AUTOMATION ANYWHERE

Seguridad de calidad empresarial para la automatización robótica de procesos

INTRODUCCIÓN

¿Por qué, después de más de 20 años de inversión en tecnologías de automatización de los procesos empresariales, se han automatizado menos del 20 % de las tareas? La primera razón es la falta de interfaces de programación de aplicaciones (API, por sus siglas en inglés) bien definidas en el 85 % de los sistemas empresariales. El resultado es un creciente aumento de trabajo pendiente de TI en cuanto a solicitudes de integración por parte de las líneas de negocio.

La automatización robótica de procesos nació con la visión de otorgar a los usuarios de negocios la posibilidad de crear bots de software que puedan interactuar con los sistemas empresariales tal como lo hacen los humanos. Los bots de RPA (Automatización robótica de procesos, por sus siglas en inglés) pueden iniciar sesión en las aplicaciones empresariales por medio de credenciales, igual que los humanos, y automatizar las tareas que involucran cualquier aplicación empresarial, incluidas las aplicaciones preexistentes sin API. El procesamiento de reclamos, el procesamiento de préstamos, las conciliaciones de cuentas, la creación o el envío de facturas y la generación de informes son solo algunos ejemplos de las automatizaciones posibles que se extienden a través de las diferentes disciplinas empresariales.

Es fácil ver el potencial de los ahorros sustanciales en tiempo y costos, la mejora en la satisfacción del cliente, el aumento en la moral de los empleados y la habilidad de construir una ventaja imponente por encima de los competidores mediante el uso de RPA. Sin embargo, la obtención completa de estas ganancias depende de si se cuenta con una solución de calidad empresarial.

Algunos de los criterios esenciales de la automatización son proveer confiabilidad sólida y absoluta, escalabilidad y una amplia gama de funciones determinadas para maximizar la aplicabilidad y la utilidad. Pero estos elementos no cubren el requisito fundamental de las empresas: la seguridad integral. Una arquitectura de seguridad sólida con funciones que permitan el soporte completo para los principios fundamentales, tales como privilegios menores y la separación de tareas durante la entrega de protección integral para las aplicaciones cruciales y los datos confidenciales involucrados, son esenciales.

En este artículo, se presenta una reseña sobre el estándar más alto de la industria en cuanto a la seguridad de calidad empresarial, tal como se demuestra en la plataforma de fuerza de trabajo digital líder del mercado, Automation Anywhere Enterprise.

“

Es fácil ver el potencial de los ahorros sustanciales en tiempo y costos, la mejora en la satisfacción del cliente, el aumento en la moral de los empleados y la habilidad de construir una ventaja imponente por encima de los competidores mediante el uso de RPA. Sin embargo, la obtención completa de estas ganancias depende de si se cuenta con una solución de calidad empresarial.

ARQUITECTURA Y OPERACIONES

Comprender los controles de seguridad que se necesitan para la implementación de RPA de calidad empresarial depende de la compresión de los componentes que constituyen la solución y las operaciones.

Componentes básicos

Tal como se muestra en la **Figura 1**, los componentes básicos de Automation Anywhere Enterprise son la sala de control, los creadores de bots y los ejecutores de bots.

Sala de control

La sala de control cumple la función de cerebro del entorno de automatización. Es un sistema de gestión de Windows basado en servidores, con una base de datos integral, que proporciona una visión unificada para el sistema de administración en general. La sala de control es también el lugar donde los operadores de RPA organizan la fuerza de trabajo digital; en otras palabras, programan, implementan, ejecutan, monitorean y administran las operaciones de los bots de la organización. Además, las funciones de control integradas de la versión (Apache Subversion Server) facilitan la colaboración de múltiples usuarios mientras que ejecutan las mejores prácticas de gestión de cambio y establecen un depósito centralizado de los bots listos para producción.

Creador de bots

El creador de bots se utiliza para construir bots. Es una aplicación de escritorio de Windows que funciona en una estación de trabajo o en una máquina virtual. Los expertos en procesos empresariales utilizan los creadores de bots para crear y evaluar las automatizaciones. Los bots se crean mediante el uso del editor de bots, mientras que las pruebas de bots, que utilizan datos de pruebas locales, no productivas e instancias de aplicaciones, se facilitan mediante el ejecutor de bots. Luego de las pruebas exitosas (por ej., de rendimiento, integridad de los datos y seguridad), los bots se registran en el depósito de la sala de control y quedan disponibles para la implementación de producción.

Ejecutor de bots

El ejecutor de bots pone en funcionamiento a los bots. Por medio del mismo código de aplicación que el creador de bots, pero con una clave de licencia diferente, el ejecutor de bots pone en funcionamiento a los bots en el entorno de producción; es decir, utiliza las instancias de producción de la aplicación de destino y de los almacenes de datos de producción. De hecho, poner en funcionamiento a los bots es todo lo que los ejecutores de bots pueden hacer, ya que las funciones de creación y edición no están disponibles para ellos. Para operaciones altamente confiables y de gran escala, también se admiten combinaciones de ejecutores de bots.

