Novell® Sentinel™

5.1.3

www.novell.com

Volume IV – Guia de Referência do Sentinel

7 de julho de 2006

Novell®

Informações legais

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

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

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

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

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

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

Marcas registradas da Novell

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

Materiais de terceiros

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

Informações legais de terceiros

O Sentinel 5 pode conter as seguintes tecnologias de terceiros:

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

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

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

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

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

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

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

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

Prefácio

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

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

- Volume I – Guia de Instalação do Sentinel™ 5
- Volume II – Guia do Usuário do Sentinel™ 5
- Volume III – Guia do Usuário do Assistente do Sentinel™ 5
- Volume IV – Guia de Referência do Usuário do Sentinel™
- 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 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
- Tags META do Assistente e do Sentinel
- Permissões de usuário
- Mecanismo de correlação do Sentinel
- Opções da linha de comando de correlação
- Esquema do banco de dados do Sentinel

Volume V – Guia de Integração de Terceiros do Sentinel

- Remedy
- Operações do HP OpenView
- HP Service Desk

Sumário

12 Telas do banco de dados do Sentinel para Microsoft SQL Server 12-1

1 Guia de Referência do Usuário do Sentinel™ 5

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

O Guia de Referência do Usuário do Sentinel é a sua referência para:

- Linguagem de criação de scripts do Assistente
- Comandos de análise do Assistente
- Funções do administrador do Assistente
- Tags META do Assistente e do Sentinel
- Permissões de usuário do console do Sentinel
- Mecanismo de correlação do Sentinel
- Opções da linha de comando do Sentinel
- Telas do banco de dados do Sentinel Server

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

Índice

Este guia contém os seguintes capítulos:

Convenções usadas

Nota e avisos

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

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

Comandos

Os comandos aparecem na fonte Courier. Por exemplo:

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

Outras referências do Sentinel

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

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

Entrando em contato com a Novell

- Website: 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 Linguagem de criação de scripts do Assistente

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

Este e o próximo capítulo descrevem como usar a linguagem de script do Assistente para construir scripts. Os operadores nas várias strings e os comandos de análise utilizados na construção de Coletor também são explicados.

Os seguintes itens são discutidos:

- Strings conclusivas
- Expressões regulares

Strings conclusivas

As strings distinguem maiúsculas de minúsculas.

Enquanto é feito poll dos Coletores, várias informações são coletadas no buffer de recebimento interno. As strings do tipo conclusiva especificam que uma conclusão será tomada em relação aos dados recebidos e armazenados no buffer interno. Uma string conclusiva é avaliada como verdadeira ou falsa. Se houver um erro de sintaxe ou se a caixa Tipo Conclusiva for deixada em branco, a decisão será falsa.

A string conclusiva é avaliada somente se a opção Tipo Conclusiva estiver definida como string ou dados.

Manipulando o indicador do Buffer Rx (Buffer de Recebimento)

Cada porta do Assistente possui seu próprio indicador do Buffer de Recebimento. O indicador do Buffer de Recebimento indica os bytes de dados no Buffer de Recebimento. Antes de cada string conclusiva avaliada, o indicador do Buffer de Recebimento é redefinido para o seu valor mantido (normalmente zero, a não ser que seja modificado por uma decisão que tenha utilizado o operador de pesquisa (:)).

- 0 não indica nenhum byte no buffer de recebimento
- 1 indica o primeiro byte de dados, 2 indica o segundo byte de dados, e assim por diante.

Formato

Uma string conclusiva assume a forma de uma sequência de operadores lógicos (LO) e expressões regulares.

Os operadores lógicos e os operadores de strings não precisam estar presentes em todas as seqüências. Veja a seguir algumas regras relacionadas ao uso desses operadores:

- Os operadores lógicos criam expressões booleanas (verdadeiras ou falsas) dentro da string conclusiva e são avaliados com base nas seguintes precedências:
  `~ Not`
  `& And`
- Um operador de string especifica uma string de caracteres a ser pesquisada no buffer de recebimento. A utilização do operador de strings realiza uma pesquisa byte a byte começando na posição do indicador do Buffer de Recebimento em diante.

NOTA: Como a caixa Tipo Conclusiva é cortada no último caractere imprimível, o equivalente hexadecimal a um espaço deve ser usado. O operador : não pode ser usado com o operador NULO.

Nomes de parâmetro

Para especificar um parâmetro em uma string conclusiva, o nome do parâmetro deve estar entre chaves ({ }). Quando o script é construído, o nome do parâmetro e as chaves são substituídos pelo valor do parâmetro.

Se o nome do parâmetro especificado não existir no arquivo de parâmetro do qual o script foi construído, a expressão do nome do parâmetro e as chaves permanecerão nos dados da string conclusiva.

As expressões de nome de parâmetro podem ocorrer em qualquer lugar da string conclusiva. Elas não podem, porém, ficar aninhadas (incluir outra expressão de nome de parâmetro dentro de si mesma).

Hierarquia de operações em uma string conclusiva

Cada operação em uma string conclusiva é avaliada tanto como verdadeira (1) ou falsa (0). As operações em uma string conclusiva são sempre seguidas na ordem controlada pela sintaxe do operador lógico.

- Quando mais de uma operação é usada, as avaliações de string são realizadas em ordem, da esquerda para a direita.
- Quando parênteses são usados, o operador lógico dentro de cada conjunto de parênteses é avaliado primeiro.
- As próximas operações lógicas a serem avaliadas não são (~) e (&).

Uma ordem de operação também é seguida quando é usada a sintaxe de operador de string:

- O indicador do buffer Rx redefinido é avaliado primeiro.
- Todos os outros caracteres de sintaxe possuem precedência igual e são avaliados em ordem, da esquerda para a direita.

Regras do indicador do Buffer de Recebimento

As seguintes regras controlam o indicador do Buffer de Recebimento:

- Quando a pesquisa de uma string de caracteres for realizada com êxito, a pesquisa será considerada verdadeira e o indicador do Buffer de Recebimento será posicionado no primeiro byte da string encontrada.

String Conclusiva: DE

```
 A BCDE F GH
^
 A BCDE F GH
     ^
```

- Quando a pesquisa de uma string de caracteres não for realizada com êxito, a pesquisa será considerada falsa e o indicador do Buffer de Recebimento será retornado para o valor mantido.

  String Decidir: DEJ

```
 A BCDE F GH
^
 A BCDE F GH
^
```

Verificando um Buffer de Recebimento vazio

Para verificar um buffer de recebimento vazio, use a seguinte string conclusiva:

```
NULL
```

Avaliações de string conclusiva e exemplo de resultados

Strings conclusivas alfanuméricas

Apresentamos a seguir strings conclusivas alfanuméricas para um Buffer de Recebimento de exemplo:

```
ABCDEFGHIJKLMNO (alimentação de linha) YZ<[&
```

String conclusiva	Expressão lógica	Resultado
A	1	1
P	0	0
\41\(HEX para A)	1	1
AB	1	1
\4142\(HEX para AB)	1	1
ABD	0	0
A&B	1 & 1	1
A&P	1 & 0	0
A+P	1 + 0	1
A\42\(HEX para B)	1	1
A&BC	1 & 1	1
DEF&ABC	1 & 0	0
ABC&DEF	1 & 1	1
ABC&BCD	1 & 1	1
ABC&ABC	1 & 0	0
\OA\(HEX por alimentação de linha)	1	1
NULL *	0	0

Se não forem encontrados caracteres no Buffer de Recebimento, o resultado será VERDADEIRO.

Strings conclusivas HEX

Apresentamos a seguir strings conclusivas HEX para um buffer de recebimento de exemplo (HEX):

```
02 0A 10 FF 1F 2E 3C 03
```

String decidir	Expressão lógica	Resultado
\020A\&\FF\	1 & 1	1
\02\	0	0
\02\&\03\	1 & 1	1
\03\&\02\	1 & 0	0

Expressões regulares

Caracteres especiais e sequências de caracteres são usados nos padrões de gravações de expressões regulares.

O Sentinel usa uma biblioteca compatível com POSIX (Portable Operating System Interface for UNIX – Interface de Sistemas Operacionais Portáteis para UNIX) para expressões regulares. POSIX é um conjunto de padrões IEEE e ISO que ajuda a garantir a compatibilidade entre sistemas operacionais compatíveis com POSIX, que incluem a maior parte das variantes do UNIX.

Resumo de caracteres especiais para expressões regulares

A tabela seguinte resume os caracteres especiais que podem ser usados em expressões regulares para as funções de SEARCH e REPLACE.

Caractere	Uso/Exemplo
\	Marca o próximo caractere como especial. n corresponde ao caractere "n". A seqüência \n corresponde ao caractere de alimentação de linha ou nova linha (fim de linha), mas para passar o "\" pelo analisador, você deve prefixá-lo com o caractere de exceção "/"; portanto, para passar um \n, deve usar /\n.
^	Corresponde ao início da entrada ou linha.
$	Corresponde ao final da entrada ou linha.
*	Corresponde ao caractere precedente zero ou mais vezes. go* corresponde a "g" ou "goo".
+	Corresponde ao caractere precedente um ou mais vezes. go+ corresponde a "goo", mas não a "g".
?	Corresponde ao caractere precedente zero ou uma vez. a?te? corresponde ao "te" em "eater".
.	Corresponde a qualquer caractere único, exceto o caractere nova linha (fim de linha).
x|y	Corresponde a x ou y. z|good? corresponde a "goo" ou "good" ou "z".
{n}	n é um inteiro não negativo. Corresponde exatamente n vezes. e{3} não corresponde ao "e" de "Ted", mas corresponde aos três primeiros "e"s de "greeeeeed".
{n,}	n é um inteiro não negativo. Corresponde a pelo menos n vezes. e{3} não corresponde ao "e" de "Ted" e corresponde a todos os "e"s de "greeeeeed". e{1,} é o equivalente a e+.

{n,m}	m e n são inteiros não negativos. Corresponde a pelo menos n e na maioria das m vezes. e{1,3} corresponde aos três primeiros "e"s de "greeeeeed".
[xyz]	Um conjunto de caracteres. Corresponde a qualquer um dos caracteres entre as chaves. [xyz] corresponde ao "y" de "play."
[^xyz]	Um conjunto de caracteres negativos. Corresponde a qualquer um dos caracteres que não estão entre as chaves. [^xyz]/ corresponde ao "v" de "vain".
[0-9]	Corresponde a um caractere de dígito.
[^0-9]	Corresponde a um caractere diferente de dígito.
[A-Za-z0-9_]	Corresponde a qualquer caractere de palavra, incluindo traço baixo.
[^A-Za-z0-9_]	Corresponde a qualquer caractere diferente de palavra.
/n/	Corresponde a n, em que n é um valor de fuga octal, hexadecimal ou decimal. Permite que códigos ASCII sejam embutidos em expressões regulares.

Espaços em branco em expressões regulares

Nas expressões regulares, os espaços em branco consistem de um ou mais brancos, que podem ser qualquer um dos seguintes caracteres:

Nome simbólico	UCS	Descrição
<tabulação>	<U0009>	CARACTERE DE TABULAÇÃO (HT)
<retorno de carro>	<U000D>	RETORNO DE CARRO (CR)
<nova linha>	<U000A>	ALIMENTAÇÃO DE LINHA (LF)
<tabulação vertical>	<U000B>	TABULAÇÃO DE LINHA (VT)
<alimentação de formulário>	<U000C>	ALIMENTAÇÃO DE FORMULÁRIO (FF)
<espaço>	<U0020>	ESPAÇO

Comandos de análise

A linguagem de análise do Assistente é orientada pela função. A maioria das funções de análise permitem que você manipule as variáveis do Assistente e o seu conteúdo. A linguagem de análise do Assistente suporta quatro tipos de variáveis:

- Inteiro (o nome da variável começa com i)
- Flutuante (o nome da variável começa com f)
- Strings com tamanho variável (o nome da variável começa com outra letra diferente de i ou f)
- Matrizes de variáveis (o nome da variável termina com [ ]). Os tipos de variáveis de matriz podem ser matrizes de inteiros, flutuantes ou strings

Essas variáveis são locais para cada porta do Assistente e não são compartilhadas globalmente por todas as portas do Assistente. Os comandos de análise permitem que você copie dados do buffer de recebimento em variáveis de string.

O buffer de recebimento contém os dados que foram recebidos da porta de comunicação, porta de soquete, arquivo ou processo do Assistente.

O tamanho dos bytes a serem copiados, assim como a posição para copiar os bytes, podem ser controlados utilizando um dos seguintes comandos de análise:

- SEARCH()
- SKIP()

- SKIPWORD()
- NEGSEARCH()
- RESET()
- COPY()

Os dados do buffer de recebimento podem ser anexados a uma variável de string com o comando APPEND(). A linguagem de análise do Assistente também permite que você copie ou anexe dados de variáveis de string em outras variáveis de string.

Tipos de dados simples

número

Os numerais só podem ser precedidos por um + ou - no caso dos comandos SKIP, SKIPWORD, e SET. Por exemplo:

```
0, 10, 2.5
```

ivar (variável de inteiro)

Variáveis de inteiro são números atribuídos de 32-bit. O nome da variável deve começar com um I ou i. Por exemplo:

```
i_count, I_severity, i, i[55], i[index]
```

A variável de inteiro, i[55], é o 55º. índice na matriz de inteiro, i[]. Além disso, o índice em uma matriz pode ser um inteiro variável.

fvar (variável flutuante)

Variáveis flutuantes são números de indicadores flutuantes de 32-bit. O nome da variável deve começar com um F ou f. Por exemplo:

```
f_rate, F_queue, f, f[1], f[index]
```

svar (variável de string)

As variáveis de string contém strings de tamanhos variados. Os nomes da variável de string não podem começar com um I, i, F ou f. Por exemplo:

```
resource, date, _message, string[1000], string[i_sev]
```

matriz (matriz de variável)

As matrizes de variável podem representar matrizes de variáveis dos tipos ivar, fvar e svar. Por exemplo:

```
i_bits[], F_values[], s_resources[]
```

As matrizes podem ser indexadas com um índice numérico, sem desperdício de espaço de memória. O acesso a ivar[1000] não significa que a memória está alocada para 1.000 variáveis de inteiro.

Uma variável de matriz indexada é tratada como qualquer outra variável (ivar, svar e fvar)

O exemplo a seguir seria uma sintaxe válida para o comando POPUP:

```
POPUP(xterm_display[4], data[i_count])
```

Dados entre aspas

Os dados entre aspas são explorados e analisados da seguinte forma:

- /=Caractere de exceção: incluir byte após o /, sem relação com nenhum significado especial; para usar um dos caracteres especiais na string, / deve ser colocado na frente do caractere. Por exemplo, corp/\router é usado para corp\router
- \xx x xx\=Hex data (pode ser um ou dois caracteres por byte): \0ad\, \0a0d\, \a d\,\0a 0d\, and \0a d\ todos significando alimentação de linha/retorno de carro

Todos os outros caracteres são especificados diretamente.

Tipos de dados agregados derivados

A tabela a seguir lista os tipos de dados agregados derivados:

Tipo	**Descrição**
todos	número, ivar, fvar, svar, aspas
valor numérico	número, ivar, fvar, ivar[index], fvar[index]
string	svar, svar[index], aspas
variável	ivar, fvar, svar, ivar[index], fvar[index], svar[index]
numvar	ivar, fvar, ivar[index], fvar[index]
matriz	ivar[], fvar[], svar[]
matriz numvar	ivar[], fvar[]
matriz de variável de string:	svar[]

Regras especiais para variáveis

A seguir, algumas regras especiais para variáveis.

- Os nomes de variáveis distinguem maiúsculas de minúsculas.
- Quando uma numvar é usada pela primeira vez, é definida para zero, exceto nos casos em que tem os seus valores definidos.
- Quando uma svar é usada pela primeira vez, é definida para nulo (""), exceto nos casos em que tem seus valores definidos.
- Uma matriz indexada é tratada como qualquer outra variável do seu tipo, ivar, fvar ou svar
- Para comentar um ou mais comandos de análise, ou para incluir comentários no texto de análise, coloque o comentário entre /* */

Por exemplo:

```
/* este é um comentário */
/* esses são comandos de análise comentados
COPY(s: "test")
DISPLAY()
*/
```

3 Comandos de Análise do Assistente

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

Este capítulo descreve os comandos de análise de assistente usados na criação do Coletor em ordem alfabética. Veja a seguir uma lista dos comandos de análise por função.

Função	Comando de análise
Interação de bancos de dados	DBCLOSE DBDELETE DBGETROW DBINSERT DBOPEN DBSELECT
Depuração	BREAKPOINT DISPLAY POPUP
Interação de arquivos	FILEA FILEL FILER FILEW

Operações lógicas	COMPARE
	ELSE
	ENDFOR
	ENDIF
	ENDWHILE
	FOR
	IF
	LOOKUP
	ENDWHILE

Interação de redes	SOCKETW
Notificação	ALERT CLEARTAGS CONSTANTTAGS EVENT INDICATOR PAUSE

Função	Comando de análise
Manipulação de dados iniciais	BITFIELD BYTEFIELD CONVERT CRC DECODE DECODEMIME ENCODE ENCODEMIME HEXTONUM NUMTOHEX SETBYTES STRIP STRIP-ASCII-RANGE
Manipulação de strings	APPEND COPY COPY-FROM-RX-BUFF-UNTIL-SEARCH COPY-FROM-RX-BUFF COPY-FROM-STRING-TO-STRING-UNTIL-SEARCH COPY-STRING-TO-STRING LENGTH LENGTH-OPTION2 NEGSEARCH PARSER_ATTACHVARIABLE PARSER_CREATEBASIC PARSER_NEXT PARSER_PARSESTRING PRINTF REGEXPREPLACE REGEXPSEARCH REGEXPSEARCH_EXPLICIT REGEXPSEARCH_STRING REPLACE SEARCH SKIP SKIPWORD STONUM TOKENIZE TOLOWER TOUPPER TOKENIZE TRANSLATE
Utilitário	DATE DATETIME PAUSE SHELL TBOSSETCOMMAND TBOSSETREQUEST TIME

Função	Comando de análise
Gestão de variáveis	CLEAR DELETE GETCONFIG GETENV INC RESET RXBUFF SET SETCONFIG
Exploração de vulnerabilidades	INFO_CLEARTAGS INFO_CLOSE INFO_CONSTANTTAGS INFO_CREATE INFO_DUMP INFO_PUSH INFO_SEND INFO_SETTAG

Utilizando matrizes e formatos de comandos

Os formatos de comandos de análise usam certos símbolos para transmitir significados específicos. Veja a seguir exemplos desses símbolos:

Exemplo de símbolo em uso	Significado do símbolo de exemplo
`[parâmetro]`	Colchetes indicam parâmetros opcionais.
`<parâmetro>`	Colchetes angulares indicam parâmetros obrigatórios fornecidos pelo usuário.
`a`	a deve ser literalmente digitado aqui
`a|b`	use exatamente a ou b, mas não ambos
`<item> ::= <definição>`	o item pode ser substituído pela definição

`<varList>`
onde:
`<varList> ::= var [, <varList>]`
	usado em definições recursivas para descrever uma lista de variáveis em que pelo menos uma variável é necessária

`...`	A repetição do(s) parâmetro(s) precedente(s) é permitida.
`/`	A barra é usada como um caractere de "escape" para permitir que sejam usados caracteres especiais, como a barra invertida (\).

Matrizes são aceitas em expressões, como:

Dado	As expressões a seguir são equivalentes:
`SET(i_var = 2)`	`i_arr[3]`

`SET(i_arr[3]=2`	`i_arr[i_var]`
	`i_arr[1+2]`
	`i_arr[1+1_var]`
	`i_arr[i_arr[3]]`

Comandos

ALERT

O comando ALERT encaminha mensagens de eventos para o Sentinel.

- O primeiro parâmetro necessário define o nome do recurso;
- O segundo parâmetro define o texto da mensagem de evento;
- O terceiro define a gravidade do evento;
- A data e o horário da mensagem de evento podem ser definidos como parâmetros opcionais;
  - O parâmetro de data pode ser usado sozinho;
  - Já o parâmetro de horário deve acompanhar o parâmetro de data.

Formato

```
ALERT(recurso, mensagem, iseverity)
```

ou

```
ALERT(recurso, mensagem, iseverity[, data[, hora]])
```

Você não pode usar o parâmetro de horário se não estiver acompanhado pelo parâmetro de data.

NOTA: Use o Comando STONUM para converter a gravidade iseverity de uma string em um número inteiro.

Tipos de dados

Argumento	Tipo	Descrição
resource	string (ENTRADA)	Recurso e, opcionalmente, sub-recurso para enviar um evento para (por exemplo: `xterm:tcp_retransmits`).
message	(ENTRADA)	Texto da mensagem de evento.
iseverity	valor numérico (ENTRADA)	Representação numérica da prioridade desta mensagem de evento (0 -5). 0 = Informativa 1 = Advertência 2 = Aviso 3 = Leve 4 = Média 5 = Crítica
date	(ENTRADA) [OPCIONAL]	Define a data da mensagem de evento no formato DD/MM/AAAA (por exemplo: "01/12/2002") (padrão = data atual).
time	(ENTRADA) [OPCIONAL]	Define o horário da mensagem de evento no formato HH:MM:SS (por exemplo: "15:14:34") (padrão = horário atual); deve ser usado com o parâmetro de data.

Por exemplo:

```
ALERT("xterm:tcp_retransmits", mesg_txt,ivar[3])
ALERT("router_subnet_15", msg_txt, "c")
ALERT(resource, "Servidor não responde", iseverity)
ALERT("Mux184:card1", "C1 não está funcionando bem.", 4)
ALERT("Firewall", "Conexão com Firewall perdida.", 5)
ALERT("CB5", "Canal Banco 5 em manutenção", "Manut")
ALERT(recurso, mensagem, isev, thedate, thetime)
ALERT("Switch3", oos_msg, 5, "07-30-1997", "07:03:23")
```

APPEND

O comando APPEND adiciona dados do buffer de recebimento, uma variável de string ou uma string entre aspas a uma variável de string. Os seguintes itens são aplicáveis:

- Todo parâmetro APPEND é opcional, exceto o parâmetro de destino;
- O destino dos dados (variável de string) pode ser especificado com os parâmetros APPEND;
- Uma diferença na origem pode ser especificada para controlar onde os dados são copiados dos dados de origem;
- O número de bytes a ser anexado à variável de destino pode ser especificado com o parâmetro de tamanho (ilen), senão o tamanho padrão será o tamanho dos dados de origem;
- Além da especificação de um parâmetro de tamanho numérico, uma string pode ser usada para definir o tamanho;
- Se uma string é usada como parâmetro de tamanho, o parâmetro de origem deve ser o buffer de recebimento ou um parâmetro svar;
- Usando uma string como parâmetro de tamanho, o Mecanismo de Coletor anexa bytes dos dados de origem (começando na diferença) à variável de destino até, mas sem incluir, o primeiro caractere da string (se foi localizada) (se a string não foi localizada, nenhum byte será anexado);
- Se a diferença ou os parâmetros de tamanho forem especificados fora da faixa da variável de origem, serão anexados quantos bytes forem possíveis, até o fim dos dados de origem;
- Se a diferença for superior ou igual ao tamanho dos dados de origem, nenhum byte será anexado à variável de destino (se não for especificada uma diferença, o padrão para ela será zero).

Formato

```
APPEND(<dest>: [origem] [, [pesquisa] [, [ilen] [,
   [ioffset] ]]])
APPEND(<dest>: [origem] [, [ilen] [, [ioffset] ]])
APPEND(<dest>: [ilen] [, [diferença]])
```

Tipo de dados

Argumento	Tipo	Descrição
dest	svar	Variável de string de dados à qual os bytes são

Argumento	Tipo	Descrição
	(SAÍDA)	anexados.
source	string (ENTRADA) [OPCIONAL] ou svar	String em que se localizam os bytes de origem que serão anexados à string de destino. (padrão = Buffer de Recebimento) Se o parâmetro de pesquisa for usado.
search	string (ENTRADA) [OPCIONAL]	String usada para especificar: cópia dos bytes a serem pesquisados na string de origem.
ilen	valor numérico (ENTRADA) [OPCIONAL]	Número de bytes a serem anexados da origem ao destino.
ioffset	valor numérico (ENTRADA) [OPCIONAL]	Diferença na origem na qual os dados devem começar a ser anexados.

Os exemplos a seguir anexam bytes do buffer de recebimento a um parâmetro svar de destino (dest). O indicador de buffer Rx é adicionado ao valor da diferença para especificar o primeiro indicador dos dados a serem anexados. O símbolo ^ mostra o indicador de buffer Rx.

```
APPEND(svar:ilen)
APPEND(svar:3)
APPEND(svar:,ioffset)
APPEND(origem:ilen,ioffset)
APPEND(svar: 10, 12)
```

O exemplo acima foi criado com as seguintes suposições.

```
rxbuff="buffer de recebimento"
   ^ (indicador de buffer Rx)
dest="String de destino"
source="String de origem"
ilen=3
ioffset=3
```

Digite o seguinte:

```
APPEND(dest:)
```

O resultado será:

```
dest = "Buffer de recebimento da string de destino"
```

Se você digitar:

```
APPEND(dest:ilen)
```

O resultado será:

```
dest = "Recebimento de string de destino"
```

Se você digitar:

```
APPEND(dest:,ioffset)
```

O resultado será:

```
dest = "Buffer de recebimento da string de destino"
```

Os exemplos a seguir anexam bytes do buffer de recebimento até, mas sem incluir, a string de pesquisa a um parâmetro svar de destino (dest). Se a string de pesquisa não for localizada no buffer de recebimento (após o indicador de buffer Rx + diferença), nenhum byte será anexado.

Digite o seguinte:

```
APPEND(dest:,"buffer")
```

O resultado será:

```
dest = "Recebimento de string de destino "
```

Digite o seguinte:

```
APPEND(dest:,"buffer", 9)
```

O resultado será:

```
dest = "String de destino"
```

Os exemplos a seguir anexam uma substring do buffer de recebimento à suposição:

```
Rx Buffer = "Alarme de Firewall leve A"
```

Digite o seguinte:

```
COPY(message:"Nome do recurso: ")
APPEND(mensagem:,6)
```

O resultado será:

```
message = "Nome do recurso: Alarme de Firewall A"
```

BITFIELD

O comando BITFIELD converte bytes em bits. Esse comando converte cada byte de uma string de tamanho arbitrário em 8 bits (0 ou 1) colocando-a em uma matriz inteira, matriz flutuante ou string.

AVISO: A saída é 8 vezes maior que a entrada, portanto o comando de análise bitfield pode ocupar muita memória se usado de forma inadequada. Um exemplo é o uso de strings de entrada com um número muito grande de bytes.

Formato

```
BITFIELD(s_bytes, dest_var)
```

Tipos de dados

Argumento	Tipo	Descrição
s_bytes	string (ENTRADA)	Qualquer número de bytes ASCII ou hexadecimais em uma string.
dest_var	matriz numvar (SAÍDA)	Matriz inteira (definida como 0 ou 1). O número de bits é igual ao número de bytes em s_bytes vezes 8. Para cada conjunto de 8 bits, os bits são posicionados do Bit Mais Importante (MSB) para o Bit Menos Importante (LSB). Por exemplo: idest_var[0] = MSB do byte 1 idest_var[1] = Próximo MSB do byte 1 idest_var[2] = Próximo MSB do byte 1 idest_var[3] = Próximo MSB do byte 1 idest_var[4] = Próximo MSB do byte 1 idest_var[5] = Próximo MSB do byte 1 idest_var[6] = Próximo MSB do byte 1 idest_var[7] = LSB do byte 1 idest_var[8] = MSB do byte 2 idest_var[9] = Próximo MSB do byte 2 ... idest_var[n * 8 - 1] = LSB do byte n String contendo um múltiplo de 8 bytes, em que cada byte representa um bit Nos bytes de entrada. Os bytes desta string serão sempre definidos como um ASCII 0 ou 1.
	Ou svar (SAÍDA)	Para cada 8 bits consecutivos representados em cada string, o ASCII (0s e 1s) será posicionado de MSB para LSB. Por exemplo: Se s_bytes = "\5AFE\" Então dest_var= "0101101011111110"

NOTA: O segundo parâmetro do bitfield (`dest_var`) deve ser uma string (por exemplo, `ivar[]` ou `fvar[]`).

Por exemplo:

```
BITFIELD("\00\", f_bit_array[])
BITFIELD(s_bytes, i_bit_array[])
BITFIELD(s_byte, string_out)
```

```
BITFIELD("Isso funcionará", i_bit_array[])
BITFIELD("\563F\", string_out)
```

No exemplo a seguir, o sbyte da string é definido como um byte hexadecimal e enviado ao comando BITFIELD duas vezes (uma para uma matriz inteira e outra para uma string).

```
COPY(sbyte:"\AE\")
BITFIELD(sbyte, ibits[])
BITFIELD(sbyte, sbits)
```

Conteúdo das variáveis de saída atuais

```
ibits[0] = 1
ibits[1] = 0
ibits[2] = 1
ibits[3] = 0
ibits[4] = 1
ibits[5] = 1
ibits[6] = 1
ibits[7] = 0
sbits = "10101110"
```

BREAKPOINT

O comando BREAKPOINT interrompe a execução de um script de análise. Quando o depurador do script do Assistente está sendo executado, o comando breakpoint pára a intervenção do usuário pendente do analisador. Por exemplo, no painel Depurador do Assistente, selecione o botão OK ou Etapa para retomar o processo de depuração.

Formato

```
BREAKPOINT()
```

BYTEFIELD

O comando BYTEFIELD adota uma representação de byte(s) de bits (0 ou 1) e coloca os bytes em uma variável de string.

A entrada pode ser uma:

- string
- matriz inteira;
- matriz flutuante.

A saída é sempre uma variável de string.

Formato

AVISO: Se o primeiro parâmetro for uma matriz inteira ou flutuante, não use valores maiores que 100 para i_num_bytes, pois a matriz será inicializada para esse mesmo número de entradas (isso pode ocupar muita memória com valores altos de i_num_bytes).

```
BYTEFIELD(source_var, s_bytes[, i_num_bytes])
```

NOTA: O primeiro parâmetro do BYTEFIELD (`source_var`) deve ser `svar`, `ivar[]` ou `fvar[]`.

Tipos de dados

Argumento	Tipo	Descrição
source_var	matriz numvar (ENTRADA)	Matriz inteira (definida como 0 ou 1). O número de bits é igual ao número de bytes em s_bytes vezes 8. Para cada conjunto de 8 bits, os bits são posicionados do Bit Mais Importante (MSB) para o Bit Menos Importante (LSB) (veja exemplos na tabela a seguir).
	svar (ENTRADA)	String que contém um múltiplo de 8 bytes, em que cada byte representa um bit nos bytes de entrada. Os bytes dessa string devem ser sempre definidos como um ASCII 0 ou 1. Para cada 8 bits consecutivos representados em cada string, o ASCII (0s e 1s) deve ser posicionado do MSB para o LSB. Por exemplo: Se source_var = "0101101011111110" e i_num_bytes = 2, Então s_bytes = "\5AFE\"
s_bytes	string (SAÍDA)	Qualquer número de bytes de dados hexadecimais ou ASCII em uma string.
i_num_bytes	valor numérico (ENTRADA) [OPCIONAL]	Número de bytes a ser colocado em _bytes. Como é opcional, o padrão será 1, a menos que seja usado quando a entrada for do tipo STRING. Se a entrada for do tipo STRING, o padrão será o tamanho da string dividido por 8.

Veja exemplos específicos de source_var:

```
ISOURCE_VAR[0] = MSB do byte 1
ISOURCE_VAR[1] = Próximo MSB do byte 1
ISOURCE_VAR[2] = Próximo MSB do byte 1
ISOURCE_VAR[3] = Próximo MSB do byte 1
ISOURCE_VAR[4] = Próximo MSB do byte 1
ISOURCE_VAR[5] = Próximo MSB do byte 1
```

```
ISOURCE_VAR[6] = Próximo MSB do byte 1
ISOURCE_VAR[7] = LSB do byte 1
ISOURCE_VAR[8] = MSB do byte 2
ISOURCE_VAR[9] = Próximo MSB do byte 2
...
ISOURCE_VAR[n * 8 - 1] = LSB do byte n
```

Veja alguns exemplos do comando BYTEFIELD:

```
BYTEFIELD(i_bit_array[], s_bytes)
BYTEFIELD(string_bits_in, s_bytes)
BYTEFIELD(f_bit_array[], string_bytes, 2)
BYTEFIELD(i_bit_array[], string_bytes, i_num_bytes)
```

No exemplo a seguir, a string, o sbyte e a matriz inteira ivar são definidos como a representação de bit de um byte hexadecimal e enviados ao comando BYTEFIELD duas vezes (uma para uma matriz de número inteiro e outra para uma entrada de string).

```
SET(ivar[0] = 0)
SET(ivar[1] = 0)
SET(ivar[2] = 0)
SET(ivar[3] = 0)
SET(ivar[4] = 1)
SET(ivar[5] = 1)
SET(ivar[6] = 1)
SET(ivar[7] = 1)
COPY(sbits:"11110000")
BYTEFIELD(ivar[], sbyte1)
BYTEFIELD(sbits, sbyte2, 1)
```

Conteúdo das variáveis de saída atuais:

```
sbyte1 = "\0F\"
sbyte2 = "\F0\"
```

CLEAR

O comando CLEAR trunca variáveis de string para zero byte ou define variáveis inteira e flutuante como zero. É possível especificar até 100 variáveis em um comando CLEAR.

Formato

```
CLEAR(<varlist>)
```

Onde:

```
varlist ::= var [, <varlist>]
Var ::= variável a limpar (fvar, ivar ou svar)
```

Número máximo de variáveis: 100

Tipos de dados

Argumento	Tipo	Descrição
var1	variável (ENTRADA/ SAÍDA)	Variável a limpar (fvar, ivar ou svar).
var2	variável (ENTRADA/ SAÍDA) [OPCIONAL]	Variável a limpar (fvar, ivar ou svar).
var3	variável (ENTRADA/ SAÍDA) [OPCIONAL]	Variável a limpar (fvar, ivar ou svar).
...	variável (ENTRADA/ SAÍDA) [OPCIONAL]	Outras variáveis a limpar (fvar, ivar ou svar).

Por exemplo:

```
CLEAR(var1)
CLEAR(var1,var2)
CLEAR(var1,var2,var3)
CLEAR(svar[45])
CLEAR(imatrix[5][5])
CLEAR(ivar, fvar, i_len, data_string[i_var])
CLEAR(temp)
CLEAR(sdata[index_x][index_y])
CLEAR(f_bits[3], i_var_array[2])
CLEAR(i_counter, temp)
```

Nos exemplos a seguir, são atribuídos valores para variáveis de string, que são usadas em uma mensagem de evento e cujos valores são limpos.

```
COPY(res_var: "Firewall")
COPY(msg_var: "Alarme de Firewall leve 116")
ALERT(res_var, msg_var, 4)
CLEAR(res_var, msg_var)
RESULTADO:
res_var = ""
msg_var = ""
```

CLEARTAGS

O comando CLEARTAGS faz uma limpeza em todas as variáveis reservadas de evento e de data/horário não protegidas pelo comando CONSTANTTAGS.

Esse comando deve ser chamado no estado de inicialização (estado 4 no modelo padrão do Sentinel) do Coletor para que qualquer entrada seja analisada nas variáveis reservadas.

O comando CLEARTAGS opera nas variáveis reservadas de evento e nas variáveis reservadas de data/horário. Ele não adota nenhum parâmetro. As variáveis de string são definidas como string vazia ""; por exemplo:

```
s_EVT e s_Sec.
```

A variável inteira i_Severity é definida como zero.

Formato

```
CLEARTAGS ()
```

Por exemplo:

```
SET(i_Severity = 3)
COPY(s_BM:"Mensagem base")
COPY(s_Example:"Teste")
CLEARTAGS()
```

O resultado será:

```
i_Severity = 0
s_BM = ""
s_Example = "Teste"
```

NOTA: s_Example não é uma variável reservada de evento ou de data/horário, portanto não foi limpa.

COMMENT

Esse comando inclui um argumento opcional, que é uma string. Método para digitar comentários no arquivo de gabarito do Coletor. Permite digitar comentários pelo Editor Visual sem entrar no editor de texto.

Formato

```
/*[string]*/
```

Por exemplo:

```
/* INFORMAÇÕES DO COLETOR
; -------------------------------------------------
Collector_Name:              Gabarito padrão
Collector_Description:       Gabarito no qual novos
   Coletores Assistentes são baseados
Collector_Manufacturer:      N/A
Collector_Product/Version:   N/A
Collector_Version:           versão 4.1
Collector_Date:              Agosto de 2003
; -------------------------------------------------*/
```

COMPARE

O comando COMPARE examina dois argumentos e define uma variável de acordo com o resultado. O resultado da comparação entre uma string ou um valor numérico de tipo pode ser armazenado em uma variável. Se for do tipo ivar, fvar ou string, a variável conterá o valor -1, 0 ou 1.

- -1 é usado se arg1 é menor que arg2;
- 0 é usado se arg1 é igual a arg2;
- 1 é usado se arg1 é maior que arg2.

Formato

```
COMPARE(arg1, arg2, dest)
```

Tipos de dados

Argumento	Tipo	Descrição
arg1	todos (ENTRADA)	Comparar dados 1. Devem ser uma string ou um valor numérico.
arg2	todos (ENTRADA)	Compare os dados 2. Devem ser do mesmo tipo que Comparar dados 1.
dest	variável (SAÍDA)	Variável em que os resultados da comparação serão incluídos: svar = "-1", "0" ou "1" ivar = -1, 0 ou 1 fvar = -1.0, 0.0 ou 1.0

NOTA: Os tipos arg1 e arg2 devem ser ambos uma string ou valor numérico.

Por exemplo:

```
COMPARE(i_counter, 0, temp)
COMPARE(sdata, "ALM", i_sdata_cmp_val)
COMPARE(i_counter, i_counter2, temp)
COMPARE(i_counter, i_counter2, i_result[i_counter])
```

No exemplo a seguir, o texto é comparado ao conteúdo de uma variável de string e o resultado da comparação é armazenado em uma variável inteira. Um evento será gerado se o texto não for igual ao valor da variável de string.

```
COMPARE(s_data_var, "ALARME", i_compare_var)
IF(i_compare_var = 0)
ALERT(res_var, "ALARME médio", 5)
ENDIF()
```

NOTA: Os comandos IF( ),ELSE( ) e ENDIF( ) executam a mesma função que o comando COMPARE, exceto a comparação de números negativos.

CONSTANTTAGS

O comando CONSTANTTAGS adota um número variável de parâmetros de nomes de variáveis reservadas (evento e data/horário). Declarando uma variável reservada como constante, ele a protege de ser limpa por uma chamada do comando CLEARTAGS.

Um exemplo de variável semelhante é s_PN, que leva o nome do produto que está sendo processado pelo Coletor. A variável s_PN deve ser declarada uma constante e definida uma vez no estado de configuração do Coletor.

Esse comando deve ser chamado no estado de configuração do Coletor (estado 1 no modelo padrão 4.1) para que variáveis reservadas não sejam alteradas à medida que o Coletor processa os eventos.

