Aprimorando o Gerenciamento de Senha Incluindo Segurança, Flexibilidade e Agilidade

Guia da Solução IBM Redbooks

O número de logins e senhas que os funcionários devem gerenciar diariamente continua sendo uma fonte de frustrações e de perda de produtividade. Os funcionários devem se lembrar de informações de login para inúmeros aplicativos. Muitos desses aplicativos requerem nomes de usuários e senhas diferentes, requisitos de complexidade de senha diferentes e mudanças de senha forçadas em pequenos intervalos. O número de logins que um funcionário deve gerenciar aumenta com a implementação de cada aplicativo de negócios adicional. O help desk corporativo costuma suportar o processo de restauração de informações de login perdidas ou esquecidas dos funcionários. Esses fatores juntos contribuem com riscos para a segurança e aumentam os custos do help desk que algumas organizações não podem bancar.

Usando o IBM® Security Access Manager for Enterprise Single Sign-On, sua organização pode abordar sérios desafios de segurança, produtividade e conformidade em uma solução gerenciada centralmente. A Figura 1 ilustra uma visão geral dessa solução.

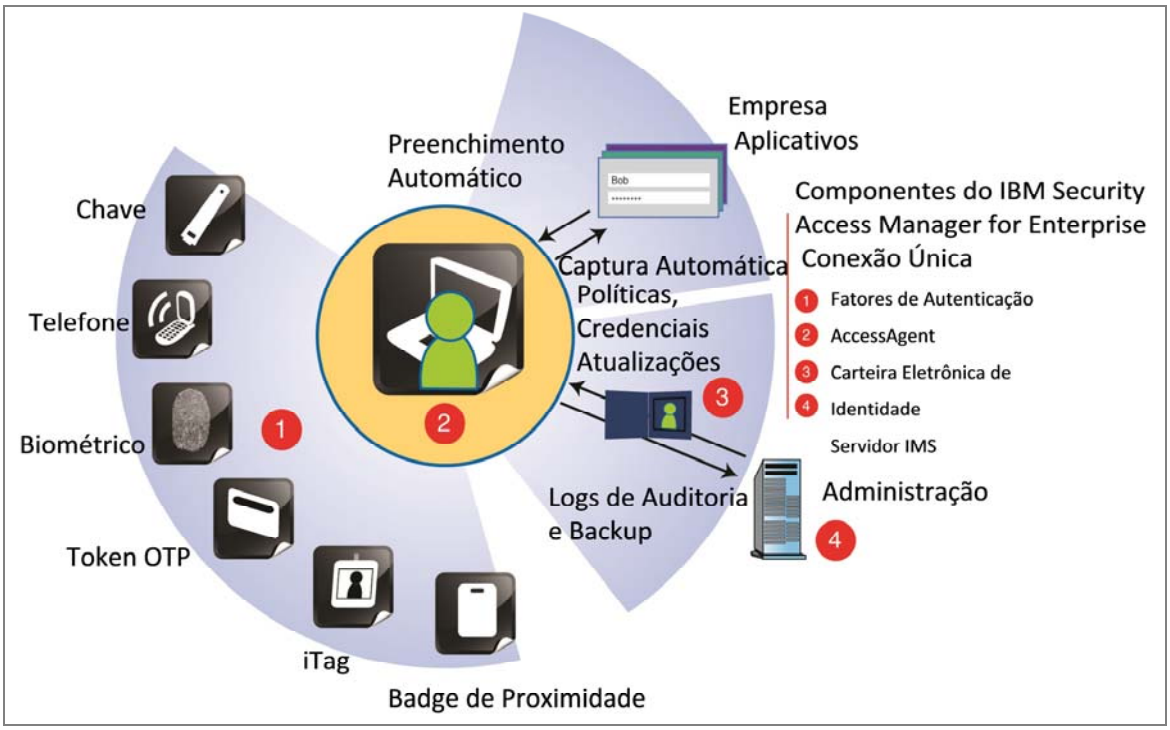

Figura 1. Visão geral do IBM Security Access Manager for Enterprise Single Sign-On

Você sabia?

Uma reclamação frequente do usuário é o requisito para se lembrar de várias senhas, e o principal ponto fraco da segurança do computador é a seleção de senha fraca. As violações de segurança como resultado de senhas fracas ou gerenciamento não seguro de senhas são comuns. O fornecimento de uma solução centralizada para gerenciamento de senha e autoatendimento, mecanismos de autenticação forte flexíveis e capacidade de usar estações de trabalho virtuais e compartilhadas fazem a solução IBM Security Access Manager for Enterprise Single Sign-On se destacar.