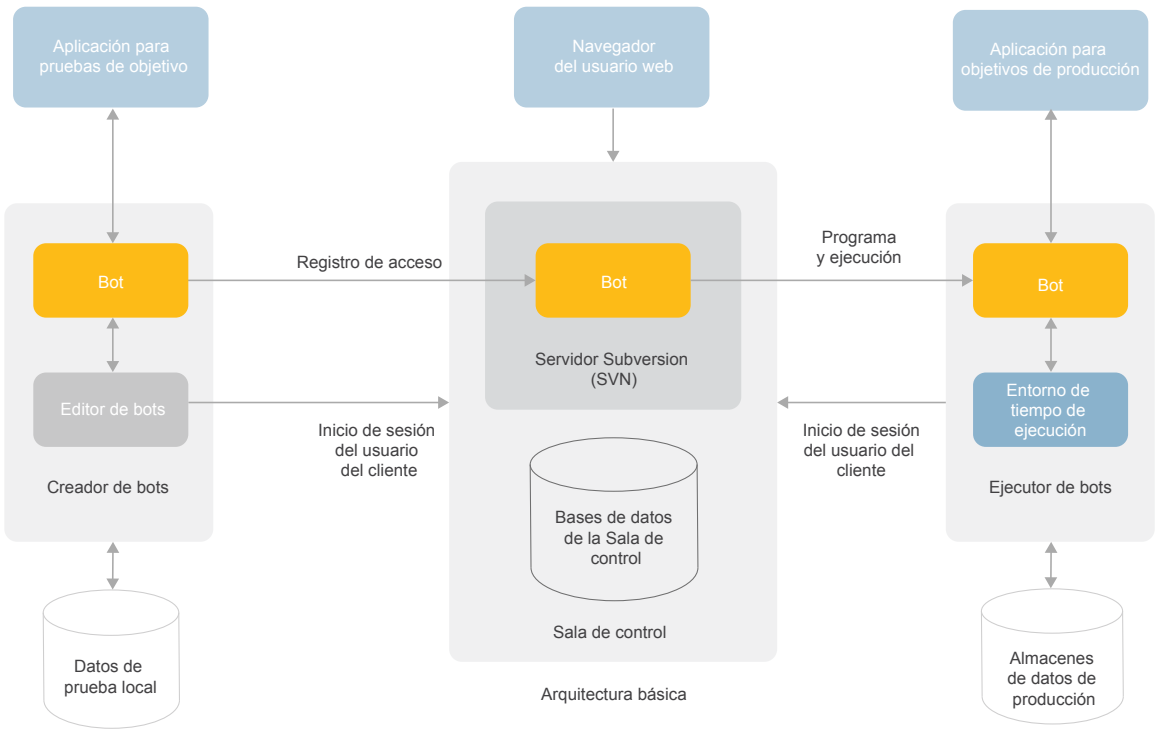

Figura 1: Arquitectura básica de Automation Anywhere Enterprise

Componentes adicionales de calidad empresarial

Al considerar operaciones de gran escala, surgen dos soluciones de RPA importantes para las organizaciones que buscan implementaciones de nivel empresarial: escalamiento bajo demanda y Bot Insight.

Escalamiento bajo demanda

Gracias a la nube pública Amazon Web Services (AWS, por sus siglas en inglés), Automation Anywhere Enterprise ofrece de manera eficaz a la RPA como un servicio, con todas las capacidades del asistente, que incluyen refuerzo o disminución flexible, medición basada en el uso, escalabilidad horizontal ilimitada, y monitoreo continuo y registro de auditoría de la infraestructura del ejecutor de bots. Como resultado, se obtiene una alta disponibilidad de varios nodos que alimenta el rendimiento basado en acuerdos de nivel de servicio (SLA, por sus siglas en inglés) y la continuidad del negocio, aun cuando existen fluctuaciones drásticas en la carga de trabajo de automatización.

Bot Insight

Bot Insight, un subsistema completamente integrado dentro de la sala de control, lleva a cabo análisis casi en tiempo real de las operaciones de los bots y de los datos de los procesos empresariales. Bot Insight genera automáticamente paneles personalizables mediante el uso de algoritmos únicos para cada bot. El nivel de detalle que Bot Insight proporciona, basado en el registro de incidencias detallado de las operaciones de los bots, permite enviar alertas sutiles, hacer descubrimientos ad hoc, hacer análisis en profundidad interactivos, series temporales de análisis y tener una visión completa de los procesos operacionales o empresariales. Además, todos los datos se pueden exportar a un Sistema de gestión de eventos e información de seguridad (SIEM, por sus siglas en inglés) para guardar los registros a fin de realizar análisis, investigaciones e informes adicionales.

Bots en acción: existen dos tipos de automatización

Antes de comenzar con las capacidades de seguridad de alto nivel de Automation Anywhere Entrerprise, es necesario aclarar que existen dos tipos básicos de automatización: asistida e independiente.

La automatización asistida es aquella en la que el usuario está registrado en la máquina del ejecutor de bots para observar o ayudar de manera activa en la ejecución del bot. Las razones para tener a un usuario presente se pueden deber a que el bot cumple una función de utilidad que ayuda en el trabajo o que el bot realiza un trabajo de tipo en lotes que requiere un aporte periódico o dirección circunstancial por parte de un usuario. A las automatizaciones asistidas también se las conoce como automatizaciones de servicio al cliente.