O comando CONSTANTTAGS opera nas variáveis reservadas de evento e nas variáveis reservadas de data/horário.

Formato

```
CONSTANTTAGS (<reserved_variable> [, ...])
```

Tipos de dados

Argumento	Tipo	Descrição
reserved_variable		Lista de variáveis reservadas que serão definidas como constantes e não serão limpas pelo comando CLEARTAGS.

Por exemplo:

```
COPY(s_PN:"PN")
COPY(s_ST:"ST")
COPY(s_BM:"BM")
CONSTANTTAGS(s_PN,s_ST)
CLEARTAGS()
```

O resultado será:

```
s_PN = "PN"
s_ST = "ST"
s_BM = ""
```

Das três variáveis reservadas de evento, s_BM não foi protegida no comando CLEARTAGS pelo comando CONSTANTTAGS, por isso foi limpa.

CONVERT

O comando CONVERT transforma uma string de entrada de tipo binário, octal, decimal, hexadecimal ou inicial em uma variável de string de saída de tipo binário, octal, decimal, hexadecimal ou inicial.

Formato

```
CONVERT(string_in, type_in, svar_out, type_out)
```

Tipos de dados

Argumento	Tipo	Descrição
string_in	String (ENTRADA)	String de entrada a ser convertida.
type_in	Lista de escolhas String Variável de string (ENTRADA)	Tipo da string de entrada (string_in): Binário = "B" ou "b" Octal = "O" ou "o" Decimal = "D" ou "d" Hexadecimal = "H" ou "h" Inicial = "R" ou "r"
svar_out	svar (SAÍDA)	Variável de string que contém os dados da string convertida.
type_out	Lista de escolhas String Variável de string (ENTRADA)	Tipo no qual converter os dados (a string convertida será colocada em svar_out): Binário = "B" ou "b" Octal = "O" ou "o" Decimal = "D" ou "d" Hexadecimal = "H" ou "h" Inicial = "R" ou "r"

Por exemplo:

```
CONVERT("10101010", "b", shex, "h")
CONVERT(sdata, "B", sraw, "r")
CONVERT("2356", "d", soctal, "o")
CONVERT("\3A\", "r", sbinary, "b")
CONVERT("2A3E", "h", sraw, "r")
CONVERT(dados, "r", sdecimal, "d")
CONVERT(dados, "o", shex, "H")
```

No exemplo a seguir, o comando CONVERT é chamado para executar várias conversões.

```
CONVERT("\0afe\", "R", sdecimal, "D")
CONVERT("63", "d", sbinary, "b")
CONVERT("63", "d", shex, "h")
CONVERT("63", "d", soctal, "o")
CONVERT("1101010111110101", "b", sraw, "r")
```

Conteúdo das variáveis de saída atuais:

```
sdecimal = "2814"
sbinary = "00111111"
shex = "3F"
soctal = "077"
sraw = "\d5 f5\"
```

COPY

O comando COPY duplica dados do buffer de recebimento ou da string de origem, colocando-os em uma variável de string ou em uma string entre aspas de uma variável de string. O indicador de buffer Rx não é alterado quando esse comando é usado.

O destino dos dados (svar) deve ser especificado com os parâmetros de cópia.

NOTA: No Editor Visual do Construtor de Coletores, os comandos COPY, COPY-FROM-RX-BUFF-UNTIL-SEARCH, COPY-FROM-RX-BUFF, COPY-FROM-STRING-TO-STRING-UNTIL-SEARCH e COPY-STRING-TO-STRING são listados como comandos separados. Eles são o mesmo comando. São fornecidos como descrições de variações do mesmo comando. Para usar qualquer variação do comando COPY no editor de texto, digite COPY.

Quando esse comando é usado:

- Especifique uma diferença na origem para controlar onde os dados são copiados dos dados de origem;
- O número de bytes a ser copiado à variável de destino pode ser especificado com o parâmetro de tamanho (ilen), senão o tamanho padrão poderá ser o tamanho dos dados de origem;
- Além da especificação de um parâmetro de tamanho numérico, uma string pode ser usada; Usando uma string, o Mecanismo de Coletor copia bytes dos dados de origem (começando na diferença) para a variável de destino até, mas sem incluir, o primeiro caractere da string (se tiver sido localizada); Se a string não é localizada, nenhum byte é copiado;

- Se os parâmetros de diferença (ioffset) ou de tamanho (ilen) forem especificados fora da faixa da variável de origem, serão copiados quantos bytes forem possíveis, até o fim dos dados de origem;

  Se a diferença for superior ou igual ao tamanho dos dados de origem, nenhum byte será copiado para a variável de destino;

  Se não for especificada uma diferença, o padrão para ela será zero.

Formato

```
COPY(<DEST>: [ORIGEM] [, [PESQUISA] [, [ILEN] [,
   [IOFFSET] ]]])
COPY(<DEST>: [ORIGEM] [, [ILEN] [, [IOFFSET] ]])
COPY(<DEST>: [ILEN] [, [DIFERENÇA]])
```

Tipos de dados

Argumento	Tipo	Descrição
dest	svar (SAÍDA)	Variável de string de dados à qual os bytes são copiados.
string source	(ENTRADA) [OPCIONAL] Ou svar	String em que são copiados bytes do (padrão = Buffer de Recebimento). Se o parâmetro de pesquisa for usado.
search	string (ENTRADA) [OPCIONAL]	String usada para especificar: cópia dos bytes a serem pesquisados na string de origem.
ilen	valor numérico (ENTRADA) [OPCIONAL]	Número de bytes a serem copiados da origem ao destino.
ioffset	valor numérico (ENTRADA) [OPCIONAL]	Diferença na origem em que a cópia de dados é iniciada; copia todos os caracteres do buffer de recebimento para o buffer de transmissão.

Os exemplos a seguir copiam bytes do buffer de recebimento para um parâmetro svar de destino (dest). O indicador de buffer Rx é adicionado ao valor da diferença para especificar o primeiro indicador dos dados a serem copiados. O símbolo ^ identifica o indicador de buffer Rx.

As seguintes suposições são feitas:

```
rxbuff="buffer de recebimento"
^ (indicador de buffer Rx)
dest=""
source="String de origem"
ilen=3
ioffset=3
```

Comando	Resultado
`COPY(dest:)`	`dest = "buffer de recebimento"`
`COPY(dest:5)`	`dest = "receb"`
`COPY(dest:,5)`	`dest = "buffer ve"`

Os exemplos a seguir copiam bytes de uma string de origem para um parâmetro svar de destino (dest).

Comando	Resultado
`COPY(dest:origem)`	`dest = "String de origem"`
`COPY(dest:origem,5)`	`dest = "Orig A"`
`COPY(dest:origem,5,6)`	`dest = "ce st"`

Os exemplos a seguir copiam bytes do buffer de recebimento até, mas sem incluir, a string de pesquisa para uma variável de string. Se a string de pesquisa não for localizada no buffer de recebimento (após o indicador de buffer Rx + diferença), nenhum byte será copiado.

NOTA: Na substituição hexadecimal, \0000\ encerra uma string. Portanto, "xxxx\0000\yyyy" se torna "xxxx".

Os exemplos a seguir copiam bytes do buffer de recebimento até, mas sem incluir, a string de pesquisa para um parâmetro svar de destino (dest). Se a string de pesquisa não for localizada no buffer de recebimento (após o indicador de buffer Rx + diferença), nenhum byte será copiado.

Comando	Resultado
`COPY(dest:,"buffer")`	`dest = "receber"`
`COPY(dest:,"receber")`	`dest = ""`

Os exemplos a seguir copiam bytes de uma string de origem (deve ser uma variável de string) até, mas sem incluir, a string de pesquisa para uma variável de string de destino (dest). Se a string de pesquisa não for localizada no buffer de recebimento (após o indicador de buffer Rx + diferença), nenhum byte será copiado.

Comando	Resultado
`COPY(dest:origem," string")`	`dest = "origem"`
`COPY(dest:origem," .string")`	`dest = ""`

CRC

O comando CRC calcula uma verificação de redundância cíclica em uma string de bytes (hexadecimais ou ASCII).

Formato

```
CRC(source_data, dest_crc)
```

Tipo de dados

Argumento	Tipo	Descrição
source_data	string (ENTRADA)	Dados da string para executar o comando CRC.
dest_crc	svar (SAÍDA)	Variável de string em que os resultados do comando CRC de 2 bytes são armazenados.

Por exemplo:

No exemplo a seguir, o valor de CRC calculado é comparado com um valor salvo. Se os dois valores de CRC forem iguais, uma mensagem de evento será gerada.

```
CRC(svar, s_crc_var)
IF(s_crc_var = "\0A5F\")
EVENT(res, "CRC correto gerado", 0)
ENDIF()
```

NOTA: Na substituição hexadecimal, \0000\ encerra uma string, portanto "xxxx\0000\yyyy" se torna "xxxx".

DATE

O comando DATE copia a data atual (no formato DD/MM/AAAA) em uma variável de string. Você também pode copiar o dia da semana atual em uma variável de string, inteira ou flutuante.

Formato

```
DATE(date_string [, day_of_week] [, i_day_of_week]
   [, f_day_of_week])
```

Tipo de dados

Argumento	Tipo	Descrição
date_string	svar (SAÍDA)	Variável de string em que a data será armazenada (por exemplo: svar = "11-18-2002").
day_of_week	svar (SAÍDA) [OPCIONAL] ivar (SAÍDA) [OPCIONAL] Ou fvar (SAÍDA) [OPCIONAL]	(Opcional) Variável de string em que o dia da semana será armazenado; gravado com o nome completo do dia (por exemplo: svar = sábado) (Opcional) Variável inteira ou flutuante em que o dia da semana será armazenado; gravado com o nome completo do dia = número: Segunda-feira = 1 Terça-feira = 2 Quarta-feira = 3 Quinta-feira = 4 Sexta-feira = 5 Sábado = 6 Domingo = 7 (Por exemplo: segunda-feira é ivar = 1)

Por exemplo:

No exemplo a seguir, a data do sistema é comparada com uma string de data. Se as duas datas forem iguais, uma mensagem de evento será gerada.

```
DATE(date_var, day_of_week)
IF(date_var = "11-18-2002")
ALERT(res, "Feliz 23º aniversário!", 0)
ENDIF()
IF(day_of_week = "Sábado")
ALERT(res, "Dia de ir à praia," 0)
ENDIF()
```

DATETIME

O comando DATETIME converte uma representação, em números inteiros, do número de segundos desde o dia 1º de janeiro de 1970 em variáveis de string de data e horário. Você também pode copiar o dia da semana atual em uma variável de string, inteira ou flutuante.

Formato

```
DATETIME(itime_secs, svar_date, svar_time [, day_of_week]
   [, i_day_of_week] [, f_day_of_week])
```

Tipos de dados

Argumento	Tipo	Descrição
itime_secs	valor numérico (ENTRADA)	Número inteiro que contém o número de segundos desde 1970.
svar_date	svar (SAÍDA)	Variável de string em que a data será armazenada (por exemplo: 02-19-96).
svar_time	svar (SAÍDA)	Variável de string em que o horário será armazenado (por exemplo: 15:14:33).
day_of_week	svar (SAÍDA) [OPCIONAL] ivar (SAÍDA) [OPCIONAL] Ou fvar (SAÍDA) [OPCIONAL]	(Opcional) Variável de string em que o dia da semana será armazenado; gravado com o nome completo do dia (por exemplo: svar = sábado) (Opcional) Variável inteira ou flutuante em que o dia da semana será armazenado; gravado com o nome completo do dia = número: Segunda-feira = 1 Terça-feira = 2 Quarta-feira = 3 Quinta-feira = 4 Sexta-feira = 5 Sábado = 6 Domingo = 7 (Por exemplo: segunda-feira é ivar = 1)

Por exemplo:

No exemplo a seguir, o comando DATETIME converte o número de segundos desde 1970 em strings de data e horário:

```
DATETIME(0, sdatevar, stimevar)
```

No exemplo a seguir, o comando DATETIME fornece a você o dia da semana, assim como a data e o horário:

```
DATETIME(946728000, sdate, stime, sday)
```

Conteúdo das variáveis de saída atuais:

```
sdatevar = "01-01-70"
stimevar = "00:00:00"
sdate = "01-01-2000"
stime = "12:00:00"
sday = "Sábado"
```

DBCLOSE

O comando DBCLOSE fecha a conexão com o banco de dados. Existem dois parâmetros necessários.

- O primeiro é o handle de banco de dados, retornado pelo comando DBOPEN. Ele pode ser um inteiro ou uma variável inteira;
- O segundo parâmetro necessário é o status do comando close. Ele pode ser uma variável inteira ou flutuante. Um número "1" será retornado quando bem-sucedido;

Formato

```
DBCLOSE(i_dbhandle, i_closestatus)
```

DBDELETE

O comando DBDELETE exclui linhas da tabela selecionada com base nos critérios de seleção. Existem quatro parâmetros necessários.

- O primeiro é o handle de banco de dados, retornado pelo comando DBOPEN. Ele pode ser um inteiro ou uma variável inteira;
- O segundo parâmetro necessário é o status do comando delete. Ele pode ser uma variável inteira ou flutuante. O número de linhas apagadas será retornado quando bem-sucedido, inclusive 0;
- O terceiro é o nome da tabela da qual serão excluídas linhas. Ele pode ser uma string ou uma variável de string;
- O quarto parâmetro opcional é a cláusula where, que permite ao usuário filtrar dados indesejados por meio de um critério de seleção. Se esse parâmetro for deixado em branco, o comando delete apagará todas as linhas da tabela.

Os códigos de erro do comando DBDELETE são os seguintes:

```
>0Nenhum erro
0Nenhuma linha excluída
-1Handle BD inválido
```

Formato

```
DBDELETE(i_dbhandle, i_deletestatus, "tablename",
   "cláusula where")
```

Por exemplo:

```
DBDELETE(i_dbhandle, i_deletestatus, "nome de tabela")
DBDELETE(i_dbhandle, i_deletestatus, s_tablename,
   "cláusula where")
```

DBGETROW

O comando DBGETROW funciona em conjunto com o comando DBSELECT. O usuário deve obter uma seleção primeiro, usando o comando DBSELECT, antes de recuperar linhas com o comando DBGETROW. Esse comando recuperará a próxima linha disponível de uma seleção, mantendo um cursor aberto para que esse comando possa ser chamado em um loop, recuperando a próxima linha após cada chamada. Existem quatro parâmetros necessários.

- O primeiro é o handle de banco de dados, retornado pelo comando DBOPEN. Ele tanto pode ser um inteiro como uma variável inteira;
- O segundo parâmetro necessário é o handle para a seleção. Ele pode ser uma string ou uma variável de string. Esse é o mesmo handle que foi atribuído durante o comando DBSELECT;
- O terceiro é o status do comando get. Ele pode ser uma variável inteira ou flutuante. Um número "1" será retornado quando bem-sucedido;
- O quarto parâmetro necessário e os parâmetros opcionais subseqüentes são os dados da coluna retornados pelo comando. Essas colunas podem ser variáveis de string, flutuante ou inteiras. Dados da coluna de um tipo diferente do tipo de parâmetro são convertidos no tipo de parâmetro apropriado, se possível. Portanto, se a tabela contiver uma coluna flutuante, mas o parâmetro for uma string, os dados serão convertidos de uma coluna flutuante em uma string. O usuário pode incluir até 48 desses parâmetros.

NOTA: O comando preencherá o menor número de parâmetros definido e o número de colunas reais no banco de dados. Se o banco de dados tiver 4 colunas, mas você fornecer 7 desses parâmetros, apenas os 4 primeiros serão preenchidos.

Os códigos de erro do comando DBGETROW são os seguintes:

```
1Nenhum erro
-1Erro ao recuperar linha
```

Formato

```
DBGETROW(i_dbhandle, "select1", i_selectstatus, s_col1,
   s_col2, s_col3, ..., s_col48)
```

Por exemplo:

```
DBGETROW(i_dbhandle, s_selecthandle, i_selectstatus,
   s_col1, s_col2)
```

DBINSERT

O comando DBINSERT insere uma linha de dados no banco de dados em uma tabela selecionada. Existem quatro parâmetros necessários.

- O primeiro é o handle de banco de dados, retornado pelo comando DBOPEN. Ele pode ser um inteiro ou uma variável inteira;
- O segundo parâmetro necessário é o status do comando insert. Ele pode ser uma variável inteira ou flutuante. Um número "1" será retornado quando bem-sucedido;
- O terceiro é o nome da tabela na qual os dados são inseridos;
- O quarto parâmetro necessário e os parâmetros opcionais subseqüentes são os dados da coluna a serem inseridos. Essas colunas podem ser de qualquer tipo. O usuário pode incluir até 48 desses parâmetros.

O comando deve incluir o número exato de parâmetros necessários para inserir uma linha de dados. O DBINSERT não adicionará um novo registro se uma restrição exclusiva for violada.

Os códigos de erro do comando DBINSERT são os seguintes:

```
1 Nenhum erro
-1 Handle BD inválido / nenhuma linha inserida
-2 Não é possível criar solicitação de dados
-7 Erro de execução de SQL
-16 Erro de sintaxe SQL
```

Formato

```
DBINSERT(i_dbhandle, i_insertstatus, "theTableName",
   "data1", "data2", ..., "data48")
```

Por exemplo:

```
DBINSERT(i_dbhandle, i_insertstatus, s_theTableName,
   "data1", I_data2, f_data3)
DBINSERT(i_dbhandle, i_insertstatus, "theTableName",
   s_data1, "data2")
```

DBOPEN

O comando DBOPEN abre uma conexão com um banco de dados suportado.

Apenas no Coletor do Microsoft Windows NT, o DBOPEN não funcionará quando o nome do banco de dados for configurado para indicar uma "unidade mapeada". Como o Coletor é executado como um serviço, ele (geralmente) é executado na conta do "sistema". Essa conta não tem permissões de acesso a compartilhamentos remotos, incluindo unidades mapeadas.

Isso significa que qualquer conexão com bancos de dados (nem mesmo pelo OBDC) no Coletor do Windows deve ser feita com um banco de dados totalmente local.

Existem cinco parâmetros necessários.

- O primeiro é o tipo de banco de dados. Ele pode ser selecionado em uma lista de escolhas ou usando uma string ou uma variável de string. O valor aceitável para esse parâmetro é Oracle9i;
- O segundo parâmetro necessário é o nome do banco de dados com o qual será estabelecida a conexão. Ele pode ser uma string ou uma variável de string;
- O terceiro é o nome de usuário no banco de dados. Ele pode ser uma string ou uma variável de string. Esse campo poderá conter qualquer texto se os usuários não tiverem sido especificamente configurados para acessar o banco de dados;
- O quarto parâmetro é a senha do usuário. Ele pode ser uma string ou uma variável de string; Esse campo poderá conter qualquer texto se os usuários não tiverem sido especificamente configurados para acessar o banco de dados;
- O quinto parâmetro necessário é o handle de banco de dados, retornado por esse comando na variável inteira ou flutuante. O handle de banco de dados será maior que 0 se bem-sucedido.

Formato

```
DBOPEN("oracle9i", "Nome do banco de dados", "nome de
   usuário", "senha", i_dbhandle)
```

Por exemplo:

```
DBOPEN(s_dbtype, s_dbname, s_username, s_password,
   i_dbhandle)
DBOPEN(s_dbtype, "nomebd", s_username, "senha",
   i_dbhandle)
```

DBSELECT

O comando DBSELECT funciona em conjunto com o comando DBGETROW. Ele abre um cursor de seleção no banco de dados, que capta um instantâneo dos registros atuais do banco de dados correspondentes aos critérios de seleção. Os registros digitados após o comando DBSELECT não aparecerão na recuperação dos registros enquanto não for emitido outro comando DBSELECT para atualizar a seleção.

Existem sete parâmetros necessários.

- O primeiro é o handle de banco de dados, retornado pelo comando DBOPEN. Ele pode ser um inteiro ou uma variável inteira;
- O segundo parâmetro necessário é o status do comando select. Ele pode ser uma variável inteira ou flutuante. Um número "1" será retornado quando bem-sucedido;
- O terceiro parâmetro necessário é o identificador do comando select. Ele pode ser uma string ou uma variável de string. Ele deve ser exclusivo, caso você tenha mais de um comando DBSELECT;

- O quarto parâmetro é o número de linhas a ignorar após ocorrer a seleção. Isso permite ao usuário posicionar o indicador no comando DBGETROW em novos dados, ao mesmo tempo que dados antigos são ignorados. Ele tanto pode ser um inteiro como uma variável inteira;
- O quinto parâmetro necessário é a tabela da qual os dados são obtidos. Ele pode ser uma string ou uma variável de string;
- O sexto parâmetro opcional é a cláusula where, que permite ao usuário filtrar dados indesejados por meio de um critério de seleção. Se esse parâmetro for deixado em branco, a seleção conterá todas as linhas da tabela. O formato da cláusula where é: where nome-coluna='dados';
- O sétimo parâmetro opcional consiste nas colunas retornadas pelo comando DBSELECT. Se for deixado em branco, a seleção conterá todas as colunas da tabela.

Os códigos de erro do comando DBSELECT são os seguintes:

```
1 Nenhum erro
-1 DB_Handle inválido
-2 Não é possível criar solicitação de dados
-3 Falha ao configurar autocommit
-4 Erro de alocação de memória
-5 Erro de sintaxe SQL
-6 Erro de execução de SQL
```

Formato

```
DBSELECT( i_dbhandle, i_selectstatus, "select1",
   i_rows_to_skip, "f_atom"<, "cláusula where"><,
   "col1<col2><...>">)
```

Por exemplo:

```
DBSELECT(i_dbhandle, i_selectstatus, "select1",
   i_rows_to_skip, "f_atom")
DBSELECT(i_dbhandle, i_selectstatus, s_select1, 23,
   S_TABLENAME, s_whereclause)
DBSELECT(i_dbhandle, i_selectstatus, s_select1, 23,
   S_TABLENAME, "where fname='BOB'")
DBSELECT(i_dbhandle, i_selectstatus, s_select1, 23,
   S_TABLENAME, "where fname='BOB'", "NOME, SOBRENOME,
   ENDEREÇO")
```

DEC

O comando DEC diminui uma variável numérica em 1. Ao usar o comando DEC, você deve especificar um parâmetro ivar ou fvar.

Formato

```
DEC(i_numvar)
```

Tipos de dados

Argumento	Tipo	Descrição
i_numvar	numvar (ENTRADA/ SAÍDA)	Variável a ser reduzida (ivar ou fvar).

Por exemplo:

```
SET(icounter = 2)
DEC(icounter)
DEC(icounter)
```

O resultado será:

```
icounter = 0
```

DECODE

O comando DECODE reverte uma string que foi codificada para preservar a identificação de pacote. Ele identifica os bytes (ou caracteres) correspondentes e os byte(s) (ou caracteres) de escape para remover o caractere de escape. O comando remove cada ocorrência da string de escape anterior aos bytes correspondentes sempre que ela é encontrada nos dados.

Formato

```
DECODE(data_decode, correspondência, escape)
```

Tipos de dados

Argumento	Tipo	Descrição
data_decode	svar (ENTRADA/ SAÍDA)	Variável de dados da string a ser decodificada. O resultado decodificado é colocado de volta nessa variável.
match	string (ENTRADA)	String de bytes correspondente na variável de string data_decode.
escape	string (ENTRADA)	String de escape a ser removida da variável data_decode.

Por exemplo:

O exemplo a seguir codifica uma string, copia essa string para salvar a versão codificada e a decodifica com os mesmos parâmetros.

```
COPY(svar:"Este é só um teste de decodificação")
ENCODE(svar, " ", "\00\")
COPY(svar_encode:svar)
DECODE(svar, " ", "\00\")
```

Conteúdo das variáveis de saída atuais:

```
svar ="Este é só um teste de decodificação"
svar_encode = "Este\00\ é\00\ só\00\ um\00\ teste\00\
   de\00\ decodificação"
```

DECODEMIME

O comando DECODEMIME permite ao usuário decodificar uma string codificada de base-64 ou uma variável de string usando a decodificação de base-64 e armazenar a string decodificada resultante em uma variável de string. Se houver um erro, o tamanho da string de dados resultante seria zero e o sucesso da variável de número opcional seria definido como 0. Se a decodificação for bem-sucedida, o sucesso da variável de número será definido como 1.

Formato

```
DECODEMIME(encoded_data, dados, sucesso)
```

Tipos de dados

Argumento	Tipo	Descrição
encoded_data	String/variável de string (ENTRADA).	String codificada de base-64 que precisa ser decodificada.
data	Variável de string (SAÍDA).	Dados decodificados resultantes.
success	Variável inteira/Variável flutuante (SAÍDA). [OPCIONAL]	Definido como um se a decodificação for bem-sucedida; caso haja erro, é definido como zero.

Por exemplo:

```
DECODEMIME("VGVzdGluZyBEYXRhIEVuY29kaW5n", s_data,
   i_success)
```

No exemplo acima, o comando DECODEMIME decodifica a string entre aspas usando a decodificação de base-64 e armazena a string decodificada resultante em s_data. S_data é preenchido com o seguinte:

```
test encode64 command
```

Como a decodificação é bem-sucedida, o valor 1 é atribuído à variável inteira i_success.

Consulte também o comando ENCODEMIME.

DELETE

O comando DELETE remove variáveis do sistema para liberar a memória alocada para armazená-las (isso é especialmente útil para variáveis de string).

Recomenda-se que você apague parâmetros svar ao terminar para economizar memória. É possível especificar até 100 variáveis em um comando DELETE.

Formato

```
DELETE(<varlist>)
```

Onde:

```
varlist ::= var [, <varlist>]
Var ::= variável a limpar (fvar, ivar ou svar)
```

Número máximo de variáveis: 100

Tipos de dados

Argumento	Tipo	Descrição
var1	variável (ENTRADA/ SAÍDA)	Variável a ser apagada (fvar, ivar ou svar).
var2	variável (ENTRADA/ SAÍDA) [OPCIONAL]	Variável a ser apagada (fvar, ivar ou svar).
var3	variável (ENTRADA/ SAÍDA) [OPCIONAL]	Variável a ser apagada (fvar, ivar ou svar).
...	variável (ENTRADA/ SAÍDA) [OPCIONAL]	Outras variáveis a serem apagadas (fvar, ivar ou svar).

Por exemplo:

```
DELETE(ivar1)
DELETE(sdata, i_len, i_count, svar[22])
DELETE(imatrix3d[ix][iy][iz])
DELETE(f_array[i_count], svar[4], sdata)
DELETE(ichart[3][icount])
```

DISPLAY

O comando DISPLAY exibe as variáveis de script e seus valores atuais em uma janela popup.

Você pode fazer o seguinte:

- Usar o comando ao depurar scripts;
- Se uma string for usada como parâmetro, ele exibirá o conteúdo dessa string;
- Strings que contêm dados hexadecimais são exibidas no formato hexadecimal (ou seja, string="\0a 0d\").

O programa primeiro tenta exibir a string no ASCII. Se a string contém tanto dados hexadecimais que podem ser impressos como que não podem ser impressos, os caracteres são exibidos no ASCII e a string remanescente é exibida em formato hexadecimal. Na substituição hexadecimal, \0000\ encerra uma string, portanto "xxxx\0000\yyyy" se torna "xxxx".

Formato

```
DISPLAY(string_data)
```

Tipos de dados

Argumento	Tipo	Descrição
string_data	string (ENTRADA) [OPCIONAL]	Qualquer string específica a ser exibida. Se for deixada de fora, todos os conteúdos de variáveis serão exibidos (strings, números e matrizes) em todos os scripts.

Por exemplo:

```
DISPLAY( )
DISPLAY(sdata_var)
DISPLAY("Oi, isso são dados de string")
DISPLAY(sdata_var)
```

ELSE

O comando ELSE marca o fim da parte verdadeira do comando IF() associado anterior. Os comandos de análise após o ELSE() são executados se o resultado do comando IF() é FALSE. Os comandos são executados até o próximo comando ENDIF() correspondente.

Formato

```
ELSE()
```

Por exemplo:

```
IF(i = 10)
ALERT("I é 10")
ELSE()
ALERT("I não é 10")
ENDIF()
```

Você não pode fazer comparações diretas com um número negativo. Para isso, use um destes dois métodos:

- Use a comparação de funções de análise;
- Compare indiretamente como mostrado a seguir:

```
SET(i_compare_val=-10)
IF(ivar > i_compare_val)
```

```
ALERT("ivar é maior que -10")
endif()
```

ENCODE

Use o comando ENCODE para preservar a identificação de pacote. Esse comando faz a correspondência de bytes (ou caracteres) nos dados e inclui (ou inclui como prefixo) uma string de escape nos bytes correspondentes. A string de escape é colocada na frente dos bytes correspondentes sempre que esses caracteres são encontrados nos dados.

Formato

```
ENCODE(data_encode, correspondência, escape)
```

Tipos de dados

Argumento	Tipo	Descrição
data_encode	svar (ENTRADA/ SAÍDA)	Variável de dados da string a ser codificada. O resultado codificado é colocado de volta nessa variável.
match	string (ENTRADA)	String de bytes correspondente na variável de string data_encode.
escape	string (ENTRADA)	String de escape a ser colocada na frente de cada byte correspondente dentro da variável data_encode.

Por exemplo:

No exemplo a seguir, duas strings de dados são codificadas para anteceder todos os espaços com um "#" e outra, para anteceder todas as letras 't' e 'h' com "!!".

```
COPY(data:"Anteceder todos os espaços com '#'")
ENCODE(dados, " ", "#")
COPY(svar:"Anteceder letras 't' e 'h' com '!!'")
ENCODE(svar, "th", "!!")
```

O resultado será:

```
data = "Anteceder# todos# os# espaços# com# '#'"
svar = "Anteceder le!!tras '!!t' e '!!h' com '!!'"
```

ENCODEMIME

O comando ENCODEMIME permite ao usuário codificar uma string ou variável de string usando a codificação de base-64 e armazenar a string codificada resultante em uma variável de string.

Formato

```
ENCODEMIME(dados, encoded_data)
```

Tipos de dados

Argumento	Tipo	Descrição
data	String/variável de string (ENTRADA).	String de dados que precisa ser codificada.
encoded_data	Variável de string (SAÍDA)	Dados codificados resultantes.

Por exemplo:

```
COPY(s_data:"test encode64 command")
ENCODEMIME(s_data, s_encd_data)
```

No exemplo acima, o comando ENCODEMIME codifica a string na variável s_data usando a codificação de base-64 e armazena a string codificada resultante em s_encd_data. S_encd_data é preenchido com o seguinte:

```
VGVzdGluZyBEYXRhIEVuY29kaW5n
```

Consulte também o comando DECODEMIME.

ENDFOR

O comando ENDFOR marca o fim do bloco FOR() anterior.

Formato

```
ENDFOR()
Exemplo
FOR(i=0,i<3,i=i+1)
ALERT("Ainda em loop")
ENDFOR()
```

ENDIF

O comando ENDIF marca o fim do bloco IF() anterior.

Formato

```
ENDIF()
```

Por exemplo:

```
IF(i = 10)
ALERT("I é 10")
ELSE()
ALERT("I não é 10")
ENDIF()
```

Você não pode fazer comparações diretas com um número negativo. Para isso, use um destes dois métodos:

- Use a comparação de funções de análise;
- Compare indiretamente como mostrado a seguir:

```
SET(i_compare_val=-10)
IF(ivar >i_compare_val)
ALERT("ivar é maior que -10")
ENDIF()
```

ENDWHILE

O comando ENDWHILE marca o fim do bloco WHILE() anterior.

Formato

```
ENDWHILE()
Exemplo
WHILE(i<3)
SET(i=i+1)
ENDWHILE()
```

EVENT

O comando EVENT cria e envia uma mensagem de alerta. Ele não adota nenhum parâmetro. O comando EVENT cria automaticamente a mensagem de alerta usando o conteúdo das variáveis reservadas.

A maioria das variáveis reservadas é mapeada diretamente para as metatags do gabarito do Assistente do v3.2. Somente as variáveis usadas no script e que não são definidas para "" são enviadas. Variáveis como i_Severity e s_Res são necessárias para que uma mensagem de alerta seja processada pelo Gerenciador de Coletores.

Variáveis reservadas de evento

NOTA: Quando uma etiqueta é precedida por um 'e', como e.crt, isso se refere a eventos atuais. Se uma etiqueta é precedida por um 'w.', como w.crt, isso se refere a eventos do histórico.

Variável	Descrição rápida	Mapas para metatag (etiqueta)
s_BM	Mensagem base	Mensagem (msg)
i_Severity	Gravidade	Gravidade (sev)
s_Res	Recurso	Recurso (res)
s_SubRes	Sub-recurso	Sub-recurso (sres)
s_ET	Horário do evento	Horário do evento (et)
s_P	Protocolo	Protocolo (prot)
s_DP	Porta de destino	Porta de destino (dp)
s_SP	Porta de origem	Porta de origem (sp)
s_EVT	Nome do evento	Nome do evento (evt)
s_SN	Nome do sensor	Nome do sensor (sn)
s_SIP	IP de origem	IP de origem (sip)
s_DIP	IP de destino	DestinationIP (dip)
s_SHN	Nome do host de origem	Nome do host de origem (shn)
s_DHN	Nome do host de destino	Nome do host de destino (dhn)
s_SUN	Nome de usuário de origem	Nome de usuário de origem (sun)
s_DUN	Nome de usuário de destino	Nome de usuário de destino (dun)
s_FN	Nome do arquivo	Nome do arquivo (fn)
s_EI	Informações completas	Informações completas (ei)
s_RN	Nome do relator	Nome do relator (rn)
s_ST	Tipo de sensor	Tipo de sensor (st)
s_PN	Nome do produto	Nome do produto (pn)
s_CRIT	Importância	Importância (crt)
s_VULN	Vulnerabilidade	Vulnerabilidade (vul)
s_CT1	Cliente reservado 1	Ct1 (ct1)
s_CT2	Cliente reservado 2	Ct2 (ct2)
s_CT3	Cliente reservado 3	Ct3 (ct3)
s_RT1	Nome do ataque ao dispositivo (Sentinel reservado 1)	Rt1 (rt1)
s_RT2	Sentinel reservado 2	Rt2 (rt2)
s_RT3	Sentinel reservado 3	Rt3 (rt3)
s_CV1 to s_CV100	Variáveis de cliente de 1 a 100 **NOTA**: 1 a 10 são do tipo long (numéricas) 11 a 20 são do tipo date 21 a 100 são do tipo string	Cv1 a Cv100 (cv1 a cv100)
s_RV1 to s_RV29	Valores reservados de 1 a 29 **NOTA**: Reservado para uso da Novell.	Rv1 a Rv31 (rv1 a rv29)
s_RV30	AttackID	Rv30
s_RV31	Nome do dispositivo	Rv31

Variável	Descrição rápida	Mapas para metatag (etiqueta)
s_RV32	Categoria do dispositivo	Rv32 (rv32)
s_RV33	Contexto do evento	Rv33 (rv33)
s_RV34	Nível de ameaça de origem	Rv34 (rv34)
s_RV35	Contexto do usuário de origem	Rv35 (rv35)
s_RV36	Contexto dos dados	Rv36 (rv36)
s_RV37	Função de origem	Rv37 (rv37)
s_RV38	Contexto operacional de origem	Rv38 (rv38)
s_RV39	Nome do cliente MSSP	Rv39 (rv39)
s_RV40 to s_RV43	Valores reservados de 40 a 43 **NOTA:** Reservado para uso da Novell.	Rv40 a Rv43 (rv40 a rv43)
s_RV44	Nível de ameaça de destino	Rv44 (rv44)
s_RV45	Contexto do usuário de destino	Rv45 (rv45)
s_RV46	Status de vírus	Rv46 (rv46)
s_RV47	Função de destino	Rv47 (rv47)
s_RV48	Contexto operacional de destino	Rv48 (rv48)
s_RV49	Variável reservada 49 **NOTA:** Reservada para uso da Novell.	Rv49 (rv49)
s_RV50	Nível de taxonomia eSec 1	Rv50 (rv50)
s_RV51	Nível de taxonomia eSec 2	Rv51 (rv51)
s_RV52	Nível de taxonomia eSec 3	Rv52 (rv52)
s_RV53	Nível de taxonomia eSec 4	Rv53 (rv53)
s_RV54 to s_RV100	Valores reservados de 54 a 100 **NOTA:** Reservado para uso da Novell.	Rv54 a Rv100 (rv54 a rv100)

Auto-formatação

As variáveis reservadas s_DP, s_SP e s_P são definidas em letras minúsculas antes de a mensagem de evento ser enviada. As variáveis reservadas s_ST e s_PN são definidas em letras maiúsculas antes de a mensagem de evento ser enviada. A variável s_ET da variável de horário do evento será definida se for deixada em branco com o formato de horário padrão, como mostrado a seguir:

```
s_Year-s_Month-s_Day~sHour:s_Min:s_Sec~s_AMPM24~s_TZ
```

Você pode substituir esse recurso definindo a variável s_ET com outras informações. Pelo menos as variáveis s_Hour e s_Month devem ser definidas para que ET seja criada. Todos os campos vazios aparecerão no campo ET como NULL.

Variáveis reservadas de data/horário

A variável s_ET da metatag ET será preenchida automaticamente se s_ET for deixada em branco e s_Hour e s_Month não estiverem vazias. As variáveis reservadas de data/horário

devem ter valores definidos. Qualquer campo vazio aparecerá como NULL. O campo s_Day é formatado com valores de dois dígitos de 01 a 09. O gravador de scripts pode optar por converter o valor de mês em um número de dois dígitos usando o comando TRANSLATE e o arquivo months.csv. As tags reservadas de data/horário são as seguintes:

- s_Year
- s_Month
- s_Day
- s_Hour
- s_Min
- s_Sec
- s_TZ
- s_AMPM24

Variáveis reservadas de controle de evento

Duas variáveis, s_SendEITag e s_SendETTag, são usadas para determinar se o comando EVENT incluirá os campos EI e ET, respectivamente, em uma mensagem de alerta. Para o envio de qualquer desses campos ser desativado, as variáveis devem ser definidas como OFF.

Formato

```
EVENT ()
```

Por exemplo:

```
COPY(s_Res:"Resource")
SET(i_Severity = 3)
COPY(s_BM:"Alerta")
EVENT()
```

FILEA

O comando FILEA anexa o conteúdo de uma string ao final de um arquivo simples armazenado em disco. Quando esse comando é usado:

- Especifique o nome do arquivo que está usando uma string;
- No Windows, o nome do arquivo faz referência ao arquivo conforme especificado, se o nome começar com a letra da unidade, dois-pontos e barra invertida (por exemplo, c:\);
- O caminho completo do arquivo deve ser especificado;
- Se ainda não existir, o arquivo será criado;
- Se o arquivo não puder ser criado, o comando FILEA não fará nada;
- O arquivo é fechado depois que os dados são anexados a ele.

Se estiver criando esse comando como parte de um script para ser executado por um Coletor, você deve usar a sintaxe de caminho correta, incluindo as barras (/). Ao especificar o caminho, lembre-se de anteceder os caracteres de barra e barra invertida com um caractere de escape. O zero final no encerramento da string não é gravado no arquivo.

