Novell® Sentinel™

5.1.3

www.novell.com

Volume II – GUIA DO USUÁRIO DO SENTINEL

7 de julho de 2006

Novell®

Informações legais

A Novell, Inc. não faz representações ou garantias quanto ao conteúdo ou à utilização desta documentação e especificamente se isenta de quaisquer garantias de comercialização explícitas ou implícitas ou adequação a qualquer propósito específico. Além disso, a Novell, Inc. reserva-se o direito de revisar esta publicação e fazer mudanças em seu conteúdo a qualquer momento, sem obrigação de notificar qualquer pessoa ou entidade sobre essas revisões ou mudanças.

A Novell, Inc. não representa nem garante nenhum software e especificamente se isenta de qualquer garantia explícita ou implícita de comercialização ou adequação a qualquer propósito específico. A Novell, Inc. reserva-se o direito de mudar qualquer parte do software da Novell a qualquer momento, sem ter a obrigação de notificar nenhuma pessoa ou entidade sobre tais mudanças.

Quaisquer produtos ou informações técnicas sob este Contrato estão sujeitos aos controles de exportação vigentes nos Estados Unidos e à legislação comercial de outros países. Você concorda em cumprir todos os regulamentos do controle de exportação e em obter as licenças ou a classificação necessárias para exportar, reexportar ou importar produtos finais. Você concorda em não exportar nem reexportar para entidades que constem nas listas atuais de exclusão de exportação dos Estados Unidos ou para qualquer país embargado ou com histórico de terrorismo, como especificam as leis de exportação norte-americanas. Você concorda em não utilizar os produtos finais em atividades proibidas, relacionadas a mísseis, equipamentos nucleares e armas químico-biológicas. Consulte o site www.novell.com/info/exports/ para obter mais informações sobre a exportação do software da Novell. A Novell não assumirá qualquer responsabilidade se você não obtiver as aprovações necessárias para exportação.

A Novell, Inc. possui os direitos de propriedade intelectual com relação à tecnologia utilizada no produto descrito neste documento. Em particular, e sem limitação, esses direitos de propriedade intelectual podem incluir uma ou mais patentes americanas listadas em http://www.novell.com/company/legal/patents/ e uma ou mais patentes adicionais ou pedidos de patentes pendentes nos EUA e em outros países.

Novell, Inc.
404 Wyman Street, Suite 500
Waltham, MA 02451
EUA
http://www.novell.com

Documentação Online: Para acessar a documentação online deste produto e de outros produtos da Novell e obter atualizações,visite www.novell.com/documentation.

Marcas registradas da Novell

Para obter informações sobre as marcas registradas da Novell, consulte a lista Marcas registradas da Novell e marcas de serviços em (http://www.novell.com/company/legal/trademarks/tmlist.html).

Materiais de terceiros

Todas as marcas registradas de terceiros pertencem aos seus respectivos proprietários.

Informações legais de terceiros

O Sentinel 5 pode conter as seguintes tecnologias de terceiros:

- Apache Axis e Apache Tomcat, Copyright © 1999 a 2005, Apache Software Foundation. Para obter mais informações, isenções de responsabilidade e restrições, consulte http://www.apache.org/licenses/
- ANTLR. Para obter mais informações, isenções de responsabilidade e restrições, consulte http://www.antlr.org
- Boost, Copyright © 1999, Boost.org.
- Bouncy Castle, Copyright © 2000-2004, the Legion of Bouncy Castle. Para obter mais informações, isenções de responsabilidade e restrições, consulte http://www.bouncycastle.org.
- Checkpoint. Copyright © Check Point Software Technologies Ltd.
- Concurrent, pacote de utilitários. Copyright © Doug Lea. Usado sem as classes CopyOnWriteArrayList e ConcurrentReaderHashMap.
- Crypto++ Compilation. Copyright © 1995-2003, Wei Dai, incorporando o seguinte trabalho protegido por lei de direitos autorais: mars.cpp por Brian Gladman e Sean Woods. Para obter mais informações, isenções de responsabilidade e restrições, consulte http://www.eskimo.com/~weidai/License.txt.
- Crystal Reports Developer e Crystal Reports Server. Copyright © 2004 Business Objects Software Limited.
- DataDirect Technologies Corp. Copyright © 1991-2003.
- edpFTPj, licenciado sob a Licença Pública GNU Menos Restritiva. Para obter mais informações, isenções de responsabilidade e restrições, consulte http://www.enterprisedt.com/products/edtftpj/purchase.html.
- Enhydra Shark, licenciado sob a Licença Pública GNU Menos Restritiva, disponível em: http://shark.objectweb.org/license.html.
- ICEsoft ICEbrowser. ICEsoft Technologies, Inc. Copyright © 2003-2004.
- ILOG, Inc. Copyright © 1999-2004.
- Installshield Universal. Copyright © 1996–2005, Macrovision Corporation e/ou Macrovision Europe Ltd.
- Java 2 Platform, Standard Edition. Copyright © Sun Microsystems, Inc. Para obter mais informações, isenções de responsabilidade e restrições, consulte http://java.sun.com/j2se/1.4.2/j2re-1_4_2_10-license.txt.

  O Java 2 Platform também pode conter os seguintes produtos de terceiros:

  - CoolServlets © 1999
  - DES e 3xDES © 2000 por Jef Poskanzer
  - Crimson © 1999-2000 The Apache Software Foundation
  - Xalan J2 © 1999-2000 The Apache Software Foundation
  - NSIS 1.0j © 1999-2000 Nullsoft, Inc.
  - Eastman Kodak Company © 1992

- Lucinda, uma marca comercial registrada ou marca registrada da Bigelow e Holmes
- Taligent, Inc.
- IBM, algumas partes disponíveis em: http://oss.software.ibm.com/icu4j/

Para obter mais informações sobre essas tecnologias de terceiros e suas isenções de responsabilidade e restrições associadas, consulte: http://java.sun.com/j2se/1.4.2/j2se-1_4_2-thirdpartylicensereadme.txt.

- JavaBeans Activation Framework (JAF). Copyright © Sun Microsystems, Inc. Para obter mais informações, isenções de responsabilidade e restrições, consulte http://www.java.sun.com/products/javabeans/glasgow/jaf.html e clique em download > license.
- JavaMail. Copyright © Sun Microsystems, Inc. Para obter mais informações, isenções de responsabilidade e restrições, consulte http://www.java.sun.com/products/javamail/downloads/index.html e clique em download > license.
- Java Ace, por Douglas C. Schmidt e seu grupo de pesquisa na Washington University e Tao (com agrupadores ACE) por Douglas C. Schmidt e seu grupo de pesquisa em Washington University, University of California, Irvine e Vanderbilt University. Copyright © 1993-2005.Para obter mais informações, isenções de responsabilidade e restrições, consulte http://www.cs.wustl.edu/~schmidt/ACE-copying.html e http://www.cs.wustl.edu/~pjain/java/ace/JACE-copying.html
- Java Authentication e Authorization Service Modules, licenciados sob a Licença Pública Geral Menos Restritiva. Para obter mais informações, isenções de responsabilidade e restrições, consulte http://free.tagish.net/jaas/index.jsp.
- Java Network Launching Protocol (JNLP). Copyright © Sun Microsystems, Inc. Para obter mais informações, isenções de responsabilidade e restrições, consulte http://www.java.sun.com/products/javawebstart/downloads-jnlp.html e clique em download > license.
- Java Service Wrapper. Partes protegidas por lei de direitos autorais da seguinte maneira: Copyright © 1999, 2004 Tanuki Software e Copyright © 2001 Silver Egg Technology. Para obter mais informações, isenções de responsabilidade e restrições, consulte http://wrapper.tanukisoftware.org/doc/english/license.html.
- JIDE. Copyright © 2002 a 2005, JIDE Software, Inc.
- O jTDS é licenciado sob a Licença Pública GNU Menos Restritiva. Para obter mais informações, isenções de responsabilidade e restrições, consulte http://jtds.sourceforge.net/.
- MDateSelector. Copyright © 2005, Martin Newstead, licenciado sobre a Licença Pública Geral Menos Restritiva. Para obter mais informações, isenções de responsabilidade e restrições, consulte http://web.ukonline.co.uk/mseries.
- Monarch Charts. Copyright © 2005, Singleton Labs.
- Net-SNMP. Partes do código são protegidas por lei de direitos autorais por várias entidades, que se reservam todos os direitos. Copyright © 1989, 1991, 1992 por Carnegie Mellon University; Copyright © 1996, 1998 a 2000, the Regents of the University of California; Copyright © 2001 a 2003 Networks Associates Technology, Inc.; Copyright © 2001 a 2003, Cambridge Broadband, Ltd.; Copyright © 2003 Sun Microsystems, Inc. e Copyright © 2003 a 2004, Sparta, Inc. Para obter mais informações, isenções de responsabilidade e restrições, consulte http://net-snmp.sourceforge.net.
- The OpenSSL Project. Copyright © 1998-2004. the Open SSL Project. Para obter mais informações, isenções de responsabilidade e restrições, consulte http://www.openssl.org.
- Oracle Help for Java. Copyright © 1994-2006, Oracle Corporation.
- RoboHELP Office. Copyright © Adobe Systems Incorporated, antiga Macromedia.
- Skin Look and Feel (SkinLF). Copyright © 2000-2006 L2FProd.com. Licenciado sob a Licença de Software do Apache. Para obter mais informações, isenções de responsabilidade e restrições, consulte https://skinlf.dev.java.net/.
- Sonic Software Corporation. Copyright © 2003-2004. O software SSC contém software de segurança licenciado pela RSA Security, Inc.

- Tinyxml. Para obter mais informações, isenções de responsabilidade e restrições, consulte http://grinninglizard.com/tinyxmldocs/index.html.
- SecurityNexus. Copyright © 2003 a 2006. SecurityNexus, LLC. Todos os direitos reservados.
- Xalan e Xerces, licenciados pela Apache Software Foundation Copyright © 1999-2004. Para obter mais informações, isenções de responsabilidade e restrições, consulte http://xml.apache.org/dist/LICENSE.txt.
- yWorks. Copyright © 2003 a 2006, yWorks.

NOTA: A partir da publicação desta documentação, os links acima se tornaram ativos. Caso você descubra que quaisquer dos links acima foram desfeitos ou que as páginas da Web vinculadas estão inativas, contate a Novell, Inc. no endereço 404 Wyman Street, Suite 500, Waltham, MA 02451 EUA.

Prefácio

A documentação técnica do Sentinel consiste no guia de referência e operação para finalidade geral. Essa documentação é destinada aos profissionais de segurança da informação. O texto foi desenvolvido para ser usado como fonte de referência sobre o Sistema de Gerenciamento de Segurança Empresarial do Sentinel. A documentação adicional está disponível no portal da Novell na Web

A documentação técnica do Sentinel está dividida em cinco volumes.São eles:

- Volume I – Guia de Instalação do Sentinel™ 5
- Volume II – Guia do Usuário do Sentinel™ 5
- Volume III – Guia do Usuário do Assistente do Sentinel™ 5
- Volume IV – Guia de Referência do Usuário do Sentinel™ 5
- Volume V – Integração de Terceiros do Sentinel™ 5

Volume I – Guia de Instalação do Sentinel

Este guia explica como instalar:

- Sentinel Server
- Console do Sentinel
- Mecanismo de Correlação do Sentinel
- Crystal Reports do Sentinel
- Construtor de Coletor Assistente
- Gerenciador de Coletor do Assistente
- Consultor

Volume II – Guia do Usuário do Sentinel

Este guia aborda o seguinte:

- Operação do Console do Sentinel
- Recursos do Sentinel
- Arquitetura do Sentinel
- Comunicação do Sentinel
- Encerramento/Inicialização do Sentine
- Avaliação de vulnerabilidade
- Monitoramento de eventos
- Filtragem de eventos
- Correlação de eventos
- Gerenciador de Dados do Sentinel
- Configuração de Eventos para Relevância Comercial
- Serviço de Mapeamento
- Geração de relatórios de histórico
- Gerenciamento de Host do Assistente
- Incidentes
- Casos
- Gerenciamento de usuários
- Workflow

Volume III – Guia do Usuário do Assistente

Este guia aborda o seguinte:

- Operação do Construtor de Coletor Assistente
- Gerenciador de Coletor do Assistente
- Coletores
- Gerenciamento de Host do Assistente
- Construção e manutenção de coletores

Volume IV – Guia de Referência do Usuário do Sentine

Este guia aborda o seguinte:

- Linguagem de criação de scripts do assistente
- Comandos de análise do Assistente
- Funções do administrador do Assistente
- Metatags do Assistente e do Sentinel
- Mecanismo de correlação do Sentinel
- Permissões de usuário
- Opções da linha de comando de correlação
- Esquema do banco de dados do Sentinel

Volume V – Guia de Integração de Terceiros do Sentinel

- Remedy
- Operações do HP OpenView
- HP Service Desk

Sumário

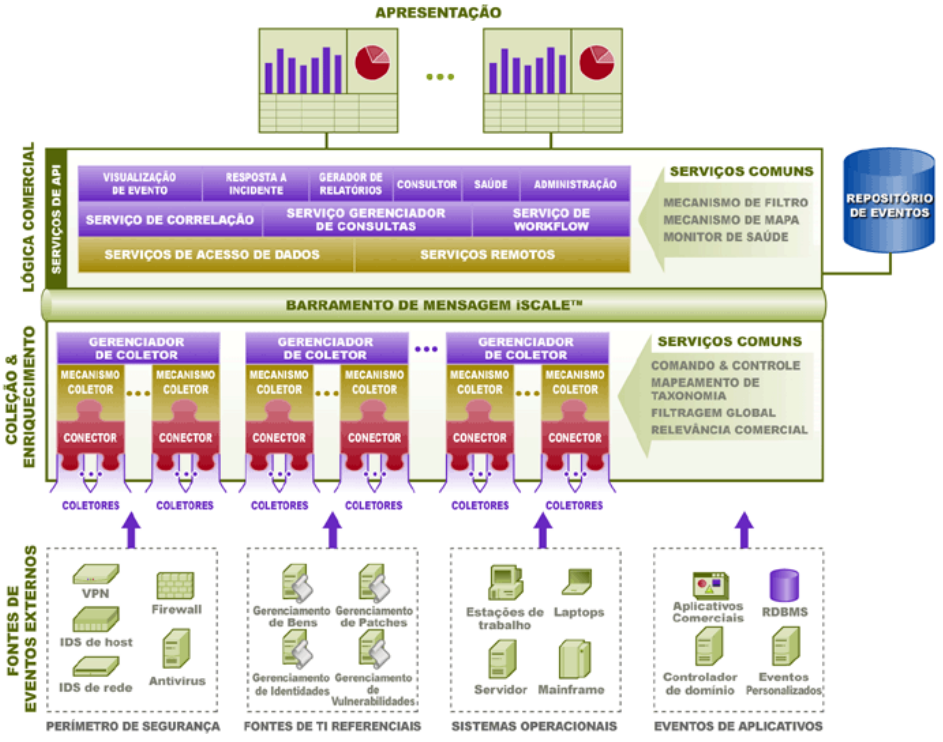
1 Introdução ao Sentinel

NOTA: O termo Agente é intercambiável com Coletor. Mais para a frente, Agentes será referido como Coletores.

O Sentinel™ 5 é a solução líder de gerenciamento de informações de segurança e monitoramento de conformidade que recebe informações coletadas de várias fontes em toda a empresa, padroniza-as, estabelece a prioridade de cada uma delas e executa a correlação de todas em tempo real. O Sentinel reúne dados de vários produtos de segurança no mercado e oferece a flexibilidade de coletar dados de novas tecnologias e produtos à medida que os requisitos empresariais e de instalações evoluem.

Muitos dos recursos do Sentinel 5 resultam da remodelagem da arquitetura do Sentinel 4.0 e estão voltados para atender às necessidades dos clientes da Novell. Com o aumento das ameaças e pressões normativas em relação à segurança, as organizações procuram uma solução que permita:

- Obter a visibilidade e as informações necessárias para gerenciar um ambiente de segurança com uma melhor relação custo-benefício.
- Monitorar continuamente a conformidade com as normas e políticas governamentais (por exemplo, Sarbanes-Oxley, HIPAA, GLBA, FISMA, NISPOM, DCID 6/3 e DITSCAP).
- Identificar e resolver incidentes com maior rapidez e economia por meio da coleta centralizada e automatizada e da resolução de dados sobre ameaças e políticas.
- Fornecer métricas operacionais e executivas para avaliar continuamente a segurança e a postura de conformidade, bem como tratar das metas táticas e estratégicas.
- Reduzir os custos operacionais associados à segurança e ao monitoramento de conformidade, identificação de incidentes e reparo.



Um evento é uma ação ou ocorrência reportada ao Sentinel. Um evento recebido de um dispositivo de segurança é chamado um evento externo e um evento gerado pelo Sentinel é chamado evento interno. Os eventos podem ser relacionados a segurança, desempenho ou informação. Por exemplo, um evento externo poderia ser um ataque detectado por um Sistema de Detecção de Intrusão (IDS, Intrusion Detection System), um login executado com êxito informado por um sistema operacional ou uma situação definida pelo cliente, como um usuário acessando um arquivo. Eventos internos são gerados pelo Sentinel para indicar uma mudança notável no estado do sistema, como um Coletor sendo interrompido ou uma regra de correlação sendo desabilitada.

Correlação é o processo de analisar eventos de segurança para identificar padrões em um evento ou um fluxo de eventos. Por exemplo, uma regra de correlação pode ser criada para detectar quando trinta ou mais eventos ICMP ocorrerem em um período de tempo de um minuto. Um tráfego de alto volume (inundação) de ICMP poderia resultar em uma recusa de ataque de serviço. A correlação pode detectar padrões em um fluxo de eventos de um único dispositivo, um conjunto de dispositivos semelhantes ou uma coleção arbitrária de dispositivos. Isso permite que o usuário faça uma melhor determinação do risco e da gravidade do incidente.

O Sentinel também incorpora informações adicionais na alimentação, como informações sobre as máquinas na rede e suas vulnerabilidades e serviços conhecidos. Essas informações são disponibilizadas em tempo real, refinando ainda mais a importância dos eventos monitorados.

O Sentinel Control Center usa processos em segundo plano para exibir em tempo real eventos e resumos de eventos (Active Views™), Incidentes, relatórios históricos (análises) e relatórios do Consultor.

Eventos considerados importantes podem ser agrupados em um objeto chamado *Incidente*. Um incidente pode ser criado manualmente pelo usuário ou automaticamente pelo mecanismo de correlação. O incidente pode conter ainda informações adicionais, recuperadas pelo componente Sentinel Advisor, sobre os bens que estão sendo atacados, as vulnerabilidades desses bens e o ataque. Também é possível que outras informações sejam incluídas como anexos.

Este guia supõe que você esteja familiarizado com os fundamentos básicos de segurança de rede, administração de bancos de dados e ambientes dos sistemas operacionais Windows e UNIX.

Este capítulo descreve a arquitetura lógica e funcional do Sentinel 5, seguida pelos módulos principais do produto.

Arquitetura funcional

O Sentinel 5 é composto de três subsistemas que formam o núcleo da arquitetura funcional:

- Plataforma do iSCALE – uma estrutura escalável orientada por eventos;
- Integração de origem de dados – uma estrutura de Coletor extensível;
- Integração de aplicativos – uma estrutura de aplicativo extensível.

O Sentinel trata "serviços" e "aplicativos" como pontos de extremidade de serviço abstratos que podem responder prontamente a eventos assíncronos. Serviços são "objetos" que não precisam entender protocolos nem como as mensagens são roteadas aos serviços de peer.

Recursos do Sentinel

O Sentinel é um aplicativo de usuário final rico em recursos que permite a monitoração e o gerenciamento de várias funções. A seguir estão algumas das principais funções:

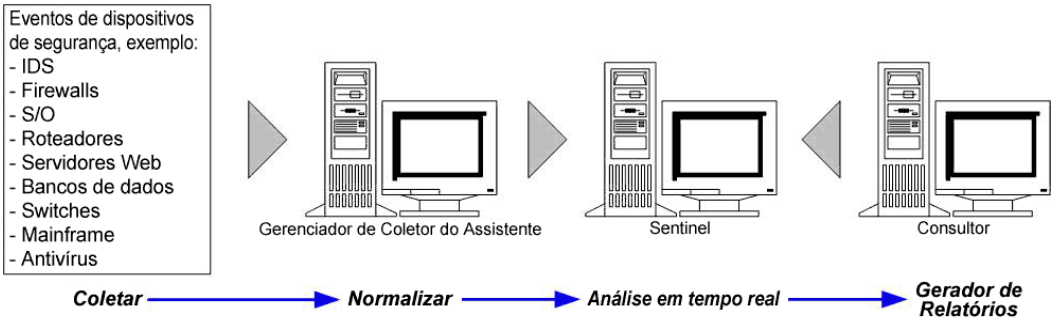
- Exibições em tempo real de grandes fluxos de eventos;
- Ferramentas para geração de relatórios baseados em eventos históricos e em tempo real;
- Controle de usuários e do que eles podem ver e fazer de acordo com a designação de permissão;
- Meios de restringir a quais eventos os usuários terão acesso;
- Organização de eventos em incidentes para permitir o gerenciamento e o monitoramento eficientes de respostas;
- Detecção de padrões em eventos e fluxos de eventos.

Visão geral da arquitetura

O sistema Sentinel é responsável por receber eventos do Gerenciador de Coletor do Assistente. Os eventos são exibidos em tempo real e registrados em um banco de dados para análise histórica.

De modo geral, o sistema Sentinel usa um banco de dados relacional e consiste em processos do Sentinel e um mecanismo de geração de relatórios. O sistema aceita eventos do gerenciador de Coletor como sua entrada. O gerenciador de Coletor trabalha em conjunto com produtos de terceiros e normaliza os dados obtidos de tais produtos. Em seguida, os dados normalizados são enviados aos processos e ao banco de dados do Sentinel.

A análise histórica e a geração de relatórios podem ser feitas com o mecanismo integrado de geração de relatórios do Sentinel. Esse mecanismo extrai os dados do banco de dados e integra as exibições de relatório no Sentinel Control Center usando documentos HTML em uma conexão HTTP.



A seguir estão os recursos do Sentinel:

- Processamento em tempo real de eventos recebidos do Gerenciador de Coletor do Assistente;
- Linguagem baseada em regras intuitiva e flexível para correlação;
- Regras compiladas para alto desempenho;
- Arquitetura escalável, classificável, extensível e com threads múltiplos.

Os processos do Sentinel comunicam-se entre si através de um MOM (Message-Oriented Middleware - Middleware Orientado por Mensagem).

Plataforma iSCALE

A arquitetura iSCALE™ do Sentinel é criada a partir de uma arquitetura SOA (Service-Oriented Architecture) baseada em padrões, que combina as vantagens do processamento na memória e da computação distribuída. O principal componente da iSCALE é um barramento de mensagens especializado, capaz de lidar com altos volumes de dados. Desenvolvida desde o início usando a mais avançada abordagem baseada em padrões, a iSCALE permite sua expansão de modo econômico.

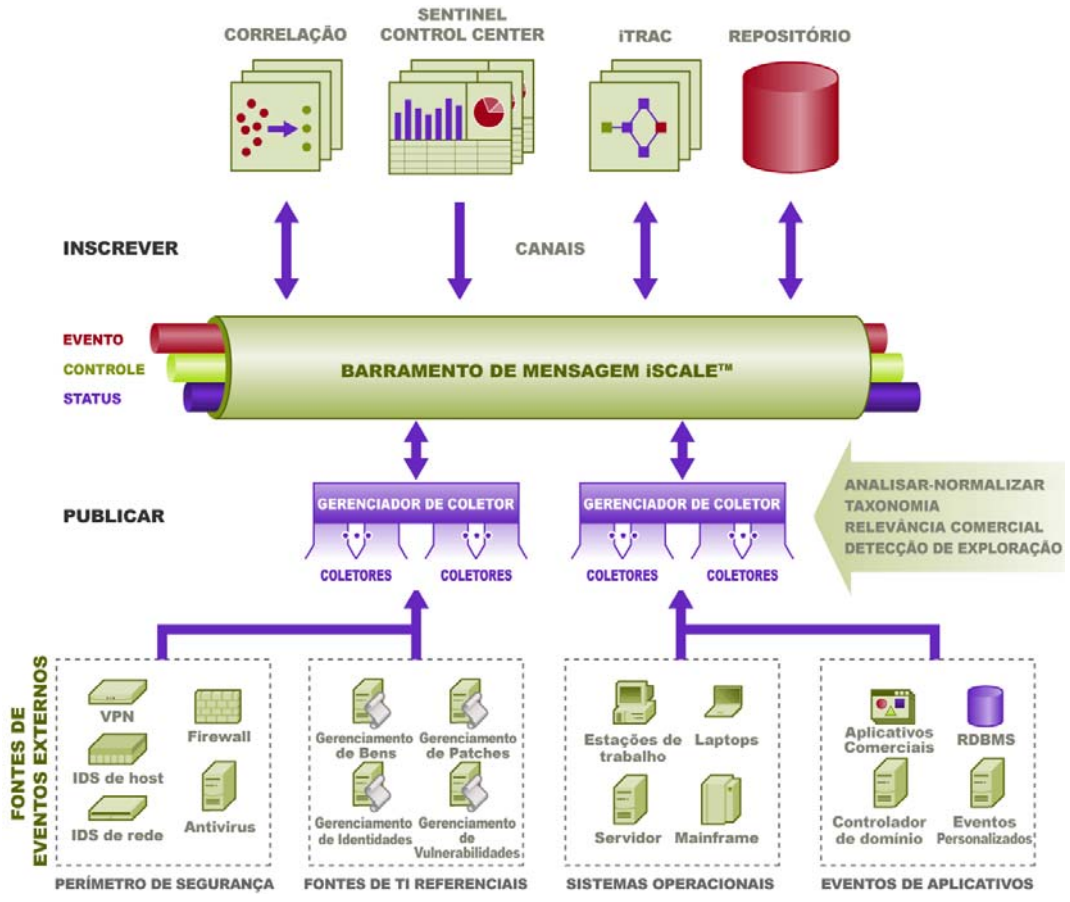
Barramento de mensagens

O barramento de mensagens da iSCALE permite escalar de modo independente os componentes individuais, ao mesmo tempo em que possibilita a integração baseada em padrões com aplicativos externos. O segredo da escalabilidade é o fato de que, ao contrário de outros softwares distribuídos, nenhum componente (peer) comunica-se com outro diretamente. Todos os componentes comunicam-se por meio do barramento de mensagens, capaz de mover milhares de pacotes de mensagens por segundo.

Ao tirar proveito dos exclusivos recursos do barramento de mensagem, o canal de comunicação de alto throughput pode maximizar e manter a alta taxa de throughput de dados que atravessam os componentes independentes do sistema. Os eventos são compactados e criptografados via cabo para distribuição segura e eficiente da borda da rede ou pontos de coleta para o hub do sistema, no qual são realizadas análises em tempo real.

O barramento de mensagens da iSCALE emprega uma série de serviços de enfileiramento que melhoram a confiabilidade da comunicação além dos aspectos de segurança e desempenho da plataforma. Com inúmeras filas transientes e permanentes, o sistema oferece confiabilidade e tolerância a falhas inigualáveis. Por exemplo, mensagens importantes em

trânsito são gravadas (ao serem colocadas em fila) em caso de falha na via de comunicação. A mensagem em fila é enviada ao destino depois que o sistema se recupera do estado de falha.



Canais

A plataforma iSCALE emprega um modelo orientado por dados ou eventos que permite escalar os componentes de todo o sistema de maneira independente e de acordo com a carga de trabalho. Isso proporciona um modelo de distribuição flexível, uma vez que o ambiente de cada cliente é diferente: um local pode ter vários dispositivos com baixos volumes de eventos, enquanto outro pode ter menos dispositivos com um alto volume de eventos. As densidades de evento (ou seja, o padrão de agregação e de multiplexação dos eventos no cabo a partir dos pontos de coleta) são diferentes nesses casos e o barramento de mensagens permite escalar de modo coerente cargas de trabalho díspares.

A iSCALE tira proveito de um ambiente independente e com canais múltiplos que praticamente elimina a contenção e promove o processamento paralelo de eventos. Esses canais e subcanais trabalham não somente para transportar dados de eventos, como também para oferecer um controle refinado de processos a fim de escalar e equilibrar a carga do sistema em condições de carga variáveis. Ao usar canais de serviço independentes, como os canais de controle e de status, além do canal de eventos principal, a iSCALE permite escalar de modo econômico e sofisticado a arquitetura orientada por eventos.

Evento do Sentinel

O Sentinel recebe informações de dispositivos, normaliza essas informações em uma estrutura chamada *Evento do Sentinel*, ou simplesmente *Evento*, e envia o evento para processamento. Os eventos são processados pela exibição em tempo real, mecanismo de correlação e servidor back end.

Um evento consiste em mais de 200 tags. As tags têm tipos e finalidades diferentes. Algumas são predefinidas, como gravidade, importância, IP de destino e porta de destino. Há dois conjuntos de tags configuráveis: tags reservadas são de uso interno da Novell para permitir uma expansão futura, e tags do cliente são para extensões do cliente.

Para mudar a finalidade de uma tag, basta renomeá-la. A origem de uma tag pode ser *referencial* ou *externa*, a qual é definida explicitamente pelo dispositivo ou pelo Coletor correspondente. O valor de uma tag referencial é computado como uma função de uma ou mais tags que usam o serviço de mapeamento. Por exemplo, uma tag pode ser definida como o código da construção que contém o bem mencionado como o IP de destino de um evento. Por exemplo, uma tag pode ser computada pelo serviço de mapeamento por meio de um mapa definido pelo cliente usando o IP de destino do evento.

Serviço de Mapeamento

O Serviço de Mapeamento permite que um mecanismo sofisticado propague dados comerciais importantes por todo o sistema. Esse recurso auxilia a escalabilidade e oferece a vantagem da extensão por meio da transferência de dados inteligente entre diferentes nós do sistema distribuído.

O Serviço de Mapeamento é um recurso de propagação de dados que permite a referência cruzada entre dados do Verificador de Vulnerabilidades e assinaturas do Sistema de Detecção de Intrusão (IDS), entre outros dados (por exemplo, dados de bens, dados importantes da empresa). Isso permite a notificação imediata em caso de tentativa de ataque para explorar um sistema vulnerável. Três componentes separados proporcionam essa funcionalidade:

- Coleta de eventos em tempo real de uma fonte de detecção de intrusão;
- Comparação dessas assinaturas com as últimas verificações de vulnerabilidade; e
- referência cruzada de uma alimentação de ataque por meio do Sentinel Advisor (um módulo opcional do produto, que efetua a referência cruzada entre assinaturas de ataque do IDS em tempo real e dados do verificador de vulnerabilidades do usuário).

O Serviço de Mapeamento propaga informações de modo dinâmico por todo o sistema sem afetar a carga do sistema. Quando conjuntos de dados importantes (ou seja, “mapas” como informações de bens ou de atualizações de patch) são atualizados no sistema, o Serviço de Mapeamento propaga por todo o sistema essas atualizações, que com freqüência consistem em centenas de megabytes.

Os algoritmos do Serviço de Mapeamento da iSCALE processam grandes conjuntos de dados referenciais através de um sistema de produção que processa grandes volumes de dados em tempo real. Esses algoritmos estão cientes das atualizações e enviam de modo seletivo apenas as mudanças ou “conjuntos de dados delta” do repositório para a borda ou perímetro do sistema.

Transmitindo mapas

O Serviço de Mapeamento emprega um modelo de atualização dinâmica e transmite os mapas de um ponto para outro, evitando o acúmulo de grandes mapas estáticos na memória dinâmica. A importância desse recurso de transmissão é especialmente relevante em um sistema em tempo real que seja vital para os negócios, como o Sentinel, no qual é preciso haver uma movimentação de dados constante, previsível e ágil, qualquer que seja a carga transiente no sistema.

Detecção de exploração (serviço de mapeamento)

O Sentinel permite a referência cruzada entre as assinaturas dos dados de eventos e os dados do Vulnerability Scanner. Os usuários são notificados de forma automática e imediata em caso de tentativa de ataque para explorar um sistema vulnerável. Isso é possível graças ao seguinte:

- Alimentação do Consultor
- Detecção de intrusão
- Verificação de vulnerabilidades
- Firewalls

O Consultor fornece uma referência cruzada entre as assinaturas de dados do evento e os dados do verificador de vulnerabilidades. O Consultor possui uma alimentação de alerta e ataque. Além disso, contém informações sobre vulnerabilidades e ameaças. A alimentação de ataque é uma normalização das assinaturas do evento e dos plug-ins de vulnerabilidade. Para obter informações sobre a instalação do Consultor, veja o Guia de Instalação do Sentinel.

Os sistemas suportados são:

Sistemas de detecção de intrusão

- Cisco Secure IDS
- Enterasys Dragon Host Sensor
- Enterasys Dragon Network Sensor
- Intrusion.com (SecureNet_Provider)
- ISS BlackICE
- ISS RealSecure Desktop
- ISS RealSecure Network
- ISS RealSecure Server
- ISS RealSecure Guard
- Snort
- Symantec Network Security 4.0 (ManHunt)
- Symantec Intruder Alert
- McAfee IntruShield

Verificadores de vulnerabilidades

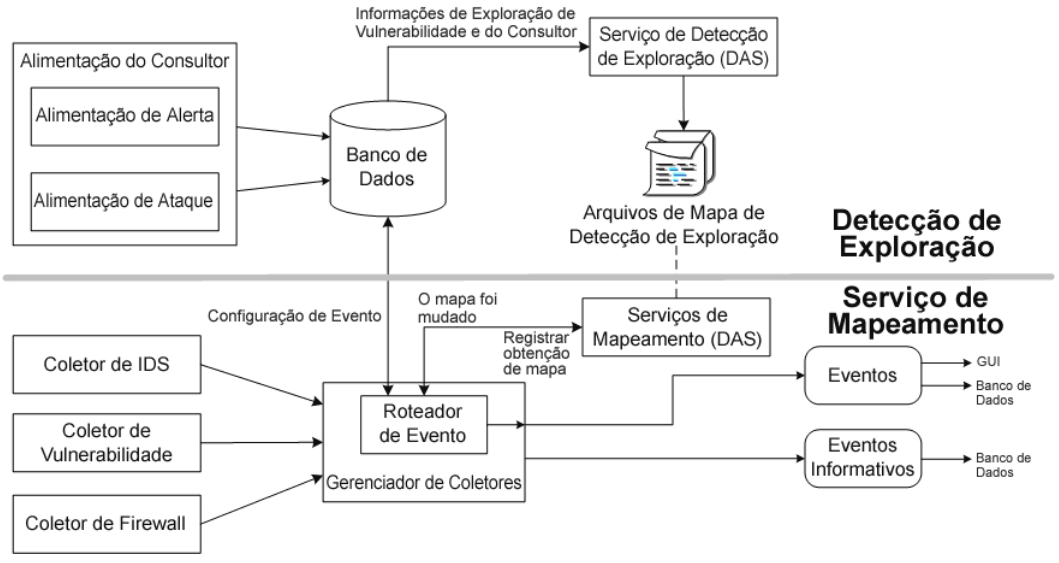
- eEYE Retina
- Foundstone Foundscan
- ISS Database Scanner
- ISS Internet Scanner
- ISS System Scanner
- ISS Wireless Scanner
- Nessus
- nCircle IP360
- Qualys QualysGuard

Firewalls.

- Cisco IOS Firewall

Você precisará de pelo menos um verificador de vulnerabilidades e um IDS ou firewall de cada categoria acima. O DeviceName (rv31) do IDS e Firewall deve aparecer no evento destacado em cinza como na tabela acima. Além disso, o IDS e Firewall devem preencher corretamente o campo DeviceAttackName (rt1) (por exemplo, WEB-PHP Mambo uploadimage.php access).

A alimentação do Consultor é enviada ao banco de dados e ao Serviço de Detecção de Exploração. Esse serviço gera um ou dois arquivos, de acordo com o tipo dos dados atualizados.



O Serviço de Mapeamento usa os arquivos de mapeamento da Detecção de Exploração para corresponder os ataques à exploração de vulnerabilidades.

Os verificadores de vulnerabilidades exploram as áreas vulneráveis do sistema (bens). O IDS detecta ataques (se houver) a essas áreas vulneráveis. Os firewalls determinam se há tráfego em direção a uma dessas áreas vulneráveis. Se um ataque for associado a qualquer vulnerabilidade, isso significa que o bem foi explorado.

O Serviço de Detecção de Exploração gera dois arquivos localizados em:

```
$ESEC_HOME/sentinel/bin/map_data
```

Os nomes desses arquivos são attackNormalization.csv e exploitDetection.csv.

O attackNormalization.csv é gerado após:

- A alimentação do Consultor;
- A inicialização do DAS (se habilitado em das_query.xml; está desabilitado por padrão).

O exploitDetection.csv é gerado após um dos seguintes processos:

- A alimentação do Consultor;
- Verificação de vulnerabilidades;
- Inicialização do Sentinel Server (se habilitado em das_query.xml; está desabilitado por padrão).

Por padrão, há duas colunas de eventos configuradas, utilizadas para detecção de exploração e referenciadas a partir de um mapa (todas as tags mapeadas terão o ícone de rolagem).

- Vulnerabilidade
- AttackID

Severity	Vulnerability	AttackId
2	0	
3	0	

Quando o campo de vulnerabilidade (*vul*) é igual a 1, o bem ou dispositivo de destino é explorado. Se o campo de vulnerabilidade (*vul*) é igual a 0, o bem ou dispositivo de destino não é explorado.

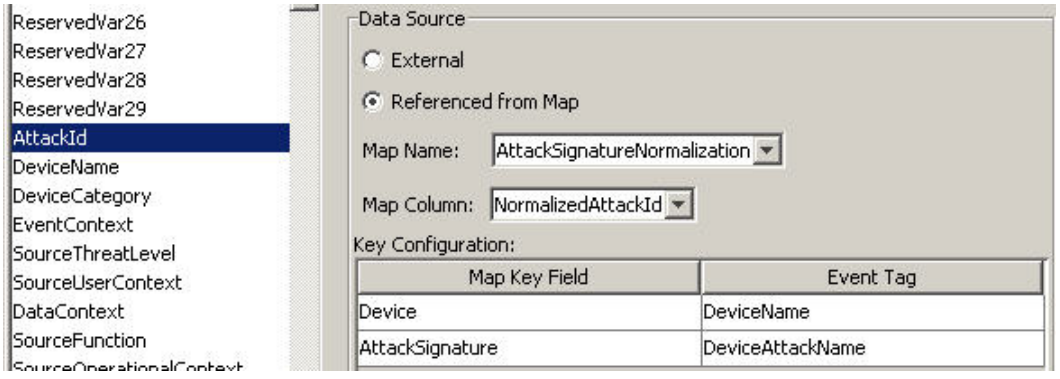
O Sentinel vem pré-configurado com os seguintes nomes de mapas associados aos arquivos attackNormalization.csv e exploitDetection.csv.

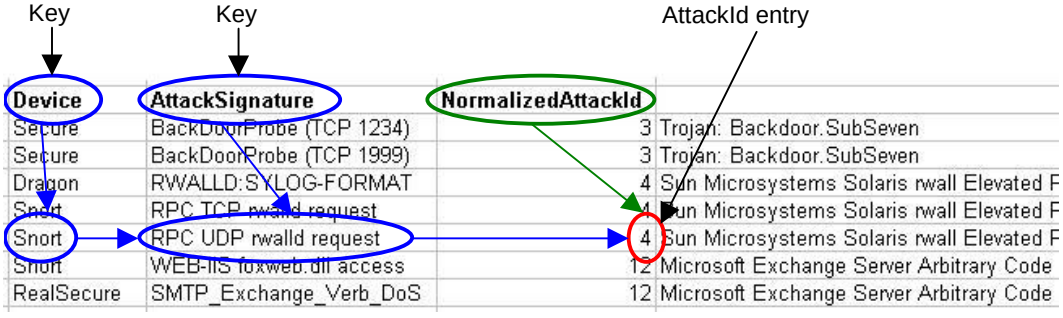
Nome do mapa	Nome do arquivo csv
▪ AttackSignatureNormalization	▪ attackNormalization.csv
▪ IsExploitWatchlist	▪ exploitDetection.csv

Existem dois tipos de origem de dados:

- Externa – recupera informações do agente;
- Referência do Mapa – recupera informações do arquivo de mapeamento para preencher a tag.

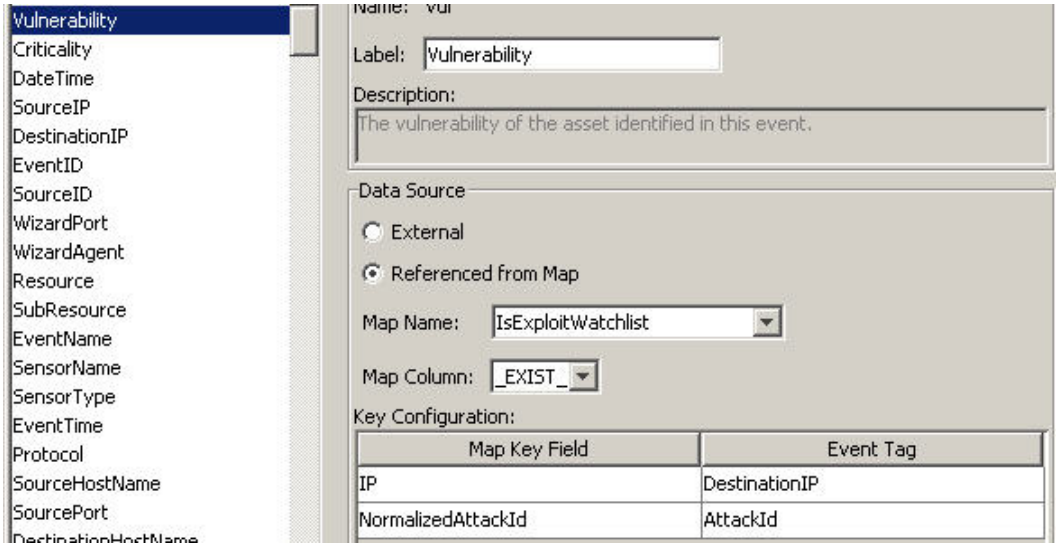
A tag AttackId contém as colunas Dispositivo (tipo de dispositivo de segurança, por exemplo, Snort) e AttackSignature definidas como Chaves e usa a coluna NormalizedAttackID no arquivo attackNormalization.csv. Em uma linha na qual a tag de evento DeviceName (um dispositivo IDS como Snort, informações preenchidas pelo Consultor e informações de vulnerabilidade obtidas do banco de dados do Sentinel) é igual ao Dispositivo e na qual a tag de evento DeviceAttackName (informações do ataque preenchidas pelo Consultor no banco de dados do Sentinel por meio do Serviço de Detecção de Exploração) é igual a AttackSignature, o valor da coluna AttackId está onde a linha encontra-se com a coluna NormalizedAttackID.





A tag Vulnerabilidade tem uma entrada de coluna "_EXIST_" que significa que o valor resultante do mapeamento será 1 se a chave estiver em IsExploitWatchlist (arquivo exploitDetection.csv) ou 0 se não estiver. As colunas de chave da tag de vulnerabilidade são IP e NormalizedAttackId. Quando um evento de entrada tem uma tag de evento DestinationIP

correspondente à entrada da coluna IP e uma tag de evento AttackId correspondente à entrada de coluna NormalizedAttackId na mesma linha, o resultado é um (1). Se nenhuma correspondência for encontrada na mesma linha, o resultado será zero (0).



Integração de origem de dados

O uso de tecnologia adaptável e flexível é crucial para a estratégia de integração de origens de dados do Sentinel, alcançada por meio de Coletores interpretativos (também chamados de Coletores) que analisam e normalizam os eventos no fluxo de dados.

Esses Coletores podem ser modificados conforme necessário e não estão vinculados a um ambiente específico. A criação, modificação, distribuição e manutenção dos Coletores são processos simples que podem ser realizados diretamente pelos usuários. Um ambiente de desenvolvimento integrado permite a criação interativa de Coletores usando um paradigma "arrastar e soltar" com base em uma interface gráfica de usuário. Usuários não programadores podem criar Coletores, garantindo o cumprimento das exigências atuais e futuras em um ambiente de TI em constante mudança. A operação de comando e controle de Coletores (por exemplo, iniciar, parar) é realizada de modo centralizado a partir do Sentinel Control Center.1

Integração de aplicativos

A integração de aplicativos externos por meio de APIs padrão é crucial para o Sentinel. Por exemplo, uma API bidirecional para sistemas de comunicação de problemas, que inclui o Remedy® e o HP OpenView ServiceDesk®, permite a integração direta com sistemas externos.

A API é baseada nos Serviços Web e, portanto, permite que qualquer sistema externo compatível com SOAP aproveite a integração total com o sistema Sentinel.

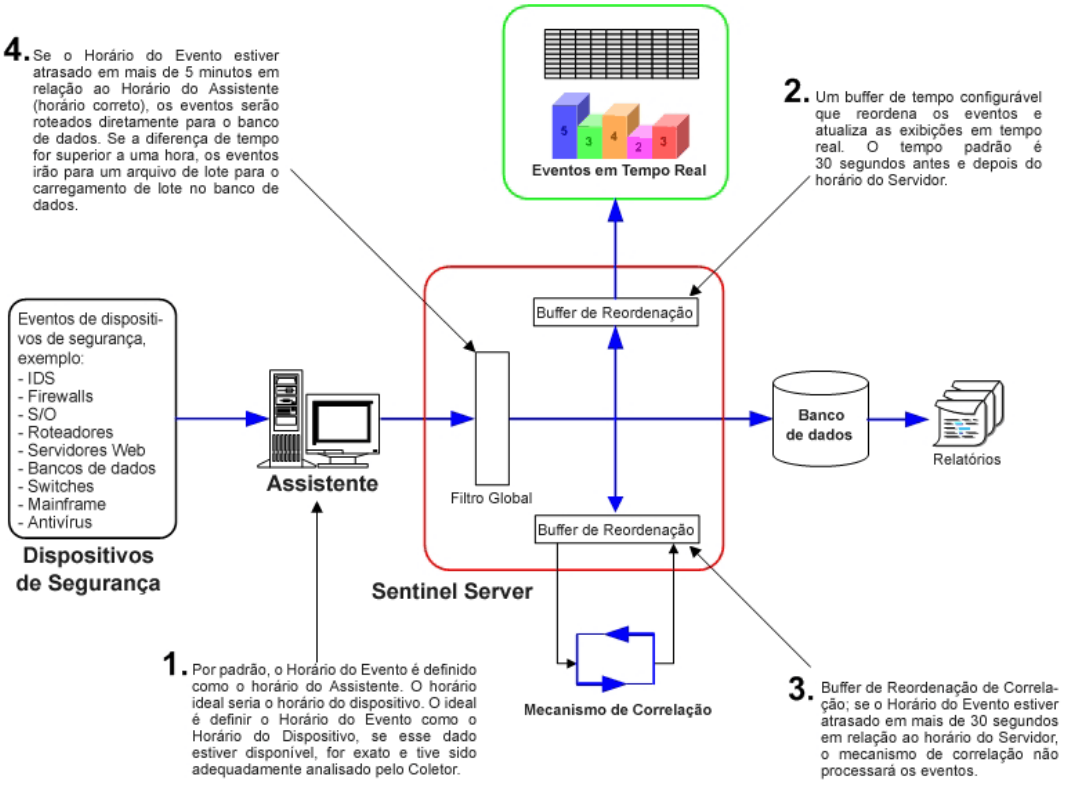
Horário

O horário de um evento é vital em seu processamento. É um dado importante para fins de auditoria e geração de relatórios, bem como para o processamento em tempo real. O mecanismo de correlação processa fluxos de eventos seqüenciais e detecta padrões nos eventos, bem como padrões temporais no fluxo. Entretanto, o dispositivo que gerou o evento talvez não tenha registrado o horário real em que o evento foi gerado. Para contornar essa

situação, o Sentinel oferece duas opções ao processar alertas de dispositivos de segurança: confiar no horário relatado pelo dispositivo e usá-lo como o horário do evento ou então descartá-lo e marcar o evento com o horário em que ele foi processado inicialmente pelo Sentinel (pelo Coletor).

O Sentinel é um sistema distribuído e consiste em vários processos que podem ocorrer em partes diferentes da rede. Além disso, pode haver algum atraso introduzido pelo dispositivo. Para lidar com essa situação, os processos do Sentinel reordenam os eventos em um fluxo ordenado por horário antes de realizar o processamento.

A ilustração a seguir explica o conceito do Horário do Sentinel.



1. Por padrão, o Horário do Evento é definido como o horário do Assistente. O horário ideal seria o horário do dispositivo. Portanto, convém definir o Horário do Evento como o Horário do Dispositivo, se este dado estiver disponível, for exato e tiver sido adequadamente analisado pelo Coletor.
2. Um buffer de tempo configurável que reordena os eventos e atualiza as exibições em tempo real. O tempo padrão é 30 segundos antes e depois do horário do servidor.
3. Buffer de reordenação de correlação, se o horário do evento estiver atrasado em mais de 30 segundos em relação ao horário do servidor, o mecanismo de correlação não processará os eventos.
4. Se o horário do evento estiver atrasado em 5 minutos ou mais em relação ao Horário do Assistente (horário correto), os eventos serão roteados diretamente para o banco de dados.

Eventos internos ou de sistema

Eventos Internos ou de Sistema significam informações sobre o status e as mudanças de status do sistema. Estes são os dois tipos de eventos gerados pelo sistema interno:

- Eventos internos
- Eventos de desempenho

Os eventos internos são informativos e descrevem um estado único ou uma mudança de estado no sistema. Eles informam quando um usuário efetua login ou não consegue efetuar a autenticação, quando um processo é iniciado ou quando uma regra de correlação é ativada. Os eventos de desempenho são gerados periodicamente e descrevem os recursos médios usados por diferentes partes do sistema.

Todos os eventos de sistema preenchem os seguintes atributos:

- Campo ST (Tipo de Sensor): para eventos internos, este campo é definido como 'I' e para eventos de desempenho, como 'P';
- ID do Evento: um UUID exclusivo do evento;
- Horário do Evento: o horário em que o evento foi gerado;
- Origem: o UUID do processo que gerou o evento;
- Nome do Sensor: o nome do processo que gerou o evento (por exemplo, DAS_Binary);
- RV32 (Categoria do Dispositivo): definida como 'ESEC';
- Coletor: ‘Desempenho’ para eventos de desempenho e ‘Interno’ para eventos internos.

Além dos atributos comuns, cada evento de sistema também define o recurso, o sub-recurso, a gravidade, o nome do evento e as tags de mensagem. No caso de eventos internos, o nome do evento específico o suficiente para identificar o significado exato do evento (por exemplo, Falha_Autenticação_Usuário). As tags de mensagens adicionam alguns detalhes específicos; no exemplo acima, a tag de mensagem contém o nome do usuário, nome do OS e, se disponível, o nome da máquina. O nome de um evento de desempenho é genérico e descreve o tipo de dados estatísticos. Os dados propriamente ditos encontram-se na tag de mensagem.

Os eventos de desempenho são enviados diretamente para o banco de dados. Para exibi-los, faça uma consulta rápida.

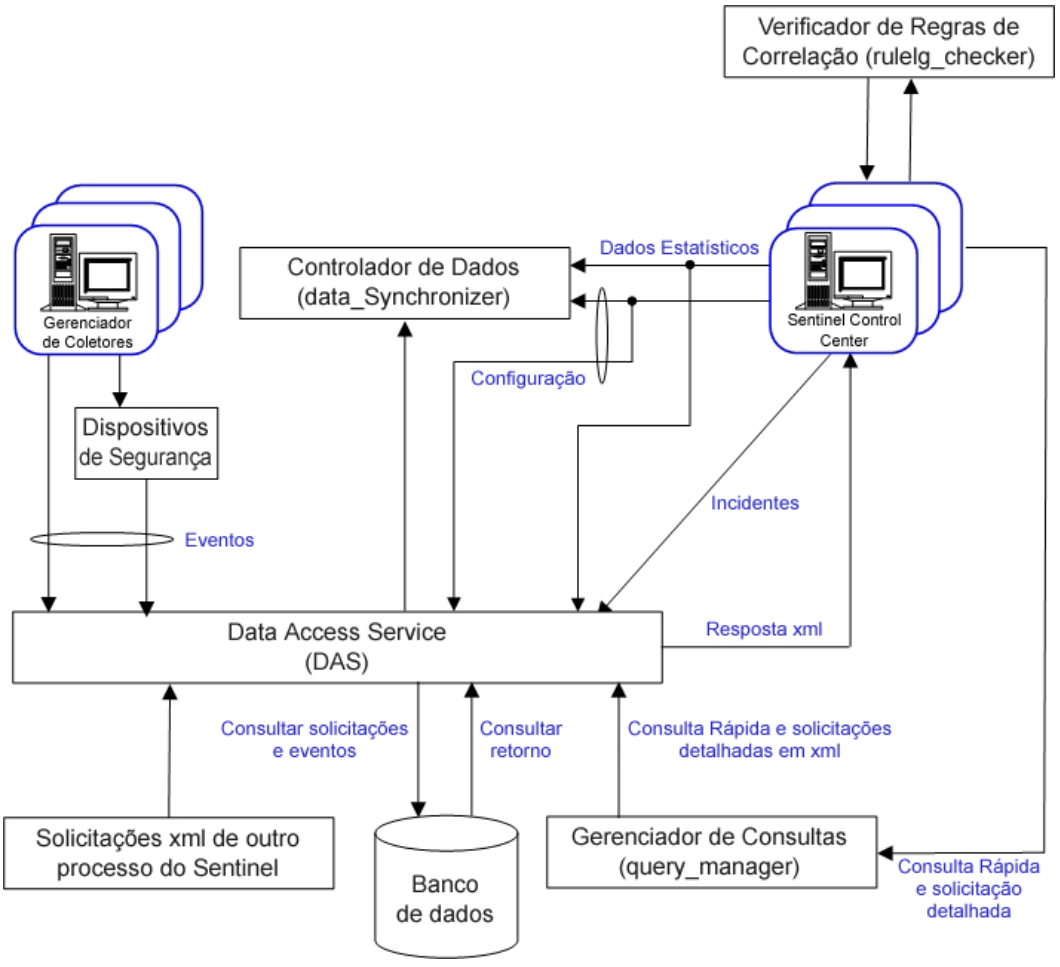
Consulte o *apêndice A – Eventos do Sistema*.

Processos

Os seguintes processos e serviços do Windows comunicam-se entre si através do iSCALE – um message-oriented middleware (middleware orientado por mensagem).

- Watchdog
- Estatísticas do Evento
- Sincronizador de Dados (Controlador de Dados)
- Mecanismo de Correlação
- Verificador de RuleLg (Verificador de Regra de Correlação)
- Serviços de Acesso a Dados (DAS) – binário, consulta e Active Views™
- Gerenciador de Consultas
- Sentinel Service (somente MSSQL) – consulte Watchdog

A seguir está a arquitetura do Sentinel Server.



Processo Watchdog

O Watchdog é um Processo do Sentinel que gerencia outros Processos desse programa. Se um processo que não seja o Watchdog é interrompido, o Watchdog reporta a ocorrência e reinicia esse processo.

No caso do Windows, o watchdog é um serviço e é chamado eSecurity. Se esse serviço for interrompido, todos os processos do Sentinel também serão interrompidos nessa máquina.

Estatísticas do Evento

O mecanismo Estatísticas do Evento é um componente do processo das_binary, que gerencia os dados usados pelos gráficos e tabelas de eventos das telas do Active Views no Sentinel Control Center.

O mecanismo mantém um conjunto de eventos e dados estatísticos para cada combinação de filtro e atributo de evento especificada no Assistente do Active Views. A primeira vez em que o usuário cria uma Tela Ativa com um determinado filtro e atributo de evento, um novo conjunto de dados é criado. Esse conjunto de dados contém as contagens desse atributo em intervalos fixos, bem como a maioria dos eventos recentes para cada um desses intervalos. Cada conjunto de dados é configurado para manter os dados referentes às últimas 24 horas.

Os intervalos são enviados para o Sentinel Control Center depois de um breve atraso, para estabilizar os dados que possam ter chegado com atraso em virtude de atrasos da rede e diferenças de horário.

As telas do Active Views serão compartilhadas automaticamente por vários usuários se o filtro e atributo de evento desejados forem iguais. Quando o usuário deixa de usar uma Tela Ativa, essa exibição será descartada após uma hora. Entretanto, se uma Tela Ativa for gravada nas preferências do usuário, ela continuará a coletar dados por até 100 horas.

Processo do Sincronizador de Dados (Controlador de Dados)

O processo do Sincronizador de Dados (data_synchronizer) gerencia as modificações de dados de configuração por múltiplos usuários. Quando um usuário pede para modificar os dados através do Sentinel Control Center, o registro de dados é bloqueado pelo data_synchronizer. Os detalhes sobre quem bloqueou os dados são publicados para os outros Sentinel Control Centers ativos e nenhum outro usuário poderá modificar os dados.
Se o Sentinel Control Center for fechado antes de desbloquear os dados que tiver bloqueado, o tempo de espera do bloqueio será excedido.

Processo do Mecanismo de Correlação (correlation_engine)

O processo do Mecanismo de Correlação (correlation_engine) recebe eventos do Gerenciador de Coletor do Assistente e publica eventos correlacionados com base em regras de correlação definidas pelo usuário.

Processo do Verificador de RuleLg (rulelg_checker)

O processo do Verificador de RuleLg (rulelg_checker) valida a sintaxe de filtro e as expressões de regra de correlação. O Sentinel Control Center usa esses resultados para determinar se um filtro ou uma regra de correlação pode ser gravada.

Processo do Serviço de Acesso a Dados (DAS, Data Access Service)

O processo do Serviço de Acesso a Dados (DAS, Data Access Service) é o serviço de persistência do Sentinel Server e fornece uma interface para o banco de dados, bem como o acesso dirigido a dados para o back end do banco de dados.

O DAS é um container composto de cinco processos diferentes. Cada processo é responsável por diferentes tipos de operações de banco de dados. Esses processos são controlados pelos seguintes arquivos de configuração:

- das_binary.xml: usado para operações de inserção de evento e evento correlacionado;
- das_query.xml: todas as outras operações de banco de dados;
- activity_container.xml: usado para executar e configurar o serviço de atividade;
- workflow_container.xml: usado para configurar o serviço de workflow (iTRAC);
- das_rt.xml: usado para configurar a função do Active Views no Sentinel Control Console.

O DAS recebe solicitações dos diferentes processos do Sentinel, converte-as em uma consulta ao banco de dados, processa o resultado do banco de dados e converte-o em uma resposta. Ele oferece suporte a solicitações para recuperar eventos para Consulta Rápida e Detalhamento de Eventos, para recuperar informações de vulnerabilidade e informações do consultor e para manipular informações de configuração. O DAS também gerencia o registro de todos os eventos recebidos do Gerenciador do Coletor Assistente e pede a recuperação e o armazenamento das informações de configuração.

Processo do Gerenciador de Consultas (query_manager)

O processo do gerenciador de consultas (query_manager) recebe uma consulta rápida, detalha as solicitações do Sentinel Control Center e as encaminha para o banco de dados através do DAS. As solicitações do Sentinel Control Center definem os eventos necessários com base em um filtro. Se um filtro for usado, o Gerenciador de Consultas recuperará a definição de filtro e converterá o filtro em um critério xml. O Gerenciador de Consultas envia a solicitação para o DAS. Nem todos os filtros podem ser completamente convertidos em consultas que podem ser processadas pelo banco de dados. Se o filtro for totalmente convertido, o Gerenciador de Consultas instruirá o DAS a enviar a resposta diretamente para o Sentinel Control Center. Se o filtro contiver expressões regulares que não puderem ser convertidas em SQL, o Gerenciador de Consultas vai converter o que puder e gerar um critério conservador que retornará um superconjunto de eventos necessários. Nesse caso, o Gerenciador de Consultas instruirá o DAS a retornar os resultados para o Gerenciador de Consultas. Quando a resposta voltar para o Gerenciador de Consultas, ele a filtrará na memória e enviará esses eventos que passarem pelo filtro para o Sentinel Control Center.

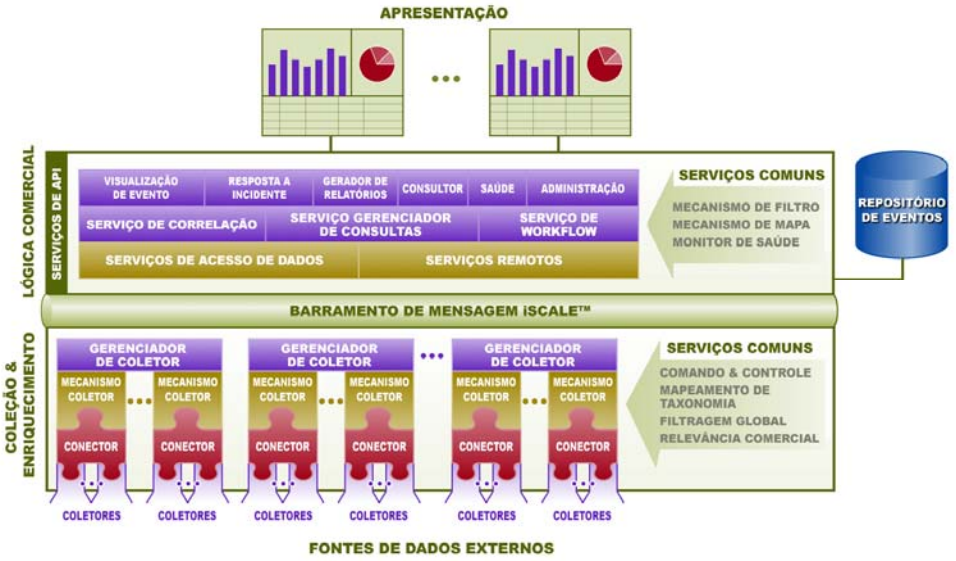
Arquitetura lógica

O Sentinel 5 é composto de três camadas lógicas:

- camada de coleta e enriquecimento;
- camada de lógica comercial;
- camada de apresentação.

A camada de coleta/enriquecimento agrega os eventos de origens de dados externas, transforma os formatos específicos dos dispositivos no formato do Sentinel, enriquece a origem dos eventos nativos com dados relevantes à empresa e despacha os pacotes de eventos para o barramento de mensagens. O componente principal que faz parte dessa função é o Coletor, auxiliado pelo mapeamento de taxonomia e pelo serviço de filtro global.

A camada de lógica comercial contém um conjunto de componentes classificáveis. O componente básico é um serviço remoto que adiciona recursos de mensagens aos serviços e objetos de dados para habilitar o acesso transparente aos dados em toda a rede, e o serviço de Acesso a Dados, que consiste em um serviço de gerenciamento de objetos com o qual os usuários podem definir objetos usando metadados. Outros serviços incluem Correlação, Gerenciador de Consultas, Workflow, Visualização de Eventos, Resposta a Incidentes, Saúde, Consultor, Relatórios e Administração.



A camada de apresentação proporciona a interface entre o aplicativo e o usuário final. Um painel abrangente chamado Sentinel Control Center oferece um workbench de usuário integrado que consiste em uma matriz de sete aplicativos diferentes que podem ser acessados por meio de uma única estrutura comum. Essa estrutura de várias plataformas foi desenvolvida com base nos padrões Java™ 1.4 e proporciona uma visualização unificada dos componentes independentes da lógica comercial – gráficos interativos em tempo real, respostas a incidentes processáveis, workflow automatizado de incidentes de uso obrigatório, relatórios, solução de incidentes associados a explorações conhecidas e muito mais.

