RESUMEN DE LA SOLUCIÓN
CA IDENTITY SUITE

El control y la gestión de identidades que dotan a los usuarios empresariales de los recursos que necesitan

Reducción de la distancia entre la tecnología informática y los usuarios empresariales

ca technologies

Resumen ejecutivo

Reto

Si es líder de TI, ejecutivo de seguridad o gestor empresarial, estará viviendo unos momentos muy cambiantes y difíciles. Los entornos de TI cada vez están más distribuidos y son más complejos y heterogéneos. Sin embargo, decidir quién tiene acceso a qué y conseguir que se cumplan esas políticas de una forma fiable es un reto con múltiples facetas en el que las tres partes implicadas deberían estar involucradas:los responsables de la actividad comercial, los responsables de la seguridad y los de las TI.

Al mismo tiempo, los departamentos de TI suelen tener asignado un presupuesto reducido y menos recursos para llevar a cabo sus responsabilidades; Por lo tanto, necesita una forma fiable, pero rentable de superar estos importantes retos que plantean las identidades:

- Incorporar rápidamente nuevos usuarios para que sean productivos lo antes posible.
- Asegurarse de que todos los usuarios dispongan únicamente de las atribuciones de acceso adecuadas según sus roles.
- Automatizar los principales procesos de identidad para mejorar la eficiencia y reducir los costes.
- Identificar y prevenir las posibles infracciones de políticas (cuentas huérfanas, atribuciones inadecuadas, etc.) antes de que ocurran.
- Cumplir con los requisitos de auditoría al saber quién tiene acceso a qué.

Por último, una de las medidas facilitadoras más importantes en el entorno actual es la siguiente:

- Proporcionar una experiencia sencilla e intuitiva para que los usuarios empresariales puedan acceder de forma fácil y cómoda a sus servicios de identidad principales.

Oportunidad

El creciente interés por proporcionar a los usuarios empresariales los recursos que necesitan ha generado muchos retos para los usuarios de la mayoría de las soluciones de gestión de identidades de hoy en día. Lamentablemente, las pocas soluciones que aportan una experiencia de usuario razonable suelen carecer de la amplitud de capacidades de aprovisionamiento, gestión de roles y control, y de la habilidad de ampliarse y dar soporte a la gestión de identidades de toda la empresa. Esta situación le obliga a elegir entre una gama de funcionalidades y facilidades de uso.

CA Identity Suite contribuye de una forma excepcional a acabar con la división entre los usuarios empresariales y las tecnologías IAM actuales. Es un conjunto de programas integrado de gestión de identidades y capacidades de control que combina una sólida funcionalidad con una experiencia intuitiva, cómoda y orientada a la empresa. Este conjunto de programas puede simplificar los procesos de gestión de identidades, mejora la satisfacción del usuario, es compatible con aplicaciones tanto in situ como en la nube y ofrece escalabilidad para el consumidor. Además, lo mejor de todo es que se puede implementar fácil y rápidamente.

Principales retos para un control y una gestión de identidades eficientes

Este documento subraya la importancia de algunos de los retos principales de la gestión de identidades de las empresas abiertas de hoy en día y describe la razón por la cual estos retos pueden impulsar o entorpecer el desarrollo de su empresa, además de ofrecer una descripción general de las capacidades que CA Identity Suite ofrece y que pueden ayudar a que su organización afronte estos retos con éxito.

Cada uno de los retos que se enumeran a continuación presenta un aspecto empresarial y de TI. En el pasado, la experiencia del usuario con respecto a los servicios de identidad estaba dominada por una perspectiva informática, cuyo resultado fueron interfaces difíciles y una satisfacción reducida. No obstante, los entornos actuales exigen una unión entre la tecnología informática y los usuarios empresariales para ampliar el uso de los servicios de identidad y mejorar la experiencia general del usuario. Se explorarán los aspectos empresariales y técnicos de estos retos.

Estos últimos requieren una amplia planificación y deberían formar parte de todo plan de lanzamiento:

- **Adopción de los usuarios**: Mejora y simplificación de la experiencia general del usuario para aumentar la adopción de procesos de identidad por parte del usuario.
- **Solicitudes de acceso**: Simplificación del proceso de acceso a aplicaciones que el usuario necesita.
- **Gestión de los riesgos de las atribuciones**: Prevención de la infracción de políticas de atribuciones.
- **Certificaciones de acceso**: Mejora de la productividad de los gestores.
- **Acceso a las aplicaciones del usuario**: Ofrece a los usuarios una forma cómoda de acceder a sus aplicaciones principales.
- **Análisis de identidades en tiempo real**: Garantía de eficiencia en los servicios fundamentales relacionados con las entidades.
- **Retos de la implementación**: Mejora del retorno de la inversión y el tiempo de recuperación de la inversión.

