Vorteile von Cisco HyperFlex Security

Sichern Sie Ihre gespeicherten Daten

- Verschlüsselung ruhender Daten mit selbstverschlüsselnden Laufwerken.
- Integration mit der Key-Management-Unternehmenssoftware für das Key Management
- Verwalten Sie Ihren gesamten Security-Lebenszyklus mit der Cisco HyperFlex™ Connect-Schnittstelle.

Erfüllung gesetzlicher Vorschriften

- Die Verschlüsselung ruhender Daten gewährleistet die Vertraulichkeit der Daten und damit die Einhaltung der Datenschutzbestimmungen.

Verwenden Sie eine sichere Plattform

- Wir führen kontinuierlich Schwachstellenanalysen durch, um Sie vor Bedrohungen zu schützen.
- Wir verstärken und warten jede Komponente im Rahmen unseres Produktentwicklungsprozesses.

Der Verlust sensibler Daten kann ein erhebliches Geschäftsrisiko darstellen. Wir helfen Ihnen, die Vertraulichkeit und Integrität Ihrer Daten zu wahren.

Sichern Sie Ihre gespeicherten Daten mithilfe einer einfachen Schnittstelle auf einem Cisco HyperFlex™-Cluster mit Verschlüsselung ruhender Daten. Unser richtlinienbasierter Sicherheitsansatz bietet Ihnen höchsten Schutz dank einheitlicher, konsistenter, konformer und sicherer Verschlüsselungsverwaltung und -bereitstellung in Ihrem gesamten Cluster.

Wenn Sie Ihre unternehmenskritischen Anwendungen auf Cisco HyperFlex-Systeme umstellen, bieten wir Ihnen einen ganzheitlichen Ansatz, der die Sicherheit tief in unsere Plattform integriert. Die Verschlüsselung ruhender Daten hilft Ihnen, Vorschriften einzuhalten, die die Verwendung von Best Practices beim Thema Sicherheit erfordern. Wir bieten Ihnen auch eine robuste Plattform, die auf einem sicheren Entwicklungslebenszyklus basiert und vor Schwachstellen und Bedrohungen schützt. All diese Funktionen zusammen machen Cisco HyperFlex-Systeme zu einer Wahl, der Sie bei Ihren wichtigsten Geschäftsanwendungen vertrauen können.

Sichern Sie Ihre gespeicherten Daten

Die Sicherheit ruhender Daten für Cisco HyperFlex-Knoten integriert die folgenden Komponenten, um Ihre Daten mit hoher Sicherheit zu schützen:

- Selbstverschlüsselnde Laufwerke (SEDs) bieten Verschlüsselung ohne Leistungseinbußen.
- Key Management für Unternehmen schützt Verschlüsselungscodes.
- Die Cisco HyperFlex Connect-Schnittstelle ermöglicht einfache Konfiguration und Verwaltung der Datensicherheit.

Hochwertige Sicherheitskomponenten

Am Anfang steht die Integration von selbstverschlüsselnden Festplatten (HDDs) und Solid-State-Disks (SSD) in jedem Knoten. Bei hardwarebeschleunigten kryptografischen Modulen im Datenstrom sind die Auswirkungen auf die Leistung bei der Übertragung von Daten zu und von den Laufwerken minimal. SEDs werden sowohl für Hybrid- (HDD und SSD-Laufwerk) als auch für All-Flash-Knoten unterstützt.

Ihre Daten sind nicht sicher, wenn Sie die Schlüssel unter der Fußmatte lassen. Deshalb bieten wir integrierte Unternehmenssysteme zum Key Management an. Ihre Verschlüsselungsschlüssel für Festplatten werden mit branchenführenden Key-Management-Lösungen geschützt, darunter:

- Gemalto SafeNet KeySecure
- Thales Vormetric Data Security Manager

Key-Management-Prozesse, die diese Lösungen einsetzen, sind in unsere Plattform integriert, um eine sichere, einfachere Verschlüsselung zu gewährleisten. Die Lösungen bieten auch Funktionen für Berichte, Compliance-Nachverfolgung und Audits. Das Cisco HyperFlex-System ist konform mit dem Key Management Interoperability Protocol (KMIP) 1.1, so dass andere kompatible Key-Management-Systeme in Zukunft problemlos qualifiziert werden können.

