# IBM Guardium Key Lifecycle Manager

## تحقيق المركزية في إدارة مفاتيح التشفير وتبسيطها وأتمتتها

**أهم المميزات**

إدارة مفاتيح التشفير مركزيًا

الحصول على إدارة وصول قوية وأمن فعَّال مع تبسيط تكوين المفاتيح وإدارتها

مراقبة سلامة وحالة شهادات نقاط النهاية المُدارة

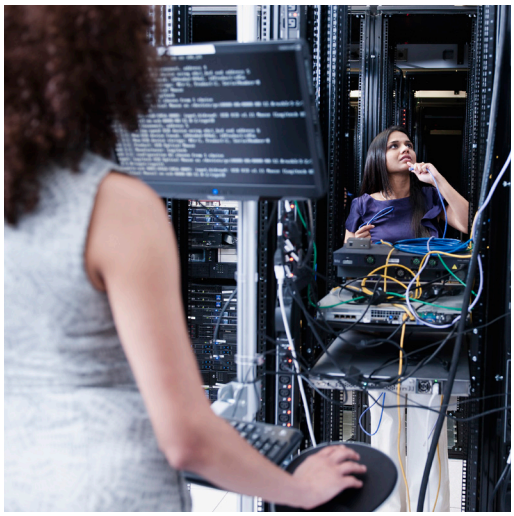
تسريع عملية النشر من خلال المساعدة القائمة على معالج الإرشادات

تنمو بيانات الأعمال بمعدلات هائلة، مما يعني زيادة الطلب على حماية البيانات في البيئات المحلية والسحابية. تستجيب المؤسسات من خلال تطبيق التشفير على مستويات مختلفة -على الأجهزة، والملفات، والتطبيقات- وقد يؤدي ذلك إلى ظهور صوامع تشفير وتباين في أساليب إدارة مفاتيح التشفير. في بعض الحالات، لا توجد عملية رسمية لإدارة المفاتيح.

إذا كانت استراتيجية إدارة مفاتيح التشفير مقسمة إلى أجزاء مختلفة أو كانت غير موجودة أصلًا، فستواجه المؤسسات خطر فقدان التحكم في بياناتها. وتتطلب هذه الحالات حلًا يمكنه التكامل مع مديري مفاتيح التشفير الآخرين والأجهزة ذاتية التشفير باستخدام بروتوكولات قياسية لتوحيد إدارة دورة حياة مفاتيح التشفير.

يقدِّم تطبيق IBM Guardium Key Lifecycle Manager إدارة مبسطة لمفاتيح التشفير ودعمًا لاحتياجات دورة حياة مفاتيح التشفير المتنوعة من خلال توفير حل بسيط للمشكلات المعقدة المتعلقة بإدارة مفاتيح التشفير. تتميز مفاتيح التشفير بدورات حياة خاصة بها مستقلة عن البيانات التي تحميها. يساعدك تطبيق Guardium Key Lifecycle Manager على التحكم في عمليات دورة حياة المفاتيح بدءًا من التهيئة والتفعيل وحتى التدوير، ووصولًا إلى الحذف. يساعدك الحل على تبسيط المهام اليدوية وأتمتتها، ما يُسهم في خفض التكاليف التشغيلية.

مع تزايد تخزين المزيد من البيانات في بيئات التخزين المتنوعة أو بيئات التخزين الهجين، تزداد مخاطر فقدان البيانات أو تعرضها للاختراق. ولتقليل هذه المخاطر، يجب تشفير البيانات مع تمكين المؤسسة من التحكم في المفاتيح. يساعد Guardium Key Lifecycle Manager على ضمان حماية المعلومات الحساسة في حال تعرُّض مخازن البيانات المشفرة للفقدان أو الإساءة أو السرقة.



