Segurança de nível empresarial para Automação Robótica de Processos

INTRODUÇÃO

A Automation Anywhere começou há 15 anos fazendo uma pergunta simples: por que, após mais de 20 anos de investimento em tecnologias de automação de processo de negócios, menos de 20% das tarefas que poderiam ser automatizadas foram realmente automatizadas? Ela rapidamente dedicou atenção total ao desafio principal: 85% dos sistemas corporativos não têm APIs bem definidas, o que resulta em uma crescente lista de pendências de TI de solicitações de integração da linha de negócios.

A automação robótica de processos nasceu com a visão de capacitar os usuários de negócios a criarem bots de software que pudessem interagir com sistemas corporativos, assim como os humanos. A RPA permite que qualquer usuário de negócios que entenda de macros do Excel registre as etapas usadas em tarefas repetitivas e as transforme em um script fácil de entender para bots. Os bots de RPA podem entrar em aplicativos corporativos usando credenciais, assim como os humanos, e automatizar tarefas que envolvem qualquer aplicativo corporativo, incluindo aplicativos herdados sem APIs. Processamento de sinistros, processamento de empréstimos, conciliações contábeis, criação/envio de faturas e criação de relatórios são apenas alguns dos exemplos de possíveis automações que se estendem às diferentes disciplinas empresariais.

É fácil ver o potencial de economia significativa de tempo e dinheiro, melhor satisfação do cliente, maior motivação da força de trabalho e a habilidade de criar uma vantagem ponderosa sobre concorrentes usando a RPA. No entanto, entender por completo esses ganhos depende de uma solução de classe empresarial.

Fornecer um conjunto de recursos altamente confiáveis, dimensionáveis e sólidos para maximizar a aplicabilidade e a usabilidade são alguns dos critérios básicos essenciais para automação. Mas esses elementos não cobrem o requisito empresarial mais crítico: segurança de ponta a ponta. É difícil oferecer uma arquitetura de segurança robusta com recursos que possibilitam suporte completo para princípios essenciais, como menos privilégios e separação de tarefas, e fornecer uma proteção de ponta a ponta para os aplicativos críticos e dados sigilosos.

Este documento fornece uma visão geral do mais alto padrão da indústria para segurança de nível empresarial, como demonstrado pela plataforma de força de trabalho digital líder do mercado, o Automation Anywhere Enterprise.

“

É fácil ver o potencial de economia significativa de tempo e dinheiro, melhor satisfação do cliente, maior motivação da força de trabalho e a habilidade de criar uma vantagem ponderosa sobre concorrentes usando a RPA. No entanto, entender por completo esses ganhos depende de uma solução de classe empresarial.

ARQUITETURA E OPERAÇÕES

Entender os controles de segurança necessários para uma implementação da RPA de nível empresarial depende da compreensão dos componentes que incluem a solução e suas operações.

Componentes principais

Como ilustrado na Figura 1, os componentes principais de arquitetura do Automation Anywhere Enterprise são a Control Room, os Bot Creators e os Bot Runners.

Control Room

A Control Room funciona como o cérebro do ambiente de automação. É um sistema de gerenciamento baseado no Windows Server, com um banco de dados integral, que fornece uma exibição unificada para a administração geral do sistema. A Control Room também é onde operadores da RPA vão para orquestrar a força de trabalho digital. Em outras palavras, para agendar, implementar, executar, monitorar e gerenciar a operação dos bots da organização. Além disso, recursos de controle de versão integrados (Apache Subversion Server) facilitam a colaboração multiusuário enquanto impõem as melhores práticas de gerenciamento de mudança e estabelecem um repositório centralizado de bots prontos para produção.

Bot Creator

O Bot Creator é usado para criar bots. Ele é um aplicativo de área de trabalho do Windows sendo executado em um hardware de estação de trabalho ou máquina virtual. O client Bot Creator é usado por especialistas de processo de negócios que criam e testam suas automações. Os bots são criados utilizando o Task Editor, enquanto o teste dos bots (usando dados de teste não advindos de produção locais e instâncias de aplicativo) é facilitado pela função de reprodução local. Depois do teste bem-sucedido (por exemplo, para desempenho, integridade de dados e segurança), os bots são verificados no repositório da Control Room e ficam disponíveis para implantação de produção.

Bot Runner

O Bot Runner coloca os bots para trabalhar. Usando o mesmo código de aplicativo que o client Bot Creator, mas com uma chave de licença diferente, o Bot Runner usa a função de reprodução para executar bots no ambiente de produção. Isto é, utilizando instâncias de produção do aplicativo-alvo e armazenamentos de dados de produção. Na verdade, executar bots é tudo o que Bot Runners podem fazer, já que as funções de criação e edição não estão disponíveis para eles. Para operações em grande escala altamente confiáveis, a centralização dos Bot Runners também é suportada.