Sie können auch einen lokalen Schlüssel oder eine Passphrase verwenden, indem Sie eine in den Cisco UCS® Manager integrierte Option verwenden.

Vereinfachtes Management

Unabhängig davon, ob Sie Key-Management für Unternehmen oder lokale Schlüssel verwenden, wird der Workflow vollständig über die Cisco HyperFlex Connect-Schnittstelle gesteuert (Abbildung 1). Die intuitive HTML-5-Oberfläche erleichtert Aktivierung, Konfiguration, die Erstellung neuer Schlüssel und die sichere Löschung von Daten auf den SEDs in Ihrem Cluster.

Der Workflow schafft eine zertifikatsbasierte Vertrauenskette

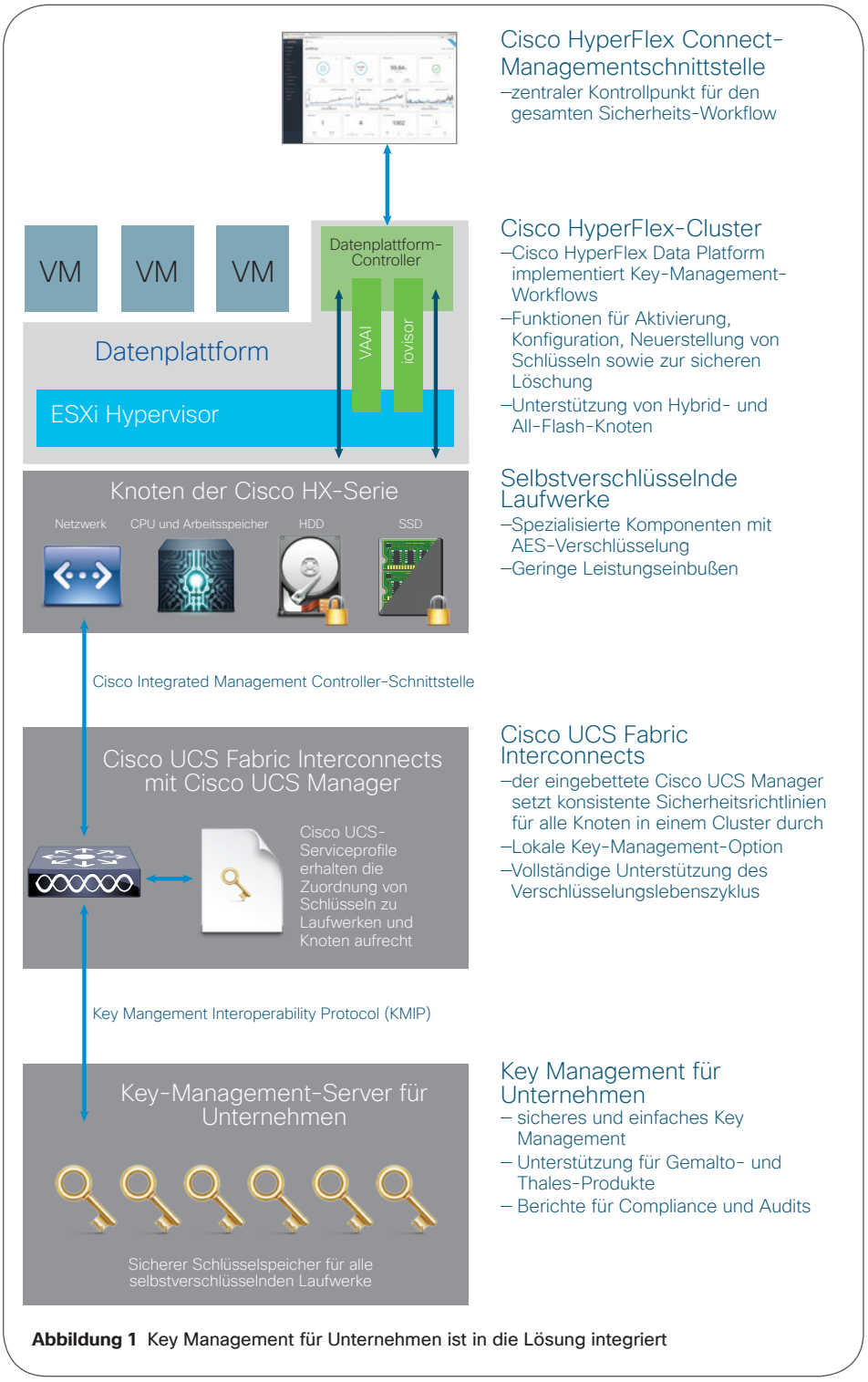

Abbildung 1 Key Management für Unternehmen ist in die Lösung integriert

Sichern Sie Ihre ruhenden Daten

- Verschlüsselung ruhender Daten mit selbstverschlüsselnden Laufwerken
- Integration mit der Key-Management-Unternehmenssoftware für das Key Management
- Verwaltung Ihres gesamten Sicherheitslebenszyklus mit der Cisco HyperFlex Connect-Schnittstelle

zwischen der Cisco HyperFlex HX Data Platform und dem Key-Management-Server. Über diese Verbindung können die Knoten die zur Freischaltung der Laufwerke erforderlichen Verschlüsselungscodes sicher übertragen

Betriebssicherheit

Unser Sicherheitsansatz legt Richtlinien fest und setzt sie durch, sodass Verschlüsselung und Key Management einheitlich und konsistent im gesamten Cluster eingesetzt werden. Mit diesem Ansatz brauchen Sie sich keine Sorgen mehr über inkonsistente Sicherheitspraktiken zu machen, die die Sicherheit beeinträchtigen könnten. Da die Implementierung von Richtlinien automatisiert ist, ist die Konfiguration auf allen Knoten und SEDs in einem Cluster wiederholbar.

