Mejorando la Gestión de Contraseñas al Adicionar Seguridad, Flexibilidad, y Agilidad

Guía de Solución de IBM Redbooks

El número de inicios de sesión y contraseñas que los empleados deben gestionar diariamente continúa siendo fuente de frustración y productividad perdida. Los empleados deben recordar información de inicio de sesión para varias aplicaciones. Muchas de estas aplicaciones requieren diferentes nombres de usuario y contraseñas, diferentes requerimientos de complejidad de contraseñas, y cambios forzados de contraseña en intervalos más cortos. El número de inicios de sesión que debe gestionar un empleado crece con el desarrollo de cada aplicación de negocios adicional. El help desk corporativo usualmente padece el proceso de restauración de información de inicio de sesión perdida u olvidada para un empleado. Juntos, estos factores contribuyen a riesgos de seguridad e incrementan los costos de help desk, que pocas organizaciones pueden darse el lujo de no abordar.

Al usar IBM® Security Access Manager for Enterprise Single Sign-On, su organización puede abordar estos serios desafíos de seguridad, productividad y conformidad en una solución gestionada centralmente. La Figura 1 ilustra la visión general de esta solución.

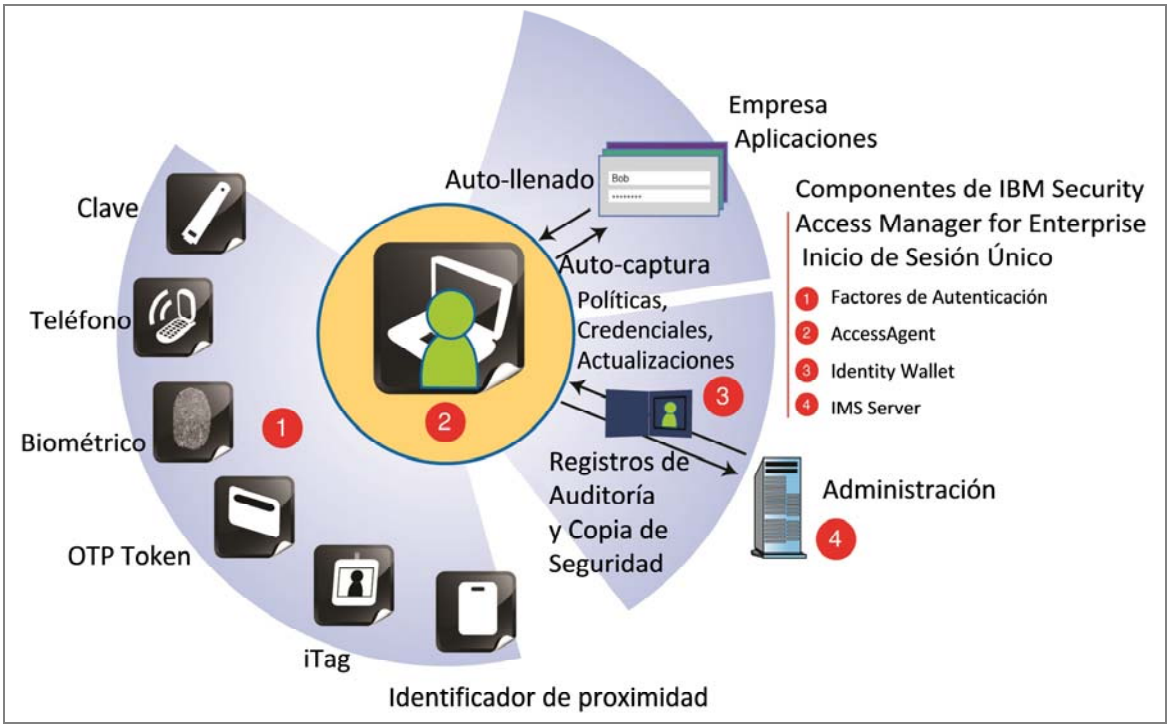

Figura 1. Visión General de IBM Security Access Manager for Enterprise Single Sign-On

¿Sabía qué?

Una queja frecuente de los usuarios es el requerimiento de recordar múltiples contraseñas, y una mayor debilidad en la seguridad de computadoras es una contraseña débil. Las violaciones de seguridad como resultado de contraseñas débiles o gestión no segura de contraseñas son comunes. Proporcionando una solución centralizada para gestión de contraseñas y autoservicio, mecanismos de autenticación fuertes y flexibles, y la posibilidad de usar estaciones de trabajo compartidas y virtuales hacen de IBM Security Access Manager for Enterprise Single Sign-On una solución destacada.