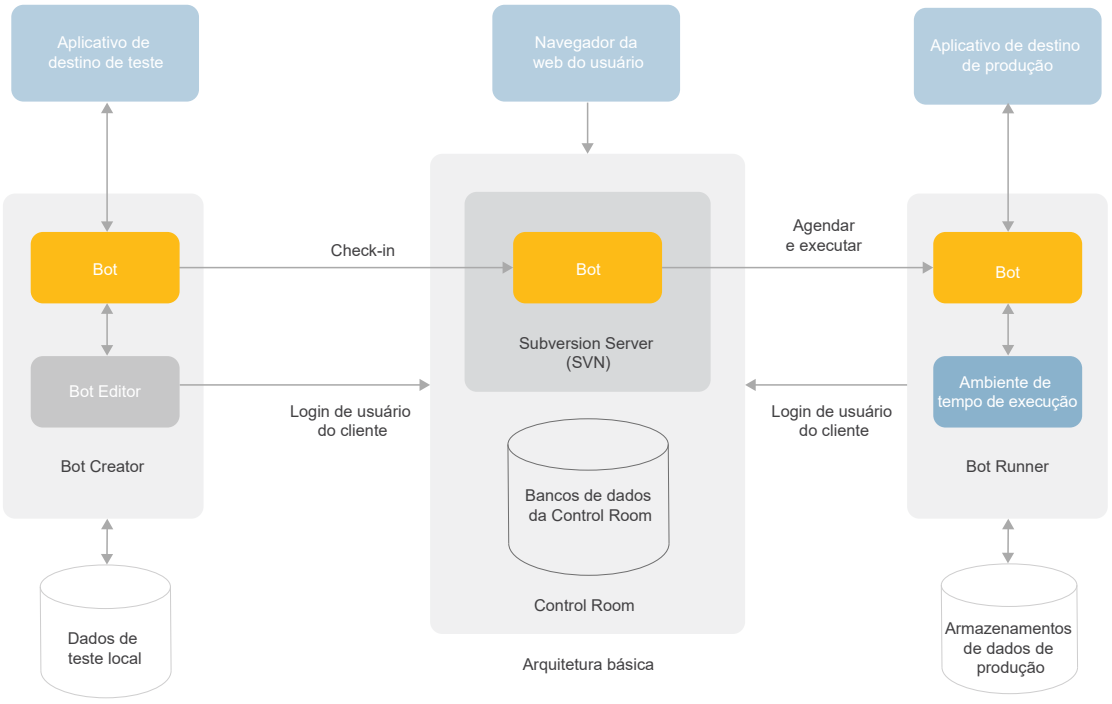


Figura 1: Arquitetura básica do Automation Anywhere Enterprise

Componentes de classe empresarial adicionais

Ao considerar operações de grande escala, duas outras soluções da RPA importantes e relevantes a organizações que buscam utilizar implantações de nível empresarial surgem: escalabilidade sob demanda e Bot Insight.

Escalabilidade sob demanda

Com o aproveitamento de nuvem pública da Amazon Web Services (AWS), o Automation Anywhere Enterprise entrega, de forma eficaz, a RPA como um serviço com todos os recursos de assistente, incluindo aumento/diminuição elástico, medição com base em uso, escalabilidade horizontal ilimitada, monitoramento contínuo e log de auditoria da infraestrutura do Bot Runner. O resultado é alta disponibilidade de nós múltiplos que aprimora o desempenho com base em SLA e continuidade empresarial, mesmo quando há variações drásticas na carga de trabalho de automação.

Bot Insight

Um subsistema completamente integrado dentro da Control Room, o Bot Insight realiza análises quase que em tempo real de operações de bot e dados de processo empresarial. O Bot Insight gera automaticamente painéis personalizáveis usando algoritmos avançados específicos para cada bot. O nível de detalhes que o Bot Insight fornece baseado em logs de evento detalhados sobre operações de bot permite alertas diferenciados, descoberta ad-hoc, pesquisas interativas, análises de série de tempo e informações abrangentes sobre os processos operacional/de negócios. Além disso, todos os dados podem ser exportados para logs de informações de segurança e gerenciamento de evento (SIEM) para análise, investigação e relatórios adicionais.

Bots em ação: dois tipos de automações

Um último ponto a ser esclarecido antes de entrar nas funcionalidades de segurança de alto nível do Automation Anywhere Enterprise são os dois tipos básicos de automações: assistida e não assistida.

Uma automação assistida ocorre quando um usuário está logado em uma máquina do Bot Runner para observar e/ou dar suporte ativo à execução do bot. Um dos motivos para haver um usuário presente é que o bot pode ter uma função de utilitário que ajuda em seu trabalho, ou que o bot realiza trabalho em lote que requer entrada periódica ou direcionamento situacional de um usuário. Automações assistidas também são conhecidas como automações de front office.

Automações não assistidas, como o nome sugere, operam sem a necessidade de um usuário empresarial ou interação de operador. Automações não assistidas geralmente são executadas por um operador que tem pouco ou nenhum conhecimento sobre o bot, o aplicativo sendo automatizado ou o motivo da automação. O operador, em conjunto com a unidade empresarial, agenda bots para executar nos Bot Runners. Durante a execução, o operador monitora aspectos operacionais dos bots em execução, como CPU, memória e uso de armazenamento para garantir que eles sejam executados sem quaisquer erros ou exceções. Painéis da Control Room exibem todos os detalhes operacionais dos bots conforme eles são executados.

IDENTIFICAÇÃO E AUTENTICAÇÃO DE MULTICAMADAS DE SEGURANÇA DA RPA EMPRESARIAL

Um princípio fundamental da arquitetura de segurança do Automation Anywhere Enterprise é que nenhum acesso ou ação é permitido sem autorização prévia da entidade envolvida. Isso se aplica a humanos e a bots também. Para compreender a autorização na RPA, é preciso primeiramente compreender o processo da autenticação para automações assistidas e não assistidas.

QUEM É QUEM: AUTENTICAÇÕES TÍPICAS EMPRESARIAIS

Credenciais e identidades podem ser multicamadas. Considere um cenário de autenticação empresarial simples (consulte a Figura 2). Uma usuária empresarial, Alice, autentica-se para sua estação de trabalho do Windows. Alice entra em um aplicativo que está em execução remotamente, autenticando por meio de um login do Active Directory de domínio do Windows ou talvez por Kerberos, baseado em sua estação de trabalho que tem um tíquete válido. Neste cenário, a cadeia de autenticação envolve uma única pessoa e suas credenciais.

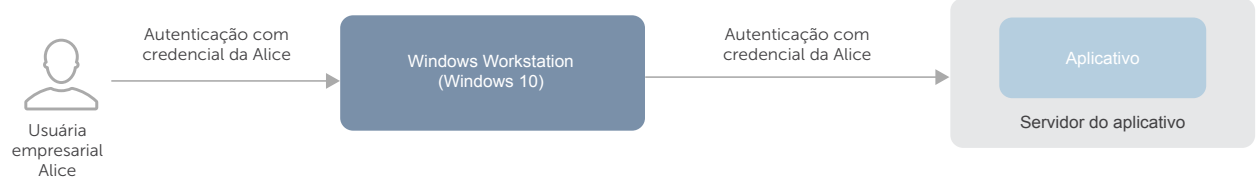


Figura 2: Autenticação típica empresarial

Agora, considere o cenário de automação assistido mostrado na Figura 3. Neste caso, o usuário, Bob, está testando um bot ou executando uma automação assistida como parte de seu dia de trabalho típico. Na etapa 1, ele autentica para a estação de trabalho do Bot Runner usando suas credenciais pessoais (como no cenário de Alice acima). Na etapa 2, ele inicia o client do Automation Anywhere Enterprise e insere seu ID de usuário da Control Room e senha, autenticando o software de client para a Control Room. Na etapa 3, ele executa o bot que, por sua vez, acessa um aplicativo que precisa de autenticação. As credenciais usadas pelo bot nesta etapa podem ser armazenadas no Enterprise Credential Vault e recuperadas pelo bot durante o tempo de execução ou podem ser uma passagem da credencial pessoal de Bob (com base no fato de Bob ter sido autenticado no domínio e ter um tíquete Kerberos ou com base em qualquer logon único que seja usado). De qualquer forma, o resultado são três camadas de identificação e autenticação no total.