Cisco UCS Manager verwendet Cisco Unified Computing System™ (Cisco UCS)-Serviceprofile, um die Interaktion zwischen Sicherheitsrichtlinien, der Datenplattform und der Key-Management-Software festzulegen. Mit diesen Profilen und den mehr als 100 Identitäts-, Konfigurations- und Konnektivitätsvariablen, die Cisco UCS Manager für jeden Server festlegt, ist eine konsistente und konforme Bereitstellung auf jedem Knoten gewährleistet. Dank der automatisierten Konfiguration und Bereitstellung lässt sich Ihr Cluster einfach und nahtlos um neue Knoten erweitern.

Erfüllung gesetzlicher Vorschriften

Datenschutz

Datenschutz ist für die Einhaltung gesetzlicher Vorschriften unerlässlich – und Verschlüsselung ermöglicht Datenschutz. Cisco HyperFlex-Systeme mit Verschlüsselung ruhender Daten helfen Ihnen dabei, viele branchenspezifische Vorschriften einzuhalten. Es gibt zahlreiche solche Regelungen, beispielsweise:

- Health Insurance Portability and Accountability Act (HIPAA)
- Payment Card Industry Data Security Standard (PCI-DSS)
- Federal Information Security Management Act (FISMA)
- Datenschutz-Grundverordnung (DSGVO)
- Sarbanes-Oxley Act

Mit der Cisco HyperFlex Connect-Managementschnittstelle können Sie die Verschlüsselung Ihrer ruhenden Daten einfach konfigurieren und den gesamten Sicherheitslebenszyklus verwalten. Cisco HyperFlex Connect nutzt die Leistungsfähigkeit der Cisco UCS-Serviceprofile, um die Konfigurations- und Sicherheitsmerkmale jedes Knotens festzulegen. Diese Funktion reduziert das Risiko von Konfigurationsveränderungen, die zu Ausfallzeiten und Sicherheitsschwachstellen führen können.

Zertifizierungen

Für die Sicherheit von Daten im Ruhezustand verwenden

Erfüllung gesetzlicher Vorschriften

- Die Verschlüsselung ruhender Daten trägt dazu bei, die Vertraulichkeit der Daten und die Einhaltung der Datenschutzbestimmungen zu gewährleisten.

Cisco HyperFlex-Systeme selbstverschlüsselnde Laufwerke und integrieren sich in Key-Management-Systeme des Unternehmens, die für FIPS 140-2 validiert sind.

Cisco HyperFlex-Systeme erhalten außerdem eine Zertifizierung für Common Criteria for Evaluation Assurance Level (EAL) 2 for Information Sicherheitsbewertung von Technologien Criteria (ITSEC).

