

Oracle Sun Data Center InfiniBand Switch 36

Security Configuration Supplement for the
United States Department of Defense

ORACLE WHITE PAPER | SEPTEMBER 2016





Table of Contents

| | |
|---|----|
| Overview | 3 |
| Product Description | 3 |
| Product Security Guide | 3 |
| Version and Update Information | 4 |
| Security Configuration Information | 4 |
| Default Accounts and Passwords | 4 |
| Default Exposed Network Services | 5 |
| Security Configuration Hardening | 6 |
| Disable Unnecessary Services | 6 |
| Disable HTTP service | 7 |
| Disable NTP Protocol | 7 |
| Disable Unapproved SNMP Protocols | 8 |
| Configure SNMP Community Strings | 8 |
| Replace Default Self-Signed Certificates | 9 |
| Configure Administrative Interface Inactivity Timeout (CLI) | 9 |
| Management Network Recommendations | 10 |
| Security Control Responses | 11 |
| Additional Information | 11 |

Overview

United States Department of Defense (DoD) Instruction 8500.01 (effective March 2014) instructs DoD Component Heads to "ensure that all DoD IT under their purview complies with applicable STIGs, security configuration guides, and SRGs with any exceptions documented and approved by the responsible authorizing official (AO)." Within the DoD, Security Technical Implementation Guides (STIGs) help to define the security configuration baselines for IA and IA-enabled devices. Specifically, STIGs contain prescriptive steps that can be used to both assess and improve the security configuration of systems and devices deployed on DoD networks. For more information on DoD STIGs, see: <http://iase.disa.mil/stigs/Pages/index.aspx>.

As of this white paper's publication, STIGs can only be developed when they align to one of the published DoD Security Requirements Guides (SRGs) per the STIG development vendor process, documented at: <http://iase.disa.mil/stigs/Pages/vendor-process.aspx>. Unfortunately, while the published SRGs map to common technology areas, there is no suitable SRG for IT appliances. As a result, there is no published STIG for the Oracle Sun Data Center InfiniBand Switch 36 (Oracle InfiniBand Switch) as it is a dedicated, fixed-function appliance.

To mitigate this shortcoming, this technical white paper will provide prescriptive security configuration hardening guidance that will allow DoD customers to improve upon the default security configuration of the Oracle InfiniBand Switch in a manner suitable to what would otherwise have been published as a DoD STIG.

Product Description

The Oracle Sun Data Center InfiniBand Switch 36 is a quad data rate (QDR) InfiniBand switch connecting 36 fully non-blocking ports across a 40-Gbps low latency network fabric. Used by many Oracle Engineered Systems, this Oracle InfiniBand Switch provides the network foundation for a high performance, highly scalable, and fully redundant backplane across which all of their internal components are connected. For more information on the Oracle Sun Data Center InfiniBand Switch 36, see:

<http://www.oracle.com/us/products/networking/infiniband/switch36/overview/index.html>

The Oracle InfiniBand Switch incorporates an embedded Oracle Integrated Lights Out Manager (Oracle ILOM) to provide advanced management and monitoring capabilities. In particular, the embedded Oracle ILOM enables the monitoring and control of users, hardware, services, protocols, and other configuration parameters. For more information on this component, see the Oracle Integrated Lights Out Manager Supplement for the Oracle Sun Data Center InfiniBand Switch 36 at: http://docs.oracle.com/cd/E36265_01/pdf/E36270.pdf.

Product Security Guide

This white paper is intended to provide common information and procedures necessary to improve the "out of the box" security configuration of this product. The Oracle Sun Data Center InfiniBand Switch 36 security guide, available as a standard part of the Oracle product documentation, has additional information on the product's security features, capabilities and configuration options. It is strongly recommended that customers review the product security guide before implementing the recommendations contained within this technical white paper.

» Oracle Sun Data Center InfiniBand Switch 36 Firmware Version 2.1 Hardware Security Guide
http://docs.oracle.com/cd/E36265_01/pdf/E26701.pdf

Always review the correct version of the product security guide as the security features, capabilities and configuration options will often vary based upon product version.