**إدارة مفاتيح التشفير مركزيًا**

يقدِّم Guardium Key Lifecycle Manager مفاتيح التشفير عندما يحين وقت استخدامها، ويوفرها من موقع مركزي محمي يخزِّن البيانات السرية الخاصة بكل مفتاح. وينجح في تمكين هذه القدرة بفضل دعمه للبروتوكولات الخاصة والمعايير الدولية لإدارة المفاتيح المتماثلة وغير المتماثلة. وتشمل البروتوكولات المدعومة بروتوكول التوافق بين إدارة المفاتيح (KMIP v3.0)، وبروتوكول الملكية من IBM (اختصارًا IPP)، وبروتوكول نقل الحالة التمثيلية (REST)، مما يسمح لبرنامج Guardium Key Lifecycle Manager بإدارة مفاتيح التشفير للحلول التابعة لشركة IBM والحلول غير التابعة لها. أما المؤسسات التي ترغب في تحقيق تحكم مركزي وإدارة مفاتيح معتمدة على السياسات، فيقدِّم Guardium Key Lifecycle Manager إدارة موحَّدة للمفاتيح بين النطاقات ويتكامل جيدًا مع معظم منهجيات فِرَق الأمن الحالية.

يوفر تطبيق Guardium Key Lifecycle Manager دعم مفاتيح التشفير لمجموعة كبيرة من الحلول. راجع هذه الصفحة لمزيد من المعلومات.

**الحصول على إدارة وصول قوية وأمن فعَّال مع تبسيط تكوين المفاتيح وإدارتها**

يُتيح تطبيق Guardium Key Lifecycle Manager للمؤسسات تحديد المسؤولين الذين يمكنهم تنفيذ الإجراءات المتعلقة بالمفاتيح. كما يمكنه تقييد الأذونات لتقتصر فقط على الوظائف التي يحتاج المستخدمون إلى أدائها في وظائفهم. وتوفر ميزات التحكم في الوصول حسب هذه الأدوار إمكانية فصل المهام من خلال تعيين الأذونات للإجراءات التي يتم تنفيذها على الكائنات وفرض عزل البيانات وتحقيق الأمن. كما يمكن للمستخدمين المصرَّح لهم أيضًا تجميع الأجهزة في نطاقات منفصلة. ووفقًا للإعدادات الافتراضية، تكون مجموعات الأجهزة هذه قادرة على الوصول إلى مفاتيح التشفير المحددة داخل مجموعتها فقط.

يتم تسجيل كل جهاز في النظام قبل إدارة مفاتيح التشفير الخاصة به. في كل مرة يُعيد فيها جهاز تشفير الاتصال لطلب مفتاح، يعمل Guardium Key Lifecycle Manager على التحقق من هويته ومصادقته تشفيريًا باستخدام شهادة التعريف الخاصة بكل جهاز. يتم رفض أي جهاز غير معروف أو وضعه في قائمة انتظار حتى يوافق عليه المسؤول. ومن خلال هذه الاستراتيجية، تقل بدرجة كبيرة احتمالية نشر جهاز مريب على الشبكة ومنع استخدامه في إيقاف عمل مفاتيح التشفير.

علاوةً على المصادقة القوية، يتوفر أيضًا أمن معزز بين جهاز تشفير البيانات وبين تطبيق Guardium Key Lifecycle Manager. يتم استخدام مفاتيح الجلسة المؤقتة لتشفير مفتاح التشفير وجميع البيانات إلى الجهاز. ويساعد هذا النهج في التشفير على تحسين أمن البيانات مع تبسيط إدارة المفاتيح. ويكون تأثير ذلك على الأداء محدودًا للغاية لأن كل حل تشفير يؤدي مهام تشفيرية بدلًا من الاعتماد على الشبكة.

يوفر تطبيق IBM Guardium Key Lifecycle Manager واجهة مستخدم رسومية سهلة الاستخدام وقائمة على الويب تساعد على تبسيط مهام تكوين إعدادات مفاتيح التشفير وإدارتها.

