Legal Notices

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

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

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

Copyright © 2009 Novell, Inc. All rights reserved. No part of this publication may be reproduced, photocopied, stored on a retrieval system, or transmitted without the express written consent of the publisher.

Novell, Inc., has intellectual property rights relating to technology embodied in the product that is described in this document. In particular, and without limitation, these intellectual property rights may include one or more of the U.S. patents listed on the Novell Legal Patents Web page (http://www.novell.com/company/legal/patents/) and one or more additional patents or pending patent applications in the U.S. and in other countries.

Novell, Inc.
404 Wyman Street, Suite 500
Waltham, MA 02451
U.S.A.
www.novell.com

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

Novell Trademarks

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

Third-Party Materials

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

**Introduction** 5

**SECTION 1 Manage Networking** 7

- Exercise 1-1 Configure a Network Bridge 8
- Exercise 1-2 Bond Network Interfaces 9
- Exercise 1-3 Configure VLAN Tagging 10

**SECTION 2 Manage Server Storage** 11

- Exercise 2-1 Configure a SAN with iSCSI 12

**SECTION 3 Work with Xen Virtualization** 13

- Exercise 3-1 Install and Use Xen Virtualization 14
  - Part II: Migrate a Xen Virtual Machine to Another Host 15

**SECTION 4 Harden Servers** 17

- Exercise 4-1 Harden a SLES 11 Server 18
- Exercise 4-2 Protect Services with Apparmor 19
- Exercise 4-3 Configure AIDE 22

**SECTION 5 Update Servers** 23

- Exercise 5-1 Implement an SMT Server 24

**SECTION 6 Prepare Servers for Disasters** 29

- Exercise 6-1 Use an LVM Snapshot Volume to Create a Consistent Backup 30
- Exercise 6-2 Access Remote Storage Using Multipath I/O 31

**SECTION 7 Monitor Server Health** 33

- Exercise 7-1 Use Nagios to Monitor Network Hosts 34
Introduction

This workbook is designed to help you practice the skills associated with SUSE Linux Enterprise Server 11: Certified Linux Engineer (Course 3107) objectives.

The purpose of these exercises is to teach you advanced practical Linux skills, using SUSE Linux Enterprise Server 11, and to prepare you for the Novell Certified Linux Engineer Practicum examination.

NOTE: Instructions for setting up a self-study environment are in the 3107_setup.pdf on the Course DVD.

The exercises do not contain detailed step-by-step instructions (this is different from the CLP 11 courses), but only general instructions on how to perform the task. We assume that students who meet the course prerequisites do not need these detailed instructions anymore.

Before starting the exercises in this workbook, please review the following exercise conventions.

Exercise Conventions

When working through an exercise, you will see conventions that indicate information you need to enter that is specific to your server.

The following describes the most common conventions:

- *italicized text*: This is refers to your unique situation, such as the hostname of your server.
  
  For example, supposing the hostname of your server is da50 and you see the following

  `hostname.digitalairlines.com`

  You would enter

  `da50.digitalairlines.com`

- **172.17.8.xx**: This is the IP address that is assigned to your SUSE Linux Enterprise Server 11.
  
  For example, supposing your IP address is 172.17.8.50 and you see the following

  `172.17.8.xx`

  You would enter

  `172.17.8.50`
- **Select**: The word *select* is used in exercise steps with reference to menus where you can choose between different entries, such as drop-down menus.

- **Enter and Type**: The words *enter* and *type* have distinct meanings.

  The word *enter* means to type text in a field or at a command line and press the Enter key when necessary. The word *type* means to type text without pressing the Enter key.

  If you are directed to type a value, make sure you do not press the Enter key or you might activate a process that you are not ready to start.

- **Key combinations**: Ctrl+Alt+F1 indicates that all three keys should be pressed at the same time. Ctrl, Alt, F1 indicates that the three keys should be pressed and released one after the other.
SECTION 1  Manage Networking

In this section of the workbook, you learn how to do the following:

1. “Configure a Network Bridge” on page 8
2. “Bond Network Interfaces” on page 9
3. “Configure VLAN Tagging” on page 10
**Exercise 1-1  Configure a Network Bridge**

In this lab, configure a network bridge on the dax1 server.

