solaris

ELIMINATING WEB PAGE HIJACKING USING SOLARIS™ 10 SECURITY

> **Solaris™ 10** How To Guides

Mark Thacker, Solaris Marketing

Sun microsystems

About This Security How To Guide

This How to Guide instructs Solaris system administrators and security professionals in the process of securing common Web servers. By the end of the guide, an example configuration will be created that allows Web content to be maintained securely by content owners, while the Web server itself will run with a minimized set of privileges in its own secured Container.

Administrators are guided step-by-step through the process and at the end of the guide should be able to:

- Create a basic Solaris Container for hosting applications
- Configure the Apache2 Web server to run in a Solaris Container
- Use User and Process Rights Management to reduce application privileges
- Use the Solaris Service Manager to reduce security risk of a Container
- Share data securely between two Containers

This guide is not exhaustive and will not cover all optional features of these technologies. However, the reference section provided at the end of the document provides pointers to where administrators can learn more.

Contents

Solaris Security: An Overview **Page 1 > 2**
Solaris User and Process Rights Management Page 2
Solaris Service Manager Profiles Page 2
Solaris Containers Page 2

Build the Secured Web Server Environment **Page 2 > 2**

Create the Data Container **Page 2 > 5**

Create the Web Server Container **Page 5 > 8**

Reduce Network Exposure **Page 8 > 9**

Reduce Privileges of the Apache2 Service **Page 9 > 11**

Verify the Configuration **Page 11 > 11**

Additional Enchancements **Page 12 > 12**

Conclusion **Page 12 > 12**

For More Information **Page 13 > 13**

Security How To Guide

Solaris Security: An Overview

The Solaris 10 Operating System (OS) contains a number of breakthrough technologies for security enhancements and this guide will deal with three of them in particular:

- Solaris User and Process Rights Management
- Solaris Service Manager
- Solaris Containers

These three tools can work together to allow system administrators to secure and consolidate multiple functions or applications together on a system, without the need to change or modify existing application code.

This guide combines existing material for a unique solution to a common problem facing enterprises today: Web page hijacking. Malicious modification or *hijacking* of Web pages typically occurs when a vulnerability in a Web server application is exploited by hackers. Such vulnerabilities often allow the hacker to upload new Web pages, gain super-user shell access to a system or otherwise modify the pages that are being serviced by the Web server process. This guide shows how this issue can be easily solved without the need for costly additional software or specially modified applications.

Figure 1 is a diagram of the example configuration built in the course of this guide using Solaris 10 Operating System (OS) security features. It features a simple system with two network interfaces. One interface (bge1) is connected to a company's intranet/LAN and the other (bge0) is connected to the public Internet through a firewall or other means. The system is running the Solaris 10 OS and is configured with two Containers. One Container, the Data Container, has write access to the HTML files and is connected only to the intranet/LAN. The other Container, the Web Container, is running the Web server process itself with a reduced set of privileges. The Web Container has read-only access to the HTML files served by the Data Container.

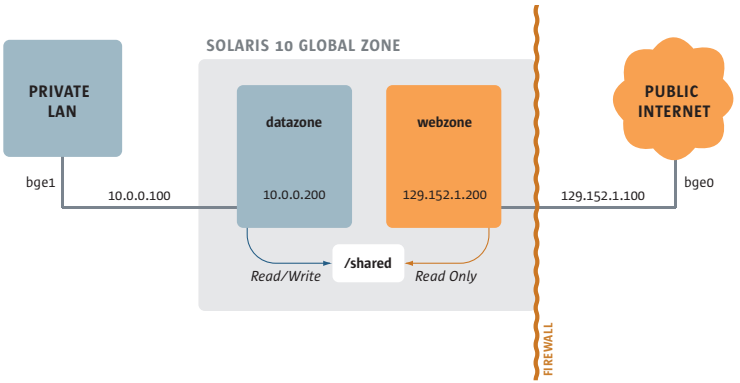

Figure 1—An Example Configuration to Prevent Web Page Hijacking

To create a secure Web server you need to use several of Solaris' newer security features that are reviewed in the following sections.

