Novell® Sentinel™

5.1.3

7 de julho
de 2006

www.novell.com

Volume III – GUIA DO USUÁRIO
DO ASSISTENTE DO SENTINEL™ 5

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
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.

Índice

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 do Sentinel 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
- Advisor

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 Sentinel
- 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 Assistente
- Coletores
- Gerenciamento de Host do Assistente
- Construção e manutenção de coletores

Volume IV – Guia de Referência do Usuário do Sentinel

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

1 Introdução ao Assistente

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

O Guia do Usuário do Assistente serve de introdução à operação do Assistente da Novell. Este guia explica cada componente e a operação de todos os componentes.

Este guia supõe que você está familiarizado com segurança de rede, administração de bancos de dados e dos sistemas operacionais Windows e UNIX.

Índice

Este guia contém os seguintes capítulos:

- Capítulo 1 – Introdução ao Assistente
- Capítulo 2 – Gerenciando hosts do Assistente
- Capítulo 3 – Construindo e mantendo Coletores
- Apêndice A – Conector Syslog
- Apêndice B – Configurando um servidor de soquete em um host UNIX
- Apêndice C – Informações legais

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
```

Assistente

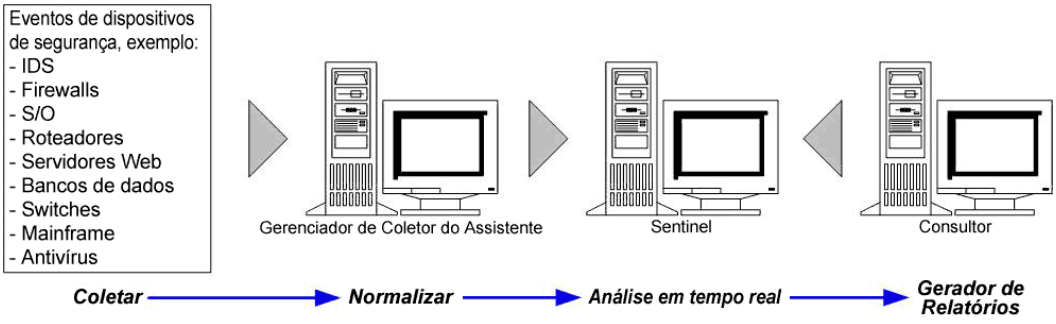
O Assistente permite construir, configurar e controlar Coletores. Os Coletores são usados para coletar e normalizar eventos de dispositivos e programas de segurança. Em seguida, esses eventos normalizados são enviados ao Sentinel para uso na correlação de análise em tempo real, nos relatórios e na resposta a incidentes.

NOTA: Embora não seja um requisito, recomenda-se que em uma configuração múltipla de Construtor de Coletor do Assistente um Construtor de Coletor seja designado como o Construtor Principal. Essa máquina passa a ser usada para armazenar, desenvolver ou modificar coletores e configurar portas.

Os componentes a seguir compõem o Assistente:

- O Construtor de Coletor é a interface do usuário do Assistente que permite construir, configurar, distribuir e controlar coletores. Além de executar coletores em nível local, o Construtor de Coletor pode ser usado para upload, download e controle de coletores em sistemas remotos.
- O Gerenciador de Coletor é o back end do Assistente que gerencia os coletores e as mensagens de status do sistema e executa a filtragem global de eventos.

Coletor é o receptor que coleta e normaliza eventos iniciais de dispositivos e programas de segurança e que possibilita a saída de eventos normalizados que podem ser correlacionados, informados e usados para resposta a incidentes. O software Sentinel vem com coletores do nível da camada 1. Visite o Sentinel Customer Portal para fazer download de coletores adicionais: http://www.esecurityinc.com/.



Coletores

Os coletores são usados para filtrar e padronizar dados de eventos críticos em um formato normalizado e disponibilizá-lo ao processo do Sentinel. Existem três níveis de Coletores, mostrados a seguir:

- Coletores Suportados (T1) – trata-se de coletores:
  - documentados
  - dotados de metadados
  - disponíveis a todos os clientes
  - com Suporte Técnico
- Coletores Documentados (T2) – trata-se de coletores:
  - destinados à biblioteca de coletores
  - documentados
  - dotados de metadados
  - baseados em gabaritos padrão do Sentinel
  - com Suporte Técnico limitado

- Coletores de Exemplo (T3) – trata-se de coletores:
  - dotados de prova de conceito
  - desenvolvidos para um cliente específico
  - que podem não ter metadados nem documentação suportada
  - com Suporte Técnico limitado

Os coletores permitem o acesso a dados de eventos de qualquer origem, inclusive:

- Sistemas de detecção de intrusão (host)
- Sistemas de detecção de intrusão (rede)
- Firewalls.
- Sistemas operacionais
- Monitoramento de políticas
- Autenticação
- Roteadores e Switches
- VPN
- Antivírus
- Servidores da web
- Banco de dados
- Mainframe
- Avaliação de vulnerabilidade
- Serviços de diretório
- Gerenciador de Redes
- Sistemas proprietários

Os coletores são constituídos de:

- Arquivos de gabarito
- Arquivos de parâmetro
- Arquivos de pesquisa
- Arquivos de mapeamento
- Arquivo de descrição de parâmetros e arquivos de manifesto

O arquivo de gabarito e o arquivo de parâmetro associado a ele são fundidos em diferentes arquivos de script quando o Script do Coletor é criado.

Cada arquivo de script é nomeado de acordo com o nome da coluna do conjunto de valores do arquivo de parâmetro. Os arquivos de script são agrupados em seqüência ordenada, em seqüências de inicialização e de backout.

As seqüências de inicialização e backout são atribuídas a uma porta, que executa a série de scripts que ela contém quando é iniciada ou interrompida. Um script deve ser incluído em uma seqüência de inicialização ou backout para ser usado por uma porta. As portas possibilitam que um coletor localize os hosts do Assistente na rede, fornecendo o endereço IP ou nome de arquivo desses hosts. Elas também fornecem ao Sentinel informações sobre a localização de sensores e o Coletor usado para gerenciar dados desses sensores.
As opções a seguir são configuráveis para portas:

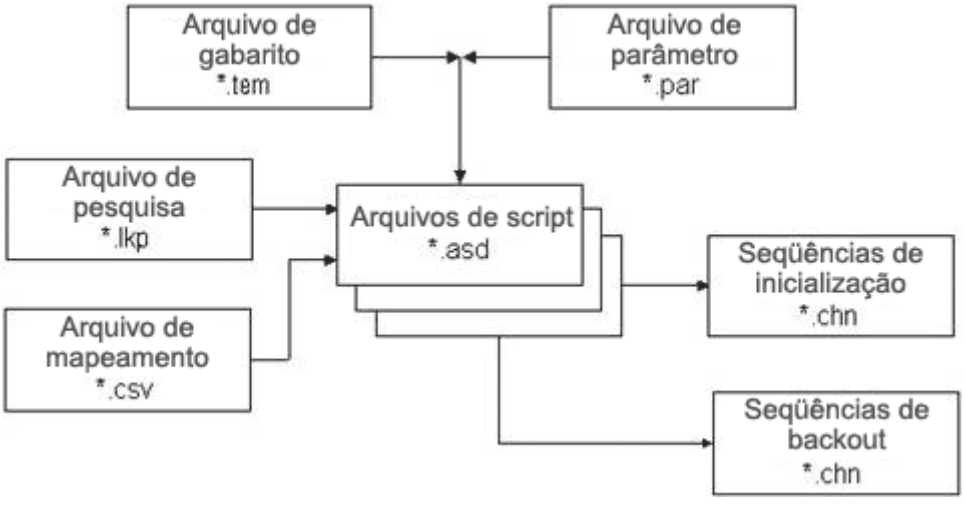
- Tipo de conexão
  - Serial – dados lidos de uma porta serial RS-232C
  - Soquete – uma conexão de soquete TCP
  - Arquivo novo – lê somente dados de evento de segurança que são adicionados a um arquivo depois que o script é iniciado (lê a partir do final do arquivo)
  - Arquivo todos – lê todos os dados de evento de segurança em um arquivo
  - Processo Persistente – inicia um processo persistente quando a porta é iniciada, comunica-se entre o Coletor designado àquela porta e um aplicativo externo através do recebimento e da transmissão de estados e continua a executar para o arquivo ativo da porta.
  - Processo Transitório – comunica-se entre o Coletor designado àquela porta e um aplicativo externo através de estados de recebimento e transmissão. O processo transitório pode ser iniciado várias vezes.

- SNMP – recebe detecções de SNMP v1, v2 e v3
- Nenhum

- Nome do coletor – é possível nomear, copiar e adicionar coletores

Quando um gabarito usa o comando de análise LOOKUP(), um bloco específico de comandos de análise para execução é pesquisado no arquivo de pesquisa apropriado.

Quando um gabarito usa o comando de análise TRANSLATE , o comando carrega um arquivo de mapeamento que permite a rápida pesquisa de entradas-chave.



Arquivos de gabarito

É possível criar, adicionar estados, editar e apagar gabaritos. Os gabaritos determinam como os registros serão processados. A maioria das decisões sobre gabaritos gira em torno de quais tipos de registros você está trabalhando e o seu formato. Existe um arquivo de gabarito equivalente com uma extensão .tem. Eles ficam localizados em %WORKBENCH_HOME%\elements\<Nome do coletor>.

Os arquivos de gabarito são baseados em estados. Um estado é um ponto de decisão dentro do fluxo lógico ou caminho de um gabarito. Cada ponto (estado) contém informações indicando o processo a ser realizado. Os estados incluem referência a parâmetros quando o gabarito é fundido com um arquivo de parâmetro; valores específicos substituem os parâmetros. Quando os parâmetros são substituídos por valores específicos, um ou mais arquivos de script são criados.

Como um estado é inserido em um gabarito, ele é atribuído a um número que permanece com ele, mesmo que ele seja movido no gabarito. Há três agrupamentos de estados.

- Os estados Transmitir, Receber, Decidir e Analisar são numerados na ordem em que são inseridos no gabarito.
  - O estado Transmitir (Tx) – transmite uma string a uma porta definida.
  - O estado Receber (Rx) - define se o Assistente deve ou não receber informações de um aplicativo de segurança em um buffer. Informações são extraídas da definição de porta.
  - O estado Decidir - usa uma string de dados ou variável para determinar o estado a avançar.
  - O estado Analisar - usa os comandos de análise a fim de criar gabaritos para processar as informações coletadas no buffer de recebimento.
- Os estados Avançar e Ir para são identificados pelo número do estado para o qual estão apontando.
  - Estado Avançar - indica o estado para o qual saltar no script seguinte.
  - Estado Ir - usado para retroceder a outro estado dentro do script atual
- O estado Parar é sempre o número zero. Indica quando parar o processamento em uma porta.

Estado Transmitir

O Estado Transmitir envia uma string ou variável (dependendo do tipo de dado selecionado) ao tipo de conexão configurado para o coletor. Se a conexão for interrompida durante a entrada no estado Transmitir e um valor for digitado na caixa Valor de Rx/Tx no painel Informações de Porta do gabarito, ocorrerá o evento a seguir, serão feitas tentativas de restabelecer a conexão até que uma reconexão bem sucedida seja alcançada.

Há um atraso dentro do caractere que especifica o número de milissegundos (ms) entre o envio de cada byte de dados.

Estado Receber

O Estado Receber especifica o método a ser usado pelo Assistente para determinar o momento do recebimento de dados do coletor. No Estado Receber, são especificados:

- Tipo de recebimento
- Bytes mínimos
- String conclusiva do delimitador

Se a conexão for interrompida durante a entrada no estado Transmitir e um valor for digitado na caixa Valor de Rx/Tx no painel Informações de Porta do gabarito, ocorrerá o evento a seguir, serão feitas tentativas de restabelecer a conexão até que uma reconexão bem sucedida seja alcançada.

Após o Estado Receber do RxBuffer, duas variáveis são automaticamente preenchidas com os resultados desse estado:

- s_RXBufferString contém o texto recebido pelo RxBuffer.
- i_RXBufferLength contém o tamanho de s_RXBufferString.

Isso equivale a executar o código de script a seguir após um Estado Receber:

- COPY(s_RXBufferString:)
- LENGTH(i_RXBufferLength,s_RXBufferString)

Essas variáveis de preenchimento automático facilitam a comparação em um Estado Decidir para determinar se o tempo de espera do Estado Receber foi excedido (i_RXBufferLength = 0). Também permitem o uso direto do RXbuffer por meio da variável s_RXBufferString.

Tipos de recebimento - Existem quatro tipos de recebimento no editor de gabarito. São elas:

- Tempo de Espera - Permite que um script continue a ser processado mesmo que não sejam recebidos dados em um período de tempo especificado. A seleção do tempo de espera permite ao Assistente receber dados até que o período de tempo de espera seja atingido, conforme definido pela variável RX_TIMEOUT_DELAY.
- Espera - Usado principalmente no momento do recebimento de mensagens de eventos não solicitadas. O Assistente aguarda a duração do "tempo de espera" até que sejam recebidos dados.

  NOTA: No caso dos tipos de recebimento de tempo de espera e espera, o processamento no script somente prossegue depois que o número mínimo de bytes é recebido ou quando o tempo de espera é alcançado no caso dessa opção.

- tempo de espera do delimitador - Usa uma string de caracteres predefinida para indicar ao Assistente que dados foram recebidos. Os dados da caixa String Conclusiva do Delimitador são comparados com os dados do buffer de recebimento à medida que cada byte é recebido.
- Espera do delimitador - Usado quando mensagens não solicitadas são aguardadas. Uma string de caracteres definida pelo usuário indica ao Assistente que dados foram recebidos. O Assistente usa os dados da caixa String Conclusiva do Delimitador para verificar dados à medida que cada byte é recebido. O parâmetro RX_TIMEOUT_DELAY não tem efeito quando a opção espera do delimitador é usada.

  NOTA: No caso dos tipos de recebimento de tempo de espera do delimitador e espera do delimitador, o processamento no script somente prossegue depois que a string conclusiva do delimitador é avaliada como verdadeira e o número mínimo de bytes é recebido, ou quando o tempo de espera é alcançado no caso da opção tempo de espera do delimitador.

Bytes Mínimos - O número mínimo de bytes é a quantidade de bytes que precisa ser recebida para que o Assistente use o período de tempo de espera padrão ou dê continuidade ao processamento. O processamento no script somente continua após o recebimento do número mínimo de bytes.

String conclusiva do delimitador - Essa string é concluída quando o tipo de recebimento é o tempo de espera de delimitador ou a espera de delimitador. O processamento do coletor somente passa para o próximo estado depois que a string conclusiva de delimitador faz a correspondência dos dados lidos e o número mínimo de bytes é recebido.

A string conclusiva de delimitador é uma expressão regular compatível com POSIX 1003.2.

Cenários de tipos de recebimento - Existem quatro tipos de cenários de tipo de recebimento. São eles:

- Cenário de tempo de espera – Depois que o Estado Receber é digitado, o processamento é interrompido até que os bytes mínimos sejam lidos ou até que RX_TIMEOUT_DELAY segundos se decorram. Depois que o Assistente recebe o número mínimo de bytes especificado, ou depois que o tempo de espera é excedido, o processamento da porta do coletor passa para o próximo estado do script.

- Cenário de espera - O tipo de Estado Esperar Recebimento aguarda até que o coletor do Assistente receba o número mínimo de bytes especificado na caixa Bytes Mínimos. Depois que o Assistente recebe mais do que número mínimo de bytes especificado na caixa Bytes Mínimos, o processamento da porta do coletor passa para o próximo estado do script. Se o número mínimo de bytes não for recebido, o processamento da porta do coletor nunca excederá o tempo de espera.
- Cenário de tempo de espera do delimitador - Se a string conclusiva do delimitador for encontrada após o recebimento da posição de bytes mínimos definida na caixa Bytes Mínimos, os dados até o delimitador, e com o delimitador incluso, são armazenados no Buffer Rx. Se a string conclusiva do delimitador não for encontrada, não haverá transferência de dados para o buffer de recebimento e o tempo de espera do processamento da porta do coletor será excedido no período de tempo de espera padrão.
- Cenário de espera do delimitador - Se a string conclusiva do delimitador for encontrada após o recebimento do número mínimo de bytes definido na caixa Bytes Mínimos, o processamento da porta do coletor prosseguirá e os dados serão processados. Se a string conclusiva do delimitador não for encontrada, não haverá transferência de dados para o buffer de recebimento e o tempo de espera da porta não será excedido. Se a string conclusiva do delimitador não for encontrada em momento algum, o processamento da porta do coletor nunca excederá o tempo de espera. Além disso, se a string conclusiva do delimitador for encontrada, mas se não houver o recebimento do número mínimo de bytes, o tempo de espera do processamento da porta do coletor não será excedido em momento algum.

Estado Decidir

O Estado Decidir avalia o conteúdo do buffer de recebimento ou variável para determinar a ação a ser executada. Se as informações do buffer de recebimento contiverem o tipo conclusivo selecionado, o Gerenciador de Coletor processará o comando como verdadeiro e a rota Sim será seguida. Se o buffer de recebimento não contiver o tipo conclusivo selecionado, o Gerenciador de Coletor processará a decisão como falsa e a rota Não será seguida.

O buffer de recebimento (Rxbuffer de tamanho) é um parâmetro editável localizado em:

```
$WORKBENCH_HOME/config/wizard.properties/
   system.max_receive_buffer_size
```

Esse parâmetro permite configurar o buffer de recebimento do Gerenciador de Coletor (buffer Rx). O padrão é de 50.000 eventos. O mínimo é de 5.000 eventos. Quando o buffer Rx alcança o tamanho máximo, novos eventos são eliminados ao serem recebidos já que são obstruídos.

Existem quatro tipos conclusivos. São eles:

- String - Compara uma string conclusiva definida pelo usuário com o conteúdo do buffer de recebimento. O conteúdo da string conclusiva é comparado com o conteúdo do buffer de recebimento, ou de uma variável, para determinar a rota decisória a ser processada. A string conclusiva é uma expressão regular compatível com POSIX 1003.2. Uma variável dá suporte a strings, inteiros e flutuantes.
- Verdadeiro - Força uma avaliação com resultado verdadeiro, e o Gerenciador de Coletor segue a rota Sim.

- Falso - Força uma avaliação com resultado falso, e o Gerenciador de Coletor segue a rota Não.
- Dados - Compara uma string conclusiva definida pelo usuário com outra string ou com o valor de uma variável.

Estado Analisar

O Estado Analisar é usado para desenvolver os scripts a serem executados nas portas. Os comandos de análise podem incluir parâmetros fundidos com o gabarito no momento da criação dos scripts. Um Editor Visual e um Editor de Texto estão disponíveis para definir os comandos de análise.

O Estado Analisar também é usado para inserir comandos de análise em um gabarito. Os comandos de análise podem incluir parâmetros, que são substituídos por valores específicos quando o gabarito é fundido com um arquivo de parâmetro no processo de criação de scripts. A fusão de um gabarito com um arquivo de parâmetro pode acionar a execução de vários scripts nas portas.

Arquivos de parâmetro

Os parâmetros equivalem a variáveis Os arquivos de parâmetro (arquivos .par) são tabelas usadas para definir nomes de variáveis nos arquivos de script de execução associados. Eles são usados quando mencionados no código de análise. e são armazenados como strings. Qualquer valor numérico precisa ser convertido em uma string para manipulação. Quando novos valores de parâmetros são inseridos, entram em vigor depois que o script é construído. Eles são fundidos com o arquivo de gabarito durante a criação de um script.

Os nomes de arquivos de script em execução são exibidos na primeira linha da tabela e os nomes ou etiquetas de parâmetros são exibidos na primeira coluna da tabela. A segunda linha da tabela é usada para definir os ícones exibidos na árvore do Coletor. As linhas restantes definem os valores de variáveis ou parâmetros a serem usados para parâmetros, à medida que se relacionam ao script específico.

Os valores dentro de um arquivo de parâmetro são:

- Tags META, informações e comentários – existem mais de 200 tags META disponíveis; 100 são configuráveis pelo usuário e as outras são reservadas.
- Regra – os nomes de arquivos definidos são exibidos na linha do cabeçalho da tabela, enquanto os próprios parâmetros são exibidos na primeira coluna da tabela.
- Bitmap - a segunda linha da tabela define o bitmap usado para aquele arquivo. O bitmap será exibido na lista de Coletores.

Arquivos de Pesquisa

Os arquivos de Pesquisa são tabelas opcionais (arquivos .lkp) com as quais os valores recebidos são comparados para determinar quais ações, se houver, serão executadas em resposta aos eventos de segurança. Os arquivos de pesquisa contêm cláusulas de correspondência, que são usadas para comparar strings individuais. Com base nas cláusulas de correspondência em um arquivo de pesquisa específico e nos dados recebidos dos dispositivos de origem, o comando LOOKUP determinará se a string de pesquisa será encontrada ou não.

Opcionalmente, os comandos de análise podem ser associados à string de correspondência. Os comandos de análise serão executados se uma correspondência for encontrada.

Arquivos de Mapeamento

Os arquivos de Mapeamento são arquivos opcionais (.cvs) que possibilitam uma pesquisa rápida das principais entradas. O arquivo csv é um caminho relativo de um diretório de scripts do Coletor. Atualmente, a edição desses arquivos não fica disponível no Construtor de Coletor, mas eles podem ser editados no Excel.

Exemplo de um possível arquivo de mapeamento:

```
~Mês~      ~Número~
Jan                1
Fev                2
Mar                3
Abr                4
Mai                5
Jun                6
Jul                7
Ago                8
Set                9
Out               10
Nov               11
Dez               12
```

As entradas podem ser um número de variáveis de script (string, variável ou flutuante) usado para indicar em quais variáveis os dados serão armazenados. Esse exemplo em particular é usado para converter (mapear) mês em número (p. ex., Jan para 1).

Arquivos de manifesto

Os arquivos de manifesto são o que diferencia os coletores da versão 5.* dos anteriores. Esses arquivos dão suporte à distribuição de coletores do Console do Sentinel e as versões de coletores. A análise de coletores é definida no arquivo agent.lkp. Esses casos de pesquisa são os seguintes:

- Setup - Configuração única de variáveis e parâmetros.
- Check_Setup - Verificação única das variáveis e parâmetros.
- Initialize_Vars - O início de todo loop, em que as variáveis são inicializadas uma vez por análise.
- Parse - O local onde a análise é realizada.

Isso permite fazer o plugin da análise do novo coletor em gabaritos existentes. Além disso, permite sobrepor novas versões da análise do coletor para atualizar o código. A seguir está uma lista dos arquivos de manifesto e seu conteúdo na v5.0:

- agent.nfo
  - product,Snort
  - product.vendor,GNU
  - product.version,2.0
  - product.security.type,IDS
  - product.sensor.type,N
  - product.name,IDSx_GNUx_SNRT
  - file.version,1

Outras referências do Sentinel

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

- Sentinel™ – Guia de Instalação do Sentinel
- Guia do Usuário do Sentinel™
- Guia do Usuário do Assistente do Sentinel™
- Guia de Referência do Usuário do Sentinel™
- Guia de Integração de Terceiros do Sentinel™
- Notas de 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, 7 dias por semana, ligue 800-858-4000

2 Gerenciando hosts do Assistente

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

Os hosts do Assistente são máquinas que têm o Gerenciador de Coletor instalado. Os hosts interagem com máquinas do Construtor de Coletor e com o Sentinel na rede. Os coletores recebem e analisam dados. Com base nesses dados, os hosts enviam alertas ao Sentinel.

O Assistente automaticamente detecta hosts na rede e os adiciona à lista da guia Host do Assistente. Não é possível adicionar hosts manualmente. Você pode renomear hosts existentes e apagar hosts que deixaram de estar fisicamente presentes e de se comunicar na rede.

O Construtor de Coletor coleta mensagens sobre a saúde nos hosts. Se um host não responder com uma mensagem sobre a saúde, exibirá um X vermelho na árvore Hosts do Assistente. É possível remover um host com um X vermelho, mas se o Construtor de Coletor detectar comunicações desse host, ele reaparecerá na árvore Hosts do Assistente. De modo semelhante, se um host que já está se comunicando for removido, a mensagem sobre a saúde o retornará à árvore Hosts do Assistente.

Quando um host é detectado, é atribuído a um número de identificação.

Os coletores mais recentes podem ser encontrados no CD do Service Pack. Para obter mais informações, consulte as Notas de Versão do Service Pack.

NOTA: Para obter mais informações sobre a configuração dos Coletores Demo, consulte o Guia de Instalação do Sentinel – Teste da Instalação.

Como um host do Assistente obtém dados de coletores

Para habilitar um host do Assistente (uma máquina com o Gerenciador de Coletor instalado) a receber dados de um coletor, faça upload do coletor de uma máquina do Construtor de Coletor para o host do Assistente através de uma porta configurada no Construtor de Coletor. Após o upload de um coletor para um host, ele pode receber dados desse coletor.

Cada host do Assistente pode ser conectado a várias portas e monitorar dados de vários coletores. Um host do Assistente pode ter portas com coletores que se conectam a vários tipos diferentes de fontes de dados. Deve ser feito upload de coletores específicos em um host para que sejam executados. Além disso, as portas fornecem informações sobre o local da fonte de dados ao Gerenciador de Coletor.

Permissões de hosts do Assistente

As permissões de hosts do Assistente são administradas por meio da guia Admin do Sentinel Control Center. As permissões de usuário dos hosts do Assistente são:

Nome da permissão	Descrição
Exibir Coletores	▪ Ver a guia 'Coletores' no Sentinel Control Center. ▪ Ver a guia 'Hosts do Assistente' no Construtor de Coletor.
Controlar Coletores	▪ Inclui todos os recursos como a permissão 'Exibir Coletores' ▪ Permite o comando e o controle de Coletores do Sentinel Control Center. ▪ Permite o comando e o controle de coletores no Construtor de Coletor do Assistente.
Administração do Coletor	▪ Inclui todos os recursos como a permissão 'Comandar Coletores' ▪ No Construtor de Coletor, edição e implantação do Coletor. ▪ No Construtor de Coletor, criação, edição, compilação e depuração de Coletores. ▪ No Construtor de Coletor, upload e download de Coletores. ▪ No Construtor de Coletor, exportação de hosts do Assistente. ▪ No Construtor de Coletor, adição, edição e exclusão de portas. ▪ No Construtor de Coletor, definição de opções de porta.

O comando e o controle consistem em

- iniciar/parar portas específicas
- iniciar/parar todas as portas
- reiniciar hosts
- renomear hosts

Gerenciamento de Host do Assistente

Os seguintes temas serão explicados neste capítulo:

- Iniciando o Gerenciador de Coletor
- Parando o Gerenciador de Coletor
- Administração do Gerenciador de Coletor
- Renomear um host
- Apagar um host
- Reiniciar um host
- Exportar um host
- Exibir propriedades de hosts
- Editar um arquivo de gabarito
- Apagando um arquivo de gabarito
- Renomeando um arquivo de pesquisa
- Apagando um arquivo de pesquisa
- Apagando uma seqüência de inicialização
- Iniciando e parando portas do Assistente
- Editando uma porta do Assistente
- Apagando uma porta do Assistente
- Fazendo upload e download de um coletor
- Depurando portas do Assistente

Iniciando e parando o Gerenciador de Coletor

NOTA: Na primeira vez em que o Construtor de Coletor do Assistente for executado, a seguinte mensagem poderá ser exibida: "O diretório 'Coletores' não existe." Ele será criado automaticamente para você. Algumas informações podem ter sido perdidas." Selecione OK; o diretório será criado e o Construtor de Coletor do Assistente será iniciado. Se essa mensagem for exibida outras vezes além da primeira execução do Construtor de Coletor, talvez o diretório Coletor tenha sido apagado inadvertidamente; será necessário verificar se as informações foram perdidas

Iniciando ou parando o serviço Gerenciador de Coletor para Windows

Iniciando ou parando os serviços Gerenciador de Coletor para Windows

1. Clique em *Iniciar* > *Configurações* > *Painel de Controle*.
2. No *Painel de Controle*, clique duas vezes em *Ferramentas Administrativas* e depois clique em *Serviços*.
3. Na caixa de diálogo Serviços, clique o botão direito do mouse em *Gerenciador de Coletor* e clique em *Iniciar* ou *Parar*.

Iniciando os serviços Gerenciador de Coletor para Windows (linha de comando)

1. Vá para %WORKBENCH_HOME%
2. Para iniciar o Gerenciador de Coletor:
   - ./agent-manager start
   - ./agent-manager restart - inicia o script do Gerenciador de Coletor em segundo plano e inicia automaticamente o processo do Gerenciador de Coletor se for interrompido. Se o processo agentmanager já estiver em execução, será interrompido e reiniciado.
   - ./agent-manager.sh console – inicia o processo do Gerenciador de Coletor no primeiro plano.

NOTA: Quando estiver no modo de console, verifique se apenas uma instância do Gerenciador de Coletor está em execução na máquina.

Parando os serviços Gerenciador de Coletor para Windows (linha de comando)

1. Vá para %WORKBENCH_HOME%
2. Para parar o Gerenciador de Coletor:

```
./agent-manager stop
```

Iniciando o Gerenciador de Coletor para UNIX (Normal e Console)

Iniciando o Gerenciador de Coletor para UNIX

1. Como usuário esecadm, vá para

```
$WORKBENCH_HOME
```

2. Digite o seguinte comando:

```
./agent-manager.sh start
```

- ./agent-manager.sh restart - inicia o script do Gerenciador de Coletor em segundo plano e automaticamente inicia o processo do Gerenciador de Coletor se for interrompido. Se o processo do Gerenciador de Coletor já estiver em execução, será interrompido e reiniciado.
- ./agent-manager.sh console – inicia o processo do Gerenciador de Coletor no primeiro plano.

Parando o Gerenciador de Coletor para UNIX

Parando o Gerenciador de Coletor para UNIX

1. Como usuário esecadm, use cd para passar ao diretório

   ```
   $WORKBENCH_HOME
   ```

2. Digite o seguinte comando:

   ```
   ./agent-manager.sh stop
   ```

Administração do Gerenciador de Coletor

Há um arquivo executável do Gerenciador de Coletor (Windows) e um script (UNIX) que permitem:

- Instalar o serviço Gerenciador de Coletor do Windows (somente no Windows)
- Remover o serviço Gerenciador de Coletor do Windows (somente no Windows)
- Definir o serviço Gerenciador de Coletor
- Imprimir informações de depuração extensas
- Exibir a versão do build
- Exibir ajuda

Instalando o serviço Gerenciador de Coletor do Windows (somente no Windows)

Instalando o serviço Gerenciador de Coletor do Windows (somente no Windows)

1. No prompt de comando, vá para %workbench_home%.
2. Digite o seguinte comando:

   ```
   agent-manager.bat -install
   ```

3. Para iniciar o serviço:
   - No prompt de comando, digite o seguinte:

     ```
     net start "agent manager"
     ```

   - Clique em *Iniciar* > *Configurações* > *Painel de Controle*. Clique duas vezes em *Serviços* e selecione *Gerenciador de Coletor*. Iniciar *serviço Gerenciador de Coletor*.

NOTA: Se a janela Serviços já estiver aberta, clique em *Ação* > *Atualizar* e inicie o serviço *Gerenciador de Coletor*.

Removendo o serviço Gerenciador de Coletor do Windows (Windows)

Removendo o serviço Gerenciador de Coletor do Windows (Windows)

1. Pare o serviço Gerenciador de Coletor:
   - No prompt de comando, digite o seguinte:

     ```
     net stop "agent manager"
     ```

   - Clique em *Iniciar* > *Configurações* > *Painel de Controle*. Clique duas vezes em *Serviços* e selecione *Gerenciador de Coletor*. Pare o serviço *Gerenciador de Coletor*. Feche a janela Serviços.
2. No prompt de comando, vá para %workbench_home%.
3. Digite o seguinte comando:

   ```
   agent-manager.bat -remove
   ```

Mudando a senha do Gerenciador de Coletor para Windows

NOTA: Para obedecer às rígidas configurações de segurança exigidas pela Certificação de Critérios Comuns, é altamente recomendável que uma senha forte seja usada 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).

Mudando a senha do Gerenciador de Coletor para Windows

1. No prompt de comando, vá para %workbench_home%.
2. Digite o seguinte comando:

   CUIDADO: Você não será solicitado a fornecer a confirmação de senha nem será solicitado a fornecer a senha antiga.

   ```
   agent-manager.bat –password <nova senha>
   ```

3. Para que a senha tenha efeito:
   - No prompt de comando, digite o seguinte:

     ```
     net stop "agent manager"
     net start "agent manager"
     ```

- No Construtor de Coletor, clique o botão direito do mouse no computador do host e selecione reiniciar host.
- Clique em *Iniciar* > *Configurações* > *Painel de Controle*. Clique duas vezes em *Serviços* e selecione *Gerenciador de Agente*. Pare e inicie o serviço *Gerenciador de Agente*.

Mudando a senha do Gerenciador de Coletor para UNIX

NOTA: Para obedecer às rígidas configurações de segurança exigidas pela Certificação de Critérios Comuns, é altamente recomendável que uma senha forte seja usada 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).

Mudando a senha do Gerenciador de Coletor para UNIX

1. Como usuário esecadm, vá para $WORKBENCH_HOME.
2. Digite o seguinte comando:

CUIDADO: Você não será solicitado a fornecer a confirmação de senha nem será solicitado a fornecer a senha antiga.

```
./agent-manager.sh -password <new password>
```

3. Para que a senha tenha efeito, vá para /usr/local/bin e digite o comando a seguir;