This lab requires two network interfaces in the dax1 server, with one NIC connected to dax2 and the other connected to dax3. Skip this exercise if dax1 does not have two NICs.

On dax1, create a network bridge that includes both interfaces and allows dax2 and dax3 to connect to each other.

To create a network bridge, do the following:

1. On dax1, note the current network configuration, as you will need to restore it after this lab.
2. On dax1, install the bridge-utils package.
3. Make sure one NIC of dax1 is connected to dax2 and the other is connected to dax3.
4. On dax1, open the YaST Network Settings dialog and delete the existing network configuration; then add a new bridge.
5. Add the eth0 and eth1 interfaces to the bridge. Assign the bridge a static IP address, such as 10.0.0.x1/24.

---

**NOTE:** The bridge does not need an IP address of its own to connect computers in the connected network segments; it only needs the IP address to be able to connect to the bridging machine itself.

---

6. On dax2, configure the interface connected to dax1 with the IP address 10.0.0.x2/24.
7. On dax3, configure the interface connected to dax1 with the IP address 10.0.0.x3/24.
8. You should be able to ping dax2 from dax3 and vice versa.
9. Restore the original network configuration.

*(End of Exercise)*
**Exercise 1-2  Bond Network Interfaces**

In this lab, you combine two physical network interfaces into one logical interface. This lab requires two computers that are connected via two network interfaces.

To bond two network interfaces, do the following together with another student:

1. Make sure each network interface in your computer is connected (via a cross-link cable) to an interface of your partner’s computer.

2. Open the *YaST Network Settings* dialog and delete the current network configuration. Then select *Add* to add an interface. Under *Device Type*, select *Bond*, then select *Next*.

3. In the *Network Card Setup* dialog, select or enter:
   - *Statically assigned IP address*, such as 10.0.1.x.2/24 on dax2.
   - In the *Bond Slaves* frame, select the network interfaces you want to bond.
   - Under Bond driver options, make sure the entry says *mode=active-backup miimon=100*
   - Conditional: If one or both of your connections include a switch, use `arp_ip_target=ip_addressof_other_machine` `arp_interval=100` instead of `miimon=100`.

4. Select *Next*; then select *OK*.

5. Ping the other machine. While the ping command is running, remove a network cable and see what happens. Put it back and remove the other cable. What happens?

6. Restore the original network configuration.

*(End of Exercise)*
Exercise 1-3  Configure VLAN Tagging

In this lab, you work with VLAN tags so that only computers that belong to the same VLAN “speak” to each other.

To configure VLANs, do the following together with another student:

1. Open the YaST Network Settings dialog and delete the existing network configuration.

2. In the Network Settings dialog select Add to add an interface. Under Device Type select VLAN. For the Configuration Name select 5, then select Next.

3. In the Network Card Setup dialog, select or enter:
   - Real Interface for VLAN: eth0.
   - Statically assigned IP address, such as 10.0.1.x2/24 on dax2.

4. Select Next; then select OK.

5. Ping the other machine; you should see echo replies.

6. On one of the two machines, delete the VLAN5 interface and create it again with the same parameters, however, use a different Configuration Name, such as 6.

7. Ping the other machine, you should see “Destination host unreachable” messages.

8. Restore the original network configuration.

(End of Exercise)
SECTION 2  Manage Server Storage

In this section of the workbook, you learn how to do the following:

1. “Configure a SAN with iSCSI” on page 12
Exercise 2-1 Configure a SAN with iSCSI

In this exercise, you configure a dedicated SAN using iSCSI.

The dax1 server will function as a storage server (iSCSI target) while dax2 and dax3 will function as storage consumers (iSCSI initiators).

