FIPS 140-2 Security-konforme FlexPod Lösung für das Gesundheitswesen

FlexPod

NetApp
March 25, 2024

This PDF was generated from https://docs.netapp.com/de-de/flexpod/security/flexpod-fips-introduction.html on March 25, 2024. Always check docs.netapp.com for the latest.

Inhalt

FIPS 140-2 Security-konforme FlexPod Lösung für das Gesundheitswesen . . . 1
TR-4892: FIPS 140-2 Security-konforme FlexPod Lösung für das Gesundheitswesen . . . 1
Cyber-Sicherheitsbedrohungen im Gesundheitswesen . . . 2
Überblick über FIPS 140-2 . . . 4
Kontrollebene oder Datenebene . . . 5
FlexPod Cisco UCS Computing und FIPS 140-2 . . . 6
FlexPod Cisco Networking und FIPS 140-2 . . . 7
FlexPod NetApp ONTAP Storage und FIPS 140-2 . . . 12
Lösungsvorteile der konvergenten FlexPod Infrastruktur . . . 18
Weitere Sicherheitsaspekte bei FlexPod . . . 21
Schlussfolgerung . . . 22
Danksagungen, Versionsverlauf und weitere Informationen finden . . . 23

FIPS 140-2 Security-konforme FlexPod Lösung für das Gesundheitswesen

TR-4892: FIPS 140-2 Security-konforme FlexPod Lösung für das Gesundheitswesen

JayaKishore Esanakula, NetApp John McAbel, Cisco

Das Health Information Technology for Economic and Clinical Health Act (HITECH) erfordert die Federal Information Processing Standard (FIPS) 140-2-validierte Verschlüsselung elektronischer geschützter Gesundheitsdaten (ePHI). Anwendungen und Software FÜR den Bereich Health Information Technology (HITS) müssen mit FIPS 140-2 konform sein, um die Zertifizierung zum Promoting Interoperability Program (ehemals sinnvoller Einsatz des Incentive-Programms) zu erhalten. Teilnahmeberechtigte Anbieter und Krankenhäuser müssen einen FIPS 140-2 (Level 1)-konformen TREFFER für die Aufnahme von Incentives für Medicare und Medicaid sowie die Vermeidung von Kostenerstattungen durch das Center for Medicare and Medicaid (CMS) verwenden. Nach FIPS 140-2 zertifizierte Verschlüsselungsalgorithmen gelten als technische Sicherheitsmaßnahmen, die gemäß der erforderlich sind "Sicherheitsregel" Des Health Information Portability and Accountability Act (HIPAA).

FIPS 140-2 ist eine USA Dieser Standard erfüllt die Sicherheitsanforderungen für kryptografische Module in Hardware, Software und Firmware, die sensible Daten schützen. Die Einhaltung der Standards ist für die Verwendung durch die USA vorgeschrieben Regierungsbehörden und IT wird häufig auch in regulierten Branchen wie Finanzdienstleistungen und Gesundheitswesen eingesetzt. Dieser technische Bericht hilft dem Leser, den FIPS 140-2-Sicherheitsstandard auf hohem Niveau zu verstehen. Außerdem hilft es dem Publikum, verschiedene Bedrohungen zu verstehen, denen Organisationen im Gesundheitswesen gegenüberstehen. Außerdem hilft der technische Bericht einem zu verstehen, wie ein FIPS 140-2-konformes FlexPod System zum Schutz von Gesundheitsressourcen bei der Implementierung auf einer konvergenten FlexPod Infrastruktur beitragen kann.

Umfang

Dieses Dokument bietet eine technische Übersicht zu einem Cisco Unified Computing System (Cisco UCS), Cisco Nexus, Cisco MDS und einer auf NetApp ONTAP basierenden FlexPod Infrastruktur zum Hosten von IT-Applikationen oder Lösungen im Gesundheitswesen, die FIPS 140-2 Sicherheit erfordern.

Zielgruppe

Dieses Dokument richtet sich an technische Leiter im Gesundheitswesen sowie an Lösungstechniker von Cisco und NetApp Partnern und Professional Services-Mitarbeiter. NetApp geht davon aus, dass der Leser gute Kenntnisse der Konzepte zur Berechnung der Storage- und Computing-Größenbemessung sowie der technischen Vertrautheit mit Bedrohungen für das Gesundheitswesen, mit der Sicherheit im Gesundheitswesen, MIT IT-Systemen im Gesundheitswesen, mit Cisco UCS und NetApp Storage-Systemen hat.

"Die nächste: Cyber-Sicherheitsbedrohungen im Gesundheitswesen."

Cyber-Sicherheitsbedrohungen im Gesundheitswesen

"Zurück: Einführung."

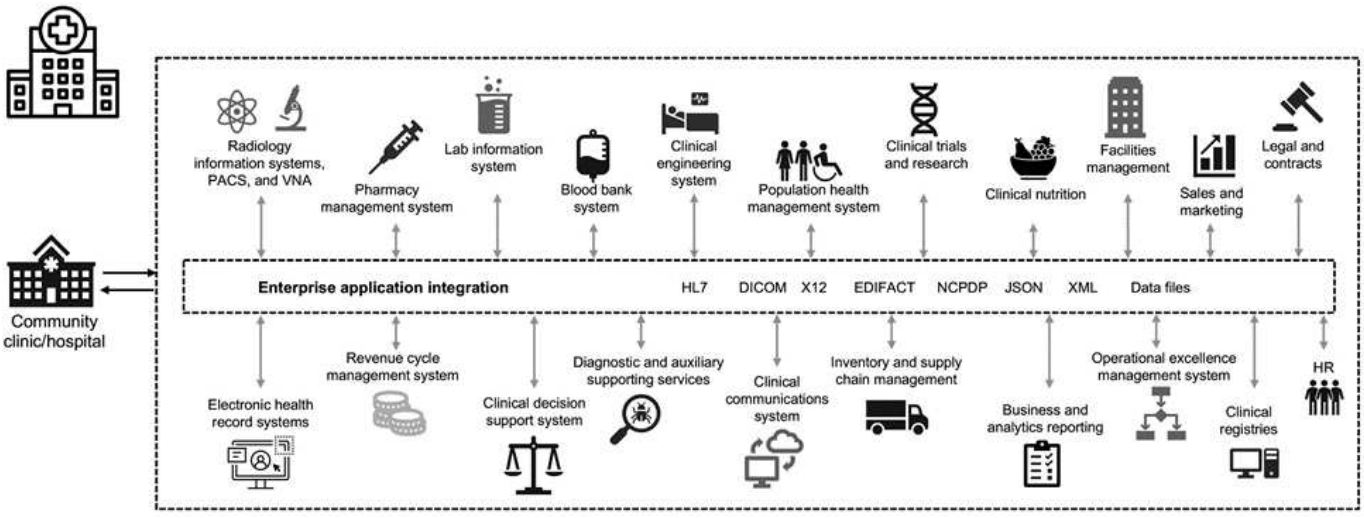
Jedes Problem stellt eine neue Chance dar – ein Beispiel für eine solche Chance wird von der COVID-Pandemie präsentiert. Laut A "Bericht" Durch das Department of Health and Human Services (HHS) Cybersecurity Program hat die COVID-Antwort zu einer erhöhten Anzahl von Ransomware-Angriffen geführt. In der dritten Märzwoche 2020 wurden 6,000 neue Internet-Domains registriert. Mehr als 50 % der Domänen haben Malware gehostet. Ransomware-Angriffe verliefen 2020 fast 50 % aller Datenschutzverstöße im Gesundheitswesen mit Auswirkungen auf mehr als 630 Organisationen im Gesundheitswesen und rund 29 Millionen Datensätze im Gesundheitswesen. 19 Leaker/Sites verdoppelten die Erpressung. Mit 24.5 % Sicherheitsverletzungen hat sich die Branche im Jahr 2020 die höchste Anzahl von Datenverletzungen festgestellt.

Böswillige Mitarbeiter versuchten, die Sicherheit und den Datenschutz von geschützten Gesundheitsdaten (PHI) zu verletzen, indem sie die Informationen verkaufen oder sie bedrohen, sie zu zerstören oder auszusetzen. Es werden häufig gezielte und Massenübertragungsversuche unternommen, um sich unbefugten Zugriff auf ePHI zu verschaffen. Rund 75 % der exponierten Patientenakten im zweiten Halbjahr 2020 waren auf kompromittierte Geschäftspartner zurückzuführen.

Die folgende Liste der Gesundheitseinrichtungen wurde von den böswilligen Agenten ins Visier gesetzt:

- Krankenhaussysteme
- Life-Science-Labore
- Forschungslabors
- Rehabilitationseinrichtungen
- Kommune Krankenhäuser und Kliniken

Die Vielfalt der Applikationen, die ein Gesundheitswesen ausmachen, ist unbestreitbar und wird zunehmend komplexer. Büros für Informationssicherheit stehen vor der Herausforderung, eine Governance für eine Vielzahl VON IT-Systemen und -Assets zu gewährleisten. Die folgende Abbildung zeigt die klinischen Möglichkeiten eines typischen Krankenhaussystems.



Patientendaten bilden das Herzstück dieses Bildes. Der Verlust von Patientendaten und das Stigma, das mit sensiblen Erkrankungen verbunden ist, sind sehr real. Weitere sensible Themen sind das Risiko sozialer Ausgrenzung, Erpressung, Profiling, die Anfälligkeit für zielgerichtetes Marketing, Ausbeutung und die mögliche finanzielle Haftung gegenüber Kostenträgern über medizinische Informationen jenseits der Privilegien des Zahlers.

Bedrohungen für die Gesundheit sind multidimensional in der Natur und in der Wirkung. Regierungen weltweit haben verschiedene Bestimmungen zur Sicherung von ePHI erlassen. Die schädlichen Auswirkungen und die sich immer weiter entwickelnden Bedrohungen für das Gesundheitswesen erschweren es Organisationen im Gesundheitswesen, alle Bedrohungen zu schützen.