Cada uma das camadas está ilustrada na figura acima e será explicada em detalhes nas seções a seguir.

Camada de coleta e enriquecimento

Os eventos são agregados por meio de um conjunto flexível de Coletores configuráveis, que reúnem dados de diversos sensores e outros dispositivos e origens. O usuário pode usar Coletores predefinidos, modificar Coletores existentes ou criar seus próprios Coletores para garantir que o sistema atenda a todas as exigências.

Subseqüentemente, os dados agregados pelos Coletores na forma de eventos são normalizados e convertidos no formato XML, enriquecidos com uma série de metadados (ou seja, dados sobre dados) usando um conjunto de serviços de relevância comercial e propagados para o lado do servidor onde serão submetidos a análises adicionais computadorizadas por meio da plataforma do barramento de mensagens. A camada de coleta e enriquecimento consiste nos seguintes componentes:

- Conectores e Coletor;
- Gerenciador e Mecanismo de Coletores;
- Construtor de Coletor.

Conectores e Coletores

Um conector é um concentrador ou adaptador multiplexado que conecta o Mecanismo do Coletor aos dispositivos efetivamente monitorados.

Os Coletores atuam no nível do componente como um agregador de dados do evento a partir de uma origem específica. O Sentinel 5 suporta basicamente conexões remotas "sem Coletores" às origens. Entretanto, os Coletores podem ser distribuídos em dispositivos específicos nos quais uma abordagem remota é menos eficiente.

Os Coletores são controlados a partir do Sentinel Control Center, que orquestra a comunicação entre os Coletores e a plataforma do Sentinel para análises em tempo real, computação de correlação e resposta a incidentes.

Gerenciador e Mecanismo de Coletores

O Gerenciador de Coletor gerencia os Coletores, monitora as mensagens de status do sistema e executa a filtragem de eventos conforme necessário. As principais funções do Gerenciador de Coletor incluem transformar eventos, adicionar relevância comercial aos eventos por meio de taxonomia, executar filtragem global dos eventos, rotear eventos e enviar mensagens sobre a saúde do sistema ao Sentinel Server.

Um Mecanismo de Coletores é o componente de interpretação que analisa o código dos Coletores.

Construtor de Coletor

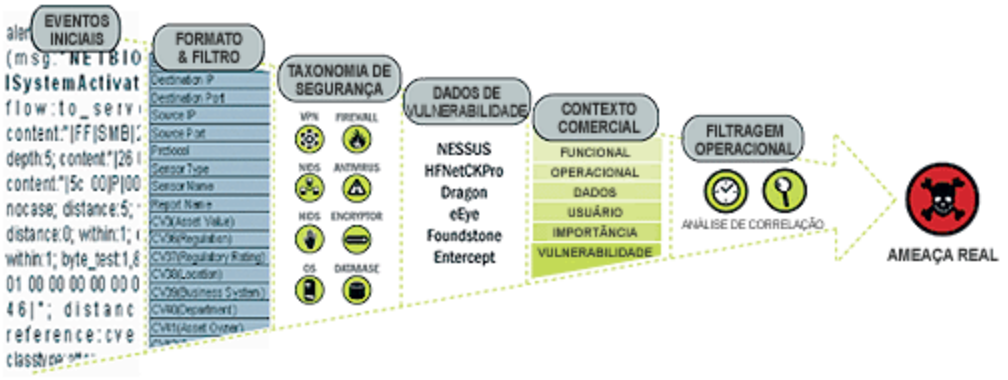
O Construtor de Coletor é um aplicativo independente utilizado para construir, configurar e depurar Coletores. Esse aplicativo funciona como um IDE (Integrated Development Environment – Ambiente de Desenvolvimento Integrado) que permite ao usuário criar novos Coletores para analisar dados dos dispositivos de origem usando uma linguagem interpretativa com finalidade especial desenvolvida para lidar com a natureza dos eventos de rede e de segurança.

Serviços comuns

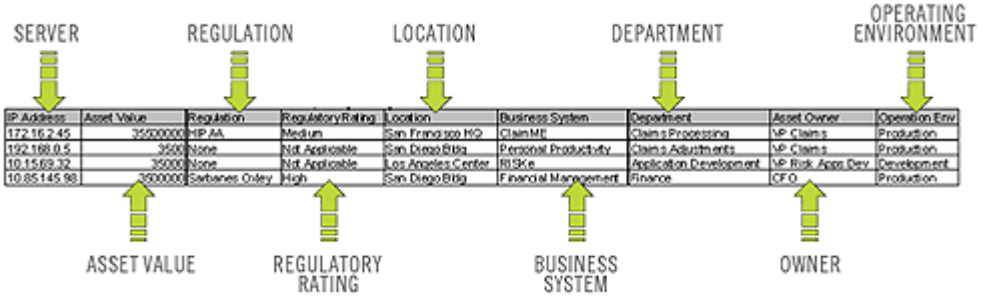
Todos os componentes descritos acima na camada de coleta e enriquecimento são orientados por um conjunto de serviços comuns. Esses serviços utilitários estruturam a coleta e enriquecimento de dados e auxiliam na filtragem do ruído das informações (por meio de filtros globais), aplicando tags definidas pelo usuário para enriquecer as informações dos eventos (por meio dos serviços de mapeamento de taxonomia e relevância comercial) e controlando as funções dos Coletores de dados (por meio de serviços de comando e controle).

Taxonomia – quase todos os produtos de segurança geram eventos em formatos e conteúdos diferentes. Por exemplo, o Windows e o Solaris registram as falhas de maneiras distintas.

A taxonomia do Sentinel traduz automaticamente os dados de produtos heterogêneos em termos inteligíveis, permitindo uma visualização homogênea em tempo real de toda a segurança da rede. A taxonomia do Sentinel formata e filtra dados iniciais de eventos de segurança antes de adicionar o contexto dos eventos ao fluxo de dados. Esse processo formata todos os dados de segurança numa estrutura otimizada para que o mecanismo Sentinel Correlation faça o processamento, conforme exibição no diagrama a seguir.



Relevância comercial – o Sentinel 5 insere dados contextuais de relevância comercial diretamente no fluxo de eventos. Ele inclui até 135 campos personalizáveis nos quais os usuários podem adicionar informações específicas sobre os bens, como unidades de negócios, proprietário, valor do bem e localização geográfica. Quando essas informações são adicionadas ao sistema, todos os outros componentes podem aproveitar o contexto adicional.



Detecção de exploração – possibilita a notificação imediata e processável de ataques em sistemas vulneráveis. Essa detecção vincula em tempo real as assinaturas IDS e os resultados de verificação de vulnerabilidades, notificando os usuários de modo automático e imediato mediante uma tentativa de ataque para explorar um sistema vulnerável. Isso melhora sensivelmente a eficiência e a eficácia da resposta a incidentes.

A detecção de exploração fornece aos usuários atualizações e mapeamentos entre as assinaturas IDS e as dos scanners de vulnerabilidade. Os mapeamentos incluem uma lista abrangente de scanners de vulnerabilidades e do IDS. Os usuários precisam apenas fazer o upload dos resultados das verificações de vulnerabilidade para o Sentinel. A detecção de exploração analisa esses resultados automaticamente e atualiza os respectivos Coletores IDS. Ela usa o conhecimento incorporado do status de vulnerabilidade para priorizar com eficácia e eficiência as respostas às ameaças à segurança em tempo real.

Quando é iniciado um ataque contra um bem vulnerável, a detecção de exploração alerta os usuários sobre o nível de gravidade correspondente à vulnerabilidade explorada. Desse modo, os usuários podem tomar uma atitude imediata em relação aos eventos de alta prioridade. Isso elimina o trabalho de "tentativa e erro" do monitoramento de alertas e aumenta a eficiência das respostas aos incidentes concentrando a reação nos ataques conhecidos contra bens vulneráveis.

A detecção de exploração também permite que os usuários mapeiem ou "desmapeiem" assinaturas e vulnerabilidades para filtrar falsos positivos e negativos, bem como para aproveitar assinaturas personalizadas ou verificações de vulnerabilidade.

Camada de lógica comercial

O kernel da plataforma do Sentinel 5 consiste em um conjunto de serviços levemente integrados que podem ser executados em uma configuração independente ou em uma topologia distribuída. Essa SOA (Service-Oriented Architecture - Arquitetura Orientada por Serviço) é chamada iSCALE. Especificamente, a SOA do Sentinel consiste em um conjunto de mecanismos, serviços e APIs que funcionam juntos para proporcionar a expansão linear da solução de acordo com o aumento da carga de dados e/ou carga de trabalho de processamento.

Os serviços do Sentinel são executados em containers especializados e permitem processamento e expansão inigualáveis, pois são otimizados para computação e transporte com base em mensagens. Os principais serviços que formam o Sentinel Server incluem:

- Serviço Remoto
- Serviço de Acesso a Dados
- Serviço de Gerenciador de Consultas
- Serviço de Correlação
- Serviço de Workflow
- Visualização de Eventos
- Resposta a Incidentes
- Relatórios
- Consultor
- Saúde
- Administração

Serviço Remoto

O Serviço Remoto do Sentinel 5 fornece o mecanismo pelo qual o servidor e os programas do cliente se comunicam. Esse mecanismo geralmente é conhecido como aplicativo de objetos distribuídos.

Especificamente, o Serviço Remoto oferece:

- Localização de objetos remotos: alcançado por meio de metadados que descrevem o nome do objeto ou o token de registro, embora a verdadeira localização não seja necessária, pois o barramento de mensagens da iSCALE permite a transparência das localizações.
- Comunicação com objetos remotos: os detalhes da comunicação entre os objetos remotos são processados pelo barramento de mensagens da iSCALE.
- Transmissão e empacotamento de objetos: quando grandes volumes de dados precisam transitar do cliente para o servidor e vice-versa, esses objetos são otimizados para carregar os dados sob demanda.
- Callbacks: outro padrão e camada de abstração incorporados no Serviço Remoto que permite a comunicação de objetos remotos PTP.
- Estatísticas e monitoramento de serviço: fornece estatísticas sobre desempenho e carga para uso desses serviços remotos.

Serviço de Acesso a Dados

O DAS (Data Access Service - Serviço de Acesso a Dados) é um serviço de gerenciamento de objetos com o qual os usuários podem definir objetos usando metadados. O DAS gerencia o objeto e o acesso aos objetos e automatiza a transmissão e a persistência. Além disso, o DAS atua como uma fachada de acesso a dados a partir de qualquer armazenamento de dados persistente, como bancos de dados, serviços de diretórios ou arquivos. As operações do DAS incluem acesso uniforme aos dados por meio de JDBC e, como alternativa, estratégias de inserção de eventos de alto desempenho usando conectores nativos (ou seja, OCI para Oracle 9i e ADO para Microsoft SQL Server).

Serviço de Gerenciador de Consultas

O Serviço de Gerenciador de Consultas orquestra as solicitações de histórico de eventos e detalhamento do Sentinel Control Center. Esse serviço é um componente integral para implementação do algoritmo de paginação usado no recurso de pesquisa do Histórico de Eventos. Ele converte os filtros definidos pelo usuário em critérios válidos, aos quais anexa critérios de segurança antes da recuperação dos eventos. Esse serviço também assegura que os critérios não serão modificados durante uma transação de histórico de evento paginado.

Serviço de Correlação

O algoritmo de correlação do Sentinel 5 computa os eventos correlacionados analisando o fluxo de dados em tempo real. Esse serviço publica os eventos correlacionados com base nas regras definidas pelo usuário antes que os eventos cheguem ao banco de dados. As regras no mecanismo de correlação conseguem detectar um padrão em um evento único de uma janela em execução de eventos. Quando uma correspondência é detectada, o mecanismo de correlação gera um evento correlacionado descrevendo o padrão encontrado e pode criar um incidente ou acionar um workflow de resolução por meio do iTRAC. O mecanismo de correlação funciona com um componente verificador de regras que computa as expressões das regras de correlação e valida a sintaxe dos filtros. Além de proporcionar um conjunto abrangente de regras de correlação, o mecanismo de correlação do Sentinel oferece vantagens específicas em relação aos mecanismos de correlação centrados no banco de dados.

- Uma vez que depende do processamento na memória em vez de inserções e leituras do banco de dados, o mecanismo de correlação funciona tanto em volumes altos e constantes quanto em picos de eventos sob ataques, circunstâncias em que o desempenho da correlação é mais crítico.
- Como o volume de correlação não diminui a velocidade de outros componentes do sistema, a interface do usuário permanece responsiva, especialmente com altos volumes de eventos.
- Correlação distribuída – as organizações podem distribuir vários mecanismos de correlação, cada qual em seu próprio servidor, sem precisar replicar configurações ou adicionar bancos de dados. A expansão independente de componentes proporciona escalabilidade e desempenho com excelente relação custo-benefício.
- O mecanismo de correlação pode adicionar eventos ao incidente após a determinação deste.

Os usuários são incentivados a utilizar uma métrica chamada ERPS (Event Rules per Second – Regras de Eventos por Segundo). A ERPS corresponde ao número de eventos que podem ser examinados por uma regra de correlação por segundo. Essa medida é um bom indicador de desempenho, pois prevê o impacto sobre este quando dois fatores se cruzam: eventos por segundo e o número de regras em uso.

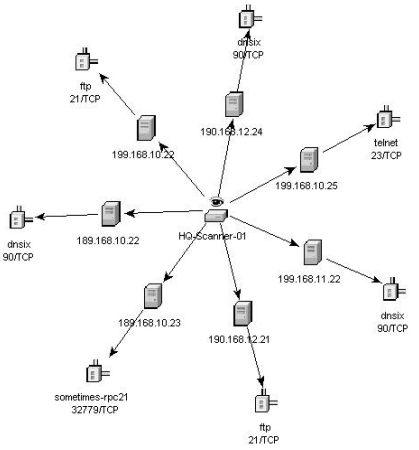
Serviço de Workflow (iTRAC)

O Serviço de Workflow recebe acionadores na criação do incidente e inicia os processos de workflow com base em modelos de workflow predefinidos. Esse serviço gerencia o ciclo de vida desses processos gerando itens de trabalho ou executando atividades. Além disso, mantém um histórico dos processos concluídos que pode ser usado para auditoria das respostas aos incidentes.

Visualização de Eventos

Active Views™, a interface gráfica interativa de usuário para visualização de eventos, oferece um painel de gerenciamento de segurança integrado e um conjunto abrangente de ferramentas analíticas e de visualização em tempo real para facilitar a detecção e análises de ameaças. Os usuários podem monitorar eventos em tempo real e efetuar detalhamentos de segundos a horas no passado. Uma ampla variedade de gráficos e recursos de visualização permitem o monitoramento das informações através de representação gráfica 3D em barras, 2D em barras empilhadas, linhas e faixas, entre outras. É possível visualizar outras informações importantes no painel do Active Views, como notificação de explorações de bens (detecção de exploração), visualizando informações de bens e associações gráficas entre IPs de origem e de destino pertinentes.

Como o Active Views usa a arquitetura iSCALE, os analistas podem detalhar dados rapidamente para executar uma análise mais aprofundada, pois o Active Views oferece acesso direto aos dados de eventos residentes na memória em tempo real, processando facilmente milhares de eventos por segundo sem qualquer prejuízo ao desempenho. Os dados são mantidos na memória e gravados no banco de dados conforme necessário (o Active Views pode armazenar até 8 horas de dados na memória com cargas de eventos típicas). Essa visualização em tempo real, ininterrupta e orientada ao desempenho é essencial em situações de ataque ou estáveis.

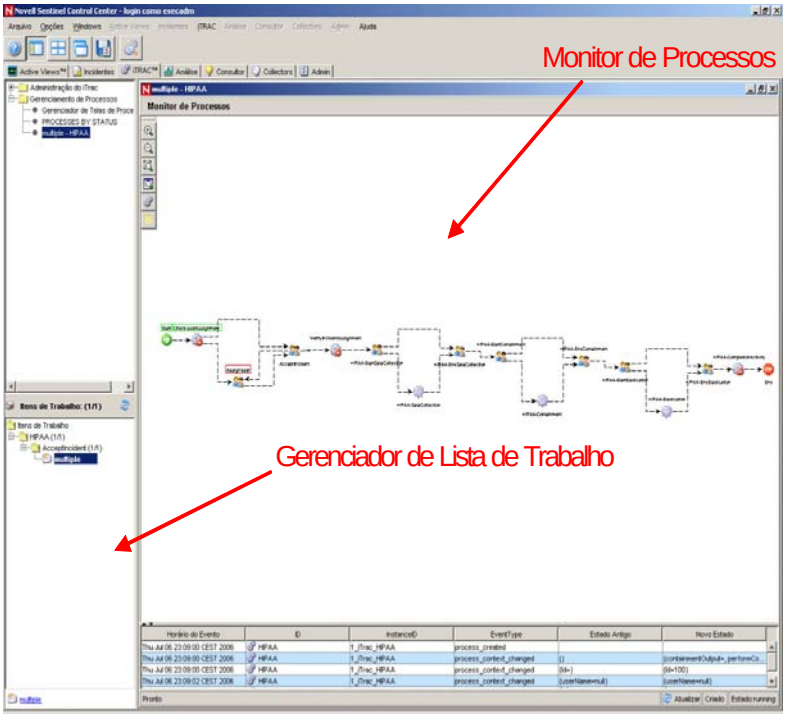


Resposta a incidentes pelo iTRAC

Com o iTRAC, o gerenciamento tradicional de informações de segurança passa de uma função passiva de "alerta e visualização" para um papel ativo oferecendo "respostas a incidentes processáveis", o que permite às organizações definir e documentar os processos de resolução de incidentes e orientar, aplicar e monitorar esses processos assim que um incidente ou violação é detectado.

O Sentinel 5 conta com gabaritos de processos já prontos para o uso que utilizam as diretrizes do SANS Institute para processamento de incidentes. Os usuários podem começar com esses processos predefinidos e configurar atividades específicas para refletir as práticas recomendadas de sua organização. Os processos do iTRAC podem ser acionados automaticamente a partir da criação do incidente ou de regras de correlação, ou manualmente, por um profissional autorizado de auditoria ou segurança. O iTRAC mantém uma trilha de

auditoria de todas as ações para oferecer suporte à criação de relatórios de conformidade e análises de histórico.



Uma lista de trabalho disponibiliza ao usuário todas as tarefas a ele designadas, e um monitor de processos proporciona visibilidade em tempo real do status dos processos durante o ciclo de vida da resolução.

A estrutura de atividades do iTRAC permite que os usuários personalizem suas tarefas automatizadas ou manuais para processos específicos de resolução de incidentes. Os gabaritos de processos do iTRAC podem ser configurados usando a estrutura de atividades para corresponder o gabarito às práticas recomendadas da organização. As atividades são executadas diretamente do Sentinel Control Center.

A estrutura de automação do iTRAC funciona com dois componentes principais – o container de atividades e o de workflow. O primeiro automatiza a execução das atividades do conjunto de etapas especificado com base nas regras de entrada e o segundo automatiza a execução do workflow com base nas atividades por meio de uma lista de trabalho. As regras de entrada são baseadas no padrão XPDL (XML Processing Description Language) e oferece um modelo formal para expressar processos executáveis em uma empresa. Essa abordagem baseada em padrões à implementação de regras e conjuntos de regras específicos da empresa garante definições duradouras dos processos para os clientes.

Serviço de relatórios

O Serviço de Relatórios permite a geração de relatórios históricos e de vulnerabilidade, entre outros. O Sentinel 5 oferece relatórios prontos para o uso e permite que os usuários configurem seus próprios relatórios usando Crystal Reports. Estes são alguns exemplos de relatórios incluídos no Sentinel 5:

- Análises de tendências;
- Status de segurança das linhas de negócios ou de bens críticos;
- Tipos de ataque;
- Bens em risco;
- Tempos de resposta e resolução;
- Violações à conformidade com políticas.

Advisor

O Sentinel Advisor é um módulo opcional que efetua a referência cruzada entre os dados de alerta em tempo real do Sentinel e as vulnerabilidades conhecidas e informações de resolução, possibilitando uma melhor detecção e resposta ao incidente. Com o Advisor, as organizações podem determinar se os eventos exploram vulnerabilidades específicas e como esses ataques afetam seus bens. O Advisor também contém informações detalhadas sobre as vulnerabilidades que os ataques pretendem explorar, os possíveis efeitos dos ataques caso obtenham êxito, e as etapas necessárias para resolução. As etapas de resolução recomendadas são aplicadas e monitoradas pelos processos de resposta a incidentes do iTRAC.

Saúde

Com o serviço Saúde, os usuários obtêm uma visualização abrangente da plataforma distribuída do Sentinel 5. Esse serviço agrega as informações de saúde de vários processos que normalmente são distribuídos em vários servidores. As informações sobre saúde são exibidas periodicamente no Sentinel Control Center para o usuário final.

Administração

O recurso Administração oferece os recursos de gerenciamento de usuários e definição da configuração normalmente necessários aos administradores do Sentinel 5.

Serviços comuns

Todos os componentes descritos acima na camada de lógica comercial da arquitetura são orientados por um conjunto de serviços comuns. Esses serviços utilitários ajudam a refinar a filtragem (por meio do Mecanismo de Filtro) dos eventos para usuários, a efetuar o monitoramento contínuo das estatísticas da saúde do sistema (por meio do Monitor de Saúde) e a obter atualizações dinâmicas dos dados no âmbito do sistema (com o Serviço de Mapas). Juntos, esses utilitários estruturam os serviços levemente integrados que permitem o processamento e a expansão inigualáveis do veículo baseado em barramento de mensagens para análises e computação em tempo real.

Camada de apresentação

A camada de apresentação proporciona a interface entre o aplicativo e o usuário final. O Sentinel Command Center é um painel abrangente que apresenta informações ao usuário.

Módulos do produto

Sentinel Control Center

O Sentinel Control Center consiste em um robusto painel de gerenciamento de segurança integrado. Exibições intuitivas permitem que os analistas identifiquem rapidamente as novas tendências ou ataques, manipulem e interajam com informações gráficas em tempo real e respondam a incidentes. Os principais recursos incluem:

- Active Views – análises e visualizações em tempo real;
- Incidentes – criação e gerenciamento de incidentes;
- Análise – definição e gerenciamento de regras de correlação;
- iTRACc – gerenciamento de processos de documentação, garantia de uso e monitoramento dos processos de resolução de incidentes;
- Relatórios – métricas e relatórios de histórico.

Sentinel Wizard

O Sentinel Wizard coleta dados dos dispositivos de origem e distribui um fluxo de eventos enriquecido ao aplicar a taxonomia, detecção de exploração e relevância comercial no fluxo de dados antes de correlacionar, analisar e enviar os eventos para o banco de dados. Um fluxo de eventos enriquecido significa que os dados estão correlacionados ao contexto comercial necessário para identificar e resolver ameaças internas ou externas e violações às políticas. Em qualquer configuração, pode haver um ou mais Assistentes distribuídos, proporcionando aos clientes a capacidade de distribuir componentes do produto na infra-estrutura da empresa, de acordo com sua topologia de rede.

Sentinel Advisor

O Sentinel Advisor é um módulo opcional que efetua a referência cruzada entre os dados de alerta em tempo real do Sentinel e as vulnerabilidades conhecidas e informações de resolução.

Índice

Este guia contém o seguinte:

Convenções usadas

Nota e avisos

NOTA: as notas apresentam informações adicionais que podem ser úteis.

AVISO: Os avisos apresentam informações adicionais que podem impedir danos ou perda de dados do sistema.

Comandos

Os comandos aparecem na fonte Courier. Por exemplo:

```
useradd –g dba –d /export/home/oracle –m –s /bin/csh
   oracle
```

Outras referências da Novell

Os seguintes manuais estão disponíveis nos CDs de instalação do Sentinel.

- Guia de Instalação do Sentinel™ 5
- Guia do Usuário do Sentinel™
- Guia do Usuário do Assistente do Sentinel™ 5
- Guia de Referência do Usuário do Sentinel™ 5
- Guia de Integração de Terceiros do Sentinel™ 5
- Notas da versão

Entrando em contato com a Novell

- Site na Web: http://www.novell.com
- Suporte Técnico da Novell: http://www.novell.com/support/index.html
- Suporte Técnico Internacional da Novell: http://support.novell.com/phone.html?sourceidint=suplnav4_phonesup
- Suporte Pessoal: http://support.novell.com/support_options.html?sourceidint=suplnav_supportprog
- Para obter suporte 24 horas por dia, 7 vezes por semana, ligue para 800-858-4000

2 Navegando pelo Sentinel Control Center

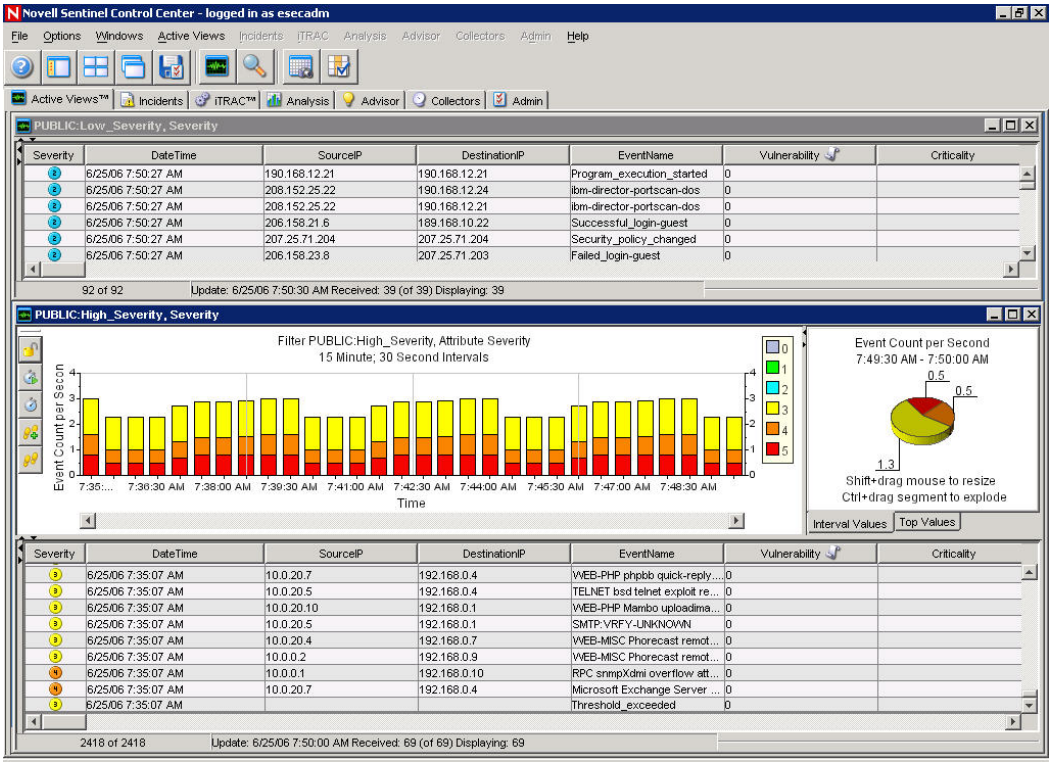
NOTA: O termo Agente é intercambiável com Coletor. Mais adiante, Agentes será referido como Coletores.

O Sentinel Control Center é composto de:

- Barra de menus
- Barra de ferramentas
- Guias

Além disso, os seguintes temas serão explicados neste capítulo:

- Iniciando o Sentinel Control Center
- Mudando a aparência do Sentinel Control Center
- Gravando as preferências do usuário
- Mudando a senha do Sentinel



Iniciando o Sentinel Control Center

Iniciando o Sentinel Control Center no Windows

Iniciando o Sentinel Control Center no Windows

1. Clique em *Iniciar* > *Sentinel* > *Sentinel Control Center* ou clique no ícone *Sentinel Control Center* na área de trabalho.
2. Digite seu nome do usuário e senha, e clique em *OK*.

Iniciando o Sentinel Control Center no UNIX

Iniciando o Sentinel Control Center no UNIX

1. Como usuário esecadm, use cd para passar a este diretório:

   ```
   $ESEC_HOME/sentinel/console
   ```

2. Execute o seguinte comando:

   ```
   ./run.sh
   ```

3. Digite seu nome do usuário e senha, e clique em *OK*.

Barra de menus

Há dez menus abaixo da barra de título. Começando pelo lado esquerdo da janela, estão os menus Arquivo, Opções, Windows, Active Views, Incidentes, iTRAC, Consultor, Coletores, Admin e Ajuda.

As opções Arquivo, Opções, Windows e Ajuda estão sempre disponíveis. As outras opções tornam-se disponíveis de acordo com a guia ativada e com as permissões do usuário.

Menu Arquivo

- Gravar Preferências
- Sair

Menu Opções

- Mudar Senha
- Posicionamento da Guia
  - Acima
  - Abaixo
- Ancorar Navegador
- Mostrar Navegador

Menu Janelas:

- Colocar Tudo em Cascata
- Colocar Tudo Lado a Lado
  - Lado a Lado com o Melhor Ajuste
  - Lado a Lado Horizontal
  - Lado a Lado Vertical
- Minimizar Tudo
- Restaurar Tudo
- Fechar Tudo

Active Views™

- Propriedades
- Criar Tela Ativa
- Consulta de Eventos
- Tempo Real de Evento
  - Instantâneo
  - Gerenciar Colunas

Incidentes

- Exibir Gerenciador de Telas de Incidentes
- Criar Incidente
- Configuração de Viewer de Anexos

iTRAC™

- Exibir Gerenciador de Processos

Análise

- Criar Relatório

Consultor

- Criar Relatório

Coletores

- Exibir Gerenciador de Telas de Coletor

Admin

- Configuração de Relatórios
- Regras de Correlação
- Gerenciador de Mecanismos de Correlação
- Configuração de Filtro Global
- Configuração de Menu
- Configuração de Filtro
- Configuração do Usuário

Ajuda

- Ajuda
- Sobre o Sentinel

Barra de Ferramentas

Cinco botões que abrangem o sistema são constantemente exibidos na barra de ferramentas. Os outros botões são exibidos de acordo com a guia ou janela ativada e com as permissões do usuário.

Barra de ferramentas no âmbito do sistema

Estes são os cinco botões no âmbito do sistema:

-  Ver Ajuda do Sentinel
-  Mostrar/Ocultar Janela de Navegação
-  Colocar Lado a Lado Todas as Janelas de Exibição
-  Colocar em Cascata Todas as Janelas de Exibição
-  Gravar Preferências do Usuário

Guia Active Views™

Quando a guia ActiveViews™ está ativa, os seguintes botões tornam-se disponíveis.

-  Active Views
-  Iniciar Consulta de Eventos

Janela Contagem de Evento sobre Tempo

Quando uma janela Contagem de Evento sobre Tempo está ativa, os seguintes botões tornam-se disponíveis.

-  Instantâneo de uma Tabela de Contagem de Evento sobre Tempo
-  Gerenciar Colunas da Tabela de Contagem de Evento sobre Tempo

Gráfico de Contagens de Eventos sobre Tempo

Quando o gráfico Contagens de Eventos sobre Tempo está ativo, os seguintes botões tornam-se disponíveis no respectivo gráfico.

- Bloquear/Desbloquear o Gráfico
- Aumentar Intervalo de Exibição
- Diminuir Intervalo de Exibição
- Aumentar Tempo de Exibição
- Diminuir Tempo de Exibição

Quando você clica no botão Bloquear, os seguintes botões tornam-se disponíveis:

- Bloquear/Desbloquear o Gráfico
- Aumentar Intervalo de Exibição
- Diminuir Intervalo de Exibição
- Aumentar Tempo de Exibição
- Diminuir Tempo de Exibição
- Ampliar
- Reduzir
- Detalhar para Eventos
- Gravar como Arquivo hml

Janela Instantâneo

Quando a janela Instantâneo está ativa, o seguinte botão torna-se disponível.

-  Gerenciar Colunas

Guia Incidentes

Quando a guia Incidentes está ativa, os seguintes botões tornam-se disponíveis.

-  Exibir Gerenciador de Telas de Incidentes
-  Criar um Novo Incidente
-  Configurar Viewers de Anexos

Incidente

Quando um Incidente está aberto, o seguinte botão torna-se disponível.

-  Gerenciar Colunas de Eventos Associados

iTRAC

Quando a guia iTRAC está ativa, o seguinte botão torna-se disponível.

-  Exibir Gerenciador de Telas de Processos

Guia Análise e Consultor

Quando uma dessas guias está ativa, o seguinte botão torna-se disponível.

-  Criar Relatório

Guia Coletores

Quando a guia Coletores está ativa, os seguintes botões tornam-se disponíveis.

-  Exibir Gerenciador de Telas do Gerenciador de Coletor
-  Exibir Gerenciador de Telas do Coletor

Guia Admin

Quando a guia Admin está ativa, o seguintes botões tornam-se disponíveis.

-  Exibir Configuração de Relatórios
-  Exibir Regras de Correlação
-  Exibir Gerenciador de Mecanismos de Correlação
-  Exibir Configuração de Filtro Global
-  Exibir Configuração de Menu
-  Exibir Gerenciador de Filtros
-  Exibir Gerenciador de Usuários
-  Gerenciador de Telas de Servidor

Janela Gerenciador de Filtros

Quando a janela Gerenciador de Filtros está ativa, os seguintes botões tornam-se disponíveis.

-  Criar um Novo Filtro
-  Apagar o Filtro Selecionado (ativo quando o filtro está selecionado)

Menu Configuração de Menu

Quando a janela Configuração de Menu estiver ativa e no modo de modificação, os seguintes botões estarão disponíveis.

-  Criar Novo item de menu
-  Apagar Item de Menu
-  Ativar Item de Menu
-  Desativar Item de Menu

Guias

Dependendo de suas permissões de usuário, o Sentinel Control Center exibirá as seguintes guias. Você deve ter a permissão específica para ver cada uma delas.

- Active Views™
- Incidentes
- iTRAC™
- Análise
- Consultor
- Coletores
- Admin

Para obter mais informações sobre Guias, consulte o capítulo respectivo a cada guia.

Mudando a aparência do Sentinel Control Center

Para mudar a aparência do Sentinel Control Center, siga as instruções das seguintes seções:

Definindo a posição da guia

Para definir a posição da guia

1. Clique em *Opções* > *Posicionamento da Guia*.
2. Selecione Acima ou Abaixo.

Mostrando ou ocultando a janela do Navegador

Para mostrar ou ocultar a janela do Navegador

1. Clique em *Opções* > *Mostrar Navegador* ativar ou desativar.

Ancorando ou flutuando a janela do Navegador

Para ancorar ou flutuar a janela do Navegador

1. Clique em *Opções* > *Ancorar Navegador* para ativar ou desativar.

Colocando as janelas em cascata

Para colocar as janelas em cascata

1. Clique em *Janelas* > *Colocar Tudo em Cascata.* Todas as janelas abertas no painel direito serão colocadas em cascata.

Colocando as janelas lado a lado

Para colocar as janelas lado a lado

1. Clique em *Janelas* > *Colocar Tudo Lado a Lado.*
2. Aponte para:
   - Lado a Lado com o Melhor Ajuste
   - Lado a Lado Vertical
   - Lado a Lado Horizontal

Minimizando e restaurando todas as janelas

Para minimizar todas as janelas

1. Clique em *Janelas* > *Minimizar Tudo.* Todas as janelas abertas no painel direito serão minimizadas.

Para restaurar todas as janelas ao tamanho original

Para restaurar todas as janelas ao tamanho original

1. Clique em *Janelas* > *Restaurar Tudo*. Todas as janelas abertas no painel direito serão restauradas ao tamanho original.

Para restaurar uma janela individual

Para restaurar uma janela individual

1. Clique na janela minimizada. A janela será restaurada ao tamanho original.

Fechando todas as janelas abertas de uma vez

Para fechar todas as janelas

1. Clique em *Janelas* > *Fechar Tudo*.

Gravando preferências do usuário

Você deve ter a permissão de usuário Gravar Área de Trabalho.

Estas são as preferências que podem ser gravadas:

- Janelas permanentes, as que podem ser recriadas porque não dependem dos dados que estavam disponíveis no momento de sua criação original. Por exemplo, as exibições de Resumo e Active Views podem ser gravadas. No entanto, não é possível gravar janelas temporárias, como instantâneos e consultas rápidas. Todas as janelas relacionadas no Navegador do Admin podem ser gravadas, mas nenhuma das janelas secundárias que você abrir clicando duas vezes em uma seleção de uma dessas janelas será gravada.
- Posições das janelas
- Tamanhos das janelas, inclusiva da janela do aplicativo
- Posições das guias
- Navegador ancorado ou flutuante e exibido ou oculto

Para gravar suas preferências

1. Clique em *Arquivo* > *Gravar Preferências* ou clique no botão *Gravar Preferências*.

Mudando a senha do Sentinel Control Center

NOTA: Para obedecer às rígidas configurações de segurança exigidas pela Certificação de Critérios Comuns, a Novell exige uma senha forte com as seguintes características:

1. Escolha senhas com no mínimo 8 caracteres, que incluam ao menos um dígito em MAIÚSCULA, um em minúscula, um símbolo especial (!@#$%^&*()_+), e um dígito numérico (0-9).

2. A senha não pode conter o nome usado no e-mail nem partes do nome completo.

3. A senha não deve ser uma palavra “comum” (por exemplo, não deve ser uma palavra registrada em dicionário nem gíria de uso comum).

4. A senha não deve conter palavras de idioma algum, pois existem vários programas de invasão de senha capazes de verificar milhões de possibilidades de combinações de palavras em segundos.

5. Escolha uma senha de que possa se lembrar, mas que seja complexa. Por exemplo, Mft5#AIdade (meu filho tem 5 anos de idade) OU EmnCh5#a (eu moro na Califórnia há 5 anos).

Para mudar sua senha do Sentinel Control Center

1. Clique em *Opções* > *Mudar Senha*.
2. Digite a senha antiga.
3. Digite a nova senha duas vezes para confirmá-la.

NOTA: A Novell recomenda, como melhor prática, uma extensão mínima de senha de oito caracteres que incluam alfanuméricos.

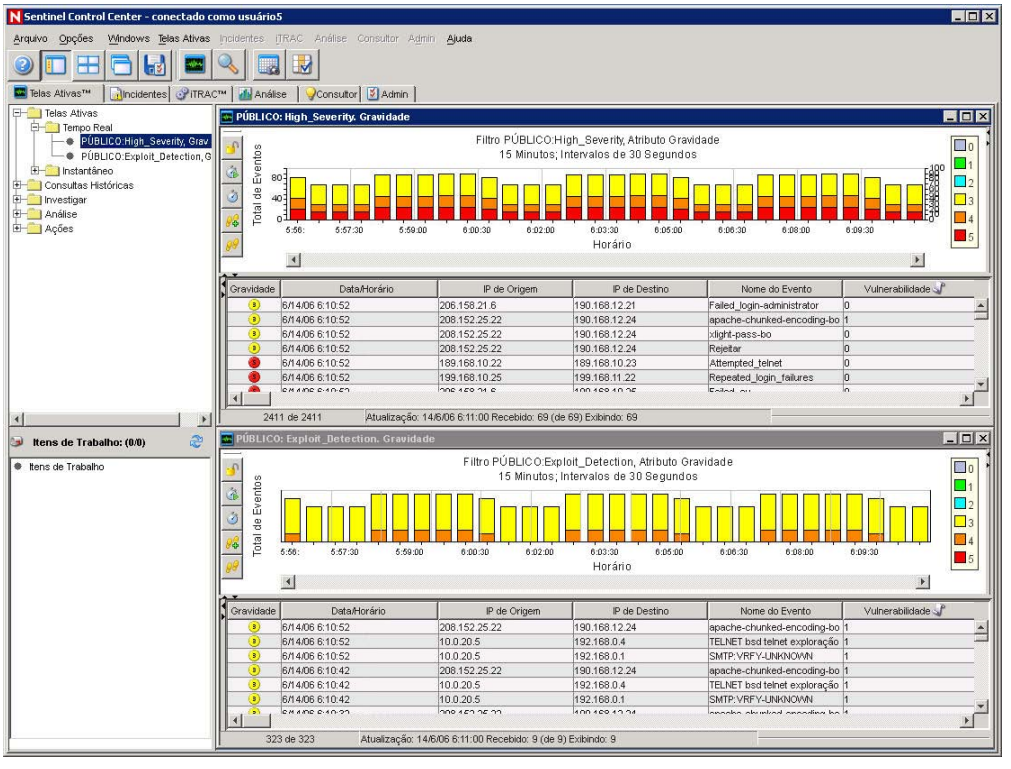
4. Clique em *OK*.

3 Guia Active Views™

NOTA: O termo Agente é intercambiável com Coletor. Mais adiante, Agentes será referido como Coletores.

Você deve ter a permissão adequada para usar a guia Active Views™. Caso esta permissão não seja concedida, nenhuma das permissões relacionadas às ações que usam esta guia estará disponível.

A guia Active Views permite monitorar eventos quase em tempo real e realizar consultas nesses eventos. Você pode monitorá-los no formato de tabela ou por meio de representação gráfica 3D em barras, 2D de barra empilhada, linhas ou faixas.

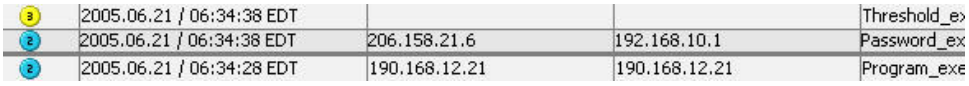


Guia Active Views - Descrição

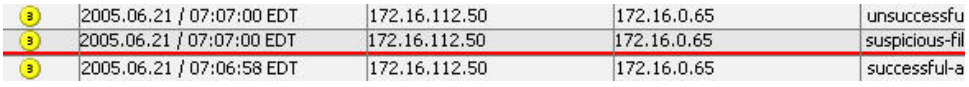
As telas de eventos são apresentadas no formato de tabela. A configuração da tela ativa é determinada pelo arquivo das_rt.xml. Uma Tabela de Eventos Quase em Tempo Real com uma apresentação gráfica e o Instantâneo são os dois tipos de Active Views.

- Tabela de Eventos Quase em Tempo Real
  - Contém até 750 eventos por período de 30 segundos.

- Por padrão, o cliente mantém um período de 24 horas de eventos em cache. É possível mudar essa configuração usando as Propriedades do Active Views.
- Por padrão, a tabela exibirá um máximo de 30.000 eventos. É possível mudar essa configuração usando as Propriedades do Active Views.
- Por padrão, a tabela de eventos é atualizada a cada 30 segundos (atraso de envio). Essa condição é representada por uma linha cinza na tabela de eventos.



Quando ocorrem mais de 750 eventos a cada 30 segundos, uma linha de separação vermelha aparece indicando que há eventos além dos exibidos.



- Quando as preferências do usuário são gravadas, a tabela continua a coletar dados por até 4 dias. Por exemplo, se você gravar as preferências, efetuar logout e voltar a efetuar login no dia seguinte, sua Tela Ativa exibirá todos os dados como se você não tivesse efetuado logout.
- Se uma Tela Ativa for criada e não gravada, ela continuará a coletar dados por até uma hora. Nesse período de uma hora, se uma Tela Ativa idêntica for criada, exibirá os dados referentes à última hora.

- Instantâneo – telas com marcação de horário de uma tabela de Telas de Eventos em Tempo Real.

As características a seguir tornam uma Tela Ativa exclusiva.

- Um filtro atribuído a uma Tela Ativa;
- O atributo Eixo Z;
- O filtro de segurança atribuído a um usuário.

A Guia Active Views permite acessar:

- Reconfigurar Active Views
- Adicionar Eventos a um incidente
- Fechar um Instantâneo ou janela de Navegador Visual
- Criar um incidente
- Personalizar Opções de Menu com Eventos
- Apagar uma janela de Instantâneo ou Navegador Visual
- Consultas de Eventos
- Mapa de Gráficos
- Visualizar Dados do Consultor
- Gerenciar Colunas
- Enviar mensagens sobre Eventos por e-mail
- Mostrar ou Ocultar Detalhes de Eventos
- Instantâneo de uma Janela do Navegador Visual
- Visualizar Eventos que acionaram um evento correlacionado
- Tela de Visualização de Vulnerabilidade
- Visualizar Dados de Bens
- Executar HP – Operações OpenView e Service Desk
- Executar Operações de Resolução

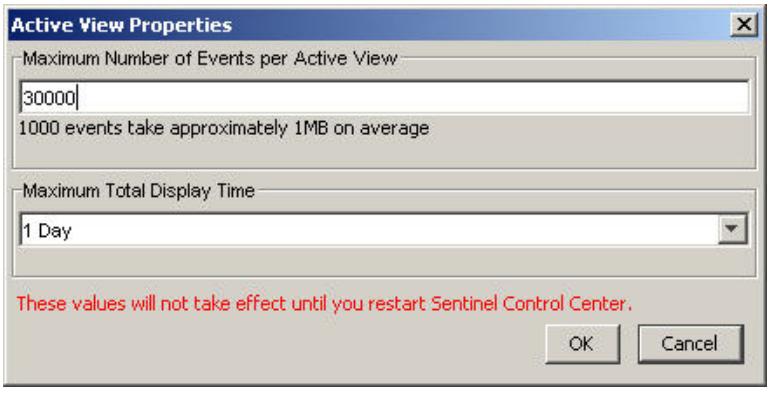
Um usuário pode mudar valores (nomes de colunas) para exibir nomes lógicos e preenchê-los em todo o sistema. É possível aplicar ao fluxo de eventos atributos relevantes para a sua empresa. Para obter mais informações, consulte o *Guia do Usuário do Assistente*, *Capítulo 10 – Gerenciador de Dados do Sentinel*, e *o Guia de Referência do Usuário do Sentinel*.

Reconfigurar o valor de cache e o máximo de eventos de Active Views

As Propriedades do Active Views permitem configurar o número máximo de eventos que podem ser exibidos em uma Tela Ativa e o tempo em cache em cada cliente. O padrão para o número total de eventos em uma Tela Ativa é de 30.000 eventos. O valor padrão para o tempo em cache em uma Tela Ativa é de 24 horas.

Para configurar o Número Máximo de Eventos por Tela Ativa e o Valor em Cache

1. Clique na guia *Active Views.*
2. Clique em *Active Views* > *Propriedades*.
3. Faça as alterações.



Os novos valores entrarão em vigor apenas quando você reiniciar o Sentinel Control Center.

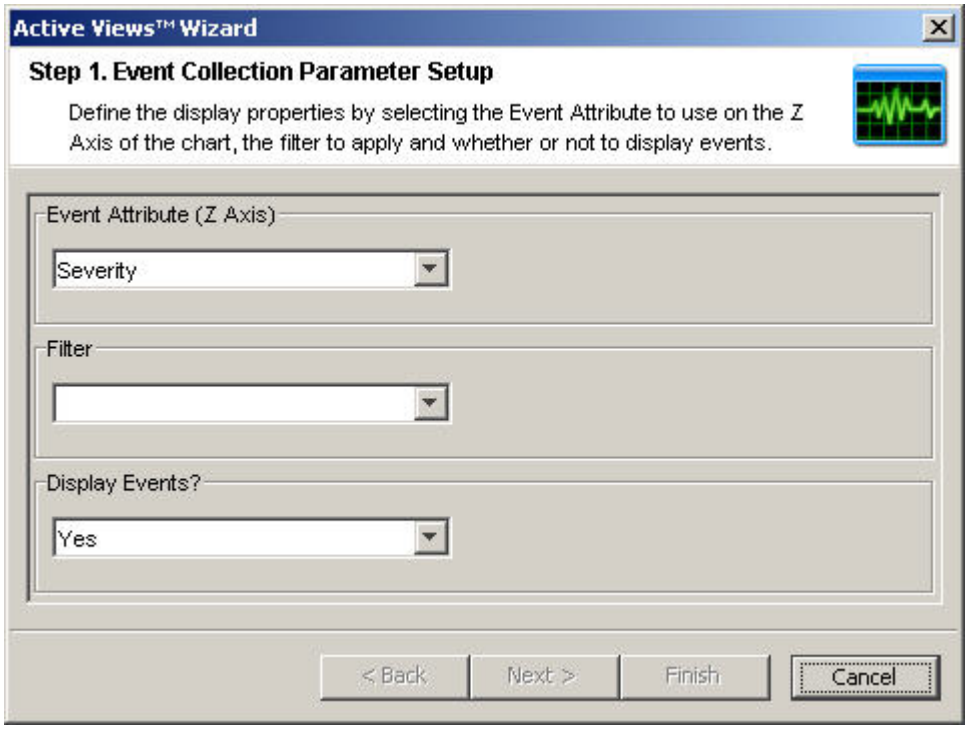
Para visualizar eventos em tempo real

Para visualizar eventos em tempo real

1. Clique na guia *Active Views.*
2. Clique em *Active Views* > *Criar Tela Ativa* ou no botão *Criar Tela Ativa*.

3. Na janela Assistente de Visualização de Eventos, clique nas setas para baixo para selecionar seu eixo Z, Filtro e para Exibir Eventos (Sim ou Não).

NOTA: Na janela de seleção de filtro, você pode desenvolver seu próprio filtro ou selecionar um dos já definidos. A seleção do filtro *Todos* permite que todos os eventos apareçam na janela. Se o filtro atribuído a uma Tela Ativa for mudado ou apagado após a criação da Tela Ativa, essa tela não será afetada.



Depois de fazer a seleção, clique em *Avançar* ou *Concluir*. Se você clicar em *Concluir*, serão escolhidos os seguintes valores padrão:

- Taxa de Atualização e Exibição de 30 segundos
- Tempo de exibição de 15 minutos
- Eixo Y como Total do Evento
- Tipo de gráfico - 2D de barra empilhada

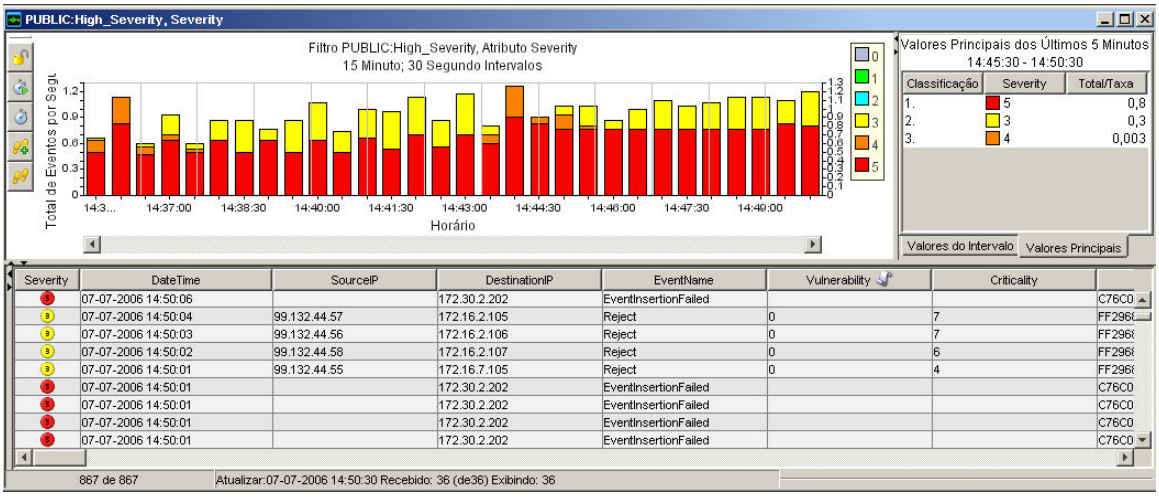
4. Se você clicar em *Avançar*, clique nas setas para baixo para selecionar:
   - Taxa de Atualização e Exibição – número de segundos para atualização da taxa de eventos
   - Tempo de Exibição – tempo de exibição do gráfico
   - Eixo Y – Total de Eventos ou Total de Eventos por Segundo

   Clique em *Avançar*.
5. Selecione o tipo de gráfico. Clique em *Avançar*.
   - Tipo de gráfico – 3D em barras, 2D de barra empilhada, linhas ou faixas
6. Além da seleção do filtro, é possível refinar ainda mais a tabela de eventos. Você tem as condições de opções a seguir:
   - Nenhum
   - exatamente
   - não é
   - é (menor do que)
   - é <= (menor do que ou igual a)
   - é > (maior do que)
   - é >= (maior do que ou igual a)
   - contém
   - não contém
   - vazio
   - não está vazio

Depois que você criar os critérios, clique no botão *Adicionar à Lista*. Clique em *Concluir*.

NOTA: Depois de criar a tela, você pode editar ou remover esse refinamento da tabela de eventos clicando o botão direito do mouse na área do gráfico e selecionando as propriedades. Para obter mais informações, consulte Para redefinir parâmetros, tipo de gráfico ou tabela de eventos de uma Tela Ativa.

Seu gráfico ficará semelhante a este:



NOTA: Propriedades de Active Views – a opção Refinar Tabela de Eventos não afetará a representação gráfica.

Os cinco botões à esquerda do gráfico executam as seguintes funções:

- Bloquear/Desbloquear o Gráfico – usada para detalhar, ampliar, reduzir, aplicar zoom para seleção e gravar um gráfico como arquivo html.
- Aumentar Intervalo de Exibição – aumenta o intervalo de exibição dos eventos recebidos.
- Diminuir Intervalo de Exibição – diminui o intervalo de exibição dos eventos recebidos.
- Aumentar Tempo de Exibição – aumenta o intervalo ao longo do eixo X.
- Diminuir Tempo de Exibição – diminui o intervalo ao longo do eixo X.

Quando você clica no botão *Bloquear*, os seguintes botões adicionais tornam-se disponíveis:

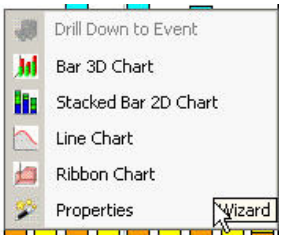
- Bloquear/Desbloquear o Gráfico – usada para detalhar, ampliar, reduzir, aplicar zoom para seleção e gravar um gráfico como arquivo html.
- Ampliar – amplia sem mudar as configurações de tempo do gráfico
- Reduzir – reduz sem mudar as configurações de tempo do gráfico
- Zoom para Seleção – amplia uma seleção de intervalos dos eventos.
- Grava os detalhes do navegador como um arquivo html com gráficos como imagens e eventos em formato tabular.

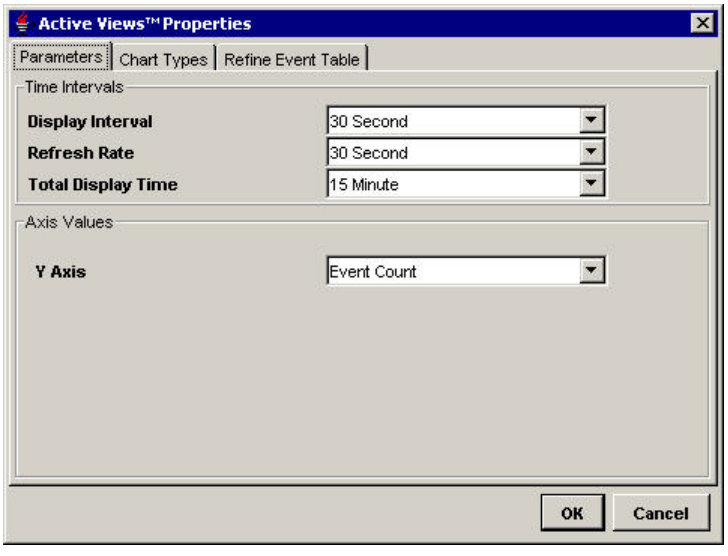
Para redefinir parâmetros, tipo de gráfico ou tabela de eventos de uma Tela Ativa

Ao visualizar uma Tela Ativa, você pode redefinir os parâmetros e mudar o tipo do gráfico. Além disso, se houver eventos de seu interesse, poderá separá-los de outros eventos em vez de criar um nova Tela Ativa e filtro.

Para redefinir os parâmetros, tipo de gráfico ou tabela de eventos de uma Tela Ativa

1. Em uma Tela Ativa que exibe um gráfico, clique o botão direito do mouse e selecione *Propriedades*.



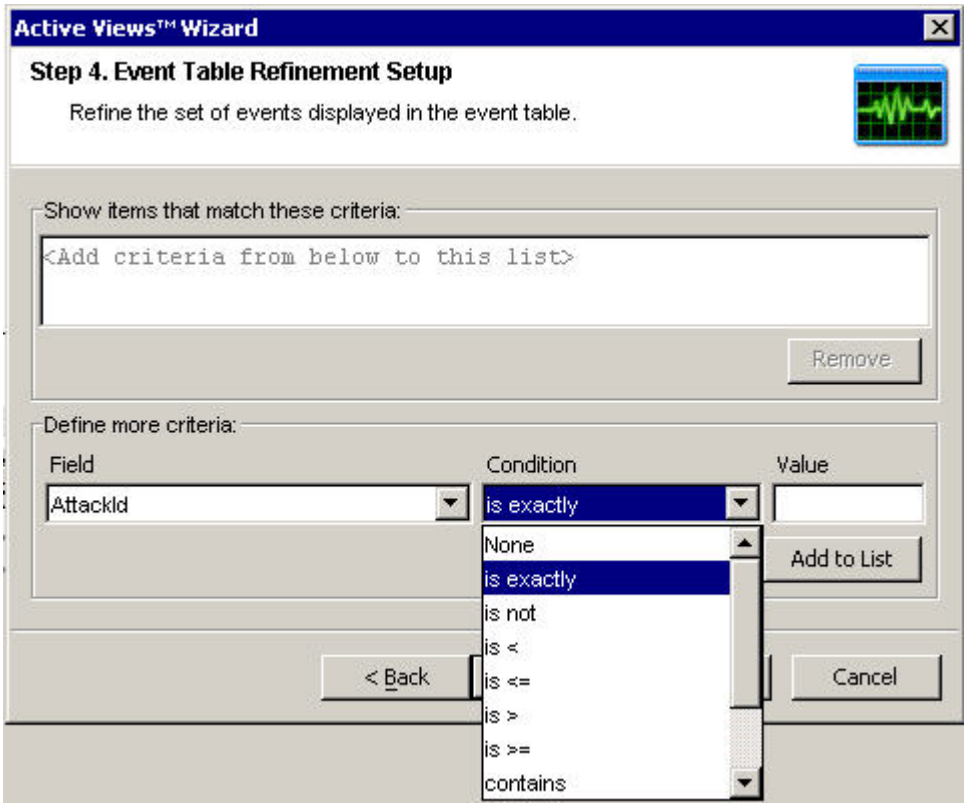


Na guia Parâmetros, você pode definir:

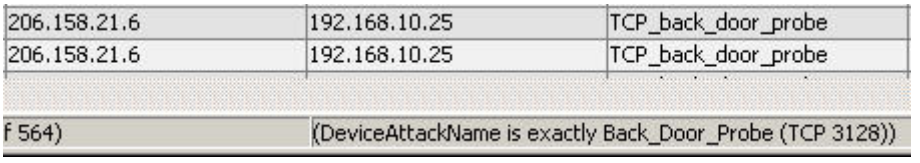
- Intervalo de Exibição – tempo entre cada intervalo
- Taxa de Atualização – número de segundos para atualização da taxa de eventos
- Tempo Total de Exibição – tempo de exibição do gráfico
- Eixo Y – Total de Eventos ou Total de Eventos por Segundo

Na guia Tipos de Gráficos, você pode definir seu gráfico como 3D em barras, 2D de barra empilhada, linhas e faixas.

Em Refinar Tabela de Eventos, você pode filtrar o campo Eventos em sua Tela Ativa.



Por exemplo, você pode filtrar os eventos com uma entrada específica no campo, por exemplo, DeviceAttackName é exatamente Back_Door_Probe (TCP 3128). Isso resultará em uma tabela com eventos que contêm somente DeviceAttackName equivalente a Back_Door_Probe (TCP 3128).



Ao refinar uma tabela de eventos, você verá os critérios de filtro na parte inferior direita da tabela.

Girando um gráfico 3D em barras ou faixas

Para girar um gráfico 3D em barras ou faixas

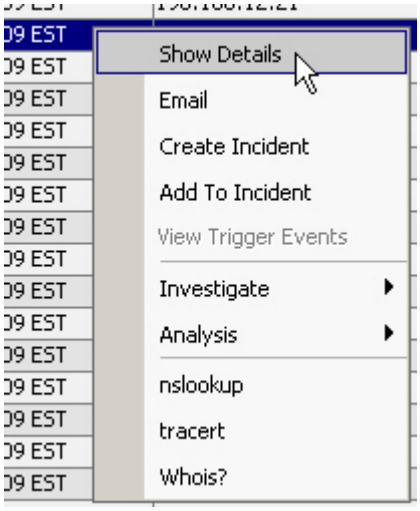
1. Clique em qualquer lugar do gráfico e mantenha o botão do mouse pressionado.
2. Reposicione o gráfico conforme desejado movendo o mouse com o botão pressionado.

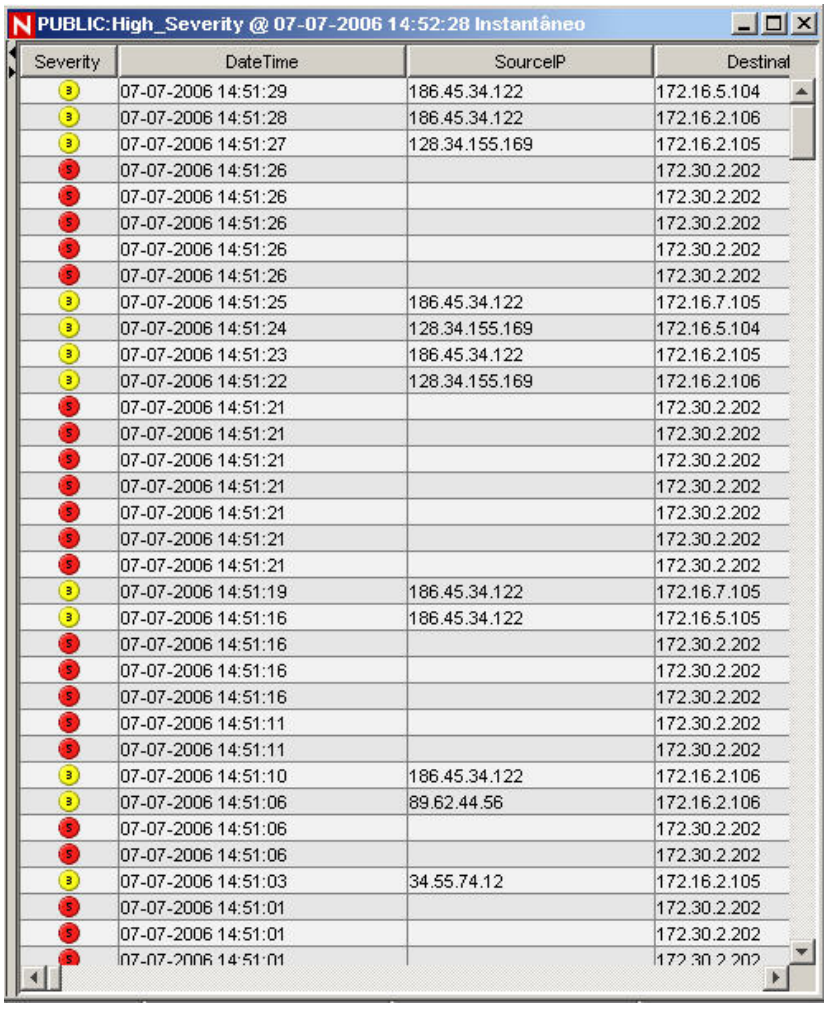
Mostrando ou ocultando detalhes de eventos

Para mostrar detalhes de eventos

1. Em uma tabela Tempo Real de Evento do Navegador Visual ou Instantâneo, clique duas vezes ou clique o botão direito do mouse em um evento e clique em *Mostrar*

Detalhes. Os detalhes de um evento serão exibidos no painel esquerdo da tabela Tempo Real de Evento.