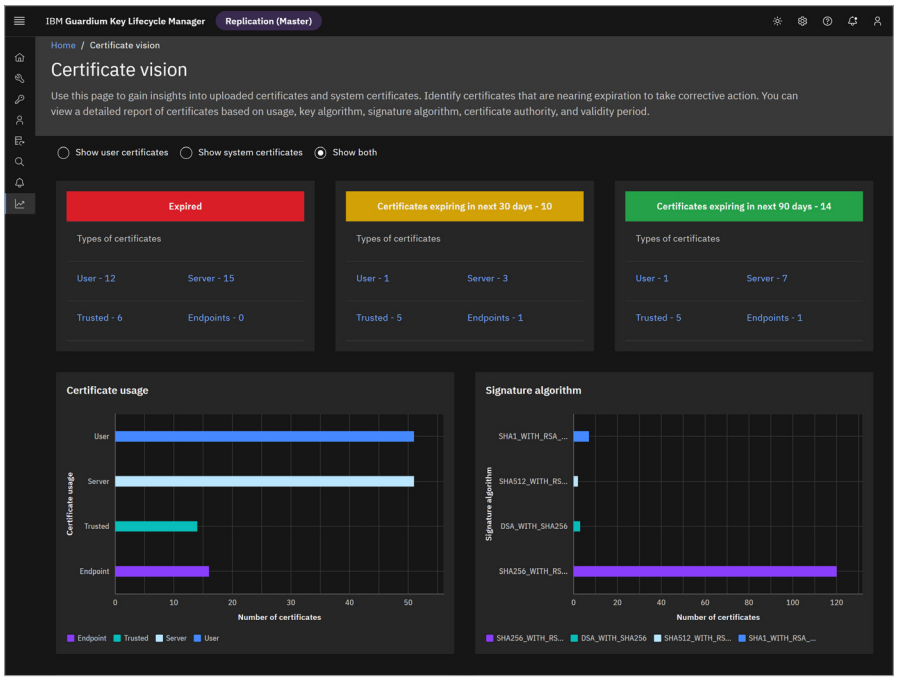
لضمان عدم انقطاع الوصول المصرَّح به إلى البيانات المحمية، يوفر تطبيق Guardium Key Lifecycle Manager طريقتين للتكرار الاحتياطي والتوفر العالي. يُتيح تكوين النسخ الرئيسي، المتوفر في هذا الحل/ للمستخدمين نشر ما يصل إلى 20 نسخة احتياطية من مدير مفاتيح التشفير الذي يمكنه تقديم المفاتيح لأي نقطة نهاية متصلة. ويوفر التكوين متعدد النسخ مزامنة شبه حقيقية لما يصل إلى 21 مثيلًا في مختلف مراكز البيانات والبيئات.

بينما يجري التحقق من التشفير داخل Guardium Key Lifecycle Manager وفقًا لمعيار FIPS 140-3 المستوى 1، يمكن للمستخدمين أيضًا استخدام الأجهزة التي تم التحقق من مطابقتها لمعيار FIPS 140-3 المستوى 2 أو المستوى 3 لتعزيز أمن مفاتيح التشفير. يمكن نشر Guardium Key Lifecycle Manager باستخدام وحدة أمن أجهزة (HSM) اختيارية لتخزين مفتاح التشفير الرئيسي، مما يضمن حماية جميع المفاتيح المخزنة فيه. ويمكن تفعيل هذه الميزة لعمليات التثبيت التي تحتوي على بيانات حالية أو لعمليات التثبيت الجديدة لتطبيق Guardium Key Lifecycle Manager.

يتميز تطبيق Guardium Key Lifecycle Manager بواجهة مستخدم حديثة وبديهية تعتمد على نظام تصميم البرامج IBM Carbon Design System. ويركِّز هذا التصميم على تحسين التصفح وتحسين العرض المصور للبيانات وتبسيط مهام إدارة المفاتيح.

بمجرد التثبيت، تُتيح واجهة المستخدم الرسومية للمسؤولين إدارة دورة حياة مفاتيح التشفير المحلية الأساسية، ولا تقتصر على توفير أدوات التكوين والإعداد فحسب، بل توفر أيضًا دعم التدقيق والامتثال. يوفر البرنامج ثلاث طرق لإضافة الأجهزة التي تدعم التشفير: القبول التلقائي للأجهزة الواردة، أو الموافقة على الأجهزة حيث يُطلب من المسؤولين اختيار الأجهزة من قائمة الأجهزة المعلّقة وقبولها، أو الإضافة اليدوية للأجهزة لمزيد من الأمان.

