



Technical FAQ

NetApp Volume Encryption

ONTAP 9.1

Juan Mojica, Andrae Middleton, Dan Tulledge, NetApp
Version 1.3
July 2017

Abstract

NetApp® Volume Encryption (NVE) provides a software-based method to encrypt and protect data from theft if a disk is repurposed, sent in for return merchandise authorization, misplaced, or stolen. This document addresses common questions asked about NetApp Volume Encryption.

Information Classification

NetApp Confidential

Version History

Version	Date	Document Version History
Version 1.0	September 2016	Juan Mojica: initial commit
Version 1.1	January 2017	Andrae Middleton: updates
Version 1.2	June 2017	Dan Tulledge: updates
Version 1.3	June 2017	Dan Tulledge: formatting fix after review

TABLE OF CONTENTS

Version History	1
1 Overview	5
1.1 Solution Overview	5
1.2 Comparison with NetApp Storage Encryption	5
2 Requirements	6
Are there any platform requirements?	6
In addition to a platform, what else do I need to run NVE?	6
Is NVE a licensed feature?	6
What if I want to enable NVE on an existing system?	6
I understand that ONTAP 9.1 includes NVE, which has cryptographic functions. What if I'm selling to a customer in a country where export control policies prevent the export of strong cryptographic algorithms?	6
Which key managers are compatible or available with NVE?	6
What if I have an existing NSE system with an external KMIP key manager and want to use NVE as well?	6
Must all of my volumes be encrypted like NSE?	6
Can I use NSE drives as well as NVE?	6
Can I have NVE-capable and non-NVE-capable platforms in the same cluster and still use NVE?	6
3 Architecture	7
What is encrypted with NVE?	7
Are the NetApp storage efficiencies still maintained when using NVE?	7
What type of algorithms does NVE use for encrypting data?	7
Are Snapshot copies encrypted?	7
Are FlexClone volumes encrypted?	7
Are data volume encryption keys reused?	7
Can I assign a specific key to a data volume?	7
If I use NetApp SnapMirror to mirror my encrypted volume to a different cluster, is the same encryption key used at the destination?	7
Does NVE encrypt data in flight?	7
If I use SnapMirror to mirror my encrypted volume to a different cluster, is the data encrypted in flight or over the wire by NVE?	7
Are encryption keys replicated across clusters?	8
Where are data volume encryption keys stored?	8
Can my source volume be encrypted and my SnapMirror target be unencrypted or vice versa?	8
Is NVE FIPS 140-2 validated?	8
Does NVE provide a special mechanism or procedure to protect against or deal with data spills?	8
4 Configuration	9
How do I encrypt a new data volume?	9
Can I encrypt existing data volumes?	9
Can I encrypt an existing data volume in place (without a volume move)?	9

Can I instantaneously delete a volume encryption key without deleting the volume?.....	9
What do I do after the encrypted volume is created?	9
Can I unencrypt a data volume?	9
Can I rekey an existing volume or have the encryption key changed for an encrypted volume?.....	9
Do I have to encrypt all of my data volumes with NVE?	9
How do I confirm which volumes are encrypted?	9
Where can I download an NVE-capable image?	9
What happens when you install an ONTAP non-NVE-capable release (for example, the version for restricted countries) over an ONTAP release that is NVE-capable?.....	10
How can I switch to an NVE-capable version (for example, the version for restricted countries) from a non-NVE-capable version?.....	10
5 Performance.....	11
What is the performance impact of NVE?.....	11
Do certain platforms perform better with NVE?	11
Is there a performance difference between SSDs and HDDs while using NVE?.....	11
Is there an impact on nonencrypted volumes?	11
What if I want to enable NVE on an existing system? How do I know or gauge the impact?	11
Given that there are a limited number of CPU cores dedicated to the encryption function so that the nonencrypted volumes are not affected by encryption, what happens if the encryption cores are overloaded?	11
6 Interoperability.....	12
Can I use NVE with MetroCluster?	12
Can I use NVE with ONTAP Select?	12
Can I use NVE with NetApp FlexArray® software?	12
Can I use NVE with ONTAP Cloud?.....	12
Is NVE supported for NetApp Flash Cache cards?.....	12
Is data in NetApp Flash Pool intelligent caching encrypted by NVE?	12
Are certain features incompatible with NVE?.....	12
Is NVE supported with backup applications (for example, Commvault backup)?	12
Does NVE support data partitioning (for example, ADP/ADPv2 and so on)?	12
7 Upcoming Details	13
This NVE FAQ is marked NetApp Confidential. Do we have anything containing these details that I can share with my customers?	13
Who are the contacts for NVE-related questions?	13
Additional Resources	14
Contact Us	15

