ORACLE
PUBLIC SECTOR

# Oracle ZFS Storage Appliance

## Security Configuration Supplement for the United States Department of Defense

ORACLE WHITE PAPER | OCTOBER 2014

ORACLE

## Table of Contents

## 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 ZFS Storage Appliance product 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 Oracle ZFS Storage Appliance in a manner suitable to what would otherwise have been published as a DoD STIG.

## Product Description

The Oracle ZFS Storage Appliance is a hybrid storage system based on a unique cache-centric architecture featuring massive DRAM plus Flash and is powered by a multi-threaded SMP operating system. As a result, 70%-90% of I/Os are served from DRAM enabling customers to use Oracle ZFS Storage ZS3 Series for storage consolidation in a variety of demanding workloads, including business intelligence, data warehousing, virtualization, development and test, and data protection.

Oracle ZFS Storage Appliance delivers leading performance and superior efficiency in enterprise-class network-attached storage (NAS) environments, accelerating business functions, and reducing complexity. This first application-engineered storage system provides unique integration points with Oracle Solaris and Oracle Database that help to automate storage tuning and data lifecycle management, reduce capacity requirements, and lowering total cost of ownership.

## 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 security guide for the Oracle ZFS Storage Appliance, 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 ZFS Storage Appliance Release 2013.1.2.0 Security Guide
http://docs.oracle.com/cd/E51475_01/pdf/E41348.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 ZFS Storage Appliance software to the latest, supported version for their respective platform. To determine the version of the Oracle ZFS Storage Appliance software that is being used on the platform, execute the following command after first logging into the device:

```
[hostname]:> configuration version show
[...]
Appliance Product: Oracle ZFS Storage ZS3-ES
Appliance Type: Sun ZFS Storage 7335
Appliance Version: 2013.06.05.2.6,1-1.2
[...]
```

In the above example, the Oracle ZFS Storage Appliance software is version `2013.06.05.2.6`. Note that for Oracle Engineered Systems such as the Oracle SuperCluster, Oracle Virtual Compute Appliance or Oracle Exalogic Elastic Cloud, additional restrictions may limit what versions of the Oracle ZFS Storage Appliance 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

The Oracle ZFS Storage Appliance itself does not come pre-configured with a default `root` password. Initial configuration of the Oracle ZFS Storage Appliance is performed through a console session from its embedded Oracle ILOM. The `root` password for the appliance is set during this initial configuration session.

The embedded Oracle ILOM for the appliance does have a default account and password:

**ORACLE ZFS STORAGE APPLIANCE DEFAULT ACCOUNTS AND PASSWORDS**

| Account Name | Account Type | Default Password | Account Description |
|---|---|---|---|
| `root` | Administrator | `changeme` | This is the sole default account that is delivered and enabled with the Oracle ZFS Storage Appliance. As noted above, this is an Oracle ILOM account. This account is used to perform initial configuration of the appliance. |

Upon accessing the console of the appliance, a shell interface configuration screen appears. Verify the information on the screen and enter the required values. The `root` password to the ZFS Storage Appliance is set during this process. To change the `root` password at a later time, use the command:

```
[hostname]:> configuration users select root set initial_password=<password>
             initial_password = *************
[hostname]:configuration users> done
```

In the above example, the value `<password>` should be replaced by a password that complies with DoD password complexity policy. For more information on the initial installation and configuration of this storage appliance, see the Oracle ZFS Storage Appliance installation guide at: http://docs.oracle.com/cd/E27998_01/.