يقدِّم تطبيق Guardium Key Lifecycle Manager أيضًا العديد من الطرق لنسخ المفاتيح احتياطيًا واستعادتها في حالة حدوث فشل كارثي. ويمكن للمسؤولين تكوين قواعد لأتمتة تدوير مجموعات المفاتيح ليتم استخدام مفاتيح تشفير جديدة تلقائيًا وفقًا لجدول قابل للتكوين. وبهذه الطريقة، يمكن للمسؤولين تحديد كمية البيانات المشفرة باستخدام مفاتيح معينة، وتقليل التعرض للخطر عند اختراق مفتاح، وتنفيذ الحذف التشفيري للبيانات من خلال حذف المفاتيح ذات الصلة عند اقتراب انتهاء صلاحية البيانات. وهذا التعيين التلقائي للمفاتيح يُعفي فريق العمليات من ضرورة التفاعل بشكل متكرر مع إدارة المفاتيح.




### مراقبة سلامة وحالة شهادات نقاط النهاية المُدارة

قد تتسبب الشهادات الرقمية منتهية الصلاحية في تدمير استقرار الشبكة، ولا شك أن ضعف صيانة الشهادات قد يؤدي إلى فتح الباب أمام المخاطر الأمنية مثل هجوم "الوسيط". وللحماية من هذه السيناريوهات، توفر لوحة المعلومات الخاصة برؤية الشهادات في تطبيق Guardium Key Lifecycle Manager للمستخدمين نظرة عامة عن سلامة وحالة انتهاء صلاحية شهادات نقاط النهاية الخاصة بهم. كما تساعد لوحة المعلومات هذه على تقليل الثغرات الأمنية وتجنب الاضطرابات المحتملة في الشبكة. حيث يمكن للمستخدمين بسهولة تحديد الشهادات التي تحتاج إلى تحديث أو تصحيح، ثم تنفيذ هذه الأنشطة باستخدام أداة خارجية لإدارة دورة حياة الشهادات.

### تسريع عملية النشر من خلال المساعدة بمعالج الإرشادات

يستخدم Guardium Key Lifecycle Manager دليلًا قائمًا على المساعدة بمعالج الإرشادات لمساعدة المسؤولين على التنقل عبر سلسلة من الشاشات البسيطة المستندة إلى المهام التي تعرض إنشاء المفاتيح والأجهزة ومعالجة طلبات الأجهزة الجديدة. كما يمكن للمسؤولين تكوين إعدادات أجهزة مختلفة لاستخدام بروتوكولات الاتصال المحددة مثل KMIP.

بمجرد التسجيل، تظهر أجهزة التشفير في قسم إدارة مفاتيح التشفير في Guardium Key Lifecycle Manager وتصبح جاهزة للاستخدام كنقطة نهاية آمنة للغاية. ثم يمكن بعد ذلك إدارة المفاتيح المرتبطة بالأجهزة عبر واجهة المستخدم الرسومية، بما في ذلك تحديث مفاتيح التشفير أو إنهاء صلاحيتها أو تدميرها. توفر صفحة الترحيب الخاصة بإدارة مفاتيح التشفير في Guardium Key Lifecycle Manager إشعارات مهمة للمسؤولين، تشمل معلومات عن آخر النسخ الاحتياطية والبروتوكولات المتاحة.

## الخاتمة

يُعَد IBM Guardium Key Lifecycle Manager تطبيقًا قابلاً للنشر على مجموعة متنوعة من أنظمة التشغيل تشمل Windows وUnix وLinux ومنصات الحاويات وأجهزة الكمبيوتر المركزي من IBM. ولا يتطلب تصميم التطبيق وبنيته موارد كبيرة من الذاكرة العشوائية أو المعالجة. وفي الواقع، يمكن نشر هذا الحل عادةً بمتطلبات لا تتجاوز 8 جيجابايت من الذاكرة العشوائية ومعالج ثنائي النواة.

