Dell EMC VxFlex Ready Node

Version 2.x

AMS Security Configuration Guide

302-003-665

REV 05

DELL EMC

Copyright © 2017-2018 Dell Inc. or its subsidiaries. All rights reserved.

Published June 2018

Dell believes the information in this publication is accurate as of its publication date. The information is subject to change without notice.

THE INFORMATION IN THIS PUBLICATION IS PROVIDED "AS-IS." DELL MAKES NO REPRESENTATIONS OR WARRANTIES OF ANY KIND WITH RESPECT TO THE INFORMATION IN THIS PUBLICATION, AND SPECIFICALLY DISCLAIMS IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. USE, COPYING, AND DISTRIBUTION OF ANY DELL SOFTWARE DESCRIBED IN THIS PUBLICATION REQUIRES AN APPLICABLE SOFTWARE LICENSE.

Dell, EMC, and other trademarks are trademarks of Dell Inc. or its subsidiaries. Other trademarks may be the property of their respective owners. Published in the USA.

Dell EMC
Hopkinton, Massachusetts 01748-9103
1-508-435-1000 In North America 1-866-464-7381
www.DellEMC.com

CONTENTS

Tables 5

Preface 7

Chapter 1 Introduction 9
Overview 10

Chapter 2 Access Control Settings 11
General 12
User authentication 13
Default accounts 13
Authentication configuration 14
MDM password reset 15
Login banner 15
Component access control 15
Component authentication 15
Component authorization 16
VxFlex Ready Node deployment phase 16
System IP address information 16
AMS recovery 16
AMS take ownership 16

Chapter 3 AMS Sampling 17
General 18

Chapter 4 Log Settings 19
Log description 20
Log management and retrieval 21

Chapter 5 Communication Security Settings 23
Port usage and changing default ports 24
VLAN support 25
Network encryption 25

Chapter 6 Secure Secret Information 27
Lockbox overview 28

Chapter 7 Data Security Settings 29
Data integrity 30

Chapter 8 Known Issues 31
Known Issues 32
Prevent certificate errors when ESX hosts are added using hostnames 33
iDRAC certificate replacement issue 34

TABLES

1 Default accounts.....13
2 Log files.....20
3 Default ports.....24

Preface

As part of an effort to improve its product lines, Dell EMC periodically releases revisions of its software and hardware. Therefore, some functions described in this document might not be supported by all versions of the software or hardware currently in use. The product release notes provide the most up-to-date information on product features.

Contact your Dell EMC technical support professional if a product does not function properly or does not function as described in this document.

Note

This document was accurate at publication time. Go to Dell EMC Online Support (https://support.emc.com) to ensure that you are using the latest version of this document.

Previous versions of Dell EMC VxFlex OS were marketed under the name Dell EMC ScaleIO.

Similarly, previous versions of Dell EMC VxFlex Ready Node were marketed under the name Dell EMC ScaleIO Ready Node.

References to the old names in the product, documentation, or software, etc. will change over time.

Note

Software and technical aspects apply equally, regardless of the branding of the product.

Related documentation

The release notes for your version includes the latest information for your product.

The following Dell EMC publication sets provide information about your VxFlex OS or VxFlex Ready Node product:

- VxFlex OS software (downloadable as VxFlex OS Software <version> Documentation set)
- VxFlex Ready Node with AMS (downloadable as VxFlex Ready Node with AMS Documentation set)
- VxFlex Ready Node no AMS (downloadable as VxFlex Ready Node no AMS Documentation set)
- VxRack Node 100 Series (downloadable as VxRack Node 100 Series Documentation set)

You can download the release notes, the document sets, and other related documentation from Dell EMC Online Support.