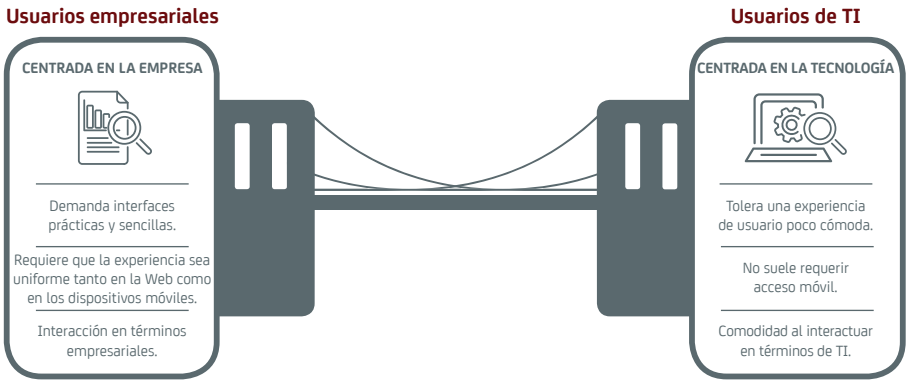
El reto: La adopción de los usuarios

"Mis usuarios están frustrados por la incomodidad de la interfaz de usuario que provocan muchas de las funciones de identidad con las que deben lidiar, lo que está limitando considerablemente la posibilidad de ofrecer estos servicios a más usuarios de mi empresa."

Uno de los mayores retos de las implementaciones de gestión de identidades eficaces es que la experiencia del usuario en cuanto a los servicios de identidad suele estar muy orientada a las TI. En el pasado, podría haberse considerado aceptable; sin embargo, a medida que la gestión de identidades llega mucho más allá del simple usuario de TI, este enfoque ya no es efectivo. La terminología y los procesos que podrían ser lo más normal para un usuario experto en TI, pueden ser confusas y frustrantes para la mayoría de los usuarios empresariales. El resultado es una adopción reducida de los procesos de identidad, una mayor carga para el personal de TI, el incumplimiento de requisitos normativos y la frustración de los usuarios. Los usuarios necesitan disponer de aplicaciones empresariales fáciles, rápidas y que no necesiten formación, disponibles en el dispositivo de su elección. Estas deben integrarse en los procesos básicos de identidad, pero estos últimos solo funcionarán si consideran que son simples e intuitivos y, lo más importante, si están orientados a los usuarios empresariales, y no a los de TI.

La solución de CA Identity Suite

CA Identity Suite contribuye de una forma excepcional a acabar con la división entre los usuarios empresariales y las tecnologías IAM actuales. Es un conjunto de programas integrado de gestión de identidades y capacidades de control que combina una sólida funcionalidad con una experiencia intuitiva, cómoda y orientada a la empresa. Mediante la mejora de la productividad y la satisfacción de los usuarios empresariales, la experiencia de usuario de CA Identity Suite está diseñada para aumentar de forma drástica la proposición de valor de la solución IAM para grandes empresas a la vez que acaba con la significativa carga administrativa de la organización de TI.



Algunas de las ventajas de la experiencia de usuario más importantes que ofrece la Suite son estas:

- Un catálogo de atribuciones adecuado para la empresa
- Un selector y un cuadro de mandos de aplicaciones móviles y para la Web
- Una plataforma para todo, centralizada y de fácil acceso para todos los servicios de identidad dirigidos a usuarios empresariales
- Una experiencia de carrito de la compra para el seguimiento y las solicitudes de acceso
- Experiencias similares a las de las redes sociales para realizar el seguimiento de solicitudes de acceso
- Herramientas de asesoramiento proactivo
- Aplicaciones móviles que permiten que los usuarios gestionen identidades en cualquier momento y lugar

CA Identity Suite también facilita la generación de cuadros de mandos personalizados e individualizados, y adaptados a las necesidades específicas de cada rol, como los ejecutivos, los responsables de seguridad y los partners empresariales. Los administradores pueden configurar una interfaz basada en los roles de los usuarios y en los servicios a los que pueden acceder. La interfaz de Suite también puede personalizarse completamente según las necesidades de marca de su organización, incluido el logotipo corporativo, el esquema de colores, las fuentes, las imágenes de fondo seleccionadas y mucho más. El portal reflejará perfectamente la identidad de su negocio.

