root root    4096 Mar 13 11:41 .
dr-xr-xr-x. 28 root root    4096 Mar  6 11:37 ..
drwxr-xr-x. 12 root root    4096 Mar 13 11:38 httpd-2.2.22
-rw-r--r--.  1 root root 7200529 Mar 13 11:38 httpd-2.2.22.tar.gz
-rw-r--r--.  1 root root     835 Mar 13 11:38 httpd-2.2.22.tar.gz.asc
-rw-r--r--.  1 root root  373101 Mar 13 11:38 KEYS
[root@vantgvmlnxpb01 software]#
```

8. Verify the integrity of the httpd source using the gpg command that comes standard with RHEL 6. Run the following commands:
> gpg --import KEYS
> gpg --verify httpd-2.2.22.tar.gz.asc

```
[root@vantgvmlnxpb01 Apache2.2.22]# gpg --verify httpd-2.2.22.tar.gz.asc
gpg: Signature made Wed 25 Jan 2012 02:27:28 PM PST using RSA key ID 60C5442D
gpg: Good signature from "William A. Rowe, Jr. <wrowe@rowe-clan.net>"
gpg:                 aka "William A. Rowe, Jr. <wrowe@apache.org>"
gpg:                 aka "William A. Rowe, Jr. <wrowe@vmware.com>"
gpg: WARNING: This key is not certified with a trusted signature!
gpg:          There is no indication that the signature belongs to the owner.
Primary key fingerprint: B1B9 6F45 DFBD CCF9 7401  9235 193F 180A B55D 9977
     Subkey fingerprint: 627B E9D7 D7C6 9D30 A2F5  B008 5593 BCA9 60C5 442D
```

On the Apache site, under the "Verify the integrity of the files" section, we notice this line:

httpd-2.2.22.tar.* are signed by William A Rowe Jr B55D9977(60C5442D)

The PGP signature in the file we downloaded matches this one.

9. Run the following command to extract the source from the httpd tarball:
> tar -xvf httpd-2.2.22.tar.gz

This creates a new directory under software containing the source code for the httpd distribution.

10. Before building the Apache source, fulfill the prerequisites for setting permissions on the ServerRoot directories described in Apache's Security Tips.
Run the following commands:
> mkdir /usr/local/apache
> cd /usr/local/apache
> mkdir bin conf logs
> chown 0 . bin conf logs

> chgrp 0 . bin conf logs
> chmod 755 . bin conf log

11. Run the following command to install the GCC C compiler needed to build Apache httpd:
    For Red Hat only
    > yum install gcc
    For SUSE only
    > zypper install gcc
12. Run the following command to install the zlib compression and development headers required to build mod_deflate:
    For Red Hat only
    > yum install zlib-devel

    For SUSE only
    > zypper install zlib-devel
13. Run the following command to install the OpenSSL development libraries required to build mod_ssl:
    For Red Hat only
    > yum install openssl-devel

    For SUSE only
    > zypper install openssl-devel

14. To build Apache, run the following command to change the directory:
    > cd /software/httpd-2.2.22
15. Configure the Apache source tree for the Linux platform and customize it to suit the pattern requirements.

    This is done using the script Configure located in the root directory of the distribution.

    For complete details regarding the Configure program, see configure - Configure the source tree.

    Run the following command:

    > ./configure --prefix=/usr/local/apache --with-mpm=worker --enable-mods-shared=all --enable-cache --enable-disk-cache --enable-mem-cache --enable-proxy --enable-proxy-ajp --enable-proxy-balancer --enable-proxy-http --enable-ssl

    The following list examines each segment of the command in more detail:

--prefix=/usr/local/apache specifies the directory in which Apache is installed.

--with-mpm=worker specifies the multi-process multi-threaded server Multi-Processing Module (MPM) that is a common selection for thread safe applications such as BI platform. For details on the available MPM, see Multi-Processing Modules (MPMs).

--enable-mods-shared=all builds all common Dynamic Shared Objects (DSO) for use with Apache. Though this increases the size of the distribution slightly it provides more flexibility in testing different web server configurations. For details on DSO support, see Dynamic Shared Object (DSO) Support.

--enable-cache --enable-disk-cache --enable-mem-cache enables disk- or memory-based caching of static resources. For details on mod_cache, see Apache Module mod_cache.

--enable-proxy --enable-proxy-ajp --enable-proxy-balancer --enable-proxy-http enables a variety of reverse proxy scenarios for use throughout the pattern. For details on mod_proxy, see Apache Module mod_proxy.

--enable-ssl builds the mod_ssl module, which allows web browsers to communicate with Apache over SSL. For details on mod_ssl, see Apache Module mod_ssl.

```
[root@vantgvmlnxpb01 httpd-2.2.22]# ./configure --prefix=/usr/local/apache --wit
h-mpm=worker --enable-mods-shared=all --enable-cache --enable-disk-cache --enabl
e-mem-cache --enable-proxy --enable-proxy-ajp --enable-proxy-balancer --enable-p
roxy-http --enable-ssl
checking for chosen layout... Apache
checking for working mkdir -p... yes
checking build system type... x86_64-unknown-linux-gnu
checking host system type... x86_64-unknown-linux-gnu
checking target system type... x86_64-unknown-linux-gnu

Configuring Apache Portable Runtime library ...

checking for APR... reconfig
configuring package in srclib/apr now
checking build system type... x86_64-unknown-linux-gnu
checking host system type... x86_64-unknown-linux-gnu
checking target system type... x86_64-unknown-linux-gnu
Configuring APR library
Platform: x86_64-unknown-linux-gnu
checking for working mkdir -p... yes
APR Version: 1.4.5
checking for chosen layout... apr
checking for gcc... gcc
checking for C compiler default output file name...
```

16. Run the following command to build the various parts that form the Apache package:
    > make
17. Run the following command to install the package in the configured directory:
    > make install
18. Run the following command to change the directory to the Apache install directory:
    > cd /usr/local/apache
19. Run the following command to view all of the files and subdirectories in this directory:
    > ls –al

```
[root@vantgvmlnxpb01 apache]# pwd
/usr/local/apache
[root@vantgvmlnxpb01 apache]# ls -al
total 68
drwxr-xr-x. 15 root root  4096 Feb 16 19:14 .
drwxr-xr-x. 13 root root  4096 Feb 16 16:26 ..
drwxr-xr-x.  2 root root  4096 Feb 16 19:45 bin
drwxr-xr-x.  2 root root  4096 Feb 16 19:45 build
drwxr-xr-x.  2 root root  4096 Feb 16 19:14 cgi-bin
drwxr-xr-x.  4 root root  4096 Feb 16 19:14 conf
drwxr-xr-x.  3 root root  4096 Feb 16 19:14 error
drwxr-xr-x.  2 root root  4096 Jan 25 14:24 htdocs
drwxr-xr-x.  3 root root  4096 Feb 16 19:14 icons
drwxr-xr-x.  2 root root  4096 Feb 16 19:45 include
drwxr-xr-x.  3 root root  4096 Feb 16 19:45 lib
drwxr-xr-x.  2 root root  4096 Feb 16 16:26 logs
drwxr-xr-x.  4 root root  4096 Feb 16 19:14 man
drwxr-xr-x. 14 root root 12288 Jan 25 14:26 manual
drwxr-xr-x.  2 root root  4096 Feb 16 19:45 modules
```

20. Run the following commands to finish securing httpd command from non-root users access:
    > chown 0 /usr/local/apache/bin/httpd
    > chgrp 0 /usr/local/apache/bin/httpd
    > chmod 511 /usr/local/apache/bin/httpd
21. Create a user called apache with the password Apache*123. Run the following commands:
    > useradd -s /bin/bash -m apache
    > passwd apache
    You are prompted to type the password for the user apache:

Changing password for user apache. New password: Apache*123 Retype new password: Apache*123 passwd: all authentication tokens updated successfully.

22. Run the following commands to make the Apache user the owner of the htdocs directory containing deployed web pages:
    > chown apache . htdocs
    > chgrp apache . htdocs
23. Run the following commands to back up and edit the httpd.conf file, which is the main configuration file for Apache:
    > cd /usr/local/apache/conf
    > cp httpd.conf httpd.conf.bak
    > vi httpd.conf
24. In the vi editor, configure the httpd process to run under the previously created User / Group Apache by modifying the corresponding directives. Change the User and Group properties to apache:

```
# If you wish httpd to run as a different user or group, you must run
# httpd as root initially and it will switch.
#
# User/Group: The name (or #number) of the user/group to run httpd as.
# It is usually good practice to create a dedicated user and group for
# running httpd, as with most system services.
#
User apache
Group apache
```

25. In the vi editor, configure the ServerName directive to match the DNS name and port for the server. Be sure to uncomment the line by removing the #:

```
# ServerName gives the name and port that the server uses to identify itself.
# This can often be determined automatically, but we recommend you specify
# it explicitly to prevent problems during startup.
#
# If your host doesn't have a registered DNS name, enter its IP address here.
#
ServerName vantgvmlnxpb01.pgdev.sap.corp:80
```

26. Save the file and close vi.
27. Run the following commands to create an Apache httpd service to ensure the web server starts when the machine starts up:
    > cd /etc/init.d
    > vi httpd

    Information: Apache may already be installed on your machine by default, so there may already exist an httpd file. If there is, move this file with the command > mv httpd httpdCopy.bak.

28. Add the following text to the /etc/init.d/httpd file you created:

```
#!/bin/bash
# description: Apache httpd Start Stop Restart
# processname: httpd
# chkconfig: 234 20 80
\\
# Define some variables

apachectl=/usr/local/apache/bin/apachectl
httpd=/usr/local/apache
pid=$httpd/logs/httpd.pid

case $1 in
start)
$apachectl \-k start
;;
stop)
$apachectl \-k stop
;;
restart)
$apachectl \-k restart
;;
esac
exit 0
```

Save and close the file.

29. Run the following command to grant executing rights to the httpd script:
> chmod 755 httpd

30. Run the following commands to configure the service to start upon machine boot and stop upon machine shutdown:
> chkconfig --add httpd
> chkconfig --level 234 httpd on
> chkconfig --list httpd

```
[root@vantgvmlnxpb01 init.d]# chkconfig --list httpd
httpd           0:off   1:off   2:on    3:on    4:on    5:off   6:off
```

31. Run the following commands to start the Apache service and confirm that it is running:
> service httpd start
> ps -ef | grep httpd

```
[root@vantgvmlnxpb01 init.d]# ps -ef | grep httpd
root     17580     1  0 18:56 ?        00:00:00 /usr/local/apache/bin/httpd -k start
apache   17581 17580  0 18:56 ?        00:00:00 /usr/local/apache/bin/httpd -k start
apache   17582 17580  0 18:56 ?        00:00:00 /usr/local/apache/bin/httpd -k start
apache   17583 17580 10 18:56 ?        00:00:02 /usr/local/apache/bin/httpd -k start
apache   17588 17580  2 18:56 ?        00:00:00 /usr/local/apache/bin/httpd -k start
```

You have successfully installed Apache.

Configuring the mod_jk connector

Mod_jk is an Apache-to-Tomcat connector that enables software load balancing, failover, and a variety of performance tuning options that are covered in other sections of this pattern. The AJP13 protocol is used for mod_jk communications between Apache and Tomcat. Connections are made using the TCP protocol. You can find complete details regarding mod_jk Configuration and AJP13 Protocol Reference on the Apache Software Foundation website.

1. Log into lnxpb01 as root.
2. Run the following command to create a directory under software to store the mod_jk source and associated files:
   > mkdir /software/mod_jk
3. Download the latest version of the mod_jk source in tar.gz format and save it to the mod_jk directory.

   Information: In the following steps, we are using version 1.2.32 of mod_jk. Replace this version number with your own version of mod_jk.

4. Download the Tomcat Connectors KEYS and save it to the mod_jk directory.
5. Download the .tar.gz.asc version of the PGP Signature and save it to the mod_jk directory.
6. Verify the source using the instructions on the Apache site.
   Run the following commands:
   > cd /software/mod_jk
   > gpg --import KEYS
   > gpg --verify tomcat-connectors-1.2.32-src.tar.gz.asc

   You will see the following output:

```
gpg: Signature made Fri 01 Jul 2011 10:47:47 PM PDT using DSA key ID
564C17A3 gpg:
Good signature from "Mladen Turk (*** DEFAULT SIGNING KEY ***)
<mturk@apache.org>
```

On the Tomcat Connectors site, under the "Verify the integrity of the files" section, we notice this line:
tomcat-connectors-1.2.32-src.* is signed by Mladen Turk (564C17A3).
The signing keys match.

7. Install a C++ compiler to build the mod_jk from source. Run the following command:
   For Red Hat only
   > yum install gcc-c++

   For SUSE only
   > zypper install gcc-c++
8. Run the following command to extract the mod_jk source:
   > tar -xvf tomcat-connectors-1.2.32-src.tar.gz
9. Change to the native directory and build mod_jk. Run the following commands:
   > cd tomcat-connectors-1.2.32-src/native
   > ./configure -with-apxs=/usr/local/apache/bin/apxs
   > make
   > cp apache-2.0/mod_jk.so /usr/local/apache/modules/

   apxs is the Apache Extension Tool that enables building of shared modules such as mod_jk. It is part of the Apache installation built in To configure Apache using the mod_ssl module.
10. Configure mod_jk for simple forwarding of requests to a single Tomcat instance. Run the following commands:
    > cd /usr/local/apache/conf
    > /usr/local/apache/bin/apachectl -k stop
    > cp httpd.conf httpd.conf.bak
    > vi httpd.conf

    Search for "LoadModule":
    /LoadModule

    Scroll down to the last entry in the Load Module section and insert the following lines:

```
# Load mod_jk to forward AJP requests to Tomcat
LoadModule jk_module modules/mod_jk.so
```

11. Go to the end of the httpd.conf file.
    You can use G key in the vi editor to jump directly to the last line.
12. Insert the following:

```
#====================Configure mod_jk==============
# Where to find workers.properties
# Update this to match your conf directory location where
we place workers.properties
JkWorkersFile conf/workers.properties
# Where to put jk shared memory
# Write shared memory to the logs directory
JkShmFile logs/mod_jk.shm
# Where to put jk logs
# Update this path to match your logs directory location
(put mod_jk.log next to access_log)
JkLogFile logs/mod_jk.log
# Set the jk log level [debug/error/info]
JkLogLevel info
# Select the timestamp log format
JkLogStampFormat "[%a %b %d %H:%M:%S %Y]"
JkMount /* ajp13
```

    This configures mod_jk with the location of the workers.properties file that directs Apache to forward certain requests to Tomcat.

    Initially we willll forward everything to Tomcat and fine-tune the configuration later in the pattern.

    Save and close the file.
13. Create a new file named workers.properties in the conf directory. Run the following command:
    > vi workers.properties
14. Add the following information to the workers.properties file:

```
# Define 1 worker using ajp13
worker.list=ajp13
# Set properties for worker1 (ajp13)
worker.ajp13.type=ajp13
worker.ajp13.host=vantgvmlnxpb02
worker.ajp13.port=8009
```

This configures a single worker, named ajp13, that forwards requests to lnxpb02 (Tomcat machine) on port 8009.

Save and close the file.

15. Restart Apache and verify that mod_jk is loaded correctly. Run the following commands:
    > /usr/local/apache/bin/apachectl -k start
    > cat /usr/local/apache/logs/mod_jk.log

    You will output similar to the following:

```
[Sat Feb 18 09:44:57 2012][18258:140216672573184] [info]
init_jk::mod_jk.c (3252): mod_jk/1.2.32 () initialized
[Sat Feb 18 09:44:57 2012][18259:140216672573184] [info]
init_jk::mod_jk.c (3252): mod_jk/1.2.32 () initialized
```

16. Try to access the Tomcat landing page through the Apache web server. The Tomcat Landing Page appears.

You have successfully configured the mod_jk connector.

Configuring Apache using the mod_ssl module

The openssl libraries needed to generate the server private key and an SSL certificate are present on the Red Hat system by default. This pattern book describes both using a self-signed certificate for testing purposes as well as requesting a certificate signed by a Corporate Certificate Authority (CA). Production use certificates should always come from a CA to ensure they are trusted by client browsers.

1. Log into lnxpb01 as root and run the following command to create a directory to store the SSL related files:
   > mkdir /usr/local/apache/conf/ssl
2. Run the following command to change to the ssl directory:
   > cd /usr/local/apache/conf/ssl
3. Run the following command to generate a private key with 2048-bit encryption:
   > openssl genrsa -des3 -out apachekey.pem 2048

4. Enter a strong password to protect the web server key pair.
A strong password contains at least eight characters, include numbers and/or punctuation, and not be a word in the dictionary.