Typographical conventions

Dell EMC uses the following type style conventions in this document:

Bold	Used for names of interface elements, such as names of windows, dialog boxes, buttons, fields, tab names, key names, and menu paths (what the user specifically selects or clicks)

Italic	Used for full titles of publications referenced in text
`Monospace`	Used for: • System code • System output, such as an error message or script • Pathnames, filenames, prompts, and syntax • Commands and options
Monospace italic	Used for variables
`Monospace bold`	Used for user input
[ ]	Square brackets enclose optional values
|	Vertical bar indicates alternate selections - the bar means “or”
{ }	Braces enclose content that the user must specify, such as x or y or z
...	Ellipses indicate nonessential information omitted from the example

Where to get help

Dell EMC support, product, and licensing information can be obtained as follows:

Product information

For documentation, release notes, software updates, or information about Dell EMC products, go to Dell EMC Online Support at https://support.emc.com.

Technical support

Go to Dell EMC Online Support and click Service Center. You will see several options for contacting Dell EMC Technical Support. Note that to open a service request, you must have a valid support agreement. Contact your Dell EMC sales representative for details about obtaining a valid support agreement or with questions about your account.

Your comments

Your suggestions will help us continue to improve the accuracy, organization, and overall quality of the user publications. Send your opinions of this document to techpubcomments@emc.com.

CHAPTER 1

Introduction

This guide provides an overview of the security settings available in VxFlex Ready Node to ensure secure operation of the product.

- Overview 10

Overview

This topic provides an overview of the product's security features.

The security features described here are used by the AMS solution, which manages the VxFlex Ready Node® product family.

Security settings are divided into the following categories:

- *Access Control Settings* describes the settings available to limit access by end-user or external product components.
- *AMS Sampling* describes the monitoring schedule used for the continuous sampling of the system by the AMS.
- *Log Settings* describes settings related to the logging of events.
- *Communication Security Settings* describes settings related to security for the product's network communications.
- *Secure Secret Information* describes the secure password retention mechanism used by the AMS.
- *Data Security Settings* describes settings available to ensure protection of the data handled by the product.

CHAPTER 2

Access Control Settings

This section describes the access control settings used to protect resources against unauthorized access. Topics include:

- General 12
- User authentication 13
- Component access control 15

General

This topic describes access control settings supported by the system.

AMS

- The username and password are needed to access the VxFlex Ready Node AMS (management server).
- The username is initially `admin`, but can be configured to use LDAP or other local usernames.
- The password should be set during the first login by the user, but may be modified after the first login.
- Authentication is done with the AMS server.
- Restricted SDC mode—a system can be configured to only allow "approved" SDCs to connect to the MDM. This mode requires you to map volumes only to SDCs which have been previously approved by the user, by configuring them either by IP address or GUID. For more information, see your system's *User Guide*.
- Access to REST via the AMS requires a password.
- REST authenticates user access, using the *AMSAdminPassword* (for more information, see the *VxFlex Ready Node REST API Reference Guide*).
- SSL authentication of internal components to the MDM—allows secure authentication of VxFlex OS SDS components to the MDM using a Public and Private Key (Key-Pair) associated with a certificate. The trust is established when adding the SDS, and reconnecting will require reauthentication.
- Secure connectivity with external components—allows external components to authenticate the MDM with a certificate and authenticate back to the MDM with a username and password. After authentication, communication between the MDM and external components is performed using TLS (Transport Layer Security) protocols. External components include: VxFlex OS CLI client, VxFlex OS GUI client, and LIAs.
- A manually generated public-private key pair can be used to perform SSH key authentication, instead of passwords, between the VxFlex OS Gateway and VxFlex OS servers.
- An RSA Lockbox is used to store MDM credentials on the VxFlex OS Gateway. These credentials are required for authentication purposes by the SNMP trap sender and ESRS.
- The VxFlex OS GUI and VxFlex OS CLI use AMS Local authentication.
  - For more information about logging in to the VxFlex OS CLI, see the chapter "Security and User Management" in the *VxFlex Ready Node User Guide*.
  - For more information about logging in to the VxFlex OS GUI, see the chapter "Using the Graphical User Interface" in the *VxFlex Ready Node User Guide*.
- SNMP feature enabler—the SNMP trap sender can be enabled or disabled by configuring the SNMP Trap receiver. For detailed information, see the topic "Modifying System Settings, SNMP", in the chapter "Using the Graphical User Interface" in the *VxFlex Ready Node User Guide*.
- REST feature enabler—access to the REST gateway can be blocked by configuring the `gatewayUser.properties` file located on the VxFlex Ready Node AMS. The feature is enabled by default. For detailed information, see

"Configuring the VxFlex OS Gateway by editing the user properties file," in the *VxFlex Ready Node REST API Reference Guide*.