```
./agent-manager.sh -restart
```

Iniciando o Construtor de Coletor

Iniciando o Construtor de Coletor

1. Clique em *Iniciar* > *Programas* > *Sentinel* > *Construtor de Coletor* ou clique duas vezes no ícone *Construtor de Coletor* na área de trabalho.
2. Dependendo da instalação, efetue login como usuário esecadm ou com o nome de usuário da autenticação do Windows.

Renomeando um host do Assistente

Renomeando um host do Assistente

1. No Construtor de Coletor (Assistente), clique na guia Hosts do Assistente para abrir o painel de árvore Hosts do Assistente.
2. Na árvore Hosts do Assistente, clique o botão direito do mouse no host a ser renomeado e clique em *Renomear Host%%.* Somente é possível renomear hosts ativos.
3. Digite o novo nome do host e pressione Enter.

NOTA: Quando um host é renomeado, não é alterado o número de ID atribuído a um host do Assistente quando ele é instalado. Essas informações ficam armazenadas em %WORKBENCH_HOME%\wizard\agents\names.dat.

Apagando um host do Assistente

Para apagar um host, ele primeiro precisa ser removido da rede. Os hosts que estejam se comunicando pela rede não podem ser removidos. Se um host estiver presente na rede, mas sem se comunicar, será exibido com um X vermelho no ícone do host na árvore Hosts do Assistente.

Apagando um host do Assistente

1. Clique na guia *Hosts do Assistente* para abrir o painel de árvore Hosts do Assistente.
2. Na árvore Hosts do Assistente, clique o botão direito do mouse no host.
3. Clique em *Apagar Host*.

Reiniciando um host do Assistente

Reiniciando um host do Assistente

1. Clique na guia *Hosts do Assistente* para abrir o painel de árvore Hosts do Assistente e selecione um host.
2. Clique o botão direito do mouse em um host e clique em *Iniciar Portas*. Somente é ossível reiniciar hosts do Assistente ativos.

Exportando um host do Assistente

Exportando um host do Assistente

1. Clique na guia *Hosts do Assistente* para abrir o painel de árvore Hosts do Assistente. Selecione um host.
2. Clique em *File* (Arquivo) > *Export Host* (Exportar Host). O subdiretório a seguir é criado:

   ```
   %WORKBENCH_HOME%\upload_<nome do host>
   ```

   Esse subdiretório pode ser movido para uma máquina remota usando o Secure Shell (SSH) ou um disco. Depois que o subdiretório for colocado na máquina remota, execute o comando uploadhost. Isso copia os arquivos necessários nos diretórios apropriados.

NOTA: Se as configurações SNMP forem mudadas, o Construtor de Coletor não será capaz de se comunicar com o máquina remota do momento em que o botão Exportar for pressionado até o upload dos arquivos exportados do coletor.

Exibindo propriedades de hosts do Assistente

Exibindo propriedades de hosts do Assistente

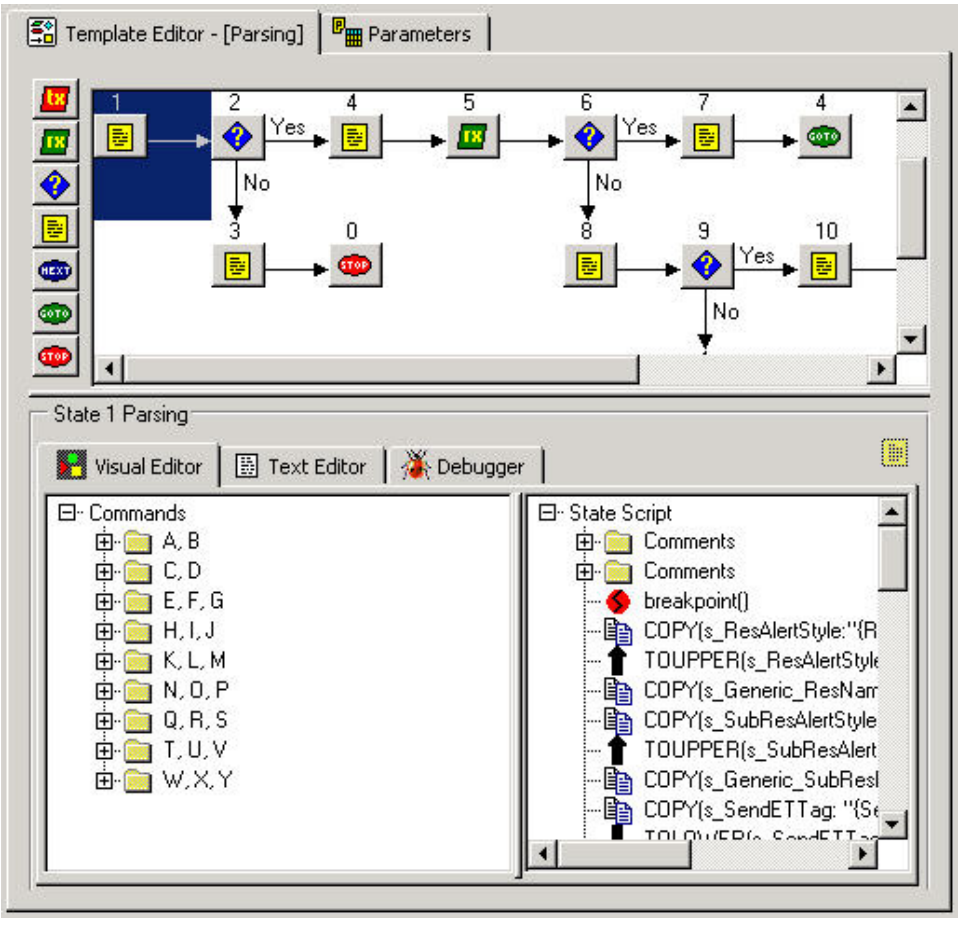
1. Clique na guia *Hosts do Assistente* para abrir o painel de árvore Hosts do Assistente.
2. Na árvore Hosts do Assistente, clique o botão direito do mouse no host e clique em *Propriedades*. A janela Propriedades do Assistente exibe as informações a seguir:
   - Nome
   - ID
   - HostName
   - Endereço IP
   - Versão
   - Uptime
3. Clique em *OK* para fechar a janela Propriedades.

NOTA: Se o host não estiver em execução, uma janela Nenhuma Resposta será exibida quando as propriedades forem selecionadas.

Editando um arquivo de gabarito

Editando um arquivo de gabarito

1. Clique na guia *Coletores* para abrir o painel de árvore Coletor.
2. Na árvore Coletor, clique no gabarito e clique na guia Editor de Gabarito à direita.
3. No Editor de Gabarito, clique no estado para editar e fazer as mudanças desejadas. É possível editar um estado usando o Editor Visual ou o Editor de Texto. Para obter informações sobre os comandos de análise, consulte o Guia de Referência do Usuário do Sentinel.



Apagando um arquivo de gabarito

Apagando um arquivo de gabarito

1. Clique na guia *Coletores* para abrir o painel de árvore Coletores.
2. Na árvore Coletores, clique o botão direito do mouse em um gabarito e clique em *Apagar Gabarito*.

Renomeando um arquivo de pesquisa

Renomeando um arquivo de pesquisa

1. Clique na guia *Coletores* para abrir o painel de árvore Coletores.
2. Clique o botão direito no mouse no arquivo de pesquisa e clique em *Renomear Arquivo de Pesquisa*.
3. Digite o novo nome e pressione *Enter*.

Apagando um arquivo de pesquisa

Apagando um arquivo de pesquisa

1. Clique na guia *Coletores* para abrir o painel de árvore Coletores.
2. Clique o botão direito no mouse no arquivo de pesquisa e clique em *Apagar Arquivo de Pesquisa*.

Apagando um script

Apagando um script

1. Há duas formas de apagar um script.
   - Na árvore Coletor, clique o botão direito do mouse em um script e clique em *Apagar*.
   - Clique o botão direito do mouse no script na coluna Scripts de Inicialização ou na coluna Scripts de Backout e selecione Apagar Script.

Apagando uma seqüência de inicialização

Apagando uma seqüência de inicialização

1. No painel Scripts de Inicialização, selecione a seqüência de inicialização no menu suspenso para que o nome da seqüência seja exibido na caixa Scripts de Inicialização.
2. Clique o botão direito do mouse no script na árvore Coletores e selecione Apagar Seqüência de Inicialização Atual. A seqüência de inicialização é removida da lista Scripts de Inicialização.

NOTA: Se a seqüência de inicialização padrão for apagada, os scripts atribuídos a ela serão removidos da coluna Scripts de Inicialização, mas o padrão ainda será exibido no menu Seqüências de Inicialização.

Portas do Assistente

Esta seção explica como parar, iniciar, editar, apagar e depurar uma porta do Assistente.

Iniciando e parando uma porta do Assistente - Interface do Usuário

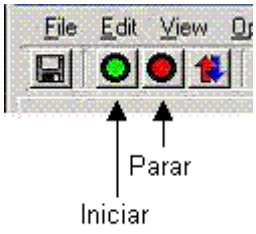
Quando um coletor é iniciado ou interrompido, o botão Iniciar ou Parar na coluna Iniciar/Parar muda no momento em que o coletor é iniciado ou interrompido de fato. Se você estiver trabalhando com um coletor remoto, essa mudança pode ser retardada enquanto aguarda o recebimento do status do coletor.

Quando uma porta é iniciada ou interrompida, o script de inicialização e o script de backout selecionados são executados.

Quando todas as portas forem iniciadas, uma porta somente será iniciada se a caixa Executar Porta na Inicialização estiver marcada em Opções de Outras Portas, no menu Opções.

Iniciando e parando todas as portas do Assistente

1. Na janela Assistente:
   - Para parar todas as portas, clique no botão Parar na barra de ferramentas.
   - Para iniciar todas as portas, clique no botão Iniciar na barra de ferramentas.



Iniciando e parando uma porta individual do Assistente

1. Na janela Assistente:
   - Para parar uma porta, clique no botão Parar na coluna Iniciar/Parar correspondente à porta.
   - Para iniciar uma porta, clique no botão Iniciar na coluna Iniciar/Parar correspondente à porta.

Editando uma porta do Assistente

Se a configuração de uma porta for editada durante sua execução, a porta será interrompida. Para evitar a perda de dados, pare a porta manualmente antes de editar suas configurações.

Editando uma porta do Assistente

1. Pare a porta do host apropriado.
2. Complete as etapas de criação de uma porta do Assistente no Capítulo 3. A nova configuração substituirá a configuração existente quando você gravar ou fizer o upload da porta.

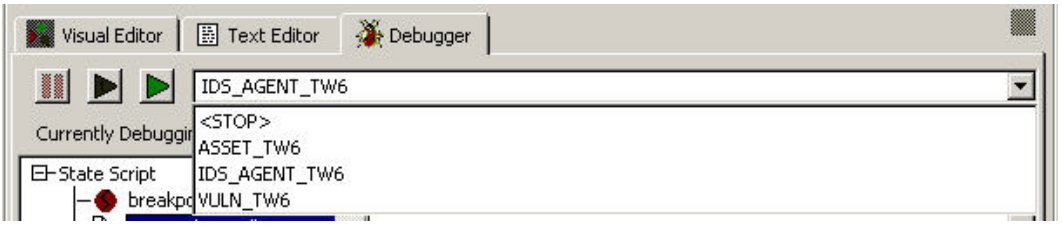
Apagando uma porta do Assistente

Apagando uma porta do Assistente

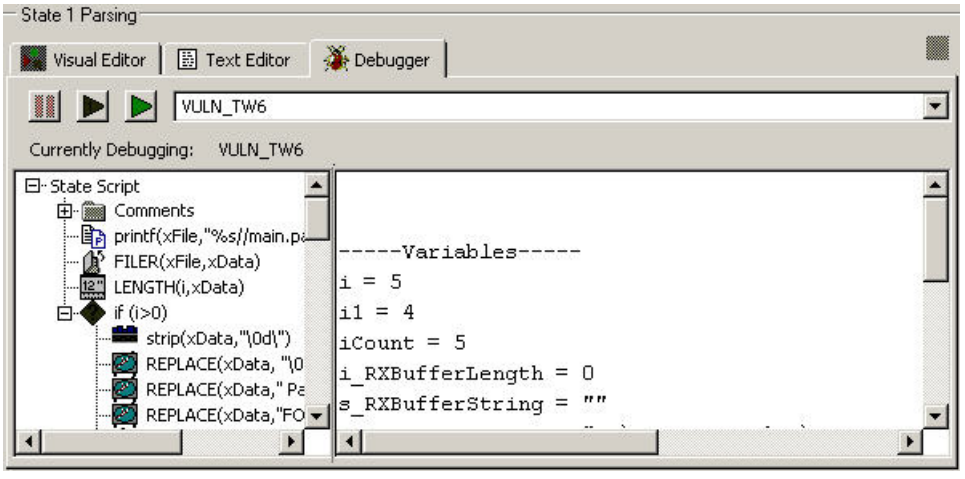
1. Pare a porta.
2. No painel Informações de Porta do Construtor de Coletor, clique o botão direito do mouse no nome da porta e clique em Apagar Porta. Todas as portas abaixo da porta apagada serão interrompidas automaticamente.
3. Se estiver apagando de um:
   - Host local - Clique em *Arquivo* > *Gravar* e selecione Informações de Porta.
   - Host remoto - Clique em *Arquivo* > *Upload/Download*.

Depurando uma porta do Assistente

O Depurador permite solucionar o código de coletor em execução em uma porta. O lado esquerdo do painel do Depurador exibe o script de estado. O lado direito do painel exibe scripts e variáveis do tipo RX_Buffer, que podem ter nomes com até 32 caracteres.



Para que o Depurador tenha efeito, é necessário ter um estado de análise como o primeiro estado, além de ter comandos Breakpoint().



Durante a depuração, espere até o Buffer Rx ser atualizado antes de realizar outra função.

NOTA: Se o host do Gerenciador de Coletor tiver perdido a conectividade (), não será possível depurar uma porta desse host.

Depurando uma porta do Assistente

1. No Editor de Gabarito, selecione a guia Depurador, no painel de edição, para acessá-lo. O painel em branco exibido permite selecionar a porta do Assistente a ser depurada em uma lista suspensa.

   Se você clicar na guia Hosts do Assistente, a porta que está sendo depurada indicará que está em modo de depuração.

VULN_TW6	File All	C:\workarea\vuln_inf	DemoVulnerabilityUploa	Stop	Debug
ASSET_TW6	File All	c:\workarea\asset_o	T1_GNUx_NMAP_035	Start	Off

2. Na lista suspensa, selecione uma porta para iniciar o processo de depuração.
   Para depurar a porta:
   - Pressione F6 para passar por um comando de cada vez, ou clique no botão Executar Um Comando.
     
     Clique no botão novamente ou pressione F6 para continuar a execução do script.
   - Pressione F7 para passar pelos comandos, ou clique no botão Continuar Execução do Comando.
     
     Pressione F5 para pausar, ou clique no botão Pausar Execução de Comandos.
     
     A pausa permanece até que você pressione F7 ou o botão Continuar Execução do Comando.

   O Depurador pára em todos os pontos de interrupção, mas sua execução continua. O status da porta é "ligado".

   Nenhum evento é enviado durante as pausas no modo de depuração.

   Quando o analisador é encerrado, os botões ficam esmaecidos, e a lista de seleção exibe "Nenhuma porta está sendo depurada".

   Como o Depurador não anulará uma pausa, se você estiver depurando um analisador que atingiu um comando de pausa, o botão Parar ou o botão Etapa aguardarão até que a pausa seja concluída para fazer efeito.

Fazendo upload e download de coletores e hosts

Existem três guias na janela Upload/Download:

- Hosts – faz o upload de cada configuração de porta e da coleção de coletores para cada um dos hosts especificados. Cada host mantém sua própria configuração de porta e coleção de coletores.
- Coletores – para o upload de coletores específicos.
- Preencher Rede – faz o upload da configuração de porta/agentes de um host especificado para todos os hosts selecionados. Todos os hosts selecionados ficam com a mesma configuração de porta e coleção de coletores que o host de origem.

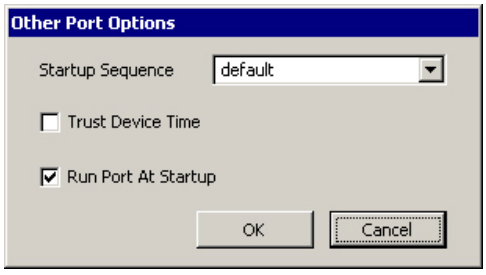
Durante o download, as configurações de porta de um coletor remoto aparecerão no host escolhido para download e os coletores do host remoto com o mesmo nome que o host local serão sobregravados.

Fazendo upload de um coletor para um único host

Fazendo upload de um coletor para um único host

1. Se o coletor já estiver configurado corretamente e você tiver criado um script, pode pular para as etapas 2 a 11.
2. Clique na guia Hosts do Assistente e selecione um host.
3. Na coluna Nome da Porta, clique duas vezes em *Novo...* Digite o nome de sua preferência.
4. Na coluna Coletor, selecione um coletor.

5. Conforme a documentação do coletor (`%WORKBENCH_HOME%\Elements\<Nome do coletor>\docs\<file name>.pdf`), configure o coletor.
6. Clique na guia *Coletores*, expanda o coletor e realce o arquivo do gabarito.
7. Clique na guia *Parâmetros* à direita.
8. Conforme a documentação do coletor, defina os valores dos parâmetros.
9. (opcional) Caso deseje que esse coletor não comece na inicialização ou caso deseje descartar o horário do dispositivo, clique na guia *Host do Assistente*, clique o botão direito do mouse no nome da porta do Assistente, selecione *Outras Opções de Porta...* e anule a seleção de *Executar Porta na Inicialização*, ou clique em *Confiar no Horário do Dispositivo*. Clique em *OK*.



10. Clique em *Gravar*.
11. Clique na guia *Coletores*, clique o botão direito do mouse no arquivo de gabarito e selecione *Criar Script*.
12. Clique em:
    - *Arquivo* > *Upload/Download.*
    - Clique o botão direito do mouse no coletor e clique em *Fazer Upload de Coletor*.
    - Clique no botão *Upload/Download* 

    A janela *Upload/Download* é exibida.
13. Na janela Upload/Download, clique na guia *Coletores*.
14. Na lista suspensa, selecione o coletor para upload.
15. Clique em *Upload*. Na primeira vez que fizer isso, você será solicitado a fornecer a senha do Gerenciador de Coletor, mesmo no caso de um host local do Assistente. A janela Andamento da Transferência é aberta e mostra o andamento do upload.

NOTA: Você pode usar a janela Andamento da Transferência para reiniciar hosts após uma transferência.

Fazendo upload de um coletor para vários hosts