Las automatizaciones independientes, como su nombre lo indica, funcionan sin la necesidad de contar con la interacción del usuario u operador empresarial. Las automatizaciones independientes, por lo general, se ejecutan por medio de un operador que tiene poco conocimiento del bot, de la aplicación que se está automatizando o del propósito de la automatización. El operador, junto con la unidad de negocio, programa los bots para que funcionen por medio de los ejecutores de bots. Durante la ejecución, el operador monitorea los aspectos operacionales de los bots en funcionamiento, tales como el CPU, la memoria y el uso del almacenamiento, para asegurarse de que los bots se estén ejecutando sin errores o excepciones. Los paneles de la sala de control muestran todos los detalles operacionales de los bots mientras están en funcionamiento. Si una automatización independiente no termina su función debido a un error, el operador puede implementar procedimientos para reparar la automatización y reiniciarla; en caso contrario, el operador elevará la situación al equipo de RPA o a la unidad de negocio para diagnosticar y reparar el inconveniente.

IDENTIFICACIÓN Y AUTENTICACIÓN MULTICAPA PARA LA SEGURIDAD EMPRESARIAL PARA RPA MULTICAPA

Un principio fundamental de la arquitectura de seguridad de Automation Anywhere Enterprise es que no se permite el acceso o la acción sin la autenticación previa de la entidad involucrada. Esto aplica tanto para los humanos como para los bots. El resultado es un proceso de autenticación multicapa para ambas automatizaciones, asistidas e independientes.

QUIÉN ES QUIÉN: AUTENTICACIONES EMPRESARIALES TÍPICAS

Tanto las credenciales como las personas pueden ser multicapa. Considere un escenario de autenticación empresarial simple (vea la **Figura 2**). Un usuario de la empresa, Alice, se autentica en su estación de trabajo de Windows. Luego, Alice inicia sesión en una aplicación que se está ejecutando de manera remota. Lo hace mediante la autenticación de Directorio Activo de dominio de Windows o tal vez por medio de Kerberos instalado en su estación de trabajo y con un ticket válido. En este escenario, la cadena de autenticación involucra a una sola persona y sus credenciales.

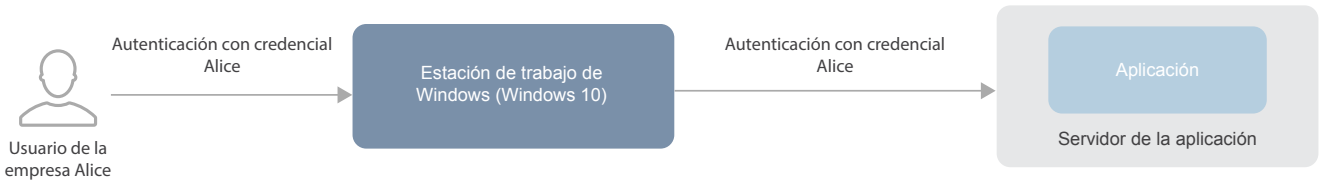

Figura 2: Autenticación empresarial típica

Ahora, considere un escenario de autenticación asistida como se ejemplifica en la **Figura 3**. En este caso, el usuario, Bob, le está realizando pruebas a un bot o bien está llevando a cabo una automatización asistida como parte de un día típico de trabajo. En el paso 1, él se autentica en la estación de trabajo del ejecutor de bots mediante sus credenciales personales (igual que en el escenario de Alice que se mencionó anteriormente). En el paso 2, él ejecuta el cliente de Automation Anywhere Enterprise e ingresa su identificación de usuario de la sala de control y contraseña; de esta manera, autentica el software del cliente con la sala de control. En el paso 3, pone en funcionamiento al bot que, a su vez, accede a la aplicación que requiere autenticación. Las credenciales que utiliza el bot en este paso pueden estar almacenadas en la bóveda de credenciales de la empresa y el bot las puede recuperar durante el tiempo de ejecución, o bien, puede haber una transmisión de las credenciales personales de Bob (basada en una autorización otorgada por su estación de trabajo y el servidor de la aplicación que se encuentra en el mismo dominio). En cualquiera de los casos, el resultado es un proceso de identificación y autenticación de tres capas en total.

Existen tres capas de autenticación que se utilizan en el escenario de automatización independiente que se describe en la **Figura 4**, pero con algunos cambios. En este caso, el usuario, Charles, comienza con la autenticación en la sala de control para poder seleccionar un bot para poner en funcionamiento, ya sea de manera inmediata o a una hora programada.

En el paso 2, cuando comienza la hora de ejecución del bot, la sala de control comienza un inicio de sesión automático en la estación de trabajo del ejecutor de bots, mediante el uso de la credencial del usuario del ejecutor de bots. Luego de que el bot se descarga en la función de jugador local (paso 3) y se empieza a ejecutar, se autentica en la aplicación de destino mediante el uso de la credencial del usuario de la aplicación bot (paso 4). Igual que en el caso del escenario de automatización asistida, la credencial del usuario de la aplicación bot puede ser una que se recuperó de la bóveda de credenciales o una que se transfirió de la credencial del usuario del ejecutor de bots.