MDM

- Restricted SDC mode—a system can be configured to only allow “approved” SDCs to connect to the MDM

Note

OpenSSL 64-bit v1.0.1 or higher is required for secure authentication. In Linux, this version of OpenSSL is only supported in CentOS and RHEL 6.5 or higher.

User authentication

This section describes the user authentication settings that control the process of verifying an identity claimed by a user for accessing the product.

Default accounts

This topic provides details about the system's default accounts.

Table 1 Default accounts

User Account	Password	Description
AMS admin	Password is set in the AMS	The account provides full administrator privileges to all configuration and monitoring activities via the AMS. The root password is saved on the AMS using the RSA lockbox solution.
ESX root user	Password is set in the AMS	The account provides full administrator privileges to all configuration and monitoring activities via the AMS to the ESX. The root password is saved on the AMS using the RSA lockbox solution.
SVM root user	Password is set in the AMS	The account provides full administrator privileges to all configuration and monitoring activities via the AMS to the Storage VM (SVM). The root password is saved on the AMS using the RSA lockbox solution.
Dell node root user	Password is set in the AMS	The account provides full administrator privileges to all configuration and monitoring activities via the AMS to the IPMI interface. The root password is saved on the AMS using the RSA lockbox solution.
MDM admin	Password is set in the AMS	The MDM has only one default account (*admin*) with a password ("admin”) set by the AMS. The password is used only during the initial Deployment flow and then is changed to "ams_admin". The account provides full administrator privileges to all configuration and monitoring activities via the CLI and the VxFlex OS GUI. The admin password is saved on the AMS using the RSA lockbox solution.
MDM ams_admin	Password is set in the AMS	The AMS creates this password to manage all mdm queries and actions. The account provides full administrator privileges to all configuration and

Table 1 Default accounts (continued)

User Account	Password	Description
		monitoring activities via the AMS to the MDM. The admin password is saved on the AMS using the RSA lockbox solution.
MDM ams_monitor	Password is set in the AMS	ams_monitor is created during deployment, and is used for ongoing queries to the MDM only. Any additional users created later using scli in the MDM allow actions based on the permission of the group to which the user belongs. Refer to the *User Guide* and to the *VxFlex OS User Roles and LDAP Usage Technical Notes* for more information about user groups.

Authentication configuration

This topic describes local password requirements.

Note

For LDAP users, the requirements are defined by the authenticating server according to the organization's user policy.

User authentication is initially configured during VxFlex Ready Node installation. The AMS, ESX, SVM and BMC (iDRAC) passwords must meet the following criteria:

- Include at least 3 of the following groups: [a-z], [A-Z], [0-9]
- Contain between 6 and 31 characters
- No white spaces

Note

The ESXi 6 password policy has the following additional requirements:

- Passwords must contain characters from at least three character classes.
- Passwords containing characters from three character classes must be at least seven characters long.

An uppercase character that begins a password does not count toward the number of character classes used. A number that ends a password does not count toward the number of character classes used.

For more information, see the chapter "Security and User Management" in the *VxFlex Ready Node User Guide*.

Note

ESXi 6 security policy is disabled.

MDM password reset

This topic explains what to do when you need to change the MDM password for troubleshooting purposes.

The MDM admin password can be reset for troubleshooting. For more information, refer to "Issuing SCLI commands without the MDM password" in the *VxFlex Ready Node User Guide*.

Login banner

A login banner can be configured for both VxFlex OS GUI and CLI users.