```
[root@vantgvmlnxpb01 ssl]# openssl genrsa -des3 -out apachekey.pem 2048
Generating RSA private key, 2048 bit long modulus
................+++
.......................................................+++
e is 65537 (0x10001)
Enter pass phrase for apachekey.pem:
Verifying - Enter pass phrase for apachekey.pem:
[root@vantgvmlnxpb01 ssl]# ls
apachekey.pem
[root@vantgvmlnxpb01 ssl]#
```

5. Run the following command to generate a Certificate Signing Request (CSR) using the private key:

> openssl req -new -key apachekey.pem -out apache.csr
Provide the appropriate information when prompted. For example, in our pattern, we used the following information:

```
[root@vantgvmlnxpb01 ssl]# openssl req -new -key apachekey.pem -out apache.csr
Enter pass phrase for apachekey.pem:
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [XX]:CA
State or Province Name (full name) []:British Columbia
Locality Name (eg, city) [Default City]:Vancouver
Organization Name (eg, company) [Default Company Ltd]:SAP
Organizational Unit Name (eg, section) []:BIP
Common Name (eg, your name or your server's hostname) []:vantgvmlnxpb01.pgdev.sap.corp
Email Address []:

Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []:
An optional company name []:
```

The critical part of this step is to ensure that the common name attribute matches the fully qualified domain name (FQDN) of the web server. If it does not match, client browsers receive a warning when they try to access the BI platform environment using SSL.

6. Self-sign a certificate for testing purposes. This test certificate will be valid for 1 year (365 days). Run the following command:
> openssl x509 -req -days 365 -in apache.csr -signkey apachekey.pem -out apache.crt
Warning: Never use a self-signed certificate for production use
It is recommended that you use a commercial certificate for use in production environments. Self-signed certificates are

not trusted by client browsers, and cause problems for business users in the form of security warnings. Purchase a certificate from one of the commercial providers, such as Thawte or Verisign. You can also use a company-hosted Certificate Authority if one is available to you.

Enter the password for the private key and note the addition of the apache.csr certificate to the directory:

```
[root@vantgvmlnxpb01 ssl]# openssl x509 -req -days 365 -in apache.csr -signkey a
pachekey.pem -out apache.crt
Signature ok
subject=/C=CA/ST=British Columbia/L=Vancouver/O=SAP/OU=BIP/CN=vantgvmlnxpb01.pgd
ev.sap.corp
Getting Private key
Enter pass phrase for apachekey.pem:
[root@vantgvmlnxpb01 ssl]# ls
apache.crt  apache.csr  apachekey.pem
```

7. Make an unprotected version of the private key (apachekey.pem) that does not cause Apache to prompt for the password. Run the following command:
   > openssl rsa -in apachekey.pem -out server.key

8. Secure all files so only root has access.
   Run the following commands:
   > chmod 600 -Rf ./*
   > ls –al
   Information: This is a critical step because anyone obtaining this insecure key can decrypt the HTTPS traffic and defeat the purpose of using SSL.

```
total 24
drwxr-xr-x. 2 root root 4096 Mar 20 12:44 .
drwxr-xr-x. 5 root root 4096 Mar 19 16:01 ..
-rw-------. 1 root root 1273 Mar 20 12:39 apache.crt
-rw-------. 1 root root 1037 Mar 19 16:35 apache.csr
-rw-------. 1 root root 1751 Mar 19 16:05 apachekey.pem
-rw-------. 1 root root 1679 Mar 20 12:44 server.key
```

The following four files are in the directory:

apache.crt	Self-signed server certificate
apache.csr	Server certificate signing request

apachekey.pem	Protected private server key, which requires a password when starting Apache
server.key	Private server key, which does not require a password when starting Apache

9. Enable SSL for Apache by modifying the httpd-ssl.conf file. Run the following commands:
> cd /usr/local/apache/conf/extra
> cp httpd-ssl.conf httpd-ssl.conf.bak
> vi httpd-ssl.conf

Search for "<VirtualHost _default_:443>":
/<VirtualHost _default_:443>

Find the following section:

```
DocumentRoot "/usr/local/apache/htdocs"
ServerName www.example.com:443
ServerAdmin you@example.com
ErrorLog "/usr/local/apache/logs/error_log"
TransferLog "/usr/local/apache/logs/access_log"
```

Modify the section so it looks like the following:

```
DocumentRoot "/usr/local/apache/htdocs"
ServerName vantgvmlnxpb01.pgdev.sap.corp:443
ServerAdmin admin@vantgvmlnxpb01.pgdev.sap.corp
ErrorLog "/usr/local/apache/logs/error_log"
TransferLog "/usr/local/apache/logs/access_log"
JkMount /lbstatus lbstatus
JkMount /* ajp13
```

The following table examines the modified lines in more detail:

DocumentRoot	htdocs directory in Apache
ServerName	FQDN and port for which SSL is enabled
ServerAdmin	Email address for the Server Administrator
JkMount	Directs SSL requests to be sent to the mod_jk connector

10. Update the location of the certificate file. Search for "SSLCertificateFile":
/SSLCertificateFile

    Change the parameter so it looks like the following:
    SSLCertificateFile "/usr/local/apache/conf/ssl/apache.crt"
11. Update the path to the unprotected server private key. Search for "SSLCertificateKeyFile":
/SSLCertificateKeyFile

    Change the parameter so it looks like the following:
    SSLCertificateKeyFile "/usr/local/apache/conf/ssl/server.key"

    Save the file and exit.

12. Run the following commands to include the httpd-ssl.conf file in the main configuration file:
> cd /usr/local/apache/conf/
> vi httpd.conf

    Search for "httpd-ssl.conf":
    /httpd-ssl.conf

    Uncomment the line:

```
#Include conf/extra/httpd-ssl.conf
```

    It now looks like this:

```
Include conf/extra/httpd-ssl.conf
```

    Save the file and exit.

13. Restart Apache to apply the changes. Run the following command:
> service httpd restart

14. Test the SSL capabilities by going to the URL https://vantgvmlnxpb01.pgdev.sap.corp.

    Information:
    You may receive a warning stating that the site certificate is not verified. This occurs with self-signed certificates, and you can proceed to the site. If you see the Tomcat Landing Page, then SSL is configured.

You have successfully configured Apache for SSL.

Configuring the load balancer

Mod_jk provides support for load balancing to deliver a robust, high availability solution for the BI platform web tier.
For a general "how-to" on load balancing with the Tomcat Connectors, see The Apache Tomcat Connector - Generic HowTo.

To configure load balancing with mod_jk, perform the following steps:

1. Log into lnxpb01 as root
2. Navigate to the Apache conf directory and update the workers.properties file. Run the following commands:
   > cd /usr/local/apache/conf
   > cp workers.properties workers.properties.bak
   > vi workers.properties

   Locate the following section:

```
# Define 1 worker using ajp13
worker.list=ajp13
# Set properties for worker1 (ajp13)
worker.ajp13.type=ajp13
worker.ajp13.host=vantgvmlnxpb02
worker.ajp13.port=8009
```

   Modify the section so it looks like the following:

```
# Name the Load Balancer ajp13 to leverage
wdeploy auto-config
worker.list=ajp13
worker.ajp13.type=lb
```

```
# Balance workers from each of the application
server nodes
worker.ajp13.balance_workers=vantgvmlnxpb02,van
tgvmlnxpb03

# Define the first member worker vantgvmlnxpb02
worker.vantgvmlnxpb02.type=ajp13
worker.vantgvmlnxpb02.host=vantgvmlnxpb02
worker.vantgvmlnxpb02.port=8009
# Define preferred failover
node for vantgvmlnxpb02
worker.vantgvmlnxpb02.redirect=vantgvmlnxpb03

# Define the second member worker
vantgvmlnxpb03
worker.vantgvmlnxpb03.type=ajp13
worker.vantgvmlnxpb03.host=vantgvmlnxpb03
worker.vantgvmlnxpb03.port=8009
# Define preferred failover
node for vantgvmlnxpb03
worker.vantgvmlnxpb03.redirect=vantgvmlnxpb02

