## Dell EMC Networking SmartFabric OS10

## Release 10.5.1

# Common Criteria Guide

**Version 1.5**

**September 2020**

**Document prepared by**


www.lightshipsec.com

# Table of Contents



# List of Tables

# 1 About this Guide

## 1.1 Overview

1 This guide provides supplemental instructions to achieve the Common Criteria evaluated configuration of the Dell EMC Networking SmartFabric OS10 and related information.

## 1.2 Audience

2 This guide is intended for system administrators and the various stakeholders involved in the Common Criteria evaluation. It is assumed that readers will use this guide in conjunction with the related documents listed in Table 2.

## 1.3 About the Common Criteria Evaluation

3 The Common Criteria for Information Technology Security Evaluation (ISO/IEC 15408) is an international standard for security certification of IT products and systems. More information is available at https://www.commoncriteriaportal.org/

### 1.3.1 Protection Profile Conformance

4 The Common Criteria evaluation was performed against the requirements of the Network Device collaborative Protection Profile (NDcPP) v2.1 available at https://www.niap-ccevs.org/Profile/PP.cfm

### 1.3.2 Evaluated Software and Hardware

5 The Target of Evaluation (TOE) includes Dell EMC Networking SmartFabric OS 10.5.1 and the following hardware models:

a) PowerSwitch S3048-ON
b) PowerSwitch S4048-ON/S4048T-ON
c) PowerSwitch S4112F-ON/S4112T-ON
d) PowerSwitch S4128F-ON/S4128T-ON
e) PowerSwitch S4148F-ON/S4148T-ON
f) PowerSwitch S4148U-ON
g) PowerSwitch S4248FB-ON/S4248FBL-ON
h) PowerSwitch S6010-ON
i) PowerSwitch Z9100-ON
j) PowerSwitch S5212F-ON
k) PowerSwitch S5224F-ON
l) PowerSwitch S5232F-ON
m) PowerSwitch S5248F-ON
n) PowerSwitch S5296F-ON
o) PowerSwitch Z9264F-ON
p) PowerSwitch Z9332F-ON

q) Dell EMC Networking MX5108n

r) Dell EMC Networking MX9116n

### 1.3.3 Evaluated Functions

6 The following functions have been evaluated under Common Criteria:

a) **Protected Communications.** The TOE provides secure communication channels:

i) **CLI.** Administrator access to the CLI via direct serial connection or SSH.

ii) **Logs.** Secure transmission of log events to a Syslog server via TLS.

b) **Secure Administration.** The TOE enables secure management of its security functions, including:

i) Administrator authentication with passwords

ii) Configurable password policies

iii) Role Based Access Control

iv) Access banners

v) Management of critical security functions and data

vi) Protection of cryptographic keys and passwords

c) **Trusted Update.** The TOE ensures the authenticity and integrity of software updates via published hash.

d) **System Monitoring.** The TOE generates logs of security relevant events. The TOE stores logs locally and is capable of sending log events to a remote audit server.

e) **Self-Test.** The TOE performs a suite of self-tests to ensure the correct operation and enforcement of its security functions.

f) **Cryptographic Operations.** The cryptographic algorithms used in the above functions have been validated for correct implementation.

7 **NOTE:** No claims are made regarding any other security functionality.

### 1.3.4 Evaluation Assumptions

8 The following assumptions were made in performing the Common Criteria evaluation. The guidance shown in the table below should be followed to uphold these assumptions in the operational environment.

**Table 1: Evaluation Assumptions**

| Assumption | Guidance |
|---|---|
| Physical security, commensurate with the value of the TOE and the data it contains, is provided by the environment. | Ensure that the device is hosted in a physically secure environment, such as a locked server room. |
| There are no general-purpose computing capabilities (e.g., compilers or user applications) available on the TOE, other than those services necessary for the | Do not install other software on the device hardware. |

| Assumption | Guidance |
|---|---|
| operation, administration and support of the TOE. | |
| The TOE does not provide any protection of traffic that traverses it. It is assumed that protection of this traffic will be covered by other security and assurance measures in the operational environment. | The Common Criteria evaluation focused on the management plane of the device. |
| Security Administrators are trusted to follow and apply all guidance documentation in a trusted manner. | Ensure that administrators are trustworthy – e.g. implement background checks or similar controls. |
| The TOE firmware and software is updated by an Administrator on a regular basis in response to the release of product updates due to known vulnerabilities. | Apply updates regularly according to your organization's policies. |
| The Administrator's credentials (private key) used to access the TOE must be protected on any other platform on which they reside. | Administrators should take care to not disclose credentials and ensure private keys are stored securely. |
| The Security Administrator ensures that there is no unauthorized access possible for sensitive residual information (e.g. cryptographic keys, keying material, PINs, passwords etc.) on networking equipment when the equipment is discarded or removed from its operational environment. | Administrators should sanitize the device before disposal or transfer out of the organization's control. |

## 1.4 Conventions

9 The following conventions are used in this guide:

a) `CLI Command <replaceable>` - This style indicates to you that you can type the word or phrase on the command line and press [Enter] to invoke a command. Text within <> is replaceable. For example:

Use the `cat <filename>` command to view the contents of a file

b) [key] or [key-combo] – key or key combination on the keyboard is shown in this style. For example:

The [Ctrl]-[Alt]-[Backspace] key combination exits your graphical session and returns you to the graphical login screen or the console.

c) **GUI => Reference** – denotes a sequence of GUI screen interactions. For example:

Select **File => Save** to save the file.

d) [REFERENCE] *Section* – denotes a document and section reference from Table 2. For example:

Follow [ADMIN] *Configuring Users* to add a new user.