Version and Update Information

To leverage the most recent features, capabilities and security enhancements, customers are encouraged to update their Oracle InfiniBand Switch software to the latest, supported version for their respective platform. To determine the version of the Oracle InfiniBand Switch software that is being used on the platform, execute the following command after first logging into the device using the `ilom-admin` account:

```
-> version
SP firmware 2.1.8-1
SP firmware build number: 47111
SP firmware date: Thu Feb 19 12:16:50 IST 2015
SP filesystem version: 0.1.22
```

In the above example, the Oracle InfiniBand Switch software is version 2.1.8-1. For detailed instructions describing how to update the Oracle InfiniBand Switch software and embedded Oracle ILOM software, see the Oracle Integrated Lights Out Manager supplement for the Oracle Sun Data Center InfiniBand Switch 36 at: http://docs.oracle.com/cd/E36265_01/pdf/E36270.pdf.

Note that for Oracle Engineered Systems such as the Oracle Exadata Database Machine or Oracle SuperCluster, additional restrictions may limit what versions of the Oracle InfiniBand Switch software that can be used as well as how those versions are updated. In these situations, refer to the Oracle Engineered System product documentation to understand the process for updating system components.

Security Configuration Information

Default Accounts and Passwords

This section describes the default accounts and passwords associated with this device:

ORACLE INFINIBAND SWITCH DEFAULT ACCOUNTS AND PASSWORDS

| Account Name | Account Type | Default Password | Account Description |
|---------------|---------------|------------------|---|
| root | Administrator | changeme | The root account is used to access the Oracle InfiniBand Switch operating system. This account will generally not be used in favor of <code>ilom-admin</code> , <code>ilom-operator</code> or customer defined accounts. |
| ilom-admin | Administrator | ilom-admin | The <code>ilom-admin</code> account is used to perform administrative functions on the embedded Oracle ILOM software, perform software upgrades, configure users and services, as well as to perform Oracle InfiniBand Switch diagnostic and fabric management functions. |
| ilom-operator | Operator | ilom-operator | The <code>ilom-operator</code> account is used only for Oracle ILOM monitoring and InfiniBand fabric diagnostic functions. |
| nm2user | Read Only | changeme | This account has read only privileges to the Oracle InfiniBand Switch's command line administrative interface. This account is often used by Oracle Enterprise Manager to support monitoring of the switch hardware and software. |

The Oracle InfiniBand Switch maintains system accounts in two locations. The `root` and `nm2user` accounts are configured and exposed by the underlying switch's operating system. It is not supported to add, remove, or change accounts at this layer (except to set individual account passwords). To change the password of the `root` or `nm2user` account, use the `passwd` command as follows:

```
$ passwd <account name>
```

In addition, the default Oracle ILOM accounts and any customer-defined accounts are managed through the embedded Oracle ILOM. To list the accounts currently configured on the embedded Oracle ILOM, run the following command:

```
-> show /SP/users
```

To set the password for the `ilom-admin` account, use the following commands:

```
-> set /SP/users/ilom-admin password=<value>
```

Note that the Oracle InfiniBand Switch does not have the ability to define or enforce password complexity, aging, history or other rules. Customers are encouraged to ensure that passwords assigned comply with DoD password complexity requirements and processes are implemented to ensure passwords are updated in accordance with DoD policy.

For more information on Oracle InfiniBand Switch account management including how to create new accounts, assign permissions to existing accounts, or remove accounts, see:

- » Oracle Sun Data Center InfiniBand Switch 36 Hardware Security Guide
http://docs.oracle.com/cd/E36265_01/pdf/E26701.pdf
- » Oracle Integrated Lights Out Manager Supplement for the Oracle Sun Data Center InfiniBand Switch 36
http://docs.oracle.com/cd/E36265_01/pdf/E36270.pdf

Default Exposed Network Services

This section describes the default network services that are exposed by this device:

ORACLE INFINIBAND SWITCH DEFAULT EXPOSED NETWORK SERVICES

| Service Name | Protocol | Port | Service Description |
|--------------|----------|------|---|
| SSH | TCP | 22 | This port is used by the integrated Secure Shell service to enable administrative access to the Oracle InfiniBand Switch using a command-line interface. |
| HTTP (BUI) | TCP | 80 | This port is used by the integrated HTTP service to enable administrative access to the Oracle InfiniBand Switch using a browser interface. While TCP/80 is typically used for clear-text access, by default the Oracle InfiniBand Switch will automatically redirect incoming requests to the secure version of this service running on TCP/443. |
| NTP | UDP | 123 | This port is used by the integrated Network Time Protocol (NTP) (client only) service used to synchronize the local system clock to one or more external time sources. |
| SNMP | UDP | 161 | This port is used by the integrated SNMP service to provide a management interface to monitor the health of the Oracle InfiniBand Switch and to monitor received trap notifications. |



| Service Name | Protocol | Port | Service Description |
|--------------|----------|------|--|
| HTTPS (BUI) | TCP | 443 | This port is used by the integrated HTTPS service to enable administrative access to the Oracle InfiniBand Switch over an encrypted (SSL/TLS) channel using a browser interface. |
| IPMI | TCP | 623 | This port is used by the integrated Intelligence Platform Management Interface (IPMI) service to provide a computer interface for various monitoring and management functions. This service is should not be disabled as it is used by Oracle Enterprise Manager Ops Center to collect hardware inventory data, field replaceable unit descriptions, hardware sensor information, and hardware component status information. |
| ServiceTag | TCP | 6481 | This port is used by the Oracle ServiceTag service. This is an Oracle discovery protocol used to identify servers and facilitate service requests. This service is used by products such as Oracle Enterprise Manager Ops Center to discover Oracle InfiniBand Switch software and to integrate with other Oracle automatic service solutions. |

For additional information on these services, refer to the Oracle InfiniBand Switch documentation referenced above.

Security Configuration Hardening

Disable Unnecessary Services

It is recommended that customers disable any services that are not required to support the operational and management requirements of the platform. By default, the Oracle InfiniBand Switch employs a network "secure by default" configuration whereby non-essential services are already disabled by default. That said, based upon customer security policies and requirements, it may be necessary to disable additional services.

To determine the list of services supported by the Oracle InfiniBand Switch, use the command:

```
-> show /SP/services
```

To determine if a given service is enabled, use the command, substituting the parameter <servicename> with the name of a service returned using the previous command:

```
-> show /SP/services/<servicename> servicestate
```

While the majority of services recognize and use the `servicestate` parameter to record whether the service is enabled or disabled, there are a few services such as `servicetag` that use a parameter called `state`. Regardless of the actual parameter used, a service is enabled if the service state parameter returns a value of `enabled` as in the following examples:

```
-> show /SP/services/https servicestate
```

```
/SP/services/https
Properties:
  servicestate = enabled
```



```
-> show /SP/services/servicetag state
```

```
/SP/services/servicetag  
Properties:  
state = enabled
```

To disable a service that is no longer required, set the service state to disabled using a command such as:

```
-> set /SP/services/http servicestate=disabled
```

As noted above, the Oracle InfiniBand Switch is delivered in a network secure by default state where non-essential services are disabled by default. That said, depending upon the tools and methods used, the following additional services may be disabled if they are not required or used:

```
» Browser Administrative Interface (HTTP, HTTPS)  
-> set /SP/services/http servicestate=disabled  
-> set /SP/services/http secureredirect=disabled  
-> set /SP/services/https servicestate=disabled
```

Disable HTTP service

By default, the Oracle InfiniBand Switch enables the HTTP service which allows the administrator to manage the switch using a browser. The HTTP service can be secured by enabling the HTTP redirection to HTTPS service. However this adds a significant amount of overhead. It is recommended to disable the HTTP service and use the HTTPS service instead.