To complete this exercise, you need to do the following tasks:

1. Create a “dedicated” network for iSCSI SAN communications.
   
   This can be accomplished in several different ways. Do one the following:
   
   - Install a second Ethernet network interface board in each of your SLES 11 servers (or enable a disabled Ethernet interface on the motherboard) and connect it to a dedicated Ethernet switch.
   
   - If installing or enabling a second Ethernet network interface board in each of your SLES 11 servers is not feasible, add a second IP address and subnet mask to the existing Ethernet network interfaces in your servers.
   
   While this strategy doesn’t actually create a dedicated SAN network, it approximates this functionality; which is usually sufficient in a classroom environment.

   NOTE: Whichever strategy you choose, we strongly recommend that you use Gigabit (1000 Mbps) network interfaces and switches. While this exercise can be completed using Fast Ethernet (100 Mbps) equipment, we have found that performance is generally unsatisfactory.

2. Create two 1 GB blank, unformatted Linux partitions in the free space available on the hard drive of dax1.

3. Install and configure the iSCSI target daemon (ietd) on dax1.

4. Configure the blank, unformatted Linux partitions you created in Step 2 as iSCSI targets. Configure them to use no authentication.

5. Install and configure the iSCSI initiator daemon (iscsid) on dax2 and dax3. Connect one of the targets you configured on dax1 to dax2, the other to dax3.

6. Configure the iscsid daemon to automatically connect to these targets each time the service starts.

7. Use a partitioning utility to create a Linux partition and an ext3 file system on the connected iSCSI targets.

8. Test the functionality of the system.

9. (Optional) Install and configure an iSNS server on dax1. Create the appropriate discovery domains and domain sets. Configure your iSCSI target daemon on dax1 to register with the iSNS server. Configure your iSCSI initiator daemons to use the iSNS server as well. Test the functionality of the system.

(End of Exercise)
SECTION 3  Work with Xen Virtualization

In this section of the workbook, you practice how to do the following:

1. “Install and Use Xen Virtualization” on page 14
Exercise 3-1 Install and Use Xen Virtualization

In this lab, you install Xen on your physical machine and create Xen virtual machines.

You first install Xen on your dax2/dax3 server. Then you configure NFS on dax1 to store the Xen image files and use the da5-xen.xml AutoYaST file from the Student DVD to automatically install SLES 11 in a Xen virtual machine on dax2/dax3, using the remote NFS server to store the image files.

In the second part of this lab, you migrate the new virtual machine to your teammate’s host.

Do the following:

2. “Part II: Migrate a Xen Virtual Machine to Another Host” on page 15


To automatically install SLES 11 in a Xen virtual machine, do the following:

1. Using YaST, on your dax2 (or dax3) machine, install the Xen pattern. You can do this via the Software Management module, or via the Install Hypervisor and Tools module. Reboot the machine to boot the Xen kernel.

2. On dax1, create a /srv/xen/ directory and export it with NFS. On dax2 and dax3, create an /import/xen/ directory and mount the /srv/xen/ directory from dax1 to /import/xen/on dax2 and dax3.

3. Conditional: Instead of using NFS, you could also create two iSCSI targets on dax1 and corresponding initiators on dax2 and dax3. Then install Xen using the iSCSI storage devices as devices for the Xen disks. If you use iscsi: to designate the disk in the vm-install dialog, be sure to replace the /etc/xen/scripts/block-iscsi script with the version in the /exercises/section_03 directory on the Student DVD (see “Install a Xen Virtual Machine Using Remote Storage” in the Student Manual).

4. Copy the da5-xen.xml file from the /exercises/section_03/ directory on the Student DVD to the /tmp/ directory.

5. Using vm-install, install a SLES 11 Xen virtual machine automatically using the remote storage. Make sure to
   - Use a different name for the Xen virtual machine than your partner
   - Use the installation DVD as installation source.
   - Use the /tmp/da5-xen.xml file for the automated installation.
Use /import/xen/`vm-name`/ to hold the disk image files

Specify a MAC address that is unique in the network.