1 Overview

NetApp Volume Encryption (NVE) is a software-based, data-at-rest encryption solution available starting with NetApp ONTAP® 9.1 management software. NVE allows ONTAP to encrypt data and to have that data be stored on disk without requiring self-encrypting drives. NVE also allows customers to leverage storage efficiency features that would be lost if the customer decided to encrypt at the application layer. Customers can use any existing disk with NVE, which also includes NetApp Storage Encryption (NSE) drives for double or layered encryption. NVE is also the only option available for encrypting data in NetApp MetroCluster™ software and ONTAP Select.

1.1 Solution Overview

NVE is composed of a software cryptographic module, encryption keys, and a key manager.

1.1.1 Software Cryptographic Module

The software cryptographic module performs the data encryption operations and generates encryption keys for the volumes.



The cryptographic module performs the data encryption at the RAID layer, which is what allows the storage efficiencies to work. On a read operation, after the data leaves the RAID layer, it is unencrypted.

1.1.2 Encryption Keys

A unique XTS-AES-256 data encryption key is generated per volume. An encryption key hierarchy is used to encrypt and protect all volume keys. These encryption keys are never displayed, shown, or reported in an unencrypted format.

1.1.3 Key Manager

The encryption keys are stored within the key manager. The key manager keeps track of all the encryption keys used by ONTAP.

1.2 Comparison with NetApp Storage Encryption

NSE requires all drives in an HA pair to be purpose-built, self-encrypting drives. These drives perform the data encryption themselves through a hardware-accelerated mechanism. Because of the hardware acceleration, NSE systems, in most cases, outperform NVE systems when encrypting data.

NSE drives also are FIPS 140-2 level 2 validated, whereas NVE has not gone through the validation process yet. If FIPS 140-2 data-at-rest encryption is required, then NSE is the only solution available today for ONTAP.

2 Requirements

Are there any platform requirements?

Answer: Yes. NVE requires that the platform CPU provide an offload called AES-NI. The platforms that have the required offload are 6280, 6290, 8020, 8040, 8060, 8080, and all next-generation platforms introduced with ONTAP 9.1.

In addition to a platform, what else do I need to run NVE?

Answer: You need the ONTAP software image that can encrypt and the NVE software license. ONTAP images that are *not* capable of encrypting data are marked with a special extension.

Is NVE a licensed feature?

Answer: Yes, it is, for Global Trade Compliance purposes.

What if I want to enable NVE on an existing system?

Answer: You can add a license to existing systems through Salesforce.

I understand that ONTAP 9.1 includes NVE, which has cryptographic functions. What if I'm selling to a customer in a country where export control policies prevent the export of strong cryptographic algorithms?

Answer: ONTAP has two different builds: the normal build and a no data at rest (NODAR) encryption build. The NODAR builds are distinguishable by the word nodar in the version string of the "version -v" or "run local version" command.

Which key managers are compatible or available with NVE?

Answer: With ONTAP 9.1, only the Onboard Key Manager (OKM) is available for NetApp Volume Encryption. No other key manager is supported.

What if I have an existing NSE system with an external KMIP key manager and want to use NVE as well?