Visão geral de solução e valor de negócios

O IBM Security Access Manager for Enterprise Single Sign-On pode ajudá-lo a resolver o paradoxo das senhas. Os usuários devem se lembrar de apenas uma senha e não precisarão mais lidar com senhas fortes para todos os aplicativos corporativos. Eles se autenticarão uma vez e o IBM Security Access Manager for Enterprise Single Sign-On cuidará do resto. O IBM Security Access Manager for Enterprise Single Sign-On fornece os principais valores de negócios a seguir:

- Gerenciamento de senhas com segurança

  O IBM Security Access Manager for Enterprise Single Sign-On protege dados e aplicativos relacionados a senhas. Ele usa a mais forte criptografia disponível, incluindo Padrão de Criptografia Avançado (AES) e Padrão de Criptografia de Dados triplo (DES). O IBM Security Access Manager for Enterprise Single Sign-On opera em conformidade com o Federal Information Processing Standard (FIPS) 140-2 para ajudar instituições financeiras, agências do governo, assistência médica e outras organizações a atenderem aos mais rigorosos regulamentos de segurança e privacidade que controlam suas operações. O IBM Security Access Manager for Enterprise Single Sign-On also oferece autenticação de dois fatores para aumentar a segurança. Ele permite a combinação e a correspondência de diferentes fatores, dependendo do usuário ou da máquina. Se esses fatores existirem, o IBM Security Access Manager for Enterprise Single Sign-On poderá usá-los.

- Reduzindo os custos do help desk e melhorando a produtividade do funcionário

  A funcionalidade de reconfiguração de senha do autoatendimento do IBM Security Access Manager for Enterprise Single Sign-On pode reduzir ou eliminar custos associados a senhas esquecidas e à perda de produtividade do funcionário devido a bloqueios de conta. Senhas esquecidas e bloqueios de conta, como resultado de muitas falhas nas tentativas, podem sobrecarregar o help desk de uma empresa. O IBM Security Access Manager for Enterprise Single Sign-On fornece funções configuráveis para que os usuários possam realizar o autoatendimento de senha de maneiras que atendam a vários requisitos de segurança. A forma como os usuários interagem com mudanças de senha, reconfigurações e funções de bloqueio e desbloqueio de conta pode ser customizada e permitida ou proibida com base em políticas configuráveis. O IBM Security Access Manager for Enterprise Single Sign-On concede às empresas a flexibilidade para decidir se essas funções de serviço de conta e senha serão designadas ao help desk, ao usuário ou a uma combinação de ambos. A função de reconfiguração de senha fornece a capacidade de reconfigurar a senha do IBM Security Access Manager for Enterprise Single Sign-On para resgatar o acesso ao ambiente de desktop. Ele não reconfigura nenhuma senha específica de aplicativo.

- Demonstrando conformidade por meio de auditoria e relatório

  O IBM Security Access Manager for Enterprise Single Sign-On inclui auditoria e relatório integrados para atividades do usuário de baixa granularidade no desktop corporativo. Ele pode registrar eventos de auditoria, incluindo o login e o logout do usuário nos aplicativos. O mecanismo de auditoria pode ser customizado para capturar outras informações relevantes que estão relacionadas com as atividades do usuário. O produto é enviado com vários relatórios incluídos, mas os relatórios customizados podem ser gerados porque todos os dados de auditoria estão em um único banco de dados relacional que pode ser consultado.

- Fácil de implementar

  A implementação e o gerenciamento do IBM Security Access Manager for Enterprise Single Sign-On são efetivos com um console administrativo baseado na web, integração superior de diretórios e software do lado do cliente facilmente implementável. Todas as funções administrativas são executadas a partir de um console administrativo da web centralizado (AccessAdmin). Os assistentes de apontar-e-clicar no aplicativo AccessStudio conduzem o administrador pelas tarefas de configuração de perfil. Um administrador pode acessar o console AccessAdmin a partir de qualquer lugar em que um navegador da web possa se conectar ao servidor. O IBM Security Access Manager for Enterprise Single Sign-On usa um repositório do usuário pré-existente sem a necessidade de modificar o esquema de diretório e qualquer outro aspecto do repositório do usuário.

- Alto desempenho

  Em todos os ambientes de desktop particulares, compartilhados e móveis, o IBM Security Access Manager for Enterprise Single Sign-On apresenta velocidade inflexível. Ele usa o mínimo de recursos ao fornecer experiência de conexão única (SSO) dos usuários com os aplicativos. Com seu uso de recurso específico de evento, o efeito do IBM Security Access Manager for Enterprise Single Sign-On no cliente e na rede é mínimo. Nenhum hardware ou software adicional é necessário.