6. Log in to the Xen virtual machine you just installed (root password: novell) and adjust the eth0 IP address to be unique within the network (change it to 172.17.8.1x5, for example).

**Part II: Migrate a Xen Virtual Machine to Another Host**

To migrate a Xen Virtual Machine to another host, do the following:

- On both hosts involved, modify `/etc/xen/xend-config.sxp` to allow migration and restart the xend daemon.
- Start a virtual machine that has its disk on a remote storage server.
- Migrate the machine to another host using the `xm migrate` command. When doing a live migration, open a terminal window and `ping` the migrating machine. Watch the progress on yet another terminal using the `xm top` command.

*(End of Exercise)*
SECTION 4  Harden Servers

In this section of the workbook, you learn how to do the following:

1. “Harden a SLES 11 Server” on page 18
2. “Protect Services with Apparmor” on page 19
3. “Configure AIDE” on page 22
Exercise 4-1  Harden a SLES 11 Server

In this lab, you harden an existing SLES 11 installation.

You first install the Xen virtual machine named da4 provided on the Student DVD on dax2 and dax3. da4 is intended to be deployed as a Web server and an FTP server. This server is newly installed and it needs to be hardened before being deployed in a production environment.

NOTE: The root password in da4 is n0v3LL.

Do the following:

1. On dax3 and dax3, unpack the /setup/da4-xen.tgz archive to /var/lib/xen/disks/ and start the da4 Xen virtual machine using the vm-install command.
2. Configure da4 to use an IP address appropriate for your network segment.
3. Use seccheck to analyze the file system of da4 for files that represent security risks.
4. Check da4 for installed software that is not necessary for its role as a Web/FTP server.
5. Use nmap to check for unnecessary ports open on the system.
6. Verify that user accounts are secure.
7. Use sudo and ACLs to configure the geeko user as a delegated admin user.
   Create a group named home_admin and make geeko a member of this group. Use ACLs and sudo to allow members of the home_admin group to manage (including creating and deleting) directories in /home.
8. Enable the SSH daemon on the server and harden it.
9. Use SuSEfirewall2 to configure your host firewall to allow only the following traffic through:
   - SSH
   - HTTP/HTTPS
   - FTP
   - TFTP

(End of Exercise)
**Exercise 4-2  Protect Services with Apparmor**

In this lab, you configure AppArmor to protect services.

Use AppArmor to protect either the FTP or the Web services running on da4. You decide which you want to protect in this exercise (you can protect both if time permits).

In this exercise, you create an AppArmor profile for the PureFTPd server that prevents anonymous uploads of files even if the PureFTPd configuration erroneously permits them.

You also create an AppArmor profile with a hat for specific files. A sample PHP file is provided on the Student DVD in the `/exercises/section_04` directory that you can use to verify that your profile prevents the creation of files by Web users.

Complete the following:

1. Protect the pureFTPd application with AppArmor by doing the following:
   - Install PureFTPd if it is not installed
   - Configure PureFTPd for anonymous access.
   - Copy some files for download to the `/srv/ftp/` directory.
   - Create an AppArmor profile for PureFTPd using either YaST or the `genprof` command.
   - Change the PureFTPd configuration to allow anonymous uploads (this could occur as a result of a configuration mistake).
   - Verify that the AppArmor profile prevents anonymous FTP uploads despite your configuration error.