Answer: The external key manager has to be unconfigured, and the OKM has to be configured. OKM can be used for both the NSE drives and NVE.

Must all of my volumes be encrypted like NSE?

Answer: No. With NVE, you can choose which volumes are encrypted and which are not.

Can I use NSE drives as well as NVE?

Answer: Yes. NVE provides the ability to add another layer of encryption on top of what the NSE drives already provide.

Can I have NVE-capable and non-NVE-capable platforms in the same cluster and still use NVE?

Answer: Yes. You can have mixed platforms per the standard ONTAP platform mixing rules. Both platforms in the HA pair must be NVE-capable. The non-NVE-capable platforms in the cluster are not able to host encrypted volumes.

3 Architecture

What is encrypted with NVE?

Answer: Data volumes, specifically NetApp FlexVol® volumes, are encrypted. Controller root volumes and SVM root volumes are not encrypted. Anything that is part of the data volume is encrypted, including Snapshot® copies and clones.

Are the NetApp storage efficiencies still maintained when using NVE?

Answer: Yes. As depicted in the solution overview (section 1.1), the cryptographic module performs the data encryption at the RAID layer, which allows the storage efficiencies to stay in place because they are performed prior to the encryption functions.

What type of algorithms does NVE use for encrypting data?

Answer: NVE data-at-rest encryption uses XTS-AES-256. The keys required for XTS-AES-256 are generated using a NIST SP800-90A DRBG in CTR_DRBG mode with predictive resistance and health checks always on.

Are Snapshot copies encrypted?

Answer: Yes.

Are FlexClone volumes encrypted?

Yes. NetApp FlexClone® volumes are encrypted with the same key as the original volume.

Can FlexClone volumes be encrypted with a different encryption key than the original volume?

Answer: Yes. The FlexClone volume must first be split from the original volume. A warning message is issued telling the user to perform a volume move to give the split clone a new encryption key. After the user performs the volume move, the split clone has a new encryption key.

Are data volume encryption keys reused?

Answer: No. Each data volume key is unique to that volume.

Can I assign a specific key to a data volume?

Answer: No. Encryption keys are automatically generated when the volume is created.

If I use NetApp SnapMirror to mirror my encrypted volume to a different cluster, is the same encryption key used at the destination?

Answer: No. The destination volume is its own volume and has its own unique key.

Does NVE encrypt data in flight?

Answer: No. NVE is specifically for data that is stored on disk.

If I use SnapMirror to mirror my encrypted volume to a different cluster, is the data encrypted in flight or over the wire by NVE?

Answer: No. SnapMirror® sits above the NetApp WAFL® (Write Anywhere File Layout) layer, and thus the data sent by SnapMirror is not encrypted by NVE. For more information, see the solution overview in section 1.1.

Are encryption keys replicated across clusters?

Answer: No. Encryption keys apply only to a single cluster.

Where are data volume encryption keys stored?

Answer: Data volume encryption keys are stored in the WAFL metadata, which is not accessible by the user, and the volume location database (VLDB).

Can my source volume be encrypted and my SnapMirror target be unencrypted or vice versa?

Answer: Yes. The source volume and destination volume can have different settings with respect to encryption.

Is NVE FIPS 140-2 validated?

Answer: No. However, the algorithms have been put in place so that the NVE or, more precisely, the cryptographic module can be FIPS 140-2 level 1 validated. The validation process has begun and can be viewed at the NIST website in the Implementation Under Test list at <http://csrc.nist.gov/groups/STM/cmvp/inprocess.html>.

Does NVE provide a special mechanism or procedure to protect against or deal with data spills?

Answer: No. Because of wear-leveling in SSDs and the requirement to use the OKM, NVE cannot guarantee that a volume key is no longer on the disk. This problem is not unique to NetApp; any vendor using SSDs with a local or an OKM has this same problem.

4 Configuration

How do I encrypt a new data volume?

Answer: For more information, see the NetApp Volume Encryption Power Guide.