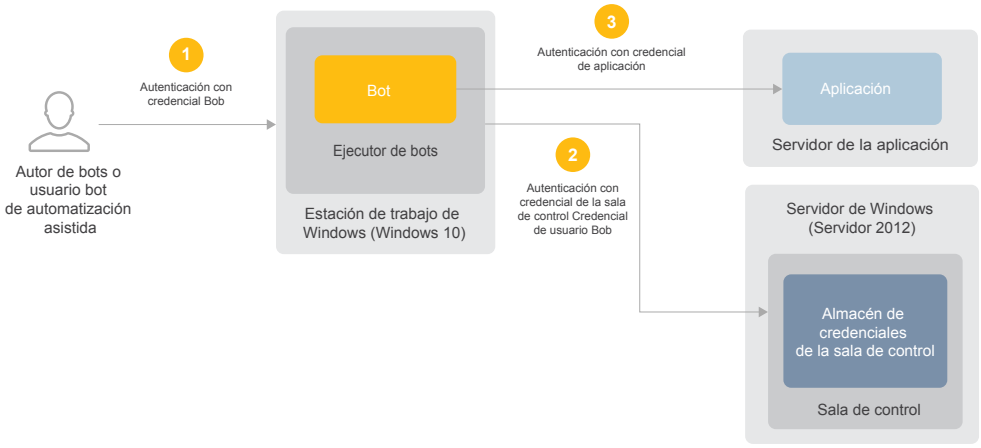

Figura 3: Proceso de autenticación en un escenario de automatización asistida

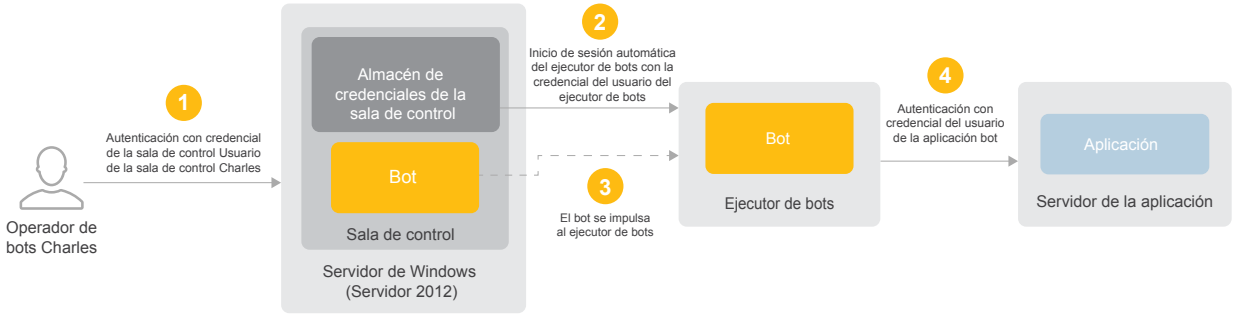

Figura 4: Proceso de autenticación en un escenario de automatización independiente

Opciones de autenticación e integraciones de Administración de identidad y acceso (IAM, por sus siglas en inglés)

Las opciones admitidas para la autenticación de la sala de control son Directorio Activo mediante Protocolo Simplificado de Acceso a Directorios (LDAP, por sus siglas en inglés), Directorio Activo mediante Kerberos y la autenticación local por medio del uso de la bóveda de credenciales integrada (que se desarrolla en una sección posterior).

Otras opciones de administración de identidad y acceso disponibles para las implementaciones empresariales son:

+ Soporte para SAML 2.0 basado en inicio de sesión único
+ Integración con soluciones de administración para accesos o credenciales privilegiados de terceros (por ej., CyberArk, One Identity y Thycotic)

CONTROL DE ACCESO BASADO EN ROLES COMPLETO

La autenticación exitosa es solo el primer nivel de la implementación del control de acceso obligatorio ofrecido por la arquitectura de seguridad de Automation Anywhere Enterprise. El soporte para el control de acceso basado en roles o RBAC detallado tiene igual importancia, especialmente a la hora de adherir a los principios fundamentales de los privilegios menores y la separación de tareas.

Se deben distinguir cinco roles diferentes (ver **Tabla 1**) dentro de la arquitectura básica y las funciones principales de la plataforma RPA. Los diseñadores de bots utilizan el creador de bots para capturar la lógica empresarial y así crear las automatizaciones correspondientes. Los diseñadores de bots trabajan con aplicaciones de prueba y conjuntos de datos para no producir un impacto en los sistemas de producción durante la etapa de desarrollo. Normalmente, un bot individual pasará por varias iteraciones y versiones diferentes, no solo durante el desarrollo inicial, sino también siempre que los procesos de negocios asociados o las aplicaciones de destino se actualicen. Los evaluadores de bots también trabajan con los creadores de bots para realizar pruebas en cuanto al desempeño, la integridad de datos y la seguridad, con el objetivo de garantizar que cada bot esté realizado las funciones para las cuales está destinado de manera segura. Los evaluadores de bots funcionan como una segunda etapa de autorización de los bots antes de que se puedan ejecutar con los datos y las aplicaciones de producción.

Una vez que el bot se evaluó y que pasó por una revisión de seguridad, el promotor de bots trabaja con los diseñadores de bots o evaluadores de bots para designar la versión del bot que se debería usar en la producción. Esta es la única versión del bot que estará visible para el operador de bots, que es el que coordina junto con las unidades de negocio para organizar y poner los bots en funcionamiento. El operador de bots también es responsable de monitorear el desempeño de los bots dentro de la sala de control, que incluye solucionar cualquier problema relativo al tiempo de ejecución que pueda ocurrir. Por último, la responsabilidad sobre la administración de la plataforma en general, como por ejemplo, la configuración de los componentes, las interfaces y todos los permisos o roles, recae en el administrador de RPA.