2. Protect Apache with AppArmor by doing the following:
   - If necessary, install Apache along with the `apache2-mod_apparmor` and `apache2-mod_php5` packages.
   - Create the following files in the `/srv/www/htdocs` directory:
     - **index.html**: This file should already exist if the `example_pages` package has been installed. It should appear as follows:
       ```html
       <html>
       <body>
       <h1>It works!</h1>
       </body>
       </html>
       ```
     - **info.php**:  
       ```php
       <?php phpinfo(); ?>
       ```
   - Using YaST or the `genprof` command, create an AppArmor profile for Apache. Access the above pages and assign `info.php` to a hat of its own and `index.html` to the `DEFAULT_URI` hat.
Create a file named touch-file.php in the /srv/www/htdocs/ directory that contains the following content (this file is available on the Student DVD in the /exercises/section_04/ directory):

```html
<html>
<head>
    <meta http-equiv="Content-Type" content="text/html;charset=UTF-8">
    <title>Touch a file in /tmp</title>
</head>
<body bgcolor="#ffffff">
<h3>Touch a file in /tmp</h3>
<p>Enter a file name</p>
<form action="touch-file.php" method="POST">
    <p><input name="filename"></p>
    <p><input type="submit" name="Create" value="Create"></p>
</form>

<h4>Result</h4>
<?php
if ($_POST['filename'])
{
    $file_to_create = $_POST['filename'];
    if($file_to_create !="")
    {
        echo "<p> Touching /tmp/".$file_to_create ."</p>"
    }
    echo "<p> Output of ls -l /tmp/".$file_to_create .": 

     // Create file:
     exec("/bin/touch /tmp/".$file_to_create , $touchresult, $touch_returnvalue);
     echo "<p> Output of ls -l /tmp/".$file_to_create .": 

     // List file:
     exec("/bin/ls -l /tmp/".$file_to_create , $lsresult, $ls_returnvalue);
     echo "<p> "$lsresult[0]."</p>"
    }
}
?>
</body>
</html>
```

Try to access the above page from a browser. Put the httpd2-prefork profile in AppArmor complain mode and try again. Put the profile back in AppArmor enforce mode.

Open the /etc/apparmor.d/usr.sbin.httpd2-prefork profile in an editor. Copy the ^/index.php hat to a new hat named ^/touch-file.php. In the new hat, change the following line

```
/srv/www/htdocs/index.php r,
```

```
/srv/www/htdocs/touch-file.php r,

- Reload the AppArmor profiles and try to access touch-file.php. Check /var/log/audit/audit.log for new entries while you access the page.
- View the Security Event Report in YaST.
- Configure the Security Event Notification in YaST.

(End of Exercise)
Exercise 4-3  Configure AIDE

In this lab, you configure AIDE and use it to detect changes in the file system.

You use AIDE to create an initial database of checksums on da4. You then change some files and use AIDE to detect the changes. Do the following:

1. Use the sample rules in /etc/aide.conf as a basis to work from.
2. Add rules that will monitor the /srv/www/ and /srv/ftp/ directories.
3. Verify the syntax of your configuration.
4. Create your initial AIDE database.
5. If equipment is available, move the AIDE binary, configuration file, and database to a read-only device such as a CD-R or a USB drive that can be write-disabled.
6. Once your initial database has been created, test your AIDE configuration by doing the following on da4:
   a. Open a terminal session and switch to root using the su - command and a password of n0v3LL.
   b. At the shell prompt, enter /root/aide_lab_1.sh.
   c. Use AIDE to identify and mitigate the security problems created by running the script.

NOTE: You can run the aide_lab_2.sh script to undo the changes made by the aide_lab_1.sh script.

(End of Exercise)
SECTION 5  Update Servers

In this section of the workbook, you learn how to do the following:

1. “Implement an SMT Server” on page 24
Exercise 5-1  Implement an SMT Server

In this lab, you configure an SMT server.

NOTE: Using the free 60 days evaluation licence for SLES 11 you can mirror the SDK repositories. The SLES 11 repositories can only be mirrored with a paid SLES 11 subscription.

At the time of this writing, the SLE11-SDK-Updates repository for a single CPU architecture (such as i586) is over 6 GB in size. Accordingly, downloading these updates in class can take quite some time. Depending on your Internet bandwidth, it could take 3 hours or more to complete.

To allow you to become familiar with SMT without having to download an entire repository, we have included a Xen virtual machine image on Student DVDs 2 and 3 that already has the SLE11-SDK-Updates repository downloaded and mirrored for the i586 hardware architecture.

NOTE: This repository was current as of February 2010.

You have two options for completing this exercise. You can either

- Configure SMT from scratch on your dax1 server.
  
  If you choose this option, you must download the SLE11-SDK-Updates repository appropriate for your CPU architecture from the Novell Customer Center, which may take several hours to complete.

- Use the DA-SMT Xen virtual machine image provided on the Student DVDs to set up your SMT server.
  
  As noted previously, this virtual machine already has a base SMT server installed and the SLE11-SDK-Updates repository downloaded for you.

Whichever option you choose, you will configure your dax2 and dax3 servers as SMT clients that use your SMT server to get updates.

To do this, complete the following:


   The Get Activation Code button is displayed when you search for the SLES 11 installation media and select the SUSE Linux Enterprise Server 11 for x86, AMD64, Intel64 e-Media Kit link.

NOTE: The activation code is sent to the email address associated with your Novell account.

4. (Conditional) If you want to use the virtual machine provided on your Student DVDs for your SMT server, do the following on your dax1 server:

   NOTE: If you want to install and configure SMT on dax1 without using the DA-SMT virtual machine, skip this step and go to Step 5 on page 26.

   a. Insert Student DVD 2 in the DVD drive of dax1 and copy the da-smt-xen.tgz.00 file to the /tmp directory.

   b. When complete, insert Student DVD 3 in the DVD drive of dax1 and copy the da-smt-xen.tgz.01 file and the da-smt-xen.md5 file to the /tmp directory.

   c. When complete, join the da-smt-xen.tgz.01 file and the da-smt-xen.tgz.00 file together into a file named da-smt-xen.tgz using the following command:

```
   cat /tmp/da-smt-xen.tgz.* > /tmp/da-smt-xen.tgz
```

   The resulting file should be about 8 GB in size.

   d. View the contents of the /tmp/da-smt-xen.md5 file and note the checksum value listed for the da-smt-xen.tgz file.

   e. At the shell prompt, generate an MD5 checksum of your local copy of the da-smt-xen.tgz file by entering the following command:

```
   md5sum /tmp/da-smt-xen.tgz
```

   f. Compare the checksum value you just generated with the value in the da-smt-xen.md5 file and verify that they are the same.

   NOTE: If disk space is low, you can delete the da-smt-xen.tgz.00 and da-smt-xen.tgz.01 files from /tmp at this point.

   g. Unpack the tar archive you just created to the /var/lib/xen/images directory by entering the following commands on dax1:

```
   cd /var/lib/xen/images
   tar -xzvf /tmp/da-smt-xen.tgz
```

   The result is a file named /var/lib/xen/images/DA-SMT/disk0 that should be about 20 GB in size.

   h. Install the Xen kernel on dax1 so that it can run virtual machines.

   i. Using vm-install, configure and start the DA-SMT server on dax1.

   j. Log in to DA-SMT as root with a password of n0v3LL and reconfigure the system’s network addressing parameters as appropriate for your network.

   k. Add an entry to the /etc/hosts file on your dax2 and dax3 servers that resolves da-smt.digitalairlines.com to the IP address your configured for DA-SMT in the previous step.
WARNING: It is very important that you do this. Otherwise, the SMT client software will not accept the `smt.crt` certificate file from the SMT server.

1. Use the Novell Customer Center Configuration module in YaST to activate the DA-SMT server using the activation code you obtained previously.

m. Use the SMT Server Configuration module in YaST on DA-SMT to supply your mirror credentials.

On the Customer Center Access tab, enter the mirroring credentials you obtained earlier as well as the email address associated with your Novell account.

When done, select OK to continue.

When prompted for the MySQL root password, enter `novell`.

NOTE: If a message is displayed indicating the system is not registered with the NCC, register the system.

n. Launch the YaST SMT Server Management module and review the available mirrored repositories.

5. (Conditional) If you want to install and configure SMT on da\$1 from scratch instead of using the virtual machine supply on your Student DVDs, do the following:

NOTE: Do not complete this step if you configured the DA-SMT virtual machine in Step 4 on page 25.

a. Use the Novell Customer Center Configuration module in YaST to activate your da\$1 server using the activation codes you downloaded previously.

b. Install and configure MySQL on da\$1.

c. Install SMT as an add-on product to da\$1.

Copy the `/exercises/section_05/SLE-11-SDK-DVD-i586-GM-Media1.iso` file from your Student DVD to a folder on da\$1 and use it to install SMT on the server.

During the SMT installation process, you will be prompted to enter your mirror credentials. Enter the mirror credentials you obtained earlier in Step 3 on page 25.

During the installation, a MySQL database for the SMT server is created on your da\$1 server. When prompted for the MySQL root user’s password, enter the `password` you created when you installed MySQL.

NOTE: This is the MySQL root user account. It is not the same as the Linux root user account.
6. Configure your SMT server’s job schedule such that SMT tasks are completed within the time constraints of the classroom environment.

7. If necessary, enable mirroring for the SLE 11 repositories.

   You can use the Mirror Now option to download the updates immediately instead of waiting for the scheduled job to occur.

   Consult with your instructor to determine which repositories are appropriate for the hardware architecture in your classroom.

