RESUMEN DE LA SOLUCIÓN

¿Cómo puedo proteger credenciales con privilegios en todos mis centros de datos tradicionales y virtuales, nubes públicas y privadas, y entornos híbridos?

ca technologies

La gestión y protección de las credenciales con privilegios constituyen el pilar para reducir los riesgos y abordar los requisitos en materia de conformidad. Las organizaciones tienen que evaluar las soluciones de gestión de contraseñas con privilegios teniendo en cuenta el nivel de control, el ámbito de aplicación y el grado de armonización con la nube. CA Privileged Access Manager se ajusta a estas tres dimensiones, ya que proporciona una solución de última generación que implanta unos procesos de gestión de credenciales con privilegios que reducen los riesgos en materia de TI, aumentan la eficiencia operativa y protegen la inversión de una organización. Todo esto se consigue gracias a su compatibilidad con infraestructuras tradicionales, virtualizadas y en la nube híbrida.

Resumen ejecutivo

Reto

La adopción de la virtualización y la informática en la nube están acentuando la importancia y la complejidad de un problema que no es nuevo: gestionar y proteger de manera eficaz las contraseñas de cuentas con privilegios. La gestión de contraseñas con privilegios en infraestructuras tradicionales (dispositivos de red, servidores, mainframes, etc.) ha sido un problema *de larga data*. Asimismo, la multitud de credenciales con privilegios integradas directamente en las aplicaciones complica aún más la situación. Algunos ejemplos de este tipo de credenciales son los pares de claves SSH y las claves codificadas en formato PEM que se emplean para acceder a recursos de Amazon Web Services (AWS).

Oportunidad

La protección eficaz de las credenciales con privilegios en las empresas híbridas puede ayudar a las organizaciones a mitigar los riesgos de que los atacantes externos y los empleados internos con malas intenciones aprovechen las brechas de seguridad. Las organizaciones tienen la oportunidad de adoptar enfoques de gestión del acceso con privilegios que se ajusten a las 12 capacidades imprescindibles, que explicaremos en este resumen, con el fin de reducir los riesgos de auditorías fallidas e infracciones en materia de conformidad, la pérdida de datos de gran valor, y las costosas interrupciones del servicio. Hay que señalar que todos estos peligros se atribuyen a las cuentas con privilegios desprotegidas.

Ventajas

CA Privileged Access Manager proporciona un completo conjunto de controles para proteger y gestionar todo tipo de credenciales de toda clase de recursos, con independencia de su ubicación, de una forma que satisface los requisitos de los entornos en la nube híbrida de hoy en día. De este modo, las organizaciones pueden reducir aún más los riesgos, el coste de propiedad y las cargas de trabajo operativas que si utilizaran enfoques alternativos que no pueden brindar un nivel comparable de control, ámbito de aplicación y grado de armonización con la informática en la nube.

Sección 1:

Aspectos básicos de la gestión de contraseñas de usuarios con privilegios

Las contraseñas de usuarios con privilegios (de ahora en adelante, "contraseñas con privilegios") se distinguen de las habituales de los usuarios finales en que pueden regular de manera uniforme el acceso a los recursos más confidenciales de una organización; concretamente, a las cuentas administrativas (por ejemplo, administrador, raíz, SYS y sa) y a las capacidades asociadas que se utilizan para configurar y controlar la infraestructura de TI de una organización. Dado el riesgo que esto conlleva, resulta bastante evidente que es importante gestionar y proteger estas credenciales —un aspecto que se valida mediante numerosos conjuntos de requisitos asociados que están plasmados en normas y estándares de seguridad que se aplican habitualmente, como las normativas NIST Special Publication 800-53 y Payment Card Industry Data Security Standard (PCI-DSS).

Además de los requisitos normativos, la gestión de contraseñas con privilegios no solo constituye una buena práctica desde el punto de vista del control de los riesgos, sino que también resulta esencial para acabar con la larga lista de prácticas inseguras que son habituales en las organizaciones de hoy en día. Las contraseñas débiles, obsoletas o expuestas (por ejemplo, porque se apunten en pósits o se almacenen en hojas de cálculo); tener demasiadas contraseñas; compartirlas; no observar por completo la atribución de las actividades de los usuarios con cuentas compartidas; la ausencia de medidas de autenticación sólidas, y la falta de una capacidad de revocación centralizada son tan solo un ejemplo de los problemas que nos encontramos días tras día.