"En una encuesta llevada cabo por una firma externa especialista en análisis, el 97 % de los clientes preguntados notificaron que la experiencia de usuario que ofrecía Identity Suite era superior a la de la competencia".

Fuente: Encuesta de TechValidate

El reto: las solicitudes de acceso

"A mis usuarios les cuesta solicitar fácilmente el acceso a las aplicaciones y los sistemas que necesitan para su trabajo. El proceso resulta complicado y a mis usuarios empresariales los nombres de los recursos suelen parecerles confusos".

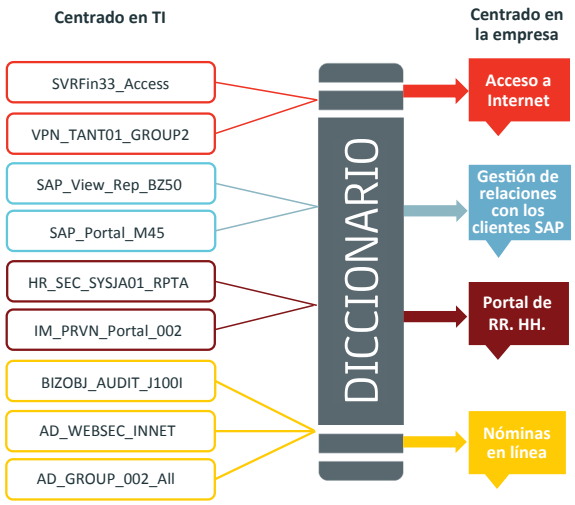
Los usuarios necesitan acceder a las aplicaciones y los datos que necesiten de una forma rápida y fácil mientras siguen cumpliendo con los requisitos normativos. Sin embargo, los sistemas de solicitud de acceso solían estar basados en un conjunto de atribuciones que se diseñaron para los administradores que entendían su significado y se impusieron a usuarios que tenían que aprender prácticamente un nuevo idioma con la terminología de la "jerga de TI". A medida que más y más usuarios empresariales emplean los procesos de identidad, esta experiencia no intuitiva dificulta la adopción, reduce la satisfacción y, normalmente, termina involucrando, de todos modos, a los encargados de TI para que ayuden a responder las preguntas de los usuarios empresariales que estén confundidos.

Es necesaria una nueva manera de interactuar con los usuarios empresariales y el área de solicitudes de acceso es un ejemplo excelente de las ventajas que puede ofrecer este nuevo enfoque. No obstante, los departamentos de TI también tiene unas necesidades básicas en esta área, como la automatización de procesos de solicitudes de acceso básicos y una auditoría sencilla de solicitudes y aprobaciones. Por tanto, es esencial contar con capacidades que satisfacen las necesidades de automatización de las TI, pero que también pueden usar los usuarios empresariales sin ninguna dificultad.

La solución de CA Identity Suite

CA Identity Suite ofrece un "carro de la compra" sencillo e intuitivo que simplifica considerablemente el proceso de solicitud de acceso. Diseñado según el familiar proceso de los sitios web de compras al por menor, permite a los usuarios identificar cómodamente los roles y las atribuciones necesarios para desempeñar su trabajo, ver los privilegios de acceso de los que disponen y comprobar el estado de solicitudes anteriores.

El sencillo catálogo de atribuciones adecuado para la empresa es el núcleo de cómo CA Identity Suite ayuda a proporcionar una experiencia sencilla y orientada a la empresa. Además, traduce nombres de recursos crípticos, como "TSS_MNG_per_view" en unos más intuitivos, como "Nómina en línea", lo que facilita a los usuarios empresariales la localización de los recursos que necesitan. Además, puede agrupar aplicaciones en categorías lógicas para que el acceso sea más fácil (por ejemplo, mediante la creación de un grupo llamado "acceso de control de respuesta del sistema [SRM]", que incluya las aplicaciones de SAP, las de Oracle y las capacidades de SalesForce que los usuarios empresariales suelen necesitar) y con términos con los que estos usuarios estén familiarizados. En el siguiente gráfico se destacan las asignaciones entre términos centrados en las TI y en la empresa que el catálogo ofrece.



