



Visão geral dos principais recursos:

- **Detalhado controle de acesso de acordo com a função do usuário**
- **Restrições do super usuário e delegação de direitos**
- **Prevenção contra invasão no servidor**
- **Distribuição automática de políticas**
- **Mecanismo para distribuição automática**
- **Administração centralizada e delegada**
- **Rígidas políticas e gerenciamento de senhas**
- **Completa trilha de auditoria**
- **Implementação em fases**
- **Ampla cobertura a plataformas**

Novidades

- **Solução integrada de gestão de identidade e acesso**
- **Interface web de administração**
- **Mais políticas para definição de senha**
- **Políticas predefinidas de proteção às aplicações**
- **Novas regras de reforço**
- **Suporte à LDAP externo**
- **Autenticação via PAM**
- **Suporte a novas plataformas**



Computer Associates®

eTrust™ Access Control r8

O eTrust™ Access Control protege a infra-estrutura corporativa de missão crítica e minimiza os riscos à segurança, regulando o acesso a dados corporativos confidenciais e serviços de missão crítica. Essa poderosa solução oferece controle baseado em políticas de quem está autorizado a acessar cada sistema, quando e o que a pessoa pode fazer em cada um deles. O eTrust Access Control pode ser implementado em fases e as políticas podem ser criadas, gerenciadas e distribuídas por toda a empresa.

Protegendo os ativos eletrônicos e reforçando a conformidade com a segurança

Na maioria das empresas, as informações e processos de missão crítica como transações comerciais, Web Services, informações sobre clientes e registros financeiros confidenciais ficam armazenados em servidores distribuídos. Proteger esses dados e restringir o acesso a esses serviços apresenta-se como um grande desafio, já que os sistemas operacionais nativos não oferecem segurança adequada. Com o aumento do poder de processamento e do número cada vez maior de aplicações corporativas utilizando a tecnologia da Internet, aumentou também potencialmente o risco de ameaças a esses ativos.

De acordo com relatórios anuais do CSI e FBI, o acesso interno não regulamentado é um dos principais contribuintes para ameaça à segurança, à confidencialidade dos dados e perdas financeiras eletrônicas. A isso soma-se o compartilhamento da conta do super usuário que afeta a responsabilidade e figura como um grande ponto de falha. É necessário implementar um poderoso sistema de gerenciamento, capaz para proteger os valiosos ativos eletrônicos, acabar com as falhas na segurança e ajudar na conformidade com os requisitos regulamentares.

Outra grande ameaça são os ataques de códigos maliciosos aos servidores de missão crítica. Os ciberataques como as “pestes” agora invadem as aplicações, deixando firewalls, proteção antivírus baseada em assinaturas e o gerenciamento de patches praticamente sem ação. As empresas estão deixando de lado as estratégias que prometem evitar riscos: é essencial segurança proativa para as aplicações de missão crítica.

Ambiente computacional seguro

Para atender a esses desafios, a Computer Associates International, Inc. (CA) oferece o eTrust™ Identity and Access Management.

Um componente fundamental da Gestão de Identidade e Acesso é gerenciar o acesso aos recursos críticos da empresa. O premiado eTrust Access Control permite que as empresas gerenciem centralizadamente os privilégios de acesso dos usuários e implementem políticas de segurança de forma que as pessoas certas tenham acesso às informações certas. Essa solução garante o acesso seguro aos dados e aplicações armazenados em servidores Linux, UNIX e Windows da empresa.

O eTrust Access Control oferece avançada tecnologia de prevenção contra invasão para tudo, de servidores Web a aplicações RDBMS. Pode ser implementado em fases e utilizado desde departamentos a grandes empresas. Reforça a proteção contra ataques de códigos maliciosos com gerador automatizado de regras e políticas de segurança customizáveis para qualquer aplicação corporativa.