Formato

```
FILEA("nome do arquivo", data)
```

Tipos de dados

Argumento	Tipo	Descrição
filename	string (ENTRADA)	Nome do arquivo ao qual os dados devem ser aplicados.
data	string (ENTRADA)	String de dados a ser anexada ao arquivo.

Por exemplo:

No exemplo a seguir, o arquivo \temp\mux_data é criado e o conteúdo da variável s_variable é adicionado ao arquivo:

```
FILEA("c:/\temp/\mux_data", s_variable)
FILEA("mux_data", "literal")
FILEA("mux_data", s_variable)
```

No exemplo a seguir, uma string é adicionada ao final de um arquivo de registro de auditoria.

```
COPY(audit_str: "Enviados 5 alertas de gravidade 20.")
FILEA("h:/\temp/\audit.log", audit_str)
```

FILEL

O comando FILEL captura o tamanho (em bytes) de um arquivo simples e coloca o valor em uma variável numérica. Quando esse comando é usado:

- Especifique o nome do arquivo que está usando uma string;
- No Windows, o nome do arquivo faz referência ao arquivo conforme especificado, se o nome começar com a letra da unidade, dois-pontos e barra invertida (por exemplo, c:\);
- Se o arquivo não existir, o comando FILEL não fará nada e o conteúdo da variável numérica numvar não será alterado;
- O arquivo é fechado depois que os dados são lidos nele;

Se estiver criando esse comando como parte de um script para ser executado por um Coletor, você deve usar a sintaxe de caminho correta, incluindo as barras (/). Ao especificar o caminho, lembre-se de anteceder os caracteres de barra e barra invertida com um caractere de escape.

Formato

```
FILEL("nome do arquivo", i_length)
```

Tipos de dados

Argumento	Tipo	Descrição
filename	string (ENTRADA)	Nome do arquivo cujo tamanho será determinado.
i_length	numvar (SAÍDA)	Tamanho do arquivo, em bytes.

Por exemplo:

```
FILEL("h:/\tmp/\onfotron.log", i_length)
```

Retorna o tamanho do arquivo infotron.log, em bytes, por exemplo:

```
i_length = 2390
```

FILER

O comando FILER copia o conteúdo de um arquivo simples armazenado em disco para uma variável de string. Quando esse comando é usado:

- Especifique o nome do arquivo que está usando uma string;
- No Windows, o nome do arquivo faz referência ao arquivo conforme especificado, se o nome começar com a letra da unidade, dois-pontos e barra invertida (por exemplo, c:\);
- Se o arquivo não existir, o comando FILER não fará nada e o conteúdo da variável svar não será alterado;
- O arquivo é fechado depois que os dados são lidos nele;
- Se preferir, digite o número máximo de bytes a serem lidos. Você não pode usar o parâmetro max_bytes se não estiver acompanhado pelo parâmetro i_offset;

Se estiver criando esse comando como parte de um script para ser executado por um Coletor, você deve usar a sintaxe de caminho correta, incluindo as barras (/). Ao especificar o caminho, lembre-se de anteceder os caracteres de barra e barra invertida com um caractere de escape.

Formato

```
FILER("nome do arquivo", dest, [i_offset [,
   i_max_bytes]])
```

NOTA: Você não pode usar o parâmetro max_bytes se não estiver acompanhado pelo parâmetro i_offset.

Tipos de dados

Argumento	Tipo	Descrição
filename	string (ENTRADA)	Nome do arquivo do qual a string de dados deve ser lida.
data	svar (SAÍDA)	Os dados lidos no arquivo são colocados nesta variável de string.
i_offset	inteiro (ENTRADA) [OPCIONAL]	Especifica o número de caracteres de diferença no qual começar a leitura.

Argumento	Tipo	Descrição
max_bytes	inteiro (ENTRADA) [OPCIONAL]	Se preferir, especifique o número máximo de bytes a serem lidos. **NOTA:** Quando você usa esse argumento, o argumento i_offset deve ser especificado.

Por exemplo:

```
CLEAR(data)
FILER("nome do arquivo", data, 0, 20)
if(data = "")
ALERT(s_res_var, "Arquivo de dados inexistente ou
   vazio.", 0)
ENDIF()
```

FILEW

O comando FILEW grava o conteúdo de uma string em um arquivo simples armazenado em disco. Quando esse comando é usado:

- O conteúdo anterior do arquivo é sobregravado;
- Especifique o nome do arquivo que está usando uma string;
- No Windows, o nome do arquivo faz referência ao arquivo conforme especificado, se o nome começar com a letra da unidade, dois-pontos e barra invertida (por exemplo, c:\);
- Se ainda não existir, o arquivo será criado;
- Se o arquivo não puder ser criado, o comando FILEW não fará nada;
- O arquivo é fechado depois que os dados são gravados nele.

Se estiver criando esse comando como parte de um script para ser executado por um Coletor, você deve usar a sintaxe de caminho correta, incluindo as barras (/). Ao especificar o caminho, lembre-se de anteceder os caracteres de barra e barra invertida com um caractere de escape.

Formato

```
FILEW("nome do arquivo", data)
```

Tipos de dados

Argumento	Tipo	Descrição
filename	string (ENTRADA)	Nome do arquivo no qual a string de dados deve ser gravada.
data	svar (SAÍDA)	Dados a serem gravados no arquivo.

Por exemplo:

```
FILEW("nome do arquivo", data)
FILEW("h:/\tmp/\infotron.stat", "EXECUÇÃO BEM-SUCEDIDA")
```

FOR

O comando FOR fornece recursos de loop do fluxo de controle. Quando esse comando é usado:

- A declaração de inicialização sempre é executada;
- Se o resultado da declaração de comparação FOR() é verdadeiro, os comandos de análise após o comando FOR(), até o próximo ENDFOR(), são executados; A declaração de incremento é, então, executada e o fluxo de controle retorna para a declaração de comparação;
- Se o resultado da declaração de comparação FOR() é falso, nenhum comando de análise é executado entre os comandos FOR() e ENDFOR(); A declaração de incremento não é executada;
- Embora todos os tipos de dados sejam aceitos em cada lado da declaração de comparação FOR(), valores numéricos só podem ser comparados com valores numéricos e strings, só com strings;
- O operador da comparação FOR() pode ser <, =, >, <=, >=, <>, &, + ou ^.

Você não pode fazer comparações diretas com um número negativo. Para isso, use um destes dois métodos:

- Use a função de análise COMPARE;
- Compare indiretamente como mostrado a seguir:

```
SET(i_compare_val=-10)
FOR(ivar=0, ivar>i_compare_val, ivar=ivar-1)
ALERT("Ainda em loop")
ENDFOR()
```

Formato

```
FOR(inicialização, comparar, incremento)
```

Tipos de dados

Argumento	Tipo	Descrição
initialization	SET() parameter	Qualquer parâmetro válido que possa ser passado para o comando SET(). Consulte a definição do comando SET().
conditional	IF() conditional	Qualquer parâmetro válido que possa ser passado para o comando IF(). Consulte a definição do comando IF().
increment	SET() parameter	Qualquer parâmetro válido que possa ser passado para o comando SET(). Consulte a definição do comando SET().

Por exemplo:

```
FOR(i=0, i<3, i=i+1)
```

GETCONFIG

Recupera a configuração atual de uma propriedade do sistema. Esse comando é usado para recuperar a configuração de propriedades de sistema usando o comando SETCONFIG. Esses comandos são usados para definir variáveis e recuperar valores atuais de propriedades de sistema que podem mudar periodicamente, como um arquivo de registro que é renomeado diariamente com a data atual.

As propriedades de sistema disponíveis são:

Propriedade de sistema	**Exemplo(s):**
▪ System.OS.Family	Solaris e Windows
▪ System.OS.Name	Windows 2000
▪ System.OS.Version.Major	5
▪ System.OS.Version.Minor	0
▪ System.Net.Hostname	ESECServer
▪ System.Net.IP_List	Lista de IPs para este host separados por ponto e vírgula, por exemplo "172.163.3.45;172.45.2.1"

Consulte também o comando SETCONFIG.

Existem dois parâmetros necessários.

- O primeiro define a opção de configuração (FileConnector.InputFile) ou (FileConnector.OutputFile).
- O segundo parâmetro necessário define o valor de configuração a ser recuperado.

Formato

```
GETCONFIG(Opção de configuração, Valor)
```

Tipos de dados

Argumento	**Tipo**	**Descrição**
Opção de Opção	string (ENTRADA)	Nome da variável de configuração a ser recuperada. Arquivo de entrada = "FileConnector.InputFile" Arquivo de saída = "FileConnector.OutputFile"
Valor	string (ENTRADA)	Configuração a ser recuperada.

Por exemplo:

```
GETCONFIG("FileConnector.InputFile", s_inputfilename)
GETCONFIG("FileConnector.OutputFile", s_outputfilename)
```

Conteúdo das variáveis de saída atuais

```
"C:/\nome_do_arquivo.txt"
```

GETENV

O comando GETENV recupera o valor de uma variável de ambiente.

Formato

```
GETENV(Chave de ambiente, variável a armazenar valor)
```

Tipo de dados

Argumento	Tipo	Descrição
Chave de ambiente	string (ENTRADA)	Nome da variável de ambiente.
Variável a armazenar valor	Variável de string (ENTRADA)	Destino em que a variável de ambiente será colocada.

Por exemplo:

```
GETENV("ESEC_HOME", s_EsecHome)
```

HEXTONUM

O comando HEXTONUM converte uma string hexadecimal com até 4 bytes de dados hexadecimais em um número decimal e coloca esse número em uma variável inteira ou flutuante. Mais de 4 bytes resultam em dados inválidos.

Formato

```
HEXTONUM(bytes_data, i_val [,[-]i_4] [, ioffset])
```

Tipos de dados

Argumento	Tipo	Descrição
bytes_data	string (ENTRADA)	String de 1 a 4 bytes. (Por exemplo: "\FF\", "\FF FF\", "\3C 4A F2\", "\43 76 F3 FF\" ou "TEST"). O número hexadecimal representado por esses bytes será convertido em um valor inteiro, i_val.
i_val	numvar (SAÍDA)	O equivalente decimal de número hexadecimal é colocado nessa variável, ivar ou fvar.

Argumento	Tipo	Descrição
i_len	valor numérico (ENTRADA) [OPCIONAL]	Número de bytes hexadecimais a serem convertidos em um inteiro (deve haver uma faixa de valores absolutos de 1 - 4). Se você não definir esse parâmetro, o valor padrão será o número de bytes na string de entrada, bytes_data, até 4 bytes. Se o parâmetro i_len for positivo, os bytes serão interpretados como Esquerda-para-Direita (Byte-Mais-Importante para Byte-Menos-Importante). Se o parâmetro i_num_bytes for negativo, os bytes serão interpretados como Direita-para-Esquerda (Byte-Menos-Importante para Byte-Mais-Importante).
ioffset	valor numérico (ENTRADA) [OPCIONAL]	Número de bytes de diferença a ser ignorado em bytes_data.

Por exemplo:

No exemplo a seguir, os dados na string hexadecimal "\5A32\" são convertidos em um valor inteiro, interpretado como do MSB para LSB (Mais Importante para Menos Importante) e, em seguida, como do LSB para MSB.

```
COPY(dados:"\5A 32\")
HEXTONUM(dados, ivar1)
HEXTONUM(dados, ivar2, -2)
```

NOTA: Na substituição hexadecimal, \0000\ encerra uma string, portanto "xxxx\0000\yyyy" se torna "xxxx".

Conteúdo das variáveis de saída atuais:

```
ivar1 = 23090
ivar2 = 12890
```

IF

O comando IF compara dois valores.

- Se o resultado da declaração IF() é verdadeiro, os comandos de análise após o comando IF(), até o próximo ELSE() ou ENDIF(), são executados;
- Se o resultado da declaração IF() é falso, os comandos de análise após o comando ELSE() até ENDIF() são executados;
- Se nenhum comando ELSE() é usado, nenhum comando de análise é executado entre os comandos IF() e ENDIF() quando o resultado da declaração IF() é falso;

- Embora todos os tipos de dados sejam aceitos em cada lado da declaração IF(), valores numéricos só podem ser comparados com valores numéricos e strings, só com strings;
- O operador da comparação IF() pode ser <, =, >, <=, >=, <>, &, + ou ^; Não utilize o operador NOT lógico (^) junto com uma variável de string. Isso causará um erro de sintaxe.

Você não pode fazer comparações diretas com um número negativo. Para isso, use um destes dois métodos:

- Use a função análise COMPARE;
- Compare indiretamente como mostrado a seguir:

```
SET(i_compare_val=-10)
IF(ivar > i_compare_val)
ALERT("ivar é maior que -10")
ENDIF()
```

Formato

```
IF(<expr>)
Onde:
expr ::= var
        | (<expr>)
        | ^ <expr>
```

Onde <expr> deve ser avaliado como variável inteira ou flutuante.

```
        | <expr> <|=|>|<=|>=|<>|&|+ <expr>
```

Onde ambos os parâmetros <expr> devem ser avaliados como o mesmo tipo.

Tipos de dados

Argumento	Tipo	Descrição
data1	variável (ENTRADA)	Dados a serem comparados com data2. Se data2 não for usado, ele se tornará um operador lógico (0 = false, todos os outros = true).
Operador lógico	< = > <= >= <> & + ^	Menor que Igual a Maior que Menor que ou Igual a Maior que ou Igual a Diferente de Operador lógico AND Operador lógico OR Operador lógico NOT
data2	todos (ENTRADA) [OPCIONAL]	Dados a serem comparados com o data1. Devem ser do mesmo tipo que o data1.
…	idem acima	Use até 200 parâmetros individuais para criar expressões lógicas complexas.

Por exemplo:

```
IF(s = "teste" & i_count < 5)
script(test)
ELSE()
IF((i <= i_num) + (i_count <> 10) & (i_page))page("111")
ENDIF()
ENDIF()
```

INC

O comando INC aumenta uma variável numérica em 1. Ao usar esse comando, você deve especificar uma variável inteira flutuante.

Formato

```
INC(i_counter)
```

Tipos de dados

Argumento	Tipo	Descrição
i_counter	numvar (ENTRADA/ SAÍDA)	Variável numérica à qual acrescentar 1.

Por exemplo:

```
SET(icounter = 0)
INC(icounter)
INC(icounter)
```

O resultado será:

```
icounter = 2
```

INDICATOR

O comando INDICATOR envia mensagens do indicador ao Sentinel. As mensagens contêm textos a serem exibidos no indicador especificado no Sentinel.

Formato

```
INDICATOR(name, value)
```

NOTA: Antes da versão v4.0, o comando INDICATOR tinha argumentos adicionais que não são mais usados. Para compatibilidade com Coletores antigos, esses argumentos são marcados com a etiqueta "Não usado" na janela do Editor de Comandos do Assistente.

Tipos de dados

Argumento	Tipo	Descrição
nome	string (ENTRADA)	Nome do indicador.
value	string (ENTRADA)	Texto do indicador a ser exibido no Console do Sentinel. Por exemplo: `IMPRESSORA LIGADA`

Por exemplo:

```
INDICATOR("memória", "5 MB")
INDICATOR(name, value)
```

NOTA: O nome do indicador no comando de análise deve corresponder ao nome do indicador no Sentinel; caso contrário, o indicador não será atualizado no Console do Sentinel.

INFO_CLEARTAGS

Essa função zera (ou limpa, no caso de strings) todas as variáveis que fazem parte do conjunto do bloco de informações a que faz referência o handle. Use o comando INFO_CONSTANTTAGS para evitar que isso aconteça com um subconjunto dessas tags.

Formato

```
INFO_CLEARTAGS(<handle IN>)
```

Tipos de dados

Argumento	Tipo	Descrição
Handle IN	string (ENTRADA)	Tipo de bloco de informações.

INFO_CLOSE

Esse comando é usado para encerrar uma sessão de bloco de informações. Quando chamado, ele primeiro envia qualquer bloco de informações não enviado, assim como faria o comando INFO_SEND. Em seguida, ele envia uma mensagem de fechamento de sessão do bloco de informações, definindo o atributo EOD (fim dos dados) do elemento de informações como "true" (verdadeiro). Depois de enviar a mensagem de fechamento, o número de segmentos ("segnum") é aumentado em 1.

Formato

```
INFO_CLOSE(<handle IN>)
```

Tipos de dados

Argumento	Tipo	Descrição
Handle IN	string (ENTRADA)	Tipo de bloco de informações.

INFO_CONSTANTTAGS

Use esse comando para nomear tags que não serão limpas quando INFO_CLEARTAGS for chamado. Inclua zero ou mais nomes de tag para criar o conjunto de tags constantes. Múltiplas chamadas para essa função redefinirão a lista de tags constantes.

Formato

```
INFO_CONSTANTTAGS(<HANDLE IN>, [<Nome da tag IN>, …])
```

Tipos de dados

Argumento	Tipo	Descrição
Handle IN	string (ENTRADA)	Tipo de bloco de informações.
Nome da tag IN	string (ENTRADA)	Nome de referência ao handle IN

INFO_CREATE

Esse comando cria um novo conjunto de bloco de informações. Você deve passar um handle (que será usado um comando sim, um comando não para afetar esse conjunto de blocos de informações). Você também deve passar um tipo. Esta é uma string de sua escolha, mas deve ser formalizada (consulte INFO_SEND).

Se você chamar o comando INFO_CREATE em um handle existente, ele limpará o conteúdo desse handle como se você estivesse começando um handle novo. Será necessário chamar os comandos INFO_SETTAG e INFO_CONSTANTTAGS novamente.

Formato

```
INFO_CREATE(<Handle OUT>,<Tipo IN>)
```

Tipos de dados

Argumento	Tipo	Descrição
Handle OUT	string (SAÍDA)	Nome de referência ao tipo IN
Tipo	string (ENTRADA)	Tipo de bloco de informações.

INFO_DUMP

Esse comando fará persistir o atual estado do conjunto de bloco de informações em uma variável de string. Isso foi incluído para facilitar os testes, mas também pode ser usado para reproduzir conjuntos de blocos de informações ou para salvá-los em um arquivo de texto ou de outro tipo que você preferir. Além disso, não tem o efeito colateral do comando INFO_SEND de não eliminar o estado atual.

Formato

```
INFO_DUMP(<Handle IN>, <Variável de string OUT>)
```

Tipos de dados

Argumento	Tipo	Descrição
Handle IN	string (ENTRADA)	Tipo de bloco de informações.
Variável de string OUT	string (SAÍDA)	Variável de string de referência ao handle IN

INFO_PUSH

Esse comando irá colocar uma tag nos valores atuais de todos os nomes de tags (por meio de suas variáveis associadas) e as empurrará para o final de uma lista de blocos de informações com referência de um handle. Os blocos continuarão sendo acumulados no conjunto até que este seja esvaziado por um comando INFO_CREATE, INFO_SEND ou INFO_CLOSE. Para o INFO_CREATE, nenhuma ação é tomada. Para o INFO_SEND, os blocos de informações são enviados ao Gerenciador do Coletor. Para o INFO_CLOSE, os blocos de informações são enviados ao Gerenciador do Coletor e uma mensagem de fechamento do bloco de informações (EndOfData ou EOD) é enviada.

Formato

```
INFO_PUSH(<Handle IN>)
```

Tipos de dados

Argumento	Tipo	Descrição
Handle IN	string (ENTRADA)	Tipo de bloco de informações.

INFO_SEND

Esse comando pega o atual conjunto de blocos de informações e os envia por um canal de comunicação especificado pelo tipo usado durante o INFO_CREATE, anexado à palavra "infoblock.", inclusive o ponto final. Portanto, se o tipo era "vulnerabilidade", o nome do canal pelo qual a mensagem seria enviada seria "infoblock.vulnerabilidade".

Além disso, esse comando removerá o conjunto atual de blocos de informações e aumentará o número de segmentos ("segnum") em 1.

Formato

```
INFO_SEND(<Handle IN>)
```

Tipos de dados

Argumento	Tipo	Descrição
Handle IN	string (ENTRADA)	Tipo de bloco de informações.

INFO_SETTAG

Esse comando irá vincular uma variável de script ao nome de um atributo. Quando INFO_PUSH é chamado (consulte INFO_PUSH), todas as variáveis vinculadas a esse comando são definidas como atributos em uma entrada de bloco.

Formato

```
INFO_SETTAG(<handle IN, nome da tag IN, variável IN)
```

Tipos de dados

Argumento	Tipo	Descrição
Handle IN	string (ENTRADA)	Tipo de bloco de informações.
Nome da tag IN	string (ENTRADA)	Tipo de nome da tag
Variável IN	string (ENTRADA)	Tipo de variável

Tags de bloco de informações sobre vulnerabilidade

Veja a seguir tags válidas de Blocos de informações sobre vulnerabilidade para o comando INFO_SETTAG. As tags marcadas como obrigatórias devem ser definidas para que o bloco de informações seja armazenado como uma vulnerabilidade. Mesmo que o bloco de informações não seja armazenado como uma vulnerabilidade, as tags marcadas como constantes ainda serão extraídas do bloco de informações. Se uma tag definida não constar nesta lista, o back end da vulnerabilidade ignorará a tag.

Nome da tag	Explicação	Tipo	Constante	Obrigatória
ScannerInstance	Nome dado pelo usuário a esta ocorrência do scanner. Geralmente definido nos parâmetros do Coletor.	String	X	
ProductName	Nome do scanner.	String	X	

Nome da tag	Explicação	Tipo	Constante	Obrigatória
ProductVersion	Versão do scanner.	String	X	
ScannerType	Tipo de scanner.	String	X	
Fornecedor	Nome do fabricante do scanner.	String	X	
ScanType	PARCIAL ou TOTAL	String	X	
ScanStartDate	Hora em que a exploração começou.	String		
ScanEndDate	Hora em que a exploração terminou.	String		
IP	IP do recurso.	String		X
HostName	Nome de host do recurso.	String		
Local	Localização do recurso.	String		
Departamento	Departamento do recurso.	String		
BusinessSystem	Sistema da empresa do recurso.	String		
OperationalEnvironment	Ambiente operacional do recurso.	String		
Regulation	Regulamento do recurso.	String		
RegulationRating	Classificação do regulamento do recurso.	String		
Importância	Importância do recurso [1 – 25].	Número		
VulnModule	Módulo usado para detectar a vulnerabilidade.	String		
PortNumber	Número de porta da vulnerabilidade.	Número		
PortName	Nome de porta da vulnerabilidade.	String		
NetworkProtocol	Protocolo de rede da vulnerabilidade.	Número		
ApplicationProtocol	Protocolo de aplicativo da vulnerabilidade.	String		
AssignedVulnSeverity	Gravidade atribuída da vulnerabilidade.	Número		
ComputedVulnSeverity	Gravidade calculada da vulnerabilidade.	Número		
VulnDescription	Descrição da vulnerabilidade.	String		
VulnSolution	Solução da vulnerabilidade.	String		

Nome da tag	Explicação	Tipo	Constante	Obrigatória
VulnSummary	Solução da vulnerabilidade.	String		
VulnCrossRefs	Lista de códigos da vulnerabilidade.	String		
DetectedOs	Sistema operacional detectado quando a vulnerabilidade foi descoberta.	String		
DetectedOsVersion	Versão do sistema operacional detectado quando a vulnerabilidade foi descoberta.	String		
ScannedApp	Aplicativo detectado quando a vulnerabilidade foi descoberta.	String		
ScannedAppVersion	Versão do aplicativo detectado quando a vulnerabilidade foi descoberta.	String		
VulnUserName	Nome de usuário da vulnerabilidade.	String		
VulnUserDomain	Domínio do usuário da vulnerabilidade.	String		
VulnTaxonomy	Taxonomia da vulnerabilidade.	String		
ScannerClassification	Classificação da vulnerabilidade dada pelo scanner.	String		
ExtendedInformation	Informações completas a armazenar nesta vulnerabilidade.	String		
VulnName	Nome da vulnerabilidade dado pelo scanner.	String		

Exemplo de comando INFO_*

A vulnerabilidade de lotes do Sentinel explora pacotes menores (sessões de blocos de informações) que podem ser processados com mais facilidade. Uma sessão de bloco de informações contém múltiplos conjuntos de blocos de informações com um número crescente de segmentos ("segnum"), seguidos por uma mensagem de fechamento da sessão de bloco de informações. A ocorrência de uma sessão de bloco de informações é conhecida por seu "id" globalmente exclusivo. Sempre que INFO_SEND é chamado, um conjunto de blocos de informações com os valores "distribuídos" atuais e o número de segmentos ("segnum") atual serão enviados. Logo após o envio do conjunto, o número de segmentos (segnum) é aumentado em 1. O comando INFO_SEND é chamado para cada lote de dados depois que o

comando INFO_CLOSE é chamado para fechar a sessão de bloco de informações. A mensagem de fechamento do bloco de informações consiste em um conjunto de blocos de informações com o atributo EOD (fim dos dados) definido como "true" (verdadeiro).

Por exemplo:

```
INFO_CREATE(h_vuln,"vulnerabilidade")
INFO_SETTAG(h_vuln,"ALPHA", s_alpha)
INFO_SETTAG(h_vuln,"BETA", i_beta)
INFO_SETTAG(h_vuln,"GAMMA", s_gamma)
INFO_SETTAG(h_vuln,"DELTA", i_delta)
INFO_SETTAG(h_vuln,"^1E*P$S I(L)O.N--", f_epsilon)
INFO_CONSTANTTAGS(h_vuln,"GAMMA","DELTA","^1E*P$S
   I(L)O.N--")
SET(i_beta=12345)
SET(i_delta=123456789)
SET(f_epsilon=1.234)
COPY(s_alpha:"a de arroz")
COPY(s_gamma:"c de cereja")
INFO_PUSH(h_vuln)
INFO_CLEARTAGS(h_vuln)
INFO_PUSH(h_vuln)
INFO_DUMP(h_vuln, s_simulate)
INFO_SEND(h_vuln)
SET(i_beta=6789)
SET(i_delta=987654321)
SET(f_epsilon=3.1415926)
COPY(s_alpha:"a de ameixa")
COPY(s_gamma:"c de cenoura")
INFO_PUSH(h_vuln)
INFO_SEND(h_vuln)
INFO_CLOSE(h_vuln)
```

Os resultados serão:

```
<?xml versão="1.0" codificação="UTF-8"?>
<infos id="B008961E00CB1026B8F000065BBD13AB"
   type="vulnerabilidade" segnum="0" version="4.2.0.0"
   EOD="false">
<info ALPHA="a de arroz" BETA="12345" DELTA="123456789"
   GAMMA="c de cereja" _1EPSILON="1.234"/>
<info ALPHA="" BETA="0" DELTA="123456789" GAMMA="c de
   cereja" _1EPSILON="1.234"/>
</infos>
```

```
<?xml versão="1.0" codificação="UTF-8"?>
<infos id="B008961E00CB1026B8F000065BBD13AB"
   type="vulnerabilidade" segnum="1" version="4.2.0.0"
   EOD="false">
<info ALPHA="a de ameixa" BETA="6789" DELTA="987654321"
   GAMMA="c de cenoura" _1EPSILON="3.1415926"/>
</infos>
<?xml versão="1.0" codificação="UTF-8"?>
<infos id="B008961E00CB1026B8F000065BBD13AB"
   type="vulnerabilidade" segnum="2" version="4.2.0.0"
   EOD="true">
</infos>
```

IPTONUM

O comando IPTONUM converte uma representação de string do endereço IPv4 em um número inteiro e coloca esse número em uma variável inteira. Essa função só suporta endereços IPv4. Um endereço IPv4 que não se inclui na faixa de endereços válida resulta em dados inválidos.

Formato

```
IPTONUM(ip_address, i_integer, i_valid)
```

Tipos de dados

Argumento	Tipo	Descrição
ip_address	svar(ENTRADA)	Endereço IPv4 de string.
i_integer	valor numérico (SAÍDA)	O endereço IPv4 de string é convertido em um valor inteiro. Esse valor é colocado nessa variável.
i_invalid	ivar(SAÍDA) [OPCIONAL}	O valor 0 implica que o IP é inválido. O valor 1 implica que o IP é válido.

Por exemplo:

No exemplo a seguir, o endereço IPv4 "10.10.10.255" é convertido em um número inteiro. i_valid é definido como 1, o que significa que o resultado é válido.

```
IPTONUM("10.10.10.255", i_y, i_valid)
```

Conteúdo da variável de saída atual:

```
i_y = 168430335
i_valid = 1
```

No exemplo a seguir, o endereço IPv4 inválido "10.10.10.258" é convertido em um número inteiro 0. i_valid é definido como 0, o que significa que o resultado não é válido.

```
IPTONUM("10.10.10.258", i_y, i_valid)
```

Conteúdo da variável de saída atual:

```
i_y = 0
i_valid = 0
```

O comando NUMTOIP converte um número em um IP. Consulte NUMTOIP para obter mais informações.

LENGTH ou LENGTH-OPTION2

O comando LENGTH define uma variável numérica com base no tamanho em bytes de uma variável de string (sem contar o zero final).

NOTA: No Editor Visual do Construtor de Coletores, LENGTH e LENGTH-OPTION2 são listados como comandos separados. Eles são o mesmo comando. São fornecidos como descrições de variações do mesmo comando. Para usar o LENGTH-OPTION2 no editor de texto, digite LENGTH.

Formato

```
LENGTH(i_length, s_variable)
```

Tipos de dados

Argumento	Tipo	Descrição
s_variable	string (ENTRADA)	String (geralmente uma variável de string) na qual o tamanho é calculado.
i_length	numvar (SAÍDA)	O tamanho da variável de string, s_variable, é colocado nessa variável numérica.

Por exemplo:

```
LENGTH(i_length, origem)
LENGTH(i_num_bytes, "Fazer isso não tem sentido, pois
   sabemos qual a string cujo tamanho está sendo
   verificado")
```

Os resultados serão:

```
i_num_bytes = 80
```

LOOKUP

O comando LOOKUP faz a correspondência de dados encontrados no buffer de recebimento ou em uma string com strings principais encontradas em um arquivo principal de pesquisa especificado.

Se for encontrado um registro correspondente ao byte de dados do byte, os comandos de análise no registro do arquivo principal de pesquisa serão processados.

Se uma string for especificada como o primeiro parâmetro no comando LOOKUP, esse comando usará essa string quando fizer pesquisas no arquivo principal de pesquisa.

Há cinco argumentos ou parâmetros com esse comando.

- compare – Se um valor numérico for especificado como esse parâmetro, esse número de bytes (o valor numérico) de dados do buffer de recebimento, começando no indicador de buffer Rx, será usado como a string quando as strings principais do arquivo principal de pesquisa forem comparadas;
- lookup name – Esse parâmetro especifica o nome do arquivo principal de pesquisa relativo ao diretório WORKBENCH_HOME;
- imatch – Variável inteira opcional que pode ser especificada para retornar o status do comando LOOKUP. (0=nenhuma correspondência encontrada, 1=correspondência encontrada);
- parameter file – Parâmetro opcional que consiste no nome de um arquivo de parâmetros a ser usado que é diferente do arquivo de parâmetros padrão. O nome do arquivo de parâmetros padrão é <Coletor>.par. Esse nome de arquivo não deve incluir a extensão .par;
- column name – Um parâmetro opcional é a coluna com o arquivo de parâmetro a ser usado para valores de pesquisa. O nome da coluna padrão é o nome do gabarito. Se você especificar esse parâmetro, também deverá usar um nome de arquivo de parâmetro.

Formato

```
LOOKUP(comparar, arquivo de pesquisa [, imatch] [, [nome
   de arquivo do parâmetro] [, nome de coluna]])
```

Tipos de dados

Argumento	Tipo	Descrição
compare	string (ENTRADA) ou valor numérico (ENTRADA)	Dados a serem usados para comparar com os campos no arquivo principal de pesquisa. Essa é uma comparação byte por byte. Número de bytes do buffer de recebimento, usando o indicador de buffer Rx atual, a ser usado para comparar com os campos no arquivo principal de pesquisa. Essa é uma comparação byte por byte. **NOTA:** Isso só funcionará se o rxbuff tiver sido usado para definir o buffer de recebimento.
lookup filename	string (ENTRADA)	Nome do arquivo principal de pesquisa
imatch	numvar (SAÍDA) [OPCIONAL]	Correspondência encontrada. 0=Não 1=Sim
parameter filename	string (ENTRADA)	Nome do arquivo de parâmetro. Padrão: Collector.par
column name	string (ENTRADA)	Coluna no arquivo de parâmetros a ser usada. Padrão: `Nome do Coletor`

Por exemplo:

```
LOOKUP(dados, nome de arquivo, imatch)
```

No exemplo a seguir, o nome do arquivo key_01 é determinado com base no nome colocado no arquivo de parâmetro, não no nome do arquivo principal de pesquisa.

```
LOOKUP(s_variable, {key_01})
LOOKUP(s_variable, {key_01}, imatch, "Enviar Alerta",
   "Elementos Geo")
```

Se houver definições de parâmetro no arquivo de pesquisa, procure-as na coluna Elementos Geo do arquivo de parâmetro Enviar Alerta.

NEGSEARCH

O comando NEGSEARCH realiza uma pesquisa retroativa de uma string no buffer de recebimento. Há dois parâmetros com esse comando.

- search – A pesquisa começa no indicador de buffer Rx atual e continua retroativamente até localizar a string ou chegar ao começo do buffer de recebimento. Se a string é encontrada na pesquisa, o indicador de buffer Rx é atualizado para apontar para o primeiro byte da string pesquisada. Se a string não é encontrada na pesquisa, o indicador de buffer Rx não é alterado;
- ifound – Parâmetro opcional, consistindo em uma variável inteira definida como 1 se a pesquisa localiza a string e como zero se a pesquisa não a localiza.

Formato

```
NEGSEARCH(pesquisa[, ifound])
```

Tipos de dados

Argumento	Tipo	Descrição
search	string (ENTRADA)	String pesquisada no buffer de recebimento, começando com o indicador de buffer Rx atual e pesquisando retroativamente.
ifound	numvar (SAÍDA) (OPCIONAL)	Retorna se a string foi ou não localizada. 0=não localizada 1=localizada

Por exemplo:

```
NEGSEARCH("ALARME LEVE")
NEGSEARCH(search_string)
```

Os exemplos a seguir pesquisam um retorno de carro e uma alimentação de linha:

```
NEGSEARCH("\0d0a\")
NEGSEARCH(dados, ifound)
```

Outro exemplo:

A letra grifada representa o indicador de buffer Rx atual no exemplo.

NOTA: Na substituição hexadecimal, \0000\ encerra uma string, portanto "xxxx\0000\yyyy" se torna "xxxx".

```
Rx Buffer = "Alarme de Rádio leve A"
NEGSEARCH("Ala")
```

O resultado será:

```
Rx Buffer = "Alarme de Rádio leve A"
```

NUMTOHEX

O comando NUMTOHEX converte um número em dados hexadecimais e coloca esses bytes hexadecimais (até 4 bytes) em uma string.

Formato

```
NUMTOHEX(i_decimal, hex_data)
```

Tipos de dados

Argumento	Tipo	Descrição
i_decimal	valor numérico (ENTRADA)	Valor inteiro a ser convertido em dados hexadecimais.
hex_data	svar (SAÍDA)	String de 1 a 4 bytes que são os byte(s) hexadecimal(is) fornecido(s) pelo valor numérico, i_decimal.

Por exemplo:

No exemplo a seguir, o número decimal 16777215 é convertido em dados hexadecimais.

```
SET(i_decimal = 16777215)
NUMTOHEX(i_decimal, shex)
```

Conteúdo da variável de saída atual:

```
shex = "\ff ff ff\"
```

NUMTOIP

O comando NUMTOIP converte um valor numérico em um endereço IPv4, e coloca o endereço IP em uma string.

Formato

```
NUMTOIP(i_integer, ip_address)
```

Tipos de dados

Argumento	Tipo	Descrição
i_integer	valor numérico (ENTRADA)	Valor inteiro a ser convertido em um endereço IPv4.
ip_address	svar(SAÍDA)	Endereço IPv4 de string.

Por exemplo:

No exemplo a seguir, o número decimal 16777215 é convertido em um endereço IPv4.

```
SET(i_integer = 167772161)
NUMTOIP(i_integer, s)
```

Conteúdo da variável de saída atual:

```
s = "10.0.0.1"
```

O comando IPTONUM converte um IP em um número. Consulte NUMTOIP para obter mais informações.

PARSER_ATTACHVARIABLE

O comando PARSER_ATTACHVARIABLE permite que o nome de um par de valores de nome seja associado a uma variável de destino.

Na maioria dos casos, recomenda-se que você crie um analisador e anexe uma variável no estado de inicialização fora do loop. Depois você pode reutilizar esse analisador no loop de análise.

Para obter comandos de análise relacionados, consulte o comando PARSER_CREATEBASIC e o comando PARSER_PARSESTRING.

Analisador NVP (Name-value Pair - Par de Valores de Nome)

O fragmento de código a seguir demonstra o analisador NVP:

```
PARSER_CREATEBASIC (h_nvp, "nvp", "separator==",
   "entry_separator= ", "value_quotes=/"",
   value_quotes_optional=yes")
PARSER_ATTACHVARIABLE (h_nvp,"este",s_this)
PARSER_ATTACHVARIABLE (h_nvp,"me",s_me)
PARSER_ATTACHVARIABLE (h_nvp,"olá",s_hello)
PARSER_PARSESTRING (h_nvp, "this=/"that/" me=/"you =
   them/" hello=/"goodbye/"")
```

Parâmetros

Os parâmetros a seguir são reconhecidos quando aparecem no seguinte formato:

```
"<parameter>=<value>"
```

O <parameter> é um dos itens a seguir e <value> é o respectivo valor para ele.

- separator – Caractere usado para separar o nome do valor;
- entry_separator – Caractere usado para separar um NVP do seguinte;
- name_quotes – Caractere usado em volta do nome (" ou ', por exemplo);
- value_quotes – Caractere usado em volta do valor;
- name_quoted – Defina como "yes" (sim) para que o analisador NVP leve em conta a opção name_quotes;

- value_quoted – Defina como "yes" para que o analisador NVP leve em conta a opção value_quotes;
- name_quotes_optional – Defina como "yes" para permitir aspas opcionais no nome. Se estiver definido como "yes" e as aspas forem omitidas, o nome será terminado pelo espaço em branco opcional seguido do parâmetro separator;
- value_quotes_optional – Defina como "yes" para permitir aspas opcionais no nome.

Se estiver definido como "yes" e as aspas forem omitidas, o valor será terminado pelo espaço em branco opcional seguido do parâmetro entry_separator.

Formato

```
PARSER_ATTACHVARIABLE(<parser_handle>, <name>,
   <target_variable>)
```

Tipos de dados

Argumento	Tipo	Descrição
parser_handle	variável de string (ENTRADA)	Variável de handle de um analisador criado.
nome	string (ENTRADA)	Nome de um NVP.
target_variable	qualquer variável (SAÍDA)	Variável que será definida com o valor associado ao nome de um NVP.