Valor para los negocios y visión general de la solución

IBM Security Access Manager for Enterprise Single Sign-On puede ayudarle a resolver la paradoja de las contraseñas. Los usuarios sólo deben recordar una contraseña y ya no tienen que lidiar con contraseñas robustas para todas las aplicaciones corporativas. Auntentican en una sola ocasión, e IBM Security Access Manager for Enterprise Single Sign-On realiza el resto. IBM Security Access Manager for Enterprise Single Sign-On proporciona los siguientes valores importantes para los negocios:

- Gestionando contraseñas de una manera abundante en seguridad

  IBM Security Access Manager for Enterprise Single Sign-On da seguridad a las aplicaciones y datos relacionados con contraseñas. Usa la criptografía más robusta que está disponible, incluyendo Advanced Encryption Standard (AES) y Triple Data Encryption Standard (DES). IBM Security Access Manager for Enterprise Single Sign-On está en conformidad con el Federal Information Processing Standard (FIPS) 140-2 para ayudar a las instituciones financieras, agencias gubernamentales, cuidado de la salud, y otras organizaciones a cumplir con las rígidas normatividades de privacidad y seguridad que gobiernan sus operaciones. IBM Security Access Manager for Enterprise Single Sign-On también ofrece autenticación de segundo factor para incrementar más la seguridad. Permite la mezcla y coincidencia de diferentes factores, dependiendo del usuario o de la máquina. Si estos factores existen, IBM Security Access Manager for Enterprise Single Sign-On puede usarlos.

- Reduciendo los costos de help desk y mejorando la productividad de los empleados

  La funcionalidad de restablecimiento de contraseñas de autoservicio de IBM Security Access Manager for Enterprise Single Sign-On puede reducir o eliminar costos que son asociados con contraseñas olvidadas y pérdida de productividad de empleados debido a cierres de cuentas. Las contraseñas olvidadas y cierres de cuentas, como resultado de demasiados intentos fallidos, pueden ser una gran carga para el help desk de la compañía. IBM Security Access Manager for Enterprise Single Sign-On proporciona funciones configurables de manera que los usuarios puedan realizar autoservicio de contraseñas de maneras que satisfagan los diversos requerimientos de seguridad. El cómo los usuarios pueden interactuar con cambios en contraseñas, restablecimientos, y funciones de trabado y destrabado de cuentas puede personalizarse y permitirse o no con base en políticas configurables. IBM Security Access Manager for Enterprise Single Sign-On otorga a las compañías la flexibilidad para decidir si estas funciones de contraseñas y servicio de cuentas permanecen con el help desk, el usuario, o una combinación de ambos. La función de restablecimiento de contraseñas proporciona la posibilidad de restablecer su contraseña de IBM Security Access Manager for Enterprise Single Sign-On para volver a obtener acceso a su entorno de escritorio. No restablece ninguna contraseña específica de aplicación.

- Demostrando la conformidad a través de auditorías e informes

  IBM Security Access Manager for Enterprise Single Sign-On incluye auditoría e informes incorporados para actividades de usuario detalladas en el escritorio empresarial. Puede registrar eventos de auditoría, incluyendo inicio de sesión de usuario y cierre de sesión de aplicaciones. El mecanismo de auditoría puede ser personalizado para capturar otra información relevante que esté relacionada a las actividades del usuario. El producto se embarca con varios informes incluidos, pero se pueden generar informes personalizados debido a que todos los datos de auditoría están en una única base de datos relacional que puede ser consultada.

- Fácil de desplegar

  La implementación y la gestión de IBM Security Access Manager for Enterprise Single Sign-On se hacen efectivas con una consola administrativa basada en web, integración de directorios de primera, y software del lado del cliente fácilmente desplegable. Todas las funciones administrativas son realizadas desde una consola administrativa web centralizada(AccessAdmin). Los asistentes de apuntar y hacer clic en la aplicación AccessStudio acompañan al administrador a través de las tareas de configuración de perfil. Un administrador puede acceder a la consola AccessAdmin desde cualquier lugar donde un navegador web pueda conectarse al servidor. IBM Security Access Manager for Enterprise Single Sign-On usa un repositorio de usuario pre-existente sin necesidad de modificar el esquema del directorio o cualquier otro aspecto del repositorio del usuario.