Solaris User and Process Rights Management

Solaris User Rights Management and Process Rights Management offer fine-grained privileges in the kernel and user access space of Solaris. The practical benefit of these technologies is the elimination of the need for applications or users to have unlimited access to the system in order to perform their duties. The kernel itself in Solaris 10 checks only for Process Rights Management attributes, not 'root' or super-user access. This guide utilizes Process Rights Management to run the Apache2 Web server from a non-super-user account and with just one special privilege (net_privaddr) to dramatically reduce or eliminate the risk normally associated with Web servers on Unix systems.

Solaris Service Manager Profiles

Solaris Service Manager is a new feature introduced in Solaris 10 that starts long-running processes (also referred to as *services*), monitors their status and automatically restarts services as needed. The Service Manager works with the Solaris Fault Manager to isolate and report hardware and software errors and provide graceful shutdown of services, hardware components and dependant processes. It is part of the Solaris Predictive Self-Healing functionality and is designed to aid in system administration and diagnosability.

This guide uses the Service Manager's capability to specify run-time attributes with a service, such as the privileges and userid a service runs as, to put constraints on the execution of the Apache2 Web server. This guide also uses the Service Manager's profile capability to limit what network services are running in the Web and Data Containers.

Solaris Containers

Solaris Containers are a new virtualization and security isolation technology in Solaris 10 that allows customers to securely host multiple applications on the same system. Containers make use of zones(5), privileges(5) and resource management technologies to create a secure, isolated, virtual environment. This guide uses Solaris Containers to create an isolated environment for the Apache2 Web server to run in and a separate isolated environment from which Web pages are maintained. By doing this, administration of the Web server and maintenance of the Web pages are isolated from each other. Solaris Containers also allow for audit file entries to be stored 'outside' the Container in the Global Zone, which prevents attackers from erasing the audit trail should they successfully break into a Container.

Build the Secured Web Server Environment

To build a secured system which will offer Web services, you will need to perform the following steps:

- Create the Data Container
- Create the Web Server Container
- Reduce network exposure for the Containers using the Service Manager
- Reduce the privileges associated with the Apache2 service
- Verify the configuration is working

The following four sections describe each of these steps in detail, with examples. For simplicity, assume that all commands are run as the 'root' user or another role that has appropriate authorization. Creation of such a role is outside the scope of this guide.

Create the Data Container

The Data Container in this example has the following characteristics:

- Write access to the HTML and CGI-BIN directory (located at /shared)
- Read-only access to the Apache2 log files and PID file (located at /shared/logs and /shared/run)
- Root directory mounted from /zones/datazone
- Accessible only from the private intranet/LAN interface (bge1)

This guide utilizes a unique capability of Solaris Containers to share common directories using different mount point names and different write permissions on these mount points. To clarify, Figure 2 shows how the common /shared directory is mounted in the Web and Data Containers and what write policy is used.

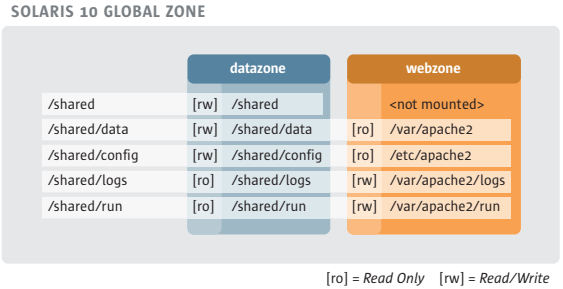

Figure 2—Shared Directory Mount Points

To create a Data Container with these characteristics, perform the following steps:

1. From the Global zone, create the /shared documents folder and populate it with Apache2 sample data files and configuration files. Note that this directory tree will be mounted by both the Data Container and the Web Container, each using a different set of write permissions.

```
# mkdir /shared
# mkdir /shared/data
# mkdir /shared/config
# mkdir /shared/logs
# mkdir /shared/run
# chown -R webservd:webservd /shared/run
# chown -R webservd:webservd /shared/logs
# mkdir /shared/data/run
# cp -R /etc/apache2/* /shared/config
# cp -R /var/apache2/* /shared/data
# mkdir /zones
```

2. Create the Data Container; specify its root directory in /zones.

```
# zonecfg -z datazone
datazone: No such zone configured Use 'create' to begin configuring a new
zone.
zonecfg:datazone> create
zonecfg:datazone> set zonepath=/zones/datazone
zonecfg:datazone> set autoboot=true
```