Veja a seguir um exemplo de Analisador de Ponto de Verificação.

```
COLLECTOR SETUP STATE:
PARSER_CREATEBASIC(h_nvp,"nvp", "separator==",
   "entry_separator= ", "value_quotes=/"",
   "value_quotes_optional=yes")
PARSER_ATTACHVARIABLE(h_nvp,"ação", s_EVT)
PARSER_ATTACHVARIABLE(h_nvp,"d_port", s_DP)
PARSER_ATTACHVARIABLE(h_nvp,"proto", s_P)
PARSER_ATTACHVARIABLE(h_nvp,"src", s_SIP)
PARSER_ATTACHVARIABLE(h_nvp,"dst", s_DIP

PARSE STATE:
PARSER_PARSESTRING(h_nvp,s_RXBufferString)
```

PARSER_CREATEBASIC

O comando PARSER_CREATEBASIC define um analisador e o associa a um parâmetro parser_handle. Para obter mais informações, consulte NVP (Name-value Pair) Parser em PARSER_ATTACHVARIABLE.

Na maioria dos casos, recomenda-se que você crie um analisador e anexe uma variável no estado de inicialização fora do loop. Depois você pode reutilizar esse analisador no loop de análise.

Para obter outro comando de análise relacionado, consulte o comando PARSER_PARSESTRING.

Formato

```
PARSER_CREATEBASIC(<parser_handle>, <parser_name>, [,
   <nvp> [, ...]])
```

Tipos de dados

Argumento	Tipo	Descrição
parser_handle	variável de string (SAÍDA)	Variável com que você se refere a este analisador daqui em diante.
parser_name	string (ENTRADA)	Nome da string do analisador simples que está sendo criado. **NOTA:** No momento, só nvp é reconhecido.
nvp	string (ENTRADA) (OPCIONAL)	Par de valores de nome. Zero ou mais strings que contêm um nome de propriedade, seguido por um sinal de igual, seguido por um valor. Os parâmetros reconhecidos são determinados pelo parser_name escolhido. **NOTA**: Quando o nome do analisador é definido como nvp, você deve usar is seguintes argumentos: "separator==" "entry_separator= " "value_quotes=/"" "value_quotes_optional=yes"
nvp1	string (ENTRADA) (OPCIONAL)	Par de valores de nome 1.
nvp2	string (ENTRADA) (OPCIONAL)	Par de valores de nome 2.
…	string (ENTRADA) (OPCIONAL)	Outros pares de valores de nome.

Por exemplo, consulte Exemplo de análise de ponto de verificação em PARSER_ATTACHVARIABLE, Tipos de dados.

PARSER_NEXT

O comando PARSER_NEXT adianta o analisador para a posição seguinte na string de análise, preenchendo as variáveis definidas pelo comando PARSER_ATTACHVARIABLE.

Formato

```
PARSER_NEXT(<parser_handle>, <success_flag>)
```

Tipo de dados

Argumento	Tipo	Descrição
parser_handle	string variável (ENTRADA)	Variável de handle de um analisador criado.
success_flag	numvar (ENTRADA)	0: falha na análise 1: análise bem-sucedida

PARSER_PARSESTRING

O comando PARSER_PARSESTRING processará o string_to_parse usando o analisador criado citado pelo parser_handle. Isso permite que você crie qualquer string arbitrária para análise, em vez de insistir em uma origem de fluxo ou no buffer Rx.

Para obter mais informações, consulte os comandos PARSER_ATTACHVARIABLE e PARSER_CREATEBASIC.

A variável reservada s_RXBufferString pode ser usada como um string_to_parse depois que o Estado de Recebimento analisar a entrada de script. Para obter mais informações, consulte NVP (Name-value Pair) Parser em PARSER_ATTACHVARIABLE.

Formato

```
PARSER_PARSESTRING(<parser_handle>, <string_to_parse>)
```

Tipos de dados

Argumento	Tipo	Descrição
parser_handle	string variável (ENTRADA)	Variável de handle de um analisador criado.
string_to_parse	string (ENTRADA)	A única string que será executada por este analisador.

Por exemplo, consulte Exemplo de análise de ponto de verificação em PARSER_ATTACHVARIABLE, Tipos de dados.

PAUSE

O comando PAUSE faz com que o script atual faça uma pausa imediata de um número "n" de segundos. O comando PAUSE funciona entre as instruções em um estado de análise e entre estados. Ele é útil para definir tempos de ciclo de poll ou para garantir que você não execute poll muito rapidamente (como ao executar poll do registro de um banco de dados).

Você pode especificar vários comandos PAUSE durante uma análise.

Formato

```
PAUSE(iseconds)
```

Argumento	Tipo	Descrição
iseconds	valor numérico (ENTRADA)	Número de segundos de pausa antes de seguir para o próximo estado.

Por exemplo:

```
PAUSE(10)
   PAUSE(iseconds)
```

Ou

```
IF(slowing=true)
   pause(50)
ENDIF( )
```

POPUP

O comando POPUP exibe o conteúdo de uma string em uma tela de uma janela de texto rolável.

Formato

```
POPUP(dados [, título])
```

Tipos de dados

Argumento	Tipo	Descrição
data	string (ENTRADA)	Mensagem de string de dados a ser colocada na janela popup.
title	string (ENTRADA) [OPCIONAL]	String a ser usada como título da janela popup (padrão = "Popup DATA").

Por exemplo:

```
POPUP(data)
POPUP("Olá mundo", "String de título")
POPUP(data, title)
```

PRINTF

O comando PRINTF copia dados formatados em uma variável de string (svar). O comando PRINTF é um comando de análise avançado. Se você começou a linguagem de comandos de análise agora, recomendamos que use os comandos COPY e APPEND até se sentir familiarizado com ela.

Quando esse comando é usado:

- Especifique uma svar como string de destino;
- Especifique uma string de formatação;
- Especifique parâmetros adicionais opcionais para serem explorados com base na string de formatação.

String de formatação

Para usar dados hexadecimais na string de formatação, adote a seguinte convenção:

```
\HX HX HX\
```

Para incluir uma alimentação de linha ao final da string de formatação, esta deve se parecer com a string a seguir:

```
String de formatação\0a\
```

A string de formatação de um retorno de carro, por exemplo, é \0d0a\:

```
PRINTF(message,"Voltagem de %lf \0d0a\",f_volts)
```

A string de formatação de uma guia, por exemplo, é \09\:

```
PRINTF(message,"Voltagem = \09\ %lf",f_volts)
```

Formato

```
PRINTF(dest, format [, <paramList>])
```

onde:

```
<paramList> ::= var [, <paramList>]
```

Tipos de dados

Argumento	Tipo	Descrição
dest	svar (SAÍDA)	Variável de string de destino na qual a string formatada é colocada.
format	string (ENTRADA)	Formato da string a ser copiado na variável de string de destino. Semelhante ao formato do comando C printf; por exemplo, "Executando loop de %d em %s" (consulte % Caracteres para o Formato de Saída).
parm1	todos (ENTRADA) [OPCIONAL]	Todos os tipos de dados, exceto matriz. Deve corresponder à string de formatação.
parm2	todos (ENTRADA) [OPCIONAL]	Todos os tipos de dados, exceto matriz. Deve corresponder à string de formatação.
…	todos (ENTRADA) [OPCIONAL]	Todos os tipos de dados, exceto matriz. Deve corresponder à string de formatação.

Formato

```
% Caracteres para o Formato de Saída
```

Caractere	Tipo	Formato de saída
%d	inteiro	Inteiro decimal com sinal.
%le	flutuante	Valor com sinal no formato [-]d.dddd e [sign]ddd ... onde d é um dígito decimal único, dddd, um ou mais dígitos decimais, ddd, exatamente três dígitos decimais e o sinal, + ou -.

Caractere	Tipo	Formato de saída
%lf	flutuante	Valor com sinal no formato [-]dddd.dddd ... onde dddd é um ou mais dígitos decimais. O número de dígitos antes do ponto decimal depende da magnitude do número e o número de dígitos após o ponto decimal depende da precisão desejada.
%lg	flutuante	Valor com sinal impresso em formato f ou e, o que for mais compacto para o valor e a precisão desejados. O formato e é usado quando o expoente do valor é menor que -4 ou maior que ou igual ao argumento de precisão. Zeros à direita são truncados e o ponto decimal só aparece se for seguido por um ou mais dígitos.
%s	string	Imprime uma variável de string.

Exibindo dígitos de precisão

Por padrão, o comando PRINTF exibe um número em ponto flutuante (float) com seis dígitos de precisão. O padrão de seis dígitos de precisão também se aplica a números de precisão dupla (double).

Para exibir dígitos de precisão adicionais, especifique um valor para o campo de precisão na especificação de formato PRINTF():

```
%[<width>][.<precision>] type>
```

Por exemplo:

```
PRINTF(dest, "%2.3lf", fvar)
```

Produziria o resultado de saída: 22.012, representando 2 casas à esquerda e 3 casas à direita do ponto decimal.

Os exemplos a seguir mostram como passar variáveis de string e inteiras.

```
PRINTF(dest,format_string) PRINTF(mystring,
   "val de matriz[%d][%d] = %s",
   index_x, index_y, matrix[index_x][index_y])
   PRINTF(dest,"Loop de %d no estado %s",iloop,state)
   PRINTF(dest,"%s Dados Formatados em
   %s","string","dest")
```

O exemplo a seguir mostra como passar uma variável flutuante para uma string.

```
PRINTF(message,"Voltagem de %lf",f_volts)
```

Para imprimir números em ponto flutuante (float), use %lf ou %le.

REGEXPREPLACE

O comando REGEXPREPLACE pesquisa e substitui strings usando expressões regulares. Quando a pesquisa encontra a string, ela substitui a string regexpreplace. O comando REGEXPREPLACE faz uma substituição global, não substitui apenas a primeira ocorrência.

Formato

```
REGEXPREPLACE(dest_string, search, replace)
```

Tipos de dados

Argumento	Tipo	Descrição
dest_string	svar (ENTRADA/ SAÍDA)	Variável de string cujos bytes serão substituídos.
search	string (ENTRADA) ou svar (ENTRADA/ SAÍDA)	String de pesquisa a ser substituída.
replace	string (ENTRADA) Ou svar (ENTRADA/ SAÍDA)	String de substituição; pode ser de tamanho zero para indicar uma string nula.

Por exemplo:

```
COPY(string:"A 1a vez")
REGEXREPLACE(string, "1a", "2a")
```

O resultado será:

```
string = "A 2a vez"
```

NOTA: Nesse exemplo, você pode substituir uma expressão regular pela

```
"1a" string.
```

Para substituir a string nula:

```
COPY(string:"A 1a vez")
REGEXPREPLACE(string, "1a", "")
```

O resultado será:

```
string="A vez"
```

Para obter mais informações sobre expressões regulares e o conjunto de caracteres portáteis, consulte Expressões regulares.

O Sentinel usa uma biblioteca compatível com POSIX (Portable Operating System Interface for UNIX – Interface de Sistemas Operacionais Portáteis para UNIX) para expressões regulares. POSIX é um conjunto de padrões IEEE e ISO que ajuda a garantir a compatibilidade entre sistemas operacionais compatíveis com POSIX, que incluem a maior parte das variantes do UNIX.

REGEXPSEARCH, REGEXPSEARCH_EXPLICIT ou REGEXPSEARCH_STRING

O comando REGEXPSEARCH faz uma pesquisa a partir do buffer de recebimento (buffer Rx) ou designa uma variável de string de entrada para uma string, usando expressões regulares. Ele também suporta grupos de expressões.

NOTA: No Editor Visual do Construtor de Coletores, REGEXPSEARCH, REGEXPSEARCH_EXPLICIT e REGEXPSEARCH_STRING são listados como comandos separados. Eles são o mesmo comando. São fornecidos como descrições de variações do mesmo comando. Para usar qualquer variação do comando REGEXPSEARCH_EXPLICIT ou REGEXPSEARCH_STRING no editor de texto, digite REGEXPSEARCH.

Buffer de recebimento

A pesquisa no buffer de recebimento ocorre da seguinte maneira:

- A pesquisa começa do indicador de buffer Rx atual em diante até localizar a string ou chegar ao fim do buffer de recebimento;
- Se a string é encontrada na pesquisa, o indicador de buffer Rx é atualizado para apontar para o primeiro byte da string pesquisada; Esse indicador de buffer Rx é mantido na transição entre estados, a menos que seja explicitamente alterado com o comando RESET;
- Se a string não é encontrada na pesquisa, o indicador de buffer Rx não é movido.

Quando esse comando é usado para pesquisar o buffer de recebimento, o segundo parâmetro opcional consiste em uma variável inteira definida como 1 se a pesquisa localiza a string e como zero se a pesquisa não a localiza.

Variável de string

Variáveis de string não suportam o indicador de análise, portando a dinâmica durante a pesquisa em uma variável de string é diferente. O padrão de expressões regulares corresponderá a uma das strings de entrada ou a todas elas. Se esse padrão for configurado com grupos de expressões, o conteúdo da string de entrada que corresponde aos grupos de expressões poderá ser armazenado em variáveis de saída. Existem duas opções de saída de grupos de expressões. Uma é preencher a lista de variáveis na ordem dos grupos de expressões e a outra é designar uma matriz de string.

Se a expressão regular corresponder corretamente à variável de string de entrada, uma lista de variáveis designadas ou uma matriz de saída será definida com os valores do grupo e a variável localizada será definida como um a mais que o número de grupos ou como zero, caso não haja correspondência.

Quando a saída dos valores de grupo for uma matriz de string, o primeiro elemento indexado com "0" conterá a string correspondente. A string correspondente conterá o conteúdo correspondente a toda a expressão regular, independentemente de grupos de expressões. Portanto, o conteúdo do primeiro grupo de expressões será armazenado na posição da matriz indexada com "1". Ao executar loop na matriz de saída, lembre-se de que o valor i_Found_Tokens compensa o fato de o primeiro elemento ser a string correspondente sendo sempre um a mais que o número total de grupos. Em um loop do comando FOR, a condição de interrupção de ser menor que o valor i_Found_Tokens ainda funcionará, mas você provavelmente iniciará seu índice em "1" em vez de "0".

Ao designar valores do grupo a serem armazenados em uma lista de variáveis de saída em vez de uma matriz, o comando é capaz de efetuar a conversão de tipos. Mesmo que a string de entrada seja do tipo string, os componentes dentro da string poderão ser numéricos. Se a intenção é tratar esse números como valores em ponto flutuante (float), basta designar as variáveis de saída com o tipo correto para causar a conversão a ser realizada.

Correspondência simples de REGEX

Expressão	Descrição
.	Qualquer caractere
\d	Qualquer dígito
\w	Qualquer caractere alfanumérico
\s	Qualquer espaço em branco
+	1 ou mais do anterior
*	0 ou mais do anterior

Formato

Como um buffer de recebimento:

```
REGEXPSEARCH(search[, ifound])
```

Como uma variável de string:

```
REGEXPSEARCH(Input_String, s_Regular_Exp_Pattern,
   i_Found_Tokens[, s_Output_Results[]])
REGEXPSEARCH(s_Input_String, s_Regular_Exp_Pattern,
   i_Found_Tokens, s_Match[, var1, var2, ...)]
```

Tipos de dados

Argumento	Tipo	Descrição
s_Input_String	String ou variável de string. (ENTRADA) [OPCIONAL]	String ou variável de string na qual pesquisar correspondências de regex especificadas no comando regex.
s_Regular_Exp_Pattern	String (ENTRADA)	String a ser pesquisada no buffer de recebimento (começando do indicador de buffer Rx atual em diante) ou em uma string de entrada literal ou variável de string de entrada.

Argumento	Tipo	Descrição
i_Found_Tokens	numvar (SAÍDA) [OPCIONAL]	Retorna se a string foi ou não localizada. 0: O padrão de expressão regular não é correspondente; 1: O padrão de expressão regular é correspondente, mas nenhum grupo de expressões é designado; 2: O padrão de expressão regular corresponde a 1 grupo de expressões designado; N+1: O padrão de expressão regular corresponde a N grupos de expressões designados. **NOTA:** A variável I_found_tokens pode ser usada como um teste de correspondência, pois o valor será diferente de zero quando a expressão regular for correspondente.
s_Match	String (SAÍDA) [CONDICIONAL]	Preenchida somente no padrão de correspondência. Deve ser designada quando forem usadas variáveis de saída de grupos de expressões da lista. Quando valores do grupo forem armazenados em uma matriz de saída, s_Match NÃO será um parâmetro válido.
Lista de variáveis Ou s_Output_Results[]	Todos são possíveis (SAÍDA) [OPCIONAL] Ou Matriz de string (SAÍDA) [OPCIONAL]	Lista de variáveis na qual os valores do grupo serão colocados. A atribuição de valores é feita na ordem de valores do grupo designados quando a precedência seguinte deve ser obedecida.

Os exemplos a seguir pesquisam um retorno de carro e uma alimentação de linha no buffer de recebimento:

```
REGEXPSEARCH("\0d0a\")
```

O exemplo a seguir pesquisa um alarme de texto no buffer de recebimento:

```
REGEXPSEARCH("alarm")
```

NOTA: Na substituição hexadecimal, \0000\ encerra uma string, portanto "xxxx\0000\yyyy" se torna "xxxx".

Veja um exemplo detalhado de pesquisa de um padrão dentro de um valor de string literal:

```
REGEXPSEARCH("2003 Jan 15 13:34:20",
   "(/\d+)/\s+(/\w+)/\s+(/\d+)/\s+(/\d+):(/\d+):(/\d+)",
```

```
i_Success, s_Match, s_Year, s_Month, s_Day, s_Hour,
s_Minute, s_Second)
```

Onde:

```
i_Success = 7
s_Match = 2003 jan 15 13:34:20
s_Year = 2003
s_Month = jan
s_Day = 15
s_Hour = 13
s_Minute = 34
s_Second = 20
```

Para obter mais informações sobre expressões regulares e o conjunto de caracteres portáteis, consulte a seção Expressões regulares no capítulo 2.

O Sentinel usa uma biblioteca compatível com POSIX (Portable Operating System Interface for UNIX – Interface de Sistemas Operacionais Portáteis para UNIX) para expressões regulares. POSIX é um conjunto de padrões IEEE e ISO que ajuda a garantir a compatibilidade entre sistemas operacionais compatíveis com POSIX, que incluem a maior parte das variantes do UNIX.

REPLACE

O comando REPLACE pesquisa e substitui strings.

Quando a pesquisa encontra a string, ela substitui a string replace. O comando REPLACE faz uma substituição global, não substitui apenas a primeira ocorrência.

Formato

```
REPLACE(dest_string, pesquisa, substituir)
```

Tipos de dados

Argumento	Tipo	Descrição
dest_string	svar (ENTRADA/ SAÍDA)	Variável de string cujos bytes serão substituídos.
search	string (ENTRADA)	String de pesquisa a ser substituída.
replace	string (ENTRADA)	String de substituição.

Por exemplo:

```
COPY(string:"A 1a vez")
REPLACE(string, "1a", "2a")
```

O resultado será:

```
string = "A 2a vez"
```

NOTA: Nesse exemplo, você pode substituir uma expressão regular pela "1a" string.

RESET

O comando RESET redefine o indicador de buffer Rx como zero.

Formato

```
RESET()
```

Por exemplo, o indicador de buffer Rx é mostrado pelo símbolo ^.

```
rxbuff = "abcdefg"
                ^
RESET()
```

O resultado será:

```
"abcdefg"
 ^
```

RXBUFF

O comando RXBUFF sobregrava o buffer de recebimento com o conteúdo de uma variável de string ou de uma string entre aspas. O conteúdo do buffer de recebimento é alterado imediatamente e o indicador de buffer Rx e o valor mantido são redefinidos como zero.

Formato

```
RXBUFF(s_data)
```

Tipos de dados

Argumento	Tipo	Descrição
s_data	string (ENTRADA)	String de dados a ser gravada no buffer de recebimento. Essa string será imediatamente a nova string do buffer de recebimento.

Por exemplo:

No exemplo a seguir, o comando FILER lê um arquivo chamado alert.data e coloca o conteúdo desse arquivo em uma variável de string chamada s_data. Esse exemplo pressupõe que:

```
alert.data: "Alarme de Xterminal leve A")
```

Em seguida, o comando RXBUFF coloca esses dados no buffer de recebimento, como se os dados tivessem sido recebidos de uma porta.

```
FILER("alert.data", s_data)
```

```
RXBUFF(s_data)
//copa dados do Rx BUFFER para o S_Alarm_Priority,
   parando antes da string "Alarm")
COPY(S_Alarm_Priority:," Alarm")
```

O resultado será:

```
S_Alarm_Priority= "Leve"
```

SEARCH

O comando SEARCH pesquisa uma string no buffer de recebimento (Buffer Rx).

A pesquisa ocorre da seguinte maneira:

- A pesquisa começa do indicador de buffer Rx atual em diante até localizar a string ou chegar ao fim do buffer de recebimento;
- Se a string é encontrada na pesquisa, o indicador de buffer Rx é atualizado para apontar para o primeiro byte da string pesquisada; Esse indicador de buffer Rx é mantido na transição entre estados, a menos que seja explicitamente alterado com o comando RESET;
- Se a string não é encontrada na pesquisa, o indicador de buffer Rx não é movido.

Quando esse comando é usado, o segundo parâmetro opcional consiste em uma variável inteira definida como 1 se a pesquisa localiza a string e como zero se a pesquisa não a localiza.

Formato

```
SEARCH(pesquisa[, ifound])
```

Tipos de dados

Argumento	Tipo	Descrição
search	string (ENTRADA)	String a ser pesquisada no buffer de recebimento, começando do indicador de buffer Rx atual em diante.
ifound	numvar (SAÍDA) [OPCIONAL]	Retorna se a string foi ou não localizada. 0=não localizada 1=localizada

Por exemplo:

Os exemplos a seguir pesquisam um retorno de carro e uma alimentação de linha:

```
SEARCH("\0d0a\")
SEARCH(data, ifound)
```

O exemplo a seguir pesquisa um alarme de texto:

```
SEARCH("alarm")
```

NOTA: Na substituição hexadecimal, \0000\ encerra uma string, portanto "xxxx\0000\yyyy" se torna "xxxx".

SET

O comando SET processa uma expressão matemática e atualiza um valor numérico (numvar) com o resultado da avaliação.

Quando esse comando é usado:

- Especifique uma variável numvar de destino, seguida por um sinal de igual, seguido por uma combinação de ( ) - + * /, números e variáveis numéricas;
- Você deve especificar pelo menos um valor numérico à direita do sinal de igual;
- Não há restrição no número de parênteses incorporados;
- Todos os argumentos são convertidos em uma variável flutuante; o resultado é convertido no tipo (inteira ou flutuante) da variável numérica (numvar) de destino;
- É possível inserir até 98 entradas após o sinal de igual; essas entradas incluem: (,), *, /, +, -, quaisquer valores e variáveis numéricos;
- Quando as operações têm a mesma ordem de nível operacional, são manipuladas da esquerda para a direita; a ordem de operação é descrita na tabela seguinte.

Nível 1	:	()	Por exemplo: parênteses.
Nível 2	:	*/	Por exemplo: multiplicação, divisão.
Nível 3	:	+ -	Por exemplo: soma, subtração.

Formato

```
SET(idest = <expr>) ou SET(fdest = <expr>)
```

Onde:

```
set_command ::= SET(<idest>=<expr>) | SET(<fdest>=<expr>)
expr ::= (<expr>)
         | expr ( '+' | '-' | '*' | '/' ) expr
         | ivar | fvar | number
```

Tipo de dados

Argumento	Tipo	Descrição
idest	numvar (SAÍDA)	Variável numérica (fvar ou ivar) em que o valor será salvo.
inum1	valor numérico (ENTRADA)	Uma fvar, ivar ou um número.
inum2	valor numérico (ENTRADA) [OPCIONAL]	Uma fvar, ivar ou um número.
inum3	valor numérico (ENTRADA) [OPCIONAL]	Uma fvar, ivar ou um número.
…	valor numérico (ENTRADA) [OPCIONAL]	Uma fvar, ivar ou um número.

Por exemplo:

```
SET(idest=inum1)
SET(i_loop=10)
SET(idest=inum1+inum2)
SET(idest=(inum1+inum2) * inum3)
SET(i_counter=i_counter+1)
SET(i_val = (ivar)*(ivar/3) + 15/fvar - (5 + 20/iloop))
```

SETBYTES

O comando SETBYTES permite que você defina bytes em uma variável de string com um valor específico, seja um número inteiro ou uma string. No caso de um inteiro, os valores válidos vão de 0 a 255. Se uma string for usada como parâmetro de substituição, ela será colocada começando na posição de índice da variável de string de destino.

Formato

```
SETBYTES(dest_string, index, replace)
```

Tipos de dados

Argumento	Tipo	Descrição
dest_string	svar (ENTRADA/ SAÍDA)	Variável de string cujos bytes serão substituídos.
index	valor numérico (ENTRADA)	Índice (bytes contados começando com 0 para o primeiro byte) no parâmetro dest_string em que os bytes serão usados para a substituição.
replace	string (ENTRADA) Ou inteiro (ENTRADA)	Bytes da string que serão gravados no parâmetro dest_string. Valor a ser definido para o byte #n do índice na string de destino.

Por exemplo:

```
COPY(string:"Util. de Largura de Banda = 22%")
SETBYTES(string, 18, "44")
```

Conteúdo das variáveis de saída atuais:

```
string = "Util. de Largura de Banda = 44%"
```

SETCONFIG

O comando define uma propriedade de sistema. A definição atual da propriedade de sistema pode ser recuperada usando o comando SETCONFIG. Esses comandos são usados para definir propriedades de sistema e recuperar valores atuais de propriedades de sistema que

podem mudar periodicamente, como um arquivo de registro que é renomeado diariamente com a data atual.

As propriedades de sistema disponíveis são:

Propriedade de sistema	Exemplo(s):
▪ System.OS.Family	Solaris e Windows
▪ System.OS.Name	Windows 2000
▪ System.OS.Version.Major	5
▪ System.OS.Version.Minor	0
▪ System.Net.Hostname	ESECServer
▪ System.Net.IP_List	Lista de IPs para este host separados por ponto e vírgula, por exemplo "172.163.3.45;172.45.2.1"

Consulte também o comando SETCONFIG.

Há dois parâmetros com esse comando.

- O primeiro define a opção de configuração ("FileConnector.InputFile" ou "FileConnector.OutputFile").
- O segundo parâmetro necessário define o valor de configuração.

Formato

```
SETCONFIG(Config Option, Value)
```

Tipos de dados

Argumento	Tipo	Descrição
Config Option	string (ENTRADA)	Nome da variável de configuração a ser definida. Arquivo de entrada = "FileConnector.InputFile" Arquivo de saída = "FileConnector.OutputFile"
Valor	string svar (ENTRADA)	Configuração.

Por exemplo:

```
SETCONFIG("FileConnector.InputFile", s_inputfilename)
SETCONFIG("FileConnector.OutputFile", s_outputfilename)
```

Conteúdo das variáveis de saída atuais:

```
"C:/\test.dat"
```

SHELL

O comando SHELL executa um script ou comando shell.

Formato

```
SHELL(comando [, wait_parameter][, wait_return_status])
```

Tipos de dados

Argumento	Tipo	Descrição
command	string (ENTRADA)	O caminho e o nome do arquivo do comando a ser executado. Por padrão, a variável de ambiente PATH é usada.
wait/no_wait	numvar [OPCIONAL]	Permite que o comando SHELL aguarde (ou não aguarde) o programa iniciado terminar de ser executado antes de continuar o processamento. 0 = no_wait (não aguardar) 1 = wait (aguarda o programa ser concluído)
return_status	numvar [OPCIONAL]	Valor numérico para quando a opção wait/no_wait é usada. Êxito = 1 Falha = 0

O exemplo a seguir inicia um arquivo de lote PC ou um script shell UNIX:

```
SHELL("device_poll")
```

O exemplo a seguir inicia o Notepad:

```
SHELL("c:/\winnt/\system32/\notepad.exe")
```

O exemplo a seguir aguarda o comando clock terminar de ser executado:

```
SHELL("clock",1)
```

O exemplo a seguir aguarda um arquivo de lote PC ou um script shell UNIX terminar de ser executado e, em seguida, recebe seu status de retorno:

```
SHELL("device_poll",1,i_ret)
```

O exemplo a seguir executa o processo do comando clock e não aguarda sua conclusão:

```
SHELL("clock",0)
```

SKIP

O comando SKIP adiciona um número ao valor do indicador de buffer Rx como zero.

O número pode ser positivo ou negativo. Se o indicador de buffer Rx resultante for menor que zero, será definido como zero. Se o indicador de buffer Rx ultrapassar o final do buffer de recebimento, será definido para apontar para o último byte do buffer de recebimento.

Formato

```
SKIP([+ | -] iskip_amount)
```

Tipos de dados

Argumento	Tipo	Descrição
iskip_amount	valor numérico (ENTRADA)	Número de bytes pelos quais mover o Rx.

Por exemplo:

```
SKIP(iskip_amount)
SKIP(+iskip_amount)
SKIP(-iskip_amount)
SKIP(5)
SKIP(-1)
```

Veja a seguir exemplos do indicador de buffer Rx após um comando SKIP, para os dados:

```
aaaaaa bbbbb c d ee
      ^

SKIP(-2)
aaaaaa bbbbb c d ee
    ^

SKIP(-1)
aaaaaa bbbbb c d ee
     ^

SKIP(0)
aaaaaa bbbbb c d ee
      ^

SKIP(1)
aaaaaa bbbbb c d ee
       ^
SKIP(2)
aaaaaa bbbbb c d ee
        ^

SKIP(3)
aaaaaa bbbbb c d ee
         ^

SKIP(4)
aaaaaa bbbbb c d ee
          ^

SKIP(8)
aaaaaa bbbbb c d ee
              ^
```

SKIPWORD

O comando SKIPWORD modifica o indicador de buffer Rx para que ele aponte para o começo de uma palavra.

Esse comando considera como uma palavra cada seqüência de bytes imprimíveis contínuos separados por pelo menos um byte não imprimível. Bytes imprimíveis são definidos como ASCII e ASCII-0-255 estendido (de acordo com a certificação ISO 8859-1).

Usando valores SKIP positivos e negativos, o indicador de buffer Rx ignora os bytes à frente e atrás no buffer de recebimento até alcançar o primeiro ou o próximo byte imprimível nesse buffer.

O indicador de buffer Rx não será movido para além do final do buffer de recebimento ou para antes do seu início, mesmo que o comando SKIPWORD assim indique.

Um valor de zero não faz com o que o indicador de buffer Rx seja alterado. O comando SKIPWORD trata todos os caracteres abaixo de 33 e entre 126 e 161 como espaços em branco.

Formato

```
SKIPWORD([+ | -] iwords)
```

Tipos de dados

Argumento	Tipo	Descrição
iwords	valor numérico (ENTRADA)	Número de palavras pelas quais mover o indicador de buffer Rx no buffer de recebimento.

Por exemplo:

```
SKIPWORD(iwords)
SKIPWORD(3)
SKIPWORD(+iwords)
SKIPWORD(-iwords)
SKIPWORD(-4)
```

Veja a seguir exemplos do indicador de buffer Rx após um comando SKIPWORD, para os dados:

```
aaaaaa bbbbb c d ee
      ^

SKIPWORD(-2)
aaaaaa bbbbb c d ee
^

SKIPWORD(-1)
aaaaaa bbbbb c d ee
^
```

```
SKIPWORD(0)
aaaaaa bbbbb c d ee
      ^

SKIPWORD(1)
aaaaaa bbbbb c d ee
       ^

SKIPWORD(2)
aaaaaa bbbbb c d ee
            ^

SKIPWORD(3)
aaaaaa bbbbb c d ee
              ^

SKIPWORD(4)
aaaaaa bbbbb c d ee
                ^

SKIPWORD(5)
aaaaaa bbbbb c d ee
                 ^
```

SOCKETW

O comando SOCKETW efetua uma gravação de dados INDIVIDUAIS (soquete de FLUXO de bytes da rede) aberta, conectada em um soquete (porta IP e TCP) e fecha o soquete. Opcionalmente, ele retorna o status da tentativa de gravação do soquete.

Formato

```
SOCKETW(address, i_port, data [, istat])
```

Tipos de dados

Argumento	Tipo	Descrição
address	string (ENTRADA)	Endereço IP do soquete.
i_port	valor numérico (ENTRADA)	Número da porta TCP do soquete.
data	string (ENTRADA)	String de dados a serem gravados no soquete.

Argumento	Tipo	Descrição
istat	numvar (SAÍDA)	Status retornado opcional. istat = Número de bytes gravados; > 0 (Êxito) istat = 0 (Falha)

Veja exemplos:

```
SOCKETW("192.168.15.25", 5051, "Soquete de Gravação de
   Dados")
SOCKETW("192.168.15.25", i_port, "Dados para
   Soquete\0d\")
SOCKETW(s_ip_address, i_port, "\54AF0D0B91\", i_status)
SOCKETW(s_ip_address, i_port, "\54AF0D0B91\", f_status)
SOCKETW(s_ip_address, 6004, "\54AF0D0B91\", f_status)
SOCKETW(s_ip_address, 6004,sdata, f_status)
```

STONUM

O comando STONUM (string para número) converte uma variável de string (svar) em uma variável numérica (numvar).

AVISO: Variáveis de string compostas por algo diferente da representação de string de um valor inteiro ou flutuante podem produzir resultados imprevisíveis. Todos os valores inteiros são limitados a 2147483647; valores maiores que isso são truncados como 2147483647.

Formato

```
STONUM(string, ivar)
```

Tipos de dados

Argumento	Tipo	Descrição
inum	numvar (SAÍDA)	Variável numérica em que o número será armazenado (ivar ou fvar).
string	string (ENTRADA)	Representação de string de um número (por exemplo: "306").

Por exemplo:

```
STONUM(origem, idest)
STONUM(string_number, ivar)
STONUM("6512", ivar)
```

STRIP ou STRIP-ASCII-RANGE


O comando STRIP remove todas as ocorrências da string de eliminação ou faixa de ASCII da svar. Ele sempre faz eliminações de múltiplas passagens, até que a string STRIP ou ASCII RANGE não seja mais encontrada na variável de string de destino.

Ao usar esse comando, especifique a variável de string da qual os caracteres podem ser eliminados. Os parâmetros restantes podem ser um valor tanto de início como de final de uma faixa de string ou numérica.

> **NOTA:** No Editor Visual do Construtor de Coletores, STRIP e STRIP-ASCII-RANGE são listados como comandos separados. Eles são o mesmo comando. São fornecidos como descrições de variações do mesmo comando. Para usar qualquer variação do comando STRIP-ASCII-RANGE no editor de texto, digite STRIP.

Formato

```
STRIP(dest, strip)
STRIP(dest, iniciar faixa de ASCII, parar faixa de ASCII)
```

Tipos de dados

Argumento	Tipo	Descrição
dest	svar (ENTRADA/ SAÍDA)	Variável de string que contém os dados da string a serem eliminados de bytes, dependendo do segundo argumento.
strip ou start ASCII range	string ou valor numérico (ENTRADA)	String ou valor ASCII inicial a ser eliminado da string dest.
stop ASCII range	valor numérico (ENTRADA [opcional])	Valor ASCII final **NOTA**: Se start ASCII range for especificado, esse parâmetro será obrigatório.

Os exemplos a seguir são eliminações de múltiplas passagens.

```
COPY(teste:"THHELLOE")
STRIP(teste, "HELLO")
```

Após o comando STRIP(), o teste de variável tem o valor de THE.

```
COPY(test2:"ABCDDEDDDFGDDH")
STRIP(test2, "D")
```

Após o comando STRIP(), o teste 2 de variável tem o valor de ABCEFGH.

```
COPY(test3:"ABCDDEDDDFGDDH")
STRIP(test3, 68, 69)
```

Após o comando STRIP(), o teste 3 de variável tem o valor de ABCFGH.

TBOSSETCOMMAND

O comando TBOSSETCOMMAND cria um pacote de comandos TBOS de 3 bytes que pode ser transmitido a um dispositivo usando o protocolo TBOS.

O número de exibição, o número do comando e o tipo de comando TBOS são usados para colocar o pacote de comandos TBOS (3 bytes) correto na variável de string de saída.
O formato do pacote TBOS criado usando esse comando de análise é descrito nas seguintes tabelas de Pedidos de Comando Remoto.

Caractere 1		
Número(s) de bits	**Valor**	**Significado**
8 7	0 1	Código da Operação: 01 = Pedido de Comando Remoto (caractere 1)
6 5 4	MSB LSB	Número de Exibição: 000 = Nº 1 001 = Nº 2 ... 111 = Nº 7
3	0	Nenhum Significado
2 1	MSB LSB	Tipo: 00 = temporário 01 = finalizado 10 = não finalizado

Caractere 2		
Número(s) de bits	**Valor**	**Significado**
8 7	1 0	Código da Operação: 10 = Pedido de Comando Remoto (caractere 2)
6 5 4 3 2 1	MSB LSB	Número de Comando Remoto: 000000 = Nº 1 000001 = Nº 2 ... 111111 = Nº 63

Caractere 3		
Número(s) de bits	**Valor**	**Significado**
8 7 6 5 4 3 2 1	1 1 0 0 1 1 0 0	Repetição de Caractere: A resposta do comando remoto é a repetição desse byte de volta para a porta.

Formato

```
TBOSSETCOMMAND(cmd_bytes, idisp_num, icmd_num, type)
```

Tipos de dados

Argumento	Tipo	Descrição
cmd_bytes	svar (SAÍDA)	Bytes de dados hexadecimais (total de 3 bytes) que serão colocados nessa variável de string e que podem ser usados na transmissão para um dispositivo TBOS na caixa Próxima Transmissão de Estado.
idisp_num	valor numérico (ENTRADA)	Número (ou endereço) de exibição TBOS do dispositivo (1 - 8). **NOTA:** As faixas válidas para o parâmetro idisp_num vão apenas de 1 a 8; usando qualquer outro valor, a saída (cmd_bytes) é definida como tudo zero, "\00 00 00\".
i_cmd_num	valor numérico (ENTRADA)	Número de comando TBOS (1-64). **NOTA:** As faixas válidas para o parâmetro i_cmd vão apenas de 1 a 64; usando qualquer outro valor, a saída (cmd_bytes) é definida como tudo zero, "\00 00 00\".

Argumento	Tipo	Descrição
type	valor numérico (ENTRADA) Ou string (ENTRADA)	Tipo de comando TBOS (0-2): 0 = temporário 1 = finalizado 2 = não finalizado **NOTA:** As faixas válidas para o parâmetro vão apenas de 0 a 2; usando qualquer outro valor, o tipo é definido como 0 = "temporário" por padrão. Tipo de comando TBOS no formato de string. "temporário" ou "t" = temporário "finalizado" ou "f" = finalizado "não finalizado" ou "n" = não finalizado Essa string distingue maiúsculas de minúsculas.

