República Federativa do Brasil
Ministério da Economia
Instituto Nacional da Propriedade Industrial

(11) BR 112016020337-2 B1

(22) Data do Depósito: 18/03/2015

(45) Data de Concessão: 30/08/2022

(54) Título: DISPOSITIVO, MÉTODO IMPLEMENTADO POR COMPUTADOR E MEIO DE ARMAZENAMENTO LEGÍVEL POR MÁQUINA PARA FORNECER SEGURANÇA DE REDE ATRAVÉS DE CONTAS FORNECIDAS JUST-IN-TIME

(51) Int.Cl.: G06F 21/62.

(30) Prioridade Unionista: 20/03/2014 US 14/220,486.

(73) Titular(es): MICROSOFT TECHNOLOGY LICENSING, LLC.

(72) Inventor(es): SHANE BRADY; SIDDHARTHA MATHUR; RAJALAKSHMI DANI; SANTOSH KUMAR; LUKE SCHOEN; DAVID HETHERINGTON.

(86) Pedido PCT: PCT US2015021120 de 18/03/2015

(87) Publicação PCT: WO 2015/142965 de 24/09/2015

(85) Data do Início da Fase Nacional: 02/09/2016

(57) Resumo: DISPOSITIVO, MÉTODO IMPLEMENTADO POR COMPUTADOR E HARDWARE DE ARMAZENAMENTO LEGÍVEL POR COMPUTADOR PARA FORNECER SEGURANÇA DE REDE ATRAVÉS DE CONTAS FORNECIDAS JUST-IN-TIME. Técnicas para conter movimento lateral de invasores através de contas fornecidas just-in-time (JIT) compreendendo um componente de gerenciamento de conta para receber uma solicitação de uma primeira conta através de um dispositivo do cliente para uma segunda conta para acessar um dispositivo do servidor em um conjunto de dispositivos do servidor, um componente de autorização de conta para autorizar a solicitação para a segunda conta com base pelo menos parcialmente na informação da conta associada com a primeira conta, um componente de fornecimento de conta para fornecer a segunda conta para permitir que um cliente acesse o dispositivo do servidor e um componente de notificação de conta para fornecer informação da conta associada com a segunda conta a um cliente através do dispositivo do cliente. Outras modalidades são descritas e reivindicadas.

Relatório Descritivo da Patente de Invenção para **"DISPOSITIVO, MÉTODO IMPLEMENTADO POR COMPUTADOR E MEIO DE ARMAZENAMENTO LEGÍVEL POR MÁQUINA PARA FORNECER SEGURANÇA DE REDE ATRAVÉS DE CONTAS FORNECIDAS JUST-IN-TIME ".**

ANTECEDENTES

[001] Com várias metodologias de desenvolvimento de ritmo acelerado disponíveis hoje para elaboração de sistemas de Software Como Serviço (SaaS) sistemas, inúmeros usuários (por exemplo, analistas, engenheiros, empreiteiros, clientes internos e/ou clientes externos) podem precisar de acesso aos servidores hospedando um ou mais serviços dos sistemas de SaaS com a finalidade de teste, atualização, depuração, desenvolvimento, implantação e/ou manutenção desses servidores diariamente. Com inúmeros usuários exigindo acesso aos servidores, cada usuário pode ser atribuído com uma ou mais contas do usuário para acessar esses servidores. Entretanto, conforme o número de contas de usuário aumenta, também aumenta o risco de segurança do associado segurança. Isso ocorre porque cada conta de usuário adicional pode expor um ponto de entrada em potencial para invasores e, consequentemente, aumentar a superfície ou vetor de ataque para os invasores obterem acesso não autorizado. Esses pontos de entrada em potencial se tornam particularmente problemáticos quando alguma conta de usuário pode ter privilégios elevados (por exemplo, privilégios administrativos) para realizar suas tarefas diárias. Mesmo quando invasores não tem acesso inicialmente a uma conta de usuário tendo privilégios elevados, os invasores podem empregar técnicas, como por exemplo, uma "passagem de ataque hash" para obter acesso a uma conta de usuário com privilégios elevados para interromper serviços de sistemas SaaS. Tal acesso não autorizado por invasores pode causar prejuízo considerável a um negócio e despertas

preocupações de segurança e privacidade relevantes aos clientes.

Sumário

[002] A seguir é apresentado um sumário simplificado a fim de fornecer um entendimento básico de algumas modalidades novas aqui descritas. Esse sumário não é uma visão geral extensiva e não é destinado à identificação de elementos chave/críticos ou delinear o escopo do mesmo. Sua única finalidade é apresentar alguns conceitos em uma forma simplificada como um prelúdio à descrição mais detalhada que é posteriormente apresentada.

[003] Várias modalidades são geralmente direcionadas às técnicas para melhorar a segurança de rede contendo movimento lateral de invasores através das contas fornecidas *Just-In-Time* (JIT) ou contas JIT. Algumas modalidades são especificamente direcionadas às técnicas para gerenciar contas JIT. Em uma modalidade, por exemplo, um dispositivo pode compreender um circuito do processador; e um aplicativo do servidor para execução pelo circuito do processador. O aplicativo do servidor pode compreender um componente de gerenciamento de conta para receber uma solicitação de uma primeira conta através de um dispositivo do cliente para uma segunda conta para acessar um dispositivo do servidor em um conjunto de dispositivos do servidor, um componente de autorização de conta para autorizar a solicitação para a segunda conta com base pelo menos parcialmente na informação da conta associada com a primeira conta, um componente de fornecimento de conta para fornecer a segunda conta para permitir que um cliente acesse o dispositivo do servidor, e um componente de notificação de conta para fornecer informação da conta associada com a segunda conta a um cliente através do dispositivo do cliente. Outras modalidades são descritas e reivindicadas.

[004] Para a realização do supracitado e finalidades relacionadas, certos aspectos ilustrativos são aqui descritos em conexão com a

seguinte descrição e desenhos anexos. Esses aspectos são indicativos das várias formas nas quais os princípios aqui revelados podem ser praticados e todos os aspectos e equivalentes dos mesmos são destinados a estarem dentro do escopo da matéria reivindicada. Outras vantagens e novos recursos ficarão mais evidentes a partir da descrição detalhada quando consideradas em conjunto com os desenhos.

BREVE DESCRIÇÃO DOS DESENHOS

[005] A figura 1 ilustra uma modalidade de uma conta JIT que fornece o sistema para fornecimento de contas JIT.

[006] A figura 2 ilustra outra modalidade do sistema de fornecimento de conta JIT para segmentação, fornecimento e/ou configuração de um ou mais recursos e/ou ativos em um ou mais limites de violação.

[007] A figura 3 ilustra ainda outra modalidade do sistema de fornecimento de conta JIT para autorizar clientes e gerenciar tokens de autenticação associados com contas JIT.

[008] A figura 4A ilustra uma modalidade de um fluxo lógico para fornecer contas JIT.

[009] A figura 4B ilustra uma modalidade de um fluxo lógico para autorizar as solicitações recebidas para contas JIT tendo permissões elevadas de acesso.

[0010] A figura 4C ilustra uma modalidade de um fluxo lógico para habilitar as contas JIT fornecidas.

[0011] A figura 4D ilustra uma modalidade de um fluxo lógico para configurar permissões de acesso associados com contas JIT.

[0012] A figura 4E ilustra uma modalidade de um fluxo lógico para gerenciar vidas úteis associadas com contas JIT.

[0013] A figura 5 ilustra uma modalidade de uma arquitetura computacional.

DESCRIÇÃO DETALHADA

[0014] Várias modalidades são direcionadas a um sistema de fornecimento de conta de rede disposto para fornecer segmentação de identidade implementando os limites de violação e dividindo as credenciais. Utilizando os limites de violação e fornecendo contas *just-in-time* (JIT) aos clientes que mantém, gerenciam, e/ou utilizam um ou mais recursos e/ou ativos associados com um sistema SaaS, a segurança e privacidade do sistema SaaS podem ser substancialmente melhoradas. Para atingir essas e outras melhorias, o sistema de fornecimento de conta de rede pode geralmente estar disposto para dividir ou segmentar pelo menos uma porção (por exemplo, um domínio) do sistema SaaS em dois ou mais limites de violação, onde cada limite de violação pode ser associado com um ou mais recursos e/ou ativos (por exemplo, servidores, estações de trabalho, dispositivos computacionais, dispositivos móveis, aplicativos, serviços, e/ou componentes de software/hardware) e ainda associado com um grupo de segurança disposto para gerenciar permissões de acesso àqueles recursos dentro desse limite de violação.

[0015] Para permitir que os clientes (por exemplo, usuários, engenheiros, empreiteiros, clientes, e/ou componentes de software/hardware) acessem a esses recursos e/ou ativos, o sistema de fornecimento de conta JIT pode ser ainda disposto para adicionar uma ou mais contas JIT como membros em um grupo de segurança associado com o limite de violação incluindo esses recursos e/ou ativos. Dessa forma, as contas JIT podem permitir que clientes com contas existentes tendo privilégios e/ou permissões inferiores ou mais baixos, para obter uma conta JIT com privilégios elevados para realizar um ou mais serviços (por exemplo, testar, melhorar, depuração, desenvolvimento, implementação, e/ou manutenção de um ou mais recursos de um Sistema SaaS) que pode precisar de privilégios necessários a realizar.

[0016] Para obter as contas JIT com privilégios elevados para realizar um ou mais serviços em um ou mais recursos e/ou ativos no sistema SaaS, o sistema de fornecimento de conta JIT pode ser disposto para receber solicitações de clientes para permissões de acesso elevado a fim de acessar os recursos e/ou ativos do sistema SaaS. Em resposta, o sistema de fornecimento de conta JIT pode ser disposto para fornecer as contas JIT como parte das solicitações para permissões de acesso elevado. Cada solicitação pode ser ainda associada com uma função solicitada e escopo fornecido pelo cliente de modo que o sistema de fornecimento de conta JIT pode fornecer cada conta JIT com permissões minimamente abrangentes necessárias para realizar uma tarefa ou serviço conforme solicitado pelo cliente.

[0017] Uma vez que a solicitação é aprovada por outro cliente e/ou automaticamente autenticado pelo sistema de fornecimento de conta JIT, o sistema de fornecimento de conta JIT pode ser ainda disposto criando a conta JIT para a função solicitada e o escopo em resposta à aprovação. Nos casos quando uma conta JIT associada com o cliente já existe, o sistema de fornecimento de conta JIT pode ser disposto para reutilizar a conta JIT existente previamente criada para a mesma função e escopo solicitado pelo cliente. Pelo lento fornecimento das contas JIT em conjunto com a reutilização das contas JIT previamente criadas, o número de contas JIT do sistema de fornecimento de conta JIT pode ser necessário para gerenciar pode ser significativamente reduzido.

[0018] Para informar os clientes se uma solicitação foi autenticada, aprovada, e/ou rejeitada, o sistema de fornecimento de conta JIT pode ser ainda disposto para fornecer notificação ao cliente se a solicitação de uma conta JIT com permissões de acesso elevado foi autenticada, aprovada e/ou rejeitada. Se a solicitação para a conta JIT com permissões de acesso elevado foi autenticada e/ou aprovada, o sistema de

fornecimento de conta JIT pode ainda notificar os clientes com relação à aprovação e fornecer informação da conta JIT associada com a conta JIT fornecida. O cliente pode então utilizar a informação da conta JIT para acessar e/ou operar, com permissões de acesso elevado, um ou mais recursos e/ou ativos dentro da função e escopo da conta JIT fornecida.

[0019] Para ainda garantir a segurança e privacidade do sistema SaaS, o sistema de fornecimento de conta JIT pode ser ainda disposto para associar cada conta JIT com uma vida útil (por exemplo, 4 horas) de modo que cada conta JIT possa ser desabilitada no final da sua vida útil associada. A vida útil associada com cada conta pode ser explicitamente fornecida pelos clientes em suas solicitações para contas JIT. De modo alternativo ou adicional, as vidas úteis podem ser intrínsecas aos escopos e funções associadas com contas JIT específicas. Para uma ou mais contas JIT que permaneceram inativas por períodos longos de tempo (por exemplo, um mês), o sistema de fornecimento de conta JIT pode ser ainda disposto para remover ou destruir as contas JIT inativas do sistema de fornecimento de conta JIT.

[0020] Como um resultado, o sistema de fornecimento de conta JIT pode melhorar a segurança e a privacidade do sistema SaaS limitando o movimento lateral de invasores entre os limites de violação e conformando os invasores em um único limite de violação de modo que o melhor que um invasor possa fazer comprometendo uma conta JIT é para lateralmente mover entre os recursos e/ou ativos dentro do mesmo escopo de impacto. O sistema de fornecimento de conta JIT também torna qualquer conta existente de clientes associados com clientes desinteressante aos invasores, pois eles serão geralmente restritos ao nível inferior ou mais baixo de permissões de acesso e qualquer solicitação para uma conta JIT com permissões de acesso elevado pode precisar de autorização prévia. Mesmo quando uma con-

ta JIT com permissões de acesso elevado é comprometida, o invasor será confinado a um único limite de violação e seu acesso terá uma vida útil limitada antes da conta JIT ficar desabilitada. Dessa forma, segurança e privacidade do sistema SaaS podem ser muito melhoradas.

[0021] Com referência geral às notações e nomenclatura aqui utilizadas, as descrições detalhadas que seguem podem ser apresentadas em termos de procedimentos de programa executados em um computador ou rede de computadores. Essas descrições procedurais e representações são utilizadas pelos técnicos no assunto para conduzir mais efetivamente a substância de seu trabalho a outros técnicos no assunto.

[0022] Um procedimento é aqui e, de modo geral, concebido para ser uma sequência auto consistente de operações levando a um resultado desejado. Essas operações são aquelas que precisam de manipulações físicas de quantidades físicas. Geralmente, embora não necessariamente, essas quantidades tomam a forma de sinais elétricos, magnéticos ou ópticos capazes de serem armazenados, transferidos, combinados, comparados e, caso contrário, manipulados. Demonstra-se conveniente, principalmente por razões de uso comum, para referir a esses sinais como bits, valores, elementos, símbolos, caracteres, termos, números ou similares. Deve ser observado, entretanto, que todos esses termos e similares devem estar associados com as quantidades físicas apropriadas e são meramente identificações convenientes aplicadas a essas quantidades.

[0023] Ainda, as manipulações realizadas são geralmente referidas em termos, como adição ou comparação, que são geralmente associadas com operações mentais realizadas por um operador humano. Nenhuma capacidade de um operador humano é necessária, ou desejável na maioria dos casos, em qualquer uma das operações aqui des-

critas que formam parte de uma ou mais modalidades. Ainda, as operações são operações de máquina. As máquinas úteis para realizar as operações de várias modalidades incluem computadores digitais de finalidade geral ou dispositivos similares.

[0024] Várias modalidades também se referem ao dispositivo ou sistemas para realizar essas operações. Esse dispositivo pode ser especialmente construído para a finalidade necessária ou pode compreender um computador de finalidade geral como seletivamente ativado ou reconfigurado por um programa de computador armazenado no computador. Os procedimentos aqui apresentados não estão inerentemente relacionados a um computador ou outro dispositivo específico. Várias máquinas de finalidade geral podem ser utilizadas com programas gravados de acordo com os ensinamentos na presente invenção, ou pode demonstrar-se conveniente para construir dispositivo mais especializado para realizar as etapas de método necessárias. A estrutura necessária para uma variedade dessas máquinas aparecerá a partir da descrição dada.

[0025] A referência é agora feita aos desenhos, em que os numerais de referência similares são utilizados para se referir aos elementos similares por todo o relatório. Na seguinte descrição, para finalidades de explicação, vários detalhes específicos são definidos para fornecer um entendimento completo do mesmo. Pode ser evidente, entretanto, que as novas modalidades podem ser praticadas sem esses detalhes específicos. Em outros exemplos, estruturas e dispositivos bem conhecidos são mostrados na forma de diagramas em blocos a fim de facilitar uma descrição do mesmo. A intensão é abranger todas as modificações, equivalentes e alternativas consistentes com a matéria reivindicada.

[0026] A figura 1 ilustra uma modalidade do sistema de fornecimento de conta JIT 100. Em várias modalidades, o sistema de forne-

cimento de conta JIT 100 pode ser implementado em ou com um ambiente computacional empresarial 150 (por exemplo, sistemas de armazenamento em nuvem, centros de dados, etc.) compreendendo um ou mais clientes 102-a (por exemplo, usuários, engenheiros, empreiteiros, clientes, e/ou componentes de software/hardware) onde cada cliente (por exemplo, cliente 102-1 ou 102-2) pode ser associado com uma ou mais contas do cliente e cada conta do cliente de uma ou mais contas do cliente pode ainda ser associada com informação da conta do cliente. A informação da conta do cliente pode incluir, mas é limitado à, informação de autenticação da conta do cliente (por exemplo, nome principal do usuário (UPN), identificador da conta, senha da conta ou derivados em hash e/ou de sal do mesmo, domínio da conta, certificados do smart card, biométrica, etc.), informação de autorização da conta do cliente (por exemplo, função da conta do cliente e informação de escopo, permissões de acesso, grupos associados, etc.), e/ou qualquer outra informação relevante à autenticação e autorização de um ou mais clientes 102-a.

[0027] Um ou mais clientes 102-*a* podem utilizar uma ou mais contas do cliente para solicitar contas JIT tendo permissões de acesso elevado para operar um ou mais recursos e/ou ativos como, por exemplo, dispositivos do servidor 140-*i-j* dispostos para fornecer um ou mais serviços de um ou mais sistemas SaaS (por exemplo, MICROSOFT Office 365, MICROSOFT Exchange Online MICROSOFT SharePoint Online, MICROSOFT Dynamics CRM, etc.). Os dispositivos do servidor 140-*i-j* podem ser ainda interconectados entre si através da interconexão de rede 112 a fim de fornecer os serviços dos sistemas SaaS. Pode ser observado que os dispositivos do servidor 140-*i-j* em várias modalidades são meramente referenciados para finalidades de ilustração e não limitação. Assim, qualquer um ou todos os dispositivos do servidor 140-*i-j* em várias modalidades podem ser substi-

tuídos por quaisquer outros recursos e/ou ativos como, por exemplo, dispositivos virtuais, estações de trabalho, dispositivos computacionais, dispositivos móveis, aplicativos, serviços, e/ou outros componentes de software/hardware.

[0028] Vale ressaltar também que "a" e "b" e "c" e designadores similares como aqui utilizados são destinados para serem variáveis que representam qualquer número inteiro positivo. Assim, por exemplo, se uma implementação define um valor para a = 2, então um conjunto completo de clientes 102-*a* pode incluir clientes 102-1 e 102-2. Em outro exemplo, se uma implementação define valores para i = 1 e j = 6, então um conjunto completo de dispositivos do servidor 140-*i-j* pode incluir dispositivos do servidor 140-1-1, 140-1-2, 140-1-3, 140-1-4, 140-1-5, e 140-1-6. As modalidades não são limitadas nesse contexto.