# Define the status worker to monitor load
balancer
worker.list=lbstatus
worker.lbstatus.type=status
worker.lbstatus.mount=/lbstatus
```

Save and close the file.

3. Modify the server.xml file on each Tomcat node to match the worker names with the corresponding jvmRoute.
The purpose of this is to ensure mod_jk requests are routed to the correct Tomcat instance.

   a. Log into lnxpb02 as tomcat.

   b. Change to the Tomcat conf directory and modify the server.xml file. Run the following commands:
   > cd /opt/apache-tomcat-7.0.25/conf
   > cp server.xml server.xml.bak

> vi server.xml
> /jvmRoute

Locate the following line:
<Engine defaultHost="localhost">

Modify this line so it looks like the following:
<Engine defaultHost="localhost" jvmRoute="vantgvmlnxpb02">

c. Log into lnxpb03 as tomcat.

d. Change to the Tomcat conf directory and modify the server.xml file. Run the following commands:
> cd /opt/apache-tomcat-7.0.25/conf
> cp server.xml server.xml.bak
> vi server.xml

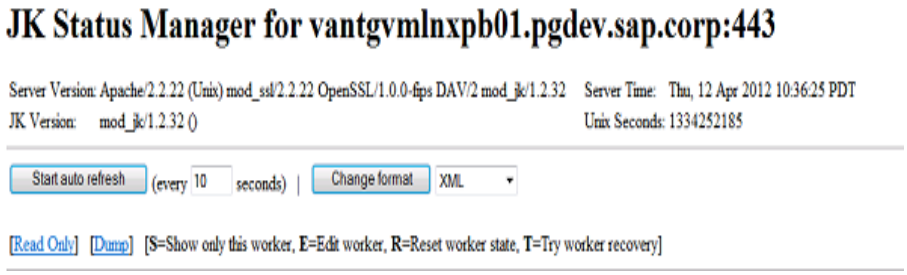
Search for "jvmRoute":
> /jvmRoute

Locate the following line:
<Engine defaultHost="localhost">

Modify this line so it looks like the following:
<Engine defaultHost="localhost" jvmRoute="vantgvmlnxpb03">

Save and close the file.

4. Run the following command to restart Tomcat on each server:
> service tomcat7 restart
5. Run the following command to restart Apache on the lnxpb01 machine:
> service httpd restart
6. Confirm that the load balancer is active by accessing the status URL https://vantgvmlnxpb01.pgdev.sap.corp/lbstatus.
This should return the JK Status Manager page, which contains useful metrics on the state of each load balancer worker.



You have successfully configured the load balancer.

Authentication Server

This pattern uses LDAP for the authentication server. The following sections provide step-by-step instructions and details for the setup:

- Setting up the Active Directory server
- Setting up the LDAP connector
- Testing the LDAP authentication
- Kerberos overview
    - Kerberos and SSO

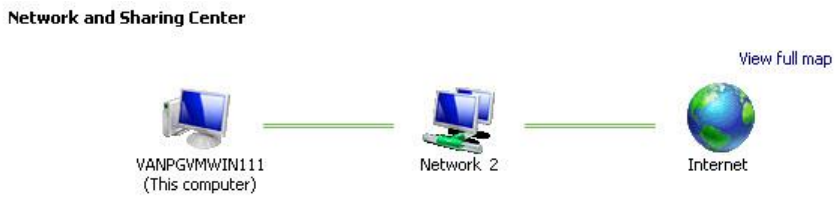
Setting up the Active Directory server

Checking for Active Directory installation

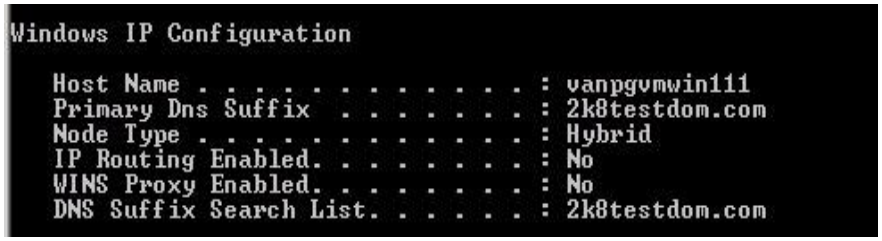
Verify if the Active Directory Server is installed on Windows 2008.

Information:
Microsoft Active Directory (AD) requires DNS to resolve AD resources. Promoting a Windows 2003 server to AD Domain Controller (DC) installs and configures the DNS if one does not already exist.

1. Go to **Network Properties** and view the status of the Local Area Connection.



2. Click **Properties**, then **TCP/IPv6**, and then **Properties** again.
3. Ensure that the preferred DNS server is set to the correct DNS server IP.



If the Windows 2008 server already has the Active Directory installed, go directly to the "To configure basic groups and users in the Active Directory server" section. Otherwise, you must perform the steps below prior to configuring the Active Directory Server.

Installing the Active Directory

First, install the Active Directory role.

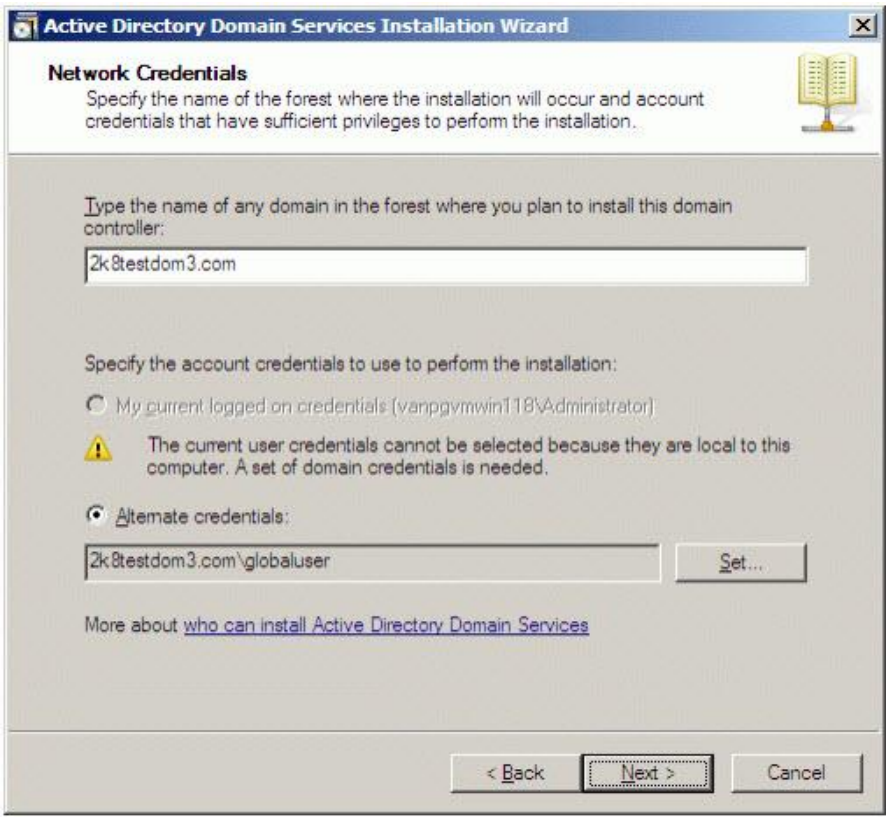
1. Open **Server Manager**.
2. Under **Role Summary**, click **Add Roles**. This launches the Add Roles Wizard.
3. Click **Next**.
4. In "Server Roles", select **Active Directory Domain Services**.
5. Click **Next** twice.
6. Click **Install**.
   The Active Directory Role is installed.

   Next, configure the Active Directory Domain Services.

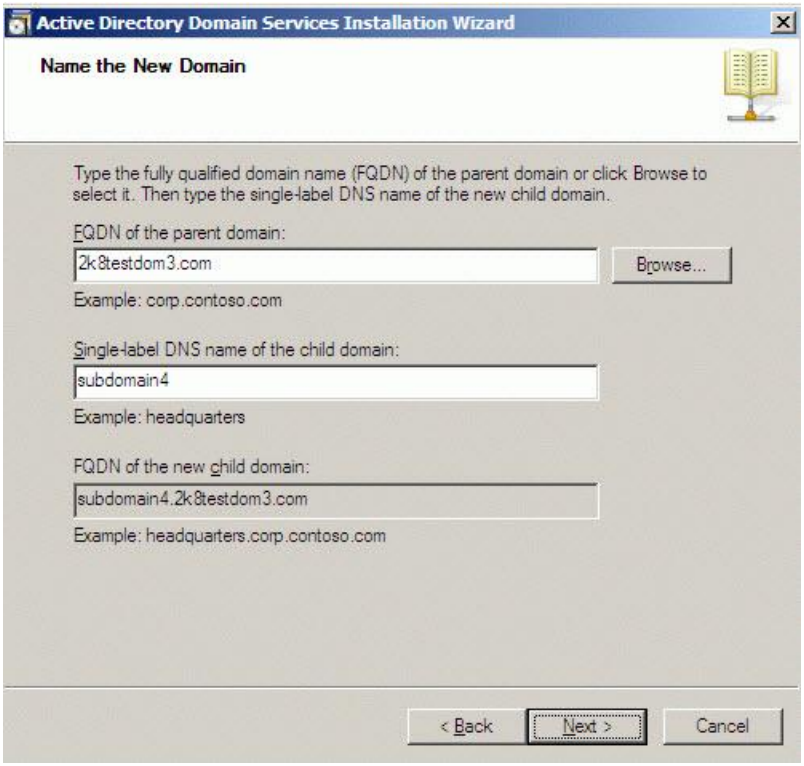
7. Close the Add Roles Wizard and launch the Active Directory Domain Services Installation Wizard (dcpromo.exe).
8. Click **Next** twice.
9. In "Choose a Deployment Configuration", ensure the **Existing Forest** and **Create a new domain in an existing forest** radio buttons are selected and the **Create a new domain tree root instead of a new child domain** checkbox is not selected.

   These options are configured this way because a child domain is a domain in an existing forest.

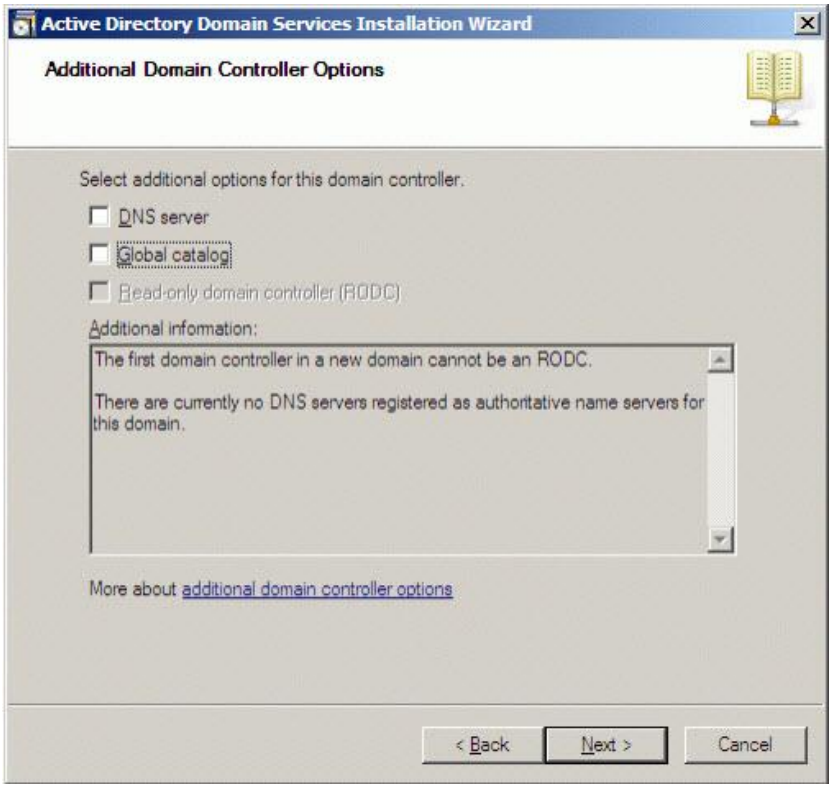
10. Click **Next**.
11. In "Network Credentials", provide the name of the primary DNS server in the domain where the child subdomain will be added (for example, 2k8testdom.com, 2k8testdom2.com, and 2k8testdom3.com).



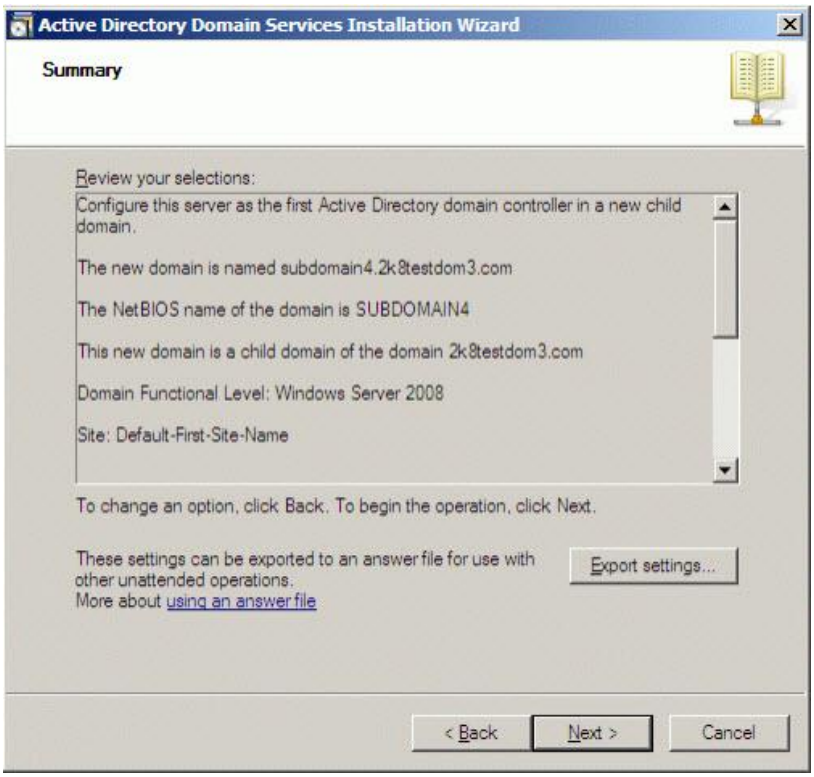
12. Set **Alternate credentials** to the Administrator and verify that the correct domain is specified (for example,2K8TESTDOM\Administrator, 2K8TESTDOM2\Administrator, or 2K8TESTDOM3\Administrator).
13. Click **Next**.
14. In "Name the New Domain", enter the name of the primary DNS server in the **FQDN of the parent domain** field.

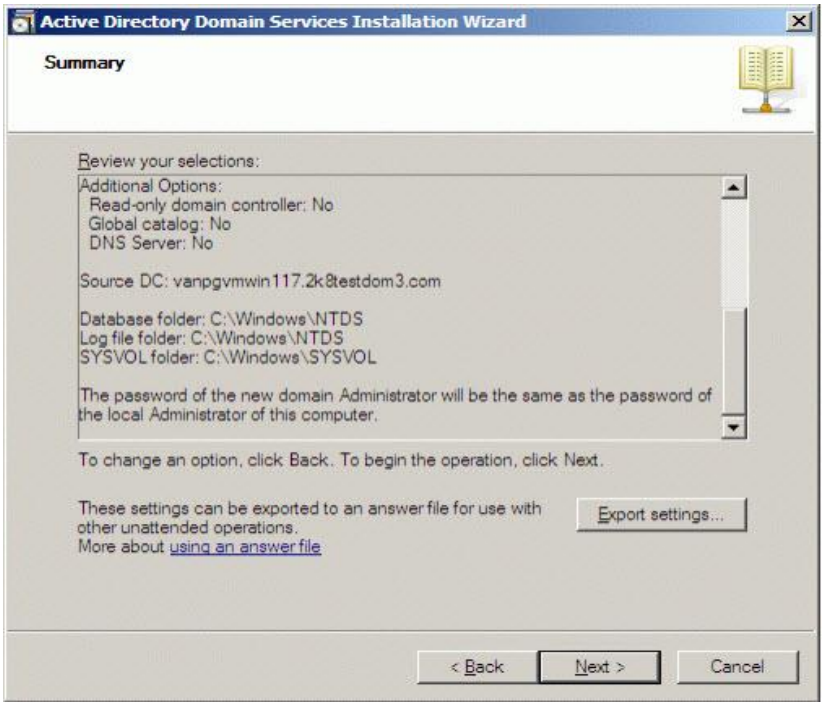


15. In the **Single-label DNS name of the child domain** field, enter an appropriate name for the child subdomain.
16. Ensure that the value in the **FQDN of the new child domain** field is correct.
17. Click **Next**. You may receive a permission warning, but you can ignore it.
18. Verify the NetBIOS name when prompted.
19. In "Additional Domain Controller Options", ensure the **DNS Server** and **Global catalog** options are not selected.



20. Click **Next**.
21. Verify that all the information is correct.


Active Directory Domain Services Installation Wizard
Summary
Review your selections:
Configure this server as the first Active Directory domain controller in a new child domain.
The new domain is named subdomain4.2k8testdom3.com