- Alto Rendimiento

  En todos los entornos de escritorio privados, compartidos y de roaming, IBM Security Access Manager for Enterprise Single Sign-On puede entregar velocidad exigente. Usa recursos mínimos cuando proporciona una experiencia única de inicio de sesión(SSO) para los usuarios en sus aplicaciones. Con su uso de recursos específicos para evento, el efecto de IBM Security Access Manager for Enterprise Single Sign-On en el cliente y en la red es mínimo. No se requiere de hardware o software adicional.

- Integración con un sistema de gestión de identidad empresarial

  The IBM Security Access Manager for Enterprise Single Sign-On Provisioning Bridge amplía los beneficios que son generados por IBM Security Access Manager for Enterprise Single Sign-On a través de la automatización del proceso de distribución de credenciales. IBM Security Access Manager for Enterprise Single Sign-On Provisioning Bridge usa sus bibliotecas API libraries para permitir que el software de gestión de identidad suministre automáticamente credenciales de usuario IBM Security Access Manager for Enterprise Single Sign-On. De esta manera, los usuarios nunca tienen que saber su nombre de usuario o contraseña para sus aplicaciones porque pueden gestionarse transparentemente para ellos.

  Si los usuarios necesitan saber su nombre de usuario y contraseña para una aplicación particular, pueden obtener la información accediendo a la tienda de credenciales (Wallet). Este acceso es posible solo si son autenticados para IBM Security Access Manager for Enterprise Single Sign-On. Si no están trabajando en una estación de trabajo con un AccessAgent, pueden acceder esa información usando la interfaz basada en navegador web AccessAssistant. Incluso si no están integrados con el software de gestión de identidad, IBM Security Access Manager for Enterprise Single Sign-On permite un proceso seguro de revelación de contraseñas altamente disponible para estos componentes.

- Llevando SSO a las máquinas de quiosco y escritorios virtuales

  La conveniencia de permitir a otros compartir una estación de trabajo desafortunadamente no viene sin riesgos. Muy frecuentemente los usuarios salen de una máquina de quiosco sin cerrar sesión, potencialmente exponiendo datos delicados. IBM Security Access Manager for Enterprise Single Sign-On aborda esta amenaza con su habilidad de automatizar la finalización de sesiones inactivas y cierre de aplicaciones. Esa automatización incluye características como cierres de sesión automáticos, a través de llaves de proximidad de identificación de radio frecuencia (RFID), o remoción de tarjeta inteligente.

  IBM Security Access Manager for Enterprise Single Sign-On proporciona soporte de gestión de sesión robusta para implementaciones de escritorio de servicio itinerante. Usa tecnologías como Microsoft Windows Terminal Services y Citrix XenApps, y usa escritorios compartidos o máquinas de quiosco y escritorios privados. Los usuarios pueden usar servicio itinerante fácilmente y de manera segura de una estación de trabajo a otra. IBM Security Access Manager for Enterprise Single Sign-On también incluye soporte para dar seguridad a tecnologías de infraestructura de escritorio virtual (VDI), como VMware View. Adicionalmente, IBM Security Access Manager for Enterprise Single Sign-On incluye acceso de cliente ligero y sin cliente a través del modo de escritorio de servicio itinerante y a través de Lugar de Trabajo Web.

Arquitectura de la solución

IBM Security Access Manager for Enterprise Single Sign-On proporciona su funcionalidad SSO al introducir una capa que autentica un usuario una vez y luego automáticamente detecta y maneja solicitudes subsecuentes para credenciales de usuarios.

IBM Security Access Manager for Enterprise Single Sign-On puede dividirse en los siguientes componentes arquitectónicos, como se ilustra en la Figura 1:

- Factores de Autenticación

  IBM Security Access Manager for Enterprise Single Sign-On da soporte a diversos factores de autenticación para autenticar al usuario. Además de la autenticación basada en nombre de usuario y contraseña estándares, los usuarios pueden ser autenticados por un identificador de proximidad o edificio. Los ejemplos son RFID activo o pasivo, una huella digital, una contraseña de un único uso (OTP) que se proporciona mediante Servicio de Mensajes Cortos (SMS) o token OTP, o un token USB.

- AccessAgent

  AccessAgent se ejecuta en cada punto final de escritorio Windows, sesión de Windows Server Terminal Services, sesión de interfaz de escritorio virtual VMware vSphere, y sesión de Citrix XenApp Presentation Server. AccessAgent es responsable por autenticar al usuario. Puede automatizar SSO en Windows y en el conjunto de aplicaciones que se definen en AccessProfiles. AccessAgent puede ampliar la cadena de la biblioteca de enlaces dinámica(DLL) de Windows Graphical Identification and Authentication (GINA) para proporcionar funciones adicionales additional para autoservicio o autenticación robusta.