[0029] O sistema de fornecimento de conta JIT 100 pode compreender um ou mais dispositivos do cliente 104-6 (por exemplo, laptops, computadores, telefones, estações de trabalho, ou quaisquer outros dispositivos computacionais) utilizados pelos clientes 102-*a* para operar os dispositivos do servidor 140-*i-j* de um ou mais sistemas SaaS (por exemplo, teste, modernização, depuração, desenvolvimento, implantação, e/ou manutenção um ou mais recursos e/ou ativos dos Sistemas SaaS) através da interconexão de rede 112. Além disso, a interconexão de rede 112 pode estar disposta para fornecer conectividade de rede entre uma variedade de dispositivos, componentes, aplicativos, servidores, recursos, e/ou ativos no ambiente computacional empresarial 150 sobre uma ou mais redes (por exemplo, intranet e/ou internet) utilizando um ou mais dispositivos de rede (por exemplo, repetidores, pontes, cubos, interruptores, roteadores, gateways, balanças, etc.).

[0030] O sistema de fornecimento de conta JIT 100 pode compreender ou ser integrado com um ou mais dispositivos do servidor de

serviço de diretório 130-/ que podem ser geralmente dispostos para executar, entre outros aplicativos, aplicativo do serviço de diretório (não mostrado) a fim de organizar os dispositivos do servidor 140-*i*-*j* em uma hierarquia de um ou mais grupos lógicos, subgrupos lógicos, e/ou sub-subgrupos lógicos (por exemplo, florestas 132-*k*, domínios 136-*d*, e/ou unidades organizacionais 134-*e*-*f*). Os dispositivos do servidor de serviço de diretório 130-/ também podem estar dispostos para armazenar a hierarquia em um ou mais armazenamentos de dados do serviço de diretório (não mostrado) compreendendo informação de serviço de diretório.

[0031] A informação de serviço de diretório pode compreender informação da conta JIT associada com uma ou mais contas JIT de modo que um ou mais dispositivos do servidor de serviço de diretório 130-/ possam autenticar as solicitações de acesso de um ou mais clientes 102-*a* utilizando contas JIT para acessar um ou mais recursos e/ou ativos. A informação da conta JIT pode incluir, mas é limitado à, informação de autenticação da conta JIT (por exemplo, nome principal do usuário (UPN), identificador da conta, senha da conta ou derivados de hash e/ou de sal do mesmo, domínio da conta, certificados do smart card, biométrica, etc.), informação de autorização da conta JIT (por exemplo, função da conta JIT e informação de escopo, permissões de acesso da conta JIT, grupos associados da conta JIT, etc.), informação de vida útil da conta JIT (por exemplo, vida útil de uma conta JIT), a informação de serviço de diretório (por exemplo, um dispositivo do servidor de serviço do diretório associado com uma conta JIT), e/ou qualquer outra informação relevante à autenticação, autorização e vida útil de uma ou mais contas JIT.

[0032] Em várias modalidades, cada dispositivo do servidor de serviço do diretório (por exemplo, dispositivo do servidor de serviço do diretório 130-l) pode compreender ou implementar um aplicativo do

serviço de diretório (não mostrado). Aplicativos do serviço de diretório exemplares podem incluir, mas não se limitam à, MICROSOFT Active Directory, NOVELL eDirectory, APPLE Open Directory, ORACLE Internet Directory (OID), IBM Tivoli Directory Server, ou qualquer outro aplicativo que implementa o Protocolo de Acesso de Diretório (DAP | *Directory Access Protocol*), Protocolo de Acesso de Diretório Leve (LDAP | *Lightweight Directory Access Protocol*), e/ou X.500 padrões promulgados pela União de Telecomunicação Internacional (ITU | *International Telecommunication Union*), Setor de Padronização de Telecomunicação (ITU-T | *Telecommunication Standardization Sector*).

[0033] Em modalidade, o dispositivo do servidor de serviço do diretório 130-l pode compreender ou implementar pelo menos uma porção de Diretório Ativo da MICROSOFT (por exemplo, Serviços de Domínio de Diretório Ativo, Controladores de Domínio de Diretório Ativo, Armazenamentos de Dados de Diretório Ativo, etc.). Cada dispositivo do servidor de serviço do diretório (por exemplo, dispositivo do servidor de serviço do diretório 130-*l*) de um ou mais dispositivos do servidor de serviço de diretório 130-/ pode ser disposto para gerenciar um grupo lógico de nível superior como, por exemplo, floresta 132-1. Uma ou mais florestas 132-*k*pode compreender um ou mais grupos lógicos inferiores, por exemplo, subgrupos lógicos, como, por exemplo, domínios 136-*d*. Cada domínio (por exemplo, domínio 136-1) de um ou mais domínios 136-*d* pode ser disposto para gerenciar grupos lógicos de nível inferior, por exemplo, sub-subgrupos lógicos, como, por exemplo, unidades organizacionais 134-*e*-*f*. Opcionalmente, os domínios 136-*d* podem ainda ser logicamente agrupados em um ou mais grupos lógicos intermediários entre as florestas 132-*k* e domínios 136-*d*, como, por exemplo, árvores (não mostradas). Cada unidade organizacional (por exemplo, unidade organizacional 134-1-1) de uma ou mais unidades organizacionais 134-e-f pode compreender um ou mais

recursos e/ou ativos, como, por exemplo, dispositivos do servidor 140-*g*-*h*.

[0034] Pode ser observado que as florestas 132-*k*, domínios 136-*d*, e/ou unidades organizacionais 134-*e*-*f* em várias modalidades são meramente referenciados para finalidades de ilustração e não limitação. Assim, quaisquer ou todas as florestas 132-*k*, domínios 136-*d*, e/ou unidades organizacionais 134-*e*-*f* em várias modalidades podem ser substituídas com seus equivalentes substanciais para uma dada implementação. Por exemplo, em uma implementação onde o dispositivo do servidor de serviço do diretório 130-l pode compreender ou implementar pelo menos uma porção de NOVELL eDirectory, as florestas 132-*k*, domínios 136-*d* e unidades organizacionais 134-*e*-*f* podem ser substituídos por árvores, divisões e unidades organizacionais conforme implementado em NOVELL eDirectory, respectivamente. As modalidades não estão limitadas nesse contexto.

[0035] Para conter o movimento lateral de um invasor, cada domínio (por exemplo, domínio 136-1) do sistema de fornecimento de conta JIT 100 pode ainda compreender um ou mais limites de violação 138-*g*-*h*. Por exemplo, o domínio 136-1 pode compreender limites de violação 138-1-1 e 138-1-2. Adicionalmente, em algumas implementações, os limites de violação 138-*g*-*h* podem ser independentes de uma ou mais unidades organizacionais 134-*e*-*f*. Por exemplo, no domínio 136-1, as unidades organizacionais 134-1-1, 134-1-2, 134-1-3 podem abranger limites transversais de violação 138-1-1 e 138-1-2, de modo que um único limite de violação, como limite de violação 138-1-1 possa incluir recursos e/ou ativos, como, por exemplo, dispositivos do servidor 140-1-1, 140-1-2, 140-1-3, de todas as três unidades organizacionais 134-1-1, 134-1-2, 134-1-3. Em outros domínios, como, por exemplo, domínios 136-*d*, limites de violação 138-*g*-*h*, como, por exemplo, limite de violação 138-*g*-*h* pode coexistir com unidades organizacionais

134-*e*-*f* como, por exemplo, unidade organizacional 134-*e*-*f* de modo que a único limite de violação como limite de violação 138-*g*-*h* possa incluir recursos e/ou ativos, como, por exemplo, dispositivos do servidor 140-*i*-1, 140-*i*-4, de uma única unidade organizacional 134-*e*-*l*.

[0036] Um ou mais limites de violação 138-*g*-*h* podem ser geralmente gerenciados por um ou mais dispositivos do servidor de serviço de diretório 130-*l* e dispostos para conceder ou fornecer um conjunto de permissões de acesso para uma ou mais contas JIT que podem ser associadas com o limite de segurança de modo que uma ou mais contas JIT possam acessar um ou mais recursos e/ou ativos dentro do limite de segurança. Para ainda garantir que um invasor tendo acesso a uma conta JIT não possa mover entre um ou mais limites de violação 138-*g*-*h* utilizando uma "passagem pelo ataque *hash*", cada limite de violação (por exemplo, limites de violação 138-1-1 e 138-1-2) de um ou mais limites de violação 138-*g*-*h* pode ainda estar disposto para incluir um conjunto de recursos e/ou ativos mutualmente exclusivo ou não sobreposto de modo que não haja sobreposição entre quaisquer limites de violação 138-*g*-*h*.

[0037] O sistema de fornecimento de conta JIT 100 pode compreender dispositivo do servidor 108 que pode ser geralmente disposto para executar, entre outros aplicativos, o aplicativo do serviço de diretório 110. O aplicativo do serviço de diretório 110 pode geralmente ser disposto para armazenar e fornecer informação da conta do cliente associada com uma ou mais contas do cliente de clientes 102-*a*. O aplicativo do serviço de diretório 110 também pode ser disposto para armazenar informação de hierarquia organizacional compreendendo estrutura hierárquica de uma organização que um ou mais clientes 102-*a* podem ser um membro ou afiliado de (por exemplo, uma corporação) de modo que quaisquer supervisores e/ou gestores de um ou mais clientes 102-*a* possam ser identificados. O aplicativo do serviço

de diretório 110 pode ser ainda disposto para autenticar ou auxiliar na autenticação de um ou mais clientes 104-*a* solicitando contas JIT tendo permissões de acesso elevado através do aplicativo de gerenciamento de administração 114. Aplicativos de serviço de diretório exemplares ou implementações podem incluir, mas não se limitam à, aqueles previamente discutidos com relação aos dispositivos do servidor de serviço de diretório 130-/.

[0038] Para autenticar ou facilitar a autenticação de um ou mais clientes 102-*a* que solicitam uma conta JIT tendo permissões de acesso elevado, o aplicativo do serviço de diretório 110 pode ainda expor e/ou implementar uma ou mais interfaces de programa de aplicativo (APIs) para o aplicativo de gerenciamento de administração 114 autenticar um ou mais clientes 102-*a* que solicitam permissões de acesso elevado. Por exemplo, o aplicativo de gerenciamento de administração 114 pode autenticar um ou mais clientes 102-*a* que solicitam permissões de acesso elevado utilizando através da interconexão de rede 112, uma ou mais APIs, e/ou um ou mais mecanismos de chamada de procedimentos locais (LPC) e/ou chamada de procedimentos remotos (RPC) do aplicativo do serviço de diretório 110. APIs exemplares podem incluir, mas não se limitam à, ADP API, LADP API, MICROSOFT Active Directory Service Interfaces (ADSI) API, MICROSOFT Messaging API (MAPI), MICROSOFT Directory System Agent (DSA) API, e/ou qualquer outra API que possibilita a autenticação de clientes 102-*a*.

[0039] O sistema de fornecimento de conta JIT 100 pode compreender o dispositivo do servidor 106 que pode ser geralmente disposto para executar, entre outros aplicativos, o aplicativo de gerenciamento de administração 114. O aplicativo de gerenciamento de administração 114 pode geralmente ser disposto para receber solicitações de um ou mais clientes 102-*a* para elevar permissões de acesso e autenticar

uma ou mais solicitações recebidas dos clientes 102-*a*. Adicionalmente, o aplicativo de gerenciamento de administração 114 pode ser ainda disposto para gerenciar, autorizar, fornecer uma ou mais contas JIT tendo as permissões de acesso elevado solicitadas pelas clientes 102-*a* e notificar os clientes 102-*a* com a informação da conta JIT associada com as contas JIT fornecidas.

[0040] Em várias modalidades, o aplicativo de gerenciamento de administração 114 pode compreender um componente de gerenciamento de conta 116. O componente de gerenciamento de conta 116 pode ser geralmente disposto para autenticar um ou mais clientes 102-*a* que solicitam contas JIT tendo permissões de acesso elevado e recebem uma ou mais solicitações de um ou mais clientes 102-*a* através de dispositivos do cliente 104-*b* para elevar permissões de acesso a fim de realizar uma ou mais ações ou tarefas em um recurso e/ou ativo.

[0041] Em modalidade, o componente de gerenciamento de conta 116 pode permitir que o cliente 102-1 autentique ao aplicativo de gerenciamento de administração 114 antes de permitir que o cliente 102-1 solicite uma conta JIT tendo permissões de acesso elevado. Para permitir que o cliente 102-1 seja autenticado, o componente de gerenciamento de conta 116 pode solicitar e/ou receber pelo menos uma porção da informação da conta do cliente (por exemplo, identificador da conta e/ou senha da conta) do cliente 102-1 onde a informação da conta do cliente recebida pode ser associada com a conta do cliente do cliente 102-1. O componente de gerenciamento de conta 116 pode receber a informação da conta do cliente (por exemplo, UPN, identificador da conta, e/ou senha) através de um ou mais aplicativos e/ou componentes do dispositivo do cliente 104-1 (por exemplo, um navegador de um dispositivo computacional). Em resposta à informação da conta do cliente recebida, o componente de gerenciamento de conta

116 pode autenticar o cliente 102-1 com base pelo menos parcialmente na informação da conta do cliente recebida e na informação da conta do cliente previamente armazenada acessível pelo aplicativo do serviço de diretório 110. Além disso, para autenticar o cliente 102-1 com base pelo menos parcialmente na informação da conta do cliente previamente armazenada acessível pelo aplicativo do serviço de diretório 110, o componente de gerenciamento de conta 116 pode ser configurado para utilizar através da interconexão de rede 112 e uma ou mais APIs do aplicativo do serviço de diretório 110.

[0042] Continuando com o exemplo acima, uma vez que o cliente 102-1 foi autenticado, o componente de gerenciamento de conta 116 pode ser configurado para permitir que o cliente 102-1 insira a informação de solicitação de conta JIT. A informação de solicitação de conta JIT pode incluir, mas não se limita a, uma ou mais ações ou tarefas a serem realizadas, um ou mais dispositivos do servidor 140-*i*-*j* e uma informação de vida útil solicitada associada com uma ou mais ações ou tarefas. A informação de vida útil solicitada pode incluir, mas não se limita a, um tempo específico ou tempo decorrido de quando a conta JIT expira e fica desabilitada e/ou tempo específico ou tempo decorrido quando a conta JIT é removida.

[0043] De modo alternativo ou adicional, o componente de gerenciamento de conta 116 pode ser configurado para limitar a informação de vida útil solicitada recebida de um ou mais clientes 102-*a* em um valor máximo de modo que a vida útil associada com uma conta JIT não possa exceder uma quantidade de tempo predeterminada (por exemplo, minutos, horas, dias, semanas, anos, etc.). Em uma modalidade exemplar, o componente de gerenciamento de conta 116 pode limitar uma informação de vida útil solicitada para uma conta JIT tendo permissões de acesso elevado em um valor máximo de 72 horas ou 3 dias de modo que qualquer solicitação para uma conta JIT com uma

vida útil maior que 72 horas (por exemplo, 4 dias) será limitada a 72 horas ou 3 dias. As modalidades não são limitadas nesse contexto.

[0044] De modo alternativo ou adicional, o componente de gerenciamento de conta 116 também pode ser configurado para fornecer uma ou mais funções predefinidas e escopo associado com o ambiente computacional empresarial 150 e permite que um ou mais clientes 102-*a* selecione uma ou mais funções predefinidas e escopo com base nas ações ou tarefas a serem realizadas e cujo recurso e/ou ativo as ações ou tarefas devem ser realizadas.

[0045] Ações ou tarefas exemplares a serem realizadas podem incluir, mas não se limitam à depuração de aplicativo remoto, backups de aplicativo, modernizações e/ou manutenção de aplicativo, modernizações e/ou manutenção do servidor, teste e/ou quaisquer outras ações ou tarefas que podem precisar de acesso e/ou modificação de um ou mais recursos e/ou ativos. A informação de vida útil exemplar solicitada pode incluir, mas não se limita ao, o número de dias, minutos, horas, e/ou segundos para uma conta JIT pode permanecer tempo habilitado e/ou específico do dia e a data antes da conta JIT pode permanecer habilitada.

[0046] Em várias modalidades, o aplicativo de gerenciamento de administração 114 pode ainda compreender um componente de autorização de conta 118. O componente de autorização de conta 118 pode ser geralmente disposto para determinar a função solicitada e a informação de escopo e a função da conta do cliente e a informação de escopo. O componente de autorização de conta 118 pode ser ainda disposto para fornecer a função da conta do cliente e a informação de escopo aos clientes e autorizar a solicitação para elevar as permissões de acesso com base na função solicitada e a informação de escopo e a função da conta do cliente e a informação de escopo.

[0047] Em uma modalidade, o componente de autorização de con-

ta 118 pode ser configurado para determinar a função solicitada e a informação de escopo com base pelo menos parcialmente na informação de solicitação de conta JIT recebida e na informação de serviço de diretório fornecida pelos dispositivos do servidor de serviço de diretório 130-*l*. Para determinar a função solicitada e a informação de escopo, o componente de gerenciamento de conta 116 pode ser configurado para identificar uma ou mais funções solicitadas com base nas ações ou tarefas solicitadas fornecidas por um ou mais clientes 102-*a* através de um ou mais dispositivos do cliente 104-*b*.

[0048] Para determinar o escopo solicitado, o componente de autorização de conta 118 pode ser ainda configurado para se comunicar com os dispositivos do servidor de serviço de diretório 130-*l* e identificar o limite de segurança compreendendo os recursos e/ou ativos que os clientes 102-*a* solicitam para realizar as ações ou as tarefas. Funções solicitadas exemplares podem incluir, mas não se limitam à, administradores, operadores de backup, depuradores, usuários remotos, testadores e similares. Pode ser observado que cada função pode ser ainda associada com um conjunto de permissões de acesso que possa conceder e/ou negar acesso a um ou mais recursos e/ou ativos e/ou componentes de um ou mais recursos e/ou ativos. O escopo solicitado exemplar pode incluir, mas não se limita à, um ou mais dispositivos do servidor 140-1-1, 14-1-2, 14-1-3 ou quaisquer outros recursos e/ou ativos e/ou componentes dos recursos e/ou ativos.

[0049] Em modalidade, quando o cliente 102-1 solicita realizar a depuração de aplicativo remoto no dispositivo do servidor 140-1-1, a informação de função e escopo solicitada determinada pelo componente de autorização de conta 118 e associada com a ação ou tarefa solicitada pode incluir funções para um usuário remoto e um depurador e o escopo pode incluir o limite de violação 138-1-1. De modo alternativo ou adicional, a informação de solicitação de conta JIT recebida do

cliente 102-1 pode compreender uma seleção do cliente de uma ou mais funções predefinidas e informação de escopo previamente discutidas com relação ao componente de gerenciamento de conta 116, de modo que o componente de gerenciamento de conta 116 possa fácil e prontamente determinar a informação de função e escopo solicitada com base na informação de solicitação de conta JIT recebida.