- Integração com um sistema de gerenciamento de identidade corporativo

  O IBM Security Access Manager for Enterprise Single Sign-On Provisioning Bridge estende os benefícios que são gerados pelo IBM Security Access Manager for Enterprise Single Sign-On por meio da automação do processo de distribuição de credencial. O IBM Security Access Manager for Enterprise Single Sign-On Provisioning Bridge usa suas bibliotecas de API para permitir que o software de gerenciamento de identidade forneça automaticamente as credenciais do usuário do IBM Security Access Manager for Enterprise Single Sign-On. Dessa forma, os usuários nunca precisam saber seu nome de usuário ou senha para seus aplicativos porque eles são gerenciados de modo transparente.

  Se o usuário precisar saber seu nome de usuário e sua senha para um determinado aplicativo, ele poderá obter essas informações acessando o armazenamento de credencial (carteira eletrônica). Esse acesso só é possível se ele estiver autenticado no IBM Security Access Manager for Enterprise Single Sign-On. Se ele não estiver trabalhando em uma estação de trabalho com um AccessAgent, ele poderá acessar essas informações usando a interface com o usuário baseada no navegador da web AccessAssistant. Mesmo se não estiver integrado ao software de gerenciamento de identidade, o IBM Security Access Manager for Enterprise Single Sign-On permite um processo de revelação de senha seguro e altamente disponível por meio desses componentes.

- Trazendo a SSO para quiosques e desktops virtuais

  Infelizmente a comodidade do compartilhamento de uma mesma estação de trabalho entre várias pessoas vem acompanhada de riscos. Muitas vezes os usuários saem de um quiosque sem efetuar logoff, expondo potencialmente dados sensíveis. O IBM Security Access Manager for Enterprise Single Sign-On aborda essa ameaça com sua capacidade de automatizar a finalização de sessões inativas e encerramento de aplicativo. Essa automação inclui recursos como logout automático de usuário ausente, por meio de chaves de proximidade Radio Frequency Identification (RFID) ou remoção de cartão inteligente.

  O IBM Security Access Manager for Enterprise Single Sign-On fornece suporte ao gerenciamento robusto para implementações em desktop móvel. Ele usa tecnologias, como Microsoft Windows Terminal Services e Citrix XenApps, e desktops ou quiosques compartilhados e desktops particulares. Os usuários podem se mover de maneira fácil e segura de uma estação de trabalho para outra. O IBM Security Access Manager for Enterprise Single Sign-On also inclui suporte para proteger tecnologias Virtual Desktop Infrastructure (VDI), como VMware View. Além disso, o IBM Security Access Manager for Enterprise Single Sign-On inclui acesso thin client e sem cliente por meio do modo de desktop móvel e Web Workplace.

Arquitetura da solução

O IBM Security Access Manager for Enterprise Single Sign-On fornece sua funcionalidade de SSO introduzindo uma camada que autentica um usuário uma vez e depois detecta e manipula automaticamente solicitações subsequentes para credenciais do usuário.

O IBM Security Access Manager for Enterprise Single Sign-On pode ser dividido nos seguintes componentes de arquitetura, conforme ilustrado na Figura 1:

- Fatores de autenticação

  O IBM Security Access Manager for Enterprise Single Sign-On suporta vários fatores de autenticação para autenticar um usuário. Além da autenticação padrão baseada em senha e nome de usuário, o usuário pode ser autenticado por um badge de proximidade ou crachá. Os exemplos são RFID ativo ou passivo, impressão digital, senha descartável (OTP) fornecida por Serviço de Mensagens Curtas (SMS) ou token OTP ou token USB.

- AccessAgent

  AccessAgent é executado em cada terminal de desktop Windows, sessão do Windows Server Terminal Services, sessão de interface de desktop virtual VMware vSphere e sessão do Citrix XenApp Presentation Server. O AccessAgent é responsável pela autenticação do usuário. Ele pode automatizar a SSO no Windows e no conjunto de aplicativos definidos no AccessProfiles. O AccessAgent pode estender a cadeia de biblioteca de links dinâmicos (DLL) do Windows Graphical Identification and Authentication (GINA) para fornecer funções adicionais para autenticação forte ou autoatendimento.

- Carteira Eletrônica de Identidade

  A Carteira Eletrônica de Identidade (ou Carteira Eletrônica) retém as credenciais do usuário que são requeridas para SSO. Ela é carregada do IBM IMS™ Server no AccessAgent após uma autenticação bem-sucedida do usuário, de modo que fique disponível mesmo quando o terminal estiver desconectado da rede do computador. Para proteger as credenciais contra violação e deturpação, a Carteira Eletrônica de Identidade é criptografada com mecanismo de criptografia avançada.