A login banner is a text file that is displayed upon login to the system. It can be used to communicate messages or to obtain user consent to real-time monitoring of information and retrieval of stored files. When the login banner is set up, it appears during the system login process before the login credential prompts. The login banner displays differently in the VxFlex OS GUI and in the CLI interfaces:

- GUI—When logging in, the login banner is displayed, and must be approved.
- CLI—When logging in, the user is prompted to press any key, after which the banner is displayed. To continue, the banner must be approved.

If a login banner is not required, the feature can be disabled. For more information about configuring these banners, refer to your system's *User Guide*.

Component access control

This section describes component access control. Component access control settings define control over access to the product by external and internal systems or components.

Component authentication

The system provides secure connectivity between internal and external components.

Secure connectivity with internal and external components

SSL authentication is used to authenticate both internal system components, and communication between the MDM and external components such as the AMS, VxFlex OS GUI clients, and CLI clients. Secure communication is typically installed and configured by default during system deployment. An administrator may supply a self-signed certificate.

Note

After renewing certificates, you cannot change the connection between AMS and VxFlex OS components from secure mode to non-secure mode.

LIA

LIA establishes trust with the AMS via a configurable token. The LIA token is stored in `/opt/emc/scaleio/lia/cfg/conf.txt`. The line in the file that can be configured is:

lia_token=xxxx

Where xxxx represents the token. The token should be added to every request sent to LIA. LIA checks that the token received is equal to the one that appears in the configuration file.

To change the LIA password you must run an AMS recovery flow that will generate a new LIA password and modify it for all devices.

Component authorization

This topic describes the configurable LIA parameters for component authorization.

All the configurable parameters of LIA are included in the file `/opt/emc/scaleio/lia/cfg/conf.txt`. The list includes:

lia_token, *lia_enable_install*, *lia_enable_uninstall*, *lia_enable_configure*, and *lia_enable_fetch_logs*.

VxFlex Ready Node deployment phase

This topic describes automated password creation during the deployment phase.

- During the deployment phase, a new user called *ams_admin* is created in the MDM. This user is used by the AMS to communicate with the MDM. Its password is set randomly, and should NEVER be altered.
- During deployment of the VxFlex Ready Node environment, passwords are set for each of the discovered nodes for the ESX SVM and BMC (iDRAC).

System IP address information

This topic describes the system IP information that is saved on the AMS.

The following information is saved in text files on the AMS:

- `ams.cfg`—contains all IP address ranges used by the VxFlex Ready Node system
- `nodes.cfg`—contains the node list with internal information

AMS recovery

This topic describes what happens when an AMS enters the recovery phase.

During the AMS recovery phase, all AMS admin, admin (MDM), ams_admin (mdm), and LIA are regenerated and set on all relevant entities.

For more information on how to run AMS recovery, see "Recovering a lost AMS server" in the *VxFlex Ready Node Deployment Guide*.

AMS take ownership

The AMS can "take ownership" of all the nodes in an existing VxFlex Ready Node system that is currently running VxFlex OS without AMS management. When the process is complete, all the servers in the system are managed with the AMS.

The LIA passwords are modified during the take ownership. After the take ownership process is complete, you should run the renew certificate process.

CHAPTER 3

AMS Sampling

This section explains the AMS sampling mechanism. Topics include:

- General 18

General

This topic provides an overview of AMS sampling mechanisms.

The AMS samples Storage VMs (SVMs), ESXs and BMCs every 60 seconds, via an SSH connection that is kept alive in normal operating conditions. This mechanism prevents the need to initiate a login every 60 seconds.

The folder `model_cache` is the cache sampling folder, containing text files for all the hardware and system information that is collected every 60 seconds.

CHAPTER 4

Log Settings

This section describes the logs collected by VxFlex OS. A log is a chronological record of system activities that is sufficient to enable the reconstruction and examination of the sequence of environments and activities surrounding or leading to an operation, procedure, or event in a security-relevant transaction from inception to final results. Topics include:

- Log description 20
- Log management and retrieval 21

Log description

This topic describes the logs collected by the system.

The AMS collects logs from Storage VMs (SVMs) via the LIA agent (similar to what is done in the software-only VxFlex OS solution). The log only collects information for VxFlex OS components; the Storage VM (SVM) log is collected as part of the LIA log. In addition, the AMS logs are collected.

