IBM Guardium Key Lifecycle Manager

Zentralisieren, vereinfachen und automatisieren Sie die Verwaltung von Chiffrierschlüsseln.

Wesentliche Vorteile
Chiffrierschlüssel zentral verwalten

Profitieren Sie von einer starken Zugriffsverwaltung und -sicherheit bei gleichzeitiger Vereinfachung der Schlüsselkonfiguration und -verwaltung

Überwachen Sie den Zustand und Status verwalteter Endgerät-Zertifikate

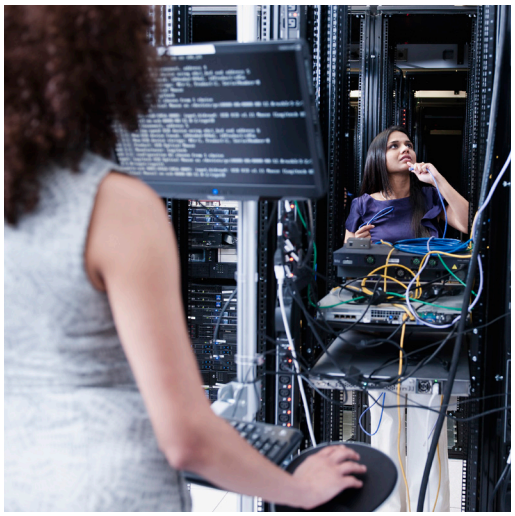
Beschleunigen Sie die Bereitstellung mit assistentenbasierter Unterstützung

Die Zahl der Geschäftsdaten wächst rasant und treibt die Nachfrage nach dem Schutz von Daten On-Premises und in der Cloud in die Höhe. Unternehmen reagieren darauf, indem sie die Verschlüsselung auf verschiedenen Ebenen implementieren – in der Hardware, in Dateien und in Anwendungen – was zu Verschlüsselungssilos mit unstimmigen Ansätzen bei der Verwaltung von Chiffrierschlüsseln führen kann. In einigen Fällen gibt es keinen formellen Schlüsselverwaltungsprozess.

Unabhängig davon, ob die Strategie der Schlüsselverwaltung fragmentiert oder nicht vorhanden ist, besteht die Gefahr, dass Unternehmen die Kontrolle über ihre Daten verlieren. In einer solchen Situation ist eine Lösung erforderlich, die sich in andere Schlüsselverwaltungen und eigenständig verschlüsselnde Geräte integrieren lässt, die Standardprotokolle verwenden, um das Lebenszyklusmanagement des Verschlüsselungscodes zu zentralisieren.

Der IBM® Guardium Key Lifecycle Manager bietet eine optimierte Chiffrierschlüsselverwaltung und Unterstützung für Ihre vielfältigen Anforderungen an den Schlüssellebenszyklus in Form einer einfachen Lösung für das komplexe Problem der Verwaltung von Chiffrierschlüsseln. Chiffrierschlüssel haben ihren ganz eigenen Lebenszyklus, der unabhängig von den dadurch geschützten Daten anzusehen ist. Der Guardium Key Lifecycle Manager unterstützt Sie bei der Steuerung von Lebenszyklusprozessen des Codes – von der Initialisierung und Aktivierung bis hin zur Rotation und Löschung. Die Lösung hilft Ihnen, manuelle Aufgaben zu vereinfachen und zu automatisieren, wodurch die Betriebskosten gesenkt werden können.

Da immer mehr Daten in verschiedenen oder hybriden Speicherumgebungen gespeichert werden, steigt das Risiko von Datenverlust oder -kompromittierung. Um diese Risiken zu reduzieren, sollten die Daten so verschlüsselt werden, dass das Unternehmen die Schlüssel kontrolliert. Der Guardium Key Lifecycle Manager trägt dazu bei, dass vertrauliche Informationen geschützt sind, falls verschlüsselte Datenspeicher verlegt, missbraucht oder gestohlen werden.