Cisco verfügt im gesamten Unternehmen über umfangreiche Sicherheitskompetenz und unser Team für Global Certification and Common Security Modules hat einen innovativen Ansatz für die FIPS-Zertifizierung entwickelt. Die Gruppe hat ein kryptographisches Modul entwickelt, das bereits nach FIPS validiert ist und in eine Reihe von vertrauenswürdigen Cisco®-Produkten eingebettet werden kann. Der Compliance-Prozess verifiziert, dass das Produkt die Kryptographie normgerecht implementiert hat. Die Verwendung dieses Moduls durch Cisco HyperFlex Systems wurde einer Konformitätsprüfung unterzogen.

Verwenden Sie eine sichere Plattform

IT-Organisationen vertrauen auf Cisco-Sicherheit, weil wir sie zu einem integrierten Bestandteil des Software-Lebenszyklus gemacht haben. Sicherheit wird von Anfang an in die Produkte integriert und durch den von unseren Softwareentwicklungsteams implementierten sicheren Entwicklungslebenszyklus kontinuierlich verbessert und gestärkt.

Plattform-Verstärkung

Die gesamte Software, die in Cisco HyperFlex-Systeme integriert ist, hat eine erhebliche Verstärkung erfahren: Cisco UCS Manager, Cisco HyperFlex HX Data Platform und Hypervisor selbst.

Für die Verstärkung haben wir den Secure Technical Implementation Guide (STIG) genutzt und Empfehlungen aus Zertifizierungsstandards angewandt. So wurde beispielsweise das System durch die Implementierung von Cisco HyperFlex Best Practices und mehreren VMware ESX Server-Sicherheitsempfehlungen validiert.

Kontinuierliche Schwachstellenanalyse

Um die Sicherheit unserer verstärkten Systeme auf lange Sicht zu gewährleisten, führen wir regelmäßig eine Schwachstellenanalyse mit Nessus-Scans mit häufig aktualisierten Schwachstellen-Datenbanken durch.

Management-Sicherheit

Das Management Ihres Cisco HyperFlex-Systems ist von Anfang an sicher. Mit der Cisco HyperFlex Connect-Schnittstelle können Sie alle Aspekte Ihres Clusterbetriebs verwalten, einschließlich des End-to-End-Lebenszyklus der Verschlüsselung ruhender Daten. Die Cluster-Verwaltung wird durch die in vSphere Single Sign-On (SSO) integrierten Authentifizierungs- und Autorisierungsmechanismen Ihres Unternehmens gesichert, einschließlich Microsoft Active Directory und Lightweight Directory Access Protocol (LDAP).

Verwenden Sie eine sichere Plattform

- Wir führen kontinuierlich Schwachstellenanalysen durch, um Sie vor Bedrohungen zu schützen.
- Wir verstärken und warten jede Komponente im Rahmen unseres Produktentwicklungsprozesses.

Weitere Informationen

Weitere Informationen zu Cisco HyperFlex-Systemen finden Sie unter http://cisco.com/go/hyperflex.

Mit der rollenbasierten Zugriffskontrolle (RBAC) können Sie festlegen, welche Administratoren Konfigurationen ändern dürfen und welche lediglich Leserechte für Überwachungszwecke haben. Änderungen, die über die Cisco HyperFlex Connect-Schnittstelle, die Representational State Transfer (REST)-APIs oder die Kommandozeile (CLI) vorgenommen werden, werden überprüft, sodass nicht autorisierte Änderungen auf ihre Quellen zurückgeführt werden können.

Hinter den Managementschnittstellen implementiert der Cisco UCS Manager ein konsistentes Konfigurations- und Key-Management im gesamten Cluster.

Fazit

Cisco HyperFlex-Systeme sind bereit, Ihre Unternehmensanwendungen mit einem ganzheitlichen Sicherheitsansatz zu unterstützen:

- Sicherung ruhender Daten
- einfache Einhaltung von Datenschutzvorschriften
- Schutz vor aktiven Angriffen durch eine sichere Plattform

Die Sicherheit, die wir in Cisco HyperFlex-Systeme integriert haben, ist Teil einer langen Geschichte der Integration von Sicherheit in den Software-Lebenszyklus bei Cisco. Da die Sicherheit in den Lebenszyklus Ihres Cisco HyperFlex-Systems integriert ist, können auch Sie die Vorteile unserer langjährigen Spitzenposition beim Thema Sicherheit genießen.

LE-60301-00 07/17