Note

VxFlex OS uses Apache Tomcat, which has its own set of standard logs. For more information about Tomcat logs, refer to Apache Tomcat documentation.

Table 2 Log files

Component	Location
MDM log The logs do not contain any user data (as the user data do not pass through the MDM) The logs may contain the MDM's user names (but never passwords), IP addresses, MDM configuration commands, events etc.	Linux: `/opt/emc/scaleio/mdm/logs` Windows: `c:\Program Files\emc\scaleio\mdm\logs`
REST logs	<AMS installed folder>\logs For example: Windows—`c:\Program Files\emc\scaleio\ams\logs` Linux—`/opt/emc/scaleio/ams/logs` The following logs are available: • `scaleio.log` • `scaleio-trace.log` • `operations.log` • `localhost_access_log.log` • `audit.log` • `api_operations.log`
AMS logs and cfg files	AMS logs are located in the following locations: • Windows: ▪ `c:\Program Files\EMC\ScaleIO\AMS\logs\` ▪ `c:\Program Files\EMC\ScaleIO\AMS\webapps\ROOT\WEB-INF\classes\` ▪ `C:\Program Files\EMC\ScaleIO\AMS\cfg` ▪ `C:\Users\<username>\AppData\Roaming\EMC\scaleiologs`

Table 2 Log files (continued)

Component	Location

	• Linux:
	  ▪ `/opt/emc/scaleio/ams/logs/`
	  ▪ `/opt/emc/scaleio/ams/webapps/ROOT/WEB-INF/classes/`
	  ▪ `/opt/emc/scaleio/ams/cfg/`
	The following logs are available:
	• `scaleio.log`
	• `operations.log`
	• `localhost_access_log.log`
	• `nodes.cfg`
	• `ams.cfg`
	• `model_cache` folder
	• AMS configuration files

LIA logs	Windows: • `C:\Program Files\emc\scaleio\lia\logs` Linux: • `/opt/emc/scaleio/lia/logs`
Tomcat logs	Windows: • `C:\Program Files\EMC\ScaleIO\ams\logs\tomcat.log` Linux: • `/opt/emc/scaleio/ams/logs`
VxFlex OS GUI logs	Windows: • `%AppData%\EMC\ScaleIO\logs` Linux: • `%AppData%\EMC\ScaleIO\logs`
ESXi Log:	Kernel logs
iDRAC event Log:	IDRAC event logs
perrcli Log:	Event logs

Log management and retrieval

This topic describes the ways in which logs can be managed and retrieved.

- Log roll-over (AMS)
  - In the configuration of the log's behavior (`logback.xml`—see below), each log is defined to be no greater than 10 MB. Once it reaches this size, a new log

file is created. Once the maximum (10) is reached, the oldest log is overwritten (roll-over). The log files are: `name_xxx.log, name_xxx.1.log.zip, … name_xxx.10.log.zip`.

- AMS log collection has been enhanced in the following ways:
  - In addition to the VxFlex OS and AMS Logs, now RAID controller, iDRAC, and OS logs (including ESX) are collected.
  - You can make on-the-fly selection of which log types to collect and on which nodes.
  - The multi-phase collection process enables you to know log file size and to manage space and resource limits before they occur.
  - In the deployment wizard, a log collection button was added to simplify collecting logs during this process.
- Configuration of an external Syslog server:
  - During VxFlex OS installation, you can use scli commands to configure Syslog event reporting. You can also configure these features after installation, using the scli. For more information, see the appendix "System Events and Alerts" in the *VxFlex Ready Node User Guide* for CLI commands.
- Configuration of logging levels:
  - VxFlex OS GUI—Logging levels can be modified. For more information, see the topic "Customizing System Preferences" in the chapter "Using the Graphical User Interface", in the *VxFlex Ready Node User Guide*.
  - REST gateway—The log can be configured by editing the file: `<ams installation folder>\webapps\ROOT\WEB-INF\classes \logback.xml`
  - AMS—The log can be configured by editing the file: `<ams installation folder>\webapps\ROOT\WEB-INF\classes\logback.xml`
- ESRS feature (EMC Secure Remote Support)—ESRS support enables secure, high-speed, 24x7, remote connection between EMC and customer installations, including:
  - Remote monitoring
  - Remote diagnosis and repair
  - Daily sending of logs, alerts, and VxFlex OS topology configured post AMS deployment of the VxFlex Ready Node. For more information, see the topic "Settings windows – Set ESRS server" in the *VxFlex Ready Node Depolyment Guide*.
- Viewing events locally—In the GUI, all events are stored in the **Alerts** view, where any active alert appears in the **Alert** table