Identity Suite incluye herramientas de asesoramiento proactivo que pueden simplificar en gran medida el proceso de solicitud de acceso. El usuario puede ver sugerencias de roles y derechos de acceso de usuarios similares a los suyos. Este asesoramiento proactivo ayuda a los usuarios a realizar la solicitud correcta sobre el acceso que quieren. También proporciona una valoración del riesgo, basada en los accesos que solicitó y en lo peligrosos que puede que sean. El usuario puede tomar decisiones más fundamentadas en cuanto a qué acceso solicitar.

El reto: Gestión de los riesgos de las atribuciones

"A veces, se asigna a los usuarios por error atribuciones que infringen nuestras políticas de seguridad. Quiero que prevenir esas infracciones antes de que sucedan".

El uso inadecuado de las atribuciones ha sido la causa raíz de una gran cantidad de infracciones públicas que han tenido lugar últimamente. Este es especialmente el caso de los usuarios con privilegios porque tienden a tener atribuciones muy amplias. Sin embargo, el principio es el mismo para todos los usuarios: necesitamos corregir las atribuciones inadecuadas que infringen las políticas de seguridad antes de que se concedan (control preventivo) y anular todas las que ya se hayan concedido en el pasado (control reactivo). A menos que se realicen controles eficaces para ambos casos, el riesgo aumentará y las auditorías de conformidad serán más complicadas.

De forma similar, a veces las políticas cambian y el acceso concedido en el pasado infringe ahora la nueva política. Durante las certificaciones de acceso normales, esto debe hacerse muy visible para el gestor, de forma que también pueda quitar el certificado al usuario para esa atribución de acceso en cuestión.

La solución de CA Identity Suite

CA Identity Suite le permite formular, aplicar y validar conjuntos de reglas de procesos empresariales para implementar la segregación de funciones u otras restricciones lógicas sobre las relaciones que existen entre los usuarios, los roles y los privilegios. Por ejemplo, una regla de procesos empresariales permite crear una restricción como "las personas con permiso para acceder a X no pueden tener permiso para acceder a Y" o una relación de dependencia como "únicamente las personas con acceso a B pueden tener permiso para hacer A". Así, se pueden prevenir las infracciones de estas políticas de seguridad antes de que sucedan.

Además, Suite puede advertirle si se solicitan derechos que entren en conflicto (controles preventivos descritos anteriormente) y asigna una valoración del riesgo basada en el acceso solicitado y la política relacionada. La valoración del riesgo está basada en el usuario, sus otras atribuciones y todos los factores contextuales que pudieran ser pertinentes. Este nivel del riesgo se le proporciona al solicitante cuando se realiza la solicitud de aprobación para advertirle de la existencia de una solicitud que podría no ser adecuada. De forma similar, el aprobador ve esta valoración del riesgo durante el proceso de aprobación, lo que ofrece una visibilidad total que puede prevenir la concesión de acceso de alto riesgo.

Además, Suite proporciona controles reactivos para corregir el acceso inadecuado que se ha concedido. En el momento de la certificación, Suite ejecuta comprobaciones de políticas contra el acceso y le informa sobre si el usuario cuenta con derechos de acceso inadecuados que infrinjan cualquier política. El gestor ve las infracciones de cada usuario claramente marcadas para permitir una corrección inmediata. Ambos tipos de controles pueden reducir de manera significativa el riesgo de que se concedan o sigan sin detectarse atribuciones inadecuadas.

El reto: Certificación de accesos

"Quiero realizar certificaciones sencillas e intuitivas para poder aumentar la productividad de mis gestores y simplificar mis auditorías de conformidad".

Ya hemos visto la importancia de contar con una capacidad automatizada de traducir la información de acceso de los usuarios al idioma y formato adecuados para cada tipo de campaña de certificación que ponga en marcha. Si los nombres de acceso son intuitivos y fáciles de usar para los usuarios empresariales, se puede designar un flujo de trabajo flexible para satisfacer sus necesidades individuales, y si el seguimiento y el estado de todas las campañas están disponibles fácilmente, su programa de certificación tendrá más posibilidades de funcionar correctamente.