## 1.5 Related Documents

10 This guide supplements the below documents.

**Table 2: Related Documents**

| Reference | Document |
|---|---|
| [ADMIN] | Dell EMC SmartFabric OS10 User Guide, Release 10.5.1<br>https://topics-cdn.dell.com/pdf/smartfabric-os10-5-1_en-us.pdf |

11 **NOTE:** The information in this guide supersedes related information in other documentation.

# 2 Secure Acceptance and Update

## 2.1 Obtaining the TOE

12 Your Dell EMC Networking switch will be delivered via commercial courier. Perform the following checks upon receipt (return the device if either of the checks fail):

a) Confirm that the correct device has been delivered

b) Inspect the packaging to confirm that there are no signs of tampering

13 Follow the instructions at [ADMIN] *Download OS10 image* to obtain the TOE software.

## 2.2 Verifying the TOE

14 To validate the software image on the flash drive, after you transfer the image to the system, but before you install the image, use the `image verify` command in EXEC Priv mode. The validation calculates a hash value of the downloaded image file on system's flash drive. You can compare this hash with the Dell Networking published hash for that file.

15 The SHA256 hash provides a method of validating that you have downloaded the original software. Calculating the hash on the local image file and comparing the result to the hash published for that file, provides a high level of confidence that the local copy is exactly the same as the published software image. This validation procedure, and the verify command to support it, prevents the installation of corrupted or modified images.

16 See section 2.4 below for detailed instructions on the `image verify` command.

## 2.3 Self-Tests

17 On start-up, the system will run a series of self-tests:

a) **BIOS POST.** If there is an issue with any of the POST results, the system does not boot.

b) **System Software Self-tests.** If there is any major issue at startup that prevents the system from proceeding, the system automatically reboots itself, if possible. If there are missing components that are non-critical, the system continues the boot process but report a warning message.

c) **Secure Boot.** The TOE performs kernel image digital signature verification and file integrity checking. This is not performed by default and must be enabled in accordance with section 2.13.

d) **FIPS Self-tests.** The TOE includes a suite of FIPS self-tests that validate the integrity of the Dell OpenSSL Cryptographic Library and verify the implementation of the FIPS DRBG and the cryptographic algorithms. If any of these self-tests fail, the system will be unable to operate in a FIPS-validated manner and a 'Test Failed' message will be displayed to the user along with an indication of the failed test. A corresponding audit event will also be generated. If this occurs, restart the TOE.

18 If restarting the system does not clear the issue, consult your Dell support procedures.

## 2.4 Updating the TOE

19 To update the TOE, follow the instructions in [ADMIN] *OS10 upgrade.*

20 Use the `image verify` command to verify the authenticity of the update prior to installation. The verify command calculates and displays the hash of any file on the specified local flash drive. Compare the displayed hash against the published hash. For example:

a) `OS10# image verify image://mltest.bin sha256 [hash string]`

21 **NOTE:** If the image did not validate successfully, ensure you have copied the correct binary file for upgrading your system. Repeat the procedure if there is an issue with either the selected file or the download process.

22 **NOTE:** You should verify that the configuration described in the following sections has carried over subsequent to upgrade.

## 2.5 Installation

23 Follow the instructions of [ADMIN] augmented by the configuration steps in the following sections.

## 2.6 Administration Interfaces

24 Only the below listed administration interfaces may be used. See [ADMIN] *CLI basics* for general CLI usage.

a) **Console.** Connecting a serial cable and terminal emulator to the console serial port — serial port settings are 115200, 8 data bits, and no parity.

i) See [ADMIN] *Login banner* to configure a banner message.

ii) Perform the following steps to prevent the console from locking out a designated user:

Determine a username(s) to be reserved for use as console-only administrator accounts.

Create the username(s) on the system using the `username` command and ensure they have sysadmin role.

Login to system as linuxadmin and sudo to root.

Edit the /etc/ssh/sshd_config.startup file and add the following lines to the END of the file (must be after all other Match blocks):

```
Match User <username or list of usernames with comma separator – no spaces>
        MaxAuthTries 1
        PubKeyAuthentication no
        PasswordAuthentication no
```

Save the file.

Verify the configuration file with: `sshd -t -f /etc/ssh/sshd_config.startup`

If it verifies as entered, then logout of system. Log back in as admin and save the running-configuration and reload using commands `write memory` followed by `reload`.

iii) Session termination on timeout is supported – use the following commands to configure the inactivity time period and disable access to shell commands:

Navigate to the terminal context:

```
OS10#configure terminal
```

To set the inactivity time out to 10 minutes and 0 seconds (minutes must be set to between 1 and 10 for the CC config):

```
OS10(configure)#exec-timeout 10 0
```

Disable shell commands:

```
OS10(configure)#system-cli disable
```

b) **SSH.** Remote access to the CLI via SSH. See [ADMIN] *Remote access* and *SSH Server* for usage.