- Identity Wallet

  Identity Wallet (o Wallet) contiene las credenciales de usuario que se requieren para SSO. Es cargado del IBM IMS™ Server en AccessAgent después de la autenticación exitosa del usuario de manera que esté disponible incluso cuando el punto final esté desconectado de la red de cómputo. Para proteger a las credenciales contra manipulación o robo, Identity Wallet está cifrado con un robusto mecanismo de cifrado.

- IMS Server

  IMS Server es el repositorio central para datos de usuario, AccessProfiles, Identity Wallets, y perfiles de máquina. IMS Server proporciona una interfaz basada en web para administrar usuarios y políticas.

Casos de ejemplo de usos

En este escenario de uso, un proveedor de cuidado de la salud opera varias clínicas independientes, donde cada clínica ocupa su propio edificio y proporciona cuidado preventivo, cirugía cardiaca, y servicios de pacientes externos. El proveedor de cuidado de la salud cuenta con un gran grupo de personal médico y de soporte que está directamente empleado por la compañía y un grupo más pequeño de cirujanos independientes que son contratados por la compañía.

El proveedor de cuidado de la salud mantiene los datos financieros y los datos privados de los clientes (pacientes, asociados de investigación y hospitales afiliados). La mayoría de los registros se mantienen en forma electrónica en sistemas SAP. Adicionalmente, hay email disponible para todo el personal de la compañía para comunicación interna y con el exterior (pacientes y asociados externos).

La Figura 2 muestra el diagrama de arquitectura de la compañía de cuidado de la salud, que incluye las líneas de comunicación importantes entre las zonas de red separadas.

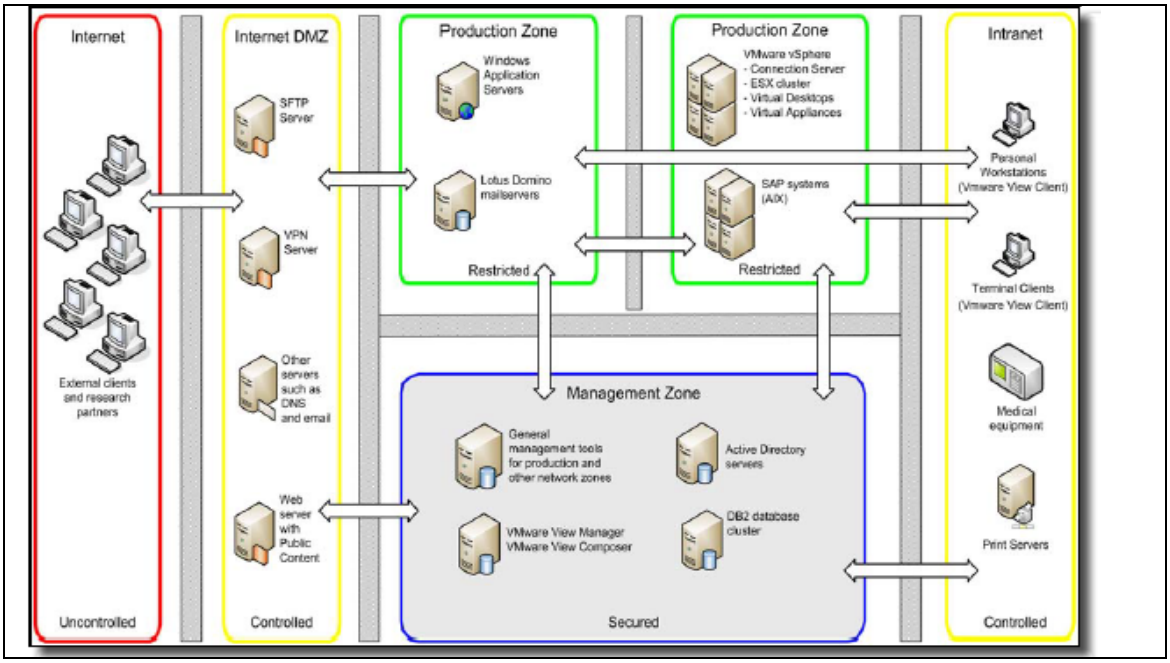

Figura 2. Visión general de la arquitectura actual de la compañía de cuidado de la salud

La compañía de cuidado de la salud desea cumplir las siguientes metas de negocios de corto plazo:

- Mejorar la calidad y disponibilidad del cuidado de los pacientes y su satisfacción al entregar una excelente experiencia individual de cuidado de la salud.
- Incrementar la protección de toda la información relacionada a pacientes, y abordar los diversos riesgos para la seguridad que son conducidos por los requerimientos de conformidad, tecnologías emergentes y explosión de datos.
- Facilitar la gestión y demostración de la postura general de conformidad con las leyes de privacidad de datos y regulaciones de la industria, como Health Insurance Portability and Accountability Act (HIPAA) y Payment Card Industry Data Security Standard (PCI-DSS).