Según el informe Verizon Data Breach Investigations Report de 2015, el 95 % de las infracciones podrían atribuirse a credenciales robadas, mientras que otro 10 % se produjeron como consecuencia del uso indebido de credenciales por parte de empleados internos de confianza.[1]

El problema real es la posibilidad de que cualquiera de estas condiciones provoque que métodos como el *spear phishing* (ataques directos de *phishing*), los ataques dirigidos y, en última instancia, el robo de datos se perpetren con éxito; sin olvidar las infracciones en materia de conformidad. Le convenceremos con hechos. Según el informe Verizon Data Breach Investigations Report de 2015, el 95 % de las infracciones podrían atribuirse a credenciales robadas, mientras que otro 10 % se produjeron como consecuencia del uso indebido de credenciales por parte de empleados internos de confianza.[1] De revelaciones como estas se deduce claramente el motivo por el que las organizaciones de hoy en día necesitan sacar partido de una solución empresarial, como CA Privileged Access Manager, con el objetivo de gestionar y proteger las credenciales con privilegios, así como controlar el acceso a estas.

El impacto de la nube híbrida

Los problemas tradicionales que mencionamos anteriormente son tan solo la punta del iceberg. Dadas las atractivas ventajas en materia de costes, adaptabilidad y capacidad de respuesta que ofrecen las configuraciones en la nube híbrida —donde las aplicaciones y los servicios de TI aprovechan la infraestructura virtualizada y tradicional que abarca tanto los centros de datos empresariales como en la nube—, resulta inevitable que se estén adoptando de forma generalizada. Además de todo esto, las nubes híbridas también introducen nuevos retos en la esfera de la gestión de contraseñas con privilegios. Estos son algunos de ellos:

- Mayor volumen y escalabilidad. Como consecuencia de las demandas operativas y la facilidad de implementar máquinas virtuales, cada vez son más las empresas que exigen accesos con privilegios (y, por ende, contraseñas con privilegios).
- Mayor cobertura. El potencial concentrado de las consolas de gestión en la nube y la virtualización introduce en el panorama un nuevo tipo de cuenta o recurso con privilegios.
- Mayor dinamismo. Se pueden agregar a petición nuevos servidores y sistemas, sin mencionar que este proceso puede realizarse en bloque (por ejemplo, 10, 20 o más a la vez).
- La posibilidad de que se generen islas de seguridad (cada servicio en la nube cuenta con su propio almacén de identidades e infraestructura[2]).

Aparte de los retos que plantea la nube híbrida, los gestores de seguridad de TI también tienen que considerar otros dos aspectos del problema de la gestión de contraseñas con privilegios a la hora de evaluar las posibles soluciones. En primer lugar, necesitan tener cuenta el escenario entre equipos o aplicaciones (A2A), donde las contraseñas que se utilizan en un sistema o una aplicación para acceder a otro recurso de este tipo se integran directamente en la aplicación que efectúa el acceso o se incluyen en un archivo de configuración de texto sin formato. El segundo aspecto que hay que considerar es un problema que suele pasarse por alto y que tienen la mayoría de las organizaciones, y es que cuentan con miles de claves (por ejemplo, para implementaciones SSH) que, aunque no se trata de contraseñas tradicionales y que incluyan frases, siguen funcionando como credenciales de cuentas con privilegios y, por tanto, siguen precisando que se implanten medidas de gestión y protección para reducir los riesgos asociados.

El resultado es que la gestión de contraseñas con privilegios nunca había sido tan importante y compleja en la era de la nube híbrida.

Sección 2:

La solución de gestión del acceso con privilegios de CA Technologies

CA Privileged Access Manager proporciona una solución completa para la gestión del acceso con privilegios. Por tanto, además de poder controlar el acceso y monitorizar y registrar las actividades de los usuarios con privilegios en los entornos en la nube híbrida, CA Privileged Access Manager también incorpora las capacidades que se precisan de una solución de última generación para gestionar contraseñas con privilegios. De hecho, es importante que los equipos de seguridad de TI reconozcan que, aunque la gestión y la protección de contraseñas son valiosas por sí mismas, también resultan útiles para conseguir mejores resultados en otras tareas. En concreto, constituye el primer paso (o el complementario) del proceso de controlar y gestionar verdaderamente el acceso a los recursos de alto riesgo, que es más extenso pero igual de importante. Si la diferencia parece sutil, en gran parte se debe a que, en la práctica, es raro que las implementaciones funcionales de mecanismos de autenticación (es decir, de contraseñas) y control del acceso se realicen de forma separada; por tanto, solemos *meterlos en el mismo saco*.