**NOTE:** Enable FIPS mode via the console per 2.7.1 below prior to using SSH.

i) Configure SSH to use the following algorithms (in configuration mode):

```
OS10# ip ssh server cipher aes128-ctr aes256-ctr
OS10# ip ssh server mac hmac-sha1 hmac-sha2-256
hmac-sha2-512
```

ii) Password authentication is enabled by default. To enable public key authentication (RSA):

```
OS10# ip ssh server pubkey-authentication
```

iii) To generate 2048-bit RSA host keys:

```
OS10# crypto ssh-key generate rsa
```

iv) See [ADMIN] *Login banner* to configure a banner message.

v) Session termination on timeout is supported (set as per console above).

**NOTE:** Loading of DSS keys is not permitted by the TOE. Any such attempt is rejected by the TOE with the error “key is not a RSA key”, on the CLI. Attempting to load a DSS key will result in the following audit message:

```
Jul  2 15:49:56 10.19.2.10 1 2020-07-
02T15:51:11.625787+00:00 OS10 .clish 3966 - - Node.1-
Unit.1:PRI [audit], User admin on console used cmd:
'username testadmin sshkey "ssh-dss <key>=
root@lightship-sd"' - completed
```

## 2.7 Cryptography

25 Federal information processing standard (FIPS) cryptography provides cryptographic algorithms conforming to various FIPS standards published by the National Institute of Standards and Technology (NIST), a non-regulatory agency of the US Department of Commerce. FIPS mode is also validated for numerous platforms to meet the FIPS-140-2 standard for a software-based cryptographic module.

26 To ensure you are using the correct cryptographic algorithms, enable FIPS mode.

### 2.7.1 Enable FIPS mode

27 Enable FIPS mode as follows:

28
```
OS10(configure)#crypto fips enable
"WARNING: Upon committing this configuration, the system will
regenerate SSH keys. Please consult documentation and toggle
FIPS mode only if you know what you are doing! Continue?
[yes/no(default)]:"
```

29 **NOTE:** If the system fails to transition to FIPS mode, an error message will be displayed. The system is not in a FIPS-compliant state.

30 To verify that FIPS mode is enabled, use the `show fips status` command.

31 The following example shows that FIPS mode is successfully enabled:

```
OS10#show fips status
FIPS Mode: Enabled
```

## 2.8 Default Passwords

32 The following default user accounts have default passwords that must be changed:

a) admin - refer to [ADMIN] Log into OS10 (you will be prompted to change password at first login.)

b) linuxadmin – refer to [ADMIN] *Log into OS10 device* (you will be prompted if the password has not been changed from its default value)

## 2.9 Setting Time

33 The Common Criteria configuration does not use NTP. Set the time manually per [ADMIN] *System clock.*

## 2.10 Audit Logging

34 The Common Criteria evaluation confirmed that the log events listed at Annex A: Log Reference are generated by the TOE.

35 Refer to [ADMIN] *Audit log* and [ADMIN] *System logging* for details about enabling and viewing logs.

### 2.10.1 Configuring Syslog Servers

36 See [ADMIN] *System logging* for details on configuring a syslog server.

37 **NOTE:** Syslog must be used with TLS per the instructions a [ADMIN] *System logging over TLS*.

## 2.11 Configuring X.509v3

38 Refer to [ADMIN] *X.509v3 certificates* for details on configuring X.509 certificates, signing requests and CRLs.

39 Prior to installing host certificates, checking of the certificate chain should be performed. The necessary CA and root certificates must first be installed using the '`crypto ca-cert install`' command for each one.

40 The validity of various fields for a host certificate are checked during the host certificate installation using the ‘`crypto cert install`’ command. To specifically check the certificate chain of a host certificate, it is necessary to copy the candidate host certificate to the home directory of the userid, e.g. admin userid, on the system.

41 Then login as the ‘linuxadmin’ userid.

42 Enter the command as shown in a). This does not perform revocation checking.

a) `openssl verify -verbose -CAfile /config/certs/store/ca-certificates.crt /config/home/<e.g. admin userid>/<candidate certificate filename>`

b) The output of the command will show either success or failure. In the event of failure, the candidate certificate should be discarded.

c) Exit from the ‘linuxadmin’ login.

43 Refer to [ADMIN] *System logging over TLS* for details on configuration the Syslog server reference identifier (ipv4–address). This reference identifier will be compared to the CN or SAN in the X.509 certificate presented by the Syslog server when establishing a TLS connection.