Três camadas de autenticação também são usadas para o cenário não assistido mostrado na Figura 4, embora com um pouco de reviravoltas. Nesse caso, o usuário (um operador de RPA chamado Charles) começa autenticando a Control Room para que ele possa selecionar um bot para a ser executado imediatamente ou em um período agendado.

Na etapa 2, quando o período de execução do bot iniciar, a Control Room inicia um login automático para a estação de trabalho do Bot Runner, usando a credencial do usuário do Bot Runner. Depois de um bot ser baixado para a função de reprodução local (Etapa 3) e iniciar sua execução, ele autentica o aplicativo de destino usando a credencial de usuário do aplicativo de bot (Etapa 4). Assim como com o cenário de automação assistida, a credencial de usuário do aplicativo de bot pode ser aquela recuperada do Credential Vault ou pode ser uma transferência da credencial de usuário do Bot Runner.

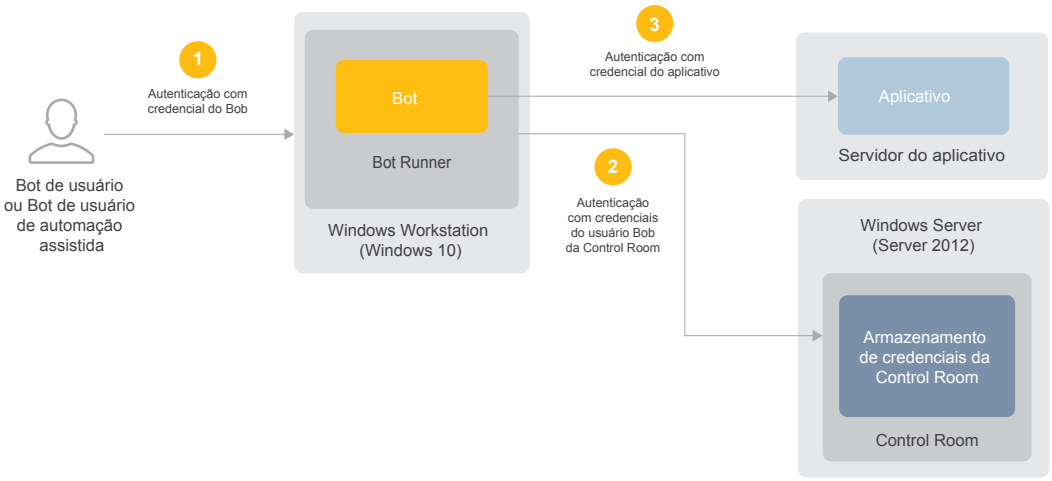


Figura 3: Processo de autenticação para cenário de automação assistida

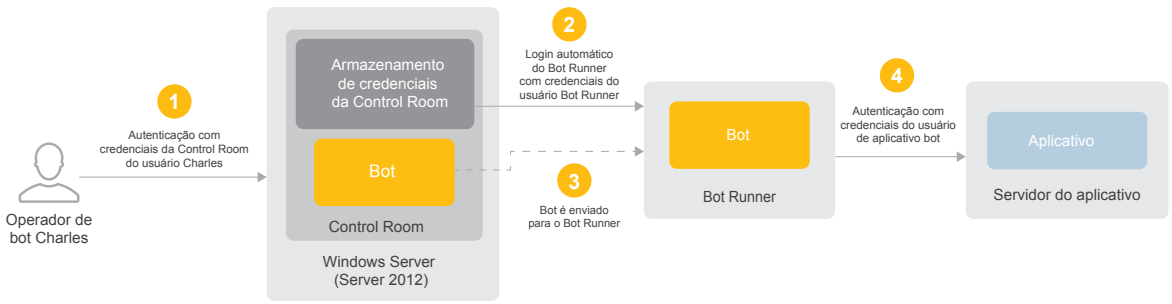


Figura 4: Processo de autenticação para cenário de automação não assistida

Opções de autenticação e integrações do IAM

Opções compatíveis para autenticação da Control Room incluem Active Directory usando LDAP, Active Directory usando Kerberos e autenticação local usando o Credential Vault integrado (discutido em uma seção posterior).

Outras opções de identidade e gerenciamento de acesso disponíveis para implantações empresariais incluem:

+ Suporte ao SAML 2.0 baseado em logon único
+ Integração com soluções de gerenciamento de acesso/credencial privilegiado de terceiros (por exemplo, CyberArk)

CONTROLE DE ACESSO BASEADO NA FUNÇÃO ABRANGENTE

A autenticação bem-sucedida é apenas o primeiro nível de execução de controle de acesso obrigatório oferecido pela arquitetura de segurança do Automation Anywhere Enterprise. A autorização é igualmente importante, especialmente quando se trata de aderir aos princípios fundamentais de privilégios mínimos e separação de deveres. A autorização dentro da Automation Anywhere é configurada com controle de acesso otimizado baseado em função, ou RBAC.

Para ilustrar o RBAC, definiremos algumas funções distintas. As funções que você usa na sua implantação podem ser um pouco diferentes, e você pode ter funções adicionais. Há cinco funções distintas (consulte a Tabela 1) para considerar dentro da arquitetura básica e principais funções da plataforma da RPA. Bot Authors utilizam o client Bot Creator para capturar lógica empresarial e para criar automações correspondentes. Bot Authors trabalham com aplicativos de teste e conjuntos de dados para que os sistemas de produção não sejam impactados durante a fase de desenvolvimento. Um bot individual geralmente passará por muitas iterações e versões diferentes, não apenas durante o desenvolvimento inicial, mas também sempre que processos de negócios e/ou aplicativos de destino associados forem atualizados. Os Bot Testers também trabalham com o client Bot Creator para testar bots com relação a desempenho, integridade de dados e segurança, garantindo que cada bot realize sua tarefa específica de forma segura. Bot Testers funcionam como um segundo estágio de autorização para o bot, antes de ele poder ser executado com aplicativos e dados de produção.