The NetBIOS name of the domain is SUBDOMAIN4
This new domain is a child domain of the domain 2k8testdom3.com
Domain Functional Level: Windows Server 2008
Site: Default-First-Site-Name
To change an option, click Back. To begin the operation, click Next.
These settings can be exported to an answer file for use with other unattended operations.
More about using an answer file
Export settings...
< Back
Next >
Cancel


Active Directory Domain Services Installation Wizard
Summary
Review your selections:
Additional Options:
Read-only domain controller: No
Global catalog: No
DNS Server: No
Source DC: vanpgvmwin117.2k8testdom3.com
Database folder: C:\Windows\NTDS
Log file folder: C:\Windows\NTDS
SYSVOL folder: C:\Windows\SYSVOL
The password of the new domain Administrator will be the same as the password of the local Administrator of this computer.
To change an option, click Back. To begin the operation, click Next.
These settings can be exported to an answer file for use with other unattended operations.
More about using an answer file
Export settings...
< Back
Next >
Cancel

22. Click **Next** twice.
23. Ensure the parent domain controller is selected as a replication partner for the child domain, and then click **Next**.
24. Set the **Directory Services Restore Mode Administrator password** to password_1, and then click **Next**.
25. Click **Next** to set up the domain controller.
    This process may take a few minutes to complete.
26. Restart the machine.
27. Once the machine has restarted, ensure you can connect using the host name (for example, SUBDOMAIN4\Administrator).
    Next, edit the group policy management.
28. Open the Group Policy Management Editor (open **gpedit** in Microsoft Management Console, or MMC).
29. Expand **Windows Settings** > **Security Settings** > **Account Policy** > **Password Policy**.
30. Set the **Password must meet complexity requirements** option to **Disabled**.
31. Disable the **Maximum password age** policy by setting the value to **0 days**.
    These settings ensure the Administrator's password never expires and that we can set user passwords to something simple.
    Next, create some Organizational Units.
32. Open the Active Directory Users and Computers console (open **DSA** in MMC).
33. Under the new subdomain create a new organizational unit called "PG".
34. Under the PG organizational unit, create a new organizational unit called "BIP".
35. Under the BIP organizational unit, create a new organizational unit using your name.
36. Create some users and groups in your organization unit.
37. Under the Users folder create a new user called **globaluser** and set its password.
38. Add globaluser to the following groups: Account Operators, Domain Users, and Remote Desktop Users.

You have installed the Active Directory.

Before proceeding, ensure the following:

- The firewall is deactivated.
- IPv6 is activated since the rest of the AD domains pass DNS information over IPv6

Configuring basic groups and users in the Active Directory server

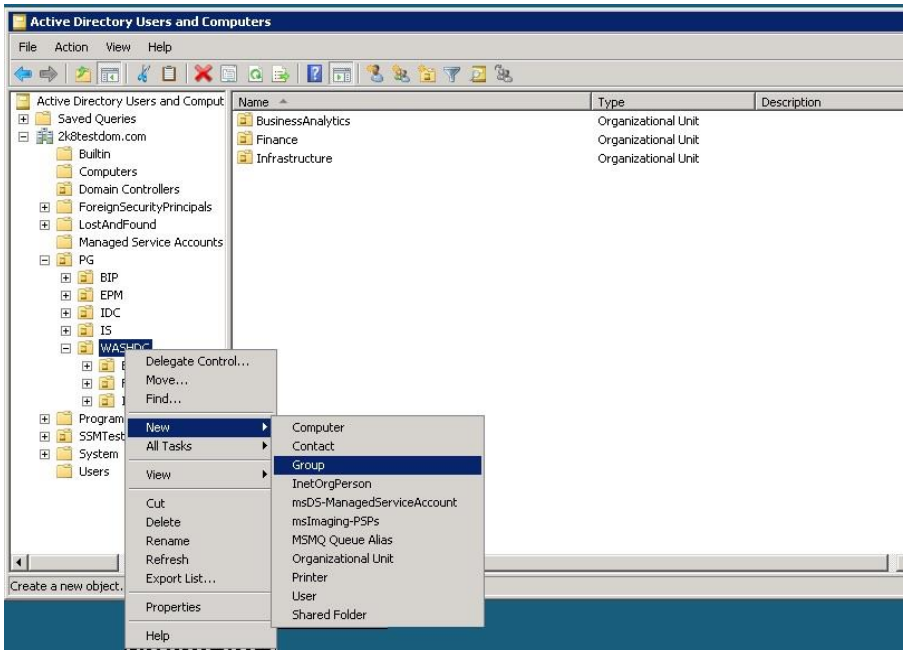
First, create a group.

This procedure creates a new domain group in the "Active Directory Users and Computers" Microsoft Management Console (MMC).

Information: Membership in **Domain Admins**, or equivalent, is the minimum requirement needed to perform this procedure.

Begin by creating a new group account using the Windows interface.

1. To open the "Active Directory Users and Computers" MMC, click **Start** > **Control Panel**, double-click **Administrative Tools**, and then double-click **Active Directory Users and Computers**.
2. In the console tree, right-click the folder under which you want to create a new group.



The file path should look similar to the following:
Active Directory Users and Computers*domain node**folder*

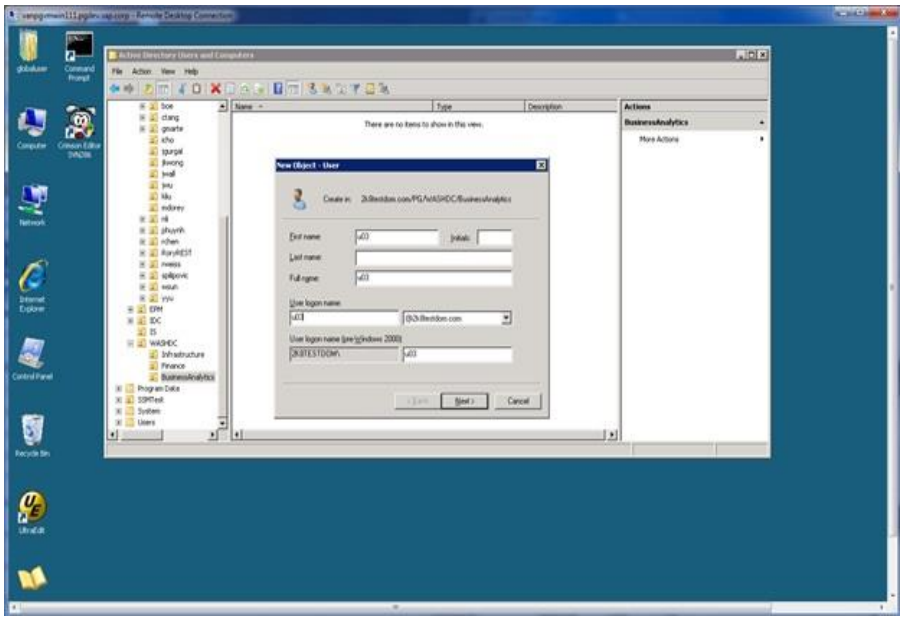
3. Click **New** > **Group**.
4. Type the name of the new group.
   By default, the name that you enter is also entered as the pre-Windows 2000 name of the new group.
5. In Group scope, click one of the available options.
   For more information, see the "Understanding group scope" section in Understanding Group Accounts.

6. In **Group type**, click one of the available options.
   For more information, see the "Understanding group types" section in Understanding Group Accounts.
   Next, create a user account.
   This procedure is used to create a new domain user account in the "Active Directory
   Users and Computers" MMC.
   Information: Membership in **Domain Admins**, or equivalent, is the minimum requirement needed to perform this procedure.

7. Click **Start** > **Administrative Tools** > **Active Directory Users and Computers**.
   The "Active Directory Users and Computers" MMC opens.

   If it is not already selected, click the node for your domain. For example, in our example the domain is DC=2k8testdom,DC=com, so we click **2k8testdom.com**.
8. In the details pane, right-click the folder in which you want to add a user account.

   The file path should look similar to the following:
   Active Directory Users and Computers*domain node**folder*
9. Click **New** > **User**.
10. In "First name", type the user's first name.
11. In "Initials", type the user's initials.
12. In "Last name", type the user's last name.
13. Modify "Full name" to add initials or reverse the order of the first and last names.