- Servidor IMS

  O Servidor IMS é o armazenador central de dados do usuário, AccessProfiles, Carteiras Eletrônicas de Identidade e perfis de máquina. O servidor IMS fornece uma interface baseada na web para administrar usuários e políticas.

Cenários de uso

Neste cenário de uso, um provedor de assistência médica opera em várias clínicas independentes, sendo que cada uma tem seu próprio edifício e fornece assistência preventiva, cirurgia cardíaca e serviços de ambulatório. O provedor de assistência médica consiste em um grupo grande de médicos e equipe de apoio empregados diretamente pela empresa e em um grupo menor de cirurgiões independentes contratados pela empresa.

O provedor de assistência médica mantém dados financeiros e dados particulares do cliente (pacientes, parceiros de pesquisa e hospitais afiliados). A maioria dos registros é mantida em formulário eletrônico em sistemas SAP. Além disso, um email fica disponível para a equipe inteira da empresa para se comunicar internamente com pessoas de fora (pacientes e parceiros externos).

A Figura 2 mostra o diagrama de arquitetura da empresa de assistência médica, que inclui as principais linhas de comunicação entre as zonas de rede separadas.

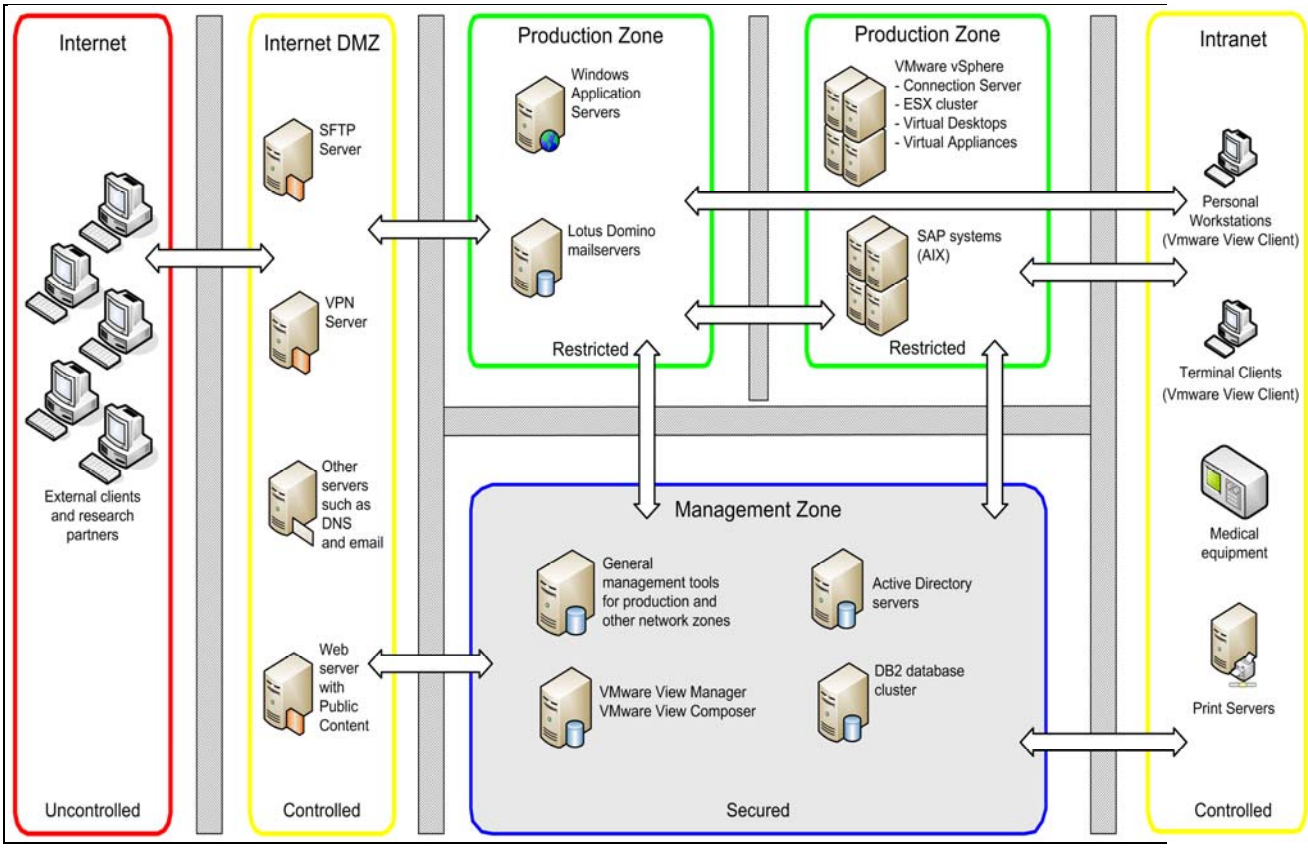

Figura 2. Atual Visão Geral da Arquitetura da Empresa de Assistência Médica

A empresa de assistência médica deseja atingir as seguintes metas de negócio a curto prazo:

- Melhorar a qualidade e a disponibilidade do atendimento ao paciente e sua satisfação, oferecendo excelente experiência de assistência médica individualizada.
- Aumentar a proteção de todas as informações relacionadas ao paciente e abordar os diferentes riscos de segurança que são acionados por requisitos de conformidade, tecnologias emergentes e explosão de dados.
- Facilitar o gerenciamento e a demonstração da postura de conformidade geral com leis de privacidade de dados e regulamentos do segmento de mercado, como Health Insurance Portability and Accountability Act (HIPAA) e Payment Card Industry Data Security Standard (PCI-DSS).

No geral, a empresa de assistência médica deseja amadurecer as soluções de segurança que podem evitar fugas de informações e assegurar autenticação confiável, além de rastreabilidade e prestação de contas individuais de todas as ações que afetam os pacientes.

Os componentes a seguir são implementados para uma implementação de nível base do IBM Security Access Manager for Enterprise Single Sign-On:

- Diretório ou repositório do usuário central

  O repositório do usuário central pode ser um dos vários repositórios suportados, incluindo Active Directory, Novell e Lightweight Directory Access Protocol (LDAP) genérico. O repositório do usuário central deve estar em vigor antes da instalação de qualquer componente do IBM Security Access Manager for Enterprise Single Sign-On. No ambiente da empresa de assistência médica, o repositório do usuário central é o Active Directory, conforme mostrado na Figura 2.

- Servidor IMS

  O Servidor IMS é um aplicativo baseado em Java que é executado em sua própria instância do IBM WebSphere® Application Server. Ele pode ser uma instalação de software em uma plataforma de servidor Windows ou ser integrado a um dispositivo virtual compactado. O Servidor IMS é implementado na Zona de Gerenciamento mostrada na Figura 2.

- Banco de Dados IMS

  O banco de dados IMS armazena todos os dados de configuração, de política e do usuário para o IBM Security Access Manager for Enterprise Single Sign-On. Esse banco de dados pode ser criado em um servidor de banco de dados existente ou ser instalado no mesmo sistema que o Servidor IMS. Os bancos de dados suportados incluem IBM DB2®, Microsoft SQL e Oracle. No ambiente da empresa de assistência médica, um banco de dados do DB2 existente é usado como banco de dados, conforme mostrado na Figura 2.

- AccessAgent

  Um AccessAgent é instalado em cada sistema do cliente, Windows Terminal Server, VMware Virtual Desktop e Citrix XenApp Server que devem ser gerenciados pelo IBM Security Access Manager for Enterprise Single Sign-On.

- AccessStudio

  AccessStudio é uma ferramenta administrativa usada para criar AccessProfiles. Ele deve ser instalado em apenas uma estação de trabalho, normalmente a de um ou mais administradores de Servidor IMS. Como o AccessStudio requer AccessAgent, você instala o AccessAgent na mesma estação de trabalho antes de instalar o AccessStudio.

Após implementar os componentes da infraestrutura base, o provedor de assistência médica implementa os seguintes recursos:

- Autoatendimento de senha

  Se os usuários na empresa de assistência médica esquecerem sua senha da Microsoft Windows, eles deverão entrar em contato com a central de suporte de TI para que a equipe da central de suporte reconfigure a senha em seus nomes após executar as verificações de segurança necessárias. O IBM Security Access Manager for Enterprise Single Sign-On supera esse problema fornecendo a função de autoatendimento de senha do produto. Os usuários que têm uma conexão com o Servidor IMS podem reconfigurar suas próprias senhas.