Im Folgenden finden Sie eine Liste der häufigsten Bedrohungen, die im Gesundheitswesen identifiziert werden:

- Ransomware-Angriffe
- Verlust oder Diebstahl von Geräten oder Daten mit vertraulichen Informationen
- Phishing-Angriffe
- Angriffe auf angeschlossene medizinische Geräte, die die Patientensicherheit beeinträchtigen können
- E-Mail-Phishing-Angriffe
- Verlust oder Diebstahl von Geräten oder Daten
- Protokollkompromiss für Remote Desktops
- Softwareschwachstelle

Einrichtungen im Gesundheitswesen arbeiten in juristischen und gesetzlichen Regelungen, die so kompliziert sind wie ihre digitalen Ökosysteme. Zu dieser Umgebung gehören u. a. die folgenden:

- Office des National Coordinators (for Healthcare Technology) ONC-zertifizierte Standards für Interoperabilität in der elektronischen Gesundheitsinformationstechnologie
- Medicare Access und das Kinderversicherungsprogramm ReacreAuthorization Act (MACRA)/sinnvolle Nutzung
- Mehrfachverpflichtungen nach der Food and Drug Administration (FDA)
- Die Gemeinsame Akkreditierungsverfahren der Kommission
- HIPAA-Anforderungen erfüllt
- Anforderungen von HITECH
- Mindeststandards für akzeptable Risiken für Kostenträger
- Datenschutzregeln und Sicherheitsregeln
- Anforderungen des Bundesgesetzes zur Modernisierung der Informationssicherheit, die in Bundesverträge und Forschungszuschüsse von Behörden wie den nationalen Gesundheitseinrichtungen aufgenommen werden
- Payment Card Industry Data Security Standard (PCI-DSS)
- Substanzmissbrauch und Mental Health Services Administration (SAMHSA) Anforderungen
- Der Gramm-Leach-Bliley Act für die Finanzverarbeitung
- Das Stark-Gesetz bezieht sich auf die Erbringung von Dienstleistungen an verbundene Organisationen
- Family Educational Rights and Privacy Act (FERPA) für Institutionen, die an der Hochschulbildung teilnehmen

- Genetic Information Nondiscrimination Act (GINA)
- Die neue Datenschutz-Grundverordnung (DSGVO) in der Europäischen Union

Die Standards der Sicherheitsarchitektur entwickeln sich rasant weiter, um zu verhindern, dass böswillige Akteure ein System der Gesundheitsinformationen beeinträchtigen. Einer dieser Standards ist FIPS 140-2, definiert durch das National Institute of Standards and Technology (NIST). Die FIPS-Veröffentlichung 140-2 enthält Angaben zu den USA Behördliche Anforderungen für ein kryptografisches Modul. Die Sicherheitsanforderungen decken Bereiche ab, die sich auf eine sichere Konstruktion und Implementierung eines kryptografischen Moduls beziehen und können auf EINEN TREFFER angewendet werden. Klar definierte kryptografische Grenzen sorgen für ein einfacheres Sicherheitsmanagement und bleiben mit den kryptografischen Modulen auf dem aktuellen Stand. Diese Grenzen verhindern schwache Crypto-Module, die problemlos von böswilligen Akteuren genutzt werden können. Sie können auch menschliche Fehler beim Management von Standard-kryptografischen Modulen verhindern.

NIST hat zusammen mit dem Communications Security Establishment (CSE) das Cryptographic Module Validation Program (CMVP) eingerichtet, um kryptografische Module für FIPS 140-2 Validierungsstufen zu zertifizieren. Mithilfe eines FIPS 140-2-2-zertifizierten Moduls sind Bundesbehörden zum Schutz sensibler oder wertvoller Daten während der Übertragung und im Ruhezustand verpflichtet. Aufgrund des Erfolgs beim Schutz sensibler oder wertvoller Informationen haben sich viele Gesundheitssysteme für die Verschlüsselung von ePHI entschieden, indem FIPS 140-2-2-kryptografische Module verwendet werden, die über das gesetzlich geforderte Mindestsicherheitsniveau hinausgehen.

Die Nutzung und Implementierung der FlexPod FIPS 140-2 Funktionen dauert nur Stunden (nicht Tage). Die FIPS-Compliance-Konformität ist für die meisten Unternehmen im Gesundheitswesen verfügbar, unabhängig von der Größe. Mit klar definierten kryptografischen Grenzen und gut dokumentierten und einfachen Implementierungsschritten legt eine FIPS 140-2-2-konforme FlexPod-Architektur solide Sicherheitsgrundlage für die Infrastruktur fest und ermöglicht einfache Verbesserungen zur weiteren Erhöhung des Schutzes von Sicherheitsbedrohungen.

"Weiter: Überblick über FIPS 140-2."

Überblick über FIPS 140-2

"Früher: Cybersicherheitsbedrohungen im Gesundheitswesen."

"FIPS 140-2" Gibt die Sicherheitsanforderungen für ein kryptografisches Modul an, das in einem Sicherheitssystem verwendet wird, das vertrauliche Informationen in Computer- und Telekommunikationssystemen schützt. Ein kryptografisches Modul sollte aus Hardware, Software, Firmware oder einer Kombination verschiedener Komponenten besteht. FIPS gilt für die kryptografischen Algorithmen, die Schlüsselgenerierung und den Schlüsselmanager, die sich innerhalb einer kryptografischen Grenze befinden. Es ist wichtig zu wissen, dass sich FIPS 140-2 speziell auf das kryptografische Modul bezieht, nicht auf das Produkt, die Architektur, die Daten oder das Ecosystem. Das kryptografische Modul, das in den Schlüsselbegriffen später in diesem Dokument definiert wird, ist die spezifische Komponente (ob Hardware, Software und/oder Firmware), die zugelassene Sicherheitsfunktionen implementiert. Zudem gibt FIPS 140-2 vier Level an. Genehmigte kryptografische Algorithmen sind auf allen Ebenen gemeinsam. Zu den wichtigsten Elementen und Anforderungen der einzelnen Sicherheitsstufen gehören:

- **Sicherheitsstufe 1**

- Legt grundlegende Sicherheitsanforderungen für ein kryptografisches Modul fest (mindestens ein genehmigter Algorithmus oder eine Sicherheitsfunktion ist erforderlich).
- Für Stufe 1 über die grundlegenden Anforderungen für produktionsbereite Komponenten hinaus sind keine festgelegten physischen Sicherheitsmechanismen erforderlich.

- **Sicherheitsstufe 2**
  - Erweitert die physikalischen Sicherheitsmechanismen durch Hinzufügen der Notwendigkeit für Manipulationsbeweise durch die Verwendung von manipulationssicheren Lösungen wie Beschichtungen oder Dichtungen, Verriegelungen an abnehmbaren Abdeckungen oder Türen der kryptografischen Module.
  - Erfordert mindestens die rollenbasierte Zugriffssteuerung (Role-Based Access Control, RBAC), bei der das kryptografische Modul die Autorisierung eines Bedieners oder Administrators authentifiziert, eine bestimmte Rolle anzunehmen und entsprechende Funktionen auszuführen.
- **Sicherheitsstufe 3**
  - Baut auf den manipulationssicheren Anforderungen der Stufe 2 auf und versucht, einen weiteren Zugriff auf kritische Sicherheitsparameter (CSPs) innerhalb des kryptografischen Moduls zu verhindern.
  - Physische Sicherheitsmechanismen, die auf Ebene 3 erforderlich sind, sollen eine hohe Wahrscheinlichkeit haben, Versuche auf physischen Zugriff zu erkennen und darauf zu reagieren, oder jede Verwendung oder Änderung des kryptografischen Moduls. Beispiele dafür sind starke Gehäuse, Sabotagedetektion und Reaktionsschaltungen, die alle Klartext-CSPs aufzählen, wenn eine abnehmbare Abdeckung auf dem kryptografischen Modul geöffnet wird.
  - Erfordert identitätsbasierte Authentifizierungsmechanismen zur Verbesserung der Sicherheit der in Level 2 angegebenen RBAC-Mechanismen. Ein kryptografisches Modul authentifiziert die Identität eines Operators und stellt sicher, dass der Operator berechtigt ist, eine Rolle zu verwenden und die Funktionen der Rolle auszuführen.
- **Sicherheitsstufe 4**
  - Höchster Sicherheitsgrad in FIPS 140-2.
  - Die nützlichste Stufe für Vorgänge in physisch ungeschützten Umgebungen
  - Auf dieser Ebene sollen die physischen Sicherheitsmechanismen einen vollständigen Schutz um das kryptografische Modul gewährleisten, der dafür verantwortlich ist, unbefugte physische Zugriffsversuche zu erkennen und darauf zu reagieren.
  - Das Eindringen oder Eindringen des kryptografischen Moduls sollte eine hohe Erkennungswahrscheinlichkeit haben und zur sofortigen Zeroisierung aller unsicheren oder plaintext CSPs führen.

"Nächster: Kontrollebene oder Datenebene."

Kontrollebene oder Datenebene

"Zurück: Übersicht von FIPS 140-2."

Bei der Implementierung einer FIPS 140-2-2-Strategie ist es wichtig zu verstehen, welche Daten geschützt werden. Diese kann leicht in zwei Bereiche unterteilt werden: Kontrollebene und Datenebene. Eine Kontrollebene bezieht sich auf die Aspekte, die Einfluss auf die Kontrolle und den Betrieb der Komponenten im FlexPod System haben, z. B. Administratorzugriff auf die NetApp Storage Controller, Cisco Nexus Switches und

Cisco UCS Server. Der Schutz auf dieser Ebene wird durch die Einschränkung der Protokolle und kryptografischen Cypher ermöglicht, mit denen Administratoren Geräte verbinden und Änderungen vornehmen können. In einer Datenebene werden die tatsächlichen Informationen, wie zum Beispiel PHI, innerhalb des FlexPod-Systems bezeichnet. Diese wird durch Verschlüsselung von Daten im Ruhezustand und bei FIPS geschützt, sodass die verwendeten kryptografischen Module die Standards erfüllen.

"Als Nächstes: FlexPod Cisco UCS Computing und FIPS 140"

FlexPod Cisco UCS Computing und FIPS 140-2

"Zurück: Kontrollebene vs. Datenebene."

Eine FlexPod Architektur kann mit einem Cisco UCS Server konzipiert werden, der FIPS 140-2 konform ist. Gemäß der U. S. NIST, Cisco UCS Server können im Compliance-Modus nach FIPS 140-2 Level 1 betrieben werden. Eine vollständige Liste FIPS-konformer Cisco Komponenten finden Sie unter "Cisco FIPS 140 Seite". Cisco UCS Manager ist nach FIPS 140-2 zertifiziert.

Cisco UCS und Fabric Interconnect

Der Cisco UCS Manager ist implementiert und läuft über die Cisco Fabric Interconnects (FIS).

Weitere Informationen zum Cisco UCS und zur Aktivierung von FIPS finden Sie im "Dokumentation zu Cisco UCS Manager".

Um den FIPS-Modus auf dem Cisco Fabric Interconnect auf jedem Fabric A und B zu aktivieren, führen Sie die folgenden Befehle aus:

```
fp-health-fabric-A# connect local-mgmt
fp-health-fabric-A(local-mgmt)# enable fips-mode
FIPS mode is enabled
```

Um eine FI in einem Cluster auf Cisco UCS Manager Release 3.2(3) durch EINE FI-FUNKTION auf einer älteren Version als Cisco UCS Manager Release 3.2(3) zu ersetzen, deaktivieren Sie den FIPS-Modus (deaktivieren `fips-mode`) Auf dem vorhandenen FI vor dem Hinzufügen der Ersatz-FI zum Cluster. Nach der Bildung des Clusters wird der FIPS-Modus als Teil des Starts des Cisco UCS Managers automatisch aktiviert.