[0050] Em uma modalidade, o componente de autorização de conta 118 pode ser ainda configurado para determinar a função da conta do cliente e a informação de escopo utilizando através da interconexão de rede 112 e uma ou mais APIs do aplicativo do serviço de diretório 110 para recuperar a função da conta do cliente e a informação de escopo associada com um ou mais clientes 102-*a* que solicitam contas JIT com permissões de acesso elevado. De modo alternativo ou adicional, o componente de autorização de conta 118 pode ser ainda configurado para fornecer, através do componente de notificação de conta 122, a função da conta recuperada do cliente e a informação de escopo associada com um ou mais clientes 102-*a* antes de receber a função solicitada e a informação de cliente de um ou mais clientes 102-*a* através de dispositivos do cliente 104-*b*. Isso pode permitir que um ou mais clientes 102-*a* forneça a informação de função e escopo solicitada que está dentro ou compatível com sua informação de função e escopo da conta do cliente.

[0051] Uma vez que a informação de função e escopo da conta do cliente é recuperada do aplicativo do serviço de diretório 110, o componente de autorização de conta 118 pode automaticamente autorizar a solicitação por permissões de acesso elevado com base pelo menos parcialmente em se a função solicitada e o escopo estão dentro ou compatível com a função da conta do cliente e escopo associado com os clientes 102-*a* que solicitam as contas JIT. Se a função solicitada e escopo por um cliente for equivalente ou estiver dentro de uma função

da conta do cliente e escopo associado com o cliente, então o componente de autorização de conta 118 pode ser configurado para autorizar a solicitação por uma conta JIT tendo permissões elevadas de acesso. Caso contrário, o componente de autorização de conta 118 pode rejeitar a solicitação para um JIT tendo permissões de acesso elevado.

[0052] Em modalidade, quando o cliente 102-1 solicita realizar a depuração de aplicativo remoto no dispositivo do servidor 140-1-1, a informação de função e escopo solicitada pode incluir funções para um usuário remoto e um depurador e o escopo pode incluir limite de violação 138-1-1. A informação de função e escopo da conta do cliente associado com a conta do cliente do cliente 102-1 e recuperada do aplicativo do serviço de diretório 110 pode incluir funções para um usuário remoto e um depurador e o escopo pode incluir floresta 132-1. Com base na informação de função e escopo solicitada e informação de função e escopo da conta do cliente, o componente de autorização de conta 118 pode autorizar a solicitação por uma conta JIT por causa da função solicitada pelo cliente 102-1 (por exemplo, usuário remoto e depurador) é equivalente à função da conta do cliente (por exemplo, usuário remoto e depurador) e o escopo solicitado pelo cliente (por exemplo, limite de violação 138-1-1) está dentro do escopo da conta do cliente (por exemplo, floresta 132-1).

[0053] Em outra ilustração, a informação de função e escopo solicitada pode ser determinada para incluir funções para um usuário remoto e um depurador e o escopo pode incluir limite de violação 138-1-1. A informação de função e escopo da conta do cliente do cliente 102-1 recuperada do aplicativo do serviço de diretório 110 pode incluir funções para depurador, mas não usuário remoto e o escopo pode incluir floresta 132-2 (não mostrado). O componente de autorização de conta 118 pode rejeitar a solicitação, porque a função solicitada pelo cliente 102-1 (por exemplo, usuário remoto e depurador) não é equivalente à

ou dentro da função da conta do cliente (por exemplo, depurador, mas não incluindo usuário remoto) e o escopo solicitado pelo cliente (por exemplo, limite de violação 138-1-1) também não está dentro do escopo da conta do cliente (por exemplo, floresta 132-2).

[0054] De modo alternativo ou adicional, para garantir segurança e privacidade dos sistemas SaaS, a informação de função e escopo da conta do cliente pode ser ainda limitada a fim de restringir a informação de função e escopo solicitada, limitando o número e o tipo de funções solicitadas e o escopo que um cliente pode solicitar. Assim, em algumas modalidades, a informação de função e escopo da conta do cliente pode ainda limitar o número de funções solicitadas em uma única função e os tipos de funções em uma coleção específica de funções (por exemplo, usuário remoto, depuração e/ou teste), e o escopo em um único limite de violação, de modo que qualquer função solicitada e escopo recebido de um cliente que não se encaixa dentro daquelas restrições serão rejeitados pelo componente de autorização118. Consequentemente, qualquer conta JIT fornecida pelo componente de fornecimento de conta 120 ainda será limitada em sua função e escopo.

[0055] Em modalidade, a informação de função e escopo solicitada pode ser determinada para incluir funções para um usuário remoto e um depurador e o escopo pode incluir limite de violação 138-1-1. A informação de função e escopo da conta do cliente associado com o cliente 102-1 pode incluir funções para um usuário remoto e um depurador, entretanto, a informação de função e escopo da conta do cliente pode ainda limitar a função a uma única função (por exemplo, um usuário remoto ou depurador, mas não ambos) e o escopo pode ser limitado a um único limite de violação. O componente de autorização de conta 118 pode rejeitar a solicitação, pois a função solicitada pelo cliente 102-1 (por exemplo, ambos o usuário remoto e o depurador) não

está dentro da única restrição de função (por exemplo, usuário remoto ou depurador, mas não ambos).

[0056] Pelo menos uma vantagem técnica percebida por ainda limitar a função da conta do cliente e escopo é que cada conta JIT autorizada e posteriormente fornecida pelo componente de fornecimento de conta 120 será com função e escopo limitados a fim de garantir que cada conta JIT seja fornecia com permissões minimamente abrangidas necessárias para realizar uma tarefa ou serviço conforme solicitado pelo cliente. Assim, embora a superfície de invasão ou vetor de invasão possa aumentar com o aumento no número de contas JIT, o efeito é mitigado, pois cada conta JIT fornecida será limitada na função e no escopo.

[0057] De modo alternativo ou adicional, para ainda garantir segurança e privacidade dos sistemas SaaS, o componente de autorização de conta 118 pode ser ainda configurado para determinar um supervisor ou gestor de um ou mais clientes 102-*a* que solicitam permissões de acesso elevado utilizando através de interconexão de rede 112 e uma ou mais APIs do aplicativo do serviço de diretório 110 para identificar o supervisor ou o gestor de um ou mais clientes 102-*a* com base na informação de hierarquia organizacional acessível pelo aplicativo do serviço de diretório 110. Uma vez que o supervisor ou o gestor de um ou mais clientes 102-*a* é determinado, o componente de autorização de conta 118 pode ser configurado para notificar e fornecer o supervisor ou o gestor através da informação de aprovação de supervisão do componente de notificação de conta 122. A informação de aprovação da supervisão pode incluir informação da conta solicitada de função e escopo, informação de vida útil solicitada e informação de função e escopo da conta do cliente para um ou mais clientes 102-*a* que solicitam contas JIT. O componente de autorização de conta 118 também pode ser configurado para solicitar e receber aprovação do

supervisor ou gestor de um ou mais clientes 102-*a* antes de autorizar a solicitação.

[0058] Em modalidade, antes de autorizar ou solicitar uma conta JIT para elevar permissões de acesso para o cliente 102-1, mas após determinar a informação de função e escopo solicitada e informação de função e escopo da conta do cliente, o componente de autorização de conta 118 pode determinar que o supervisor ou o gestor é cliente 102-2 e pode notificar e fornecer ao cliente 102-2 a informação de função e escopo solicitada e a informação de função e escopo da conta do cliente do cliente 102-1 através do componente de notificação de conta 122. O componente de autorização de conta 118 pode ainda solicitar e receber aprovação do cliente 102-2 antes de autorizar ou solicitar.

[0059] Em várias modalidades, o aplicativo de gerenciamento de administração 114 pode ainda compreender um componente de fornecimento de conta 120 de forma comunicável acoplado a um armazenamento de dados de contas JIT 126. O armazenamento de dados de conta JIT 126 pode ser geralmente disposto para armazenar informação da conta JIT associada com uma ou mais contas JIT. O componente de fornecimento de conta 120 pode geralmente ser disposto para fornecer uma conta JIT após a solicitação por uma conta JIT ter sido autorizada. O componente de fornecimento de conta 120 pode ser ainda disposto para determinar se uma conta JIT tendo mesma ou função solicitada e escopo substancialmente similar já existe para um cliente. O componente de fornecimento de conta 120 pode ser disposto para recuperar uma conta JIT existente associada com o cliente quando a conta JIT tendo mesma ou função solicitada e escopo substancialmente similar já existir para o cliente. De modo alternativo, quando a conta JIT tendo mesma ou função solicitada e escopo substancialmente similar ainda não existe para o cliente, o componente de

fornecimento de conta 120 pode ser geralmente disposto para criar uma nova conta JIT. Após criar e/ou recuperar a conta JIT, o componente de fornecimento de conta 120 pode ser ainda disposto para permitir a conta JIT.

[0060] Em uma modalidade, o componente de fornecimento de conta 120 pode ser configurado para determinar se uma conta JIT tendo uma função e escopo que é equivalente ou substancialmente similar à função e escopo solicitados por um cliente já existir no armazenamento de dados de contas JIT 126 para esse cliente. O componente de fornecimento de conta 120 pode determinar a existência de uma conta JIT previamente criada buscando e/ou analisando o armazenamento de dados de contas JIT 126 e comparando e combinando a informação de função e escopo solicitada com a função da conta JIT e a informação de escopo das contas JIT existentes. Quando o componente de fornecimento de conta 120 determina que uma conta JIT tendo a função e escopo solicitados já existe para esse cliente, então o componente de fornecimento de conta 120 pode ser configurado para recuperar a informação da conta JIT associada com a conta JIT previamente criada do armazenamento de dados de conta JIT 126 para esse cliente.

[0061] De modo alternativo, quando o componente de fornecimento de conta 120 determina que uma conta JIT tendo a função e escopo solicitados não existe para esse cliente, o componente de fornecimento de conta 120 pode ser configurado para automaticamente criar uma nova conta JIT para esse cliente. Isso é, caso contrário, conhecido como provisionamento preguiçoso de uma conta JIT, onde o componente de fornecimento de conta 120 pode ser configurado para criar contas JIT apenas quando uma conta JIT prévia com função e escopo equivalentes ou substancialmente similares já não existe para o cliente.

[0062] Em uma modalidade, o componente de fornecimento de conta 120 pode criar a nova conta JIT e sua informação da conta JIT associada com base pelo menos parcialmente na informação de solicitação de conta JIT (por exemplo, a informação de função e escopo solicitada, informação de vida útil solicitada, etc.), e a informação da conta do cliente. Por exemplo, assume-se que a informação da conta do cliente para o cliente 102-1 pode compreender UPN "EllenAdams@domain-136.contoso.com" e que as funções solicitadas incluem um usuário remoto e um depurador e o escopo solicitado inclui limite de violação 138-1-1. O componente de fornecimento de conta 120 pode criar a nova conta JIT com informação da conta JIT compreendendo o UPN "EllenAdams_RemoteDebugger_Boundaryl38-l-l@domain136-1.contoso.com" de modo que o cliente 102-1 possa identificar uma ou mais funções e escopo para a conta JIT com base pelo menos parcialmente no UPN. Adicionalmente, o componente de fornecimento de conta 120 também pode armazenar a conta JIT recentemente criada no armazenamento de dados de contas JIT 126 e associar a conta JIT recentemente criada com a conta do cliente para esse cliente.

[0063] Para garantir que os recursos e/ou ativos gerenciados por um ou mais dispositivos do servidor de serviço de diretório 130-*l* sejam acessíveis e/ou operáveis por um ou mais clientes 102-*a* utilizando as contas JIT criadas recentemente, o componente de fornecimento de conta 120 pode ser ainda configurado para identificar o dispositivo do servidor de serviço do diretório apropriado que gerencia um ou mais limites de violação 138-*g*-*h* que incluem um ou mais recursos e/ou ativos que o cliente solicitou para acessar e/ou operar. Uma vez que o dispositivo do servidor de serviço do diretório apropriado é identificado, o componente de fornecimento de conta 120 pode ser ainda configurado para se comunicar com o dispositivo do servidor de serviço do

diretório identificado através da interconexão de rede 112 e uma ou mais APIs do dispositivo do servidor de serviço do diretório identificado a fim de criar a conta JIT. Adicionalmente, o componente de fornecimento de conta 120 pode ser configurado para armazenar a conta JIT recentemente criada e a informação da conta JIT associada no armazenamento de dados de contas JIT 126 e associar a conta JIT recentemente criada e a informação da conta JIT associada com a conta do cliente de modo que possa ser recuperada e reutilizada.

[0064] Em modalidade, assume-se que as funções solicitadas para o cliente 102-1 incluem um usuário remoto e um depurador, o escopo solicitado inclui limite de violação 138-1-1 e a solicitação foi autorizada pelo componente de autorização de conta 118, o componente de fornecimento de conta 120 pode primeiro determinar se uma conta JIT tendo as funções de um usuário remoto e um depurador e escopo que inclui limite de violação 138-1-1 foi previamente criada. Quando uma conta JIT previamente criada foi encontrada no armazenamento de dados de contas JIT 126 e sua informação da conta JIT associada inclui funções para um usuário remoto e um depurador e o escopo inclui limite de violação 138-1-1, então o componente de fornecimento de conta 120 pode recuperar a informação da conta JIT previamente criada e/ou armazenada associada com a conta JIT.

[0065] Continuando com a ilustração acima, quando nenhuma conta JIT associada com o cliente 102-1 foi encontrada no armazenamento de dados de conta JIT 126, o componente de fornecimento de conta 120 pode identificar o dispositivo do servidor de serviço do diretório 130-*I* para a criação de uma nova conta JIT, pois o escopo solicitado inclui limite de violação 138-1-1 que é gerenciado pelo dispositivo do servidor de serviço do diretório 130-*I*. O componente de fornecimento de conta 120 pode então se comunicar com o dispositivo do servidor de serviço do diretório 130-*I* para criar a nova conta JIT. O

componente de fornecimento de conta 120 pode ainda armazenar a conta JIT recentemente criada e a informação da conta JIT associada no armazenamento de dados de contas JIT 126 para recuperação e reutilização.

[0066] Uma vez que uma conta JIT é recuperada ou criada, o componente de fornecimento de conta 120 pode ser ainda configurado para permitir que a conta JIT com base pelo menos parcialmente na informação de função e escopo solicitada, de modo que a conta JIT recuperada ou criada tenha a mesma função e escopo conforme solicitado pelo cliente. Isso também garante que cada conta JIT que é criada ou recuperada compreenda um conjunto de permissões de acesso elevado minimamente abrangidas necessárias para acessar ou realizar um serviço em um recurso e/ou ativo conforme solicitado pelo cliente. Para habilitar a conta JIT, o componente de fornecimento de conta 120 pode ser ainda configurado para conceder ou fornecer um conjunto de permissões de acesso à conta JIT com base pelo menos parcialmente na informação de função e escopo solicitada.

[0067] Em várias modalidades, o aplicativo de gerenciamento de administração 114 pode ainda compreender o componente de notificação de conta 122. O componente de notificação de conta 122 pode geralmente ser disposto para notificar e fornecer a um ou mais clientes 102-*a* através de um ou mais dispositivos do cliente 104-*b*, a informação da conta do cliente (por exemplo, função da conta do cliente e escopo), informação de aprovação da solicitação (por exemplo, se a solicitação para elevar permissões de acesso foi aprovada ou rejeitada), a informação de aprovação da supervisão e a informação da conta JIT em uma ou mais mensagens de notificação. Mensagens de notificação exemplares podem incluir, mas não se limitam à, mensagem SMS móvel, chamadas de voz automatizadas, e-mail, formulários com base na web interativos, alertas da web, aplicativos de mensagem com base na

internet e/ou intranet, ou qualquer outro meio para notificar um ou mais clientes 102-*a* referentes à aprovação e/ou rejeição de permissões de acesso elevado e fornecer um ou mais clientes 102-*a* com informação de aprovação da solicitação, informação de aprovação da supervisão, e/ou informação da conta JIT.

[0068] Em uma modalidade, após a solicitação para elevar permissões de acesso ter sido rejeitada, o componente de notificação de conta 122 pode ser configurado para notificar o cliente (por exemplo, cliente 102-1) através de um ou mais aplicativos e/ou componentes de um ou mais dispositivos do cliente 104-b em uma ou mais mensagens de notificação que a solicitação foi rejeitada. Adicionalmente, uma ou mais mensagens de notificação também podem incluir informação de rejeição da conta JIT que pode indicar uma ou mais razões para a rejeição (por exemplo, a solicitação excede a função e/ou o escopo da conta do cliente).

[0069] Após uma solicitação por uma conta JIT com permissões de acesso elevado ter sido aprovada e a conta JIT ter sido fornecida, o componente de notificação de conta 122 pode ser configurado para notificar o cliente (por exemplo, o cliente 102-1) através de um dispositivo do cliente (por exemplo, dispositivo do cliente 104-1) em uma ou mais mensagens de notificação que a solicitação foi aprovada. O componente de notificação de conta 122 também pode ser configurado para fornecer informação da conta JIT associada com a conta JIT fornecida tendo permissões de acesso elevado suficientes para permitir que um cliente (por exemplo, dispositivo do cliente 104-1) acesse e/ou opere um ou mais recursos e/ou ativos (por exemplo, dispositivo do servidor 104-1-1) compatíveis com a função e o escopo da conta JIT.

[0070] Em outra modalidade, antes de autorizar uma solicitação para uma conta JIT com permissões de acesso elevado para um cliente (por exemplo, cliente 102-1) e após determinar a informação de fun-

ção e escopo solicitada e a informação de função e escopo da conta do cliente para esse cliente, o componente de notificação de conta 122 pode ser ainda configurado para solicitar aprovação de um supervisor ou gestor (por exemplo, cliente 102-2) desse cliente (por exemplo, cliente 102-1) através de uma ou mais mensagens de notificação antes de autorizar uma solicitação por uma conta JIT com permissões de acesso elevado. Para ainda auxiliar o supervisor ou gestor (por exemplo, cliente 102-2) na aprovação ou rejeição de uma ou mais solicitações, o componente de notificação de conta 122 pode ser ainda configurado para fornecer a informação de aprovação da supervisão (por exemplo, informação da conta solicitada de função e escopo, informação de vida útil solicitada e informação de função e escopo da conta do cliente associado com cliente 102-1 que solicitam as permissões de acesso elevado) em uma ou mais mensagens de notificação ao supervisor ou gestor (por exemplo, cliente 102-2).

[0071] Embora o sistema de fornecimento de conta JIT 100 mostrado na figura 1 tenha um número de elementos limitado em uma certa topologia, pode ser observado que o sistema de fornecimento de conta JIT 100 pode incluir mais ou menos elementos em topologias alternadas conforme desejado para uma dada implementação. De modo similar, enquanto várias modalidades podem ilustrar o ambiente computacional empresarial 150 abrangendo um ou mais dispositivos do cliente 104-*b*, o dispositivo do servidor 108, o dispositivo do servidor 106 e uma ou mais florestas 132-*k*, pode ser observado que pelo menos alguns dos clientes e/ou dispositivos do servidor podem ser externos ao ambiente computacional empresarial 150 para uma dada implementação.