Depois de o bot ser testado e tiver passado por uma revisão de segurança, o Bot Promoter trabalha com o Bot Author/Bot Tester para designar a versão do bot que deve ser usada na produção. Essa é a única versão do bot que estará visível para o Bot Operator, que coordena com as unidades empresariais para agendar e executar o bot. O Bot Operator também é responsável pelo monitoramento do desempenho de bot dentro da Control Room, incluindo a solução de quaisquer problemas relacionados ao tempo de execução que aparecerem. Por fim, a responsabilidade para a administração geral da plataforma, incluindo componentes de configuração, interfaces e todas as outras funções/permissões, se encaixam na administração da RPA.

Separação avançada de tarefas

Este conjunto central de funções demonstra um ponto de início básico de RBAC, mas uma separação ainda maior de tarefas é possível dentro da plataforma Automation Anywhere Enterprise. Usando o assistente de criação de função, os administradores podem definir facilmente funções personalizadas e privilégios/permissões que são responsáveis pelo pacote completo dos objetos e funções da Control Room, incluindo gerenciamento de usuários, licenciamento, Credential Vault, conjuntos de Bot Runners, agendamentos de bot, operações/painéis de bot e logs de auditoria. Conforme cada privilégio é selecionado, o assistente adicionará, de forma dinâmica, etapas para privilégios eventuais/derivados.

Por exemplo, quando os privilégios BOTS > View my bots > Run My bots (BOTS > Exibir meus bots > Executar meus bots) são selecionados (consulte a Figura 5), o fluxo de trabalho adicionará uma etapa para indicar as Pastas de bot específicas, ou seja, conjuntos de bots, às quais o acesso está sendo concedido. O resultado final é a habilidade de estabelecer funções altamente leais com controles de acesso otimizados suficientemente para atender às necessidades dos ambientes mais rigorosos, seguros e regulamentados para conformidade.

Função	Descrição
RPA Admin	Administra o sistema (configurando componentes, funções, interfaces)
Bot Builder	Um especialista de processo empresarial que cria bots com o Editor de tarefas e realiza testes funcionais básicos
Bot Tester	Um verificador de garantia de qualidade que revisa os bots com relação a precisão funcional, desempenho e segurança
Bot Promoter	Um administrador que aprova e move bots entre estágios de desenvolvimento, teste e produção
RPA Operator	Um operador que agenda, executa e monitora o desempenho dos bots

Tabela 1: Principais funções de RPA no Automation Anywhere Enterprise

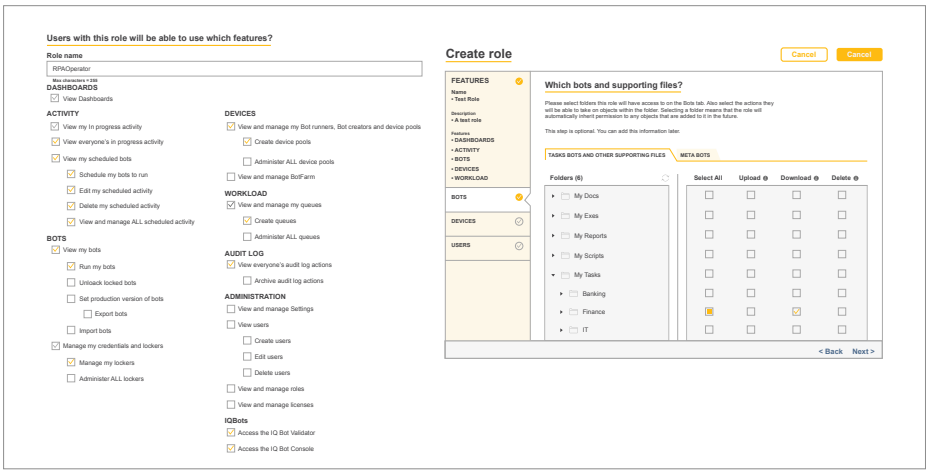


Figura 5: Criação de função com autorização otimizada

Painéis de controle independentes

Além dos recursos de RBAC extensos, o Automation Anywhere Enterprise realiza, de forma inerente, a separação lógica de tarefas implantando uma arquitetura que separa por completo as tarefas de desenvolvimento e execução de bot.

Os Bot Creators só podem carregar e baixar bots para o sistema de controle da versão e a partir dele dentro da Control Room. Ao mesmo tempo, os Bot Runners são limitados a executar bots; eles não têm acesso à criação de bots e à funcionalidade de teste. Essa separação imposta de forma arquitetônica de tarefas constitui uma autorização dupla consistente com as melhores práticas do National Institute of Standards, pois ela requer (no mínimo) um usuário desenvolvedor e empresarial para habilitar, por fim, uma automação de processo de negócios.

Domínios de processamento independentes

Um caso de uso poderoso dos recursos de RBAC da plataforma, principalmente para grandes empresas, é o estabelecimento de domínios de processamento independentes (consulte a Figura 6). Nesse contexto, o "domínio de processamento" é uma coleção de automações (bots), bot runners e usuários. Isso pode ser realizado com organização/armazenamento rigoroso de bots para cada domínio desejado em uma pasta correspondente dentro da Control Room.

Caso em questão: Bots associados com aplicativos de finanças seriam colocados em uma pasta de finanças, enquanto aqueles associados com RH seriam colocados em uma pasta de RH. Operadores de bot do departamento financeiro receberiam privilégios apenas para bots financeiros e Bot Runners financeiros; Operadores de bot para RH receberiam privilégio apenas para bots e Bot Runners de RH, e assim por diante, para outros domínios de processamento/automação (consulte a **Figura 6**).

O resultado final é a separação adicional de tarefas e isolamento de aplicativos e dados associados, esse momento no nível de domínio de processamento, pois operadores individuais não conseguem ver ou operar bots fora de determinado domínio.