## 2.12 Administrator Authentication

44 Refer to [ADMIN] *Security* for configuration of administrator authentication.

**NOTE:** The Common Criteria configuration mandates local authentication.

## 2.13 Enabling Secure Boot

45 Use the command at [ADMIN] *secure-boot enable* to enable secure boot.

## 2.14 Exiting the CLI

46 Use command `exit` to exit the CLI.

# Annex A: Log Reference

## 2.15 Format

47 Refer to [ADMIN] *Audit log* for details of the audit log format.

## 2.16 Events

48 The TOE generates the following log events.

**Table 3: Audit Events**

| Requirement | Audit Events | Examples |
|---|---|---|
| FAU_GEN.1 | Start-up and shutdown of the audit functions | The audit function can only be restarted by the commands 'logging audit enable' and 'no logging audit enable'.<br>Start up of the audit log:<br>Feb 4 15:31:52 10.19.2.10 1 2020-02-04T15:31:17.284591+00:00 OS10 dn_etl 666 - - Node.1-Unit.1:PRI [audit], Enabling audit log<br>Feb 4 15:31:52 10.19.2.10 1 2020-02-04T15:31:17.290292+00:00 OS10 .clish 26148 - - Node.1-Unit.1:PRI [audit], User admin on /dev/pts/2 from 10.100.0.137 used cmd: 'logging audit enable' – completed<br>Shutdown of the audit functions is tied to the shutdown of the TOE:<br>Oct 3 12:30:48 10.19.2.10 1 2019-10-03T13:04:37.461674+00:00 OS10 .clish 3687 - - Node.1-Unit.1:PRI [audit], User admin on console requesting system reboot |
| | Administrative login and logout | Administrative login:<br>Oct 1 16:43:15 10.19.2.10 1 2019-10-01T17:17:03.054742+00:00 OS10 sshd 19035 - - Node.1-Unit.1:PRI [event], Dell EMC (OS10) pam_unix(sshd:session): session opened for user admin by (uid=0)<br>Oct 1 16:43:15 10.19.2.10 1 2019-10-01T17:17:03.072994+00:00 OS10 dn_alm 700 - - Node.1-Unit.1:PRI [event], Dell EMC (OS10) %ALM_AUTH_EVENT: Authentication event was raised MESSAGE=pam_unix(sshd:session): session opened for user admin by (uid=0)<br>Oct 1 16:43:20 10.19.2.10 1 2019-10-01T17:17:07.848570+00:00 OS10 .clish 19028 - - Node.1-Unit.1:PRI [audit], CLI session started for user admin with role sysadmin on /dev/ttyS0 |

| Requirement | Audit Events | Examples |
|---|---|---|
| | | Administrative logout:<br><br>Oct 3 15:10:49 10.19.2.10 1 2019-10-03T15:41:55.546954+00:00 OS10 sshd 32261 - - Node.1-Unit.1:PRI [event], Dell EMC (OS10) pam_unix(sshd:session): session closed for user admin<br><br>Oct 3 15:10:49 10.19.2.10 1 2019-10-03T15:41:55.497025+00:00 OS10 .clish 32258 - - Node.1-Unit.1:PRI [audit], User admin on console used cmd: 'exit' - completed<br><br>Oct 3 15:10:49 10.19.2.10 1 2019-10-03T15:41:55.835845+00:00 OS10 systemd 1 - - Node.1-Unit.1:PRI [audit], Dell EMC (OS10) Stopped Serial Getty on ttyS0. |
| | Changes to TSF data related to configuration changes | All configuration events in this table. |
| | Generating/import of, changing, or deleting of cryptographic keys | When generating a new private key as part of a CSR operation:<br><br><110>1 2019-10-10T19:30:23.083842+00:00 OS10 .clish 4289 - - Node.1-Unit.1:PRI [audit], User testadmin on /dev/pts/1 from 10.100.0.137 used cmd: 'crypto cert generate request cert-file home://test.csr key-file home://test.key country CA state ON locality Ottawa organization "Lightship Security" orgunit CC1902 cname 10.19.2.10 length 2048 altname IP:10.19.2.10 email test@lightshipsec.com' – completed<br><br>When deleting a private key as part of a key pair operation:<br><br><110>1 2019-10-10T20:47:53.861110+00:00 OS10 mgmtsys.py 675 - - Node.1-Unit.1:PRI [audit], Host certificate with CN = 10.19.2.10 successfully deleted<br><br><110>1 2019-10-10T20:47:53.966863+00:00 OS10 mgmtsys.py 675 - - Node.1-Unit.1:PRI [audit], Key for certificate with CN = 10.19.2.10 successfully deleted. Key hash y6X080yH<br><br><110>1 2019-10-10T20:47:54.284548+00:00 OS10 .clish 3494 - - Node.1-Unit.1:PRI [audit], User admin on /dev/pts/0 from 10.100.0.137 used cmd: 'crypto cert delete client_cert.crt fips' – completed<br><br>Keys cannot be changed. They can only be added or deleted. |

| Requirement | Audit Events | Examples |
|---|---|---|
| | Resetting passwords | Sep 16 11:42:32 10.19.2.10 1 2019-09-16T11:48:33.924057+00:00 OS10 mgmtsys.py 683 - - Node.1-Unit.1:PRI [audit], User admin password may have changed.<br><br>Sep 16 11:42:32 10.19.2.10 1 2019-09-16T11:48:33.927819+00:00 OS10 .clish 28974 - - Node.1-Unit.1:PRI [audit], User admin on console used cmd: 'username admin password ***** role sysadmin priv-lvl 15' - completed |
| FCS_SSHS_EXT.1 | Failure to establish an SSH session | Bad packet length:<br><br>Oct 3 15:58:31 10.19.2.10 1 2019-10-03T16:29:38.580741+00:00 OS10 dn_alm 697 - - Node.1-Unit.1:PRI [event], Dell EMC (OS10) %ALM_AUTH_EVENT: Authentication event was raised MESSAGE=pam_unix(sshd:session): session opened for user admin by (uid=0)<br><br>Oct 3 15:58:31 10.19.2.10 1 2019-10-03T16:29:38.229654+00:00 OS10 sshd 1433 - - Node.1-Unit.1:PRI [audit], Dell EMC (OS10) Bad packet length 263168.<br><br>Oct 3 15:58:31 10.19.2.10 1 2019-10-03T16:29:38.230866+00:00 OS10 sshd 1433 - - Node.1-Unit.1:PRI [audit], Dell EMC (OS10) ssh_dispatch_run_fatal: Connection from user admin 10.19.2.192 port 34202: Connection corrupted<br><br>Oct 3 15:58:31 10.19.2.10 1 2019-10-03T16:29:38.581820+00:00 OS10 dn_alm 697 - - Node.1-Unit.1:PRI [event], Dell EMC (OS10) %ALM_AUTH_EVENT: Authentication event was raised MESSAGE=pam_unix(sshd:session): session closed for user admin |
| FCS_TLSC_EXT.2 | Failure to establish a TLS Session | Bad certificate type:<br><br>Dec 17 15:02:32 10.19.2.10 1 2019-12-17T16:04:53.536619+00:00 OS10 syslog-ng 5061 - [meta sequenceId="1"] Node.1-Unit.1:PRI [audit], Dell EMC (OS10) Peer's certificate not valid for SSL/TLS server, rejecting;<br><br>Dec 17 15:02:32 10.19.2.10 1 2019-12-17T16:04:53.536619+00:00 OS10 syslog-ng 5061 - [meta sequenceId="2"] Node.1-Unit.1:PRI [audit], Dell EMC (OS10) Certificate validation failed; subject='CN=10.100.0.137, OU=CC1902, O=Lightship Security, L=Ottawa, ST=ON, C=CA', |

