

Sun Server X3-2 (formerly Sun fire X4170 M3)

Security Guide



Part No.: E26714-05
May 2014

Copyright © 2013, 2014 Oracle and/or its affiliates. All rights reserved.

This software and related documentation are provided under a license agreement containing restrictions on use and disclosure and are protected by intellectual property laws. Except as expressly permitted in your license agreement or allowed by law, you may not use, copy, reproduce, translate, broadcast, modify, license, transmit, distribute, exhibit, perform, publish, or display any part, in any form, or by any means. Reverse engineering, disassembly, or decompilation of this software, unless required by law for interoperability, is prohibited.

The information contained herein is subject to change without notice and is not warranted to be error-free. If you find any errors, please report them to us in writing.

If this is software or related software documentation that is delivered to the U.S. Government or anyone licensing it on behalf of the U.S. Government, the following notice is applicable:

U.S. GOVERNMENT END USERS. Oracle programs, including any operating system, integrated software, any programs installed on the hardware, and/or documentation, delivered to U.S. Government end users are "commercial computer software" pursuant to the applicable Federal Acquisition Regulation and agency-specific supplemental regulations. As such, use, duplication, disclosure, modification, and adaptation of the programs, including any operating system, integrated software, any programs installed on the hardware, and/or documentation, shall be subject to license terms and license restrictions applicable to the programs. No other rights are granted to the U.S. Government.

This software or hardware is developed for general use in a variety of information management applications. It is not developed or intended for use in any inherently dangerous applications, including applications which may create a risk of personal injury. If you use this software or hardware in dangerous applications, then you shall be responsible to take all appropriate fail-safe, backup, redundancy, and other measures to ensure its safe use. Oracle Corporation and its affiliates disclaim any liability for any damages caused by use of this software or hardware in dangerous applications.

Oracle and Java are registered trademarks of Oracle and/or its affiliates. Other names may be trademarks of their respective owners.

Intel and Intel Xeon are trademarks or registered trademarks of Intel Corporation. All SPARC trademarks are used under license and are trademarks or registered trademarks of SPARC International, Inc. AMD, Opteron, the AMD logo, and the AMD Opteron logo are trademarks or registered trademarks of Advanced Micro Devices. UNIX is a registered trademark of The Open Group.

This software or hardware and documentation may provide access to or information on content, products, and services from third parties. Oracle Corporation and its affiliates are not responsible for and expressly disclaim all warranties of any kind with respect to third-party content, products, and services. Oracle Corporation and its affiliates will not be responsible for any loss, costs, or damages incurred due to your access to or use of third-party content, products, or services.

Copyright © 2013, 2014 Oracle et/ou ses affiliés. Tous droits réservés.

Ce logiciel et la documentation qui l'accompagne sont protégés par les lois sur la propriété intellectuelle. Ils sont concédés sous licence et soumis à des restrictions d'utilisation et de divulgation. Sauf disposition de votre contrat de licence ou de la loi, vous ne pouvez pas copier, reproduire, traduire, diffuser, modifier, breveter, transmettre, distribuer, exposer, exécuter, publier ou afficher le logiciel, même partiellement, sous quelque forme et par quelque procédé que ce soit. Par ailleurs, il est interdit de procéder à toute ingénierie inverse du logiciel, de le désassembler ou de le décompiler, excepté à des fins d'interopérabilité avec des logiciels tiers ou tel que prescrit par la loi.

Les informations fournies dans ce document sont susceptibles de modification sans préavis. Par ailleurs, Oracle Corporation ne garantit pas qu'elles soient exemptes d'erreurs et vous invite, le cas échéant, à lui en faire part par écrit.

Si ce logiciel, ou la documentation qui l'accompagne, est concédé sous licence au Gouvernement des Etats-Unis, ou à toute entité qui délivre la licence de ce logiciel ou l'utilise pour le compte du Gouvernement des Etats-Unis, la notice suivante s'applique :

U.S. GOVERNMENT END USERS. Oracle programs, including any operating system, integrated software, any programs installed on the hardware, and/or documentation, delivered to U.S. Government end users are "commercial computer software" pursuant to the applicable Federal Acquisition Regulation and agency-specific supplemental regulations. As such, use, duplication, disclosure, modification, and adaptation of the programs, including any operating system, integrated software, any programs installed on the hardware, and/or documentation, shall be subject to license terms and license restrictions applicable to the programs. No other rights are granted to the U.S. Government.