2. Se você quiser ver detalhes como a hora em que abriu o Sentinel Control Center, clique em *Arquivo* > *Gravar Preferências* ou clique no botão *Gravar Preferências do Usuário*.

Para ocultar detalhes de um evento

1. Em uma tabela Tempo Real de Evento do Navegador Visual ou Instantâneo, com os detalhes dos eventos exibidos no painel esquerdo, clique duas vezes ou clique o botão direito do mouse em um evento e clique em *Mostrar Detalhes*. A janela de detalhes do evento será fechada.
2. Se você não quiser ver detalhes exibidos ao abrir novamente o Sentinel Control Center, clique em *Arquivo* > *Gravar Preferências* ou clique no botão *Gravar Preferências do Usuário*.

Enviando mensagens sobre eventos e incidentes por e-mail

A capacidade de enviar e-mails é definida no arquivo execution.properties durante a instalação. Esse arquivo pode ser editado após a instalação. Este é o local do arquivo:

Para Windows:

```
%ESEC_HOME%\sentinel\config
```

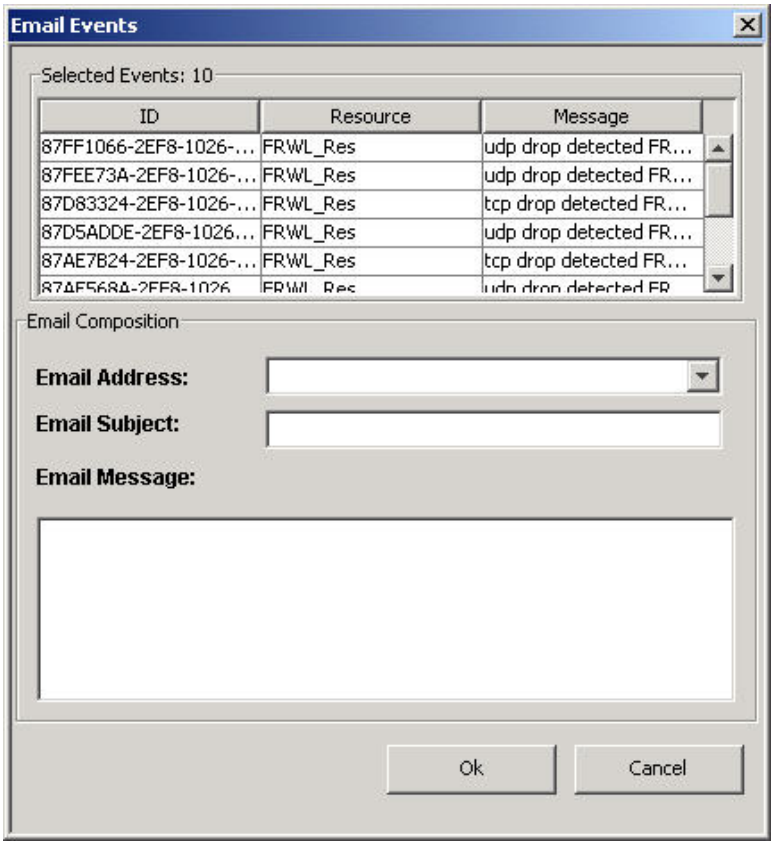
Para UNIX:

```
$ESEC_HOME/sentinel/config
```

Para obter mais informações, consulte o capítulo 11, *Utilitários, Configurando e-mails do Sentinel*.

Para enviar uma mensagem de evento por e-mail

1. Em uma tabela Tempo Real de Evento do Navegador Visual ou Instantâneo, selecione um evento ou grupo de eventos, clique o botão direito do mouse e selecione *E-mail*.



2. Preencha os seguintes campos:
   - Endereço de E-mail
   - Assunto do E-mail
   - Mensagem de E-mail
3. Clique em *OK*.

Para enviar uma mensagem de incidente por e-mail

1. Depois de gravar o incidente, clique na guia Incidentes, *Incidentes > Exibir Gerenciador de Telas de Incidentes*.
2. Clique duas vezes em *Todos os Incidentes.*
3. Clique duas vezes em um Incidente.
4. Clique no botão *Incidente de E-mail*  .
5. Digite:
   - Endereço de E-mail
   - Assunto do E-mail
   - Mensagem de E-mail
6. Clique em *OK*. A mensagem de e-mail terá anexos em html com detalhes do incidente, eventos, bens, vulnerabilidades, informações do consultor e histórico do incidente.

Criando um incidente

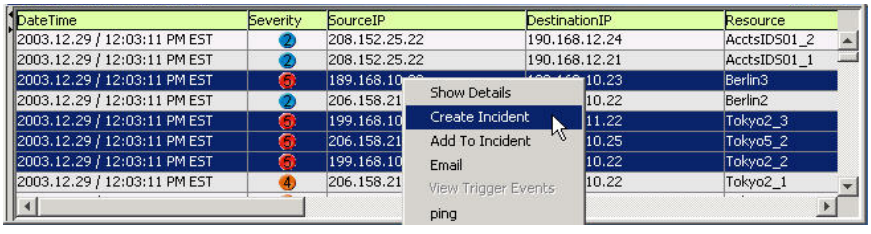
Para executar esta função, você deve ter a permissão do usuário Criar Incidente(s).

Essa função é útil no agrupamento de um conjunto de eventos reunidos como um todo, representando alguma coisa de interesse (um grupo de eventos semelhantes ou um conjunto de eventos diferentes que indicam um padrão de interesse, como um ataque).

NOTA: Se os eventos não forem exibidos inicialmente em um Incidente recém-criado, a causa provável é uma lacuna entre o momento da exibição na janela Eventos em Tempo Real e o instante da inserção no banco de dados. Se isso ocorrer, aguarde alguns minutos para que os eventos originais sejam finalmente inseridos no banco de dados e exibidos no incidente.

Para criar um incidente

1. Em uma tabela Tempo Real de Evento do Navegador Visual ou uma Tabela de Tempo Real de Eventos de Instantâneos, selecione um evento ou grupo de eventos, clique o botão direito do mouse e selecione *Criar Incidente*.



   Na janela Novo Incidente, estão as seguintes guias:

   - Eventos – mostra quais eventos compõem o incidente
   - Bens – mostra os bens afetados
   - Vulnerabilidade – mostra as vulnerabilidades relacionadas aos bens
   - Consultor – ataque a um bem e informações de alerta
   - Workflow – nesta guia, você atribui um WorkFlow (iTrac)
   - Histórico – histórico do Incidente
   - Anexos – é possível anexar qualquer documento ou arquivo de texto com informações pertinentes a este incidente

   Na caixa de diálogo Criar Incidente, preencha o seguinte:

   - Título
   - Estado
   - Gravidade
   - Prioridade
   - Categoria
   - Responsável – a conta de usuário atribuída ao caso
   - Descrição
   - Resolução

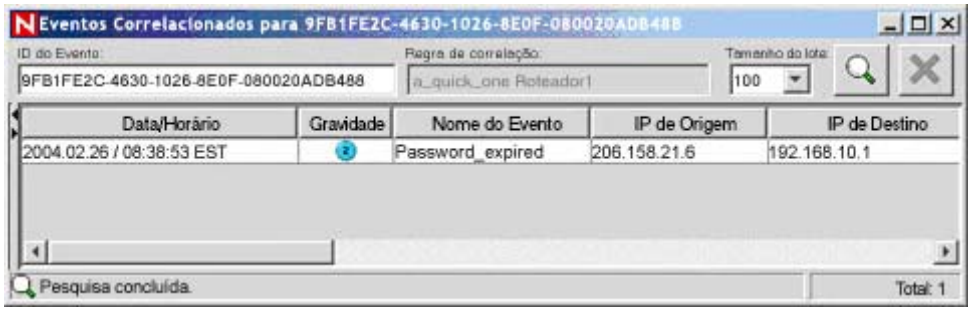
2. Clique em *Gravar*. O incidente é adicionado na guia Incidentes do Sentinel Control Center.

Visualizando os eventos que acionaram um evento correlacionado

Você deve clicar o botão direito do mouse em um evento correlacionado para ver quais eventos acionaram aquele evento correlacionado. Na tabela da qual você está selecionando o evento, olhe no painel de exibição de resumo à direita e procure um evento com a propriedade SensorType com um Valor de C (C: evento correlacionado) ou W (W: watchlist).

Para visualizar os eventos que acionaram um evento correlacionado

1. Em uma tabela Tempo Real de Evento do Navegador Visual ou Instantâneo, ou uma Consulta de Eventos, clique o botão direito do mouse em um evento correlacionado e selecione Mostrar Eventos Acionadores. Será aberta uma janela mostrando os eventos que acionaram a regra e o nome da Regra de Correlação.



Investigando um ou mais eventos

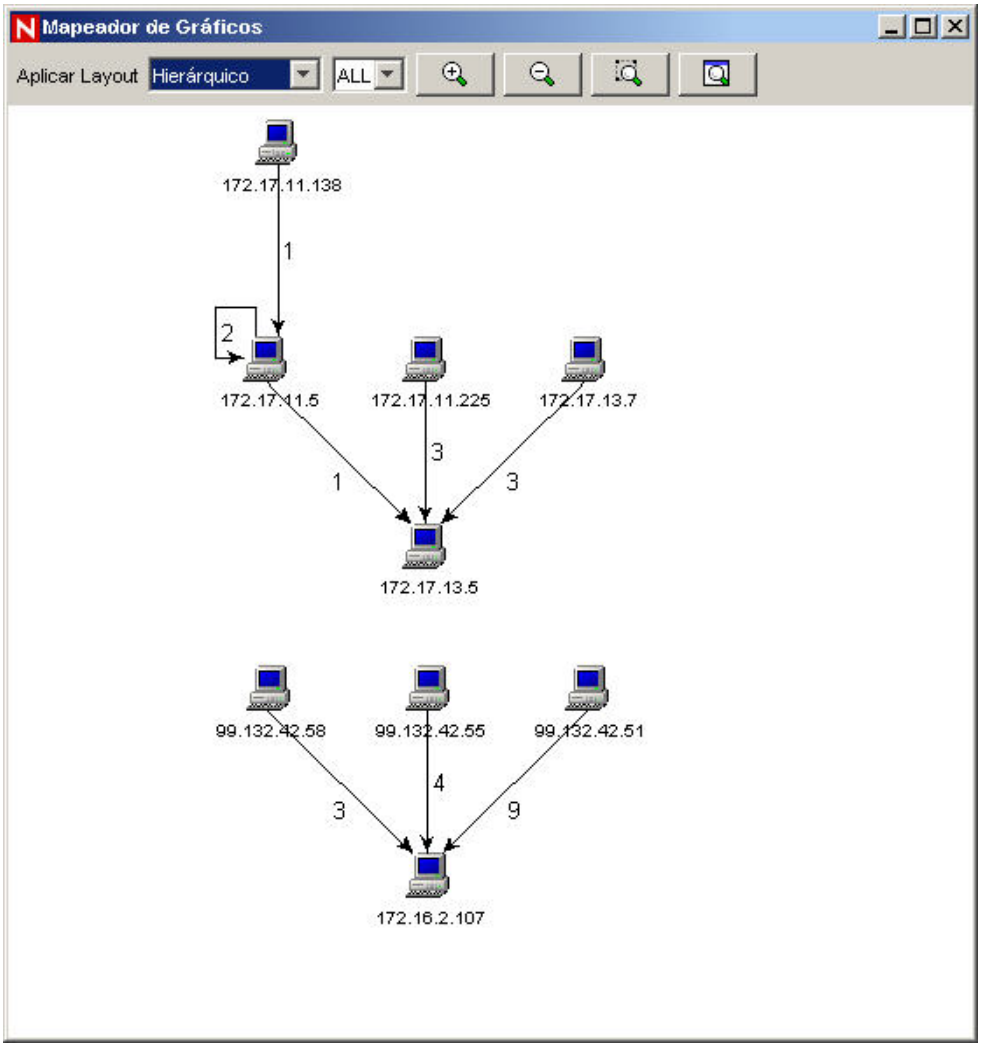
Essa função permite:

- Exibir graficamente os campos de origem (IP, porta, evento, tipo de sensor, nome de Coletor etc.) mapeados a campos de destino (IP, porta, evento, tipo de sensor, nome de Coletor etc.) de eventos selecionados.
- Executar uma Consulta de Eventos referentes à última hora de um único evento para:

  NOTA: Você não pode executar uma consulta sobre um campo nulo (vazio).

  - Endereços IP de Destino
  - Endereços IP de Origem
  - Nome do evento

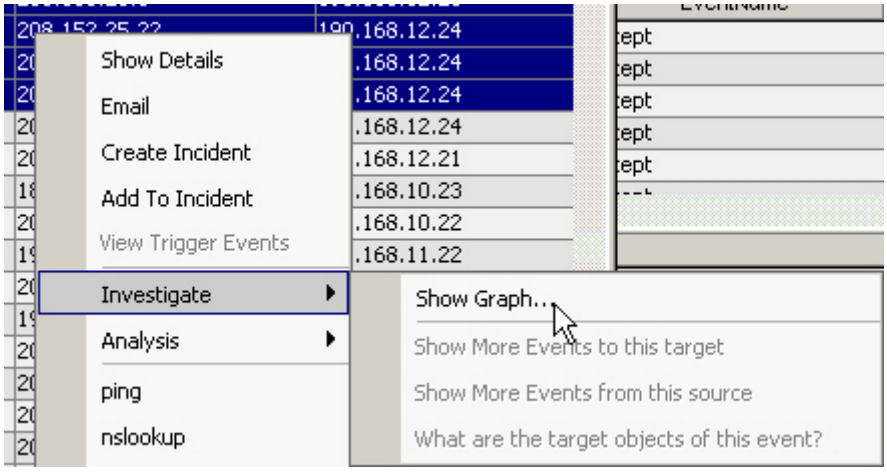
Segue uma ilustração dos endereços IP de origem e de destino.



Investigar – Mapeador de Gráficos

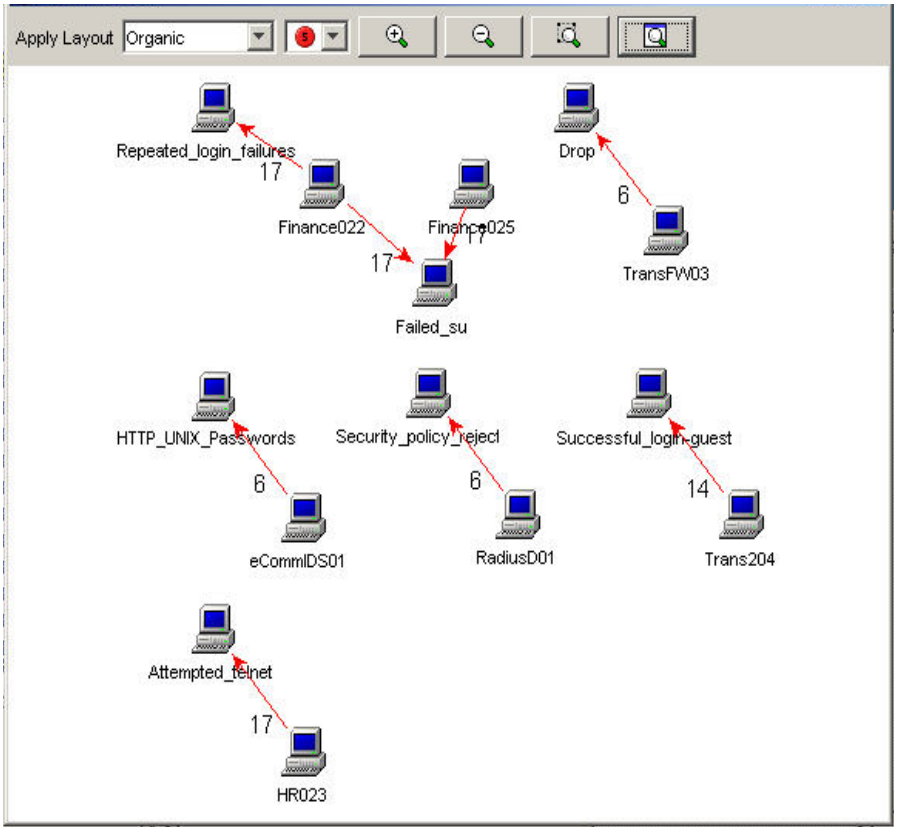
Para criar um mapa de gráficos

1. No Tempo Real de um Evento do Navegador Visual ou Instantâneo, clique o botão direito do mouse em um ou mais eventos e clique em *Investigar* > *Visual* > *Mostrar Gráfico*.



Segue uma descrição gráfica do Nome do Sensor para o Nome do Evento de gravidade 5 em um formato orgânico. Você pode visualizar um mapeamento de gráficos nos seguintes formatos:

- Circular
- Hierárquico
- Orgânico
- Ortogonal



Investigar – Consulta de Eventos

Esta função permite consultar eventos ocorridos na última hora.

Para executar uma Consulta de Eventos usando a função Investigar

1. Em uma janela do Navegador Visual ou Instantâneo, *clique o botão direito do mouse em um evento e clique em Investigar > < selecione uma das três opções abaixo>*

Opção	Função
Mostrar Mais Eventos para este destino	Endereço IP de Destino
Mostrar Mais Eventos desta fonte	Endereço IP de Origem
Quais os objetos de destino deste evento?	Nome do evento

Análise – Visualizando os dados do Consultor

O Consultor fornece uma referência cruzada entre assinaturas de ataque IDS em tempo real e sua base de conhecimento de vulnerabilidades. O Consultor possui uma alimentação de alerta e ataque. Além disso, contém informações sobre vulnerabilidades e vírus. A alimentação de ataque relaciona as explorações associadas às vulnerabilidades.

Estes são os sistemas de detecção de intrusão suportados:

- Cisco Secure IDS
- Enterasys Dragon Host Sensor
- Enterasys Dragon Network Sensor
- ISS BlackICE PC Protection
- ISS RealSecure Desktop
- ISS RealSecure Network
- ISS RealSecure Server Sensor
- ISS RealSecure Guard
- Snort/Sourcefire
- Symantec ManHunt
- Symantec Intruder Alert
- McAfee IntruShield

O Coletor de IDS preenche o campo DeviceAttackName (rt1) de um evento. O Consultor usa essas informações para gerar as informações de ataque e vulnerabilidade. Estes são alguns exemplos de vulnerabilidades:

- FINGER: Cfinger Search Probe
- SMTP: SmartServer3 MAIL FROM Buffer Overflow
- HTTP: Dragon Fire IDS Web Interface Remote Execution
- FTP:MKDIR-DOS
- hp-printer-flood
- wh00t-backdoor
- nt-telnet
- FINGER / execution attempt
- tellurian-tftpdnt-filename-bo
- FTP MKD Stack Overflow

Para visualizar os dados do Consultor

1. Em uma tabela Tempo Real de Evento do Navegador Visual ou Instantâneo, clique o botão direito do mouse em um ou mais eventos selecionados e clique em *Análise > Dados do Consultor*. Se o campo DeviceAttackName estiver devidamente preenchido, aparecerá um relatório semelhante ao deste exemplo. O relatório a seguir é um exemplo de um WEB-MISC amazon 1-click cookie theft.

Análise – Visualizando dados de bens

Esta função permite visualizar e gravar sua tela como um arquivo HTML do Relatório de Bens. Você deve executar o Coletor de gerenciamento de bens para visualizar estes dados. Estes são os dados disponíveis para visualização:

Hardware

- Endereço MAC
- Nome
- Tipo
- Fornecedor
- Produto
- Versão
- Valor
- Importância
- Distinção
- Ambiente
- Local

Rede

- Endereço IP
- HostName

Software

- Nome
- Tipo
- Fornecedor
- Produto
- Versão

Contatos

- Ordem
- Nome
- Função
- E-mail
- Telefone

Local

- Sala
- Rack
- Endereço

Para visualizar os Dados de Bens

1. Em uma tabela Tempo Real de Evento do Navegador Visual ou janela do Instantâneo, clique o botão direito do mouse em um ou mais eventos e clique em *Análise* > *Dados de Bens*. Será exibida uma janela parecida com esta.

Asset Report

desk.acmeinc.net

Hardware

MAC Address	A0:12:56:78:90:00		
Name	Build Machine	**Value**	500
Type	Server	**Criticality**	High
Vendor	Dell	**Sensitivity**	Low
Product	Precision	**Environment**	Production
Version	360	**Location**	Internal

Network

IP	Hostname
199.16.2.23	desk.acmeinc.net

Software

Name	Type	Vendor	Product	Version
ClearCase	APPLICATION	IBM	ClearCase	5.0
C++	APPLICATION	Microsoft	Visual C++	6.0

Contacts

Order	Name	Role	Email	Phone Number
1	Erickson, Stein	USER	serickson@acmedomain.net	(703) 555-8865
2	IT	Administrator	LAN_FOLKS@acemedomain.net	(703) 555-9876

Location

Room	server room
Rack	#17
Address	HQ Agent 86 Security Circle Suite 86 Washington DC 12345 USA

Análise - Visualização de vulnerabilidade

A Novell tem Coletores disponíveis que processam explorações de vulnerabilidade do Nessus, do ISS, do Foundstone, do eEye e explorações do Qualys. A Visualização de Vulnerabilidade oferece uma representação gráfica de dados de evento em tempo real em relação a sistemas vulneráveis e que fica disponível em um evento para vulnerabilidade atual e no momento do evento.

Esse recurso recupera e exibe os dados de vulnerabilidade referentes aos IP's de destino dos eventos selecionados. Para obter mais informações, consulte a documentação dos Coletores em PDF localizada em %ESEC_HOME%\wizard\elements\<Collector name>\doc. Você deve ter um dos Coletores de Scanner carregados e em execução para obter quaisquer dados de vulnerabilidade.

NOTA: O Coletor de vulnerabilidade reúne informações, não eventos.

A visualização da vulnerabilidade pode ser exibida nos formatos:

- HTML
- gráfico
  - circular (orgânico)
  - hierárquico
  - todos
  - Nós de Eventos Mapeados
  - ortogonal

A visualização em HTML é um tipo de relatório que relaciona:

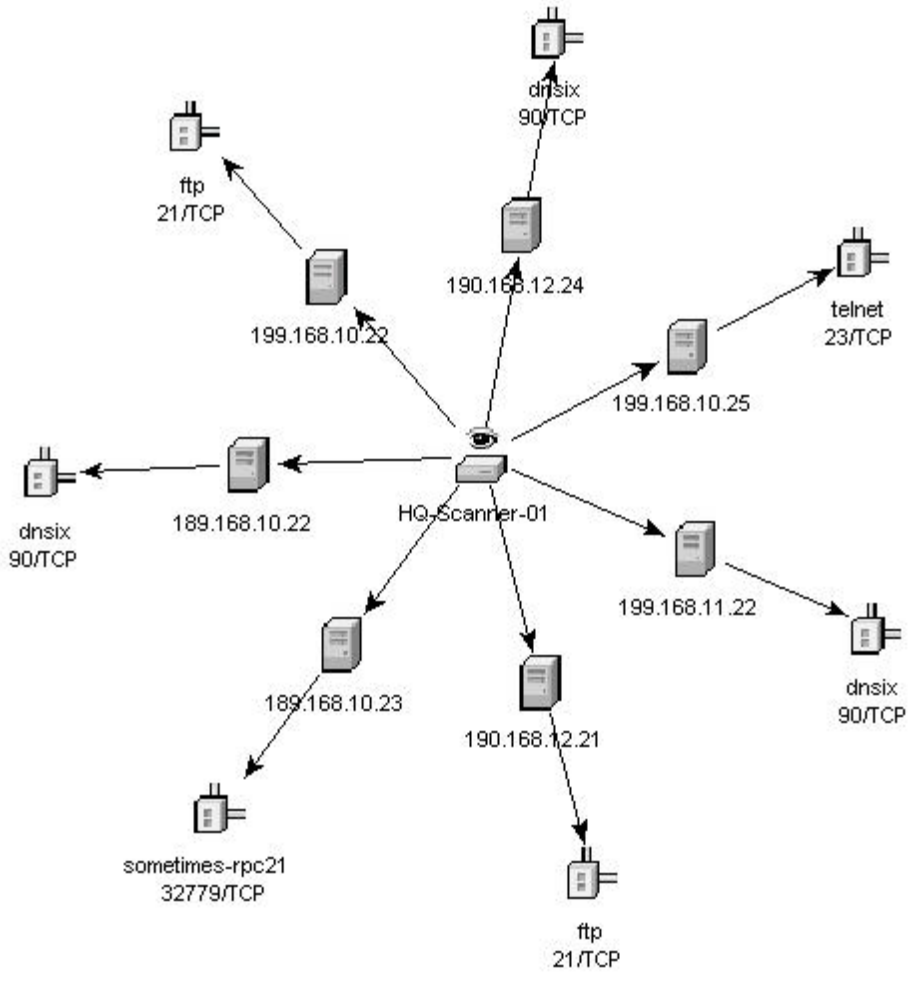
- IP
- host
- vulnerabilidade
- porta/protocolo

Segue um exemplo de uma exploração do Nessus.

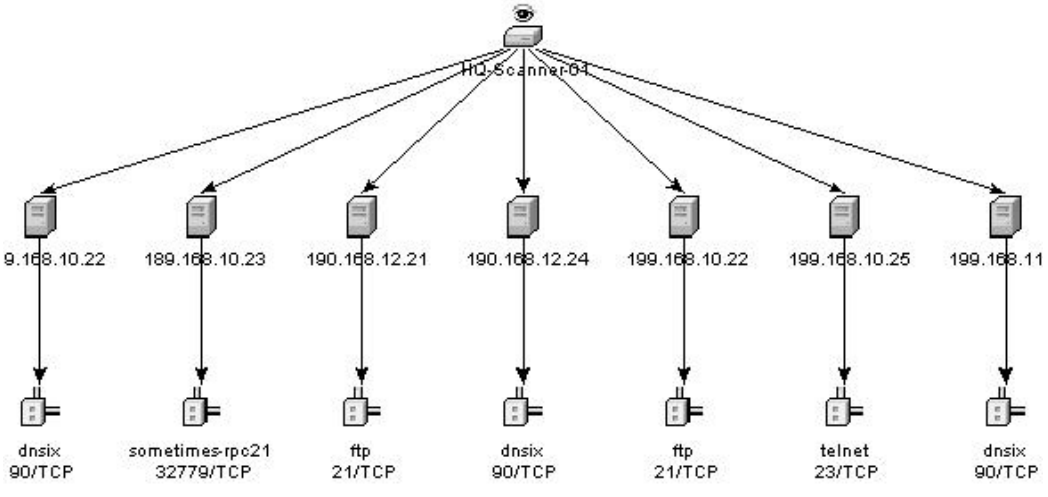
Vulnerability Summary

IP	Host	Vulnerabilities	Port/Protocol
172.16.0.132		18	0|/TCP, 21(ftp)/TCP, 21(ftp)/TCP, 21(ftp)/TCP, 22(ssh)/TCP, 22(ssh)/TCP, 22|ssh)/TCP, 23(telnet|/TCP, 23|telnet)/TCP, 25(smtp|/TCP, 25(smtp|/TCP, 25(smtp|/TCP, 587(submission)/TCP, 587(submission)/TCP, 587|submission)/TCP, 1241(nessus)/TCP, 1241|nessus|/TCP, 3306(mysql)/TCP
172.16.0.71		49	0|/TCP, 0()/TCP, 21(ftp)/TCP, 21(ftp)/TCP, 22(ssh)/TCP, 23(telnet)/TCP, 23|telnet)/TCP, 23(telnet)/TCP, 25|smtp)/TCP, 25(smtp|/TCP, 25(smtp|/TCP, 25(smtp|/TCP, 25|smtp)/TCP, 25|smtp)/TCP, 25(smtp)/TCP, 25(smtp)/TCP, 25(smtp|/TCP, 25(smtp|/TCP, 90(dnsix)/TCP, 90(dnsix|/TCP, 90(dnsix)/TCP, 90(dnsix)/TCP, 90(dnsix)/TCP, 90|dnsix)/TCP, 90|dnsix)/TCP, 90|dnsix)/TCP, 111(sunrpc)/TCP, 111|sunrpc)/TCP, 161|snmp)/UDP, 512(exec|/TCP, 513(login)/TCP, 514|shell|/TCP, 587(submission|/TCP, 587(submission|/TCP, 587(submission)/TCP, 587(submission)/TCP, 587|submission)/TCP, 587|submission)/TCP, 587(submission|/TCP, 587(submission|/TCP, 587(submission)/TCP, 587(submission)/TCP, 6000(x11)/TCP, 7100(font-service)/TCP, 32778(sometimes-rpc19)/TCP, 32779(sometimes-rpc21)/TCP, 32779(sometimes-rpc21)/TCP, 32779(sometimes-rpc21)/TCP
172.16.0.132		18	0|/TCP, 21(ftp)/TCP, 21(ftp)/TCP, 21(ftp)/TCP, 22(ssh)/TCP, 22(ssh)/TCP, 22|ssh)/TCP, 23(telnet|/TCP, 23|telnet)/TCP, 25(smtp|/TCP, 25(smtp|/TCP, 25(smtp|/TCP, 587(submission)/TCP, 587(submission)/TCP, 587|submission)/TCP, 1241(nessus)/TCP, 1241|nessus|/TCP, 3306(mysql)/TCP
172.16.0.71		49	0|/TCP, 0()/TCP, 21(ftp)/TCP, 21(ftp)/TCP, 22(ssh)/TCP, 23(telnet)/TCP, 23|telnet)/TCP, 23(telnet)/TCP, 25|smtp)/TCP, 25(smtp|/TCP, 25(smtp|/TCP, 25(smtp|/TCP, 25|smtp)/TCP, 25|smtp)/TCP, 25(smtp)/TCP, 25(smtp)/TCP, 25(smtp|/TCP, 25(smtp|/TCP, 90(dnsix)/TCP, 90(dnsix|/TCP, 90(dnsix)/TCP, 90(dnsix)/TCP, 90(dnsix)/TCP, 90|dnsix)/TCP, 90|dnsix)/TCP, 90|dnsix)/TCP, 111(sunrpc)/TCP, 111|sunrpc)/TCP, 161|snmp)/UDP, 512(exec|/TCP, 513(login)/TCP, 514|shell|/TCP, 587(submission|/TCP, 587(submission|/TCP, 587(submission)/TCP, 587(submission)/TCP, 587|submission)/TCP, 587|submission)/TCP, 587(submission|/TCP, 587(submission|/TCP, 587(submission)/TCP, 587(submission)/TCP, 6000(x11)/TCP, 7100(font-service)/TCP, 32778(sometimes-rpc19)/TCP, 32779(sometimes-rpc21)/TCP, 32779(sometimes-rpc21)/TCP, 32779(sometimes-rpc21)/TCP

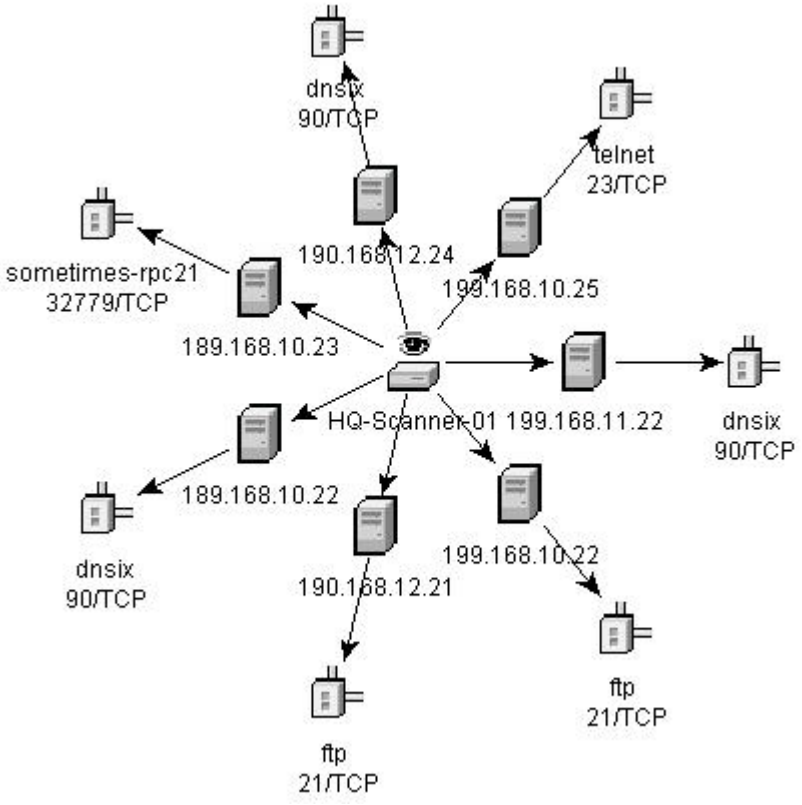
A exibição gráfica é uma renderização das vulnerabilidades que as vincula a um evento através de portas comuns. Segue um exemplo das quatro telas disponíveis.


dnsix
90/TCP
ftp
21/TCP
190.168.12.24
199.168.10.22
telnet
23/TCP
199.168.10.25
dnsix
90/TCP
189.168.10.22
HQ-Scanner-01
199.168.11.22
dnsix
90/TCP
189.168.10.23
190.168.12.21
sometimes-rpc21
32779/TCP
ftp
21/TCP

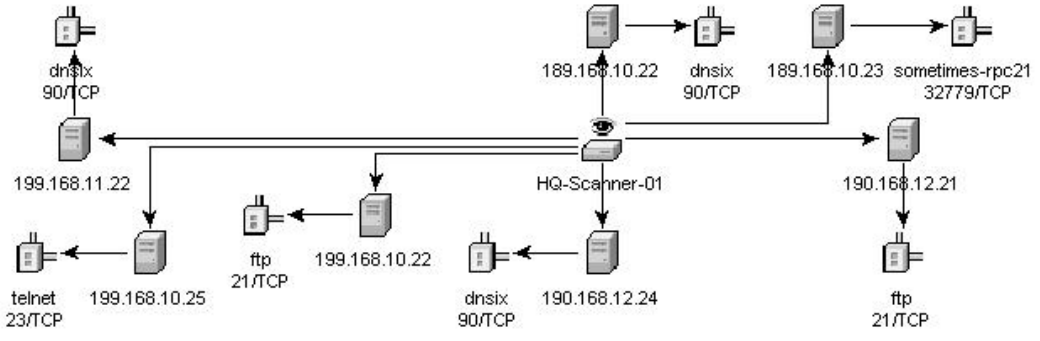
Orgânico


HQ-Scanner-01
9.168.10.22
189.168.10.23
190.168.12.21
190.168.12.24
199.168.10.22
199.168.10.25
199.168.11
dnsix
90/TCP
sometimes-rpc21
32779/TCP
ftp
21/TCP
dnsix
90/TCP
ftp
21/TCP
telnet
23/TCP
dnsix
90/TCP

Hierárquico



Circular



Ortogonal

Há quatro painéis disponíveis na exibição gráfica. São eles:

- painel gráfico
- painel de árvore
- painel de controle
- painel de detalhes/eventos

A exibição do painel gráfico associa as vulnerabilidades a uma combinação de porta/protocolo de um recurso (endereço IP). Por exemplo, se um recurso tiver cinco combinações exclusivas de porta/protocolo vulneráveis, haverá cinco nós anexados a esse recurso. Os recursos são agrupados sob o scanner que explorou os recursos e relatou as vulnerabilidades. Se dois scanners diferentes forem usados (ISS e Nessus), haverá dois nós de scanner independentes, com vulnerabilidades a eles associadas.

NOTA: O mapeamento de eventos ocorre somente entre os eventos selecionados e os dados de vulnerabilidade retornados.

O painel de árvore organiza os dados na mesma hierarquia do gráfico. Esse tipo de painel também permite que os usuários ocultem/exibam nós em qualquer nível da hierarquia.

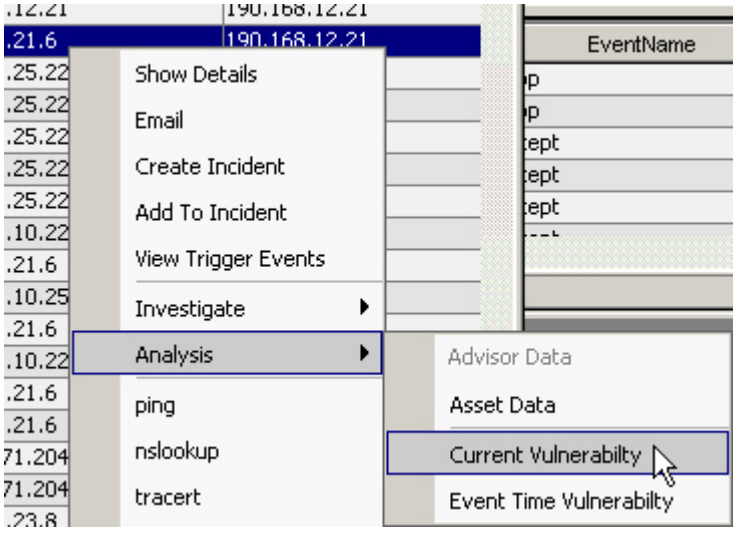
O painel de controle expõe todas as funcionalidades disponíveis na exibição. Entre as quais estão:

- quatro algoritmos diferentes para exibição
- capacidade de mostrar todos os nós ou apenas os selecionados, com eventos a eles mapeados
- ampliação e redução de áreas selecionadas do gráfico

No painel de Detalhes/Eventos, existem duas guias. Quando a guia Detalhes está selecionada, se você clicar em um nó, serão exibidos os detalhes do nó. Quando a guia Eventos está selecionada, se você clicar em um evento associado a um nó, esse nó será exibido no formato tabular como em uma janela em Tempo Real ou de Consulta de Eventos.

Para executar uma Visualização de Vulnerabilidade

1. Em uma tabela Tempo Real de Evento do Navegador Visual ou Instantâneo, clique o botão direito do mouse em um ou mais eventos selecionados e clique em:
   - Análise
     - Vulnerabilidade Atual – consulta o banco de dados quanto a vulnerabilidades ativas (efetivas) na data e hora atuais.
     - Vulnerabilidade no Horário do Evento – consulta o banco de dados quanto às vulnerabilidades que estavam ativas (efetivas) na data e hora do evento selecionado.



2. Na parte inferior da janela de resultados de vulnerabilidade, clique em uma destas opções:
   - Gráfico de Eventos-Vulnerabilidades
   - Relatório de Vulnerabilidades
3. (Para Gráfico de Eventos-Vulnerabilidades) na exibição, você pode:
   - mover nós e suas etiquetas
   - usar um dos quatro algoritmos de layout para exibir o gráfico
   - mostrar todos os nós ou apenas aqueles com eventos a eles mapeados
   - filtrar a árvore em linha no evento no qual um grande número de recursos são retornados como vulneráveis
   - ampliar e reduzir áreas selecionadas

Integração de Terceiros

A Integração de Terceiros permite enviar eventos de qualquer tela de exibição, inclusive incidentes e objetos associados ao:

- HP Service Desk
- Remedy

Para enviar um ou vários eventos para um software de terceiros

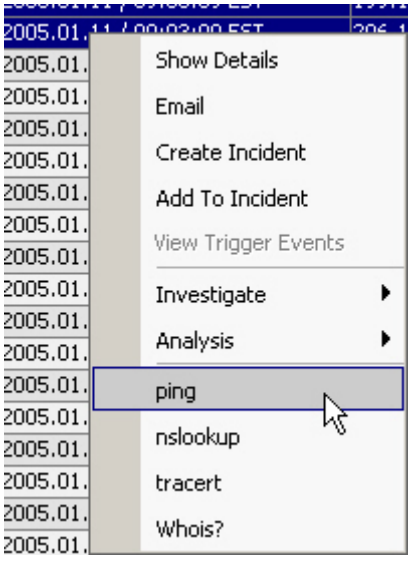
1. Em uma tabela Tempo Real de Evento do Navegador Visual ou janela do Instantâneo, dependendo do software da Integração de Terceiros que estiver instalado, clique o botão direito do mouse em um evento e clique em Enviar Evento para:
   - HP Service Desk
   - Remedy

Usando opções de menu personalizadas com eventos

Para usar uma opção de menu personalizada com um evento

1. Em uma tabela Tempo Real de Evento do Navegador Visual ou Instantâneo, selecione um evento ou grupo de eventos, clique o botão direito do mouse e selecione uma opção. Será aberta uma caixa de diálogo com as informações da configuração da opção de menu ou com campos a serem preenchidos com as informações necessárias para executar uma ação. Estas são as opções de menu personalizadas padrão:
   - ping
   - nslookup
   - traceroute
   - Whois?

   É possível atribuir outras permissões de usuário à Visualização de Vulnerabilidade e para a execução de Ações do HP. Você pode adicionar opções usando a janela Configuração de Menu disponível na guia Admin.

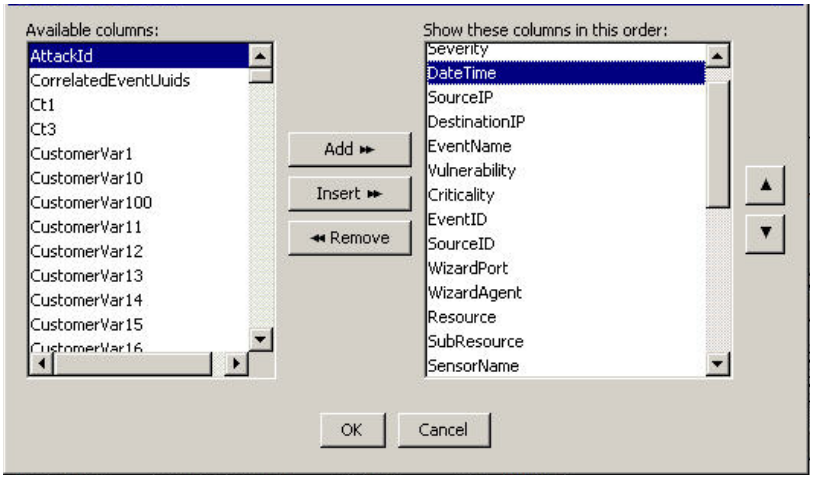


Gerenciando as colunas em uma janela Instantâneo ou Navegador Visual

Para selecionar e organizar colunas em um Instantâneo ou Navegador Visual

1. Com um janela aberta do Instantâneo ou Navegador Visual, clique em *Tela Ativa* > *Tempo Real do Evento* > *Gerenciar Colunas* ou clique na opção *Gerenciar Colunas* da Tabela de Tempo Real de Eventos.

2. Use os botões *Adicionar* e *Remover* para mover os títulos das colunas entre as listas Colunas Disponíveis e Mostrar Colunas nesta Ordem. O botão Inserir pode ser usado para colocar um item de coluna disponível em uma posição específica. Por exemplo, na ilustração a seguir, se o usuário clicasse no botão *Inserir*, colocaria a coluna AttackId acima da DateTime.



Use os botões de seta para cima e para baixo para organizar a ordem das colunas como quiser exibi-las na tabela Tempo Real do Evento. A ordem de cima para baixo em que os títulos das colunas aparecem na caixa de diálogo Gerenciar Colunas determina a ordem da esquerda para a direita em que as colunas serão exibidas na tabela Tempo Real do Evento.

3. Na caixa de diálogo Gerenciar Colunas, clique em *OK*.
4. Se você quiser manter as colunas nessa ordem na próxima vez em que abrir o Sentinel Control Center, clique em *Arquivo* > *Gravar Preferências* ou clique no botão *Gravar Preferências do Usuário*.

Tirando um instantâneo de uma janela Navegador Visual

Para executar esta função, você deve ter a permissão de usuário Instantâneo.

Esse recurso é útil para analisar eventos de seu interesse, pois o Navegador Visual é atualizado automaticamente e o alerta que você procura pode sair da tela. Além disso, um instantâneo pode ser classificado por colunas.

Para tirar um instantâneo de uma tabela Tempo Real de Evento

1. Com um janela Navegador Visual aberta, clique em *Tela Ativa* > *Tempo Real do Evento* > *Instantâneo* ou clique no botão Tabela de *Tempo Real de Eventos de Instantâneos*.

Uma janela de Instantâneo é aberta e adicionada à lista de pastas de instantâneos nas Telas de Eventos no Navegador. A exibição gráfica não fará parte do instantâneo.

Classificando colunas em um instantâneo

Para classificar colunas em um instantâneo

1. Clique em qualquer cabeçalho de coluna para classificar em ordem ascendente e clique duas vezes para organizar na ordem descendente.

Fechando um instantâneo ou Navegador Visual

Para fechar uma tabela Tempo Real de Evento ou instantâneo

1. Com um Instantâneo ou janela do Navegador Visual aberta, se você quiser que a tabela esteja disponível na próxima vez em que abrir o Sentinel Control Center, clique em *Arquivo* > *Gravar Preferências*.
2. Feche a tabela com o botão Fechar (canto superior direito no Windows ou superior esquerdo no UNIX).

Apagando um instantâneo ou Navegador Visual

Para apagar um Instantâneo ou janela Navegador Visual

1. Feche o Instantâneo ou o Navegador Visual aberto com o botão Fechar (canto superior direito no Windows ou superior esquerdo no UNIX).
2. Clique em *Arquivo* > *Gravar Preferências* ou clique no botão *Gravar Preferências do Usuário*.

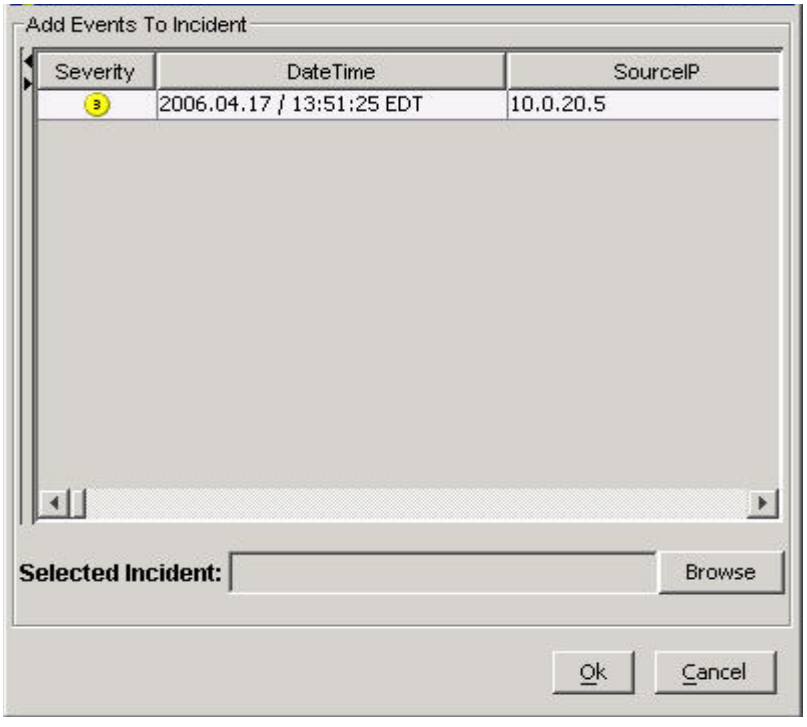
   A tela ou instantâneo não será exibida novamente quando você fechar e abrir novamente o Sentinel Control Center.

Adicionando eventos a um incidente

Para executar esta função, você deve ter as permissões de usuário Modificar Incidente(s) e Atribuir Incidente(s).

Para adicionar eventos a um incidente

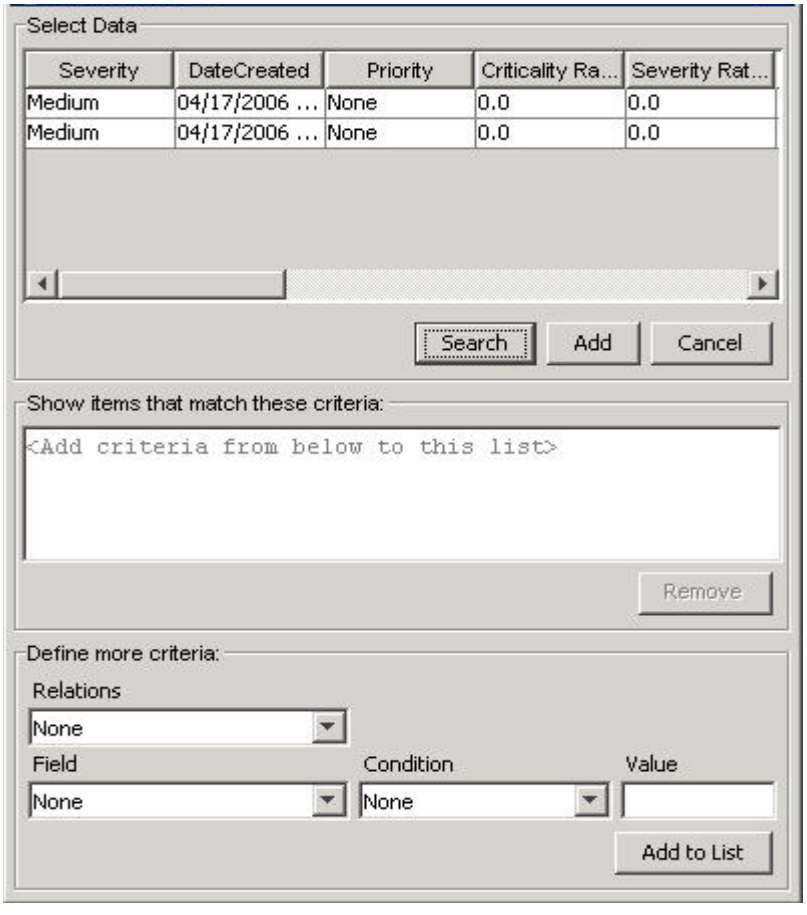
1. Em uma tabela Tempo Real de Evento ou Instantâneo, selecione um evento ou grupo de eventos, clique o botão direito do mouse para exibir e clique em *Adicionar ao Incidente*.
2. Na caixa de diálogo *Adicionar ao Incidente*, clique no botão Procurar.



3. Clique em *Procurar* para relacionar os incidentes disponíveis.

NOTA: Você pode definir critérios para melhorar a busca de um ou mais incidentes específicos.

4. Clique em *Pesquisar* para ver uma lista de incidentes.



5. Realce um incidente e clique em *Adicionar*.
6. Clique em *OK*. Os eventos selecionados serão adicionados ao incidente no Navegador de Incidentes.

NOTA: Se os eventos não forem exibidos inicialmente em um Incidente recém-criado, a causa provável é uma lacuna entre o momento da exibição na janela Eventos em Tempo Real e o instante da inserção no banco de dados. Se isso ocorrer, aguarde alguns minutos para que os eventos originais sejam finalmente inseridos no banco de dados e exibidos no incidente.

4 Guia Incidentes

NOTA: O termo Agente é intercambiável com Coletor. Mais adiante, Agentes será referido como Coletores.

Você deve ter a permissão adequada para usar a guia Ver Incidentes. Caso essa permissão não seja concedida, nenhuma das outras permissões relacionadas às ações que usam essa guia estará disponível.

Este capítulo descreve incidentes. Agrupamentos de um ou mais eventos importantes são chamados Incidentes.

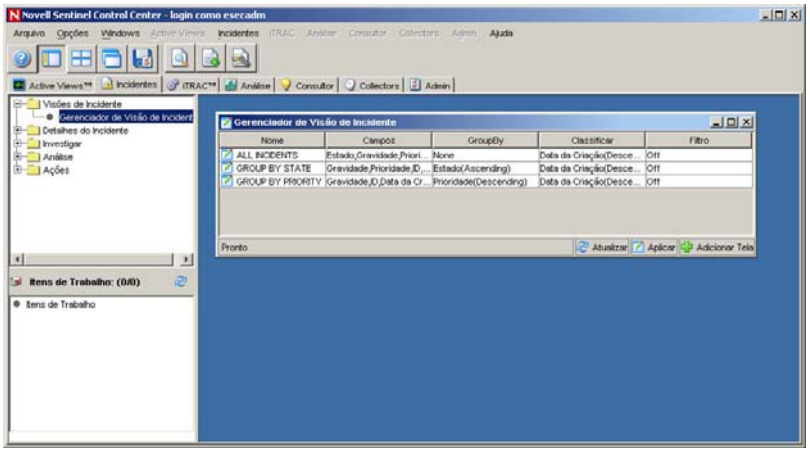
Para criar um Incidente:

- Na janela Tempo Real, os eventos podem ser selecionados individualmente para criar um novo incidente ou adicionados a um incidente existente.
- Também é possível criar incidentes automaticamente através das regras de correlação acionadas

Guia Incidentes – Descrição

Com incidentes, você pode:

- Enviar um incidente por e-mail
- Modificar um incidente
- Visualizar um incidente
- Apagar um incidente
- Adicionar uma tela de incidente



Relacionamento entre eventos e incidentes

Um evento é uma ação ou ocorrência detectada por um dispositivo de segurança ou programa. Os eventos "não contam com informações de estado".

Um incidente é o agrupamento de um ou mais eventos importantes (como um possível ataque). Os Incidentes possuem "estados" nos quais requerem uma resposta ou fechamento.

Visualizando um incidente

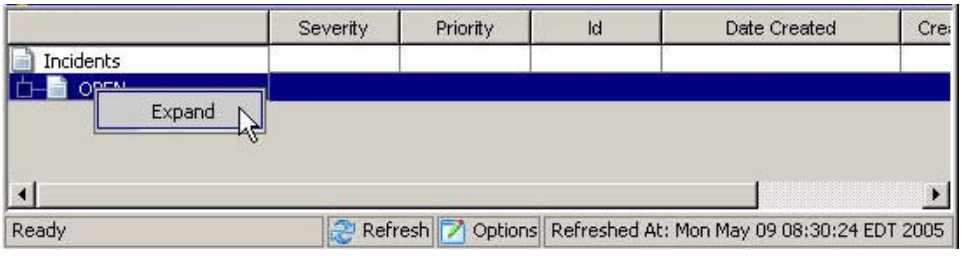
Você deve ter a permissão de usuário Ver Incidente(s).

Para ver um incidente

1. Clique na guia *Incidentes*.
2. Clique em *Incidentes* > *Exibir Gerenciador de Telas de Incidentes* ou clique no botão *Gerenciador de Visão de Incidente*.

3. Na janela Gerenciador de Visão de Incidente, você pode escolher as seguintes telas:
   - Todos os incidentes
   - Agrupar por Estado
   - Agrupar por Prioridade

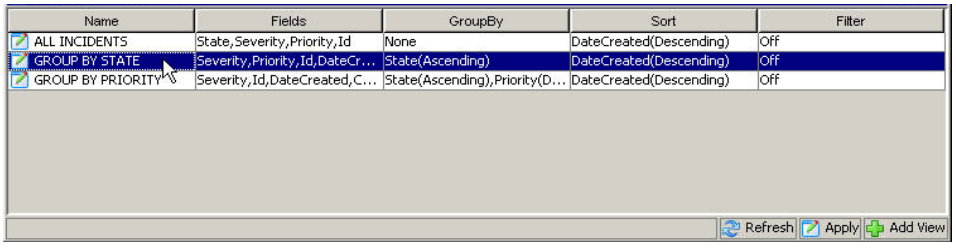
   Clique duas vezes no nome de uma tela.
4. Clique o botão direito do mouse em > *Expandir* para ver os incidentes.



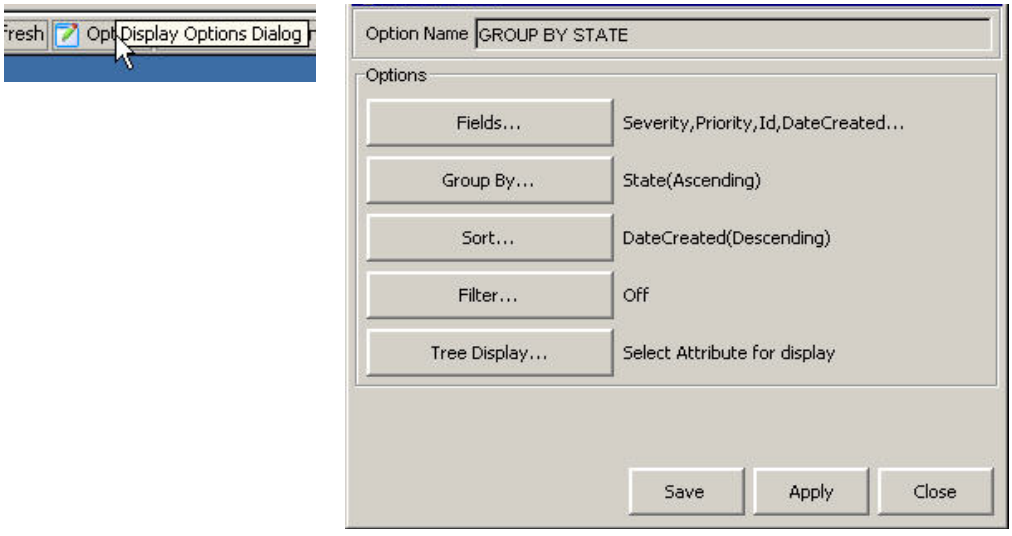
Para configurar uma opção de visualização de um incidente

1. Clique na guia *Incidentes*.
2. Clique em *Incidentes* > *Exibir Gerenciador de Telas de Incidentes* ou clique em *Gerenciador de Visão de Incidente*.

3. Na janela Gerenciador de Visão de Incidente, clique duas vezes no nome de uma tela:



4. Clique em *Opções*.



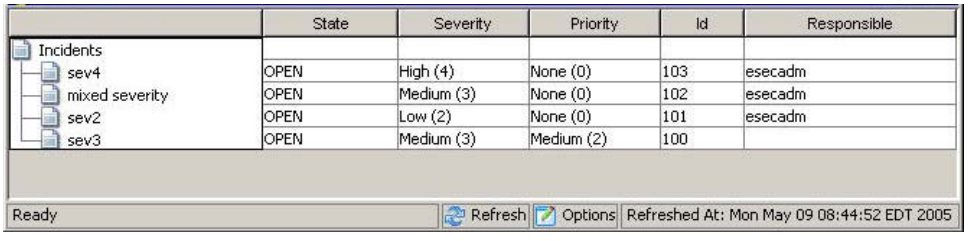
Nessa janela, você também pode configurar o seguinte:

- Campos...
- Agrupar por...
- Classificar...
- Filtro...
- Exibição em árvore

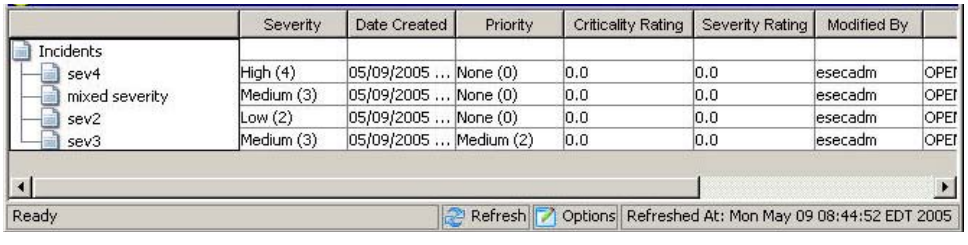
Clique em *Aplicar* e em *Gravar*.

5. Na janela Gerenciador de Visão de Incidente, clique duas vezes no nome de uma tela:

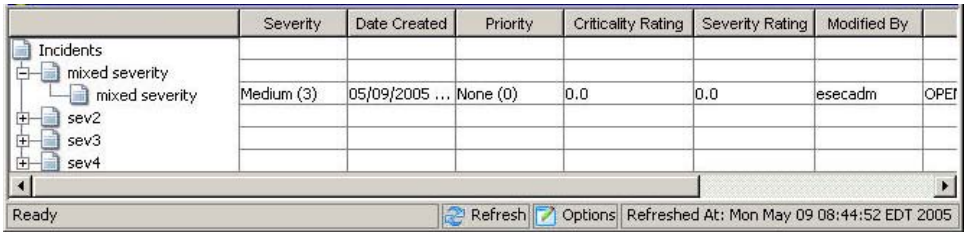
   Segue uma tela padrão da janela Todos os Incidentes:



   A tela a seguir está classificada por gravidade, com os campos (gerenciamento de colunas) referentes às primeiras quatro colunas definidos como Gravidade, Data de Criação, Prioridade e Classificação de Importância.



Esta tela foi agrupada por título.



Esta tela está organizada em árvore pela data de criação (DateCreated).