[0072] A figura 2 ilustra outra modalidade para o sistema de fornecimento de conta JIT 100. Em várias modalidades do sistema de fornecimento de conta JIT 100 pode ainda compreender o dispositivo do

servidor 202 que pode ser geralmente disposto para executar, entre outros aplicativos, o aplicativo de gerenciamento de recurso e ativo 204. Os dispositivos do servidor de serviço de diretório 130-*l* podem ser ainda dispostos para implementar um ou mais limites de segurança 138-*g*-*h* que utilizam um ou mais grupos de segurança associados, onde cada grupo de segurança pode ser disposto para gerenciar um conjunto de permissões de acesso de um ou mais recursos e/ou ativos para um ou mais membros de cada grupo de segurança.

[0073] O aplicativo de gerenciamento de ativo 204 pode ser geralmente disposto para configurar ou separar um ou mais recursos e/ou ativos em um ou mais grupo de seguranças através da interconexão de rede 112 e uma ou mais APIs dos aplicativos de serviço do diretório (não mostrados) de um ou mais dispositivos do servidor de serviço de diretório 130-*l*. Em uma modalidade, o aplicativo de gerenciamento de ativo 204 pode ser configurado para implementar um ou mais limites de segurança 138-*g*-*h* criando um ou mais grupos de segurança do limite de violação 210-*m*-*n*. Para ainda conter movimento lateral de um invasor que ganhou acesso a uma conta JIT comprometida, em algumas modalidades, o aplicativo de gerenciamento de ativo 204 pode ser ainda disposto para configurar ou separar um ou mais recursos e/ou ativos em um ou mais grupos de segurança do limite de violação 210-*m*-*n* mutualmente exclusivos ou não sobrepostos de modo que nenhum recurso e/ou ativo única seja acessível ou operável a partir das contas JIT sendo membros de dois diferentes grupos de segurança do limite de violação.

[0074] Em outra modalidade, o aplicativo de gerenciamento de ativo 204 pode ser ainda configurado para atribuir cada grupo de segurança de limite de violação de um ou mais grupos de segurança do limite de violação 210-*m*-*n* um conjunto de permissões de acesso a um ou mais recursos e/ou ativos, de modo que qualquer membro (por

exemplo, uma ou mais contas JIT) adicionado a um grupo de segurança de limite de violação possa acessar um ou mais recursos e/ou ativos gerenciados por esse grupo de segurança de acordo com o conjunto de permissões de acesso. De modo alternativo ou adicional, nas implementações onde um ou mais recursos e/ou ativos compreendem dispositivos virtuais (por exemplo, dispositivos do servidor virtuais implementados utilizando uma ou mais máquinas virtuais), o aplicativo de gerenciamento de ativo 204 pode ser ainda configurado para fornecer ou implantar um ou mais recursos e/ou ativos de modo que cada recurso e/ou ativo fornecido esteja associado com um grupo de segurança de limite de violação.

[0075] Em modalidade, o aplicativo de gerenciamento de ativo 204 pode implementar limites de segurança 138-1-1 e 138-1-2 criando grupos de segurança do limite de violação associados 210-1-1 e 210-1-2, respectivamente, utilizando interconexão de rede 112 e uma ou mais APIs do aplicativo do serviço de diretório (não mostrado) do dispositivo do servidor de serviço do diretório 130-*I*. Adicionalmente, o aplicativo de gerenciamento de ativo 204 também pode configurar os dispositivos do servidor 140-1-1, 140-1-2, 140-1-3 a serem gerenciados pelo grupo de segurança de limite de violação 138-1-1 e dispositivos do servidor 140-1-4, 140-1-5, 140-1-6 a serem gerenciados pelo grupo de segurança 138-1-2.

[0076] Continuando com a ilustração acima, o aplicativo de gerenciamento de ativo 204 pode ainda configurar o grupo de segurança de limite de violação 210-1-1 para conceder ou fornecer um conjunto de permissões de acesso aos dispositivos do servidor 140-1-1, 140-1-2, 140-1-3. O conjunto de permissões de acesso pode permitir que uma conta JIT acesse de acordo com o conjunto de permissões de acesso associado com o grupo de segurança 210-1-1, os dispositivos do servidor 140-1-1, 140-1-2, 140-1-3, quando a conta JIT é adicionada ao

grupo de segurança de limite de violação 210-1-1.

[0077] Ainda continuando com a ilustração acima, o aplicativo de gerenciamento de ativo 204 também pode configurar o grupo de segurança de limite de violação 210-1-2 em uma forma similar conforme discutido com relação ao grupo de segurança do limite de violação 210-1-1, de modo que uma conta JIT que é um membro do grupo de segurança de limite de violação 210-1-2 possa acessar, de acordo com um conjunto de permissões de acesso associado com o grupo de segurança de limite de violação 210-1-2, os dispositivos do servidor 140-1-4, 140-1-5, 140-1-6. Nas implementações onde os dispositivos do servidor 140-1-1 a 140-1-6 são dispositivos do servidor virtuais implementados utilizando uma ou mais máquinas virtuais que residem nos dispositivos do servidor 140-*i-j*, o aplicativo de gerenciamento de ativo 204 pode automaticamente configurar os dispositivos do servidor virtuais durante o processo de provisionamento (por exemplo, criação e/ou implantação) dos dispositivos do servidor virtuais.

[0078] Pode ser observado que enquanto apenas dois grupos de segurança do limite de violação 210-1-1 e 210-1-2 são ilustrados em várias modalidades, o aplicativo de gerenciamento de ativo 204 pode ser configurado para criar uma pluralidade de grupos (por exemplo, grupo de acesso remoto, grupo do depurador, etc.) para uma ou mais funções, onde cada grupo pode ser associado com o conjunto de permissões de acesso (por exemplo, acesso remoto a um ou mais recursos e/ou ativos, depuração de um ou mais recursos e/ou ativos, etc.) associado com as funções, de modo que uma conta JIT possa ser um membro de múltiplos grupos em uma forma agrupada para atingir o Controle de Acesso com Base na Função (RBAC). As modalidades não são limitadas nesse contexto.

[0079] Para garantir que um conjunto de permissões de acesso adequado seja concedido ou fornecido a uma conta JIT fornecida, o

componente de fornecimento de conta 120 do aplicativo de gerenciamento de administração 114 pode ser ainda configurado para identificar um dispositivo do servidor de serviço do diretório implementando os grupos de segurança do limite de violação apropriados 210-*m*-*n* e identificar um ou mais grupos de segurança do limite de violação 210-*m*-*n* configurados para conceder acesso a um ou mais recursos e/ou ativos utilizando interconexão de rede 112 e uma ou mais APIs dos aplicativos de serviço do diretório (não mostrados) de um ou mais dispositivos do servidor de serviço de diretório 130-*I*. Uma vez que o dispositivo do servidor de serviço do diretório apropriado e um ou mais grupos de segurança do limite de violação 210-*m*-*n* foram identificados, o componente de fornecimento de conta 120 pode ser configurado para associar a conta JIT fornecida com o grupo de segurança de limite de violação identificado.

[0080] Em uma modalidade, o componente de fornecimento de conta 120 pode associar a conta JIT com grupos de segurança do limite de violação 210-*m*-*n* adicionando a conta JIT a um ou mais grupos de segurança do limite de violação 210-*m*-*n* como membros de modo que a conta JIT possa receber um conjunto de permissões de acesso para acessar um ou mais recursos e/ou ativos dentro de um limite de violação associado com o grupo de segurança de limite de violação. Em algumas modalidades, o componente de fornecimento de conta 120 pode ser ainda configurado para limitar o número de grupos de segurança do limite de violação 210-*m*-*n* ao qual uma conta JIT pode ser associada (por exemplo, cada conta JIT pode apenas ser associada com um único grupo de segurança de limite de violação) a fim de ainda limitar o escopo de impacto que um invasor pode causar utilizando uma conta JIT comprometida.

[0081] Em modalidade, assume-se que a informação de função e escopo solicitada recebida do cliente 102-1 para uma conta JIT com

permissões de acesso elevado inclui um usuário remoto e depurador para limite de violação 138-1-1 e a conta JIT ser fornecida, o componente de fornecimento de conta 120 pode primeiro identificar o dispositivo do servidor de serviço do diretório 130-*l* entre um ou mais dispositivos do servidor de serviço de diretório 130-*l* que está implementando o limite de violação 138-1-1 utilizando o grupo de segurança de limite de violação 210-1-1. O componente de fornecimento de conta 120 também pode identificar o grupo de segurança de limite de violação 210-1-1 como o grupo de segurança de limite de violação configurado para conceder um conjunto de permissões de acesso aos dispositivos do servidor 140-1-1, 140-1-2, 140-1-3. O componente de fornecimento de conta 120 pode ainda associar adicionando a conta JIT fornecida pelo menos ao grupo de segurança de limite de violação 210-1-1 identificado a fim de conceder à conta JIT fornecida um conjunto de permissões de acesso aos dispositivos do servidor 140-1-1, 140-1-2, 140-1-3. Pode ser observado que o componente de fornecimento de conta 120 também pode associar adicionando a conta JIT fornecida a outros grupos (por exemplo, grupo de usuário remoto, grupos de depurador, etc.) a fim de conceder permissões de acesso como usuário remoto e depurador de modo que a conta JIT fornecida possa ser utilizada pelo cliente 102-1 para realizar a depuração remota nos dispositivos do servidor 140-1-1, 140-1-2, 14-1-3.

[0082] Em várias modalidades, o aplicativo de gerenciamento de administração 114 pode ainda compreender o componente de vida útil da conta 124. O componente de vida útil da conta 124 pode ser geralmente disposto para gerenciar a vida útil associada com cada conta JIT com base na informação de vida útil da conta JIT ou uma informação de vida útil da conta JIT predefinida. O componente de vida útil da conta 124 pode ser ainda disposto para desativar e/ou remover uma ou mais contas JIT após um período de tempo decorrer. A informação

de vida útil da conta JIT pode incluir, mas não se limita a, um período específico ou tempo decorrido de quando a conta JIT expira e fica desabilitada e um tempo específico ou tempo decorrido de quando a conta JIT é removida.

[0083] Pode ser observado que em algumas modalidades, a informação de vida útil da conta JIT pode ser determinada e/ou derivada com base na informação de solicitação de conta JIT recebida de um ou mais clientes 102-*a* através dos dispositivos do cliente 104-*b* para uma dada implementação. Em outras modalidades, a informação de vida útil da conta JIT pode ser determinada e/ou derivada com base em uma ou mais funções conforme indicado pela função da conta JIT e informação de escopo, onde algumas funções (por exemplo, um usuário remoto e um depurador) podem ter uma vida útil da conta JIT associada de 2 horas enquanto outras funções (por exemplo, um operador de backup) pode ter uma vida útil associada de 4 horas. As modalidades não são limitadas nesse contexto.

[0084] Em uma modalidade, o componente de vida útil da conta 124 pode ser ainda configurado para receber uma ou mais solicitações de aprovação de acesso de um ou mais dispositivos do servidor de serviço de diretório 130-*l* através da interconexão de rede 112, quando um ou mais clientes 102-*a* acessam um ou mais recursos e/ou ativos gerenciados por um ou mais dispositivos do servidor de serviço de diretório 130-*l*. O componente de vida útil da conta 124 pode ser ainda configurado para automaticamente aprovar ou permitir que um ou mais clientes 102-*a* acessem um ou mais recursos e/ou ativos gerenciados pelos respectivos dispositivos do servidor de serviço de diretório 130-*l*, quando a vida útil da conta JIT não expirou.

[0085] De modo alternativo, o componente de vida útil da conta 124 pode ser configurado para automaticamente negar um ou mais clientes 102-*a* qualquer acesso a um ou mais recursos e/ou ativos ge-

renciados pelos respectivos dispositivos do servidor de serviço de diretório 130-*l*, quando a vida útil da conta JIT expirou. Adicionalmente, em uma modalidade, o componente de vida útil da conta 124 também pode ser configurado para desativar a conta JIT e/ou dissociar a conta JIT de um ou mais grupos de segurança do limite de violação. Por exemplo, o componente de vida útil da conta 124 pode desabilitar a conta JIT negando quaisquer solicitações de aprovação de acesso e gerar um novo token de autenticação sem fornecer o token de autenticação recentemente gerado aos clientes 102-*a*. O componente de vida útil da conta também pode dissociar a conta JIT removendo a conta JIT da sociedade em um ou mais grupos de segurança do limite de violação.

[0086] Em uma modalidade exemplar, a vida útil da conta JIT pode começar do tempo quando a conta JIT é fornecida (por exemplo, fornecida pelo componente de fornecimento de conta 120) e termina no tempo especificado ou tempo decorrido com base na informação de vida útil da conta JIT. De modo alternativo, a vida útil da conta JIT pode começar do período quando a conta JIT é primeiro utilizada (por exemplo, um cliente tenta acessar um recurso e/ou ativo) e termina no tempo especificado ou tempo decorrido com base na informação de vida útil da conta JIT. As modalidades exemplares não são limitadas nesse contexto.

[0087] De modo alternativo ou adicional, o componente de vida útil da conta 124 pode ser ainda configurado para periodicamente digitalizar o armazenamento de dados de contas JIT 124 para quaisquer contas JIT ativadas e desativar quaisquer contas JIT com vidas úteis que expiraram com base na informação de vida útil da conta JIT. Em algumas modalidades, uma conta JIT que é desativada também terminará imediatamente (por exemplo, um desligamento forçado) quaisquer contas JIT atualmente em uso e suas ações ou tarefas ativas associa-

das. Para garantir que um ou mais dispositivos do servidor do diretório 130-*I* que gerenciam um ou mais recursos e/ou ativos são corretamente sincronizados com o armazenamento de dados de contas JIT 126, o componente de vida útil da conta 124 pode ser ainda configurado para se comunicar através da interconexão de rede 112 e uma ou mais APIs do aplicativo do serviço de diretório 110 para atualizar a informação de vida útil da conta JIT das contas JIT e/ou desabilitar quaisquer contas JIT com vidas úteis expiradas.

[0088] De modo alternativo ou adicional, o componente de vida útil da conta 124 pode ser ainda configurado para periodicamente digitalizar o armazenamento de dados de contas JIT 124 para quaisquer contas JIT desabilitadas e remover quaisquer contas JIT desabilitadas que não foram utilizadas por um período de tempo predefinido (por exemplo, contas JIT inativas) com base na informação de vida útil da conta JIT. Para garantir que um ou mais dispositivos do servidor do diretório 130-*I* que gerenciam um ou mais recursos e/ou ativos sejam corretamente sincronizados, o componente de vida útil da conta 124 pode ser ainda configurado para remover essas contas JIT desabilitadas comunicando-se através da interconexão de rede 112 e uma ou mais APIs de um ou mais aplicativos de serviço do diretório (não mostrados) de um ou mais dispositivos do servidor do diretório 130-*I*.

[0089] Em modalidade, assume-se que o cliente 102-1 solicitou uma conta JIT com permissões de acesso elevado como um usuário remoto e um depurador para limite de violação 138-1-1 de modo que a informação de solicitação de conta JIT compreenda uma informação de vida útil solicitada indicando que a vida útil solicitada para uma conta JIT é de 4 horas. Ainda se assume que uma conta JIT foi fornecida ao meio-dia ao cliente 102-1 tendo uma informação de vida útil da conta JIT indicando que a conta JIT fornecida vida útil é de 4 horas e a vida útil para a conta JIT fornecida começa do momento quando a con-

ta JIT é fornecida, que é meio-dia, de modo que a vida útil da conta JIT termina às 16:00. Em uma modalidade exemplar, o componente de vida útil da conta 124 pode conceder solicitação de aprovação de acesso do dispositivo do servidor de serviço do diretório 130-*l*, quando o cliente 102-1 tenta acessar remotamente o dispositivo do servidor 140-1-1 (por exemplo, utilizando Protocolo da Área de Trabalho Remota (RDP, *Remote Desktop Protocol*)) utilizando a conta JIT fornecida através do dispositivo do cliente 104-1 e interconexão de rede 112 antes das 16:00.

[0090] Continuando com o exemplo acima, em outra modalidade exemplar, o componente de vida útil da conta 124 pode rejeitar uma solicitação de aprovação de acesso do dispositivo do servidor de serviço do diretório 130-*l*, quando o cliente 102-1 tenta acessar remotamente o dispositivo do servidor 140-1-1 (por exemplo, utilizando o Protocolo da Área de Trabalho Remota (RDP, *Remote Desktop Protocol*)) utilizando a conta JIT fornecida após às 16:00. O componente de vida útil da conta 124 também pode automaticamente negar qualquer acesso ao dispositivo do servidor 140-1-1 e desativar a conta JIT fornecida após às 16:00. Adicionalmente, o componente de vida útil da conta 124 pode dissociar a conta JIT fornecida do grupo de segurança de limite de violação 210-1-1 removendo a sociedade da conta JIT fornecida do grupo de segurança de limite de violação 210-1-1. Ainda, o componente de vida útil da conta 124 também pode automaticamente digitalizar, determinar e remover a conta JIT desabilitada como uma conta JIT inativa quando a conta JIT desabilitada não tem sido utilizada pelo cliente 102-1 após um período contínuo (por exemplo, um dia, uma semana, um mês, um ano, etc.) de inatividade (por exemplo, sem login).

[0091] Pelo menos uma vantagem técnica que pode ser percebida através da associação de cada conta JIT com uma vida útil é que um

invasor será limitado ao ganho de acesso a qualquer conta JIT apenas quando a conta JIT ainda estiver habilitada. Adicionalmente, mesmo quando uma conta JIT está comprometida durante o período quando a conta JIT ainda está habilitada, a capacidade de um invasor prejudicar será o tempo limitado com base pelo menos parcialmente na vida útil associada com a conta JIT comprometida. Outra vantagem técnica que pode ser percebida é a redução da efetividade associada com uma "passagem do ataque hash", pois um invasor que ganha acesso a um ou mais tokens de autenticação para as contas JIT (por exemplo, senhas com hash e/ou sal para a conta JIT) devem ainda encontrar uma conta JIT que está atualmente habilitada. Ainda outra vantagem técnica que pode ser percebida é a redução da superfície de ataque ou vetor de ataque pela remoção de uma ou mais contas JIT inativas. Ainda outra vantagem técnica que pode ser percebida é que qualquer aumento na superfície de ataque ou vetor de ataque associado com o aumento no número de contas JIT fornecidas pode ser mitigado, quando as contas JIT são fornecidas com vida útil limitada (por exemplo, restrita a 4 horas), função limitada (por exemplo, restrita a uma única função), tipo de função limitada (por exemplo, restrito ao depurador) e escopo limitado (por exemplo, restrito a um único limite de violação). Adicionalmente, quando a vida útil limitada, a função limitada, o tipo de função limitada e o escopo limitado são combinados com os limites de violação que estão dispostos para serem mutualmente exclusivos ou não sobrepostos, qualquer movimento lateral (por exemplo, movimento entre limites de violação) por um invasor tendo acesso a uma conta JIT comprometida será muito restrito ou ainda ficará impossível.