Ce logiciel ou matériel a été développé pour un usage général dans le cadre d'applications de gestion des informations. Ce logiciel ou matériel n'est pas conçu ni n'est destiné à être utilisé dans des applications à risque, notamment dans des applications pouvant causer des dommages corporels. Si vous utilisez ce logiciel ou matériel dans le cadre d'applications dangereuses, il est de votre responsabilité de prendre toutes les mesures de secours, de sauvegarde, de redondance et autres mesures nécessaires à son utilisation dans des conditions optimales de sécurité. Oracle Corporation et ses affiliés déclinent toute responsabilité quant aux dommages causés par l'utilisation de ce logiciel ou matériel pour ce type d'applications.

Oracle et Java sont des marques déposées d'Oracle Corporation et/ou de ses affiliés. Tout autre nom mentionné peut correspondre à des marques appartenant à d'autres propriétaires qu'Oracle.

Intel et Intel Xeon sont des marques ou des marques déposées d'Intel Corporation. Toutes les marques SPARC sont utilisées sous licence et sont des marques ou des marques déposées de SPARC International, Inc. AMD, Opteron, le logo AMD et le logo AMD Opteron sont des marques ou des marques déposées d'Advanced Micro Devices. UNIX est une marque déposée d'The Open Group.

Ce logiciel ou matériel et la documentation qui l'accompagne peuvent fournir des informations ou des liens donnant accès à des contenus, des produits et des services émanant de tiers. Oracle Corporation et ses affiliés déclinent toute responsabilité ou garantie expresse quant aux contenus, produits ou services émanant de tiers. En aucun cas, Oracle Corporation et ses affiliés ne sauraient être tenus pour responsables des pertes subies, des coûts occasionnés ou des dommages causés par l'accès à des contenus, produits ou services tiers, ou à leur utilisation.



Contents

Sun Server X3-2 Security Guide	1
Security Principles	1
Using Server Configuration and Management Tools	3
Oracle System Assistant Security	3
Oracle ILOM Security	4
Oracle Hardware Management Pack Security	6
Planning a Secure Environment	7
Password Protection	7
Oracle Operating System Guidelines	8
Network Ports and Switches	8
VLAN Security	9
Infiniband Security	9
Maintaining a Secure Environment	10
Hardware Power Control	10
Asset Tracking	10
Updates for Software and Firmware	11
Network Security	11
Data Protection and Security	12
Log Maintenance	12

Sun Server X3-2 Security Guide

This document provides general security guidelines to help you protect the Oracle Sun Server X3-2, its network interfaces, and the network switches to which it is connected.

Contact your IT Security Officer for additional security requirements that pertain to your system and specific environment.

The following sections are in this chapter:

- [“Security Principles” on page 1](#)
- [“Using Server Configuration and Management Tools” on page 3](#)
- [“Planning a Secure Environment” on page 7](#)
- [“Maintaining a Secure Environment” on page 10](#)

Security Principles

There are four basic security principles: access, authentication, authorization, and accounting.

Contact your IT Security Officer for additional security requirements that pertain to your system and specific environment.

■ Access

Access refers to physical access to hardware, or physical or virtual access to software.

- Use physical and software controls to protect your hardware and data from intrusion.
- Change all default passwords when installing a new system. Most types of equipment use default passwords, such as `changeme`, that are widely known and could allow unauthorized access to hardware or software.
- Refer to the documentation that came with your software to enable any security features available for the software.

- Install servers and related equipment in a locked, restricted access room.
- If equipment is installed in a rack with a locking door, keep the door locked except when you have to service components in the rack.
- Restrict access to connectors or ports, which can provide more powerful access than SSH connections. Devices such as system controllers, power distribution units (PDUs), and network switches provide connectors and ports.
- Restrict access to hot-plug or hot-swap devices in particular because they can be easily removed.
- Store spare field-replaceable units (FRUs) and customer-replaceable units (CRUs) in a locked cabinet. Restrict access to the locked cabinet to authorized personnel.

■ **Authentication**

Authentication refers to ensuring that users of hardware or software are who they say they are.

- Set up authentication features such as a password system in your platform operating systems to ensure that users are who they say they are.
- Ensure that your personnel use employee badges properly to enter the computer room.
- For user accounts: use access control lists where appropriate; set time-outs for extended sessions; set privilege levels for users.