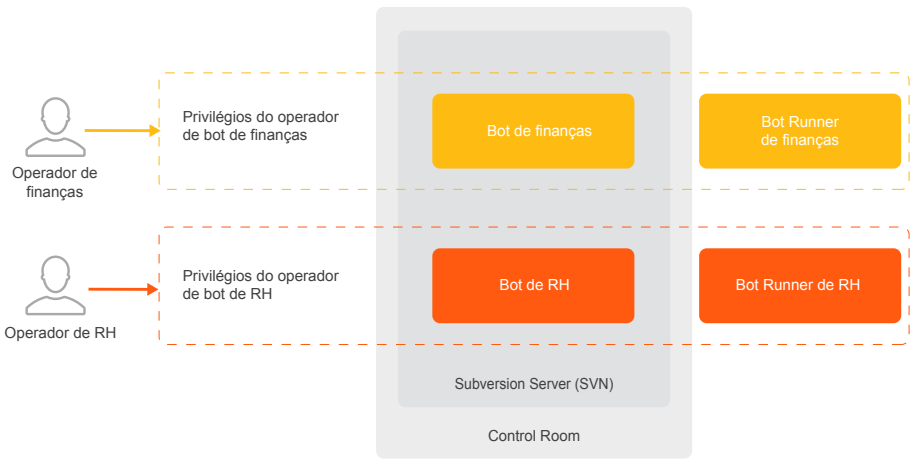


Figura 6: Suporte para domínios de processamento independente

PROTEÇÃO DE DADOS DE PONTA A PONTA

Autenticação multicamada e controle de acesso otimizado são essenciais para um ambiente de controle rigoroso. O mesmo acontece com a proteção de ponta a ponta, que também é necessária para manter a confidencialidade e a integridade de processos empresariais críticos, dados sigilosos e segredos relacionados (por exemplo, credenciais).

A plataforma Automation Anywhere Enterprise aborda essa necessidade com um Credential Vault integrado e fornece um conjunto extenso de proteções que não só protegem dados tanto em repouso quanto em trânsito, mas também enquanto estiverem em uso em sistemas individuais.

Chaves de criptografia e o Credential Vault

A **Figura 7** exibe as principais chaves de criptografia usadas pela plataforma, juntamente com seu relacionamento com o Credential Vault. Toda criptografia é realizada usando módulos criptográficos FIPS 140-2 validados de Nível 1.

Durante a instalação (a parte à esquerda da **Figura 7**), o sistema gera um par de chaves públicas/privadas RSA de 2048 bits e uma chave AES de 256 bits. A chave privada do par RSA 2048 é conhecida como a Chave principal, enquanto a chave AES 256 é conhecida como Chave de dados. A Chave principal é apresentada ao administrador de instalação para manter a segurança em um local seguro fisicamente fora do sistema. A chave pública é usada para criptografar a Chave de dados. Tanto a chave pública quanto a Chave de dados criptografada são armazenadas no banco de dados.

Durante a inicialização ou reinicialização da Control Room (a parte à direita da **Figura 7**), o administrador recebe um aviso para fornecer a Chave principal. A Chave de dados criptografados é recuperada do banco de dados e descriptografada usando a Chave principal. A Chave de dados agora está pronta para uso. Como o sistema armazena e recupera dados do Credential Vault, a Chave de dados é usada para criptografar e descriptografar esses dados.

O Credential Vault é usado para armazenar todas as credenciais gerenciadas do sistema e dados de configuração de sistema críticos. Ele também pode ser usado para armazenar outros dados confidenciais (por exemplo, pares de nome-valor) usados nas automações de uma organização. Como resultado, Bot Authors podem evitar a prática insegura de credenciais pesadas e outros argumentos/dados confidenciais diretamente dentro de suas automações. Dentro do Credential Vault, os dados são organizados por cofres. Os cofres permitem a alocação de dados de credencial criptografados por usuário, protegidos por privilégios e funções como parte dos recursos do Controles de acesso com base em função (RBAC) da Automation Anywhere. Cada cofre pode ser atribuído a um usuário ou função individual para restringir o acesso ao cofre apenas a usuários específicos da RPA.

Proteção de dados estáticos

Além de criptografar credenciais locais e alguns dados de tempo de execução usados por bots, o Credential Vault fornece armazenamento seguro para parâmetros de configuração sigilosa e detalhes com relação ao controle de versão integral e serviços de e-mail.

Proteção de dados em trânsito

Todos os serviços de rede de clientes e da Control Room usam Transport Layer Security (TLS) 1.2 para garantir dados de segurança e integridade durante transporte entre componentes.

Credenciais usadas para autenticação de Bot Creator/Runner para a Control Room são criptografados antes de serem enviados por uma conexão TLS segura. Essa camada extra de criptografia não protege apenas contra problemas de empilhamento de rede (como com Heartbleed), mas também previne a exposição de credenciais para implementações onde a conexão de TLS da camada externa é encerrada no balanceador de carga de front-end.

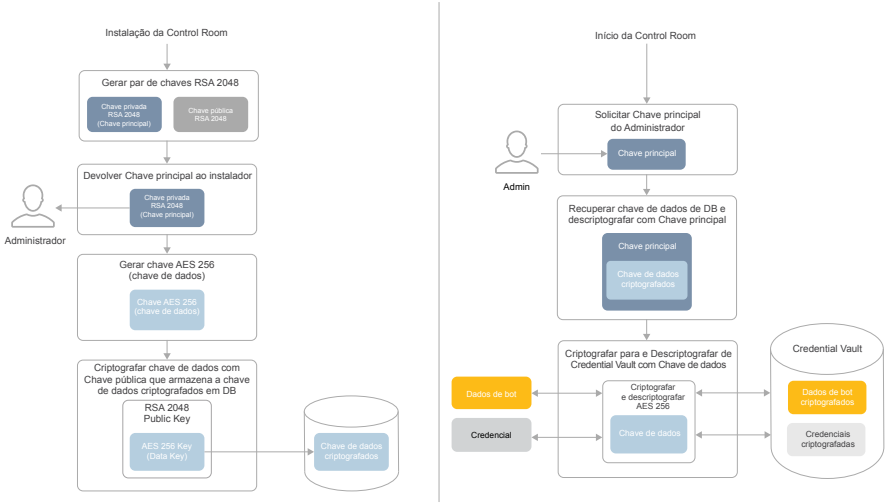


Figura 7: A arquitetura de criptografia do Automation Anywhere Enterprise

Proteção de dados em uso

A segurança de tempo de execução começa com proteção de credencial distribuída. Especificamente, não há armazenamento de credencial local nos Bot Runners. Credenciais e outros dados recuperados dinamicamente do Credential Vault para uso dentro das automações são retidos apenas em formato criptografado em memória volátil e são apagados depois que o bot associado termina sua execução.