Zentrale Verwaltung von Chiffrierschlüsseln
Der Guardium Key Lifecycle Manager stellt Schlüssel zum Zeitpunkt der Verwendung von einem geschützten, zentralen Ort aus bereit, an dem wichtige Materialien gespeichert sind. Diese Funktion wird durch die Unterstützung proprietärer und international standardisierter Protokolle zur Bereitstellung symmetrischer und asymmetrischer Schlüssel ermöglicht. Zu den unterstützten Protokollen gehören das Key Management Interoperability Protocol (KMIP v3.0), das IBM Proprietary Protocol (IPP) und der Representational State Transfer (REST), mit denen der Guardium Key Lifecycle Manager Chiffrierschlüsseln für IBM und nicht-IBM Lösungen verwalten kann. Für Unternehmen, die eine zentralisierte Kontrolle und richtliniengesteuerte Schlüsselverwaltung wünschen, bietet der Guardium Key Lifecycle Manager eine konsolidierte Verwaltung von Schlüsseln über Domains hinweg und lässt sich gut in die meisten bestehenden Methoden des Sicherheitsteams integrieren.

Der Guardium Key Lifecycle Manager bietet Unterstützung für die Chiffrierschlüssel einer Vielzahl von Lösungen. Weitere Informationen finden Sie auf dieser Seite.

Profitieren Sie von einer starken Zugriffsverwaltung und -sicherheit bei gleichzeitiger Vereinfachung der Schlüsselkonfiguration und -verwaltung
Der Guardium Key Lifecycle Manager ermöglicht es Unternehmen, zu definieren, welche Administratoren Verwahrungsaktionen für Schlüssel ausführen können. Er kann zudem Berechtigungen auf die Funktionen beschränken, die Benutzer zum Ausführen ihrer Aufgaben benötigen. Mit diesen rollenbasierten Zugriffssteuerungsfunktionen können Sie Aufgaben trennen, indem Sie Berechtigungen für Aktionen zuordnen, die für Objekte ausgeführt werden, und Datenisolation und -sicherheit erzwingen. Autorisierte Benutzer können Geräte auch in separaten Domains gruppieren. Standardmäßig haben die Gerätegruppen nur Zugriff auf die Verschlüsselungscodes, die in ihrer Gruppe definiert sind.

Vor der Verwaltung der Chiffrierschlüssel wird jedes Gerät in der Lösung registriert. Jedes Mal, wenn ein Verschlüsselungsgerät wieder eine Verbindung herstellt, um einen Schlüssel anzufordern, überprüft der Guardium Key Lifecycle Manager seine Identität und authentifiziert es kryptografisch anhand des Identifizierungszertifikats des Geräts. Jedes unbekannte Gerät wird entweder abgelehnt oder in eine Warteschlange gestellt, um vom Administrator genehmigt zu werden. Mit dieser Strategie ist es viel unwahrscheinlicher, dass ein nicht autorisiertes Gerät im Netzwerk bereitgestellt und zum Abfangen von Schlüsseln verwendet wird.

Neben der starken Authentifizierung gibt es auch eine erhöhte Sicherheit zwischen dem Datenverschlüsselungsgerät und dem Guardium Key Lifecycle Manager. Temporäre Sitzungsschlüssel werden verwendet, um Chiffrierschlüssel sowie den gesamten Datenverkehr zum Gerät zu verschlüsseln. Dieser Ansatz zur Verschlüsselung trägt dazu bei, die Datensicherheit zu verbessern und gleichzeitig die Schlüsselverwaltung zu vereinfachen. Die Auswirkungen auf die Leistung sind minimal, da jede Verschlüsselungslösung kryptografische Aufgaben ausführt, anstatt über das Netzwerk zu greifen.

Der IBM Guardium Key Lifecycle Manager bietet eine benutzerfreundliche, webbasierte GUI, die die Konfiguration und Verwaltung von Schlüsseln vereinfacht.