■ **Authorization**

Authorization refers to restrictions placed on personnel to work with hardware or software.

- Allow personnel to work only with hardware and software that they are trained and qualified to use.
- Set up a system of Read/Write/Execute permissions to control user access to commands, disk space, devices, and applications.

■ **Accounting**

Accounting refers to software and hardware features used to monitor login activity and maintenance of hardware inventories.

- Use system logs to monitor user logins. Monitor system administrator and service accounts in particular because those accounts can access powerful commands.
- Keep a record of the serial numbers of all your hardware. Use component serial numbers to track system assets. Oracle part numbers are electronically recorded on cards, modules, and motherboards, and can be used for inventory purposes.
- To detect and track components, provide a security mark on all significant items of computer hardware such as FRUs. Use special ultraviolet pens or embossed labels.

Using Server Configuration and Management Tools

Follow these security guidelines when using software and firmware tools to configure and manage your server.

- “Oracle System Assistant Security” on page 3
- “Oracle ILOM Security” on page 4
- “Oracle Hardware Management Pack Security” on page 6

Contact your IT Security Officer for additional security requirements that pertain to your system and specific environment.

Oracle System Assistant Security

Oracle System Assistant is a preinstalled tool that helps you to locally or remotely configure and update server hardware, and to install supported operating systems. For information about how to use Oracle System Assistant, refer to the *Sun Server X3-2 (formerly Sun Fire X4170 M3) Administration Guide* at:

http://docs.oracle.com/cd/E22368_01/pdf/E22365.pdf

The following information will help you to understand security issues related to Oracle System Assistant.

- **Oracle System Assistant contains a bootable root environment**

Oracle System Assistant is an application that runs on a preinstalled, internal USB flash drive. It is built on top of a bootable Linux root environment. Oracle System Assistant also provides the ability to access its underlying root shell. Users who have physical access to the system, or who have remote KVMs (keyboard, video, mouse, and storage) access to the system through Oracle ILOM, will be able to access Oracle System Assistant and the root shell.

A root environment can be used to change system configuration and policies, as well as to access data on other disks. To increase security, protect physical access to the server and assign administrator and console privileges for Oracle ILOM users sparingly.

The Oracle System Assistant shell is designed to permit users with appropriate privileges to use the Oracle Hardware Management Pack CLI Tools for systems management purposes. The shell is not designed to provide network services. These are disabled by default to ensure the highest level of security and should not be enabled.

- **Oracle System Assistant mounts a USB storage device that is accessible to the operating system**

In addition to being a bootable environment, Oracle System Assistant is also mounted as a USB storage device (flash drive) that is accessible to the host operating system after installation. This is useful when accessing tools and drivers for maintenance and reconfiguration. The Oracle System Assistant USB storage device is both readable and writable and could potentially be exploited by viruses.

For increased security, apply to the Oracle System Assistant storage device the same methods you use for protecting disks, including regular virus scans and integrity checking.

- **Oracle System Assistant can be disabled**

Oracle System Assistant is a useful tool to help set up the server, update and configure firmware, and install the host operating system. However, if the security implications described above are unacceptable, or if the tool is not needed, Oracle System Assistant can be disabled. Disabling Oracle System Assistant means that the USB storage device will no longer be accessible to the host operating system. In addition, it will not be possible to boot Oracle System Assistant.

You can disable Oracle System Assistant from either the tool itself or from BIOS. Once disabled, Oracle System Assistant can only be re-enabled from the BIOS Setup Utility. It is recommended that BIOS Setup be password-protected so that only authorized users can re-enable Oracle System Assistant.

- **Refer to the Oracle System Assistant documentation**

For information about Oracle System Assistant features and functions, refer to the *Sun Server X3-2 (formerly Sun Fire X4170 M3) Administration Guide* at:

http://docs.oracle.com/cd/E22368_01/pdf/E22365.pdf

Oracle ILOM Security

You can actively secure, manage, and monitor system components using Oracle Integrated Lights Out Manager (ILOM) management firmware, which is embedded on Oracle x86-based servers and Oracle SPARC-based servers. Depending on the authorization level granted to system administrators, functions might include the ability to power off the server, create user accounts, mount remote storage devices, and so on.