3. Mount the /shared directory, which contains the Apache2 configuration data, content to be served, CGI-BIN scripts and more, with Read-Write permissions at the /shared mount point of the Data Container.

```
zonecfg:datazone> add fs
zonecfg:datazone:fs> set dir=/shared
zonecfg:datazone:fs> set special=/shared
zonecfg:datazone:fs> set options=[rw,nodevices,noexec,nosuid]
zonecfg:datazone:fs> set type=lofs
zonecfg:datazone:fs> end
```

4. Mount the /shared/run directory, which contains the Apache2 PID data, with Read-Only permissions at the /shared/run mount of the Data Container.

```
zonecfg:datazone> add fs
zonecfg:datazone:fs> set dir=/shared/run
zonecfg:datazone:fs> set special=/shared/run
zonecfg:datazone:fs> set options=[ro,nodevices,noexec,nosuid]
zonecfg:datazone:fs> set type=lofs
zonecfg:datazone:fs> end
```

5. Mount the /shared/logs directory, which contains the Apache2 log data, with Read-Only permissions at the /shared/logs mount point of the Data Container. In this way, Web page content owners can analyze, but not remove or modify, Web page log files.

```
zonecfg:datazone> add fs
zonecfg:datazone:fs> set dir=/shared/logs
zonecfg:datazone:fs> set special=/shared/logs
zonecfg:datazone:fs> set options=[ro,nodevices,noexec,nosuid]
zonecfg:datazone:fs> set type=lofs
zonecfg:datazone:fs> end
```

6. Create the virtual network interface for the Container on the private/LAN interface.

```
zonecfg:datazone> add net
zonecfg:datazone:net> set address=10.0.0.200
zonecfg:datazone:net> set physical=bge1
zonecfg:datazone:net> end
```

7. Set the Containers name in the comment field. [Optional—useful if you want to check the configuration parameters later with 'zoneadm -z webzone info' from the Global Zone]

```
zonecfg:datazone> add attr
zonecfg:datazone:attr> set name=comment
zonecfg:datazone:attr> set type=string
zonecfg:datazone:attr> set value="Data Container"
zonecfg:datazone:attr> end
```

8. Verify and commit the Container.

```
zonecfg:datazone> verify
zonecfg:datazone> commit
zonecfg:datazone> exit
```

9. Install, boot and verify the Container.

```
# zoneadm -z datazone install
Preparing to install zone <datazone>.
Creating list of files to copy from the global zone.
[Some output was omitted here for brevity]
# zoneadm -z datazone boot
# zoneadm list -c -v
ID NAME             STATUS          PATH
 0 global           running         /
 1 datazone         running         /zones/datazone
```

10. Login on the console device of the Container and configure its root password information, hostname and name service data.

```
# zlogin -C datazone
SunOS Release 5.10 Version Generic_118822-22 64-bit
Copyright 1983-2005 Sun Microsystems, Inc. All rights reserved.
Use is subject to license terms.
Hostname: datazone
[Some output was omitted here for brevity]


datazone console login:
(Press ~. to disconnect from the console session)
(logout)
```

Create the Web Server Container

Creating a Container for the Web server is almost identical to the process for creating the Data Container. The only differences are:

- The Container is bound to the external interface (bge0)
- The name of the Container is “webzone”
- The Web server configuration data is mounted Read-Only
- The Web server is allowed to write to its log files via the /shared/logs directory
- The Web data files are mounted Read-Only as well

To create the Web Container, perform the following steps:

1. Create a zone; specify its root directory.

```
# zonecfg -z webzone
webzone: No such zone configured Use 'create' to begin configuring a new
zone.
zonecfg:webzone> create
zonecfg:webzone> set zonepath=/zones/webzone
zonecfg:webzone> set autoboot=true
```

2. Mount the /shared/config directory, which contains the Apache2 configuration data, with Read-Only permissions at the /etc/apache2 mount point of the Web Container.

```
zonecfg:webzone> add fs
zonecfg:webzone:fs> set dir=/etc/apache2
zonecfg:webzone:fs> set special=/shared/config
zonecfg:webzone:fs> set options=[ro,nodevices,nosuid,noexec]
zonecfg:webzone:fs> set type=lofs
zonecfg:webzone:fs> end
```

3. Mount the /shared/data directory, which contains the Apache2 HTML files, CGI-BIN scripts and other data to be served, with Read-Only permissions at the /var/apache2 mount point of the Web Container. Please note that this mount point is at the /var directory and not at the /etc directory as in the previous step.

```
zonecfg:webzone> add fs
zonecfg:webzone:fs> set dir=/var/apache2
zonecfg:webzone:fs> set special=/shared/data
zonecfg:webzone:fs> set options=[ro,nodevices,nosuid,noexec]
zonecfg:webzone:fs> set type=lofs
zonecfg:webzone:fs> end
```