Separación avanzada de tareas

Este conjunto principal de roles demuestra un punto de partida básico para el Control de acceso basado en roles (RBAC, por sus siglas en inglés), pero una separación de tareas aun mayor es posible dentro de la plataforma Automation Anywhere Enterprise. Mediante el uso del asistente de creación de rol integrado, los administradores pueden, de manera fácil, definir los roles personalizados y configurar los privilegios o permisos que justifican el paquete completo de los objetos y las funciones de la sala de control, que incluye la administración de usuarios, licencias, bóveda de credenciales, conjuntos de ejecutores de bots, cronogramas de bots, operaciones o paneles de bots y registros de auditoría. A medida que se selecciona cada privilegio, el asistente agregará pasos de manera dinámica para los privilegios contingentes o derivados.

Por ejemplo, cuando se seleccionan los privilegios BOTS > Ver mis bots > Ejecutar mis bots (ver **Figura 5**), el flujo de trabajo agregará un paso para indicar las carpetas de bots específicas (es decir, conjuntos de bots) para las cuales se ha permitido el acceso. El resultado neto es la capacidad de establecer roles de alta confiabilidad con controles de acceso lo suficientemente detallados para cumplir con las necesidades de los entornos más rigurosos, seguros y regulados en cuanto a cumplimiento.

Rol	Descripción
Administrador de RPA	Administrador del sistema (configura los componentes, los roles, las interfaces
Diseñador de bots	Experto en procesos empresariales que diseña los bots con el editor de tareas y lleva a cabo pruebas funcionales básicas.
Evaluador de bots	Encargado de pruebas de control de calidad que revisa los bots en cuanto a la precisión operativa, desempeño y seguridad.
Promotor de bots	Administrador que aprueba y mueve a los bots entre las etapas de desarrollo, pruebas y producción.
Operador de RPA	Operador que programa, ejecuta y monitorea el el desempeño y la seguridad

Tabla 1: Roles de RPA principales en Automation Anywhere Enterprise

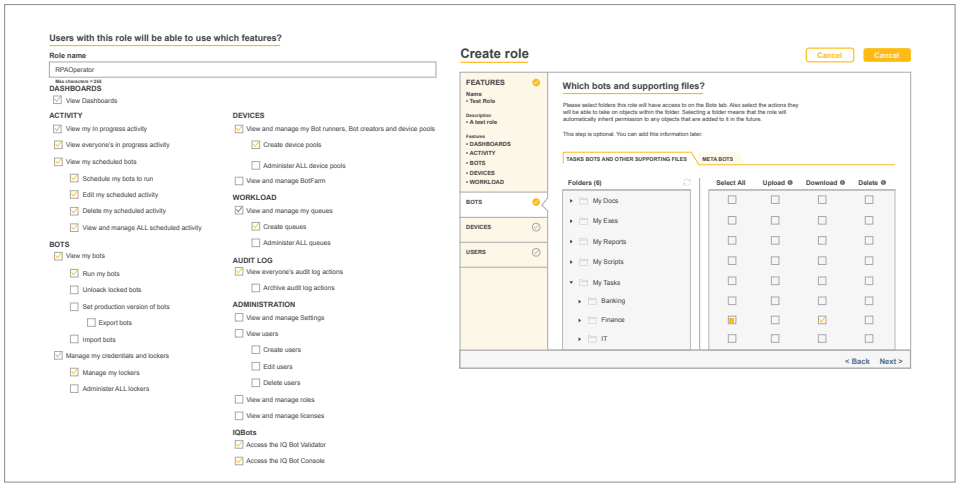

Figura 5: Creación de roles con autorización específica

Planos de control independientes

Más allá de las amplias capacidades de RBAC, Automation Anywhere Enterprise ofrece intrínsecamente una separación lógica de tareas al emplear una arquitectura que separa de manera minuciosa las operaciones de desarrollo y ejecución de bots.

Los creadores de bots solo pueden subir o descargar bots desde y hacia el sistema de control de versiones dentro de la sala de control. Al mismo tiempo, los ejecutores de bots se limitan a la ejecución de los bots, ya que no tienen acceso a las funciones de creación ni de pruebas. Esta separación de tareas ejecutada arquitectónicamente constituye una autorización doble acorde con las mejores prácticas del Instituto Nacional de Estándares y Tecnología (NIST, por sus siglas en inglés), puesto que requiere (como mínimo) un desarrollador y un usuario empresarial para habilitar en última instancia el proceso de automatización empresarial.

Dominios de procesamiento independientes

La creación de dominios de procesamiento independientes es un caso de uso importante para las capacidades de RBAC de la plataforma, en especial, para las empresas grandes (ver **Figura 6**). Esto se puede lograr mediante la estricta organización o almacenamiento de los bots para cada dominio en carpetas correspondientes dentro de la sala de control.

Buen ejemplo: aquellos bots asociados a aplicaciones de finanzas se deberán colocar en la carpeta de finanzas mientras que los asociados a RR. HH. se deberán asignar a la carpeta de RR. HH. A los operadores de bots del departamento de finanzas se les asignarán privilegios únicamente para los bots y ejecutores de bots de finanzas. De la misma manera, los operadores de bots de RR. HH. recibirán privilegios solo para bots y ejecutores de bots de RR. HH. y lo mismo sucederá para los otros dominios de procesamiento o automatización (ver **Figura 6**).

Como resultado final, se produce una separación de tareas adicional y el aislamiento de aplicaciones y datos asociados, en esta ocasión, en el nivel de UO o dominio, ya que los operadores individuales no pueden ver u operar los bots que se encuentran fuera de sus dominios establecidos.