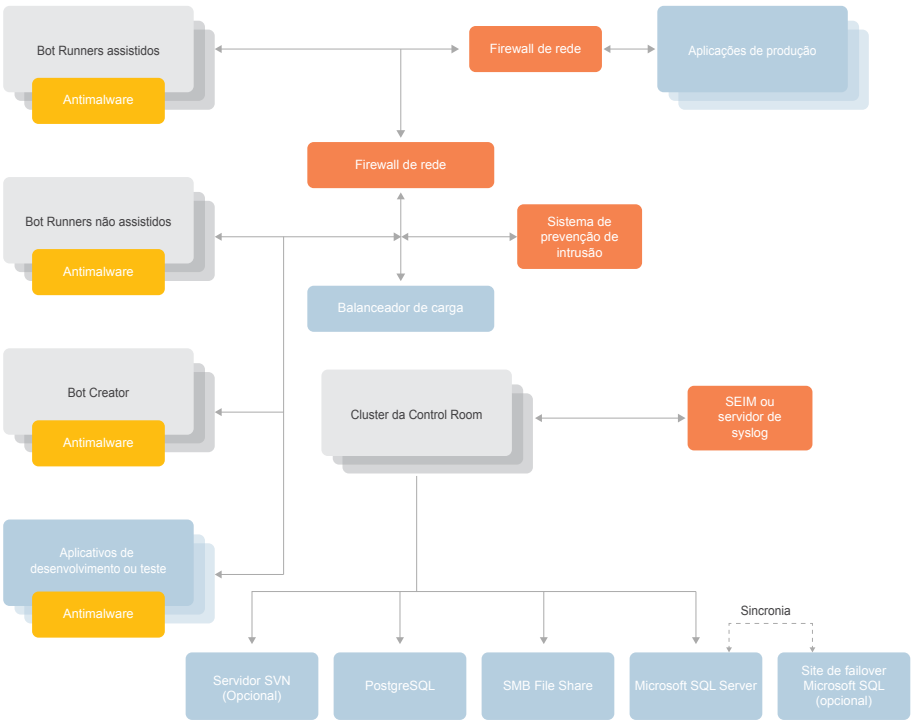
Outros recursos e opções de configuração que podem ser usados para prevenir acesso não autorizado para informações confidenciais (ou seja, vazamento de dados) ou manipulação com bots durante o tempo de execução incluem:

+ Modo oculto: onde nenhuma janela de programa é exibida na tela local, e os usuários logados têm a opção de desabilitar a captura de imagem de Bot Creators e Bot Runners, evitando assim que informações sigilosas exibidas na tela sejam armazenadas em bots
+ Bloqueio de entrada: a habilidade de desabilitar o mouse e teclado da máquina onde a automação está sendo executada
+ Limite de tempo: a habilidade de definir um limite de tempo após o qual uma automação será encerrada se sua execução ainda não tiver terminado
+ Controle central: a habilidade de controlar centralmente (por exemplo, pausar, retomar, parar) a operação de automações sendo executadas remotamente dentro da Control Room

PROTEGER A IMPLANTAÇÃO DA RPA

A arquitetura do AAE consiste na infraestrutura de classe de servidor e área de trabalho padrão para os clientes e a Control Room. Esta seção explica sobre as práticas recomendadas de segurança em RPA relacionadas a controles de segurança externos que estão em vigor em qualquer empresa. Firewalls baseados em rede, sistemas de detecção de intrusão, antimalware e servidores de log externos são controles de segurança padrão que são tão relevantes para a implantação de RPA quanto para a outra infraestrutura em seu ambiente. O diagrama abaixo mostra de forma lógica onde esses componentes são colocados na implantação da RPA.

Cada controle de segurança externo é explicado detalhadamente abaixo em termos de posicionamento e configuração. O suporte a serviços de rede, como Active Directory, SVN Server, PostgreSQL, SMB File Share, Microsoft SQL e aplicações de produção, pode ser acessado por meio de firewalls de rede ou diretamente, dependendo do seu posicionamento em relação aos componentes da RPA.



Controle de acesso baseado em rede: proteção da RPA com firewalls

Firewalls baseados em rede e firewalls locais baseados em servidor são usados para proteger a Control Room ou todos os nós em um cluster de Control Room ao utilizar uma implantação clusterizada. Por padrão, somente protocolos necessários na Control Room devem ser permitidos da rede corporativa. Além disso, os protocolos de clustering só devem ser permitidos entre nós no cluster da Control Room. Firewalls baseados em rede são usados para isolar ambientes de RPA de desenvolvimento, teste e produção da rede corporativa e uns dos outros (consulte a seção Ciclo de vida de desenvolvimento de software seguro abaixo).

Para ambientes de automação não assistidos, os bot runners são colocados em uma rede isolada distinta e protegidos por um firewall baseado em rede. As automações assistidas são executadas em estações de trabalho corporativas com o client do bot runner instalado e são protegidas por firewalls de perímetro corporativo ou firewalls internos que protegem a infraestrutura corporativa da área de trabalho, como qualquer área de trabalho.

Consulte as tabelas abaixo para ver os protocolos em uso pelo cliente e Control Room.

3.10 List of Port Numbers

Below table lists the configurable ports used by our platform

3.10.1 Client

Port	Description	Deployment	Used for
110 995	POP3	Client	"Email Automation" command to retrieve emails from mail server.
143 993	IMAP	Client	
21	FTP/SFTP	Client	"FTP/SFTP" command
25 465 587	SMTP	Client	"Send email, Error handling" command "Email notification" feature
161	UDP	Client	"SNMP" command
22 23	Terminal Emulator	Client	"Terminal Emulator" command
4530	TCP	Client (AAProxyServer.exe)	Used by the client to communicate with plugins via TCP socket for AAE Client, Editor or Player

80	HTTP	Control Room	Web UI access (No TLS, not recommended)
443	HTTPS	Control Room	Web UI access (Recommended)
25 465 587	SMTP	Control Room	Send email when important events occur (user created, password set/reset, role changed etc.)
1433	TCP	Microsoft SQL Server	Default port used by Microsoft SQL Server
5672	TCP	Control Room	Cluster Messaging
47500-47600	TCP	Control Room	Cluster Messaging and Caching
47100-47200	TCP	Control Room	Cluster Messaging and Caching

Antimalware: proteção da RPA contra vírus e malware

O client AA é executado na infraestrutura de classe da área de trabalho e deve ser considerado uma área de trabalho corporativa em todos os aspectos. Um software antimalware/antívirus é usado para proteger o ambiente do cliente contra software malicioso na forma de vírus e malware.