[0092] A figura 3 ilustra outra modalidade para o sistema de fornecimento de conta JIT 100. Em várias modalidades do sistema de fornecimento de conta JIT 100 pode ainda compreender dispositivos do

servidor 302 e 306 que podem ser geralmente dispostos para executar, entre outros aplicativos, o aplicativo de identidade federada 304 e aplicativo de gerenciamento de token de autenticação 308, respectivamente. Adicionalmente, pelo menos um dispositivo do cliente pode ser ainda disposto para armazenar um ou mais tokens de autenticação associado com contas JIT em um armazenamento de dados do token de autenticação 310.

[0093] Em várias modalidades, o aplicativo de identidade federada 304 pode ser geralmente disposto para fornecer autenticação de fatores múltiplos (por exemplo, autenticação de dois fatores utilizando um *smart card*, uma senha/pin, e/ou impressão digital) utilizando um ou mais protocolos de autenticação (por exemplo, protocolo Kerberos). O aplicativo de identidade federada 304 também pode ser geralmente disposto para fornecer serviço de token de segurança e emitir um ou mais tokens de segurança (por exemplo, um token *Security Assertion Markup Language* (SAML)) a um ou mais clientes 102-*a* e/ou reivindicar aplicativos habilitados de modo que um ou mais aplicativos habilitados de reivindicação possam identificar um cliente sem ter que receber e/ou processar diretamente a informação da conta do cliente (por exemplo, nome principal do usuário (UPN), identificador da conta, senha da conta ou derivados hash do mesmo, domínio da conta, certificados do smart card, etc.) associada com um ou mais clientes 102-*a*. Aplicativos de identidade federada exemplares 304 podem incluir, mas não se limitam à, MICROSOFT Active Directory Federation Services (AD FS), MICROSOFT Federation Gateway, ou quaisquer outros provedores de serviço de identidade federada configurados para emitir tokens de segurança compreendendo reivindicações que afiram a identidade de um cliente previamente autenticado.

[0094] Em várias modalidades, o componente de gerenciamento de conta 116 do aplicativo de gerenciamento de administração 114

pode ser ainda configurado para receber tokens de segurança emitidos pelo aplicativo de identidade federada 304 de um ou mais dispositivos do cliente 104-*b* e identificar um ou mais clientes 102-*a* que solicitam permissões de acesso elevado com base nos tokens de segurança recebidos. Os tokens de segurança recebidos também podem compreender a informação da conta do cliente associada com um ou mais clientes 102-*a* e permitir que o componente de autorização de conta 118 determine a informação de função e escopo da conta do cliente para um ou mais clientes 102-*a*.

[0095] Em várias modalidades o aplicativo de gerenciamento de token de autenticação 308 pode ser geralmente disposto para gerenciar tokens de autenticação (por exemplo, senhas) de uma ou mais contas JIT associadas com um cliente. Em uma modalidade, o aplicativo de gerenciamento de token de autenticação 308 pode ser configurado para receber tokens de segurança emitidos pelo aplicativo de identidade federada 304 de um ou mais dispositivos do cliente 104-b e identificar um ou mais clientes 102-*a*.

[0096] Em uma modalidade, o aplicativo de gerenciamento de token de autenticação 308 pode ser ainda configurado para fornecer a um ou mais clientes 102-*a* uma coleção de contas JIT e suas informações da conta JIT associada (por exemplo, informação de vida útil da conta JIT, função da conta JIT e informação de escopo, identificador da conta JIT, etc.) para gerenciamento, em resposta às solicitações de um ou mais clientes 102-*a* para obter uma coleção de contas JIT associadas com um ou mais clientes 102-*a*. O aplicativo de gerenciamento de token de autenticação 308 pode ser ainda configurado para associar um token de autenticação para uma ou mais contas JIT recebidas de um ou mais clientes 102-*a* ou automaticamente gerar e associar um ou mais tokens de autenticação para uma ou mais contas JIT.

[0097] Em outra modalidade, o aplicativo de gerenciamento de to-

ken de autenticação 308 pode ser ainda configurado para armazenar o token de autenticação recebido ou gerado para cada conta JIT no armazenamento de dados de contas JIT 126. O aplicativo de gerenciamento de token de autenticação 308 pode ser configurado para atualizar uma ou mais contas JIT com token de autenticação recebido ou gerado utilizando a interconexão de rede 112 e uma ou mais APIs dos aplicativos de serviço do diretório (não mostrados) dos dispositivos do servidor de serviço de diretório 130-*l* de modo que um ou mais clientes 102-*a* possam ser capazes de acessar um ou mais recursos e/ou ativos gerenciados pelos dispositivos do servidor de serviço de diretório 130-*l*.

[0098] Em outra modalidade, o aplicativo de gerenciamento de token de autenticação 308 também pode fornecer o token de autenticação a um ou mais clientes 102-*a* através da interconexão de rede 112 e dispositivos do cliente 104-*b* através de uma conexão segura (por exemplo, conexão confiada ou criptografada) utilizando um ou mais protocolos de comunicações seguros (por exemplo, *Hypertext Transfer Protocol Secure* (HTTPS)). Pode ser observado que pelo menos alguns dos dispositivos do cliente 104-*b* como, por exemplo, dispositivo do cliente 104-2 podem ser acoplados de forma comunicável a um armazenamento de dados do token de autenticação 310 para seguramente armazenar pelo menos o identificador da conta JIT e seus tokens de autenticação associados em um formato criptografado utilizando um ou mais algoritmos de encriptação (por exemplo, *Twofish symmetric key block cipher*). Assim, em algumas modalidades, o dispositivo do cliente 104-2 pode ser configurado para automaticamente criptografar e armazenar quaisquer tokens de autenticação fornecidos ao cliente 102-2 no armazenamento de dados do token de autenticação 310 e permitir que o cliente 102-2 posteriormente recupere o identificador das contas JIT previamente armazenado e seus tokens de

autenticação associados para acessar um ou mais recursos e/ou ativos.

[0099] Nas implementações onde o token de autenticação para uma conta JIT são *p. 28 senhas puro texto, o aplicativo de gerenciamento de token de autenticação 308 pode ser configurado para gerar uma senha aleatória tendo exigências de complexidade variáveis, como, por exemplo, pelo menos duas classes de caractere diferentes (por exemplo, números, letras e/ou símbolos) acopladas com um comprimento mínimo de caractere (por exemplo, mínimo de 8 caracteres). O aplicativo de gerenciamento de token de autenticação 308 pode ser ainda configurado para hash e/ou sal gerado ou cliente que recebeu senhas puro texto de modo que as senhas puro texto não possam ser recuperadas quando um ou mais dispositivos do servidor de serviço de diretório 130-/ e/ou um ou mais recursos e/ou ativos são comprometidos por um invasor. Entretanto, pode ser observado que embora as senhas puro texto sejam com hash e/ou sal, os clientes 102-*a* podem continuar utilizando as contas JIT para acessar um ou mais recursos e/ou ativos utilizando as senhas puro texto fornecidas aos clientes 102-*a*.

[00100] Para facilitar o cliente ao definir ou gerar tokens de ação autêntica, o componente de notificação 122 do aplicativo de gerenciamento de administração 114 pode ser ainda configurado para fornecer, em uma ou mais mensagens de notificação, uma referência ao aplicativo de gerenciamento de token de autenticação 308 de modo que um ou mais clientes 102-*a* possam acessar o aplicativo de gerenciamento de autenticação 308 para definir e/ou gerar um ou mais tokens de autenticação para uma ou mais contas JIT fornecidas.

[00101] Em forma de ilustração, assume-se que uma conta JIT foi fornecida para o cliente 102-2 para limite de violação 138-1-2, o componente de notificação 122 pode fornecer, entre outras informações,

um identificador da conta JIT associado com a conta JIT fornecida e uma URL para o aplicativo de gerenciamento de token 308 através de e-mail ao cliente 102-2. O cliente 102-2 pode então utilizar um ou mais aplicativos e/ou componentes do dispositivo do cliente 104-2 (por exemplo, um navegador de um dispositivo computacional) para acessar o aplicativo de gerenciamento de token 308 para recuperar uma coleção de contas JIT incluindo a conta JIT fornecida associada com o cliente 102-2. O cliente 102-2 pode ainda definir e/ou gerar uma senha puro texto aleatória para a conta JIT fornecida e subsequentemente armazenar um identificador da conta JIT e a senha puro texto aleatória associada no armazenamento de dados do token de autenticação 310. Para acessar ou operar os dispositivos do servidor 140-1-4, 140-1-5, 140-1-6 utilizando a conta JIT fornecida, o cliente 102-2 através do dispositivo do cliente 104-2 pode então recuperar o identificador da conta JIT e a senha puro texto aleatória associada armazenada no armazenamento de dados do token de autenticação 310 e utilizar o identificador da conta JIT recuperado e a senha puro texto aleatória associada para acessar o dispositivo do servidor 140-1-4.

[00102] Incluído aqui está um conjunto de fluxogramas representativos das metodologias exemplares para realizar os novos aspectos da arquitetura revelada. Enquanto isso, para finalidades de simplicidade de explicação, uma ou mais metodologias aqui mostradas, por exemplo, na forma de um fluxo ou fluxograma, são mostradas e descritas como uma série de ações, deve ser entendido e observado que as metodologias estão limitadas pela ordem das ações, pois algumas ações podem, de acordo com elas, ocorrer em uma ordem diferente e/ou simultaneamente com outras ações diferentes das mostradas e descritas aqui. Por exemplo, os técnicos no assunto entenderão e observarão que uma metodologia poderia de modo alternativo ser representada como uma série de estados ou eventos relacionados, como em um

diagrama de estado. Além disso, nem todas as ações ilustradas em uma metodologia podem ser necessárias para uma nova implementação.

[00103] A figura 4A ilustra uma modalidade de um fluxo lógico 400. O fluxo lógico 400 pode ser representante de algumas ou todas as operações executadas por uma ou mais modalidades descritas aqui.

[00104] Na modalidade ilustrada mostrada na figura 4A, o fluxo lógico 400 pode começar no bloco 402 e pode autenticar um cliente para solicitar uma conta JIT com permissões de acesso elevado no bloco 404. Por exemplo, o componente de gerenciamento de conta 116 pode autenticar o cliente 102-1 tendo uma conta de cliente associada para solicitar uma ou mais contas JIT com permissões de acesso elevado. O componente de gerenciamento de conta 116 também pode permitir que o cliente 102-1 solicite através do dispositivo do cliente 104-1 a conta JIT com permissões de acesso elevado para acessar ou operar o dispositivo do servidor 140-1-1 que exige permissões de acesso mais altas que a conta do cliente.

[00105] O fluxo lógico 400 pode receber solicitação de uma conta JIT com permissões de acesso elevado no bloco 406. Por exemplo, o componente de gerenciamento de conta 116 pode receber uma solicitação do cliente 102-1 tendo uma conta de cliente associada através do dispositivo do cliente 104-1 para uma conta JIT com um conjunto de permissões de acesso elevado para acessar ou operar o dispositivo do servidor 140-1-1.

[00106] O fluxo lógico 400 pode determinar se autoriza a solicitação recebida no bloco 408. Por exemplo, o componente de autorização de conta 118 pode determinar se autorizar uma solicitação por uma conta JIT com base pelo menos parcialmente na informação da conta do cliente associada com a conta do cliente do cliente 102-1 e a informação de solicitação de conta JIT recebida da conta do cliente associado com

cliente 102-1 através do dispositivo do cliente 104-1.

[00107] O fluxo lógico 400 pode fornecer uma conta JIT quando a solicitação está autorizada no bloco 412. Por exemplo, o componente de fornecimento de conta 120 pode fornecer uma conta JIT com permissões de acesso elevado para permitir que o cliente 102-1 acesse o dispositivo do servidor 140-1-1, quando uma solicitação por uma conta JIT foi autorizada pelo componente de autorização de conta 118.

[00108] O fluxo lógico 400 pode fornecer informação da conta JIT ou fornecer informação de rejeição da conta JIT no bloco 414 e terminar no bloco 416. Por exemplo, o componente de notificação de conta 122 pode fornecer informação da conta JIT associada com a conta JIT fornecida tendo permissões de acesso elevado ao cliente 102-1, quando uma solicitação por uma conta JIT foi autorizada. De modo alternativo, quando uma solicitação por uma conta JIT não foi autorizada pelo componente de autorização de conta 118, o componente de notificação de conta 122 pode fornecer informação de rejeição da conta JIT ao cliente 102-1 através do dispositivo do cliente 104-1, onde a informação de rejeição da conta JIT pode indicar uma ou mais razões para a rejeição. As modalidades não são limitadas a esses exemplos.

[00109] A figura 4B ilustra uma modalidade de um fluxo lógico 420 e em particular, bloco 408 da figura 4A. O fluxo lógico 420 pode ser representante de algumas ou todas as operações executadas por uma ou mais modalidades aqui descritas.

[00110] Na modalidade ilustrada mostrada na figura 4B, o fluxo lógico 420 pode começar no bloco 422 e pode determinar função e escopo associados com solicitação no bloco 424. Por exemplo, o componente de autorização de conta 118 pode determinar as funções (por exemplo, um usuário remoto e um depurador) e escopo (limite de violação 138-1-1) associado com uma solicitação por uma conta JIT com base pelo menos parcialmente na informação de solicitação de conta

JIT recebida do cliente 102-1 através do dispositivo do cliente 104-1.

[00111] O fluxo lógico 420 pode determinar função e escopo associados com a conta do cliente no bloco 426. Por exemplo, o componente de autorização de conta 118 pode determinar as funções (por exemplo, usuário remoto e depurador) e escopo (floresta 132-1) associadas com a conta do cliente do cliente 102-1 com base pelo menos parcialmente na informação da conta do cliente associada com o cliente 102-1. O componente de autorização de conta 1 18 pode receber a informação da conta do cliente para o cliente 102-1 do aplicativo do serviço de diretório 110 e/ou de um token de segurança fornecido pelo cliente 102-1 através do dispositivo do cliente 104-1.

[00112] O fluxo lógico 420 pode determinar se a função e escopo solicitados está dentro da função e escopo da conta no bloco 428. Por exemplo, o componente de autorização de conta 118 pode determinar se a função e escopo solicitados estão dentro ou compatíveis com as funções e escopo da conta comparando as funções e o escopo solicitados com as funções e escopo da conta.

[00113] O fluxo lógico 420 pode rejeitar a solicitação quando função e escopo solicitados não estão dentro da função e escopo da conta no bloco 432 e terminam no bloco 436. Por exemplo, o componente de autorização de conta 118 pode rejeitar a solicitação quando as funções solicitadas incluem usuário remoto e depurador e a solicitação de escopo inclui limite de violação 138-1-1 enquanto a função da conta inclui depurador, mas não o usuário remoto, e o escopo da conta inclui floresta 132-2.

[00114] O fluxo lógico 420 pode autorizar a solicitação quando função e escopo solicitados estão dentro da função e escopo da conta no bloco 432 e terminam no bloco 436. Por exemplo, o componente de autorização de conta 118 pode autorizar a solicitação quando as funções solicitadas incluem usuário remoto e depurador e a solicitação

escopo inclui limite de violação 138-1-1 enquanto as funções da conta também incluem usuário remoto e depurador e o escopo da conta inclui floresta 132-1, que inclui limite de violação 138-1-1. As modalidades não são limitadas a esses exemplos.

[00115] A figura 4C ilustra uma modalidade de um fluxo lógico 440 e em particular, bloco 412 da figura 4A. O fluxo lógico 440 pode ser representante de algumas ou todas as operações executadas por uma ou mais modalidades aqui descritas.

[00116] Na modalidade ilustrada mostrada na figura 4C, o fluxo lógico 440 pode começar no bloco 442 e pode determinar a existência de uma conta JIT com função e escopo solicitados no bloco 444. Por exemplo, o componente de fornecimento de conta 120 pode determinar a existência da conta JIT com função e escopo solicitados e um conjunto de permissões de acesso elevado buscando e/ou digitalizando o armazenamento de dados de contas JIT 126 e comparando a informação de função e escopo solicitada com a função da conta JIT e informação de escopo de contas JIT existentes. O componente de fornecimento de conta 120 pode ainda determinar uma combinação substancial entre a função da conta JIT e a informação de escopo associadas com uma conta JIT existente e a informação de função e escopo solicitada recebida do cliente 102-1.

[00117] O fluxo lógico 440 pode recuperar a conta JIT existente quando a conta JIT já existir com a função e escopo solicitados para esse cliente no bloco 448. Por exemplo, o componente de fornecimento de conta 120 pode recuperar a informação da conta JIT associada com a conta JIT previamente criada do armazenamento de dados de conta JIT 126 para cliente 120-1, quando o componente de fornecimento de conta 120 determina que a conta JIT tendo função e escopo solicitados já existe para o cliente 120-1.

[00118] O fluxo lógico 440 pode criar a conta JIT quando a conta

JIT com função e escopo solicitados já não existe para esse cliente no bloco 450. Por exemplo, o componente de fornecimento de conta 120 pode criar a conta JIT para o cliente 102-1 acessar o dispositivo do servidor 140-1-1 quando uma conta JIT existente com a solicitação de função e escopo não foi encontrada no armazenamento de dados de contas JIT 126.

[00119] O fluxo lógico 440 pode habilitar a conta JIT no bloco 452 e terminar no bloco 454. Por exemplo, uma vez que a conta JIT foi criada ou recuperada, o componente de fornecimento de conta 120 pode habilitar a conta JIT com um conjunto de permissões de acesso elevado de modo que o cliente 102-1 possa utilizar a conta JIT habilitada para acessar ou operar o dispositivo do servidor 140-1-1. As modalidades não estão limitadas a esses exemplos.

[00120] A figura 4D ilustra uma modalidade de um fluxo lógico 470 e em particular, o bloco 452 da figura 4C. O fluxo lógico 470 pode ser representante de algumas ou todas as operações executadas por uma ou mais modalidades aqui descritas.

[00121] Na modalidade ilustrada mostrada na figura 4D, o fluxo lógico 470 pode começar no bloco 472 e pode identificar o grupo de segurança configurado para conceder acesso ao limite de violação no bloco 474. Por exemplo, supondo que o escopo solicitado para a conta JIT inclui limite de violação 138-1-1, o componente de fornecimento de conta 120 pode identificar grupo de segurança de limite de violação 210-1-1 como sendo configurado para conceder acesso ao limite de violação 138-1-1 utilizando interconexão de rede 112 e uma ou mais APIs do aplicativo do serviço de diretório (não mostradas) do dispositivo do servidor de serviço do diretório 130-*I*.