O Controle de Acesso é especialmente importante no suporte à conformidade aos requisitos regulamentares, bem como às certificações de segurança. Muitas regulamentações sobre proteção da privacidade e da confidencialidade como SOX, HIPAA, ou certificações de segurança como a BS 7799 exigem rígido controle de acesso aos dados confidenciais, o que inclui limitação dos direitos do super usuário e na concessão dos direitos de acesso, tudo isso acompanhado por detalhados relatórios de auditoria. O eTrust Access Control oferece acesso regulado que pode ajudar as empresas a atender os requisitos regulamentares e de auditoria.

Recursos e funções diferenciados

Controle de acesso de acordo com a função do usuário.

O eTrust Access Control possibilita que os usuários acessem as informações que eles necessitam, evitando e registrando todas as solicitações de informação não-autorizadas.

- **Detalhado controle de acesso.** O eTrust Access Control oferece controle individual de acesso para cada logon ao sistema e regula o acesso aos recursos, programas, arquivos e processos, utilizando uma série de critérios bastante rígidos como horário, método de login, atributos da rede e programa de acesso.
- **Limitação do superusuário.** O eTrust Access Control é capaz de reduzir e delegar os privilégios associados a contas de superusuário:
 - "Administrador" no Windows
 - "Root" em UNIX/LinuxEsse ponto de falha nativo em cada plataforma distribuída pode ser removido para evitar abuso interno e invasões externas.
- **Administração e responsabilidade delegadas.** O eTrust Access Control elimina o excesso de privilégios com a delegação de direitos de acesso aos operadores designados do sistema.
- **Definição de caminhos.** Os usuários podem ser limitados a acessar recursos apenas através de um determinado

programa. Isso é muito interessante no caso de operadores de backup e gerentes de bancos de dados que utilizam alguns programas específicos para executar suas tarefas.

Prevenção de invasão ao servidor. O eTrust Access Control oferece proteção contra ataques do tipo "stack overflow", bloqueio de ataques de cavalos de Tróia, definição de melhores práticas de segurança e recursos de softwares de firewall que evitam invasões no sistema ou a maioria dos ataques por pestes.

- **Proteção contra ataques baseados em "stack overflow" (STOP).** STOP evita que os hackers utilizem explorações do tipo "stack overflow" que poderiam permitir a execução de comandos arbitrários para entrada em outros sistemas em rede.
- **Políticas predefinidas de melhores práticas.** O eTrust Access Control oferece exemplos de melhores práticas de segurança que podem ser instaladas nas aplicações mais populares como servidores web, servidores de bancos de dados e servidores corporativos.
- **Proteção via firewall baseada no host.** O eTrust Access Control regula as conexões de dentro e fora da rede com base nas portas, método de conexão, origens de acesso, atributos da rede e horário.

Gerenciamento de políticas. O eTrust permite que os administradores definam políticas de acesso para serem aplicadas em vários diferentes servidores em diversos domínios, garantindo que essas políticas de acesso sejam reforçadas de forma consistente em todas as plataformas.

Distribuição automatizada de políticas. O eTrust Access Control emprega infra-estrutura PMDB (Policy Model Database) para propagação automática de políticas para uma hierarquia de nós de servidores.

Combinação de políticas herdadas. É possível definir políticas que sejam resultado da combinação de outras políticas (por exemplo, políticas do sistema, políticas de aplicações, políticas de servidores web etc.) As mudanças em uma política mestre são automaticamente propagadas para os assinantes.

Gerenciamento de políticas nativo. Os administradores responsáveis pela segurança podem usar o eTrust Access Control para gerenciar a segurança de contas nativas de usuários e ACLs, reduzindo substancialmente a



necessidade de dois conjuntos de ferramentas de gerenciamento.

Grupos de perfis. O eTrust Access Control oferece uma função de modelo de política de definição de senhas de fácil implementação que permite adicionar usuários a grupos com regras predefinidas de senhas.