CHAPTER 5

Communication Security Settings

This section describes the VxFlex OS system's security settings. Communication security settings enable the establishment of secure communication channels between the product components, as well as between product components and external systems or components. Topics include:

- Port usage and changing default ports 24
- VLAN support 25
- Network encryption 25

Port usage and changing default ports

The following table lists the TCP ports that are used by VxFlex OS. Prior to installing or upgrading a system, ensure that these ports are not in use by other processes.

If they are in use, either free them or change them to another available port.

Table 3 Default ports

Port used by	Port #	Protocol	File to change	Field to modify (or to add, if it does not exist)	Notes
AMS and MDM listener	6611	Protobuf over TCP	**Note** Cannot be modified, and must be available		
MDM Cluster member	9011	Protobuf over TCP	`/opt/emc/scaleio/mdm/cfg/conf.txt`	`actor_cluster_port=`*<NEW_PORT>*	
SDS listener	7072	Proprietary protocol over TCP	`/opt/emc/scaleio/sds/cfg/conf.txt`	`tgt_port=`*<NEW_PORT>*	SDCs connect through this port for data communication and to the MDM for meta-data communication. When multiple SDSs are installed on the same physical server, use ports 7072+*x*, where *x* is the index of the SDS (for example, 70721, 70722).
LIA listener	9099	Protobuf over TCP	`/opt/emc/scaleio/lia/cfg/conf.txt`	`lia_port=`*<NEW_PORT>*	The VxFlex OS Installation Manager connects to the LIA to perform installation and maintenance-related operations.
SNMP	162	SNMP v2 over UDP			SNMP traps for system alerts are sent to a trap receiver via this port. The VxFlex OS Gateway sends messages to: snmp.traps_receiver_ip on the port snmp.port
SDBG for MDM (Manager)	25620				Used by VxFlex OS internal debugging tools to extract live information from the system for debugging purposes. When multiple SDSs are installed on the same physical server, use ports 2564+*x*, where *x* is the index of the SDS (for example, 25641, 25642).
SDBG for MDM (Tie Breaker)	25600				
SDBG for SDS	25640				
AMS (secure)	443		`AMS installation directory\conf\server.xml`	`redirectPort=`*<NEW_PORT>* `Connector port=`*<NEW_PORT>*	After changing the port, you must restart the VxFlex OS Gateway service/daemon: • Linux: Run `service scaleio-gateway restart`

Table 3 Default ports (continued)

Port used by	Port #	Protocol	File to change	Field to modify (or to add, if it does not exist)	Notes
AMS (not secure)	80		`AMS installation directory\conf\server.xml`	`Connector port=`*<NEW_PORT>*	• Windows: Restart the VxFlex OS Gateway service

VLAN support

The AMS supports VLAN tagging.

The VLAN tagging feature enables segregation of the networks to separate VLANs, allowing only the AMS to communicate with all networks. The network administrator may configure a different VLAN ID for each of the following networks:

- Management ESX—1 GbE network
- Management SVM—1 GbE network
- Management BMC (iDRAC)—1 GbE network
- Data A—10/25/100 Data A and B GbE network
- Data B—10/25/100 Data A and B GbE network

The ESX image is configured to accept all VLANs during deployment, by using the VLAN ID 4095 in the ESX Port group.

During the deployment Set IP phase, the requested VLAN ID is set in the relevant Port group or vmkernel on the ESX or the BMC (iDRAC) port, using IPMI-related commands.