Sistemas de detecção de intrusão: proteção da RPA contra ataques diretos

Os sistemas de detecção e prevenção de intrusão (IPS) protegem a rede corporative, detectando ataques baseados na rede através da análise do tráfego da rede. Como qualquer outra seção crítica do datacenter, a plataforma de RPA é protegida no ponto de saída, atrás do firewall baseado em rede, por um sistema IPS. A colocação de IPS em sua rede deve ser considerada com base na convenção corporativa e deve ser aplicada igualmente à plataforma de RPA.

Gerenciamento de incidentes de eventos de segurança: proteção da RPA com auditoria externa

Os logs da Control Room podem ser encaminhados para um SIEM (Security information and event management, Gerenciamento de eventos e informações de segurança) para armazenamento externo, processamento e alerta. A integração com o SIEM ou qualquer sistema de redução e consolidação de auditoria baseado em syslog aumenta consideravelmente a postura de segurança e conformidade de governança. Configure a Control Room para encaminhar logs de auditoria ao servidor de coleta de syslog apropriado no ambiente.

VALIDAÇÃO EXTERNA DE CONTROLES DE SEGURANÇA

Para as agências federais, um dos requisitos para implantar o AAE é cumprir as normas de controle de segurança da FISMA (Federal Information Security Management Act, Lei de gerenciamento de segurança de informações federais), quando implantado em um sistema de TI no local.

O AAE oferece suporte a recursos de segurança que integram AAE com um ambiente compatível com a FISMA já existente e que hajam controles de suporte como autenticação centralizada (por exemplo, Active Directory (AD), gerenciamento de log centralizado, análise e relatórios recursos através de um Gerenciamento de eventos e informações de segurança (SIEM) e particionamento de rede e controle de acesso à rede por meio de VLANs (redes locais virtuais) e firewalls) que possam ser integrados ao AAE, quando apropriado.

O AAE apoia a implementação de controles de segurança aplicáveis, permitindo que os profissionais de TI atualizem o SSP de um sistema de TI para abordar a implantação e o uso seguros de AAE. Para obter mais detalhes sobre os controles FISMA, consulte os recursos do AAE e as capacidades principais que foram comparadas com os controles selecionados do FISMA Moderate do NIST SP 800-53 Rev. 4 e analisados em relação ao impacto e suporte dos requisitos de controle. A estrutura NIST pode ser mapeada para outras estruturas, como HIPAA e PCI. Consulte o whitepaper Automation Anywhere Enterprise: pela lente da FISMA para obter mais detalhes sobre os controles FISMA que são implementados no Automation Anywhere Enterprise.

SUPORTE DE CICLO DE VIDA DE DESENVOLVIMENTO DE SOFTWARE SEGURO (SDLC)

Para maximizar os controles e proteções posicionadas no ambiente de automação, o cenário de implantação básico descrito anteriormente pode ser "expandido" para entrega adicional nas práticas recomendadas do Secure Software Development Lifecycle (SDLC), como aqueles necessários para FISMA, FedRamp e PCI DSS. O modelo de implantação avançado resultante fornece três zonas de RPA distintas, uma para desenvolvimento, uma para teste de aceitação de usuário (UAT) e uma para produção (consulte a Figura 8). Cada zona é logicamente separada (isolada) com grupos de usuário diferentes com funções e privilégios distintos. As linhas verticais tracejadas representam a segmentação de rede e firewalls.

Como no modelo de implantação básica, o ciclo de vida do bot começa no desenvolvimento. Quando os Bot Authors estão satisfeitos com o bot, Bot Promoters de UAT transferem o bot do repositório de versionamento de desenvolvimento (SVN) para o repositório de UAT. O objetivo exclusivo da zona UAT é testar os bots com relação a precisão, desempenho e segurança. Depois que o bot passa no teste de aceitação, um Bot Promoter de produção o transfere para a zona de produção. Neste ponto, ele obtém o status de produção e torna-se disponível para Operadores da RPA para uso sem aplicativos de produção. Em cada etapa no processo, verificações e certificações são realizadas por administradores distintos com funções e privilégios diferentes. Separação rigorosa de tarefas e controles multicamadas são integrados por design para garantir que a força de trabalho digital seja confiável, escalável, eficiente, segura e compatível.

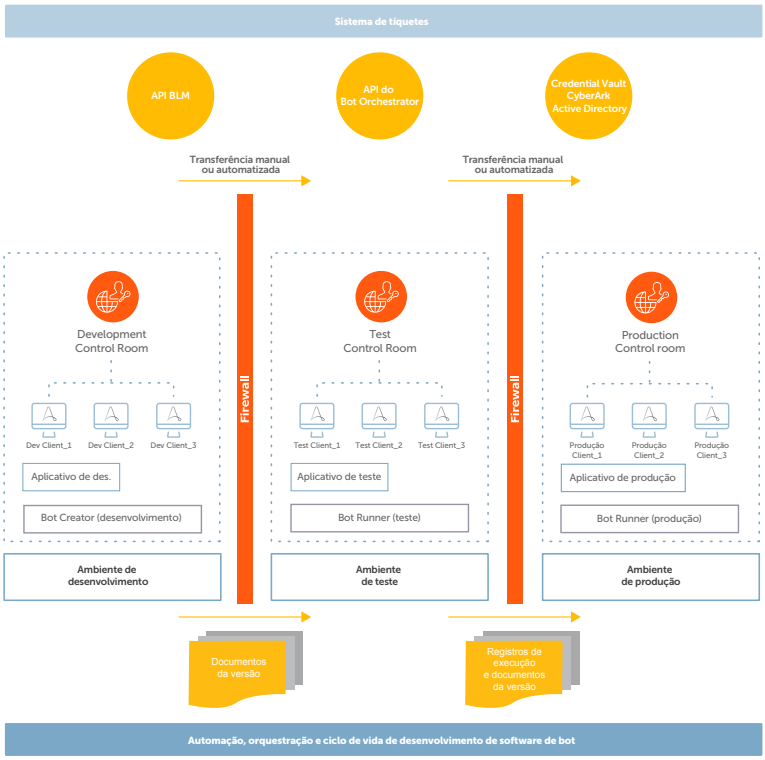


Figura 8: Modelo de implantação avançado para SDLC completo

LOG E MONITORAMENTO

Recursos de log de auditoria abrangente, monitoramento e relatórios são componentes essenciais da arquitetura de segurança para qualquer solução importante de TI. O Automation Anywhere Enterprise não é uma exceção.