Melhor segurança. O eTrust Access Control integra-se perfeitamente com o sistema operacional, proibindo ignorar as verificações de autorização e com isso garantindo sua própria integridade.

- **Auto-proteção.** É praticamente impossível para os usuários atacarem, alterarem ou excluírem serviços e dados do eTrust Access Control. Ele se protege contra hackers e monitora constantemente seus processos protegidos e logs de auditoria, garantindo a integridade do seu serviço de segurança.
- **Bibliotecas personalizáveis de criptografia.** Para substituir um algoritmo de criptografia alternativo, basta que as empresas substituam o módulo utilizado para proteger a comunicação administrativa do eTrust Access Control.
- **Recursos de segurança B1.** O eTrust Access Control é capaz de definir e reforçar o acesso, com base no nível de segurança segundo os critérios do National Computer Security Council B1 (Departamento de Defesa dos Estados Unidos).

Administração. Ao gerenciar um ambiente distinto de servidores, a capacidade de ter um console central para gestão da segurança é crucial para reduzir custos e consolidar as operações redundantes. O console permite que o responsável pela segurança defina políticas centralizadamente e execute tarefas urgentes como suspender um usuário em tempo real.

- **Administração centralizada.** O eTrust Access Control permite que os usuários administrativos gerenciem centralizadamente políticas, usuários e senhas em diversos departamentos e plataformas.

- **Console de administração.** O gerenciamento das contas de usuários e das regras de acesso pode ser efetuado através de várias interfaces a escolher, incluindo web, gráfica e de linha de comando.

Gerenciamento de usuários e senhas. Quando o acesso a servidores de missão crítica que hospedam aplicações corporativas, políticas relacionadas a senhas e contas de usuários precisa ser definido de forma consistente e reforçado para garantir a atribuição correta de acesso.

- **Gerenciamento de contas de usuários.** O eTrust Access Control consegue sincronizar a criação, atualização, suspensão e revogação dos direitos do usuário em todas as versões de UNIX/Linux e Windows e isso pode ser ampliado para os pacotes de segurança para mainframe. Ele é totalmente compatível com os sistemas NIS, NIS+ e Active Directory.
- **Qualidade da senha.** O eTrust Access Control permite que uma empresa crie e reforce a qualidade da senha, incluindo sua composição, comprimento mínimo e máximo, repetição e dicionário personalizado.
- **Sincronização com senhas do mainframe.** As senhas dos usuários podem ser sincronizadas com os pacotes de segurança para mainframe (eTrust CA_ACF2 Security, eTrust CA_Top Secret Security, IBM RACF.)

Extensibilidade. O eTrust Access Control inclui recursos que suportam um ambiente heterogêneo e adaptam-se as necessidades específicas das empresas.

Implementação em fase. O eTrust Access Control pode ser instalado em um único servidor com total funcionalidade e chegar a uma implementação em larga escala. Ele também se integra, de forma transparente, com a infraestrutura IAM do eTrust para configuração completa de gestão de Identidade e Acesso.

Suporte multiplataforma. Os administradores podem definir uma única política que pode ser aplicada a qualquer combinação de sistemas e aplicações Windows, UNIX ou Linux.

PAM (Pluggable Authentication Module). As empresas podem instalar um mecanismo customizado para autenticação de administradores do eTrust Access Control.



Auditoria segura e flexível. Uma segurança abrangente precisa incluir um registro completo e confiável das atividades de cada pessoa. O eTrust Access Control é capaz de auditar todos os eventos de segurança e imediatamente ativar alertas e medidas no caso de um incidente.