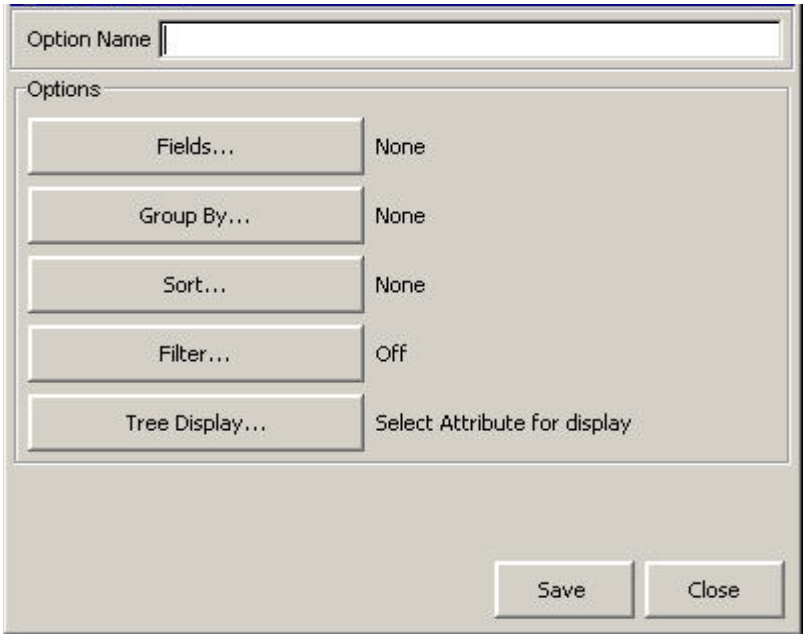
Adicionando uma Tela de Incidente

Ao adicionar uma Tela de Incidente, você tem as opções:

- Campos...
- Agrupar por...
- Classificar...
- Filtro...
- Exibição em árvore

Para adicionar uma Tela de Incidente

1. No Gerenciador de Visão de Incidente, clique em *Adicionar Tela*.



2. Digite o Nome da Opção e selecione as opções desejada. Clique em *Gravar*.

Campos e detalhes do Incidente

Campos do Incidente

- Título – Nome do incidente
- Estado
  - Abrir
  - Confirmado
  - Atribuído
  - Investigando
  - Falso Positivo
  - Verificado
  - Aprovado
  - Fechado
- Gravidade
  - Nenhuma (0)
  - Trivial (1)
  - Baixa (2)
  - Média (3)
  - Alta (4)
  - Severa (5)
- Prioridade
  - Baixa (1)
  - Média (2)
  - Alta (3)
  - Urgente (4)
  - Máxima (5)
- Categoria – (opcional), entrada de texto que pode ser usada para identificar melhor o incidente.
- Responsável – a conta de usuário atribuída ao caso
- Descrição – entrada de texto
- Resolução – entrada de texto

Detalhes do Incidente

- Eventos – eventos associados ao incidente.
- Bens – lista de todos os bens associados ao incidente.
- Vulnerabilidade – exibe qualquer vulnerabilidade associada ao incidente
- Consultor – exibe qualquer informação de ataque associada ao incidente
- Workflow – exibe qualquer workflow associado ao incidente. Nessa guia, você pode atribuir:
  - Nenhum
  - Processo de Conformidade HIPAA
  - Processo de Resposta a Incidentes SANS
  - Processo de Conformidade Sarbanes Oxley FTP
  - Resposta Automática
- Histórico – histórico do incidente (relaciona todas as ações executadas no incidente, inclusive data/hora da ação do usuário e informações sucintas)
- Anexos – é possível anexar qualquer informação pertinente (arquivos de texto ou documentos) ao incidente
- Dados Externos

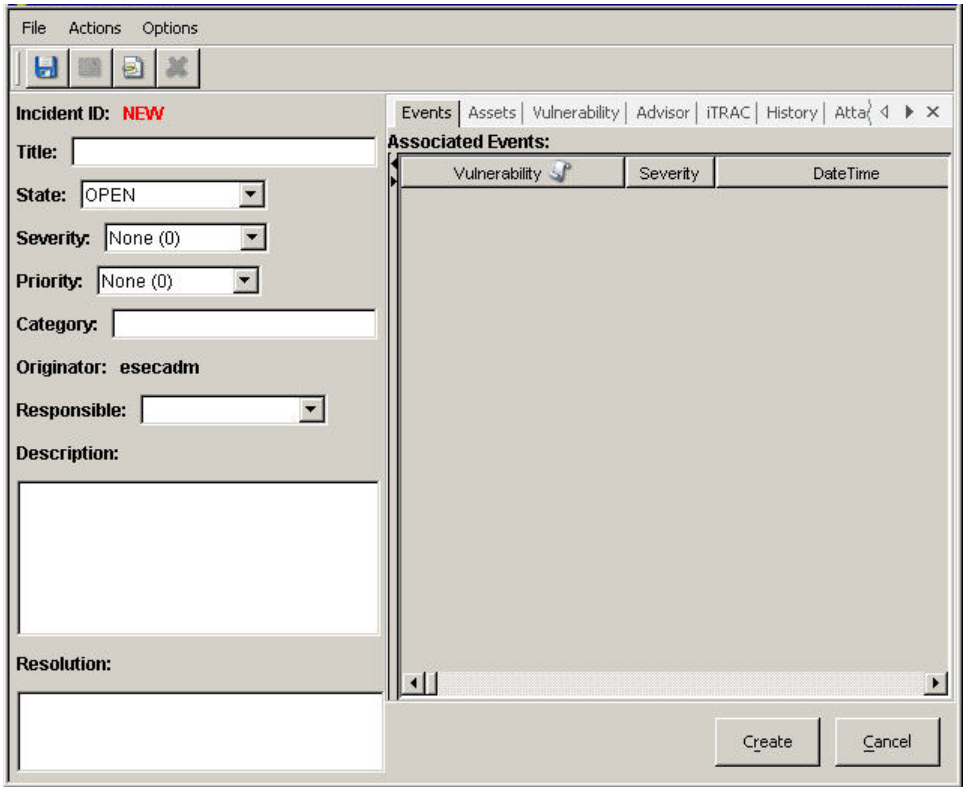
NOTA: Quando eventos são adicionados a um incidente, os campos de bens/vulnerabilidade e a guia Consultor são preenchidos com uma lista de todos os dados de Bens/Vulnerabilidade/Consultor correspondentes aos nomes do DIP/Host de Destino dos eventos associados.

NOTA: Os botões *Adicionar* e *Remover* na guia Bens/Vulnerabilidade/Consultor permitem que os usuários adicionem ou removam manualmente dados de bens, vulnerabilidade ou do consultor.

Criando um incidente

Criando um incidente

1. Clique na guia *Incidente*.
2. Clique em *Incidentes* > *Criar Incidente* ou clique em *Criar um Novo Incidente*.



Na caixa de diálogo Criar Incidente, digite as informações nos campos em branco.

3. Clique em *Gravar*.

Visualizando e gravando anexos

Para ver um anexo

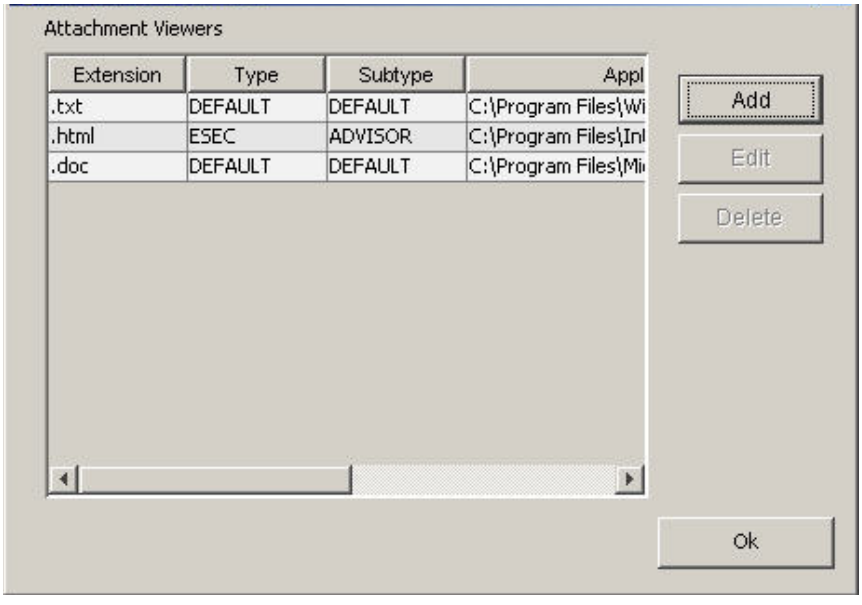
1. Clique o botão direito do mouse em um anexo. Em seguida, clique em *Ver* ou *Gravar*.

NOTA: Para ver um anexo, é necessário ter um Viewer de anexos configurado. Se um anexo não estiver configurado para abrir um arquivo, um prompt será exibido perguntando qual programa deve ser usado para abrir o arquivo. Arquivos de anexo são gravados no banco de dados do Sentinel.

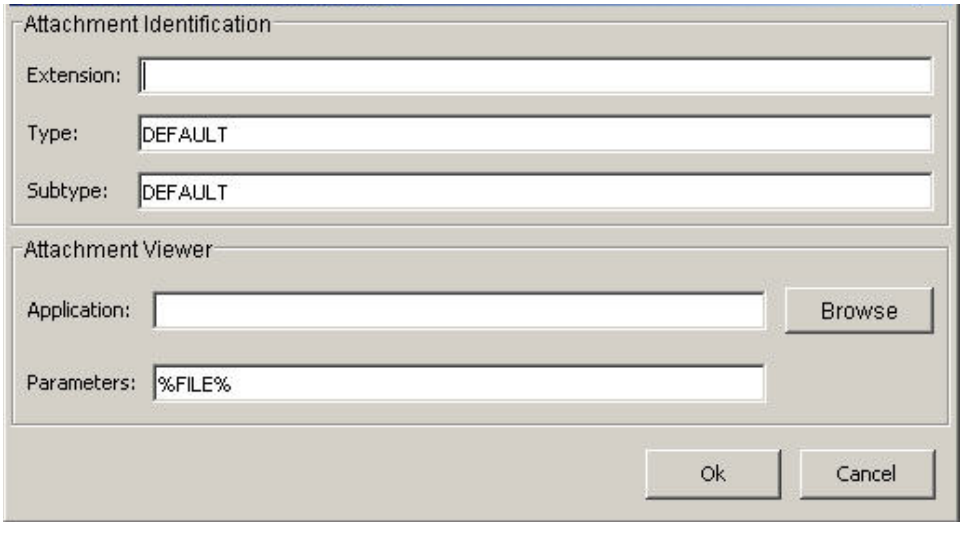
Configurando o Viewer de Anexo

Configurando o Viewer de Anexo

1. Clique na guia *Incidente*.
2. Clique em *Incidentes* > *Configuração de Viewer de Anexo* ou clique em *Configurar Viewers de Anexos*.



3. Clique em *Adicionar*.



Digite o tipo de extensão (como .doc, .xls, .txt, .html, etc...) e clique em *Procurar* ou digite o aplicativo a ser usado para abrir o tipo de arquivo escolhido (por exemplo, notepad.exe para o Bloco de Notas).

4. Clique em *OK*.

Enviando um incidente por e-mail

A capacidade de enviar e-mails é definida no arquivo execution.properties durante a instalação. Para configurar esse arquivo, consulte o *Capítulo 11 - Utilitários*.

Enviando um incidente por e-mail

1. Clique na guia *Incidentes*.
2. Se disponível no Navegador, expanda a pasta Incidentes ou clique em *Incidentes* > *Visualizar Lista de Incidentes* ou clique em *Visualizar Lista de Incidentes*.

3. Clique duas vezes no nome de uma *Tela de Incidente*.
4. Clique duas vezes em um incidente.
5. Clique em *Incidente de E-mail*  .
6. Digite:
   - Endereço de E-mail
   - Assunto do E-mail
   - Mensagem de E-mail
7. Clique em *OK*. A mensagem de e-mail terá anexos em html com detalhes do incidente, eventos, bens, vulnerabilidades, informações do consultor e histórico do incidente.

Modificando um incidente

Para modificar um incidente

1. Clique na guia *Incidentes*.
2. Clique em *Incidentes* > *Exibir Gerenciador de Telas de Incidentes* ou clique em *Gerenciador de Visão de Incidente*.

3. Clique duas vezes na tela de um incidente.
4. Clique duas vezes em um incidente.
5. A janela de detalhes do incidente será aberta.
6. Se quiser, você pode editar os seguintes campos em um Incidente:
   - Título
   - Estado
   - Gravidade
   - Prioridade
   - Categoria
   - Responsável
   - Descrição
   - Resolução
7. Na guia Anexos, você pode adicionar ou remover anexos.
8. Clique em *Gravar*.

Apagando um incidente

NOTA: Para apagar um incidente com um WorkFlow (iTRAC) anexado, é necessário terminar o Processo do iTRAC.

Para apagar um incidente

1. Clique na guia *Incidentes*.
2. Clique em *Incidentes* > *Exibir Gerenciador de Telas de Incidentes* ou clique em *Exibir Gerenciador de Telas de Incidentes*.

3. Clique duas vezes na tela de um incidente.
4. Na janela Visão de Incidente, clique o botão direito do mouse em um incidente e depois em *Apagar*.

NOTA: Para apagar um incidente com um WorkFlow (iTRAC) anexado, é necessário terminar o Processo do iTRAC. Para terminar um Processo do iTRAC, você pode usar o Gerenciador de Telas de Processos na guia iTRAC. Para obter mais informações, consulte o *Capítulo 5 – Guia do iTRAC*.

5. Na janela de confirmação, clique em *Sim*.

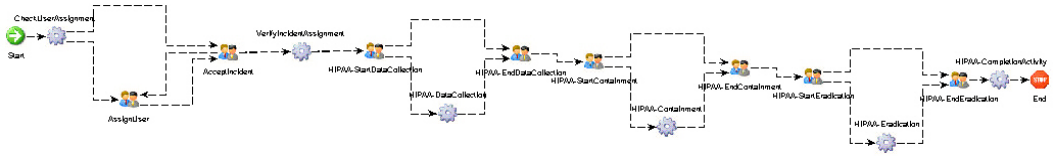
5 Guia iTRAC™

NOTA: O termo Agente é intercambiável com Coletor. Mais adiante, Agentes será referido como Coletores.

O iTRAC (workflow) envolve a automação de procedimentos e a capacidade de responder a incidentes. O Sentinel fornece um sistema de gerenciamento de iTRAC que oferece automação de procedimentos de processos. A estrutura de atividades do Sentinel está vinculada ao iTRAC. Essa estrutura fornece as atividades que podem ser executadas automaticamente em cada etapa do processo do iTRAC.

Juntas, as opções Gabaritos (Definição de Processo) e Execução de Processo consistem no sistema de gerenciamento de workflows.

Gabaritos (Definição de Processo)



O gabarito é o projeto que controla o fluxo de execução no iTRAC. Esse gabarito consiste na rede de atividades e seus relacionamentos, critérios de transição entre as atividades e informações sobre atividades específicas. Os gabaritos contêm atributos que podem ser modificados pelo usuário.

O iTRAC permite que os usuários definam atributos de tempo de espera em um gabarito do iTRAC.

Uma atividade é uma unidade de trabalho lógica e completa dentro do processo do iTRAC. Uma atividade representa o trabalho que será processado pelos usuários/funções (atividade manual) ou pelos aplicativos de computador (atividades automáticas).

As atividades também possuem tempos de espera que os usuários podem ativar/desativar em todas as atividades manuais ou automáticas.

Nas atividades manuais, além dos atributos de tempo de espera, os usuários podem configurar o atributo de recurso que determina o usuário/função que está executando a respectiva atividade.

Nas atividades automáticas, além dos atributos de tempo de espera, os usuários podem configurar a atividade automática na estrutura de atividades do Sentinel a ser executada.

Template Manager

O iTRAC permite que os usuários criem novos gabaritos, manipulem atributos de processo e atividade em um gabarito existente e apaguem gabaritos usando a janela do gerenciador de gabaritos na guia iTRAC.

Para acessar o gerenciador de gabaritos, basta clicar no nó Gerenciador de Gabaritos na árvore do navegador na guia iTRAC.

Gabaritos padrão

O iTRAC fornece quatro gabaritos padrão que consistem em atividades automáticas e manuais. Os atributos de processo e atividade desses gabaritos foram configurados com alguns valores predefinidos. Os usuários podem modificar esses valores de acordo com suas necessidades. Estes são os gabaritos padrão:

- HIPAA
- Sarbanes Oxley
- Gestão de Incidentes do SANS
- Resposta Automática

Criando novos gabaritos

1. Clique na guia *iTRAC*.
2. No Navegador, clique em *Administração do iTRAC* > *Gerenciador de Gabaritos*.
3. Realce um processo existente (HIPAA, Sarbanes-Oxley, SANS ou outro definido pelo usuário), clique o botão direito do mouse em > *Criar Cópia*.
4. Digite um nome.
5. Se você selecionar um tempo de espera, deverá digitar um tempo e um endereço de e-mail. O tempo deve ser informado em números inteiros. Você pode selecionar minutos, segundos, horas ou dias.
6. Digite uma descrição. Consulte Modificando Gabaritos Existentes para mudar atributos de processo e atividade. Clique em *OK*.
7. No Personalizador de Gabaritos, clique em *Gravar*.

Modificando gabaritos existentes

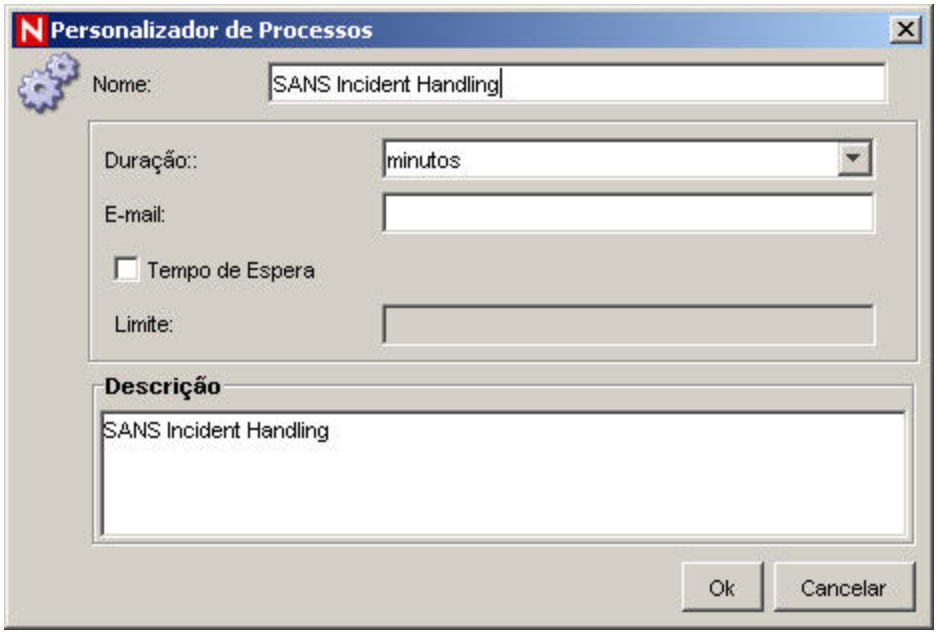
Ao modificar um processo, você pode mudar atributos do processo ou das atividades dentro do processo:

É possível modificar os seguintes atributos de processo:

- nome
- tempo de espera ou desativar o tempo de espera
- descrição

Modificando atributos de processo

1. Clique na guia *iTRAC*.
2. No Navegador, clique em *Administração do iTRAC* > *Gerenciador de Gabaritos*.
3. Destaque um gabarito existente, clique o botão direito do mouse e selecione *Exibir*.
   Na janela do gabarito, clique no botão Detalhes do Processo.
   
4. Na caixa de diálogo Personalizador de Processos, você pode editar o seguinte:
   - Nome
   - Duração (minutos, segundos, horas ou dias).
   - Tempo de espera (se essa opção estiver ativada, você terá de digitar um tempo e um endereço de e-mail)
   - Descrição



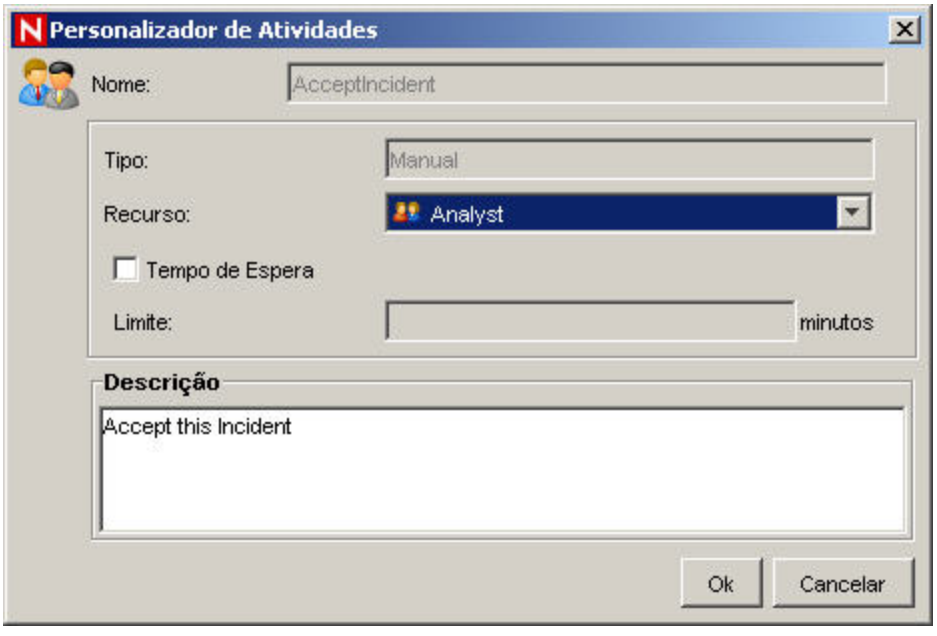
Modificando atividades manuais

Você pode editar o recurso (usuário/função), o Tempo de Espera e a Descrição de atividades manuais.

1. Clique na guia *iTRAC*.
2. No Navegador, clique em *Administração do iTRAC > Gerenciador de Gabaritos*.
3. Destaque um gabarito existente, clique o botão direito do mouse e selecione *Exibir*.
4. O Gabarito é exibido em uma janela separada.
5. Para editar, clique duas vezes em qualquer ícone de atividade manual no gabarito e faça as alterações.

NOTA: as seguintes atividades manuais nos gabaritos existentes podem ser modificadas de acordo com essa explicação:

- AssignUser
- AcceptIncident
- ConfirmStartDataCollection
- ConfirmEndDataCollection
- ConfirmStartContainment
- ConfirmEndContainment
- ConfirmStartEradication
- ConfirmEndEradication



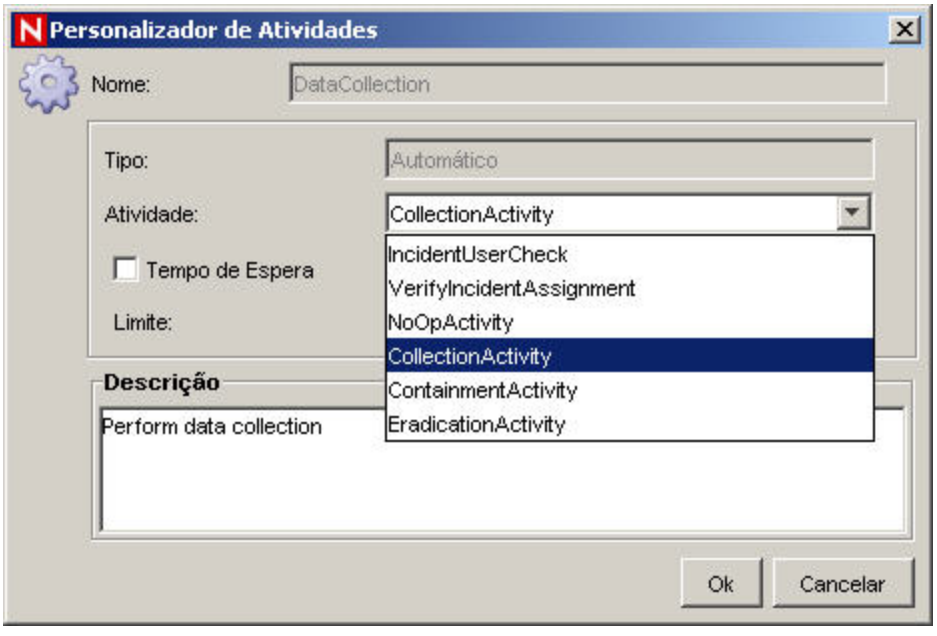
Modificando atividades automáticas

Você pode editar a atividade, o Tempo de Espera e a Descrição de uma atividade automática.

1. Para editar, clique duas vezes em qualquer ícone de atividade automática no gabarito e faça as alterações.
2. A lista suspensa nas caixas de diálogo do personalizador de atividades exibe a lista das atividades que podem ser usadas como atividades automáticas. As atividades na lista são criadas com a estrutura de atividades.

NOTA: as seguintes atividades automáticas nos gabaritos existentes podem ser modificadas de acordo com essa explicação:

- DataCollection
- Containment
- Eradication



Apagando gabaritos

1. Clique na guia *iTRAC*.
2. No Navegador, clique em *Administração do iTRAC* > *Gerenciador de Gabaritos*.
3. Destaque um gabarito existente, clique o botão direito do mouse e selecione *Apagar*.
4. Clique em *Sim* na caixa de diálogo pop-up para apagar o gabarito.

Execução de processo

A Execução de Processo é o período durante o qual o processo está em operação, com instâncias sendo criadas e gerenciadas.

Quando um processo do iTRAC é executado ou colocado em instâncias no servidor do iTRAC, uma instância de processo é criada, gerenciada e, finalmente, terminada pelo servidor do iTRAC de acordo com a definição do processo. Conforme avança rumo à conclusão ou término, o processo executa várias atividades definidas no gabarito do workflow com base nos critérios para as transições entre eles. O servidor de workflow do iTRAC processa atividades manuais e automáticas de maneiras diferentes.

Um processo do iTRAC depende de um incidente do Sentinel. Uma instância de processo não pode existir se não houver um incidente relacionado a ela. Por outro lado, um incidente pode existir sem estar relacionado ao servidor de workflow. Somente um incidente pode estar associado a uma instância de processo do iTRAC.

Criando instâncias de um processo

Para criar instâncias de um processo do iTRAC no servidor do iTRAC, é preciso associar um incidente a um processo do iTRAC por estes três métodos:

- Associar um processo do iTRAC ao incidente na hora da criação deste.
- Associar um processo do iTRAC ao incidente após a criação deste.
- Associar um processo do iTRAC ao incidente por meio de correlação.

Consulte o capítulo sobre a guia Incidentes para obter mais detalhes sobre como associar um processo a um incidente.

Execução de atividade automática

Quando executa uma atividade automática, a instância de processo executa a atividade associada definida no gabarito. A atividade associada é uma atividade criada por meio da estrutura de atividades. O servidor do iTRAC executa a atividade, armazena o resultado em variáveis do processo e passa para a próxima atividade incluída no gabarito do iTRAC.

Por exemplo, uma atividade da estrutura pode ser definida como emitir um comando Ping para um servidor e anexar os resultados ao incidente associado.

Execução de atividade manual

Ao encontrar uma atividade manual, o servidor do iTRAC envia notificações na forma de itens de trabalho ao recurso atribuído. Se o recurso atribuído for um usuário, o item de trabalho será enviado somente para esse usuário. Se a atividade for atribuída a uma função, o item de trabalho será enviado a todos os usuários com essa função. O servidor do iTRAC espera o usuário concluir o item de trabalho antes de prosseguir para a próxima atividade.

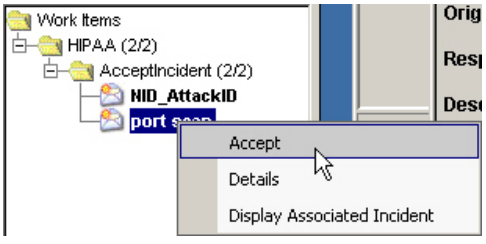
Listas de trabalho

Os itens de trabalho são apresentados ao usuário por meio da lista de trabalho que contém detalhes de todos os itens de trabalho alocados a esse usuário. Essa é uma lista de tarefas para o usuário.

A lista de trabalho pode ser exibida a partir de qualquer guia na interface de usuário do Sentinel. Os itens de trabalho são agrupados por processos e atividades aos quais pertencem. O negrito indica os itens de trabalho que ainda não foram aceitos pelo usuário.

A lista de trabalho permite que os usuários interajam com itens específicos.

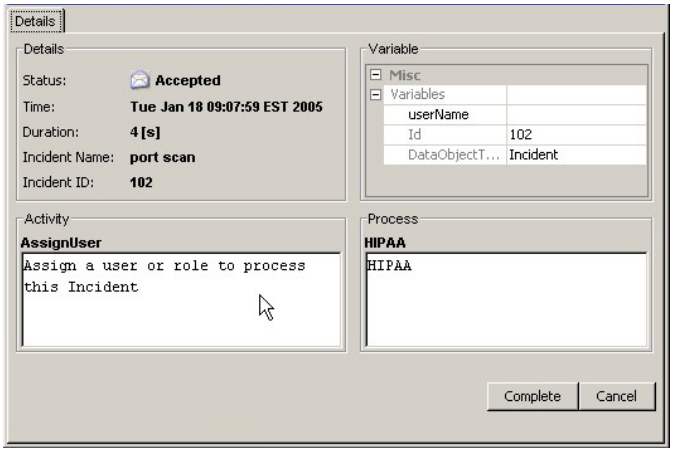
- O usuário pode clicar duas vezes ou clicar o botão direito do mouse em *Detalhes* para ver os detalhes do item de trabalho.
- Os usuários podem clicar o botão direito do mouse e *aceitar* itens de trabalho ainda não aceitos
- Os usuários podem clicar o botão direito do mouse e *ver* os detalhes do incidente associado



Item de trabalho

Um item de trabalho consiste na tarefa a ser executada pelo usuário com relação à atividade manual que ele está executando em um processo do iTRAC. O controle e o progresso do item de trabalho ficam a cargo do usuário.

O servidor do iTRAC espera o usuário concluir a tarefa antes de prosseguir para a próxima atividade dentro da instância do processo.



A caixa de diálogo com detalhes do item de trabalho mostrada acima apresenta as seguintes informações:

- Detalhes do item de trabalho
- Variáveis do item de trabalho
- Descrição da atividade
- Descrição do processo

Estas são as três etapas envolvidas na interação com um item de trabalho:

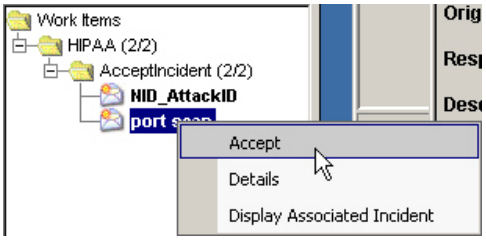
- Aceitar o item de trabalho;
- Atualizar as variáveis do item de trabalho;
- Concluir o item de trabalho.

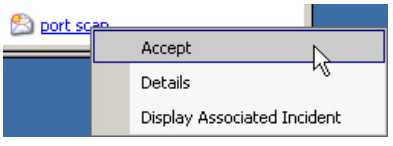
Aceitando o item de trabalho

Um item de trabalho será atribuído a todos os usuários dentro de uma função ou a um único usuário. O usuário precisa aceitar o item de trabalho antes de executar qualquer outra ação sobre esse item. Ao aceitar o item de trabalho, o usuário torna-se proprietário dele e o item é removido da lista de trabalho de todos os outros usuários atribuídos.

Aceitando itens de trabalho

1. Na lista de trabalho, você pode clicar o botão direito do mouse em um item de trabalho e fazer o seguinte:





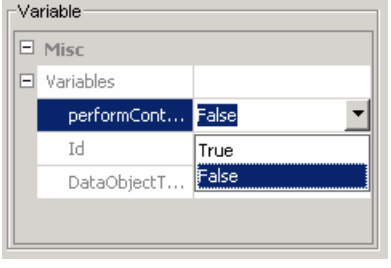
   - Aceitar (quando o processo está em uma etapa Aceitar)
   - Ou então, você pode ativar a janela de detalhes e clicar no botão Aceitar.

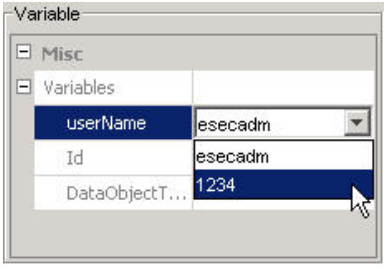
Atualizando as variáveis do item de trabalho

O servidor do iTRAC usa itens de trabalho para obter informações dos usuários na forma de variáveis de itens de trabalho para determinar a próxima atividade em um processo. O usuário pode acessar as variáveis somente depois de aceitar o item de trabalho.

O iTRAC suporta variáveis apenas leitura e variáveis atualizáveis. As variáveis apenas leitura podem ser usadas para informar ao usuário o status de uma atividade, o id de um incidente, etc.

As variáveis atualizáveis são usadas para aceitar entradas dos usuários. Atualmente, o iTRAC oferece dois tipos de variáveis atualizáveis: Lista de usuários e Lista de booleanos.





Atualizando variáveis

1. Clique duas vezes ou clique o botão direito do mouse no item de trabalho para ver a caixa de diálogo de detalhes.
2. O modo de edição aceita somente as variáveis atualizáveis. As variáveis apenas leitura não podem ser editadas.
3. Clique na caixa de combinação e selecione o valor apropriado.

Concluindo o item de trabalho

A conclusão do item de trabalho sinaliza a conclusão da tarefa ao servidor do iTRAC. As variáveis atualizáveis do item de trabalho são processadas pelo servidor para que o processo siga para a próxima atividade com base em alguns critérios. O item de trabalho é removido da lista de trabalho do usuário. Um item de trabalho precisa ser aceito para que possa ser concluído.

Concluindo itens de trabalho

1. Clique duas vezes ou clique o botão direito do mouse no item de trabalho para ver a caixa de diálogo de detalhes.

2. Clique no botão *Concluir* na caixa de diálogo

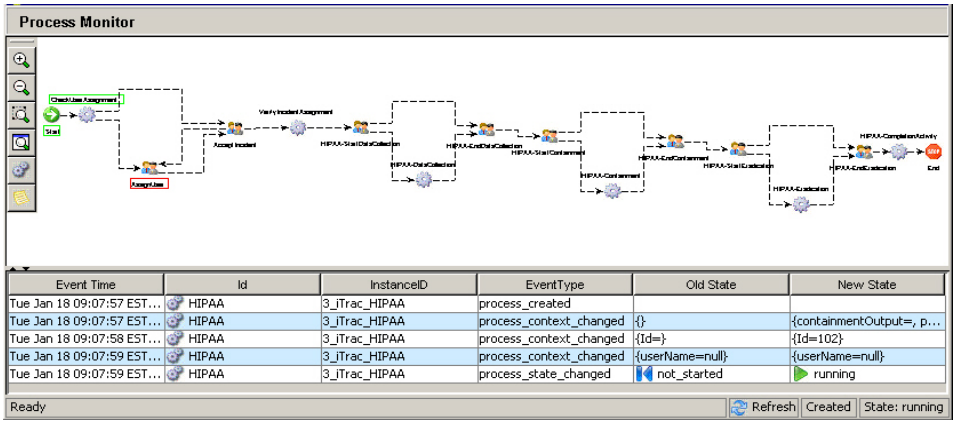
Gerenciamento de processos

O gerenciamento de processos permite:

- Exibir o status do processo (Monitor de Processos);
- Iniciar o processo;
- Terminar o processo.

Monitor de Processos

A função Monitor de Processos monitora o andamento de um processo. Conforme a instância do processo avança de uma atividade para a outra, o usuário pode rastrear visualmente o progresso clicando no botão Atualizar. O Monitor de Processos também fornece uma trilha de auditoria de todas as ações executadas pelo servidor do iTRAC durante a execução do processo.

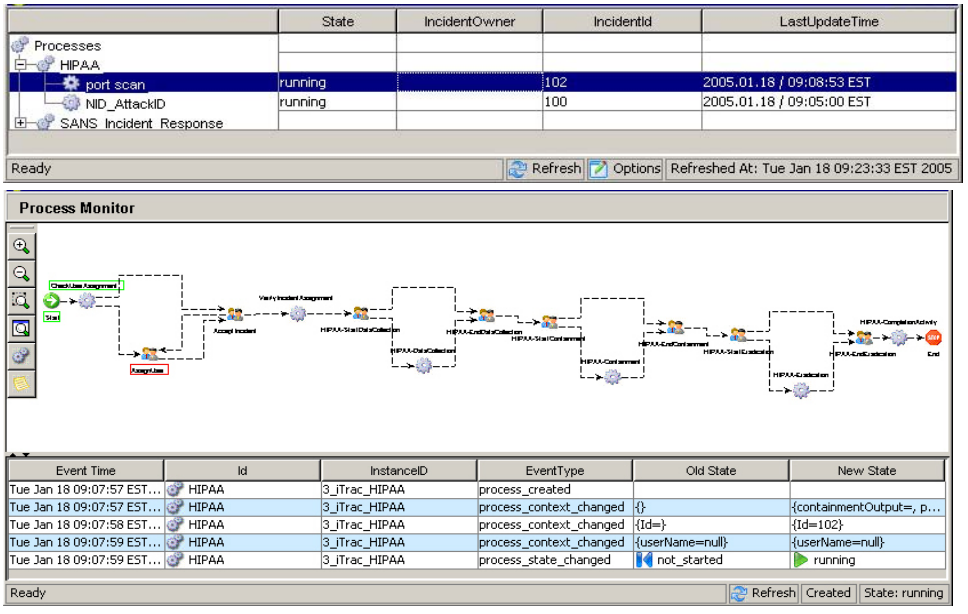


As atividades concluídas pelo processo são exibidas com uma borda verde, enquanto as que estão em andamento são exibidas com uma borda vermelha.

Acessando o monitoramento de processos

1. Clique na guia *iTRAC*.
2. Clique no botão *Gerenciador de Opções de Tela*.

3. Clique duas vezes em uma das telas padrão ou crie uma nova tela. As telas padrão são:
   - Todos os Processos
   - Processos por Incidente
   - Processos por Status
4. No Gerenciador de Processos Ativos, realce e clique duas vezes em um processo.

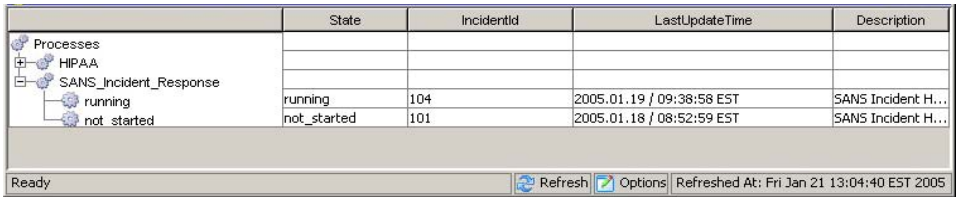


Para configurar uma opção do Gerenciador de Processos

1. Clique na guia *iTRAC*.
2. Clique duas vezes em qualquer processo.
3. Clique no botão Opções. Nessa janela, você também pode configurar o seguinte:
   - Campos...
   - Agrupar por...
   - Classificar...
   - Filtro...
   - Exibição em árvore

4. Clique em *Aplicar* e em *Gravar*.

   Segue uma tela com a Exibição em árvore definida como Status (em execução e não iniciada).



Iniciando ou terminando um processo

Iniciando ou terminando um processo

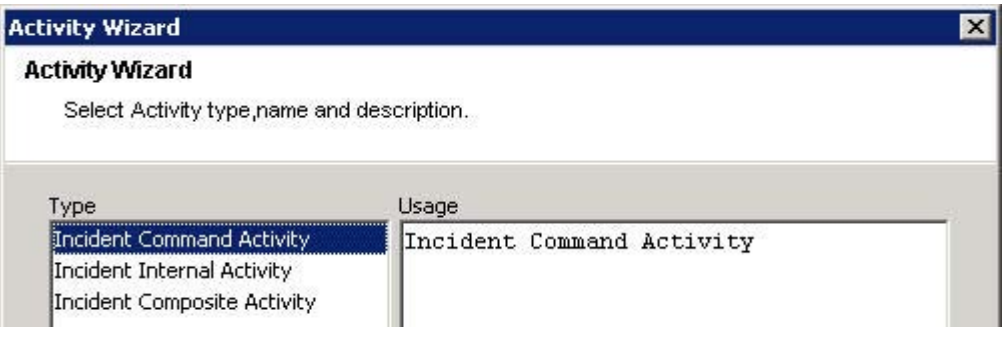
1. Clique na guia *iTRAC*.
2. Clique no botão *Gerenciador de Opções de Tela*.

3. Clique duas vezes em uma das telas padrão ou crie uma nova tela. As telas padrão são:
   - Todos os Processos
   - Processos por Incidente
   - Processos por Status
4. No Gerenciador de Processos Ativos, realce um processo, clique o botão direito do mouse e selecione *Iniciar Processo* ou *Terminar Processo*.

Criando uma atividade usando a estrutura de atividades

Criando uma atividade

1. Clique na guia *iTRAC*.
2. No Navegador, clique em *Administração do iTRAC > Gerenciador de Atividades.*
3. Clique o botão direito em *Nova Atividade*.
4. Selecione uma das seguintes opções:



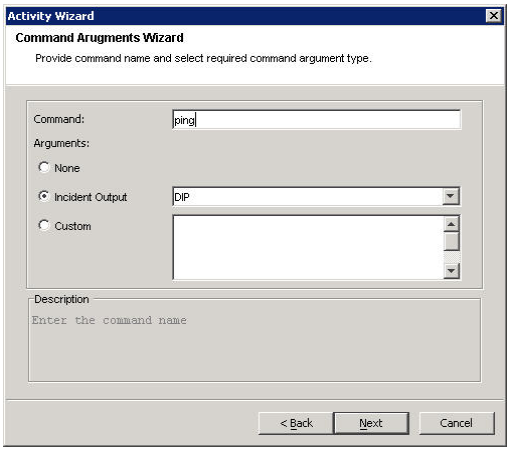
- Atividade de Comando de Incidente – inicia um comando específico com ou sem argumentos.

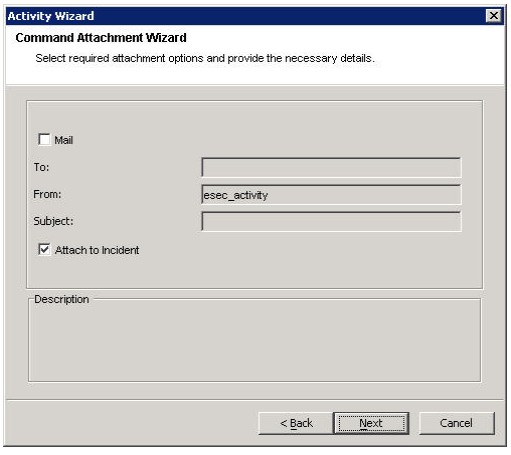
  Saída de Incidente oferece os seguintes argumentos:

  - DIP
  - DIP:Porta
  - Incidente
  - RT1 (DeviceAttackName)
  - SIP
  - SIP:Porta
  - Texto

  O usuário pode personalizar seus próprios argumentos.

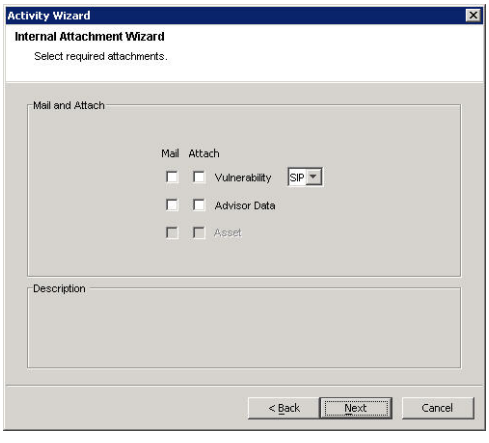
  Para esta atividade, você também pode configurar o envio do resultado por e-mail e/ou anexar o resultado ao incidente.



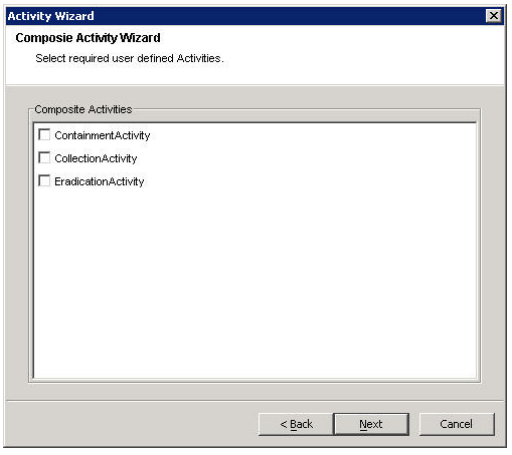


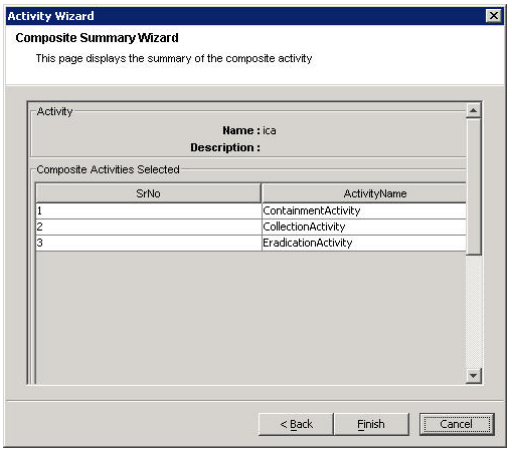
- Atividade Interna de Incidente – permite enviar por e-mail e/ou anexar as informações sobre:

  - Vulnerabilidade para (SIP ou DIP)
  - Dados do Consultor
  - Bem



- Atividade Composta de Incidente – permite criar uma atividade combinando uma ou mais atividades existentes.





Modificando uma atividade

Modificando uma atividade

1. Clique na guia *iTRAC*.
2. No Navegador, clique em *Administração do iTRAC > Gerenciador de Atividades > Atividades do iTRAC*.
3. Clique duas vezes em uma atividade do iTRAC. Edite e clique em *OK*.

Importando/exportando uma atividade

As atividades são exportadas como arquivos xml. Esses arquivos podem ser importados de um sistema para o outro.

Exportando uma atividade

1. Clique na guia *iTRAC*.
2. No Navegador, clique em *Administração do iTRAC > Gerenciador de Atividades.*
3. Clique o botão direito em *Atividades do iTRAC > Atividade de Importação/Exportação*.
4. Selecione Exportar Atividade e clique no botão *Explorar*.
5. Navegue até o local desejado e grave o arquivo exportado.
6. Dê um nome ao arquivo e clique em *Exportar*.
7. Clique em *Avançar*.
8. Selecione uma ou mais atividades a serem exportadas.
9. Clique em *Avançar* e *Concluir*.

Importando uma atividade

1. Clique na guia *iTRAC*.
2. No Navegador, clique em *Administração do iTRAC > Gerenciador de Atividades.*
3. Clique o botão direito em *Atividades do iTRAC > Atividade de Importação/Exportação*.
4. Selecione Importar Atividade e clique no botão Explorar.
5. Navegue até o arquivo de importação. Clique em *Importar*.
6. Clique em *Avançar*.
7. Clique em *Avançar* e *Concluir*.

6 Guia Análise

NOTA: O termo Agente é intercambiável com Coletor. Mais adiante, Agentes será referido como Coletores.

Você deve ter permissão adequada para usar a guia Análise. Caso essa permissão não seja concedida, nenhuma das outras permissões relacionadas às ações que usam essa guia estará disponível.

Descrição

A guia Análise permite a criação de relatórios históricos. Relatórios históricos e de vulnerabilidade são publicados em um servidor Web, são executados diretamente em um banco de dados e exibidos nas guias Análise e Consultor da barra de navegação.

NOTA: O Sentinel é integrado ao Crystal Reports® para gerar e exibir relatórios. O administrador deve configurar o local do Crystal Enterprise Server que publica relatórios na janela Opções gerais da guia Admin. Na janela de navegação há uma lista de relatórios disponíveis.

Para executar os gabaritos dos relatórios, você deve ter o Crystal Reports Enterprise Edition instalado e o Sentinel Control Center configurado para acessar o servidor. Para obter mais informações, consulte o *Guia de Instalação do Sentinel*™ 5.

Também são fornecidos exemplos dos relatórios no formato pdf.

Dez relatórios principais

Para a execução dos 10 relatórios principais, a agregação deve estar habilitada e EventFileRedirectService no DAS_Binary.xml deve estar ativado. Para obter mais informações sobre como habilitar uma agregação, vá para o *Capítulo 10 do Guia do usuário do Sentinel, Gerenciador de dados do Sentinel*, seção *Guia Relatando dados*.

Habilitando EventFileRedirectService para os 10 relatórios principais do Sentinel.

Habilitando EventFileRedirectService

1. Em sua máquina com DAS, usando o editor de textos, abra:

   Para UNIX:

   ```
   $ESEC_HOME/sentinel/config/das_binary.xml
   ```

   Para Windows:

   ```
   %ESEC_HOME%\sentinel\config\das_binary.xml
   ```

2. Para EventFileRedirectService, altere o status para ativado.

```
<property name="status">on</property>
```

3. No Windows, reinicie o serviço do Sentinel. No UNIX, reinicialize a máquina com DAS.

Executando um relatório do Crystal Reports

Para criar um relatório de um gabarito do Crystal Reports

1. Clique na guia *Análise.*
2. No *Navegador de análise*, clique em um dos relatórios disponíveis.

NOTA: Para a execução dos 10 relatórios principais, a agregação deve estar habilitada e EventFileRedirectService no DAS_Binary.xml deve estar ativado. Para obter mais informações sobre como habilitar uma agregação, consulte o *Capítulo 10 do Guia do usuário do Sentinel, Gerenciador de dados do Sentinel*, seção *Guia Relatando dados*.

3. Clique em *Análise* > *Criar Relatório*, ou clique em *Criar Relatório*.

4. Preencha as informações do gabarito e clique em *Ver Relatório*. O relatório será exibido.

Executando um relatório de consulta de evento

Para criar um relatório de consulta de evento

1. Clique na guia *Análise.*
2. No Navegador de Análise, abra a pasta Relatórios de Histórico.
3. Clique em *Consulta de Evento*.
4. Clique em *Análise* > *Criar Relatório*, ou clique em *Criar Relatório*.

Uma janela Consulta de Evento será aberta.

5. Defina o seguinte:
   - espaço de tempo
   - filtro
   - nível de severidade
   - tamanho do lote (este é o número de eventos a ver – eventos exibidos dos mais antigos para os mais recentes)
6. Clique em *Atualizar Consulta*.
7. Para ver o próximo lote de eventos, clique em *Mais*.
8. Reorganize as colunas arrastando-as e soltando-as, e organize a ordem de classificação clicando no cabeçalho da coluna.
9. Quando sua consulta estiver completa, ela será adicionada à lista de consultas rápidas do navegador.

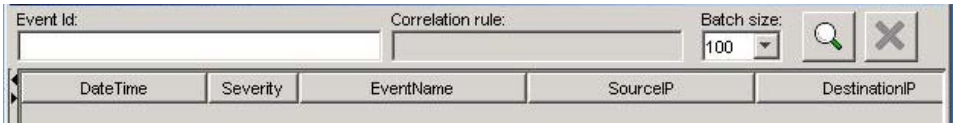
Executando um relatório de eventos correlacionados

Para criar um relatório de eventos correlacionados

1. Clique na guia *Análise.*
2. No Navegador de Análise, abra a pasta Relatórios de Histórico.
3. Clique em *Eventos Correlacionados*.
4. Clique em *Análise* > *Criar Relatório*, ou clique em *Criar Relatório*.

   Uma janela Relatório de Eventos Correlacionados será aberta.

5. No campo ID de Correlação, digite:
   - Número de ID do evento ou
   - CorrelatedEventUUID

   NOTA: CorrelatedEventUUID só fica disponível em uma tabela de eventos em tempo real.

6. Para ver o próximo lote de eventos, clique em *Mais*.

7 Guia Consultor

NOTA: O termo Agente é intercambiável com Coletor. Mais para a frente, Agentes será referido como Coletores.

Você deve ter permissão adequada para usar a guia Consultor. Caso essa permissão não seja concedida, nenhuma das outras permissões relacionadas às ações que usam essa guia estará disponível.

O Consultor é um módulo opcional. Se você não tiver licença do Consultor, quando clicar na guia Consultor, obterá uma tela de notificação indicando esse fato.

O Consultor do Sentinel é fornecido pela SecurityNexus. O Consultor fornece informações em tempo real quanto a vulnerabilidades da empresa, conselhos de especialistas e passos recomendados para a resolução. O Consultor fornece uma referência cruzada entre assinaturas de ataque de IDS em tempo real e a base de conhecimentos de vulnerabilidades do Consultor. Visite http://www.esecurity.net/Software/Products/Advisor.asp para obter mais informações.

A alimentação de dados do Consultor contém duas partes:

- Dados de alerta: Informações relacionadas a vulnerabilidades e ameaças de segurança conhecidas.
- Dados de ataque Normalização de assinaturas de detecção de intrusão e plug-ins de exploração de vulnerabilidade.

NOTA: Durante a instalação e até a alimentação de dados inicial do SecurityNexus, a função de clique o botão direito do mouse em um evento (com o campo rt 1 preenchido) dos dados do Consultor não estará totalmente operacional.

Executando relatórios do Consultor

Para criar um relatório do Consultor

1. Clique na guia Consultor.
2. No Navegador do Consultor, clique em um gabarito de relatório.
3. Clique em *Consultor* > *Criar Relatório*.
4. Preencha as informações do gabarito e clique em *Ver Relatório*.

Instalação independente – Atualização manual do Consultor

Atualização manual da alimentação do Consultor

1. Vá para url //advisor.esecurityinc.com/advisordata/.
2. Digite seu nome de usuário e sua senha.

3. Vá para o último mês nas pastas de ataque e alerta e faça download dos arquivos compactados
4. Insira os novos arquivos de dados de alimentação de ataque e alerta (os arquivos estarão no formato zip) no computador.

NOTA: Não coloque os arquivos compactados nos diretórios de alerta e ataque.

5. Descompacte os arquivos de alimentação de ataque em:

   Para Windows:

   ```
   <local especificado durante a instalação para arquivos
      de dados do Consultor>\attack
   ```

   ou

   Para UNIX:

   ```
   <local especificado durante a instalação para arquivos
      de dados do Consultor>/attack
   ```

6. Descompacte os arquivos de alimentação de alerta em:

   Para Windows:

   ```
   <local especificado durante a instalação para arquivos
      de dados do Consultor>\alert
   ```

   ou

   Para UNIX:

   ```
   <local especificado durante a instalação para arquivos
      de dados do Consultor>/alert
   ```

7. Vá para:

   Para Windows:

   ```
   %ESEC_HOME%\sentinel\bin
   ```

   Para UNIX:

   ```
   $ESEC_HOME/sentinel/bin
   ```

8. Execute o seguinte comando:

   Para Windows:

   ```
   advisor.bat
   ```

   Para UNIX:

   ```
   ./advisor.sh
   ```

NOTA: advisor.sh e advisor.bat atualizarão o banco de dados e, em seguida, apagarão os arquivos de ataque e alerta que foram descompactados nos diretórios de ataque e alerta.

Download direto da internet – atualização manual do Consultor

Atualização de alimentação manual do Consultor

1. Vá para:

   Para Windows:

   ```
   %ESEC_HOME%\sentinel\bin
   ```

   Para UNIX:

   ```
   $ESEC_HOME/sentinel/bin
   ```

2. Execute o seguinte comando:

   Para Windows:

   ```
   advisor.bat
   ```

   Para UNIX:

   ```
   ./advisor.sh
   ```

NOTA: advisor.sh e advisor.bat atualizarão o banco de dados e, em seguida, apagarão os arquivos de ataque e alerta que foram descompactados nos diretórios de ataque e alerta.

Mudando a senha do servidor do Consultor e a configuração de e-mail

Mudando a senha do servidor do Consultor (independente)

Este procedimento não é aplicável para configurações independentes.

Mudando a senha do servidor do Consultor (download direto)

Para mudar a senha do servidor do Consultor (download direto)

1. Envie uma mudança de senha para o Suporte Técnico da Novell.
2. Depois de ser informado pela Novell sobre a mudança de senha, para UNIX, efetue login como esecadm ou, para Windows, efetue login com direitos administrativos.
3. cd para:

   Para UNIX:

   ```
   $ESEC_HOME/sentinel/bin
   ```

   Para Windows:

   ```
   %ESEC_HOME%\sentinel\bin
   ```

4. Digite os seguintes comandos:

   Para UNIX:

   ```
   ./adv_change_passwd.sh <oldpassword> <newpassword>
   ```

   Para Windows:

   ```
   adv_change_passwd.bat <oldpassword> <newpassword>
   ```

Mudando a configuração de e-mail do Consultor

Para mudar a configuração de e-mail do servidor do Consultor

1. Para Unix, efetue login como esecadm ou, para Windows, efetue login com direitos administrativos.
2. cd para:

   Para UNIX:

   ```
   $ESEC_HOME/sentinel/config
   ```

   Para Windows:

   ```
   %ESEC_HOME%\sentinel\config
   ```

3. Usando um editor de texto, abra alertcontainer.xml e alertcontainer.xml. Faça as mudanças editoriais na área cinza.

   ```
   <property
      name="advisor.mail.from">fromNAME@domain.com</prope
      rty>
   ```

   ```
   <property
      name="advisor.mailto.list">toNAME@domain.com</prope
      rty>
   ```

   NOTA: No caso de mais de um endereço de e-mail, digite os endereços de e-mail separados por vírgula, sem espaços.

Mudando o horário de alimentação de dados

Por padrão, os horários de alimentação de dados são:

- Seis horas 01:00, 07:00, 13:00 e 19:00
- Doze horas: 02:00 e 14:00

Para mudar horários de alimentação de dados

1. Efetue login em sua máquina com Consultor (para UNIX, efetue login como esecadm).
2. Para editar os horários de alimentação de dados:

   Para UNIX: use o comando 'crontab'

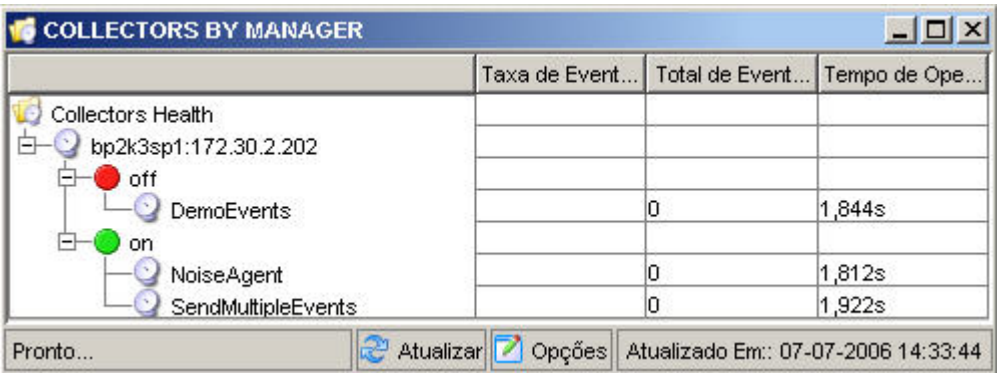
   Para Windows: use o comando 'at'

8 Guia Coletores

NOTA: O termo Agente é intercambiável com Coletor. Mais para a frente, Agentes será referido como Coletores.

Você deve ter permissão adequada para usar a guia Coletores. A guia Coletores proporciona funcionalidade limitada do Assistente. Para obter a funcionalidade completa do Assistente, use o Construtor de Coletor. A guia Coletores permite o seguinte:

- monitorar o Host do Assistente
- monitorar um Coletor
- iniciar e parar Coletores (Gerenciador de Coletor) para um host selecionado



Layout

O painel esquerdo na guia Coletores contém uma árvore de telas. Por padrão, a raiz tem dois filhos: Telas do Gerenciador de Coletor e Tela do Coletor. O painel direito exibe as telas em tabelas. Cada tela no painel direito tem uma entrada na árvore à esquerda.

Quatro telas são exibidas no painel direito:

- Tela Coletor
  - Gerenciador de Telas de Coletor
- Telas do Gerenciador de Coletor
  - Gerenciador de Telas do Gerenciador de Coletor

A Tela Coletor exibe informações sobre Coletores e a Tela Gerenciador de Coletor exibe informações sobre Gerenciadores de Coletor. Cada tela é exibida como uma tabela em árvore: o objeto é agrupado por um ou mais atributos. A configuração da tela é ajustável. As opções de uma tela podem ser mudadas e novos tipos de tela podem ser adicionados. A configuração da tela é exibida em um Gerenciador de Tela (Gerenciador de Telas de Coletor ou Gerenciador de Telas de Gerenciador de Coletor).

Quando a guia é exibida pela primeira vez, a árvore no painel esquerdo é preenchida com os dois gerenciadores de tela e o Gerenciador de Tela de Coletor é exibido no painel direito.

O Gerenciador de Tela de Coletor tem três opções de tela pré-configuradas por padrão; novas opções podem ser criadas. São elas: Todos os Coletores, Coletores por Gerenciador e Coletores por Status.

A tela Todos os Coletores exibe todos os Coletores agrupados pelo gerenciador em que estão sendo executados.

O Gerenciador de Tela de Gerenciador de Coletores agrupa todos os Coletores pelo gerenciador e também pelo status (ativado ou desativado) dentro de cada gerenciador.

A tela Coletores por Status agrupa todos os Coletores por status (Ativado ou Desativado) e, dentro de cada status, eles são agrupados por gerenciador.

Há uma tela padrão para ver Gerenciadores de Coletor: a tela Todos os Gerenciadores. Ela exibe todos os gerenciadores de Coletor ativos no sistema, sem agrupamento.

Monitorando um Coletor

Na Janela Host de Assistente, por padrão, você pode monitorar o seguinte:

Gerenciador da tela Gerenciador do Coletor

- StartTime — Horário em que o Gerenciador do Coletor foi iniciado, fornecido em mm/dd/aa hh:mm:ss, e fuso horário
- UpTime — Período em que o Gerenciador de Coletor está sendo executado, fornecido em dias, horas, minutos e segundos.
- EventReceivedCount — Número de eventos recebidos de todos os coletores pelo Gerenciador de Coletor desde o início de sua operação.
- EventReceivedRate — Média da taxa de evento por segundo que o Gerenciador do Coletor recebeu no último minuto.

Gerenciador da tela Gerenciador dos coletores

- Status — ligado ou desligado
- EventsReceivedRate — Média da taxa de evento por segundo que a Porta do Coletor recebeu no último minuto.
- EventsReceivedCount — Número de eventos recebidos pela Porta do Coletor desde o início de sua operação.
- UpTime — Período em que a Porta do Coletor está sendo executada, fornecido em dias, horas, minutos e segundos.

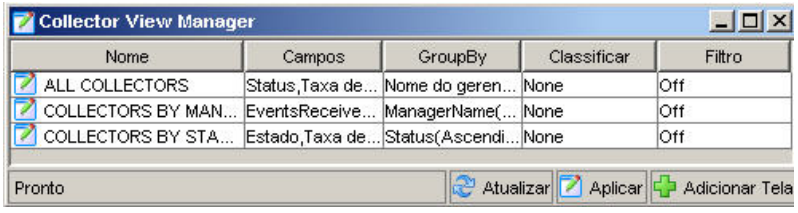
Você pode criar suas próprias telas e, com isso, obter mais ou menos campos.

Monitorando um host do assistente

Monitorando um host do assistente

1. Clique na guia *Coletores*.
2. Clique em *Gerenciador da tela Gerenciador do Coletor*.

3. Selecione uma opção de tela clicando duas vezes em uma tela, ou crie uma tela nova. Uma janela do Host do Assistente será exibida.



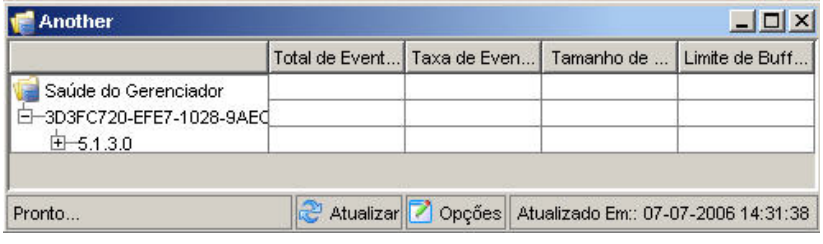
Criando uma tela Coletor

Criando uma tela Coletor

1. Clique na guia *Coletores*.
2. Clique em *Gerenciador da tela Gerenciador do Coletor*.

3. Para criar uma nova tela, clique no botão *Adicionar Tela*.
   - Insira seu nome de opção
   - Para organizar os campos que deseja mostrar, clique em *Campos*.
   - Para agrupar títulos diferentes, clique em *Agrupar*.
   - Para classificar por título, clique em *Classificar*
   - Para filtrar, clique em *Filtrar*.

   A seguir há um conjunto de telas com o Grupo definido como ManagerUUID e por Versão.

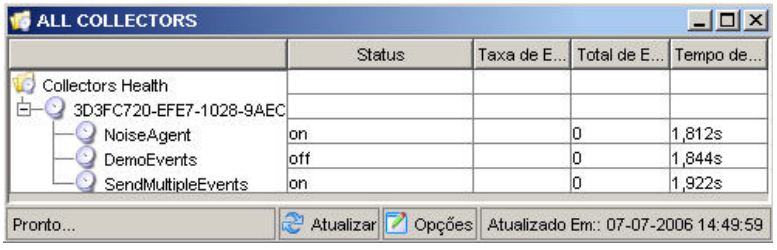


Modificando uma tela Coletor

Modificando uma tela Coletor

1. Abra o Gerenciador da tela Coletor.
2. Clique duas vezes em qualquer um dos nomes.
3. Clique em *Opções*. Nessa janela, você também poderá definir:
   - Campos...
   - Agrupar por...
   - Classificar...
   - Filtro...
   - Exibição em árvore
4. Clique em *Aplicar* e em *Gravar*.