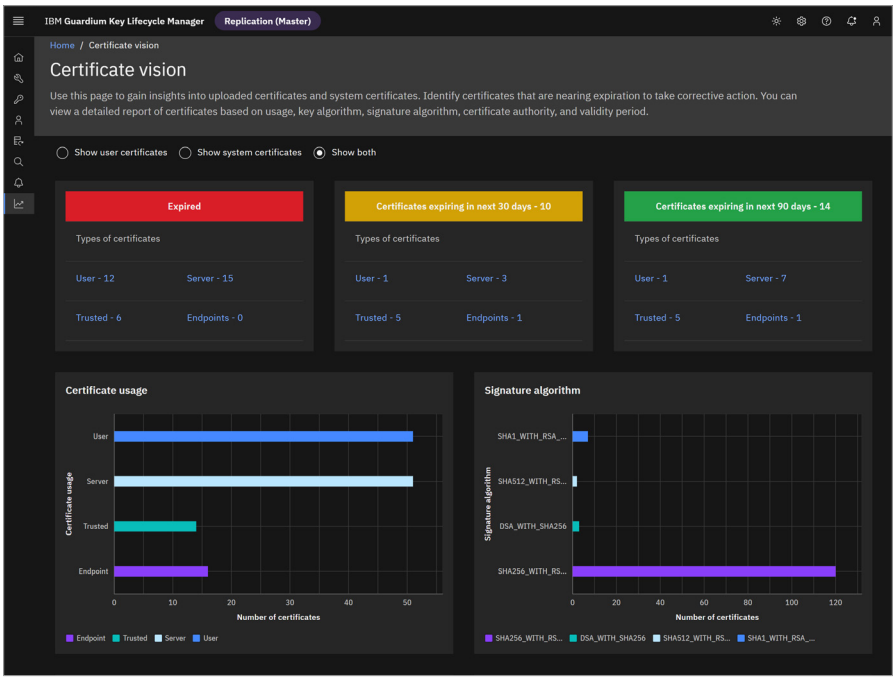
Um sicherzustellen, dass der autorisierte Zugriff auf geschützte Daten nicht unterbrochen wird, bietet der Guardium Key Lifecycle Manager zwei Methoden für Redundanz und Hochverfügbarkeit. Die Master-Clone-Konfiguration der Lösung ermöglicht es Benutzern, bis zu 20 Backup-Kopien des Schlüsselmanagers mit Schlüsseln für jedes angeschlossene Endgerät bereitzustellen. Die Multimaster-Konfiguration ermöglicht nahezu in Echtzeit die Synchronisierung von bis zu 21 Instanzen über Rechenzentren und Umgebungen hinweg.

Während die Kryptografie im Guardium Key Lifecycle Manager nach FIPS 140-3 Level 1 validiert ist, haben Benutzer auch die Möglichkeit, FIPS 140-3 Level 2- oder Level 3-validierte Hardware zu verwenden, um die Schlüsselsicherheit zu erhöhen. Der Guardium Key Lifecycle Manager kann mit einem optionalen Hardware Security Module (HSM) bereitgestellt werden, um den Hauptschlüssel zu speichern und so alle Schlüssel zu schützen, die im Guardium Key Lifecycle Manager gespeichert sind. Diese Funktion kann sowohl für Installationen mit vorhandenen Daten als auch für Neuinstallationen des Guardium Key Lifecycle Managers aktiviert werden.

Der Guardium Key Lifecycle Manager verfügt über eine moderne, intuitive Benutzeroberfläche, die auf dem IBM Carbon Design System basiert. Der Fokus des Designs liegt auf der Verbesserung von Navigation und Datenvisualisierung und der Verschlankung der Aufgaben der Schlüsselverwaltung.

Nach der Installation ermöglicht die GUI Administratoren die Durchführung eines grundlegenden Lebenszyklusmanagements für lokale Schlüssel und bietet nicht nur Konfigurations- und Einrichtungstools, sondern auch Audit- und Compliance-Unterstützung. Die Software bietet drei Möglichkeiten, verschlüsselungsfähige Geräte hinzuzufügen: automatische Annahme eingehender Geräte, Genehmigung von Geräten, bei denen Administratoren aus einer ausstehenden Geräteliste auswählen und akzeptieren müssen, oder manuelles Hinzufügen von Geräten für zusätzliche Sicherheit.