| Requirement | Audit Events | Examples |
|---|---|---|
| | | issuer='CN=Intermediate CA, OU=CC1902, O=Lightship Security, L=Ottawa, ST=ON, C=CA', error='unsupported certificate purpose', depth='0'<br><br>Dec 17 15:02:32 10.19.2.10 1 2019-12-17T16:04:53.536619+00:00 OS10 syslog-ng 5061 - [meta sequenceId="3"] Node.1-Unit.1:PRI [audit], Dell EMC (OS10) Alert ; vers='TLSv1.2 >>> unknown - unsupported certificate'<br><br>Dec 17 15:02:32 10.19.2.10 1 2019-12-17T16:04:53.536619+00:00 OS10 syslog-ng 5061 - [meta sequenceId="4"] Node.1-Unit.1:PRI [audit], Dell EMC (OS10) SSL error while writing stream; tls_error='SSL routines:ssl3_get_server_certificate:certificate verify failed' |
| FIA_AFL.1 | Unsuccessful login attempts limit is met or exceeded. | The “tally 4” indicates that this was the 4th attempt and the “deny 3” indicate that the login attempts limit has exceeded.<br>Reason for the failure in the 3rd audit message for this event indicates the source of the attempt (IP).<br>Sep 13 16:26:29 10.19.2.10 1 2019-09-13T16:32:25.129249+00:00 OS10 sshd 8513 - - Node.1-Unit.1:PRI [event], Dell EMC (OS10) pam_tally2(sshd:auth): user admin (1002) tally 4, deny 3<br>Sep 13 16:26:29 10.19.2.10 1 2019-09-13T16:32:25.547833+00:00 OS10 dn_alm 671 - - Node.1-Unit.1:PRI [event], Dell EMC (OS10) %ALM_AUTH_EVENT: Authentication event was raised MESSAGE=pam_tally2(sshd:auth): user admin (1002) tally 4, deny 3<br>Sep 13 16:26:35 10.19.2.10 1 2019-09-13T16:32:31.150973+00:00 OS10 sshd 8513 - - Node.1-Unit.1:PRI [audit], Dell EMC (OS10) Failed password for admin from 10.19.2.192 port 60430 ssh2 |
| FIA_UIA_EXT.1 | All use of identification and authentication mechanism. | Serial, good password:<br>Oct 1 16:43:15 10.19.2.10 1 2019-10-01T17:17:03.054742+00:00 OS10 sshd 19035 - - Node.1-Unit.1:PRI [event], Dell EMC (OS10) pam_unix(sshd:session): session opened for user admin by (uid=0)<br>Oct 1 16:43:15 10.19.2.10 1 2019-10-01T17:17:03.072994+00:00 OS10 dn_alm 700 - - |
| FIA_UAU_EXT.2 | All use of identification and authentication mechanism. | |