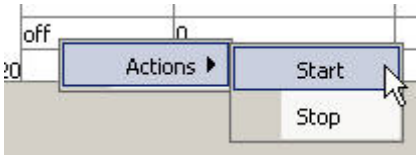
   Esta é uma tela com a exibição em árvore definida como UUID de Gerenciador.



Interrompendo/Iniciando/Detalhes dos coletores

Interrompendo/Iniciando coletores

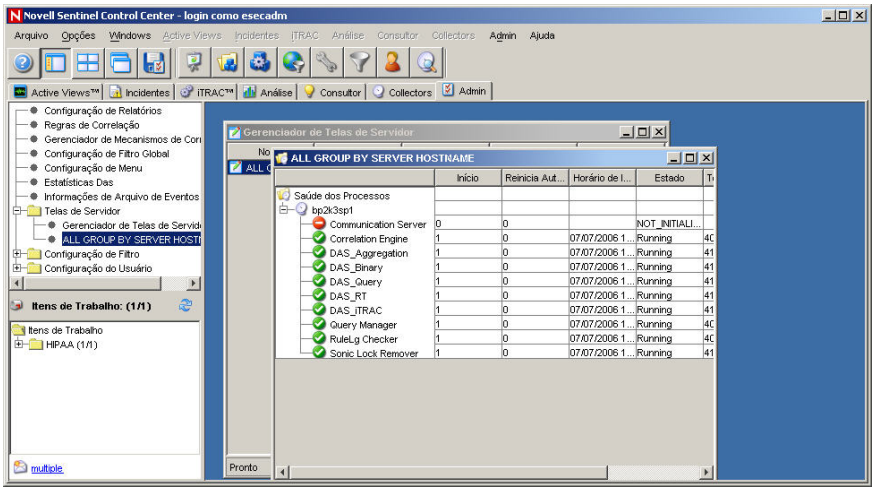
1. Clique na guia *Coletores*.
2. Abra um Gerenciador da tela Coletor
3. Para interromper/iniciar/mostrar detalhes em um único Coletor, clique o botão direito do mouse em um *Coletor* > *Ações* > *Iniciar ou Parar*.



9 Guia Admin

NOTA: O termo Agente é sinônimo de Coletor. De agora em diante, Agentes serão referidos como Coletores.

Para usar este recurso, você deve ter a permissão adequada. Caso essa permissão não seja concedida, nenhuma das outras permissões relacionadas às ações que usam essa guia estará disponível.



Guia Admin – descrição

A Guia Admin permite o acesso a:

- Configuração de relatórios de análise e consultor do Advisor
- Gerenciar filtros
- Trabalhando com as Regras de Correlação do Sentinel
- Configurar o menu de Configuração de Menu
- Estatísticas do DAS
- Informações de arquivos de evento
- Telas de Servidor
- Configurar contas de usuário

Opções de configuração de relatórios de análise e consultor

Para configurar o URL para os Relatórios de análise e consultor

1. Clique na guia *Admin*.
2. No *Navegador de Admin*, clique em *Configuração de Relatório*.

3. Na janela de *Configuração de Relatório*, clique em *Modificar*.
   - Na caixa URL de Análise, insira o URL para o Crystal Enterprise Server e clique em *Atualizar*.

     ```
     http://<IP>/GetReports.asp?APS=<IP>&user=Guest&passwor
        d=&tab=Analysis
     ```

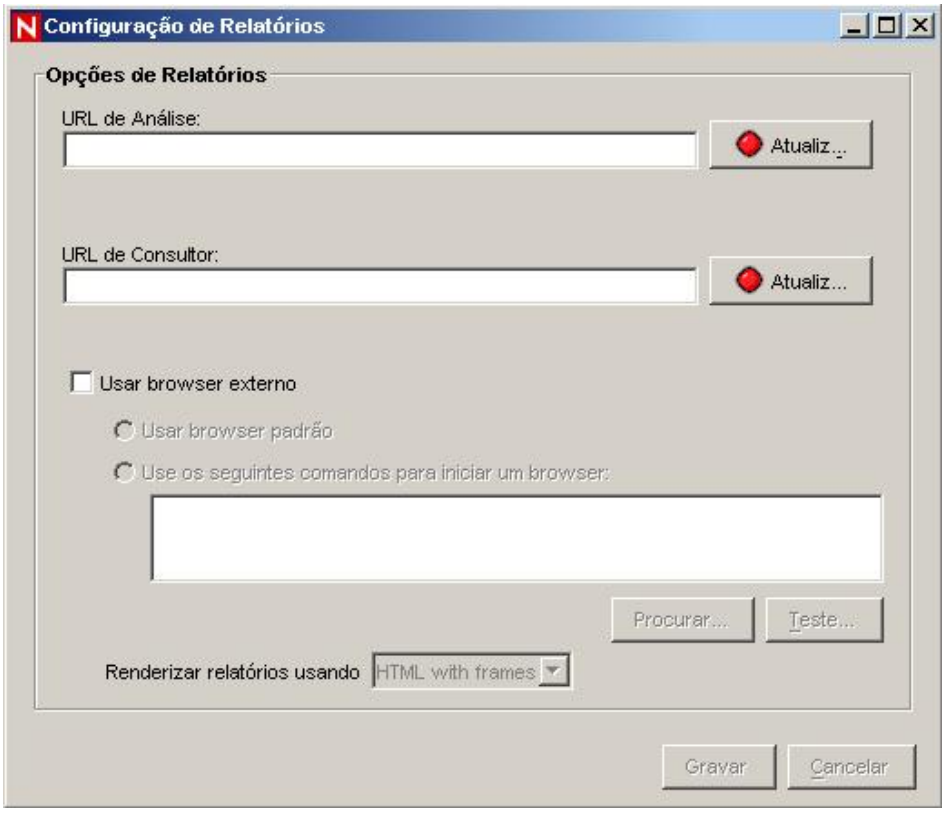
NOTA: <IP> é o endereço IP do Crystal Enterprise Server.

   - Na caixa URL de Consultor, insira o URL para o Crystal Enterprise Server e clique em *Atualizar*.

     ```
     http://<IP>/GetReports.asp?ASP=<IP>&user=Guest&passwor
        d=&tab=Advisor
     ```

NOTA: <IP> é o endereço IP do Crystal Enterprise Server.

Para obter mais informações, consulte o *Guia de Instalação*.



A opção de browser externo permite usar seu browser padrão ou outro browser. Ao usar um navegador diferente do browser padrão, sua linha de comando deve ser seguida por um %URL%. Por exemplo:

```
C:\Arquivos de Programas\Internet
   Explorer\IEXPLORE.EXE %URL%
```

4. Aguarde o botão Atualizar ficar verde e clique em *Gravar*. Você terá que efetuar logout do Sentinel Control Center e efetuar login novamente.

Regras de correlação do Sentinel

A correlação agrega inteligência ao gerenciamento de eventos de segurança, permitindo que você automatize a análise do fluxo de eventos de entrada para encontrar padrões de interesse. A correlação permite definir regras que identificam as ameaças importantes e padrões complexos de ataque, para que você consiga priorizar os eventos e iniciar o gerenciamento e a resposta eficazes aos incidentes.

As pastas de regras são o agrupamento lógico das regras de correlação. As regras de correlação de agrupamento nas pastas de regra também permitem que você tenha um conjunto de regras que é executado durante o dia útil ou um conjunto que seja executado à noite, e outro conjunto que funciona no final de semana. Em essência, observar atividades diferentes de acordo com a hora do dia.

Por exemplo, você pode habilitar todas as regras de correlação do período diurno de uma só vez, às 8h, de segunda a sexta-feira, e também desabilitar as regras durante a noite, todas ao mesmo tempo. Especificamente, se você não precisar agrupar as regras de correlação em pastas de regras, poderá criar apenas uma pasta de regra e criar nela todas as regras de correlação.

Não há limite no número de usuários que podem acessar as regras de correlação. Quando mais de um usuário estiver editando a mesma regra, a última pessoa a gravar sobrescreverá todas as gravações anteriores.

Esta seção discute o seguinte:

NOTA: você não pode correlacionar em um valor nulo (vazio).

Pastas de regras e regras

Veja a seguir a definição do relacionamento entre Pastas de Regra e Regras. As pastas de regras e as regras são exibidas de forma hierárquica na janela regras de correlação.

- Uma pasta de regra pode conter zero ou mais regras
- O número de pastas de regras e regras só é limitado pelo espaço em disco disponível (armazenamento)
- Clicar duas vezes em uma pasta de regra exibe o Editor de Regra para aquele tipo de regra de correlação
- A extensão máxima do nome das pastas de regras é de 255 caracteres para o caminho da pastas, e o nome da regras é de 255 caracteres
- As descrições das pasta de regras e da regra podem ser de até 1024 caracteres

Tipos de Regra de Correlação

Há quatro tipos de regra de correlação que você pode escolher ao definir as regras. São eles:

- Lista de Avisos
- Correlação Básica

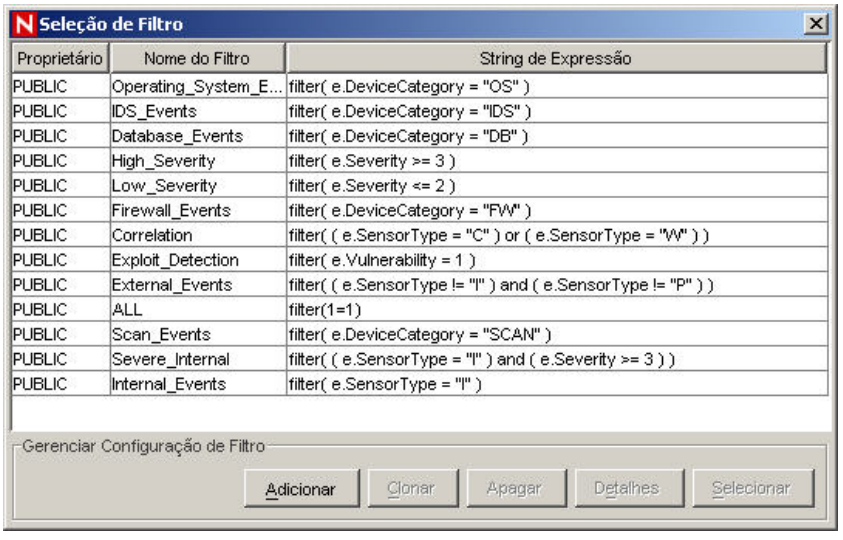
- Correlação Avançada
- RuleLg de Formato Livre

AVISO: Você deve estar familiarizado com o idioma de definição da regra de correlação de RuleLg antes de usar esse tipo de regra de correlação. Além disso, se renomear uma tag, não use o nome original ao criar uma regra de correlação com o RuleLg.

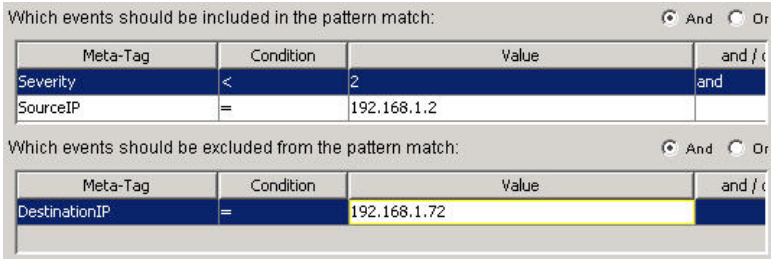
Lista de Avisos

Há quatro tipos diferentes de filtros dentre os quais escolher. São eles:

- Permitir tudo – Permite todos os eventos.
- Padrão – Qualquer expressão regular com uma sintaxe semelhante a grep.
- Gerenciador de Filtro – Uma lista suspensa que exibe o Gerenciador de Filtro para a seleção ou criação de um novo filtro.



- Construtor – Criação de critérios para inclusão ou exclusão de eventos com base na álgebra booleana. Estão disponíveis dois painéis (incluir e excluir). Insira seus valores aqui, por exemplo:



Correlação Básica

Há quatro tipos diferentes de filtros dentre os quais escolher. São eles:

- Permitir tudo – Permite todos os eventos.
- Padrão – Qualquer expressão regular com uma sintaxe semelhante a grep.

- Gerenciador de Filtro – Uma lista suspensa que exibe o Gerenciador de Filtro para a seleção ou criação de um novo filtro.
- Construtor – Criação de critérios para inclusão ou exclusão de eventos com base na álgebra booleana.

Essa regra permite contar o número de vezes que certas condições são atendidas dentro de determinado espaço de tempo.

Por exemplo, uma regra de Correlação Básica pode procurar pelo mesmo endereço IP reportado cinco vezes em cinco minutos, mesmo que os eventos sejam reportados de diferentes dispositivos, como um sistema de detecção de invasão (IDS) e um firewall.

Correlação Avançada

Há quatro tipos diferentes de filtros dentre os quais escolher. São eles:

- Permitir tudo – Permite todos os eventos.
- Padrão – Qualquer expressão regular com uma sintaxe semelhante a grep.
- Gerenciador de Filtro – Uma lista suspensa que exibe o Gerenciador de Filtro para a seleção ou criação de um novo filtro.
- Construtor – Criação de critérios para inclusão ou exclusão de eventos com base na álgebra booleana.

Esta regra permite que você:

- Conte o número de vezes que certas condições são atendidas dentro de determinado período de tempo.
- Incorpore todos os recursos da regra de correlação simples e também avalie eventos em relação a eventos passados.

Por exemplo, uma regra de Correlação Avançada pode procurar por eventos do mesmo endereço IP fonte para o mesmo endereço de destino com o mesmo nome de evento que ocorre tanto dentro quanto fora de um firewall (o que quer dizer que o ataque ocorreu através do firewall).

Correlação de RuleLg de formato livre

A linguagem de definição de regra de correlação RuleLg permite que você tenha controle total sobre a definição das regras de correlação. Para usar esse tipo de regra de correlação, você deve estar familiarizado com a linguagem de definição das regras de correlação RuleLg.

Distribuição da regra do mecanismo de correlação

Para usar esse recurso, você deve ter a permissão de usuário Iniciar/Parar Mecanismo de Correlação. O Mecanismo de Correlação apresenta dois estágios, ativado ou desativado. O estado atual é exibido no ícone.

- Ativado - 
- Desativado - 

Quando o Mecanismo de Correlação é ativado, ele está processando as pastas de regras de correlação ativas.

Quando o mecanismo é desativado, todos os dados de sua memória interna são preservados e nenhum evento novo de correlação é gerado. Este estado é equivalente à desativação de todas as pastas de regras. A desativação do mecanismo de correlação não afeta outras partes do sistema. Os eventos de entrada ainda vão passar, preenchendo o banco de dados do Sentinel.

Importando e exportando as regras de correlação

O recurso de exportação permite que o Sentinel crie e exporte regras de correlação “fornecidas” e torne-as disponíveis para você para importação para o sistema. Esses documentos XML são formatados especificamente para o mecanismo de correlação. Essas regras pré-empacotadas são desenvolvidas pelo Sentinel e estão disponíveis no Portal do Cliente, no endereço http://www.esecurityinc.com.

A capacidade de exportar regras como documentos XML o ajuda quando você precisar da ajuda da Novell para resolver problemas nas suas regras de correlação. Exportar também é algo benéfico quando você tiver um Sentinel "em produção" e um Sentinel em "desenvolvimento". Você pode desenvolver e testar as regras de correlação no ambiente de desenvolvimento e depois exportar essas regras para o ambiente de produção. A extensão do arquivo para as regras exportadas de correlação é .crf.

Função do banco de dados ao armazenar regras de correlação

Ao ativar o Mecanismo de Correlação (um processo do Sentinel Server) no Sentinel Control Center, ela solicita as informações e as regras de distribuição do banco de dados. Ao modificar as regras de correlação e depois gravá-las, elas são enviadas para o banco de dados para fins de armazenamento. As mudanças na regra não se refletirão no Mecanismo de Correlação, a menos que um dos seguintes itens seja realizado:

- a regra distribuída é desativada e depois ativada
- a regra foi recentemente distribuída

Ao modificar as regras de distribuição e depois gravá-las, elas são enviadas para o banco de dados para armazenamento e para o Mecanismo de Correlação, onde são colocadas em uso.

Condições lógicas para as regras de correlação

A seguir são apresentadas as condições lógicas usadas ao criar regras de correlação. Para obter mais informações sobre as metatags, consulte o *Guia de Referência do Usuário do Sentinel*.

Condição	Campo de tipo	Descrição
=	valor numérico string	O conteúdo da metatag selecionada é igual ao valor inserido.
!=	valor numérico string	O conteúdo da metatag selecionada não é igual ao valor inserido.
<	valor numérico	O conteúdo da propriedade selecionada é menor do que o valor inserido.
>	valor numérico	O conteúdo da metatag selecionada é maior do que o valor inserido.
<=	valor numérico	O conteúdo da metatag selecionada é menor que ou igual ao valor inserido.
>=	valor numérico	O conteúdo da metatag selecionada é maior que ou igual ao valor inserido.
=Metatag	valor numérico string	O conteúdo da metatag selecionada na lista suspensa à esquerda é igual ao conteúdo da metatag selecionada à direita da expressão.

Condição	Campo de tipo	Descrição
!=Metatag	valor numérico string	O conteúdo da metatag selecionada na lista suspensa à esquerda não é igual ao conteúdo da metatag selecionada à direita da expressão.
<Metatag	valor numérico	O conteúdo da metatag selecionada na lista suspensa à esquerda é menor do que o conteúdo da metatag selecionada à direita da expressão.
>Metatag	valor numérico	O conteúdo da metatag selecionada na lista suspensa à esquerda é maior do que o conteúdo da metatag selecionada à direita da expressão.
<=Metatag	valor numérico	O conteúdo da metatag selecionada na lista suspensa à esquerda é menor que ou igual ao conteúdo da metatag selecionada à direita da expressão.
>=Metatag	valor numérico	O conteúdo da metatag selecionada na lista suspensa à esquerda é maior que ou igual ao conteúdo da metatag selecionada à direita da expressão.
=Regex	valor numérico string	Use um ponto (.) e um asterisco (*) com o string para o valor.
Sub-rede	valor numérico string	Uma operação correspondente de sub-rede corresponderá caso o endereço IP que está sendo comparado estiver na mesma sub-rede, como especificado na operação de sub-rede de correspondência.

Abrindo a janela Regras de Correlação

A janela Regras de Correlação permite fazer o seguinte:

- Nova pasta – para criar uma nova Pasta de Regra
- Nova regra – para criar uma regra para uma pasta
- Copiar uma pasta de regra – permite modificar as Pastas de Regra copiadas ou as Regras enquanto grava a Pasta de Regra ou a Regra original
- Apagar uma pasta de regra ou regra – você não pode recuperar uma Pasta de Regra ou Regra apagadas depois de confirmar a exclusão
- Renomear – para renomear uma regra ou pasta de regra
- Importar uma pasta de regra – abrirá uma janela do browser
- Exportar uma pasta de regra – abrirá uma janela do browser, exportando a pasta de regra como arquivo xml.
- Editar – permite editar e visualizar as regras e as propriedades da pasta

Abrindo a janela de Regras de Correlação

1. Clique na guia *Admin*.
2. No *Navegador de Admin*, clique em *Regras de Correlação*.

Copiando e criando uma pasta de regra ou regra

Criando uma pasta de regra

1. Abra a janela de Regras de correlação.

2. Selecione a pasta de origem que vai conter a nova pasta.
3. Clique o botão direito do mouse em > *Nova pasta*.
4. Digite o nome da pasta de regra, com limite de 255 caracteres que diferenciam maiúsculas e minúsculas, sem pontos.
5. (Opcional) Digite a Descrição da regra, com limite de 1024 caracteres.
6. Clique em *OK*.

Criando uma regra

1. Selecione a pasta de origem que vai conter a nova regra.
2. Clique o botão direito do mouse em > *Nova regra*.
3. Abrirá o Assistente de Regra; selecione um dos seguintes tipos de regra:
   - Lista de Avisos
   - Correlação Básica
   - Correlação Avançada
   - Formato livre

   NOTA: Para ver descrições dos tipos de regra, vá para a seção Tipos de regra de correlação.
4. Clique em *Concluir*.

Apagando uma pasta de regras de correlação ou regras

Apagando uma pasta de regra de correlação ou regra

1. Abra a janela de Regras de correlação.
2. Selecione a pasta de regra ou a regra que você deseja apagar.
3. Clique o botão direito em > *Apagar*.
4. Aparecerá uma caixa de confirmação:
   - Sim – ao apagar uma pasta de regra, as regras naquela pasta de regra também serão apagadas. Você não pode recuperar uma regra apagada depois de clicar em *OK*.
   - Não – fará você retornar à janela Regras de Correlação

Importando ou exportando uma pasta de regra de correlação

Importando ou exportando uma pasta de regra de correlação

1. Abra a janela de Regras de correlação.
2. Selecione uma pasta de regra.
3. Clique o botão direito do mouse em > *[Importar Pasta de Regra ou Exportar Pasta de Regra]*
   - Importar – Abrirá um browser de arquivo; vá até a pasta de regra a ser importada e clique em *OK*.
   - Exportar – Abrirá um browser de arquivo; vá até o dispositivo de destino ao qual a pasta de regra será gravada e clique em *OK*. A pasta de regra será exportada como um arquivo crf.

Editando na janela de correlação

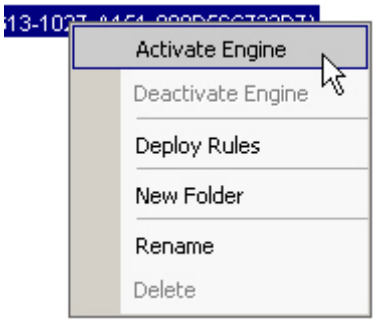
Editando na janela de correlação

1. Abra a janela de Regras de correlação.
2. Clique o botão direito do mouse em > *Editar*.
3. Edite a regra e clique em *Concluir*.

Ativando ou desativando um mecanismo de correlação

Ativando ou desativando um mecanismo de correlação

1. Abra a janela do Gerenciador do mecanismo de correlação.
2. Realce e clique o botão direito do mouse em um *Mecanismo de correlação* > *Ativar ou Desativar Mecanismo.*

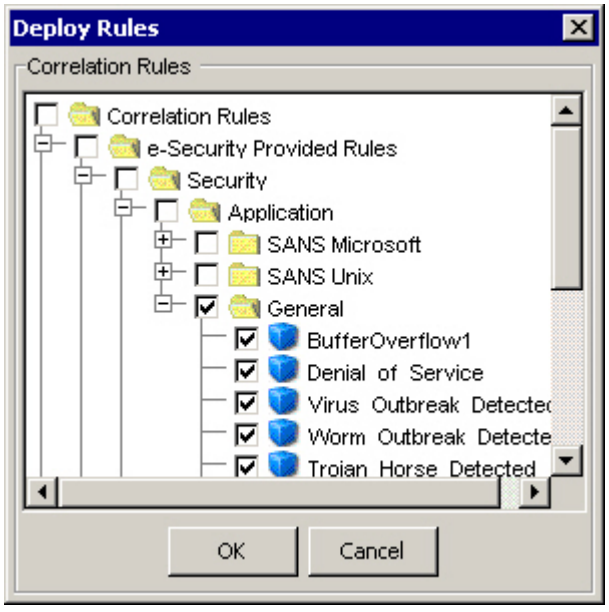


Distribuindo as regras de correlação

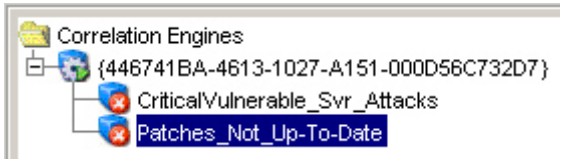
Distribuindo as regras de correlação

1. Abra a janela do Gerenciador do mecanismo de correlação.

2. Clique o botão direito do mouse (em qualquer pasta na janela ou realce o mecanismo para fazer com que a regra seja distribuída de lá) > *Distribuir regras*.
3. Coloque uma marca de verificação próximo às regras que você deseja distribuir. Clique em *OK*.

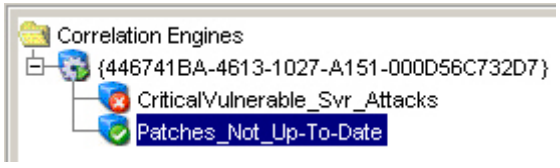


4. Para iniciar sua regra, você deve mover a regra para um mecanismo de correlação.



NOTA: as regras são distribuídas habilitadas.

5. No mecanismo de correlação, realce sua regra e clique o botão direito em > *Habilitar Regra*.



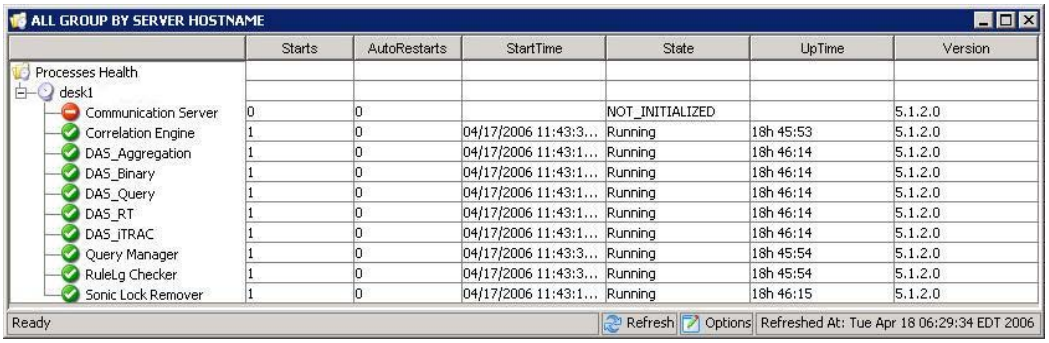
Telas de Servidor

As Telas de Servidor permitem fazer o seguinte:

- Monitorar o status de todos os processos do Sentinel Server no sistema
  - Servidor de Comunicação
  - Mecanismo de Correlação
  - DAS_Binary
  - DAS_iTrac
  - DAS_Query
  - DAS_RT
  - Gerenciador de Consultas
  - Verificador de RuleLg
  - Sonic Lock Remover

NOTA: No Windows, o Servidor de Comunicação é executado como um Serviço do Windows e, portanto, não pode ser monitorado pelas Telas de Servidor. Para monitorar o Servidor de Comunicação no Windows, use o Windows Service Manager.

O processo do Sonic Lock Remover é habilitado apenas no Windows. Quando um processo não for habilitado em um servidor particular, a sua coluna Habilitado será definida como "0" e sua coluna Estado será mostrada como NOT_INITIALIZED.



- Processos iniciar, interromper ou reiniciar – Clique o botão direito do mouse na entrada do processo para que essas ações possam ser levadas em um processo.

NOTA: As ações realizadas com o botão direito do mouse no Servidor de Comunicação não são habilitadas porque a interrupção do Servidor de Comunicação resultaria na perda do contato com todos os processos.

Os termos *Starts* e *AutoRestarts*, no contexto da *Tela do Servidor*, são definidos da seguinte forma:

- Starts – O número de vezes que o processo foi iniciado, por qualquer que seja o motivo. Isso inclui as inicializações feitas pelo usuário através da GUI ou feitas automaticamente.
- AutoRestarts – O número de vezes que o processo foi automaticamente reiniciado. Como isso só se aplica a cenários de reinicialização puramente automática, não se aplica às reinicializações feitas por um usuário. Este campo é útil para determinar se o processo foi interrompido (por exemplo, devido a um erro) e foi automaticamente reinicializado pelo Sentinel Watchdog.

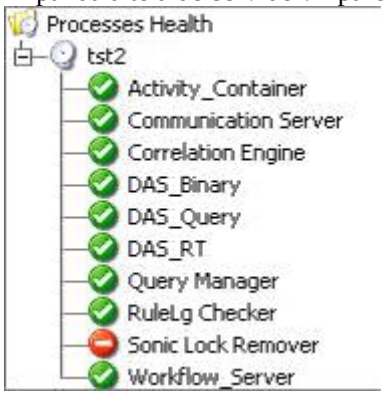
Monitorando um processo

Monitorando um processo

1. Clique na guia *Admin*.
2. Clique em *Telas de Servidor*.

3. Clique duas vezes em uma tela. Aparecerá uma tela.

4. Expanda a tela do servidor. Aparecerão na lista todos os processos.



Criando uma tela de servidor

Criando uma tela de servidor

1. Clique na guia *Admin*.
2. Clique em *Telas de Servidor*.

3. Para criar uma nova tela, clique em *Adicionar Tela*.
   - Digite seu nome de opção
   - Para organizar os campos que deseja mostrar, clique em *Campos*.
   - Para agrupar títulos diferentes, clique em *Agrupar*.
   - Para classificar por título, clique em *Classificar*
   - Para filtrar, clique em *Filtrar*.
4. Clique em *OK* e, em seguida, em *Gravar*.

Iniciando, interrompendo e reiniciando processos

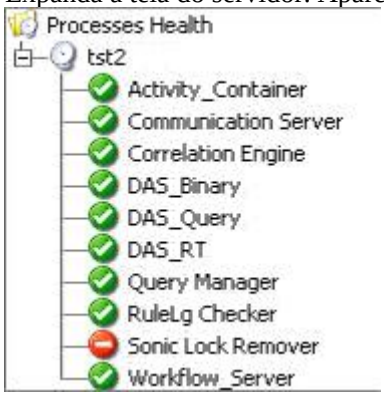
Você não pode parar o Servidor de Comunicação usando este recurso.

Iniciando, interrompendo e reiniciando processos

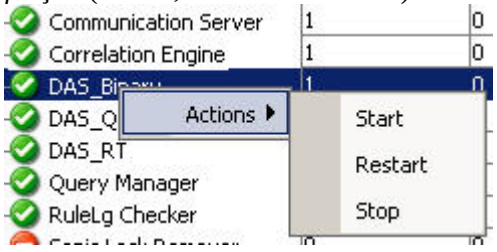
1. Clique na guia *Admin*.
2. Clique em *Telas de Servidor*.

3. Clique duas vezes em uma tela. Aparecerá uma tela.

4. Expanda a tela do servidor. Aparecerão na lista todos os processos.



5. Selecione um processo, clique o botão direito do mouse em > *Ações* > *selecione uma função* (*Iniciar, Reiniciar ou Parar*).



Filtros

Os filtros permitem o processamento de dados com base em um critério específico para os eventos em tempo real e para usuários do sistema. Os filtros permitem gerenciar os dados vistos no Sentinel Control Center. O mecanismo de filtro orienta as janelas de Evento em tempo real mantendo a estrutura de dados para cada filtro de segurança. Os filtros impedem que os usuários visualizem os eventos não-autorizados e os eventos de queda que os usuários não desejam ver. Os filtros são criados na guia Admin do Sentinel Control Center.

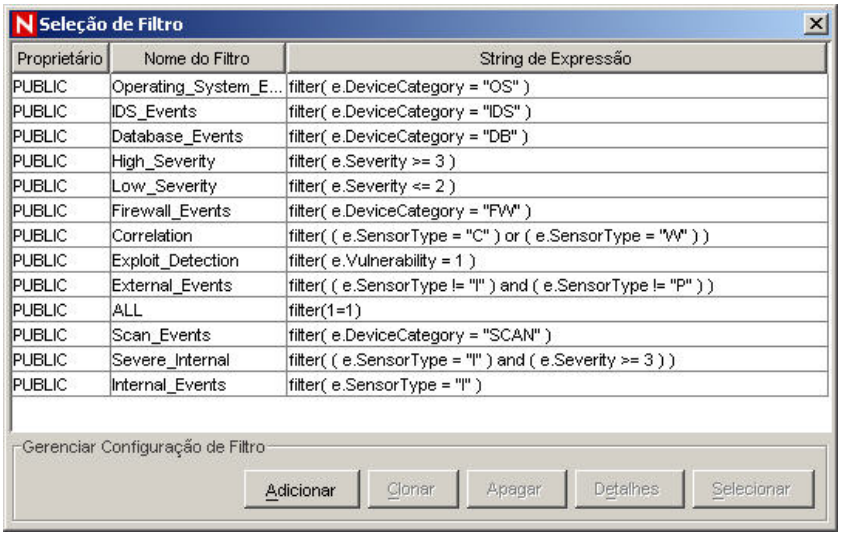
NOTA: a seguir há caracteres inválidos de nome de filtro: $ # . * & : < >.

Há três tipos de filtros:

- Filtros públicos
- Filtros privados
- Filtros globais

Filtros públicos

Os filtros públicos são de propriedade do sistema. Os filtros públicos podem ser usados como filtros de segurança ou filtros de exibição. Os filtros de segurança são baseados em permissões do usuário. Os filtros de exibição determinam quais eventos são descritos nas tabelas e nos gráficos de eventos em tempo real.



Filtros particulares

Os filtros Privados são de propriedade do usuário. Os filtros particulares são filtros de exibição e poderão ser compartilhados se você tiver a permissão Ver Filtros Particulares.

Filtros globais

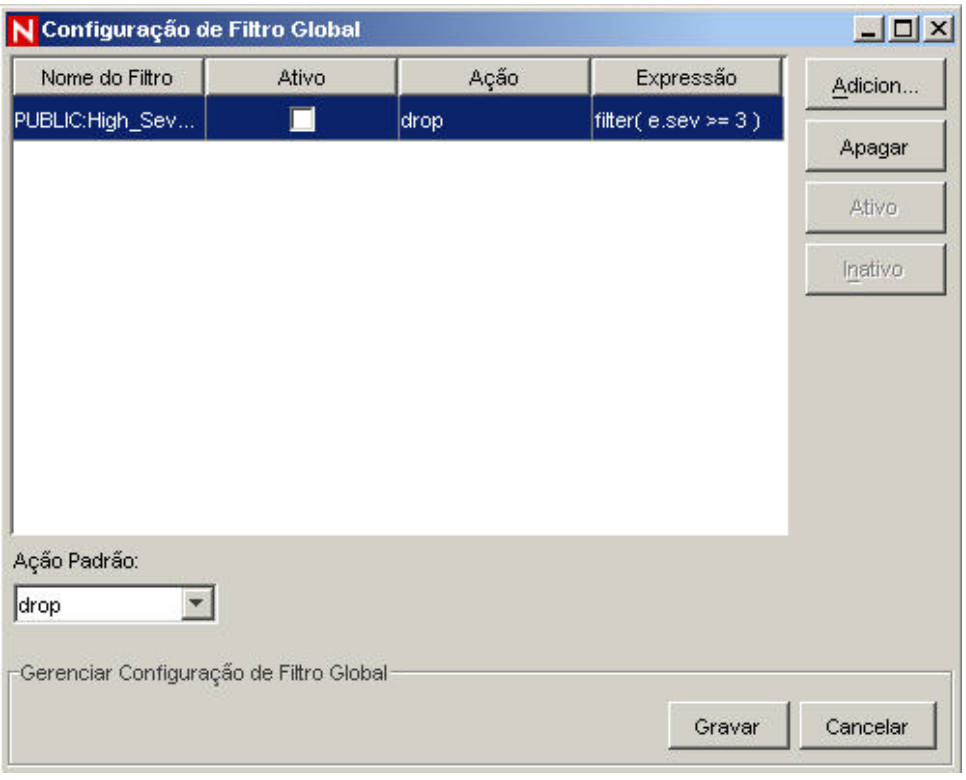
Os filtros globais são classificados como Filtros Públicos. Os filtros globais são processados no Gerenciador do coletor seqüencialmente para cada evento, até que seja encontrada uma correspondência. A avaliação do filtro global é interrompida para esse evento, e a ação do filtro global que corresponde é assumida para aquele evento. A ordem da avaliação dos filtros globais é de cima para baixo, como aparece no Console. Eles podem ser ativados ou desativados conforme necessário.

Os filtros globais fazem o seguinte:

- Habilitam uma ação global nos eventos, como eventos de queda, eventos de roteamento apenas ao banco de dados ou eventos de roteamento ao banco de dados e ao Sentinel Control Center
- São processados pelo Gerenciador de coletor do Assistente
- São configurados na guia Admin na opção Configuração de filtro global, na qual podem ser ativados e desativados
- Descartam eventos
- Podem rotear os eventos apenas para o banco de dados
- Podem rotear os eventos para o banco de dados e para o Sentinel Control Center.

Na janela Configuração Global, você pode:

- Criar filtro global
- Reorganizar um filtro global
- Apagar um filtro global



Criando um filtro global

Criando um Filtro Global

1. Clique na guia *Admin*.
2. Clique em *Admin* > *Configuração de Filtro Globa*l, ou selecione *Configuração de Filtro Global* na árvore de navegação.
3. Na janela Configuração Global, clique em *Modificar* e clique em *Adicionar*.
4. Na nova fila em branco, clique na coluna *Nome do filtro*.
5. Selecione um filtro e clique em *Selecionar* ou *Adicionar* (se você precisar criar um filtro).
6. Na coluna Ativo, clique na caixa Ativo.
7. Na coluna Ação, selecione a ação que o filtro global terá nos eventos que passam por este filtro global. Caso um evento não atender a nenhum dos filtros globais ativos, a ação-padrão determina como o evento é tratado.

   Você pode configurar a caixa Ação padrão da seguinte forma:

   - queda – os eventos não vão para o Sentinel Control Center, nem para o banco de dados do Sentinel Server
   - banco de dados – os eventos serão enviados diretamente para o banco de dados, pulando o Sentinel Control Center
   - banco de dados e GUI – os eventos serão enviados para o Sentinel Control Center e para o banco de dados do Sentinel Server
8. Continue adicionando filtros até você concluir.
9. Clique em *Gravar*.

Reorganizando os filtros globais

Reorganizando os filtros globais

1. Na janela de Configuração global, clique em *Modificar*.
2. Selecione um filtro e clique em *Para cima* ou *Para baixo* para movê-lo para um local diferente na lista.
3. Clique em *Gravar*.

Apagando um filtro global

NOTA: ao apagar um filtro global, você não vai receber uma mensagem de confirmação.

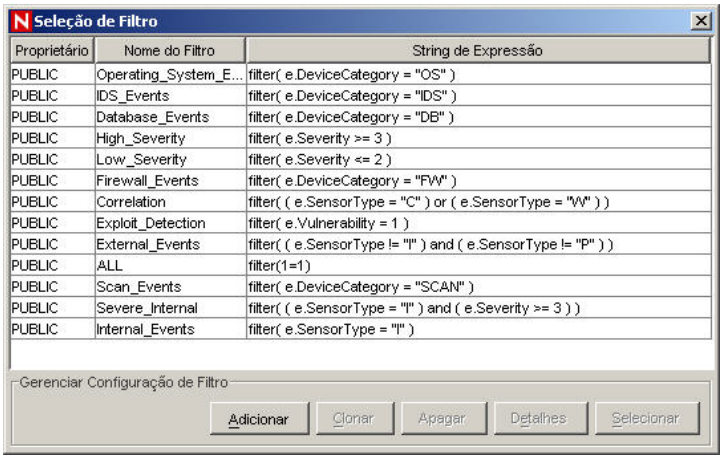
Para apagar um filtro global

1. Na janela de *Configuração global*, clique em *Modificar*.
2. Selecione um filtro da lista e clique em *Apagar*.
3. Clique em *Gravar*.

Configurando filtros públicos e particulares

A configuração de filtros públicos e particulares permite fazer o seguinte:

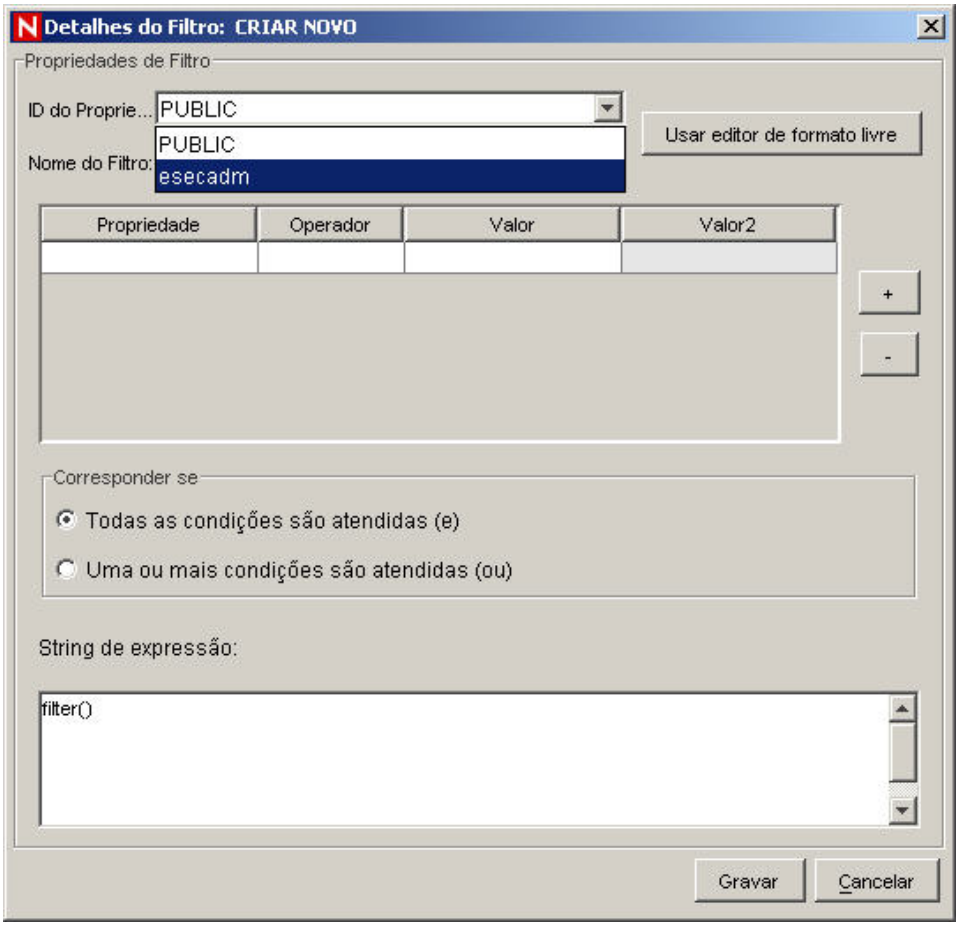
- Adicionar um filtro
- Clonar um filtro
- Modificar um filtro
- Visualizar os detalhes de um filtro
- Apagar um filtro



Adicionando um filtro

Para adicionar um filtro público e particular

1. Clique na guia *Admin*.
2. Clique em *Admin* > *Gerenciador de Filtros* ou selecione *Gerenciador de Arquivo* na pasta *Configuração de Filtro* no navegador.
3. Clique em *Adicionar*.
4. Selecione um ID de proprietário (particular ou privado [propriedade do usuário]).



5. Insira um nome de filtro.
6. O editor de tabela é a seleção-padrão para editar o conteúdo.

NOTA: Como opção, você pode clicar em Usar editor de formato livre para ver um editor de formato livre. O editor de formato livre permite criar expressões complexas que seriam impossíveis com o editor de tabela. No entanto, depois que a expressão é modificada com o editor de formato livre, o editor de tabela não pode ser usado com a expressão.

---

7. Selecione os critérios para as seguintes colunas:
   - Propriedade
   - Operador
   - Colunas de valor.

   Suas escolhas são exibidas na caixa String de expressão.
8. Na caixa Corresponder se, clique em:
   - Todas as condições são atendidas (e)
   - Uma ou mais condições são atendidas (ou)
9. Para criar outra expressão de filtro, clique no botão *Criar uma Nova Expressão de Filtro* (+) para adicionar outra linha à tabela de expressão do filtro.

10. Para remover uma expressão de filtro, selecione uma expressão de filtro da tabela e clique no botão Remover a Expressão Selecionada (-).
11. Clique em *Gravar*.

Para clonar um filtro público e particular

A clonagem é uma forma conveniente de duplicar um filtro para garantir consistência de critérios entre um grupo de filtros ou usuários.

Para clonar um filtro público e particular

1. Abra a janela do Gerenciador de Filtro.
2. Clique em *Clonar*.
3. Insira um novo nome de filtro.
4. Mude qualquer critério do filtro original.
5. Clique em *Gravar*.

Modificando um filtro público e particular

Para modificar um filtro público e particular

1. Abra o Gerenciador de filtro.
2. Selecione um filtro e clique em *Detalhes*.
3. Mude qualquer critério conforme desejado. Você não vai conseguir mudar o ID do Proprietário e o *Nome do Filtro*.
4. Clique em *Gravar*.

Visualizando os detalhes de um filtro público e particular

Para ver um filtro público ou particular

1. Abra a janela do *Gerenciador de Filtro*.
2. Selecione um filtro e clique em *Detalhes*.

Apagando um filtro público e particular

Para apagar um filtro público e particular

1. Abra a janela do *Gerenciador de Filtro*.
2. Selecione um filtro e clique em *Apagar*.
3. Abrirá uma janela de confirmação.

Definir configuração do menu

Para usar este recurso, você deve ter a permissão do usuário Configuração de Menu.

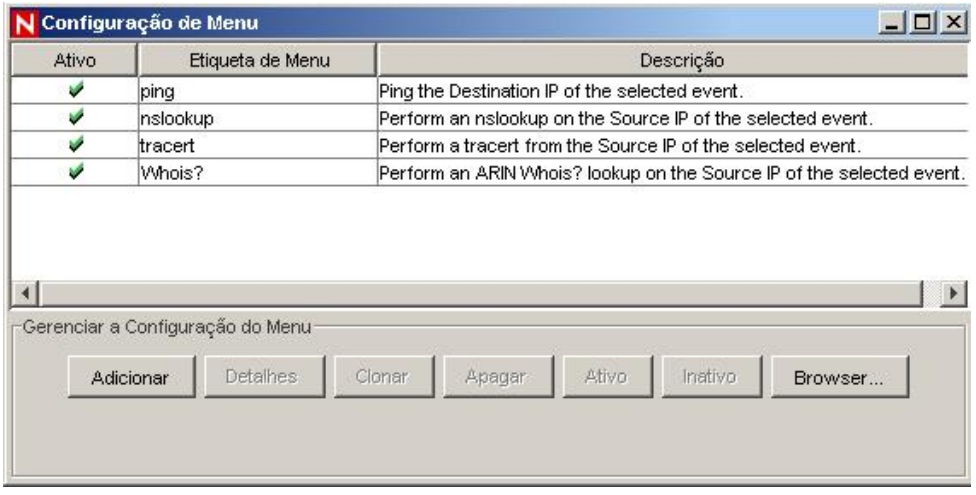
Use a janela Configuração de Menu para criar os itens de menu que aparecem no menu Evento, que aparece em qualquer tabela que exibe um evento (por exemplo, janela Tempo real de evento, janela Instantâneo, janela Eventos de incidentes, etc.) ao selecionar um ou mais eventos e clique o botão direito do mouse. O Sentinel tem os seguintes itens-padrão de Configuração do Menu que você pode clonar, ativar ou desativar:

- ping – Faz ping do IP de destino do evento selecionado
- nslookup – Realiza um nslookup no IP de origem do evento selecionado

- traceroute (tracert no MS SQL) – Realiza um traceroute do IP de origem do evento selecionado no Sentinel Server
- Whois? – Realiza uma pesquisa ARIN Whois? no IP de origem do evento selecionado

A Configuração do Menu permite fazer o seguinte:

- Adicionando uma opção ao menu de Configuração de Menu
- Clonando uma opção de menu Configuração de Menu
- Modificando uma opção de Configuração de Menu
- Exibindo os parâmetros da opção Configuração de Menu
- Ativando ou desativando uma opção de menu Configuração de Menu
- Reorganizando as opções do menu de evento
- Apagando uma opção de menu Configuração de Menu
- Adicionar um recurso de browser à sua opção de Configuração do Menu



Adicionando uma opção ao menu de Configuração do Menu

NOTA: se renomear uma tag, como CustomerVar24 para PolicyName, você deve usar o novo nome ao configurar os parâmetros.

Para adicionar uma opção de menu Configuração de Menu

1. Clique na guia *Admin*.
2. No Navegador de Admin, clique em *Admin* > *Configuração de Menu*.
3. Na caixa de diálogo Configuração do Menu, insira o seguinte:
   - Nome
   - Descrição
   - Ação – execute um comando ou abra um browser
   - Usar browser – se você escolheu a ação "Executar comando" e suas configurações de browser estão configuradas para "Usar browser externo" (consulte Editando as configurações de browser de Configuração do Menu para editar as configurações do browser), você tem a opção de selecionar Usar browser. A seleção desta opção fará com que a saída do seu comando seja exibida usando-se as configurações do browser da Configuração do Menu para o seu Sentinel Control Center.

- Tipo de arquivo – se você escolheu a ação "Executar comando", suas configurações de browser estão configuradas para "Usar browser externo" e você selecionou a opção "Usar browser", você tem a opção de configurar o tipo de arquivo para a saída deste comando.
- Linha de comando/URL

NOTA: para UNIX, o script/aplicativo ou o link simbólico para o script/aplicativo devem estar localizados no diretório $ESEC_HOME\sentinel\exec. Para qualquer script, aplicativo ou link simbólico, insira apenas o comando. Qualquer caminho inserido será ignorado.

NOTA: Para o Windows (correlação), o script/aplicativo deve estar localizado em um dos diretórios listados nas suas Variáveis de Ambiente do Windows. Qualquer caminho inserido será ignorado.

NOTA: Para o Windows (não-correlação), é opcional inserir um caminho. Inserir um comando sem um caminho definirá como padrão %ESEC_HOME%\sentinel\bin e todos os outros caminhos especificados em suas variáveis de ambiente.

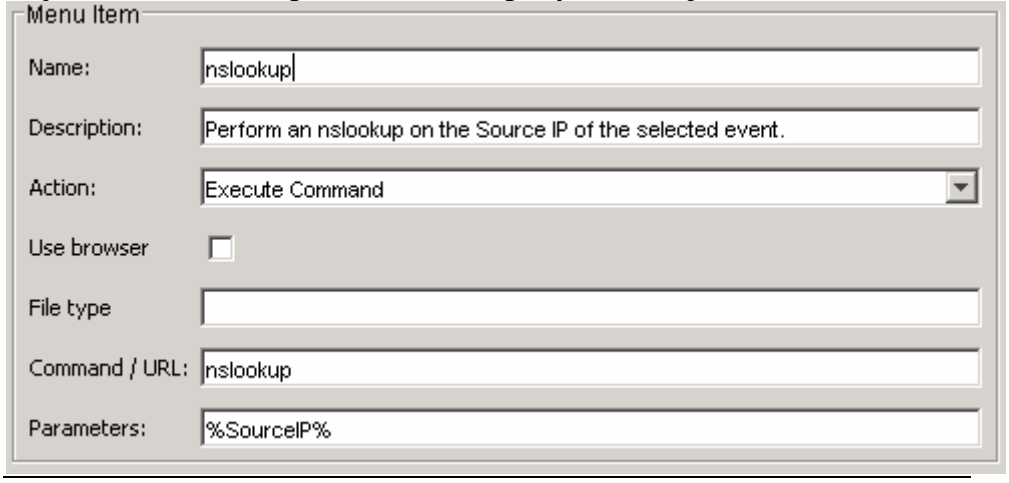
- Parâmetros – precisam vir dentro do sinal de porcentagem (por exemplo, %EventName%)

NOTA: Para obter uma lista das tags disponíveis que você pode usar ao especificar parâmetros, clique em *Ajuda* na caixa de diálogo *Configuração de Menu*, ou vá até o capítulo Metatag no *Guia de Referência do Usuário Sentinel*.

---

4. Clique em *OK*. A nova opção é adicionada à lista de itens de menu na janela Configuração do Menu.

NOTA: Para obter um exemplo, realce qualquer um dos itens de menu padrão e clique em *Detalhes*. A seguir está uma configuração nslookup:



Clonando uma opção de menu Configuração de Menu

Para clonar uma opção de menu Configuração do Menu

1. Abra a janela Configuração de Menu.
2. Selecione um item do menu da tabela e clique em *Clonar*.
3. Na caixa de diálogo Configuração de Menu, edite o seguinte:
   - Nome
   - Descrição
   - Ação
   - Para usar um browser ou não. Para obter informações, consulte Adicionar um recurso de browser à sua opção de Configuração do Menu.
   - Linha de comando/URL
   - Parâmetros
   - Selecione uma ação:
     - Executar comando
     - Iniciar browser da Web.

   NOTA: Para obter uma lista das tags disponíveis que você pode usar ao especificar parâmetros, clique em *Ajuda* na caixa de diálogo Configuração de Menu, ou vá até o capítulo Metatag no *Guia de Referência do Usuário Sentinel.*
4. Clique em *OK*. A nova opção é adicionada à lista de itens de menu na janela Configuração do Menu.

Modificando uma opção de menu Configuração de Menu

Para modificar uma opção de menu de Configuração de Menu

1. Abra a janela Configuração de Menu.
2. Clique duas vezes em uma opção do menu.
3. Digite suas mudanças desejadas e clique em *OK*.

Visualizando os parâmetros da opção Configuração de Menu

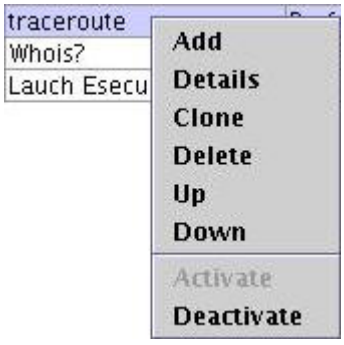
Para visualizar os parâmetros para uma opção de menu Configuração de Menu

1. Abra a janela Configuração de Menu.
2. Realce um item do menu e clique em *Detalhes*.

Ativando ou desativando uma opção de menu Configuração de Menu

Para ativar ou desativar uma opção de menu Configuração de Menu

1. Abra a janela Configuração de Menu.
2. Selecione uma opção de menu, clique o botão direito do mouse e selecione *Ativar* ou *Desativar*.



Reorganizando as opções do menu de evento

Para mover uma opção de menu Evento para cima ou para baixo

1. Abra a janela Configuração de Menu.
2. Selecione uma opção de menu e clique em *Para cima* ou *Para baixo.*

Apagando uma opção do menu Configuração do Menu

Para apagar uma opção de menu Configuração de Menu

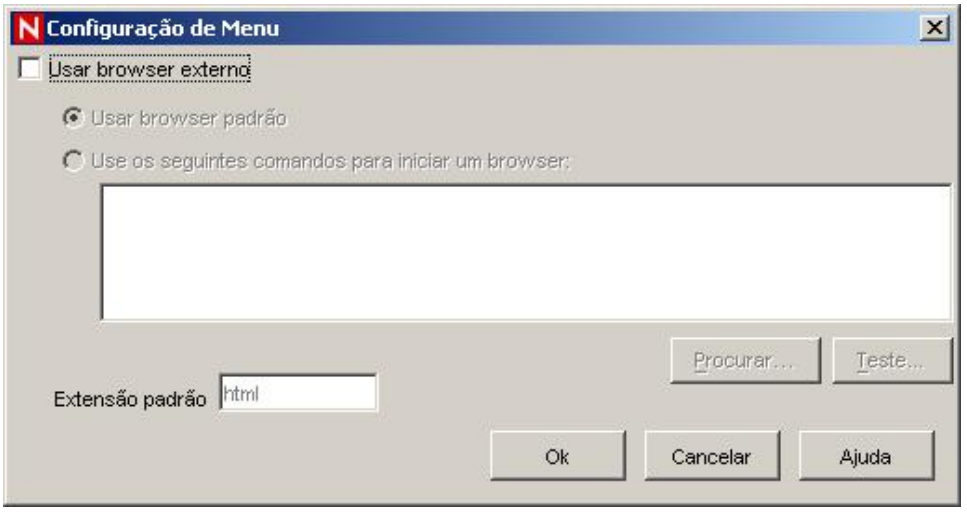
1. Abra a janela Configuração do Menu.
2. Selecione uma opção de menu e clique em *Apagar*.
   - Clique em *Sim* para apagar a opção de menu
   - Clique em *Não* para manter a opção de menu

Editando as configurações de browser Configuração do Menu

Essa opção permite que você envie sua saída de Opção de Configuração do Menu para um browser externo. O browser externo pode ser qualquer aplicativo. Não há restrição para browser de Internet. Ao mudar a extensão do arquivo, você pode iniciar qualquer aplicativo que esteja associado com aquela extensão. Por exemplo, o formato txt está geralmente associado com o Bloco de notas. Você também pode escolher iniciar um programa específico, por exemplo, fazer com que um arquivo txt seja aberto pelo Wordpad ou outro editor.

Editando as configurações do seu browser de Configuração de Menu

1. Abra a janela Configuração do Menu.
2. Clique em *Browser*.



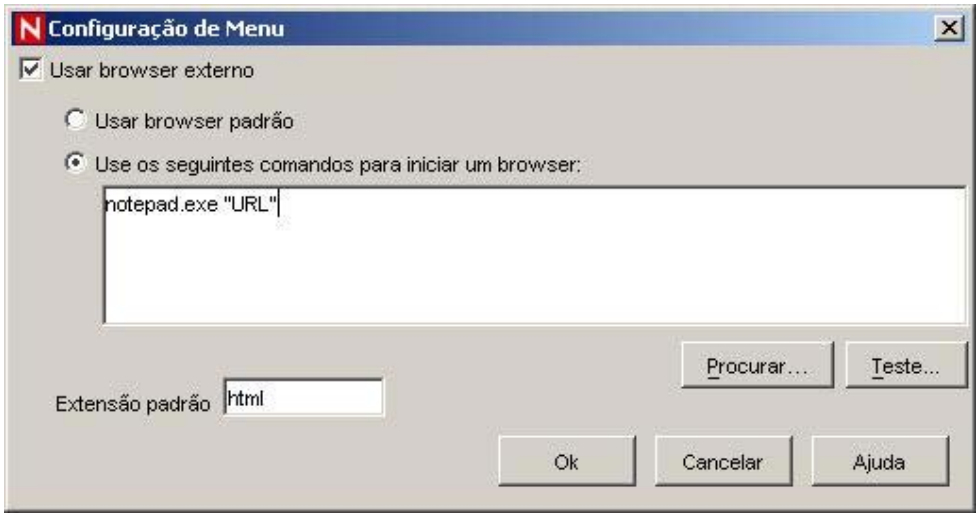
Se você selecionar "Usar browser" ao configurar uma opção de Configuração do Menu com o Recurso de browser definido como configuração-padrão (como apresentado), a Opção de Configuração do Menu reagirá como se a caixa "Usar browser" não estivesse marcada.

Se marcar a caixa "Usar browser externo", você tem a opção de fazer uma das seguintes opções:

- "Usar browser padrão" – usa o browser padrão (aplicativo) que está associado com a extensão de arquivo definida no campo Extensão de arquivo.
- "Use os seguintes comandos para iniciar um browser:" – permite especificar um aplicativo específico a ser iniciado. Ao usar um navegador diferente do browser padrão, sua linha de comando deve ser seguida por um %URL%. Por exemplo:

```
C:\Arquivos de Programas\Internet
   Explorer\IEXPLORE.EXE %URL%
```

A seguir há um exemplo em que a saída da Opção do menu abrirá no Bloco de notas.



3. Depois de ajustar sua configuração, clique em *OK*.

Estatísticas DAS

Esse recurso é para monitoramento interno do seu sistema. Sua intenção não é o usuário médio. As Estatísticas DAS monitora o seguinte:

- DAS_Binary
- DAS_Query
- DAS_rt

As estatísticas são divididas da seguinte forma:

- Serviço – nome do serviço como DAS_Query
- Hora – Hora desde a última atualização
- num – número de solicitações processadas para esta entrada
- Tempo de espera – tempo de espera médio em segundos para uma solicitação antes de o processamento iniciar
- Tempo de execução – tempo médio para processar uma solicitação (em segundos)
- #wait – Tamanho médio da fila de espera
- #run – Tamanho médio da fila de execução

As informações são divididas em três seções:

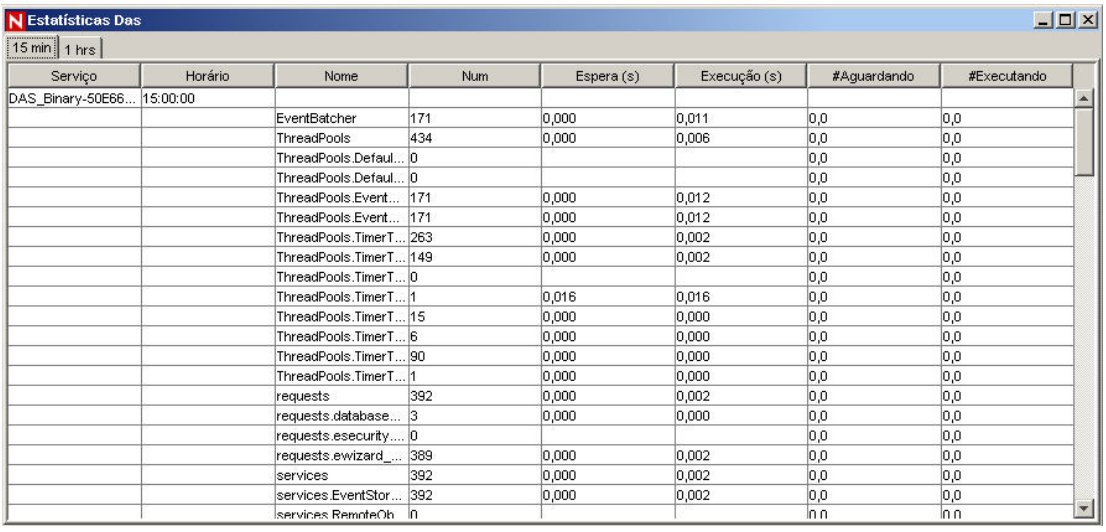
- Solicitações
- Serviços
- ThreadPools

Em Solicitações, mantém todas as solicitações por canal (tais como services.CorrelationService). Em serviços, faz o mesmo por serviço. Às vezes, fornece uma decomposição acrescentando "<category>" no nome, como Services.CorrelationService ou Services.RemoteObjectService.EMap.getMapPK.

Em Serviços, todas as chamadas de método remoto dos serviços definidos pelo usuário (seus serviços XML) estão em services.RemoteObjectService. Além disso, coloca o nome do serviço (EMap) no exemplo acima e, se solicitado, o nome do método (getMapPK acima).

Quando uma solicitação é recebida por um servidor, como DAS Query, é criada e agendada uma tarefa. A tarefa é então atribuída a um pool de thread para execução. Pode haver mais de um pool de thread, e um pool de thread pode atender a múltiplos serviços. Por essa razão, a solicitação pode ter que esperar um thread disponível mesmo que o serviço não esteja sendo muito usado. Caso as estatísticas indiquem que o tempo de espera para uma solicitação seja grande, e o número de solicitações para este serviço seja baixo, verifique as informações sobre os pools de thread.

Os números próximos a uma entrada são a soma de todos os seus derivados. Assim, 15 indica que há 15 solicitações para todas as chamadas de método de solicitação. Neste ponto, requests.configurations 1 indica que 1 das 15 é para configuração, requests.esecurity.correlation.config 2 indica que 2 das 15 são para esecurity.correlation.config e assim por diante.