En cualquier caso, los objetivos de diseño de las capacidades de gestión de contraseñas con privilegios que incluye CA Privileged Access Manager son los mismos que los que se aplican en el resto de la solución. En concreto, nuestro objetivo consiste en entregar una solución que no solo proporcione un complejo conjunto de controles y capacidades para un gran número de objetivos y casos de uso, sino que también lo haga de una forma coherente con las opciones, prácticas y arquitecturas de entrega de la era de la nube en que vivimos.

Controles exhaustivos

Cuando se trata de evaluar soluciones de gestión de contraseñas con privilegios, recomendamos analizar en primer lugar si la solución incorpora un exhaustivo conjunto de controles que ayuden al equipo de seguridad a abordar los riesgos que plantean los enfoques tradicionales en cuanto a creación, gestión y uso de credenciales administrativas confidenciales. Entre las áreas concretas que hay que analizar se encuentran la detección, la salvaguarda en almacén, la aplicación de políticas, la recuperación, y la posibilidad de respaldar una transición fluida a un enfoque de implementación de capacidades de gestión del acceso con privilegios completas.

Sección 3:

Las 12 capacidades imprescindibles de la gestión del acceso con privilegios

1. Detección automatizada y simplificada

Sin una forma de automatizar o simplificar la detección, el proceso de gestionar las contraseñas con privilegios puede ser farragoso, sin olvidar los numerosos errores u omisiones que convierten al entorno informático de una organización en el blanco de los ataques sofisticados de hoy en día. Por este motivo, CA Privileged Access Manager incluye diversos métodos para detectar dispositivos, sistemas, aplicaciones, servicios y cuentas, así como la posibilidad de utilizar conocidos datos del directorio, API, consolas de gestión y asociaciones de puerto. Por ejemplo, CA Privileged Access Manager aprovecha las API disponibles para que las soluciones de gestión en la nube y virtualización compatibles notifiquen a los administradores cuando se creen nuevas máquinas virtuales. Asimismo, la solución facilita el proceso de importación en bloque de listas del sistema a partir de archivos de texto, y crea entradas *ad hoc* a través de la consola de gestión. Finalmente, también es importante comprender que, por motivos de diseño, hemos decidido evitar las técnicas de detección más perjudiciales (y posiblemente que generen más riesgos) que precisan el uso de agentes basados en objetivos que utilizan la pila TCP local.

2. Salvaguarda en almacén y almacenamiento seguros

Un almacén cifrado proporciona un punto de control centralizado y constituye la clave para eliminar los métodos de almacenamiento no seguros (como las hojas de cálculo) que facilitan que las credenciales se compartan y queden expuestas. El almacén de CA Privileged Access Manager constituye una caja fuerte para las credenciales; una solución de conformidad con los FIPS 140-2 de clasificación 1 que aprovecha el cifrado AES de 256 bits para almacenar de forma segura todo tipo de credenciales, no solo contraseñas. Estas son otras de las atractivas funciones que incluye la solución:

- Se incluye la opción para aprovechar módulos de seguridad de hardware integrados (HSM), como los de SafeNet y Thales, para llevar a cabo una implementación de FIPS 140-2 de clasificación 2 o 3. Esto es especial relevante para los clientes importantes y que no quieren correr riesgos, como aquellos que utilizan sistemas financieros y bancarios en los que desean almacenar las claves usadas para cifrar las credenciales independientemente de las ya cifradas. Se admiten numerosas opciones de implementación, incluidos los dispositivos de hardware de CA Privileged Access Manager con tarjetas PCI incorporadas, dispositivos virtuales de CA Privileged Access Manager que efectúan llamadas a dispositivos HSM conectados a la red y dispositivos de CA Privileged Access Manager de cualquier tipo que realice llamadas a una oferta de HSM como servicio de AWS.
- Asimismo, las rutinas criptográficas genéricas protegen las claves de cifrado mientras se utilizan (es decir, mientras están en la memoria) en un sistema. Este enfoque se ha diseñado para evitar que los piratas informáticos obtengan o descifren las claves monitorizando la memoria y las API criptográficas estándares, y dejando de lado alternativas inferiores basadas en fragmentar las claves u ocultarlas de forma simple. La inclusión de esta tecnología resulta especialmente relevante para los casos de uso de A2A, en los que el sistema que efectúa el acceso debe salvaguardar en un almacén las credenciales y, por tanto, hay un mayor riesgo de que sean blanco de los ataques (por ejemplo, porque se encuentre en una ubicación relativamente vulnerable).