Cisco bietet die folgenden wichtigen Produkte, die auf Computing- oder Applikationsebene implementiert werden können:

- **Cisco Advanced Malware Protection (AMP) für Endpunkte.** unterstützt auf Microsoft Windows- und Linux-Betriebssystemen bietet diese Lösung Funktionen für Prävention, Erkennung und Reaktion. Diese Sicherheitssoftware verhindert Verstöße, blockiert Malware am Einstiegspunkt und überwacht und analysiert kontinuierlich die Datei- und Prozessaktivitäten, um Bedrohungen schnell zu erkennen, einzudämmen und zu beseitigen, die den Schutz vor der Front-Line-Lösung ausweichen können. Die Komponente „bösartiger Aktivitätsschutz“ (MAP) von AMP überwacht kontinuierlich alle Endpoint-Aktivitäten und ermöglicht die Laufzeiterkennung und das Blockieren des anormalen Verhaltens eines

laufenden Programms auf dem Endpunkt. Wenn beispielsweise das Endpunktverhalten auf Ransomware hinweist, werden die abgebrochene Prozesse beendet, um Endpunktverschlüsselung zu verhindern und den Angriff zu stoppen.

- **AMP für E-Mail-Sicherheit.** E-Mails sind das Hauptfahrzeug, um Malware zu verbreiten und Cyberangriffe auszuführen. Im Durchschnitt werden an einem einzigen Tag rund 100 Milliarden E-Mails ausgetauscht, die Angreifern einen ausgezeichneten Penetrationsvektor in die Systeme des Benutzers bieten. Daher ist es absolut unerlässlich, sich gegen diese Angriffslinie zu verteidigen. AMP analysiert E-Mails auf Bedrohungen wie Zero-Day-Exploits und entstickende Malware, die in bösartigen Anhängen verborgen sind. Darüber hinaus nutzt es branchenführende URL-Informationen, um schädliche Links zu bekämpfen. Anwender erhalten erweiterten Schutz vor Spear-Phishing, Ransomware und anderen anspruchsvollen Angriffen.
- **Next-Generation Intrusion Prevention System (NGIPS).** Cisco Firepower NGIPS kann als physische Appliance im Datacenter oder als virtuelle Appliance auf VMware (NGIPSv für VMware) eingesetzt werden. Dieses hocheffiziente Abwehrsystem für Angriffe sorgt für zuverlässige Leistung und niedrige Gesamtbetriebskosten. Der Schutz vor Bedrohungen kann durch optionale Abonnementlizenzen erweitert werden, um AMP, Transparenz und Kontrolle von Anwendungen sowie URL-Filterfunktionen bereitzustellen. Das virtualisierte NGIPS überprüft den Datenverkehr zwischen Virtual Machines (VMs) und vereinfacht die Bereitstellung und das Management von NGIPS-Lösungen an Standorten mit begrenzten Ressourcen. Dadurch wird der Schutz sowohl für physische als auch für virtuelle Ressourcen erhöht.

"Als Nächstes: Cisco Networking mit FlexPod und FIPS 140-2"

FlexPod Cisco Networking und FIPS 140-2

"Früher: FlexPod Cisco UCS Computing und FIPS 140-2."

Cisco MDS

Plattform der Cisco MDS 9000 Serie mit Software 8.4.x ist "FIPS 140-2 konform". Cisco MDS implementiert kryptografische Module und folgende Services für SNMPv3 und SSH.

- Sitzungseinrichtung unterstützt jeden Service
- Alle zugrunde liegenden kryptografischen Algorithmen, die die wichtigsten Ableitfunktionen der Dienste unterstützen
- Hashing für jeden Service
- Symmetrische Verschlüsselung für jeden Service

Führen Sie vor Aktivierung des FIPS-Modus die folgenden Aufgaben auf dem MDS-Switch aus:

1. Geben Sie Ihren Passwörtern mindestens acht Zeichen lang.
2. Deaktivieren Sie Telnet. Benutzer sollten sich nur mit SSH einloggen.
3. Deaktivieren Sie die Remote-Authentifizierung über RADIUS/TACACS+. Nur lokale Benutzer des Switches können authentifiziert werden.
4. Deaktivieren Sie SNMP v1 und v2. Alle bestehenden Benutzerkonten auf dem Switch, die für SNMPv3 konfiguriert wurden, sollten nur mit SHA für die Authentifizierung und AES/3DES für den Datenschutz konfiguriert werden.
5. VRRP deaktivieren.
6. Löschen Sie alle IKE-Richtlinien, die MD5 für die Authentifizierung oder DES für die Verschlüsselung besitzen. Ändern Sie die Richtlinien, sodass sie SHA für die Authentifizierung und 3DES/AES für die

Verschlüsselung verwenden.

7. Löschen Sie alle SSH Server RSA1-Tastenfelder.

Gehen Sie wie folgt vor, um den FIPS-Modus zu aktivieren und den FIPS-Status auf dem MDS-Switch anzuzeigen:

1. Zeigt den FIPS-Status an.

```
MDSSwitch# show fips status
FIPS mode is disabled
MDSSwitch# conf
Enter configuration commands, one per line.  End with CNTL/Z.
```

2. Richten Sie den 2048-Bit-SSH-Schlüssel ein.

```
MDSSwitch(config)# no feature ssh
XML interface to system may become unavailable since ssh is disabled
MDSSwitch(config)# no ssh key
MDSSwitch(config)# show ssh key
**************************************
could not retrieve rsa key information
bitcount: 0
**************************************
could not retrieve dsa key information
bitcount: 0
**************************************
no ssh keys present. you will have to generate them
**************************************
MDSSwitch(config)# ssh key
dsa   rsa
MDSSwitch(config)# ssh key rsa 2048 force
generating rsa key(2048 bits).....
...
generated rsa key
```

3. Aktivieren Sie den FIPS-Modus.

```
MDSSwitch(config)# fips mode enable
FIPS mode is enabled
System reboot is required after saving the configuration for the system
to be in FIPS mode
Warning: As per NIST requirements in 6.X, the minimum RSA Key Size has
to be 2048
```

4. Zeigt den FIPS-Status an.

```
MDSSwitch(config)# show fips status
FIPS mode is enabled
MDSSwitch(config)# feature ssh
MDSSwitch(config)# show feature | grep ssh
sshServer            1        enabled
```

5. Speichern Sie die Konfiguration in der laufenden Konfiguration.

```
MDSSwitch(config)# copy ru st
[########################################] 100%
exitCopy complete.
MDSSwitch(config)# exit
```

6. Starten Sie den MDS-Switch neu

```
MDSSwitch# reload
This command will reboot the system. (y/n)?  [n] y
```

7. Zeigt den FIPS-Status an.

```
Switch(config)# fips mode enable
Switch(config)# show fips status
```

Weitere Informationen finden Sie unter "Aktivieren des FIPS-Modus".

Cisco Nexus

Die Switches der Cisco Nexus 9000 Serie (Version 9.3) sind "FIPS 140-2 konform". Cisco Nexus implementiert kryptografische Module und die folgenden Services für SNMPv3 und SSH.

- Sitzungseinrichtung unterstützt jeden Service
- Alle zugrunde liegenden kryptografischen Algorithmen, die die wichtigsten Ableitfunktionen der Dienste unterstützen
- Hashing für jeden Service
- Symmetrische Verschlüsselung für jeden Service

Führen Sie vor Aktivierung des FIPS-Modus die folgenden Aufgaben auf dem Cisco Nexus-Switch aus:

1. Deaktivieren Sie Telnet. Benutzer sollten sich nur mit Secure Shell (SSH) anmelden.
2. Deaktivieren Sie SNMPv1 und v2. Alle bestehenden Benutzerkonten auf dem Gerät, die für SNMPv3 konfiguriert wurden, sollten nur mit SHA für die Authentifizierung und AES/3DES für den Datenschutz

konfiguriert werden.

3. Löschen Sie alle SSH-Server RSA1-Schlüsselpaare.
4. Aktivieren Sie die HMAC-SHA1-Nachrichtenintegritätsprüfung (MIC) für die Verwendung während der Aushandlung des Cisco TrustSec Security Association Protocol (SAP). Geben Sie dazu den sap-Hash-Algorithmus ein `HMAC-SHA-1` Befehl aus dem `cts-manual` Oder `cts-dot1x` Modus.

Gehen Sie wie folgt vor, um den FIPS-Modus auf dem Nexus Switch zu aktivieren:

1. Einrichten des SSH-Schlüssels mit 2048 Bit.

```
NexusSwitch# show fips status
FIPS mode is disabled
NexusSwitch# conf
Enter configuration commands, one per line.  End with CNTL/Z.
```

2. Richten Sie den 2048-Bit-SSH-Schlüssel ein.

```
NexusSwitch(config)# no feature ssh
XML interface to system may become unavailable since ssh is disabled
NexusSwitch(config)# no ssh key
NexusSwitch(config)# show ssh key
**************************************
could not retrieve rsa key information
bitcount: 0
**************************************
could not retrieve dsa key information
bitcount: 0
**************************************
no ssh keys present. you will have to generate them
**************************************
NexusSwitch(config)# ssh key
dsa   rsa
NexusSwitch(config)# ssh key rsa 2048 force
generating rsa key(2048 bits).....
...
generated rsa key
```

3. Aktivieren Sie den FIPS-Modus.

```
NexusSwitch(config)# fips mode enable
FIPS mode is enabled
System reboot is required after saving the configuration for the system
to be in FIPS mode
Warning: As per NIST requirements in 6.X, the minimum RSA Key Size has
to be 2048
Show fips status
NexusSwitch(config)# show fips status
FIPS mode is enabled
NexusSwitch(config)# feature ssh
NexusSwitch(config)# show feature | grep ssh
sshServer            1        enabled
Save configuration to the running configuration
NexusSwitch(config)# copy ru st
[########################################] 100%
exitCopy complete.
NexusSwitch(config)# exit
```

4. Starten Sie den Nexus Switch neu.

```
NexusSwitch# reload
This command will reboot the system. (y/n)?  [n] y
```

5. Zeigt den FIPS-Status an.

```
NexusSwitch(config)# fips mode enable
NexusSwitch(config)# show fips status
```

Darüber hinaus unterstützt die Cisco NX OS-Software die NetFlow-Funktion, die eine verbesserte Erkennung von Netzwerkanomalien und -Sicherheit ermöglicht. NetFlow erfasst die Metadaten jedes Gesprächs im Netzwerk, die an der Kommunikation beteiligten Parteien, das verwendete Protokoll und die Dauer der Transaktion. Nachdem die Informationen aggregiert und analysiert wurden, können sie einen Einblick in das normale Verhalten geben. Die gesammelten Daten ermöglichen außerdem die Identifizierung fragwürdiger Aktivitätsmuster, wie etwa die Verbreitung von Malware im Netzwerk, die ansonsten unbemerkt bleiben kann. NetFlow verwendet Flows, um Statistiken für die Netzwerküberwachung bereitzustellen. Ein Flow ist ein unidirektionaler Strom von Paketen, der auf einer Quellschnittstelle (oder VLAN) ankommt und die gleichen Werte für die Schlüssel hat. Ein Schlüssel ist ein identifizierter Wert für ein Feld innerhalb des Pakets. Sie erstellen einen Flow mithilfe eines Flow-Datensatzes, um die eindeutigen Tasten für Ihren Flow zu definieren. Sie können die Daten, die NetFlow für Ihre Ströme sammelt, mit Hilfe eines Flow-Exporterers in einen Remote NetFlow Collector, wie z. B. Cisco Stealthwatch, exportieren. Stealthwatch verwendet diese Informationen für die kontinuierliche Überwachung des Netzwerks und bietet Bedrohungserkennung in Echtzeit sowie eine Forensik zum Vorfallsreaktion, falls ein Ransomware-Ausbruch auftritt.