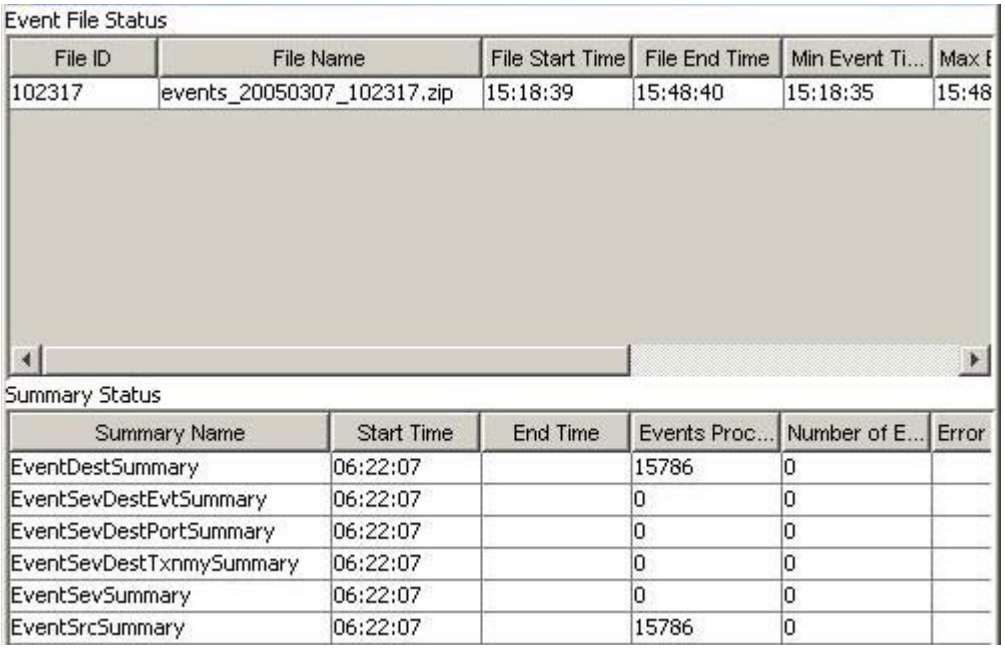
Serviço	Horário	Nome	Num	Espera (s)	Execução (s)	#Aguardando	#Executando
DAS_Binary-50E66...	15:00:00						
		EventBatcher	171	0,000	0,011	0,0	0,0
		ThreadPools	434	0,000	0,006	0,0	0,0
		ThreadPools.Defaul...	0			0,0	0,0
		ThreadPools.Defaul...	0			0,0	0,0
		ThreadPools.Event...	171	0,000	0,012	0,0	0,0
		ThreadPools.Event...	171	0,000	0,012	0,0	0,0
		ThreadPools.TimerT...	263	0,000	0,002	0,0	0,0
		ThreadPools.TimerT...	149	0,000	0,002	0,0	0,0
		ThreadPools.TimerT...	0			0,0	0,0
		ThreadPools.TimerT...	1	0,016	0,016	0,0	0,0
		ThreadPools.TimerT...	15	0,000	0,000	0,0	0,0
		ThreadPools.TimerT...	6	0,000	0,000	0,0	0,0
		ThreadPools.TimerT...	90	0,000	0,000	0,0	0,0
		ThreadPools.TimerT...	1	0,000	0,000	0,0	0,0
		requests	392	0,000	0,002	0,0	0,0
		requests.database...	3	0,000	0,000	0,0	0,0
		requests.esecurity....	0			0,0	0,0
		requests.ewizard_...	389	0,000	0,002	0,0	0,0
		services	392	0,000	0,002	0,0	0,0
		services.EventStor...	392	0,000	0,002	0,0	0,0
		services.RemoteOb...	0			0,0	0,0

As informações podem ser úteis pois mostram o que está havendo. O número de solicitações é especialmente útil; você pode ver onde elas estão indo ou estão concentradas. O #waiting é útil pois mostra o quão ocupado está o servidor. Esse número deve ser pequeno. Se for grande, as novas solicitações (mesmo para tarefas simples) terão que esperar as potencialmente lentas. Esta não é uma boa situação. O tempo médio de execução é muito importante pois mostra quais solicitações estão na verdade tomando todo o tempo, sem esperar pelas outras.

Informação do arquivo de eventos

O painel superior mostra as informações de Status para cada arquivo de evento. O status é dos arquivos de evento quando a janela estava aberta. O painel não mostrará o status de qualquer status passado de arquivo de evento. Fornece file_id (que é o arch_id na tabela de eventos), nome de arquivo e estatísticas do arquivo (caso esteja completo, o tempo de início e fim de gravar em um arquivo, o tempo mínimo e máximo de eventos contidos no arquivo, etc).

Ao realçar um arquivo do painel superior, o painel inferior mostrará o status de resumo para aquele arquivo de evento. O painel inferior mostra o nome do resumo, o tempo inicial e final de processamento, o número de eventos processados e se havia alguma mensagem de erro.



Event File Status

File ID	File Name	File Start Time	File End Time	Min Event Ti...	Max E
102317	events_20050307_102317.zip	15:18:39	15:48:40	15:18:35	15:48

Summary Status

Summary Name	Start Time	End Time	Events Proc...	Number of E...	Error
EventDestSummary	06:22:07		15786	0	
EventSevDestEvtSummary	06:22:07		0	0	
EventSevDestPortSummary	06:22:07		0	0	
EventSevDestTxnmySummary	06:22:07		0	0	
EventSevSummary	06:22:07		0	0	
EventSrcSummary	06:22:07		15786	0	

Configurações do usuário

Para usar este recurso, você deve ter a Configuração de Usuário com permissão para funcionar na janela de Configuração de usuário.

A Configuração de usuário permite fazer o seguinte:

- Criar uma conta de usuário
- Modificar uma conta de usuário
- Visualizar detalhes de uma conta de usuário
- Clonar uma conta de usuário
- Apagar uma conta de usuário
- Encerrando uma sessão ativa
- Adicionar uma função iTRAC
- Apagar uma função iTRAC
- Detalhes de uma função iTRAC

O instalador criará os seguintes usuários-padrão no Sentinel Server:

Autenticação Oracle e MS SQL: usuários:padrão *Consulte* usuário padrão

- esecdba – Proprietário de esquema (configurável no momento da instalação).
- esecadm – Usuário administrador do Sentinel (configurável no momento da instalação).

NOTA: Para UNIX, o Instalador também cria o usuário do sistema operacional com o mesmo nome de usuário e senha.

- esecrpt – Usuário relator, senha como usuário admin.
- ESEC_CORR – Usuários do Mecanismo de Correlação, usado para criar incidentes.
- esecapp – Nome de usuário do aplicativo Sentinel para conexão com o banco de dados.

Autenticação do Windows:

- Administrador de BD do Sentinel – Proprietário do esquema (configurável no momento de instalação).
- Administrador do Sentinel – Usuário administrador do Sentinel (configurável no momento da instalação).
- Usuário do relatório do Sentinel – Usuário relator, senha como usuário administrador.
- Usuário de BD do aplicativo Sentinel – Nome de usuário do aplicativo Sentinel para conexão com o banco de dados.

Abrindo a janela do Gerenciador de usuário.

Para abrir a janela do Gerenciador do Usuário

1. Clique na guia *Admin*.
2. Clique em *Admin* > *Configuração do usuário*.

Criando uma conta de usuário

NOTA: Para obedecer às rígidas configurações de segurança exigidas pela Certificação de Critérios Comuns, o Sentinel exige uma senha forte com as seguintes características:

1. Escolha senhas com no mínimo 8 caracteres, que incluam ao menos um dígito em MAIÚSCULA, um em minúscula, um símbolo especial (!@#$%^&*()_+), e um dígito numérico (0-9).

2. A senha não pode conter o nome usado no e-mail nem partes do nome completo.

3. A senha não deve ser uma palavra “comum” (por exemplo, não deve ser uma palavra registrada em dicionário nem gíria de uso comum).

4. A senha não deve conter palavras de idioma algum, pois existem vários programas de invasão de senha capazes de verificar milhões de possibilidades de combinações de palavras em segundos.

5. Escolha uma senha de que possa se lembrar, mas que seja complexa. Por exemplo, Mft5#AIdade (meu filho tem 5 anos de idade) OU EmnCh5#a (eu moro na Califórnia há 5 anos).

Para usar este recurso, você deve ter a permissão do usuário para Criar conta de usuário. As permissões de usuário são amplamente detalhadas; consulte o *Manual de referência do Usuário Sentinel*, *Permissões de usuário* para obter informações.

NOTA: A senha do usuário esecrpt deve ser trocada diretamente no banco de dados. O Enterprise Manager pode ser usado para se fazer isso.

Para criar uma conta de usuário

1. Abra a janela do Gerenciador de usuário.
2. Clique no botão *Adicionar novo Usuário*,

ou realce qualquer usuário e clique o botão direito do mouse em > *Adicionar Usuário*.

3. Em Autorização, insira:
   - Nome do usuário
   - Senha
   - Confirmar senha
   - Filtro de segurança – Para selecionar um filtro, clique na seta para baixo. Abre a janela de Seleção de filtro. Realce um filtro ou clique em *Adicionar* para criar um filtro para esta conta de usuário.

   NOTA: Depois de atribuir um filtro de segurança para um usuário, você não pode apagar esse filtro.

   - Clique em *Selecionar*.

   NOTA: Como melhor prática, é altamente recomendável uma extensão mínima de senha de oito caracteres que incluam alfanuméricos.

   (Opcional) Em Detalhes, insira:
   - Nome
   - Sobrenome
   - Departamento
   - Telefone
   - E-mail
4. Clique na guia *Permissões* e atribua permissões de usuário.
5. Clique na guia *Funções* e selecione a função para o usuário.
6. Clique em *OK*.

   NOTA: a Oracle não permite a criação de usuários que tenham o mesmo nome das palavras reservadas da Oracle. Além disso, o Sentinel não permite que você use esses nomes.

Modificando uma conta de usuário

Para usar este recurso, você deve ter a permissão do usuário para Modificar uma conta de usuário atual.

NOTA: A senha do usuário esecrpt deve ser trocada diretamente no banco de dados. O Enterprise Manager pode ser usado para se fazer isso.

Para modificar uma conta de usuário

1. Abra a janela do Gerenciador de usuário.
2. Clique duas vezes em uma conta de usuário ou clique o botão direito do mouse em > *Detalhes do usuário*.
3. Modifique a conta.
4. Clique em *OK*.

Visualizando detalhes de uma conta de usuário

Para usar este recurso, você deve ter a permissão do usuário para Usar/visualizar a conta de usuário.

Para visualizar os detalhes da conta de usuário

1. Abra a janela do Gerenciador de usuário.
2. Clique duas vezes em uma conta de usuário ou clique o botão direito do mouse em > *Detalhes do usuário*.
3. Reveja os detalhes da conta do usuário e feche a janela.

Clonando uma conta de usuário

Para clonar uma conta de usuário

1. Abra a janela do Gerenciador de usuário.
2. Selecione um ID de conta de usuário e clique o botão direito do mouse em > *Clonar Usuário.*
3. Mude as informações e as permissões do usuário.
4. Clique em *Gravar*.

Apagando uma conta de usuário

Para usar este recurso, você deve ter a permissão do usuário para Apagar a conta de usuário.

NOTA: Quando um usuário é apagado, ele não pode ser criado novamente. Por exemplo, se você criar um usuário chamado João e depois apagar o João, você não vai pode recriar um usuário chamado João.

Para apagar uma conta de usuário

1. Abra a janela do Gerenciador de usuário.
2. Selecione um ID de conta do usuário e clique o botão direito do mouse em > *Apagar Usuário*.

Encerrando uma sessão ativa

Terminando uma sessão ativa

1. Abra a janela de Sessões de usuário ativo.
2. Realce uma sessão ativa que você deseja encerrar.
3. Clique o botão direito do mouse em > *Eliminar Sessão*.
4. Você receberá uma mensagem de encerramento. Feito isso, você pode informar o usuário por que você está eliminando a sessão.

Adicionando uma função iTRAC

Para adicionar uma função iTRAC

1. Abra a janela do Gerenciador de funções.
2. Clique em *Adicionar uma nova Função*,

ou clique o botão direito do mouse em > *Adicionar Nova Funçã*o.

Apagando uma função iTRAC

Para apagar uma função iTRAC

1. Abra a janela do Gerenciador de funções.
2. Selecione uma função e clique o botão direito do mouse em > *Apagar Função*.

Visualizando detalhes de uma função

Para visualizar detalhes da função

1. Abra a janela do Gerenciador de funções.
2. Selecione uma função e clique o botão direito do mouse em > *Detalhes da Função*.

10 Gerenciador de Dados do Sentinel

NOTA: O termo Agente é intercambiável com Coletor. Mais para a frente, Agentes será referido como Coletores.

SDM Consulte o Gerenciador de Dados do Sentinel. O Gerenciador de Dados do Sentinel (SDM) é uma ferramenta com a qual os usuários podem gerenciar o banco de dados do Sentinel. O SDM permite que os usuários realizem as seguintes operações:

- Monitorar a utilização do espaço do banco de dados
- Ver e gerenciar as partições do banco de dados
- Gerenciar arquivos do banco de dados
- Importar dados para o banco de dados
- Configurar o mapeamento de dados
- Configurar nomes de tags de eventos
- Configurar definições de relatórios de resumo

Instalando o SDM

O SDM pode ser instalado diretamente através do Assistente do Sentinel 5 InstallShield selecionando o componente *Gerenciador de Dados do Sentinel* na tela Seleção de recurso do Sentinel 5.

(Apenas Oracle) Observe que, para o SDM se comunicar com os bancos de dados do Oracle, você também deve efetuar o download manual do driver Oracle 9.2.0.4 ou 9.2.0.5 JDBC e copiar o arquivo .jar baixado para o diretório $ESEC_HOME/lib, no mesmo lugar em que você instalou o SDM, ou em %ESEC_HOME%\lib, caso se esteja instalado o SDM no Windows. Você pode fazer o download do driver JDBC do seguinte URL:

NOTA: Se uma máquina UNIX com o componente DAS for instalada, o driver JDBC é automaticamente colocado no local correto pelo instalador. Portanto, nesse caso, nenhum download manual é necessário.

http://otn.oracle.com/software/tech/java/sqlj_jdbc/index.html

O nome típico deste arquivo .jar é ojdbc14.jar.

NOTA: na data de publicação deste guia, o site mencionado estava correto.

NOTA: O SDM para Oracle necessita que seja instalado o Oracle Enterprise com particionamento.

Iniciando a interface do usuário do SDM

NOTA: Para usar a interface do usuário do SDM, seu arquivo configuration.xml deve estar apontando para um Servidor de Comunicação que também tem o DAS_Binary e o DAS_Query conectados a ele. Em geral, acontecerá isso por padrão, desde que o Servidor de Comunicação e os processos DAS estejam em execução.

No UNIX: iniciando SDM GUI

1. Efetue login na caixa UNIX como membro do grupo esec (por exemplo: esecadm).
2. vá até $ESEC_HOME/sdm
3. Digite a seguinte linha de comando:

```
./sdm
```

No Windows: iniciando SDM GUI

1. Clique em *Iniciar* > *Arquivos de Programas* > *Sentinel* > *Gerenciador de Dados do Sentinel*.

NOTA: Para executar o SDM da linha de comando, consulte a seção Linha de Comando do SDM deste documento.

Conectando-se ao banco de dados

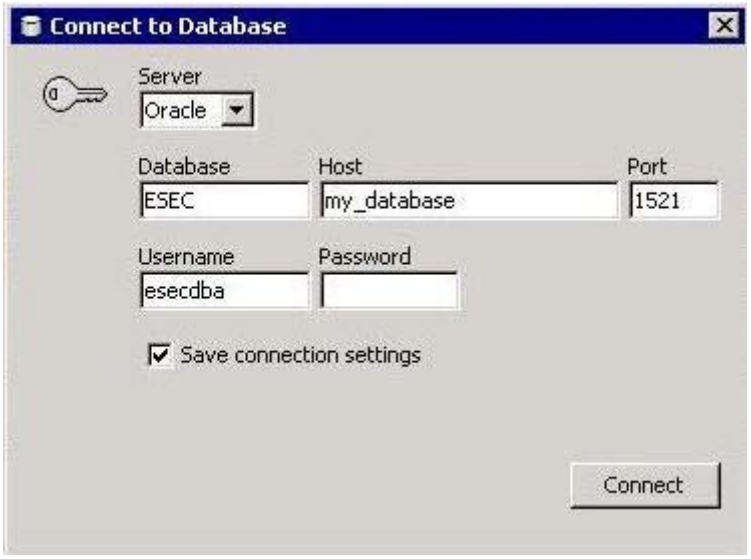
Quando o SDM for iniciado, você vai precisar estabelecer uma conexão com o seu banco de dados. Na caixa de diálogo *Conectar ao banco de dados*, insira os valores apropriados para cada campo.

Conectando ao banco de dados

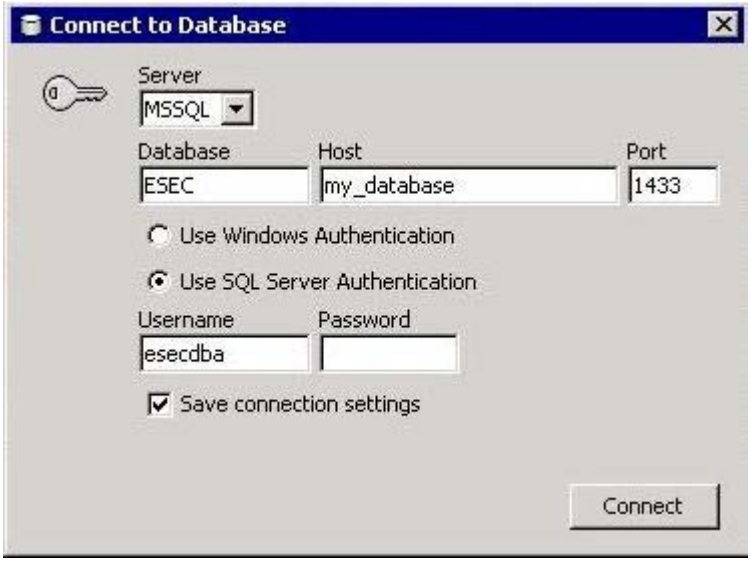
1. Inicie a interface de usuário do SDM.
2. Selecione o tipo do seu banco de dados, como Oracle ou MSSQL.
3. Especifique o nome de instância do banco de dados (por exemplo, ESEC).
4. Especifique o host do banco de dados (use o nome de host ou o endereço IP).
5. Para a porta, use a porta-padrão 1521 para o Oracle ou a porta-padrão 1433 para o MSSQL.
6. Para o nome de usuário e a senha, use o nome de usuário e a senha do Administrador do Banco de Dados do Sentinel (por exemplo, esecdba).

NOTA: Para o Windows e o MS SQL, se instalou o MS SQL no modo misto, você poderá efetuar login usando a Autenticação do Windows OU a Autenticação de Servidor SQL. se você instalou o MS SQL apenas no modo de Autenticação do Windows do misto, você pode efetuar login usando a Autenticação do Windows. Se preferir usar a Autenticação do Windows, você será autenticado com o banco de dados do MS SQL como o usuário com o qual você está atualmente conectado no Windows (ou seja, login único).

Para Oracle:



No Windows:



NOTA: se selecionar gravar suas configurações de conexão, elas serão gravadas no arquivo local sdm.connect. Na próxima vez em que você iniciar a interface do usuário, as configurações de conexão serão preenchidas novamente com base no arquivo sdm.connect. Pode-se usar este arquivo ao executar o SDM da linha de comando.

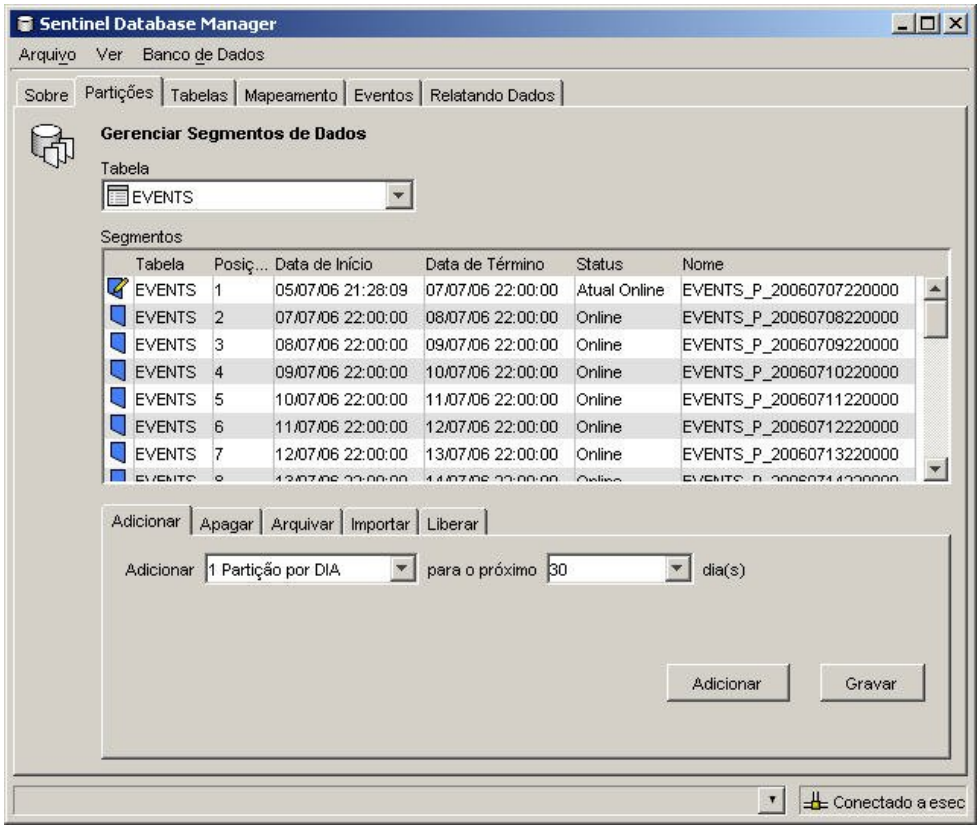
7. Clique em *Conectar*.

Partições

A guia Partições no SDM permite que os usuários visualizem e gerenciem as partições do banco de dados.

Para ver as partições na interface de usuário

1. Clique na guia *Partições*.
2. Selecione a tabela na lista suspensa que você gostaria de ver.



A tabela Segmentos exibe as partições da Tabela de Banco de Dados atualmente selecionada.

Cada linha na tabela Segmentos exibe a Tabela de Banco de Dados, o Intervalo de Tempo, o Status e o Nome da partição relacionados.

O Status de cada uma das partições mostradas na tabela Segmentos terá um dos seguintes estados:

Online	os dados na partição online estão disponíveis para acesso
Atual online	uma partição online na qual estão sendo atualmente inseridas as linhas
Arquivado online	partição cujos dados estão arquivados, mas os dados ainda estão acessíveis devido a uma das seguintes razões: ▪ partição ainda não eliminada ▪ a partição foi importada de volta
Offline	os dados em uma partição offline não estão disponíveis para acesso porque a partição foi eliminada e não foi importada
Arquivado offline	partição que foi arquivada e eliminada

Para gerenciar partições

1. Clique na guia *Partições*.
2. Selecione a tabela na lista suspensa.
3. Selecione a guia na parte inferior da janela que se relaciona à operação que você gostaria de realizar – Adicionar, Apagar, Arquivar, Importar ou Liberar.

Para adicionar partições

1. Selecione a guia *Adicionar* partições.
2. Especifique o número de partições a serem adicionadas e o número de dias para os quais se devem adicionar as partições.
3. Pressione *Adicionar*.

Para apagar partições

1. Selecione a guia *Apagar* partições.
2. Especifique o número de dias pelos quais as partições mais antigas serão apagadas.
3. Pressione *Apagar*.

Para arquivar partições

NOTA: As tabelas de agregação não são arquivadas.

1. Selecione a guia *Arquivar* partições.
2. Especifique o número de dias durante os quais as partições mais antigas serão arquivadas e o diretório no qual o arquivo será armazenado.

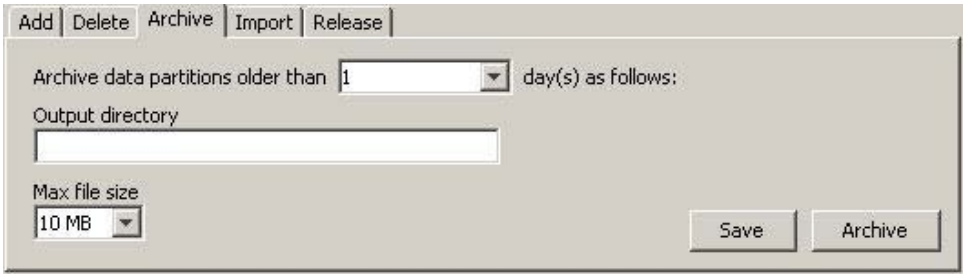
NOTA: Para UNIX, as partições não podem ser arquivadas em /root.

3. Pressione *Arquivo*.

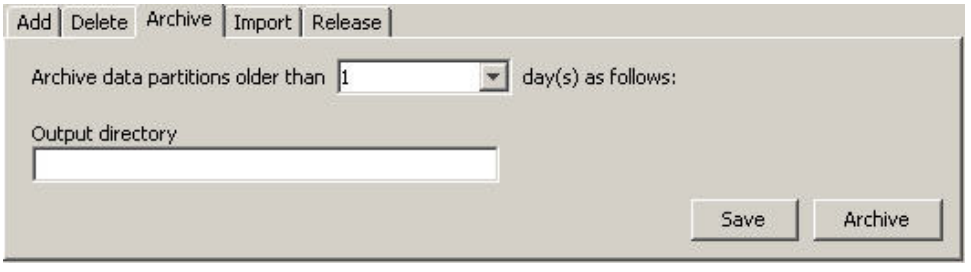
NOTA: Ao arquivar, certifique-se de inserir um caminho válido no servidor do banco de dados com as permissões corretas.

NOTA: a guia Arquivar é diferente para o MSSQL e o Oracle. No caso do Oracle, a empresa permite especificar o tamanho máximo do arquivo.

Guia Arquivar Partições do Oracle:



Guia Arquivar Partições do MSSQL:



Para importar partições

1. Selecione a guia *Importar* partições.
2. Selecione a partição na tabela Segmento para a qual os dados serão importados.
3. Especifique o diretório de entrada a partir do qual os dados arquivados serão lidos.
4. Pressione o botão *Importar*.

Para liberar as partições importadas

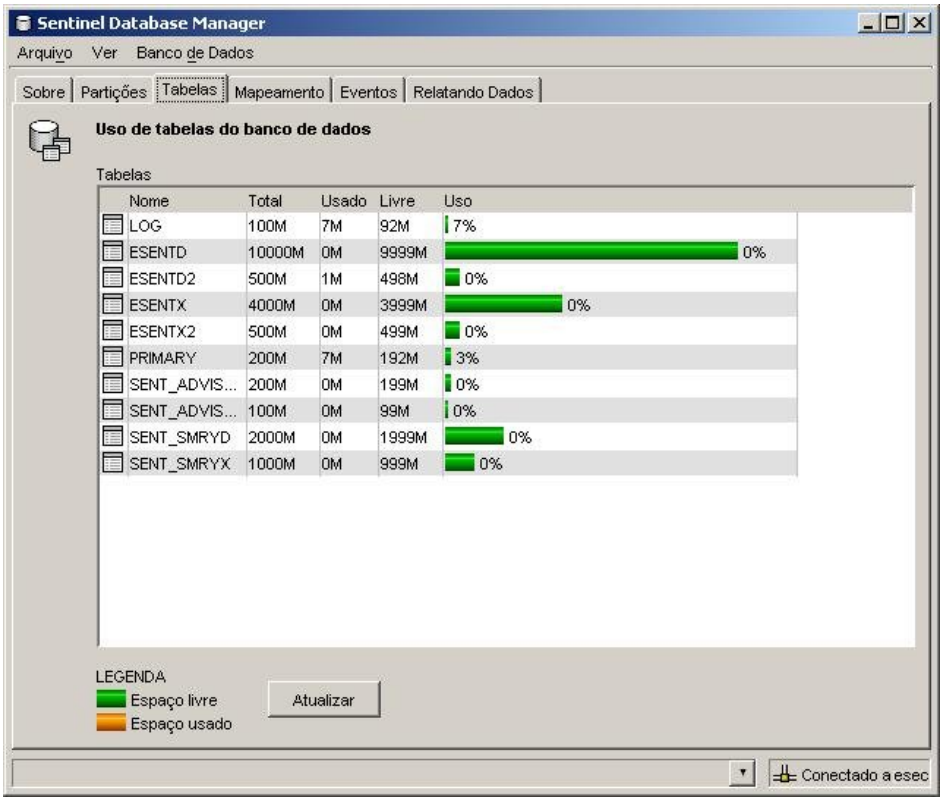
1. Selecione a guia "*Liberar*" partições.
2. Selecione a partição na tabela Segmento que será liberada.
3. Pressione *Liberar*.

Tabelas

A guia Tabelas no SDM permite que os usuários visualizem e gerenciem a utilização do espaço do banco de dados atual.

Para ver as tabelas na interface do usuário

1. Clique na guia *Tabelas*.



A tabela Utilização da Tabela exibe o espaço total alocado para cada tabela, quanta memória foi usada por cada tabela e quanta memória ainda está disponível (livre) para cada tabela. Os gráficos de barra codificados por cor ajudam a ver o espaço total alocado para cada tabela e a percentagem usada de cada tabela.

NOTA: No MS SQL, não existem tabelas, são usados grupos de arquivos.

Guia Mapeamento

NOTA: Para usar a guia Mapeamento, seu arquivo configuration.xml deve estar apontando para um Servidor de Comunicação que também tem o DAS_Binary e o DAS_Query conectados a ele. Em geral, acontecerá isso por padrão, desde que o Servidor de Comunicação e os processos DAS estejam em execução.

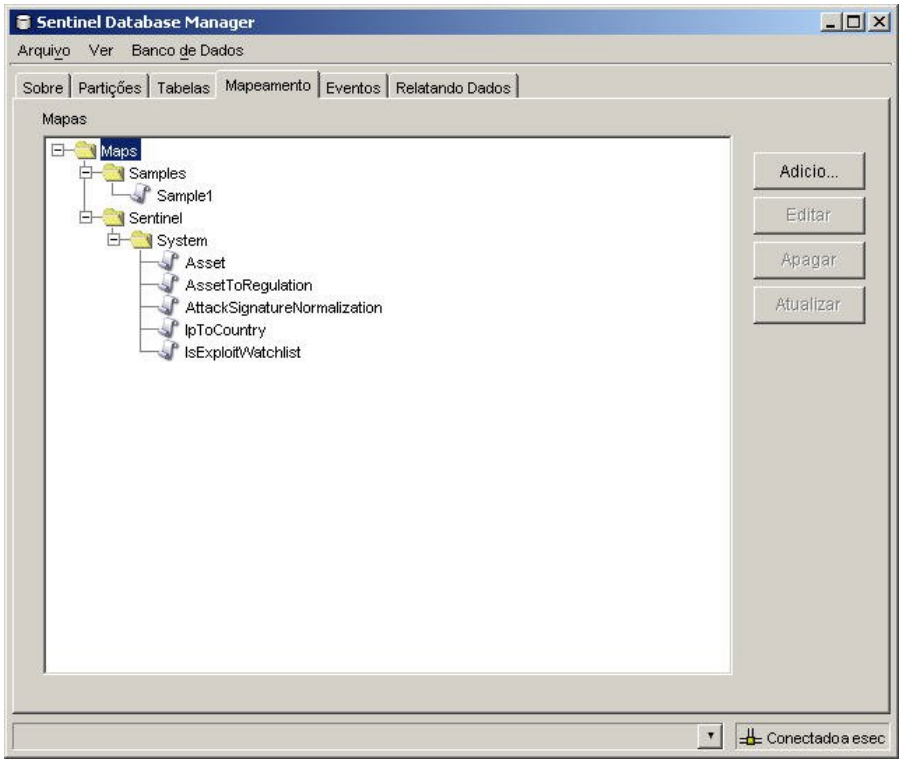
A guia Mapeamento permite:

- Adicionar novas definições de mapa
- Editar definições de mapa
- Apagar definições de mapa
- Atualizar os dados de mapa

O mapeamento funciona junto com a opção de origem de dados *Referido no mapa*, na guia Eventos. É possível mapear usando uma faixa de string ou numérica.

Para ver os mapas na interface do usuário

1. Clique na guia *Mapeamento*.



A interface do usuário principal de Mapeamento exibe uma lista de todos os mapas que foram definidos para o sistema.

NOTA: os mapas na pasta Sistema não podem ser editados ou apagados.

Adicionando definições de mapa

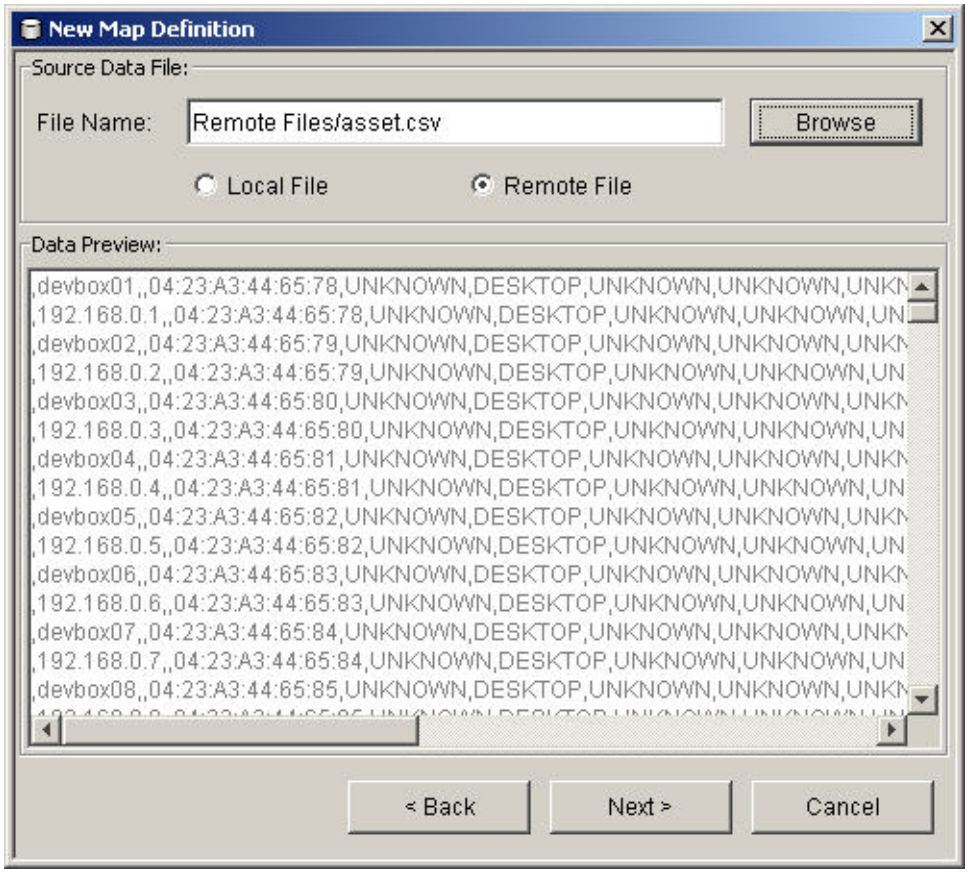
Para adicionar uma definição de mapa:

1. Clique na guia *Mapeamento*.
2. Clique em *Adicionar*.
3. Se estiver criando uma pasta de mapa, clique em *Novo*... . Insira um nome de pasta.

   NOTA: Se esta for sua primeira definição de mapa, recomenda-se que você crie uma pasta de definição de mapa. A criação de uma definição de mapa na pasta Sistema não lhe permitirá editar ou apagar sua definição de mapa.
4. Certifique-se de que a pasta em que você deseja inserir sua definição de mapa esteja selecionada. (Ou seja, a pasta indica que está aberta.)
5. Insira o nome do mapa.
6. Clique em *Avançar*.

   NOTA: A caixa de campo Tipo de mapa é desabilitada.
7. Selecione ou Arquivo local ou Arquivo remoto.
   - Arquivo local – permite procurar seu arquivo no sistema de arquivos local (na máquina do qual o SDM foi iniciado).
   - Arquivo remoto – permite escolher dentre os arquivos atuais de dados de origem de mapa no servidor em que o DAS está sendo executado. Os dois arquivos que

já podem existir no servidor (caso o Advisor esteja instalado e os dados de Vulnerabilidade tenham sido enviados) são attackNormalization.csv e exploitDetection.csv. O arquivo remoto aponta para %ESEC_HOME%\sentinel\bin\map_data (Windows) ou para $ESEC_HOME/sentinel/bin/map_data (UNIX).



Selecione o seu arquivo de definição de mapa. Clique em *Avançar*.

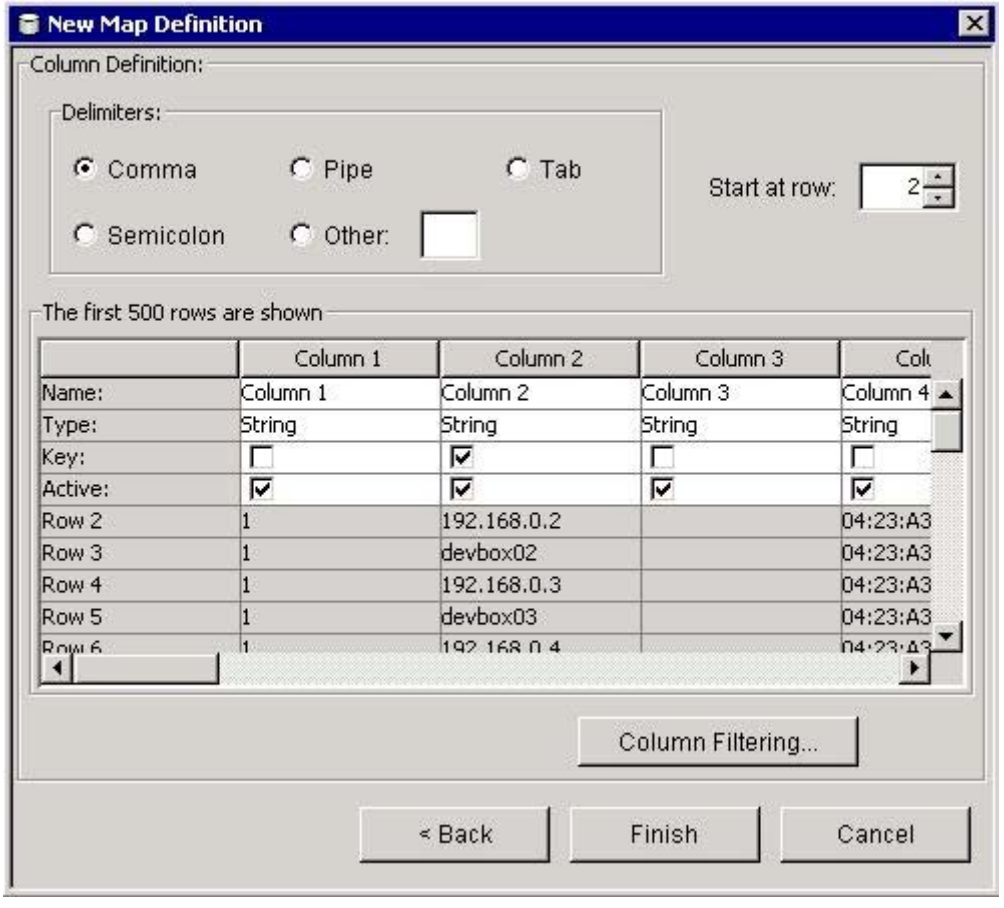
NOTA: Para os arquivos de mapa que contiverem mais de 500 linhas, você não verá todas as linhas no SDM.

8. Na janela Definição de novo mapa, configure o seguinte:
   - Delimitador (pipe, vírgula, ponto-e-vírgula, etc...) de dados nas linhas do arquivo de origem de dados do mapa
   - Iniciar na linha – o número de linhas a serem puladas a partir do início do arquivo de origem dos dados de mapa.
   - Nomes de coluna
   - Tipos de colunas – Os tipos de colunas suportados são:
     – *String* - Uma string é um grupo de caracteres usados como um único objeto por um computador. Uma string pode ser formada de uma única letra, palavra ou número. A palavra FINANÇA ou o endereço IP 192.168.2.40 poderia ser uma string. Uma string também pode ser formada por uma combinação de palavras, espaços e números. O endereço 1313 LION DOG TOWER poderia ser uma string.

- *Intervalo de Número* - um intervalo de número (NumberRange) é uma faixa de números. Por exemplo, 10 a 200 seria representado como 10-200. Para usar a funcionalidade de mapa de intervalo, a definição de mapa deve ter exatamente uma coluna de chave, e esta deve ser do tipo NumberRange. Se houver quaisquer outras colunas de chave, ou a coluna for de um tipo diferente, o serviço de mapeamento não considerará o mapa um mapa de intervalo.

- Colunas ativas – quando uma coluna é marcada como ativa, os dados na coluna serão distribuídos para os processos que usam mapas. Todas as colunas de chave devem estar ativas. Apenas as colunas que não de chave e que estão ativas podem ser selecionadas como a *Coluna de mapa* na guia Eventos.
- Colunas de chave – Uma chave é um identificador exclusivo para a linha de dados no mapa. Se mais de uma coluna for selecionada como chave, a chave geral do mapa incluirá todas as colunas selecionadas como chaves.
- Filtragem de coluna – Uma linha pode ser explicitamente incluída ou excluída com base nos critérios de correspondência para uma coluna em particular. Pode-se usar isso para apagar as linhas dos dados de origem de mapa que não são necessários, ou vão acabar interferindo no seu mapeamento.

À medida que você configurar cada ajuste e cada filtro, a tabela de dados será automaticamente atualizada para lhe permitir visualizar os dados e garantir que estejam sendo analisados da forma esperada.



9. Depois de concluir a configuração de todos os parâmetros e filtros para a definição, clique em *Concluir*.
10. Se você escolher Arquivo local na etapa 7 descrita, o sistema lhe pedirá para enviar seu arquivo para a pasta virtual Arquivos remotos localizada em %ESEC_HOME%\sentinel\bin\map_data. Insira um nome de arquivo e clique em *OK*.

Adicionando uma definição de mapa de Intervalo de Número

para usar a funcionalidade de mapa de intervalo, a definição de mapa deve ter exatamente uma coluna de chave, e esta deve ser do tipo NumberRange. Se houver quaisquer outras colunas de chave, ou a coluna for de um tipo diferente, o serviço de mapeamento não considerará o mapa um mapa de intervalo.

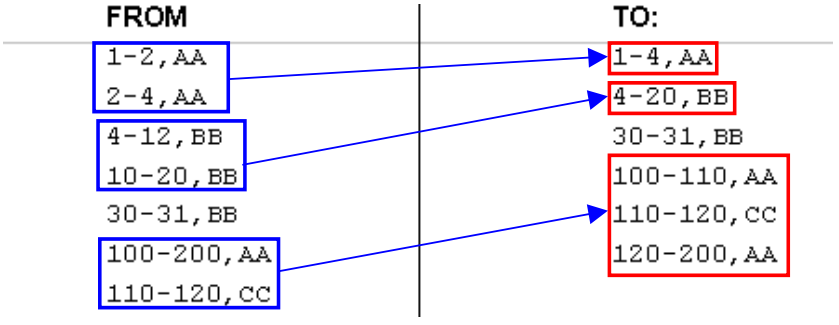
Para criar um mapa de intervalo, selecione uma única coluna para ser a chave do mapa e depois *NumberRange* como tipo da coluna. O formato dos dados em uma coluna do tipo *NumberRange* deve ser "m-n" (onde m é o número mínimo no intervalo, e n é o número máximo no intervalo (ou seja, 10-200). O número máximo no intervalo não está incluído no intervalo (ou seja, [m,n]). Isso significa que um intervalo de 10-200 somente encontrará números iguais a 10 até 199. Um conjunto de exemplo de dados é com a primeira coluna como chave:

```
1-2,AA
2-4,AA
4-12,BB
10-20,BB
30-31,BB
100-200,AA
110-120,CC
```

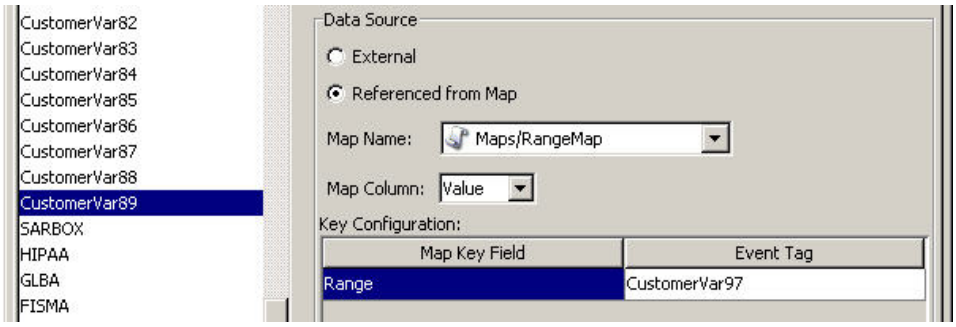
The first 500 rows are shown

	Column 1	Column 2
Name:	Range	Value
Type:	NumberRange	String
Key:	☑	☐
Active:	☑	☑
Row 0	1-4	AA
Row 1	4-20	BB
Row 2	30-31	BB
Row 3	100-110	AA
Row 4	110-120	CC
Row 5	120-200	AA

Observe como a tabela de exemplo se transforma.



Um exemplo de configuração de evento no mapa acima talvez se pareça com o seguinte:



Onde se espera que CustomerVar97 contenha um valor numérico (ou seja de um tipo que possa ser convertido em um valor numérico, como IP ou Data).

Ao realizar pesquisas no mapa de intervalo de exemplo, o valor em CustomerVar97 pegará o mapa de intervalo e pesquisará o intervalo ao qual o valor pertence (se houver). Eis alguns exemplos e seus resultados:

```
CustomerVar97 = 1; CustomerVar89 will be set to AA
CustomerVar97 = 4; CustomerVar89 will be set to BB
CustomerVar97 = 300; CustomerVar89 will not be set
```

Internamente, o Sentinel converte os endereços IP e as datas em um inteiro para tags do tipo IPv4 e Data.

As tags Ipv4 são as seguintes:

- DestinationIP (dip)
- SourceIP (sip)

As tags de data são as seguintes:

- CustomerVar11 a CustomerVar20 (cv11 a cv20)
- DateTime (dt)
- ReservedVar11 a ReservedVar20 (rv11 a rv20)

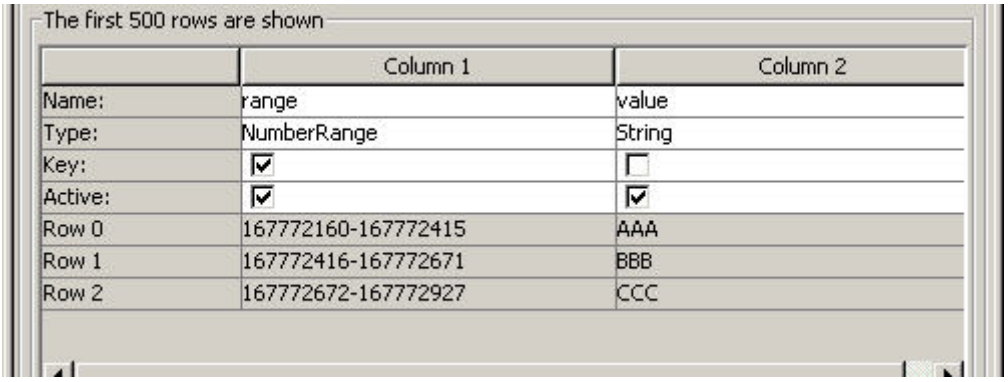
Para obter mais informações sobre as metatags, consulte o Guia de Referência do Sentinel, Capítulo 5 – Metatags do Assistente e Sentinel.

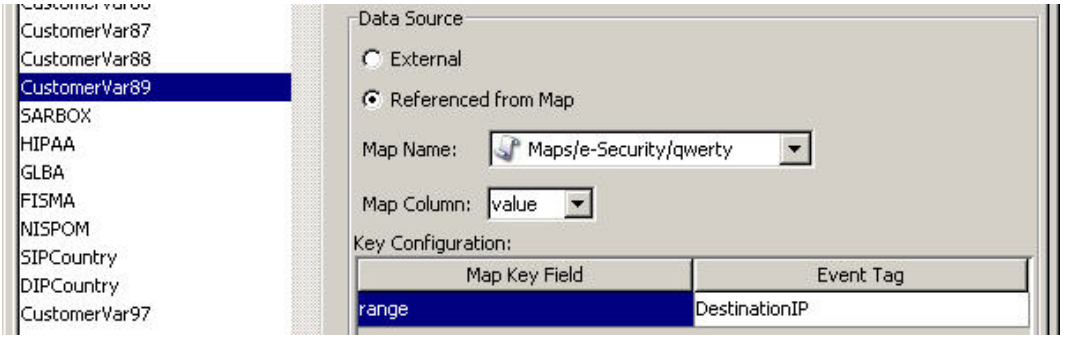
Por exemplo, na tabela a seguir, a coluna 1 é o intervalo numérico equivalente a um intervalo de IP de 10.0.0.0 a 10.0.2.255.

```
167772160-167772415,AAA
167772416-167772671,BBB
167772672-167772927,CCC
```

Usando a mesma configuração que o exemplo anterior, se:

- a Tag de Evento é configurada como DestinationIP e a coluna de chave, configurada como coluna 1 (intervalo).
- Coluna de Mapa como coluna 2 (valor 2). Os valores de saída para CustomerVar89.





Caso um evento contenha um IP de destino de 10.0.1.14 (equivalente ao valor numérico de 167772430), a saída para a coluna CustomerVar89 no evento seria BBB.

O Sentinel suporta os seguintes intervalos de número:

- Intervalo de número negativo a número negativo (por exemplo, "-234--34")
- Intervalo de número negativo a número positivo (por exemplo, "-234-34")
- Intervalo de número positivo a número positivo (por exemplo, "234-236")
- Intervalo de número único (negativo) (por exemplo, "-234") Nesse caso, o mín e o máx serão -234.
- Intervalo de número único (positivo) (por exemplo, "234") Nesse caso, o mín e o máx serão 234.
- Intervalo de número negativo a número máx (por exemplo, "-234-") Nesse caso, o mín será -234 e o máx será (2^63 - 1)
- Intervalo de número positivo a número máx (por exemplo, "234-") Nesse caso, o mín será 234 e o máx será (2^63 - 1)

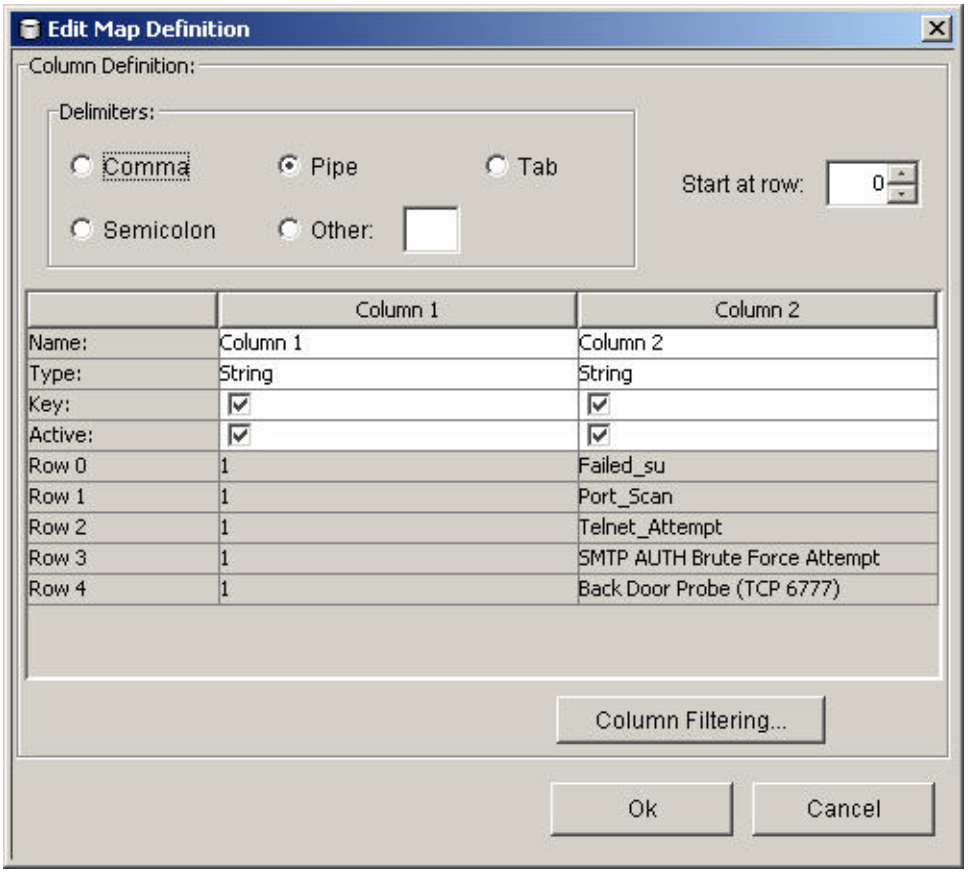
NOTA: Em todos os casos, o mín deve ser menor ou igual ao máx (por exemplo, "-234--235" NÃO é válido).

Editando as definições de mapa

Para editar uma definição de mapa:

1. Clique na guia *Mapeamento*.
2. Expanda a pasta desejada.
3. Realce uma definição de mapa e clique em *Editar*.

NOTA: A função de edição é desativada para as definições de mapa que se encontram na pasta Sistemas.



A função Editar permite fazer o seguinte:

- definir os delimitadores
- definir em qual linha iniciar seu mapa
- renomear as colunas
- ativar ou desativar uma coluna
- definir as chaves de coluna
- criar filtro de coluna

4. Depois de fazer as alterações desejadas, clique em *OK*.

Apagando as definições de mapa

Para apagar uma definição de mapa

1. Clique na guia *Mapeamento*.
2. Expanda a pasta desejada.
3. Realce a definição de mapa a ser apagada.
4. Clique em *Apagar*.

NOTA: As definições de mapa na pasta Sentinel não podem ser apagadas.

Atualizando os dados de mapa

A atualização permite substituir por outro arquivo o arquivo de dados de origem de um mapa no servidor que está executando o DAS. O novo arquivo de dados de origem do mapa deve ter o mesmo delimitador, número de colunas e estrutura geral que o arquivo atual para que o

mapa funcione adequadamente depois da atualização. A única coisa que o novo arquivo de dados de origem do mapa deve ter de diferente em relação ao arquivo atual são os valores que aparecem nas colunas. Caso o novo arquivo de dados de origem do mapa tenha uma estrutura diferente do arquivo atual, use o recurso Editar da interface do usuário do SDM para atualizar a definição do mapa.

Para atualizar dados de mapa

1. Caso você ainda não tenha feito isso, crie um arquivo contendo os novos dados de origem de mapa na máquina onde está sendo executado o SDM. Esse arquivo pode ser gerado (por exemplo, de um script de descarte de dados), criado manualmente do zero ou ser uma versão editada do arquivo atual de origem de dados do mapa.
   Se necessário, você pode obter o arquivo atual de origem de dados do mapa deste local:

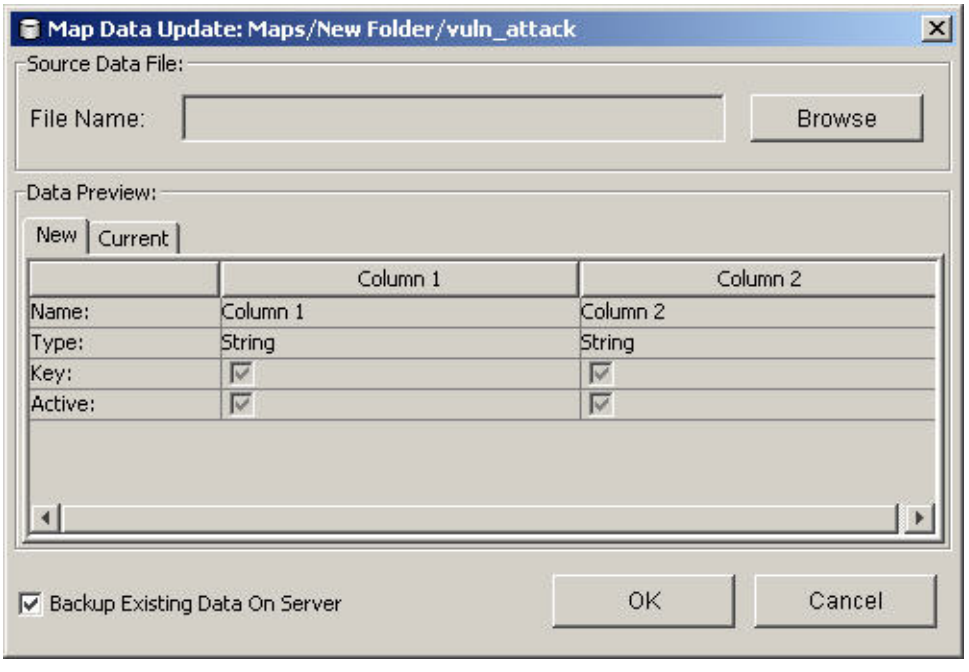
   No Windows:

   ```
   %ESEC_HOME%\sentinel\bin\map_data
   ```

   Para o UNIX

   ```
   $ESEC_HOME/sentinel/bin/map_data
   ```

2. Clique na guia *Mapeamento*.
3. Expanda a pasta desejada. Realce o mapeamento a ser atualizado. Clique em *Update* (Atualizar).



4. Selecione o novo arquivo de origem de dados do mapa clicando em *Procurar* e selecionando o arquivo com os novos dados de mapa. Depois de selecionar o arquivo, os dados do novo arquivo aparecerão na guia *Novo*. Os dados de mapa que você está substituindo estarão na guia Atual.

5. Desmarque ou deixe a configuração-padrão para *Fazer backup dos dados existentes no servidor*. A ativação dessa opção resulta no backup do arquivo atual de origem de dados do mapa que está sendo colocado na pasta %ESEC_HOME%\sentinel\bin\map_data (Windows) ou $ESEC_HOME/sentinel/bin/map_data (UNIX). O prefixo do nome do arquivo de backup da origem de dados do mapa será o nome do arquivo atual. O final do nome de arquivo conterá um conjunto de números aleatórios com o sufixo .bak. Por exemplo: ataques_vulne10197.bak.
6. Clique em *OK*.
7. Os dados do novo arquivo de origem dos dados do mapa serão atualizados no servidor, substituindo o conteúdo do arquivo atual. Depois que os dados de origem forem completamente enviados, os dados de mapa serão gerados novamente e distribuídos para os clientes de mapa (por exemplo, Gerenciador de Coletor).

Guia Eventos

NOTA: Para usar a guia Eventos, seu arquivo configuration.xml deve estar apontando para um Servidor de Comunicação que também tem o DAS_Binary e o DAS_Query conectados a ele. Em geral, acontecerá isso por padrão, desde que seu Servidor de Comunicação e os processos DAS estejam em execução.

Mapeamento de evento

O mapeamento de evento é um mecanismo que permite adicionar dados a um evento usando os dados que já estão no evento à referência e buscar os dados de uma origem externa. A origem de dados externa é um mapa, definido com a guia Mapeamento. Os dados já no evento que deve ser usado como referência no mapa e nos dados que estão sendo buscados do mapa para o evento são especificados na guia Eventos.

Como praticamente qualquer conjunto de dados pode ser transformado em mapa, o Mapeamento de Eventos é útil para incorporação nos dados de fluxo de evento de outro lugar na sua organização. Eis algumas oportunidades que o Mapeamento de Eventos fornece:

- Monitoramento da conformidade com normas
- Conformidade com políticas
- Priorização de respostas
- Habilitar a análise de dados de segurança relacionados às operações comerciais
- Aperfeiçoar a responsabilidade

Quando se define um Mapeamento de Evento, ele é aplicado a todos os eventos do sistema, de todos os Coletores. Além disso, o Sentinel distribuirá automaticamente os dados de mapa a todos os processos que realizam mapeamentos de eventos, bem como manter os dados de mapa nessa atualização de processos. Por essas razões, o Mapeamento de Eventos fornece capacidades significativas para suportar as implantações empresariais.

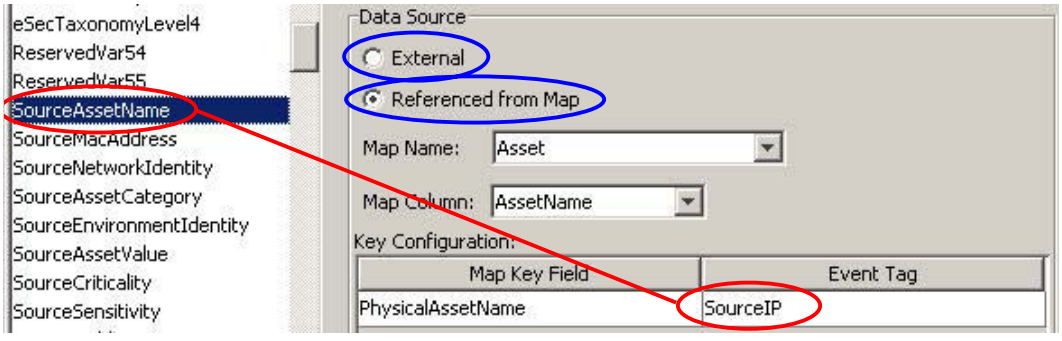
O Mapeamento de Eventos compreende quatro partes principais:

- Controlador – armazena todas as informações de mapa
- Distribuidor – redistribui automaticamente os mapas modificados a esses processos que se registraram para o mapa
- Monitor – um monitor para detectar as mudanças nos dados de origem de mapa
- Gerador – gera os mapas a partir dos dados de origem

Uma aplicação do Mapeamento de Eventos é a funcionalidade de Dados de Bens do Sentinel. Por exemplo, as informações de bens são coletadas e armazenadas no esquema de bens do Banco de Dados do Sentinel, sendo representadas por uma Entrada de Bem Físico. Os bens intangíveis, como serviços e aplicações, são representados por uma entrada que é vinculada ao Bem Físico. O mecanismo principal de atualização automatizada para dados de bens se dá através de dados de leitura do Coletor de bens de um scanner como o Nmap. O Coletor de bens automatiza a recuperação das informações de bens lendo os dados de bens do scanner e preenchendo as tabelas de esquema de bens com esses dados. Para o Mapeamento de Eventos, as informações de bens são mapeadas do IP de destino e do IP de origem.

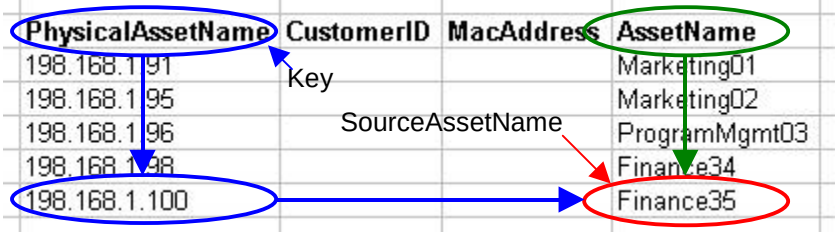
Existem dois tipos de origem de dados:

- Externa – Um Coletor preenche esse valor na tag do evento.
- Referenciado a partir de mapa – Os dados são recuperados de um mapa para preencher a tag.