4. Mount the /shared/logs directory, which contains the Apache2 log and PID data, with Read-Write permissions at the /var/apache2/logs mount point of the Web Container.

```
zonecfg:webzone> add fs
zonecfg:webzone:fs> set dir=/var/apache2/logs
zonecfg:webzone:fs> set special=/shared/logs
zonecfg:webzone:fs> set options=[rw,nodevices,nosuid,noexec]
zonecfg:webzone:fs> set type=lofs
zonecfg:webzone:fs> end
```

5. Mount the /shared/run directory, which contains the Apache2 PID data, with Read-Write permissions at the /var/apache2/run mount point of the Web Container.

```
zonecfg:webzone> add fs
zonecfg:webzone:fs> set dir=/var/apache2/run
zonecfg:webzone:fs> set special=/shared/run
zonecfg:webzone:fs> set options=[rw,nodevices,nosuid,noexec]
zonecfg:webzone:fs> set type=lofs
zonecfg:webzone:fs> end
```

6. Create the virtual network interface for the Container on the public interface.

```
zonecfg:webzone> add net
zonecfg:webzone:net> set address=129.152.1.200
zonecfg:webzone:net> set physical=bge0
zonecfg:webzone:net> end
```

7. Set the Containers name in the comment field. [Optional—useful if you want to check the configuration parameters later with 'zoneadm -z webzone info' from the Global Zone]

```
zonecfg:webzone> add attr
zonecfg:webzone:attr> set name=comment
zonecfg:webzone:attr> set type=string
zonecfg:webzone:attr> set value="Web Container"
zonecfg:webzone:attr> end
```

8. Verify and commit the Container.

```
zonecfg:webzone> verify
zonecfg:webzone> commit
zonecfg:webzone> exit
```

9. Install, boot and verify the Container.

```
# zoneadm -z webzone install
Preparing to install zone <webzone>.
Creating list of files to copy from the global zone.
[Some output was omitted here for brevity]
# zoneadm -z webzone boot
# zoneadm list -c -v
ID NAME             STATUS          PATH
 0 global           running         /
 1 datazone         running         /zones/datazone
 2 webzone          running         /zones/webzone
```

10. Log in on the console device of the Container and configure its root password information, hostname and name service data.

```
# zlogin -C webzone
SunOS Release 5.10 Version Generic_118822-22 64-bit
Copyright 1983-2005 Sun Microsystems, Inc. All rights reserved.
Use is subject to license terms.
Hostname: webzone
[Some output was omitted here for brevity]


webzone console login:
(Press ~. to disconnect from the consoles session)
(logout)
```

Reduce Network Exposure

To reduce the network services exposed to possible attack, use the profile capability of the Solaris Service Manager. In this example you will change the default services profile by loading the Generic Limited Networking profile. This profile minimizes the set of network services in each Container. However, the Generic Limited Networking profile is not the only method you can use to secure your system. There may be additional services that you wish to stop or disable. You may use the Services Manager svcadm(1M) command to disable services on a per-Container basis, or you may utilize the Solaris Security Toolkit.

Use of the Solaris Security Toolkit is not covered in this guide, please see the reference material.

1. Enable the Generic Limited Networking profile for the Web Container to be the default profile and apply it to the running copy of the Container.

```
# zlogin webzone
[Some output was omitted here for brevity]
webzone console login: root
Password: <enter password here>

# cd /var/svc/profile
# rm generic.xml
# ln -s generic_limited_net.xml generic.xml
# svccfg apply /var/svc/profile/generic_limited_net.xml
# exit
```

2. Apply the same changes to the Data Container.

```
# zlogin datazone
[Some output was omitted here for brevity]
datazone console login: root
Password: <enter password here>

# cd /var/svc/profile
# rm generic.xml
# ln -s generic_limited_net.xml generic.xml
# svccfg apply /var/svc/profile/generic_limited_net.xml
# exit
```

Now that the default services profile has been changed, each of the Containers will run with a reduced set of network services. Each Container can have its own unique services profile, so system administrators can selectively enable services such as FTP for the Data Container while allowing only ssh(1) access for the Web Container.