[00122] O fluxo lógico 470 pode associar a conta JIT com o grupo de segurança identificado no bloco 476 e terminar no bloco 478. Por exemplo, uma vez que o grupo de segurança de limite de violação

210-1-1 foi identificado, o componente de fornecimento de conta 120 pode associar a conta JIT com o grupo de segurança de limite de violação 210-1-1 adicionando essa conta JIT aos grupos de segurança do limite de violação 210-1-1 como um membro de modo que a conta JIT possa receber um conjunto de permissões de acesso para permitir acesso aos dispositivos do servidor 140-1-1, 140-1-2, 140-1-3 dentro de um limite de violação 138-1-1. As modalidades não são limitadas a esses exemplos.

[00123] A figura 4E ilustra uma modalidade de um fluxo lógico 480. O fluxo lógico 478 pode ser representante de algumas ou todas as operações executadas por uma ou mais modalidades aqui descritas.

[00124] Na modalidade ilustrada mostrada na figura 4E, o fluxo lógico 480 pode começar no bloco 482 e pode determinar a vida útil da conta JIT no bloco 484. Por exemplo, o componente de vida útil da conta 124 pode determinar a vida útil de uma conta JIT com base na informação de solicitação de conta JIT recebida do cliente 102-1 através do dispositivo do cliente 104-1. De modo alternativo, o componente de vida útil da conta 124 pode determinar a vida útil da conta JIT com base na função da conta JIT e na informação de escopo.

[00125] O fluxo lógico 480 pode determinar se a vida útil da conta JIT expirou no bloco 484. Por exemplo, assume-se que a informação de vida útil da conta JIT indica que a vida útil de uma conta JIT fornecida para acessar o dispositivo do servidor 140-1-1 é de 2 horas e a vida útil para a conta JIT começa do tempo quando a conta JIT é fornecida que foi às 13:00. O componente de vida útil da conta 124 pode determinar que a vida útil da conta JIT expirou quando o componente de vida útil da conta 124 recebe uma solicitação de aprovação de acesso para acessar o dispositivo do servidor 140-1-1 às 15:15 do dispositivo do servidor de serviço do diretório 130-*l*. De modo alternativo, o componente de vida útil da conta 124 pode determinar que a vida útil

da conta JIT ainda não expirou quando o componente de vida útil da conta 124 recebe uma solicitação de aprovação de acesso para acessar o dispositivo do servidor 140-1-1 às 13:15 do dispositivo do servidor de serviço do diretório 130-*l*.

[00126] O fluxo lógico 480 pode desabilitar a conta JIT quando a vida útil da conta JIT expirou no bloco 490 e termina no bloco 492. Por exemplo, assume-se que a informação de vida útil da conta JIT indica que a vida útil de uma conta JIT é de 2 horas e que 2 horas decorreram de modo que a vida útil da conta JIT há tenha sido expirado. O componente de vida útil da conta 124 pode então automaticamente desabilitar a conta JIT negando quaisquer solicitações de aprovação de acesso ao dispositivo do servidor 140-1-1 recebidas do dispositivo do servidor de serviço do diretório 130-*l* quando o cliente utiliza a conta JIT expirada para acessar o dispositivo do servidor 140-1-1. As modalidades não são limitadas a esses exemplos.

[00127] A figura 5 ilustra uma modalidade de uma arquitetura computacional exemplar 500 adequada para implementar várias modalidades conforme previamente descrito. Em uma modalidade, a arquitetura computacional 500 pode compreender ou ser implementada como parte dos dispositivos do cliente e/ou dispositivos do servidor. As modalidades não são limitadas nesse contexto.

[00128] Conforme utilizado nesse pedido, os termos "sistema" e "componente" pretendem se referir a uma entidade relacionada ao computador, tanto um hardware, quanto uma combinação de hardware e software, software, ou software em execução, exemplos dos quais são fornecidos pela arquitetura computacional exemplar 500. Por exemplo, um componente pode ser, mas não se limita a ser, um processo em execução em um processador, um processador, uma unidade de disco rígido, múltiplas unidades de armazenamento (de meio de armazenamento óptico e/ou magnético), um objeto, um executável, um

segmento de execução, um programa e/ou um computador. Em forma de ilustração, um aplicativo em execução em um servidor e o servidor podem ser um componente. Um ou mais componentes podem residir dentro de um processo e/ou segmento de execução, e um componente pode ser localizado em um computador e/ou distribuído entre dois ou mais computadores. Ainda, componentes podem ser comunicativamente acoplados um ao outro por vários tipos de meios de comunicação para coordenar operações. A coordenação pode envolver uma troca de informação unidirecional ou bidirecional. Por exemplo, os componentes podem transmitir informações na forma de sinais transmitidos através de meios de comunicação. As informações podem ser implementadas como sinais alocados a várias linhas de sinal. Em tais alocações, cada mensagem é um sinal. Outras modalidades, entretanto, podem de modo alternativo empregar mensagens de dados. Tais mensagens de dados podem ser enviadas através de várias conexões. Conexões exemplares podem incluir interfaces paralelas, interfaces de série e interfaces de barramento.

[00129] A arquitetura computacional 500 inclui vários elementos de computação comuns, como um ou mais processadores, processadores de vários núcleos, coprocessadores, unidades de memória, chipsets, controladores, periféricos, interfaces, osciladores, dispositivos de temporização, cartões de vídeo, cartões de áudio, componentes multimídia de entrada/saída (I/O), fontes de energia e assim por diante. As modalidades, entretanto, não são limitadas à implementação pela arquitetura computacional 500.

[00130] Conforme mostrado na figura 5, a arquitetura computacional 500 compreende uma unidade de processamento 504, uma memória de sistema 506 e um barramento de sistema 508. A unidade de processamento 504 pode ser qualquer processador de vários comercialmente disponíveis, incluindo, sem limitação, processadores AMD®

Athlon®, Duron® e Opteron®; aplicativo ARM®, processadores incorporados e protegidos; processadores IBM® e Motorola® DragonBall® e PowerPC®; processadores IBM e Sony® Cell; processadores Intel® Celeron®, Core (2) Duo®, Itanium®, Pentium®, Xeon®, e XScale® e processadores similares. Microprocessadores duplos, processadores de múltiplos núcleos, e outras arquiteturas de múltiplos processadores também podem ser empregados como a unidade de processamento 504.

[00131] O barramento do sistema 508 fornece uma interface para componentes do sistema incluindo, mas não limitado à, a memória do sistema 506 à unidade de processamento 504. O barramento do sistema 508 pode ser qualquer de vários tipos de estrutura de barramento que pode ainda se interconectar a um barramento de memória (com ou sem um controlador de memória), um barramento periférico, e um barramento local utilizando quaisquer arquiteturas de barramento de uma variedade disponível comercialmente. Adaptadores de interface podem se conectar ao barramento do sistema 508 através de uma arquitetura de ranhura. Arquiteturas de ranhura exemplares podem incluir, sem limitação, Porta Gráfica Acelerada (Accelerated Graphics Port - AGP), Card Bus, Industry Standard Architecture ((E)ISA), Micro Channel Architecture (MCA), NuBus, Interconector de Componentes Periféricos Estendido (Peripheral Component Interconnect (Extended) - (PCI(X)), Associação Internacional do Cartão de Memória de Computador Pessoal (Personal Computer Memory Card International Association – PCMCIA), PCI Express e similares.

[00132] A arquitetura computacional 500 pode compreender ou implementar vários artigos de fabricação. Um artigo de fabricação pode compreender um meio de armazenamento legível por computador para armazenar lógica. Exemplos de um meio de armazenamento legível por computador pode incluir qualquer meio tangível capaz de armaze-

nar dados eletrônicos, incluindo memória volátil ou memória não volátil, memória removível ou não removível, memória apagável ou não apagável, memória gravável ou não gravável, e assim por diante. Exemplos de lógica podem incluir instruções de programa de computador executáveis implementadas utilizando qualquer tipo adequado de código, como código de fonte, código compilado, código interpretado, código executável, código estático, código dinâmico, código orientado por objeto, código visual, e similares. Modalidades também podem ser pelo menos parcialmente implementadas conforme instruções contidas em um meio não transitório legível por computador, que pode ser lido e executado por um ou mais processadores para permitir a realização das operações descritas aqui.

[00133] A memória do sistema 506 pode incluir vários tipos de meios legíveis por computador na forma de uma ou mais unidades de memória de velocidade mais alta, como memória somente de leitura (ROM), memória de acesso aleatório (RAM), RAM dinâmica (DRAM), DRAM de Memória de Taxa Dupla de Dados (DDRAM), DRAM sincronizada (SDRAM), RAM estática (SRAM), ROM programável (PROM), ROM programável apagável (EPROM), ROM programável apagável eletricamente (EEPROM), memória flash, memória de polímero, como memória de polímero ferroelétrico, memória ovônica, mudança de fase ou memória ferroelétrica, memória de silicone-óxido-nitrito-óxido-silicone (SONOS), cartões ópticos e magnéticos, uma variedade de dispositivos como drives de Gama Redundante de Discos Independentes (RAID), dispositivos de memória de estado sólido, por exemplo, memória USB, drives de estado sólido (SSD) e qualquer outro tipo de meio de armazenamento adequado para armazenar informações. Na modalidade ilustrada mostrada na figura 5, a memória do sistema 506 pode incluir memória não volátil 510 e/ou memória volátil 512. Um sistema básico de entrada e saída (BIOS) pode ser armazenado na me-

mória não volátil 510.

[00134] O computador 502 pode incluir vários tipos de meios de armazenamento legível por computador na forma de uma ou mais unidades de memória de velocidade mais baixa, incluindo uma unidade interna de disco rígido (HDD) 514 (ou externa), uma unidade de disquete magnética (FDD) 516 para ler a partir de ou gravar para um disco magnético removível 518, e uma unidade de disco óptico 520 para ler a partir de ou gravar para um disco óptico removível 522 (por exemplo, um CD-ROM ou DVD). HDD 514, FDD 516 e unidade de disco rígido 520 podem ser conectadas ao barramento do sistema 508 através de uma interface da HDD 524, de uma interface da FDD 526 e de uma interface da unidade óptica 528, respectivamente. A interface da HDD 524 para implementações de drive externo pode incluir pelo menos uma ou ambas as tecnologias de interface de Barramento Serial Universal (USB) e IEEE 1394.

[00135] As unidades e meios de rede legíveis por computador associados fornecem armazenamento de dados volátil e/ou não volátil, estruturas de dados, instruções legíveis por computador, e assim por diante. Por exemplo, um número de módulos do programa pode ser armazenado nos drives e nas unidades de memória 510, 512, incluindo um sistema operacional 530, um ou mais programas de aplicativo 532, outros módulos do programa 534 e dados de programa 536. Em uma modalidade, um ou mais programas de aplicativo 532, outros módulos do programa 534 e dados do programa 536 podem incluir, por exemplo, os vários aplicativos e/ou componentes do sistema 100.

[00136] Um usuário pode inserir comandos e informação ao computador 502 através de um ou mais dispositivos de entrada com fio/ sem fio, por exemplo, um teclado 538 e um dispositivo indicador, como um mouse 540. Outros dispositivos de entrada podem incluir microfones, controles remotos infravermelhos (IR), controles remotos de radiofre-

quência (RF), consoles de jogos, canetas stylus, leitores de cartão, dongles, leitores de impressão digital, luvas, tablets gráficos, joysticks, teclados, leitores de retina, telas táteis (por exemplo, capacitivo, resistivo e etc.), trackballs, trackpads, sensores, agulhas e similares. Esses e outros dispositivos de entrada são frequentemente conectados à unidade de processamento 504 através de uma interface do dispositivo de entrada 542 que é acoplada ao barramento do sistema 508, mas pode ser conectada por outras interfaces, como uma porta paralela, porta serial IEEE 1394, uma porta de jogo, uma porta USB, uma interface de IR, e assim por diante.

[00137] Um monitor 544 ou outro tipo de dispositivo de exibição é também conectado ao barramento do sistema 508 através de uma interface, como um adaptador de vídeo 546. O monitor 544 pode ser interno ou externo ao computador 502. Além do monitor 544, um computador tipicamente inclui outros dispositivos de saída periféricos, como alto-falantes, impressoras, e assim por diante.

[00138] O computador 502 pode operar em um ambiente de rede utilizando conexões lógicas através das comunicações com fio e/ou sem fio um ou mais computadores remotos, como a computador remoto 548. O computador remoto 548 pode ser uma estação de trabalho, um computador servidor, um roteador, um computador pessoal, computador portátil, dispositivo de entretenimento com base no microprocessador, um dispositivo parceiro ou outro nó de rede comum, e tipicamente inclui muitos ou todos os elementos descritos com relação ao computador 502, embora, para fins de brevidade, apenas um dispositivo de memória/armazenamento 550 seja ilustrado. As conexões lógicas retratadas incluem conectividade com fio/sem fio a uma rede de área local (LAN) 552 e/ou redes maiores, por exemplo, uma rede de área ampla (WAN) 554. Tais ambientes de rede LAN e WAN são comuns em escritórios e empresas, e facilitam as redes de computador

coorporativas, como intranets, todas as quais podem se conectar a uma rede de comunicações global, por exemplo, a Internet.

[00139] Quando utilizado em um ambiente de rede LAN, o computador 502 é conectado à LAN 552 através de uma interface de rede de comunicação com fio e/ou sem fio ou adaptador 556. O adaptador 556 pode facilitar as comunicações com fio e/ou sem fio à LAN 552, que também pode incluir um ponto de acesso sem fio disposto sobre ele para se comunicar com a funcionalidade sem fio do adaptador 556.

[00140] Quando utilizado em um ambiente de rede WAN, o computador 502 pode incluir um modem 558 ou ser conectado a um servidor de comunicações na WAN 554, ou tem outros meios para estabilizar comunicações sobre a WAN 554, como por meio da Internet. O modem 558, que pode ser interno ou externo e um dispositivo com fio e/ou sem fio, se conecta a um barramento do sistema 508 através da interface do dispositivo de entrada 542. Em um ambiente de rede, os módulos de programa retratados com relação ao computador 502, ou porções do mesmo, podem ser armazenados em um dispositivo de armazenamento/memória remoto 550. Será observado que as conexões de rede mostradas são exemplares e outros meios de estabelecer um link de comunicação entre os computadores podem ser utilizados.

[00141] O computador 502 é operável para comunicar dispositivos com fio e sem fio ou entidades utilizando a família de padrões IEEE 802, como dispositivos sem fio operativamente dispostos em comunicação sem fio (por exemplo, técnicas de modulação pelo ar IEEE 802.11). Isso inclui pelo menos tecnologias sem fio, como Wi-Fi (ou Wireless Fidelity), WiMax e Bluetooth™, entre outras. Assim, a comunicação pode ser uma estrutura predefinida como com uma rede convencional ou simplesmente uma comunicação ad hoc entre pelo menos dois dispositivos. As redes Wi-Fi utilizam tecnologias de rádio

chamadas IEEE 802.1 lx (a, b, g, n, e etc.) para fornecer conectividade sem fio segura, confiável e rápida. Uma rede Wi-Fi pode ser utilizada para conectar computadores uns aos outros, à internet e às redes com fio (que utilizam funções e meios relacionados ao IEEE 802.3).

[00142] Algumas modalidades podem ser descritas utilizando a expressão "uma modalidade" juntamente com seus derivados. Esses termos significam que uma característica, estrutura ou recurso descritos em conexão com a modalidade está incluso pelo menos em uma modalidade. O aparecimento da frase "em uma modalidade" em vários lugares no relatório não é necessariamente sempre se referindo à mesma modalidade. Ainda, algumas modalidades podem ser descritas utilizando as expressões "acoplado" e "conectado", juntamente com seus derivados. Esses termos não pretendem aparecer necessariamente como sinônimos uns aos outros. Por exemplo, algumas modalidades podem ser descritas utilizando os termos "conectado" e/ou "acoplado" para indicar que dois ou mais elementos estão em contato direto elétrico ou físico um com o outro. O termo "acoplado", entretanto, também pode significar que dois ou mais elementos não estão em contato direto um com o outro, mas ainda cooperam ou interagem um com o outro.

[00143] É enfatizado que o Resumo da descrição é fornecido para permitir a um leitor determinar rapidamente a natureza da descrição técnica. É apresentado com o entendimento que não será utilizado para interpretar ou limitar o escopo ou significado das reivindicações. Além disso, na Descrição Detalhada anterior, pode ser visto que várias características são agrupadas em uma única modalidade com a finalidade de simplificar a descrição. Esse método de descrição não deve ser interpretado como refletindo uma intenção de que as modalidades reivindicadas precisem de mais características do que expressamente recitado em cada reivindicação. Preferivelmente, como as reivindica-

ções a seguir refletem, o assunto inovador encontra-se em menos de todas as características de uma única modalidade revelada. Assim, as seguintes reivindicações estão incorporadas à Descrição Detalhada, com cada reivindicação se fazendo valer como uma modalidade separada. Nas reivindicações anexas, os termos "incluindo" e "no qual" são utilizados como equivalentes em inglês simples dos respectivos termos "compreendendo" e "em que", respectivamente. Além disso, os termos "primeiro", "segundo", "terceiro", e assim por diante, são utilizados meramente como rótulos, e não pretendem impor exigências numéricas aos seus objetos.

[00144] O que foi descrito acima inclui exemplos da arquitetura revelada. Não é, com certeza, possível descrever cada combinação de componentes e/ou metodologias possível, mas um técnico no assunto pode reconhecer que outras combinações e permutações são possíveis. Em conformidade, a arquitetura inovadora pretende englobar todas essas alterações, modificações e variações que estão dentro do âmbito e do escopo das reivindicações anexas.

REIVINDICAÇÕES

1. Dispositivo, **caracterizado pelo fato de que** compreende:

um circuito do processador; e

um aplicativo do servidor para execução pelo circuito do processador, o aplicativo do servidor compreendendo

um componente de gerenciamento de conta para receber uma solicitação de um cliente tendo uma primeira conta através de um dispositivo do cliente para uma segunda conta para acessar um dispositivo do servidor em um conjunto de dispositivos do servidor,

um componente de autorização de conta para autorizar a solicitação para a segunda conta com base pelo menos parcialmente na informação da conta associada com a primeira conta,

um componente de fornecimento de conta para fornecer a segunda conta para permitir que um cliente acesse o dispositivo do servidor, e

um componente de notificação de conta para fornecer informação da conta associada com a segunda conta ao cliente através do dispositivo do cliente,

em que a segunda conta é uma conta just-in-time (JIT); e

em que o conjunto de dispositivos do servidor é segmentado em uma pluralidade de limites de violação e cada limite de violação da pluralidade de limites de violação está associado a um único grupo de segurança configurado para conceder acesso a um conjunto de dispositivos do servidor em cada limite de violação.

2. Dispositivo de acordo com a reivindicação 1, **caracterizado** pelo fato de que o componente de autorização de conta é ainda para:

determinar um escopo e uma função associados com a solicitação,

determinar um escopo e uma função associados com à primeira conta com base na informação da conta associada com a primeira conta, e

autorizar a solicitação com base pelo menos parcialmente no escopo e na função da primeira conta.