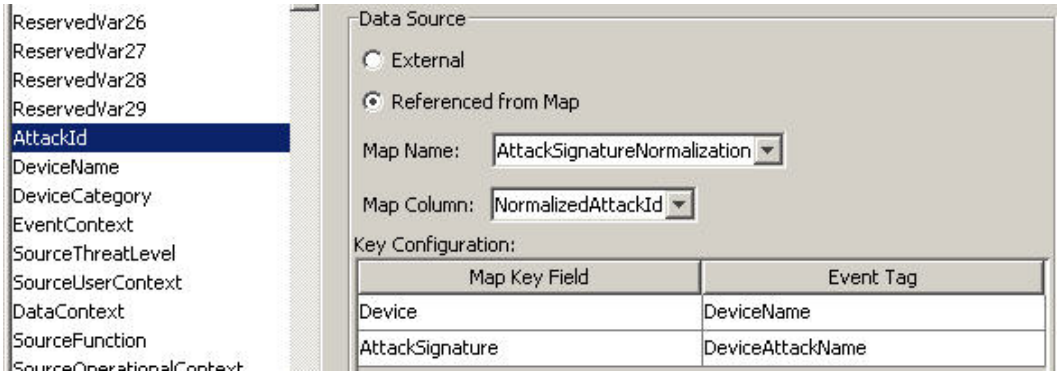
Na ilustração acima, a tag SourceAssetName é preenchida do mapa chamado Bem (que tem asset.csv como arquivo de origem dos dados de mapa). O valor específico para SourceAssetName é retirado da coluna AssetName do mapa Bem. A coluna PhysicalAsssetName é definida como a chave. Quando a tag SourceIP do evento corresponder a um dos valores de IP de origem na coluna PhysicalAsssetName do mapa, a linha com a chave correspondente é usada para interseccionar a coluna AssetName. Por exemplo, no exemplo a seguir, o IP 198.168.1.100 corresponde ao AssetName Finance35.

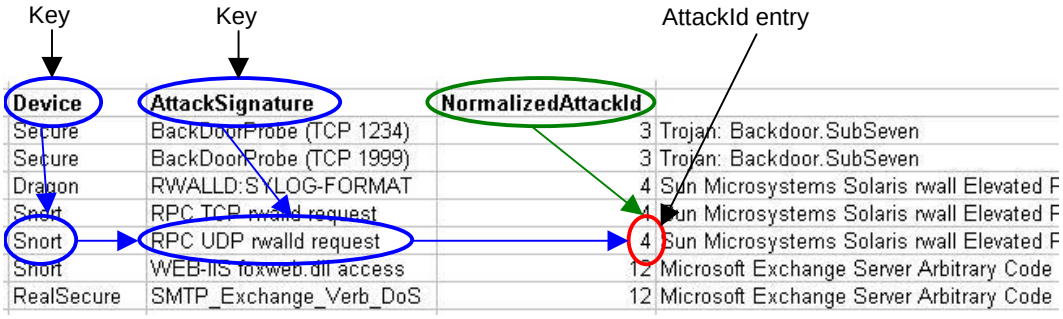
NOTA: quando uma coluna é definida como a chave, ela não aparecerá no campo suspenso Coluna.



Você pode ter mais de uma coluna definida como chave, já que você não quer que o mapa seja o Mapa de Intervalo (os Mapas de Intervalo só podem ter uma coluna de chave, com o tipo dessa coluna definido como NumberRange). Por exemplo, (com o tipo de coluna definido como String), a tag AttackId contém as colunas DeviceName (nome do dispositivo de segurança) e DeviceAttackName definidos como chaves e usa a coluna NormalizedAttackID no mapa AttackNormalization para seu valor. Em uma fila em que a tag de evento DeviceName corresponde aos dados na coluna de mapa Device e o

DeviceAttackName corresponde aos dados na coluna de mapa AttackSignature, o valor de AttackId é o valor na coluna NormalizedAttackID. A configuração do Mapeamento de Eventos recém-descrito é o seguinte:

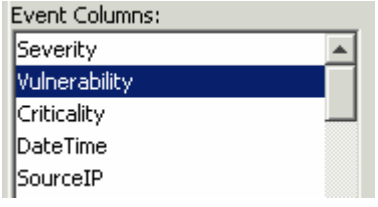




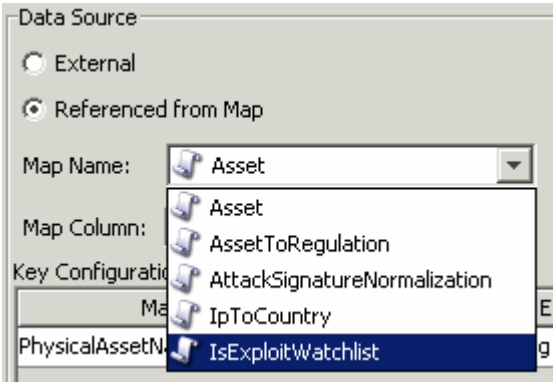
Configurando tags de Evento (colunas) para usar o Mapeamento

1. Clique na guia *Eventos*.
2. Realce uma entrada de tag de evento da lista Colunas de evento.

   NOTA: O nome original da Tag de evento aparece acima do campo Rótulo. Além disso, é fornecida a descrição da coluna de evento.



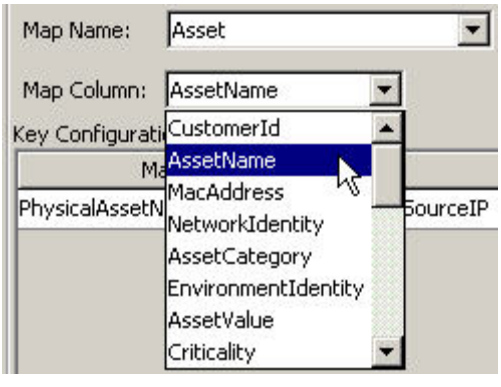
3. Clique em *Referido no Mapa* para configurar a tag de evento a ser preenchida com os dados de um mapa. Clique em *Externo* para manter qualquer valor que o Coletor colocar na tag do evento (se houver).
4. Clique na seta para baixo do campo *Nome do mapa*.

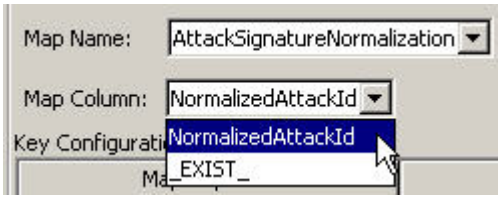


Selecione um dos seguintes mapas-padrão ou um mapa que você criou:

- Bem – Contém os dados do arquivo de origem de dados de mapa asset.csv. O asset.csv é automaticamente gerado a partir dos dados de bens do Banco de Dados do Sentinel quando um Coletor de bem é executado. Esse arquivo poderia ser preenchido manualmente no lugar, caso desejado.
- AssetToRegulation – Contém os dados do arquivo de origem de dados de mapa AssetToRegulation.csv. Esse arquivo deve ser preenchido manualmente.
- AttackSignatureNormalization – Contém os dados do arquivo de origem de dados do mapa attackNormalization.csv (assinaturas IDS). O arquivo attackNormalization.csv é automaticamente gerado a partir dos dados do Advisor do Banco de Dados do Sentinel quando se completa uma alimentação do Advisor.
- IpToCountry – Contém os dados do arquivo de origem de dados de mapa IpToCountry.csv. Esse arquivo deve ser preenchido manualmente.
- IsExploitWatchlist – Contém os dados do arquivo de origem de dados de mapa exploitDetection.csv (vulnerabilidades e ameaças). O arquivo exploitDetection.csv é automaticamente gerado a partir dos dados do Advisor e de Vulnerabilidade do Banco de Dados do Sentinel quando se completa uma alimentação do Advisor ou é executado um Coletor de vulnerabilidade.

5. Clique no campo *Coluna de mapa* e selecione um nome de *Coluna de mapa*. Dependendo da sua escolha de nome de mapa na etapa anterior, esses valores vão variar.

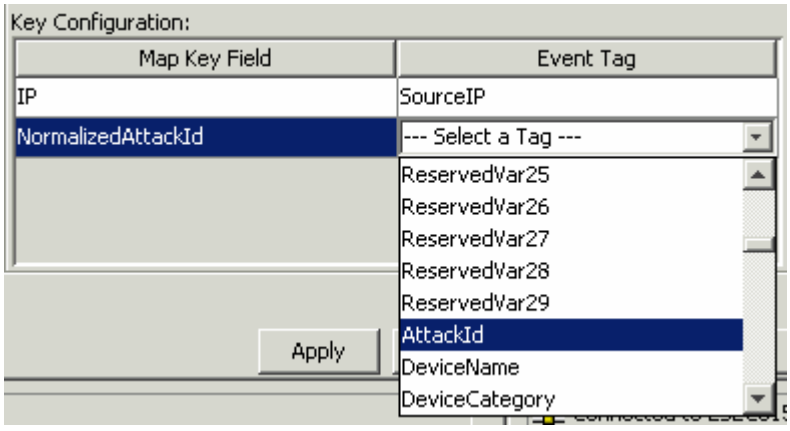




- _EXIST_ - Esta é uma coluna de mapa especial que existe em todos os mapas. Caso a Coluna de mapa seja selecionada, será colocado um "1" na tag de evento caso a chave esteja nos dados do mapa. Caso a chave não esteja nos dados do mapa, será colocado um "0" na tag de evento.
- Todas as outras opções – nomes das colunas ativas na definição do mapa que não são definidos como chave (por exemplo – a coluna CustomerId na coluna Bem ou NormalizedAttackId em AttackNormalization)

6. Na Configuração de chave, para cada linha da tabela, selecione a tag de evento na coluna Tag de evento que corresponderá à coluna de chave de mapa especificada na coluna correspondente do campo Chave do mapa. As linhas na tabela Configuração de chave dependerão do Nome de mapa selecionado.

NOTA: A chave é um identificador exclusivo para a linha de dados no mapa.



7. Clique em *Apply*.

NOTA: Clicar em *Aplicar* grava as alterações que você fez na coluna de eventos atualmente selecionada em um buffer temporário. Se você não clicar em *Aplicar*, ao selecionar uma coluna de evento diferente, as alterações que você fez na coluna de evento previamente selecionada serão perdidas. As alterações não serão gravadas no servidor até você clicar em *Gravar*.

8. Se você quiser editar o *Mapeamento de evento* de outra *Coluna de eventos*, repita as etapas descritas. Lembre-se de clicar em *Aplicar* depois de editar o *Mapeamento de evento* de cada coluna de *eventos*.
9. Clique em *Gravar*.

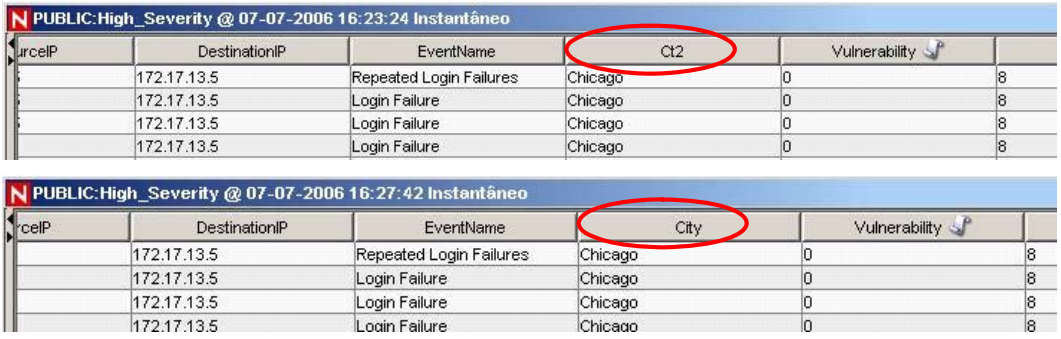
NOTA: Clicar em *Gravar* gravará suas alterações no servidor. A função de gravação grava todas as alterações armazenadas no buffer temporário (quando você clicar em *Aplicar*).

Renomeando as tags

A guia Eventos também permite atribuir nomes aos rótulos existentes da tag de evento. Por exemplo, você pode renomear o rótulo da tag de evento Ct2 para City. O resultado disso será a tag de evento que formalmente aparecia no Sentinel Control Center como "Ct2" aparece agora como "City". Entre os lugares em que as tags de evento aparecem no Sentinel Control Center estão os filtros, as regras de correlação e Active Views.

No entanto, a alteração de nome das tags não altera o nome da variável nos scripts do Coletor. Assim, mesmo que a tag de evento chamada Ct2 seja renomeada como City, a variável que deve ser usada em um script do Coletor para referenciar esta metatag ainda será a _CT2.

A seguir há uma ilustração antes e depois deste recurso em um Active View.



Renomeando uma coluna de evento

1. Clique na guia *Eventos*.

   NOTA: O nome original da Coluna de evento aparece acima do campo Rótulo. Além disso, é fornecida a descrição da coluna de evento.

2. Realce uma entrada de coluna de evento.
3. Insira um novo valor para sua Coluna de evento no campo Rótulo.

4. Clique em *Apply*.

   NOTA: Clicar em *Aplicar* grava as alterações que você fez na tag de eventos atualmente selecionada em um buffer temporário. Se você não clicar em *Aplicar*, ao selecionar uma tag de evento diferente, as alterações que você fez na tag de evento previamente selecionada serão perdidas. As alterações não serão gravadas no servidor até você clicar em *Gravar*.

5. Clique em *Gravar*.

   NOTA: Clicar em *Gravar* gravará suas alterações no servidor. A função de gravação grava todas as alterações armazenadas no buffer temporário (quando você clicar em *Aplicar*).

6. Para que as alterações sejam visíveis no Sentinel Control Center, devem-se fechar e reabrir os Sentinel Control Centers em execução.

Guia Relatando dados

NOTA: Para usar a guia Relatando dados, seu arquivo configuration.xml deve estar apontando para um Servidor de Comunicação que também tem o DAS_Binary e o DAS_Query conectados a ele. Em geral, acontecerá isso por padrão, desde que o Servidor de Comunicação e os processos DAS estejam em execução.

A guia *Relatando dados* é uma *Interface de Gerenciamento de Resumo* para o Sentinel. Essa guia permite ativar e desativar os **Resumos**. A ativação de um resumo permite que a agregação inicie o cálculo da contagem daquele resumo em particular.

O resumo é um conjunto definido de atributos que compõe a chave para a qual se deve calcular o número de ocorrências exclusivas (contagem de eventos) para cada período de uma hora (tempo do evento). No caso do *EventSevDestPortSummary*, quando *ativo*, grava a contagem de eventos para cada combinação exclusiva de porta de destino e severidade para um período de tempo de uma hora. Esses cálculos gravados dos dados de evento permitem a criação mais rápida de relatórios e pesquisas de resumo. Esses relatórios são usados pelo Crystal Reports. Consulte os capítulos de instalação do Crystal Reports no Guia de Instalação do Sentinel para obter mais informações. Certos resumos vão precisar estar *ativos* para que os relatórios de resumo sejam precisos.

A agregação é o processo de cálculo da contagem em execução para todos os resumos ativos como fluxo de eventos através do sistema. Essas contagens em execução são gravadas no banco de dados nas respectivas tabelas de resumo.

Benefícios dos resumos:

- Ampla redução do conjunto de dados de evento
- Dimensões adequadas que permitem a capacidade de detalhar, acomodar e esquadrinhar os dados de evento
- Os relatórios de Resumo são executados com muito mais rapidez do que os resumos pré-calculados

Benefícios da Agregação:

- Apenas processa os resumos ativos
- Não afeta a inserção de eventos no banco de dados de tempo real.

A guia Relatando dados permite o seguinte:

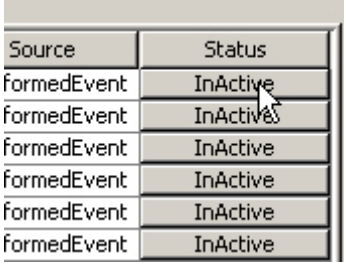
- ativar/desativar quaisquer resumos predefinidos
- visualizar os atributos de cada resumo
- ver a validade de um resumo para um período de tempo
- pesquisar os *arquivos de eventos* que precisam ser executados, de forma que o resumo esteja completo

A seguir há todos os resumos já definidos no sistema. Ele lista o nome do resumo, o nome da tabela no banco de dados e seus atributos em uma breve descrição sobre o resumo.

Nome do Resumo	**Tabela/descrição**
EventSrcSummary	EVT_SRC_SMRY_1 Este resumo soma a contagem de eventos por IP de origem, informações de bens de origem, porta de origem, usuário de origem, taxonomia, nome_evento, recurso, Coletor, severidade e tempo do evento por hora
EventDestSummary	EVT_DEST_SMRY_1 Este resumo soma a contagem de eventos por IP de destino, informações de bens de destino, porta de destino, usuário de destino, taxonomia, nome_evento, recurso, Coletor, severidade e tempo do evento por hora.
EventSevDestTxnmySummary	EVT_ DEST_TXNMY_SMRY_1 Este resumo soma a contagem de eventos por IP de destino, informações de bens de destino, taxonomia, severidade e tempo do evento por hora.
EventSevDestEvtSummary	EVT_DEST_EVT_NAME_SMRY_1 Este resumo soma a contagem de eventos por IP de destino, bens de evento de destino, taxonomia, nome do evento, severidade e tempo do evento por hora.
EventSevDestPortSummary	EVT_PORT_SMRY_1 Este resumo soma a contagem de eventos por porta de destino, taxonomia e tempo do evento por hora.
EventSevSummary	EVT_SEV_SMRY_1 Este resumo soma a contagem de eventos por taxonomia e tempo do evento por hora.

Desabilitando/habilitando o Resumo

1. Clique na guia *Relatando Dados*.
2. Para desabilitar um resumo, clique em *Ativo* na coluna Status até que mude para *Inativo.*
3. Para habilitar um resumo, clique em *Inativo* na coluna Status até que mude para *Ativo.*



Para ativar a *Agregação nos relatórios 10 Primeiros* do Crystal Reports:

- Habilite os três resumos a seguir:
  - EventDestSummary
  - EventSevSummary
  - EventSrcSummary
- Habilite EventFileRedirectService no das_binary.xml localizado em:

Para UNIX:

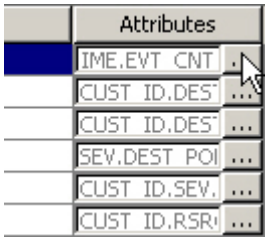
```
$ESEC_HOME/sentinel/config/das_binary.xml
```

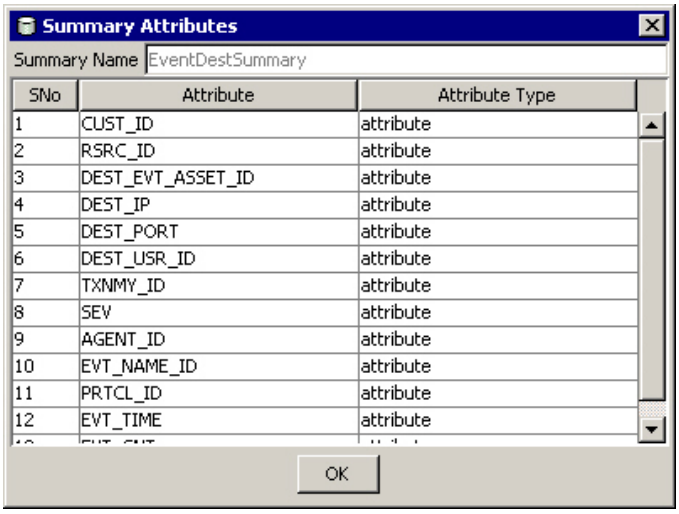
Para Windows:

```
%ESEC_HOME%\sentinel\config\das_binary.xml
```

Visualizando as informações de um Resumo

1. Clique na guia *Relatando Dados*.
2. Clique no botão "…" na coluna Atributos para ver os atributos que compõem um resumo.

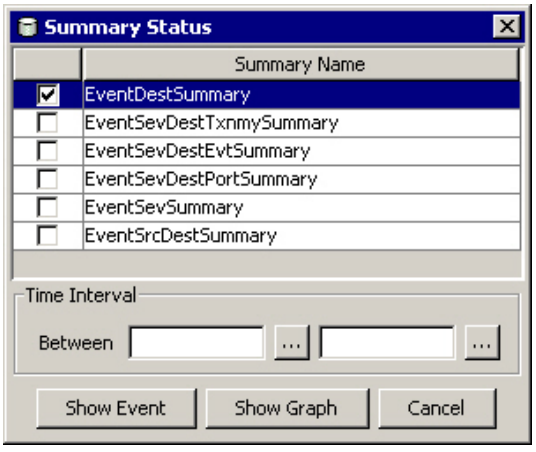




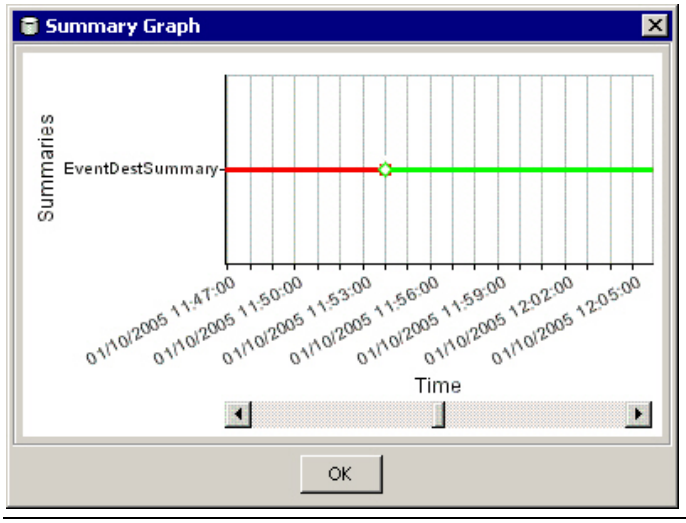
Verifique a validade de um Resumo

1. Clique na guia *Relatando Dados*.
2. Selecione *Status*.

3. Feche o(s) resumo(s) que você deseja pesquisar.



4. Selecione um intervalo de tempo.
5. Clique em *Mostrar gráfico*.
6. A barra verde indica que o resumo está completo naquele período de tempo. A seção vermelha indica que o resumo está perdendo dados durante aquele período de tempo.

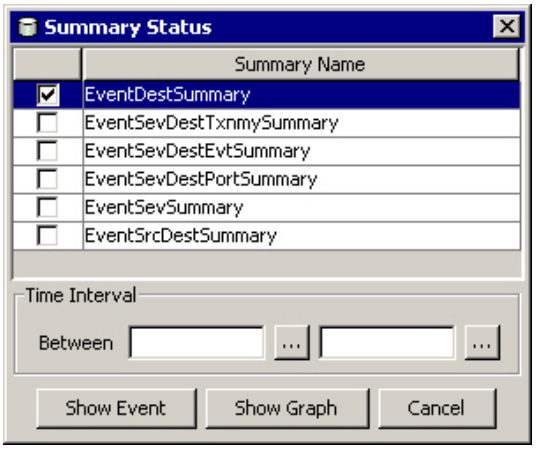


NOTA: Para completar os resumos, consulte a seção *Executar EventFiles para um resumo*.

Pesquisa os Eventfiles para um resumo

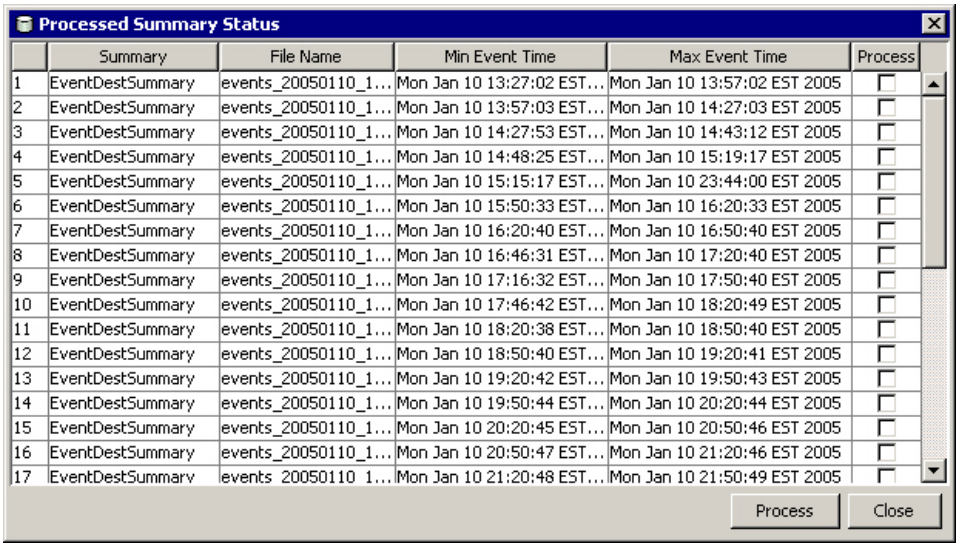
1. Clique na guia *Relatando Dados*.
2. Selecione *Status*.

3. Feche o(s) resumo(s) que você deseja pesquisar.



4. Selecione um intervalo de tempo.
5. Clique em *Mostrar Evento*.
6. Os Eventfiles necessários para completar o resumo aparecem em formato de lista.

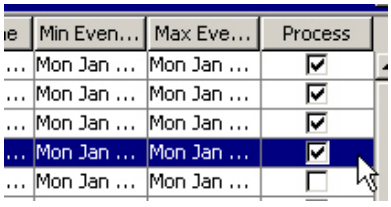
NOTA: para completar os resumos, consulte a seção *Executar EventFile(s) para um resumo*.



Executando Eventfiles para um resumo

1. Clique na guia *Relatando Dados*.
2. Selecione *Status*.
3. Feche o(s) *resumo*(s) que você deseja pesquisar.
4. Selecione um intervalo de tempo.
5. Clique em *Mostrar Evento*.
6. Os *Eventfiles* necessários para completar o resumo aparecem em formato de lista.

7. Verifique os *Eventfiles* que você gostaria de executar, de forma que o resumo esteja completo.



8. Clique em *Processar*.

Linha de comando SDM

NOTA: Se sua máquina não tiver acesso ao DAS_Binary e DAS_Query, a Linha de Comando SDM pode ser usada no lugar da interface de usuário do SDM.

Gravando as propriedades da conexão no Gerenciador de Dados do Sentinel

Essa operação deve ser realizada antes de se usar qualquer uma das ações da Linha de Comando do Gerenciador de Dados do Sentinel que não sejam saveConnection

Se você tiver executado a interface de usuário do SDM, você pode usar o arquivo sdm.connect que foi criado com a interface de usuário. Ele está localizado em %ESEC_HOME%\sdm no Windows e em $ESEC_HOME/sdm no UNIX.

A função de gravar conexão grava os seguintes detalhes da conexão junto com a senha criptografada (usando o keystore especificado em configuration.xml) no arquivo especificado.

Este comando usa os seguintes indicadores:

-action	saveConnection
-server	<oracle ou mssql>
-host	<endereço IP do host do banco de dados ou o nome de host ao qual se conectar>
-port	<número da porta do banco de dados ao qual se conectar [padrão Oracle: 1521/SQL Server padrão: 1433]>
-database	<nome/SID do banco de dados ao qual se conectar>
-user	<nome de usuário do banco de dados>
-password	<senha do banco de dados>
-winAuth	Usado para autenticação do Windows. Ao usar esta opção, não use –user e –password.
-connectFile	<nome de arquivo para gravar os detalhes de conexão [nome de arquivo de sua escolha]>

O aplicativo grava todos os detalhes de conexão acima junto com a senha criptografada no arquivo especificado. O aplicativo usa os detalhes gravados da conexão para executar o resto dos comandos. Essa etapa deve ser completada na primeira vez em que você iniciar o aplicativo e todas as vezes que desejar alterar os detalhes da conexão que o aplicativo usa.

Executando saveConnection

1. Execute o comando como segue:

```
sdm -action saveConnection -server <oracle/mssql> -
   host <hostIp/hostName> -port <portnum> -database
   <databaseName/SID> [-driverProps <propertiesFile>]
   {-user <dbUser> -password <dbPass> | -winAuth} -
   connectFile <filenameToSaveConnection>
```

O exemplo a seguir gravará as conexões de um host com um endereço IP 172.16.0.36 na porta 1521 (padrão para Oracle; no SQL Server, o padrão é 1433).

- Exemplo do Oracle:

```
./sdm -action saveConnection -server oracle -host
   172.16.0.36 -port 1521 -database esec -user esecdba
   -password XXXXXX -connectFile sdm.connect
```

- Exemplo do SQL Server:

```
sdm -action saveConnection -server mssql -host
   172.16.0.36 -port 1433 -database esec -user esecdba
   -password XXXXXX -connectFile  sdm.connect
```

O exemplo a seguir gravará as conexões de um host com um endereço IP 172.16.0.36, porta 1433, com nome do banco de dados do esec_51 para autenticação Windows.

- Exemplo do SQL Server (Autenticação do Windows):

```
sdm -action saveConnection -server mssql -host
   172.16.1.3 -port 1433 -database esec_51 –winAuth -
   connectFile  %ESEC_HOME%\sdm\sdm.connect
```

Isso gravará os detalhes de conexão no arquivo sdm.connect. Todos os outros comandos pegarão este nome de arquivo como entrada para se conectar ao banco de dados designado e realizar suas ações.

Gerenciamento de partição

Configuração de partição

Este vale apenas para o Oracle. Esta ação (partitionConfig) é usada para configurar as partições do seu banco de dados. Esta configuração determina como as partições são adicionadas a todas as tabelas particionadas do Sentinel. Esta ação usa os seguintes indicadores:

-action	partitionConfig
-freq	<"3D" ou "2D" ou "1D" ou "1W"> Estas são as únicas opções suportadas 3D – três partições por dia 2D – duas partições por dia 1D – uma partição por dia 1W – uma partição por semana
-days	<Número de dias a serem adicionados sempre que se escolher addPartitions>
-connectFile	<caminho para o nome de arquivo gravado por saveConnection>

Executando partitionConfig.

1. Execute este comando da seguinte forma:

```
./sdm -action partitionConfig –freq <3D ou 2D ou 1D ou
   1W> -days <Número de dias a serem acrescentados
   sempre que se escolher
   "addPartitions"> -connectFile <caminho para o nome
   de arquivo gravado por "saveConnection" (default:
   $ESEC_HOME/sdm/sdm.connect)>
```

   No exemplo a seguir, o sistema adicionará 30 partições (3 partições por 1 DIA = 3 * 10).

```
./sdm -action partitionConfig -freq 3D -days 10 -
   connectFile sdm.connect
```

   No exemplo a seguir, o sistema adicionará dez partições (1 partição por 1 DIA = 1 * 10).

```
./sdm -action partitionConfig -freq 1D -days 10 -
   connectFile sdm.connect
```

   No exemplo a seguir, o sistema adicionará uma partição (1 partição por 7 dias = 1 * 10/7).

```
./sdm -action partitionConfig -size 1W -days 10 -
   connectFile sdm.connect
```

Adicionando partições

Esta ação (addPartitions) adiciona o número necessário de partições de acordo com a configuração de partição nas tabelas a seguir:

- Oracle:
  - EVENTS
  - CORRELATED_EVENTS
  - EVT_DEST_EVT_NAME_SMRY_1
  - EVT_DEST_SMRY_1
  - EVT_DEST_TXNMY_SMRY_1
  - EVT_PORT_SMRY_1
  - EVT_SEV_SMRY_1
  - EVT_SRC_SMRY_1
- SQL Server
  - EVENTS
  - CORRELATED_EVENTS
  - EVT_DEST_EVT_NAME_SMRY_1
  - EVT_DEST_SMRY_1
  - EVT_DEST_TXNMY_SMRY_1
  - EVT_PORT_SMRY_1
  - EVT_SEV_SMRY_1
  - EVT_SRC_SMRY_1

Caso sua configuração tenha 10 dias que mereçam partições, todas as vezes que você executar *addPartitions* o sistema verificará se você tem 10 dias de partições no futuro. Se você tiver partições suficientes para os próximos 10 dias, ele não fará nada. Caso contrário, acrescentará o número necessário de partições por 10 dias.

Esta ação usa os seguintes indicadores:

-action	addPartitions
-connectFile	<caminho para o nome de arquivo gravado por "saveConnection">

Executando addPartitions.

1. Execute este comando da seguinte forma:

```
sdm -action addPartitions -connectFile <caminho para o
   nome de arquivo gravado por "saveConnection">
```

   Exemplo do Oracle:

```
./sdm -action addPartitions -connectFile sdm.connect
```

   Exemplo do SQL Server:

```
sdm -action addPartitions -connectFile sdm.connect
```

Eliminando partições

Esta ação (dropPartition) elimina todas as partições que são mais antigas do que o indicador keepDays das tabelas a seguir:

- Oracle:
  - EVENTS
  - CORRELATED_EVENTS
  - EVT_DEST_EVT_NAME_SMRY_1
  - EVT_DEST_SMRY_1
  - EVT_DEST_TXNMY_SMRY_1
  - EVT_PORT_SMRY_1
  - EVT_SEV_SMRY_1
  - EVT_SRC_SMRY_1
- SQL Server
  - EVENTS
  - CORRELATED_EVENTS
  - EVT_DEST_EVT_NAME_SMRY_1
  - EVT_DEST_SMRY_1
  - EVT_DEST_TXNMY_SMRY_1
  - EVT_PORT_SMRY_1
  - EVT_SEV_SMRY_1
  - EVT_SRC_SMRY_1

Esta ação não elimina nenhuma partição que não está arquivada. Se desejar apagar as partições não-arquivadas, use o indicador *forceDelete*. Caso se use forceDelete:

falso ou não especificado	elimina apenas as partições mais antigas do que keepDays e as que estão arquivadas
verdadeiro	elimina todas as partições mais antigas do que keepDays, incluindo as partições não-arquivadas

Esta ação usa os seguintes indicadores:

-action	dropPartitions
-keepDays	<número de dias a serem mantidos>
[-forceDelete]	<"verdadeiro" ou "falso">
-connectFile	<caminho para o nome de arquivo gravado por "saveConnection">

NOTA: Se você eliminar uma partição que não foi arquivada, ela não poderá ser importada.

Executando dropPartition.

1. Execute este comando da seguinte forma:

```
sdm -action dropPartitions [-forceDelete <false>] -
   keepDays <número> -connectFile <caminho para o nome
   de arquivo gravado por "saveConnection">
```

Os exemplos a seguir eliminam todas as partições que são mais antigas do que 30 dias, garantindo que todas as partições são arquivadas. Todas as partições que foram puladas (não removidas) porque não foram arquivadas aparecem na lista quando a operação é concluída.

Exemplo do Oracle:

```
./sdm -action dropPartitions -keepDays 30 -connectFile
   sdm.connect


./sdm -action dropPartitions -forceDelete false -
   keepDays 30 -connectFile sdm.connect
```

Exemplo do SQL Server:

```
sdm -action dropPartitions -keepDays 30 -connectFile
   sdm.connect


sdm -action dropPartitions -forceDelete false -
   keepDays 30 -connectFile sdm.connect
```

Visualizando os resumos da partição

Esta ação (ViewPartitions) exibe o resumo da partição das tabelas suportadas a seguir:

- Oracle:
  - EVENTS
  - CORRELATED_EVENTS
  - EVT_DEST_EVT_NAME_SMRY_1
  - EVT_DEST_SMRY_1
  - EVT_DEST_TXNMY_SMRY_1
  - EVT_PORT_SMRY_1
  - EVT_SEV_SMRY_1
  - EVT_SRC_SMRY_1
- SQL Server
  - EVENTS
  - CORRELATED_EVENTS
  - EVT_DEST_EVT_NAME_SMRY_1
  - EVT_DEST_SMRY_1
  - EVT_DEST_TXNMY_SMRY_1
  - EVT_PORT_SMRY_1
  - EVT_SEV_SMRY_1
  - EVT_SRC_SMRY_1

Este comando usa os seguintes indicadores:

-action	startGui
-tableName	<nome de uma das tabelas mencionadas>
-connectFile	<caminho para o nome de arquivo gravado por "saveConnection">

Para visualizar os Resumos da Partição.

1. Execute este comando da seguinte forma:

```
sdm -action viewPartitions -tableName <nome de tabela>
   –connectFile <caminho para o nome de arquivo
   gravado por "saveConnection">
```

   No exemplo a seguir, aparece a lista de partições da tabela EVENTOS e o status de cada partição.

   - Exemplo do Oracle:

```
./sdm -action viewPartitions -tableName EVENTS -
   connectFile sdm.connect
```

   - Exemplo do SQL Server:

```
sdm -action viewPartitions –tableName EVENTS –
   connectFile sdm.connect
```

Gerenciamento de arquivo

Configuração do arquivo

Esta ação (archiveConfig) é usada para configurar o arquivamento. Esta configuração determina como os dados são arquivados a partir das tabelas do Sentinel.

Esta ação usa os seguintes indicadores:

-action	archiveConfig
-dirPath	<caminho válido de diretório no qual gravar os arquivos armazenados>
-keepDays	<número de dias a serem mantidos>
-fileSize	(Apenas Oracle) <tamanho máximo de cada arquivo armazenado. Especifique KB, MB ou GB>
-connectFile	<caminho para o nome de arquivo gravado por "saveConnection">

No Oracle, o caminho de diretório dirPath deve ser especificado como parâmetro UTL_FILE_DIR no arquivo init.ora, de acordo com as exigências do Oracle. Você deve ter um dos seguintes:

- UTL_FILE_DIR = *
- UTL_FILE_DIR = diretório específico em que você deseja gravar os arquivos no seu arquivo init.ora

Executando archiveConfig

1. Execute este comando da seguinte forma:

```
sdm -action archiveConfig  -dirPath <caminho de
   diretório no qual são gravados os arquivos
   armazenados> -keepDays <número de dias a serem
   mantidos> -fileSize <tamanho máximo de cada arquivo
   armazenado, especificado em KB, MB ou GB> -
   connectFile <caminho ao nome de arquivo gravado por
   "saveConnection">
```

   - Exemplo do Oracle:

   O exemplo a seguir arquiva todos os dados mais antigos do que 13 dias no diretório /tmp em pacotes maiores do que 1GB.

```
./sdm -action archiveConfig  -dirPath /tmp -keepDays
   13 -fileSize 1GB -connectFile sdm.connect
```

   O exemplo a seguir arquiva todos os dados mais antigos do que 13 dias no diretório /tmp em pacotes maiores do que 40MB.

```
./sdm -action archiveConfig -dirPath /tmp -keepDays 13
   -fileSize 40MB -connectFile sdm.connect
```

Arquivando dados

Execute esta ação (archiveData) depois de definir a configuração do seu arquivo (archiveConfig). Esta ação arquiva os dados a partir do nome de tabela dado, de acordo com a configuração de arquivo. Ela arquiva os dados a partir de:

- Oracle:
  - EVENTS
  - CORRELATED_EVENTS
- SQL Server
  - EVENTS
  - CORRELATED_EVENTS

NOTA: as tabelas de agregação não são arquivadas.

Este comando usa os seguintes indicadores:

-action	archiveData
-connectFile	<caminho para o nome de arquivo gravado por "saveConnection">

Executando archiveData

1. Execute este comando da seguinte forma:

```
sdm -action archiveData -connectFile <caminho para o
   nome de arquivo gravado por "saveConnection">
```

   - Exemplo do Oracle:

   O exemplo a seguir arquiva eventos, seus valores reservados e personalizados e os eventos correlacionados da tabela EVENTS, EVT_RESERVED_VALUES, EVT_CUSTOM_VALUES e ASSOCIATIONS, de acordo com o valor definido na configuração do seu arquivo (archiveConfig). Usando este valor definido no exemplo

fornecido na seção em Gerenciamento de arquivo, será possível arquivar dados mais antigos do que 13 dias.

```
./sdm -action archiveData -connectFile sdm.connect
```

- Exemplo do SQL Server:

O exemplo a seguir arquiva os eventos e os eventos correlacionados de acordo com o valor definido na configuração do seu arquivo (archiveConfig). Usando este valor definido no exemplo fornecido na seção em Gerenciamento de arquivo, será possível arquivar dados mais antigos do que 13 dias.

```
sdm -action archiveData -connectFile sdm.connect
```

Apagando dados

Esta ação (deleteData) apaga os dados mais antigos do que os dias de conservação do nome de tabela dado. Ela apaga dados de:

- Oracle:
  - EVENTS
  - CORRELATED_EVENTS
  - EVT_DEST_EVT_NAME_SMRY_1
  - EVT_DEST_SMRY_1
  - EVT_DEST_TXNMY_SMRY_1
  - EVT_PORT_SMRY_1
  - EVT_SEV_SMRY_1
  - EVT_SRC_SMRY_1

- SQL Server
  - EVENTS
  - CORRELATED_EVENTS
  - EVT_DEST_EVT_NAME_SMRY_1
  - EVT_DEST_SMRY_1
  - EVT_DEST_TXNMY_SMRY_1
  - EVT_PORT_SMRY_1
  - EVT_SEV_SMRY_1
  - EVT_SRC_SMRY_1

Esta ação não elimina nenhuma partição que não está arquivada. Se desejar apagar as partições não-arquivadas, o indicador opcional *forceDelete* precisa ser especificado com um valor de verdadeiro. Caso se use forceDelete:

falso ou não especificado	elimina apenas as partições mais antigas do que keepDays e as que estão arquivadas
verdadeiro	elimina todas as partições mais antigas do que keepDays, incluindo as partições não-arquivadas

Este comando usa os seguintes indicadores:

-action	deleteData
-keepDays	<número de dias a serem mantidos>
[-forceDelete]	<verdadeiro ou falso>
-connectFile	<caminho para o nome de arquivo gravado por "saveConnection">

Executando deleteData

1. Execute este comando da seguinte forma:

```
sdm -action deleteData -keepDays <número de dias a
   serem mantidos> -connectFile <caminho para o nome
   de arquivo gravado por "saveConnection">
```

   - Exemplo do Oracle:

   O exemplo a seguir elimina as partições de todas as tabelas que são mais antigas do que 13 dias, garantindo que todas as partições eliminadas são arquivadas. No final, é gerada uma lista de todas as partições que não foram apagadas caso não tenham sido arquivadas.

```
./sdm -action deleteData -keepDays 13 -connectFile
   sdm.connect
```

   - Exemplo do SQL Server:

   O exemplo a seguir elimina as partições de todas as tabelas que são mais antigas do que 13 dias, garantindo que todas as partições eliminadas são arquivadas. No final, lista todas as partições que não foram apagadas caso não tenham sido arquivadas.

```
sdm -action deleteData -keepDays 13 -connectFile
   sdm.connect
```

Gerenciamento de importação

Listando os arquivos a serem importados

Esta ação (filesToImport) é usada para listar os arquivos necessários para importar os dados entre as datas determinadas das seguintes tabelas suportadas:

- Oracle:
  - HIST_EVENTS
  - HIST_CORRELATED_EVENTS
- SQL Server
  - HIST_EVENTS
  - HIST_CORRELATED_EVENTS

Este comando usa os seguintes indicadores:

-action	filesToImport
-startDate	<mm/dd/aaaa hh24:mi:ss>
-endDate	<mm/dd/aaaa hh24:mi:ss>
-connectFile	<caminho para o nome de arquivo gravado por "saveConnection">

NOTA: hh24 são as horas representadas no formato 24 horas. Por exemplo, 1:15:00 p.m. é 13h15min00 e 3:00:00 a.m. é 03h00min00.

Executando filesToImport

1. Execute este comando da seguinte forma:

```
sdm -action filesToImport -startDate <mm/dd/aaaa
   hh24:mi:ss> -endDate <mm/dd/aaaa hh24:mi:ss> -
   connectFile <caminho para o nome de arquivo gravado
   pelo "saveConnection">
```

O exemplo a seguir lista todos os arquivos que contêm dados entre as datas "09/25/2003 00:00:00" (meia-noite de 25 de setembro) e "09/26/2003 00:00:00" (meia-noite de 26 de setembro) que foram arquivados mais cedo e podem ser importados de volta.

- Exemplo do Oracle:

```
./sdm -action filesToImport -startDate 09/25/2003
   00:00:00 -endDate 09/26/2003 00:00:00 -connectFile
   sdm.connect
```

- Exemplo do SQL Server:

```
sdm -action filesToImport -startDate 09/25/2003
   00:00:00 -endDate 09/26/2003 00:00:00 -connectFile
   sdm.connect
```

O exemplo a seguir lista todos os arquivos que contêm dados entre as datas "09/25/2003 16:00:00" (4 da tarde de 25 de setembro) e "09/26/2003 18:00:00" (6 da tarde de 26 de setembro) que foram arquivados mais cedo e podem ser importados de volta.

- Exemplo do Oracle:

```
./sdm -action filesToImport -startDate 09/25/2003
   16:00:00 -endDate 09/26/2003 18:00:00 -connectFile
   sdm.connect
```

- Exemplo do SQL Server:

```
sdm -action filesToImport -startDate 09/25/2003
   16:00:00 -endDate 09/26/2003 18:00:00 -connectFile
   sdm.connect
```

Importando dados

Esta ação (importData) importa dados entre as datas determinadas nas seguintes tabelas suportadas:

- Oracle:
  - HIST_EVENTS
  - HIST_CORRELATED_EVENTS
- SQL Server
  - HIST_EVENTS
  - HIST_CORRELATED_EVENTS

Caso os dados já tenham sido importados, ou nenhum dado arquivado for encontrado entre as datas especificadas, ele devolve uma mensagem.

O aplicativo importa cada arquivo para uma tabela e constrói a visualização de histórico de todas as tabelas correspondentes. A visualização de relatório se junta à tabela original e à visualização de histórico. Todos os relatórios usam a visualização de relatório e, portanto, verão todos os dados importados.

Este comando usa os seguintes indicadores:

-action	importData
-startDate	<mm/dd/aaaa hh24:mi:ss>
-endDate	<mm/dd/aaaa hh24:mi:ss>
-dirPath	<diretório do qual importar arquivos>
-connectFile	<caminho para o nome de arquivo gravado por "saveConnection">

NOTA: hh24 são as horas representadas no formato 24 horas. Por exemplo, 1:15:00 p.m. é 13h15min00 e 3:00:00 a.m. é 03h00min00.

Executando importData

1. Coloque todos os arquivos que você deseja importar em um diretório específico (ou seja, dirPath - <diretório do qual importar arquivos>).
2. Execute este comando da seguinte forma:

```
sdm -action importData -dirPath <diretório do qual
   importar arquivos> -startDate <mm/dd/aaaa
   hh24:mi:ss> -endDate <mm/dd/aaaa hh24:mi:ss> -
   connectFile <caminho para o nome de arquivo gravado
   por "saveConnection">
```

O exemplo a seguir importa todos os arquivos arquivados do diretório tmp contendo os dados entre as datas "09/25/2003 00:00:00" (meia-noite de 25 de setembro) e "09/26/2003 00:00:00" (meia-noite de 26 de setembro) para as tabelas acima mencionadas.

- Exemplo do Oracle:

```
./sdm -action importData -dirPath /tmp -startDate
   09/25/2003 00:00:00 -endDate 09/26/2003
   00:00:00 -connectFile sdm.connect
```

- Exemplo do SQL Server:

```
sdm -action importData -dirPath c:\tmp -startDate
   09/25/2003 00:00:00 -endDate 09/26/2003
   00:00:00 -connectFile sdm.connect
```

O exemplo a seguir importa todos os arquivos arquivados do diretório tmp contendo os dados entre as datas "09/25/2003 08:30:00" (oito e meia da manhã do dia 25 de setembro) e "09/26/2003 20:00:00" (oito horas da noite do dia 26 de setembro) para as tabelas acima mencionadas.

- Exemplo do Oracle:

```
./sdm -action importData -dirPath /tmp -startDate
   09/25/2003 08:00:00 -endDate 09/26/2003
   20:00:00 -connectFile sdm.connect
```

- Exemplo do SQL Server:

```
sdm -action importData -dirPath c:\tmp -startDate
   09/25/2003 08:00:00 -endDate 09/26/2003
   20:00:00 -connectFile sdm.connect
```

Apagando dados importados

Esta ação (dropImported) apaga os dados importados entre as datas determinadas das seguintes tabelas suportadas:

- Oracle:
  - HIST_EVENTS
  - HIST_CORRELATED_EVENTS

- SQL Server
  - HIST_EVENTS
  - HIST_CORRELATED_EVENTS

Caso não haja dados importados entre as duas datas especificadas, o sistema devolve uma mensagem.

Este comando usa os seguintes indicadores:

-action	dropImported
-startDate	<mm/dd/aaaa hh24:mi:ss>
-endDate	<mm/dd/aa hh24:mi:ss>
-connectFile	<caminho para o nome de arquivo gravado por "saveConnection">

NOTA: hh24 são as horas representadas no formato 24 horas. Por exemplo, 1:15:00 p.m. é 13h15min00 e 3:00:00 a.m. é 03h00min00.

Executando dropImported

1. Execute este comando da seguinte forma:

```
sdm -action dropImported -startDate <mm/dd/aaaa
   hh24:mi:ss> -endDate <mm/dd/yyyy hh24:mi:ss> -
   connectFile <caminho para o nome de arquivo gravado
   por "saveConnection">
```

   O exemplo a seguir apaga os dados importados entre as datas determinadas das tabelas já mencionadas:

   - Exemplo do Oracle:

```
./sdm -action dropImported -startDate 09/25/2003
   00:00:00 -endDate 09/26/2003 00:00:00 -connectFile
   sdm.connect
```

   - Exemplo do SQL Server:

```
sdm -action dropImported -startDate 09/25/2003
   00:00:00 -endDate 09/26/2003 00:00:00 -connectFile
   sdm.connect
```

Gerenciamento de tabelas

No Gerenciamento de Tabelas, você tem uma opção de linha de comando e uma opção de interface de usuário. A linha de comando permite:

- Ver a utilização do espaço no banco de dados do Sentinel

A interface de usuário permite:

- Ver as partições
- Ver as partições arquivadas
- Ver as partições importadas
- Ver a utilização do espaço

Vendo a utilização do espaço no banco de dados do Sentinel (linha de comando)

Esta ação (dbstats) apresenta a utilização do banco de dados do Sentinel para todas as tabelas do Sentinel nos grupos de arquivos do Oracle e do Sentinel no MS SQL.

Este comando usa os seguintes indicadores:

-action	dbstats
-connectFile	<caminho para o nome de arquivo gravado por "saveConnection">

Vendo a utilização do espaço no banco de dados do Sentinel (linha de comando)

1. Execute o seguinte comando:

```
sdm -action dbStats -connectFile <caminho para o nome
   de arquivo gravado por "saveConnection">
```

   - Exemplo do Oracle:

   O exemplo a seguir exibe as tabelas do banco de dados do Sentinel com seu espaço total, espaço usado e espaço livre disponível.

```
./sdm -action dbStats -connectFile sdm.connect
```

   - Exemplo do SQL Server:

   O exemplo a seguir exibe os grupos de arquivo do banco de dados do Sentinel com seu espaço total, espaço usado e espaço livre disponível.

```
sdm -action dbStats -connectFile sdm.connect
```

Atualizando os mapeamentos (linha de comando)

Esta ação (updateMapData) permite substituir um arquivo de dados de origem de mapa por outro. Seu novo arquivo de dados de origem deve ter os mesmos delimitadores, colunas de chave e a coluna ativada do mapeamento anterior. Caso não tenha, use o recurso Editar da interface de usuário do SDM.

Este comando usa os seguintes indicadores:

-action	updateMapData
-map	<nome do mapa>
-file	<nome de arquivo>
-backup	<verdadeiro/falso> (padrão: verdadeiro)
-connectFile	<caminho para o nome de arquivo gravado por "saveConnection">

O indicador –backup permite fazer backup do arquivo original de mapeamento na pasta map_data. O arquivo de backup do mapa de dados será gravado como arquivo .bak com um conjunto de números aleatórios no final do arquivo. Por exemplo: ameaca10197.bak.

Atualizando (substituir) um mapeamento

1. Execute o seguinte comando:

```
sdm -action updateMapData -map <mapName> -file
   <fileName> [-backup <true/false> (DEFAULT: true)] -
   connectFile <caminho para o nome de arquivo gravado
   pelo "saveConnection">
```

O exemplo a seguir substitui os mapeamentos no mapa threat pelos mapeamentos do arquivo de mapa "vuln_attacks.txt".

```
sdm -action updateMapData -map threat -file
   vuln_attacks.txt -connectFile sdm.connect
```

Como o indicador –backup não foi usado, a operação-padrão criará um backup do mapeamento original antes de atualizar o arquivo de mapa "vuln_attack.txt".

Usando o Auto Manage Script fornecido pela Novell (apenas no Windows)

A Novell desenvolveu um arquivo de lote que pode ser agendado, de forma que muitas das ações de gerenciamento do SDM podem ser pré-formadas automaticamente.

NOTA: Se sua máquina não tiver acesso ao DAS_Binary e DAS_Query, a Linha de Comando SDM pode ser usada no lugar da interface de usuário do SDM.

Este procedimento só é aplicável ao Windows. Garante que, durante a realização da sua pré-configuração e da configuração, seja realizado o seguinte:

- Certifique-se de que sdm.connect seja inicializado com a interface de usuário do SDM ou a linha de comando.
- Certifique-se de que o diretório de arquivo exista.
- Certifique-se de que os dias de archiveConfig e dropPartitions sejam iguais.
- Certifique-se de que o arquivo de lote seja corretamente executado do prompt de comando pelo menos uma vez antes de agendá-lo para execução automática.

NOTA: Caso a tarefa agendada falhe, ela não envia uma notificação. A tarefa é registrada em SDM_*.log

Configurando o arquivo Manage_data.bat para Arquivar dados e Adicionar partições

Pré-configuração

Antes de configurar automaticamente Arquivar dados e Adicionar partições, você deve:

- Gravar propriedades de conexão
- Estabelecer parâmetros de arquivamento

NOTA: Se você gravou um arquivo de conexão em um local ou com um nome de arquivo diferentes do padrão (%ESEC_HOME%\sdm\sdm.connect), você terá que editar o arquivo manage_data.bat para atualizar o caminho para o seu arquivo de conexão.

Estabelecendo os parâmetros de arquivamento

Pode-se fazer isso com a Linha de Comando.

Esta ação (archiveConfig) é usada para configurar o arquivamento. Esta configuração determina como os dados são arquivados a partir das tabelas do Sentinel.

Esta ação usa os seguintes indicadores:

-action	archiveConfig
-dirPath	<caminho válido de diretório no qual gravar os arquivos armazenados>
-keepDays	<número de dias a serem mantidos>
-connectFile	<caminho para o nome de arquivo gravado por "saveConnection">

Estabelecendo parâmetros de arquivamento através da Linha de Comando

1. Crie um diretório de saída de arquivo na raiz chamada SDM_archive (c:\SDM_archive).

   NOTA: Se criar um diretório de saída ou local diferentes, você terá que editar o arquivo manage_data.bat.

2. Execute este comando da seguinte forma:

   ```
   sdm -action archiveConfig  -dirPath <caminho de
      diretório no qual gravar os arquivos armazenados> -
      keepDays <número de dias a serem mantidos> -
      connectFile <caminho para o nome de arquivo gravado
      por "saveConnection">
   ```

   O exemplo a seguir arquiva todos os dados mais antigos do que 30 dias no diretório c:\SDM_archive.

   ```
   sdm -action archiveConfig –dirpath c:\SDM_archive -
      keepDays 30 -connectFile sdm.connect
   ```

Estabelecendo parâmetros de arquivamento através da interface de usuário

1. Crie um diretório de saída de arquivo na raiz chamada SDM_archive (c:\SDM_archive).

   NOTA: Se criar um diretório de saída ou local diferentes, você terá que editar o arquivo manage_data.bat.

2. A interface de usuário do SDM não exige parâmetros de arquivamento. A interface de usuário pode arquivar diretamente os dados sem precisar estabelecer parâmetros de arquivamento.

Apagar dados (eliminar partições)

Esta ação (deleteData) apaga os dados mais antigos do que os dias de conservação do nome de tabela dado. Ela apaga dados de:

- EVENTS
- CORRELATED_EVENTS
- EVT_DEST_EVT_NAME_SMRY_1
- EVT_DEST_SMRY_1
- EVT_DEST_TXNMY_SMRY_1
- EVT_PORT_SMRY_1
- EVT_SEV_SMRY_1
- EVT_SRC_SMRY_1

Esta ação não elimina nenhuma partição que não está arquivada. Se desejar apagar as partições não-arquivadas, o indicador opcional *forceDelete* precisa ser especificado com um valor de verdadeiro. Caso se use forceDelete:

falso ou não especificado	elimina apenas as partições mais antigas do que keepDays e as que estão arquivadas
verdadeiro	elimina todas as partições mais antigas do que keepDays, incluindo as partições não-arquivadas

Este comando usa os seguintes indicadores:

-action	deleteData
-keepDays	<número de dias a serem mantidos>
[-forceDelete]	<verdadeiro ou falso>
-connectFile	<caminho para o nome de arquivo gravado por "saveConnection">

Executando deleteData

1. Execute este comando da seguinte forma:

```
sdm -action deleteData -keepDays <número de dias a
   serem mantidos> -connectFile <caminho para o nome
   de arquivo gravado por "saveConnection">
```

   O exemplo a seguir elimina as partições das tabelas que são mais antigas do que 30 dias, garantindo que todas as partições eliminadas são arquivadas. No final, lista todas as partições que não foram apagadas caso não tenham sido arquivadas.

```
sdm -action deleteData -keepDays 30 -connectFile
   sdm.connect
```

Agendando Manage_data.bat para Arquivar dados e Adicionar partições

NOTA: O arquivo manage_data.bat é configurado para um valor de keepDay de 30, para uma saída de arquivo para c:\SDM_archive e para um arquivo de conexão %ESEC_HOME%\sdm\sdm.connect. Caso seus valores sejam diferentes, você precisará editar o arquivo manage_data.bat.

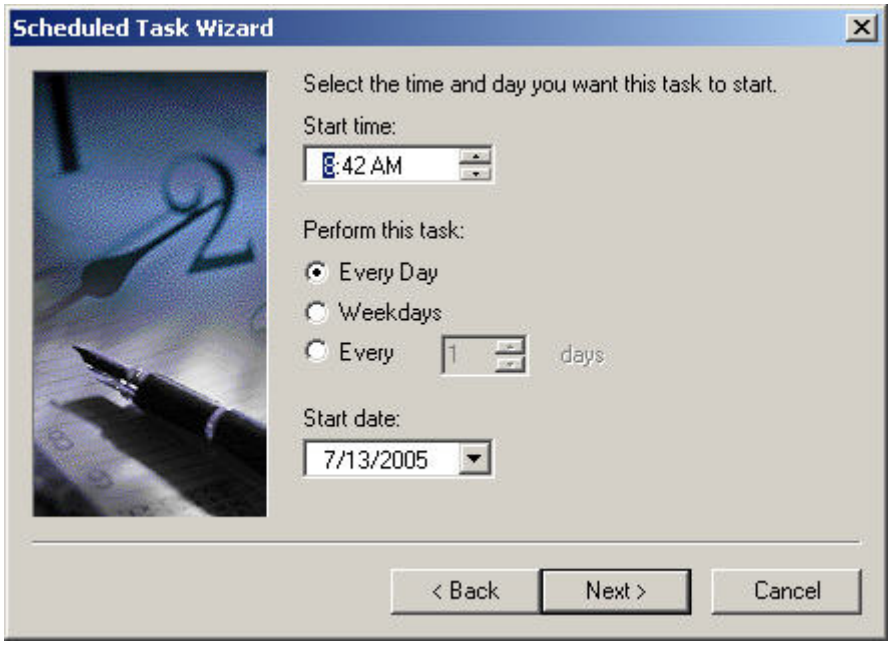
Se você tiver definido as propriedades da sua conexão e os parâmetros de arquivamento, execute manage_data.bat do prompt de comando para garantir que esteja funcionando.

Para arquivar dados e adicionar partições automaticamente

NOTA: As etapas a seguir são para o Windows 2000 Professional. As etapas para o Windows 2000 Server e o XP podem ser diferentes, embora semelhantes.

1. No Windows, clique em *Iniciar* > *Configuração* > *Painel de controle*.
2. Clique duas vezes em *Tarefas agendadas*.
3. Clique duas vezes em *Adicionar tarefa agendada*. Clique em *Avançar*.
4. Clique em *Procurar* e vá até o arquivo manage_data.bat.
5. Dê um nome para a tarefa agendada, como SDM_Archive. Selecione *Diariamente* em *Realizar esta tarefa*:. Clique em *Avançar*.

6. Selecione uma hora do dia para executar esta tarefa. Clique em *Avançar*.
7. Insira uma hora e uma data de sua preferência. Clique em *Avançar*.



8. Insira um nome com o qual esta tarefa será executada. O usuário não pode ser a conta de sistema local. Deve ser executado como usuário específico. Clique em *Avançar*.
9. Clique em *Concluir* para encerrar como tarefa agendada.

11 Utilitários

Iniciando e parando o Sentinel Server, o Gerenciador de Coletor e o UNIX

NOTA: O termo Agente é sinônimo de Coletor. De agora em diante, Agentes serão referidos como Coletores.

Iniciando o Sentinel Server do UNIX

No UNIX, a inicialização do Sentinel Server também inicia o Servidor de Comunicação.

Iniciando o Sentinel Server do UNIX

1. Como usuário esecadm, use o comando cd para trocar para o diretório $ESEC_HOME/sentinel/scripts.
2. Execute o seguinte comando:

```
./sentinel.sh start
```

Parando o Sentinel Server do UNIX

No UNIX, parar o Sentinel Server também pára o Servidor de Comunicação.

Parando o Sentinel Server do UNIX

1. Como usuário esecadm, troque para o diretório $ESEC_HOME/sentinel/scripts usando o comando cd.
2. Execute o seguinte comando:

```
./sentinel.sh stop
```

Iniciando o Gerenciador de Coletor do UNIX

Iniciando o Gerenciador de Coletor do UNIX

1. Como usuário esecadm, troque para $WORKBENCH_HOME usando o comando cd.
2. Execute o seguinte comando:

```
./agent-manager.sh start
```

Parando o Gerenciador de Coletor do UNIX

Parando o Gerenciador de Coletor do UNIX

1. Como usuário esecadm, troque para $WORKBENCH_HOME usando o comando cd.
2. Execute o seguinte comando:

```
./agent-manager.sh stop
```

Iniciando e parando o Sentinel Server e o Gerenciador de Coletor – Windows

Dependendo da configuração da sua instalação, você pode ter até três serviços do Sentinel em execução na sua máquina. São eles:

- Sentinel – Watchdog, este serviço inicia todos os outros processos de servidor do Sentinel.
- Comunicação do Sentinel – Este serviço é o seu Servidor de Comunicação criptografado.
- Gerenciador de Coletor – Este serviço é seu Assistente.

Nos Serviços do Windows, você pode iniciar, reiniciar e parar manualmente qualquer um desses serviços.