| Requirement | Audit Events | Examples |
|---|---|---|
| | | Node.1-Unit.1:PRI [event], Dell EMC (OS10) %ALM_AUTH_EVENT: Authentication event was raised MESSAGE=pam_unix(sshd:session): session opened for user admin by (uid=0)<br><br>Oct 1 16:43:20 10.19.2.10 1 2019-10-01T17:17:07.848570+00:00 OS10 .clish 19028 - - Node.1-Unit.1:PRI [audit], CLI session started for user admin with role sysadmin on /dev/ttyS0<br><br>Serial, bad password:<br><br>Oct 1 16:44:19 10.19.2.10 1 2019-10-01T17:18:07.042787+00:00 OS10 systemd 1 - - Node.1-Unit.1:PRI [audit], Dell EMC (OS10) Started Serial Getty on ttyS0.<br><br>Oct 1 16:46:35 10.19.2.10 1 2019-10-01T17:20:22.487272+00:00 OS10 audit 19152 - - Node.1-Unit.1:PRI [audit], Dell EMC (OS10) USER_AUTH pid=19152 uid=0 auid=4294967295 ses=4294967295 msg='op=PAM:authentication acct="admin" exe="/bin/login" hostname=? addr=? terminal=/dev/ttyS0 res=failed'<br><br>SSH, good password:<br><br>Oct 1 16:22:15 10.19.2.10 1 2019-10-01T16:56:02.496131+00:00 OS10 sshd 18310 - - Node.1-Unit.1:PRI [audit], Dell EMC (OS10) Accepted password for admin from 10.19.2.192 port 33916 ssh2<br><br>Oct 1 16:22:22 10.19.2.10 1 2019-10-01T16:56:10.018811+00:00 OS10 .clish 18326 - - Node.1-Unit.1:PRI [audit], CLI session started for user admin with role sysadmin on /dev/pts/0<br><br>SSH, bad password:<br><br>Oct 1 16:41:30 10.19.2.10 1 2019-10-01T17:15:18.289365+00:00 OS10 sshd 18968 - - Node.1-Unit.1:PRI [audit], Dell EMC (OS10) Failed password for admin from 10.19.2.192 port 33918 ssh2<br><br>Oct 1 16:41:30 10.19.2.10 1 2019-10-01T17:15:18.288887+00:00 OS10 audit 18968 - - Node.1-Unit.1:PRI [audit], Dell EMC (OS10) USER_AUTH pid=18968 uid=0 auid=4294967295 ses=4294967295 msg='op=PAM:authentication acct="admin" exe="/usr/sbin/sshd" |

| Requirement | Audit Events | Examples |
|---|---|---|
| | | hostname=10.19.2.192 addr=10.19.2.192 terminal=ssh res=failed'<br><br>Oct 1 16:41:30 10.19.2.10 1 2019-10-01T17:15:18.295734+00:00 OS10 sshd 18968 - - Node.1-Unit.1:PRI [audit], Dell EMC (OS10) Connection closed by authenticating user admin 10.19.2.192 port 33918 [preauth]<br><br>Unknown user:<br><br>Oct 2 15:24:14 10.19.2.10 1 2019-10-02T15:58:04.108078+00:00 OS10 sshd 14306 - - Node.1-Unit.1:PRI [audit], Dell EMC (OS10) Invalid user unknown from 10.19.2.192 port 34064<br><br>Oct 2 15:24:18 10.19.2.10 1 2019-10-02T15:58:08.345166+00:00 OS10 sshd 14306 - - Node.1-Unit.1:PRI [event], Dell EMC (OS10) pam_unix(sshd:auth): check pass; user unknown<br><br>Oct 2 15:24:18 10.19.2.10 1 2019-10-02T15:58:08.346144+00:00 OS10 sshd 14306 - - Node.1-Unit.1:PRI [event], Dell EMC (OS10) pam_unix(sshd:auth): authentication failure; logname= uid=0 euid=0 tty=ssh ruser= rhost=10.19.2.192<br><br>Oct 2 15:24:19 10.19.2.10 1 2019-10-02T15:58:08.671674+00:00 OS10 dn_alm 700 - - Node.1-Unit.1:PRI [event], Dell EMC (OS10) %ALM_AUTH_EVENT: Authentication event was raised MESSAGE=pam_unix(sshd:auth): check pass; user unknown<br><br>Oct 2 15:24:19 10.19.2.10 1 2019-10-02T15:58:08.673006+00:00 OS10 dn_alm 700 - - Node.1-Unit.1:PRI [event], Dell EMC (OS10) %ALM_AUTH_EVENT: Authentication event was raised MESSAGE=pam_unix(sshd:auth): authentication failure; logname= uid=0 euid=0 tty=ssh ruser= rhost=10.19.2.192<br><br>Oct 2 15:24:20 10.19.2.10 1 2019-10-02T15:58:10.169947+00:00 OS10 sshd 14306 - - Node.1-Unit.1:PRI [audit], Dell EMC (OS10) Failed password for invalid user unknown from 10.19.2.192 port 34064 ssh2 |
| FIA_X509_EXT.1/Rev | Unsuccessful attempt to validate a certificate | General purpose validation error or bad certificate (reason is augmented by examining packet Alert codes):<br><br><43>1 2019-10-11T18:34:42.347636+00:00 OS10 syslog-ng 10998 - [meta sequenceId="15"] Node.1-Unit.1:PRI [audit], Dell EMC (OS10) SSL error while |