Na plataforma, detalhes de evento (quem, o quê, quando, onde e o resultado) são capturados automaticamente para mais de 60 tipos de ações de usuário/entidade, incluindo a criação, a modificação, a ativação, a desativação e a remoção de usuários, bots, Bot Creators e Bot Runners. A não repudiação é alcançada por meio de uma combinação de captura automática, vinculação de cada atividade a uma identidade específica e uma política padrão de somente leitura. Em primeiro lugar, o RBAC também pode ser implantado para controlar rigorosamente quais funções têm visibilidade aos logs de auditoria.

De uma perspectiva de monitoramento, painéis automatizados e relatórios são acessíveis dentro da Control Room e podem ser personalizados para identificar e alertar atividades anormais (ou qualquer outro detalhe que a equipe de automação ou segurança decidir ser de interesse). Além disso, a habilidade de exportar logs possibilita o uso de outras análises, relatórios e infraestrutura de investigação/resposta de incidente já em uso pela organização, como SIEM, UEBA e ferramentas de análise avançadas.

FUNCIONALIDADES DE SEGURANÇA E RESILIÊNCIA EMPRESARIAIS ADICIONAIS

O Automation Anywhere Enterprise oferece suporte adicional à segurança empresarial e objetivos de resiliência com:

+ Uma arquitetura de componente distribuída (e flexível) que é capaz de se encaixar perfeitamente a uma infraestrutura e processos de alta disponibilidade/recuperação de desastre (HA/DR) existentes da organização
+ Um sistema de controle de versão integral (Apache Subversion) que, em conjunto com os recursos RBAC extensivos da plataforma, consegue implementar e aplicar uma política e processos de gerenciamento de mudança altamente rigorosos
+ Ferramentas como as estruturas de Hibernate e ReactJS durante o desenvolvimento de código de plataforma para ajudar a eliminar a suscetibilidade para ataques comuns (como Inserção de SQL e Scripts entre sites)
+ Um protocolo/plano de segurança para desenvolvimento de código que requer multiferramentas contínuas, rastreamento multicamadas para detectar e eliminar vulnerabilidades de software

Mais detalhes sobre esses e os muitos outros controles, proteções e recursos de segurança que fazem parte do Automation Anywhere Enterprise podem ser encontrados aqui: https://www.automationanywhere.com/images/Enterprise-Architecture.pdf

AUTOMAÇÃO DA API

À medida que a implantação de bots cresce exponencialmente, são revelados novos desafios para autenticação segura em escala e gerenciamento operacional do ciclo de vida do bot. Há uma necessidade de reduzir o tempo para implantar e eliminar erro humano. A Automation Anywhere fornece APIs para integração com automação de terceiros para autenticação segura e orquestração do gerenciamento do ciclo de vida do bot. Esta seção descreverá as APIs que fornecem os recursos mencionados acima.

Credential Vault – API

O Credential Vault da Automation Anywhere é usado para o armazenamento criptografado de credenciais que é usado por uma automação (bot) para a autenticação segura. As APIs do Credential Vault podem ser usadas para sincronização de credenciais com sistemas de gerenciamento de identidade (IAM) externos por meio de um programa orquestrador, cenários em que o bot recebe uma senha sob determinadas circunstâncias, que muda após cada uso e gerenciamento externo de credenciais por meio de um programa orquestrador externo.

API de implantação de bot

A API de implantação de bot permite que aplicativos externos iniciem um fluxo de trabalho de automação em um Bot Runner. Onde qualquer bot pode ser iniciado por meio da API, em um contexto de segurança, os bots que realizam funções de segurança podem ser orquestrados por um aplicativo externo. Por exemplo, uma solução SIEM pode acionar um alerta que inicia um bot para realizar a coleta de dados do sistema indicado no alerta. Essa coleta de dados pode ser qualquer coisa, como despejar tabelas de processo em execução, instantâneos de somas de verificação de arquivo, utilização de recursos e usuários conectados no momento.

API de Gerenciamento do ciclo de vida dos bots

A API de BLM (Bot Lifecycle Management, Gerenciamento do ciclo de vida dos bots) permite que um aplicativo de orquestração externo automatize o processo de mover bots de uma Control Room para outra. Isso é importante em empresas que utilizam o SDLC (Software Development Lifecycle, Ciclo de vida do desenvolvimento de software). Consulte a seção sobre SDLC para obter mais informações. O processo de SDLC pode ser automatizado integrando sistemas de tíquetes como JIRA ou Zendesk para acionar o desenvolvimento, o teste, a revisão de segurança e a promoção para a produção de bots. Um processo de SDLC automatizado fornece um livro de operação para a criação de bots, provando com maior garantia que cada bot em produção faz o que foi projetado para fazer, em um processo auditável que fornece todos os controles de governança que sua organização precisa.

CONCLUSÃO

A Automação Robótica de Processos apresenta uma grande promessa para empresas modernas que procuram diminuir seus custos operacionais, aumentar a satisfação do cliente e ganhar uma vantagem com relação à concorrência. Como líder de mercado, a plataforma de força de trabalho digital Automation Anywhere Enterprise ajuda a garantir o máximo de conquistas desses e de outros benefícios, entregando recursos não apenas de confiabilidade, escalabilidade e usabilidade necessários para o sucesso, mas também segurança de nível empresarial para preservar a confidencialidade, a integridade e a disponibilidade de todo o ambiente de automação.

Para obter mais informações sobre o Automation Anywhere Enterprise, acesse: https://www.automationanywhere.com/products/enterprise.