3. Aplicación de políticas automatizada

CA Privileged Access Manager automatiza la creación, el uso y el cambio de contraseñas, con lo que se elimina la tendencia de reutilizar las contraseñas o de confiar en aquellas que son débiles (y fáciles de recordar). Gracias a CA Privileged Access Manager, pueden establecerse políticas flexibles para aplicar reglas de complejidad de contraseñas, implementar requisitos de cambios —como alternar las contraseñas de forma periódica (diaria o semanalmente) o como respuesta a un evento concreto (por ejemplo, después de cada uso)— y controlar el uso (por ejemplo, permitiendo el acceso solo durante periodos concretos o exigiendo autorizaciones duales o múltiples para acceder a las contraseñas). Dado que estas políticas pueden aplicarse de manera jerárquica y agrupar grupos de recursos de destino, no solo pueden tenerse en cuenta diferentes requisitos y capacidades para objetivos distintos, sino que su aplicación también puede realizarse de forma dinámica y eficaz, ya que todos los recursos que se agregan a un grupo heredan automáticamente las políticas de dicho grupo. CA Privileged Access Manager también interactúa en segundo plano con los recursos de destino afectados con el fin de garantizar que todas las credenciales sigan sincronizadas (es decir, cuando se cambien en un extremo, que también se modifiquen en el otro).

4. Presentación/uso y recuperación de forma segura

Si las credenciales no pueden recuperarse y utilizarse de forma segura, será inútil colocarlas en un almacén. El primer paso de este proceso consiste en realizar una autenticación precisa de los usuarios y los recursos, en el caso de las aplicaciones y los scripts, que tenga como objetivo acceder a una credencial o utilizarla. En este sentido, CA Privileged Access Manager aprovecha al máximo su infraestructura de gestión del acceso e identidades existente, y se integra con Active Directory y directorios compatibles con LDAP, así como con sistemas de autenticación como Radius. También se ofrece compatibilidad con:

- Tokens de dos factores (por ejemplo, a través de CA Advanced Authentication o de otras soluciones como RSA y SafeNet)
- Certificados X.509/PKI
- Tarjetas de acceso común (CAC) y verificación de identidad personal (PIV), necesarias para cumplir las normativas HSPD-12 y OMB-11-11 del sector federal
- SAML
- Técnicas de varios factores complejas (por ejemplo, combinar contraseñas con tokens RSA)

En el modo de operación que se prefiera, CA Privileged Access Manager presenta la credencial solicitada al sistema de destino en representación de la entidad que efectúa el acceso (por ejemplo, un usuario o una aplicación). Gracias a este enfoque, se obtienen varias ventajas adicionales en materia de seguridad. En primer lugar, a diferencia de las soluciones de control de entrada y salida de contraseñas, las credenciales siempre están ocultas y nunca se distribuyen a la entidad que efectúa el acceso, lo que reduce en gran medida las posibilidades de que queden expuestas. Asimismo, como la autenticación del sistema de destino se automatiza íntegramente y los usuarios no necesitan nunca gestionar ni recordar sus contraseñas, pueden implementarse políticas para aumentar drásticamente la complejidad de las contraseñas. Dado que todos los accesos a los objetivos se realizan a través de CA Privileged Access Manager, la solución también puede observar la atribución completa de la actividad de los usuarios con privilegios, aunque utilicen cuentas compartidas.

Para completar, también vale la pena subrayar que todas las comunidades de red entre las entidades que efectúan el acceso, CA Privileged Access Manager y los objetivos gestionados se cifran mediante SSL. Además, CA Privileged Access Manager admite un modo de operación alternativo mediante el cual las entidades que efectúan el acceso pueden recuperar y enviar directamente y por sí mismas las credenciales solicitadas a los sistemas de destino.