   NOTE: This step may not be necessary if you are using the DA-SMT virtual machine and your classroom hardware uses the x86 hardware architecture.

   If you do need to mirror a repository, avoid mirroring more than one. A single repository can take over 3 hours to download, depending upon your network bandwidth.

8. When the mirroring of repositories is complete, stage the updates downloaded and test them.

   Register dax2 with your SMT server and configure it to function as an SMT test client.

   Apply any applicable updates to dax2. If necessary, create a software repository on dax2 that points to your SMT server using the YaST Software Repositories module or the zypper command.

   Evaluate the behavior of the updates on dax2 and verify they don’t cause any unforeseen problems.

9. When you are done testing the repositories, move them to your production environment.

   Register dax3 as a production SMT client with your SMT server and apply any applicable updates. If necessary, create a repository that points to your SMT server.

(End of Exercise)
SECTION 6  Prepare Servers for Disasters

In this section of the workbook, you learn how to do the following:

1. “Use an LVM Snapshot Volume to Create a Consistent Backup” on page 30
**Exercise 6-1  Use an LVM Snapshot Volume to Create a Consistent Backup**

In this lab, you create an LVM volume, create some files on this LVM volume, create a snapshot of the volume, and back up the snapshot.

To create a consistent backup from a snapshot LVM volume, do the following:

1. Using unused space on your hard drive on da02 or da03, create a 10 GB LVM physical volume, create a “system” LVM volume group using the entire available space, and create a 1 GB “data” logical volume. Create an ext3 file system on it and mount it to `/data/`.

2. Copy a few files to `/data/` from the `/etc/` directory.

3. Create a 200 MB LVM snapshot volume for the data LVM volume.

4. Mount the snapshot volume at `/mnt/`.

5. Compare two files under `/data/` and `/mnt/`; modify the file under `/data/` and compare again.

6. Back up the data in `/mnt/` to a tar archive or, using rsync, to another directory of your choice.

7. Unmount the snapshot and delete it.

8. Write and test a shell script that does all the above automatically when run by cron.

*(End of Exercise)*
**Exercise 6-2  Access Remote Storage Using Multipath I/O**

In this lab, you access remote storage space using iSCSI and Multipath I/O.

You create an iSCSI target on your dax1 server. When working with a partner, you have to create two iSCSI targets, one for each of you.

You then create two iSCSI initiators on your dax2/dax3 host, connecting both to your iSCSI target using different IP addresses for each initiator.

Next, you configure multipath I/O to connect to the remote storage. Finally, you partition, format, and mount the new SCSI disk that appears on your host.

To access remote storage, do the following:

1. On the dax1 server, create two 5 GB iSCSI targets, one for dax2, and one for dax3.

2. If your host (dax2 or dax3) has two NICs, make sure both can connect to the two NICs of dax1.
   
   If you have only one NIC, add an additional IP address (from a different network than the existing IP addresses) to dax1, and a matching one on your host, such as 192.168.1.1x1/24 on dax1 and 192.168.1.1x2/24 on dax2 (192.168.1.1x3/24 on dax3).

3. Create two iSCSI initiators on your dax2/dax3 host, connecting both initiators to your iSCSI target on dax1. Each initiator uses an IP address of its own.

4. Using `fdisk`, find out if the new SCSI disk appeared.

5. Enable multipathing with the `/etc/init.d/boot.multipath` script and multipathd with the `/etc/init.d/multipathd` script.

6. Create a file system on the new `/dev/dm-0` device and mount it.