"Als Nächstes: FlexPod ONTAP Storage und FIPS 140"

FlexPod NetApp ONTAP Storage und FIPS 140-2

"Früher: FlexPod Networking mit Cisco und FIPS 140-2."

NetApp bietet verschiedene Hardware, Software und Services, die verschiedene Komponenten der im Rahmen des Standards validierten kryptografischen Module umfassen können. Daher verwendet NetApp verschiedene Ansätze zur Einhaltung von FIPS 140-2 für die Kontrollebene und Datenebene:

- NetApp umfasst kryptografische Module, die eine Level-1-Validierung für die Verschlüsselung von Daten während der Übertragung und Daten im Ruhezustand erzielt haben.
- NetApp übernimmt sowohl Hardware- als auch Softwaremodule, die vom Anbieter dieser Komponenten nach FIPS 140-2 validiert wurden. So nutzt die NetApp Storage Encryption Lösung beispielsweise validierte Laufwerke der FIPS Level 2.
- NetApp Produkte können ein validiertes Modul so verwenden, dass die Standards erfüllt werden, obwohl das Produkt oder die Funktion nicht innerhalb der Validierungsgrenze liegt. Beispielsweise ist NetApp Volume Encryption (NVE) FIPS 140-2-2-konform. Obwohl diese Prüfung nicht separat durchgeführt wird, nutzt sie das nach Level 1 zertifizierte NetApp kryptografische Modul. Weitere Informationen zu Compliance-Besonderheiten für Ihre ONTAP Version erhalten Sie bei Ihrem FlexPod SME.

NetApp Cryptographic Module sind nach FIPS 140-2 Level 1 zertifiziert

- Das NetApp Cryptographic Security Module (NCSM) ist nach FIPS 140-2 Level 1 zertifiziert.

Die Self-Encrypting Drives von NetApp sind nach FIPS 140-2 Level 2 zertifiziert

NetApp erwirbt Self-Encrypting Drives (SEDs), die vom ursprünglichen Equipment-Hersteller (OEM) nach FIPS 140-2 validiert wurden. Kunden, die diese Laufwerke suchen, müssen bei der Bestellung angeben. Laufwerke werden auf Ebene 2 validiert. Die folgenden NetApp Produkte können validierte SEDs nutzen:

- AFF A-Series und FAS Storage-Systeme
- E-Series und EF-Series Storage-Systeme

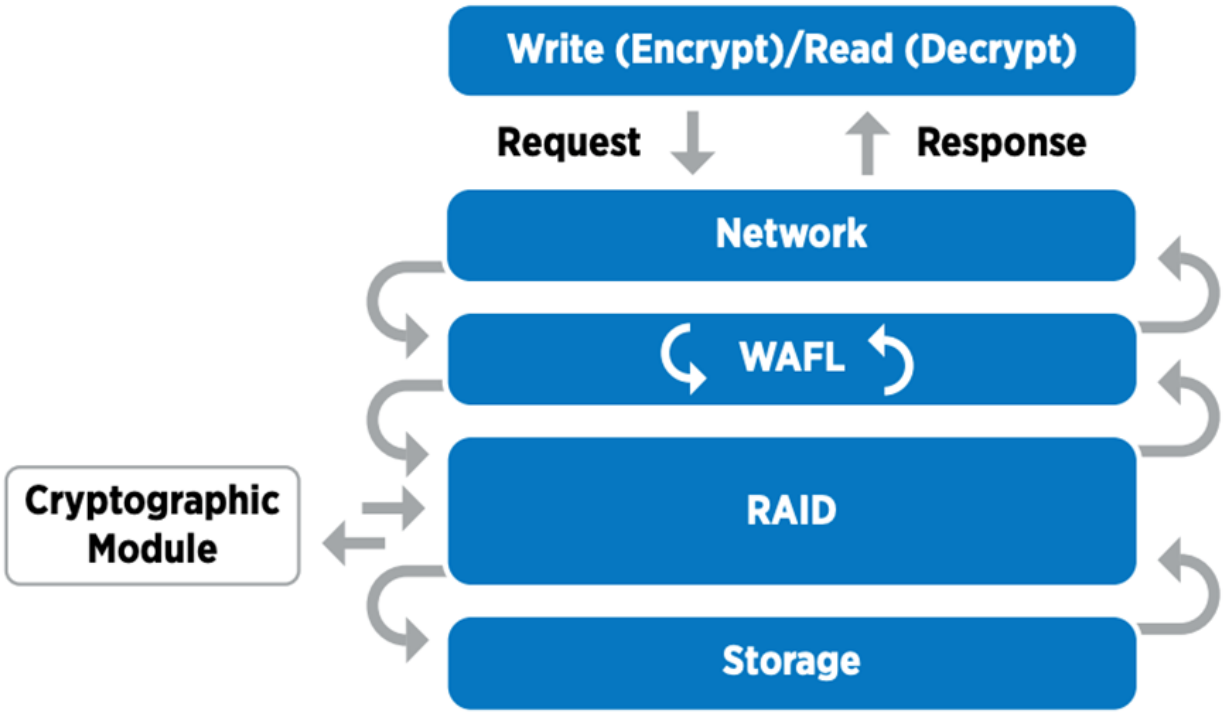
NetApp Aggregate Encryption und NetApp Volume Encryption

Die Technologien NVE und NetApp Aggregate Encryption (NAE) ermöglichen die Verschlüsselung von Daten auf Volume- und Aggregatebene. Dadurch ist die Lösung unabhängig von dem physischen Laufwerk.

NVE ist eine softwarebasierte Lösung zur Verschlüsselung von Daten im Ruhezustand, die ab ONTAP 9.1 verfügbar ist und seit ONTAP 9.2 FIPS 140-2-konform ist. Mit NVE kann ONTAP Daten mit einer Granularität pro Volume verschlüsseln. NAE, der mit ONTAP 9.6 verfügbar ist, ist ein nicht weiter ausumendes NVE-Systems. ONTAP kann Daten für jedes Volume verschlüsseln und die Volumes können Schlüssel über das Aggregat hinweg gemeinsam nutzen. Sowohl NVE als auch NAE nutzen 256-Bit-Verschlüsselung nach AES. Daten können auch ohne SEDs auf Festplatte gespeichert werden. Mit NVE und NAE können Sie Storage-Effizienzfunktionen auch bei aktivierter Verschlüsselung nutzen. Eine reine Verschlüsselung auf Applikationsebene besiegt alle Vorteile der Storage-Effizienz. Mit NVE und NAE bleiben Storage-Effizienzfunktionen erhalten, da die Daten vom Netzwerk über NetApp WAFL bis zur RAID-Schicht erfasst werden, über die bestimmt wird, ob die Daten verschlüsselt werden sollen. Für bessere Storage-Effizienz kann die Aggregatdeduplizierung mit NAE verwendet werden. NVE Volumes und NAE-Volumes können gleichzeitig im selben NAE-Aggregat bestehen. NAE-Aggregate unterstützen keine unverschlüsselten Volumes.

So funktioniert der Prozess: Wenn Daten verschlüsselt werden, wird er an das kryptografische Modul

gesendet, das nach FIPS 140-2 Level 1 zertifiziert ist. Das kryptografische Modul verschlüsselt die Daten und sendet sie zurück an die RAID-Schicht. Die verschlüsselten Daten werden dann an die Festplatte gesendet. Somit sind die Daten mit der Kombination von NVE und NAE bereits auf dem Weg zur Festplatte verschlüsselt. Lesezugriffe folgen dem umgekehrten Pfad. Mit anderen Worten: Die Daten lassen die Festplatte verschlüsselt, werden an RAID gesendet, durch das kryptografische Modul entschlüsselt und dann den Rest des Stacks, wie in der folgenden Abbildung dargestellt, hochgeschickt.



NVE kommt mit einem softwarebasierten kryptografischen Modul zum Einsatz, das nach FIPS 140-2 Level 1 zertifiziert ist.

Weitere Informationen zu NVE finden Sie im "NVE Datenblatt".

NVE schützt Daten in der Cloud. Cloud Volumes ONTAP und Azure NetApp Files bieten Daten im Ruhezustand nach FIPS 140-2-2-konform.

Ab ONTAP 9.7 werden neu erstellte Aggregate und Volumes standardmäßig bei Nutzung der NVE-Lizenz und im integrierten oder externen Verschlüsselungsmanagement verschlüsselt. Ab ONTAP 9.6 können Sie mithilfe der Verschlüsselung auf Aggregatebene dem enthaltenden Aggregat Schlüssel zuweisen, damit die Volumes verschlüsselt werden können. Die im Aggregat erstellten Volumes werden standardmäßig verschlüsselt. Sie können den Standardwert überschreiben, wenn Sie das Volume verschlüsseln.

CLI-BEFEHLE VON ONTAP NAE

Bevor Sie die folgenden CLI-Befehle ausführen, stellen Sie sicher, dass für das Cluster die erforderliche NVE-Lizenz vorhanden ist.

Um ein Aggregat zu erstellen und zu verschlüsseln, führen Sie den folgenden Befehl aus (wenn es auf einer ONTAP 9.6 und höher Cluster CLI ausgeführt wird):

```
fp-health::> storage aggregate create -aggregate aggregatename -encrypt
-with-aggr-key true
```

Um ein nicht-NAE-Aggregat in ein NAE-Aggregat zu konvertieren, führen Sie den folgenden Befehl aus (wenn Sie auf einem ONTAP 9.6 und höher Cluster CLI laufen):

```
fp-health::> storage aggregate modify -aggregate aggregatename  -node
svmname -encrypt-with-aggr-key true
```

Um ein NAE-Aggregat in ein nicht-NAE- Aggregat zu konvertieren, führen Sie den folgenden Befehl aus (wenn Sie auf einem ONTAP 9.6 und höher Cluster CLI ausführen):

```
fp-health::> storage aggregate modify -aggregate aggregatename -node
svmname -encrypt-with-aggr-key false
```

CLI-BEFEHLE VON ONTAP NVE

Ab ONTAP 9.6 können Sie mithilfe der Verschlüsselung auf Aggregatebene dem enthaltenden Aggregat Schlüssel zuweisen, damit die Volumes verschlüsselt werden können. Die im Aggregat erstellten Volumes werden standardmäßig verschlüsselt.