- **Use a secure, internal trusted network**

Whether you establish a physical management connection to Oracle ILOM through the local serial port, dedicated network management port, or the standard data network port, it is essential that this physical port on the server is always connected to an internal trusted network, or a dedicated secure management or private network.

Never connect the Oracle ILOM service processor (SP) to a public network, such as the Internet. You should keep the Oracle ILOM SP management traffic on a separate management network and grant access only to system administrators.

- **Limit the use of the default Administrator account**

Limit the use of the default Administrator account (`root`) to the initial Oracle ILOM login. This default Administrator account is provided only to aid with the initial server installation. Therefore, to ensure the most secure environment, you must change the default Administrator password (`changeme`) as part of the initial setup of the system. Gaining access to the default Administrator account gives a user unrestricted access to all features of Oracle ILOM. In addition, establish new user accounts with unique passwords and assigned authorization levels (user roles) for each new Oracle ILOM user.

- **Carefully consider risks when connecting the serial port to a terminal server**

Terminal devices do not always provide the appropriate levels of user authentication or authorization that are required to secure the network from malicious intrusions. To protect your system from unwanted network intrusions, do not establish a serial connection (serial port) to Oracle ILOM through any type of network redirection device, such as a terminal server, unless the server has sufficient access controls.

In addition, certain Oracle ILOM functions, such as password reset and the Preboot menu, are only made available using the physical serial port. Connecting the serial port to a network using an unauthenticated terminal server removes the need for physical access, and lowers the security associated with these functions.

- **Access to the Preboot menu requires physical access to the server**

The Oracle ILOM Preboot menu is a powerful utility that provides a way to reset Oracle ILOM to default values, and to flash firmware if Oracle ILOM were to become unresponsive. Once Oracle ILOM has been reset, a user is then required to either press a button on the server (the default) or type a password. The Oracle ILOM Physical Presence property controls this behavior (`check_physical_presence=true`). For maximum security when accessing the Preboot menu, do not change the default setting (`true`), so that access to the Preboot menu always requires physical access to the server.

- **Refer to the Oracle ILOM documentation**

Refer to Oracle ILOM documentation to learn more about setting up passwords, managing users, and applying security-related features. For security guidelines that are specific to Oracle ILOM, refer to the *Oracle ILOM Security Guide*, which is part of the Oracle ILOM documentation library. You can find the Oracle ILOM documentation at:

<http://www.oracle.com/goto/ILOM/docs>

Oracle Hardware Management Pack Security

Oracle Hardware Management Pack is available for your server, and for many other x86-based servers and some SPARC servers. Oracle Hardware Management Pack features two components: an SNMP monitoring agent and a family of cross-operating system command-line interface tools (CLI Tools) for managing your server.

■ Use Hardware Management Agent SNMP Plugins

SNMP is a standard protocol used to monitor or manage a system. With the Hardware Management Agent SNMP Plugins, you can use SNMP to monitor Oracle servers in your data center with the advantage of not having to connect to two management points, the host and Oracle ILOM. This functionality enables you to use a single IP address (the host's IP address) to monitor multiple servers.

The SNMP Plugins run on the host operating system of Oracle servers. The SNMP Plugin module extends the native SNMP agent in the host operating system to provide additional Oracle MIB capabilities. Oracle Hardware Management Pack itself does not contain an SNMP agent. For Linux, a module is added to the net-snmp agent. For Solaris, a module is added to the Solaris Management Agent. For Windows, the Plugin extends the native SNMP service. Any security settings related to SNMP for the Oracle Hardware Management Pack are determined by the settings of the native SNMP agent or service, and not by the Plugin.

Note that SNMPv1 and SNMP v2c provide no encryption and use community strings as a form of authentication. SNMPv3 is more secure and is the recommended version to use because it employs encryption to provide a secure channel, as well as individual user names and passwords.

■ Refer to the Oracle Hardware Management Pack documentation

Refer to the Oracle Hardware Management Pack documentation for more information about these features. For security guidelines that are specific to Oracle Hardware Management Pack, refer to the *Oracle Hardware Management Pack (HMP) Security Guide*, which is part of the Oracle Hardware Management Pack documentation library. You can find the Oracle Hardware Management Pack documentation at:

<http://www.oracle.com/goto/OHMP/docs>

Planning a Secure Environment

Use the following information when installing and configuring the server and related equipment.