5. Transición fluida a una gestión del acceso realizada exclusivamente con privilegios

CA Privileged Access Manager ofrece a las organizaciones que en sus inicios se centraban exclusivamente en gestionar las contraseñas todos los recursos lo que necesitan para que puedan empezar a adoptar un enfoque de implementación de capacidades de gestión del acceso con privilegios completas cuando tomen conciencia de que necesitan dar este paso.

A continuación figuran algunas de las capacidades más notables que podrá obtener el departamento de seguridad de TI cuando esté preparado para aprovecharlas:

- Flujos de trabajo asociados y control del acceso granular basado en roles (por ejemplo, para solicitar o autorizar permisos adicionales).
- Establecimiento automatizado de conexiones y sesiones con recursos de destino (con compatibilidad con RDP, SSH, la tecnología web y otros modos u opciones de acceso diferentes).
- Monitorización en tiempo real de las sesiones de los usuarios con privilegios, junto con aplicación basada en políticas de actividades permitidas y denegadas (por ejemplo, los comandos que un usuario concreto puede ejecutar).
- Capacidad de registro, incluida integración con SIEM basada en Syslog.
- Registro completo de sesiones con controles de reproducción semejantes a los de una grabadora DVR para saltar directamente a los eventos de interés.
- Opción para evitar que los usuarios sorteen procesos y eludan sus permisos aprovechando los objetivos accesibles con el fin de entrar en otros destinos no autorizados.

Además, resulta muy sencillo implementar estas capacidades adicionales. CA Privileged Access Manager entrega todas sus funciones de control del acceso y gestión de contraseñas con privilegios como una solución perfectamente integrada. También proporciona capacidades de gestión unificada de políticas en toda la solución, así como un enfoque que simplifica más aún las labores de implementación y administración.

Cobertura completa

La segunda principal área que evaluar a la hora de seleccionar una solución para gestionar contraseñas con privilegios es el ámbito de aplicación que proporcione. Es decir, si nos centramos en el exhaustivo conjunto de controles mencionados anteriormente, ¿con qué tipos de credenciales, sistemas de destino y entidades que efectúan el acceso es compatible realmente la solución?

6. Cobertura completa para objetivos tradicionales

CA Privileged Access Manager incluye una amplia variedad de conectores de sistemas de destino que proporcionan una integración directa con todo tipo de infraestructuras de TI, dispositivos de red, sistemas y aplicaciones; entre ellos, los siguientes:

- Cuentas de servicio, de administrador local y de dominio de Windows®
- Distribuciones comunes de Linux® y UNIX®
- AS/400
- Dispositivos de red de Cisco y Juniper
- Sistemas basados en Telnet y SSH
- SAP
- Remedy
- Bases de datos de ODBC y JDBC
- Servidores de aplicaciones y sistemas

CA Privileged Access Manager, como solución ampliable, también proporciona capacidades de personalización flexibles para que las organizaciones puedan extender sus servicios de soporte a los sistemas patentados y desarrollados internamente.

7. Compatibilidad con consolas de gestión en la nube y virtualización

La cobertura predeterminada de CA Privileged Access Manager para la gestión y protección de credenciales no se limita a los objetivos tradicionales, sino que también se extiende a las soluciones comunes en la nube y de virtualización, entre ellas VMware vSphere, VMware NSX, Amazon Web Services y Microsoft® Online Services. Además, las capacidades que se aplican a estas soluciones no se reducen a instancias individuales de máquinas virtuales, aplicaciones o servicios asociados. La cobertura también se extiende a las consolas de gestión correspondientes que, debido a la potencia que demandan, deben reconocerse como recursos privilegiados por méritos propios.