Can I encrypt existing data volumes?

Answer: Yes. You can do so by performing a volume move. For more information, see the NetApp Volume Encryption Power Guide.

Can I encrypt an existing data volume in place (without a volume move)?

Answer: No. It is not possible to encrypt in place. A volume move is required.

Can I instantaneously delete a volume encryption key without deleting the volume?

Answer: The volume encryption key is deleted with the volume until the volume's retention period expires. The retention period is a standard ONTAP volume feature. Until the retention period expires, the data remains encrypted on disk.

What do I do after the encrypted volume is created?

Answer: Nothing. ONTAP makes sure that the data with that volume is encrypted.

Can I unencrypt a data volume?

Answer: Yes. For more information, see the NetApp Volume Encryption Power Guide.

Can I rekey an existing volume or have the encryption key changed for an encrypted volume?

Answer: Yes. For more information, see the NetApp Volume Encryption Power Guide.

Do I have to encrypt all of my data volumes with NVE?

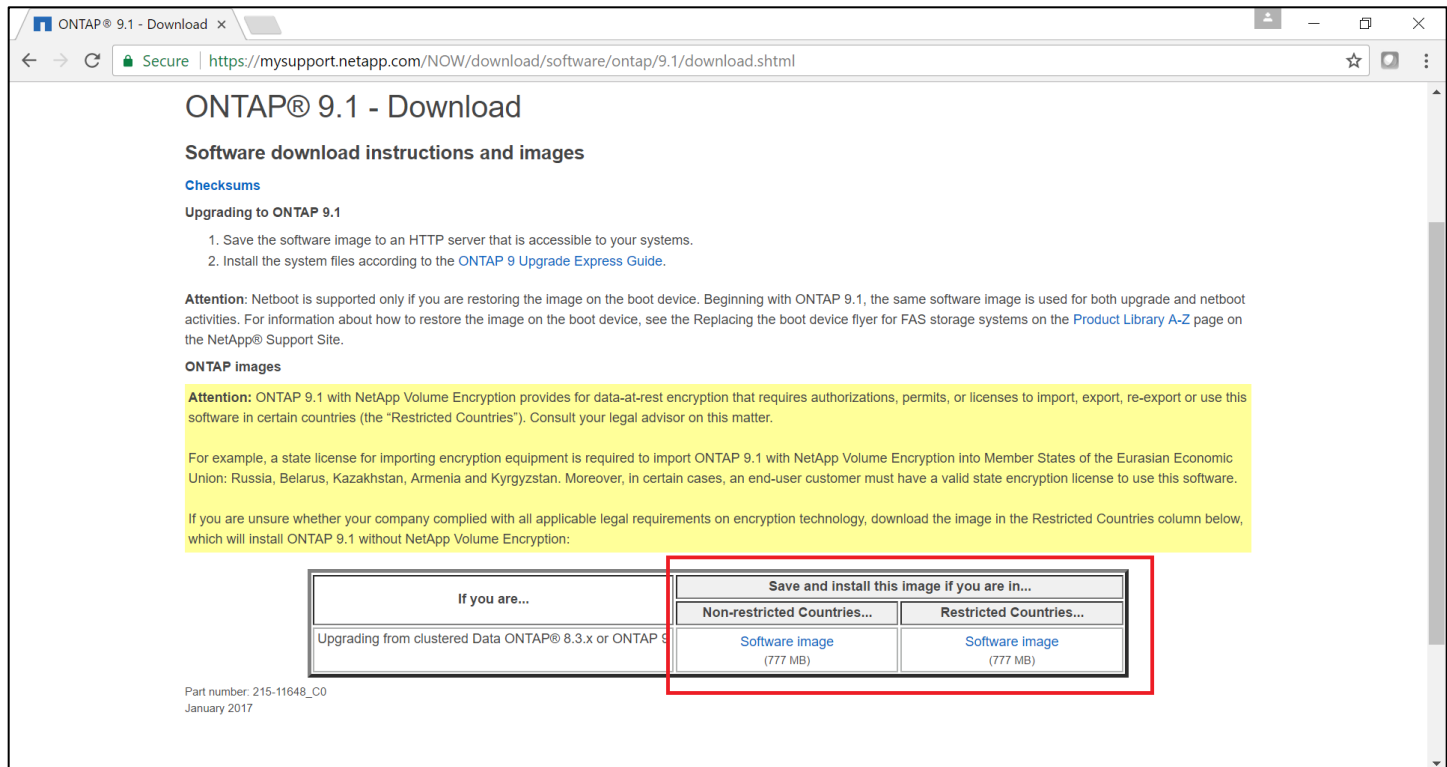
Answer: No. NVE lets you choose which data volumes are encrypted.