Por exemplo:

```
TBOSSETCOMMAND(string_cmd_bytes, 1, 1, 0)
TBOSSETCOMMAND(s_bytes, 1, 1, "finalizado")
TBOSSETCOMMAND(s_bytes, i_display, i_cmd_num, "N")
TBOSSETCOMMAND(s_bytes, i_display, i_cmd_num, 2)
TBOSSETCOMMAND(s_bytes, 1, 1, "temporário")
TBOSSETCOMMAND(s_bytes, 1, 1, "finalizado")
```

Lembre-se de verificar se o parâmetro cmd_bytes de saída foi definido como "\00 00 00\" para descobrir se há erros em entradas fora da faixa. Por exemplo:

```
TBOSSETCOMMAND(cmd_bytes, i_display, i_cmd_num, "T")
IF(cmd_bytes = "\00 00 00\") /* ENTRADAS FORA DA FAIXA */
...
ENDIF()
```

O exemplo a seguir cria um comando TBOS para o número de exibição 5, o número de comando 33 e o tipo não finalizado.

```
TBOSSETCOMMAND(sbytes, 5, 33, 2)
```

Conteúdo das variáveis de saída atuais:

```
sbytes = "\ba0 cc\"
```

TBOSSETREQUEST

O comando TBOSSETREQUESTcria um pacote de pedidos TBOS de 1 byte que pode ser transmitido a um dispositivo usando o protocolo TBOS. O número de exibição e o número do pedido TBOS são usados para colocar o byte do pedido de exploração TBOS correto na

variável de string de saída. O formato do pacote TBOS criado usando esse comando de análise é descrito nas seguintes tabelas de Pedidos e Respostas de exploração de caracteres.

Caractere 1 – Pedido de exploração de caracteres		
Número(s) de bits	**Valor**	**Significado**
8 7	0 0	Código da Operação: 00 = Pedido de Exploração de Caracteres
6 5 4	MSB LSB	Número de Exibição: 000 = Nº 1 001 = Nº 2 ... 111 = Nº 3
3 2 1	MSB LSB	Tipo: 000 = Nº 1 001 = Nº 2 ... 111 = Nº 8

Caractere 1 – Resposta de exploração de caracteres		
Número(s) de bits	**Valor**	**Significado**
8 7 6 5 4 3 2 1	MSB LSB	Cada bit nesse byte de resposta tem um significado especial baseado no número de caracteres enviados (1-8) e no protocolo do dispositivo do número de exibição enviado (1-8).

Formato

```
TBOSSETREQUEST(cmd_bytes, idisp_num, irequest_num)
```

Tipos de dados

Argumento	Tipo	Descrição
cmd_bytes	svar (SAÍDA)	Byte de dados hexadecimais colocado nessa variável de string, que pode ser usado na transmissão para um dispositivo TBOS na caixa Próxima Transmissão de Estado.
idisp_num	valor numérico (ENTRADA)	Número (ou endereço) de exibição TBOS do dispositivo (1 - 8). **NOTA:** As faixas válidas para o parâmetro idisp_num vão apenas de 1 a 8; usando qualquer outro valor, a saída (cmd_bytes) é definida como tudo zero, "\00\".

Argumento	Tipo	Descrição
irequest_num	valor numérico (ENTRADA)	Número de caracteres de exploração TBOS (1 - 8). **NOTA:** As faixas válidas para o parâmetro irequest_num vão apenas de 1 a 8; usando qualquer outro valor, a saída (cmd_bytes) é definida como tudo zero, "\00\".

Por exemplo:

```
TBOSSETREQUEST(string_request_byte, 1, 1)
TBOSSETREQUEST(s_byte, idisp_num, i_scan_number)
```

O exemplo a seguir cria um caractere de pedido de exploração TBOS para o número de exibição 2 e para o número de pedido 1.

```
TBOSSETREQUEST(sbytes, 2, 1)
```

Conteúdo das variáveis de saída atuais:

```
sbytes = "\08\"
```

TIME

O comando TIME copia o horário atual (no formato HH-MM-SS) em uma variável de string ivar ou fvar.

Formato

```
TIME(dest)
```

Tipos de dados

Argumento	Tipo	Descrição
dest	svar (SAÍDA)	A representação de string do horário é colocada nesta variável de string (por exemplo: "23-11-55").
	numvar (SAÍDA)	O número de segundos desde as 00:00:00 UTC (Universal Coordinated Time) de 1º de janeiro de 1970 é colocado nessa variável numérica (que pode ser uma fvar).

Por exemplo:

```
TIME(time_of_day)
TIME(i_num_seconds)
TIME(f_num_seconds)
```

NOTA: Se você usar uma variável fvar, o horário retornado será exato de acordo com os microssegundos.

TOKENIZE

O comando TOKENIZE copia cada componente de uma string entre os delimitadores de uma matriz de string. Isso pode ser útil quando você está lendo dados delimitados de um arquivo e passando dados para um script para serem executados sob demanda.

Cada caractere na string é tratado como um separador de token potencial. Por exemplo, usando o separador de token "THE END" não usaria a string inteira como separador. Em vez disso, usaria caracteres individuais como separadores potenciais:

```
"T"
"H"
"E"
"E"
"N"
"D"
```

Formato

```
TOKENIZE(dados, delimitador, tokens[], itokens)
```

Tipos de dados

Argumento	Tipo	Descrição
data	svar (ENTRADA)	Dados aos quais aplicar token (por exemplo: "xterm|subres|33|50").
delimiter	string (ENTRADA)	Delimitador(es) usados para separar os tokens.
token	matriz (SAÍDA)	Matriz de tokens conforme encontrada nos dados de entrada de string delimitadores.
itokens	numvar (SAÍDA)	Número de tokens colocados na matriz de string de token.

Por exemplo:

```
COPY(data:"Esses|Dados|Têm|Token")
TOKENIZE(dados, "|",tokens[], inumtokens)
```

Conteúdo das variáveis de saída atuais:

```
inumtokens = 4
tokens[0]= "Esses"
tokens[1]= "Dados"
tokens[2]= "Têm"
tokens[3]= "Token"
```

No exemplo a seguir, os dados passados para o script são:

```
"Há#vários|campos*disponíveis|na*respectiva#string".
```

Existem três separadores de token diferentes que desejamos utilizar: #, | e *.

Conteúdo das variáveis de saída atuais:

```
i_tokens = 7
messages[0] = "Há"
messages[1] = "vários"
messages[2] = "campos"
messages[3] = "disponíveis"
messages[4] = "na"
messages[5] = "respectiva"
messages[6] = "string"
```

No exemplo a seguir, os dados no buffer de recebimento são:

```
"Alarme de Firewall - Médio;Alarme de Negação de Serviço
   - Médio;"
COPY(rxbuff:)
TOKENIZE(rxbuff,";",msgs[],i_msgs)
```

Conteúdo das variáveis de saída atuais:

```
i_msgs = 2
msgs[0] = "Alarme de Firewall - Médio"
msgs[1] = "Alarme de Negação de Serviço - Médio"
```

TOLOWER

O comando TOLOWER converte todos os caracteres do conteúdo de uma variável de string em letras minúsculas. O conteúdo da variável de string que passa por esse comando se transforma todo em letras minúsculas.

Formato

```
TOLOWER(stringvar)
```

Tipos de dados

Argumento	Tipo	Descrição
stringvar	string (ENTRADA/ SAÍDA)	Variável de string que contém a string a ser convertida em letras minúsculas.

Por exemplo:

```
s_var = "Isso é Letra Minúscula"
TOLOWER(s_var)
```

O resultado será:

```
s_var = "isso é letra minúscula"
```

TOUPPER

O comando TOUPPER converte todos os caracteres do conteúdo de uma variável de string em letras maiúsculas. O conteúdo da variável de string que passa por esse comando se transforma todo em letras maiúsculas.

Formato

```
TOUPPER(stringvar)
```

Tipos de dados

Argumento	Tipo	Descrição
stringvar	string (ENTRADA/ SAÍDA)	Variável de string que contém a string a ser convertida em letras maiúsculas.

Por exemplo:

```
s_var = "Isso é Letra Maiúscula"
toupper(s_var)
```

O resultado será:

```
s_var = "ISSO É LETRA MAIÚSCULA"
```

TRANSLATE

O comando TRANSLATE carrega um arquivo csv (comma-separated value - valores separados por vírgula) na memória, permitindo uma pesquisa rápida da entrada, seja a principal ou não, contida no arquivo, além da recuperação de outros dados associados à entrada principal.

Veja a seguir informações referentes ao comando TRANSLATE.

- CSV);
- Pesquisas de entrada chave que distingue maiúsculas de minúsculas;
- Status localizado;
- Variáveis de dados.

Arquivo CSV (Comma-Separated Value – Valores Separados por Vírgulas)

O arquivo csv é um caminho relativo de um diretório de scripts do Coletor. O Criador de Coletores não suporta a edição desses arquivos, portanto a Novell sugere que sejam gerados no Microsoft Excel. O nome do arquivo pode ser uma string ou uma variável.

O formato do arquivo csv é mostrado no exemplo seguinte de um arquivo chamado friends.csv:

```
key1,data1,data2,data3
Bob,azul,25,95
```

```
Alice,verde,19,49
Pat,roxo,36,65
```

Para encontrar um determinado amigo no seu arquivo friends.csv, o comando TRANSLATE deveria ser assim:

```
TRANSLATE("Bob","friends.csv",i_found)
```

Ou

```
COPY(s_Name:"Bob")
TRANSLATE(s_Name,"friends.csv",i_found)
```

Pesquisas de entrada chave que distingue maiúsculas de minúsculas;

Os parâmetros principais podem ser tanto uma string como uma variável de string. Além disso, um número inteiro ou uma variável inteira é suportada. Como o arquivo csv é carregado na memória, a principal de cada entrada é definida em letras minúsculas. A entrada principal no comando TRANSLATE também é definida internamente em letras minúsculas para permitir pesquisas principais que não diferenciem maiúsculas de minúsculas.

Continuando com o exemplo de um arquivo csv:

```
TRANSLATE("Bob", "friends.csv",i_found)
```

Isso também localizaria Bob no arquivo csv.

Status localizado;

Esse status será definido como 1 se a entrada principal encontrar-se no arquivo csv e como zero se ela não se encontrar no arquivo csv. Um arquivo csv apenas com entradas principais pode ser usado com o comando TRANSLATE só para determinar se a entrada principal faz parte desse arquivo. Para fins de segurança, um arquivo csv pode conter uma lista de endereços IP hostis conhecidos ou nomes de usuário válidos com outras informações de política, como permissões e horários de acesso permitido.

NOTA: Entradas principais que expressem faixas não são suportadas, como endereços IP e faixas numéricas.

Variáveis de dados.

Além de determinar se uma entrada principal se encontra ou não no arquivo csv, é possível recuperar os dados associados a essa entrada. Um número de variáveis de script pode ser usado para indicar em quais variáveis os dados serão armazenados. Variáveis de string, inteiras ou flutuante são suportadas. Todas as entradas de dados são armazenadas como strings e serão convertidas no tipo de variável fornecido no comando TRANSLATE.

Continuando com o exemplo do arquivo friends.csv:

```
Bob,azul,25,95
Alice,verde,19,49
Pat,roxo,36,65
```

Você pode obter os dados associados com:

```
TRANSLATE(s_friend, "friends.csv", i_found, s_color,
   i_age, i_weight)
```

Onde:

- Se s_friend contiver Alice, i_found será igual a 1, s_color seria igual a verde, i_age seria igual a 19 e i_weight seria igual a 49;
- Se a entrada principal não for localizada, as variáveis não serão modificadas (s_color, i_age, i_weight);
- Se a entrada para Alice fosse:
  ```
  Alice,verde,19,
  ```
  Usando o mesmo comando TRANSLATE, a variável i_weight seria apagada (0 para inteiros, 0.0 para flutuantes e "" strings). s_color seria verde e i_age seria 19.
- Se a entrada para Alice fosse:
  ```
  Alice,verde,magra,Ford
  ```
  Usando o mesmo comando TRANSLATE, a variável i_age seria apagada e magra seria convertida em um inteiro (0) e colocada em i_weight. s_color seria verde e Ford seria ignorado.
- Se a entrada para Alice fosse:
  ```
  Alice,25,19,49
  ```
  Usando o mesmo comando TRANSLATE, a variável s_color conteria 25. i_age seria 19 e i_weight seria 49.

Formato

```
TRANSLATE(<chave>, <csv_file>, <found_status> [,
   <variável>, ...])
```

Tipos de dados

Argumento	Tipo	Descrição
key		Entrada principal a ser pesquisada no arquivo csv.
csv_file		Nome do arquivo csv.
found_status		Variável inteira definida como 1 se a entrada principal encontrar-se no arquivo csv ou como zero se ela não se encontrar no arquivo csv.
variável		Lista de variáveis em que os dados associados à entrada principal serão colocados.

TRIM

Remove todos os espaços em branco das duas extremidades de uma string, e substitui vários espaços em branco em uma string por espaços simples. Os vazios incluem os seguintes caracteres:

- <tabulação>
- <retorno de carro>
- <nova linha>
- <tabulação vertical>
- <alimentação de formulário>
- <espaço>

Formato

```
TRIM(svar)
```

Tipos de dados

Argumento	Tipo	Descrição
string	svar (ENTRADA)	String da qual retirar o espaço em branco. A string resultante é armazenada na variável de entrada.

Por exemplo:

```
COPY(s_var:" Olá    Mundo  "
TRIM(s_var)
```

Conteúdo das variáveis de saída atuais:

```
s_var = " Olá Mundo "
```

WHILE

O comando WHILE fornece recursos de loop do fluxo de controle.

O comando WHILE procede da seguinte maneira:

- Se o resultado da declaração WHILE() é verdadeiro, os comandos de análise após o comando WHILE(), até o próximo ENDWHILE(), são executados;
- Se o resultado da declaração WHILE() é falso, nenhum comando de análise é executado entre os comandos WHILE() e ENDWHILE();

Embora todos os tipos de dados sejam aceitos em cada lado do operador da declaração WHILE(), valores numéricos só podem ser comparados com valores numéricos e strings, só com strings.

O operador da comparação WHILE() pode ser <, =, >, <=, >=, <>, &, + ou ^.

AVISO: Não utilize o operador NOT lógico (^) junto com uma variável de string. Isso causará um erro de sintaxe.

Você não pode fazer comparações diretas com um número negativo. Para isso, use um destes dois métodos:

- Use a função de análise COMPARE;
- Compare indiretamente como mostrado a seguir:

```
SET(i_compare_val=-10)
WHILE(ivar >i_compare_val)
SET(ivar=ivar-1)
ENDWHILE()
```

Formato

```
WHILE(<expr>)
```

Onde:

```
expr ::= var
       | (<expr>)
       | ^ <expr>
```

Onde <expr> deve ser avaliado como variável inteira ou flutuante.

```
       | <expr> <|=|>|<=|>=|<>|&|+ <expr>
```

Onde ambos os parâmetros <expr> devem ser avaliados como o mesmo tipo.

Tipos de dados

Argumento	Tipo	Descrição
data1	todos (ENTRADA)	Dados a serem comparados com data2. Se data2 não for usado, ele se tornará um operador lógico (0 = false, todos os outros = true).
Operador lógico	< = > <= >= <> & + ^	Menor que Igual a Maior que Menor que ou Igual a Maior que ou Igual a Diferente de Operador lógico AND Operador lógico OR Operador lógico NOT
data2	todos (ENTRADA) [OPCIONAL]	Dados a serem comparados com o data1. Devem ser do mesmo tipo que o data1.
…	idem acima	Use até 200 parâmetros individuais para criar expressões lógicas complexas.

Por exemplo:

```
WHILE(i<3)
SET(i=i+1)
ALERT("Ainda em loop")
ENDWHILE()
ALERT("Saiu do loop")
```

4 Funções do administrador do Assistente

> **NOTA**: O termo Agente é sinônimo de Coletor. Mais para a frente, Agentes será referido como Coletores

Este capítulo é voltado para o administrador do sistema do Assistente. Ele descreve várias funções administrativas realizadas pelo administrador do sistema e fornece informações sobre os processos de segundo plano do Assistente.

> **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

Aplicativos e utilitários do Assistente

O Assistente é composto de uma interface do usuário (Construtor de Coletor) e de vários utilitários adicionais que operam com o Construtor de Coletor para realizar a monitoração de rede.

Construtor de Coletor

A interface de usuário do Assistente é o Construtor de Coletor. O Construtor de Coletor permite que você configure os Coletores de sua rede, bem como as portas e os scripts usados para comunicação com os hosts. O Construtor de Coletor só é executado no Windows.

> **NOTA:** Se houver um problema na forma como as janelas do Assistente são exibidas depois de arrastadas para outra posição, verifique suas configurações de tela no Painel de Controle do Microsoft Windows. Na guia Efeitos, desmarque Mostrar o conteúdo da janela ao arrastar.

Porta

No Assistente, as portas possibilitam que um Coletor localize os dados do evento de segurança na rede, fornecendo o endereço IP e outras informações sobre a origem (dispositivo de segurança [roteador, IDS, switch, etc…]). Cada linha na tabela de Configuração de Portas executa um script de Coletor para uma origem de evento.

Gerenciador de Coletor

O Gerenciador de Coletor inicia e pára o processamento de porta.

Mecanismo de Coletor

O mecanismo do Coletor processa a lógica de gabarito para cada porta. Um mecanismo do Coletor é executado para cada porta ativa

popup.exe

O utilitário popup.exe é usado pelo Mecanismo do Coletor para auxiliar no processamento de popup ou exibir comandos de análise.

popup.cfg

O utilitário popup.cfg é um arquivo opcional usado para controlar tempos de espera de popup e exibir comandos de análise. Se você não tiver um arquivo popup.cfg, os comandos de análise de popup e exibição não excederão o tempo de espera.

Para definir um tempo de espera para o comando de exibição, digite a declaração:

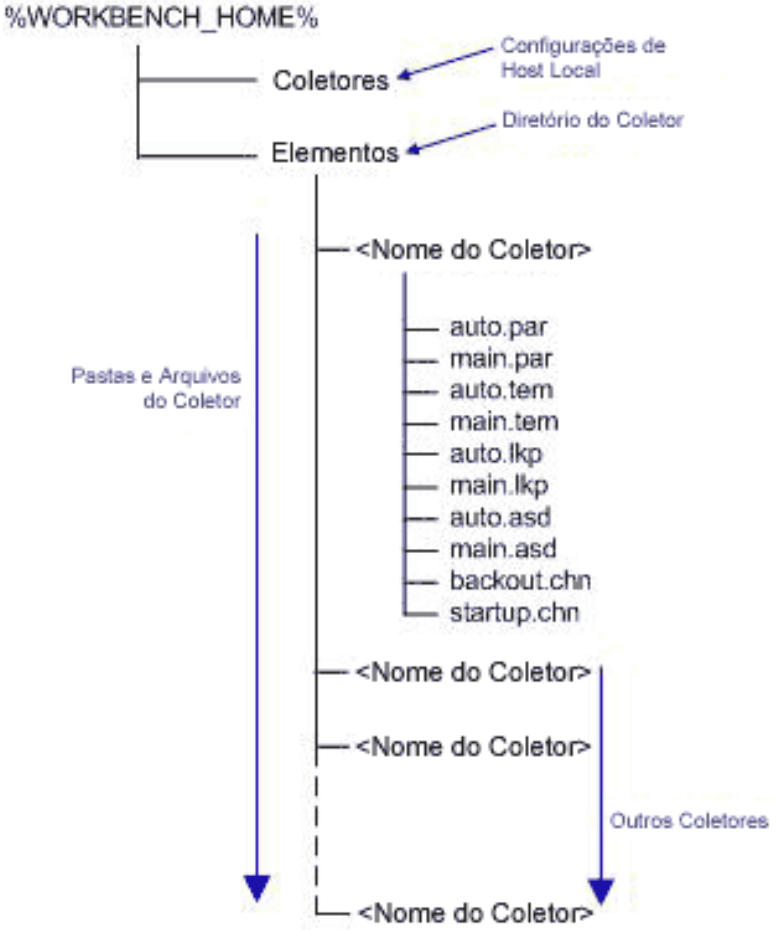
```
displaytimeout <verdadeiro/falso>.
```

O tempo de espera de exibição é definido como 20 segundos.

Para definir um tempo de espera para o comando de popup, digite a declaração:

```
timeout <tempo de espera em segundos>.
```

Estrutura de diretórios do Assistente



Chave

Coletores	Arquivos de configuração de porta (Hosts do Assistente)
Elementos	Arquivos do Coletor
.par	Arquivos de parâmetro
.tem	Arquivos de gabarito
.lkp	Arquivos de pesquisa
.asd	Arquivos de descrição de estado ativo
backout.chn	Arquivos de script de volta
startup.chn	Arquivos de script de inicialização

5 Metatags do Assistente e do Sentinel

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.

As tags META armazenam metadados. Os metadados são informações sobre dados, nomes variáveis predefinidos para metadados. Por exemplo, o IP de origem de um ataque é armazenado na tag META SourceIP. Os nomes de produtos são armazenados na tag META ProductName. Os dados usados para preencher tags META são extraídos dos dados de registro do dispositivo ou definidos como parte do processamento do Coletor.

Para acessar o recurso de configuração e mapeamento de eventos no Gerenciador de Dados do Sentinel, clique na guia Eventos.

NOTA: Na linguagem de regra de correlação RuleLg de formato livre, quando um rótulo é precedido de 'e', como e.crt, ele se refere a eventos atuais. Quando um rótulo é precedido de 'w', como w.crt, ele se refere a eventos históricos.

O valor da coluna Variável do Coletor é o nome da variável do Coletor a ser definida para preencher a tag META correspondente. Para obter mais informações sobre comandos de análise, consulte o capítulo 3 e a documentação dos Coletores específicos, localizada em:

```
%ESEC_HOME%\wizard\elements\<Nome do Coletor>\docs.
```

NOTA: Na tabela a seguir, rótulos e tags META são usados no Sentinel Control Center. As variáveis do Coletor são usadas na análise do Coletor. Nem todas as tags META têm uma variável do Coletor correspondente.

Os tipos especificados na coluna Tipo têm as seguintes propriedades:

- string – limitada a 255 caracteres (a menos que seja especificado algo diferente)
- inteiro – inteiro de 32 bits com sinal
- UUID – strings hexadecimais com 36 caracteres (com hifens) ou 32 caracteres (sem hifens) no formato XXXXXXXX-XXXX-XXXX-XXXX-XXXXXXXXXXXX (p. ex.: - 6A5349DA-7CBF-1028-9795-000BCDFFF482)
- data – a variável do Coletor deve ser definida como o número de milissegundos desde 1 de janeiro de 1970, 00:00:00 GMT Quando exibidas no Sentinel Control Center, as tags META do tipo data são exibidas no formato de data regular.
- IPv4 – Endereço IP em notação decimal com ponto (isto é, xxx.xxx.xxx.xxx)

Rótulo	Tag META	Tipo	Descrição	Variável do Coletor
CorrelatedEventUuids	ceu	string	Lista de UUIDs de evento associados a este evento correlato. Relevante apenas para eventos correlatos.	
Importância	crt	inteiro	A importância do bem identificado neste evento.	s_CRIT
Ct1 a Ct2 (Cliente reservado)	ct1 a ct2	string	Reservado para uso de clientes, para dados específicos do cliente (string)	s_CT1 e s_CT2
Ct3 (Cliente reservado)	ct3	inteiro	Reservado para uso de clientes, para dados específicos do cliente (número)	s_CT3
CustomerVar1 a CustomerVar10	cv1 a cv10	inteiro	Reservado para uso de clientes, para dados específicos do cliente (número)	s_CV1 a s_CV10
CustomerVar11 a CustomerVar20	cv11 a cv20	data	Reservado para uso de clientes, para dados específicos do cliente (data)	s_CV11 a s_CV20
CustomerVar21 a CustomerVar29	cv21 a cv29	string	Reservado para uso de clientes, para dados específicos do cliente (string)	s_CV21 a s_CV29
CustomerVar30 a CustomerVar34	cv30 a cv34	string	Reservado para uso de clientes, para dados específicos do cliente (string) Pode lidar com strings de até 4.000 caracteres.	s_CV30 a s_CV34
CustomerVar35 a CustomerVar89	cv35 a cv89	string	Reservado para uso de clientes, para dados específicos do cliente (string)	s_CV35 a s_CV89
SARBOX	cv90	string	Dados específicos da Sarbanes Oxley.	s_CV90
HIPAA	cv91	string	Dados específicos do HIPAA (Health Insurance Portability and Accountability Act)	s_CV91
GLBA	cv92	string	Dados específicos do GLBA (Gramm-Leach-Bliley Act)	s_CV92

FISMA	cv93	string	Dados específicos do FISMA (Federal Information Security Management Act)	s_CV93
NISPOM	cv94	string	Dados específicos do NISPOM (National Industrial Security Program Operating Manual)	s_CV94
SIPCountry	cv95	string	País do IP de origem.	s_CV95
DIPCountry	cv96	string	País do IP de destino.	s_CV96
CustomerVar97 a CustomerVar100	cv97 a cv100	string	Reservado para uso de clientes, para dados específicos do cliente (string)	s_CV97 a s_CV100
DateTime	dt	data	A data e a hora normalizadas do evento, conforme fornecido pelo Coletor.	
DestinationHostName	dhn	string	O nome do host de destino ao qual o evento era destinado.	s_DHN
DestinationIP	dip	IPv4	O endereço IP de destino ao qual o evento era destinado.	s_DIP
DestinationPort	dp	string (32)	A porta de destino à qual o evento era destinado.	s_DP
DestinationUserName	dun	string	O nome do usuário de destino em que uma ação foi tentada. Por exemplo: Tentativa de redefinir a senha do Root.	s_DUN
EventID	id	UUID	Identificador exclusivo deste evento.	
EventTime	et	string	A data normalizada do evento, conforme relatado pelo sensor, analisado no formato: Y-M-D-H:M:S~AMPM24~TZ.	s_ET
EventName	evt	string	O nome descritivo do evento, conforme relatado (ou fornecido) pelo sensor. Exemplo: "Exploração de porta"	s_EVT

ExtendedInformation	ei	string (1000)	Armazena informações adicionais coletadas pelo Coletor. Os valores nessa variável são separados por ponto-e-vírgula (;). Por exemplo: Um domínio para um ID ou nomes de arquivo.	s_EI
FileName	fn	string (1000)	O nome do programa executado ou do arquivo acessado, modificado ou afetado. Por exemplo: O nome de um arquivo infectado por vírus ou de um programa detectado por um IDS.	s_FN
Message	msg	string (4000)	Texto de mensagem com formato livre para o evento.	s_BM
Protocol	prot	string	O protocolo de rede do evento.	s_P
ProductName	pn	string	Indica o tipo, o fornecedor e o nome de código de produto do sensor por meio do qual o evento foi gerado. Por exemplo: Check Point FireWall=CPFW.	s_PN
ReporterName	rn	string	O nome do host ou o endereço IP do dispositivo para o qual um evento foi registrado ou do qual é enviada uma notificação do evento.	s_RN
ReservedVar1 a ReservedVar10	rv1 a rv10	inteiro	Reservado pela Novell para expansão (número).	s_RV1 a s_RV10
ReservedVar11 a ReservedVar20	rv11 a rv20	data	Reservado pela Novell para expansão (data).	s_RV11 a s_RV20
ReservedVar21 a ReservedVar25	rv21 a rv25	UUID	Reservado pela Novell para expansão (UUID).	s_RV21 a s_RV25
ControlPack	rv26	string	Classificação de controle do Sentinel nível 1	s_RV26
ControlMonitor	rv27	string	Classificação de controle do Sentinel nível 2	s_RV27
ReservedVar28	rv28	string	Reservado pela Novell para expansão (string).	s_RV28

SourceIPCountry	rv29	string	País do endereço IP de origem.	s_RV29
AttackID	rv30	string	ID de ataque normalizado (ID de ataque ao consultor)	s_RV30
DeviceName	rv31	string	Nome do dispositivo de segurança	s_RV31
Categoria do dispositivo	rv32	string	Categoria do dispositivo (AV, DB, ESEC, FW, IDS, OS AV: Antivírus DB: banco de dados ESEC: evento do sistema FW: firewall IDS: detecção de intrusão OS: sistema operacional	s_RV32
Contexto do evento	rv33	string	Contexto do evento (nível de ameaça).	s_RV33
Nível de ameaça de origem	rv34	string	Nível da ameaça de origem.	s_RV34
Contexto do usuário de origem	rv35	string	Contexto do usuário de origem.	s_RV35
Contexto dos dados	rv36	string	Contexto de dados.	s_RV36
Função de origem	rv37	string	Função de origem.	s_RV37
Contexto operacional de origem	rv38	string	Contexto operacional de origem.	s_RV38
Nome do cliente MSSP	rv39	string	Nome do cliente MSSP.	s_RV39
ReservedVar40 a ReservedVar43	rv40 a rv43	string	Reservado pela Novell para expansão (string).	s_RV40 a s_RV43
Nível de ameaça de destino	rv44	string	Nível da ameaça de destino.	s_RV44
Contexto do usuário de destino	rv45	string	Contexto do usuário de destino.	s_RV45
Status de vírus	rv46	string	Status do vírus.	s_RV46
Função de destino	rv47	string	Função de destino.	s_RV47
Contexto operacional de destino	rv48	string	Contexto operacional de destino.	s_RV48
ReservedVar49	rv49	string	Reservado pela Novell para expansão (string).	s_RV49
Nível de taxonomia eSec 1	rv50	string	Classificação do código de evento do Sentinel - nível 1	s_RV50
Nível de taxonomia eSec 2	rv51	string	Classificação do código de evento do Sentinel - nível 2	s_RV51
Nível de taxonomia eSec 3	rv52	string	Classificação do código de evento do Sentinel - nível 3	s_RV52
Nível de taxonomia eSec 4	rv53	string	Classificação do código de evento do Sentinel - nível 4	s_RV53
ReservedVar54 a ReservedVar55	rv54 a rv55	string	Reservado pela Novell para expansão (string).	s_RV54 a s_RV55

SourceAssetName	rv56	string	Origem (Gerenciamento de bens) – Nome do bem	s_RV56
SourceMacAddress	rv57	string	Origem (Gerenciamento de bens) – Endereço Mac	s_RV57
SourceNetworkIdentity	rv58	string	Origem (Gerenciamento de bens) – Identidade da rede	s_RV58
SourceAssetCategory	rv59	string	Origem (Gerenciamento de bens) – Categoria do bem	s_RV59
SourceEnvironmentIdentity	rv60	string	Origem (Gerenciamento de bens) – Identidade do ambiente	s_RV60
SourceAssetValue	rv61	string	Origem (Gerenciamento de bens) – Valor do bem	s_RV61
SourceCriticality	rv62	string	Origem (Gerenciamento de bens) – Importância	s_RV62
SourceSensitivity	rv63	string	Origem (Gerenciamento de bens) – Confidencialidade	s_RV63
SourceBuilding	rv64	string	Origem (Gerenciamento de bens) – Criação	s_RV64
SourceRoom	rv65	string	Origem (Gerenciamento de bens) – Sala	s_RV65
SourceRackNumber	rv66	string	Origem (Gerenciamento de bens) – Número do rack	s_RV66
SourceCity	rv67	string	Origem (Gerenciamento de bens) – Cidade	s_RV67
SourceState	rv68	string	Origem (Gerenciamento de bens) – Estado	s_RV68
SourceCountry	rv69	string	Origem (Gerenciamento de bens) – País	s_RV69
SourceZipCode	rv70	string	Origem (Gerenciamento de bens) – CEP	s_RV70
SourceAssetOwner	rv71	string	Origem (Gerenciamento de bens) – Proprietário do bem	s_RV71
SourceAssetMaintainer	rv72	string	Origem (Gerenciamento de bens) – Administrador do bem	s_RV72
SourceBusinessUnit	rv73	string	Origem (Gerenciamento de bens) – Unidade de negócios	s_RV73
SourceLineOfBusiness	rv74	string	Origem (Gerenciamento de bens) – Linha de negócios	s_RV74
SourceDivision	rv75	string	Origem (Gerenciamento de bens) – Divisão	s_RV75
SourceDepartment	rv76	string	Origem (Gerenciamento de bens) – Departamento	s_RV76
SourceAssetId	rv77	string	Origem (Gerenciamento de bens) – Id do bem de origem	s_RV77

DestinationAssetName	rv78	string	Destino (Gerenciamento de bens) – Nome do bem	s_RV78
DestinationMacAddress	rv79	string	Destino (Gerenciamento de bens) – Endereço Mac	s_RV79
DestinationNetworkIdentity	rv80	string	Destino (Gerenciamento de bens) – Identidade da rede	s_RV80
DestinationAssetCategory	rv81	string	Destino (Gerenciamento de bens) – Categoria do bem	s_RV81
DestinationEnvironmentIdentity	rv82	string	Destino (Gerenciamento de bens) – Identidade do ambiente	s_RV82
DestinationAssetValue	rv83	string	Destino (Gerenciamento de bens) – Valor do bem	s_RV83
DestinationCriticality	rv84	string	Destino (Gerenciamento de bens) – Importância	s_RV84
DestinationSensitivity	rv85	string	Destino (Gerenciamento de bens) – Confidencialidade	s_RV85
DestinationBuilding	rv86	string	Destino (Gerenciamento de bens) – Criação	s_RV86
DestinationRoom	rv87	string	Destino (Gerenciamento de bens) – Sala	s_RV87
DestinationRackNumber	rv88	string	Destino (Gerenciamento de bens) – Número do rack	s_RV88
DestinationCity	rv89	string	Destino (Gerenciamento de bens) – Cidade	s_RV89
DestinationState	rv90	string	Destino (Gerenciamento de bens) – Estado	s_RV90
DestinationCountry	rv91	string	Destino (Gerenciamento de bens) – País	s_RV91
DestinationZipCode	rv92	string	Destino (Gerenciamento de bens) – CEP	s_RV92
DestinationAssetOwner	rv93	string	Destino (Gerenciamento de bens) – Proprietário do bem	s_RV93
DestinationAssetMaintainer	rv94	string	Destino (Gerenciamento de bens) – Administrador do bem	s_RV94
DestinationBusinessUnit	rv95	string	Destino (Gerenciamento de bens) – Unidade de negócios	s_RV95
DestinationLineOfBusiness	rv96	string	Destino (Gerenciamento de bens) – Linha de negócios	s_RV96
DestinationDivision	rv97	string	Destino (Gerenciamento de bens) – Divisão	s_RV97
DestinationDepartment	rv98	string	Destino (Gerenciamento de bens) – Departamento	s_RV98
DestinationAssetId	rv99	string	Destino (Gerenciamento de bens) – Id do bem de destino	s_RV99

ReservedVar100	rv100	string	Reservado pela Novell para expansão (string).	s_RV100
Recurso	res	string	O nome do recurso.	s_Res
DeviceAttackName	rt1	string	Para uso com o Consultor. Nome do ataque do dispositivo de segurança	s_RT1
Rt2	rt2	string	Preenchido com o nome da regra de correlação quando uma regra de correlação gera um evento.	s_RT2
Rt3	rt3	inteiro	Reservado pela Novell para expansão (número).	s_RT3
SourceHostName	shn	string	O nome do host de origem do evento.	s_SHN
SourceID	src	UUID	Identificador exclusivo para o processo do Sentinel que gerou este evento.	
SourceIP	sip	IPv4	O endereço IP do qual evento foi originado.	s_SIP
SensorName	sn	string	O nome do último detector do evento quando recebido em dados iniciais. Exemplo: "FW1" para um firewall.	s_SN
Severity	sev	inteiro	A severidade normalizada do evento (0 a 5).	i_Severity
SourcePort	sp	string (32)	A porta da qual o evento teve origem.	s_SP
SensorType	st	string (5)	O designador de caractere exclusivo para o tipo de sensor (N, H, I, O, P, V, C, W) C: Correlação H: Baseado em host I: Interno (evento do sistema) N: Baseado em rede O: Outros P: Desempenho (evento do sistema) V: Antivírus W: Lista de Avisos	s_ST
SourceUserName	sun	string	O nome do usuário de origem usado para iniciar um evento. Exemplo: "jdoe" durante uma tentativa de "su".	s_SUN
SubResource	sres	string	O nome do sub-recurso.	s_SubRes
Vulnerabilidade	vul	inteiro	A vulnerabilidade do bem identificado neste evento.	s_VULN

WizardAgent	agent	string (64)	Coletor do Sentinel que gerou este evento. Para eventos do sistema, o Coletor será o de desempenho ou o interno.
WizardPort	port	string (64)	Descrição da porta do Coletor do Sentinel.

6 Permissões do usuário do Sentinel Control Center

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

As permissões do usuário são divididas conforme indicado a seguir:

- Geral
  - Filtros públicos
  - Filtros privados
  - Ações de integração
- Telas Ativas
  - Itens de menu
  - Telas de resumo
- iTRAC
  - Gerenciamento de gabarito
  - Gerenciamento de processo
- Incidentes
- Gerenciador do Coletor
- Análise
- Consultor
- Administração
  - Correlação
  - Estatísticas DAS
  - Informações de arquivo de evento
  - Telas de servidor
  - Filtros globais
  - Gerenciamento de função do iTRAC
  - Configuração de menu
  - Gerenciamento de usuário
  - Gerenciamento de sessão de usuário

Usuários padrão

O instalador criará os seguintes usuários-padrão n Sentinel Server:

Autenticação Oracle e MS SQL:

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

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

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

Autenticação do Windows:

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

Geral

Nome da permissão	Descrição
Gravar Espaço de Trabalho	Permite que os usuários gravem preferências. Se essa permissão estiver indisponível, o usuário nunca será solicitado a gravar alterações nas preferências, quando efetuar logout ou sair do Sentinel Control Center.
Gerenciamento de Colunas	Permite que o usuário gerencie colunas nas tabelas da Tela Ativa.
Instantâneo	Permite que o usuário tire um instantâneo das tabelas da Tela Ativa.

Geral - Filtros públicos

Nome da permissão	Descrição
Criar Filtros Públicos	Permite que o usuário crie um filtro com um ID de proprietário de PUBLIC. Se o usuário não tiver essa permissão, o valor PUBLIC não será listado como um dos IDs do proprietário para o qual o usuário pode criar um filtro.
Modificar Filtros Públicos	Permite que o usuário modifique um filtro público.
Apagar Filtros Públicos	Permite que o usuário apague um filtro público.

Geral - Filtros privados

Nome da permissão	Descrição
Criar Filtros Privados	Permite que o usuário crie filtros privados para si próprio ou para outros usuários.
Modificar Filtros Privados	Permite que o usuário modifique os próprios filtros privados e os criados por outros usuários.
Apagar Filtros Privados	Permite que o usuário apague os próprios filtros privados e os criados por outros usuários.
Ver/Usar Filtros Privados	Permite que o usuário veja os próprios filtros privados e os criados por outros usuários.

Geral – Ações de integração

Nome da permissão	Descrição
Enviar para HP Open View	Permite que os usuários enviem eventos, incidentes e objetos associados ao HP-OVO.
Enviar Evento para o HP Service Desk	Permite que os usuários enviem eventos, incidentes e objetos associados ao HP Service Desk.
Enviar para o Suporte Técnico do Remedy	Permite que os usuários enviem eventos, incidentes e objetos associados ao Remedy.

Telas Ativas

Nome da permissão	Descrição
Guia Ver Tela Ativa	Permite que o usuário veja e use a guia Tela Ativa, o menu e outras funções relacionadas associadas à guia Tela Ativa.