Führen Sie zum Erstellen eines Volumes auf einem Aggregat, das über NAE aktiviert ist, den folgenden Befehl aus (wenn Sie auf einem ONTAP 9.6 und höher Cluster CLI ausführen):

```
fp-health::> volume create -vserver svmname -volume volumename -aggregate
aggregatename -encrypt true
```

Um die Verschlüsselung eines vorhandenen Volume „inplace“ ohne Volume-Verschiebung zu aktivieren, führen Sie den folgenden Befehl aus (wenn Sie auf einer ONTAP 9.6 und höher Cluster CLI ausführen):

```
fp-health::> volume encryption conversion start -vserver svmname -volume
volumename
```

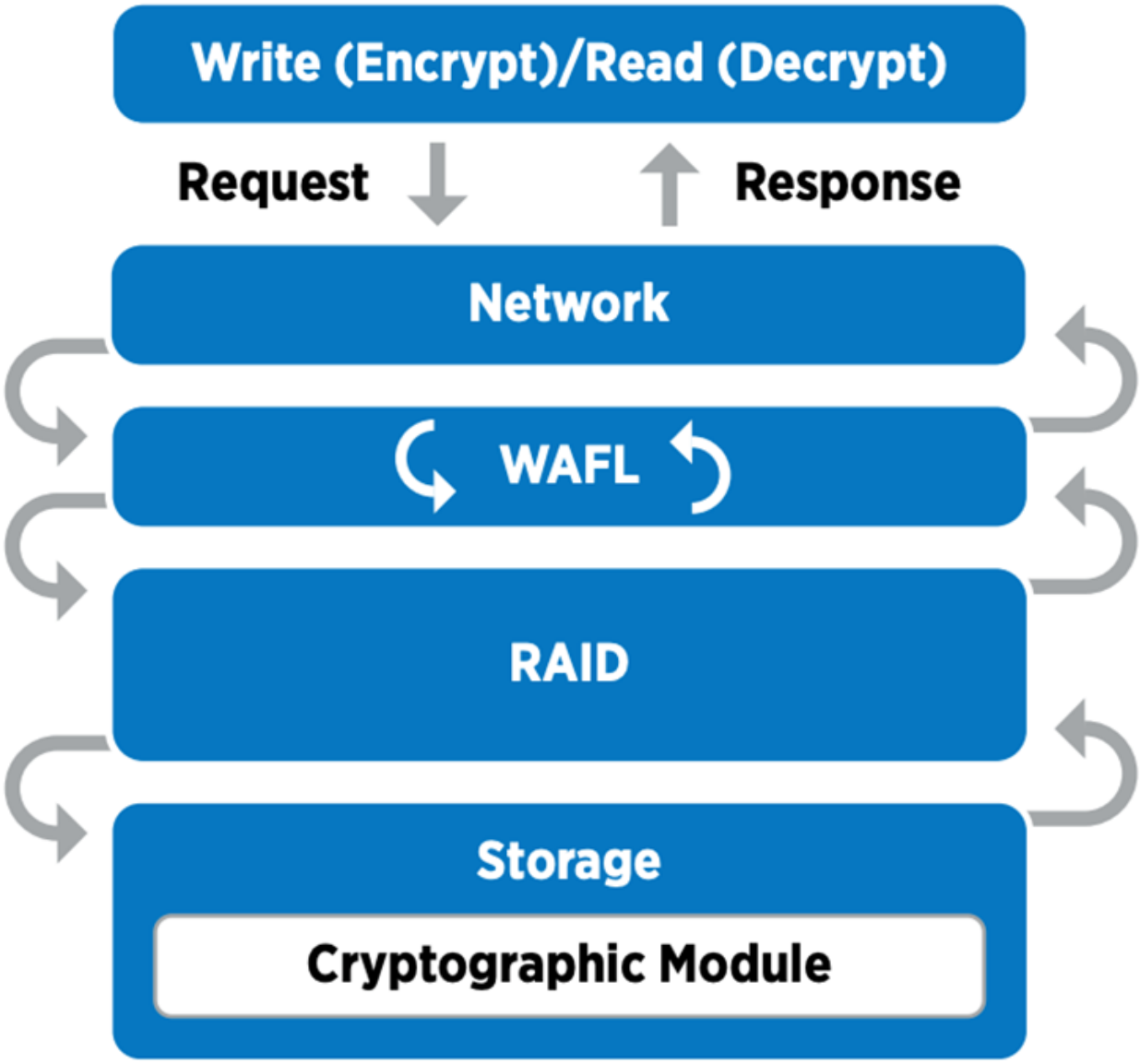
Führen Sie den folgenden CLI-Befehl aus, um zu überprüfen, ob Volumes für die Verschlüsselung aktiviert sind:

```
fp-health::> volume show -is-encrypted true
```

NSE

NSE nutzt SEDs, um die Datenverschlüsselung durch einen hardwarebeschleunigten Mechanismus durchzuführen.

NSE kann mit Self-Encrypting Drives nach FIPS 140-2 Level 2 verwendet werden, um Compliance und die Rückgabe von Ersatzteilen zu ermöglichen. Dazu wird der Schutz von Daten im Ruhezustand durch transparente AES-256-Bit-Festplattenverschlüsselung ermöglicht. Die Laufwerke führen alle Datenverschlüsselungsvorgänge intern aus, wie in der folgenden Abbildung dargestellt, einschließlich Schlüsselgenerierung. Um unbefugten Zugriff auf die Daten zu verhindern, muss sich das Speichersystem mit dem Laufwerk authentifizieren und einen Authentifizierungsschlüssel verwenden, der bei der ersten Verwendung des Laufwerks eingerichtet wurde.



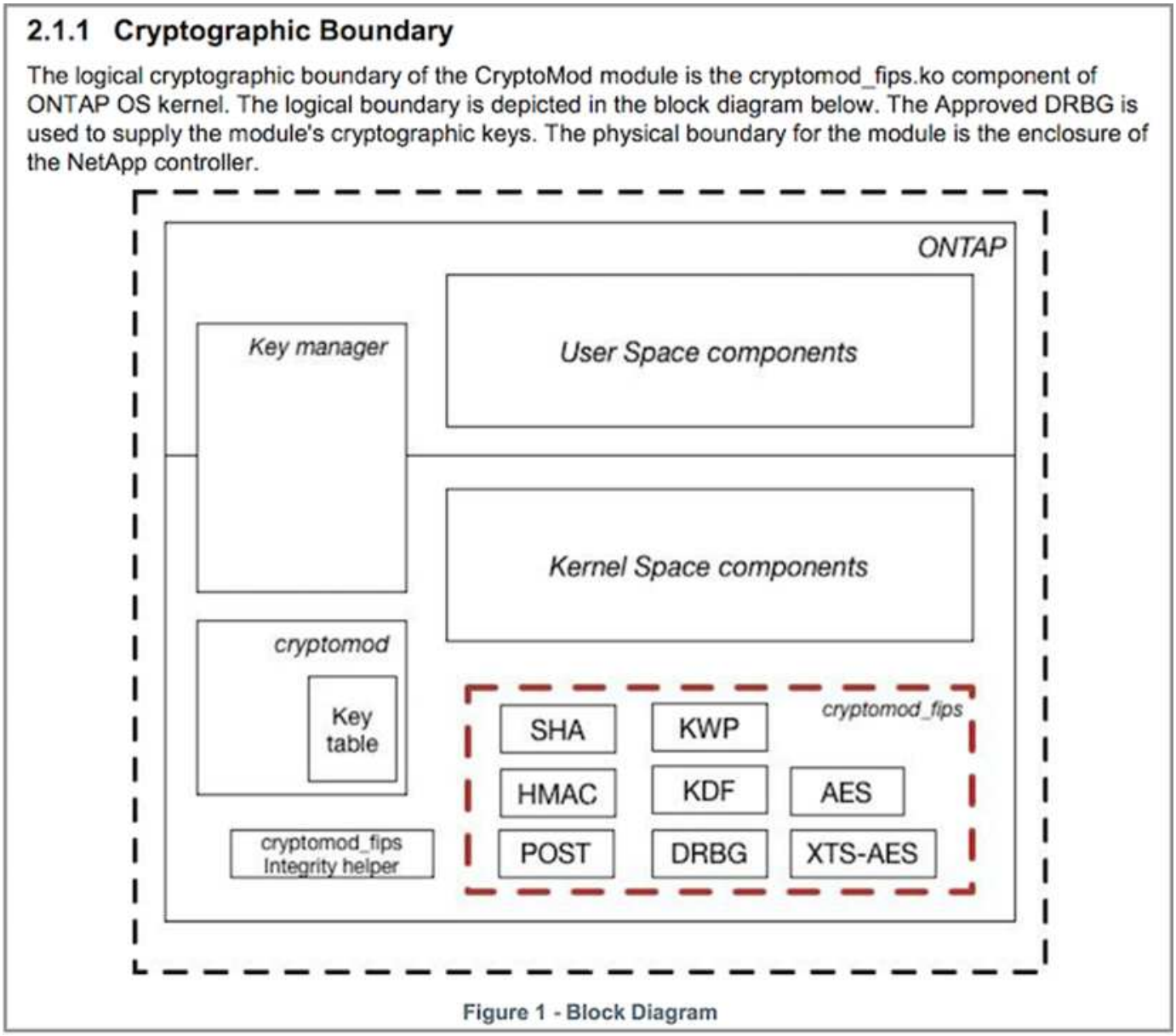
NSE verwendet Hardware-Verschlüsselung auf jedem Laufwerk, das nach FIPS 140-2 Level 2 zertifiziert ist.

Weitere Informationen zu NSE finden Sie im "NSE Datenblatt".

Schlüsselmanagement

Der FIPS 140-2-Standard gilt für das kryptografische Modul gemäß der Definition der Grenze, wie in der

folgenden Abbildung dargestellt.



Der Schlüsselmanager verfolgt alle von ONTAP verwendeten Datenschlüssel. NSE SEDs verwenden den Schlüsselmanager, um die Authentifizierungsschlüssel für NSE SEDs festzulegen. Bei Verwendung des Schlüsselmanagers besteht die kombinierte NVE und NAE-Lösung aus einem softwarebasierten kryptografischen Modul und einem Schlüsselmanager. NVE verwendet für jedes Volume einen eindeutigen XTS-AES 256-Datenverschlüsselung, der vom Schlüsselmanager gespeichert wird. Der für ein Daten-Volume verwendete Schlüssel liegt nur bei dem Daten-Volume in diesem Cluster und wird bei der Erstellung des verschlüsselten Volume generiert. Auf ähnliche Weise verwendet ein NAE-Volume eindeutige XTS-AES 256-Datenschlüssel pro Aggregat, das ebenfalls vom Schlüsselmanager gespeichert wird. NAE-Schlüssel werden erzeugt, wenn das verschlüsselte Aggregat erstellt wird. ONTAP generiert keine Schlüssel vorab, verwendet sie nicht oder zeigt sie in Klartext an. Sie werden vom Schlüsselmanager gespeichert und geschützt.