7. Bring down one of the network interfaces or remove one of the IP addresses and find out if you can still access the storage device.

*(End of Exercise)*
SECTION 7  Monitor Server Health

In this section of the workbook, you learn how to do the following:

1. “Use Nagios to Monitor Network Hosts” on page 34
**Exercise 7-1  Use Nagios to Monitor Network Hosts**

In this exercise, you implement Nagios on your da\textsubscript{x}1 SLES 11 server and use it to monitor your da\textsubscript{x}2 and da\textsubscript{x}3 server systems.

To do this, you need to complete the following:

1. Configure the NTP daemons on da\textsubscript{x}2 and da\textsubscript{x}3 to get their time from da\textsubscript{x}1.

2. Install Nagios on your da\textsubscript{x}1 server by doing the following:
   a. Install the Nagios and Nagios Plugin packages on da\textsubscript{x}1.
   b. Run the `check_ssh` plugin against one of your systems from the shell prompt to verify that Nagios has been installed correctly.
   c. Run the `nagios` executable in verification mode to ensure there are no errors in its configuration files.
   d. Configure Nagios to run as a daemon and to automatically start in runlevels 3 and 5.
   e. If necessary, manually start the Nagios daemon.

3. Configure Nagios on da\textsubscript{x}1 by doing the following:
   a. Configure Apache to support Nagios and restart Apache.
   b. Test the Nagios server using the Web console. Verify that the default service definitions are being monitored on the local server (localhost).
   c. Create new host configuration files for da\textsubscript{x}2 and da\textsubscript{x}3. Create the appropriate host definitions for each host in the respective file.
   d. Modify the nagios.cfg file with the new configuration files created above.
   e. Configure service and command objects that will monitor the following on da\textsubscript{x}1 (localhost):
      - The availability of the server using PING
      - The DNS service running on the server
      - Disk space utilization on all mounted partitions
      - The Apache web server running on the server
      - Swap partition utilization
      - The overall load average on the system with warning and critical status values of your choosing.
      - Any entries in /var/log/messages that contain the text string `Error`
      - Processes on the server, sending an alert when any process’s CPU utilization exceeds 10% or 20%
      - The number of users currently logged in, generating a warning if more than 50 users are logged in and a critical warning if more than 100 users are logged in
      - The status of the SSH daemon on the server
      - That the da\textsubscript{x}2 and da\textsubscript{x}3 hosts are reachable from da\textsubscript{x}1
f. Configure da\textsubscript{1} to remotely monitor the following on da\textsubscript{2} and da\textsubscript{3} (creating all necessary service and command objects):

- Disk space utilization on all mounted partitions on both servers
- Swap partition utilization on both servers
- The overall load average on each system with warning and critical status values of your choosing
- Processes on the server, generating a warning when any process’s CPU utilization exceeds 10% and a critical status when it exceeds 20%
- The number of users currently logged in on each server, generating a warning if more than 50 users are logged in and a critical status if more than 100 users are logged in at a time
- The status of the SSH daemon on each server
- The time offset between each server and the NTP time provider (da\textsubscript{1}), with a warning generated if they are more than 10 seconds off and critical status generated if they are more than a minute off

g. Configure contact objects that will send all notifications to the root user account on da\textsubscript{1}.

(End of Exercise)