Reduce Privileges of the Apache2 Service

Next, modify the Apache2 configuration file to use the new directories. This allows the Apache2 server to have write access for logging and PID information. Also, use the Service Manager to modify the privileges that the Apache2 Web server receives. Here is an outline of the steps required:

- Run the Apache2 Web server as userid 'webservd' rather than 'root'
- Grant just the three needed privileges to the Apache2 Web server: proc_exec, proc_fork and net_privaddr
- Change ownerships of the needed log files for Apache2
- Change the Apache2 configuration file to utilize the new Web Container directories
- Verify the Apache2 server is running with fewer privileges

It's worth noting that these extra steps are taken to further harden and reduce the risk of intrusion with the Apache2 Web service only within the Web Container. The services used in the Data Container already run with reduced privileges set as their default behavior in the Solaris 10 OS.

1. From the Global Zone, change the Apache2 httpd.conf file to use the new directories by editing two lines. Remember that the rest of the httpd.conf file settings for directories are generally fine as the Web Container mounts /shared/config as /etc/apache2 and /shared/data as /var/apache2, which are the default directories that Apache2 looks for.

```
# vi /shared/config/httpd.conf

[Some output was omitted here for brevity]
LockFile /var/apache2/logs/accept.lock
[Some output was omitted here for brevity]
PidFile /var/apache2/run/httpd.pid
[Some output was omitted here for brevity]
```

2. Log in to the Web Container to begin the modifications.

```
# zlogin webzone
[Some output was omitted here for brevity]
webzone console login: root
webzone console login: <password here>
webzone >
```

3. Modify the userid and group that the Apache2 service uses.

```
# svccfg -s apache2
svc:/network/http:apache2> setprop start/user = astring: webservd
svc:/network/http:apache2> setprop start/group = astring: webservd
```

4. Reduce the privileges the Apache2 service uses to just those necessary, complete the definition of the service and refresh the service.

```
svc:/network/http:apache2> setprop start/privileges = astring:
basic,!proc_session,!proc_info,!file_link_any,net_privaddr
svc:/network/http:apache2> setprop start/limit_privileges = astring: :default
svc:/network/http:apache2> setprop start/use_profile = boolean: false
svc:/network/http:apache2> setprop start/supp_groups = astring: :default
svc:/network/http:apache2> setprop start/working_directory = astring:
:default
svc:/network/http:apache2> setprop start/project = astring: :default
svc:/network/http:apache2> setprop start/resource_pool = astring: :default
svc:/network/http:apache2> end

# svcadm -v refresh apache2
```

5. Verify that the Apache2 service is running with fewer privileges by restarting it, verifying that there are no 'root' processes and using the ppriv(1) command to verify the reduced set of privileges used by the service. Note the output of the 'ppriv' command shows the Apache2 Web server running with just three privileges.

```
# svcadm -v enable -s apache2
svc:/network/http:apache2 enabled.
# svcs apache2
STATE STIME FMRI
online 12:02:21 svc:/network/http:apache2

# ps -aef | grep httpd | grep -v grep
webservd 5568 5559 0 12:02:22 ? 0:00 /usr/apache2/bin/httpd -k start
webservd 5567 5559 0 12:02:22 ? 0:00 /usr/apache2/bin/httpd -k start
webservd 5561 5559 0 12:02:22 ? 0:00 /usr/apache2/bin/httpd -k start
webservd 5562 5559 0 12:02:22 ? 0:00 /usr/apache2/bin/httpd -k start
webservd 5563 5559 0 12:02:22 ? 0:00 /usr/apache2/bin/httpd -k start
webservd 5559 23382 0 12:02:21 ? 0:00 /usr/apache2/bin/httpd -k start

# ppriv -S 5559         #This is the starting process
5559: /usr/apache2/bin/httpd -k start
flags = <none>
E: net_privaddr,proc_exec,proc_fork
I: net_privaddr,proc_exec,proc_fork
P: net_privaddr,proc_exec,proc_fork
L: zone
```

Verify the Configuration

At this point, the Apache2 Web server is running inside of its own Web Container, with reduced exposure on the network and with reduced privileges. It is also serving HTML files to which it has read only access. If the Web server is attacked or compromised, the HTML data files to which it is providing access cannot be damaged because of the security constraints placed by Process Rights Management and Solaris Containers.