La solución de CA Identity Suite

Las capacidades de certificación de CA Identity Suite se basan en el catálogo de atribuciones adecuado para la empresa, que hace que los gestores entiendan de una forma muy sencilla los derechos de acceso de todos los empleados, además de que puedan aprobarlos, rechazarlos o delegarlos. Asimismo, existe una valoración del riesgo disponible para los gestores si algún derecho (o combinación de derechos) de acceso es especialmente peligroso. Al activar la visibilidad de estas evaluaciones de riesgos, la certificación se convierte no solo en una proposición "sí/no", sino en una que puede destacar los riesgos que no serían visibles de otra forma.

CA Identity Suite presenta la flexibilidad necesaria para admitir muchos tipos de campañas de certificación, entre las que se incluyen:

- **Certificación de entidades:** Se utiliza para certificar los derechos de acceso asociados a los usuarios, los roles o las entidades de recursos seleccionados por gestores, los propietarios de roles y los encargados de recursos, respectivamente.
- **Renovación de la certificación:** Le permite repetir el proceso de certificación basado en una campaña previa.
- **Diferencial:** Inicia una campaña de certificación basada exclusivamente en las atribuciones que han cambiado desde una campaña anterior.
- **Autoatestación:** Permite que todos los usuarios, en lugar de un gestor o un encargado de recursos, certifiquen sus propios privilegios. Este tipo de campaña podría satisfacer algunos requisitos legales para la certificación en materia de seguridad de datos.

Las campañas de certificación pueden requerir mucho tiempo, ser tediosas y, finalmente, no ser eficaces como actividad de reducción de riesgos. CA Identity Suite no solo mejora la efectividad de este proceso en cuanto a seguridad y conformidad, sino que lo lleva a cabo de forma simple y muy intuitiva, algo que a los gestores les encanta.

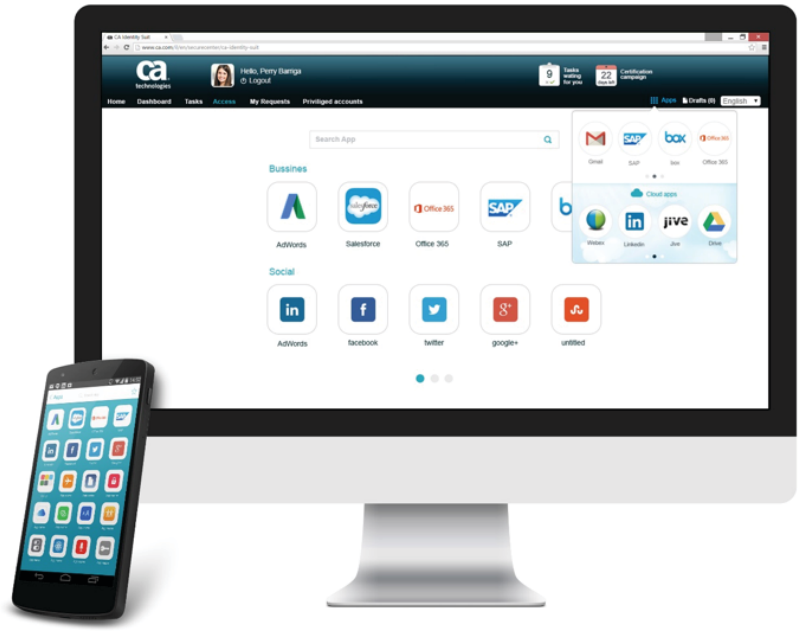
El reto: Un acceso práctico a las aplicaciones

"Me gustaría que mis usuarios pudieran acceder de una forma muy sencilla a todas sus aplicaciones, tanto en la nube como in situ, pero solo a aquellas de las que tengan los derechos de acceso adecuados. Además, necesito acceder fácilmente a todos sus dispositivos".

Los usuarios se frustran cuando tienen que realizar pasos complicados para conseguir acceder a una de sus múltiples aplicaciones. Suelen quejarse de que cuentan con muchas claves de inicio y de la incapacidad de iniciar las aplicaciones de una forma sencilla. Además, como la movilidad aumenta y los usuarios se acostumbran a convivir con las interfaces de esos dispositivos, los retos relacionados con la frustración y la productividad pueden aumentar. Es necesario un método cómodo para conseguir acceder de forma fácil y segura a todas las aplicaciones de los usuarios, que ofrezca un inicio de sesión único para todos y que solamente incluya las aplicaciones a las que cada usuario esté autorizado a acceder.