En general, la compañía de cuidado de la salud desea soluciones de seguridad maduras que puedan prevenir fugas de información y que puedan asegurar una autenticación confiable y rastreabilidad individual y rendición de cuentas para todas las acciones que afectan a los pacientes.

Los siguientes componentes son desplegados para una implementación a nivel de base de IBM Security Access Manager for Enterprise Single Sign-On:

- Repositorio o directorio central de usuario

  El repositorio central de usuario puede ser uno de varios repositorios con soporte, incluyendo Active Directory, Novell, y Lightweight Directory Access Protocol (LDAP) genérico. El repositorio central de usuario debe estar implementado antes de instalar cualquier componente de IBM Security Access Manager for Enterprise Single Sign-On. En el entorno de la compañía de cuidado de la salud, el repositorio central de usuario es Active Directory, como se muestra en la Figura 2.

- IMS Server

  IMS Server es una aplicación que se basa en Java que ejecuta su propia instancia de IBM WebSphere® Application Server. Puede ser una instalación de software en una plataforma de servidor Windows, o puede integrarse en un dispositivo virtual empacado. IMS Server se despliega en la Management Zone mostrada en la Figura 2.

- Base de datos IMS

  La base de datos IMS almacena toda la configuración, políticas, y datos de usuario para IBM Security Access Manager for Enterprise Single Sign-On. Esta base de datos puede ser creada en un servidor existente de base de datos, o puede instalarse en el mismo sistema con el IMS Server. Las bases de datos con soporte incluyen IBM DB2®, Microsoft SQL y Oracle. En el entorno de la compañía de cuidado de la salud, se usa una base de datos DB2 existente como la base de datos, como se muestra en la Figura 2.

- AccessAgent

  Un AccessAgent se instala en cada sistema de cliente, Windows Terminal Server, VMware Virtual Desktop y servidor Citrix XenApp que vaya a ser gestionado por IBM Security Access Manager for Enterprise Single Sign-On.

- AccessStudio

  AccessStudio es una herramienta administrativa que se usa para crear AccessProfiles. Debe instalarse en sólo una estación de trabajo, normalmente en la estación de trabajo de uno o más administradores de IMS Server. Debido a que AccessStudio require AccessAgent, usted instala AccessAgent en la misma estación de trabajo antes de instalar AccessStudio.

Después de desplegar los componentes de infraestructura base, el proveedor de cuidado de la salud implementa las siguientes posibilidades:

- Autoservicio de contraseñas

  Si los usuarios en la compañía de cuidado de la salud olvida su contraseña de Microsoft Windows, ellos deben ponerse en contacto con el área de soporte de TI para que dicho personal restaure su contraseña a nombre de ellos después de haber realizado las verificaciones de seguridad necesarias. IBM Security Access Manager for Enterprise Single Sign-On supera este problema al proporcionar la función de autoservicio de contraseña del producto. Los usuarios que tienen conexión al IMS Server pueden restablecer sus propias contraseñas.

Al usar el dispositivo de autoservicio de contraseña de IBM Security Access Manager for Enterprise Single Sign-On, los usuarios pueden restablecer su autenticación primaria desde cualquier estación de trabajo, con base en un proceso de respuestas a cuestionamientos. (La autenticación primaria puede ser la contraseña de IBM Security Access Manager for Enterprise Single Sign-On o la contraseña del escritorio.) Todas las preguntas son personalizables y configurables. Cuando se configura el autoservicio de contraseñas de IBM Security Access Manager for Enterprise Single Sign-On (no se necesitan instalar componentes adicionales), el usuario no tiene necesidad de llamar al soporte técnico. Además, el usuario no tiene que esperar a que un administrador restablezca la contraseña. En vez de eso, los usuarios proporcionan secretos secundarios que establecen durante la fase de inscripción a AccessAgent. No se deben instalar componentes adicionales para usar la función de autoservicio de contraseña.