## Default Exposed Network Services

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

**ORACLE ZFS STORAGE APPLIANCE 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 ZFS Storage Appliance using a command-line interface. |
| PORTMAP | TCP/UDP | 111 | This port is used by the Remote Procedure Call (RPC) port mapping daemon (known as `rpcbind` and/or `portmap`). This service is required to support NFS version 3. |
| 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 ZFS Storage Appliance and to monitor received trap notifications. |
| HTTPS (BUI) | TCP | 215 | This port is used by the integrated HTTPS service to enable administrative access to the Oracle ZFS Storage Appliance over an encrypted (SSL/TLS) channel using a browser interface. |
| Remote Replication | TCP | 216 | This port is used by the integrated remote data replication service. Remote data replication duplicates and synchronizes projects and shares between Oracle ZFS Storage Appliances over an encrypted (SSL/TLS) channel. |
| NFS | TCP/UDP | 2049<br>4045<br><various> | These ports are used by the Network File System (NFS) service. NFS provides the network file sharing service. The actual number of ports will depend on which version of the NFS protocol is used. NFS version 3 relies upon the RPC port mapping daemon (referenced above) and dynamically allocated ports to provide mounting, status, quota and related services. NFS version 4, however, relies only on TCP/2049. The NFS locking service uses TCP/4045. |
| iSCSI / iSNS | TCP | 3205<br>3260 | This port is used by the iSCSI service that provides an IP-based storage networking protocol for linking data storage facilities. The Oracle ZFS Storage Appliance can be configured to share iSCSI devices (called Logical Units or LUNs) with networked clients. |
| Service Tags | 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 ZFS Storage Appliance software and to integrate with other Oracle automatic service solutions. |
| NDMP | TCP | 10000 | This port is used by the Network Data Management Protocol (NDMP) service that enables the ZFS Storage Appliance to participate in remotely coordinated backups. |

*The Oracle ZFS Storage Appliance also supports a variety of other services that are disabled by default including HTTP, FTP, SFTP, TFTP, WebDAV, etc. Additional network ports may be exposed if those services are enabled post-installation.*

## Security Configuration Hardening

### Implement Oracle ILOM Security Configuration Hardening

The Oracle ZFS Storage Appliance includes an embedded Oracle Integrated Lights Out Manager as part of the product. As with other Oracle ILOM implementations, there are security relevant configuration changes that can be implemented to improve upon the default security configuration of the device. For more information, see the Oracle Integrated Lights Out Manager Security Configuration Supplement for the U.S. Department of Defense.

### 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 ZFS Storage Appliance 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 enable or disable additional services.

To determine the list of services supported by the Oracle ZFS Storage Appliance, use the command:

```
[hostname]:> configuration 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:

```
[hostname]:> configuration services [servicename] get <status>
```

A service is enabled if the service state parameter returns a value of `enabled` as in the following example:

```
[hostname]:> configuration services iscsi get <status>
                     <status> = online
```

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

```
[hostname]:> configuration services iscsi disable
```

### Disable Dynamic Routing

The Oracle ZFS Storage Appliance is configured to run the dynamic routing protocol by default.

*Before disabling the dynamic routing service, be sure that the Oracle ZFS Storage Appliance is either directly connected to any network with which it must communicate or has been configured to use static routing and/or a default route. This is needed to ensure there is no loss of connectivity once dynamic routing is disabled.*

To disable the dynamic routing service, run the following commands after first logging into the Oracle ZFS Storage Appliance administrative interface using Secure Shell:

```
[hostname]:> configuration services dynrouting disable
```

To determine if dynamic routing is enabled, use the command:

```
[hostname]:> configuration services dynrouting get <status>
```

### Restrict Remote Root Access Using Secure Shell

By default, the Oracle ZFS Storage Appliance is configured to allow remote administrative access to the `root` account using the Secure Shell service.

To disable the ability to remote access to the `root` account using Secure Shell, run the command:

```
[hostname]:> configuration services ssh set permit_root_login=false
```

To determine if the root account is permitted to access the system using Secure Shell, use the command:

```
[hostname]:> configuration services ssh get permit_root_login
```

*Be sure to create at least one non-`root` administrative account if Secure Shell administrative access is required. Note that once this configuration change has been made, the `root` account will no longer be able to access the system using Secure Shell. That said, the `root` account will be able to access this system using the HTTPS administrative interface.*

### Configure Administrative Interface Inactivity Timeout (HTTPS)

The Oracle ZFS Storage Appliance 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 browser user interface (HTTPS) will timeout a session after 15 minutes.

To set the inactivity timeout parameter to a customer-defined value (`[n]` in minutes) use the command:

```
[hostname]:> configuration preferences set session_timeout=15
                session_timeout = 15
```

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

```
[hostname]:> configuration preferences get session_timeout
                session_timeout = 15
```

*Note that there is no equivalent parameter that will enforce an inactivity timeout on the Secure Shell command line interface of the Oracle ZFS Storage Appliance.*

### Disable Unapproved SNMP Protocols

By default, SNMPv1 and SNMPv2c are enabled on the Oracle ZFS Storage Appliance. The Oracle ZFS Storage Appliance supports SNMPv1/v2c across all supported versions of the product. Starting with version 2013.1.2, the Oracle ZFS Storage Appliance also has support for SNMPv3. Customers should ensure that unused or older versions of the SNMP protocol are disabled unless required.

To enable the use of SNMPv3 (if available) use the command:

```
[hostname]:> configuration services snmp set version=v3
                version = v3
```

*Note that the use of SNMPv1/v2c and SNMPv3 is mutually exclusive.*

To determine which version of the SNMP protocol is used by the device, use the command:

```
[hostname]:> configuration services snmp get version
                 version = v3
```

*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 ZFS Storage Appliance does not include a username or password for the integrated (read-only) USM account. Customers are encouraged to configure the USM credentials and protocols based upon their deployment, management and monitoring requirements.*

## Configure SNMP Community Strings

*This item is only applicable if SNMP v1/v2c is configured for use.*

Given that SNMP is often used to monitor the health of the device, it is important that the default SNMP community string used by the device be changed to a customer-defined value.

To change the SNMP community string, use the command:

```
[hostname]:> configuration services snmp set community=<string>
                 community = <value>
```

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.

To verify the SNMP community string, use the command:

```
[hostname]:> configuration services snmp get community
```

## Configure SNMP Authorized Networks

*This item is only applicable if SNMP v1/v2c is configured for use.*

To minimize system configuration information disclosure, SNMP queries should only be accepted from approved network or host sources.

To configure the SNMP authorized network parameter, use the command:

```
[hostname]:> configuration services snmp set network=127.0.0.1/8
                 network = 127.0.0.1/8
```

To check the value of the SNMP authorized network parameter, use the command:

```
[hostname]:> configuration services snmp get network
                network = 127.0.0.1/8
```

In the above example, setting the `network` parameter to `127.0.0.1/8` will effectively block all network-based SNMP queries. This value should be adjusted as needed to permit approved hosts and/or networks. Note that a value of `0.0.0.0/0` will permit queries from any network location.

### Management Network Recommendations

In addition to the above security hardening procedures, the management interfaces exposed by the Oracle ZFS Storage Appliance are intended to be deployed on a dedicated, isolated management network. This will help to shield the Oracle ZFS Storage Appliance from unauthorized or unintended administrative network traffic. Access to this management network should be strictly controlled with access granted only to those administrators requiring this level of access.

Further, the Oracle ZFS Storage Appliance can be configured to enable and/or disable administrative (management) access on specific network interfaces. This change can be implemented using the following commands after first logging into the device using Secure Shell:

```
[hostname]:> configuration net interfaces select [interface] set admin=false
```

In the above example, the value `[interface]` should be replaced with the name of the actual network interface where this setting is to be applied.

## Security Findings and Recommendations

The following issues may be reported by some commercial and/or open-source vulnerability scanners when configured to assess the security posture of the Oracle ZFS Storage Appliance. This section is intended to provide information on commonly reported findings as well as specific technical recommendations to respond to these findings.

**ORACLE ZFS STORAGE APPLIANCE SECURITY FINDINGS AND RECOMMENDATIONS**

| Item | CVE | CVSS | Description and Recommendation |
|---|---|---|---|
| RIP-2 Poisoning Routing Table Modification | N/A | 5.4 (Medium) | This issue was reported for the embedded Routing Information Protocol (RIP) version 2 service that was enabled and running on UDP/520. To mitigate this issue, configure the Oracle ZFS Storage Appliance to use a static default route and then disable the dynamic routing service per the instructions above. |
| SSL Medium Strength Cipher Suites Supported | N/A | 4.3 (Medium) | This issue was reported for the HTTPS service that was enabled and running on TCP/215 as well as the Replication service that was enabled and running on TCP/216. There is currently no method available today to configure or disable specific protocols or ciphersuites related to these services. To help mitigate these issues, ensure that administrative access is restricted to only those network interfaces residing on the management network. Interested customers can track this as Bug ID #16762873. |

| Item | CVE | CVSS | Description and Recommendation |
|---|---|---|---|
| SSL Weak Cipher Suites Supported | N/A | 4.3 (Medium) | This issue was reported for the HTTPS service that was enabled and running on TCP/215. This service is used to provide administrative access to the Oracle ZFS Storage Appliance using a browser-based interface. There is currently no method available today to configure or disable specific protocols or ciphersuites related to this service. To help mitigate this issue, ensure that administrative access is restricted to only those network interfaces residing on the management network. Interested customers can track this as Bug ID #16762873. |
| SSL RC4 Cipher Suites Supported | CVE-2013-2566 | 2.6 (Low) | This issue was reported for the HTTPS service that was enabled and running on TCP/215 as well as the Replication service that was enabled and running on TCP/216. There is currently no method available today to configure or disable specific protocols or ciphersuites related to these services. To help mitigate these issues, ensure that administrative access is restricted to only those network interfaces residing on the management network. Interested customers can track this as Bug ID #16762873. |
| SSL Null Cipher Suites Supported | N/A | 4.3 (Medium) | This issue was reported for the HTTPS service that was enabled and running on TCP/215 as well as the Replication service that was enabled and running on TCP/216. There is currently no method available today to configure or disable specific protocols or ciphersuites related to these services. To help mitigate these issues, ensure that administrative access is restricted to only those network interfaces residing on the management network. Interested customers can track this as Bug ID #16762873. |
| NTP monlist Command Enabled | CVE-2013-5211 | 5 (Medium) | This issue was reported for the embedded NTP service that is running on UDP/123. There is currently no method available today to configure or disable specific functionality used by the embedded NTP implementation on this product. Interested customers can track this as Bug ID #19781207. |
| NTP ntpd Mode 7 Error Response Packet Loop Remote DoS | CVE-2009-3563 | 6.4 (Medium) | This issue was reported for the embedded NTP service that is running on UDP/123. This issue had been previously reported as Bug ID 16762973. Analysis completed by the product development organization indicates that this is a false positive findings being reported by the Nessus Vulnerability Scanner. This issue had been previously resolved as part of Bug ID #15604171. |
| SSL Self-Signed Certificate<br>SSL Certificate Cannot Be Trusted | N/A | 6.4 (Medium) | This issue was reported for the HTTPS service that was enabled and running on TCP/215 as well as the Replication service that was enabled and running on TCP/216. By default, these components include a self-signed certificate used for SSL/TLS communications. There is currently no method available today to replace the default self-signed SSL certificates with those that are provided by a customer. Interested customers can track this as Bug ID #15603956. |
| SSL/TLS Protocol Initialization Vector Implementation Information Disclosure Vulnerability | CVE-2011-3389 | 4.3 (Medium) | This issue was reported for the HTTP service that was enabled and running on TCP/215. This service is used to provide administrative access to the Oracle ZFS Storage Appliance using a browser-based interface. There is currently no method available today to configure or disable specific protocols or ciphersuites related to this service. To mitigate this issue, ensure that administrative access is restricted to only those network interfaces residing on the management network. Interested customers can track this as Bug ID #19781793. |
| SSH Weak MAC Algorithms Enabled | N/A | 2.6 (Low) | This issue was reported for the embedded Secure Shell service that is running on TCP/22. There is currently no method available today to configure or disable specific HMAC algorithms used by the embedded SSH implementation on this product. A product enhancement request has been filed to add this functionality. Interested customers can track this as RFE #18450868. |

| Item | CVE | CVSS | Description and Recommendation |
|---|---|---|---|
| Command Line Interface Inactivity Timer Not Supported | N/A | N/A | There is currently no method available today to configure a session inactivity timer for the command line administrative interface. Interested customers can track this as RFE #19514349. |
| Login Warning Banner Not Supported | N/A | N/A | There is currently no method available today to configure a login warning banner message for either the command line or browser-based administrative interface. Interested customers can track this as RFE #16900798. |

## Additional Information

For more information describing the features and capabilities of the Oracle ZFS Storage Appliance as well as detailed technical instructions for the installation, configuration and management of this product, refer to the Oracle product documentation at:

» Oracle ZFS Storage Appliance Security Release 2013.1.2.0 Product Documentation
http://docs.oracle.com/cd/E51475_01/index.html

**Oracle Corporation, World Headquarters**
500 Oracle Parkway
Redwood Shores, CA 94065, USA

**Worldwide Inquiries**
Phone: +1.650.506.7000
Fax: +1.650.506.7200



Oracle ZFS Storage Appliance Security Configuration Supplement for the United States Department of Defense
October 2014
Author: Edsel Adap
Contributing Authors: Glenn Brunette