Unterstützung von externen Schlüsselmanagern

Ab ONTAP 9.3 werden externe Schlüsselmanager sowohl in NVE als auch in NSE-Lösungen unterstützt. Der FIPS 140-2-Standard gilt für das kryptografische Modul, das bei der Implementierung des jeweiligen Anbieters verwendet wird. In den meisten Fällen nutzen FlexPod und ONTAP Kunden eine der folgenden Validierungen

(entsprechend der "NetApp Interoperabilitätsmatrix") Schlüsselmanager:

- Gemalto oder SafeNet AT
- Vormetric (Thales)
- IBM SKLM
- Utimaco (ehemals Mikrofokus, HPE)

NSE und NVMe SED-Authentifizierungsschlüssel werden mithilfe des branchenüblichen OASIS Key Management Interoperability Protocol (KMIP) an einem externen Schlüsselmanager gesichert. Nur das Storage-System, das Laufwerk und der Schlüsselmanager haben Zugriff auf den Schlüssel. Wenn das Laufwerk außerhalb der Sicherheitsdomain verschoben wird, kann es nicht entsperrt werden. So verhindert es Datenverluste. Außerdem speichert der externe Schlüsselmanager NVE Volume Encryption Keys und NAE Aggregate Encryption Keys. Wenn Controller und Datenträger keinen Zugriff mehr auf den externen Schlüsselmanager haben, sind die NVE- und NAE-Volumes nicht zugänglich und können nicht entschlüsselt werden.

Der folgende Beispielbefehl fügt zwei wichtige Managementserver zur Liste der Server hinzu, die vom externen Schlüsselmanager für Store Virtual Machine (SVM) verwendet werden. `svmname1`.

```
fp-health::> security key-manager external add-servers -vserver svmname1
-key-servers 10.0.0.20:15690, 10.0.0.21:15691
```

Wenn ein FlexPod Datacenter in einem Szenario mit Mandantenfähigkeit zum Einsatz kommt, ermöglicht ONTAP Benutzern die Trennung der Mandantenfähigkeit – und zwar aus Sicherheitsgründen auf SVM-Ebene.

Führen Sie den folgenden CLI-Befehl aus, um die Liste der externen Schlüsselmanager zu überprüfen:

```
fp-health::> security key-manager external show
```

Kombinierte Verschlüsselung für doppelte Verschlüsselung (mehrstufige Verteidigung)

Wenn Sie den Zugriff auf Daten getrennt halten und sicherstellen müssen, dass die Daten jederzeit geschützt sind, kann NSE SEDs mit Verschlüsselung auf Netzwerk- oder Fabric-Ebene kombiniert werden. NSE SEDs stehen wie ein Backstop, wenn ein Administrator die Verschlüsselung auf höherer Ebene nicht konfiguriert oder falsch konfiguriert. So können NSE SEDs mit NVE und NAE kombiniert werden, um zwei unterschiedliche Verschlüsselungsebenen zu schaffen.

NetApp ONTAP Cluster-weite Kontrollebene FIPS-Modus

Die NetApp ONTAP Datenmanagement-Software verfügt über eine FIPS-Mode-Konfiguration, die eine zusätzliche Sicherheit für den Kunden erzeugt. Dieser FIPS-Modus gilt nur für die Kontrollebene. Wenn der FIPS-Modus entsprechend den Schlüsselelementen von FIPS 140 aktiviert ist, sind Transport Layer Security v1 (TLSv1) und SSLv3 deaktiviert, und nur TLS v1.1 und TLS v1.2 bleiben aktiviert.

Die Cluster-weite ONTAP Kontrollscheibe im FIPS-Modus ist konform mit FIPS 140-2 Level 1. Im Cluster-weiten FIPS-Modus kommt ein softwarebasiertes kryptografisches Modul zum Einsatz, das von NCSM bereitgestellt wird.

FIPS 140-2 Compliance-Modus für Cluster-weite Kontrollebene sichert alle Kontrollschnittstellen von ONTAP. Standardmäßig ist der Modus nur für FIPS 140-2 deaktiviert; Sie können diesen Modus jedoch aktivieren, indem Sie den einstellen `is- fips-enabled` Parameter an `true` Für das `security config modify` Befehl.

Führen Sie den folgenden Befehl aus, um den FIPS-Modus auf dem ONTAP Cluster zu aktivieren:

```
fp-health::> security config modify -interface SSL -is-fips-enabled true
```

Wenn der SSL-FIPS-Modus aktiviert ist, wird die SSL-Kommunikation von ONTAP zu den externen Client- oder Serverkomponenten außerhalb von ONTAP auf FIPS-Beschwerde kryptografisch für SSL verwendet.

Um den FIPS-Status für das gesamte Cluster anzuzeigen, führen Sie die folgenden Befehle aus:

```
fp-health::> set advanced
fp-health::*> security config modify -interface SSL -is-fips-enabled true
```

"Als Nächstes: Lösungsvorteile der konvergenten FlexPod Infrastruktur"

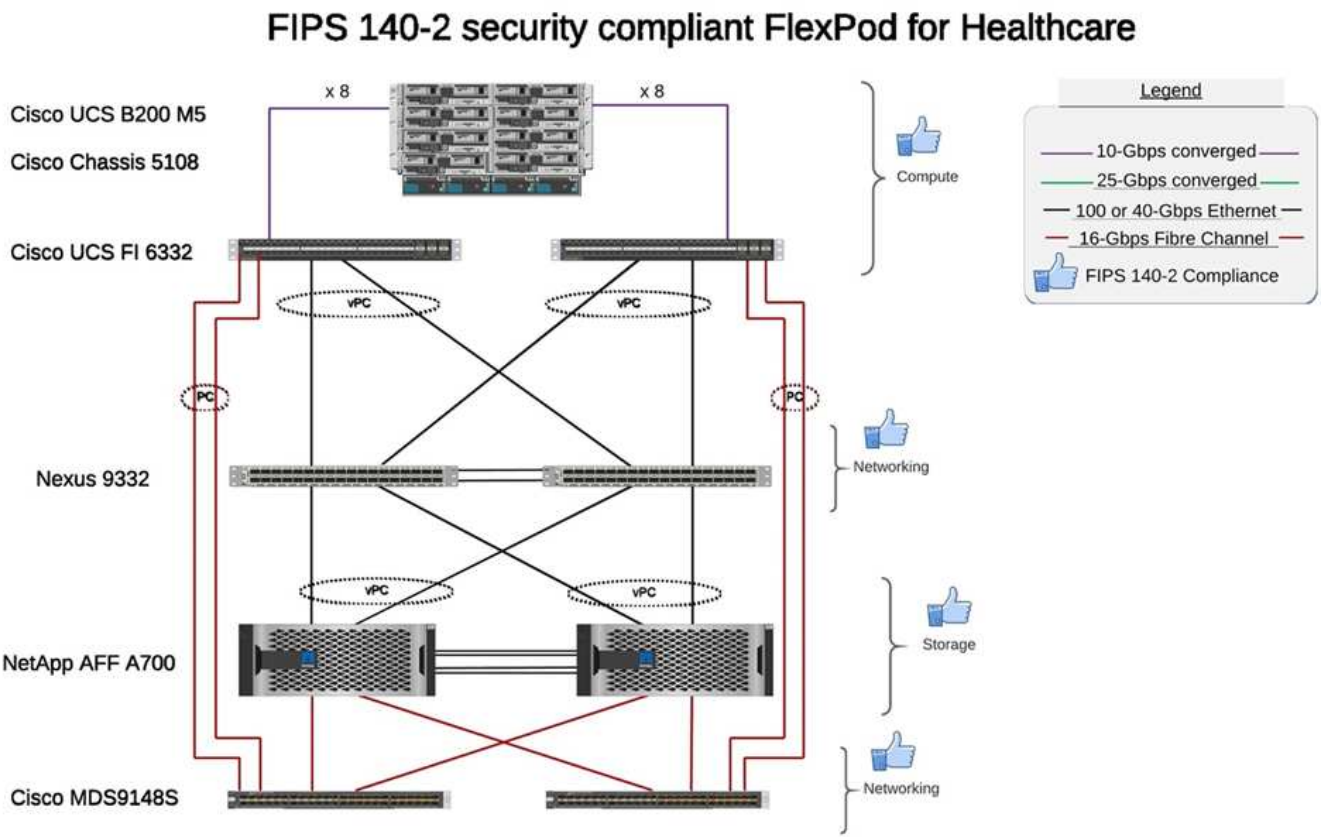
Lösungsvorteile der konvergenten FlexPod Infrastruktur

"Früher: FlexPod NetApp ONTAP Storage und FIPS 140-2."

Organisationen im Gesundheitswesen verfügen über mehrere geschäftskritische Systeme. Zwei der kritischsten Systeme sind das elektronische Gesundheitsakten (EHR) und das medizinische Bildgebungssystem. Um die FIPS-Einrichtung auf einem FlexPod System zu demonstrieren, haben wir ein Open-Source-EHR- und ein Open-Source-System für die Bildarchivierung und das Kommunikationssystem (PACS) für die Lab-Einrichtung und die Workload-Validierung im FlexPod System verwendet. Eine vollständige Liste aller EHR-Funktionen, logischen EHR-Applikationskomponenten und die Vorteile von EHR-Systemen bei Implementierung in einem FlexPod-System finden Sie unter "TR-4881: FlexPod für elektronische Krankenakten". Eine vollständige Liste der Funktionen eines Bildgebungssystems für die medizinische Bildgebung, logischer Applikationskomponenten und der Vorteile medizinischer Bildgebungssysteme bei der Implementierung mit FlexPod finden Sie unter "TR-4865: FlexPod für die medizinische Bildgebung".

Während der FIPS-Einrichtung und Workload-Validierung übten wir Workload-Merkmale aus, die einer typischen Gesundheitseinrichtung entsprechen. Wir haben beispielsweise ein Open Source EHR-System genutzt, um realistische Zugriffsszenarien für Patientendaten und Änderungen einzuschließen. Zudem wurden Workloads für die medizinische Bildgebung durchgeführt, einschließlich digitaler Bildgebung und Kommunikation in medizinischen Objekten (DICOM) `*. dcm` Dateiformat. DICOM-Objekte mit Metadaten wurden sowohl im Datei- als auch im Block-Storage gespeichert. Darüber hinaus haben wir Multipathing-Funktionen über einen virtualisierten RedHat Enterprise Linux (RHEL) Server implementiert. Wir speicherten DICOM-Objekte auf einem NFS, gemounteten LUNs über iSCSI und gemounteten LUNs über FC. Bei der FIPS-Einrichtung und -Validierung wurde festgestellt, dass die konvergente FlexPod Infrastruktur unsere Erwartungen übertroffen und sich nahtlos an eine Lösung anstellte.

Die folgende Abbildung zeigt das FlexPod System zur FIPS-Einrichtung und -Validierung. Wir haben die genutzt "FlexPod Datacenter mit VMware vSphere 7.0 und NetApp ONTAP 9.7 Cisco Validated Design (CVD)" Während des Setups.