Fazendo o upload de um coletor para vários hosts

ATENÇÃO: Se você fizer upload de um host com um coletor com o mesmo nome de um coletor do host local, o coletor do host remoto será sobregravado sem que haja aviso.

1. Se o coletor já estiver configurado corretamente e você tiver criado um script, pode pular para as etapas 2 a 11.
2. Clique na guia *Hosts do Assistente* e selecione um host.

3. Na coluna Nome da Porta, clique duas vezes em *Novo...* Digite o nome de sua preferência.
4. Na coluna *Coletor*, selecione um coletor.
5. Conforme a documentação do coletor (`%WORKBENCH_HOME%\Elements\<Nome do coletor>\docs\<file name>.pdf`), configure o coletor.
6. Clique na guia *Coletores*, expanda o coletor e realce o arquivo do gabarito.
7. Clique na guia *Parâmetros* à direita.
8. Conforme a documentação do coletor, defina os valores dos parâmetros.
9. (opcional) Caso deseje que esse coletor não comece na inicialização ou caso deseje descartar o horário do dispositivo, clique na guia *Host do Assistente*, clique o botão direito do mouse no nome da porta do Assistente, selecione *Outras Opções de Porta...* e anule a seleção de 'Executar Porta na Inicialização', ou clique em 'Confiar no Horário do Dispositivo'. Clique em OK.
10. Clique em *Gravar*.
11. Clique na guia Coletores para abrir o painel de árvore Coletores.
12. Clique em um Coletor.
13. Clique em:
    - Arquivo > Upload/Download.
    - Clique no coletor e selecione Fazer Upload de Coletor.
    - Clique no botão Upload/Download 

    A janela Upload/Download é exibida.
14. Na janela Upload/Download, clique na guia Hosts e marque ou desmarque a caixa de seleção Fazer Upload de Coletores ao Fazer Upload.

    Se essa caixa de seleção for marcada, será feito o upload dos coletores selecionados na guia Coletores. Essa caixa de seleção fica marcada por padrão. Essa opção não tem efeito no download de coletores de um host.
15. Selecione na lista os hosts do Assistente para os quais deseja fazer o upload de coletores.

    Todos os hosts do Assistente na rede serão automaticamente incluídos na lista. Os botões indicam se a máquina do host está on-line ou não.

    Clique em Selecionar Tudo para selecionar todos os hosts do Assistente na lista. Clique em Não Selecionar Nenhum para desfazer a seleção de todos os hosts do Assistente na lista.
16. Clique em Upload para fazer upload dos coletores selecionados no(s) host(s) selecionado(s). Na primeira vez que fizer isso, você será solicitado a fornecer a senha do Gerenciador de Coletor, mesmo no caso de um host local do Assistente.

Fazendo download de um host

Fazendo download de um host

CUIDADO: Se você fizer download de um host com um coletor com o mesmo nome de um coletor do host local, o coletor do host local será sobregravado sem que haja aviso.

1. Clique na guia Hosts do Assistente para abrir o painel de árvore Hosts.
2. Na árvore Hosts do Assistente, clique no host para download.
3. Clique em:
   - Arquivo > Upload/Download.
   - Clique no coletor e selecione Fazer Upload de Coletor.
   - Clique no botão Upload/Download 

   A janela Upload/Download é exibida. O coletor selecionado fica marcado por padrão.
4. Clique em Download. Na primeira vez que fizer isso, você será solicitado a fornecer a senha do Gerenciador de Coletor, mesmo no caso de um host local do Assistente. É feito o download do host e ele é adicionado à árvore Hosts do Assistente. A janela Andamento da Transferência é aberta e mostra o andamento do download.

NOTA: Você pode usar a janela Andamento da Transferência para reiniciar hosts após uma transferência.

NOTA: Somente é possível fazer download de um host de cada vez. Se você marcar mais de um host, os downloads não serão feitos.

Fazendo download de coletores de um único host

Fazendo download de coletores de um único host

1. Clique em:
   - Arquivo > Upload/Download.
   - Clique no botão Upload/Download 

   A janela Upload/Download é exibida.
2. Selecione na lista o host do Assistente do qual você deseja fazer download de coletores.

   Todos os hosts do Assistente na rede serão automaticamente incluídos na lista. Os botões indicam se a máquina do host está on-line ou não.

   Clique em Selecionar Tudo para selecionar todos os hosts do Assistente na lista. Clique em Não Selecionar Nenhum para desfazer a seleção de todos os hosts do Assistente na lista.
3. Clique em Download para fazer download dos coletores do host selecionado.

Fazendo upload de portas para vários hosts

Fazendo upload de portas para vários hosts

1. Clique em:
   - Arquivo > Upload/Download.
   - Clique no botão Upload/Download 
2. A janela Upload/Download é exibida.
3. Na janela Upload/Download, clique na guia Preencher Rede.

4. Na lista com a etiqueta ‘Selecionar configuração de porta de host e coletores dos quais deseja fazer upload’, selecione o host desejado para fazer upload de configurações de portas e coletores.
5. Na lista com a etiqueta ‘Selecionar os hosts para os quais deseja fazer upload desta configuração’, selecione o host desejado para fazer upload das configurações selecionadas.

   Todos os hosts do Assistente na rede serão automaticamente incluídos na lista. Os botões indicam se a máquina do host está on-line ou não.

   Clique em Selecionar Tudo para selecionar todos os hosts do Assistente na lista. Clique em Não Selecionar Nenhum para desfazer a seleção de todos os hosts do Assistente na lista.

Fazendo upload de vários coletores para uma rede

Fazendo upload de vários coletores para uma rede

1. Na janela principal Assistente, selecione um coletor na árvore Coletores.
2. Clique em:
   - Arquivo > Upload/Download.
   - Clique no coletor e selecione Fazer Upload de Coletor.
   - Clique no botão Upload/Download 
3. Selecione a guia Preencher Rede.
4. Na primeira caixa de seleção, no menu suspenso, selecione a configuração de porta de host e os coletores dos quais deseja fazer upload.
5. Na segunda caixa de seleção, no menu suspenso, selecione os hosts para os quais deseja fazer upload de configurações.

   NOTA: É necessário marcar pelo menos um das caixas de seleção para fazer upload de sua configuração.

   Você pode selecionar um coletor diferente para cada caixa suspensa. Cada coletor marcado na lista principal adquirirá a configuração de porta e os coletores do host selecionado na caixa com a etiqueta:

   “Selecione a configuração de porta de host e os coletores dos quais deseja fazer upload”, a menos que nenhuma esteja selecionada.
6. Ao concluir a configuração da rede, selecione o botão Upload para iniciar o processo de upload.

Fazendo upgrade de coletores

Fazendo upgrade de coletores

1. Leia a documentação que acompanha o novo coletor e que explica as mudanças.
2. Coloque a nova versão do coletor no diretório %workbench_home%/Elements no PC master do coletor.
3. Abra o arquivo de parâmetro do coletor que está sendo substituído, e corte e cole os parâmetros correspondentes no novo coletor.

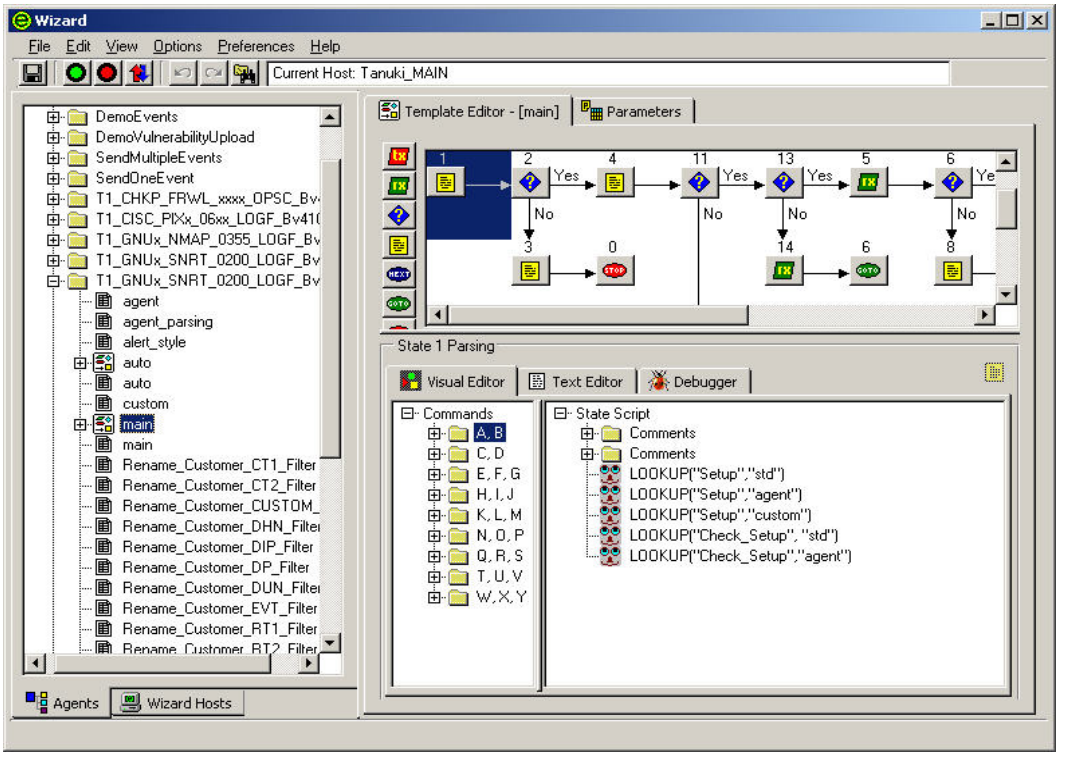
4. Se necessário, conforme a documentação do novo coletor, remova ou adicione novas variáveis de parâmetro. Se estiver adicionando novas variáveis de parâmetro, preencha a variável.
5. Grave o arquivo de parâmetro no novo coletor.
6. Crie o novo coletor.
7. Edite as informações de configuração de porta para usar o novo coletor.
8. Grave as informações de configuração de porta.
9. Faça upload do novo coletor e das configurações de porta.
10. Reinicie a porta.

3 Construindo e mantendo coletores

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

NOTA: Para usuários do MS SQL 2000, o tamanho do evento não pode ser maior que 8KB.

Um Coletor é responsável pela análise de dados de uma origem de eventos de segurança e pelo envio de eventos para o Sentinel. Coletores são construídos, ativados e mantidos por meio do Construtor de Coletor do Assistente. Clique na guia *Coletores* para exibir a árvore Coletores para ver todos os coletores e seus componentes no sistema Sentinel.



O Gerenciador de Coletor permite:

- Construir coletores
  - Criar e configurar arquivos de gabarito
  - Criar arquivos de parâmetro
  - Criar arquivos de pesquisa
  - Construir scripts
  - Criar uma porta do Assistente

Fundamentos básicos da construção de coletores

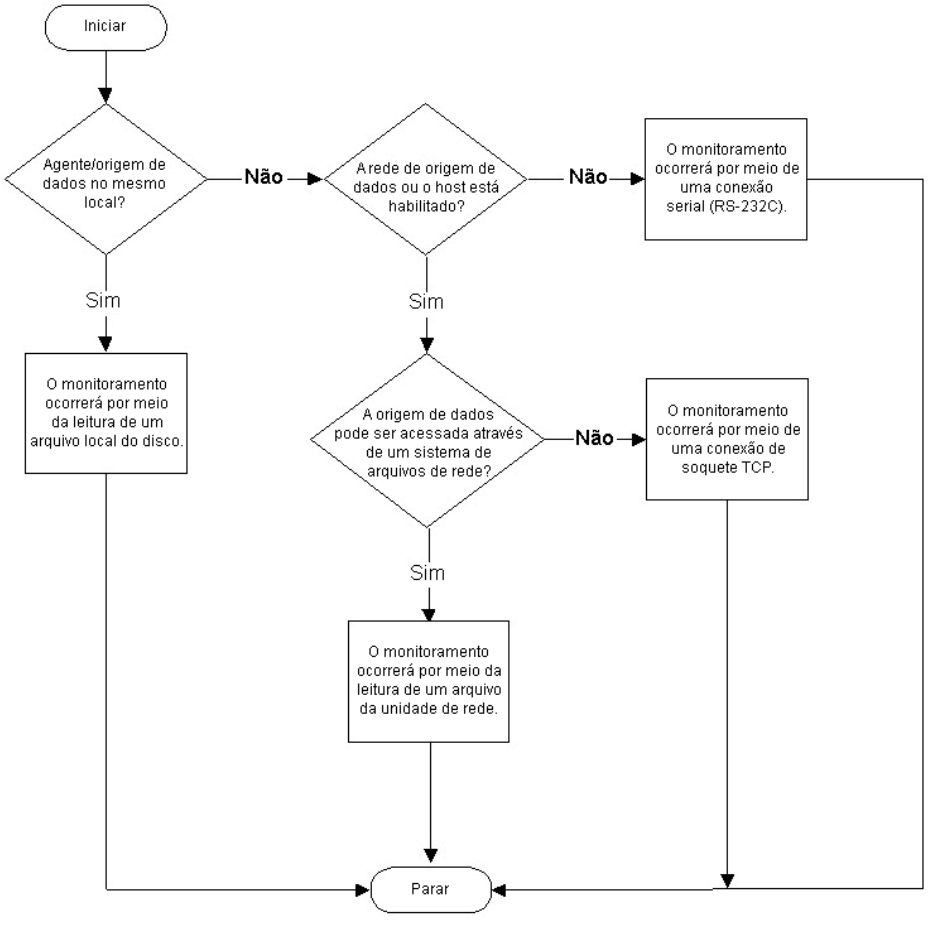
As etapas básicas da construção de coletores são:

- Criação e configuração de um arquivo de gabarito, inclusive de pontos de decisão baseados no modo de aplicação de estados.
- Criação e configuração de um arquivo de parâmetro
- Criação e configuração de um arquivo de pesquisa (opcional)
- Construção de um script
- Atribuição de uma seqüência de inicialização
- Criação de uma porta, atribuição do coletor à porta e inicialização da porta

Etapas básicas da implementação de coletores

As etapas básicas a seguir destinam-se à implementação de um coletor.

- Determinar o que deve ser monitorado
- Determinar como monitorar os dados
- Determinar o sistema operacional do produto
  - Se o host e o produto estiverem no mesmo local, a forma mais lógica de obter os dados é lê-los no arquivo de registro do produto.
  - Se o host e o produto não estiverem na mesma máquina, os dados necessários poderão ser obtidos por meio de uma configuração de sistema de arquivos de rede (como compartilhamento NFS, Samba ou SMB)
- Construir os coletores e inicializar as portas.
- Se forem usados hosts remotos, fazer upload dos arquivos de coletores para esses hosts remotos. Inicializar a porta para executar os scripts de inicialização; as informações coletadas serão relatadas por meio do sistema Sentinel.



Construindo um Coletor

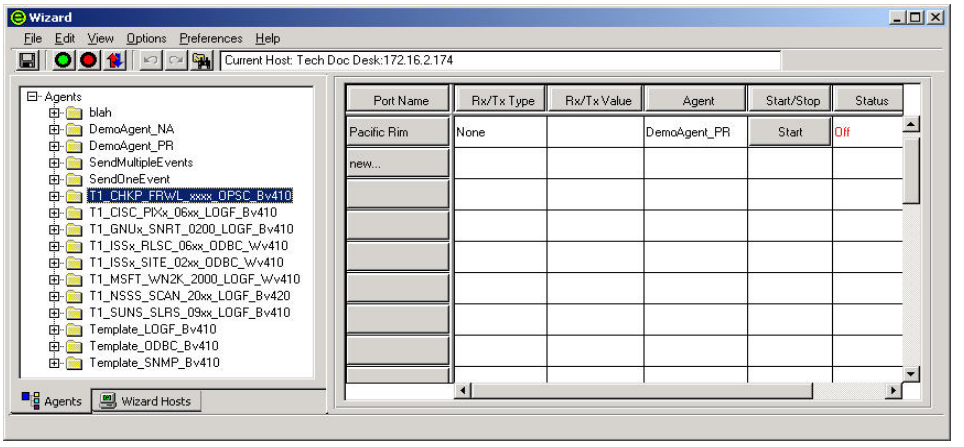
Conforme explicado anteriormente, a construção de um coletor exige a criação do seguinte:

- Arquivos de gabarito
- Arquivos de parâmetro
- Arquivos de pesquisa (opcional)
- Scripts
- Atribuição de um nome de porta do Assistente a um coletor

Criando e configurando arquivos de gabarito

Criando e configurando arquivos de gabarito

1. Inicie o Construtor de Coletor.
2. Clique na guia *Coletores* para abrir o painel da árvore Coletores.
3. Na árvore Coletores, clique o botão direito do mouse em *Coletores* e depois clique em *Novo Coletor*.
4. Digite o nome do novo coletor no espaço fornecido e pressione Enter.
5. Clique o botão direito do mouse no novo coletor e clique em *Novo Gabarito*.



6. Na caixa Novo Gabarito na árvore Coletores, digite o nome de um novo gabarito e pressione Enter.
7. Selecione o novo gabarito e clique na guia *Editor de Gabaritos*.
8. No painel *Editor de Gabaritos*, arraste e solte estados na área de edição usando os botões de estado à esquerda do painel. Para obter informações sobre a adição de estados a um gabarito, consulte Adicionando um estado a um arquivo de gabarito.
9. Clique em *Gravar*.

Adicionando um estado a um arquivo de gabarito

O processamento de todos os coletores começa no estado 1, independentemente do local onde esse estado é exibido no gabarito. Supondo que o estado 1 é um estado de processamento, insira o novo estado após o estado 1.

O Construtor de Coletor atribui automaticamente o número 1 ao primeiro estado. É recomendável que esse primeiro estado contenha somente um comando de análise BREAKPOINT(). A colocação de apenas um ponto de interrupção após o Estado 1 facilita a depuração. Durante a depuração, o analisador pára automaticamente no estado seguinte.

Ao construir um gabarito, comece com um estado de análise 'ponto de interrupção somente'. Em seguida, adicione o estado de trabalho (estado Receber, estado Analisar etc.) no Estado 2. Se precisar adicionar um estado ao início do gabarito, insira-o após o BREAKPOINT somente.

Não apague o estado de análise 'BREAKPOINT somente', a menos que seja necessário adicionar outro estado no início do gabarito. Opcionalmente, você pode digitar comentários nesse estado 'BREAKPOINT somente' sobre a funcionalidade do gabarito.

Como adicionar um estado a um gabarito

1. Clique na guia *Coletores* para abrir o painel de árvore Coletores.
2. Na árvore Coletores, selecione um gabarito para exibir o Editor de Gabaritos no painel direito.
3. Clique em *Opções > Adicionar Estado > Transmitir, Receber, Decidir, Analisar, Avançar, Ir para ou Parar,* conforme o necessário, ou clique nos botões apropriados.
   -  Transmitir
   -  Receber

-  Decidir
-  Analisar
-  Avançar
-  Ir Para
-  Parar

4. Usando os painéis de edição na parte inferior do painel Editor de Gabaritos, insira o novo código em cada estado ao adicioná-lo.

   Outro método é arrastar e soltar um botão Estado de Análise do lado esquerdo do Editor de Gabaritos na área de edição.

NOTA: Não use aspas como parte da string conclusiva no estado de recebimento (para fazer a correspondência do delimitador em um arquivo de registro, por exemplo) ou em um estado de decisão; caso contrário, você receberá a seguinte mensagem de erro:

```
***ERRO: Lendo arquivo de gabarito..."
```

Quando uma ou mais aspas são colocadas na string conclusiva ou do delimitador, ocorre a seguinte falta de correspondência entre as aspas:

```
StateDecideString: "test"123"
```

A solução é usar \22\ em vez de aspas (").

NOTA: Se você selecionar outro item na guia Coletores (mesmo que seja no mesmo coletor) e depois retornar ao gabarito irregular, o Construtor de Coletor gerará essa mensagem de erro e não exibirá partes nem estados do gabarito. O erro ocorre porque o caractere de aspas (") é usado para delimitar valores de campos em um arquivo .tem. Por exemplo:

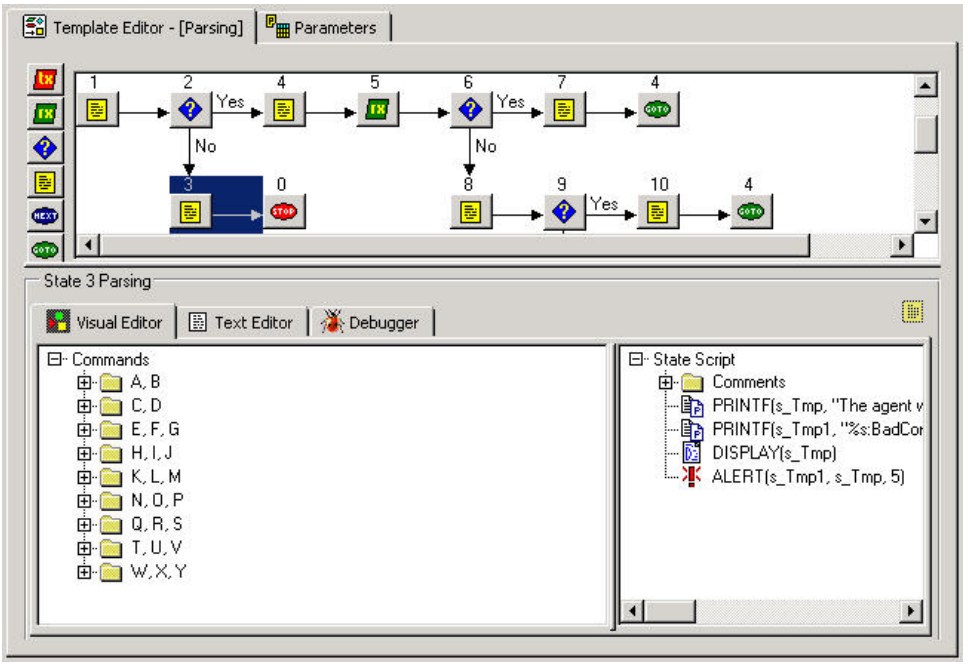
```
StateDecideString: "test"
StateDelimiterString: "123"
```

Digitando um comando de análise no Editor Visual

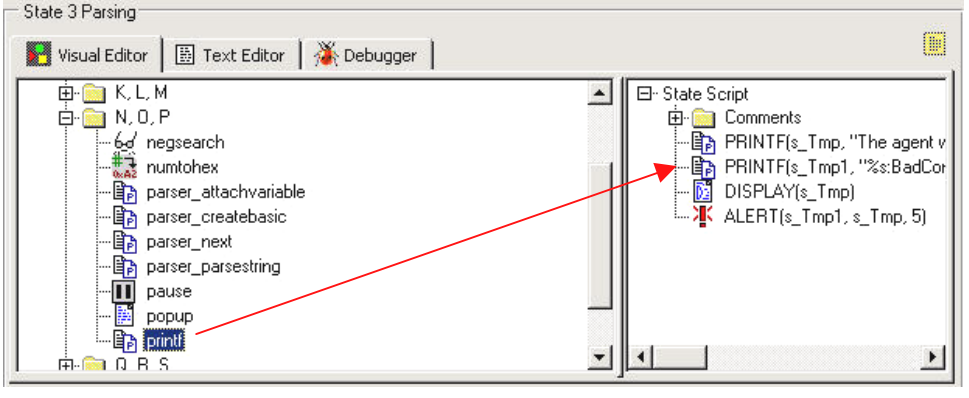
Existem dois métodos para digitar um comando de análise: usando o Editor Visual ou o Editor de Texto. Não use mais do que 4096 comandos.

Digitando um comando de análise no Editor Visual

1. Selecione um estado de análise no Editor de Gabaritos. A guia Editor Visual é aberta por padrão quando você clica em um gabarito para abri-lo.



2. No Editor Visual, arraste os comandos de análise para o lado direito do painel.



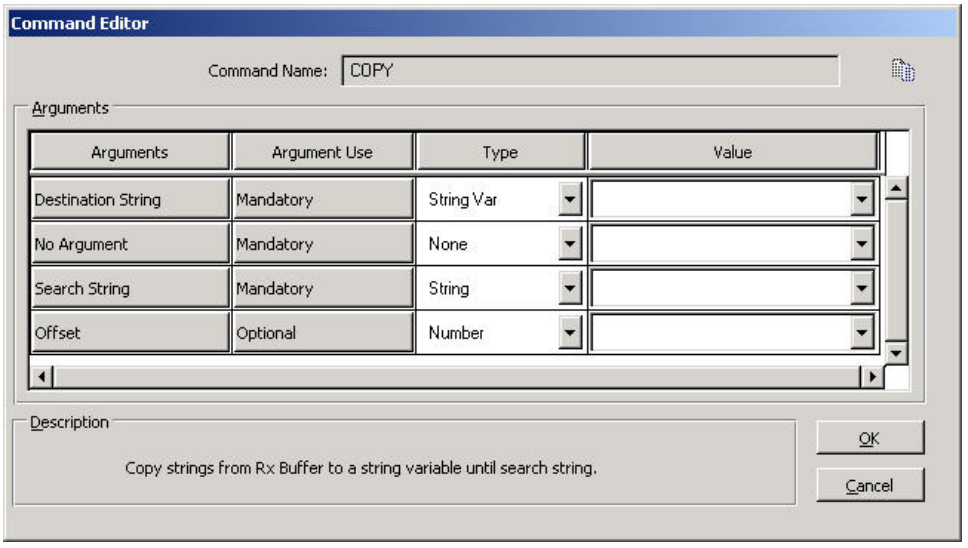
3. Digite os valores dos argumentos na janela Editor de Comandos Popup.
   - Selecione um tipo – os tipos para cada comando de análise são descritos no Guia de Referência do Usuário do Sentinel.
   - Especifique um valor – os valores são definidos para um aplicativo específico. Exemplos de valores para cada comando de análise estão contidos no Guia de Referência do Usuário do Sentinel.

Digitando um comando de análise via Editor de Texto

1. Clique na guia *Editor de Texto* no Editor de Gabaritos.
2. Digite manualmente os comandos de análise.

   Use a tecla Tab do teclado para alinhar o texto quando estiver usando uma fonte fixa. Copie, corte e cole funções de opções como faria em qualquer editor de texto padrão.

Editando um comando de análise



- Argumentos – Inclui todos os argumentos possíveis para o comando de análise selecionado no Editor Visual.
- Uso de Argumento – Define se o argumento é obrigatório ou opcional.
- Tipo – Determina o tipo de variável; por exemplo, strings, variáveis de strings, números, variáveis de números, flutuantes, variáveis de flutuantes ou variáveis predefinidas.
- Valor – Valor definido para a variável cujo nome é exibido na coluna Tipo.

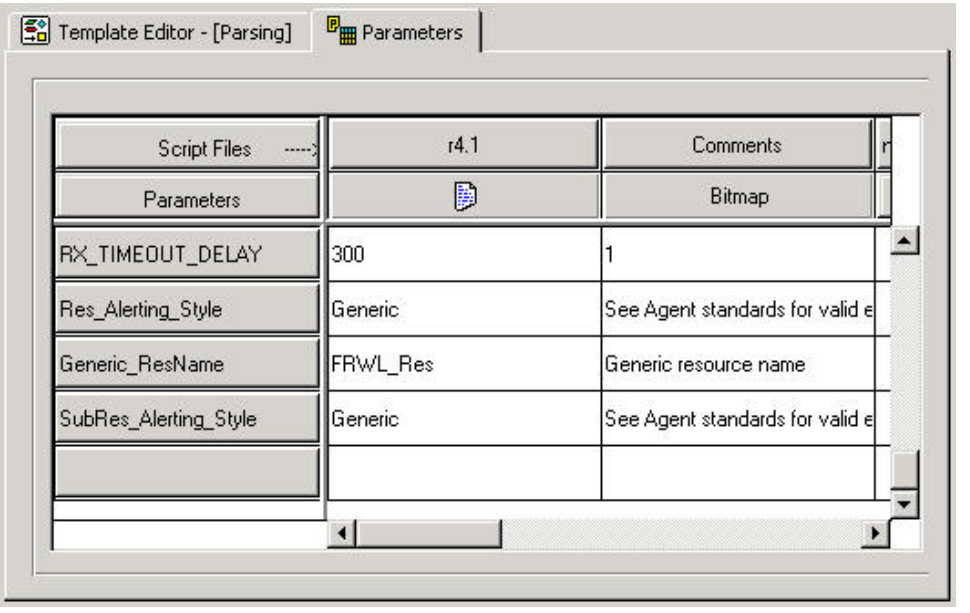
Editando um comando de análise

1. No Editor Visual:
   - Clique o botão direito do mouse em um comando de análise e escolha *Adicionar à Lista de Análise do Estado*.
   - Clique duas vezes em um comando de análise para abrir o Editor de Comando.
2. Preencha as caixas Tipo e Valor para completar a edição. Para obter mais informações sobre as descrições dos comandos de análise, consulte o Guia de Referência do Usuário do Sentinel.

Criando e configurando arquivos de parâmetro

Criando e configurando arquivos de parâmetro

1. Clique na guia *Coletores*.
2. Selecione um gabarito e clique na guia *Parâmetros* no painel direito.



3. Clique duas vezes no botão *Novo...* na primeira coluna da tabela Parâmetros.
4. Digite o nome do novo parâmetro (esse é o nome do script, como r4.1) e pressione Enter.
5. (Opcional) Clique o botão direito do mouse no botão *Bitmap* (segunda coluna/segunda linha) e clique em *Atribuir Bitmap*. Na caixa de diálogo Atribuição de Bitmap, selecione um botão *Bitmap*.
6. Clique duas vezes em cada uma das novas caixas de parâmetro e digite os valores apropriados.
7. Após a definição de todos os valores, o parâmetro e o arquivo de gabarito precisam ser compilados para a criação de um script. Vá para a seção Construindo Scripts.

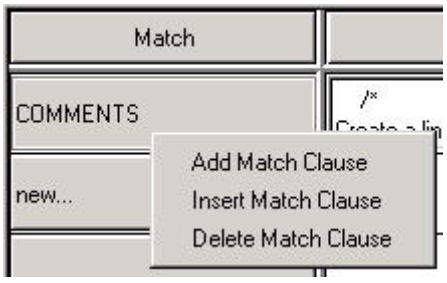
Criando e configurando arquivos de pesquisa

Esse é um procedimento opcional.

Criando e configurando arquivos de pesquisa

1. Clique na guia *Coletores* para abrir o painel de árvore Coletores.
2. Clique o botão direito do mouse em um coletor e clique em *Novo Arquivo de Pesquisa*.
3. Na caixa Novo Arquivo de Pesquisa, digite o nome de um novo arquivo de pesquisa e pressione Enter.
4. Na coluna Correspondência, clique duas vezes em *Novo...*, digite a string correspondente e pressione Enter. É possível adicionar, inserir e apagar cláusulas decorrespondência.
   - Adicionar – na coluna Correspondência, clique o botão direito do mouse em uma cláusula de correspondência e clique em *Adicionar Cláusula de Correspondência*.

- Inserir – na coluna Correspondência, clique o botão direito do mouse em uma cláusula de correspondência e clique em *Inserir Cláusula de Correspondência*.
- Apagar – na coluna Correspondência, clique o botão direito do mouse em uma cláusula de correspondência e clique em *Apagar Cláusula de Correspondência*.



5. (Opcional) Para digitar comandos de análise, clique o botão direito do mouse na coluna Análise para abrir o Editor Visual. Para obter informações sobre o uso do Editor Visual, consulte Digitando comandos de análise usando o Editor Visual.
6. Selecione os comandos de análise e complete-os na janela Editor de Comando. Os comandos são exibidos na coluna Análise.
7. Após a definição de todos os valores, é necessário compilá-los para criar um script. Vá para a seção Construindo scripts.

Scripts

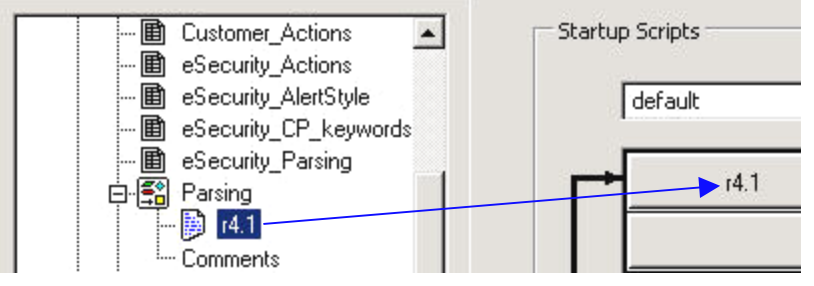
Os scripts são gerados com base em gabaritos. É possível gerar vários scripts com base em um gabarito. O Gerenciador do Coletor permite:

- Construir um script
- Depurar um script
- Atribuir uma seqüência de inicialização a um script

Construindo scripts

Construindo um script

1. Clique na guia *Coletores* para abrir o painel de árvore Coletores.
2. No painel esquerdo, selecione o gabarito com base no qual você está construindo os scripts.
3. Selecione *Arquivo* > *Criar Scripts*.
4. Na guia Editor de Gabaritos, arraste um script do gabarito para a coluna Scripts de Inicialização ou Scripts de Backout no painel direito.



Os scripts são executados na ordem em que são exibidos nas colunas Scripts de Inicialização e Scripts de Backout. Para reorganizar a ordem dos scripts, arraste-os para cima ou para baixo nas colunas.

NOTA: O script final de uma seqüência de backout precisa terminar com o estado de processamento de parada.

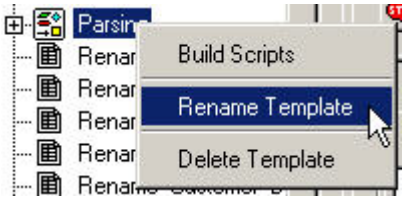
5. (Opcional) Depure usando o depurador.
6. Clique em *Arquivo* > *Gravar*.
7. Para que as mudanças tenham efeito, pare e inicie a porta usando os botões Parar e Iniciar na barra de ferramentas.

Habilitando o AutoBuild para coletores anteriores à Versão 5.0

A habilitação do recurso AutoBuild permite ignorar a etapa da criação do script quando coletores são configurados e distribuídos.

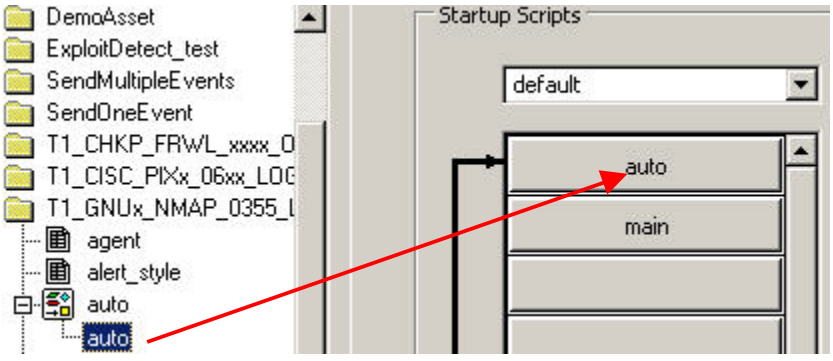
Para habilitar o AutoBuild para coletores anteriores à Versão 5.0

1. Copie os seguintes arquivos de um coletor v5.* existente e cole-os no coletor desejado para habilitar o AutoBuilding.
   - auto.tem
   - auto.asd
   - auto.lkp
   - auto.par
2. Renomeie o arquivo de gabarito como main.tem. Você pode fazer isso no Construtor de Coletor.



3. Realce o arquivo de gabarito renomeado e clique na guia *Parâmetros*. Mude o cabeçalho de coluna com o nome do arquivo de script (por exemplo, r4.1) para principal e pressione a tecla Enter.

4. Clique no botão *Gravar*.
5. Na cadeia de inicialização, clique o botão direito do mouse e arraste o auto.asd antes do principal.



Depurando um script

Quando o processo de depuração é iniciado, o status da porta é definido como “Depurar” no painel Informações de Porta. Para depurar um script, consulte Depurando uma Porta do Assistente, no Capítulo 2.

Atribuindo uma seqüência de inicialização a um script

Caso deseje que uma porta seja executada na inicialização, você pode atribuir uma seqüência de inicialização para que execute um conjunto específico de scripts na inicialização. Uma seqüência de inicialização é um arquivo que contém os nomes dos scripts a serem executados na inicialização.

Atribuindo uma seqüência de inicialização a um script

1. Clique o botão direito do mouse no nome de um script na árvore Coletores e selecione Nova Seqüência de Inicialização. A caixa de diálogo Nova Seqüência de Inicialização é exibida.
2. Na caixa de diálogo Nova Seqüência de Inicialização, digite o nome da seqüência e clique em *OK*. O nome da nova seqüência de inicialização é adicionado ao menu na parte superior do painel Scripts de Inicialização. As restrições a seguir se aplicam aos nomes de seqüências:
   - Não use inicialização nem backout como nomes de seqüências.
   - Não use nomes de seqüências duplicados no mesmo coletor.
3. Arraste os nomes dos arquivos de script da árvore Coletores para a coluna Scripts de Inicialização. Os scripts são executados na ordem em que são exibidos na coluna, de cima para baixo.
4. Para reorganizar a ordem dos scripts, arraste-os da coluna ou clique o botão direito do mouse no painel *Scripts de Inicialização* e selecione *Reordenar Scripts de Inicialização.*

Criando uma porta do Assistente

É possível criar mais de uma porta para um coletor. Para alguns tipos de sensores, talvez seja necessário criar mais de uma instância do mesmo coletor e atribuir cada instância a uma porta diferente.

O tipo de conexão de uma porta determina como os dados de segurança e as informações serão lidos, e quando uma conexão será estabelecida. Os tipos de conexão são:

- Tipo de conexão serial
- Tipo de conexão de soquete
- Tipo de conexão de novo arquivo
- Tipo de conexão de todos os arquivos
- Tipo de conexão de processo persistente
- Tipo de conexão de processo transitório
- Tipo de conexão de detecção de SNMP
- Tipo de conexão inexistente

Tipo de conexão serial

O tipo de conexão serial será usado se dados forem lidos em uma porta serial RS-232C (através de um cabo serial ou de conexão via modem). É necessário especificar a porta serial apropriada (por exemplo, COM1, COM2) na caixa Valor de Rx/Tx. O host que executa o produto a ser monitorado também precisa ter uma conexão serial com o host do coletor, através de um cabo serial diretamente ou através de modems em cada ponta da conexão.

Quando esse tipo de conexão é usado, talvez seja necessário fazer outras modificações e entradas.

Tipo de conexão de soquete

O tipo de conexão de soquete será usado se os dados forem lidos de uma conexão de soquete TCP. É necessário especificar o endereço IP e o número da porta TCP do host remoto na caixa Valor de Rx/Tx. O endereço IP e o número da porta TCP precisam ser separados por dois-pontos. Por exemplo, para especificar a porta SMTP, digite o seguinte na caixa Valor de Rx/Tx:

```
<endereço IP>:<porta>
```

Você também pode precisar colocar um processo de servidor de soquete TCP no host remoto e configurá-lo para que forneça dados à porta TCP.

Para obter mais informações sobre a configuração de coletores com esse tipo de conexão, consulte a documentação do coletor (como Collectors Snort, Cisco PIX e Solaris Syslog), localizada em:

```
%workbench_home%\elements\<Nome do coletor>\docs
```

Tipo de conexão de novo arquivo

O tipo de conexão de novo arquivo é usado para ler somente dados de evento de segurança que são adicionados a um arquivo depois que o script é iniciado. Essa conexão abre esse arquivo e lê a partir do final do arquivo. É necessário especificar o caminho para o arquivo de registro na caixa Valor de Rx/Tx.

Para obter mais informações sobre a configuração de coletores com esse tipo de conexão, consulte a documentação do coletor (como Collector Solaris Syslog), localizada em:

```
%workbench_home%\elements\<Nome do coletor>\docs
```

Tipo de conexão de todos os arquivos

O tipo de conexão de todos os arquivos é usado para ler todos os dados de evento de segurança de um arquivo.

Selecione Novo Arquivo ou Todos os Arquivos para digitar arquivo de entrada ou arquivo de saída na caixa Valor de Rx/Tx. O formato é o seguinte:

```
arquivo de entrada, arquivo de saída
```

ou

```
arquivo de entrada
```

ou

```
arquivo de saída
```

Se você selecionar Novo Arquivo ou Todos os Arquivos e o arquivo diminuir, o arquivo será lido do início.

Para obter mais informações sobre a configuração de coletores com esse tipo de conexão, consulte a documentação do coletor (como Collectors Solaris Syslog e Registro de Eventos do Windows 2000), localizada em:

```
%workbench_home%\elements\<Nome do coletor>\docs
```

Tipo de conexão de processo persistente

O tipo de conexão de processo persistente é usado para iniciar um processo persistente quando a porta é iniciada. O processo comunica-se entre o Coletor designado a essa porta e um aplicativo externo através de estados de recebimento e transmissão.

Um processo persistente é iniciado no primeiro estado de leitura/gravação e continua a ser executado durante a vida útil da porta. O processo é encerrado pela porta como parte de seu processo de encerramento. Quando a porta pára, um evento do nível 5 é enviado. Quando a porta é iniciada, um evento do nível 1 é enviado.

Para obter mais informações, vá para a seção Processos persistentes e transitórios. Para obter informações sobre a configuração do valor de Rx/Tx para esse tipo de conexão, vá para seção Configurando o valor de Rx/Tx para conexão persistente e transitória (Tipo Rx/Tx). Para obter mais informações sobre a configuração de coletores com um tipo de conexão persistente, consulte a documentação do coletor (como Collector Check Point Firewall e VPN), localizada em:

```
%workbench_home%\elements\<Nome do coletor>\docs
```

Tipo de conexão de processo transitório

O tipo de conexão de processo transitório é usado para iniciar um processo transitório quando a porta é iniciada. O processo comunica-se entre o Coletor designado a essa porta e um aplicativo externo através de estados de recebimento e transmissão.

Um processo transitório pode ser iniciado várias vezes. O processo é encerrado pela porta como parte de seu processo de encerramento.

NOTA: Se você selecionar o processo persistente ou o processo transitório, o valor de Rx/Tx deverá incluir o caminho e o nome do arquivo do processo a ser executado. Você pode usar o caminho completo e o nome do arquivo ou um caminho relativo e o nome do arquivo (para %WORKBENCH_HOME%). Por exemplo:

Caminho completo:

```
C:\Arquivos de Programas\Cisco\Csids_client – start
```

Caminho relativo:

```
.\elements\Cisco\Csids_client – start
```

No caso do processo persistente, será pressuposto o processo relativo, a menos que o valor de Rx/Tx seja digitado como o caminho completo.

Encerramento de processo transitório – Se o processo transitório parar antes do encerramento do analisador, será reiniciado no próximo estado de leitura ou gravação, sem o envio de eventos.

Para obter mais informações, vá para a seção Processos persistentes e transitórios. Para obter informações sobre a configuração do valor de Rx/Tx para esse tipo de conexão, vá para a seção Configurando o valor de Rx/Tx para conexão persistente e transitória (Tipo Rx/Tx).

Tipo de conexão de detecção de SNMP

O tipo de conexão de detecção de SNMP é usado para receber as detecções de SNMP v1, v2 e v3. Essas detecções são enviadas por sensores ao endereço IP do servidor do Assistente. Com base no endereço IP e no identificador de objetos (OID) do dispositivo de envio, o Gerenciador de Coletor permite a análise por meio do coletor apropriado. O estado Rx (análise) transmite dados de detecção de SNMP de entrada ao coletor.

As informações usadas para coletar e analisar as detecções de SNMP v1 e v3 são todas configuráveis:

- As detecções de SNMP v1 são identificadas usando o endereço IP e o identificador de objetos (OID), juntamente com um código de detecção.
- As detecções de SNMP v2/v3 são identificadas usando o endereço IP, o nome de segurança, o ID de mecanismo, as chaves de autenticação e criptografia (caso estejam habilitados na detecção) e o identificador de objetos (OID) da detecção.

Em termos de valores de detecção, o formato original da detecção é mantido com a maior proximidade possível. O formato normalmente é definido na MIB (management information base - base de gerenciamento de informações) para o sensor que originou a detecção.

Consulte Configuração de Detecção de SNMP para obter mais informações.

Tipo de conexão inexistente

O tipo de conexão inexistente é usado sem uma porta de comunicação. É mais eficiente porque não tenta se conectar. Esse tipo de conexão deverá ser usado se um coletor não usar o estado Recebimento e apenas processar comandos.

Para obter informações mais detalhadas sobre a configuração de coletores com o tipo de conexão inexistente, consulte a documentação do coletor (como Collectors ISS RealSecure e ISS SiteProtector), localizada em:

```
%workbench_home%\elements\<Nome do coletor>\docs
```

Criando, atribuindo, iniciando e parando uma porta do Assistente

Criando uma porta do Assistente

1. Consulte a documentação dos coletores localizada em %workbench_home%\elements\<Nome do coletor>\docs para obter informações sobre a configuração de coletores.
2. Clique na guia *Coletores* e selecione um coletor.
3. No Construtor de Coletor, clique na guia Hosts do Assistente para selecionar um host.
4. No painel Informações de Porta à direita, clique duas vezes em *Novo*, digite o nome da porta e pressione Enter.
5. Selecione um tipo de Rx/Tx.
6. Especifique opções de configuração com base no tipo de conexão selecionado:
   - Para conexões seriais e de soquete – Na caixa Nome da Porta, clique o botão direito do mouse no nome da porta e selecione *Editar Valor de Rx/Tx*. Especifique um dos seguintes conjuntos de opções:
     - Para conexões seriais – Selecione a taxa de transmissão, o tamanho de palavra, a paridade e os bits de fim. Clique em OK.
     - Para conexões de soquete – Digite o endereço IP e o número da porta da máquina do host, separados por dois-pontos. Se nenhum estado de recebimento for usado, defina o tipo como Nenhum e clique em *OK*.
   - Para todos os outros tipos de conexão – Clique duas vezes na célula *Valor de Rx/Tx*, digite as informações apropriadas e pressione Enter.
   - No caso do tipo de conexão de detecção de SNMP, consulte Configuração de Detecção de SNMP.
7. Clique duas vezes na célula Coletor e selecione o nome de um coletor.
8. Clique o botão direito no mouse no nome da porta e clique em *Outras Opções de Porta*. A caixa de diálogo Outras Opções de Porta é exibida.
9. Nessa caixa de diálogo, marque ou desmarque a caixa de seleção *Executar Porta na Inicialização*, selecione uma *Seqüência de Inicialização e* clique em *OK*.
10. Se estiver criando uma porta para o host local, clique em *Arquivo* > *Gravar* e selecione *Informações de Porta*.

    Se estiver criando uma porta para um host remoto, clique em *Arquivo* > *Upload/Download*.

    A porta é adicionada ao painel Informações de Porta. Não é necessário reiniciar o sistema para implementar a nova porta. Clique em *Iniciar* para mudar o status da nova porta de Desligado para Ligado.

Processos persistentes e transitórios

Usando o processo persistente ou o processo transitório, o Assistente é capaz de interagir com outro aplicativo usando scripts que recebem ou transmitem dados e analisam respostas. Cada um desses scripts é executado em uma porta separada, e cada porta é conectada aum aplicativo específico.

NOTA: Outro aplicativo é especificado na caixa Valor de Rx/Tx.

Os nomes de processos podem incluir os seguintes itens:

- Espaços
- Barras e barras invertidas (para atender a vários sistemas operacionais)
- Argumentos de comandos
- Os caminhos absoluto e relativo (a variável de ambiente WORKBENCH_HOME é considerada HOME relativa)

Quando ocorre um estado de recebimento/transmissão (Rx/Tx), o processo especificado na caixa Valor de Rx/Tx é iniciado. Quando o analisador é encerrado, o mesmo ocorre com o processo.

Quando um processo persistente é encerrado, um evento do nível 5 é enviado. Quando um processo persistente é iniciado, um evento do nível 1 é enviado.

A saída padrão (stdout) do processo persistente/transitório é conectada ao estado de "leitura" de recebimento do analisador. A entrada padrão (stdin) do processo persistente/transitório é conectada ao estado de "gravação" de transmissão do analisador.

Configurando o valor de Rx/Tx para a conexão persistente e temporária (Tipo Rx/Tx)

Existem três processos de conector disponíveis durante a configuração de conexões persistentes e transitórias. São elas:

- DBConnector (conector do processo JDBC)
- Cliente Lea
- RDEP (Remote Data Exchange Protocol - Protocolo de Intercâmbio de Dados Remotos)

Não use aspas na caixa Valor de Rx/Tx para processos persistentes e transitórios. Se o processo for um caminho absoluto para um nome executável longo com espaços, digite-o sem aspas. Por exemplo:

```
%WORKBENCH_HOME%\e-security\elements\checkpoint\lea_clien
   t checkpoint\lea_client.conf –new
```

Não use espaços em argumentos para o executável na caixa Valor de Rx/Tx. Como esses argumentos são delimitados por espaços, se contiverem espaços o software admitirá a existência de dois argumentos onde só há um. Se os argumentos estiverem passando no local do arquivo de configuração, como para Ponto de Verificação, use um caminho relativo de %WORKBENCH_HOME%. Por exemplo:

```
checkpoint/\lea_client checkpoint/\lea_client.conf -new
```

DBConnector

O DBConnector (um conector de processos JDBC) executa um cliente que se conecta a um servidor de banco de dados, executa uma consulta SQL no banco de dados e retorna o resultado à saída padrão no formato nome-valor-par. A consulta SQL para execução é lida na entrada padrão ou em um arquivo. O nome no resultado nome-valor-par é extraído do nome da coluna do conjunto de resultados. Por isso, o nome de coluna desejado deve ser declarado explicitamente no SQL. A sintaxe exata varia de acordo com o servidor de banco de dados.

Esse aplicativo é instalado com o Gerenciador de Coletor em $WORKBENCH_HOME/dbconnector.

Para obter mais informações sobre o uso do DBConnector, consulte o arquivo README que acompanha o aplicativo, a documentação de coletores do Sentinel para Entercept Host IDS 4.0 (via JDBC), ou acesse o eSecurity Customer Portal: http://www.esecurityinc.com.

Cliente Lea

O lea_client do Sentinel usa a API de Exportação de Registros do OPSEC para extrair dados do Check Point Firewall-1 e gerá-lo no formato nome-valor-par. O lea_client geralmente é usado para alimentar dados no coletor do Check Point Firewall-1 do Sentinel, no qual os dados são normalizados e, dependendo da ação do evento (por exemplo, eliminar, rejeitar ou aceitar), um alerta é enviado ao Sentinel Server.

Esse aplicativo é instalado com o Gerenciador de Coletor em $WORKBENCH_HOME/checkpoint.

Para obter mais informações sobre o Ponto de Verificação lea_client, consulte o arquivo README que acompanha o aplicativo, a documentação de coletores do Sentinel para Check Point Firewall & VPN Collector (via OPSEC), ou acesse o eSecurity Customer Portal: http://www.esecurityinc.com.

RDEP

O rdep_client, um aplicativo Java, extrai dados de sensores remotos do Cisco IDS v4.0 que executam RDEP. O rdep_client se conecta ao sensor IDS remoto usando uma conexão HTTP ou HTTPS. Após a conexão do cliente, ele abre uma inscrição ou usa uma inscrição aberta anteriormente. A inscrição descreve o tipo de dados que o sensor IDS enviará ao cliente. Para modificar o tipo de dados a ser recuperado por uma nova inscrição, edite o arquivo de configuração rdep_client. Usando a inscrição, o cliente inicia uma solicitação de dados de evento do sensor IDS. Os dados de evento são retornados pelo sensor IDS em formato XML, convertido no formato nome-valor-pares pelo cliente RDEP do Sentinel e depois, analisados e normalizados pelo coletor. O coletor repassa o evento normalizado ao Sentinel.

Esse aplicativo é instalado com o Gerenciador de Coletor em $WORKBENCH_HOME/cisco/rdep_client.

Para obter mais informações sobre RDEP, consulte o arquivo README que acompanha o aplicativo, a documentação de coletores do Sentinel para Cisco IDS 4.0 (via RDEP), ou acesse o eSecurity Customer Portal: http://www.esecurityinc.com.

Configuração de Detecção de SNMP

O Sentinel é capaz de receber detecções de SNMP que representem eventos de segurança que tenham ocorrido em um sensor em uma rede. Esses eventos são enviados ao Sentinel por uma rede usando o protocolo SNMP. As v1, v2 e v3 do SNMP são aceitas. Para habilitar o Sentinel a receber detecções de SNMP, é necessário criar um coletor do Assistente que use o tipo de conexão (Rx/Tx) de detecção de SNMP.

Você pode definir as configurações de detecção de SNMP para especificar os parâmetros que permitirão aos coletores de SNMP do Assistente repassar detecções ao Sentinel como eventos binários.

A janela Configuração de Detecção de SNMP é usada para definir configurações para coletores de SNMP do Assistente, inclusive a porta usada para detecções de SNMP, códigos de detecção, autenticação e informações de criptografia.

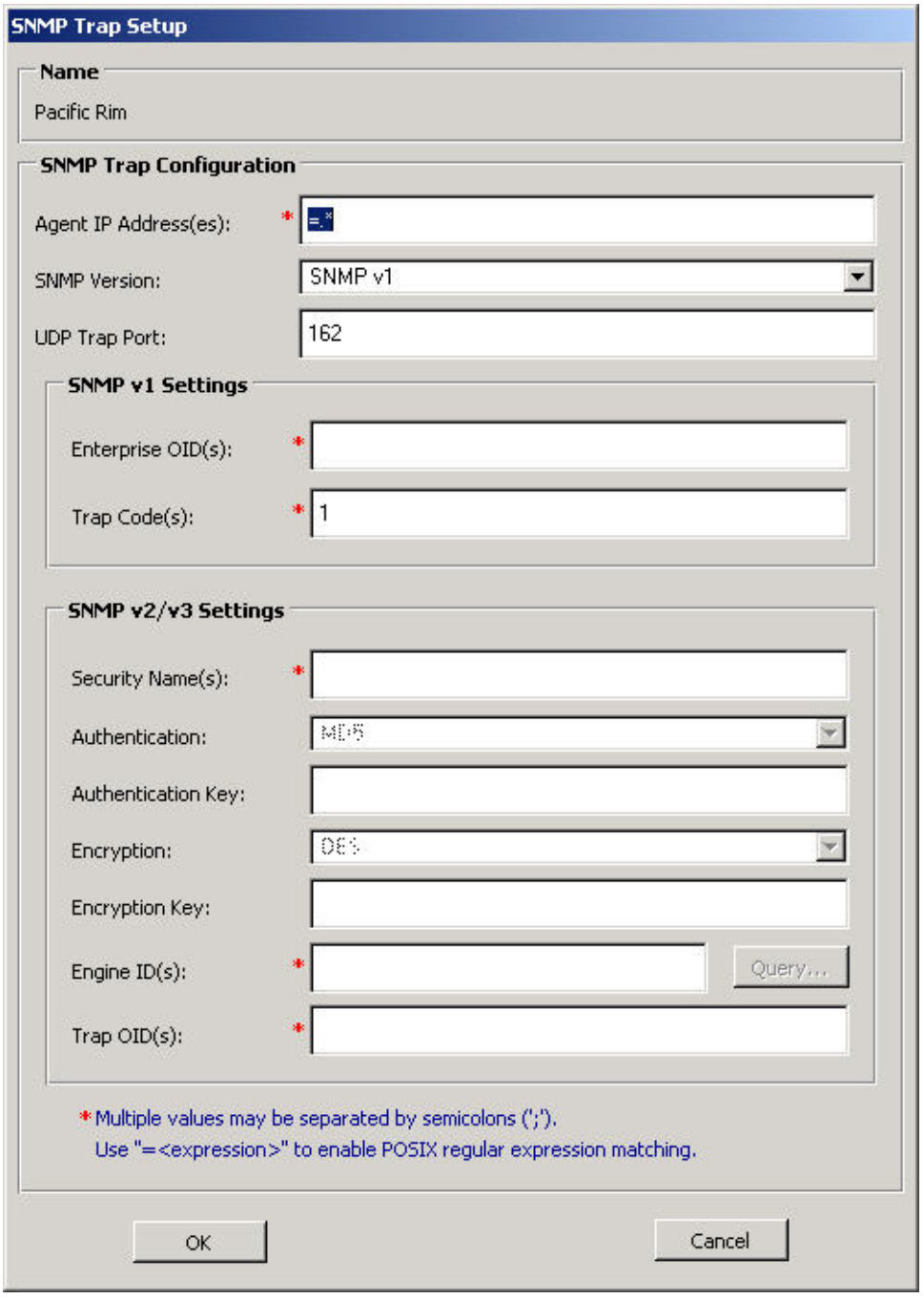
Como acessar a janela Detecção de SNMP

1. No Construtor de Coletor, atribua um nome de porta ao coletor de SNMP.
2. Em Tipo de Rx/Tx, selecione Detecção de SNMP.
3. Clique o botão direito do mouse no nome da porta e selecione *Editar Valor de Rx/Tx*.
4. Digite as informações de SNMP.

   NOTA: A porta de detecção de UDP padrão é 162. Verifique se essa porta está disponível. Em caso negativo, você pode escolher outro número de porta.

   NOTA: Diferentemente de outras portas de coletores, o campo Valor de Rx/Tx será preenchido de acordo com suas configurações da janela Configuração de Detecção de SNMP. No caso de um coletor de SNMP, não é possível editar manualmente o campo Valor de Rx/Tx.
5. O coletor de SNMP é gravado e seu upload é feito.
6. Para ativar esse coletor, pare e reinicie o Gerenciador de Coletor.

   NOTA: Para ativar esse coletor, é necessário parar e reiniciar o Gerenciador de Coletor conforme a etapa 6.



A configuração de SNMP consiste em:

- Endereço(s) IP do coletor
- Versão SNMP
- Porta de detecção de UDP
- Configurações de SNMP v1
  - OID(s) da empresa
  - Código(s) de detecção

- Configurações de SNMP v2/v3
  - Nome(s) de segurança
  - Autenticação
  - Chave de autenticação
  - Criptografia
  - Chave de criptografia
  - ID(s) de mecanismo com botão de consulta
  - OID(s) de detecção

Na caixa de diálogo Configuração de Detecção de SNMP (para abri-la, clique o botão direito do mouse no nome de uma porta no painel Informações de Porta do Construtor de Coletor e clique em Editar Valor de Rx/Tx), é possível configurar o Assistente para:

- Receber detecções em portas diferentes da porta UDP 162 (o padrão).
- Criar um script único de análise de Assistente para processar detecções de vários endereços IP, com informações como vários códigos de detecção e vários identificadores de objetos de detecção (OIDs).
- Permitir a correspondência de expressões regulares POSIX no endereço IP, no identificador de objeto de empresa (OID), no código de detecção e nos campos de OID de detecção.
- Após decodificar a detecção, o Assistente define valores para variáveis contidas no script.

Endereço(s) IP de coletores

Endereço(s) IP de coletores são endereços IP desejados para o recebimento de detecções. Separe os vários valores com um ponto-e-vírgula (;). Você pode usar o formato =<expressão> para fazer a correspondência de expressões regulares compatíveis com POSIX. O asterisco (*) é um modificador do caractere ou da expressão precedente e o ponto final (.). Poderá ser usado como um caractere curinga e poderá aparecer em qualquer parte da string se expressões regulares forem usadas.

As expressões regulares mais comuns que poderão ser usadas são:

`=`	corresponde a seqüências de caracteres de qualquer tamanho.
`= 192\.168.*`	corresponde a seqüências de caracteres que contêm 192.168. Para obter “começa com o comportamento”, use: ^192.168... Em que ^ é a âncora de início de linha. Para obter “termina com o comportamento”, use 0.47$... Em que $ é a âncora de final de linha.
`= [abc]`	corresponde a a, b ou c.
`= [a-zA-Z0-9]`	corresponde a qualquer caractere único do alfabeto. (maiúscula ou minúscula) ou qualquer dígito de 0 a 9.

Basicamente, as regras dos exemplos acima de expressões regulares comuns são:

. corresponde a qualquer caractere.

* corresponde a zero ou mais ocorrências do padrão precedente.

[] corresponde a qualquer caractere único do padrão definido entre parênteses.

NOTA: Essas regras podem ser combinadas.

Versão de SNMP

Somente uma versão de SNMP pode ser configurada. As opções dos painéis Configurações de SNMP v1 e Configurações de SNMP v2/v3 são habilitadas com base na versão selecionada.

Porta de detecção de UDP

O padrão da porta de destino UDP é 162.

Configurações de SNMP v1

Essas configurações somente serão habilitadas se você selecionar SNMP v1 na lista de Versões de SNMP.

- OID(s) de empresa - ID(s) de objeto usados para identificar o tipo de coletor que enviou a detecção. Separe os vários valores com um ponto-e-vírgula (;).
- Código(s) de detecção - Códigos de detecção para sensores que enviam as detecções de SNMP. Esses códigos de detecção representam os tipos de detecção enviados pelo coletor de SNMP específico. Separe os vários valores com um ponto-e-vírgula (;).

Configurações de SNMP v2/v3

- Nome(s) de segurança - Nome de usuário usado para acessar o coletor. Os nomes de segurança distinguem maiúsculas de minúsculas. Separe os vários valores com um ponto-e-vírgula (;).
- Autenticação - Método de autenticação. Os valores são:
  - Nenhum - Nenhuma autenticação é realizada nas detecções do SNMP v3.
  - MD5 – O nome de segurança é configurado para usar o algoritmo MD5 a fim de criar uma assinatura digital para autenticação.
- Chave de autenticação - Senha usada para autenticar o usuário no coletor. Habilitada somente se a autenticação for a MD5. Precisa ter no mínimo oito caracteres. As chaves de autenticação distinguem maiúsculas de minúsculas. A mesma chave precisa ser configurada no coletor de SNMP de envio.
- Criptografia - Método de criptografia. Os valores são:
  - Nenhum - Nenhuma criptografia é realizada nas detecções de SNMP v3
  - DES - Espera receber detecções criptografadas com o método de criptografia DES (Data Encryption Standard - Padrão de Criptografia de Dados).
- Chave de criptografia - Chave usada para decodificar detecções enviadas a coletores do Assistente. Precisa ter no mínimo oito caracteres. A chave de criptografia distingue maiúsculas de minúsculas. Habilitada somente se o DES for selecionado na lista Criptografia.

- ID(s) de mecanismo - Identificador exclusivo de um coletor de SNMP v3. Há um botão Consulta de ID de Mecanismo que procura o endereço IP a ser consultado. Uma consulta bem sucedida retorna as informações e adiciona o ID do mecanismo. Se houver um ID de mecanismo na caixa, um novo será anexado.
- OID(s) de detecção - ID de objeto da detecção que especifica o tipo de detecção recebido.

NOTA: Se forem especificados vários nomes de segurança e IDs de mecanismo, o mesmo esquema de autenticação e criptografia será usado para todos.

NOTA: Se forem necessárias diferentes chaves de autenticação e criptografia para diferentes coletores de SNMP, portas separadas deverão ser configuradas para cada uma.

Variáveis de detecção de SNMP

Algumas variáveis de detecção são válidas para todas as detecções (SNMP v1 e v3) e algumas são válidas somente para uma versão. As tabelas a seguir listam todas as variáveis de detecção de SNMP, agrupadas pela versão de SNMP com que trabalham:

- Variáveis de detecção para SNMP v1 e v3
- Variáveis de detecção para SNMP v1
- Variáveis de detecção para SNMP v3

Variáveis de detecção para SNMP v1 e v3

Variável	Descrição
`s_Trap_IP`	Endereço IP do coletor/sensor que enviou a detecção.
`s_Trap_Time`	Valor de uptime relatado pelo coletor/sensor que enviou a detecção. Normalmente, trata-se do tempo de execução do coletor. Formato: D:HH:MM:SS.ss (dias, horas, minutos, segundos, centésimos de segundo).
`i_Trap_Version`	Valor de uma versão de SNMP específica: 1 = SNMP v1 3 = SNMP v3
`i_Trap_Vars`	Número de vinculações de variáveis na detecção.
`s_Trap_OID[]`	Uma matriz (de tamanho “i_Trap_Vars”) dos nomes das variáveis MIB vinculadas na mensagem de detecção. Cada elemento da matriz s_Trap_OID é um OID, por exemplo “.1.3.6.1.4.1.4286....”
`s_Trap_Value[]`	Uma matriz (de tamanho “i_Trap_vars”) dos valores das variáveis MIB vinculadas na mensagem de detecção. Os índices dessa matriz e da matriz s_Trap_OID correspondem entre si de tal modo que s_Trap_OID[0] é o nome e s_Trap_Value[0] é o valor.

Variáveis de detecção para SNMP v1

Variável	Descrição
s_Trap_Ent	OID de empresa do coletor/sensor que enviou a detecção.
s_Trap_Code_Generic	Código genérico da detecção. Os valores são: 1-5 = tipos de detecção padrão, definidos por IETF (Força-tarefa de engenharia da Internet) 6 = detecção específica de empresa (o código é definido em s_Trap_Code_Specific)
s_Trap_Code_Specific	Código específico da detecção. Somente é relevante se s_Trap_Code_Generic = 6.

Variáveis de detecção para SNMP v3

Variável	Descrição
s_Trap_Engine_ID	ID de mecanismo do coletor de SNMP v3 que enviou a detecção.
s_Trap_OID	Identificador de objeto (OID) que identifica o tipo de detecção SNMP v3 recebido. Para fins de identificação de detecção, O OID da detecção de SNMP v3 assume o lugar do OID de empresa de SNMP v1 e códigos de detecção genéricos/específicos.
s_Trap_Security_Name	O nome de segurança como é conhecido o coletor de SNMP v3 que enviou a detecção.

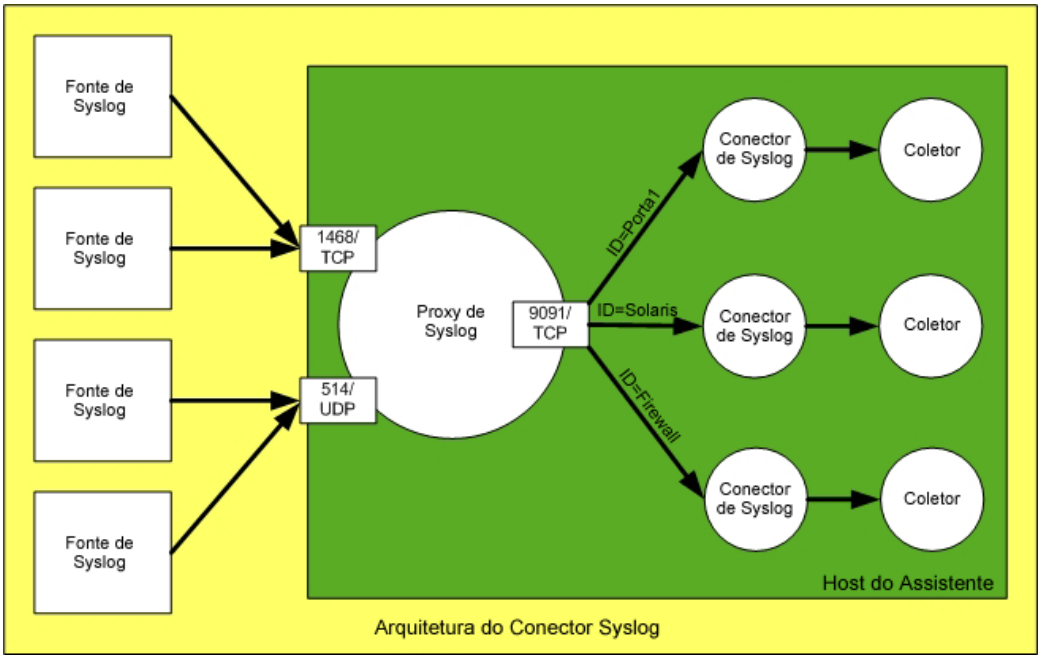
A Conector Syslog v1.0.2

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

A Novell lançou este conector syslog para facilitar a integração entre os Coletores do Sentinel e os produtos que podem gerar mensagens de syslog. O objetivo deste documento é explicar a arquitetura, a instalação, o uso e as opções do conector syslog.

Arquitetura

O conector syslog é constituído de duas partes. Uma parte é o proxy syslog e a outra é o cliente do conector syslog. O proxy syslog escuta nas portas UDP e TCP selecionadas. Por padrão, a porta UDP é a 514. A porta TCP padrão 1468 é normalmente usada pelo Cisco PIX para enviar mensagens do syslog através do protocolo TCP.



Arquitetura do Conector Syslog

As funções realizadas por cada componente do conector syslog são descritas a seguir:

- Proxy syslog
  - Escuta em uma porta TCP e/ou UDP em busca de mensagens do syslog.
  - Analisa a mensagem de entrada à procura de componentes de mensagem padrão do syslog (Prioridade, Data, Nome de Host e Mensagem)
  - Caso a origem de mensagens envie uma mensagem sem um dos componentes Prioridade, Data ou Nome de Host, ela seguirá o RFC 3164 "BSD Syslog Protocol" e inserirá dados complementares.

    - Depois de determinar o Recurso e o Nível da Prioridade, bem como o Nome de Host, o proxy publicará efetivamente a mensagem nas sessões do conector syslog que tenham interesse nela.
    - Caso termine a sessão do cliente do conector syslog, o proxy syslog colocará em fila por 10 minutos as mensagens de entrada desse cliente. Esse comportamento significa garantir que o Coletor não perca mensagens durante sua reinicialização ou interrupção temporária.
    - O proxy syslog escuta em uma porta TCP, normalmente a 9091, a fim de atender às sessões do cliente do conector syslog.
- Cliente do conector syslog
    - O conector é iniciado como um Processo Persistente com todas as opções de tempo de execução do conector syslog inseridas no valor de RX/TX.
    - O ID é um parâmetro de tempo de execução. O ID configurado para determinado conector syslog deve ser exclusivo entre todos os conectores syslog que se conectam com o mesmo proxy syslog.
    - É possível especificar um filtro de conteúdo em tempo de execução a fim de limitar o escopo das mensagens submetidas ao Coletor para análise.
    - O conector syslog estabelece uma conexão com o serviço cliente do conector proxy.
    - O conector syslog registra seu ID e filtro de conteúdo no proxy syslog.
    - As mensagens que o proxy syslog associa ao ID são lidas pelo conector syslog e direcionadas à sua saída padrão.
    - No momento, a estrutura e o conteúdo da mensagem são passados ao Coletor na forma original. Futuramente, o conector syslog poderá formatar a mensagem para atender aos requisitos de análise do Coletor.

O protocolo syslog tem sido tradicionalmente definido como um protocolo baseado em UDP. Na ausência de uma quantidade diversificada de aplicativos/dispositivos capazes de enviar mensagens através de TCP ou de um padrão reconhecido para o syslog através de TCP, foi adotada a abordagem do Cisco PIX para a terminação de mensagens do syslog (retorno de carro + alimentação de linha). A terminação de mensagens é necessária para o syslog através de TCP, já que não há um padrão definido nem um limite natural entre as mensagens. O syslog através de UDP tem uma terminação natural de mensagens, já que o pacote UDP transporta uma única mensagem e o UDP não necessita de conexão.

Fazendo e removendo instalações

O conector syslog foi criado para funcionar em qualquer plataforma do Wizard. Devido a esse requisito de portabilidade, os dois componentes foram desenvolvidos em Java. Os requisitos necessários de software e hardware estão relacionados a seguir.

Requisitos do sistema

Software

- Java 1.4.1 ou posterior
- Wizard 4.2 ou posterior
- Windows (2000/XP/2003), Solaris (8/9), RedHat Enterprise Linux (v3 ES/AS)

Hardware

- 14 MB de RAM adicional (45 MB de memória virtual) para cada instância do conector syslog e o proxy

Instalação

Os arquivos de clientes do conector e do proxy syslog são instalados automaticamente quando o Collector Service é instalado. Os arquivos do syslog estão no diretório:

Para UNIX:

```
$ESEC_HOME/wizard/syslog
```

Para Windows:

```
%ESEC_HOME%\wizard\syslog
```

O Wizard não iniciará automaticamente o proxy syslog. Se você quiser que o proxy syslog seja iniciado automaticamente, ele deverá ser instalado como um serviço. Utilize as instruções a seguir para instalar o proxy syslog como um serviço.

Instalar como Serviço do Windows (Windows)

NOTA: Para que o proxy syslog seja executado automaticamente, é possível instalá-lo como um Serviço do Windows. Para instalar o proxy syslog como um serviço, execute os seguintes comandos no prompt de comando:

1. cd /d "%ESEC_HOME%\wizard\syslog"
2. syslog-server.bat install

   Esse procedimento criará um Serviço do Windows chamado "eSecurity Syslog Server".

Instalar como serviço (UNIX)

NOTA: Para que o proxy syslog seja iniciado automaticamente durante a inicialização da máquina, é possível instalá-lo como um serviço no UNIX. Para instalar o proxy syslog como um serviço, execute os seguintes comandos:

1. Efetue login como Usuário Root.
2. cd $ESEC_HOME/wizard/syslog
3. ./syslog-server.sh install

   Esse procedimento fará com que o proxy syslog seja iniciado automaticamente durante a inicialização da máquina. Por padrão, o proxy syslog será executado como o usuário root. Isso será necessário porque o proxy syslog, por padrão, se vinculará à porta 514, o que requer privilégios de root. Para que o proxy syslog seja executado como um usuário diferente do root, modifique o script /etc/init.d/esyslogserver. Você precisará verificar se esse usuário tem privilégios para se vincular à porta em que escutará em busca de mensagens. Estes são alguns exemplos de como isso pode ser feito:

   - Use o comando "sudo" para iniciar o proxy syslog, concedendo ao usuário privilégios "sudo" para que se vincule à porta necessária.
   - Modifique a configuração do syslog (syslog.conf) e faça com que o proxy syslog se vincule a uma porta que não necessite de privilégios de root (p.ex., - >1024). Nesse caso, você provavelmente precisará redirecionar as mensagens enviadas à porta 514 para a nova porta selecionada para uso.

Desinstalação

Para desinstalar o Serviço do Windows, execute os seguintes comandos no prompt de comando:

Desinstalar como Serviço do Windows (Windows)

1. cd /d "%ESEC_HOME%\wizard\syslog"
2. syslog-server.bat remove

Desinstalar como Serviço (UNIX)

Para desinstalar o proxy syslog como um serviço, execute os seguintes comandos:

1. Efetue login como Usuário Root.
2. cd $ESEC_HOME/wizard/syslog
3. ./syslog-server.sh remove

Uso

Servidor proxy syslog

O Wizard não iniciará automaticamente o servidor proxy syslog. Se você quiser que o proxy syslog seja iniciado automaticamente, ele deverá ser instalado como um serviço.
Siga as instruções contidas na seção Instalação para instalar o proxy syslog como um serviço.

A configuração do proxy syslog é armazenada no arquivo:

Para UNIX:

```
$ESEC_HOME/wizard/syslog/config/syslog.conf
```

Para Windows:

```
%ESEC_HOME%\wizard\syslog\config\syslog.conf
```

O proxy syslog é configurado para usar a seguinte configuração por padrão:

- Escuta na porta UDP 514 para mensagens do syslog
- Escuta na porta TCP 1468 para mensagens do syslog
- Escuta na porta TCP 9091 para conexões do conector

É possível configurar o proxy syslog para escutar em outras portas de modo a receber mensagens do syslog ou aceitar conexões de clientes. Esses switches são respectivamente:

-udp <porta>	Porta a ser escutada em busca de mensagens UDP de dispositivos;514 é o padrão
-tcp <porta>	Porta a ser escutada em busca de conexões TCP de dispositivos;1468 é o padrão
-connector <porta>	Porta a ser escutada em busca de conexões TCP de conectores;9091 é o padrão

Para editar essas configurações, modifique a seguinte seção do arquivo syslog.conf:

```
wrapper.app.parameter.3=-tcp
wrapper.app.parameter.4=1468
wrapper.app.parameter.5=-udp
wrapper.app.parameter.6=514
wrapper.app.parameter.7=-connector
wrapper.app.parameter.8=9091
```

Por exemplo, se você quiser modificar as configurações da porta para o seguinte:

- Escuta na porta UDP 4514 para mensagens do syslog
- Escuta na porta TCP 4168 para mensagens do syslog
- Escuta na porta TCP 4991 para conexões do conector

A seção do syslog.conf indicada acima deve ser modificada para:

```
wrapper.app.parameter.3=-tcp
wrapper.app.parameter.4=4168
wrapper.app.parameter.5=-udp
wrapper.app.parameter.6=4514
wrapper.app.parameter.7=-connector
wrapper.app.parameter.8=4991
```

Por padrão, a configuração do proxy syslog é definida para aceitar as conexões de clientes de qualquer host. Para aumentar a segurança, é possível configurar o proxy syslog para que aceite somente as conexões de clientes que residam no mesmo host. Essa é uma precaução de segurança, já que não há privacidade, controle de acesso nem autenticação entre os conectores clientes e o proxy. Os switches a seguir realizam essa tarefa:

`-private`	Escuta em busca de conexões do conector no loopback
-shared	Escuta em busca de conexões do conector no localhost-- o padrão

O switch –shared instruirá o proxy a vincular a escuta da conexão de clientes a um soquete acessível a hosts remotos.

Para editar essas configurações, modifique a seguinte seção do arquivo syslog.conf:

```
wrapper.app.parameter.2=-shared
```

Por exemplo, para permitir somente conexões de clientes do mesmo host, você deve modificar as configurações para o seguinte:

```
wrapper.app.parameter.2=-private
```

É possível configurar o proxy syslog para incluir em um arquivo de registro todas as mensagens recebidas. O formato das mensagens aparecerá da forma que o proxy syslog usaria se tivesse de retransmitir as mensagens para outro servidor syslog. Como resultado, o <PRI> ou a Prioridade usada pelo servidor syslog receptor para avaliar o Recurso e o Nível das mensagens será apresentada no início de cada mensagem. Esse tipo de registro é habilitado pelo seguinte switch.

`-log <nome_do_arquivo>`	Nome do arquivo de registro ao qual se anexar.

Para habilitar esse tipo de registro, adicione as duas linhas a seguir ao arquivo syslog.conf após o último "wrapper.app.parameter":

```
wrapper.app.parameter.11=-log
wrapper.app.parameter.12=<nome_do_arquivo>
```

Por exemplo, para habilitar esse tipo de registro no arquivo $ESEC_HOME/wizard/syslog/messages.log, você deve modificar as configurações para o seguinte:

```
wrapper.app.parameter.7=-connector
wrapper.app.parameter.8=9091
wrapper.app.parameter.9=-messageSize
wrapper.app.parameter.10=5000
wrapper.app.parameter.11=-log
wrapper.app.parameter.12=messages.log
```

Se um caminho absoluto não for especificado para o nome do arquivo, o caminho será relativo ao diretório $ESEC_HOME/wizard/syslog.

NOTA: O arquivo de registro pode se tornar muito grande; portanto, verifique se a localização em que o arquivo será gravado tem espaço suficiente(p.ex. – um diretório diferente de $ESEC_HOME).

É recomendável que o proxy syslog seja executado com o mínimo de 64 MB e o máximo de 256 MB de memória heap JVM. Com essa configuração, você pode esperar o seguinte desempenho:

Limites do servidor proxy:

▪ Número máximo de eventos:	500 eps (total para todas as portas de clientes)
▪ Tamanho máximo do conector Q:	5000 mensagens (este será o padrão se nenhum for especificado)
▪ Máximo de conectores:	5

Para modificar as configurações de memória, edite a seguinte seção do arquivo syslog.conf:

```
# Tamanho Inicial do Heap Java (em MB)
wrapper.java.initmemory=64

# Tamanho Máximo do Heap Java (em MB)
wrapper.java.maxmemory=256
```

Cliente do conector syslog

O cliente do conector syslog se conecta ao proxy syslog que coleta as mensagens para as quais ele se inscreveu. Em seguida, as mensagens coletadas pelo cliente são enviadas à saída padrão. A sessão do cliente com o servidor não termina até que o processo do cliente ou o proxy syslog seja encerrado. Esse comportamento operacional e de saída torna-o adequado para ser usado pelo mecanismo do Coletor como um conector de Processo Persistente.

Na janela de Configuração de Porta do Construtor de Coletor, configure uma porta com um Tipo Rx/Tx de Processo Persistente e com um Valor de Rx/Tx semelhante à sintaxe genérica a seguir.

Para UNIX:

```
syslog/SyslogConnectorAgent.sh <argumentos>
```

Para Windows:

```
syslog\SyslogConnectorAgent.bat <argumentos>
```

Depois de preencher o Valor de Rx/Tx, selecione o Coletor adequado na biblioteca, faça upload da configuração da porta e, possivelmente, também do Coletor para o Wizard remoto.

O cliente do conector syslog foi criado para usar vários argumentos padrão a fim de simplificar o uso geral. A linha de comando mais simples para o cliente do conector syslog seria a seguinte:

Para UNIX:

```
syslog/SyslogConnectorAgent.sh –id “MeuIDExclusivo”
```

Para Windows:

```
syslog/SyslogConnectorAgent.bat –id “MeuIDExclusivo”
```

A interpretação dessa linha de comando é a seguinte:

- Conecte-se ao proxy syslog que escuta em 127.0.0.1:9091 em busca desta conexão
- Inscreva-se em todas as mensagens enviadas com todos os Recursos syslog possíveis
- Inscreva-se em todas as mensagens enviadas com todos os Níveis syslog possíveis
- Inscreva-se em todas as mensagens, independentemente do endereço IP de origem contido no cabeçalho IP.
- Inscreva-se em todas as mensagens, independentemente da designação de host contida na mensagem.
- Atribua a esses parâmetros de inscrição de sessão o ID “MeuIDExclusivo"

A sessão do cliente do conector syslog será registrada no proxy syslog com o filtro de inscrição acima, com o ID “MeuIDExclusivo”. O ID é necessário. O ID escolhido foi arbitrário, mas deve ser exclusivo entre todas as sessões de clientes do conector syslog com o mesmo proxy syslog. Se outro cliente do conector syslog for configurado com o mesmo ID, uma das duas conexões será rompida. Permanecerá a última sessão a ser conectada com o mesmo ID.

O filtro genérico no filtro anterior poderá desperdiçar o esforço de processamento do Coletor se as mensagens que atenderem aos requisitos do filtro, que são todas as mensagens recebidas, não forem relevantes para essa operação específica do Coletor. No exemplo acima, deve ser óbvio que a expressão de filtro é muito versátil. O exemplo a seguir, para UNIX, estabelece um descrição precisa albeit mais restritiva de quais mensagens são relevantes para o Coletor.