- “Password Protection” on page 7
- “Oracle Operating System Guidelines” on page 8
- “Network Ports and Switches” on page 8
- “VLAN Security” on page 9
- “Infiniband Security” on page 9

Contact your IT Security Officer for additional security requirements that pertain to your system and specific environment.

Password Protection

Passwords are an important aspect of security since poorly chosen passwords could result in unauthorized access to company resources. Implementing password management best practices ensures that users adhere to a set of guidelines for creating and protecting their passwords. Typical components of a password policy should define:

- Password length and strength
- Password duration
- Common password practice

Enforce the following standard practices for creating strong complex passwords:

- Do not create a password that contains the user name, employee name, or family names.
- Do not select passwords that are easy to guess.
- Do not create passwords that contain a consecutive string of numbers such as 12345.
- Do not create passwords that contain a word or string that is easily discovered by a simple Internet search.
- Do not allow users to reuse the same password across multiple systems.
- Do not allow users to reuse old passwords.

Change passwords on a regular basis. This helps to prevent malicious activity and ensures that passwords adhere to current password policies.

Oracle Operating System Guidelines

Refer to Oracle operating system (OS) documents for information on:

- How to use security features when configuring your systems
- How to operate securely when you add applications and users to a system
- How to protect network-based applications

Security Guide documents for supported Oracle operating systems are part of the documentation library for the operating system. To find the Security Guide document for an Oracle operating system, go to the Oracle operating system documentation library:

- **Oracle Solaris 10 1/13** - <http://www.oracle.com/technetwork/documentation/solaris-11-192991.html>
- **Oracle Solaris 11.x** - <http://www.oracle.com/goto/Solaris11/docs>
- **Oracle Linux 6** - <http://www.oracle.com/technetwork/documentation/ol-1-1861776.html>
- **Oracle VM 3.x** - <http://www.oracle.com/technetwork/documentation/vm-096300.html>

For information on operating systems from other vendors, such as Red Hat Enterprise Linux, SUSE Linux Enterprise Server, Windows, and VMware ESXi, refer to the vendor's documentation.

Network Ports and Switches

Different switches offer different levels of port security features. Refer to the switch documentation to learn how to do the following.

- Use authentication, authorization, and accounting features for local and remote access to the switch.
- Change every password on network switches that might have multiple user accounts and passwords by default.
- Manage switches out-of-band (separated from data traffic). If out-of-band management is not feasible, then dedicate a separate virtual local area network (VLAN) number for in-band management.
- Use the port mirroring capability of the network switch for intrusion detection system (IDS) access.
- Maintain a switch configuration file off-line and limit access only to authorized administrators. The configuration file should contain descriptive comments for each setting.

- Implement port security to limit access based upon MAC addresses. Disable auto-trunking on all ports.
- Use these port security features if they are available on your switch:
 - **MAC Locking** involves associating a Media Access Control (MAC) address of one or more connected devices to a physical port on a switch. If you lock a switch port to a particular MAC address, superusers cannot create backdoors into your network with rogue access points.
 - **MAC Lockout** disables a specified MAC address from connecting to a switch.
 - **MAC Learning** uses the knowledge about each switch port's direct connections so that the network switch can set security based on current connections.

VLAN Security

If you set up a virtual local area network (VLAN), remember that VLANs share bandwidth on a network and require additional security measures.

- Define VLANs to separate sensitive clusters of systems from the rest of the network. This decreases the likelihood that users will gain access to information on these clients and servers.
- Assign a unique native VLAN number to trunk ports.
- Limit the VLANs that can be transported over a trunk to only those that are strictly required.
- Disable VLAN Trunking Protocol (VTP), if possible. Otherwise, set the following for VTP: management domain, password and pruning. Then set VTP into transparent mode.

Infiniband Security

Keep Infiniband hosts secure. An Infiniband fabric is only as secure as its least secure Infiniband host.

- Note that partitioning does not protect an Infiniband fabric. Partitioning only offers Infiniband traffic isolation between virtual machines on a host.
- Use static VLAN configuration, when possible.
- Disable unused switch ports and assign them an unused VLAN number.

Maintaining a Secure Environment

After the initial installation and configuration, use Oracle hardware and software security features to continue controlling hardware and tracking system assets.