Hardware- und Softwarekomponenten der Lösungsinfrastruktur

In den folgenden beiden Abbildungen sind die Hardware- und Software-Komponenten aufgeführt, die jeweils bei der Aktivierung von FIPS-Tests auf einem FlexPod verwendet werden. Beispiele sind die Empfehlungen in diesen Tabellen. Sie sollten mit Ihrem NetApp SME zusammenarbeiten, um sicherzustellen, dass die Komponenten für Ihr Unternehmen geeignet sind. Vergewissern Sie sich außerdem, dass die Komponenten und Versionen von unterstützt werden "NetApp Interoperabilitäts-Matrix-Tool" (IMT) und "Cisco Hardware Compatibility List (HCL)".

Schicht	Produktfamilie	Menge und Modell	Details
Computing	Cisco UCS 5108 Chassis	1 oder 2	
	Cisco UCS Blade Server	3 B200 M5	Jeweils mit 2x 20 Cores, 2,7 GHz und 128 bis 384 GB RAM
	Cisco UCS Virtual Interface Card (VIC)	Cisco UCS 1440	Siehe
	2 Cisco UCS Fabric Interconnects	6332	-
Netzwerk	Cisco Nexus Switches	2 x Cisco Nexus 9332	-

Schicht	Produktfamilie	Menge und Modell	Details
Datennetzwerk Storage-Netzwerk	IP-Netzwerk für Storage-Zugriff über SMB-/CIFS-, NFS- oder iSCSI-Protokolle	Gleiche Netzwerk-Switches wie oben	-
	Storage-Zugriff über FC	2 x Cisco MDS 9148S	-
Storage	NetApp AFF A700 All-Flash-Storage-System	1 Cluster	Cluster mit zwei Nodes
	Festplatten-Shelf	Ein DS224C oder NS224 Festplatten-Shelf	Vollständig mit 24 Laufwerken bestückt
	SSD	>24, 1,2 TB oder mehr Kapazität	-

Software	Produktfamilie	Version/Release	Details
Verschiedene	Linux	RHEL 7.X	-
	Windows	Windows Server 2012 R2 (64-Bit)	-
	NetApp ONTAP	ONTAP 9.7 oder höher	-
	Cisco UCS Fabric Interconnect	Cisco UCS Manager 4.1 oder höher	-
	Cisco Switches der Ethernet-Serie 3000 oder 9000	Für 9000-Serie, 7.0(3)I7(7) oder höher für 3000-Serie, 9.2(4) oder höher	-
	Cisco FC: Cisco MDS 9132T	8.4(1a) oder höher	-
	Hypervisor	VMware vSphere ESXi 6.7 U2 oder höher	-
Storage	Hypervisor-Managementsystem	VMware vCenter Server 6.7 U3 (vCSA) oder höher	-
Netzwerk	NetApp Virtual Storage Console (VSC)	VSC 9.7 oder höher	-
	NetApp SnapCenter	SnapCenter 4.3 oder höher	-
	Cisco UCS Manager	4.1(1c) oder höher	
Hypervisor	ESXi		
Vereinfachtes	Hypervisor-ManagementsystemVMware vCenter Server 6.7 U3 (vCSA) oder höher		
	NetApp Virtual Storage Console (VSC)	VSC 9.7 oder höher	

Software	Produktfamilie	Version/Release	Details
	NetApp SnapCenter	SnapCenter 4.3 oder höher	
	Cisco UCS Manager	4.1(1c) oder höher	

"Als Nächstes: Weitere FlexPod-Sicherheitsüberlegungen."

Weitere Sicherheitsaspekte bei FlexPod

"Previous – Lösungsvorteile der konvergenten FlexPod Infrastruktur"

Die FlexPod-Infrastruktur ist eine modulare, konvergierte, optional virtualisierte, skalierbare (horizontale und vertikale Skalierung) und kostengünstige Plattform. Mit der FlexPod Plattform können Sie Computing-, Netzwerk- und Storage-Ressourcen unabhängig horizontal skalieren und so die Applikationsimplementierung beschleunigen. Und die modulare Architektur ermöglicht auch bei horizontale und Upgrade-Vorgängen mit Systemen einen unterbrechungsfreien Betrieb.

Für verschiedene Komponenten eines HIT-Systems müssen die Daten in den Dateisystemen SMB/CIFS, NFS, Ext4 und NTFS gespeichert werden. Diese Anforderung bedeutet, dass die Infrastruktur Datenzugriff über NFS-, CIFS- und SAN-Protokolle bieten muss. Ein einziges NetApp Storage-System kann alle diese Protokolle unterstützen, sodass keine herkömmliche Vorgehensweise bei protokollspezifischen Storage-Systemen erforderlich ist. Zusätzlich kann ein einzelnes NetApp Storage-System mehrere HIT-Workloads wie EHRs, PACS oder VNA, Genomik, VDI usw. unterstützen Bei garantierten und konfigurierbaren Performance-Leveln.

DIE IMPLEMENTIERUNG in einem FlexPod System bringt VERSCHIEDENE Vorteile mit SICH, die speziell auf das Gesundheitswesen zugeschnitten sind. Die folgende Liste enthält eine ausführliche Beschreibung der folgenden Vorteile:

- **FlexPod Sicherheit**. Sicherheit ist die Grundlage eines FlexPod Systems. In den letzten Jahren ist Ransomware zu einer Bedrohung geworden. Ransomware ist eine Art von Malware, die auf Kryptovirologie basiert, die Verwendung von Kryptographie zum Aufbau von schädlicher Software. Diese Malware kann sowohl symmetrische und asymmetrische Schlüssel Verschlüsselung verwenden, um die Daten eines Opfers zu sperren und ein Lösegeld zu verlangen, um den Schlüssel zur Entschlüsselung der Daten. Informieren Sie sich, wie die FlexPod Lösung dazu beiträgt, Bedrohungen wie Ransomware zu minimieren "TR-4802: Die Lösung gegen Ransomware". Außerdem sind FlexPod Infrastrukturkomponenten "FIPS 140-2 konform".
- **Cisco Intersight.** Cisco Intersight ist eine innovative, Cloud-basierte Management-als-Service-Plattform, die eine zentrale Konsole für FlexPod Management und Orchestrierung in einem kompletten Stack bereitstellt. Die Intersight-Plattform verwendet FIPS 140-2-2-konforme kryptografische Module. Die Out-of-Band-Management-Architektur der Plattform macht sie für einige Standards oder Audits wie HIPAA außer Reichweite. Es werden nie individuelle identifizierbare Gesundheitsinformationen im Netzwerk an das Intersight-Portal gesendet.
- **NetApp FPolicy Technologie.** NetApp FPolicy (eine Entwicklung der Namensdateirichtlinie) ist ein Benachrichtigungs-Framework für den Dateizugriff über NFS- oder SMB/CIFS-Protokolle. Diese Technologie ist seit über zehn Jahren Bestandteil der ONTAP Datenmanagement-Software und hilft bei der Erkennung von Ransomware. Diese Zero Trust Engine bietet zusätzliche Sicherheitsmaßnahmen, die über Berechtigungen in Zugriffssteuerungslisten (Access Control Lists, ACLs) hinausgehen. FPolicy verfügt über zwei Betriebsmodi: Nativ und extern:

- Der native Modus bietet sowohl Blacklisting als auch Whitelisting von Dateierweiterungen.
- Der externe Modus verfügt über die gleichen Funktionen wie der native Modus, kann aber auch mit einem FPolicy-Server integriert werden, der extern zum ONTAP-System läuft, sowie einem SIEM-System (Security Information and Event Management). Weitere Informationen zum Kampf gegen Ransomware finden Sie im "Fighting Ransomware: Teil drei – ONTAP FPolicy, ein weiteres leistungsstarkes Native Tool (aka Free)" blog:

- **Daten im Ruhezustand**. ONTAP 9 und höher verfügt über drei FIPS 140-2-konforme Verschlüsselungslösungen für Daten im Ruhezustand:
  - NSE ist eine Hardware-Lösung mit Self-Encrypting Drives.
  - NVE ist eine Softwarelösung, die die Verschlüsselung von beliebigen Daten-Volumes auf jedem Festplattentyp, auf der diese aktiviert ist, mit einem eindeutigen Schlüssel für jedes Volume ermöglicht.
  - NAE ist eine Software-Lösung, die die Verschlüsselung beliebiger Daten-Volumes auf jedem beliebigen Laufwerkstyp ermöglicht und bei jedem Aggregat mit eindeutigen Schlüsseln aktiviert wird.

> Ab ONTAP 9.7 sind NAE und NVE standardmäßig aktiviert, wenn das NetApp NVE Lizenzpaket mit dem Namen VE vorhanden ist.

- **Daten im Flug**. Ab ONTAP 9.8 unterstützt Internet Protocol Security (IPsec) die End-to-End-Verschlüsselung für den gesamten IP-Datenverkehr zwischen einem Client und einer ONTAP SVM. Die IPsec-Datenverschlüsselung für den gesamten IP-Datenverkehr umfasst NFS-, iSCSI- und SMB/CIFS-Protokolle. IPsec bietet die einzige Verschlüsselung im Flug für iSCSI-Datenverkehr.
- **End-to-End-Datenverschlüsselung in einer hybriden Multi-Cloud-Data-Fabric** Kunden, die Verschlüsselungstechnologien für ruhende Daten wie NSE oder NVE und Cluster Peering Encryption (CPE) für Datenreplizierungsverkehr verwenden, können nun mithilfe ONTAP von IPsec eine End-to-End-Verschlüsselung zwischen Client und Storage in ihrer hybriden Multi-Cloud Data Fabric verwenden 9.8. Ab ONTAP 9 können Sie den FIPS 140-2-Compliance-Modus für Cluster-weite Kontrollebene-Schnittstellen aktivieren. Standardmäßig ist der reine FIPS 140-2-Modus deaktiviert. Ab ONTAP 9.6 unterstützt CPE die TLS 1.2 AES-256 GCM-Verschlüsselung für ONTAP Datenreplizierungsfunktionen wie NetApp SnapMirror, NetApp SnapVault und NetApp FlexCache Technologien. Die Verschlüsselung wird über einen vorab freigegebenen Schlüssel (PSK) zwischen zwei Cluster-Peers eingerichtet.
- **Sichere Mandantenfähigkeit**. Dies ist auch in der Lage, die erhöhten Anforderungen virtualisierter Server- und Storage-Infrastrukturen zu erfüllen. Dies ermöglicht eine sichere Mandantenfähigkeit für applikationsspezifische Informationen, insbesondere zum Hosten mehrerer Instanzen von Datenbanken und Software.

"Weiter: Fazit."

Schlussfolgerung

"Früher: Weitere FlexPod-Sicherheitsüberlegungen."

Durch die Ausführung Ihrer Applikationen im Gesundheitswesen auf einer FlexPod Plattform ist Ihr Unternehmen im Gesundheitswesen durch eine Plattform mit FIPS 140-2-Zertifizierung besser geschützt. FlexPod bietet mehrschichtigen Schutz auf jeder einzelnen Komponente: computing, Netzwerk und Storage. Die Datensicherungsfunktionen von FlexPod schützen Daten im Ruhezustand und im Übertragungsprozess und sorgen dafür, dass Backups bei Bedarf sicher und bereit bleiben.