Telas Ativas – Itens de menu

Nome da permissão	Descrição
Usar Itens Atribuídos do Menu	Permite que o usuário utilize itens de menu atribuídos da tabela de eventos da Tela Ativa (o menu acessado com o botão direito do mouse).
Adicionar a Incidente Existente	Permite que o usuário adicione eventos a incidentes existentes utilizando a tabela de eventos da Tela Ativa (o menu de clique com o botão direito do mouse).
Remover do Incidente	Permite que o usuário remova eventos de um incidente existente utilizando a tabela de eventos da Tela Ativa (o menu de clique com o botão direito do mouse).
Enviar Eventos por E-mail	Permite que o usuário envie eventos por e-mail utilizando a tabela de eventos da Tela Ativa (o menu de clique com o botão direito do mouse).
Ver Dados de Ataque do Consultor	Permite que o usuário veja o fluxo de dados de ataque ao consultor.
Ver Vulnerabilidade	Permite que o usuário veja o resultado de uma verificação do Nessus.

Telas Ativas – Exibições de Resumo

Nome da permissão	Descrição
Usar/Ver Exibições de Resumo	Permite que o usuário acesse os gráficos da Tela Ativa.

iTRAC

Nome da permissão	Descrição
Guia Ver iTRAC	Permite que o usuário veja e use a guia iTRAC, o menu e outras funções relacionadas associadas à guia iTRAC.
Gerenciamento de Atividades	Permite que o usuário acesse os gráficos do Gerenciador de Atividades.

Gerenciamento de gabarito

Nome da permissão	Descrição
Ver/Usar Gerenciador de Gabaritos	Permite que o usuário acesse o Gerenciador de Gabaritos.
Criar/Modificar Gabaritos	Permite que o usuário crie e modifique gabaritos.

Gerenciamento de processos

Nome da permissão	Descrição
Ver/Usar Gerenciador de Processos	Permite que o usuário acesse o Gerenciador de Telas de Processos.
Controlar Processos	Permite que o usuário utilize o Gerenciador de Telas de Processos.

Incidentes

Nome da permissão	Descrição
Guia Ver Incidentes	Permite que o usuário veja e use a guia Ver Incidentes, o menu e outras funções relacionadas associadas à guia Ver Incidentes.
Administração de Incidentes	Permite que o usuário modifique um incidente.
Ver Incidente(s)	Permite que o usuário veja os detalhes de um incidente. Se o usuário não tiver permissão, a janela Detalhes do Incidente não será exibida quando o usuário clicar duas vezes em um incidente, na janela do navegador, ou em um incidente na guia Incidente do caso.
Criar Incidente(s)	Permite que o usuário crie incidentes no menu de eventos, acessível com um clique no botão direito do mouse.
Modificar Incidente(s)	Permite que o usuário modifique um incidente na janela Detalhes do Incidente.
Apagar Incidente(s)	Permite que o usuário apague incidentes.
Atribuir Incidente(s)	Permite que o usuário atribua um incidente na janela Modificar e Criar Incidente.
Enviar Incidentes por E-mail	Permite que o usuário envie por e-mail incidentes de interesse.
Ações de Incidente	Permite que o usuário habilite/desabilite a configuração/execução da ação do incidente.

Gerenciamento de Coletor

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 do 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

Análise

Nome da permissão	Descrição
Guia Ver Análise	Permite que o usuário veja e use a guia Ver Análise, o menu e outras funções relacionadas associadas à guia Exibir Visão Geral do Sistema.

Consultor

Nome da permissão	Descrição
Guia Ver Consultor	Permite que o usuário veja e use a guia Ver Consultor, o menu e outras funções relacionadas associadas à guia Ver Consultor.

Administração

Nome da permissão	Descrição
Guia Ver Administração	Permite que o usuário veja e use a guia Ver Administração, o menu e outras funções relacionadas associadas à guia Ver Administração.

Administração - Correlação

Nome da permissão	Descrição
Usar/Ver Gerenciador de Mecanismos de Correlação	Permite que o usuário veja e use o Mecanismo de Correlação.
Usar/ver Regras de Correlação	Permite que o usuário inicie ou interrompa as Regras de correlação.

Administração - Filtros globais

Nome da permissão	Descrição
Ver/Usar Filtros Globais	Permite que o usuário acesse a janela Configuração de Filtro Global.
Modificar Filtros Globais	Permite que o usuário modifique as configurações de filtro global. **NOTA:** Para acessar esta função, a permissão Ver Filtros Globais deve ser atribuída também.

Administração - Configuração de Menu

Nome da permissão	Descrição
Configuração de Menu	Permite que o usuário acesse a janela Configuração de Menu e adicione novas opções exibidas no menu Evento quando ele clica com o botão direito do mouse em um evento.

Administração – Estatísticas de DAS

Nome da permissão	Descrição
Estatísticas DAS	Permite que o usuário veja a atividade de DAS (consultas e binários de DAS).

Administração - Informações do arquivo de evento

Nome da permissão	Descrição
Informação do arquivo de eventos	Permite que o usuário veja o status do arquivo de evento.

Administração – Telas do servidor

Nome da permissão	Descrição
Ver Servidores	Permite que o usuário monitore o status de todos os processos.
Controlar Servidores	Permite que o usuário inicie, reinicie ou interrompa processos.

Administração - Gerenciamento do usuário

Nome da permissão	Descrição
Usar/Ver Conta do Usuário	Permite que o usuário utilize e veja as contas do usuário.
Criar Conta do Usuário	Permite que o usuário crie uma conta do usuário. **NOTA:** Para acessar esta função, a permissão Usar/Ver Conta do usuário deve ser atribuída também.
Modificar Conta do Usuário Existente	Permite que o usuário modifique uma conta do usuário existente. **NOTA:** Para acessar esta função, a permissão Usar/Ver Conta do usuário deve ser atribuída também.
Apagar Conta do Usuário	Permite que o usuário apague uma conta do usuário existente. **NOTA:** Para acessar esta função, a permissão Usar/Ver Conta do usuário deve ser atribuída também.

Administração - Gerenciamento da sessão do usuário

Nome da permissão	Descrição
Gerenciamento da Sessão do Usuário	Permite que o usuário veja, bloqueie e termine usuários ativos (logins no Sentinel Control Center).

Administração - Gerenciamento de função do iTRAC

Nome da permissão	Descrição
Gerenciamento de Função do iTRAC	Permite a utilização e a exibição do gerenciador de funções na guia Admin.

7 Mecanismo de Correlação do Sentinel

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

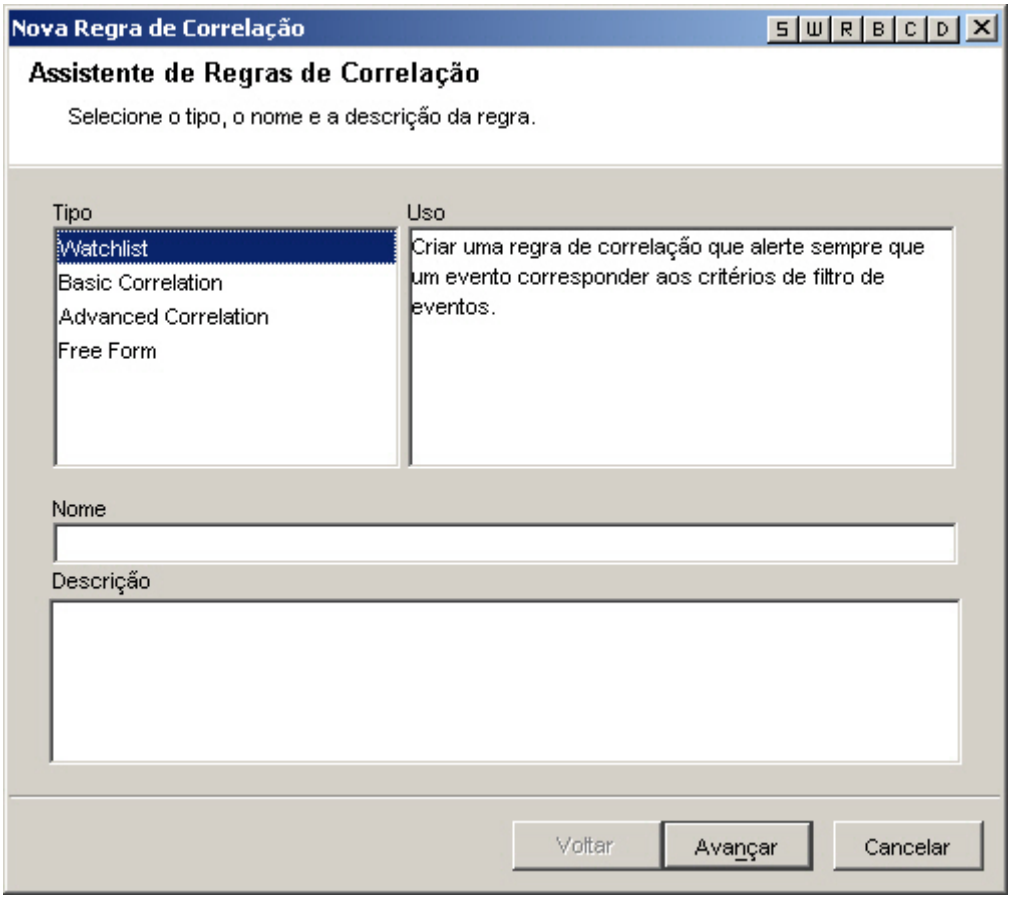
O Mecanismo de Correlação do Sentinel é um aplicativo de threads múltiplos residente na memória. Com os threads múltiplos, o mecanismo de correlação pode tirar proveito do hardware com vários processadores, como as máquinas SMP (symmetric multiprocessing – multiprocessamento simétrico).

O mecanismo de correlação foi projetado para receber dados de dispositivos de segurança, dispositivos de rede e outras fontes de aplicativos, e pesquisar padrões significativos, geralmente dentro de certos limites de tempo. Esses padrões podem indicar ataques, invasões, uso inadequado ou falha. Quando um evento correlacionado é gerado, o campo rt2 é preenchido com o nome da regra de correlação.

O Mecanismo de Correlação do Sentinel oferece uma distribuição escalável. Essa arquitetura permite a distribuição de uma rede distribuída de mecanismos de correlação que funcionam em conjunto para a correlação em tempo real com dados relevantes de segurança, inclusive eventos de segurança monitorados em tempo real, resultados de verificações de vulnerabilidade de sistemas-alvo potenciais, além de informações sobre bens que indicam a importância relativa desses sistemas para os processos de negócios críticos e sua associação com outros sistemas na organização.

O Mecanismo de Correlação do Sentinel é baseado em regras. Você coordena o processamento do mecanismo de correlação mediante regras criadas no editor de regras do Sentinel Control Center. O editor de regras se baseia em uma reunião do Assistente de Regras que fornece várias opções para a criação de regras. Os Assistentes de Regras são:

- Lista de Avisos
- Correlação Básica
- Correlação Avançada
- RuleLg de Formato Livre



Tipos de filtro de correlação

Para Lista de Avisos, Correlação Básica e Correlação Avançada, há quatro tipos diferentes de filtro dentre os quais escolher. São eles:

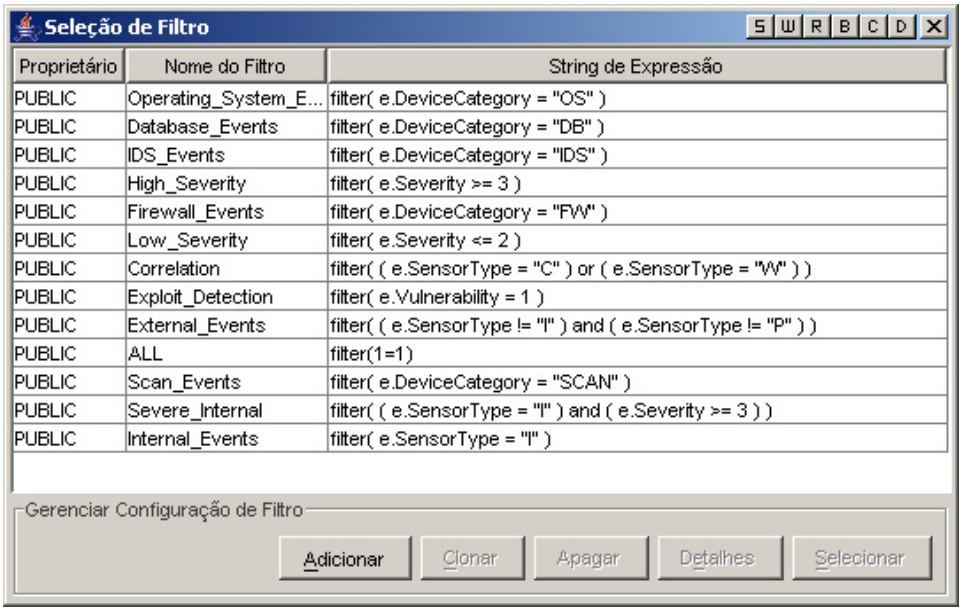
- Permitir Tudo - Equivalente a executar a gravidade de filtro maior ou igual a zero.
- Padrão - Qualquer expressão regular com uma sintaxe semelhante a grep. Uma regra pode procurar por um endereço IP de origem específico de um hacker e notificá-lo sempre que esse endereço for encontrado em qualquer mensagem de evento.
- Gerenciador de Filtro - Uma lista suspensa que exibe o Gerenciador de Filtro para a seleção ou criação de um novo filtro.
- Construtor – Criação de critérios para inclusão ou exclusão de eventos com base na álgebra booleana.

Filtro de Correlação de Tipos de Padrão

Um Filtro de Correlação de Tipos de Padrão usa qualquer expressão regular com uma sintaxe semelhante a grep. A correspondência de expressão regular é feita com uma concatenação de todas as tags META presentes para cada evento de entrada. Por exemplo, o vírus XYZ procurará a string virusXYZ em qualquer tag META presente de todos os eventos de entrada.

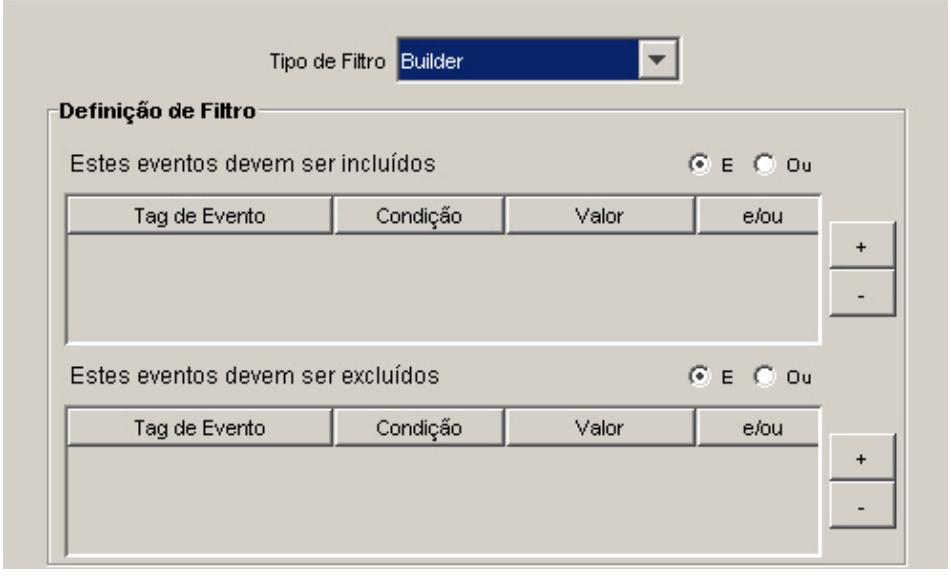
Filtro de Correlação de Tipos de Gerenciador de Filtros

Essa opção permite selecionar um filtro existente ou criar um filtro para usar na correlação por meio da janela Gerenciador de Filtros.



Filtro de Correlação de Tipos de Construtor

Há duas partes para o Filtro de Correlação de Tipos de Construtor. Uma parte são os critérios para inclusão (quais eventos devem ser incluídos na correspondência de padrões) e a outra parte é a exclusão (quais eventos devem ser excluídos da correspondência de padrões).



- Quais eventos devem estar incluídos na correspondência de padrões - Use esta tabela para especificar as condições para limitar os eventos que acionarão a correlação.
  - Tag de eventos – A coluna Tag de eventos é uma lista suspensa de tags de eventos disponíveis (também chamadas tags META) com as quais é possível estabelecer uma correlação.
  - Condição - A coluna Condição é uma lista suspensa de operadores usados na construção de uma condição de correlação.
  - Valor - A coluna Valor é um campo de formato livre que você pode usar para digitar valores se as condições =, !=, <, >, <=, ou >= forem escolhidas. Se =Meta-Tag ou !=Meta-Tag forem selecionadas na coluna Condição, a coluna Valor conterá uma lista suspensa de tags META disponíveis dentre as quais escolher. Você pode digitar qualquer item com as seguintes restrições:
    - Aspas simples nunca podem ser digitadas.
    - Caracteres curinga são um asterisco (*) e um ponto (.), os quais podem aparecer em qualquer parte da string, se for usado regex.
    - Não há caracteres de escape; ou seja, não é possível utilizar a opção de escape com os caracteres curinga.
  - e/ou - Comutação de um item para ou outro ou clicando em uma dessas caixas. Quando várias condições são especificadas nessa tabela, os botões 'e' e 'ou' permitem que você especifique se todas as condições precisam ser atendidas ou se apenas uma delas é necessária. Escolha 'e' para indicar que todas as condições devem ser atendidas. Escolha 'ou' para indicar que apenas uma das condições deve ser atendida.

  NOTA: A seleção será válida somente se a tabela contiver uma segunda ou mais linhas. Todas as linhas na tabela mudarão por padrão para esse operador lógico, exceto a última linha. Combinações de 'e' e 'ou' não são possíveis entre as linhas da tabela.

  - Botões +/-: O botão + adicionará uma linha ao final da tabela. O botão - removerá a linha selecionada da tabela, independentemente de sua posição.
- Quais eventos devem ser excluídos da correspondência de padrões - Use essa tabela para especificar as condições para limitar os eventos que não acionarão a regra de correlação.
  - Tag de eventos - Uma lista de tags de eventos disponíveis com as quais é possível estabelecer uma correlação.
  - Condição - A coluna Condição é uma lista suspensa de operadores usados na construção de uma condição de correlação.
  - Valor - A coluna Valor é um campo de formato livre que você pode usar para digitar valores se as condições =, !=, <, >, <=, ou >= forem escolhidas. Se =Meta-Tag ou !=Meta-Tag forem selecionadas na coluna Condição, a coluna Valor conterá uma lista suspensa de tags META disponíveis dentre as quais escolher. Você pode digitar qualquer item com as seguintes restrições:
    - Aspas simples nunca podem ser digitadas.
    - Caracteres curinga são um asterisco (*) e um ponto (.), os quais podem aparecer em qualquer parte da string, se for usado regex.
    - Não há caracteres de escape; ou seja, não é possível utilizar a opção de escape com os caracteres curinga.
  - e/ou - Comutação de um item para ou outro ou clicando em uma dessas caixas. Quando várias condições são especificadas nessa tabela, os botões 'e' e 'ou' permitem que você especifique se todas as condições precisam ser atendidas ou se apenas uma delas é necessária. Escolha 'e' para indicar que todas as condições devem ser atendidas. Escolha 'ou' para indicar que apenas uma das condições deve ser atendida.

NOTA: A seleção será válida somente se a tabela contiver uma segunda ou mais linhas. Todas as linhas na tabela mudarão por padrão para esse operador lógico, exceto a última linha. Combinações de 'e' e 'ou' não são possíveis entre as linhas da tabela.

- Botões +/-: O botão + adicionará uma linha ao final da tabela. O botão - removerá a linha selecionada da tabela, independentemente de sua posição.

Definição da regra de correlação

Assistentes de Regras de Correlação: Lista de Avisos, Correlação Básica e Correlação Avançada permitem adicionar rapidamente um tipo de regra pré-definida, dependendo do que você deseja obter. O assistente para cada tipo de regra lida com a geração da regra de correlação na linguagem nativa da regra do Mecanismo de Correlação. Cada uma dessas regras é criada por meio da janela Regras de Correlação, na guia Admin.

O Assistente de Regras inclui um editor de formato livre que permite usar a Linguagem de Definição de correlação RuleLg para adicionar a regra diretamente na linguagem nativa da regra do Mecanismo de Correlação.

Lista de Avisos

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

- Permitir Tudo - Equivalente a executar a gravidade de filtro maior ou igual a zero.
- Padrão - Qualquer expressão regular com uma sintaxe semelhante a grep.
- Gerenciador de Filtro - Uma lista suspensa que exibe o Gerenciador de Filtro para a seleção ou criação de um novo filtro.
- Construtor - Criação de critérios para inclusão ou exclusão de eventos com base na álgebra booleana.

Para obter mais informações, consulte Criando uma regra de Lista de Avisos.

Correlação básica

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

- Permitir Tudo - Equivalente a executar a gravidade de filtro maior ou igual a zero.
- Padrão - Qualquer expressão regular com uma sintaxe semelhante a grep.
- Gerenciador de Filtro - Uma lista suspensa que exibe o Gerenciador de Filtro para a seleção ou criação de um novo filtro.
- Construtor - Criação de critérios para inclusão ou exclusão de eventos com base na álgebra booleana.

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

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

Para obter mais informações, consulte Criando uma regra de Correlação Básica.

Correlação Avançada

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

- Permitir Tudo - Equivalente a executar a gravidade de filtro maior ou igual a zero.
- Padrão - Qualquer expressão regular com uma sintaxe semelhante a grep.
- Gerenciador de Filtro - Uma lista suspensa que exibe o Gerenciador de Filtro para a seleção ou criação de um novo filtro.
- Construtor - Criação de critérios para inclusão ou exclusão de eventos com base na álgebra booleana.

Essa regra permite que você:

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

Por exemplo, uma regra de Correlação Avançada pode procurar por eventos do mesmo endereço IP de origem para o mesmo endereço de destino com o mesmo nome de evento que ocorram tanto dentro quanto fora de um firewall (o que significa que o ataque conseguiu penetrar no firewall).

Para obter mais informações, consulte Criando uma regra de Correlação Avançada.

Correlação de RuleLg de formato livre

Com a linguagem de definição de regra de correlação RuleLg, você tem controle total sobre a definição das regras de correlação. Para usar esse tipo de regra de correlação, você deve estar familiarizado com a linguagem de definição da regras de correlação RuleLg.

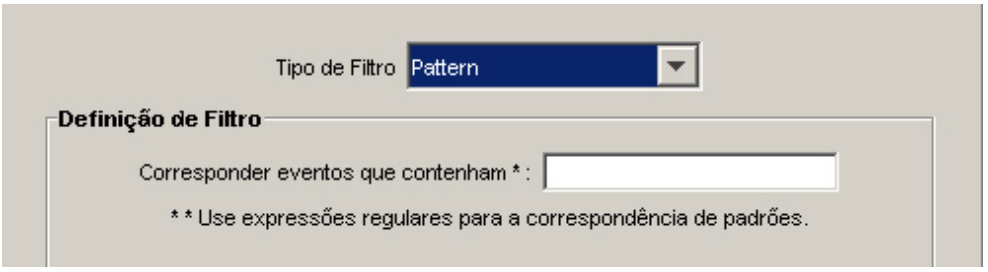
Para obter mais informações, consulte Criando uma Regra de Correlação de RuleLg de formato livre.

Criando uma Regra de Lista de Avisos

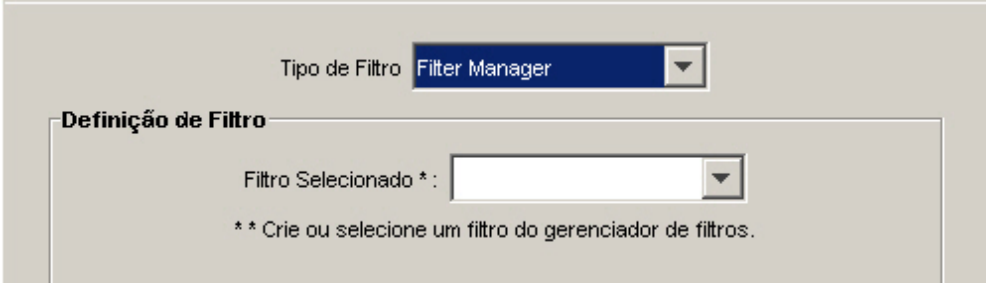
Crie uma Regra de Lista de Avisos quando você quiser especificar uma string que o Mecanismo de Correlação procurará em todos os eventos de entrada. Para criar uma Regra de Lista de Avisos:

- Selecione Regra de Lista de Avisos na primeira janela do Assistente de Regras de Correlação. Preencha as informações para:
  - Nome da Regra - nome que aparecerá na lista de regras. O número máximo de caracteres é 255, não sendo permitido o uso de pontos. Caracteres ASCII estendidos não são permitidos. O nome da Regra diferencia maiúsculas de minúsculas.
  - Descrição – Breve descrição. O tamanho máximo do texto descritivo é de 1024 caracteres.
- Tipo de Filtro
  - Permitir Tudo -

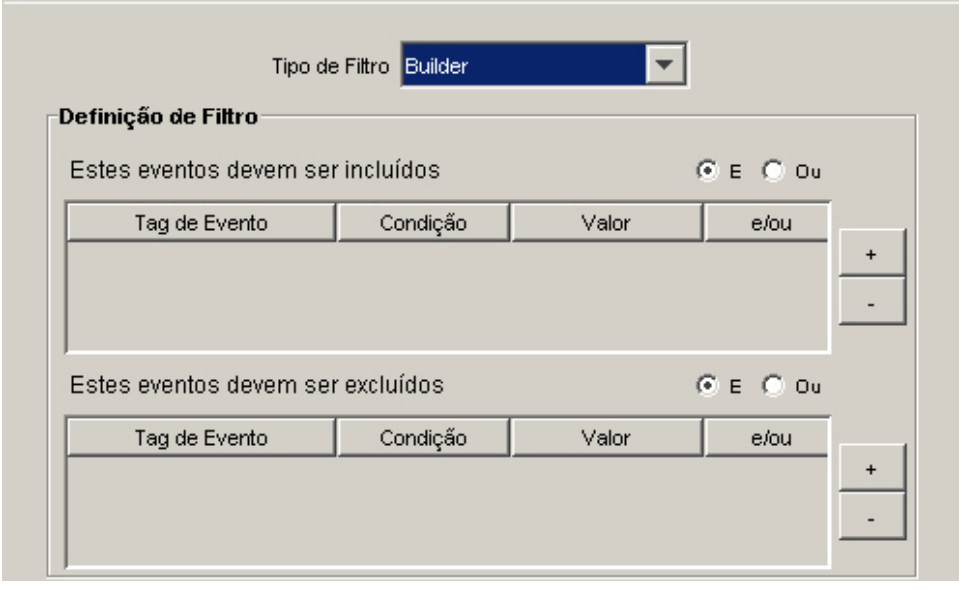
- Padrão – Procurar por eventos que contenham *



- Gerenciador de Filtros - ({id do proprietário}:{nome do Filtro}:<nome do Campo>

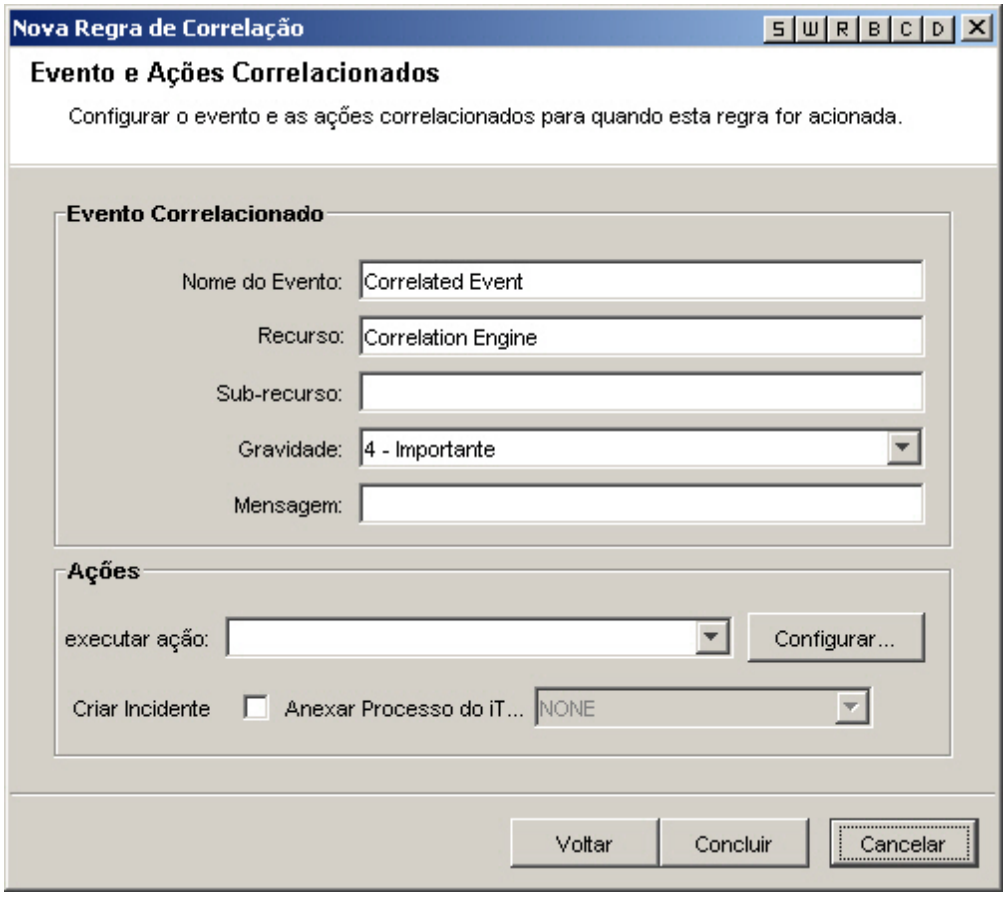


- Construtor

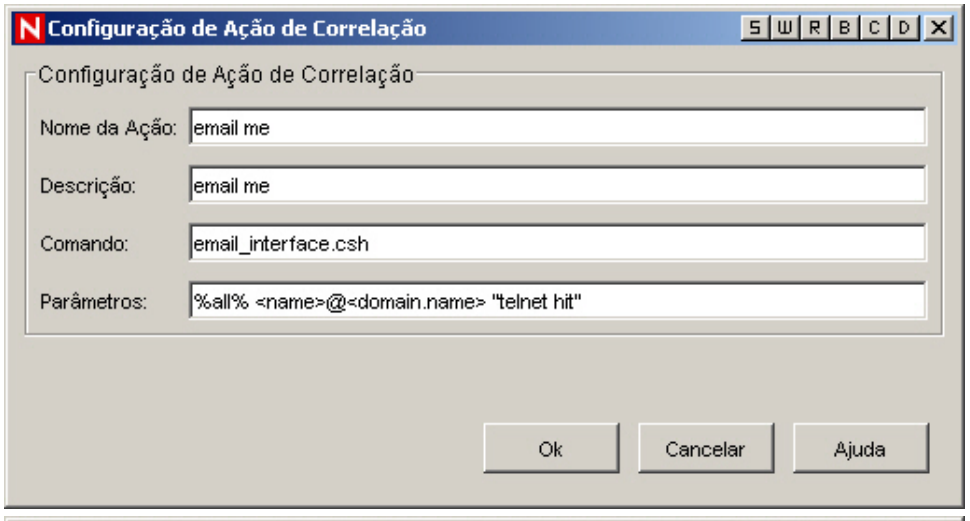


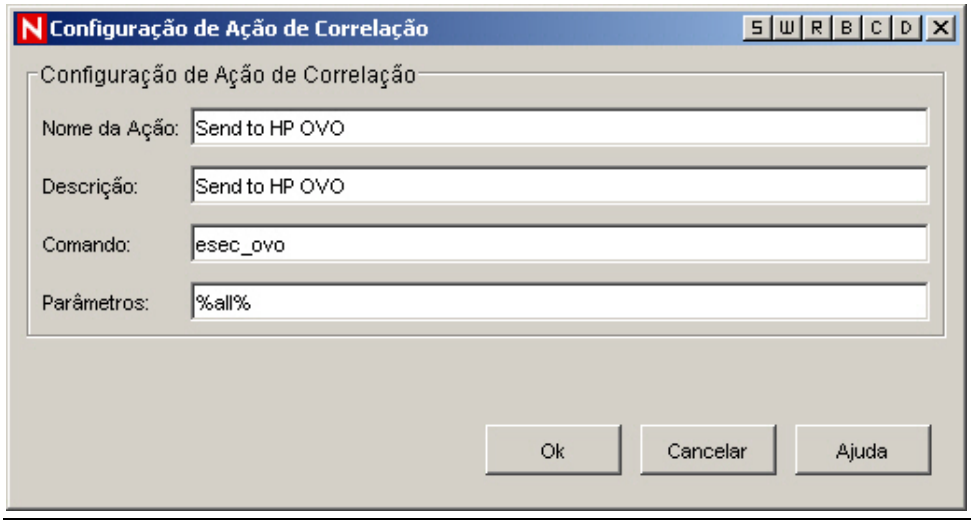
- Página Eventos e Ações Correlacionados - Esse painel define que ação será realizada automaticamente quando os eventos corresponderem a essa regra de correlação. A única entrada necessária é o nível de gravidade, que, por padrão, é o nível 4.
  - Nome do Evento – Padrão: Evento Correlacionado. Esse é o nome de texto do evento correlacionado.
  - Recurso - Padrão: Mecanismo de Correlação. Esse é o nome de texto de um recurso no sistema.
  - Sub-recurso - Padrão: <nenhum>. Esse é o nome do sub-recurso para os recursos com vários sub-recursos.

- Definir nível de gravidade como - Padrão: 4, esse é o nível de gravidade para o qual o evento será designado. Os valores válidos são 0, 1, 2, 3, 4 (padrão) e 5. Uma lista suspensa é fornecida com os níveis de gravidade válidos.
- Texto de mensagem personalizado - Padrão: <nenhum>. Esse é o texto que aparecerá com o evento. Ele é útil na identificação da condição que acionou a Regra de Lista de Avisos. O número máximo de caracteres é 4.000. O texto que você digita nessa caixa é incluído antes do texto do evento de correlação com um separador de pipe. Por exemplo, a entrada de "Nova mensagem" resultaria na mensagem correlacionada "Nova mensagem|Três instâncias de ...".
- Executar Ação (somente Oracle) - Padrão: <nenhum>. Esse é o nome de um arquivo que é executado ao ser acionada a regra de Lista de Avisos. O arquivo deve estar no diretório $ESEC_HOME/sentinel/exec e deve ser executável pelo usuário esecadm. Não há validação de entrada nessa caixa de texto de formato livre. Você pode especificar as tags META que deseja enviar ao executável.
- Executar Ação (somente MSSQL) - Padrão: <nenhum>. Esse é o nome de um arquivo executável que é executado ao ser acionada a regra. O arquivo deve estar no diretório %ESEC_HOME%\sentinel\bin e deve ser executável pelo usuário esecadm. Não há validação de entrada. Você pode especificar as tags META que deseja enviar ao executável. A seguir estão dois exemplos de uma regra de correlação que envia um e-mail e uma regra de correlação que envia o evento de correlação ao HP OVO.



As linhas de comando e de parâmetro são alimentadas como uma string. Na análise, são aplicadas as mesmas regras nas quais \ (barra invertida) é um caractere de escape. Ela pode ser usada como o escape para os caracteres \, % e ". Por exemplo, \%\"\\ é equivalente a %"\: Se precisar de um comando que contenha uma barra invertida, por exemplo, para executar um comando do Windows em um sub-diretório de sentinel\bin, digite duas barras invertidas (\\) para cada barra do diretório. Por exemplo, para executar um arquivo de lote chamado run.bat em %esec_home%\sentinel\bin\batchfiles\, você deve digitar batchfiles\\run.bat. Lembre-se de que todos os executáveis devem estar em %esec_home%\sentinel\bin\.





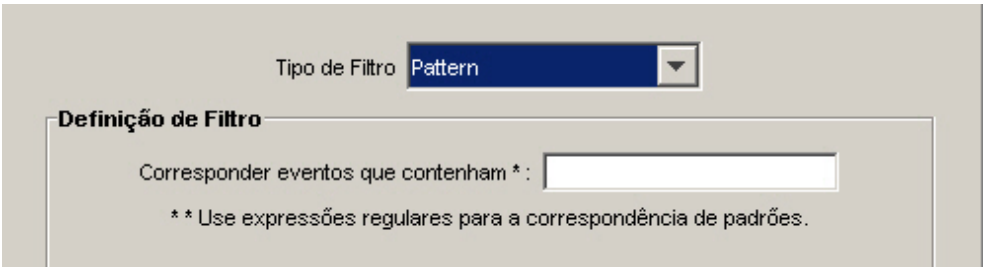
NOTA: Para obter mais informações sobre Comandos e Parâmetros, consulte o Capítulo 5 – Meta Tags do Assistente e do Sentinel no Guia de Referência do Usuário e Seção de saída de correlação.

- Criar Incidente – Uma ação de um evento correlacionado também pode ser a criação de um incidente.
- Anexar processo do iTrac – O incidente criado pode ter um processo iTrac anexado.