How do I confirm which volumes are encrypted?

Answer: The volume show command with the '-is-encrypted true' option displays a list of the currently encrypted volumes.

Where can I download an NVE-capable image?

Answer: You can download an ONTAP image release 9.1 or higher from the NetApp Support site. For example, go to <https://mysupport.netapp.com/NOW/download/software/ontap/9.1/download.shtml> for **ONTAP 9.1**.



What happens when you install an ONTAP non-NVE-capable release (for example, the version for restricted countries) over an ONTAP release that is NVE-capable?

Answer: The ONTAP install should fail if there are NVE volumes.

How can I switch to an NVE-capable version (for example, the version for restricted countries) from a non-NVE-capable version?

Answer: There are two ways to accomplish this without going through a full upgrade process:

- Use "cluster image package delete [-version] <text>" and then use "cluster image package get [-url] <text>"
- Use "system node image update [-package] <url text> [-replace-package [true]]"

5 Performance

What is the performance impact of NVE?

Answer: It depends on the customer workload, the number of active encrypted data volumes, the platform, and the disk type being used.

Do certain platforms perform better with NVE?

Answer: Yes. Platforms with higher core counts perform better with NVE. In certain situations, on the higher end, the performance impact of NVE is negligible or unobservable. For example, a FAS8080 is less affected than a FAS8040 for the same workload and the same number of active encrypted data volumes.

Is there a performance difference between SSDs and HDDs while using NVE?

Answer: Volumes residing in SSDs are typically placed there because of the desire for extremely low latencies. NVE extends the path length for each piece of data to where it can be noticed in some workloads and operating conditions. The number of IOPS at a given latency can be less with NVE when running on an All Flash FAS system, for example. For volumes residing in HDDs, the bottleneck in that system is the disk, and very little to no impact should be seen with NVE.

Is there an impact on nonencrypted volumes?

Answer: The impact of NVE comes from extending the processing for the encrypted volumes. Unencrypted volumes should remain unaffected while operating during normal conditions.

What if I want to enable NVE on an existing system? How do I know or gauge the impact?

Answer: Leverage the headroom capability on the system as is (no encryption) to see where the existing performance is. After that is noted, add an NVE volume (or convert an existing volume) and use the headroom capability once more to see what changed. Remember that NVE is per volume; therefore, you can encrypt or create one at a time based on the headroom and impact.

Given that there are a limited number of CPU cores dedicated to the encryption function so that the nonencrypted volumes are not affected by encryption, what happens if the encryption cores are overloaded?

Answer: NVE takes advantage of AES-NI in the Intel chipsets for encryption acceleration to thwart this behavior. In the event that the offload is indeed saturated, the impact would be seen in IOPS.

6 Interoperability

Can I use NVE with MetroCluster?

Answer: Yes. NVE is the only generally available data-at-rest encryption option for MetroCluster.

Can I use NVE with ONTAP Select?

Answer: Yes. NVE is the only generally available data-at-rest encryption option for ONTAP Select.

Can I use NVE with NetApp FlexArray® software?

Answer: Yes. As long as the controller supports NVE, you can use NVE.

Can I use NVE with ONTAP Cloud?