To disable the HTTP service, set the servicestate property of the HTTP service to disabled using the following command:

```
-> set /SP/services/http servicestate=disabled
```

Disable NTP Protocol

By default, the NTP protocol is enabled for use once the NTP servers are setup. This service permits correct log timestamps and prevents clock drift over time. To determine the status of NTP settings use the commands:

```
-> show /SP/clients/ntp/server/1
```

```
/SP/clients/ntp/server/1  
Properties  
Address = 140.22.75.10
```

```
-> show /SP/clients/ntp/server/2
```

```
/SP/clients/ntp/server/2  
Properties  
Address = 140.22.75.11
```



```
-> show /SP/clock usentpserver
```

```
/SP/clock
```

```
Properties
```

```
usentpserver = enabled
```

To disable the NTP service if it is not required for any reason, use the command:

```
-> set /SP/clock usentpserver=disabled
```

Set 'usentpserver' to 'disabled'

Disable Unapproved SNMP Protocols

By default, the SNMPv1 and SNMPv2c protocols are disabled. SNMPv3 is enabled by default, but this service is inaccessible from the network as there are no pre-defined SNMP accounts delivered with the switch. Customers should ensure that older versions of the SNMP protocol remain disabled unless required. To determine the status of each of the SNMP protocols, use the command:

```
-> show /SP/services/snmp v1 v2c v3
```

```
/SP/services/snmp
```

```
Properties:
```

```
v1 = disabled
```

```
v2c = disabled
```

```
v3 = enabled
```

To disable SNMPv1 and SNMPv2c, use the commands:

```
-> set /SP/services/snmp v1=disabled
```

```
-> set /SP/services/snmp v2c=disabled
```

Version 3 of the SNMP protocol introduced support for the User-based Security Model (USM). This functionality replaces the traditional SNMP community strings with actual user accounts that can be configured with specific permissions, authentication and privacy protocols, as well as passwords. By default, the Oracle InfiniBand Switch does not include any USM accounts. Customers are encouraged to configure SNMPv3 USM accounts based upon their own deployment, management and monitoring requirements.

Configure SNMP Community Strings

This item is only applicable if SNMP v1 or SNMPv2c are configured for use.

Given that SNMP is often used to monitor the health of the device, it is important that the default SNMP community strings used by the device be replaced with customer-defined values.



To create a new SNMP community string, use the command:

```
-> create /SP/services/snmp/communities/<string> permission=<access>
```

In the above example, the value of <string> should be replaced with a customer-defined value that is compliant with DoD requirements regarding the composition of SNMP community strings. Similarly, the value of the <access> should be replaced with either `ro` or `rw` depending upon whether read-only or read-write access is intended. Once new community strings are created, the default community strings should be removed.

To remove the default SNMP community strings, use the commands:

```
-> delete /SP/services/snmp/communities/public  
-> delete /SP/services/snmp/communities/private
```

To verify the SNMP community strings that are configured, use the command:

```
-> show /SP/services/snmp/communities
```

Replace Default Self-Signed Certificates

The Oracle InfiniBand Switch leverages self-signed SSL certificates to enable the "out of the box" use of the HTTPS protocol. Whenever possible, self-signed SSL certificates should be replaced with certificates that are approved for use in the customer's environment and signed by a recognized certificate authority. To determine if the Oracle InfiniBand Switch is using its default self-signed SSL certificate, use the command:

```
-> show /SP/services/https/ssl cert_status
```

```
/SP/services/https/ssl  
Properties:  
    cert_status = Using Default (No custom certificate or private key loaded)
```

To install a customer SSL certificate use the following commands:

```
-> load -source URI /SP/services/https/ssl/custom_cert  
-> load -source URI /SP/services/https/ssl/custom_key
```

The Oracle InfiniBand Switch supports a variety of methods that can be used to access the SSL certificate and private key including HTTPS, HTTP, SCP, FTP, TFTP as well as pasting the information directly into a web browser interface. For more information, see the Oracle Integrated Lights Out Manager Supplement for the Oracle Sun Data Center InfiniBand Switch 36 at: http://docs.oracle.com/cd/E36265_01/pdf/E36270.pdf

Configure Administrative Interface Inactivity Timeout (CLI)

The Oracle InfiniBand Switch supports the ability to disconnect and log out administrative sessions that have been inactive for more than some pre-defined number of minutes. By default, the command line interface (CLI) will timeout a session after 15 minutes.