بفضل صغر حجم التطبيق، يمكن نشره كجهاز افتراضي، بحيث يكون جاهزًا للعمل في حاوية مثل Red® Hat® OpenShift أو Kubernetes أو zCX أو على أجهزة تعمل دون نظام تشغيل. ومثل هذه المرونة تُتيح للمؤسسات إدارة العديد من النسخ من الحل لضمان التكرار الاحتياطي والتوفر العالي ولكي تتناسب مع الهيكل التنظيمي.اطَّلِع على هذه الصفحة لمزيد من التفاصيل حول المتطلبات الفنية.

## لمزيد من المعلومات

اكتشف كيفية الاستفادة من حلول IBM Guardium لمساعدتك على اتخاذ نهج أذكى وأكثر تكاملًا لحماية بياناتك الحساسة في بيئات السحابة المتعددة الهجينة لديك. تفضَّل بزيارة الموقع ibm.com/ae-ar/guardium.

لمعرفة المزيد عن تطبيق IBM Guardium Key Lifecycle Manager، يُرجى التواصل مع ممثل IBM أو شريك أعمال IBM، أو زيارة الموقع ibm.com/ae-ar/products/guardium-key-lifecycle-manager.

© حقوق النشر محفوظة لشركة IBM Corporation لعام 2024

أُنتج في
الولايات المتحدة الأمريكية
في ديسمبر 2024

يُعَد كل من IBM وشعار IBM وGuardium وX-Force علامات تجارية أو علامات تجارية مسجلة لشركة International Business Machines Corporation، في الولايات المتحدة و/أو دول أخرى. قد تكون أسماء المنتجات والخدمات الأخرى علامات تجارية تابعة لشركة IBM أو شركات أخرى. توجد قائمة حديثة بالعلامات التجارية الخاصة بشركة IBM على هذا الرابط: ibm.com/ae-ar/trademark.

تُستخدم العلامة التجارية المسجَّلة Linux بموجب ترخيص فرعي من Linux Foundation، المرخص الحصري من Linus Torvalds، مالك العلامة التجارية على مستوى العالم.

تُعَد Microsoft وWindows علامتين تجاريتين لشركة Microsoft Corporation في الولايات المتحدة أو دول أخرى أو في كلتيهما.

Red Hat وOpenShift هما علامتان تجاريتان أو علامتان تجاريتان مسجلتان لشركة Red Hat, Inc. أو الشركات التابعة لها في الولايات المتحدة وبلدان أخرى.

تُعَد UNIX علامة تجارية مسجَّلة لشركة The Open Group في الولايات المتحدة ودول أخرى.

يصبح هذا المستند ساريًا بدءًا من تاريخ النشر الأول، ويجوز لشركة IBM تغييره في أي وقت. لا تتوفر بعض العروض في بعض الدول التي تعمل فيها IBM.

المعلومات الواردة في هذا المستند تُقدَّمُ "كما هي" دون أي ضمانات صريحة أو ضمنية، مثل جميع ضمانات الصلاحية التجارية، أو الملاءمة لغرض معين، أو الضمانات والشروط الخاصة بعدم انتهاك حقوق الأطراف الأخرى.

تشتمل منتجات IBM على ضمان وفقًا لشروط الاتفاقيات التي تُوفَّر بموجبها وأحكامها.

بيان الممارسات الأمنية الجيدة: ينبغي عدم اعتبار أي نظام أو منتج من منتجات تقنية المعلومات آمنًا تمامًا، ولا يمكن أن يكون أي منتج أو خدمة أو إجراء أمني واحدٍ فعالاً تمامًا في منع إساءة الاستخدام أو الوصول غير المصرح به. لا تضمن شركة IBM حصانة أي أنظمة أو منتجات أو خدمات ضد السلوك الخبيث أو غير القانوني الصادر عن أي طرف، ولا تدعي أن أي من هذه الأدوات ستحصن مؤسستك ضده.

العميل مسؤول عن ضمان الامتثال لجميع القوانين واللوائح المعمول بها. لا تقدم شركة IBM مشورة قانونية، ولا تتعهد ولا تضمن قدرة خدماتها أو منتجاتها على إلزام العميل بالامتثال لأي قانون أو لائحة.