Ao usar o recurso de autoatendimento de senha do IBM Security Access Manager for Enterprise Single Sign-On, os usuários podem reconfigurar sua autenticação primária a partir de qualquer estação de trabalho com base no processo de resposta de segurança. (A autenticação primária pode ser a senha do IBM Security Access Manager for Enterprise Single Sign-On ou senha do desktop.) Todas as perguntas são customizáveis e configuráveis. Quando o autoatendimento de senha do IBM Security Access Manager for Enterprise Single Sign-On é configurado (nenhum componente adicional deve ser instalado), o usuário não precisa ligar para o suporte técnico. Além disso, o usuário não precisa esperar um administrador reconfigurar a senha. Em vez disso, os usuários fornecem os segredos secundários que configuraram durante a fase de inscrição do AccessAgent. Nenhum componente adicional deve ser instalado para usar a função de autoatendimento de senha.

- Autenticação forte usando RFID

  A empresa de assistência médica deseja usar uma forma segura de fazer a *troca rápida de usuário* para sua equipe médica. Esses usuários, que usam os clientes de terminal compartilhados que estão espalhados pelos hospitais, precisam de uma maneira mais rápida e conveniente de efetuarem logon no sistema. A equipe médica geralmente precisa atualizar o registro do paciente com alguns breves comentários antes de atender o próximo paciente, mas precisa fazer esses comentários todos os dias. Além disso, a equipe médica precisa inserir seu nome de usuário e senha (complexa) várias vezes por dia para acessar o ambiente de desktop virtual, o que causa frustração. A empresa se comprometeu a corrigir esse problema. No entanto, ela não quer comprometer a segurança.

  A empresa de assistência médica optou por implementar leitores de badge RFID em todos os clientes de terminal compartilhados. Usando essa função, a equipe médica pode vincular seu badge de acesso RFID ao seu nome de usuário e senha de SSO. A política é projetada para solicitar que a equipe médica apresente seu badge RFID e sua senha uma vez por dia. Para o restante das mudanças, a equipe pode apresentar o badge RFID para o leitor e o logon é efetuado automaticamente na Carteira Eletrônica de SSO.

- Implementação de desktop móvel

  Quando um usuário efetua logon em uma estação de trabalho compartilhada em uma área semipública usando uma senha ou um badge RFID, uma conexão com o Desktop Virtual desse usuário é iniciada automaticamente. O processo de logon do usuário nesse Desktop Virtual deve ocorrer por meio de métodos seguros protegidos contra violação.

  Um usuário que efetuou logon em um Desktop Virtual deve estar apto para usar os aplicativos suportados, sem fornecer credenciais de autenticação. Essa função deve funcionar da mesma maneira que se os aplicativos forem executados na estação de trabalho compartilhada da qual se conectaram. Quando um usuário efetuar logoff em uma estação de trabalho compartilhada, o desktop virtual móvel e seus aplicativos deverão continuar em execução na infraestrutura virtual. As políticas de inatividade da estação de trabalho compartilhada devem ser as mais rigorosas possíveis para evitar que outras pessoas acessem uma sessão do Desktop Virtual em espera. As sessões inativas precisam serem finalizadas automaticamente.

  Os membros da equipe médica usam estações de trabalho distribuídas para efetuarem logon automaticamente usando seus badges RFID e se conectarem aos desktops virtuais que são hospedados em um VMware ESXi Server. A Figura 3 ilustra a arquitetura do componente da solução alvo.