8. Compatibilidad con la autenticación entre máquinas

Tal y como hemos mencionado anteriormente, las personas no son los únicos usuarios de las credenciales con privilegios. En la mayoría de las organizaciones, a numerosos sistemas y aplicaciones se les permite acceder a recursos confidenciales, como otras aplicaciones o bases de datos. Normalmente, esto se lleva a cabo integrando las credenciales asociadas en el código de las aplicaciones que efectúan el acceso o en un archivo de configuración para que se utilicen en el momento de la ejecución; sin embargo, ninguna de estas dos opciones resulta especialmente segura o gestionable. CA Privileged Access Manager proporciona cobertura para estos casos de uso de A2A permitiendo que los desarrolladores inserten un cliente ligero de esta solución en sus aplicaciones. Gracias a este enfoque, se dota a las aplicaciones con privilegios de todo lo que necesitan para registrarse en CA Privileged Access Manager, recuperar de forma dinámica las contraseñas requeridas y, a continuación, protegerlas mientras se encuentran en la memoria del sistema local. Además, hay disponibles varios mecanismos para autenticar las aplicaciones con privilegios y verificar su integridad antes de que CA Privileged Access Manager extraiga las credenciales solicitadas.

Al utilizar CA Privileged Access Manager en escenarios de A2A, las organizaciones pueden eliminar de forma más eficaz las credenciales de A2A expuestas o no seguras colocándolas de forma central en un almacén, automatizar la aplicación de políticas y la gestión de credenciales de A2A, así como simplificar las actividades de conformidad y auditorías relacionadas.

9. Compatibilidad con la gestión de claves

Además de respaldar operaciones criptográficas, muchas claves actúan como tokens con el fin de confirmar las identidades. Aunque estas claves no son contraseñas en el sentido tradicional, siguen funcionando como tal y continúan siendo el blanco de amenazas, riesgos y retos similares, como la copia, el uso compartido, la exposición involuntaria y las puertas traseras sin auditar. Como estas claves suelen integrarse o utilizarse con transparencia en las soluciones con el fin de proteger a los usuarios de su relativa complejidad, también es más probable que queden huérfanas o proliferen con el paso del tiempo. Por tanto, cobra sentido aplicar muchos de los mismos controles que se utilizan para gestionar y proteger también las contraseñas en estas credenciales alternativas. De hecho, entre algunas de las prácticas recomendadas para combatir las amenazas relacionadas se encuentran las siguientes:

- Mover las claves autorizadas a ubicaciones protegidas
- Alternar todas las claves de forma periódica (para garantizar la finalización eventual del acceso en el caso de filtración de claves)
- Aplicar restricciones de orígenes en las claves autorizadas[3]
- Aplicar restricciones de comandos en las claves autorizadas

Como consecuencia, CA Privileged Access Manager posee controles y otras capacidades para tener en cuenta tipos de credenciales alternativos, incluidas las claves SSH y PEM para acceder a las consolas de gestión y los recursos de AWS. Es decir, gracias a esta solución, estas credenciales pueden (1) salvaguardarse en un almacén externo, (2) alternarse y controlarse mediante políticas configuradas y (3) recuperarse y utilizarse de una forma que minimiza las posibilidades de que se roben o queden expuestas.

El modelo de entrega en la era de la nube

En la era de la nube híbrida, otro importante factor determinante para el éxito de una solución de gestión de contraseñas con privilegios es cómo de bien se adapte no solo a las capacidades y requisitos de las instalaciones físicas, sino también de las redes en la nube.

10. Opciones de entrega basada en la nube, máquinas virtuales o *in situ*

CA Privileged Access Manager admite tres cómodas opciones de implementación que ayudan a las organizaciones a satisfacer los requisitos de arquitecturas complejas en la nube híbrida:

- Un dispositivo físico protegido, que se encuentra disponible en varios modelos para montarse de forma tradicional en rack en el centro de datos de la empresa.
- Una imagen de máquina de Amazon (AMI), que se ha configurado previamente para implementarse con la infraestructura de Amazon EC2.
- Un dispositivo virtual compatible con OVF, que está preparado y configurado previamente para implementarse en entornos de VMware.

Con independencia de las opciones de implementación utilizadas, las organizaciones obtendrán una solución con la que se podrá gestionar toda la infraestructura en la nube híbrida.