- Autenticación robusta usando RFID

  La compañía de cuidado de la salud desea usar una manera segura para *conmutación rápida de usuario* para su personal médico. Estos usuarios, que usan los clientes de terminal compartidos que están esparcidos a lo largo de hospitales, necesitan una manera más rápida y conveniente para iniciar sesión en el sistema. El personal médico usualmente necesita actualizar un registro de paciente con algunos breves comentarios antes de atender al próximo paciente, pero necesitan alimentar breves comentarios frecuentemente todos los días. Además, el personal médico necesita alimentar su nombre de usuario y contraseña (compleja) varias veces por día para acceder a su entorno de escritorio virtual, lo que genera frustración. La compañía está comprometida a abordar este problema. Sin embargo no está dispuesta a poner en riesgo la seguridad.

  La compañía del cuidado de la salud optó por desplegar lectores de identificadores RFID para todos los clientes de terminal compartida. Al usar esta función, el personal médico puede enlazar su identificador de acceso RFID a su nombre de usuario y contraseña SSO. Esta política está diseñada para solicitar al personal médico presentar su identificador RFID y su contraseña una vez por día. Para recordatorio de su turno, el personal puede presentar su identificador RFID en el lector, y posteriormente inician sesión automáticamente en su SSO Wallet.

- Implementación de escritorio itinerante

  Cuando un usuario inicia sesión en una estación de trabajo compartida en un área semi-pública al usar una contraseña o un identificador RFID, se inicia automáticamente una conexión al Escritorio Virtual de este usuario. El proceso de inicio de sesión del usuario en este Virtual Desktop debe darse a través de métodos seguros a prueba de falsificaciones.

  un usuario que haya iniciado sesión en una Virtual Desktop debe ser capaz de usar las aplicaciones con soporte sin proporcionar credenciales de autenticación. Esta función debe trabajar igual que las aplicaciones ejecutadas en la estación de trabajo compartida de donde se conectan. Cuando un usuario cierra sesión desde una estación de trabajo compartida, el escritorio virtual itinerante y sus aplicaciones deben continuar ejecutándose en la infraestructura virtual. Las políticas de inactividad de estación de trabajo deben ser tan estrictas como sea posible para prevenir que otras personas accedan a la sesión prolongada de Virtual Desktop. Las sesiones inactivas necesitan terminar automáticamente.

  Los miembros del personal médico usan estaciones de trabajo distribuidas para iniciar sesión automáticamente usando sus identificadores RFID y se conectan a sus escritorios virtuales que están hospedados en un VMware ESXi Server. La Figura 3 ilustra la arquitectura de componente de solución de destino.