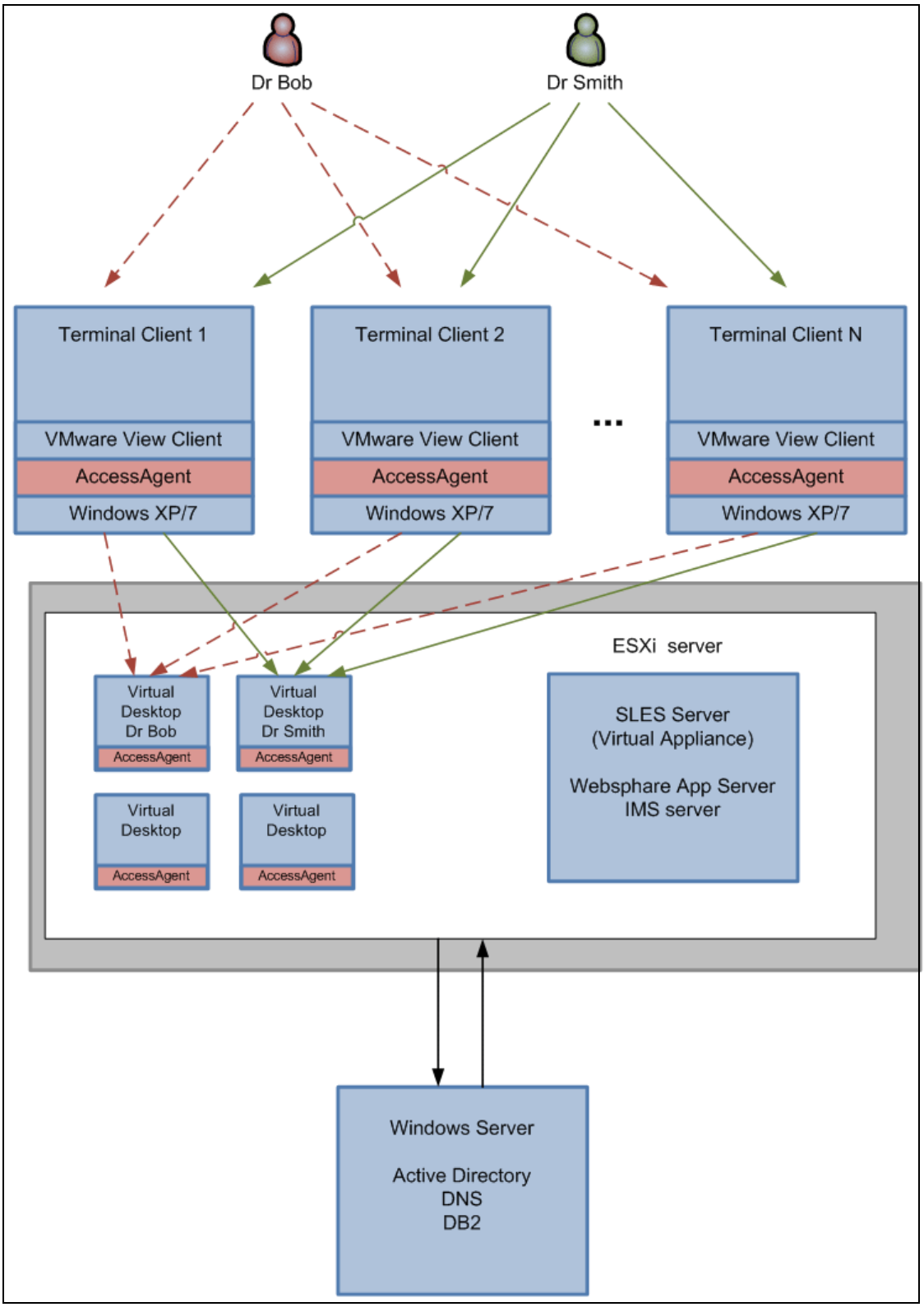

Figura 3. Arquitetura de Desktop Móvel

Informações de pedidos

Este produto está disponível apenas por meio do IBM Passport Advantage®. Ele não está disponível como um produto por contrato de adesão. As informações detalhadas sobre pedidos estão disponíveis nas cartas de anúncio da IBM (consulte a seção "Informações Relacionadas").

Informações relacionadas

Para obter mais informações, consulte os documentos a seguir:

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

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

- *A Guide to Authentication Services in IBM Security Access Manager for Enterprise Single Sign-On*, REDP-4835
  http://www.redbooks.ibm.com/abstracts/redp4835.html?Open

- *A Guide to Writing Advanced Access Profiles for IBM Tivoli Access Manager for Enterprise Single Sign-On*, REDP-4767
  http://www.redbooks.ibm.com/abstracts/redp4767.html?Open

- *Setup and Configuration for IBM Tivoli Access Manager for Enterprise Single Sign-On 8.1 for Single-Server and Cluster Environments*, REDP-4700
  http://www.redbooks.ibm.com/abstracts/redp4700.html?Open

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

- Cartas de anúncio da IBM e manuais de vendas
  http://www.ibm.com/common/ssi/index.wss?request_locale=en

  Nesta página, insira `IBM Security Access Manager for Enterprise Single Sign-On` e clique em **Procurar**. Na próxima página, estreite seus resultados de procura por tipo de informações, geografia, idioma ou todas as três opções.

Avisos

Estas informações foram desenvolvidas para produtos e serviços oferecidos nos Estados Unidos.