14. In "User logon name", enter the user logon name, and then click **Next**.
15. In "Password" and "Confirm password", enter the user's password, and then select the appropriate password options.
16. Click **Next**, review the new user account settings, and then click **Finish**.

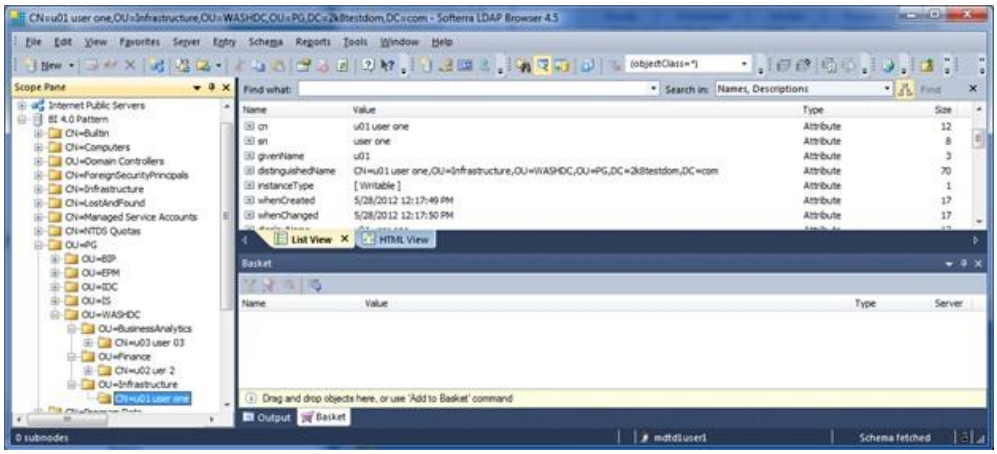


You have configured basic groups and users in the AD server.

BI 4.0 Users & Groups

We created the following new LDAP Users and Groups that are going to be used with the SAP BusinessObjects authentication:

- User: u01 Password: u01
- User: u02 Password: u02
- User: u03 Password: u03



Setting up the LDAP connector

Using LDAP authentication

When we install BI platform, the LDAP authentication plug-in is installed automatically, but not enabled by default. To use LDAP authentication, you need to first ensure that you have your respective LDAP directory set up.

LDAP security plug-in

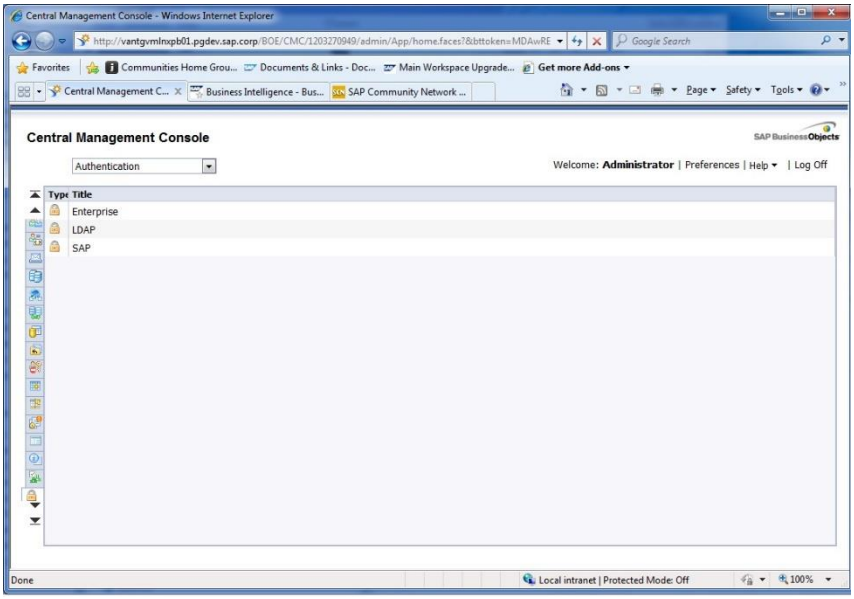
The LDAP security plug-in allows us to map user accounts and groups from our LDAP directory server to BI platform; it also enables the system to verify all login requests that specify LDAP authentication. Users are authenticated against the LDAP directory server, and have their membership in a mapped LDAP group verified before the CMS grants them an active BI platform session. User lists and group memberships are dynamically maintained by the system.

Configuring LDAP authentication

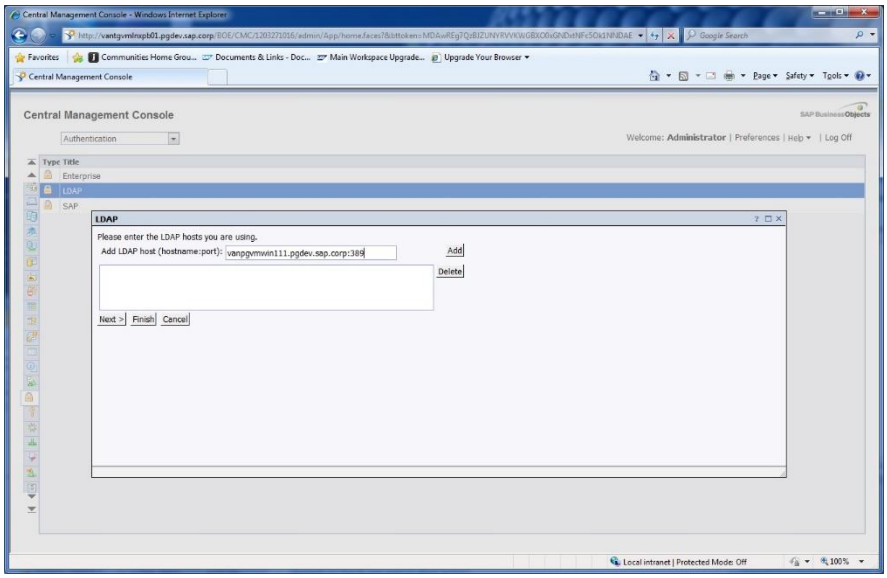
To simplify administration, BI platform supports LDAP authentication for user and group accounts. Before users can use their LDAP user name and password to log into the system, we need to map their LDAP account to BI platform. When we map an LDAP account, we can choose to create a new account or link to an existing BI platform account.

Information: To configure the LDAP host, it is recommended that you install your LDAP server and have it running before configuring the LDAP host.

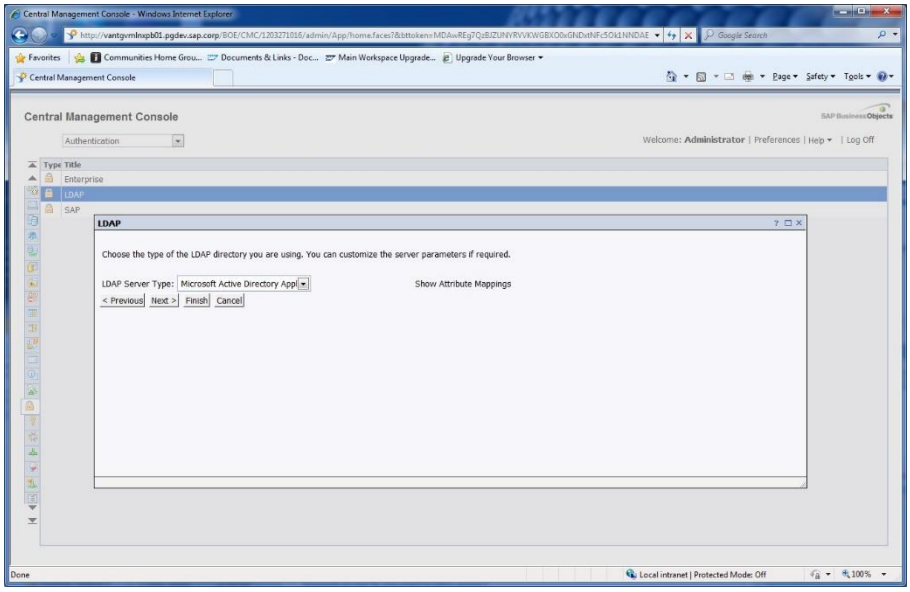
1. Go to the **Authentication** management area of the CMC, and then double-click **LDAP**.



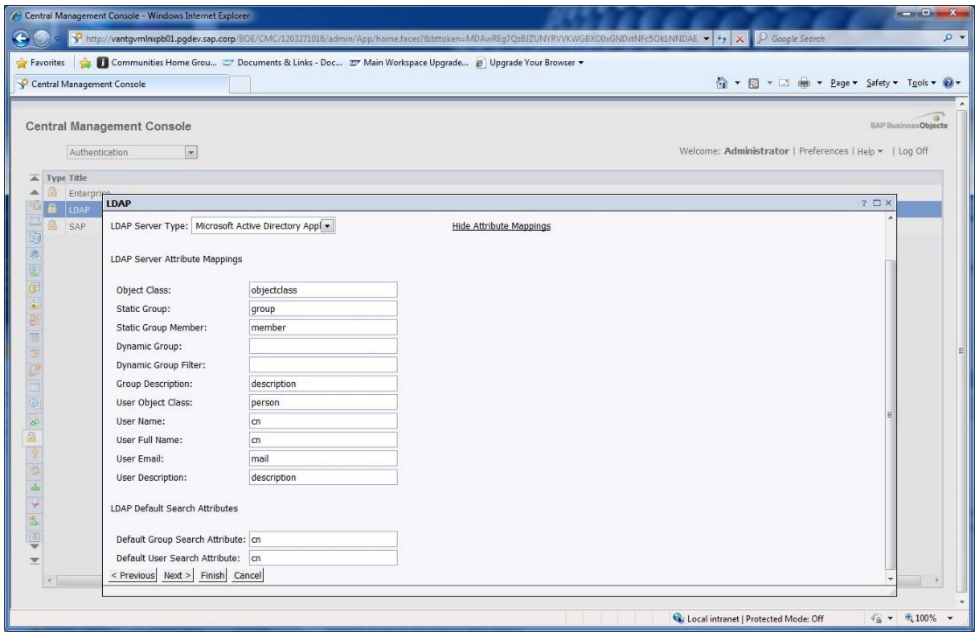
2. Enter the name and port number of your LDAP hosts in the "Add LDAP host (hostname:port)" field (for example, "myserver:123"), click **Add**, and then click **OK**.
Repeat this step to add more than one LDAP host of the same server type if you want to add hosts that can act as failover servers. If you want to remove a host, highlight the host name and click **Delete**.



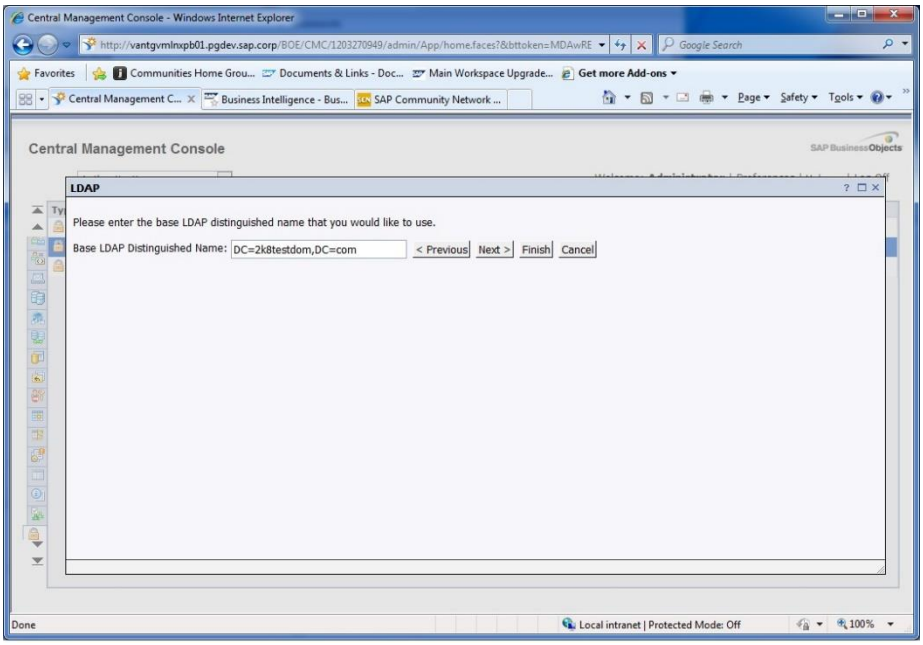
3. Select your server type from the **LDAP Server Type** list.
If you are mapping LDAP to AD, select "Microsoft Active Directory Application Server" for your server type.



4. If you want to view or change any of the LDAP Server Attribute Mappings or the LDAP Default Search Attributes, click **Show Attribute Mappings**. By default, the server attribute mappings and search attributes of each supported server type are already set.

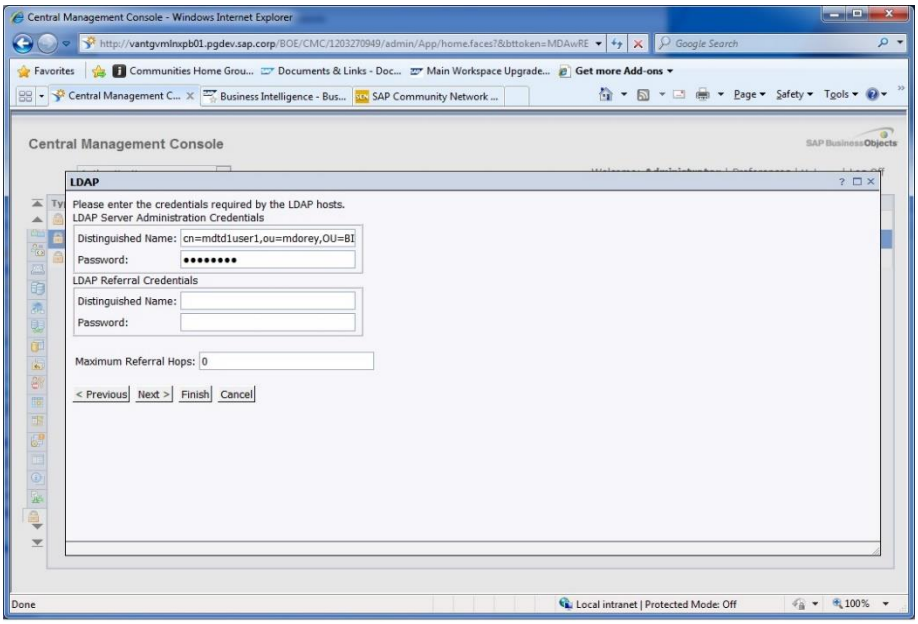


5. Click Next.
6. In the "Base LDAP Distinguished Name" field, enter the distinguished name (for example, "o=SomeBase") for your LDAP server, then click **Next**.



7. In the "LDAP Server Credentials" area, specify the distinguished name and password for a user account that has read rights to the directory. Administrator credentials are not required.

   If your LDAP Server allows anonymous binding, leave this area blank; BI platform servers and clients will bind to the primary host via anonymous login.



8. If you have configured referrals on your LDAP host, provide the authentication information in the "LDAP Referral Credentials" area, then enter the number of referral hops in the "Maximum Referral Hops" field.

   Information:

   The "LDAP Referral Credentials" area must be configured if all of the following apply:

   - The primary host has been configured to refer to another directory server that handles queries for entries under a specified base.
   - The host being referred to has been configured to not allow anonymous binding.
   - A group from the host being referred to will be mapped to BI platform.

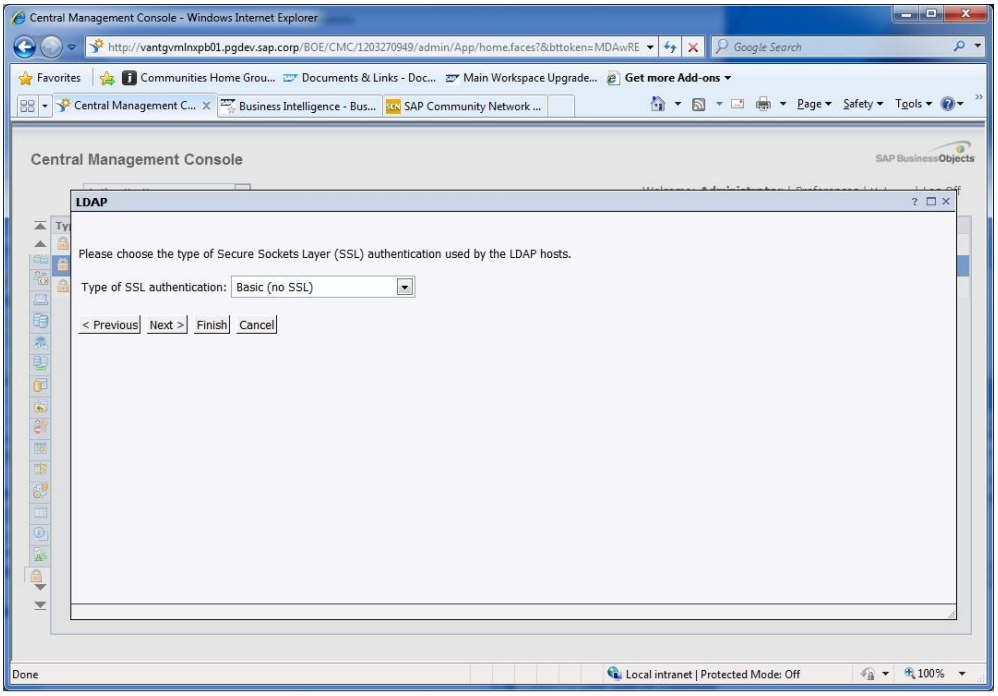
Although groups can be mapped from multiple hosts, only one set of referral credentials can be set. Therefore if you have multiple referral hosts, you must create a user account on each host that uses the same distinguished name and password.

In addition, if the "Maximum Referral Hops" field is set to zero, no referrals are followed.

9. Click Next.
10. Choose the type of Secure Sockets Layer (SSL) authentication to use, then click **Next**.

    You can select one of the following authentication types:

    - Basic (no SSL)
    - Server Authentication
    - Mutual Authentication

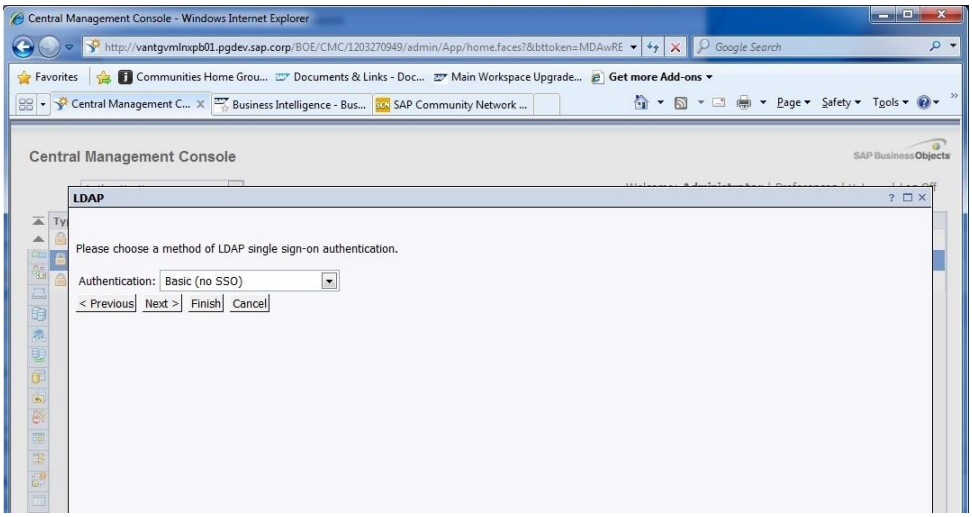


11. Choose a method of LDAP single sign-on authentication, then click **Next**.

    You can select one of the following authentication types:

    - Basic (No SSO)

- SiteMinder



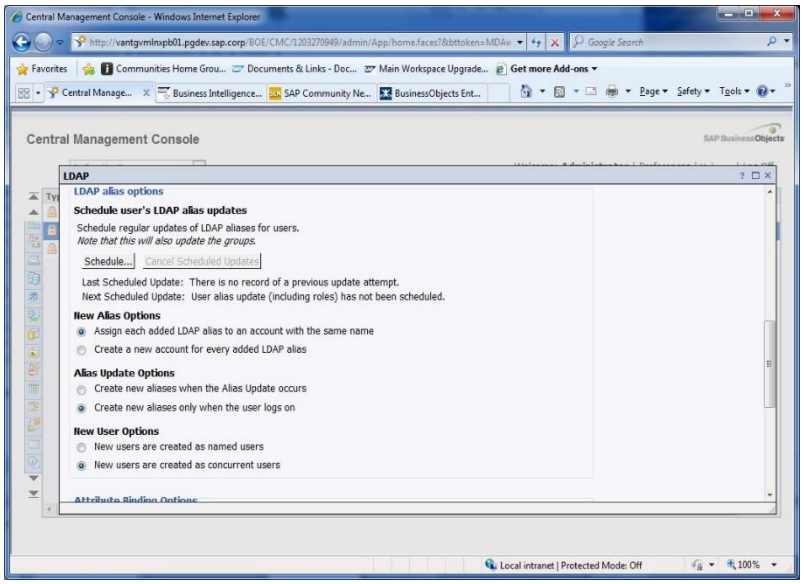
12. Select how aliases and users are mapped to BI platform accounts.

    a. In the "New Alias Options" area, select an option for mapping new aliases to Enterprise accounts:

- **Assign each added LDAP alias to an account with the same name**