3. Dispositivo de acordo com a reivindicação 2, **caracterizado** pelo fato de que o componente de fornecimento de conta é ainda para:

determinar a existência da segunda conta com um conjunto de permissões de acesso elevado com base na função e no escopo associados com a solicitação,

criar a segunda conta para acesso ao dispositivo do servidor, quando a segunda conta não existe, e

permitir que a segunda conta acesse ao dispositivo do servidor.

4. Dispositivo de acordo com a reivindicação 3, **caracterizado** pelo fato de que o componente de autorização de conta é ainda para:

identificar um grupo de segurança configurado para conceder acesso a um limite de violação compreendendo o dispositivo do servidor, e

associar a segunda conta com o grupo de segurança para permitir que a segunda conta acesse ao dispositivo do servidor no limite de violação.

5. Dispositivo de acordo com a reivindicação 1, **caracterizado** pelo fato de que a solicitação para elevar as permissões de acesso está associada com uma vida útil, a vida útil compreende um período de tempo definido para permitir o acesso ao dispositivo do servidor, e a segunda conta ser automaticamente desabilitada no final do período de tempo definido.

6. Dispositivo de acordo com a reivindicação 1, **caracterizado** pelo fato de que o dispositivo do servidor exige um conjunto de permissões de acesso mais alto que um conjunto de permissões de acesso associado com a primeira conta e a segunda conta tem um conjunto de permissões de acesso elevado mais alto que o conjunto de permissões de acesso associado com a primeira conta.

7. Meio de armazenamento legível por máquina **caracterizado pelo fato de que** compreende um método que, em resposta a ser executado em um dispositivo computacional, faz com que o dispositivo computacional perceba um dispositivo, como definido em qualquer uma das reivindicações 1 a 6.

8. Meio de armazenamento legível por máquina, de acordo com a reivindicação 7, **caracterizado** pelo fato de que a informação da conta compreende uma senha aleatória gerada por um aplicativo de gerenciamento de token de autenticação e a senha aleatória compreende pelo menos duas classes de caractere diferentes.

9. Método implementado por computador, **caracterizado pelo fato de que** compreende:

receber uma solicitação de um cliente tendo uma primeira conta através de um dispositivo do cliente para uma segunda conta com um conjunto de permissões de acesso para acessar um dispositivo do servidor em um conjunto de dispositivos do servidor;

autorizar, por circuito, a solicitação para a segunda conta com base pelo menos parcialmente na informação da conta associada com a primeira conta;

fornecer a segunda conta para permitir que um cliente acesse o dispositivo do servidor; e fornecer informação da conta associada com a segunda conta ao cliente através do dispositivo do cliente,

em que a segunda conta é uma conta just-in-time (JIT); e

em que o conjunto de dispositivos do servidor é segmenta-

do em uma pluralidade de limites de violação e cada limite de violação da pluralidade de limites de violação está associado a um único grupo de segurança configurado para conceder acesso a um conjunto de dispositivos do servidor em cada limite de violação.

10. Método implementado por computador de acordo com a reivindicação 9, **caracterizado** pelo fato de que a permissão da segunda conta para acesso ainda compreende:

identificar um grupo de segurança configurado para conceder acesso ao limite de violação compreendendo o dispositivo do servidor; e

associar a segunda conta com o grupo de segurança para permitir que a segunda conta acesse o dispositivo do servidor no limite de violação.

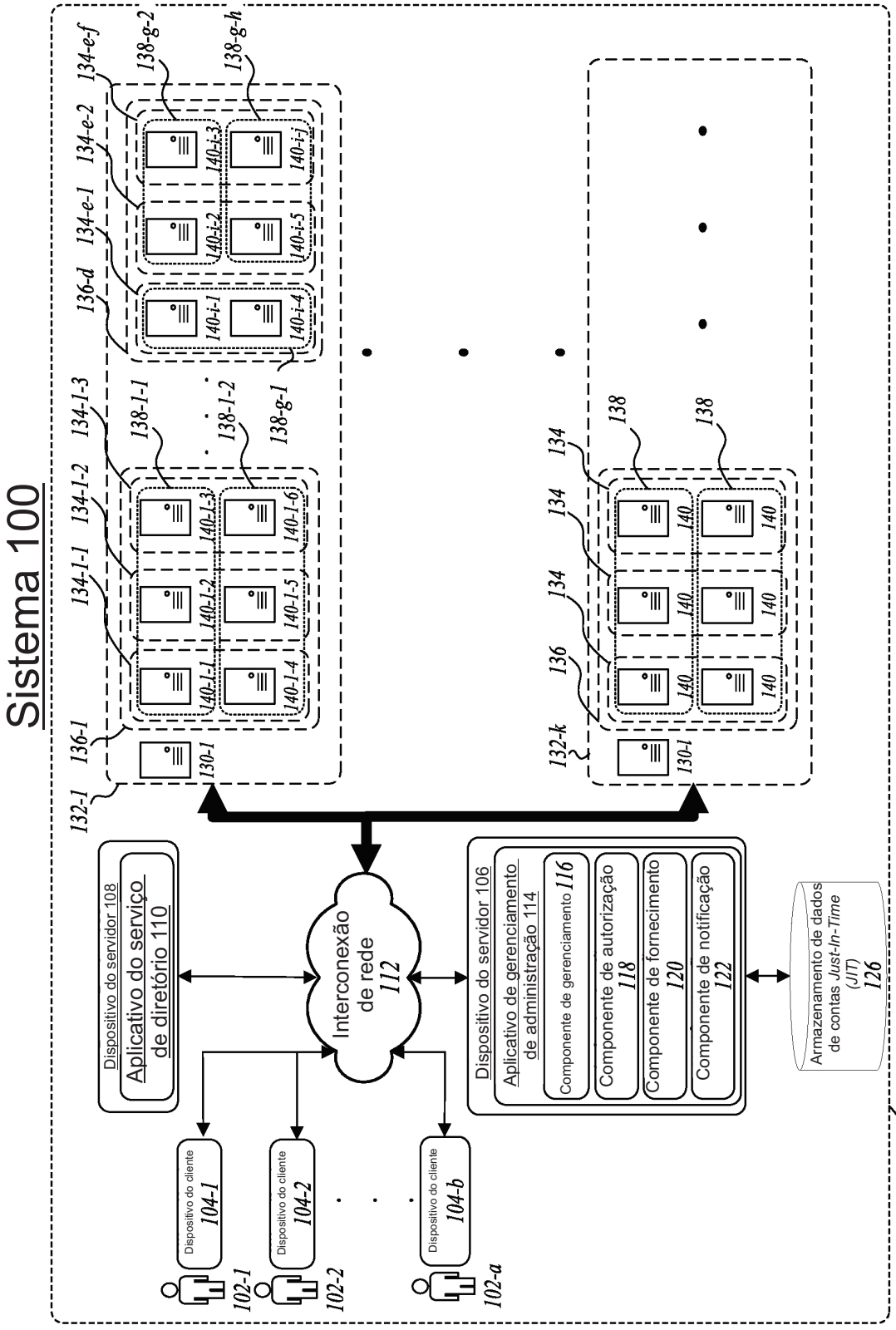
Sistema 100
Dispositivo do servidor 108
Aplicativo do serviço de diretório 110
Interconexão de rede 112
Dispositivo do servidor 106
Aplicativo de gerenciamento de administração 114
Componente de gerenciamento 116
Componente de autorização 118
Componente de fornecimento 120
Componente de notificação 122
Armazenamento de dados de contas Just-In-Time (JIT) 126
Dispositivo do cliente 104-1
Dispositivo do cliente 104-2
Dispositivo do cliente 104-b
102-1
102-2
102-a
132-1
132-k
136-1
136-d
136
130-1
134-1-1
134-1-2
134-1-3
134-e-1
134-e-2
134-e-f
134
138-1-1
138-1-2
138-g-1
138-g-2
138-g-h
138
140-1-1
140-1-2
140-1-3
140-1-4
140-1-5
140-1-6
140-i-1
140-i-2
140-i-3
140-i-4
140-i-5
140-i-j
140
150

FIG. 1

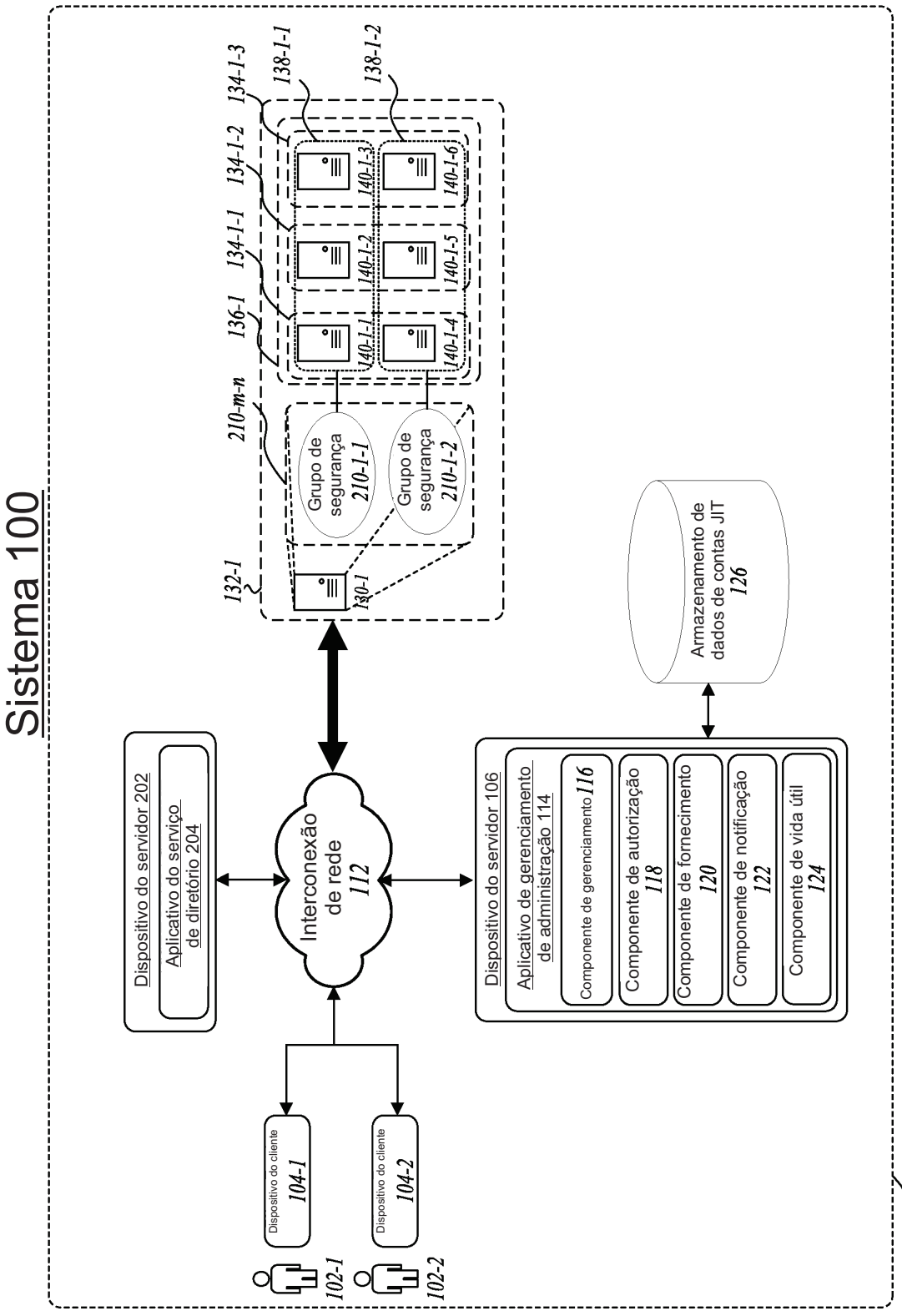
Sistema 100
Dispositivo do servidor 202
Aplicativo do serviço de diretório 204
Interconexão de rede 112
Dispositivo do servidor 106
Aplicativo de gerenciamento de administração 114
Componente de gerenciamento 116
Componente de autorização 118
Componente de fornecimento 120
Componente de notificação 122
Componente de vida útil 124
Armazenamento de dados de contas JIT 126
Grupo de segurança 210-1-1
Grupo de segurança 210-1-2
Dispositivo do cliente 104-1
Dispositivo do cliente 104-2
102-1
102-2
132-1
130-1
136-1
134-1-1
134-1-2
134-1-3
138-1-1
138-1-2
140-1-1
140-1-2
140-1-3
140-1-4
140-1-5
140-1-6
210-m-n
150

FIG. 2

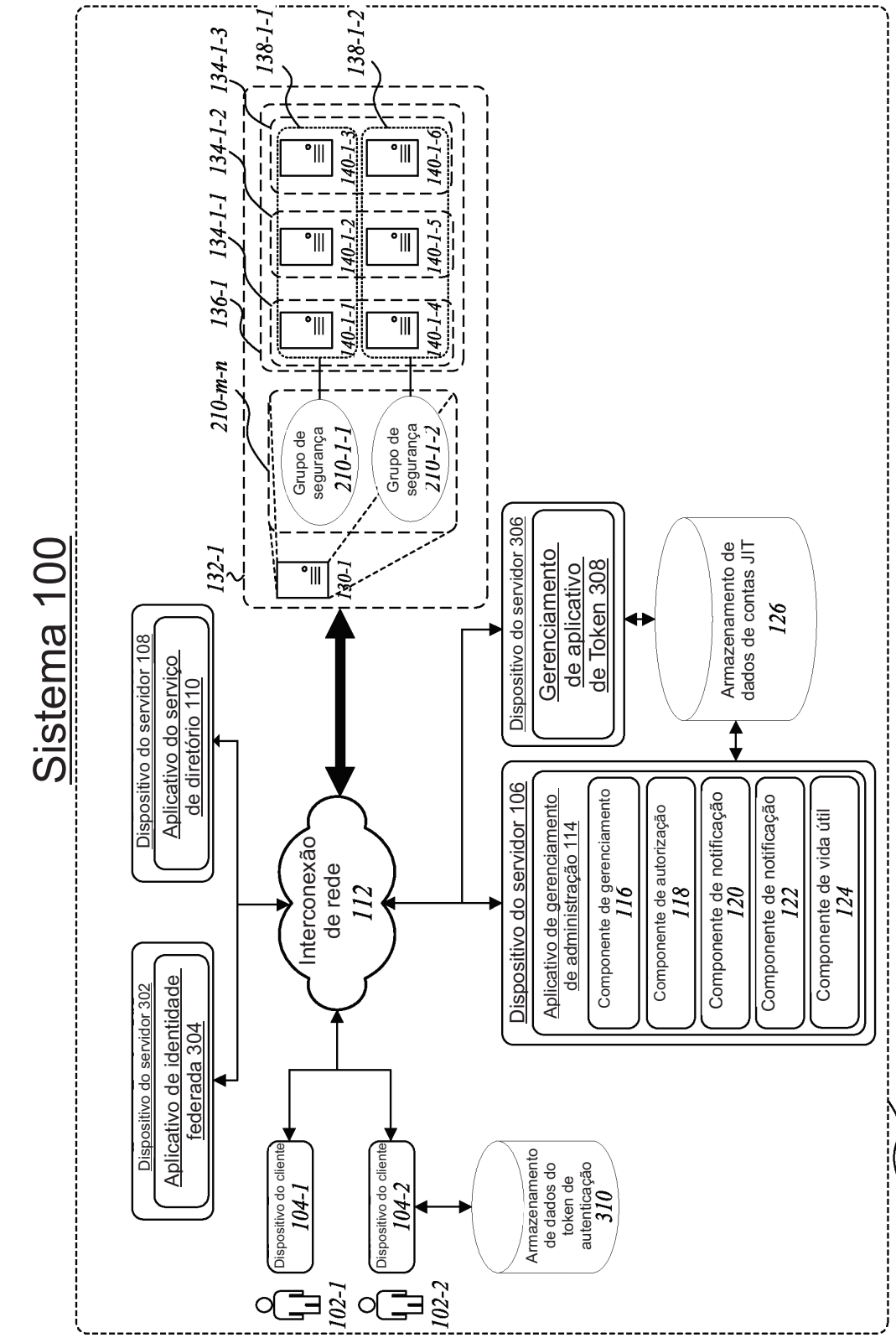
Sistema 100
Dispositivo do servidor 108
Aplicativo do serviço de diretório 110
Dispositivo do servidor 302
Aplicativo de identidade federada 304
Interconexão de rede 112
Dispositivo do cliente 104-1
Dispositivo do cliente 104-2
Armazenamento de dados do token de autenticação 310
102-1
102-2
132-1
130-1
210-m-n
Grupo de segurança 210-1-1
Grupo de segurança 210-1-2
136-1
134-1-1
134-1-2
134-1-3
138-1-1
138-1-2
140-1-1
140-1-2
140-1-3
140-1-4
140-1-5
140-1-6
Dispositivo do servidor 306
Gerenciamento de aplicativo de Token 308
Armazenamento de dados de contas JIT 126
Dispositivo do servidor 106
Aplicativo de gerenciamento de administração 114
Componente de gerenciamento 116
Componente de autorização 118
Componente de notificação 120
Componente de notificação 122
Componente de vida útil 124
150

FIG. 3

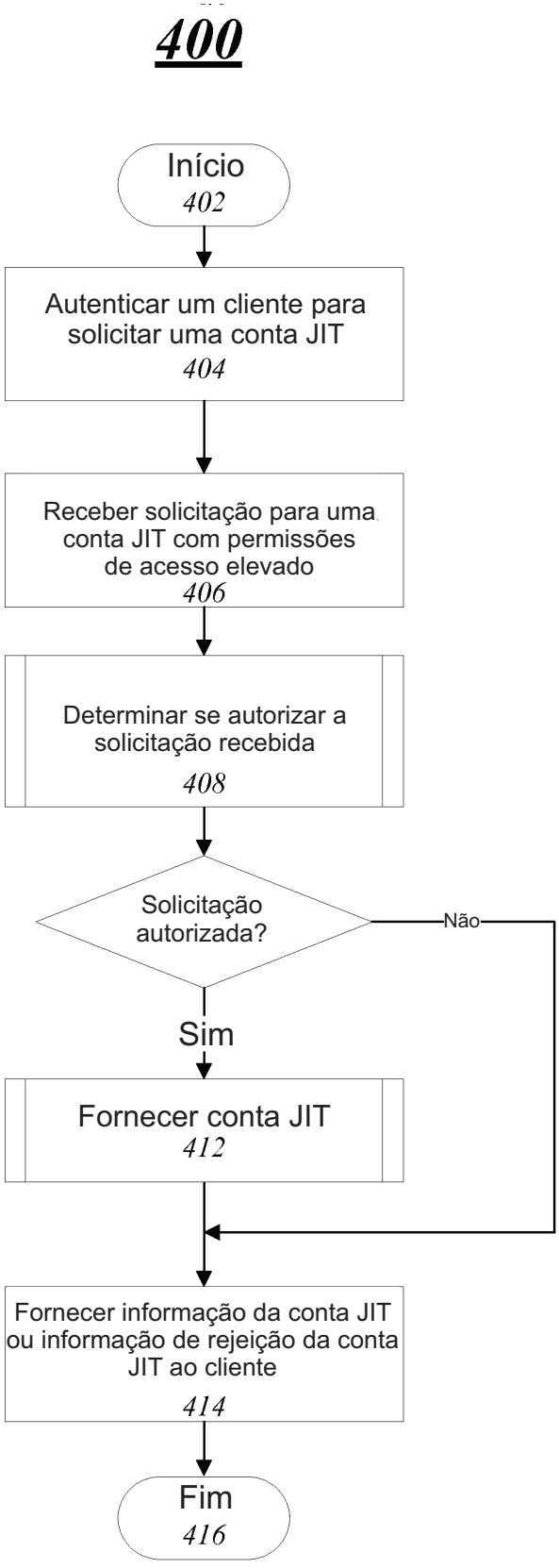
400
Início
402
Autenticar um cliente para solicitar uma conta JIT
404
Receber solicitação para uma conta JIT com permissões de acesso elevado
406
Determinar se autorizar a solicitação recebida
408
Solicitação autorizada?
Não
Sim
Fornecer conta JIT
412
Fornecer informação da conta JIT ou informação de rejeição da conta JIT ao cliente
414
Fim
416