| Requirement | Audit Events | Examples |
|---|---|---|
| | | writing stream; tls_error='SSL routines:ssl3_get_server_certificate:certificate verify failed'<br><br><45>1 2019-10-11T18:34:42.348854+00:00 OS10 syslog-ng 10998 - [meta sequenceId="16"] Node.1-Unit.1:PRI [audit], Dell EMC (OS10) Syslog connection broken; fd='42', server='AF_INET(10.100.0.137:6514)', time_reopen='60' |
| FMT_MOF.1/ ManualUpdate | Any attempt to initiate a manual update | See FPT_TUD_EXT.1 below. |
| FMT_MOF.1/ Functions | Modification of the behaviour of the transmission of audit data to an external IT entity, the handling of audit data, the audit functionality when Local Audit Storage Space is full. | 'The behaviour of the transmission of audit data to an external IT entity' cannot be modified. The old configuration has to be deleted and a new configuration should be added manually.<br><br>Jan 22 18:54:54 10.19.2.10 1 2020-01-22T19:58:13.737341+00:00 OS10 .clish 19950 - - Node.1-Unit.1:PRI [audit], User admin on /dev/pts/0 from 10.100.0.137 used cmd: 'logging server 10.100.0.177 severity log-debug tls 6514' - completed |
| FMT_SMF.1 | All management activities of TSF data. | All events in this table. |
| FPT_TUD_EXT.1 | Initiation of update; result of the update attempt (success or failure) | Updating the firmware is a 4 steps process:<br><br>Downloading the firmware:<br><br>Oct 3 10:50:10 10.19.2.10 1 2019-10-03T11:23:59.355353+00:00 OS10 dn_swupgrade 991 - - Node.1-Unit.1:PRI [audit], Download starting for scp://root:********@10.19.2.192/~/PKGS_OS10-Enterprise-10.5.0.1P1.433stretch-installer-x86_64.bin<br><br>Oct 3 10:50:10 10.19.2.10 1 2019-10-03T11:23:59.612948+00:00 OS10 .clish 3687 - - Node.1-Unit.1:PRI [audit], User admin on console used cmd: 'image download scp://root:*****@10.19.2.192/~/PKGS_OS10-Enterprise-10.5.0.1P1.433stretch-installer-x86_64.bin' - completed<br><br>Oct 3 10:51:59 10.19.2.10 1 2019-10-03T11:25:48.815297+00:00 OS10 dn_swupgrade 991 - - Node.1-Unit.1:PRI [audit], Download complete for file scp://root:********@10.19.2.192/~/PKGS_OS10- |

| Requirement | Audit Events | Examples |
|---|---|---|
| | | Enterprise-10.5.0.1P1.433stretch-installer-x86_64.bin. No error<br><br>Image verification:<br>Oct 3 11:46:35 10.19.2.10 1 2019-10-03T12:20:24.430479+00:00 OS10 dn_swupgrade 991 - - Node.1-Unit.1:PRI [audit], Verify: hash of image 2d2afd3a58a927ac9721f64ba1ac509b9568d91caf04591e6cd05f8c2e149e05<br>Oct 3 11:46:35 10.19.2.10 1 2019-10-03T12:20:24.673293+00:00 OS10 .clish 3687 - - Node.1-Unit.1:PRI [audit], User admin on console used cmd: 'image verify image://PKGS_OS10-Enterprise-10.5.0.1P1.433stretch-installer-x86_64.bin sha256' – completed<br><br>Installing the firmware:<br>Oct 3 10:58:22 10.19.2.10 1 2019-10-03T11:32:12.182835+00:00 OS10 dn_swupgrade 991 - - Node.1-Unit.1:PRI [audit], Installation starting<br>Oct 3 10:58:23 10.19.2.10 1 2019-10-03T11:32:12.477672+00:00 OS10 .clish 3687 - - Node.1-Unit.1:PRI [audit], User admin on console used cmd: 'image install image://PKGS_OS10-Enterprise-10.5.0.1P1.433stretch-installer-x86_64.bin' – completed<br>Oct 3 11:21:33 10.19.2.10 1 2019-10-03T11:55:22.638318+00:00 OS10 dn_swupgrade 991 - - Node.1-Unit.1:PRI [audit], Upgraded standby partition<br>Oct 3 11:21:33 10.19.2.10 1 2019-10-03T11:55:22.639340+00:00 OS10 dn_swupgrade 991 - - Node.1-Unit.1:PRI [audit], Installation complete<br><br>Making the installed firmware the boot firmware in the next boot:<br>Oct 3 12:08:20 10.19.2.10 1 2019-10-03T12:42:10.138322+00:00 OS10 dn_swupgrade 991 - - Node.1-Unit.1:PRI [audit], Set next-boot partition to STANDBY<br>Oct 3 12:08:20 10.19.2.10 1 2019-10-03T12:42:10.141690+00:00 OS10 .clish 3687 - - Node.1-Unit.1:PRI [audit], User admin on console used cmd: 'boot system standby' – completed |

| Requirement | Audit Events | Examples |
|---|---|---|
| FPT_STM_EXT.1 | Discontinuous changes to time - either Administrator actuated or changed via an automated process. | Oct 3 12:41:39 10.19.2.10 1 2019-10-03T15:00:01.521529+00:00 OS10 mgmtsys.py 660 - - Node.1-Unit.1:PRI [audit], Current system time changed from Thu Oct 3 13:15:27 2019 to 2019-10-03T15:00:00Z<br><br>Oct 3 12:41:39 10.19.2.10 1 2019-10-03T15:00:01.766155+00:00 OS10 .clish 2897 - - Node.1-Unit.1:PRI [audit], User admin on console used cmd: 'clock set 15:00:00 2019-10-03' - completed |
| FTA_SSL_EXT.1 | The termination of a local session by the session locking mechanism. | When the session is terminated by the session locking mechanism, there is one less audit message than when a user initiated termination (See FTA_SSL.4).<br>Oct 3 13:21:50 10.19.2.10 1 2019-10-03T13:52:56.833810+00:00 OS10 systemd 1 - - Node.1-Unit.1:PRI [audit], Dell EMC (OS10) Started Serial Getty on ttyS0.<br><br>Oct 3 13:21:50 10.19.2.10 1 2019-10-03T13:52:56.832279+00:00 OS10 dn_alm 697 - - Node.1-Unit.1:PRI [event], Dell EMC (OS10) %ALM_AUTH_EVENT: Authentication event was raised MESSAGE=pam_unix(sshd:session): session closed for user testadmin |
| FTA_SSL.3 | The termination of a remote session by the session locking mechanism. | When the session is terminated by the session locking mechanism, there is one less audit message than when a user initiated termination (See FTA_SSL.4).<br>Oct 3 15:21:04 10.19.2.10 1 2019-10-03T15:52:11.374004+00:00 OS10 audit 32474 - - Node.1-Unit.1:PRI [audit], Dell EMC (OS10) USER_END pid=32474 uid=0 auid=1006 ses=80 msg='op=PAM:session_close acct="testadmin" exe="/usr/sbin/sshd" hostname=10.19.2.192 addr=10.19.2.192 terminal=ssh res=success'<br>Oct 3 15:21:04 10.19.2.10 1 2019-10-03T15:52:11.372220+00:00 OS10 sshd 32481 - - Node.1-Unit.1:PRI [audit], Dell EMC (OS10) Received disconnect from 10.19.2.192 port 34174:11: disconnected by user<br>Oct 3 15:21:04 10.19.2.10 1 2019-10-03T15:52:11.373253+00:00 OS10 sshd 32481 - - Node.1-Unit.1:PRI [audit], Dell EMC (OS10) |