```
syslog/SyslogConnectorAgent.sh -facilities
   "usuário,kernel" -levels "aviso,erro" -sender
   "192.16.0.12,192.16.0.0/16" -host
   "17.16.8.0/24,10.1.1.13" -id "MeuOutroIDExclusivo"
```

A interpretação dessa linha de comando é a seguinte:

- Conecte-se ao proxy syslog que escuta em 127.0.0.1:9091 em busca desta conexão
- (-facilities) Inscreva-se em todas as mensagens enviadas com Recursos de usuário ou kernel
- (-levels) Inscreva-se em todas as mensagens enviadas com Níveis de aviso ou erro
- (-sender) Inscreva-se em todas as mensagens identificadas pelo endereço IP de origem das mensagens recebidas no proxy syslog. Esse argumento tem a aparência do proxy syslog nas informações do cabeçalho IP para avaliar esses critérios. Isso permite que o filtro acomode os servidores de retransmissão syslog; os servidores de retransmissão não se identificam nas mensagens retransmitidas por eles. Embora esse argumento tenha sido criado para acomodar as mensagens retransmitidas, ele pode ser usado para filtrar as mensagens enviadas diretamente da origem do syslog. Especificamente, os servidores de retransmissão ou as origens do syslog relevantes são 192.16.0.12 e 192.16.0.0/16. Na verdade, o segundo item representa uma faixa de endereços IP; desde que o endereço IP de origem esteja entre 192.16.0.0 e 192.16.255.255, essas mensagens passarão nos critérios de filtro. Os nomes de host não são válidos, pois nenhuma resolução de nomes de host é realizada para determinar os nomes de host dos endereços IP de origem.
- (-host) Inscreva-se nas mensagens que contêm o designador de host 17.16.8.0/24 ou 10.1.1.13 na mensagem do syslog. O primeiro item é uma faixa de endereços IP. Se a mensagem contiver um designador de host na forma de endereço IP e estiver dentro da faixa de 17.16.8.0 a 17.16.8.255, a mensagem passará por essa condição no filtro. Os nomes de host são aceitos pelo argumento –host. O nome do host pode ser designado literalmente ou por uma expressão regular. Lembre-se de que nenhuma resolução de nome de host é realizada também para esse argumento. Ninguém pode esperar que, em virtude da configuração de um nome de host ou de um endereço IP, o filtro acomode o esquema de nomeação oposto. Por exemplo, a configuração do –host 172.16.0.90 não fará com que um filtro encontre uma mensagem que contenha o nome de host “testbox1”, mesmo que os serviços de resolução de nomes tenha mapeado o 172.19.0.90 para “testbox1”. Portanto, a designação do host IP só corresponderá aos endereços IP, e a designação de nome de host só corresponderá aos nomes de host.

O filtro do exemplo acima pode ser descrito na seguinte expressão Booleana:

```
(Recurso=”usuário” ou Recurso=”kernel”) e (Nível=”aviso”
   ou Nível=”erro”) e (Remetente=”192.16.0.12” ou
   Remetente=192.16.0.0/16”) e (Host=”17.16.8.0/24” ou
   Host=”10.1.1.13”)
```

O número de combinações possíveis desses argumentos é o produto Cartesiano de tipos de argumento, onde cada tipo de argumento é um conjunto. De acordo com PRINCIPIA CYBERNETICA WEB (http://pespmc1.vub.ac.be/ASC/CARTES_PRODU.html) o produto Cartesiano é:

> “A coleção de todos os n-tuples solicitados que podem ser formados, de modo que contenham um elemento do primeiro conjunto, um elemento do segundo e um elemento do conjunto n-th. Essa coleção pode ser considerada como a constituição de um espaço n-dimensional em que cada n-tuple designa uma célula. O produto Cartesiano mais simples de dois conjuntos é uma tabela bidimensional ou uma tabulação cruzada cujas células podem ser usadas para inserir freqüências, para designar possibilidades (consulte

"relação") ou impossibilidades (consulte "restrição") ou para dispor em gráfico as transições que abrangem o comportamento de um sistema. (Krippendorff)"

NOTA: Na data de publicação deste documento, o site na Web mencionado acima estava correto.

Isso implica que, teoricamente, muito poucas mensagens distintas podem passar por esse filtro. Somente condições operacionais práticas poderão realmente determinar o número de mensagens distintas.

Além dos argumentos de filtro da linha de comando, há também os seguintes argumentos opcionais:

`-proxy <endereço_do_servidor>:<porta #>`	O endereço do host e o número da porta do servidor proxy syslog.
`-log <nome_do_arquivo>`	Habilita o registro no arquivo especificado.

O argumento –proxy é usado para configurar o cliente do conector para que se conecte a uma porta TCP não-padrão ou a um host diferente do localhost. Por padrão, o proxy syslog espera que haja uma conexão do cliente do conector na porta 9091. Caso a porta 9091 não seja adequada para o host em que o proxy syslog está sendo executado, a porta poderá ser ajustada durante a inicialização desse proxy e, usando o argumento –proxy, os clientes podem ser instruídos a se conectar a essa porta alternativa. Além disso, o host de destino do cliente do conector pode ser especificado como um host que não seja o do sistema local.
Caso o proxy syslog aceite sessões de clientes do conector remoto, um desses clientes poderá ser configurado para estabelecer uma sessão com esse proxy syslog remoto.
O endereço IP e a porta do cliente do conector do proxy syslog poderá ser configurada com o argumento proxy.

O argumento –log habilita o recurso de registro do cliente do conector. Esse cliente gravará as mensagens logo que forem recebidas do proxy syslog. Diferentemente do arquivo de registro do proxy syslog, o conteúdo da mensagem será filtrado pelos detalhes de inscrição registrados, e cada mensagem registrada não conterá o campo <PRI> ou Prioridade.
O conteúdo será consistente com o que o Coletor receber do mesmo cliente do conector syslog.

NOTA: O arquivo de registro pode se tornar muito grande; portanto, verifique se a localização em que o arquivo será gravado tem espaço suficiente(p.ex. – um diretório diferente de $ESEC_HOME).

Este é um exemplo, em UNIX, de como usar os argumentos –proxy e –log:

```
syslog/SyslogConnectorAgent.sh –proxy localhost:9091 –log
   connector_messages.log –id "MeuIDExclusivo"
```

Configurando o registro do servidor proxy syslog

O servidor Proxy Syslog imprime mensagens de registro no arquivo:

```
$ESEC_HOME/wizard/syslog/syslog_trace*.*.log
```

Para modificar os níveis do registro, basta editar o respectivo arquivo de propriedades:

```
$ESEC_HOME/wizard/syslog/syslog_log.prop
```

Esse é o arquivo de propriedades de registro, conforme especificado pela seguinte linha do arquivo syslog.conf:

```
wrapper.java.additional.1=-
   Djava.util.logging.config.file=syslog_log.prop
```

Faça modificações na seção a seguir para ajustar os níveis de registro:

```
###### Configure os níveis de registro
# As regras de nível de registro são lidas de cima para
   baixo.  Comece com as mais gerais e depois passe para
   as mais específicas.
…
######
```

Exemplo de argumentos da linha de comando

É possível executar o servidor Proxy Syslog e o conector cliente sem usar os scripts fornecidos na instalação. Para fazer isso, será necessário usar os argumentos da linha de comando encontrados nesta seção.

Proxy syslog:

```
java –server –Xms64m –Xmx256m –
   Djava.util.logging.config.file=syslog-logger.prop -jar
   syslog.jar [-udp <porta>] [-tcp <porta>] [-connector
   <porta>] [-private|-shared] [-log <caminho_do_arquivo>]
   [-messageSize <número>]
```

Argumentos válidos:

`-server`	Sempre deve ser usado. Usado pela JVM
`–Xms64m`	Especifica o tamanho inicial da memória do proxy syslog. Recomenda-se 64 megabytes.
`–Xmx256m`	Especifica o tamanho máximo da memória do proxy syslog. O padrão recomendado é 256 megabytes. Permite que o servidor proxy lide com oscilações nos volumes de dados, com vários conectores clientes e com buffers se houver reconexão dos conectores. Esse valor poderá ser mudado para um número superior se houver memória e volumes de dados disponíveis, bem como a conexão do número de conectores clientes. O valor não deve exceder 1.2 Gigabytes por servidor proxy syslog , isto é, '–Xmx1200m'
`–Djava.util. logging.config. file`	Esta propriedade especifica o nome do caminho/arquivo de configuração do registro de depuração. Portanto, ele precisa apontar para a localização do arquivo. Se nenhum caminho for especificado, ele procurará no diretório atual em que a JVM foi executada. Exemplo: %workbench_home%\syslog-logger.prop

`-udp <porta>`	Porta a ser escutada em busca de mensagens UDP de dispositivos;514 é o padrão
`-tcp <porta>`	Porta a ser escutada em busca de conexões TCP de dispositivos;1468 é o padrão
`-connector <porta>`	Porta a ser escutada em busca de conexões TCP de conectores;9091 é o padrão
`-private`	Escuta em busca de conexões do conector no loopback-- é o padrão
`-shared`	Escuta em busca de conexões do conector no localhost. Se não for definido, será gerado um erro de comunicação.
`-log`	Nome de um arquivo de registro ao qual se anexar
`-help`	Apresenta esta mensagem de ajuda
`-version`	Apresenta a versão do proxy (0.91-poc)
`-messageSize`	Número de mensagens armazenadas no buffer para serem enviadas novamente em virtude das conexões temporariamente perdidas. O tamanho máximo é 5000, sem vírgulas. Se o valor da opção não for usado ou se esse valor for maior que 5000, o comando assumirá 5000 como padrão.

Cliente do conector syslog:

```
java -jar syslogconnector.jar -id <IdExclusivo> [-proxy
   <host:número_da_porta>] [-facilities
   <facility1,facility2,…>] [-levels <nível1, nível2,…>]
   [-sender <Source IP1[/integer subnet mask], Source
   IP2[/integer subnet mask],…>] [-host < IP1[/integer
   subnet mask]|Hostname1 | Hostname Regex1, IP2[/integer
   subnet mask]|Hostname2 | Hostname Regex2, …>] [-log
   <caminho_do_arquivo_de_registro>]
```

Argumentos válidos:

`-proxy <host:número_da_porta>`	O proxy Syslog a ser conectado com o host:porta; o padrão é 127.0.0.1:9091
`-facilities <recurso1,recurso2,…>`	Lista separada por vírgulas com os recursos desejados. O padrão são todos os recursos
`-levels <nível1, nível2,…>`	Lista separada por vírgulas com as gravidades desejadas. O padrão são todos os níveis
`-sender <Source IP1[/integer subnet mask], Source IP2[/integer subnet mask],…>`	Lista separada por vírgulas com os remetentes desejados. O padrão são todos os remetentes
`-host < IP1[/integer subnet mask]|Hostname1 | Hostname Regex1, IP2[/integer subnet mask`	Lista separada por vírgulas com os hosts desejados. O padrão são todos os hosts
`-log <caminho do arquivo de registro>`	Nome de um arquivo de registro ao qual se anexar

`-id <IdExclusiva>`	Especifica a identidade do conector (OBRIGATÓRIO)
`-help`	Apresenta esta mensagem de ajuda
`-version`	Apresenta a versão do conector (0.91-poc)

Tabela de recursos aceitos

Os nomes de recursos não diferenciam maiúsculas de minúsculas quando especificados na linha de comando do cliente do conector syslog.

KERNEL	UUCP	LOCAL0
USER	CRON	LOCAL1
MAIL	SECURITY	LOCAL2
DAEMON	FTP DAEMON	LOCAL3
AUTH	NTP	LOCAL4
SYSLOG	LOG AUDIT	LOCAL5
LPR	LOG ALERT	LOCAL6
NEWS	CLOCK DAEMON	LOCAL7

Tabela de níveis aceitos

Os nomes de níveis não diferenciam maiúsculas de minúsculas quando especificados na linha de comando do cliente do conector syslog.

EMERGENCY	WARNING
ALERT	NOTICE
CRITICAL	INFORMATIONAL
ERROR	DEBUG

Notas de distribuição

Mensagens retransmitidas ao proxy syslog

A maioria dos servidores syslog consegue direcionar as mensagens do syslog recebidas para um servidor syslog alternativo, bem como processar essas mensagens. Em um cenário de distribuição, pode ser atraente alterar um host de registro existente para permitir a retransmissão de mensagens ao proxy syslog. Alguns servidores syslog têm comportamentos inconvenientes que podem prejudicar essa opção de distribuição.

Observou-se que as bibliotecas do servidor syslog do Solaris 7.9 e do Linux 8 (que pode ser representante de outras versões distribuídas) não colocam o nome nem o endereço IP do host nas mensagens enviadas do host. O servidor syslog receptor associa o endereço IP de origem ou o nome do host (através da resolução de nomes) às mensagens recebidas nos arquivos de registro gerados por ele. Caso o Solaris 9 atue como um retransmissor para o proxy, ele não preencherá as mensagens que encaminha para o proxy, nem com o endereço IP nem com o nome de host da origem da mensagem. Isso é estranho, pois o arquivo de registro no sistema Solaris 9 mostra um endereço IP ou um nome de host. Sem o nome de host complementar na mensagem, o proxy syslog é forçado a deduzir a mensagem originada do servidor de retransmissão, e não do host original. O proxy syslog complementará cada mensagem recebida de um retransmissor Solaris 9 com o endereço IP do host

de retransmissão. As conseqüências dessa ação são sérias. A origem de um evento de segurança não fica visível para o Coletor e, conseqüentemente, a solução do Sentinel.

É altamente recomendável que o proxy não seja destinatário de mensagens retransmitidas se estas não contiverem o endereço IP nem o nome do host da verdadeira origem. Essa recomendação poderá ter conseqüências logísticas significativas se o proxy for utilizado na produção.

Exemplo:

Ocorre um evento su no ultrabookIIi (172.16.0.70) em execução no Solaris 7, que está encaminhando mensagens do syslog ao talkabout (172.16.0.72) em execução no Solaris 9, que, por sua vez, está fazendo retransmissões para o proxy syslog. A seguir estão as mensagens geradas pelo conector do Sentinel.

Proxy:

```
<37>Apr 02 06:54:11 [172.16.0.72.151.234] su: 'su root'
   succeeded for oespadm on /dev/pts/0
```

Cliente do conector:

```
Apr 02 06:54:11 [172.16.0.72.151.234] su: 'su root'
   succeeded for oespadm on /dev/pts/0
```

A seguir está o rastreamento de pacotes da mesma mensagem que chega primeiro no talkabout e, em seguida, é retransmitida ao proxy syslog em pes020.esecurity.net.

```
# snoop -x0 udp port 514
Using device /dev/dmfe0 (promiscuous mode)
ultrabookIIi -> talkabout    SYSLOG C port=42830 <37>Apr
   1 18:54:11

0: 0000 83cd 1395 0040 2082 202b 0800 4500     .......@ .
   +..E.
16: 0061 fa09 4000 ff11 28d3 ac10 0046 ac10
   .aú.@...(....F..
32: 0048 a74e 0202 004d 5d7e 3c33 373e 4170
   .H.N...M]~<37>Ap
48: 7220 2031 2031 383a 3534 3a31 3120 7375    r  1
   18:54:11 su
64: 3a20 2773 7520 726f 6f74 2720 7375 6363    : 'su root'
   succ
80: 6565 6465 6420 666f 7220 6f65 7370 6164    eeded for
   oespad
96: 6d20 6f6e 202f 6465 762f 7074 732f 30      m on
   /dev/pts/0
```

```
talkabout -> pes020.esecurity.net SYSLOG C port=38890
   <37>Apr  1 18:54:11

0: 000a 5e02 a335 0000 83cd 1395 0800 4500
   ..^..5........E.
16: 0061 304b 4000 ff11 f031 ac10 0048 ac10
   .a0K@....1...H..
32: 02a6 97ea 0202 004d 6a82 3c33 373e 4170
   .......Mj.<37>Ap
48: 7220 2031 2031 383a 3534 3a31 3120 7375    r  1
   18:54:11 su
64: 3a20 2773 7520 726f 6f74 2720 7375 6363    : 'su root'
   succ
80: 6565 6465 6420 666f 7220 6f65 7370 6164    eeded for
   oespad
96: 6d20 6f6e 202f 6465 762f 7074 732f 30      m on
   /dev/pts/0
```

O seguinte foi registrado no talkabout:

```
Apr  1 18:54:11 ultrabookIIi su: 'su root' succeeded for
   oespadm on /dev/pts/0
```

B Configurando um servidor de soquete em um host UNIX

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

O servidor de soquete fornece um ponto de extremidade para conexões de soquete provenientes do Gerenciador de Coletor do Assistente UNIX. Por exemplo, se você quiser monitorar um arquivo de registro ou uma caixa UNIX em um Assistente remoto e tiver de ultrapassar um firewall para acessar a porta nessa caixa.

As instruções a seguir servem para configurar um servidor de soquete em um host UNIX, e você monitorará um arquivo de registro ASCII nesse host.

Para configurar o processo de um servidor de soquete em um host UNIX

1. Crie o script que fornecerá os dados à conexão de soquete TCP. Para isso, crie um novo arquivo de texto e copie para ele as linhas a seguir, substituindo <arquivo_de_registro> pelo nome do caminho completo do arquivo que você deseja monitorar:

   ```
   #!/bin/sh
   /bin/tail -f <arquivo_de_registro>
   ```

   Grave o arquivo (o caminho e o nome do arquivo são arbitrários), mas ele deve estar em uma localização em que não seja eliminado, e seu nome deve refletir sua função: Por exemplo:

   ```
   /usr/local/bin/logfileserver
   ```

2. Escolha uma porta TCP sem privilégios no host UNIX e use-a para o processo do servidor. O número da porta sem privilégios é um número arbitrário entre 1025 e 65.535. Para verificar se esse número já está em uso, adote o seguinte comando (substituindo <número_da_porta> pela porta desejada):

   ```
   netstat -an | grep LISTEN | grep <número_da_porta>
   ```

   Se uma linha como a seguir for apresentada como saída, a porta estará em uso e, portanto, você terá de escolher outra.

   ```
   *.5555*.*0000 LISTEN
   ```

3. Como usuário root, edite o arquivo /etc/services e adicione uma entrada no final do arquivo para seu novo serviço de soquete. O exemplo a seguir adiciona uma linha para um serviço chamado “syslog_monitor”, configurado para escutar na porta TCP 5555:

   ```
   syslog_monitor5555/tcp
   ```

4. Edite o arquivo /etc/inetd.conf e adicione uma entrada no final do arquivo para seu novo serviço de soquete. O exemplo a seguir adiciona uma linha referente a um serviço chamado “syslog_monitor,” configurado para executar o script /usr/local/bin/in.syslog_monitor.

   A linha a seguir deve ser inserida como campos separados por tabulações em uma única linha no arquivo, independentemente da paginação mostrada.

   ```
   syslog_monitor stream tcp nowait nobody
      /usr/local/bin/in.syslog_monitor in.syslog_monitor
   ```

5. Execute o seguinte comando para habilitar o processo do servidor de soquete:

   ```
   kill -HUP `/bin/ps -ef | grep inetd | grep -v grep |
      awk '{print $2}'`
   ```

6. Experimente o servidor de soquete. Para fazer isso, utilize o telnet para a porta escolhida, e o conteúdo de seu arquivo de registro será exibido:

   ```
   % telnet localhost 5555
   ```

   Para interromper a sessão telnet, execute ^] (control-]) e, depois, digite quit no prompt telnet>.