FIG. 4A

420

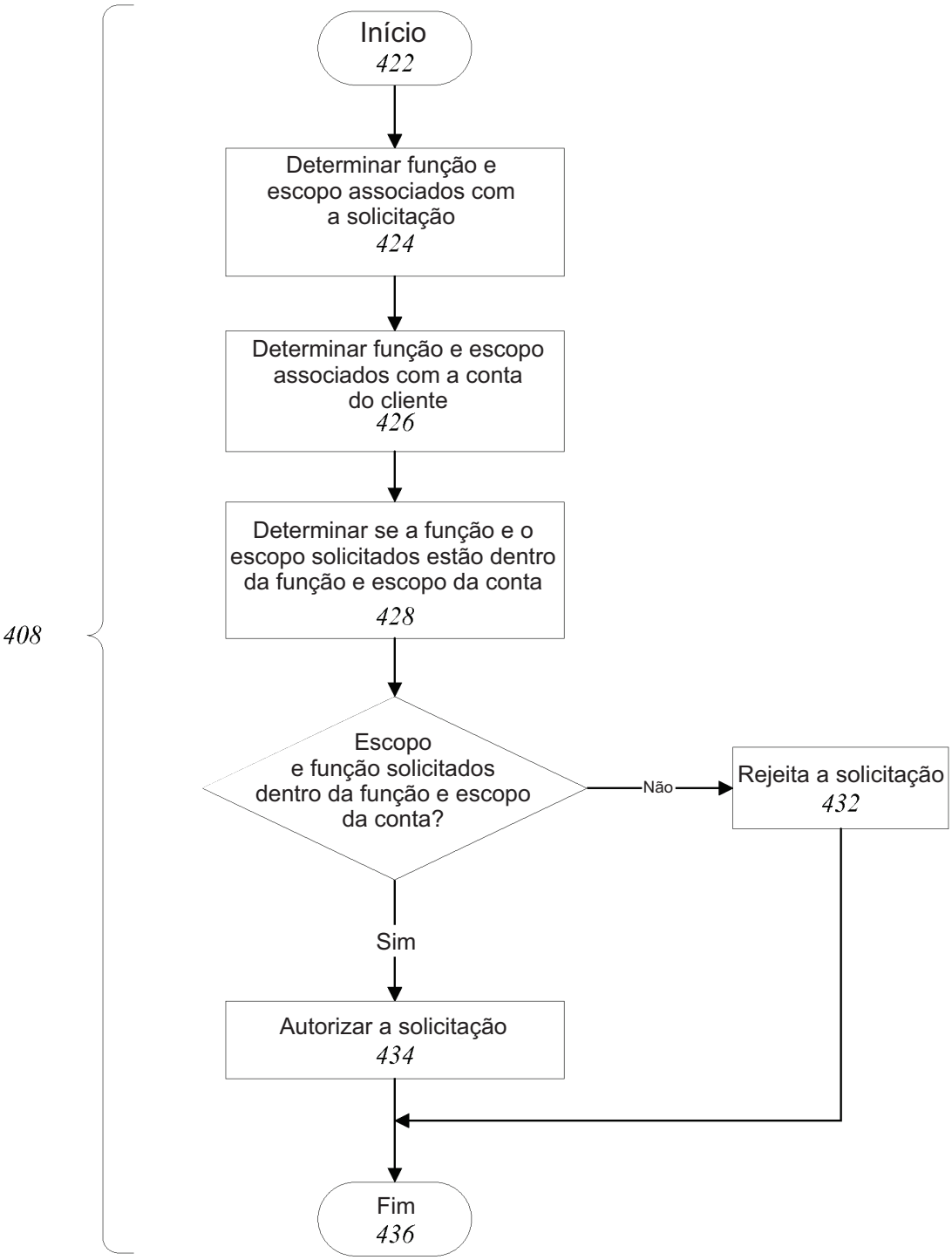
Início
422
Determinar função e escopo associados com a solicitação
424
Determinar função e escopo associados com a conta do cliente
426
Determinar se a função e o escopo solicitados estão dentro da função e escopo da conta
428
408
Escopo e função solicitados dentro da função e escopo da conta?
Não
Rejeita a solicitação
432
Sim
Autorizar a solicitação
434
Fim
436

FIG. 4B

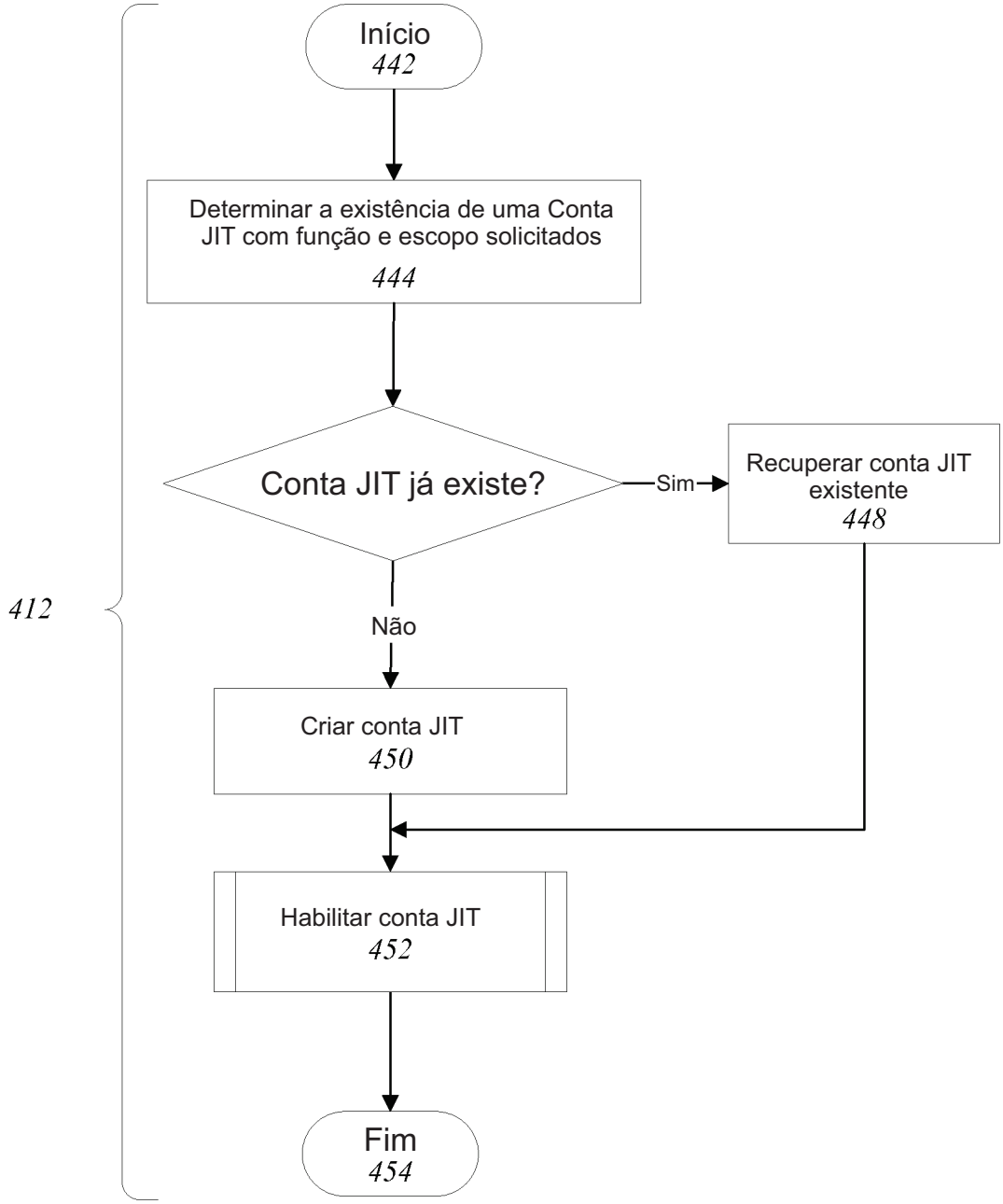
Início
442
Determinar a existência de uma Conta JIT com função e escopo solicitados
444
Conta JIT já existe?
Sim
Recuperar conta JIT existente
448
412
Não
Criar conta JIT
450
Habilitar conta JIT
452
Fim
454

FIG. 4C

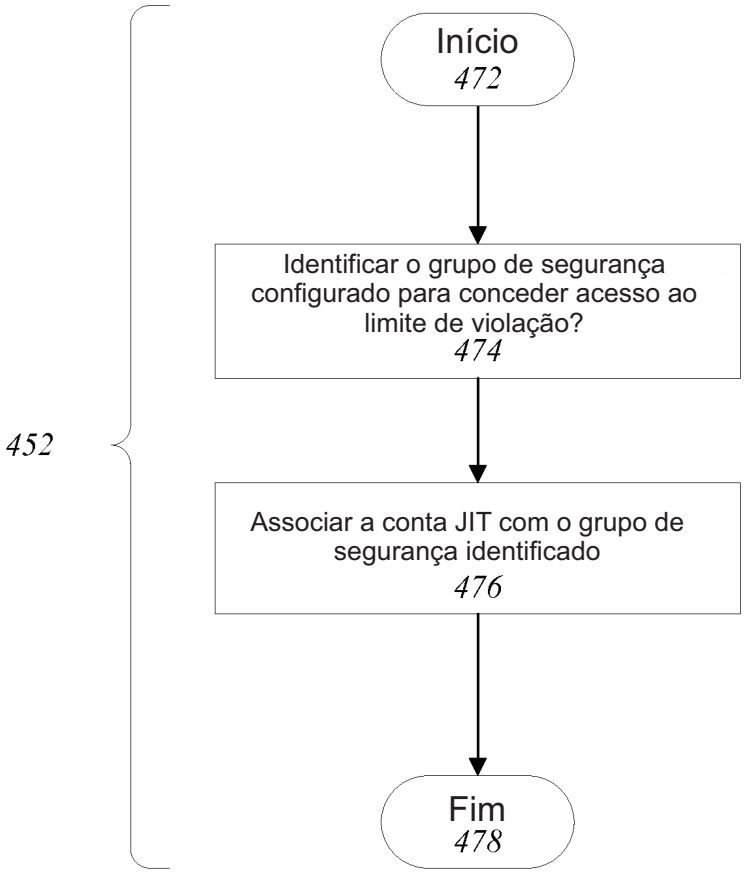
Início
472
Identificar o grupo de segurança configurado para conceder acesso ao limite de violação?
474
452
Associar a conta JIT com o grupo de segurança identificado
476
Fim
478

FIG. 4D

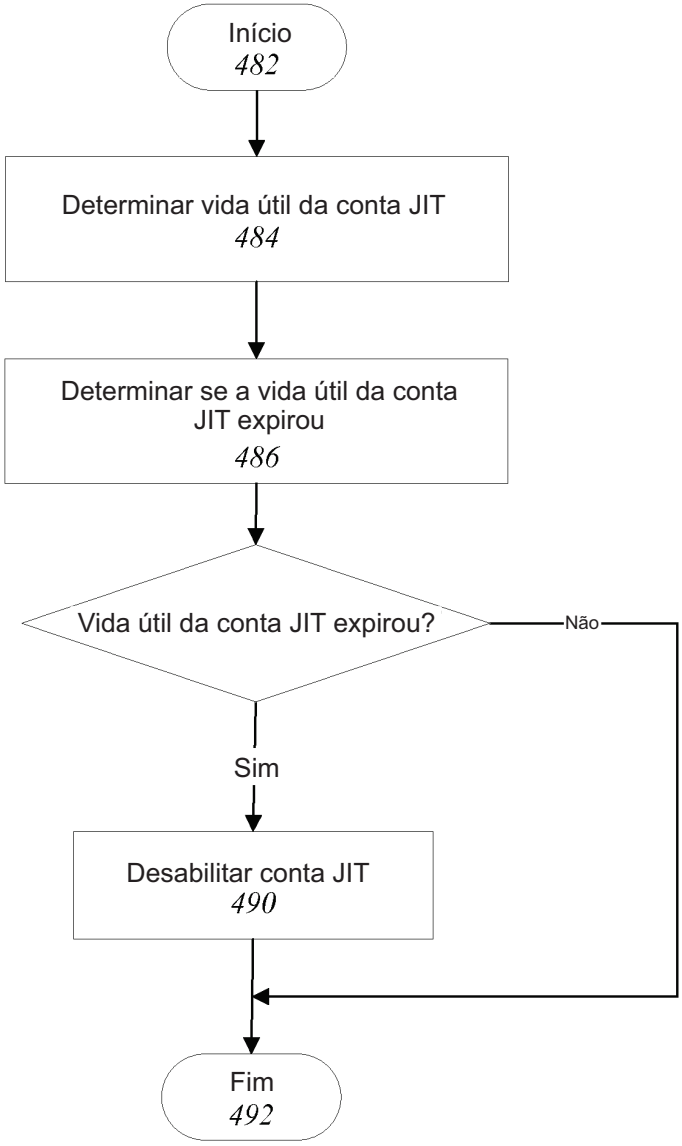
Início
482
Determinar vida útil da conta JIT
484
Determinar se a vida útil da conta JIT expirou
486
Vida útil da conta JIT expirou?
Não
Sim
Desabilitar conta JIT
490
Fim
492

FIG. 4E

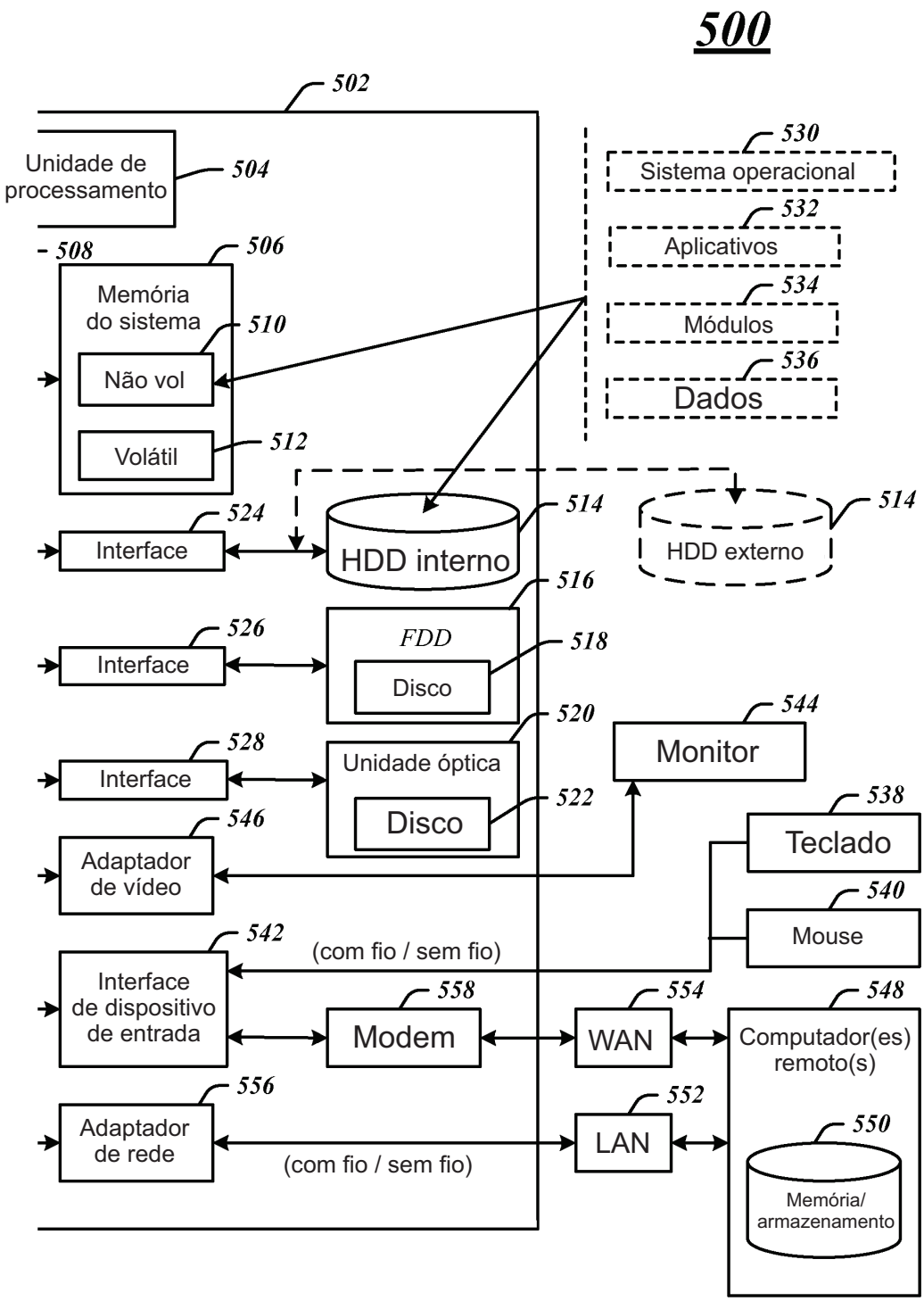
500
502
Unidade de processamento
504
508
506
Memória do sistema
510
Não vol
512
Volátil
530
Sistema operacional
532
Aplicativos
534
Módulos
536
Dados
524
Interface
514
HDD interno
514
HDD externo
516
526
Interface
FDD
518
Disco
520
528
Interface
Unidade óptica
522
Disco
544
Monitor
546
Adaptador de vídeo
538
Teclado
540
Mouse
542
(com fio / sem fio)
Interface de dispositivo de entrada
558
Modem
554
WAN
548
Computador(es) remoto(s)
556
Adaptador de rede
552
LAN
550
(com fio / sem fio)
Memória/ armazenamento

FIG. 5