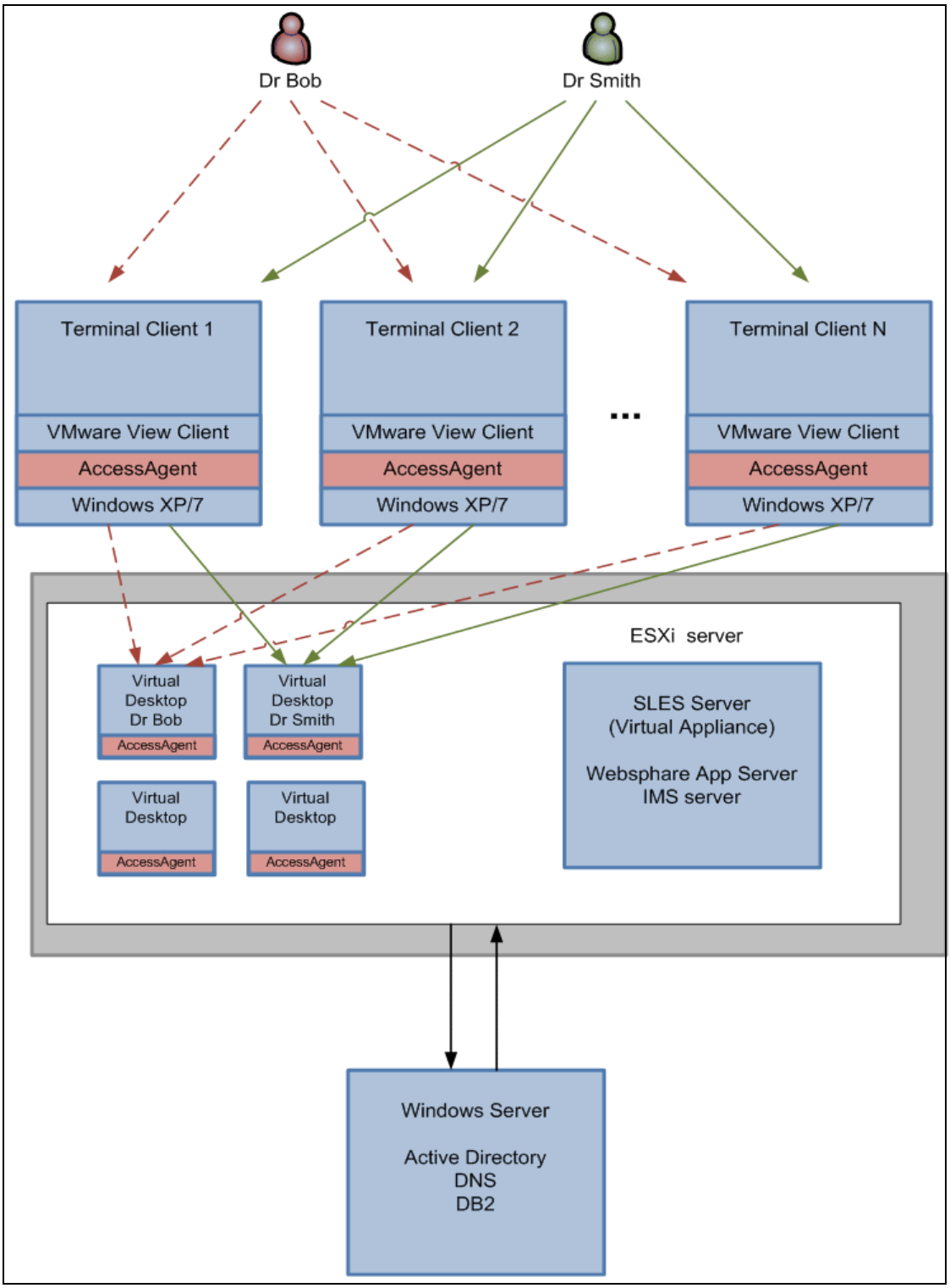

Figura 3. Arquitectura de escritorio intinerante

Información de pedido

Este producto sólo está disponible a través de IBM Passport Advantage®. No está disponible como un producto empaquetado La información detallada para pedidos está disponible en las cartas de anuncio de IBM (ver la sección de "Información Relacionada").

Información relacionada

Para información adicional, consulte los siguientes documentos:

- *Guía de Diseño de Enterprise Single Sign-On Usando IBM Security Access Manager for Enterprise Single Sign-On 8.2*, SG24-7350
  http://www.redbooks.ibm.com/abstracts/sg247350.html?Open

- *BIO-key Biometric Service Provider for IBM Security Access Manager for Enterprise Single Sign-On*, REDP-4892
  http://www.redbooks.ibm.com/abstracts/redp4892.html?Open

- *Una Guía para Servicios de Autenticación en IBM Security Access Manager for Enterprise Single Sign-On*, REDP-4835
  http://www.redbooks.ibm.com/abstracts/redp4835.html?Open

- *Una Guía para Escribir Perfiles de Acceso Avanzados para IBM Tivoli Access Manager for Enterprise Single Sign-On*, REDP-4767
  http://www.redbooks.ibm.com/abstracts/redp4767.html?Open

- *Configuración para IBM Tivoli Access Manager for Enterprise Single Sign-On 8.1 para Entornos de Único Servidor y Clúster*, REDP-4700
  http://www.redbooks.ibm.com/abstracts/redp4700.html?Open

- Página de producto IBM Security Access Manager for Enterprise Single Sign-On
  http://www.ibm.com/software/tivoli/products/access-mgr-esso

- Cartas de anuncio y Manuales de ventas IBM
  http://www.ibm.com/common/ssi/index.wss?request_locale=en

  En esta página entre a `IBM Security Access Manager for Enterprise Single Sign-On`, y haga clic en **Buscar**. En la página siguiente, refine los resultados de su búsqueda por tipo de información, geografía, idioma o las tres opciones juntas.

Avisos

Esta información ha sido desarrollada para productos y servicios ofrecidos en EE.UU.

IBM puede no ofrecer los productos, servicios o dispositivos tratados en el presente documento en otros países. Consulte a su representante IBM local, para información adicional sobre los productos y servicios disponibles en su área. Cualquier referencia a un producto, servicio o programa IBM, no pretende declarar ni implica que solo puedan utilizarse productos, servicios o programas de IBM. En su lugar, puede utilizarse cualquier producto, servicio o programa funcionalmente equivalente que no infrinja cualquier derecho de propiedad intelectual de IBM. No obstante, el usuario es responsable por evaluar y verificar el funcionamiento de cualquier producto, servicio o programa no IBM. IBM puede tener patentes o solicitudes de patentes pendientes de aplicaciones que tratan los asuntos descritos en el presente documento. La entrega del presente documento no le otorga ninguna licencia sobre dichas patentes. Puede enviar consultas sobre licencias, por escrito, a:

IBM Director of Licensing, IBM Corporation, North Castle Drive, Armonk, NY 10504-1785 U.S.A.