Network encryption

This topic explains how network encryption is performed by the system.

REST AMS uses TLSv1.1.

REST AMS through https, (over TLSv1.1). By default, the driver ignores verification of the VxFlex OS Gateway's TLSv1.1 certificate, but it can verify the certificate if the following configuration parameters are defined:

- `verify_server_certificate`—set to *True*, if the server's certificate must be verified, and to *False* if no verification is required.
- `server_certificate_path`—If the parameter *verify_server_certificate* is set to *True*, specify the location of the `.pem` file containing the server's certificate.

For instructions for generating a self-signed certificate using Keytool, see the section "Generating a self-signed certificate using the keytool utility" in the *VxFlex OS Deployment Guide*.

The following encryption methods are approved for use with your system:

- AMS components other than MDM:
  - TLS_DHE_DSS_WITH_AES_128_CBC_SHA256

- TLS_DHE_DSS_WITH_AES_128_GCM_SHA256
- TLS_DHE_RSA_WITH_AES_128_CBC_SHA256
- TLS_DHE_RSA_WITH_AES_128_GCM_SHA256
- TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256
- TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256
- TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256
- TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
- TLS_ECDH_ECDSA_WITH_AES_128_CBC_SHA256
- TLS_ECDH_ECDSA_WITH_AES_128_GCM_SHA256
- TLS_ECDH_RSA_WITH_AES_128_CBC_SHA256
- TLS_ECDH_RSA_WITH_AES_128_GCM_SHA256
- TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384
- TLS_RSA_WITH_AES_256_CBC_SHA256

CHAPTER 6

Secure Secret Information

This section describes the lockbox mechanism, into which all passwords and user names are saved. Topics include:

- Lockbox overview 28

Lockbox overview

This topic describes the lockbox use and location.

All passwords and users are saved into a lockbox mechanism, including the MDM admin user's password. The lockbox is a protected environment created by proprietary software and resides on the AMS Server.

The lockbox is located in the following directories:

- Windows: `C:\Program Files\EMC\scaleio\AMS\conf\lck_xml`
- Linux: `/opt/emc/scaleio/ams/conf/lck_xml/`

The lockbox is used for the following non-MDM users' passwords:

- ESX user
- Storage VM (SVM) user
- BMC (iDRAC user)
- ESRS user
- AMS Recovery user

Manipulation of passwords from outside the AMS is not supported.

CHAPTER 7

Data Security Settings

This section describes the data security settings used to define the controls that prevent permanently stored data from being disclosed in an unauthorized manner. Topics include:

- Data integrity 30

Data integrity

This section describes the integrity of data.

To erase data, one must use an external tool to perform the secure erasure.

CHAPTER 8

Known Issues

This chapter describes known security issues and workarounds. Topics include:

- Known Issues 32
- Prevent certificate errors when ESX hosts are added using hostnames 33
- iDRAC certificate replacement issue 34

Known Issues

This topic contains known security issues and workarounds.

Issue:

VxFlex OS versions prior to 2.0.1.1 may be vulnerable to the following vulnerabilities:

- Privilege escalation vulnerability
  A low-privileged local attacker may be able to modify the kernel memory in the SCINI driver, and may achieve code execution to escalate privileges to root on Storage Data Client (SDC) servers.
- Denial-of-service vulnerability via IOCTL calls
  A low-privileged local attacker may cause a denial-of-service by generating a kernel panic in the SCINI driver using IOCTL calls, which may render the Storage Data Client (SDC) server unavailable until the next restart.
- Denial-of-service through configuration API
  Incorrect permissions on the SCINI driver may allow a low-privileged local attacker to modify the configuration and render the Storage Data Client (SDC) server unavailable.

Resolution:

VxFlex OS version 2.0.1.1 contains resolutions to these vulnerabilities. Therefore, Dell EMC recommends a system upgrade at the earliest possible opportunity. For those who are unable to upgrade, Dell EMC recommends changing the access permission to 600. On each SDC, execute the SHELL command:

```
chmod 600 /dev/scini
```

Note

- This command should be executed "as-is" (Do not add anything else to the command).
- This command should be executed after every reload of the SDC, or after every restart.
- Once VxFlex OS is upgraded to version 2.0.1.1, there is no need to use this workaround.