La solución de CA Identity Suite

CA Identity Suite incluye una Web y un panel de inicio de aplicaciones móviles que proporciona a los usuarios un único cuadro de mandos para acceder de forma rápida y sencilla a todas las aplicaciones web, en la nube y móviles autorizadas. Al panel de inicio se puede acceder desde cualquier dispositivo y ofrece capacidades de búsqueda mejoradas. Una vez que los usuarios hayan iniciado sesión en CA Identity Portal, podrán acceder con un solo clic a todas las aplicaciones web y, además, a todas las aplicaciones a las que los usuarios acceden en su escritorio estarán siempre disponibles a través de CA Identity Portal Mobile desde sus dispositivos móviles. Este panel de inicio consigue que los empleados sigan siendo productivos estén donde estén gracias al completo inicio de sesión único a las aplicaciones web móviles en un formato adaptado a móviles.



El reto: Garantizar la eficiencia de los procesos para cumplir los acuerdos de nivel de servicio:

"Algunos procesos relacionados con las identidades no funcionan demasiado bien, así que recibo quejas de otros gestores sobre los niveles de servicio que les proporcionamos. Lo que pasa es que no dispongo de suficiente información acerca de dónde se encuentran los cuellos de botella para intentar eliminarlos".

A menudo, los procesos relacionados con las identidades son complejos y pueden involucrar etapas de distintas fases de los flujos de trabajo. Cuando los procesos no funcionan de forma eficiente, como cuando un conjunto de usuarios sencillamente no logra concluir su tarea a tiempo, todo el sistema se puede ralentizar y cabe el riesgo de incumplir los objetivos del nivel de servicio. Eso puede desembocar en debilidades que registrarán las auditorías o, sencillamente, en una mayor ineficiencia cuando no se completan procesos básicos de acuerdo con los objetivos del servicio, como las certificaciones de acceso. Sin una visibilidad adecuada sobre los detalles de las operaciones de estos procesos resulta imposible identificar la causa de estos problemas, mucho más repararlos con rapidez.

La solución de CA Identity Suite

CA Identity Suite proporciona extensas funciones de análisis en tiempo real, para comprender y optimizar mejor el funcionamiento de los procesos fundamentales relacionados con las identidades. Esto puede contribuir a detectar los cuellos de botella y asegurarse de que cumpla con sus acuerdos de nivel de servicio. A modo de sencillo ejemplo, el gráfico que figura a continuación ofrece un panorama temporal de los acuerdos de nivel de servicio actuales durante el último mes, así como las cifras clave, como los acuerdos de nivel de servicio mínimos, máximos y medios correspondientes a un proceso concreto. También presenta la tasa de llegada de nuevas solicitudes distribuidas por cada día del mes anterior, así como un resume de la disposición (rechazadas o cumplidas) de todas esas solicitudes. Esta capacidad proporciona una perspectiva notablemente mejor para el gestor, de forma que permite optimizar los procesos y visualizar fácilmente si todos esos procesos se han completado o no.

El reto: Una difícil implementación

"La implementación de mi solución de gestión de identidades es difícil y exige mucho tiempo. En primer lugar, la mera instalación y configuración del software lleva días y además, a veces hacen falta semanas enteras para poner en marcha los casos prácticos más básicos, porque hace falta escribir código personalizado y definir flujos de trabajo, políticas y una interfaz de usuario".

Implementar una solución de gestión de identidades sólida puede suponer un reto y ser cara. Es fácil que pasen semanas hasta conseguir poner en marcha algunas capacidades básicas. Además, cualquier requisito como los conectores para aplicaciones personalizadas puede agotar recursos y ser un notorio sumidero de tiempo.

La solución de CA Identity Suite

CA Identity Suite puede reducir *drásticamente* el tiempo necesario para ponerse en funcionamiento, gracias a las siguientes capacidades:

- **Virtual Appliance (vApp).** vApp elimina la fase convencional dedicada a la instalación y ofrece una imagen de máquina virtual preinstalada y preconfigurada, lista para ejecutarse en configuraciones de producción bajo las plataformas de virtualización más comunes. Virtual Appliance incrusta un sistema operativo protegido, un servidor de aplicaciones y el software CA Identity Suite. También incluye compatibilidad integrada para procedimientos comunes de DevOps, como configuraciones de alta disponibilidad, ajustes de capacidades, agregaciones de registros, parches para plataformas y actualizaciones de software.