  Select this option when you know users have an existing Enterprise account with the same name; that is, LDAP aliases are assigned to existing users (automatic alias creation is turned on). Users who do not have an existing Enterprise account, or who do not have the same name in their Enterprise and LDAP account, are added as new users.

- **Create a new account for every added LDAP alias**
  Select this option when you want to create a new account for each user.



b. In the "Alias Update Options" area, select an option for managing alias updates for the Enterprise accounts:

- **Create new aliases when the Alias Update occurs**

  Select this option to automatically create a new alias for every LDAP user mapped to BI platform. New LDAP accounts are added for users without BI platform accounts, or for all users if you selected the Create a new account for every added LDAP alias option.

- **Create new aliases only when the user logs on**

  Select this option when the LDAP directory you are mapping contains many users, but only a few of them will use BI platform. The platform does not automatically create aliases and Enterprise accounts for all users. Instead, it creates aliases (and accounts, if required) only for users who log into BI platform.

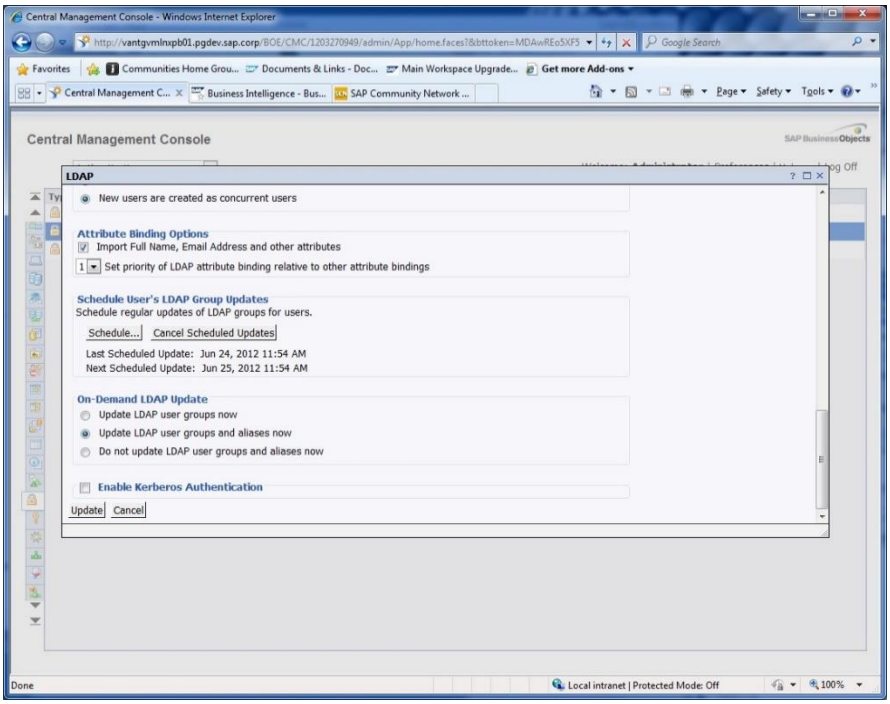
c. In the "New User Options" area, select an option for creating new users:

- **New users are created as named users**
  New user accounts are configured to use named user licenses. Named user licenses are associated with specific users and allow people to access BI platform based on their user name and password. This provides named users

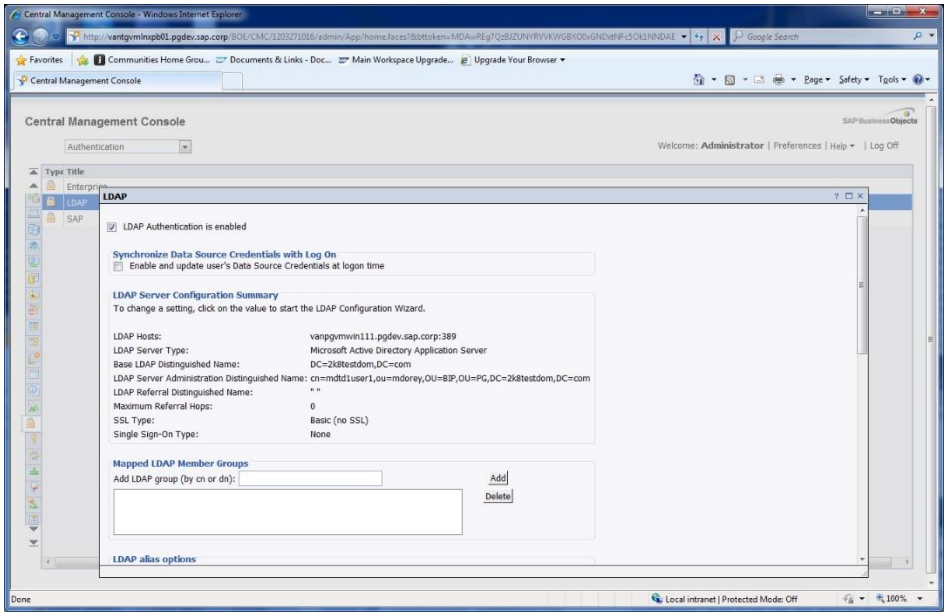
with access to the system regardless of how many other people are connected. You must have a named user license available for each user account created using this option.

- **New users are created as concurrent users**
  New user accounts are configured to use concurrent user licenses. Concurrent licenses specify the number of people who can connect to BI platform at the same time. This type of licensing is flexible because a small concurrent license can support a large user base. For example, depending on how often and how long users access the system, a 100-user concurrent license could support 250, 500, or 700 users.

13. In the "Attribute Binding Options" area you can specify the attribute binding priority for the LDAP plugin:
    - Click the **Import Full Name and Email Address** check box.
      The full names and descriptions used in the LDAP accounts are imported and stored with the user objects in BI platform.
    - Specify an option for **Set priority of LDAP attribute binding relative to other attributes binding.**
      If the option is set to "1", LDAP attributes take priority in scenarios where LDAP and other plugins (Windows AD and SAP) are enabled. If the option is set to "3", attributes from other enabled plugins take priority.



14. Click Finish.

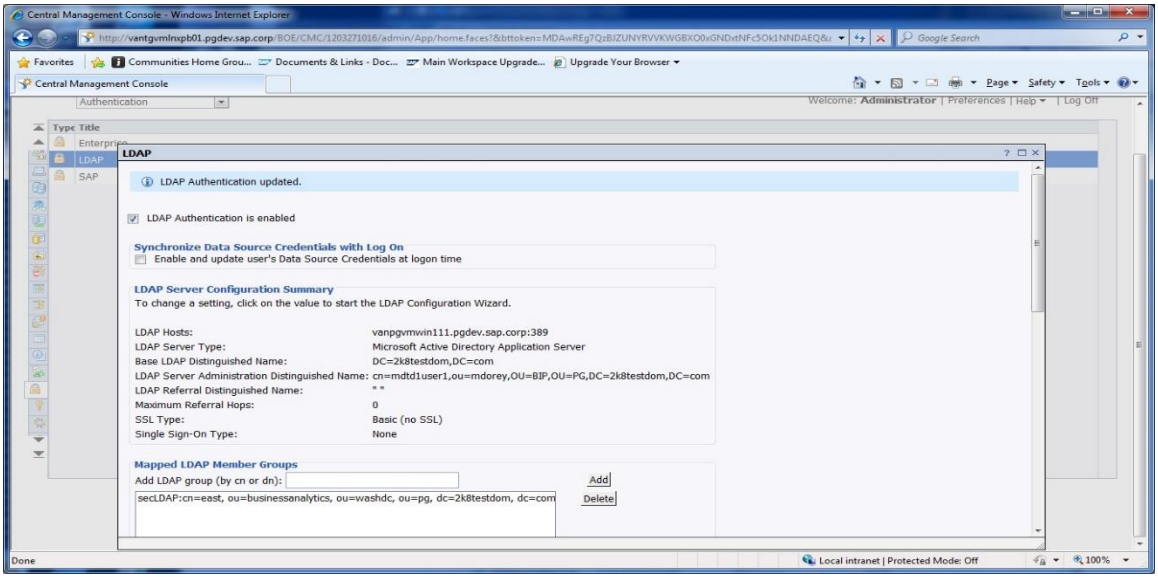


You have configured LDAP authentication.

Mapping LDAP against Windows AD

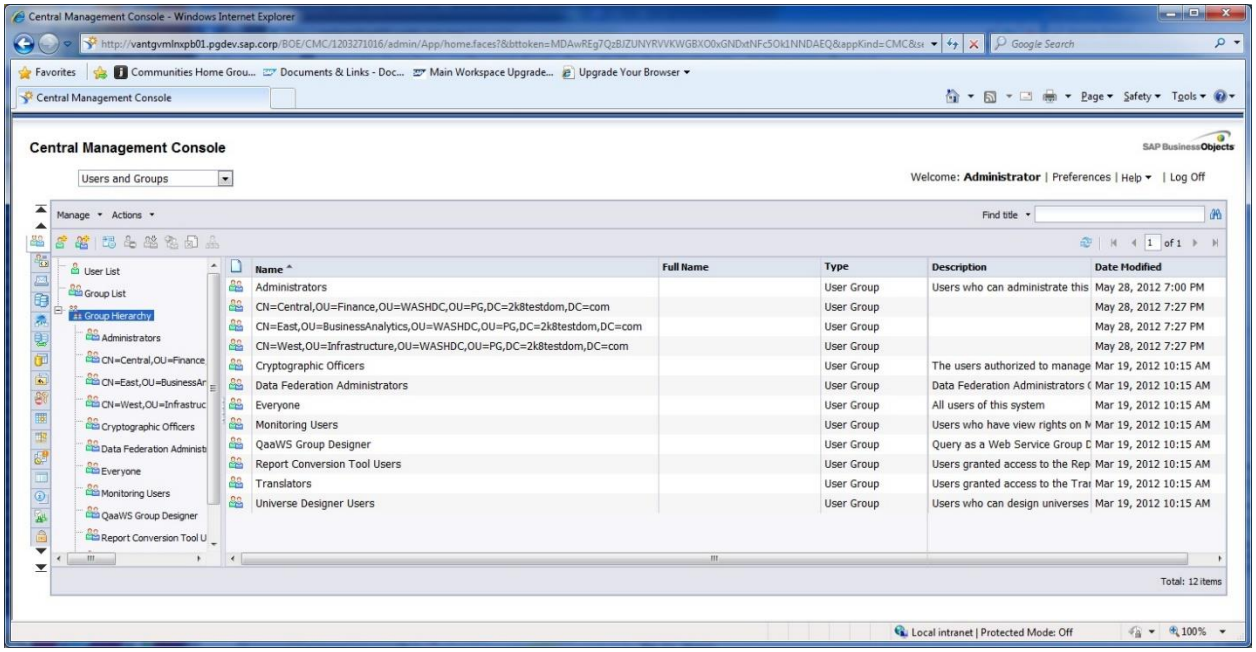
If you configure LDAP against Windows AD, note the following restrictions:

- If you configure LDAP against AD, you will be able to map your users but you will not be able to configure AD single sign-on or single sign-on to the database. However, LDAP single sign-on methods like SiteMinder and trusted authentication will still be available.
- Users who are only members of default groups from AD will not be able to log in successfully. Users must also be a member of another explicitly created group in AD and this group must be mapped. An example of such a group is the "domain users" group.
- If a mapped domain local group contains a user from a different domain in the forest, the user from a different domain in the forest will not be able to log in successfully.
- Users from a universal group from a domain different than the DC specified as the LDAP host will not be able to log in successfully.
- You cannot use the LDAP plug-in to map users and groups from AD forests outside the forest where BI platform is installed.
- You cannot map in the Domain Users group in AD.
- You cannot map a machine local group.
- If you are using the Global Catalog Domain Controller, there are additional considerations when mapping LDAP against AD:



Configuring the Group security

Groups are collections of users who share the same account privileges; therefore, you may create groups that are based on department, role, or location. Groups enable you to change the rights for users in one place (a group) instead of modifying the rights for each user account individually. Also, you can assign object rights to a group or groups and add LDAP groups to the appropriate security group.



Testing the LDAP authentication

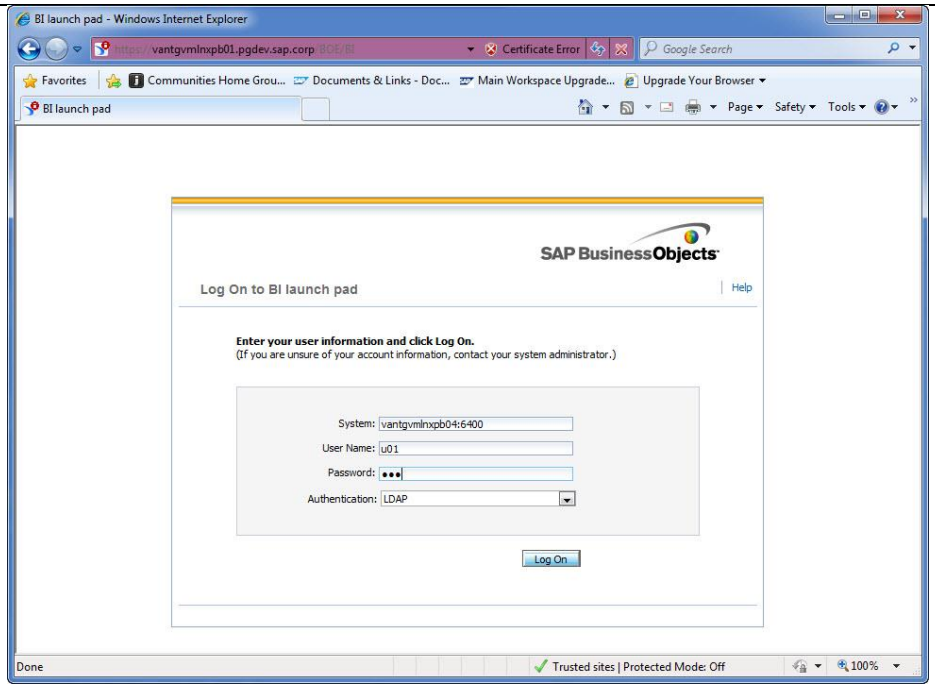
Using LDAP authentication

When BI platform is configured for secLDAP authentication or is set up by default to secEnterprise, but allows the user to select the authentication method, the user is allowed to log into BI launch pad using LDAP credentials provided that the user belongs to a mapped LDAP group.

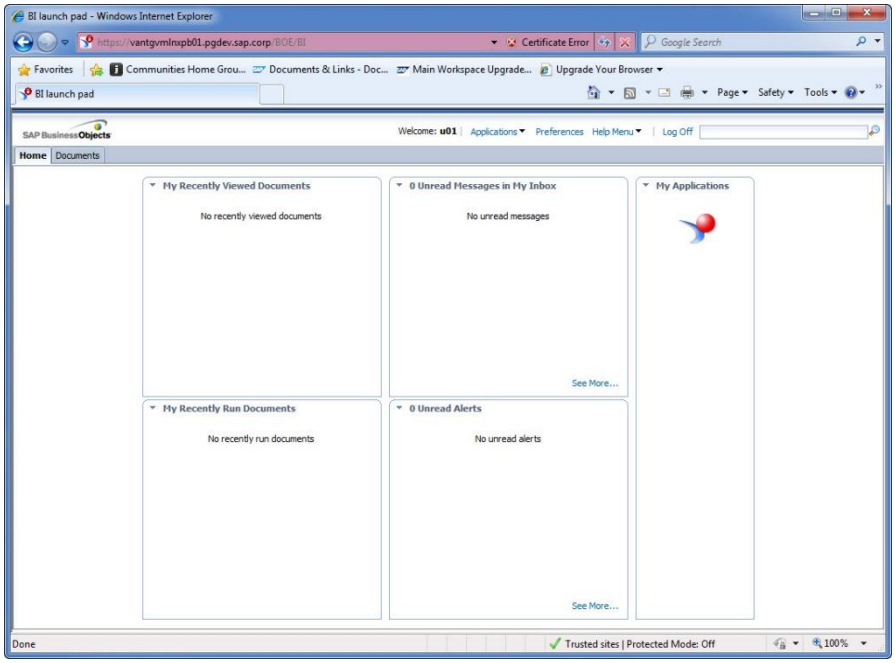
1. Go to https://vantgvmlnxpb01.pgdev.sap.corp/BOE/BI.
2. Select **LDAP** authentication instead of **Enterprise**. Enter the credentials of one of the users belonging to the group **botesters**. For example, we entered the following:

```
System: vantgvmlnxpb04:6400
User: u01
Password: u01
```

```
Authentication: LDAP
```



When you log into BI launch pad, you will see the following:



You have logged into BI launch pad with LDAP credentials.

Validating the Session

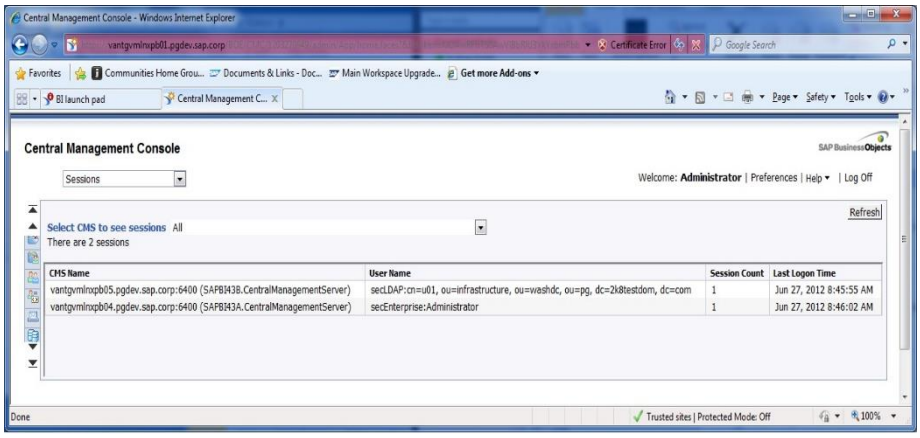
You can validate sessions in the CMC.

1. Go to https://vantgvmlnxpb01.pgdev.sap.corp/BOE/CMC.
2. Select **LDAP** authentication instead of **Enterprise**. Enter the credentials of one of the users belonging to the group **botesters**.
   For example, we entered the following:

```
System: vantgvmlnxpb04:6400
User: u01
Password: u01
Authentication: LDAP
```

3. From the dropdown list under "Central Management Console", select **Sessions**.

   You will see something similar to the following:



You have validated the session.

Kerberos overview

Kerberos is a network authentication protocol developed at MIT. Its main purpose is to allow applications to authenticate each other. In addition, it provides confidentiality and integrity for data transmitted between applications.

How Kerberos Works

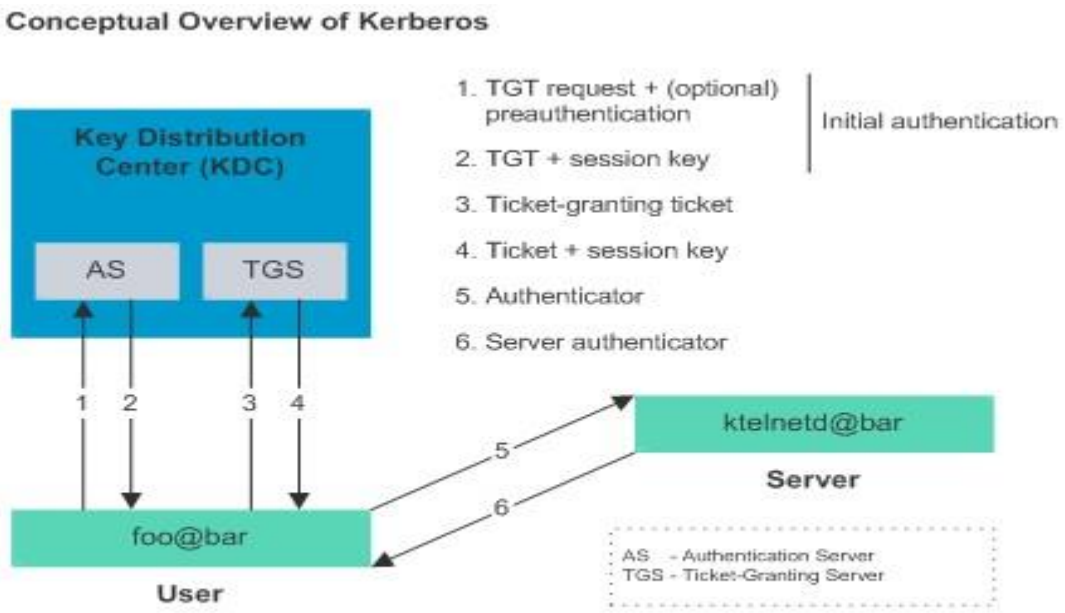
A Kerberos domain or realm consists of several entities who cooperate to communicate securely. These are:

1. *Users* - principals who wish to access services.
2. *Servers* - principals who supply services to users. Note a server may also be a user of another service.
3. *The Key Distribution Center (KDC)* - The KDC is responsible for coordinating access to services by users (by providing the Ticket Granting Service (TGS)), and for performing the initial authentication (by providing the Authentication Service (AS)) (See below). The KDC is the controller of all secure interactions, and as such is a trusted entity.

   A principal authenticates itself in Kerberos by using a principal name of the form principal-name@realm and a password. This is typically used to send an encrypted message to the Authentication Service (AS), which can then authenticate the principal and send back a session key and Ticket Granting Ticket (TGT). The TGT is like a certificate of identity which allows the principal to gain later access to one or more services. Once the user has supplied their password and obtained the TGT from the AS, authentication to any other service can happen automatically without the user having to resupply their password. For this reason, Kerberos is sometimes called a Single Sign-On (SSO) service.

   For more information about using Kerberos with SSO, see Kerberos and SSO.

A *ticket* is a credential that enables a principal to gain access to a service. A principal obtains tickets from the *Ticket Granting Service (TGS)* using the TGT obtained from the AS as described above. The ticket is used to create an *authenticator*, which is then sent to the service being requested to authenticate the user. The authenticator is then used to establish a session key for secure communication. Optionally, the user can also request to authenticate the server. If this happens, the server uses information in the user's authenticator to send back a *server authenticator*, which the user can use to verify the server's authenticity.



For more information on the Kerberos protocol, including the Kerberos V RFCs, see Kerberos Papers and Documentation

Where Kerberos is Used

Kerberos is used in Windows to provide authentication services for Windows domains. Kerberos authentication is also integrated with some Unix operating system logins (e.g. Solaris), and can be used for authentication in LDAP. Kerberos forms the basis of security in the Distributed Computing Environment (DCE), and can be used to implement a CORBA security service.

Kerberos and SSO

Kerberos is the preferred client-server authentication protocol for a multitude of SAP BusinessObjects products, including BI 4.0. The following sections provide details about using Kerberos with Single Sign-On (SSO).

Kerberos Overview

The following topic provides an overview of Kerberos, including workflows for client authentication, client service authentication, and client service request:

Purpose of Kerberos within the BI 4.0 environment

Configuring Windows Integrated Authentication using Kerberos

The following blog post examines the steps needed to configure Windows Integrated Authentication using Kerberos Authentication:

Windows Integrated Authentication via Kerberos on an LDAP data source

Setting up Active Directory SSO in UNIX or Linux

The following SAP Note examines the steps needed to configure Active Directory (AD)

SSO in a UNIX or Linux server, where Windows AD does not exist:

SAP Note 1636349 - Best Practice: How To setup Active Directory Single Sign-On when BOE CMS is on Unix or Linux for BI4

Configuring Web Services SSO with Tomcat

The following SAP Note examines the steps needed to configure LiveOffice, Query as a Web Service, BI Widgets, and Crystal Reports for Enterprise 4.0 SSO with Tomcat:

SAP Note 1646920 - How to configure Web Services Single Sign-On (dswsbobje) with Tomcat for SAP BusinessObjects Business Intelligence platform 4+

Troubleshooting the Linux Pattern

This section provides troubleshooting tips and solutions for more common problems that you may encounter during the Linux pattern setup.

- File Sharing TroubleShooting
- BusinessObjects Cluster Troubleshooting
- Application Server Troubleshooting
- Apache Troubleshooting

File Sharing Troubleshooting

NFS Troubleshooting

Problem

NFS servers are not running. Running the command "service nfs status" produces the

following output:

```
rpc.svcgssd is stopped
rpc.mountd is stopped
nfsd is stopped
rpc.rquotad is stopped
```

Cause

NFS servers have been stopped

Resolution

1. Run the following command to start the NFS servers:
   > service nfs start
2. Check to see if the servers are running now. Run the following command:
   > service nfs status

   You will see output similar to the following:

   ```
   rpc.svcgssd is stopped
   rpc.mountd (pid 1567) is running...
   nfsd (pid 1564 1563 1562 1561 1560 1559 1558 1557) is running...
   rpc.rquotad (pid 1551) is running...
   ```

BusinessObjects Cluster Troubleshooting

Error #1

Problem

./setup.sh

/home/sapbi/install/setup.env.sh: /home/sapbi/install/setup.engine/perl/bin/perl: /lib/ld-linux.so.2: bad ELF interpreter: No such file or directory

/home/sapbi/install/setupexe

./setup.sh: /home/sapbi/install/setupexe: /lib/ld-linux.so.2: bad ELF interpreter: No such file or directory

Finished, return code is 126

Cause

ld-linux.so.2 is missing

Resolution

On Red Hat, run the following commands as root:

> yum install glibc.i686

> yum install libstdc++.i686

Error #2

Problem
./setup.sh

/home/sapbi/install/setupexe

/home/sapbi/install/setupexe: error while loading shared libraries: libstdc++.so.5: cannot open shared object file: No such file or directory

Finished, return code is 127

Cause
libstdc++.so.5 is missing

Resolution
On Red Hat, run the following commands as **root**:
> yum install compat-libstdc++-33-3.2.3-69.el6.i686
> yum install compat-libstdc++-33.i686

Error #3

Problem

SAP BusinessObjects BI platform CMS: Unable to connect to the CMS system database ""cms57u05"". Reason: Login failed.
Cannot verify DB login information.
Would you like to correct them?

Cause

DB login information cannot be verified

Resolution

Make sure your user name is the correct case. For example, "SAPcms" is "SAPCMS". In addition, make sure you password is correct.

Error #4

Problem
Before running the CMS install, you want to make sure you have everything set up to access the SYBASE DB.
You might not able to connect to the DB.
How do you test to see if you have access to the DB outside of BIP?

Resolution
Run the following command:
> isql -S cms57u05 -U SAPCMS -P bobobo

Error #5

Problem

When running the stop servers command you get the following error message:

/home/bobje/BI43/sap_bobj/enterprise_xi40/linux_x86/crpe/mw//bin-i86_linux/mwxcbtest: error while loading shared libraries: libX11.so.6: cannot open shared object file: No such file or directory

Cause

Shared libraries libX11.so.6 is missing

Resolution

On Red Hat, run the following command as root:

> yum install libX11-1.3-2.el6.i686

Application Server Troubleshooting

Error #1

Problem
BIP web tier installation fails with the following error:

setupexe: /lib/ld-linux.so.2: bad ELF interpreter: No such file or directory

Finished, return code is 126

Cause
32-bit glibc libraries are missing

Resolution
On Red Hat, run the following command as **root**:
> yum install glibc-2.12-1.47.el6_2.5.i686

Error #2

Problem
BIP web tier installation fails with the following error:

setupexe: error while loading shared libraries: libstdc++.so.5: cannot open shared object file: No such file or directory

Finished, return code is 127

Cause
Compatibility standard C++ libraries are missing

Resolution
On Red Hat, run the following command as **root**:
> yum install compat-libstdc++-33-3.2.3-69.el6.i686

Troubleshooting Application Server Cluster

Problem
In BI launch pad, the java.lang.NullPointerException error occurs.

Cause
Session failover does not occur correctly

Resolution

1. Create a sample web application to test cluster failover.
   a. Log into lnxpb02 as **tomcat**.
   b. Create a directory called cluster in the webapps directory to contain the sample application. Run the following commands:
      > cd /opt/apache-tomcat-7.0.25/webapps

> mkdir -p cluster/WEB-INF
> cd cluster/WEB-INF

c. Create a web.xml file and add the **distributed** tag. Run the following command:
> vi web.xml

Insert the following code block:

```
<?xml version="1.0" encoding="ISO-8859-1"?>

<web-app xmlns="http://java.sun.com/xml/ns/javaee"
    xmlns:xsi="http://www.w3.org/2001/XMLSchema-
instance"
    xsi:schemaLocation="http://java.sun.com/xml/ns
/javaee
 http://java.sun.com/xml/ns/javaee/web-
app_2_5.xsd"
    version="2.5"
   <distributable />

</web-app>
```

d. Create a JSP file to test session failover outside of BIP. Run the following commands:
> cd /opt/apache-tomcat-7.0.25/webapps/cluster
> vi test.jsp

Insert the following code block:

```
<%
   session.setAttribute("a","a");
 %>
 <html>
 <head>
 <title>Test JSP</title>
 </head>

<body>
 <table
width="100%" border="0" cellspacing="0" cellpadding=
"0">
```

```
    <tr bgcolor="#CCCCCC">
      <td width="13%">vantgvmlnxpb02</td>
      <td width="87%"> </td>
    </tr>
    <tr>
      <td>Session ID :</td>
      <td><%=session.getId()%></td>
    </tr>
  </table>
  </body>
  </html>
```

e. Repeat steps a-d on **lnxpb03**. In test.jsp, replace "vantgvmlnxpb02" with "vantgvmlnxpb03".

f. Test session failover by accessing the test.jsp file through the load balancer. You will see output similar to the following:

```
vantgvmlnxpb02
Session ID : 26743DFB75C097ED1F8E3BC59D76229C.vantgvmlnxpb02
```

g. Stop the Tomcat instance the session is hosted on, in this case lnxpb02. Run the following command:
> service tomcat7 stop

h. Refresh test.jsp in the browser and check the session:

```
vantgvmlnxpb03
Session ID : 5E69F09D5A6679AE648F2890CE79B1D3.vantgvmlnxpb03
```

Information: The session has changed so there is a problem with clustering externally to BIP.

2. The solution can be found on the Tomcat wiki at http://wiki.apache.org/tomcat/FAQ/Clustering#Q8.
Navigate to the following section: **The cluster doesn't work under Linux with two nodes on two boxes.**
Does a multicast route to your network interface exist?

3. Run the following command as **root** on both lnxpb02 and lnxpb03. Type:
> route add -host 228.0.0.4 dev eth0

4. Next, restart the Tomcat instances on both lnxpb02 and lnxpb03 and test the process again. Run the following command on both machines:
> service tomcat7 restart

5. Use the sample application to test session failover
Note the session details:

```
vantgvmlnxpb02
Session ID : BF2462E53AEB9A74C5C8575B86A3A43D.vantgvmlnxpb02
```

a. Stop Tomcat on lnxpb02. Run the following command:
   > service tomcat7 stop
b. Refresh test.jsp in the browser.
   Note the session details:

```
vantgvmlnxpb03
Session ID : BF2462E53AEB9A74C5C8575B86A3A43D.vantgvmlnxpb03
```

   Information: Session ID remains the same but the route identifier has changed. This confirms clustering is working externally to BIP.

6. Now test BI launch pad.

a. First identify which node you are connected to

   Note the session details:

```
vantgvmlnxpb02
Session ID : D84CB1072F4788DECD86CA90E45FBD07.vantgvmlnxpb02
```

b. Next, access BI launch pad.
c. Log in as **administrator**
d. Select the **Document** list
e. Stop Tomcat on the machine we're currently connected to, which is lnxpb02. Run the following command:
   > service tomcat7 stop
f. Click the **Home** tab in BI launch pad and note that it seamlessly transitions without error.

Tomcat Application Server clustering is working as expected.

Apache Troubleshooting

Troubleshooting the Apache web server setup

Problem

Users are unable to connect to Apache through a browser

Cause

Firewall configuration prevents access to the web server from client browsers

Resolution

1. Temporarily disable the firewall for testing purposes.

a. Log into **lnxpb01** as **root**.
b. Stop the iptables service. Type:
   > service iptables stop

   You should see output similar to the following:

```
iptables: Flushing firewall rules: [ OK ]
iptables: Setting chains to policy ACCEPT: filter [ OK ]
iptables: Unloading modules: [ OK ]
```

Warning: Disabling the firewall on your system will make it vulnerable to attacks. On an internal system, the risks are fairly low but you will want to ensure that you enable your firewall protection after you have completed your testing.

The firewall has now been stopped. Attempt to access the system again to see if the problem has been resolved by this change.

2. Try to connect via both http and https connections.

3. Try pinging the server from your client machine.
   a. Launch the command prompt and run the following command:
      > ping lnxpb01
   b. Ensure that the httpd daemon is running on the Apache machine. Run the following command:
      > ps -ef |grep httpd
   c. Ensure that the http/https ports are open and listening on the Apache machine. Run the following command:
      > netstat -l |grep http
      You will see output similar to the following:

```
tcp 0 0 :http *: LISTEN
tcp 0 0 :https *: LISTEN
```

   d. Check the httpd access logs to see if the connection made it to the httpd daemon. Run the following command:
      > tail -f /var/local/usr/apache/logs/access_log

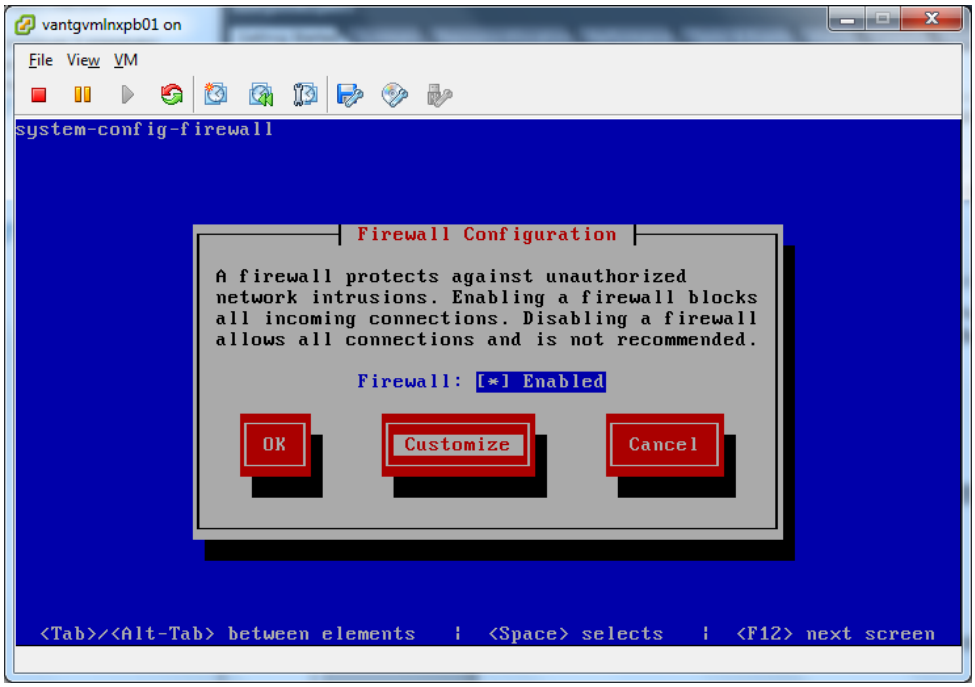
      You will see output similar to the following:

```
10.7.92.208 - - [31/May/2012:11:57:02 -0700| |] "GET / HTTP/1.1" 200
11313
```

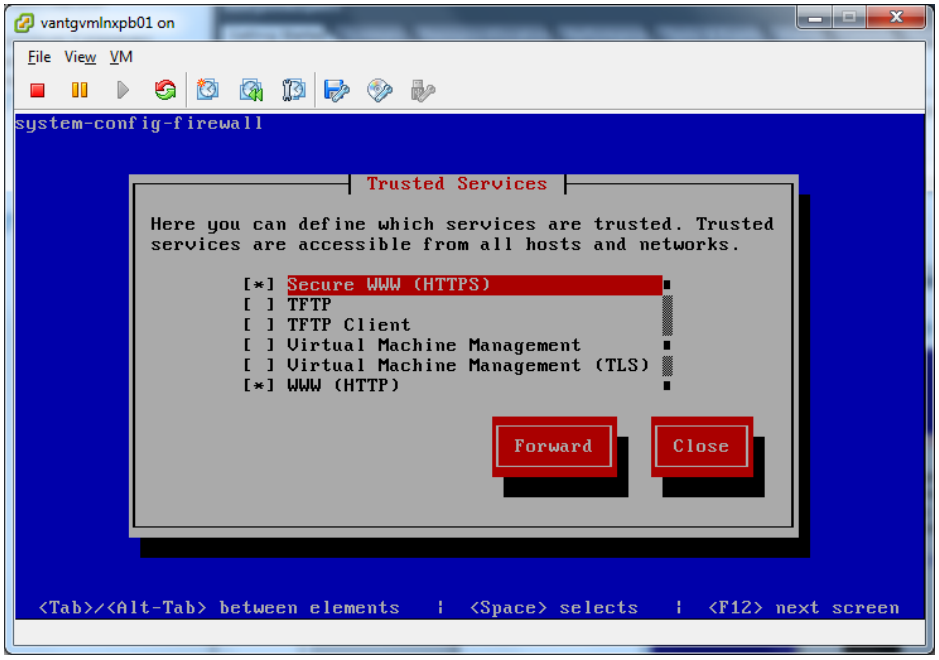
Adding iptables info for Apache process

In this section, you will configure the firewall and define which services can be trusted.

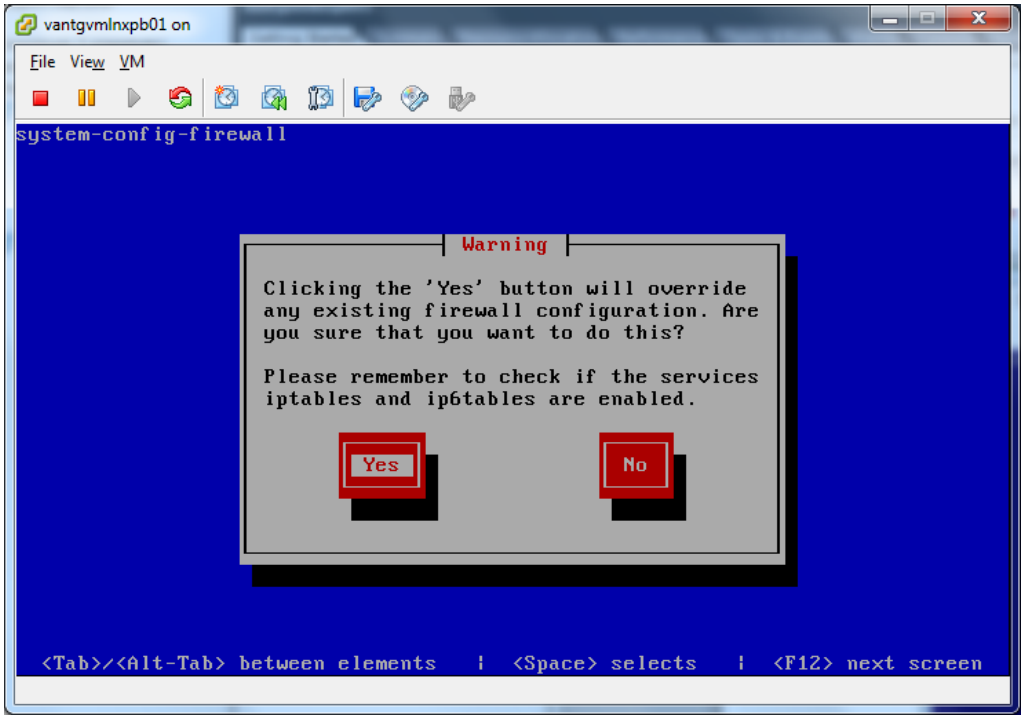
1. Log into lnxpb01 as **root**.
2. Launch the system configuration tool for firewall. Run the following command:
   > system-config-firewall-tui
3. Ensure the **Enabled** option is selected beside **Firewall**. Click **Customize**.



4. Select **Secure WWW (HTTPS)** and **WWW (HTTP)** and click **Close**:



5. Click **OK**.
6. Click **Yes**.



7. Verify the firewall is now running. Run the following command:
   > service iptables status

   You will see output similar to the following:

```
Table: filter
Chain INPUT (policy ACCEPT)
num target prot opt source destination
1 ACCEPT all – 0.0.0.0/0 0.0.0.0/0 state RELATED,ESTABLISHED
2 ACCEPT icmp – 0.0.0.0/0 0.0.0.0/0
3 ACCEPT all – 0.0.0.0/0 0.0.0.0/0
4 ACCEPT tcp – 0.0.0.0/0 0.0.0.0/0 state NEW tcp dpt:22
5 ACCEPT tcp – 0.0.0.0/0 0.0.0.0/0 state NEW tcp dpt:80
6 ACCEPT tcp – 0.0.0.0/0 0.0.0.0/0 state NEW tcp dpt:2049
7 ACCEPT tcp – 0.0.0.0/0 0.0.0.0/0 state NEW tcp dpt:443
8 REJECT all – 0.0.0.0/0 0.0.0.0/0 reject-with icmp-host-prohibited

Chain FORWARD (policy ACCEPT)
num target prot opt source destination
1 REJECT all – 0.0.0.0/0 0.0.0.0/0 reject-with icmp-host-prohibited

Chain OUTPUT (policy ACCEPT)
num target prot opt source destination
```

8. Ports 80 and 443 are now open to accept incoming connections. This should allow for your end users to connect in to your system.

Reference and System Specifications for the Linux Pattern

Web Server (lnxpb01)

Machine name	vantgvmlnxpb01.pgdev.sap.corp
OS	RHES 6.2
CPU	2 CPU
Memory	8GB RAM
Disk Space	60GB Drive

Software	Apache 2.2.22

Web Application Server 2 (lnxpb03)

Machine name	vantgvmlnxpb03.pgdev.sap.corp
OS	RHES 6.2
CPU	4 CPU
Memory	8GB RAM
Disk Space	60GB Drive
Software	Tomcat 7

FRS Share (lnxpb06)

Machine name	vantgvmlnxpb06.pgdev.sap.corp
OS	SLES 11 SP1 x64
CPU	2 CPU
Memory	4GB RAM
Disk Space	60GB Drive
Software	not applicable

BIP Cluster 1 (lnxpb04)

Machine name	vantgvmlnxpb04.pgdev.sap.corp
OS	RHES 6.2

CPU	4 CPU
Memory	16GB RAM
Disk Space	60GB Drive
Software	SAP BusinessObjects BI Platform 4.0 Feature Pack 3 Sybase ASE 15.7 Client

BIP Cluster 2 (lnxpb05)

Machine name	vantgvmlnxpb05.pgdev.sap.corp
OS	RHES 6.2
CPU	4 CPU
Memory	16GB RAM
Disk Space	60GB Drive
Software	SAP BusinessObjects BI Platform 4.0 Feature Pack 3 Sybase ASE 15.7 Client

Linux Pattern Acceptance Tests

The following topics outline the acceptance test cases performed on the Linux pattern:

- BI launch pad cases
- Central Management Console cases
- Web Intelligence cases

BI launch pad cases

Test	Result
Access report properties	✔
Add a publication to folder	✔
Add a report to folder	✔
Add and delete a category	✔
Browse categories and document lists	✔
Change user preferences and control	✔

Create and delete a folder	✅
Log on using LDAP Authentication	✅
Schedule a Crystal report	✅
Schedule a publication	✅
Schedule a Web Intelligence document	✅
Send an object to inbox	✅
Use the search function to search all documents using keyword and title	✅
View a Crystal report	✅
View a publication	✅
View a Web Intelligence document	✅
View history	✅

Central Management Console cases

Test	Result
Add servers to server groups	✅
Create LDAP users and groups	✅
Create server groups	✅
Delete server groups	✅
Enable and disable servers	✅
Log off newly created user	✅
Log on with newly created user (secLDAP)	✅
Remove servers from server groups	✅
Start, stop, restart servers	✅

Web Intelligence cases

Test	Result
View Web Intelligence on demand	✔
View Web Intelligence instances	✔
Edit query	✔
Create and sort charts	✔
Schedule Web Intelligence documents	✔