Issue:

After upgrading the Operating System, the System Stable Values (SSVs) that Lockbox uses to fingerprint the system it is part of might change. In other words, the Lockbox may not be present or may lose content after the OS upgrade.

Resolution:

To update or reconfigure the Lockbox:

1. Open Lockbox with the password that was used to create it.
2. Reconfigure the Lockbox.

Note

If the Lockbox is not present, re-create the Lockbox using the command:

```
/opt/emc/scaleio/gateway/bin/FOSGWTool.sh --set_ldap_properties --
server_url ldap://<LDAP SERVER IP> --base_dn "<BASE_DN>" --group_name
"<GROUP NAME>" --create_default_lockbox
```

LDAPS users must use: `ldaps:// <LDAP SERVER IP>`

instead of `ldap://` in the example above.

Issue:

Dell EMC is aware of the side-channel analysis vulnerabilities (also known as Meltdown and Spectre) affecting many modern microprocessors that were publicly described by a team of security researchers on January 3, 2018. We encourage customers to review the Security Advisories in the References section at the following location for more information.

http://www.dell.com/support/article/uk/en/ukbsdt1/sln308588/microprocessor-side-channel-vulnerabilities-cve-2017-5715-cve-2017-5753-cve-2017-5754-impact-on-dell-emc-products-dell-enterprise-servers-storage-and-networking-?lang=en

AMS deployment and upgrade processes implement the Meltdown and Spectre security patches automatically. During the deployment or upgrade processes, the user may choose whether to enable or disable the security patches on RHEL servers. Refer to the *VxFlex Ready Node Deployment Guide* and *VxFlex Ready Node Upgrade Guide* for detailed steps.

- AMS deployments include the patches by default.
- Upgrade to version 2.6 via AMS includes the security patching.

Prevent certificate errors when ESX hosts are added using hostnames

When hosts are added to the vCenter using hostnames, a certificate alert raised by the AMS, and certificate renewal fails. Edit the `ams.properties` file to prevent occurrence of this issue.

Note

The change made to the file that is edited in this workaround is not saved during upgrades, and may need to be performed again.

Procedure

1. On the host where AMS is installed, open the following file in a text editor:

Operating system	File path
Linux	`/opt/emc/scaleio/ams/webapps/ROOT/WEB-INF/classes/ams.properties`
Windows	`C:\Program Files\EMC\scaleio\AMS\webapps\ROOT\WEB-INF\classes\ams.properties`

2. Change the property `verifyEsxCertificates=True` to `verifyEsxCertificates=False`.
3. Save the `ams.properties` file.
4. Restart the VxFlex Ready Node AMS service:

Operating system	Action
Linux	Type the following command: `service scaleio-ams restart`
Windows	Restart the EMC ScaleIO AMS service.

iDRAC certificate replacement issue

During deployment and renew certificate flows, the certificate update action is not successful.

During deployment and renew certificate orchestration, AMS performs an AMS \ external certificate action on the VxFlex Ready Node iDRAC port. This action ensures that only authenticated communication occurs between AMS and the iDRAC port.

In 14G and 13G VxFlex Ready Nodes, a security bug was discovered, which prevents the certificate update action from occurring via WSMAN API (WSMAN is the API used by AMS). A workaround was added to AMS deployments and renew certificate flows:

- The iDRAC certificate is not replaced.
- The following flag is currently set to default true in the `ams.properties file`: "dontReplace14GiDracCerts=true" . This file can be found in the following location:
  - Linux: `/opt/emc/scaleio/ams/webapps/ROOT/WEB-INF/classes/ams.properties`
  - Windows: `C:\Program Files\EMC\scaleio\AMS\webapps\ROOT\WEB-INF\classes\ams.properties`

Once Dell EMC releases a firmware fix, the flag setting will be set to false by the upgrade action of AMS.