Vermeiden Sie menschliche Fehler durch den Einsatz der vorab validierten Designs von FlexPod, die umfassend getestete konvergente Infrastrukturen aus der strategischen Partnerschaft von Cisco und NetApp enthalten. Ein FlexPod System wurde speziell für vorhersehbare Performance mit niedriger Latenz und Hochverfügbarkeit konzipiert und bietet auch dann niedrige Auswirkungen, wenn FIPS 140-2 Computing-, Netzwerk- und Storage-Ebenen aktiviert ist. Dieser Ansatz führt zu einer optimalen Benutzererfahrung und einer optimalen Reaktionszeit für Benutzer Ihres HIT-Systems.

"Weiter: Danksagungen, Versionsverlauf, und wo finden Sie zusätzliche Informationen."

Danksagungen, Versionsverlauf und weitere Informationen finden

"Zurück: Schlussfolgerung."

Sehen Sie sich die folgenden Dokumente und Websites an, um mehr über die in diesem Dokument beschriebenen Daten zu erfahren:

- Cisco MDS 9000-Produktreihe NX-OS Security Configuration Guide

  https://www.cisco.com/c/en/us/td/docs/switches/datacenter/mds9000/sw/8_x/config/security/cisco_mds9000_security_config_guide_8x/configuring_fips.html#task_1188151

- Cisco Nexus 9000 Series NX-OS Security Configuration Guide, Release 9.3(x)

  https://www.cisco.com/c/en/us/td/docs/switches/datacenter/nexus9000/sw/93x/security/configuration/guide/b-cisco-nexus-9000-nx-os-security-configuration-guide-93x/m-configuring-fips.html

- NetApp and Federal Information Processing Standard (FIPS) Veröffentlichung 140-2

  https://www.netapp.com/company/trust-center/compliance/fips-140-2/

- FIPS 140-2

  https://fieldportal.netapp.com/content/902303

- NetApp Leitfaden zur Härtung von ONTAP 9

  https://www.netapp.com/us/media/tr-4569.pdf

- NetApp Encryption Power Guide

  https://docs.netapp.com/ontap-9/index.jsp?topic=%2Fcom.netapp.doc.pow-nve%2Fhome.html

- Datenblatt zu NVE und NAE

  https://www.netapp.com/us/media/ds-3899.pdf

- NSE Datenblatt

  https://www.netapp.com/us/media/ds-3213-en.pdf

- ONTAP 9 Dokumentationszentrum

  http://docs.netapp.com

- NetApp and Federal Information Processing Standard (FIPS) Veröffentlichung 140-2

  https://www.netapp.com/company/trust-center/compliance/fips-140-2/

- Cisco und FIPS 140-2 Compliance

  https://www.cisco.com/c/en/us/solutions/industries/government/global-government-certifications/fips-140.html

- NetApp Cryptographic Security Module

  https://csrc.nist.gov/csrc/media/projects/cryptographic-module-validation-program/documents/security-policies/140sp2648.pdf

- Cyber-Sicherheitsverfahren für mittelgroße und große Organisationen im Gesundheitswesen

  https://www.phe.gov/Preparedness/planning/405d/Documents/tech-vol2-508.pdf

- Cisco und Cryptographic Module Validation Program (CMVP)

  https://csrc.nist.gov/projects/cryptographic-module-validation-program/validated-modules/search?SearchMode=Basic&Vendor=cisco&CertificateStatus=Active&ValidationYear=0

- NetApp Storage Encryption, NVMe Self-Encrypting Drives, NetApp Volume Encryption und NetApp Aggregate Encryption

  https://www.netapp.com/pdf.html?item=/media/17073-ds-3898.pdf

- NetApp Volume Encryption und NetApp Aggregate Encryption

  https://www.netapp.com/pdf.html?item=/media/17070-ds-3899.pdf

- NetApp Storage Encryption

  https://www.netapp.com/pdf.html?item=/media/7563-ds-3213-en.pdf

- FlexPod für elektronische Krankenakten

  https://www.netapp.com/pdf.html?item=/media/22199-tr-4881.pdf

- Bild: Whitepaper „Data Now: Improving Performance in Epic EHR Environments with Cloud-Connected Flash Technology“

  https://www.netapp.com/media/10809-cloud-connected-flash-wp.pdf

- FlexPod Datacenter für Epic EHR-Infrastruktur

  https://www.netapp.com/pdf.html?item=/media/17061-ds-3683.pdf

- FlexPod Datacenter for Epic EHR Deployment Guide

  https://www.netapp.com/media/10658-tr-4693.pdf

- FlexPod-Datacenter-Infrastruktur für MEDITECH-Software

  https://www.netapp.com/media/8552-flexpod-for-meditech-software.pdf

- Der FlexPod-Standard gilt auch für MEDITECH Software

  https://blog.netapp.com/the-flexpod-standard-extends-to-meditech-software/
- FlexPod for MEDITECH Directional Sizing Guide

  https://www.netapp.com/pdf.html?item=/media/12429-tr4774.pdf
- FlexPod für medizinische Bildverarbeitung

  https://www.netapp.com/media/19793-tr-4865.pdf
- KI im Gesundheitswesen

  https://www.netapp.com/us/media/na-369.pdf
- FlexPod für das Gesundheitswesen vereinfachen den Wandel

  https://flexpod.com/solutions/verticals/healthcare/
- FlexPod von Cisco und NetApp

  https://flexpod.com/

Danksagungen

- Abhinav Singh, Technical Marketing Engineer, NetApp
- Brian O'Nahony, Solution Architect Healthcare (Epic), NetApp
- Brian Pruitt, Pursuit Business Development Manager, NetApp
- Arvind Ramakrishnan, Senior Solutions Architect, NetApp
- Michael Hommer, FlexPod Global Field CTO, NetApp

Versionsverlauf

Version	Datum	Versionsverlauf des Dokuments
Version 1.0	April 2021	Erste Version

Copyright-Informationen

Copyright © 2024 NetApp. Alle Rechte vorbehalten. Gedruckt in den USA. Dieses urheberrechtlich geschützte Dokument darf ohne die vorherige schriftliche Genehmigung des Urheberrechtsinhabers in keiner Form und durch keine Mittel – weder grafische noch elektronische oder mechanische, einschließlich Fotokopieren, Aufnehmen oder Speichern in einem elektronischen Abrufsystem – auch nicht in Teilen, vervielfältigt werden.

Software, die von urheberrechtlich geschütztem NetApp Material abgeleitet wird, unterliegt der folgenden Lizenz und dem folgenden Haftungsausschluss:

DIE VORLIEGENDE SOFTWARE WIRD IN DER VORLIEGENDEN FORM VON NETAPP ZUR VERFÜGUNG GESTELLT, D. H. OHNE JEGLICHE EXPLIZITE ODER IMPLIZITE GEWÄHRLEISTUNG, EINSCHLIESSLICH, JEDOCH NICHT BESCHRÄNKT AUF DIE STILLSCHWEIGENDE GEWÄHRLEISTUNG DER MARKTGÄNGIGKEIT UND EIGNUNG FÜR EINEN BESTIMMTEN ZWECK, DIE HIERMIT AUSGESCHLOSSEN WERDEN. NETAPP ÜBERNIMMT KEINERLEI HAFTUNG FÜR DIREKTE, INDIREKTE, ZUFÄLLIGE, BESONDERE, BEISPIELHAFTE SCHÄDEN ODER FOLGESCHÄDEN (EINSCHLIESSLICH, JEDOCH NICHT BESCHRÄNKT AUF DIE BESCHAFFUNG VON ERSATZWAREN ODER -DIENSTLEISTUNGEN, NUTZUNGS-, DATEN- ODER GEWINNVERLUSTE ODER UNTERBRECHUNG DES GESCHÄFTSBETRIEBS), UNABHÄNGIG DAVON, WIE SIE VERURSACHT WURDEN UND AUF WELCHER HAFTUNGSTHEORIE SIE BERUHEN, OB AUS VERTRAGLICH FESTGELEGTER HAFTUNG, VERSCHULDENSUNABHÄNGIGER HAFTUNG ODER DELIKTSHAFTUNG (EINSCHLIESSLICH FAHRLÄSSIGKEIT ODER AUF ANDEREM WEGE), DIE IN IRGENDEINER WEISE AUS DER NUTZUNG DIESER SOFTWARE RESULTIEREN, SELBST WENN AUF DIE MÖGLICHKEIT DERARTIGER SCHÄDEN HINGEWIESEN WURDE.

NetApp behält sich das Recht vor, die hierin beschriebenen Produkte jederzeit und ohne Vorankündigung zu ändern. NetApp übernimmt keine Verantwortung oder Haftung, die sich aus der Verwendung der hier beschriebenen Produkte ergibt, es sei denn, NetApp hat dem ausdrücklich in schriftlicher Form zugestimmt. Die Verwendung oder der Erwerb dieses Produkts stellt keine Lizenzierung im Rahmen eines Patentrechts, Markenrechts oder eines anderen Rechts an geistigem Eigentum von NetApp dar.

Das in diesem Dokument beschriebene Produkt kann durch ein oder mehrere US-amerikanische Patente, ausländische Patente oder anhängige Patentanmeldungen geschützt sein.

ERLÄUTERUNG ZU „RESTRICTED RIGHTS“: Nutzung, Vervielfältigung oder Offenlegung durch die US-Regierung unterliegt den Einschränkungen gemäß Unterabschnitt (b)(3) der Klausel „Rights in Technical Data – Noncommercial Items“ in DFARS 252.227-7013 (Februar 2014) und FAR 52.227-19 (Dezember 2007).

Die hierin enthaltenen Daten beziehen sich auf ein kommerzielles Produkt und/oder einen kommerziellen Service (wie in FAR 2.101 definiert) und sind Eigentum von NetApp, Inc. Alle technischen Daten und die Computersoftware von NetApp, die unter diesem Vertrag bereitgestellt werden, sind gewerblicher Natur und wurden ausschließlich unter Verwendung privater Mittel entwickelt. Die US-Regierung besitzt eine nicht ausschließliche, nicht übertragbare, nicht unterlizenzierbare, weltweite, limitierte unwiderrufliche Lizenz zur Nutzung der Daten nur in Verbindung mit und zur Unterstützung des Vertrags der US-Regierung, unter dem die Daten bereitgestellt wurden. Sofern in den vorliegenden Bedingungen nicht anders angegeben, dürfen die Daten ohne vorherige schriftliche Genehmigung von NetApp, Inc. nicht verwendet, offengelegt, vervielfältigt, geändert, aufgeführt oder angezeigt werden. Die Lizenzrechte der US-Regierung für das US-Verteidigungsministerium sind auf die in DFARS-Klausel 252.227-7015(b) (Februar 2014) genannten Rechte beschränkt.

Markeninformationen

NETAPP, das NETAPP Logo und die unter http://www.netapp.com/TM aufgeführten Marken sind Marken von NetApp, Inc. Andere Firmen und Produktnamen können Marken der jeweiligen Eigentümer sein.