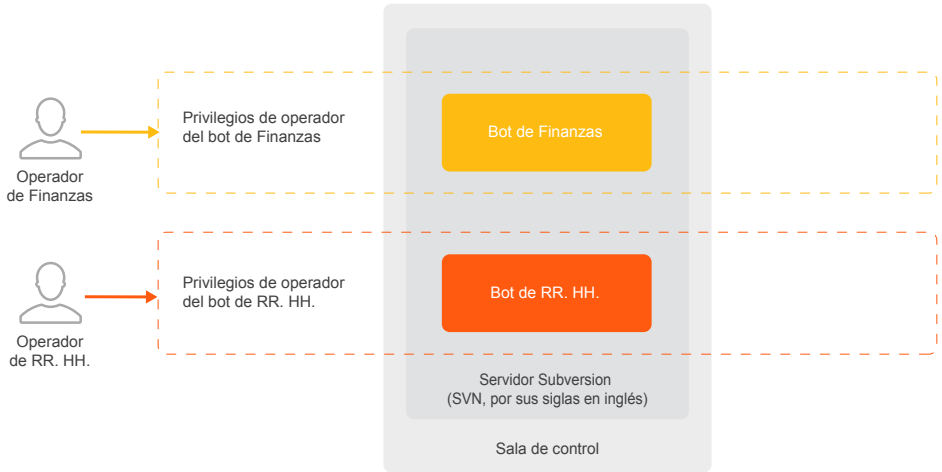

Figura 6: Soporte para dominios de procesamiento independientes

PROTECCIÓN DE DATOS INTEGRAL

La autenticación multicapa y el control de acceso específico son esenciales para conseguir un entorno estrictamente controlado. Por lo tanto, igual de importante es la protección de datos integral, ya que es necesaria para mantener la confidencialidad y la integridad de los procesos empresariales cruciales, de los datos sensibles y de los secretos asociados (por ej., credenciales).

La plataforma de Automation Anywhere Enterprise aborda esta necesidad con una bóveda de credenciales integrada y proporciona un conjunto amplio de medidas de protección que no solo protegen los datos en reposo o en tránsito, sino también cuando los datos están en uso en sistemas individuales.

Claves de cifrado y bóveda de credenciales

La **Figura 7** muestra las claves de cifrado principales que usa la plataforma, junto con su relación con la bóveda de credenciales. Todo el cifrado se realiza por medio de módulos criptográficos Nivel 1 validados por los Estándares Federales de Procesamiento de la Información (FIPS 140-2, por sus siglas en inglés).

Durante la instalación (parte izquierda de la **Figura 7**), el sistema genera un par de claves RSA de 2048 bits públicas o privadas y una clave AES de 256 bits. A la clave privada del par RSA 2048 se la denomina clave principal y a la clave AES 256 se la denomina clave de datos. Al administrador de instalación se le entrega la clave principal para que la resguarde en un lugar físicamente seguro fuera del sistema. La clave pública se usa para cifrar la clave de datos. Luego, la clave pública y la clave de datos cifrada se almacenan en la base de datos. Cuando están en uso, todas las claves y los datos cifrados se colocan en una memoria segura cifrada por medio de la API de protección de datos de Microsoft (DPAPI, por sus siglas en inglés).

Durante el arranque o reinicio de la sala de control (parte derecha de la **Figura 7**), se le solicita al administrador que ingrese la clave principal. La clave de datos cifrada se recupera desde la base de datos y se descifra con la clave principal. De esta manera, la clave de datos queda lista para usar. A medida que el sistema almacena y recupera datos desde la bóveda de credenciales, se usa la clave de datos para cifrar y descifrar esa información.

La bóveda de credenciales se usa para almacenar todas las credenciales gestionadas del sistema y los datos de configuración del sistema fundamentales. También se puede usar para guardar cualquier otro tipo de datos sensibles (por ej., pares nombre-valor) que se utilizan en las automatizaciones de las empresas. Como resultado, los diseñadores de bots pueden evitar la práctica insegura de codificar de forma rígida las credenciales y otros datos o argumentos directamente dentro de las automatizaciones.

Protección de los datos en reposo

Además de cifrar las credenciales locales y seleccionar los datos en tiempo de ejecución que utilizan los bots, la bóveda de credenciales ofrece un almacenamiento seguro para los parámetros de configuración sensibles y para los detalles pertenecientes al control de versiones integral y a los servicios de correo electrónico.

Protección de los datos en tránsito

Todos los servicios de red de los clientes y de la sala de control utilizan Seguridad de la capa de transporte 1.2 (TLS, por sus siglas en inglés) para garantizar la seguridad e integridad de los datos durante el traslado entre los componentes.

Las credenciales que se utilizan para la autenticación de los creadores o ejecutores de bots a la sala de control se cifran antes de someterse a una conexión asegurada por TLS. Esta capa extra de cifrado no solo ofrece protección contra problemas de pila de red (como por ejemplo, Heartbleed), sino que también previene la exposición de las credenciales para las implementaciones donde la capa externa de la conexión TLS finaliza en un equilibrador de carga front-end.