Der Guardium Key Lifecycle Manager bietet ebenfalls zahlreiche Methoden für die Sicherung und Wiederherstellung von Schlüsseln im Falle eines schwerwiegenden Ausfalls. Administratoren können Regeln für den automatischen Rollover von Schlüsselgruppen konfigurieren, sodass neue Chiffrierschlüssel automatisch nach einem konfigurierbaren Zeitplan verwendet werden. Auf diese Weise haben Administratoren die Möglichkeit, die Menge der mit bestimmten Schlüsseln verschlüsselten Daten zu begrenzen, die Gefährdung zu minimieren, wenn ein Schlüssel kompromittiert wird, und die kryptografische Löschung von Daten durchzuführen, indem sie relevante Schlüssel löschen, wenn Daten ablaufen. Diese automatisierte Schlüsselzuweisung befreit Betriebsteams von der Notwendigkeit, ständig mit der Schlüsselverwaltung interagieren zu müssen.



Überwachen des Zustands und des Status von verwalteten Endgerät-Zertifikaten
Abgelaufene digitale Zertifikate können die Stabilität eines Netzwerks beeinträchtigen, und eine schlechte Zertifikatswartung kann Unternehmen Sicherheitsrisiken wie einem Man-in-the-Middle-Angriff aussetzen. Um sich vor diesen Szenarien zu schützen, bietet das Guardium Key Lifecycle Manager Certificate Vision Dashboard Benutzern eine Momentaufnahme des Status und des Ablaufstatus ihrer Endgerät-Zertifikate. Dieses Dashboard trägt dazu bei, Sicherheitslücken zu reduzieren und potenzielle Netzwerkunterbrechungen zu vermeiden. Anwender können leicht erkennen, welche Zertifikate aktualisiert und erneuert werden müssen. Anschließend können diese Aktivitäten mit einem externen Tool zur Verwaltung des Zertifikatlebenszyklus ausgeführt werden.

Beschleunigen Sie die Bereitstellung mit assistentenbasierter Unterstützung
Der Guardium Key Lifecycle Manager verwendet einen assistentenbasierten Leitfaden, um Administratoren bei der Navigation durch eine Reihe einfacher, aufgabenbasierter Bildschirme zu unterstützen, die die Erstellung von Schlüsseln und Geräten sowie den Umgang mit neuen Geräteanforderungen demonstrieren. Administratoren können darüber hinaus verschiedene Geräte so konfigurieren, dass sie bestimmte Kommunikationsprotokolle wie KMIP verwenden.

Nach der Registrierung erscheinen Verschlüsselungsgeräte im Bereich Schlüsselverwaltung des Guardium Key Lifecycle Manager und stehen als hochsicheres Endgerät für den Einsatz bereit. Die mit den Geräten verknüpften Schlüssel können dann über die GUI verwaltet werden, einschließlich des Aktualisierens, Ablaufens oder Löschens der Schlüssel. Die Startseite für die Schlüsselverwaltung des Guardium Key Lifecycle Managers bietet Administratoren entscheidende Hinweise, einschließlich Informationen über das letzte Backup und verfügbare Protokolle.

Fazit

Der IBM Guardium Key Lifecycle Manager ist eine Anwendung, die auf einer Vielzahl von Betriebssystemen bereitgestellt werden kann, darunter Windows, Unix, Linux, Container-Plattformen und IBM Mainframe. Für den Entwurf und die Architektur der Anwendung sind keine umfangreichen RAM- oder Verarbeitungsressourcen erforderlich. Tatsächlich kann die Lösung in der Regel mit nur 8 GB RAM und einem Dual-Core-Prozessor bereitgestellt werden.