Iniciando o Gerenciador de Coletor do Windows

Iniciando o Gerenciador de Coletor do Windows

1. Clique em *Iniciar* > *Configurações* > *Painel de Controle*.
2. Clique duas vezes em *Ferramentas Administrativas*.
3. Clique duas vezes em *Serviços*.
4. Clique o botão direito do mouse em *Gerenciador de Coletor* > *Iniciar*.

Parando o Gerenciador de Coletor do Windows

Parando o Gerenciador de Coletor do Windows

1. Clique em *Iniciar* > *Configurações* > *Painel de Controle*.
2. Clique duas vezes em *Ferramentas Administrativa*s.
3. Clique duas vezes em *Serviços*.
4. Clique o botão direito do mouse em *Gerenciador de Coletor* > *Parar*.

Iniciando o Sentinel Server para Windows

Iniciando o Sentinel Server do Windows

1. Clique em *Iniciar* > *Configurações* > *Painel de Controle*.
2. Clique duas vezes em *Ferramentas Administrativas*.
3. Clique duas vezes em *Serviços*.
4. Na janela Serviços, realce *Sentinel*.
5. Clique o botão direito do mouse em > *Iniciar* ou clique em *Iniciar* na barra de ferramentas.

Parando o Sentinel Server para Windows

Parando o Sentinel Server do Windows

1. Clique em *Iniciar* > *Configurações* > *Painel de Control*e.
2. Clique duas vezes em *Ferramentas Administrativas*.
3. Clique duas vezes em *Serviços*.

4. Na janela Serviços, realce *Sentinel*.
5. Clique o botão direito do mouse em > *Parar* ou clique em *Parar* na barra de ferramentas.

Iniciando o Servidor de Comunicação do Sentinel para Windows

Iniciando o Servidor de Comunicação do Sentinel para Windows

1. Clique em *Iniciar* > *Configurações* > *Painel de Controle*.
2. Clique duas vezes em *Ferramentas Administrativas*.
3. Clique duas vezes em *Serviços*.
4. Na janela Serviços, realce *Comunicação do Sentinel*.
5. Clique o botão direito do mouse em > *Iniciar* ou clique em *Iniciar* na barra de ferramentas.

Parando o Servidor de Comunicação do Sentinel para Windows

Parando o Servidor de Comunicação do Sentinel para Windows

1. Clique em *Iniciar* > *Configurações* > *Painel de Controle*.
2. Clique duas vezes em *Ferramentas Administrativas*.
3. Clique duas vezes em *Serviços*.
4. Na janela Serviços, realce *Comunicação do Sentinel*.
5. Clique o botão direito do mouse em > *Parar* ou clique em *Parar* na barra de ferramentas.

Arquivos de script do Sentinel

Dependendo da configuração da sua instalação, o diretório $ESEC_HOME/sentinel/scripts ou %ESEC_HOME%\sentinel\scripts pode conter alguns ou todos os arquivos de script a seguir:

Arquivo de script:	Descrição:
▪ remove_sonic_lock.bat	Este script remove o(s) arquivo(s) de bloqueio do servidor de comunicação.
▪ start_broker.bat ▪ start_broker.sh	Estes scripts iniciam o servidor de comunicação na linha de comando no modo de console.
▪ stop_broker.bat ▪ stop_broker.sh	Estes scripts param o servidor de comunicação na linha de comando no modo de console.
▪ stop_container.bat ▪ stop_container.sh	Este script reinicie os seguintes containers: ▪ DAS_Aggregation ▪ DAS_RT ▪ DAS_iTRAC ▪ DAS_Binary ▪ DAS_Query
▪ sentinel.sh	Este script pára ou inicia o Sentinel Server. Consulte Iniciando o Sentinel Server do UNIX ou Parando o Sentinel Server do UNIX.

Removendo os arquivos de bloqueio do servidor de comunicação

Caso haja um desligamento inadequado, o servidor de comunicação pode ser bloqueado. Depois de remover os arquivos de bloqueio, você terá que reiniciar o servidor de comunicação. Esses arquivos localizam-se nestes locais:

Windows:

```
%ESEC_HOME%\3rdparty\SonicMQ\MQ6.1\esecDomain\data\_MFSys
   tem\lock
%ESEC_HOME%\3rdparty\SonicMQ\MQ6.1\SonicMQStore\db.lck
```

Para UNIX:

```
$ESEC_HOME/3rdparty/SonicMQ/MQ6.1/esecDomain/data/_MFSyst
   em/lock
$ESEC_HOME /3rdparty/SonicMQ/MQ6.1/SonicMQStore/db.lck
```

Removendo o arquivo de bloqueio do servidor de comunicação (Windows)

1. Usando o Windows Explorer, vá para:

   ```
   %ESEC_HOME%\sentinel\scripts
   ```

2. Clique duas vezes em (através do Windows Explorar) ou execute o seguinte arquivo:

   ```
   remove_sonic_lock.bat
   ```

Removendo o arquivo de bloqueio do servidor de comunicação (UNIX)

1. Em geral, não é necessário remover o arquivo de bloqueio no UNIX porque o arquivo de bloqueio é geralmente removido de forma automática quando se inicia o Sentinel Server. Se esses arquivos precisarem ser removidos manualmente, você deve removê-los usando os comandos típicos do sistema de arquivos do UNIX (como rm).

Iniciando o Servidor de Comunicação no modo de console

Estes scripts iniciam o servidor de comunicação na linha de comando no modo de console. Tais arquivos são úteis para depurar o servidor de comunicação sem forçá-lo a executar o resto do Sentinel Server. Em operações normais, você não deve usar esse script (em vez disso, use as instruções contidas em Iniciando o Sentinel Server do UNIX ou em Iniciando o Sentinel Server para Windows).

Iniciando o servidor de comunicação (Windows)

NOTA: Ao iniciar este script no Windows, ele não terá a indicação como iniciado na janela de Serviços e só será executado se a janela de Prompt de Comando continuar aberta.

1. Usando o Windows Explorer, vá para:

   ```
   %ESEC_HOME%\sentinel\scripts
   ```

2. Clique duas vezes em (através do Windows Explorar) ou execute o seguinte arquivo:

   ```
   start_broker.bat
   ```

Iniciando o Servidor de Comunicação (UNIX)

1. Faça login como usuário esecadm.
2. Use o comando cd para mudar o diretório:

   ```
   $ESEC_HOME/sentinel/scripts
   ```

3. Digite:

   ```
   ./start_broker.sh
   ```

Parando o Servidor de Comunicação no modo de console

Estes scripts param o servidor de comunicação na linha de comando no modo de console. Tais arquivos são úteis para depurar o servidor de comunicação sem forçá-lo a parar o resto do Sentinel Server. Em operações normais, você não deve usar esses scripts (em vez disso, use as instruções contidas em Parando o Sentinel Server do UNIX ou Parando o Sentinel Server para Windows).

Parando o Servidor de Comunicação (Windows)

1. Usando o Windows Explorer, vá para:

   ```
   %ESEC_HOME%\sentinel\scripts
   ```

2. Clique duas vezes em (através do Windows Explorar) ou execute o seguinte arquivo:

   ```
   stop_broker.bat
   ```

Parando o Servidor de Comunicação (UNIX)

1. Faça login como usuário esecadm.
2. Use o comando cd para mudar o diretório:

   ```
   $ESEC_HOME/sentinel/scripts
   ```

3. Digite:

   ```
   ./stop_broker.sh
   ```

Reiniciando os containers do Sentinel

Os scripts a seguir reiniciam os containers listados abaixo. O script envia uma mensagem para o serviço especificado para se desligar. O Sentinel Watchdog reinicia então o serviço.

O método preferido de parar, iniciar ou reiniciar esses serviços de container é usar o Server Views na guia Admin do Sentinel Control Center.

Nome	Descrição
▪ DAS_Aggregation	(das_aggregation.xml) usado para a execução e a configuração do serviço de agregação.
▪ DAS_RT	(das_rt.xml) usado para a execução e a configuração do serviço de exibições em tempo real.
▪ DAS_iTRAC	(das_itrac.xml) usado para configurar o serviço iTRAC.
▪ DAS_Binary	(das_binary.xml) usado para a operação de inserção de evento e evento correlacionado.
▪ DAS_Query	(das_query.xml) todas as outras operações de banco de dados.

Reiniciando o Container do Sentinel (Windows)

1. Use o comando cd para mudar o diretório:

   ```
   %ESEC_HOME%\sentinel\scripts
   ```

2. Digite:

   ```
   stop_container.bat <maquina de host> <nome do
      container>
   ```

   Por exemplo:

   ```
   stop_container.bat localhost DAS_RT
   ```

Reiniciando o Container do Sentinel (UNIX)

1. Faça login como usuário esecadm.
2. Use o comando cd para mudar o diretório:

   ```
   $ESEC_HOME/sentinel/scripts
   ```

3. Digite:

   ```
   ./stop_container <máquina de host> <nome do container>
   ```

   Por exemplo:

   ```
   ./stop_container localhost DAS_RT
   ```

Informações sobre versão

Informações de versão do Sentinel Server

O Sentinel Server tem uma opção de linha de comando para mostrar as informações sobre versão dos seguintes processos:

- Watchdog
- rulelg_checker
- correlation_engine
- data_synchronizer
- query_manager
- DAS

Como obter informações sobre a versão do Sentinel (UNIX)

1. Use o comando cd para mudar o diretório:

   ```
   $ESEC_HOME/sentinel/bin
   ```

2. Digite:

   ```
   ./<process> -version
   ```

   Por exemplo:

   ```
   ./correlation_engine –version
   ```

Como obter informações sobre a versão do Sentinel (Windows)

1. Use o comando cd para mudar o diretório:

   ```
   %ESEC_HOME%\sentinel\bin
   ```

2. Digite:

   ```
   <process> -version
   ```

   Por exemplo:

   ```
   correlation_engine –version
   ```

Informações sobre versão do arquivo .dll e .exe do Sentinel

Como obter informações sobre a versão do arquivo .dll e .exe do Sentinel

1. Usando o comando cd, vá para %ESEC_HOME%.
2. Nos vários subdiretórios diferentes, clique o botão direito do mouse no arquivo .dll ou .exe e selecione propriedades.
3. Clique na guia *Versão*.
4. No painel Nome de item, selecione Versão do produto. O número da versão do arquivo aparecerá no painel Valor.

Informações sobre versão do .jar do Sentinel

Como obter informações sobre a versão do arquivo .jar do Sentinel

1. No Sentinel Server, faça login como o usuário:

   Para UNIX:

   ```
   esecadm
   ```

   No Windows, efetue login como um usuário com direitos no Sentinel Server.

2. Use o comando cd para mudar o diretório:

   Para UNIX:

   ```
   $ESEC_HOME/utilities
   ```

   Windows:

   ```
   %ESEC_HOME%\utilities
   ```

3. Na linha de comando, digite o seguinte:

   Para UNIX:

   ```
   ./versionreader.sh <nome do arquivo jar/caminho>
   ```

   Para Windows

   ```
   versionreader <nome do arquivo jar/caminho>
   ```

Configurando o e-mail do Sentinel

As configurações do e-mail do Sentinel são armazenadas no arquivo execution.properties durante a instalação. Esse arquivo pode ser editado após a instalação. Este arquivo encontra-se na máquina em que o DAS está instalado e localiza-se em:

Windows:

```
%ESEC_HOME%\sentinel\config
```

Para UNIX:

```
$ESEC_HOME/sentinel/config
```

Há dois scripts (mailconfig.sh e mailconfigtest.sh no UNIX e mailconfig.bat e mailconfigtest.bat no Windows) que mudam e testam as configurações de e-mail no arquivo execution.properties. O script mailconfig.* altera as configurações de e-mail, e o script mailconfigtest.* testa as configurações de e-mail. As áreas em negrito são as configurações de e-mail que podem ser alteradas.

Estas são as propriedades em execution.properties:

mail.authentication.user=<dominio\\usuario>	
correlated events retry wait=5000	
mail.smtp.host=<SMTP_HOST>	O host SMTP que será usado para enviar e-mails.
mail.events.max=1000	Número máximo de eventos que serão enviados em um e-mail que é automaticamente acionado pelo mecanismo de correlação. Seu objetivo é limitar o tamanho dos e-mails para os eventos correlacionados que têm um grande conjunto de eventos acionados.
correlated events retry count=10	
mail.address.from=<SMTP_FROM_ADDR>	Endereço de e-mail que aparece no campo De do e-mail enviado do DAS.
mail.authentication.password=<senha>	senha para mail.authentication.user.

Os scripts mailconfig.sh e mailconfig.bat usam os seguintes argumentos:

-host	Nome de host SMTP ou endereço IP
-from	Campo De do e-mail
-user	O usuário de autenticação do e-mail
-password	Senha para o usuário de autenticação do e-mail

NOTA: Não insira sua senha depois do argumento –senha. O sistema lhe pedirá uma nova senha depois que você inserir o comando. A saída de console será mascarada por asteriscos (*).

O arquivo mailconfigtest.sh e mailconfig.bat usa os seguintes argumentos:

-to Endereço de e-mail de destino

Para configurar as propriedades do e-mail no arquivo execution.properties

1. Na máquina em que o DAS foi instalado, mude para o diretório:

   Para UNIX:

   ```
   $ESEC_HOME/sentinel/config
   ```

   Para Windows

   ```
   %ESEC_HOME%\sentinel\config
   ```

2. Execute mailconfig desta maneira:

   Para UNIX:

   ```
   ./mailconfig.sh -host <Servidor SMTP> -from <endereço
      de e-mail de origem> -user <usuário de autenticação
      de e-mail> –password
   ```

   Windows:

   ```
   mailconfig.bat -host <Servidor SMTP> -from <endereço
      de e-mail de origem> -user <usuário de autenticação
      de e-mail> -password
   ```

   Exemplo no UNIX:

   ```
   ./mailconfig.sh -host 10.0.1.14 -from
      meu_nome@dominio.com -user meu_nome_usuario –
      password
   ```

   Exemplo no Windows:

   ```
   mailconfig.bat -host 10.0.1.14 -from
      meu_nome@dominio.com -user meu_nome_usuario –
      password
   ```

   Depois de digitar esse comando, o sistema lhe pedirá uma nova senha.

   ```
   Digite a senha:*********
   Confirme a senha:*********
   ```

   NOTA: Ao usar a opção password, ela deve ser o último argumento.

Para testar as configurações do e-mail no arquivo execution.properties:

1. Na máquina em que o DAS foi instalado, mude para o diretório:

   Para UNIX:

   ```
   $ESEC_HOME/sentinel/config
   ```

   Para Windows

   ```
   %ESEC_HOME%\sentinel\config
   ```

2. Execute mailconfigtest desta maneira:

   Para UNIX:

   ```
   ./mailconfigtest.sh -to <endereço de e-mail de
      destino>
   ```

   Windows:

   ```
   mailconfigtest.bat -to <endereço de e-mail de destino>
   ```

   Se o e-mail for enviado com êxito, será exibida a seguinte mensagem na tela e o e-mail será recebido no endereço de destino.

   ```
   O e-mail foi enviado com êxito!
   ```

   Verifique a caixa de correio do e-mail de destino para confirmar o recebimento da mensagem. A linha de assunto e o conteúdo devem ser:

   ```
   Assunto: Testando a propriedade de e-mail do Sentinel

   Este é um teste da configuração da propriedade de
      e-mail do Sentinel. Se você vir esta mensagem,
      a propriedade de e-mail do Sentinel foi configurada
      corretamente para enviar e-mail
   ```

Atualizando sua chave de licença

Se a chave de licença do Sentinel expirou e a Novell emitiu uma nova, execute o programa da chave de software para atualizar a chave de licença.

Como atualizar a chave de licença (UNIX)

1. Faça login como usuário esecadm.
2. Vá até $ESEC_HOME/utilities.
3. Digite o seguinte comando:

   ```
   ./softwarekey
   ```

4. Digite o número 1 para definir sua chave principal. Pressione Enter.

Como atualizar a chave de licença (Windows)

1. Faça login como um usuário com direitos administrativos.
2. Vá até %ESEC_HOME%\utilities.
3. Digite o seguinte comando:

   ```
   softwarekey.exe
   ```

4. Digite o número 1 para definir sua chave principal. Pressione Enter.

12 Inicialização rápida

NOTA: O termo Agente é intercambiável com Coletor. Mais para a frente, Agentes será referido como Coletores.

Este capítulo discute procedimentos de inicialização rápida para:

- Analistas de segurança
- Analistas de relatório
- Administradores

São discutidos os seguintes tópicos:

- Active Views™
- Detecção de ataques
- Dados de bens
- Consulta de Eventos
- Reportando análise através do CrystalReports
- Correlação Básica

Analistas de segurança

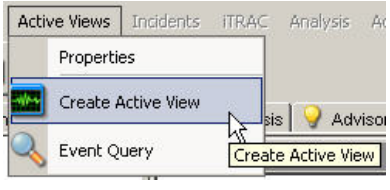
NOTA: Este capítulo presume que seu Administrador de Segurança ou você desenvolveu os filtros necessários e configurou os coletores necessários para seu sistema.

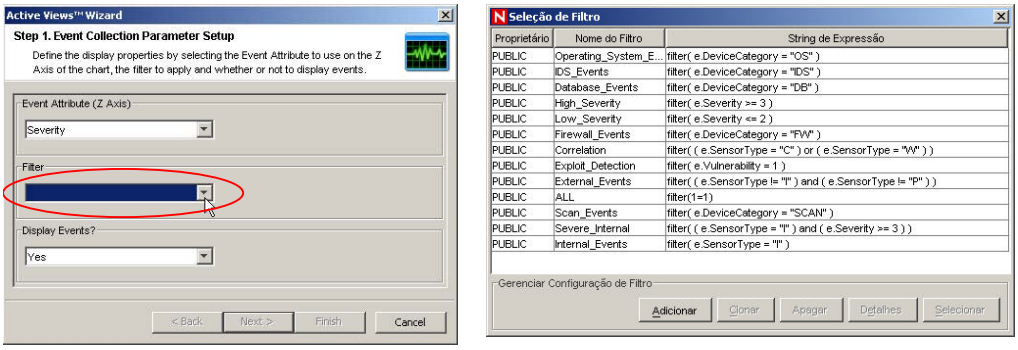
Guia Active Views

Na guia Active Views, você pode monitorar os eventos à medida que acontecem, realizando consultas nesses eventos. Você pode monitorá-los em uma forma de tabela ou através de uma representação gráfica em 3D.

Para iniciar os eventos em tempo real

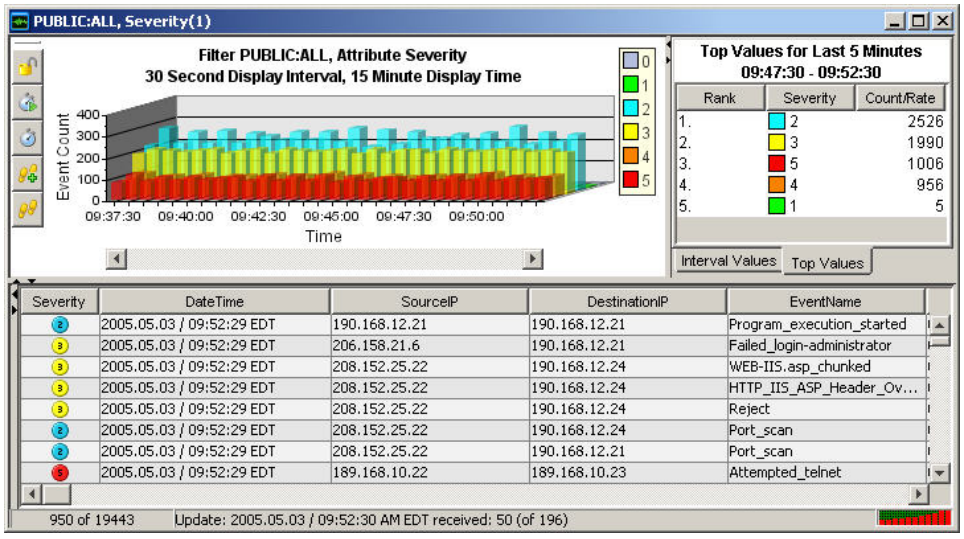
1. Clique em *Active Views* > *Criar Tela Ativa*, clique na seta para baixo do filtro, selecione um filtro e clique em *Selecionar*.





2. Clique em *Concluir*. Se você tiver uma rede ativa, poderá ver algo semelhante a:

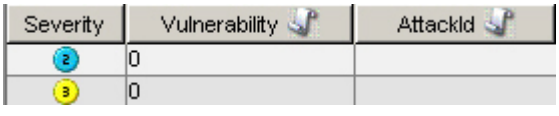
NOTA: Para exibir um gráfico 3D sem eventos em tempo real, clique na seta para baixo de Exibir Eventos e selecione o *Não*.



Detecção de Exploração

Para ver quaisquer eventos indicando uma possível exploração, você deve fazer o seguinte:

- Alimentação do Consultor;
- Detecção de intrusão;
- Verificação de vulnerabilidades; e



Em um evento, quando o campo de vulnerabilidade (*vul*) é igual a 1, o bem ou dispositivo de destino é explorado. Se o campo de vulnerabilidade (*vul*) é igual a 0, o bem ou dispositivo de destino não é explorado. Se o campo de Vulnerabilidade ficar vazio, o recurso de detecção de exploração do Sentinel não é ativo.

Para ver eventos que indiquem uma possível exploração, crie uma Tela Ativa com um filtro onde a Vulnerabilidade seja igual a 1. Se você tiver o Nmap e tiver executado o Coletor Nmap, poderá ver informações de bens no bem explorado ou em qualquer bem.

Para obter mais informações sobre como a detecção de exploração funciona e quais Sistemas de Detecção de Intrusão e Explorações de Vulnerabilidade são suportados, consulte o *Capítulo 1 – Introdução* ou o *Capítulo 10 – Gerenciador de Dados do Sentinel*.

Dados de bens

Para ver informações de Bens para qualquer evento, clique o botão direito do mouse em um evento ou eventos > *Análise* > *Dados de Bens*, uma janela semelhante à janela abaixo será exibida.

Asset Report

desk.acmeinc.net				
Hardware	**MAC Address**	A0:12:56:78:90:00		
	Name	Build Machine	**Value**	500
	Type	Server	**Criticality**	High
	Vendor	Dell	**Sensitivity**	Low
	Product	Precision	**Environment**	Production
	Version	360	**Location**	Internal

Network	**IP**	**Hostname**
	199.16.2.23	desk.acmeinc.net

Software	**Name**	**Type**	**Vendor**	**Product**	**Version**
	ClearCase	APPLICATION	IBM	ClearCase	5.0
	C++	APPLICATION	Microsoft	Visual C++	6.0

Contacts	**Order**	**Name**	**Role**	**Email**	**Phone Number**
	1	Erickson, Stein	USER	serickson@acmedomain.net	(703) 555-8865
	2	IT	Administrator	LAN_FOLKS@acemedomain.net	(703) 555-9876

Location		
	Room	server room
	Rack	#17
	Address	HQ Agent 86 Security Circle Suite 86 Washington DC 12345 USA

Consulta de Eventos

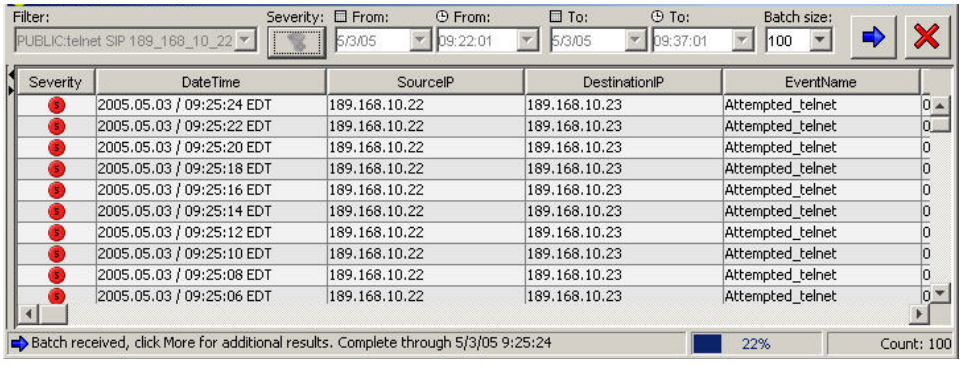
Cenário de exemplo – Durante o monitoramento, você vê inúmeras tentativas de telnet do IP de origem 189.168.10.22. As tentativas de Telnet poderiam ser um ataque. Potencialmente, a Telnet permite que um invasor se conecte remotamente a um computador remoto, como se estivesse conectado localmente. Isso pode levar a alterações não-autorizadas de configuração, instalação de programas, vírus, etc.

Você pode consultar os eventos para determinar com que freqüência esse possível invasor tentou uma telnet; é possível configurar um filtro para pesquisar este invasor em particular. Por exemplo, você sabe o seguinte:

- IP de origem: 189.168.10.22
- IP de Destino: 189.168.10.23
- Severidade: 5
- Nome do evento: Attempted_telnet
- Tipo de sensor: H (Detecção de Intrusão de Host)

Para realizar uma consulta de evento

1. Clique em *Consulta de Eventos* (ícone de lente de aumento) e clique na seta para baixo do campo Filtro.
2. Clique em *Adicionar* e insira o nome de um filtro de "telnet SIP 189_168_10_22". No campo embaixo do filtro, insira:
   - SourceIP = 189.168.10.22
   - EventName = Attempted_telnet
   - Corresponder se, selecione (e)
   - Severidade = 5
   - SensorType = H
   - DestinationIP = 189.168.10.23
3. Clique em *Gravar*. Realce seu filtro e clique em *Selecionar*.
4. Insira seu período de tempo de interesse e clique em *Pesquisar* (ícone de lente de aumento). Os resultados da sua consulta se parecerão com o seguinte:



Se desejar ver com que freqüência este usuário está tentando em geral usar telnet, retire DestinationIP, SensorType e Severidade do filtro ou crie um novo filtro. Os resultados vão mostrar todos os destinationIPs a que este usuário está tentando aplicar telnet.

Se qualquer um dos eventos for um evento correlacionado (SensorType = C ou W), você pode clicar o botão direito do mouse em > *Mostrar Eventos Acionadores* para descobrir quais eventos acionaram aquele evento correlacionado.

Outro evento de interesse poderiam ser os eventos excessivos de FTP. Esta também pode ser uma conexão remota, permitindo a transferência, a cópia e a exclusão de arquivos.

A seguir há uma breve lista de ataques de interesse. Os tipos de ataques são uma lista extensiva. Para obter mais informações sobre ataques de rede/host, há muitos recursos disponíveis (ou seja, livros e a Internet) que explicam tipos diferentes de ataques em detalhes.

- Inundação de SYN
- Inundação de ICMP e UDP
- Farejamento de pacote
- Negação de serviço
- Smurf e Fraggle
- Ataque de dicionário

Analista de relatório

NOTA: Este capítulo presume que seu Administrador de Segurança configurou seu servidor da Web Crystal Enterprise e publicou uma lista de relatórios disponíveis.

Guia Análise

A guia Análise permite a geração de relatórios de históricos. Os relatórios de histórico e vulnerabilidade são publicados em um servidor da Web Crystal, os quais são executados diretamente em relação ao banco de dados do Sentinel. Esses relatórios podem ser úteis para controlar e investigar a atividade em um grande período de tempo, por exemplo, uma semana ou um mês. Eles também podem ser usados como método de relatório de alto nível aos seus supervisores. Caso seu servidor da Web de relatório esteja instalado, olhe na barra do navegador para ver quais relatórios estão disponíveis.

NOTA: a seguir há um exemplo do Crystal 9. Os procedimentos do Crystal 11 são iguais, com nomes de relatório diferentes.

Por exemplo, se você for o responsável pela geração de relatórios para a alta administração na sua organização. É possível que você execute o SourceDestinationReports. Há 10 fontes principais de Pares de IP de Destino nos nomes de hosts, portas, IPs e usuários. Para executar esse relatório, faça o seguinte:

Executando um relatório Crystal

1. Expanda os 10 Primeiros e realce as 10 Primeiras Fontes para Resumo de Pares de IP de Destino e clique no botão *Criar Relatórios* (lente de aumento).
2. Insira esecrpt (para autenticação SQL e Oracle) como nome de usuário ou seu nome de usuário de Autenticação do Windows e insira sua senha.
3. Em Tipo de Relatório, selecione *Relatório Semanal* (selecione Intervalo de Data Específico, se desejar um intervalo de data específico).

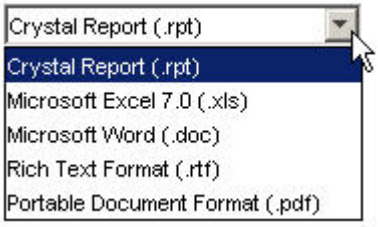
   NOTA: Outros relatórios podem ter parâmetros adicionais, como nome de recurso e intervalo de severidade.
4. Clique em Ver Relatório.

Top 10 Source to Destination IP Pairs: Weekly

Report Description: This report summarizes the Top 10 Pairs of Source IP Addresses and Destination IP Addresses for the **last full week** from all sensors (i.e., event sources) monitored by e-Security Agents.

Source IP	Destination IP	Number of Occurences
206.158.21.6	189.168.10.22	4,174
206.158.23.8	192.168.11.23	2,880
208.152.25.22	190.168.12.21	1,154
10.0.20.5	192.168.0.1	1,152
10.0.20.7	192.168.0.4	579
10.0.20.4	192.168.0.7	577
207.25.71.204	207.25.71.204	576
199.168.10.25	199.168.11.22	576
199.168.10.22	199.168.10.22	576
190.168.12.21	190.168.12.21	576

5. Você pode exportar este arquivo como Word, PDF, rtf, Excel ou como Relatório Crystal clicando em *Exportar* (envelope).



Consulta de Eventos

Semelhante ao Analista de Segurança, se você tiver um evento ou eventos de interesse nos relatórios, poderá executar uma Consulta de Evento na guia Análise. Para realizar uma consulta, realce *Eventos de Histórico* > *Consultas de Evento de Histórico* e clique em *Criar Relatórios* (lente de aumento). Para obter mais informações, consulte Analista de segurança - Exemplo de cenário de consulta de eventos.

Administradores

Correlação Básica

A correlação é o processo de analisar eventos de segurança para identificar relacionamentos em potencial entre dois ou mais eventos. A correlação permite uma rápida associação de ataques prioritários com base em elementos comuns de dados do evento.

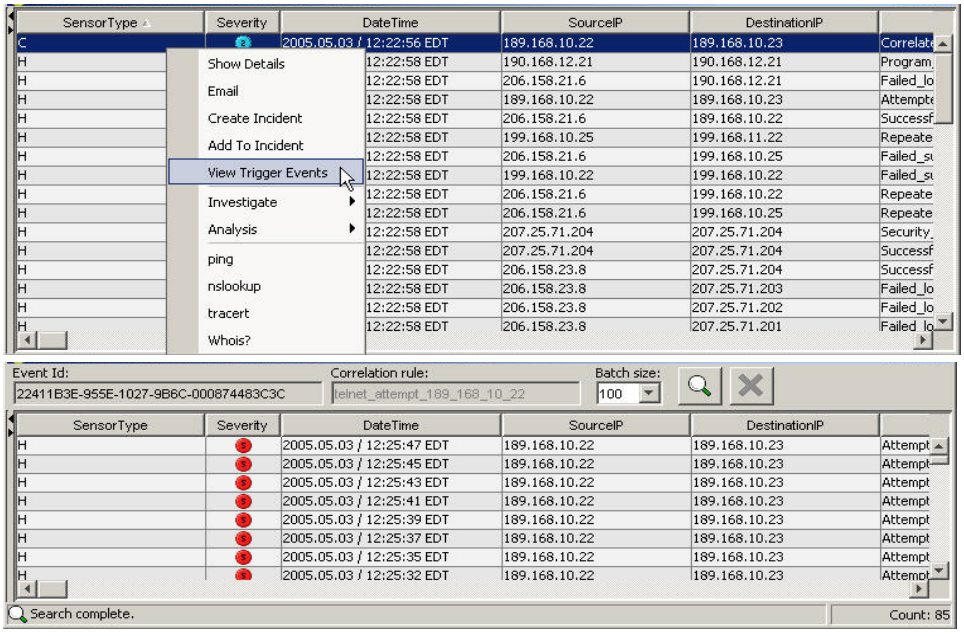
Em referência ao cenário telnet em Analista de segurança - Exemplo de cenário de consulta de eventos, pode-se criar uma Regra de Correlação Básica que acionará um evento correlacionado quando forem feitas quatro tentativas de telnet em um período de 10 segundos.

Para criar uma regra de correlação

1. Vá até a guia Admin e realce as Regras de Correlação na barra de navegação.
2. Crie uma pasta e coloque sua regra nela. Faz-se isso através de uma opção com o botão direito.
3. Realce a Correlação Básica, insira um nome e clique em *Avançar*. No próximo painel, clique na seta para baixo e selecione *Gerenciador de Filtros*. Clique na seta para baixo do filtro selecionado e, no painel de Seleção de Filtros, clique em *Adicionar*.
4. Digite o seguinte:
   - Nome: telnet_attempt_189_168_10_22
   - Nome do filtro: telnet attempt 189_168_10_22
   - SourceIP = 189.168.10.22
   - EventName = Attempted_telnet
   - selecione *And*
   - Severidade = 5
   - SensorType = H
   - DestinationIP = 189.168.10.23

5. Clique em *Gravar*. Realce seu filtro e clique em *Selecionar*.
6. Clique em *Avançar*, insira o valor 4 para quando a condição for atendida e 10 segundos no painel Critérios Agrupamento de Limite. Clique em *Avançar*.
7. No painel Eventos e ações correlacionados, mude o nível de severidade para 2 (clique na seta para baixo). Clique em *Concluir*.
8. Para distribuir esta regra, realce o Gerenciador do Mecanismo de Correlação no painel de navegação, realce um mecanismo de correlação e clique o botão direito do mouse em > *Distribuir Regras*. No painel Distribuir regras, encontre sua regra e marque-a. Clique em *OK*. Certifique-se de que seu Mecanismo de Correlação e sua Regra de Correlação tenham marcas de verificação verdes, indicando que estão ativados. Faz-se isso clicando o botão direito.
9. Há vários métodos diferentes para ver se você correlacionou os eventos.
   Eis alguns métodos:
   - Crie uma janela de Eventos do Active View usando o filtro de correlação você criou
   - Crie uma janela de Eventos do Active View usando o filtro de correlação fornecido
   - Crie uma janela de Eventos do Active View usando o filtro Todos fornecido, tire um instantâneo e classifique por SensorType; veja todos os eventos com SensorType igual a C.
   - Faça uma consulta rápida usando o filtro que você criou ou usando o filtro de correlação.

   Clique o botão direito do mouse no evento correlacionado e selecione *Mostrar Eventos Acionadores* para ver como muitos eventos de telnet (poderiam ser mais de quatro) acionaram essa regra de correlação.



A Eventos de sistema do Sentinel 5

NOTA: O termo Agente é intercambiável com Coletor. Mais adiante, Agentes será referido como Coletores.

Nas tabelas de descrição abaixo, as palavras em itálico entre <...> são substituídas por valores relevantes nas mensagens reais.

Eventos de autenticação

Falha na autenticação

Quando ocorre falha na autenticação do usuário, o seguinte evento é gerado.

Tag	Valor
Gravidade	4
Nome do evento	AuthenticationFailed
Recurso	UserAuthentication
Sub-recurso	Autenticar
Mensagem	Falha na autenticação do usuário <*nome*> com nome de SO <*Usuáriodom*> de <*IP*>

Evento de usuário não existente

Quando um usuário tenta efetuar login no aplicativo e a autenticação é bem-sucedida, mas ele não é um usuário do Sentinel, o seguinte evento é gerado.

Tag	Valor
Gravidade	4
Nome do evento	NoSuchUser
Recurso	UserAuthentication
Sub-recurso	Autenticar
Mensagem	Não foi encontrado nenhum usuário com o nome <*nome*>

Objetos de Usuário Duplicados

Quando há um segundo objeto usuário ativo inesperado (isso não deveria acontecer) o seguinte evento é gerado. Esse é um erro interno.

Tag	Valor
Gravidade	4
Nome do evento	TooManyActiveUsers
Recurso	UserAuthentication
Sub-recurso	Autenticar
Mensagem	Erro na tabela de usuário: foram encontrados vários usuários com o nome <*nome*>

Conta bloqueada

Quando uma conta de usuário é bloqueada durante uma tentativa de efetuar login, o seguinte evento é gerado.

Tag	Valor
Gravidade	4
Nome do evento	LockedUser
Recurso	UserAuthentication
Sub-recurso	Autenticação
Mensagem	Tentativa de login usando conta bloqueada <*conta*>

Sessões do usuário

Usuário efetuou logout

Quando o usuário efetua logout, o seguinte evento interno é gerado.

Tag	Valor
Gravidade	1
Nome do evento	UserLoggedOut
Recurso	UserSessionManager
Sub-recurso	Usuário
Mensagem	Fechando sessão do <*usuário*> nome do OS <*Nome_OS*> de <*IP*> ativado desde <*data*>; no momento <*núm*> usuários ativos

Usuário efetuou login

Quando o usuário efetua login, o seguinte evento interno é gerado.

Tag	Valor
Gravidade	1
Nome do evento	UserLoggedIn
Recurso	UserSessionManager
Sub-recurso	Usuário
Mensagem	Usuário <*usuário*> com nome do OS <*Nome_OS*> em <*IP*> efetuou login; no momento <*núm*> usuários ativos

Usuário descoberto

Se for reiniciado, o servidor perderá as informações da sessão. Ele reconstruirá a sessão quando receber mensagens de usuários ativos. Quando o servidor descobrir um usuário conectado, o seguinte evento interno será gerado.

Tag	Valor
Gravidade	1
Nome do evento	UserLoggedIn
Recurso	UserSessionManager
Sub-recurso	Usuário
Mensagem	Usuário ativo descoberto <*usuário*> com nome do OS <*Nome_OS*> em <*IP*> efetuou login; no momento <*núm*> usuários ativos

Evento

Erro ao mover arquivo concluído

Tão logo é concluído, um arquivo de evento é movido para o diretório de saída. Se houver falha nessa movimentação, o seguinte evento interno será gerado.

Tag	Valor
Gravidade	3
Nome do evento	MoveArchiveFileFailed
Recurso	<*Nome DAS*>
Sub-recurso	ArchiveFile
Mensagem	Erro ao mover arquivo concluído <*nome_arq*> para <*dir*>

Erro ao inserir eventos

Quando ocorre falha na inserção de eventos no banco de dados, o seguinte evento interno é gerado.

Tag	Valor
Gravidade	5
Nome do evento	InsertEventsFailed
Recurso	EventSubsystem
Sub-recurso	Eventos
Mensagem	Erro ao inserir eventos no banco de dados. Os eventos serão permanentemente perdidos. Verifique os logs do banco de dados e do servidor backend <*Exceção*>

Falha ao abrir arquivo

Quando ocorre falha na abertura do arquivo que armazena os eventos de agregação, o seguinte evento interno é gerado.

Tag	Valor
Gravidade	3
Nome do evento	OpenArchiveFileFailed
Recurso	<*Nome DAS*>
Sub-recurso	ArchiveFile
Mensagem	Erro ao abrir arquivo <*nome*> em <*dir*>

Falha na gravação do arquivo

Quando ocorre falha na abertura do arquivo que armazena os eventos de agregação, o seguinte evento interno é gerado.

Tag	Valor
Gravidade	3
Nome do evento	WriteArchiveFileFailed
Recurso	<*Nome DAS*>
Sub-recurso	ArchiveFile
Mensagem	Erro ao gravar eventos recém-recebidos no arquivo de agregação <*nome_arq*>

Gravando na partição de overflow (P_MAX)

Um evento é enviado a cada 5 minutos, aproximadamente, notificando o usuário dos eventos que estão sendo gravados na partição de overflow (P_MAX). Quando isso ocorre, o administrador precisa usar o SDM e adicionar mais partições. Do contrário, haverá uma queda no desempenho.

Tag	Valor
Gravidade	5
Nome do evento	InsertIntoOverflowPartition
Recurso	EventSubSystem
Sub-recurso	Eventos
Mensagem	Erro: as partições de overflow estão recebendo dados (P_MAX), adicionar mais partições

Inserção de evento bloqueada

Se o DAS estiver gravando em uma partição de overflow e o usuário tentar adicionar partições, o SDM enviará uma solicitação para o DAS parar temporariamente de inserir eventos no banco de dados. Quando isso acontece, o DAS envia eventos internos cada vez que tenta inserir eventos no banco de dados.

Tag	Valor
Gravidade	4
Nome do evento	EventInsertionIsBlocked
Recurso	EventSubSystem
Sub-recurso	Eventos
Mensagem	Inserção de evento bloqueada, aguardando <*núm*> segundos

Inserção de evento retomada

Quando a inserção de eventos é retomada após um bloqueio, o seguinte evento é enviado.

Tag	Valor
Gravidade	2
Nome do evento	EventInsertionResumed
Recurso	EventSubSystem
Sub-recurso	Eventos
Mensagem	Inserção de evento retomada após bloqueio

Espaço do banco de dados atingiu limite de tempo especificado

Quando a inserção de eventos é retomada após um bloqueio, o seguinte evento é enviado.

Tag	Valor
Gravidade	0
Nome do evento	DbSpaceReachedTimeThrshld
Recurso	Banco de Dados
Sub-recurso	Banco de Dados
Mensagem	Tabela <*string*> tem <*núm*> MB restante(s) e aumenta em<*núm*> bytes por segundo; ficará sem espaço disponível no limite de tempo especificado: <*núm*> segundos

Espaço do banco de dados atingiu limite de porcentagem especificado

Quando a inserção de eventos é retomada após um bloqueio, o seguinte evento é enviado.

Tag	Valor
Gravidade	0
Nome do evento	DbSpaceReachedPercentThrshld
Recurso	Banco de Dados
Sub-recurso	Banco de Dados
Mensagem	No momento, o tamanho da tabela <*string*> é de <*núm*> MB com um máx de <*núm*> MB e alcançou o limite de porcentagem de <*núm*> %

Espaço do banco de dados muito baixo

Quando a inserção de eventos é retomada após um bloqueio, o seguinte evento é enviado.

Tag	Valor
Gravidade	5
Nome do evento	DbSpaceVeryLow
Recurso	Banco de Dados
Sub-recurso	Banco de Dados
Mensagem	No momento, o tamanho da tabela <*string*> é de <*núm*> MB e alcançou o limite físico de <*núm*> MB

Agregação

Erro ao inserir dados de resumo no banco de dados

Se for encontrado um erro durante a gravação dos dados de agregação no banco de dados, o seguinte evento interno será gerado.

Tag	Valor
Gravidade	4
Nome do evento	SummaryUpdateFailure
Recurso	Agregação
Sub-recurso	Resumo
Mensagem	Erro ao gravar lote do resumo <*nome_resumo*> no banco de dados

Serviço de Mapeamento

Erro ao iniciar mapeamento com o ID

Esse evento interno é gerado do lado do cliente do serviço de mapeamento (aquele que faz parte do Gerenciador de Coletor). Esse erro é gerado quando o Gerenciador de Coletor tenta recuperar um mapa que não existe. Isso não deve acontecer, mas é possível caso os mapas sejam criados e apagados.

Tag	Valor
Gravidade	4
Nome do evento	ErrorNoSuchMap
Recurso	MappingService
Sub-recurso	ReferentialDataObjectMap
Mensagem	Erro ao iniciar mapa com o id <ID>: esse mapa não existe

Atualizando mapa do cache

Esse evento interno é gerado do lado do cliente do serviço de mapeamento (aquele que faz parte do Gerenciador de Coletor). Quando o Gerenciador de Coletor recebe uma solicitação para atualizar o mapa porque este foi modificado ou teve sua definição alterada, o gerenciador envia um evento interno. Desse modo, seu cache ficará em dia com a atualização do mapa do cache.

Tag	Valor
Gravidade	1
Nome do evento	LoadingMapFromCache
Recurso	MappingService
Sub-recurso	ReferentialDataObjectMap
Mensagem	Carregando do cache v<*versão*> do mapa <*Nome_mapa*> (ID <*id*>)

Atualizando mapa do servidor

Esse evento interno é gerado do lado do cliente do serviço de mapeamento (aquele que faz parte do Gerenciador de Coletor). Quando o Gerenciador de Coletor recebe uma solicitação para atualizar o mapa porque este foi modificado ou teve sua definição alterada, o gerenciador envia um evento interno. Isso significa que o mapa não está no cache ou que a versão no cache não está atualizada e o Gerenciador de Coletor está recuperando o mapa do servidor.

Tag	Valor
Gravidade	1
Nome do evento	RefreshingMapFromServer
Recurso	MappingService
Sub-recurso	ReferentialDataObjectMap
Mensagem	Atualizando com base no mapa do servidor <nome> com id <ID>

Tempo esgotado na atualização do mapa

Esse evento interno é gerado do lado do cliente do serviço de mapeamento (aquele que faz parte do Gerenciador de Coletor). Quando o Gerenciador de Coletor recebe uma solicitação para atualizar o mapa porque este foi modificado ou teve sua definição alterada, o gerenciador envia um evento interno. Isso significa que o Gerenciador de Coletor tentou recuperar o mapa do servidor e, como este não reconheceu a solicitação, o tempo esgotou-se. Esse erro é considerado transitório e o Gerenciador de Coletor tentará novamente.

Tag	Valor
Gravidade	4
Nome do evento	TimeoutRefreshingMap
Recurso	MappingService
Sub-recurso	ReferentialDataObjectMap
Mensagem	Tempo da solicitação esgotado durante a atualização do mapa <nome>: <exceção>

Erro na atualização do mapa

Esse evento interno é gerado do lado do cliente do serviço de mapeamento (aquele que faz parte do Gerenciador de Coletor). Quando o Gerenciador de Coletor recebe uma solicitação para atualizar o mapa porque este foi modificado ou teve sua definição alterada, o gerenciador envia um evento interno. Isso significa que houve um erro não transitório inesperado durante a tentativa de atualizar o mapa. O Gerenciador de Coletor aguardará 15 minutos e tentará novamente. Se isso acontecer durante a inicialização, esta continuará e esse mapa será ignorado até que possa ser carregado com êxito.

Tag	Valor
Gravidade	4
Nome do evento	ErrorRefreshingMapData
Recurso	MappingService
Sub-recurso	ReferentialDataObjectMap
Mensagem	Erro na atualização do mapa <*Nome_mapa*>: <*exc*>

Mapa muito grande carregado

Esse evento interno é um evento de informação enviado pelo serviço de mapeamento notificando que um mapa muito grande foi carregado no Gerenciador de Coletor. Um mapa é considerado grande quando o número de linhas ultrapassa 100.000.

Tag	Valor
Gravidade	0
Nome do evento	LoadedLargeMap
Recurso	MappingService
Sub-recurso	ReferentialDataObjectMap
Mensagem	Carga do mapa concluída <nome> com id <ID> e <núm> entradas. Tamanho total <#>Kb em <##>segundos

Tempo excessivo para carregar o mapa

Esse evento interno é um evento de informação enviado pelo serviço de mapeamento notificando que o tempo de carregamento de um mapa ultrapassou o tempo normalmente necessário (mais de um minuto).

Tag	Valor
Gravidade	0
Nome do evento	LongTimeToLoadMap
Recurso	MappingService
Sub-recurso	ReferentialDataObjectMap
Mensagem	O carregamento do mapa demorou <##> segundos com id <ID> e <núm> entradas. Tamanho total <#>Kb

TimedoutWaitingForCallback

Quando precisa atualizar um mapa, o Gerenciador de Coletor envia uma solicitação para o backend. Essa solicitação contém um callback. O backend gera o mapa e quando este está pronto, o backend o envia para o Gerenciador de Coletor usando o callback. Se a resposta demorar muito (mais de dez minutos) para chegar, o Gerenciador de Coletor enviará uma segunda solicitação presumindo que a primeira se perdeu. Quando isso ocorre, o seguinte evento interno é gerado.

Tag	Valor
Gravidade	2
Nome do evento	TimedoutWaitingForCallback
Recurso	MappingService
Sub-recurso	ReferentialDataObjectMap
Mensagem	Mapa <nome> esgotou o tempo de espera para o callback com novos dados do mapa. Tentando novamente.

ErrorApplyingIncrementalUpdate

Esse evento é enviado quando o serviço de mapeamento não consegue aplicar uma atualização a um mapa de cliente existente.

Tag	Valor
Gravidade	4
Nome do evento	ErrorApplyingIncrementalUpdate
Recurso	MappingService
Sub-recurso	ReferentialDataObjectMap
Mensagem	O erro <erro> ocorreu durante a aplicação de atualizações ao mapa <*Nome_mapa*> (ID <*Id_mapa*>) v.<*versão*>. Reprogramando atualização para concluir a atualização do mapa.

OutOfSyncDetected

Esse evento é enviado quando o serviço de mapeamento detecta um mapa desatualizado. O serviço de mapeamento programará uma atualização automaticamente.

Tag	Valor
Gravidade	2
Nome do evento	OutOfsyncDetected
Recurso	MappingService
Sub-recurso	ReferentialDataObjectMap
Mensagem	Mapa <*Nome_mapa*> detectou dados do mapa fora de sincronismo, provavelmente devido à ausência de notificação de atualização. Programando uma atualização.

Roteador de Evento

Roteador de Evento em execução

O roteador de evento é o principal componente do Gerenciador de Coletor (aquele que executa os mapas, aplica filtros globais e publica os eventos). Esse evento interno é enviado quando o roteador de evento está pronto durante a inicialização. Quando o Gerenciador de Coletor for reiniciado, outro evento será enviado quando estiver pronto.

Esse evento não será enviado até o roteador carregar com êxito todos os filtros globais e informações de mapas.

Tag	Valor
Gravidade	1
Nome do evento	EventRouterIsRunning
Recurso	AgentManager
Sub-recurso	EventRouter
Mensagem	Roteador de evento concluiu sua inicialização no modo <modo>

Roteador de Evento em inicialização

Esse evento é enviado quando um evento está em inicialização. O roteador de evento começa a inicialização assim que estabelece uma conexão com o backend (Consulta DAS).

Tag	Valor
Gravidade	1
Nome do evento	EventRouterInitializing
Recurso	AgentManager
Sub-recurso	EventRouter
Mensagem	Roteador de evento em inicialização no modo <modo>

Roteador de Evento sendo interrompido

Esse evento é enviado quando o roteador de evento recebe uma solicitação de interrupção durante o encerramento.

Tag	Valor
Gravidade	2
Nome do evento	EventRouterStopping
Recurso	AgentManager
Sub-recurso	EventRouter
Mensagem	Roteador de evento em interrupção

Roteador de Evento sendo terminado

Esse evento é enviado quando o roteador de evento recebe uma solicitação de interrupção durante o encerramento.

Tag	Valor
Gravidade	2
Nome do evento	EventRouterTerminating
Recurso	AgentManager
Sub-recurso	EventRouter
Mensagem	Roteador de evento em terminação

Mecanismo de Correlação

Mecanismo de Correlação em execução

O processo do mecanismo de correlação pode ser desativado pelo usuário. Seu estado em execução determina se o processo ativo está processando ou não os eventos. O processo inicia no estado inativo (interrompido) e aguarda a recuperação de sua configuração do banco de dados. Esse evento é enviado quando o mecanismo muda do estado interrompido para em execução.

Tag	Valor
Gravidade	1
Nome do evento	EngineRunning
Recurso	CorrelationEngine
Sub-recurso	CorrelationEngine
Mensagem	Mecanismo de Correlação processando eventos.

Mecanismo de Correlação interrompido

Esse evento é enviado quando o mecanismo muda do estado em execução para interrompido.

Tag	Valor
Gravidade	1
Nome do evento	EngineStopped
Recurso	CorrelationEngine
Sub-recurso	CorrelationEngine
Mensagem	Mecanismo de Correlação parou de processar eventos.

Distribuição de regra iniciada

Esse evento é enviado quando um mecanismo carrega uma distribuição de regra com êxito. Essa mensagem é enviada independentemente do estado de execução do mecanismo.

Tag	Valor
Gravidade	1
Nome do evento	DeploymentStarted
Recurso	CorrelationEngine
Sub-recurso	Distribuição
Mensagem	Distribuição <nome> iniciada

Distribuição de regra interrompida

Esse evento é enviado quando um mecanismo descarrega uma distribuição de regra com êxito. Essa mensagem é enviada independentemente do estado de execução do mecanismo.

Tag	Valor
Gravidade	1
Nome do evento	DeploymentStopped
Recurso	CorrelationEngine
Sub-recurso	Distribuição
Mensagem	Distribuição <nome> interrompida

Distribuição de regra modificada

Esse evento é enviado quando um mecanismo recarrega uma distribuição de regra com êxito. Essa mensagem é enviada independentemente do estado de execução do mecanismo.

Tag	Valor
Gravidade	1
Nome do evento	DeploymentModified
Recurso	CorrelationEngine
Sub-recurso	Deployment
Mensagem	Distribuição <nome> modificada

WatchDog

Processo controlado iniciado

Watchdog é executado como um serviço. Sua finalidade principal é manter os processos do Sentinel em execução. Se um processo é desativado, o Watchdog reiniciará automaticamente esse processo. Esse evento é enviado quando um processo é iniciado.

Tag	Valor
Gravidade	1
Nome do evento	ProcessStart
Recurso	WatchDog
Sub-recurso	Processo
Mensagem	Processo <Nome_programa> inicializado (<pid>)

Processo controlado interrompido

Esse evento é enviado quando um processo é interrompido. A gravidade é definida como 5 se o processo foi enviado para reinicialização (ou seja, o processo não deve ser desativado). A gravidade é definida como 1 se o processo foi enviado para execução uma vez.

Tag	Valor
Gravidade	1/5
Nome do evento	ProcessStop
Recurso	WatchDog
Sub-recurso	Processo
Mensagem	Processo <Nome_Programa> encerrado com código <código_saída>

Processo Watchdog iniciado

Quando o processo Watchdog é iniciado, o seguinte evento interno é gerado.

Tag	Valor
Gravidade	1
Nome do evento	ProcessStart
Recurso	WatchDog
Sub-recurso	WatchDog
Mensagem	Serviço Watchdog em inicialização

Processo Watchdog interrompido

Quando o serviço Watchdog é interrompido, o seguinte evento interno é gerado.

Tag	Valor
Gravidade	5
Nome do evento	ProcessStop
Recurso	WatchDog
Sub-recurso	WatchDog
Mensagem	Serviço Watchdog terminado

Gerenciador/Mecanismo de Coletores

Inicialização de porta

O Gerenciador de Coletor envia esse evento quando a porta é iniciada.

Tag	Valor
Gravidade	1
Nome do evento	PortStart
Recurso	AgentManager
Sub-recurso	AgentManager
Mensagem	Processamento iniciado para porta_<id_porta>

Interrupção da porta

O Gerenciador de Coletor envia esse evento quando a porta é interrompida.

Tag	Valor
Gravidade	1
Nome do evento	PortStop
Recurso	AgentManager
Sub-recurso	AgentManager
Mensagem	Processamento interrompido para porta_<id_porta>

Processo persistente desativado

O Mecanismo de Coletores envia esse evento quando o conector do processo persistente detecta seu processo controlado desativado.

Tag	Valor
Gravidade	5
Nome do evento	PersistentProcessDied
Recurso	AgentManager
Sub-recurso	AgentManager
Mensagem	Processo persistente na porta <id_porta) desativado

Processo persistente reiniciado

O Mecanismo de Coletores envia esse evento quando o conector do processo persistente consegue reiniciar o processo controlado que estava desativado.

Tag	Valor
Gravidade	1
Nome do evento	PersistentProcessRestarted
Recurso	AgentManager
Sub-recurso	AgentManager
Mensagem	Processo persistente na porta <id_porta) reiniciado

Serviço de Evento

Dependência cíclica

O Serviço de Evento envia esse evento quando detecta um ciclo na Definição do Evento (nas dependências entre tags em virtude das atribuições de mapas de referência). Verifique a configuração do evento no SDM e resolva a dependência.

Tag	Valor
Gravidade	5
Nome do evento	CyclicalDependency
Recurso	EventService
Sub-recurso	ObjectAttrInfos
Mensagem	Dependência cíclica detectada nas transformações do evento. Verifique a configuração do evento.

Active Views

Tela Ativa criada

DAS_Binary envia esse evento quando uma Tela Ativa é criada.

Tag	Valor
Gravidade	1
Nome do evento	RtChartCreated
Recurso	RealTimeSummaryService
Sub-recurso	ChartManager
Mensagem	Criando nova Tela Ativa com filtro <filtro> e atributo <atributo> para usuários com filtro de segurança <filtro de segurança>. No momento, <nº> Tela(s) Ativa(s) em coleta.

Ingresso em Tela Ativa

DAS_Binary envia esse evento quando um usuário estabelece conexão com uma Tela Ativa existente.

Tag	Valor
Gravidade	1
Nome do evento	RtChartJoiningExistingData
Recurso	RealTimeSummaryService
Sub-recurso	ChartManager
Mensagem	Ingressando em Tela Ativa existente com filtro <filtro> e atributo <atributo> para usuários com filtro de segurança <filtro de segurança>. No momento, <nº> Tela(s) Ativa(s) em coleta.

Tela Ativa inativa removida

DAS_Binary envia esse evento quando uma Tela Ativa não permanente é removida em virtude de inatividade.

Tag	Valor
Gravidade	1
Nome do evento	RtChartInactiveAndRemoved
Recurso	RealTimeSummaryService
Sub-recurso	ChartManager
Mensagem	Tela Ativa desativada com filtro <filtro> e atributo <atributo> para usuários com filtro de segurança <filtro de segurança>. No momento, <nº> Tela(s) Ativa(s) em coleta.

Tela Ativa permanente inativa Removida

DAS_Binary envia esse evento quando uma Tela Ativa permanente é removida em virtude de inatividade. Telas Ativas permanentes são aquelas gravadas nas preferências do usuário e expiradas após vários dias de inatividade por padrão.

Tag	Valor
Gravidade	1
Nome do evento	RtPermanentChartRemoved
Recurso	RealTimeSummaryService
Sub-recurso	ChartManager
Mensagem	Tela Ativa permanente inativa com filtro <filtro> e atributo <atributo> para usuários com filtro de segurança <filtro de segurança>. No momento, <nº> Tela(s) Ativa(s) em coleta.

Tela Ativa agora permanente

DAS_Binary envia esse evento quando detecta uma Tela Ativa que acabou de se tornar permanente. Essa verificação acontece periodicamente, portanto pode ser feita vários minutos após a gravação da Tela Ativa nas preferências antes da geração desse evento.

Tag	Valor
Gravidade	1
Nome do evento	RtChartIsNowPermanent
Recurso	RealTimeSummaryService
Sub-recurso	ChartManager
Mensagem	Tela Ativa com filtro <filtro> e atributo <atributo> para usuários com filtro de segurança <filtro de segurança> agora é permanente.

Tela Ativa não é mais permanente

DAS_Binary envia esse evento quando detecta uma Tela Ativa anteriormente permanente e que deixou de sê-lo. Essa verificação acontece periodicamente, portanto pode ser feita vários minutos após a remoção da Tela Ativa das preferências antes da geração desse evento.

Tag	Valor
Gravidade	1
Nome do evento	RtChartNotPermanent
Recurso	RealTimeSummaryService
Sub-recurso	ChartManager
Mensagem	Tela Ativa com filtro <filtro> e atributo <atributo> para usuários com filtro de segurança <filtro de segurança> não mais permanente.

Resumo

Nome do evento	Gravidade	Origem	Sub-recurso	Componente
AuthenticationFailed	4	UserAuthentication	Autenticar	Autenticação
NoSuchUser	4	UserAuthentication	Autenticar	Autenticação
TooManyActiveUsers	4	UserAuthentication	Autenticar	Autenticação
LockedUser	4	UserAuthentication	Autenticar	Autenticação
UserLoggedOut	1	UserSessionManager	Usuário	Sessão do Usuário
UserLoggedIn	1	UserSessionManager	Usuário	Usuário
UserLoggedIn	1	UserSessionManager	Usuário	Usuário
MoveArchiveFileFailed	3	*Nome DAS*	ArchiveFile	Evento
InsertEventsFailed	5	EventSubSystem	Eventos	Evento
OpenArchiveFileFailed	3	*Nome DAS*	ArchiveFile	Evento
WriteArchiveFileFailed	3	*Nome DAS*	ArchiveFile	Evento
SummaryUpdateFailure	4	Agregação	Resumo	Agregação
InsertIntoOverflowPartition	5	EventSubSystem	Eventos	Evento
EventInsertionIsBlocked	4	EventSubSystem	Eventos	Evento
EventInsertionResumed	2	EventSubSystem	Eventos	Evento
EventRouterIsRunning	1	AgentManager	EventRouter	EventRouter
EventRouterInitializing	1	AgentManager	EventRouter	EventRouter
EventRouterStopping	2	AgentManager	EventRouter	EventRouter
EventRouterTerminating	2	AgentManager	EventRouter	EventRouter
ErrorNoSuchMap	4	MappingService	ReferentialDataObjectMap	Mapeamento
LoadingMapFromCache	1	MappingService	ReferentialDataObjectMap	Mapeamento
RefreshingMapFromServer	1	MappingService	ReferentialDataObjectMap	Mapeamento
TimeoutRefreshingMapData	4	MappingService	ReferentialDataObjectMap	Mapeamento
ErrorRefreshingMapData	4	MappingService	ReferentialDataObjectMap	Mapeamento
LoadedLargeMap	0	MappingService	ReferentialDataObjectMap	Mapeamento
LongTimeToLoadMap	0	MappingService	ReferentialDataObjectMap	Mapeamento

Nome do evento	Gravidade	Origem	Sub-recurso	Componente
TimedoutWaitingForCallback	2	MappingService	ReferentialDataObjectMap	Mapeamento
ErrorApplyingIncrementalUpdate	4	MappingService	ReferentialDataObjectMap	Mapeamento
OutOfSyncDetected	2	MappingService	ReferentialDataObjectMap	Mapeamento
EngineRunning	1	CorrelationEngine	CorrelationEngine	
EngineStopped	1	CorrelationEngine	CorrelationEngine	
DeploymentStarted	1	CorrelationEngine	Deployment	
DeploymentStopped	1	CorrelationEngine	Deployment	
DeploymentModified	1	CorrelationEngine	Deployment	
ProcessStart	1	WatchDog	Processo	
ProcessStop	1/5	WatchDog	Processo	
ProcessStart	1	WatchDog	WatchDog	
ProcessStop	5	WatchDog	WatchDog	
PortStart		AgentManager	AgentManager	
PortStop		AgentManager	AgentManager	
PersistentProcessDied	5	AgentManager	AgentManager	
PersistentProcessRestarted	1	AgentManager	AgentManager	
SortDependencies	5	EventService	ObjectAttrInfo	EventService
DbSpaceReachedTimeThrshld	0	Database	Database	Evento
DbSpaceReachedPercentThrshld	0	Database	Database	Evento
DbSpaceVeryLow	5	Database	Database	Evento
RtChartCreated	1	RealTimeSummaryService	ChartManager	Active Views
RtChartJoiningExistingData	1	RealTimeSummaryService	ChartManager	Active Views
RtChartInactiveAndRemoved	1	RealTimeSummaryService	ChartManager	Active Views
RtChartPermanentAndRemoved	1	RealTimeSummaryService	ChartManager	Active Views
RtChartIsNowPermanent	1	RealTimeSummaryService	ChartManager	Active Views
RtChartNotPermanent	1	RealTimeSummaryService	ChartManager	Active Views