| Requirement | Audit Events | Examples |
|---|---|---|
| | | Disconnected from user testadmin 10.19.2.192 port 34174<br><br>Oct 3 15:21:04 10.19.2.10 1 2019-10-03T15:52:11.234812+00:00 OS10 sshd 32484 - - Node.1-Unit.1:PRI [event], Dell EMC (OS10) pam_unix(sshd:session): session closed for user testadmin |
| FTA_SSL.4 | The termination of an interactive session. | For Serial:<br><br>Oct 3 15:10:49 10.19.2.10 1 2019-10-03T15:41:55.546954+00:00 OS10 sshd 32261 - - Node.1-Unit.1:PRI [event], Dell EMC (OS10) pam_unix(sshd:session): session closed for user admin<br><br>Oct 3 15:10:49 10.19.2.10 1 2019-10-03T15:41:55.497025+00:00 OS10 .clish 32258 - - Node.1-Unit.1:PRI [audit], User admin on console used cmd: 'exit' - completed<br><br>Oct 3 15:10:49 10.19.2.10 1 2019-10-03T15:41:55.835845+00:00 OS10 systemd 1 - - Node.1-Unit.1:PRI [audit], Dell EMC (OS10) Stopped Serial Getty on ttyS0.<br><br>For SSH:<br><br>Oct 3 15:25:36 10.19.2.10 1 2019-10-03T15:56:43.100599+00:00 OS10 sshd 32578 - - Node.1-Unit.1:PRI [audit], Dell EMC (OS10) Received disconnect from 10.19.2.192 port 34176:11: disconnected by user<br><br>Oct 3 15:25:36 10.19.2.10 1 2019-10-03T15:56:42.971092+00:00 OS10 sshd 32581 - - Node.1-Unit.1:PRI [event], Dell EMC (OS10) pam_unix(sshd:session): session closed for user testadmin<br><br>Oct 3 15:25:36 10.19.2.10 1 2019-10-03T15:56:43.101570+00:00 OS10 sshd 32578 - - Node.1-Unit.1:PRI [audit], Dell EMC (OS10) Disconnected from user testadmin 10.19.2.192 port 34176<br><br>Oct 3 15:25:36 10.19.2.10 1 2019-10-03T15:56:43.102289+00:00 OS10 sshd 32570 - - Node.1-Unit.1:PRI [event], Dell EMC (OS10) pam_unix(sshd:session): session closed for user testadmin<br><br>Oct 3 15:25:36 10.19.2.10 1 2019-10-03T15:56:42.922267+00:00 OS10 .clish 32580 - - Node.1-Unit.1:PRI [audit], User testadmin on |

| Requirement | Audit Events | Examples |
|---|---|---|
| | | /dev/pts/0 from 10.19.2.192 used cmd: 'exit' - completed |
| FTP_ITC.1 | Initiation of the trusted channel.<br>Termination of the trusted channel.<br>Failure of the trusted channel functions. | Initiation of the trusted channel:<br><45>1 2019-10-21T11:34:28.259642+00:00 OS10 syslog-ng 23813 - [meta sequenceId="4"] Node.1-Unit.1:PRI [audit], Dell EMC (OS10) Syslog connection established; fd='38', server='AF_INET(10.100.0.137:6514)', local='AF_INET(0.0.0.0:0)'<br><br>Termination of the trusted channel:<br><43>1 2019-10-21T12:34:14.825451+00:00 OS10 syslog-ng 23813 - [meta sequenceId="1"] Node.1-Unit.1:PRI [audit], Dell EMC (OS10) Syslog connection failed; fd='15', server='AF_INET(10.100.0.137:6514)', error='Connection timed out (110)', time_reopen='60'<br><br>Failure of the trusted channel:<br><45>1 2019-10-21T12:31:04.357734+00:00 OS10 syslog-ng 23813 - [meta sequenceId="1"] Node.1-Unit.1:PRI [audit], Dell EMC (OS10) Syslog connection broken; fd='0', server='AF_INET(10.100.0.137:6514)', time_reopen='60' |
| FTP_TRP.1/ Admin | Initiation of the trusted path.<br>Termination of the trusted path.<br>Failure of the trusted path functions. | See FTA_SSL.4 and FCS_SSHS_EXT.1 above. |