- “Hardware Power Control” on page 10
- “Asset Tracking” on page 10
- “Updates for Software and Firmware” on page 11
- “Network Security” on page 11
- “Data Protection and Security” on page 12
- “Log Maintenance” on page 12

Contact your IT Security Officer for additional security requirements that pertain to your system and specific environment.

Hardware Power Control

You can use software to turn power on and off to some Oracle systems. The power distribution units (PDUs) for some system cabinets can be enabled and disabled remotely. Authorization for these commands is typically set up during system configuration and is usually limited to system administrators and service personnel. Refer to your system or cabinet documentation for further information.

Asset Tracking

Use serial numbers to track inventory. Oracle embeds serial numbers in firmware on option cards and system motherboards. You can read these serial numbers through local area network connections.

You can also use wireless radio frequency identification (RFID) readers to further simplify asset tracking. An Oracle white paper, *How to Track Your Oracle Sun System Assets by Using RFID*, is available at:

<http://www.oracle.com/technetwork/articles/systems-hardware-architecture/o11-001-rfid-oracle-214567.pdf>

Updates for Software and Firmware

For security reasons, update the firmware on your system with the most recent firmware whenever a new version becomes available. This is important so that you take advantage of bug fixes and enhancements that improve the overall quality and security of the system.

- Check regularly for updates.
- Always install the latest released version of the software or firmware.
- Install any necessary security patches for your software.
- Remember that devices such as network switches also contain firmware and might require patches and firmware updates.

Network Security

Follow these guidelines to secure local and remote access to your systems.

- Limit remote configuration to specific IP addresses using SSH instead of Telnet. Telnet passes user names and passwords in clear text, potentially allowing everyone on the LAN segment to see login credentials. Set a strong password for SSH.
- Use version 3 of Simple Network Management Protocol (SNMP) to provide secure transmissions. Earlier versions of SNMP are not secure and transmit authentication data in unencrypted text.
- Change the default SNMP community string to a strong community string if SNMP is necessary. Some products have PUBLIC set as the default SNMP community string. Attackers can query a community to draw a very complete network map and possibly modify management information base (MIB) values.
- Always log out after using the system controller if it uses a browser interface.
- Disable unnecessary network services, such as Transmission Control Protocol (TCP) or Hypertext Transfer Protocol (HTTP). Enable necessary network services and configure these services securely.
- Create a banner message that appears at login to state that unauthorized access is prohibited. You can inform users of any important policies or rules. The banner can be used to warn users of special access restrictions for a given system, or to remind users of password policies and appropriate use.
- Use access control lists where appropriate.
- Set time-outs for extended sessions and set privilege levels.
- Use authentication, authorization, and accounting features for local and remote access to a switch.
- If possible, use the RADIUS and TACACS+ security protocols:

- RADIUS (Remote Authentication Dial In User Service) is a client/server protocol that secures networks against unauthorized access.
- TACACS+ (Terminal Access Controller Access-Control System) is a protocol that permits a remote access server to communicate with an authentication server to determine if a user has access to the network.
- Follow LDAP security measures when using LDAP to access the system.
- Use the port mirroring capability of the switch for intrusion detection system (IDS) access.
- Implement port security to limit access based on a MAC address. Disable auto trunking on all ports.

For more information about network security, refer to the *Oracle ILOM Security Guide*, which is part of the Oracle ILOM documentation library. You can find the Oracle ILOM documentation at:

<http://www.oracle.com/goto/ILOM/docs>

Data Protection and Security

Follow these guidelines to maximize data protection and security.

- Back up important data using devices such as external hard drives or USB storage devices. Store the backed up data in a second, off-site, secure location.
- Use data encryption software to keep confidential information on hard drives secure.
- When disposing of an old hard drive, physically destroy the drive or completely erase all the data on the drive. Information can still be recovered from a drive after files are deleted or the drive has been reformatted. Deleting the files or reformatting the drive removes only the address tables on the drive. Use disk wiping software to completely erase all data on a drive.

Log Maintenance

Inspect and maintain your log files on a regular schedule. Use these methods to secure log files.

- Enable logging and send system logs to a dedicated secure log host.
- Configure logging to include accurate time information, using Network Time Protocol (NTP) and timestamps.
- Perform regularly scheduled scans of network device logs for unusual network activity or access.

- Review logs for possible incidents and archive them in accordance with a security policy.
- Periodically retire log files when they exceed a reasonable size. Maintain copies of the retired files for possible future reference or statistical analysis.