  Para implementar servicios de identidades, basta con arrastrar el nombre del servicio hasta el nombre de la máquina correspondiente y la instalación se ejecutará automáticamente. Si suelta el mismo servicio sobre varias máquinas, todos los mecanismos de comunicación para la alta disponibilidad (equilibrado de cargas, conmutación por error, etc.) se prepararán automáticamente para usted. No hacen falta procesos de configuración manual, propensos a errores y que requieren mucho tiempo. El ahorro en cuestión de horas es tremendo.

  Este enfoque se traduce en una reducción drástica del tiempo de recuperación de la inversión y del coste total de propiedad, lo que permite alcanzar unos resultados mucho mejores con el mismo equipo y presupuesto. Este método también tiene potencial para ahorrar miles de euros al año en materia de costes de licencias de software, dado que todos los componentes principales del sistema se pueden implementar de forma gratuita, sin necesidad de adquirir más licencias.
- **Deployment Xpress (Depx).** DepX representa un salto cualitativo radical en la forma de implementar el software de gestión de identidades. Consta de una colección de escenarios de usuarios preconfigurados para los casos de los usuarios más comunes, los que requiere la mayoría de organizaciones, incluidos la incorporación de nuevos usuarios, el restablecimiento de contraseñas, las certificaciones de acceso, la incorporación de partners y similares. Cada escenario está compuesto por todos los elementos necesarios para que la implantación sea sencilla, como plantillas de interfaces de usuario, flujos de trabajo y definiciones de políticas. El gestor no tiene más que elegir los escenarios que haga falta, ponerlos en el carro de la compra y pasar por caja. En este punto, todos los elementos clave se cargan automáticamente en Identity Suite y se implementan. Dichos elementos se pueden personalizar (por ejemplo, con una imagen de marca corporativa para la interfaz), pero la personalización no implica escribir código específico. Esos escenarios aceleran el proceso de implementación y tiene potencial para reducir de forma significativa el tiempo de recuperación de la inversión para la implantación de los servicios de identidades más comunes.
- **Otras herramientas Xpress.** Identity Suite incluye más herramientas para perfeccionar notablemente el proceso de gestionar su entorno de implementación como las siguientes:
  - Connector Xpress simplifica el proceso de creación de conectores para aplicaciones de desarrollo propio y facilita la conexión a sistemas que no cuenten con conectores listos para usar.
  - Config Xpress le permite trasladar de forma rápida y sencilla los componentes entre los entornos de almacenamiento intermedio para simplificar la gestión de la configuración y disponer de más tiempo para las pruebas de funcionamiento.
  - Policy Xpress le permite configurar políticas que ejecuten sus exclusivos y complejos procesos empresariales. Normalmente, esto se consigue mediante código personalizado, pero esta herramienta basada en un asistente le permite crear políticas internas en cuestión de horas, en lugar de estar semanas programando.

Funciones principales

CA Identity Suite ofrece estas funciones principales:

- Portal de identidades autoservicio (una plataforma para todo): Centraliza los datos de atribuciones y proporciona un carrito de la compra de solicitudes de acceso intuitivo.
- Reducción drástica del tiempo de implementación, de días a minutos.
- Catálogo de atribuciones adecuado para la empresa: Hace que las solicitudes de acceso y la certificación de atribuciones resulten más comprensibles para los usuarios empresariales.
- Análisis proactivo: Realiza recomendaciones, previene y alerta al usuario empresarial de posibles infracciones de las políticas.
- Aprovisionamiento de usuarios de una amplia gama de aplicaciones in situ, servicios SaaS y sistemas no conectados.
- Autoservicio de usuarios: Permite que los usuarios gestionen su propia información para reducir la carga del personal de TI.
- Deployment Xpress: Las plantillas de casos prácticos preconfiguradas facilitan en gran medida la implementación inicial y la posterior gestión continua.
- Personalización sin código personalizado: Funciones efectivas como Config Xpress, Policy Xpress y Connector Xpress, que permiten personalizar la infraestructura de gestión de identidades sin utilizar códigos personalizados.
- Depuración de privilegios: Se examinan las atribuciones del sistema existentes y se ponen de relieve los privilegios excesivos o innecesarios.
- Modelado de roles con un avanzado motor de análisis patentado: Ayuda a clasificar de manera eficaz grandes cantidades de información de usuarios y privilegios para detectar los posibles roles.

ca technologies

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**.

CS200-230014_1016