É possível que a IBM não ofereça os produtos, serviços ou recursos discutidos nesta publicação em outros países. Consulte um representante IBM local para obter informações sobre produtos e serviços disponíveis atualmente em sua área. Qualquer referência a produtos, programas ou serviços IBM não significa que apenas produtos, programas ou serviços IBM possam ser utilizados. Qualquer produto, programa ou serviço funcionalmente equivalente, que não infrinja nenhum direito de propriedade intelectual da IBM poderá ser utilizado em substituição a este produto, programa ou serviço. Entretanto, a avaliação e verificação da operação de qualquer produto, programa ou serviço não IBM são de responsabilidade do Cliente. A IBM pode ter patentes ou solicitações de patentes pendentes relativas a assuntos tratados nesta publicação. O fornecimento desta publicação não garante ao Cliente direito algum sobre tais patentes. Pedidos de licença devem ser enviados, por escrito, para:

Gerência de Relações Comerciais e Industriais da IBM Brasil Av. Pasteur, 138-146 Botafogo Rio de Janeiro, RJ CEP 22290-240

O parágrafo a seguir não se aplica a nenhum país em que tais disposições não estejam de acordo com a legislação local: A INTERNATIONAL BUSINESS MACHINES CORPORATION FORNECE ESTA PUBLICAÇÃO "NO ESTADO EM QUE SE ENCONTRA", SEM GARANTIA DE NENHUM TIPO, SEJA EXPRESSA OU IMPLÍCITA, INCLUINDO, MAS NÃO SE LIMITANDO, ÀS GARANTIAS IMPLÍCITAS DE NÃO INFRAÇÃO, COMERCIALIZAÇÃO OU ADEQUAÇÃO A UM DETERMINADO PROPÓSITO. Alguns países não permitem a exclusão de garantias expressas ou implícitas em certas transações; portanto, essa disposição pode não se aplicar ao Cliente. Essas informações podem conter imprecisões técnicas ou erros tipográficos. São feitas alterações periódicas nas informações aqui contidas; tais alterações serão incorporadas em futuras edições desta publicação. A IBM pode, a qualquer momento, aperfeiçoar e/ou alterar os produtos e/ou programas descritos nesta publicação, sem aviso prévio.

Referências nestas informações a websites não IBM são fornecidas apenas por conveniência e não representam de forma alguma um endosso a esses websites. Os materiais contidos nesses websites não fazem parte dos materiais desse produto IBM e a utilização desses websites é de inteira responsabilidade do Cliente. A IBM pode utilizar ou distribuir as informações fornecidas da forma que julgar apropriada sem incorrer em qualquer obrigação para com o Cliente. As informações relativas a produtos não IBM foram obtidas junto aos fornecedores dos respectivos produtos, de seus anúncios publicados ou de outras fontes disponíveis publicamente. A IBM não testou estes produtos e não pode confirmar a precisão de seu desempenho, compatibilidade nem qualquer outra reivindicação relacionada a produtos não IBM. Dúvidas sobre os recursos de produtos não IBM devem ser encaminhadas diretamente a seus fornecedores. Estas informações contêm exemplos de dados e relatórios utilizados nas operações diárias de negócios. Para ilustrá-los da forma mais completa possível, os exemplos podem incluir nomes de indivíduos, empresas, marcas e produtos. Todos estes nomes são fictícios e qualquer semelhança com nomes e endereços utilizados por uma empresa real é mera coincidência.

Todos os dados de desempenho aqui contidos foram determinados em um ambiente controlado. Portanto, os resultados obtidos em outros ambientes operacionais podem variar significativamente. Algumas medidas podem ter sido tomadas em sistemas em nível de desenvolvimento e não há garantia de que estas medidas serão iguais em sistemas geralmente disponíveis. Além disso, algumas medidas podem ter sido estimadas por extrapolação. Os resultados reais podem variar. Os usuários deste documento devem verificar os dados aplicáveis para seu ambiente específico.

LICENÇA DE COPYRIGHT:

Estas informações contêm programas de aplicativos de amostra na linguagem fonte, ilustrando as técnicas de programação em diversas plataformas operacionais. O Cliente pode copiar, modificar e distribuir estes programas de amostra sem a necessidade de pagar à IBM, com objetivos de desenvolvimento, utilização, marketing ou distribuição de programas aplicativos em conformidade com a interface de programação de aplicativo para a plataforma operacional para a qual os programas de amostra são criados. Esses exemplos não foram testados completamente em todas as condições. Portanto, a IBM não pode garantir ou implicar a confiabilidade, manutenção ou função destes programas.

Esse documento foi criado ou atualizado em 7 de dezembro de 2012.

Envie comentários de uma das seguintes maneiras:

- Use o formulário de revisão online **Contate-nos** localizado em:
  ibm.com/redbooks
- Envie seus comentários em um e-mail para:
  redbook@us.ibm.com
- Envie seus comentários pelo correio para:
  IBM Corporation, International Technical Support Organization
  Dept. HYTD Mail Station P099
  2455 South Road
  Poughkeepsie, NY 12601-5400 U.S.A.

Este documento está disponível online em **ibm.com**/redbooks/abstracts/tips0943.html

Marcas Registradas