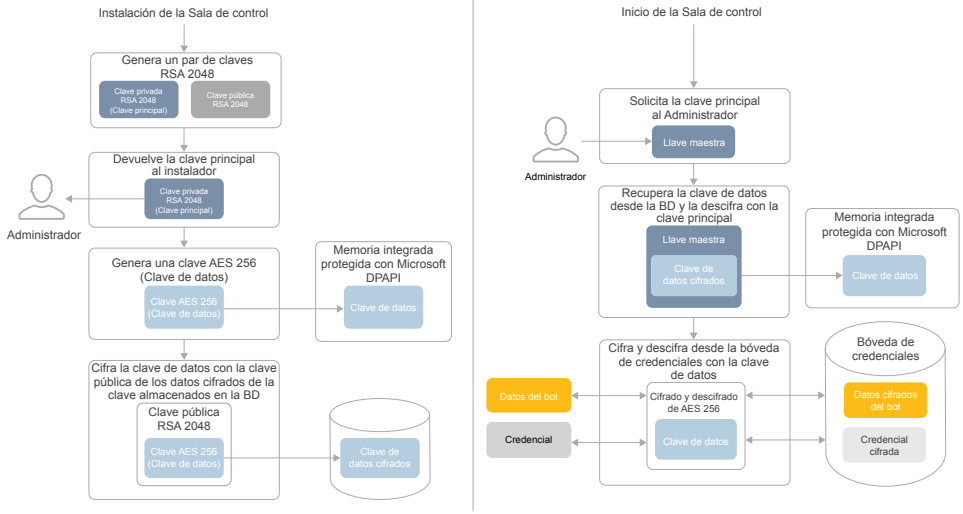

Figura 7: Arquitectura de cifrado de Automation Anywhere Enterprise

Protección de los datos en uso

La seguridad del tiempo de ejecución comienza con una protección de credenciales distribuida. Específicamente, no hay un almacenamiento local de credenciales en los ejecutores de bots. Las credenciales y otros datos que se recuperan de manera dinámica desde la bóveda de credenciales para el uso dentro de las automatizaciones solamente se conservan en un formato cifrado en una memoria volátil y se borran una vez que el bot asociado haya finalizado con su ejecución.

Otras funciones y opciones de configuración que se pueden utilizar para prevenir el acceso no autorizado a la información confidencial (es decir, filtración de datos) o la falsificación de bots durante el tiempo de ejecución son las siguientes:

+ Modo sigiloso: no se muestran las ventanas de los programas en la pantalla local y los usuarios conectados tienen la opción de deshabilitar la captura de imagen en los creadores y ejecutores de bots para prevenir, de esta manera, que la información confidencial que aparece en la pantalla se almacene en los bots.
+ Bloqueo de entrada: función para deshabilitar el mouse y el teclado de la máquina en la que se está ejecutando una automatización.
+ Límite de tiempo: función para configurar un límite de tiempo luego de que la automatización finalice, si es que no ha terminado con la ejecución.
+ Control central: función para controlar de manera centralizada (por ej., pausar, reanudar, detener) la operación de las automatizaciones que se están ejecutando de manera remota desde adentro de la sala de control.

SOPORTE PARA EL CICLO DE VIDA DE DESARROLLO DE SOFTWARE SEGURO (SDLC)

Para maximizar los controles y las medidas de protección que se encuentran en el entorno de automatización, se puede "ampliar" el escenario básico de implementación que se describió anteriormente para cumplir aún más con las mejores prácticas del ciclo de vida de desarrollo de software seguro (SDLC, por sus siglas en inglés), tales como las requeridas por la Ley de Administración de Seguridad de Información Federal (FISMA, por sus siglas en inglés), el Programa Federal de Administración de Riesgos y Autorizaciones (FedRamp, por sus siglas en inglés) y el Estándar de Seguridad de Datos de la Industria de Pagos con Tarjeta (PCI DSS, por sus siglas en inglés). El modelo de implementación avanzado resultante ofrece tres zonas de RPA distintas: desarrollo, pruebas de aceptación de usuario (UAT, por sus siglas en inglés) y producción (ver Figura 8). Cada zona está separada de manera lógica (aislada) con diferentes grupos de usuarios que tienen asignados distintos roles y privilegios. Las líneas discontinuas verticales representan la segmentación de las redes y los contrafuegos.

Al igual que en el modelo de implementación básico, el ciclo de vida de los bots comienza en la etapa de desarrollo. Una vez que los diseñadores de bots están conformes con los bots, los promotores de bots de UAT transfieren los bots desde el depósito de la versión de desarrollo (SVN) hacia el depósito de UAT. La finalidad exclusiva de la zona de UAT es evaluar los bots para garantizar precisión, buen desempeño y seguridad. Luego de que los bots pasan las pruebas de aceptación, un promotor de bots de producción los transfiere a la zona de producción. En este punto, alcanzan el estado de producción y quedan disponibles para que los operadores de RPA los utilicen con aplicaciones de producción. En cada etapa del proceso, diferentes administradores, con distintos roles y privilegios, llevan a cabo revisiones y certificaciones. La estricta separación de tareas y los controles multicapa están integrados en el diseño para garantizar que la fuerza de trabajo digital sea confiable, escalable, segura y conforme.