To check the inactivity timeout parameter associated with the command line interface, use the command:

-> **show /SP/cli timeout**

```
/SP/cli
  Properties:
    timeout = 15
```

To set the inactivity timeout parameter to a customer-defined value (<n> in minutes), use the command:

-> **set /SP/cli timeout=<n>**

Management Network Recommendations

In addition to the above security hardening procedures, the management interface of the Oracle InfiniBand Switch is intended to be deployed on a dedicated, isolated management network. This will help to shield the Oracle InfiniBand Switch from unauthorized or unintended network traffic. Access to this management network should be strictly controlled with access granted only to those administrators requiring this level of access.

Security Control Responses

This section provides Oracle product-specific responses to customer questions raised regarding various NIST 800-53 security controls. Unless otherwise specified, the responses indicated below apply to any and all security control enhancements associated with a listed security control item. For example, in the case of RA-05 (Vulnerability Scanning), the responses indicated apply to control enhancements such as RA-05 (2) and RA-05 (3) as defined in the NIST Special Publication 800-53 Revision 4. For more information on this publication, see:

<http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf>

Item(s):

- » CA-07 (Continuous Monitoring)
- » RA-05 (Vulnerability Scanning)
- » SI-03 (Malicious Code Protection)

Response:

Oracle recommends that customers regularly perform vulnerability security scans of this product using non-credentialed, network-based methods. Credentialed, host-based vulnerability scans are not supported.

As this product is designed, implemented, and deployed as a fixed-function appliance, Oracle does not permit or support the creation or modification of system accounts, the installation of third-party software, or configuration changes made outside of methods explicitly included in the product's documentation or this security supplement. Unauthorized software configuration changes made to this device may be lost when software patches are applied or upgrades are performed. Further, the introduction of software configurations or functions not tested by Oracle can pose a risk to critical system functions and can significantly impact system integrity, availability and/or performance.

To minimize risk to Oracle's customers, Oracle product teams are required to implement and follow Oracle's Software Security Assurance policies. For more information on the secure development, security testing, and vulnerability handling processes included in this framework, see:

<http://www.oracle.com/us/support/assurance/overview/index.html>

Lastly, Oracle recommends that customers stay current with all Oracle published security patches and leverage the secure configuration guidance included in this document to help minimize the attack surface associated with this product when deployed in their environments.

Additional Information

For more information describing the features and capabilities of the Oracle Sun Data Center InfiniBand Switch 36 as well as detailed technical instructions for the installation, configuration and management of this product, refer to the Oracle product documentation at:

- » Oracle Sun Data Center InfiniBand Switch 36 Firmware Version 2.1 Documentation
http://docs.oracle.com/cd/E36265_01/



CONNECT WITH US

-  blogs.oracle.com/oracle
-  facebook.com/oracle
-  twitter.com/oracle
-  oracle.com

Oracle Corporation, World Headquarters
500 Oracle Parkway

Worldwide Inquiries
Phone: +1.650.506.7000
Fax: +1.650.506.7200

Hardware and Software, Engineered to Work Together

Copyright © 2015, Oracle and/or its affiliates. All rights reserved. This document is provided for information purposes only, and the contents hereof are subject to change without notice. This document is not warranted to be error-free, nor subject to any other warranties or conditions, whether expressed orally or implied in law, including implied warranties and conditions of merchantability or fitness for a particular purpose. We specifically disclaim any liability with respect to this document, and no contractual obligations are formed either directly or indirectly by this document. This document may not be reproduced or transmitted in any form or by any means, electronic or mechanical, for any purpose, without our prior written permission.

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. 0916

Oracle InfiniBand Switch Security Configuration Supplement for the United States Department of Defense
September 2016