- **Trilha de auditoria de identidade.** O eTrust Access Control possui seu próprio log de auditoria e por isso consegue controlar a identidade do usuário mesmo que ele tente uma operação suspeita. O log mantém um trilha completa de todas as ações do usuário: do login ao logout.
- **Integridade do arquivo de log.** O eTrust Access Control protege seus logs de auditoria e logs de evento contra qualquer tentativa de invasão. Apenas as pessoas com função de auditores conseguem acessar os arquivos, e somente no modo de leitura, garantindo dessa forma a qualidade legal dos mesmos.
- **Encaminhamento de logs.** O eTrust Access Control consegue encaminhar logs de diferentes origens do eTrust Access Control para um servidor remoto, protegendo assim a integridade e análise desses logs.
- **Integração com o eTrust Security Command Center.** O registro dos eventos de acesso é um item importante na estratégia de gestão da segurança. Os eventos do eTrust Access Control podem ser monitorados e gerenciados pelo eTrust Security Command Center e consolidados em uma completa auditoria de identidade que abrange toda a rede, segurança, aplicações e operações.

Ampla cobertura de plataformas. O eTrust Access Control protege uma ampla variedade de plataformas de servidores em ambientes distribuídos.

- **Linux.** Linux x86, Linux 390 (RedHat e SuSE), assim como Linux Advanced Server e servidores VMWare ESX servers.
- **UNIX.** AIX, HP-UX, SUN Solaris, Sun Solaris/x86, HP Tru64, Dynix/Sequent, NCR MP-RAS, Silicon Graphics/IRIX e SCO/UNIXWare.

- **Windows.** Windows NT, Windows 2000, Windows 2003 e XP.

Novo Integração com eTrust Identity and Access Management. As empresas precisam gerenciar as identidades de ponta a ponta. O eTrust Access Control, componente do eTrust Identity and Access Management, protege aplicações e dados corporativos de missão crítica e controla o acesso dos usuários a essas aplicações e dados. O eTrust Access Control integra-se com recursos de provisionamento e auditoria de alto nível para total gerenciamento de identidade e acesso.

Novo Console de administração baseada na web. O eTrust Access Control agrega uma interface web de gerenciamento às existentes consoles Windows, Motif e de linha de comando. Integra-se perfeitamente com o portal de administração eTrust Identity and Access Management.

Novo Suporte à LDAP externo. Várias empresas estão migrando para centralização dos dados relacionados aos usuários em repositórios baseados em LDAP. O eTrust Access Control opera com repositórios de usuário LDAP externos como banco de dados de usuários para a criação, atualização, suspensão e revogação de contas de usuários.

Novo Sistema de gerenciamento de políticas. O eTrust Access Control Access Control agora oferece um novo sistema independente de gerenciamento de políticas que permite aos administradores gerenciar, com facilidade, políticas de segurança departamentais, com recursos de controle de versão, distribuição e download remoto dessas políticas, garantindo assim que todos os servidores tenham sempre as políticas de segurança mais recentes e facilitando o controle das versões.

Novo Gerador de políticas para aplicações. Um programa para geração automática de políticas verifica os comportamentos das aplicações e gera as devidas políticas de segurança. Ele cria uma proteção de segurança para as aplicações, ajudando a reduzir substancialmente as tarefas de criação dessas regras.



Novo Aprimoramentos operacionais.

- **Backup rápido e confiável do banco de dados.** É possível fazer backup do banco de dados do eTrust Access Control para um outro diretório, sem interromper o processamento.
- **Pacote nativo de instalação.** O novo formato RPM dos arquivos de instalação do eTrust Access Control oferece mais flexibilidade na instalação, consultas e atualizações.

Novo Segurança no modo de

manutenção. Quando o eTrust Access Control está no modo de manutenção, todos os eventos de acesso são negados para garantir a segurança durante o período de inatividade do eTrust Access Control.

Como líder no mercado de Gestão de Identidade e Acesso, o eTrust Access Control oferece segurança do mais alto nível aos servidores, protegendo contra ameaças internas e externas e ajudando as empresas a atender os requisitos de auditoria e regulamentares.

Para obter mais informações, ligue para 1-800-875-9659, ou acesse ca.com



Computer Associates®