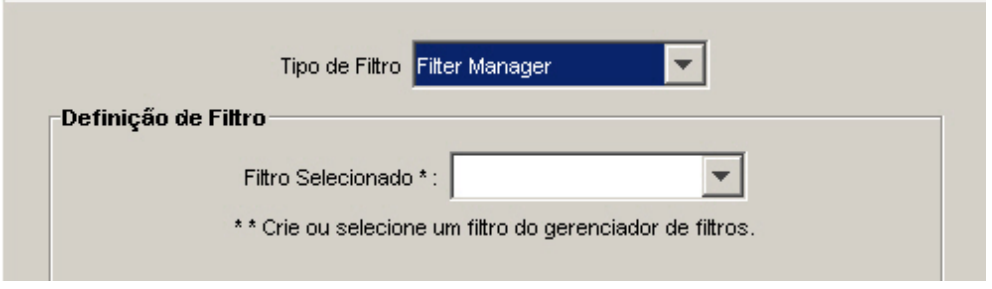
Criando uma regra de correlação básica

Crie uma regra de correlação básica quando quiser contar o número de vezes que certas condições são atendidas dentro de determinado período de tempo. As etapas são:

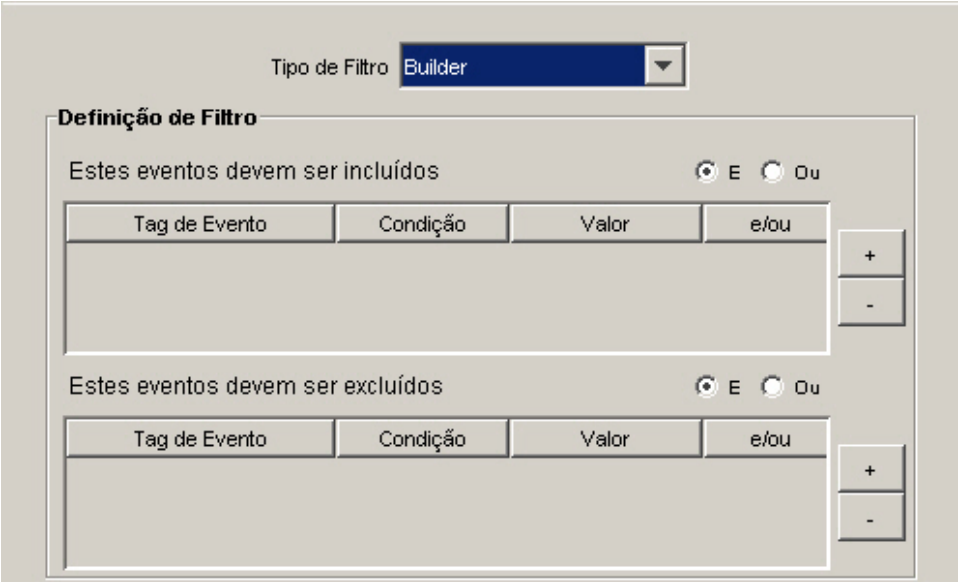
- Selecione Regra de Correlação Básica na primeira janela do Assistente de Regras de Correlação. Preencha as informações para:
  - Nome da Regra - nome que aparecerá na lista de regras. O número máximo de caracteres é 255, não sendo permitido o uso de pontos. Caracteres ASCII estendidos não são permitidos. O nome da Regra diferencia maiúsculas de minúsculas.
  - Descrição – Breve descrição. O tamanho máximo do texto descritivo é de 1024 caracteres.
- Tipo de Filtro
  - Permitir Tudo
  - Padrão



  - Gerenciador de Filtros - ({id do proprietário}:{nome do Filtro}:<nome do Campo>



- Construtor



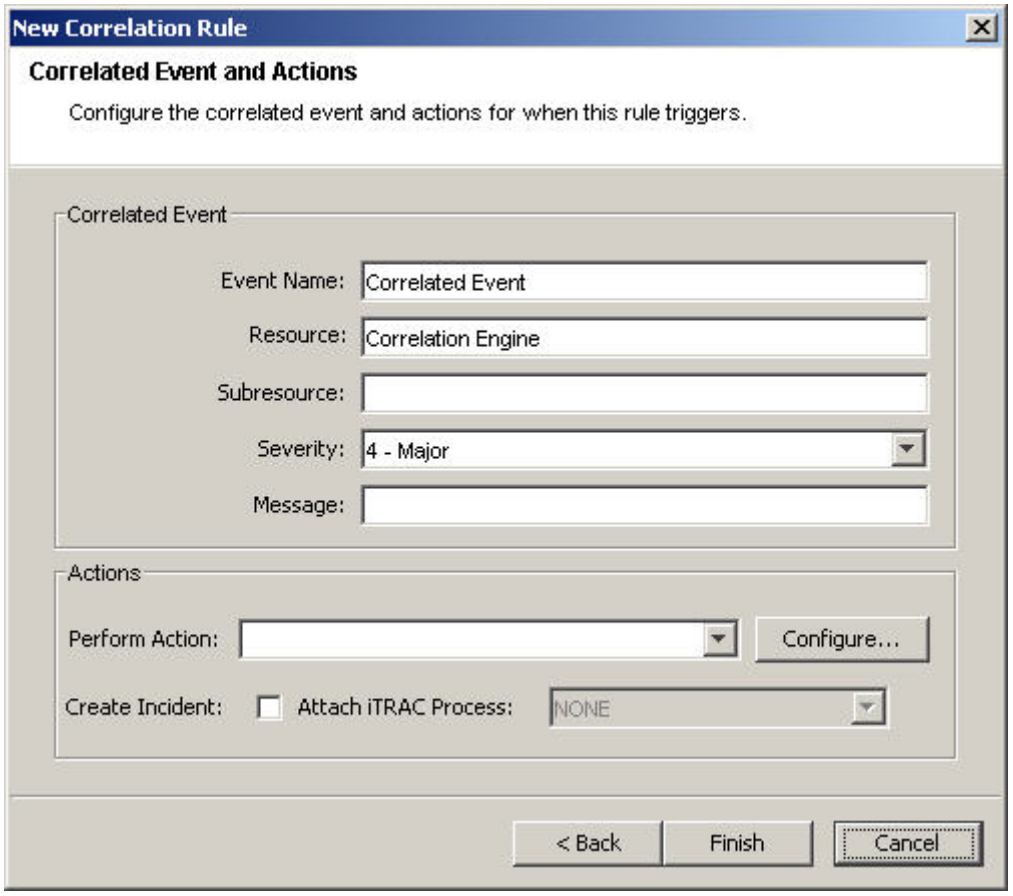
- Critérios de Limite e Agrupamento (metade superior da janela) - Ativar Regra: - Essa opção permite inserir critérios de "correspondência" para vários eventos que entram no sistema em um determinado período de tempo.
  - Quando a condição é atendida _vezes - Padrão: 1. Uma regra é acionada somente depois de ter sido detectada pelo número de vezes especificado. A faixa válida de entradas para esse valor limite é 1 ou maior.
  - dentro de (período de tempo) - Padrão: 60 segundos. Isso limitará a condição para o período de tempo. Essa é uma entrada de variável combinada e uma lista suspensa. As opções da lista suspensa são: segundos, minutos, horas e dias.

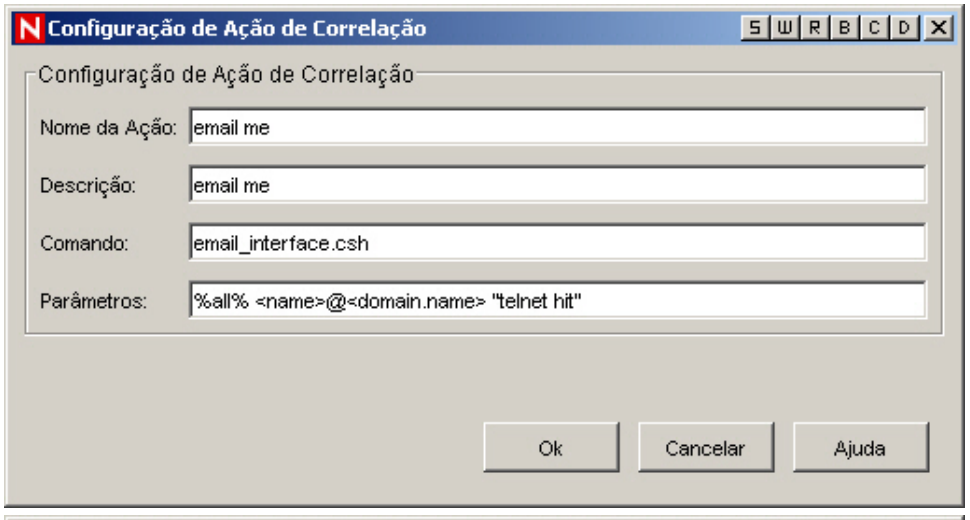
NOTA: Quando o período de tempo é 0, o acionador é considerado como instantâneo. Para a Correlação Básica, o evento acontecerá no máximo uma vez para um período de tempo instantâneo.

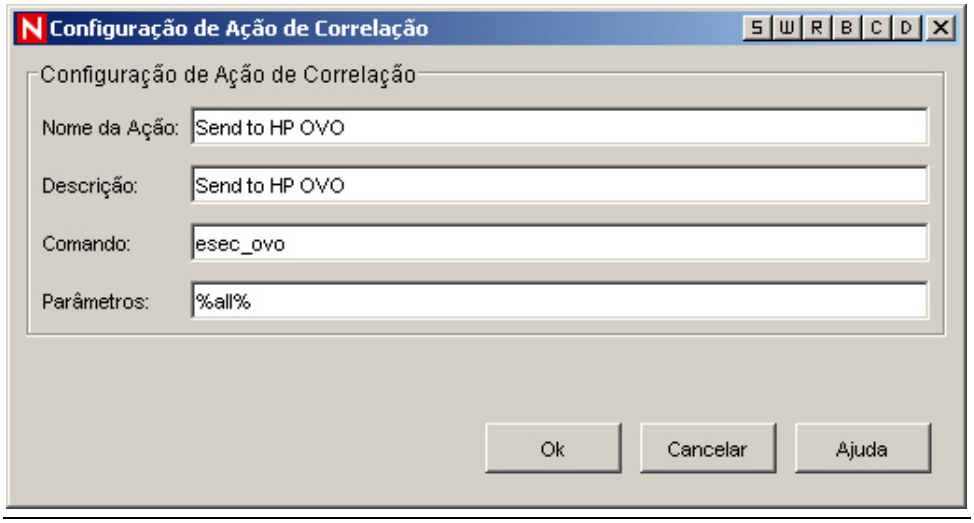
- Página Critérios de Limite e Agrupamento (metade inferior da janela) - Correlaciona combinações distintas das tags META a seguir - Selecione as tags META a serem usadas em combinação para a correlação. Os eventos são colocados em grupos com base nas tags META selecionadas.

- Página Eventos e Ações Correlacionados - Esse painel define que ação será realizada automaticamente quando os eventos corresponderem a essa regra de correlação. A única entrada necessária é o nível de gravidade, que, por padrão, é o nível 4.
  - Nome do Evento – Padrão: Evento Correlacionado. Esse é o nome de texto do evento correlacionado.
  - Recurso - Padrão: Mecanismo de Correlação. Esse é o nome de texto de um recurso no sistema.
  - Sub-recurso - Padrão: <nenhum>. Esse é o nome do sub-recurso para os recursos com vários sub-recursos
  - Definir nível de gravidade como - Padrão: 4. Esse é o nível de gravidade para o qual o evento será designado. Os valores válidos são 0, 1, 2, 3, 4 (padrão) e 5. Uma lista suspensa é fornecida com os níveis de gravidade válidos.

- Texto de mensagem personalizado - Padrão: <nenhum>. Esse é o texto que aparecerá com o evento. Ele é útil na identificação da condição que acionou a Regra de Lista de Avisos. O número máximo de caracteres é 4.000. O texto que você digita nessa caixa é incluído antes do texto do evento de correlação com um separador de pipe. Por exemplo, a entrada de "Nova mensagem" resultaria na mensagem correlacionada "Nova mensagem|Três instâncias de ...".
- Executar esse comando (somente Oracle) - Default: <nenhum>. Esse é o nome de um arquivo que é executado ao ser acionada a regra de Lista de Avisos. O arquivo deve estar no diretório $ESEC_HOME/sentinel/exec e deve ser executável pelo usuário esecadm. Não há validação de entrada nessa caixa de texto de formato livre. Você pode especificar as tags META que deseja enviar ao executável.
- Executar Ação (somente MSSQL) - Padrão: <nenhum>. Esse é o nome de um arquivo executável que é executado ao ser acionada a regra. O arquivo deve estar no diretório %ESEC_HOME%\sentinel\bin e deve ser executável pelo usuário esecadm. Não há validação de entrada. Você pode especificar as tags META que deseja enviar ao executável. A seguir estão dois exemplos de uma regra de correlação que envia um e-mail e uma regra de correlação que envia o evento de correlação ao HP OVO.







NOTA: Para obter mais informações sobre Comandos e Parâmetros, consulte o Capítulo 5 – Meta Tags do Assistente e do Sentinel no Guia de Referência do Usuário e Seção de saída de correlação.

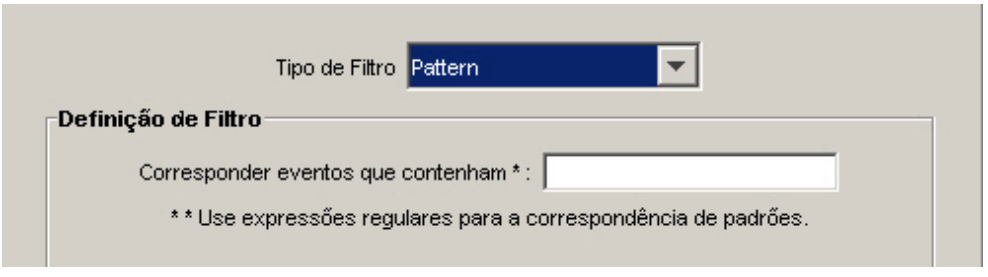
- Criar Incidente – Uma ação de um evento correlacionado também pode ser a criação de um incidente.
- Anexar processo do iTrac – O incidente criado pode ter um processo iTrac anexado

Criando uma regra de correlação avançada

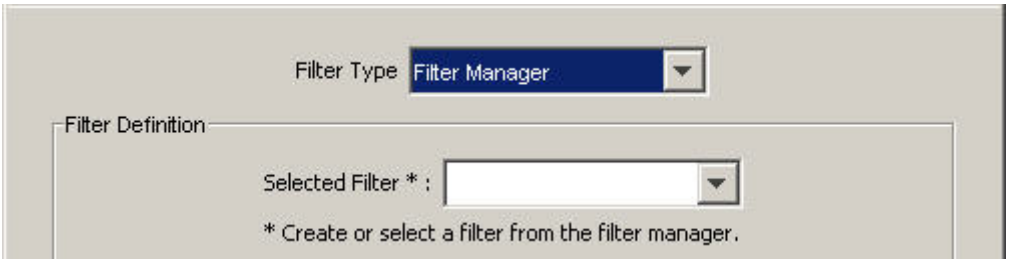
Uma Regra de Correlação Avançada permite tornar a regra mais complexa com a adição de uma nova condição na janela Critérios Adicionais, na verdade acrescentando um nível de logical AND à definição da regra.

Crie uma regra de correlação avançada quando quiser não apenas contar o número de vezes que certas condições são atendidas, mas também receber um alerta quando os eventos também satisfizerem critérios que envolvam eventos passados. As etapas são:

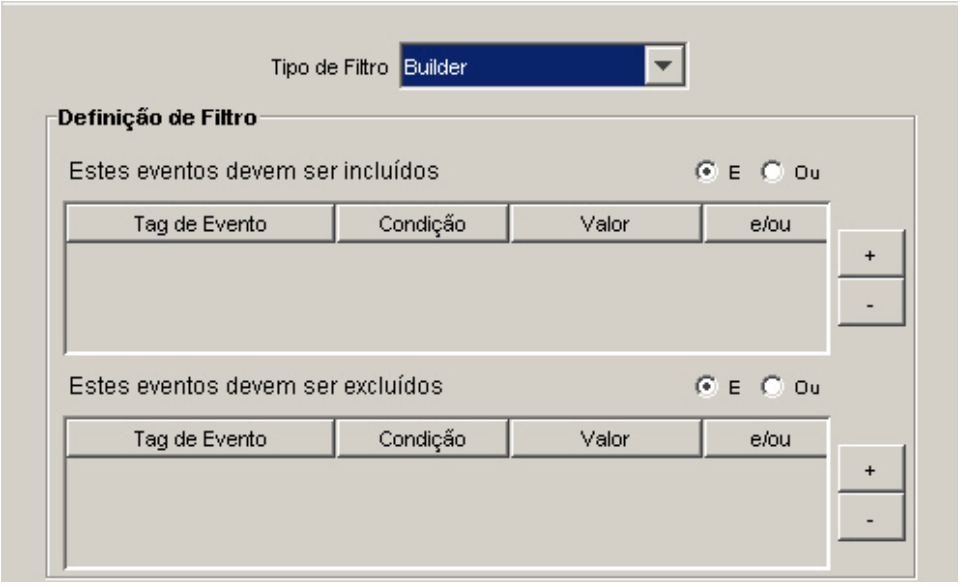
- Selecione Regra de Correlação Avançada na primeira janela do Assistente de Regras de Correlação. Preencha as informações para:
  - Nome da Regra - nome que aparecerá na lista de regras. O número máximo de caracteres é 255, não sendo permitido o uso de pontos. Caracteres ASCII estendidos não são permitidos. O nome da Regra diferencia maiúsculas de minúsculas.
  - Descrição – Breve descrição. O tamanho máximo do texto descritivo é de 1024 caracteres.
- Tipo de Filtro
  - Permitir Tudo
  - Padrão



  - Gerenciador de Filtros - ({id do proprietário}:{nome do Filtro}:<nome do Campo>



- Construtor



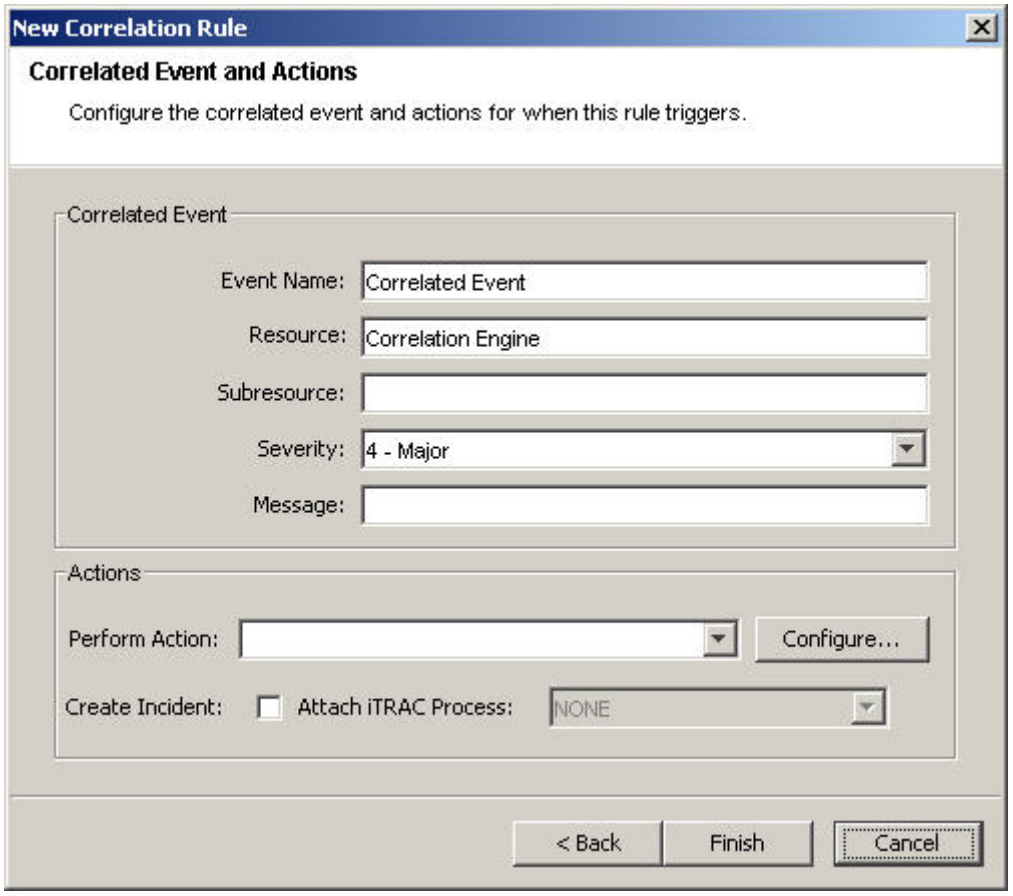
- Critérios Adicionais - Essa opção permite inserir critérios de "correspondência" para vários eventos que entram no sistema em um determinado período de tempo. O tempo padrão é de 60 segundos. Essa é uma entrada de variável combinada e uma lista suspensa. As opções da lista suspensa são: segundos, minutos, horas e dias.
- Critérios de Limite e Agrupamento (metade superior da janela) - Ativar Regra: - Essa opção permite inserir critérios de "correspondência" para vários eventos que entram no sistema em um determinado período de tempo.
  - Quando a condição é atendida _vezes - Padrão: 1. Uma regra é acionada somente depois de ter sido detectada pelo número de vezes especificado. A faixa válida de entradas para esse valor limite é 1 ou maior.
  - dentro de (período de tempo) - Padrão: 60 segundos. Isso limitará a condição para o período de tempo. Essa é uma entrada de variável combinada e uma lista suspensa. As opções da lista suspensa são: segundos, minutos, horas e dias.

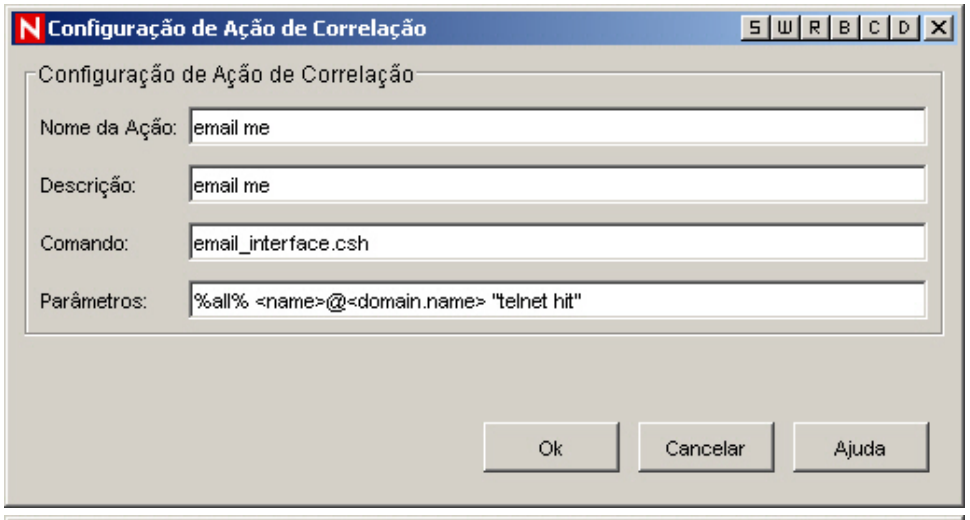
NOTA: Quando o período de tempo é 0, o acionador é considerado como instantâneo. Para a Correlação Básica, o evento acontecerá no máximo uma vez para um período de tempo instantâneo.

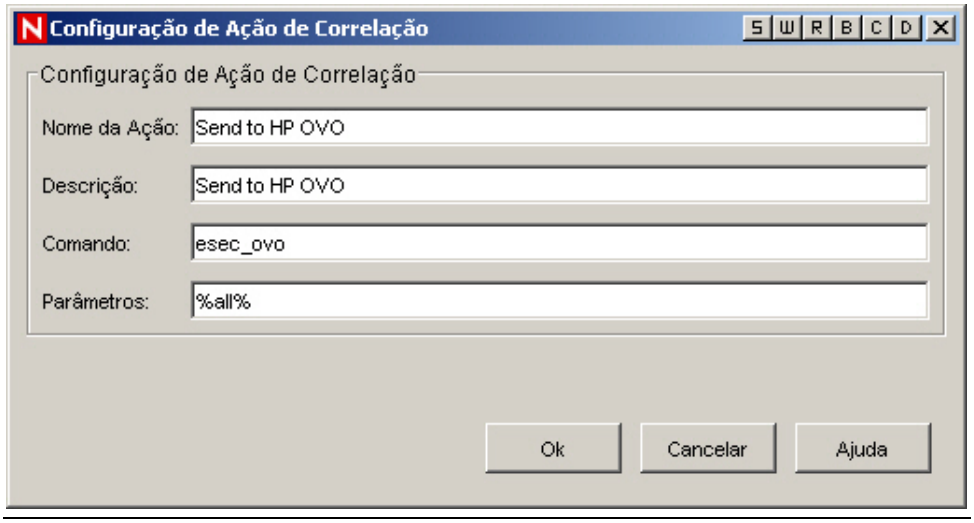
- Página Critérios de Limite e Agrupamento (metade inferior da janela) - Correlacione combinações distintas das seguintes tags META - Selecione as tags META a serem usadas em combinação para a correlação. Os eventos são colocados em grupos com base nas tags META selecionadas.

- Página Eventos e Ações Correlacionados - Esse painel define que ação será realizada automaticamente quando os eventos corresponderem a essa regra de correlação. A única entrada necessária é o nível de gravidade, que, por padrão, é o nível 4.
  - Nome do Evento – Padrão: Evento Correlacionado. Esse é o nome de texto do evento correlacionado.
  - Recurso - Padrão: Mecanismo de Correlação. Esse é o nome de texto de um recurso no sistema.
  - Sub-recurso - Padrão: <nenhum>. Esse é o nome do sub-recurso para os recursos com vários sub-recursos
  - Definir nível de gravidade como - Padrão: 4. Esse é o nível de gravidade para o qual o evento será designado. Os valores válidos são 0, 1, 2, 3, 4 (padrão) e 5. Uma lista suspensa é fornecida com os níveis de gravidade válidos.

- Texto de mensagem personalizado - Padrão: <nenhum>. Esse é o texto que aparecerá com o evento. Ele é útil na identificação da condição que acionou a Regra de Lista de Avisos. O número máximo de caracteres é 4.000. O texto que você digita nessa caixa é incluído antes do texto do evento de correlação com um separador de pipe. Por exemplo, a entrada de "Nova mensagem" resultaria na mensagem correlacionada "Nova mensagem|Três instâncias de ...".
- Executar esse comando (somente Oracle) - Default: <nenhum>. Esse é o nome de um arquivo que é executado ao ser acionada a regra de Lista de Avisos. O arquivo deve estar no diretório $ESEC_HOME/sentinel/exec e deve ser executável pelo usuário esecadm. Não há validação de entrada nessa caixa de texto de formato livre. Você pode especificar as tags META que deseja enviar ao executável.
- Executar Ação (somente MSSQL) - Padrão: <nenhum>. Esse é o nome de um arquivo executável que é executado ao ser acionada a regra. O arquivo deve estar no diretório %ESEC_HOME%\sentinel\bin e deve ser executável pelo usuário esecadm. Não há validação de entrada. Você pode especificar as tags META que deseja enviar ao executável. A seguir estão dois exemplos de uma regra de correlação que envia um e-mail e uma regra de correlação que envia o evento de correlação ao HP OVO.







NOTA: Para obter mais informações sobre Comandos e Parâmetros, consulte o Capítulo 5 – Tags META do Assistente e do Sentinel no Guia de Referência do Usuário e Seção de Saída de Correlação.

- Criar Incidente – Uma ação de um evento correlacionado também pode ser a criação de um incidente.
- Anexar processo do iTrac – O incidente criado pode ter um processo iTrac anexado.

Criando uma regra de correlação RuleLg em formato livre

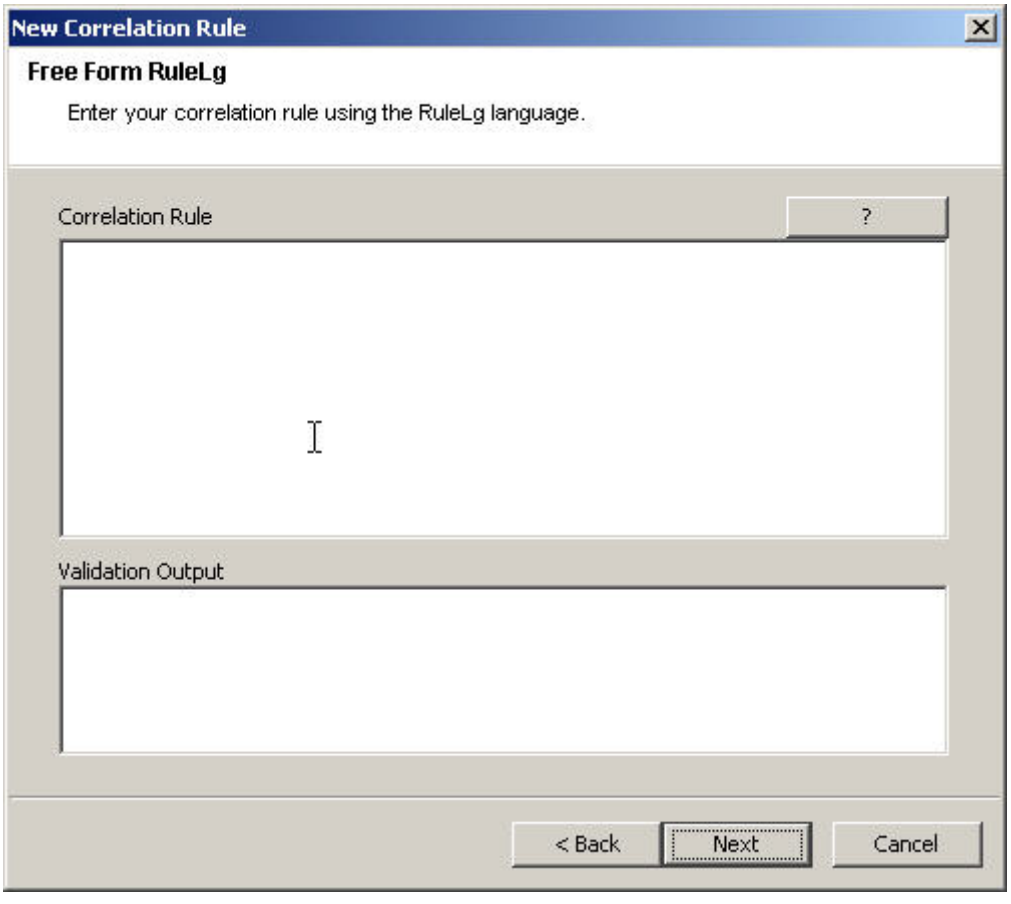
O Mecanismo de Correlação se baseia em três operações fundamentais. Essas operações são combinadas para formar uma regra com operadores de fluxo, união e interseção. As três operações fundamentais são:

- Operação de filtro
- Operação de janela
- Operação de acionador

ATENÇÃO: Se renomear uma tag, não use o nome original ao criar uma regra de correlação.

A linguagem de regras reflete diretamente essas operações e a maneira como elas podem ser combinadas de modo intuitivo para definir as regras de correlação. Cada operação foi projetada e implementada especificamente para proporcionar alto desempenho, e funciona em relação a um conjunto de eventos: ela recebe como entrada um conjunto de eventos e retorna um conjunto de eventos. O evento atual processado por uma regra normalmente tem um significado especial para a semântica da linguagem. O evento atual sempre faz parte do conjunto de eventos dentro e fora de uma operação, a menos que o conjunto esteja vazio. Se um conjunto de entrada de uma operação estiver vazio, a operação não será avaliada.

De modo simplificado, uma regra de correlação processa os eventos que chegam ao Mecanismo de Correlação em série, um por um. Na realidade, o Mecanismo de Correlação pode processar vários eventos e avaliar várias regras em relação a um evento simultaneamente.



Operação de filtro

Uma operação de filtro (expressão booleana) permite a filtragem de acordo com o conteúdo do evento atual; ou seja, seus valores de tags META e a expressão booleana especificada pelo filtro. A saída de um filtro pode ser um conjunto vazio (se o evento atual não correspondia ao

filtro) ou um conjunto que contenha o evento atual e todos os outros eventos do conjunto de entrada.

- Os filtros operam no evento atual, avaliando a expressão booleana desse evento:
  - A operação do filtro retornará o conjunto de entrada se a expressão booleana for avaliada como verdadeira.
  - A operação do filtro retornará o conjunto vazio se a expressão booleana for avaliada como falsa.
- A expressão booleana é uma composição de instruções de comparação e instruções de correspondência com os operadores booleanos 'e', 'ou' e 'não'.

Operação de filtro - Precedência do operador de RuleLg e associações

Precedência do operador booleano de filtro (do mais alto [superior] para o mais baixo [inferior]):

Operador	Significado	Tipo de operador	Associatividade
não	Não lógico	unário	nenhum
e	E lógico	binário	esquerda para a direita
ou	Ou lógico	binário	esquerda para a direita

Os seguintes itens são aplicáveis:

- As instruções de comparação permitem a avaliação de valores de tags META de eventos com restrições ou outros valores de tags META de eventos.
- Os operadores de comparação disponíveis são =, !=, >, <, >=, <=.
- As instruções de correspondência disponíveis são expressões regulares de correspondência, match regex(), ou sub-redes de correspondência, match subnet().
- É possível aninhar as instruções de comparação e correspondência por meio de parênteses, em qualquer profundidade.
- Os nomes de tags META em instruções de comparação e correspondência sempre devem ter o prefixo "e." para especificar o evento atual.
- Se um filtro for a última ou única operação de uma regra de correlação, o conjunto de saída do filtro será usado para construir um evento correlacionado (os eventos correlacionados são o conjunto de eventos de saída da operação de filtro com o evento atual em primeiro lugar).
- Se um filtro não for a última operação de uma regra de correlação (ou seja, se um operador de fluxo estiver à sua direita), o conjunto de saída de um filtro será usado como conjunto de entrada para outras operações (por meio do operador de fluxo).

Por exemplo: se o evento atual tiver a severidade 4 e a tag META de recurso contiver "FW" ou "Comm", um evento correlacionado será enviado com o evento atual (evento único) listado como o evento correlacionado.

```
filter(e.sev = 4 and (e.res match regex("FW") or e.res
   match regex("Comm")))
```

Outro exemplo: se qualquer tag META do evento atual contiver "ABC", um evento correlacionado será enviado com o evento atual (evento único) listado como o evento correlacionado.

```
filter(e.all match regex("ABC"))
```

Operação de janela

Uma operação de janela (expressão booleana simples[,expressão de filtro],int duration) funciona no evento atual em relação a uma janela de eventos passados. Os eventos passados são mantidos pela própria operação de janela. A saída de uma janela pode ser o conjunto vazio (se o evento atual não correspondia à expressão booleana simples) ou um conjunto que contenha o evento atual e todos os outros eventos passados para os quais essa expressão seja verdadeira.

A expressão booleana simples pode ser uma instrução de comparação única ou uma instrução de correspondência única de um valor de tag META de evento passado com uma constante ou um valor de tag META de evento atual. Para expressões booleanas:

- Você deve acrescentar ao nome de uma tag META o prefixo "e." para especificar o evento atual ou "w." para especificar os eventos passados
- Os operadores de comparação disponíveis são =, !=, >, <, >=, <=, em e não em
- As instruções de correspondência disponíveis são expressões regulares de correspondência, match regex(), ou sub-redes de correspondência, match subnet()
- Uma "w.[tag META]" deve existir em uma expressão booleana simples de janela
- Se algum evento passado for avaliado como verdadeiro com o evento atual para a expressão booleana simples, o conjunto de saída será o evento de entrada, juntamente com todas as correspondências na janela
- Se nenhum evento na janela corresponder ao evento atual para a expressão booleana simples, um conjunto vazio será a saída

Os eventos passados são mantidos pela duração especificada da operação de janela.

O parâmetro opcional de expressão de filtro de uma janela permite que você controle os eventos mantidos pela janela. Essa expressão pode ser qualquer filtro válido.

- Cada evento de entrada no Mecanismo de Correlação que passa por esse filtro é colocado na janela de eventos passados
- Se não houver uma expressão de filtro, todos os eventos de entrada no Mecanismo de Correlação serão mantidos pela janela
- O evento atual só é colocado na janela após a conclusão da avaliação da janela do evento atual.
- Somente as partes relevantes dos eventos passados são realmente mantidas pela janela (para diminuir a utilização da memória)

Se uma janela for a última ou única operação de uma regra de correlação, o conjunto de saída da janela será usado para construir um evento correlacionado (os eventos correlacionados são o conjunto de eventos da saída da operação de janela, com o evento atual em primeiro lugar).

Exemplo 1

```
window(e.sip = w.sip, filter(e.sip match subnet
   (<xxx.xxx.x.x/yy>)), 60)
```

No exemplo acima, se o evento atual tiver um endereço IP de origem no endereço especificado xxx.xxx.x.x/yy com máscara de sub-rede CIDR e corresponder a algum evento ocorrido nos últimos 60 segundos, um evento correlacionado será enviado com o evento atual e quaisquer eventos passados correspondentes como os eventos correlacionados (com o evento atual em primeiro lugar).

Exemplo 2

```
window(e.sip = w.dip, 3600) intersection
window(e.dp = w.dp, 3600) intersection
window(e.evt = w.evt, 3600)
```

A regra acima é do tipo dominó. Um invasor explora um sistema vulnerável, utilizando-o como uma plataforma de ataque.

Exemplo 3

```
filter(e.sev > 3) flow (window(e.sip = w.sip, filter
   (e.sev >3), 5) intersection window(e.evt = w.evt,
   filter(e.sev >3), 5) intersection window(e.dip =
   w.dip, filter(e.sev >3), 5) intersection window(e.sn!
   = w.sn, filter(e.sev > 3),5)
```

O exemplo acima é um tipo de regra interna/externa. Uma assinatura de ataque é vista em dois sistemas de detecção de intrusão, um dentro de um firewall e o outro fora, e a severidade do ataque é superior a 3.

Operação do acionador

O principal objetivo de uma operação de acionador é contar um número de eventos por determinada duração. Se o total especificado for atingido dentro da duração especificada, um conjunto de eventos que contenham todos os eventos mantidos pelo acionador será gerado como saída; caso contrário, a saída será o conjunto vazio.

- A operação do acionador recebe como entrada um conjunto de eventos a ser retornado como parte do conjunto de eventos de saída, se o total especificado, a duração e o(s) discriminador(es) dos conjuntos de entrada anteriores e o conjunto de entrada atual corresponderem aos critérios definidos pela operação do acionador.
- O total é um valor inteiro que especifica o número de eventos que precisam ocorrer dentro da janela de duração para gerar um conjunto não vazio como saída.
- A duração é um valor inteiro em segundos que especifica a duração pela qual os eventos são mantidos pela operação do acionador.
- Se a duração for igual a zero, uma operação de acionador apenas comparará o número de eventos no conjunto de entrada com o total e gerará como saída o evento atual, se esse número for maior ou igual ao total.
- Ao receber um novo conjunto de eventos de entrada, o acionador primeiro descarta os eventos desatualizados (eventos mantidos por um período maior que a duração) e, em seguida, insere o evento atual. Se o número de eventos resultantes for maior ou igual ao total especificado, o acionador gerará como saída um conjunto que conterá todos os eventos.
- Se um acionador for a última ou a única operação de uma regra de correlação, o conjunto de saída do acionador será usado para construir um evento correlacionado (os eventos correlacionados são o conjunto de eventos da saída da operação de acionador, com o evento atual em primeiro lugar).
- Se um acionador não for a última operação de uma regra de correlação (ou seja, se um operador de fluxo estiver à sua direita), o conjunto de saída de um acionador será usado como conjunto de entrada para outras operações (por meio do operador de fluxo).

- Depois que os critérios de operação do acionador forem atendidos pela primeira vez (e, assim, a operação do acionador gerar um conjunto de eventos como saída), se os critérios forem atendidos novamente, contendo pelo menos um dos eventos previamente gerados como saída, e o acionador for a última (ou a única operação), o Mecanismo de Correlação não construirá um novo evento correlacionado; em vez disso, construirá uma atualização para o evento correlacionado anterior.
- O discriminador (lista de tags META) é uma lista de tags META delimitada por vírgulas. Uma operação de acionador mantém diferentes contagens para cada combinação distinta das tags META do discriminador.

Por exemplo, se cinco eventos com o mesmo endereço IP de origem ocorrerem em 10 segundos, envie um evento correlacionado com os cinco eventos como os eventos correlacionados (com o evento atual em primeiro lugar).

```
trigger(5,10,discriminator(e.sip))
```

Embora o uso da opção de regra de formato livre permita criar expressões de complexidade ilimitada, essas regras podem não fazer sentido. O formato normal suportado de uma expressão de RuleLg é dividido em três partes: a seção de filtro, a seção de janela e a seção de acionador. As três seções são conectadas com um operador de fluxo.