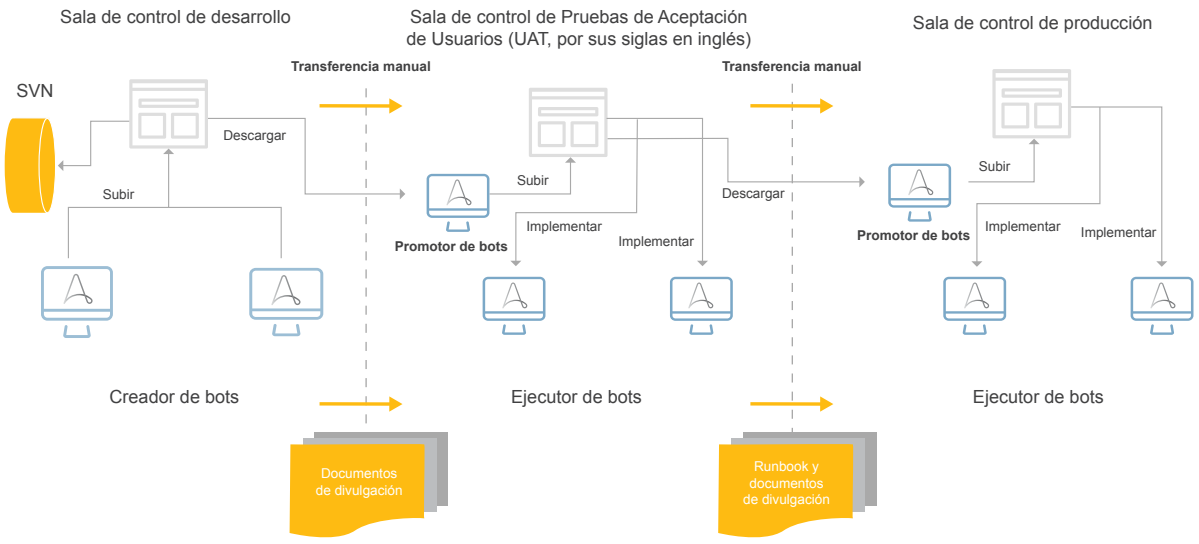

Figura 8: Modelo de implementación avanzado para soporte de SDLC total

INICIO DE SESIÓN Y MONITOREO

Las capacidades exhaustivas de registro de auditoría, monitoreo y presentación de informes son componentes esenciales de la arquitectura de seguridad para cualquier solución destacada de TI. Automation Anywhere Enterprise no es la excepción.

A lo largo de la plataforma, los detalles de los eventos (quién, qué, cuándo, dónde y resultado) se capturan de manera automática para más de 60 tipos de acciones de usuarios o entidades, incluidas la creación, modificación, habilitación, inhabilitación y eliminación de usuarios, bots, creadores y ejecutores de bots. El no repudio se logra mediante la combinación de captura automática, la vinculación de cada actividad a una identidad específica y una política predeterminada de solo lectura. El RBAC también se puede utilizar para controlar de manera estricta qué roles tienen visibilidad para los registros de auditoría en primer lugar.

Desde una perspectiva de control, los paneles e informes automatizados se encuentran accesibles dentro de la sala de control y se pueden personalizar para identificar y alertar actividades anormales (o cualquier otro detalle que los equipos de automatización o seguridad consideren importante). Asimismo, la capacidad de exportar registros respalda el uso de otros análisis, informes e infraestructura de investigación o respuesta de incidentes ya existentes y en uso por las empresas, como por ejemplo, SIEM, Análisis de comportamiento de entidades y usuarios (UEBA, por sus siglas en inglés) y herramientas de análisis avanzadas.

SEGURIDAD EMPRESARIAL ADICIONAL Y CAPACIDADES DE FORTALECIMIENTO

Automation Anywhere Enterprise también respalda la seguridad empresarial y los objetivos de fortalecimiento mediante:

+ Un componente de arquitectura distribuido (y flexible) que es capaz de “adaptarse” sin problemas a la infraestructura y a los procesos de alta disponibilidad o recuperación ante desastres (AD/RD) ya existentes de la empresa.
+ Un sistema de control de versiones integral (Apache Subversion) que, junto con las amplias funciones de RBAC de la plataforma, es capaz de implementar y hacer cumplir una política de gestión del cambio y procesos sumamente rigurosos.
+ Herramientas tales como los marcos Hibernate y ReactJS durante el desarrollo del código de plataforma para ayudar a eliminar la vulnerabilidad a los ataques comunes (como por ejemplo, inyección de código SQL y secuencias de comandos en sitios cruzados).
+ Un plan o protocolo de seguridad para el desarrollo de códigos que requiere un escaneo constante de múltiples herramientas y capas para detectar y eliminar las vulnerabilidades del software.

Puede encontrar más detalles sobre estos y muchos otros controles, medidas de protección y capacidades de seguridad que son parte de Automation Anywhere Enterprise en: Automation Anywhere Enterprise: arquitectura de seguridad.

La automatización robótica de procesos resulta muy prometedora para las empresas modernas que buscan reducir los costos operativos, mejorar la satisfacción del cliente y lograr una ventaja sobre los competidores. Como líder mundial, la plataforma de fuerza de trabajo digital de Automation Anywhere Enterprise ayuda a garantizar el logro máximo de estos y otros beneficios al ofrecer no solo la confiabilidad, escalabilidad y utilidad necesarias para tener éxito, sino también la seguridad de nivel empresarial que se requiere para preservar la confidencialidad, integridad y disponibilidad de todo el entorno de automatización.

Para obtener más información sobre Automation Anywhere Enterprise, visite: https://www.automationanywhere.es/products/enterprise.