Dank des geringen Speicher- und Platzbedarfs kann die Anwendung als Virtual Machine bereitgestellt werden, die in einem Container wie Red Hat OpenShift, Kubernetes oder zCX oder auf Bare Metal ausgeführt werden kann. Diese Vielseitigkeit ermöglicht es Unternehmen, mehrere Instanzen der Lösung einfach zu verwalten, um Redundanz und Hochverfügbarkeit zu gewährleisten oder sich an die Organisationsstruktur anzupassen. Weitere Informationen zu den technischen Anforderungen finden Sie auf dieser Seite.

Mehr erfahren

Erfahren Sie, wie Sie mit IBM Guardium Lösungen einen intelligenteren, integrierten Ansatz zum Schutz kritischer Daten in Ihren hybriden Multicloud-Umgebungen verfolgen können. Besuchen Sie ibm.com/de-de/guardium.

Um mehr über den IBM Guardium Key Lifecycle Manager zu erfahren, wenden Sie sich bitte an Ihren IBM Ansprechpartner oder IBM Geschäftspartner oder besuchen Sie ibm.com/de-de/products/guardium-key-lifecycle-manager.

© Copyright IBM Corporation 2024

IBM Deutschland GmbH
IBM-Allee 1
71139 Ehningen
ibm.com/de
IBM Corporation
New Orchard Road
Armonk, NY 10504

Erstellt in den
Vereinigten Staaten von Amerika
Dezember 2024

IBM, das IBM Logo, Guardium und X-Force sind Marken oder eingetragene Marken der International Business Machines Corporation in den Vereinigten Staaten und/oder anderen Ländern. Weitere Produkt- und Servicenamen sind möglicherweise Marken von IBM oder anderen Unternehmen. Eine aktuelle Liste der Marken von IBM finden Sie unter ibm.com/de-de/trademark.

Die eingetragene Marke Linux wird im Rahmen einer Unterlizenz der Linux Foundation verwendet, dem exklusiven Lizenznehmer von Linus Torvalds, dem Inhaber der Marke aufweltweiter Basis.

Microsoft und Windows sind Marken der Microsoft Corporation in den USA und/oder anderen Ländern.

Red Hat und OpenShift sind Marken von Red Hat, Inc. oder deren Tochtergesellschaften in den Vereinigten Staaten und anderen Ländern.

UNIX ist eine eingetragene Marke von The Open Group in den Vereinigten Staaten und anderen Ländern.

Das vorliegende Dokument ist ab dem Datum der Erstveröffentlichung aktuell und kann jederzeit von IBM geändert werden. Nicht alle Angebote sind in allen Ländern verfügbar, in denen IBM tätig ist.

DIE INFORMATIONEN IN DIESEM DOKUMENT WERDEN OHNE JEGLICHE AUSDRÜCKLICHE ODER STILLSCHWEIGENDE GARANTIE ZUR VERFÜGUNG GESTELLT, EINSCHLIESSLICH DER GARANTIE DER MARKTGÄNGIGKEIT, DER EIGNUNG FÜR EINEN BESTIMMTEN ZWECK UND DER GARANTIE ODER BEDINGUNG DER NICHTVERLETZUNG VON RECHTEN.

Die Garantie für Produkte von IBM richtet sich nach den Geschäftsbedingungen der Vereinbarungen, unter denen sie bereitgestellt werden.

Erklärung zu bewährten Sicherheitsverfahren: Kein IT-System oder -Produkt sollte als vollkommen sicher angesehen werden, und kein einzelnes Produkt, kein Service und keine Sicherheitsmaßnahme kann eine missbräuchliche Nutzung oder einen missbräuchlichen Zugriff vollständig verhindern. IBM übernimmt keine Gewähr dafür, dass Systeme, Produkte oder Services vor böswilligem oder rechtswidrigem Verhalten von Dritten geschützt sind oder Ihr Unternehmen davor schützen.

Die Einhaltung sämtlicher geltender Gesetze und Vorschriften liegt in der Verantwortung des Kunden. IBM bietet keine Rechtsberatung an und gewährleistet nicht, dass die Services oder Produkte von IBM die Konformität von Gesetzen oder Verordnungen durch den Kunden sicherstellen.