El siguiente párrafo no se aplica al Reino Unido u otros países donde dichas disposiciones sean incompatibles con la legislación local: INTERNATIONAL BUSINESS MACHINES CORPORATION SUMINISTRA LA PRESENTE PUBLICACIÓN "COMO ESTÁ" SIN GARANTÍA DE NINGUNA CLASE, EXPRESA O IMPLÍCITA, INCLUYENDO, PERO SIN LIMITACIÓN, LAS GARANTÍAS IMPLÍCITAS DE NO VULNERACIÓN, COMERCIALIZACIÓN Y ADECUACIÓN PARA UN PROPÓSITO PARTICULAR. Algunos Estados no permiten la exclusión de garantías expresas o implícitas en ciertas transacciones, por lo tanto, esta declaración puede no aplicarse a su caso. Esta información puede incluir imprecisiones técnicas o errores tipográficos. Periódicamente se hacen cambios a la presente información; dichos cambios se incorporarán en nuevas ediciones de la publicación. IBM puede introducir mejoras o cambios en los productos o programas descritos en la presente publicación a cualquier momento, sin aviso previo.

Cualquier referencia en esta información a sitios web no IBM se proporcionan únicamente para su comodidad y de ninguna manera constituyen un aval de dichos sitios web. Los materiales de dichos sitios web no forman parte de los materiales del presente producto IBM y el uso de dichos sitios web es a su propio riesgo. IBM puede utilizar o distribuir cualquier información que usted suministre de la manera que considere adecuada sin otorgarle ningún derecho. La información sobre productos no IBM se ha obtenido de los proveedores de dichos productos, de sus anuncios publicados o de otras fuentes públicamente disponibles. IBM no ha probado dichos productos y no puede confirmar la exactitud de rendimiento, compatibilidad u otras afirmaciones relacionadas a productos no IBM. Preguntas sobre las capacidades de los productos no IBM deben dirigirse a los proveedores de dichos productos. La presente información contiene ejemplos de datos e informes utilizados en las operaciones de negocio diarias. Para ilustrarlos de la manera más completa posible, los ejemplos incluyen nombres de personas, empresas, marcas y productos. Dichos nombres son ficticios y cualquier semejanza con los nombres y las direcciones utilizadas por una empresa real es pura coincidencia.

Los datos de rendimiento contenidos aquí se han determinado en un entorno controlado. Por lo tanto, los resultados obtenidos en entornos operativos diferentes pueden variar significativamente. Algunas mediciones pueden haberse realizado en sistemas en desarrollo y no existe ninguna garantía de que dichas mediciones serán las mismas en sistemas generalmente disponibles. Además, algunas mediciones pueden haber sido estimadas mediante extrapolación. Los resultados actuales pueden variar. Los usuarios del presente documento deben verificar los datos aplicables a sus entornos particulares.

LICENCIA DE COPYRIGHT:

La presente información contiene programas de aplicación de muestra en el idioma de origen, que ilustran las técnicas de programación en diferentes plataformas operativas. Los programas de ejemplo se pueden copiar, modificar y distribuir en cualquier forma sin ningún pago a IBM, para fines de desarrollo, utilización, marketing o distribución de programas de aplicación compatibles con la interfaz de programación de aplicaciones de la plataforma operativa para la cual los programas de ejemplo están escritos. Estos ejemplos no han sido completamente probados bajo todas las condiciones. Por lo tanto, IBM no puede garantizar ni hacer cualquier afirmación sobre la confiabilidad, capacidad de servicio o función de dichos programas.

Este documento fue publicado o actualizado el 7 de diciembre de 2012.

Envíenos sus comentarios por una de las siguientes maneras:

- Formulario de visión online **Contact us** disponible en:
  ibm.com/redbooks
- E-mail a:
  redbook@us.ibm.com
- Envíe sus comentarios por correo a:
  IBM Corporation, International Technical Support Organization
  Dept. HYTD Mail Station P099
  2455 South Road
  Poughkeepsie, NY 12601-5400 U.S.A.

Este documento está disponible online en **ibm.com**/redbooks/abstracts/tips0943.html

Marcas registradas