To verify configuration, connect to the Web server's IP address from your desktop session with a Web browser. You should see the Apache2 Documentation page.

For command-line verification, you can also use the ‘telnet 129.152.1.200 80’ command to connect to the Web server port and enter ‘HEAD / HTTP/1.0’, which will return the default Apache2 Web page.

For further verification, connect from a system on the private/LAN network and modify an HTML page. You will notice that your Web server has immediate access to that modified Web page. Remember that Web page authors will modify the content in the /shared/data directory while logged into the Data Container. The Web server Container will see these changes automatically because it mounts the exact same directory as /var/apache2.

Additional Enhancements

As with any complex system, there are a variety of areas for enhancement in a sample configuration such as this. Additional topics include:

- Configuring users and roles for both data management and for eliminating the need for using the 'root' role
- Using Resource Management to dynamically control the CPU, memory and network resources assigned to Containers
- Securing the Global Zone / Container to treat it more as a privileged console
- Adding Secure Sockets Layer to the Apache2 service for encrypted communications
- Performance tuning of the Apache2 Web service
- Configuring the IP Filter firewall for the Global zone to reduce network exposure
- Utilizing the BART file integrity checking tool to monitor for additional unwanted data or system file modifications
- Utilizing the Solaris Security Toolkit to reduce network exposure and risk

See the For More Information section for details on how to implement these enhancements.

Conclusion

This guide has explored combining various technologies to address the common issue of Web server security and Web page defacement. Because of the advances in Solaris 10 OS security, system administrators have new possibilities open to them to solve problems that previously would have taken many more systems, complex add-on products, changes in networking topology or other such compromises. Explore additional Sun documentation and articles for more ideas on how to use the Solaris 10 OS to creatively solve your business and security issues.

For More Information

How To Guides	
Consolidating Servers and Applications with Solaris Containers *by Joost Pronk van Hoogeveen,* *Solaris 10 How To Guides, January 2006*	www.sun.com/software/solaris/howtoguides/containersLowRes.jsp
BluePrints OnLine	
Solaris Security Toolkit v4.2	www.sun.com/download/products.xml?id=42e6becd
Limiting Service Privileges in the Solaris 10 Operating System *by Glenn Brunette, Sun BluePrints OnLine, May 2005*	www.sun.com/blueprints/0505/819-2680.pdf
Web Consolidation on the SunFire T1000 Server Using Solaris Containers *by Kevin Kelly, Sun BluePrints OnLine, December 2005*	www.sun.com/blueprints/1205/819-5149.pdf
Enforcing the Two-Person Rule Via Role Based Access Control in Solaris 10 *by Glenn Brunette, Sun BluePrints OnLine, August 2005*	www.sun.com/blueprints/0805/819-3164.pdf
Integrating BART and the Fingerprint Database in the Solaris 10 Operating System *by Glenn Brunette, Sun BluePrints OnLine, April 2005*	www.sun.com/blueprints/0405/819-2260.pdf
Manuals (All reference manuals based on the Solaris 10 3/05 release)	
System Administration Guide: Solaris Containers Resource Management and Solaris Zones	docs.sun.com/app/docs/doc/817-1592
System Administration Guide: Security Services	docs.sun.com/app/docs/doc/816-4557
Solaris Administration Guide: Basic Administration	docs.sun.com/app/docs/doc/817-1985
Sun Employee Blogs	
Glenn Brunette	blogs.sun.com/gbrunett
Alec Muffat	www.crypticide.com/dropsafe
Casper Dik	blogs.sun.com/casper
Wyllys Ingersoll	blogs.sun.com/wyllys
OpenSolaris Articles	
Privilege Bracketing in Solaris and OpenSolaris *by Glenn Brunette*	www.opensolaris.org/os/community/security/library/howto/privbracket
Whitepapers	
Solaris 10 Operating System: Unparalleled Security	www.sun.com/software/whitepapers/solaris10/s10security.pdf
Education Resources	
Solaris OS Security Administration: Course Overview	www.sun.com/training/catalog/operating_systems/security_admin.html
Solaris 10—Ten Moves Ahead of the Competition: Course Overview	www.sun.com/training/catalog/courses/WS-245.xml

sun.com/solaris

Sun Microsystems, Inc. 4150 Network Circle, Santa Clara, CA 95054 USA Phone 1-650-960-1300 or 1-800-555-9SUN Web sun.com