Answer: No. Currently ONTAP Cloud is not supported.

Is NVE supported for NetApp Flash Cache cards?

Answer: Data on the Flash Cache™ cards is encrypted by the same cryptographic module used by NVE.

Is data in NetApp Flash Pool intelligent caching encrypted by NVE?

Answer: Yes. Data in Flash Pool™ caches is encrypted by NVE.

Are certain features incompatible with NVE?

Answer: Yes. The following features are not compatible with NVE:

- NetApp SnapLock® software
- NetApp FlexGroup volumes
- External (KMIP) key managers

Is NVE supported with backup applications (for example, Commvault backup)?

Answer: Yes. NVE is independent of the backup targets/solutions. The data presented to the backup solutions is not encrypted.

Does NVE support data partitioning (for example, ADP/ADPv2 and so on)?

Answer: Yes. NVE is independent of the data partitioning process because the volumes are established after the partitioning process is performed.

7 Upcoming Details

This NVE FAQ is marked NetApp Confidential. Do we have anything containing these details that I can share with my customers?

Answer: Not today. An NVE datasheet is already in the works.

Who are the contacts for NVE-related questions?

Answer: For NVE-related questions, contact the ng-encryption mailer. This mailer is monitored by the PM and TME groups.

Additional Resources

The following references were used in this FAQ:

- Clustered Data ONTAP Storage Platform Mixing Rules
<https://fieldportal.netapp.com/content/197582?assetComponentId=197680>
- NetApp Volume Encryption Power Guide
library.netapp.com

Other useful technical reports and training presentations about NVE:

- NetApp Volume Encryption Performance Considerations
<https://fieldportal.netapp.com/content/476393?assetComponentId=477084>
- NetApp Volume Encryption Sales Training
<https://fieldportal.netapp.com/content/470722?assetComponentId=471399>
- NetApp Volume Encryption SE Training
<https://fieldportal.netapp.com/content/470762?assetComponentId=471439>

Contact Us

Do you have a question that you think we should include in this FAQ?

Ask us at docfeedback@netapp.com.

Include NETAPP VOLUME ENCRYPTION TECHNICAL FAQ in the subject line.

Refer to the [Interoperability Matrix Tool \(IMT\)](#) on the NetApp Support site to validate that the exact product and feature versions described in this document are supported for your specific environment. The NetApp IMT defines the product components and versions that can be used to construct configurations that are supported by NetApp. Specific results depend on each customer's installation in accordance with published specifications.

Copyright Information

Copyright © 2016–2017 NetApp, Inc. All rights reserved. Printed in the U.S. No part of this document covered by copyright may be reproduced in any form or by any means—graphic, electronic, or mechanical, including photocopying, recording, taping, or storage in an electronic retrieval system—without prior written permission of the copyright owner.

Software derived from copyrighted NetApp material is subject to the following license and disclaimer:

THIS SOFTWARE IS PROVIDED BY NETAPP “AS IS” AND WITHOUT ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE, WHICH ARE HEREBY DISCLAIMED. IN NO EVENT SHALL NETAPP BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

NetApp reserves the right to change any products described herein at any time, and without notice. NetApp assumes no responsibility or liability arising from the use of products described herein, except as expressly agreed to in writing by NetApp. The use or purchase of this product does not convey a license under any patent rights, trademark rights, or any other intellectual property rights of NetApp.

The product described in this manual may be protected by one or more U.S. patents, foreign patents, or pending applications.

RESTRICTED RIGHTS LEGEND: Use, duplication, or disclosure by the government is subject to restrictions as set forth in subparagraph (c)(1)(ii) of the Rights in Technical Data and Computer Software clause at DFARS 252.277-7103 (October 1988) and FAR 52-227-19 (June 1987).

Trademark Information

NETAPP, the NETAPP logo, and the marks listed at <http://www.netapp.com/TM> are trademarks of NetApp, Inc. Other company and product names may be trademarks of their respective owners.