11. Enfoque y arquitectura armonizados con la nube

CA Privileged Access Manager se ha diseñado expresamente para incorporar numerosas características que lo convierten en un componente indispensable de los entornos en la nube híbrida. A continuación, podemos ver tres ejemplos:

- Protección y detección automáticas. En los entornos en la nube híbrida, los operadores pueden crear (o retirar) cualquier número de sistemas ejecutando un solo comando. CA Privileged Access Manager tiene en cuenta esta situación mediante el uso de las API correspondientes para detectar automáticamente los recursos en la nube y virtualizados y, a continuación, aprovisionar (o anular este proceso) las políticas de gestión del acceso y credenciales adecuadas.
- Prevención de islas de identidad (es decir, federación de identidades). Una de las formas con las que CA Privileged Access Manager elimina las islas independientes de la información de identidades es aprovechando por completo la infraestructura de identidades que ya haya implantado una organización. Otra de las formas, que es específica de las implementaciones de AWS, consiste en admitir usuarios efímeros; con este enfoque, las organizaciones no tienen que mantener información de identidades independiente en el subsistema de gestión del acceso e identidades de AWS.
- Habilitación de capacidades de automatización. Una completa API puede acceder de forma programática a todas las funciones de CA Privileged Access Manager y automatizarlas (por ejemplo, mediante sistemas de articulación y gestión externos).

12. Fiabilidad y escalabilidad preparadas para la nube

La gestión de credenciales con privilegios constituye un elemento esencial de la infraestructura de TI de una organización, sobre todo cuando la implementación se extiende a casos de uso de A2A, que se llevan a cabo de forma completamente automatizada. Para ello, CA Privileged Access Manager incluye unas funciones nativas de distribución de la carga y agrupamiento en clústeres que pueden satisfacer los requisitos de disponibilidad y escalabilidad de los entornos más grandes y exigentes. En comparación con alternativas comunes, gracias a CA Privileged Access Manager, no habrá y que invertir en equilibradores de carga independientes y externos, no se producirán los retrasos del rendimiento habituales de los enfoques activos-pasivos y no se necesitarán más funciones opcionales de licencias. Si se desea y resulta aceptable desde el punto de vista de las operaciones y la latencia, los clústeres de CA Privileged Access Manager pueden configurarse incluso para permitir la redundancia en entornos en la nube y centros de datos repartidos geográficamente.

CA Privileged Access Manager ofrece una solución de última generación para gestionar contraseñas con privilegios que se ha diseñado para impulsar la reducción de los riesgos de seguridad y aumentar la eficiencia operativa en toda la infraestructura empresarial híbrida.

Sección 4:

Conclusión: el control de la gestión de credenciales con privilegios en la era de la nube

La gestión y protección de las credenciales con privilegios constituyen el pilar para reducir los riesgos y cumplir los requisitos normativos relacionados. También existe un problema que se está volviendo más complejo y significante, ya que los entornos en la nube híbrida introducen consolas de gestión con un potencial sin precedentes, así como la posibilidad de agregar o eliminar los cientos de sistemas de destino con unos pocos clics.

Las organizaciones que tienen como objetivo abordar esta área de gran importancia dentro de su estrategia de seguridad de la información tienen que evaluar las posibles soluciones teniendo en cuenta el nivel de control, el ámbito de aplicación y el grado de armonización con la nube. Tal y como se ha explicado en este resumen, CA Privileged Access Manager se ajusta a estas tres dimensiones con el fin de proporcionar a las organizaciones de hoy en día justo lo que necesitan: una solución de última generación que implanta unos procesos de gestión de credenciales con privilegios diseñada para reducir los riesgos en materia de TI, aumentar la eficiencia operativa y proteger la inversión de una organización. Todo esto se consigue gracias a su compatibilidad con infraestructuras tradicionales, virtualizadas y en la nube híbrida.

Comuníquese con CA Technologies en ca.com/es

CA Technologies (NASDAQ: CA) crea software que impulsa la transformación de las empresas y les permite aprovechar las oportunidades que brinda la economía de las aplicaciones. El software se encuentra en el corazón de cada empresa, sea cual sea su sector. Desde la planificación hasta la gestión y la seguridad, pasando por el desarrollo, CA trabaja con empresas de todo el mundo para cambiar la forma en que vivimos, realizamos transacciones y nos comunicamos, ya sea a través de la nube pública, la nube privada, plataformas móviles, entornos de mainframe o entornos distribuidos. Para obtener más información, visite ca.com/es.

1 2015 Verizon Data Breach Investigations Report

2 *"New Platforms, New Requirements. Privileged Identity Management for the Hybrid Cloud"*, Libro blanco de CA, marzo de 2013

3 *"Managing SSH Keys for Automated Access - Current Recommended Practice"*, IETF Draft, abril de 2013

CS200-169152_1215