A seção de filtro pode conter vários filtros conectados.

Por exemplo:

```
(filter(e.sev = 5) union filter(e.sev =4))
(filter(e.sev = 5 or e.sev =4))
```

NOTA: Essa seção é opcional. Quando omitida, é equivalente a filter(1=1).

A seção de janela pode conter várias janelas em interseção.

Por exemplo:

(window(w.sev = e.sev,10) intersection window(w.sip = e.sip,10))

NOTA: Essa seção é opcional.

A seção de acionador pode conter uma operação de acionador.

Exemplo

```
(trigger(5,10))
```

NOTA: Essa seção é opcional. Quando omitida, a regra se comporta como se terminasse com trigger(1,0).

Operadores que são combinados a operações para formar regras

Os operadores que são combinados a operações para formar regras são:

- Operador de fluxo
- Operador de união
- Operador de interseção

A precedência do operador de filtro, de janela e de acionador (do mais alto [superior] para o mais baixo [inferior]) é:

Operador	Significado	Tipo de operador	Associatividade
fluxo	O conjunto de saída torna-se o conjunto de entrada	binário	esquerda para a direita
interseção	definir interseção (remover duplicatas)	binário	esquerda para a direita
união	definir união (remover duplicatas)	binário	esquerda para a direita

Operador de fluxo

O conjunto de eventos de saída da operação da esquerda é o conjunto de eventos de entrada referente à operação da direita.

Por exemplo:

```
filter(e.sev = 5) flow trigger(3, 60)
```

A saída de uma operação de filtro é a entrada de uma operação de acionador. O acionador só conta eventos com severidade igual a 5.

Operador de união

A união do conjunto de saída da operação da esquerda e do conjunto de saída da operação da direita. O conjunto de saída resultante contém eventos do conjunto de saída da operação da esquerda ou do conjunto de saída da operação da direita, sem duplicatas.

Por exemplo:

```
filter(e.sev = 5) union filter(e.sip = 192.168.0.1)
```

é equivalente a

```
filter(e.sev = 5 or e.sip = 192.168.0.1)
```

Operador de interseção

A interseção do conjunto de saída da operação da esquerda e do conjunto de saída da operação da direita. O conjunto de saída resultante contém eventos comuns ao conjunto de saída da operação da esquerda e ao conjunto de saída da operação da direita, sem duplicatas.

Por exemplo:

```
filter(e.sev = 5) intersection filter(e.sip =
   192.17.16.32)
```

é equivalente a

```
filter(e.sev = 5 and e.sip = 192.17.16.32)
```

Exemplo de regras de correlação

Esse documento fornece um conjunto de regras de correlação com base em regras de exemplo, assim como os pré-requisitos (exigências) necessários para que as regras sejam eficientes. As regras podem ser diferentes, dependendo da configuração do seu sistema.

As tags e.rv50 a e.rv53 que estão nos exemplos RuleLg correspondem ao conjunto de mapeamentos no seu Coletor de arquivos de mapeamento. Por exemplo, se você abrir o arquivo windows_v2000_mapv*.csv ou snort_v20_mapv*.csv, a:

- coluna Cultura corresponde a e.rv50
- coluna Família corresponde a e.rv51
- coluna Família corresponde a e.rv52
- coluna Evento corresponde a e.rv53

Por exemplo:

```
filter (e.rv52 = "Worm") flow trigger (3, 300)
```

Essa regra refere-se à taxonomia NIDS. Se observar a coluna Família no arquivo snort de mapeamento, você encontrará cerca de quarenta exemplos da palavra Worm. Essa regra será acionada com mais de quarenta ataques diferentes de worm se eles ocorrerem três vezes durante o período de cinco minutos.

Os seguintes exemplos de regras de correlação de tipos de ataques são fornecidos.

- Força bruta - mesma origem e alvo
- Overflow de buffer - mesma origem para mesmo alvo
- Overflow de buffer - interrupção do serviço
- Negação do serviço
- Falhas de login - de qualquer origem para qualquer destino
- Falhas de login - da mesma origem para o mesmo destino
- Microsoft - login anônimo
- Microsoft - autenticação geral do windows
- Microsoft - IE
- Microsoft – IIS
- Microsoft - Autenticação do gerenciador de LAN
- Microsoft – MDAC
- Microsoft - registro de acesso remoto
- Microsoft - Servidor SQL
- Microsoft - NETBIOS
- Microsoft - criação de script do Windows
- Várias portas de fundo - origens diferentes
- Várias portas de fundo - origem única
- Cavalo de tróia
- UNIX - servidor Apache web
- UNIX - BIND/DNS
- UNIX - FTP
- UNIX - UNIX geral
- UNIX - line printer daemon
- UNIX - procedimento de discagem remota
- UNIX - serviços remotos
- UNIX - shell de segurança
- UNIX - sendmail
- UNIX – SNMP
- Epidemia de vírus
- Epidemia de worm

Ataque de overflow de buffer e interrupção de serviço

Essa regra identificará uma violação de segurança potencial após um ataque de overflow de buffer. Essa regra alertará se o destino de um ataque de overflow de buffer sofrer uma interrupção de serviço dentro de 60 segundos após um ataque. Um Coletor com base em host, HIDS/OS, pode detectar se um serviço for interrompido. Um ataque de overflow de buffer pode ser detectado por um Coletor NIDS, HIDS ou OS.

Se um sistema foi afetado por esse ataque de overflow de buffer, esse evento deverá ser investigado.

Frequência da regra	Requisitos da regra	Taxonomia da regra
1 vez	Defina os seguintes itens antes de implementar essa regra: ▪ Plataformas de rede IDS que a taxonomia do Sentinel pode traduzir (consulte a tabela Taxonomia NIDS para obter mais informações) ▪ Plataformas host IDS que a taxonomia do Sentinel pode traduzir (consulte a tabela Taxonomia HIDS & OS para obter mais informações)	NIDS HIDS/OS

RuleLg para essa regra

```
filter ((e.rv51 = "Service" and e.rv52 = "Stop" ) and
   (e.st = "H")) flow window (w.dip = e.sip, filter
   (e.rv52 = "Buffer_Overflow"), 60) flow trigger(1, 0)
```

Ataque de negação de serviço e interrupção de serviço

Esta regra identificará uma violação de segurança potencial após um ataque de negação de serviço. Essa regra alertará se o destino de um ataque de negação de serviço interromper um serviço no período de 60 segundos após um ataque. A interrupção do serviço é detectada por um Coletor com base em host, ou seja, HIDS/OS. Um ataque de overflow de buffer pode ser detectado por Coletores NIDS, HIDS ou OS.

Se um sistema foi afetado por um ataque de negação de serviço, esse evento deverá ser investigado.

Frequência da regra	Requisitos da regra	Taxonomia da regra
1 vez	Defina os seguintes itens antes de implementar essa regra: ▪ Plataformas de rede IDS que a taxonomia do Sentinel pode traduzir (consulte a tabela Taxonomia NIDS para obter mais informações) ▪ Plataformas host IDS que a taxonomia do Sentinel pode traduzir (consulte a tabela Taxonomia HIDS & OS para obter mais informações)	NIDS HIDS/OS

RuleLg para essa regra

```
filter ((e.rv51 = "Service" and e.rv52 = "Stop" ) and
   (e.st = "H")) flow window (w.dip = e.sip, filter
   (e.rv52 ="DoS" ), 60) flow trigger(1, 0)
```

Detecção de epidemia de vírus

Esta regra identificará se um vírus conhecido está atacando qualquer sistema em uma infra-estrutura.

Quando um vírus ataca, geralmente um ou vários sistemas são prejudicados, exigindo um recarregamento completo dos dados do sistema e dos aplicativos, ou acarretando a perda

completa de bens corporativos. A identificação de um vírus em progresso pode reduzir significativamente ou evitar o prejuízo.

Frequência da regra	Requisitos da regra	Taxonomia da regra
3 vezes em 5 minutos	Defina os seguintes itens antes de implementar essa regra: ▪ Plataformas de rede IDS que a taxonomia do Sentinel pode traduzir (consulte a tabela Taxonomia NIDS para obter mais informações)	NIDS

RuleLg para essa regra

```
filter (e.rv52 ="Virus") flow trigger (3, 300)
```

Detecção de epidemia de worm

Esta regra identificará se um worm conhecido está atacando qualquer sistema em uma infra-estrutura.

Quando um worm ataca, geralmente um ou vários sistemas são prejudicados, exigindo um recarregamento completo dos dados do sistema e dos aplicativo, ou acarretando a perda completa de bens corporativos. A identificação de um worm em progresso pode reduzir significativamente a responsabilidade da empresa.

Frequência da regra	Requisitos da regra	Taxonomia da regra
3 vezes em 5 minutos	Defina os seguintes itens antes de implementar essa regra: ▪ Plataformas de rede IDS que a taxonomia do Sentinel pode traduzir (consulte a tabela Taxonomia NIDS para obter mais informações)	NIDS

RuleLg para essa regra

```
filter (e.rv52 = "Worm") flow trigger (3, 300)
```

Detecção de cavalo de tróia

Esta regra identificará se um cavalo de tróia foi implantado em qualquer sistema da infra-estrutura.

Quando um cavalo de tróia tem êxito, o sistema atingido pode ser totalmente comprometido.

Frequência da regra	Requisitos da regra	Taxonomia da regra
3 vezes em 5 minutos	Defina os seguintes itens antes de implementar essa regra: ▪ Plataformas de rede IDS que a taxonomia do Sentinel pode traduzir (consulte a tabela Taxonomia NIDS para obter mais informações) ▪ Plataformas host IDS que a taxonomia do Sentinel pode traduzir (consulte a tabela Taxonomia HIDS & OS para obter mais informações)	NIDS HIDS/OS

RuleLg para essa regra

```
filter (e.rv52 ="Trojan") flow trigger (3, 500)
```

Várias tentativas de backdoor de uma origem única

Esta regra correlacionará várias tentativas para inserir ou executar um ataque de backdoor de uma origem única.

Um programa de backdoor geralmente é usado para obter o controle completo do sistema de destino, sendo então usado para iniciar outros ataques. Geralmente, essa regra identificará tentativas de um intruso que está procurando sistemas infectados ou tentando infectar um sistema.

Frequência da regra	Requisitos da regra	Taxonomia da regra
5 vezes em 2 minutos	Defina os seguintes itens antes de implementar essa regra: ▪ Plataformas de rede IDS que a taxonomia do Sentinel pode traduzir (consulte a tabela Taxonomia NIDS para obter mais informações) ▪ Plataformas host IDS que a taxonomia do Sentinel pode traduzir (consulte a tabela Taxonomia HIDS & OS para obter mais informações)	NIDS HIDS/OS

RuleLg para essa regra

```
filter (e.rv50 = "Attack" and e.rv52 = "Backdoor" ) flow
   trigger(5, 120, discriminator (e.sip))
```

Várias tentativas de backdoor de origens diferentes

Esta regra correlacionará várias tentativas para inserir ou executar um ataque de backdoor coordenado de sistemas diferentes com alvo em um único destino.

Um programa de backdoor geralmente é usado para obter o controle completo do sistema de destino, sendo então usado para iniciar outros ataques. Geralmente, essa regra identifica que:

- o sistema de destino foi comprometido
- o invasor está tentando explorar o sistema comprometido
- o invasor está tentando se ocultar por meio de um ataque coordenado
- ou o invasor sabe que o destino é vulnerável a esse tipo de ataque. Se esse for o caso, isso pode indicar que o invasor obteve informações de uma fonte interna.

Frequência da regra	Requisitos da regra	Taxonomia da regra
5 vezes em 2 minutos	Defina os seguintes itens antes de implementar essa regra: ▪ Plataformas de rede IDS que a taxonomia do Sentinel pode traduzir (consulte a tabela Taxonomia NIDS para obter mais informações) ▪ Plataformas host IDS que a taxonomia do Sentinel pode traduzir (consulte a tabela Taxonomia HIDS & OS para obter mais informações)	NIDS HIDS/OS

RuleLg para essa regra

```
filter (e.rv50 = "Attack" and e.rv52 = "Backdoor" ) flow
   trigger( 5, 120, discriminator(e.dip))
```

Várias falhas de login de qualquer origem para qualquer destino

Esta regra identificará falhas de login para o mesmo tipo de sistemas.

Falhas de login para os mesmos tipos de conta ou sistema podem indicar que o invasor possuía conhecimento prévio da rede e dos sistemas críticos nela localizados. Isso deve gerar um alarme. Quanto mais informações um invasor possuir, mais facilmente encontrará um sistema explorável.

Frequência da regra	Requisitos da regra	Taxonomia da regra
5 vezes em 2 minutos	Defina os seguintes itens antes de implementar essa regra: ▪ Plataformas de rede IDS que a taxonomia do Sentinel pode traduzir (consulte a tabela Taxonomia NIDS para obter mais informações)	NIDS

RuleLg para essa regra

```
filter ((e.rv52 = "Access" or e.rv52 = "Brute_Force") and
   e.rv51 = "User" and e.rv50 = "Attack") flow trigger
   (5, 120)
```

Várias falhas de login da mesma origem para o mesmo destino

Esta regra identificará várias falhas de login da mesma origem para o mesmo destino.

Falhas de login para os mesmos tipos de conta ou sistema podem indicar que o invasor possuía conhecimento prévio da rede e dos sistemas críticos nela localizados. Isso deve gerar um alarme. Quanto mais informações um invasor possuir, mais facilmente encontrará um sistema explorável.

Frequência da regra	Requisitos da regra	Taxonomia da regra
3 vezes em 5 minutos	Defina os seguintes itens antes de implementar essa regra: ▪ Plataformas de rede IDS que a taxonomia do Sentinel pode traduzir (consulte a tabela Taxonomia NIDS para obter mais informações)	NIDS

RuleLg para essa regra

```
filter ((e.rv52 = "Access" or e.rv52 = "Brute_Force") and
   e.rv51 = "User" and e.rv50 = "Attack") flow trigger
   (5, 120, discriminator (e.sip, e.dip))
```

Ataque de overflow de buffer da mesma origem para o mesmo destino

Esta regra identificará um ataque de overflow de buffer do mesmo endereço IP de origem para o mesmo endereço de destino.

Um ataque de overflow de buffer é o ataque mais comum na rede, sendo usado para desabilitar um sistema. Esses tipos de ataques só podem ser bloqueados no perímetro. O conhecimento sobre um sistema invasor pode ajudar a bloquear esse sistema.

Frequência da regra	Requisitos da regra	Taxonomia da regra
5 vezes em 3 minutos	Defina os seguintes itens antes de implementar essa regra: ▪ Plataformas de rede IDS que a taxonomia do Sentinel pode traduzir (consulte a tabela Taxonomia NIDS para obter mais informações) ▪ Plataformas host IDS que a taxonomia do Sentinel pode traduzir (consulte a tabela Taxonomia HIDS & OS para obter mais informações)	NIDS HIDS/OS

RuleLg para essa regra

```
filter (e.rv52 ="Buffer_Overflow" ) flow trigger (5, 180,
   discriminator (e.sip, e.dip))
```

Sucesso de ataque de força bruta quando a origem e o destino são os mesmos

Esta regra identificará um possível sistema comprometido com uma senha violada.

Tentativas constantes de usar combinações de nomes de usuário e senhas para obter acesso, seguidas de um eventual êxito no login, podem indicar que um invasor obteve acesso por meio de um ataque de força bruta. Se esse ataque tiver êxito, a conta acessada deverá ser cancelada.

Frequência da regra	Requisitos da regra	Taxonomia da regra
1 vez em 3 minutos	Defina os seguintes itens antes de implementar essa regra: ▪ Plataformas de rede IDS que a taxonomia do Sentinel pode traduzir (consulte a tabela Taxonomia NIDS para obter mais informações) ▪ Plataformas host IDS que a taxonomia do Sentinel pode traduzir (consulte a tabela Taxonomia HIDS & OS para obter mais informações)	NIDS HIDS/OS

RuleLg para essa regra

```
filter (e.rv53="Other" and rv52="Access" e.rv51 ="User"
   and e.rv50="Prob" and e.st = "H") flow window (w.dip =
   e.sip, filter (e.rv52="Brute Force" and
   e.rv50="Compromise"), 180) flow trigger(1, 180,
   discriminator(e.sip, e.dip))
```

Microsoft - Verificação de ataques do Internet Information Services (IIS)

Esta regra suporta os 10 maiores ataques SANS Microsoft em ataques Internet Information Service (IIS). Se estiver executando o aplicativo IIS da Microsoft, você poderá ser vulnerável a ataques.

Frequência da regra	Requisitos da regra	Taxonomia da regra
1 vez	Defina os seguintes itens antes de implementar essa regra: ▪ Plataformas de rede IDS que a taxonomia do Sentinel pode traduzir (consulte a tabela Taxonomia NIDS para obter mais informações)	NIDS

RuleLg para essa regra

```
filter (e.rv53 = "Sans_MS_IIS") flow trigger(1,60)
```

Microsoft - Ataque do Microsoft Data Access Conector (MDAC) - Verificação de ataque a serviços de dados remotos

Esta regra suporta os 10 maiores ataques SANS Microsoft em ataques MDAC. O uso de produtos Microsoft pode torná-lo vulnerável a ataques. O MDAC é uma ferramenta subjacente usada para integrar os produtos da Microsoft.

Frequência da regra	Requisitos da regra	Taxonomia da regra
1 vez	Defina os seguintes itens antes de implementar essa regra: ▪ Plataformas de rede IDS que a taxonomia do Sentinel pode traduzir (consulte a tabela Taxonomia NIDS para obter mais informações)	NIDS

RuleLg para essa regra

```
filter (e.rv53 = "Sans_MS_MDAC") flow trigger(1,60)
```

Microsoft – Ataques de SQL Server - Verificação de ataques de SQL Server

Esta regra suporta os 10 maiores ataques SANS Microsoft em SQL Server. O uso do Microsoft SQL Server pode causar vulnerabilidade a ataques. Há várias vulnerabilidades graves que permitem que invasores remotos obtenham informações sigilosas e conteúdo do banco de dados de alerta, comprometam servidores SQL e hosts de servidor.

Frequência da regra	Requisitos da regra	Taxonomia da regra
1 vez	Defina os seguintes itens antes de implementar essa regra: ▪ Plataformas de rede IDS que a taxonomia do Sentinel pode traduzir (consulte a tabela Taxonomia NIDS para obter mais informações)	NIDS

RuleLg para essa regra

```
filter (e.rv53 = "Sans_MS_SQLServer") flow trigger(1,60)
```

Microsoft - NETBIOS - Verificação de ataque a compartilhamentos de rede não protegidos do Windows

Esta regra suporta os 10 maiores ataques SANS Microsoft em NETBIOS. O uso de redes Microsoft com NETBIOS pode causar vulnerabilidade a ataques. O NETBIOS era o software de comunicações de rede original da Microsoft. As redes atuais da Microsoft não utilizam o NETBIOS como um meio de transporte.

Frequência da regra	Requisitos da regra	Taxonomia da regra
1 vez	Defina os seguintes itens antes de implementar essa regra: ▪ Plataformas de rede IDS que a taxonomia do Sentinel pode traduzir (consulte a tabela Taxonomia NIDS para obter mais informações)	NIDS

RuleLg para essa regra

```
filter (e.rv53 = "Sans_MS_NETBIOS") flow trigger(1,60)
```

Microsoft - Login anônimo - Verificação de ataque de seções nulas

Esta regra suporta os 10 maiores ataques SANS Microsoft em seções nulas. Se estiver usando o Microsoft Null Session, você poderá estar vulnerável a ataques. O usuário anônimo pode recuperar informações pela rede ou se conectar sem autenticação.

Frequência da regra	Requisitos da regra	Taxonomia da regra
1 vez	Defina os seguintes itens antes de implementar essa regra: ▪ Plataformas de rede IDS que a taxonomia do Sentinel pode traduzir (consulte a tabela Taxonomia NIDS para obter mais informações)	NIDS

RuleLg para essa regra

```
filter (e.rv53 = "Sans_MS_NullSessions") flow
   trigger(1,60)
```

Microsoft - Autenticação do gerenciador de LAN (LM) - Verificação de ataques de hash de LM fraco

Esta regra suporta os 10 maiores ataques SANS Microsoft em hash de LM fraco. O LM usa um esquema de criptografia muito mais fraco do que os protocolos de autenticação atuais da Microsoft (NTLM e NTLMv2), e as senhas do LM podem ser violadas em um curto período de tempo.

Frequência da regra	Requisitos da regra	Taxonomia da regra
1 vez	Defina os seguintes itens antes de implementar essa regra: ▪ Plataformas de rede IDS que a taxonomia do Sentinel pode traduzir (consulte a tabela Taxonomia NIDS para obter mais informações)	NIDS

RuleLg para essa regra

```
filter (e.rv53 = "Sans_MS_LM") flow trigger(1,60)
```

Microsoft - Verificação de ataque de autenticação geral do Windows

Esta regra suporta os 10 maiores ataques SANS Microsoft em senhas. Quando senhas fracas são descobertas, devem ser mudadas.

Frequência da regra	Requisitos da regra	Taxonomia da regra
1 vez	Defina os seguintes itens antes de implementar essa regra: ▪ Plataformas de rede IDS que a taxonomia do Sentinel pode traduzir (consulte a tabela Taxonomia NIDS para obter mais informações)	NIDS

RuleLg para essa regra

```
filter (e.rv53 = "Sans_MS_WeakPasswords") flow
   trigger(1,60)
```

Microsoft - Verificação de ataques no Internet Explorer (IE)

Esta regra suporta os 10 maiores ataques SANS Microsoft em IE. Versões mais recentes da Microsoft embutiram esse aplicativo na interface de usuário do sistema operacional. Ataques conhecidos com o IE podem resultar no comprometimento de qualquer ambiente da Microsoft posterior ao Windows 2000.

Frequência da regra	Requisitos da regra	Taxonomia da regra
1 vez	Defina os seguintes itens antes de implementar essa regra: ▪ Plataformas de rede IDS que a taxonomia do Sentinel pode traduzir (consulte a tabela Taxonomia NIDS para obter mais informações)	NIDS

RuleLg para essa regra

```
filter (e.rv53 = "Sans_MS_IE") flow trigger(1,60)
```

Microsoft – Verificação de ataque em acesso de Registro remoto

Esta regra suporta os 10 maiores ataques SANS Microsoft em registros da Microsoft.
O Registro de um sistema operacional da Microsoft é o local de todas as variáveis definidas pelo sistema. A capacidade de modificar ou substituir isso pode prejudicar bastante a operação ou a segurança de uma plataforma Microsoft.

Frequência da regra	Requisitos da regra	Taxonomia da regra
1 vez	Defina os seguintes itens antes de implementar essa regra: ▪ Plataformas de rede IDS que a taxonomia do Sentinel pode traduzir (consulte a tabela Taxonomia NIDS para obter mais informações)	NIDS

RuleLg para essa regra

```
filter (e.rv53 = "Sans_MS_Registry") flow trigger(1,60)
```

Microsoft - Verificação de ataque de scripts do Windows

Esta regra suporta os 10 maiores ataques SANS Microsoft em scripts do windows. Vários aplicativos da Microsoft são construídos usando a linguagem de programação Visual Basic. A capacidade de executar comandos fornecendo um script permite que um invasor obtenha acesso e controle de um sistema Microsoft.

Frequência da regra	Requisitos da regra	Taxonomia da regra
1 vez	Defina os seguintes itens antes de implementar essa regra: ▪ Plataformas de rede IDS que a taxonomia do Sentinel pode traduzir (consulte a tabela Taxonomia NIDS para obter mais informações)	NIDS

RuleLg para essa regra

```
filter (e.rv53 = "Sans_MS_Scripting") flow trigger(1,60)
```

UNIX - Verificação de ataque em chamada de procedimento remoto (RPC)

Esta regra suporta os maiores ataques SANS UNIX em RPC. Chamadas de procedimento remoto são um método em um ambiente UNIX para acessar ou executar algum aplicativo ou arquivo em um sistema remoto sem autenticação. Se o RPC permanecer aberto, qualquer usuário remoto poderá executar comandos privilegiados em seu sistema sem autenticação. O RPC pode permitir ataques remotos.

Frequência da regra	Requisitos da regra	Taxonomia da regra
1 vez	Defina os seguintes itens antes de implementar essa regra: ▪ Plataformas de rede IDS que a taxonomia do Sentinel pode traduzir (consulte a tabela Taxonomia NIDS para obter mais informações)	NIDS

RuleLg para essa regra

```
filter (e.rv53 = "Sans_Unix_RPC") flow trigger(1,60)
```

UNIX - Verificação de ataques ao servidor Apache Web

Esta regra suporta os maiores ataques SANS UNIX em servidores Apache Web. O servidor Apache Web é um aplicativo grátis que suportará servidores Web. A execução do servidor Apache Web pode deixá-lo vulnerável a esse ataque.

Frequência da regra	Requisitos da regra	Taxonomia da regra
1 vez	Defina os seguintes itens antes de implementar essa regra: ▪ Plataformas de rede IDS que a taxonomia do Sentinel pode traduzir (consulte a tabela Taxonomia NIDS para obter mais informações)	NIDS

RuleLg para essa regra

```
filter (e.rv53 = "Sans_Unix_Apache") flow trigger(1,60)
```

UNIX - Verificação de ataque em Secure Shell

Esta regra suporta os maiores ataques SANS UNIX em Secure Shell. Devido aos vários problemas com o telnet e o FTP, o Secure Shell foi desenvolvido para criptografar o tráfego entre duas máquinas. Esse aplicativo permite a transferência de dados ou a interação com um sistema remoto por meio de um método seguro. Contudo, em versões desse aplicativo foram identificados vários bugs que permitem ao invasor obter o controle completo do sistema atacado.

Frequência da regra	Requisitos da regra	Taxonomia da regra
1 vez	Defina os seguintes itens antes de implementar essa regra: ▪ Plataformas de rede IDS que a taxonomia do Sentinel pode traduzir (consulte a tabela Taxonomia NIDS para obter mais informações)	NIDS

RuleLg para essa regra

```
filter (e.rv53 = "Sans_Unix_SSH") flow trigger(1,60)
```

UNIX – Verificação de ataques em protocolo SNMP

Esta regra suporta os 10 maiores ataques SANS UNIX em SNMP. O SNMP foi originalmente projetado para gerenciar nós em uma rede. A segurança nunca foi implementada no SNMP V 1.0 e somente um nível baixo de segurança foi acrescentado no SNMP V 3.0. Portanto, o SNMP é alvo de vários ataques.

Frequência da regra	Requisitos da regra	Taxonomia da regra
1 vez	Defina os seguintes itens antes de implementar essa regra: ▪ Plataformas de rede IDS que a taxonomia do Sentinel pode traduzir (consulte a tabela Taxonomia NIDS para obter mais informações)	NIDS

RuleLg para essa regra

```
filter (e.rv53 = "Sans_Unix_SNMP") flow trigger(1,60)
```

UNIX - Verificação de ataques em protocolo FTP

Esta regra suporta os 10 maiores ataques SANS UNIX em FTP. O protocolo FTP é parte vital da comunicação na Internet. Assim, ele é um dos alvos principais dos invasores para redirecionar acesso de e para a Internet.

Frequência da regra	Requisitos da regra	Taxonomia da regra
1 vez	Defina os seguintes itens antes de implementar essa regra: ▪ Plataformas de rede IDS que a taxonomia do Sentinel pode traduzir (consulte a tabela Taxonomia NIDS para obter mais informações)	NIDS

RuleLg para essa regra

```
filter (e.rv53 = "Sans_Unix_FTP") flow trigger(1,60)
```

UNIX - Verificação de ataque em serviços remotos

Esta regra suporta os dez maiores ataques SANS UNIX em serviços remotos. Serviços Remotos são um método em um ambiente UNIX para o acesso ou a execução de algum aplicativo ou arquivo em um sistema remoto sem autenticação. Se os Serviços Remotos permanecerem abertos, que qualquer usuário remoto poderá executar comandos privilegiados em um sistema sem autenticação. Isso permite possíveis ataques remotos.

Frequência da regra	Requisitos da regra	Taxonomia da regra
1 vez	Defina os seguintes itens antes de implementar essa regra: ▪ Plataformas de rede IDS que a taxonomia do Sentinel pode traduzir (consulte a tabela Taxonomia NIDS para obter mais informações)	NIDS

RuleLg para essa regra

```
filter (e.rv53 = "Sans_Unix_RemoteServices") flow
   trigger(1,60)
```

UNIX - Verificação de ataque em Line Printer Daemon

Esta regra suporta os dez maiores ataques SANS UNIX em Line Printer Daemon. O Line Printer Daemon é o mecanismo que o UNIX usa para imprimir arquivos. Esse aplicativo é executado em um ambiente UNIX na conta raiz. Muitos bugs encontrados nesse aplicativo permitem que um invasor obtenha controle completo do ambiente UNIX.

Frequência da regra	Requisitos da regra	Taxonomia da regra
1 vez	Defina os seguintes itens antes de implementar essa regra: ▪ Plataformas de rede IDS que a taxonomia do Sentinel pode traduzir (consulte a tabela Taxonomia NIDS para obter mais informações)	NIDS

RuleLg para essa regra

```
filter (e.rv53 = "Sans_Unix_LPD") flow trigger(1,60)
```

UNIX - Verificação de ataque em Sendmail

Esta regra suporta os 10 maiores ataques SANS UNIX em Sendmail. O aplicativo Sendmail usa o Simple Mail Transport Protocol (SMTP). Esse aplicativo é uma parte vital da comunicação na Internet. Como tal, é um dos principais alvos de invasores para redirecionar acesso de e para a Internet.

Frequência da regra	Requisitos da regra	Taxonomia da regra
1 vez	Defina os seguintes itens antes de implementar essa regra: ▪ Plataformas de rede IDS que a taxonomia do Sentinel pode traduzir (consulte a tabela Taxonomia NIDS para obter mais informações)	NIDS

RuleLg para essa regra

```
filter (e.rv53 = "Sans_Unix_SendMail") flow trigger(1,60)
```

UNIX - Verificação de ataque em BIND/DNS

Esta regra suporta os 10 maiores ataques SANS UNIX em ataques DNS. O Domain Name Service (DNS) é uma parte vital da comunicação na Internet. Como tal, é um dos principais alvos de invasores para redirecionar acesso de e para a Internet.

Frequência da regra	Requisitos da regra	Taxonomia da regra
1 vez	Defina os seguintes itens antes de implementar essa regra: ▪ Plataformas de rede IDS que a taxonomia do Sentinel pode traduzir (consulte a tabela Taxonomia NIDS para obter mais informações)	NIDS

RuleLg para essa regra

```
filter (e.rv53 = "Sans_Unix_DNS") flow trigger(1,60)
```

UNIX - Verificação de ataque na autenticação geral do UNIX

Esta regra suporta os 10 maiores ataques SANS Microsoft em senhas fracas. Quando senhas fracas são descobertas, devem ser mudadas.

Frequência da regra	Requisitos da regra	Taxonomia da regra
1 vez	Defina os seguintes itens antes de implementar essa regra: ▪ Plataformas de rede IDS que a taxonomia do Sentinel pode traduzir (consulte a tabela Taxonomia NIDS para obter mais informações)	NIDS

RuleLg para essa regra

```
filter (e.rv53 = "Sans_Unix_WeakPasswords") flow
   trigger(1,60)
```

Tabelas de taxonomia

Essa seção contém duas tabelas. São elas:

- Taxonomia NIDS
- Taxonomia HIDS e OS

Elas listam os diferentes valores para e.rv50 a e.rv53 para os exemplos de RuleLg fornecidos.

Tabela de taxonomia NIDS

Ação – Nível1 (e.rv50)	Sistema – Nível2 (e.rv51)	Detalhe – Nível3 (e.rv52)	Resultados – Nível4 (e.rv53)
Ataque	Bate-papo	Acesso	
		Buffer_Overflow	
		Backdoor	
		Brute_Force	
		DoS	

Ação – Nível1 (e.rv50)	**Sistema – Nível2 (e.rv51)**	**Detalhe – Nível3 (e.rv52)**	**Resultados – Nível4 (e.rv53)**
	DNS	Acesso	Sans_Unix_DNS
		Buffer_Overflow	Sans_Unix_DNS
		Backdoor	
		Brute_Force	
		DoS	
	E-mail	Acesso	Sans_Unix_SendMail
		Buffer_Overflow	Sans_Unix_SendMail Sans_MS_IE
		Backdoor	
		Brute_Force	
		DoS	
	Telnet	Acesso	
		Buffer_Overflow	
		Backdoor	
		Brute_Force	
		DoS	
	Arquivo	Acesso	Sans_Unix_FTP Sans_MS_WeakPasswords Sans_MS_NETBIOS
		Buffer_Overflow	Sans_Unix_FTP
		Backdoor	Sans_Unix_FTP
		Brute_Force	
		DoS	
	Web	Acesso	Sans_Unix_Apache Sans_MS_NETBIOS Sans_MS_WeakPasswords Sans_MS_IIS Sans_MS_Scripting Sans_MS_SQLServer Sans_MS_IE SANS_MS_MDAC
		Buffer_Overflow	Sans_Unix_Apache Sans_MS_IIS
		Backdoor	
		Brute_Force	Sans_MS_IIS
		DoS	Sans_Unix_Apache Sans_MS_IIS
	PC	Vírus	Sans_MS_IE Sans_MS_IIS
		Script	
		Worm	Sans_MS_SQLServer
		Cavalo de tróia	

Ação – Nível1 (e.rv50)	**Sistema – Nível2 (e.rv51)**	**Detalhe – Nível3 (e.rv52)**	**Resultados – Nível4 (e.rv53)**
	Servidor	Acesso	Scan_MS_IIS Sans_MS_Registry Sans_MS_SQLServer Sans_MS_NETBIOS Sans_Unix_remoteServices Sans_Unix_RPC Sans_Unix_SSH
		Buffer_Overflow	Sans_Unix_RemoteServices Sans_Unix_WeakPasswords Sans_Unix_RPC Sans_Unix_LPD Sans_MS_SQLServer Sans_MS_MDAC Sans_MS_NETBIOS Sans_Unix_SSH
		Backdoor	Sans_Unix_RPC
		Brute_Force	Sans_MS_SQLServer Sans_MS_WeakPasswords
		DoS	
	Protocolo	IP	
		TCP	
		UDP	
		ICMP	
		HTTP	
		Rota	
		Talk	
		XFS	
		SSH	
		IGMP	
		Horário	
		Notícias	
		Windows	
		RIP	
		IDS	
		SNMP	Sans_Unix_SNMP
		BGP	
	Usuário	Acesso	Sans_Unix_WeakPasswords Sans_Unix_RemoteServices
		Buffer_Overflow	Sans_Unix_RemoteServices Sans_MS_NETBIOS
		Backdoor	
		Brute_Force	
		DoS	

Ação – Nível1 (e.rv50)	**Sistema – Nível2 (e.rv51)**	**Detalhe – Nível3 (e.rv52)**	**Resultados – Nível4 (e.rv53)**
Probe	Bate-papo		
	DNS		
	E-mail		
	Arquivo		Sans_Unix_FTP
	Web		Sans_MS_IIS Sans_Unix_Apache
	PC		
	Servidor		Sans_MS_NullSessions Sans_MS_Registry
	Protocolo	IP	
		TCP	
		RIP	
		SNMP	Sans_Unix_SNMP
		SSH	
		Talk	
		Horário	
		Windows	
		UDP	
		ICMP	
		DHCP	
	Explorar		
	Telnet		Sans_MS_LM
	Usuário		Sans_MS_LM
	IDS		
Política	Porn		
Compro-metimento	Bate-papo	Acesso	
		Buffer_Overflow	Sans_Unix_Weak_Passwords
		Backdoor	
		Brute_Force	
		DoS	
	DNS	Acesso	Sans_Unix_DNS
		Buffer_Overflow	
		Backdoor	
		Brute_Force	
		DoS	
	E-mail	Acesso	
		Buffer_Overflow	
		Backdoor	Sans_Unix_SendMail
		Brute_Force	
		DoS	
	Telnet	Acesso	
		Buffer_Overflow	
		Backdoor	
		Brute_Force	

Ação – Nível1 (e.rv50)	**Sistema – Nível2 (e.rv51)**	**Detalhe – Nível3 (e.rv52)**	**Resultados – Nível4 (e.rv53)**
		DoS	
	Arquivo	Acesso	
		Buffer_Overflow	
		Backdoor	
		Brute_Force	
		DoS	
	Web	Acesso	Sans_Unix_Apache
		Buffer_Overflow	Sans_MS_IIS
		Backdoor	Sans_Unix_Apache Sans_MS_Registry
		Brute_Force	
		DoS	
	PC	Vírus	
		Script	
		Worm	
		Cavalo de tróia	
	Servidor	Acesso	Sans_MS_SQLServer
		Buffer_Overflow	Sans_Unix_RPC
		Backdoor	Sans_MS_WeakPasswords Sans_MS_Registry Sans_Unix_SNMP Sans_Unix_WeakPasswords
		Brute_Force	
		DoS	
	Usuário	Acesso	
		Buffer_Overflow	
		Backdoor	
		Brute_Force	
		DoS	

Tabela de taxonomia HIDS & OS

Ação – Nível1 (e.rv50)	Sistema – Nível2 (e.rv51)	Detalhe – Nível3 (e.rv52)	Resultados – Nível4 (e.rv53)
Ataque	Arquivo	Excluir	App OS
		Executar	App OS
		Criar	App OS
		Modificar	App OS
		Acesso	App OS
	Serviço	Excluir	App OS

Ação – Nível1 (e.rv50)	Sistema – Nível2 (e.rv51)	Detalhe – Nível3 (e.rv52)	Resultados – Nível4 (e.rv53)
		Parar	App OS
		Iniciar	App OS
		Criar	App OS
		Acesso	App OS Priv E-mail ID Rede Arquivo Sistema
		Buffer_Overflow	
		Backdoor	
		DoS	
	Opção de	Excluir	App OS
		Modificar	App OS
		Criar	App OS
		Ativar	App OS
		Acesso	App OS
	Usuário	Criar	ID Auth Param Priv
		Modificar	ID Auth Param Priv
		Excluir	ID Auth Param Priv
		Acesso	Guest Priv Root Outros
	Grupo	Criar	Membro Grupo
		Modificar	Membro Grupo

Ação – Nível1 (e.rv50)	Sistema – Nível2 (e.rv51)	Detalhe – Nível3 (e.rv52)	Resultados – Nível4 (e.rv53)
		Excluir	Membro Grupo
	Sistema	Informações	
		Memória	
		Depurar	
	Anomoly		
	Telnet	Acesso	
		Buffer_Overflow	
		Backdoor	
		Brute_Force	
		DoS	
	Web	Acesso	
		Buffer_Overflow	
		Backdoor	
		Brute_Force	
		DoS	
	PC	Vírus	
		Script	
		Backdoor	
		Worm	
		Cavalo de tróia	
	DNS	Acesso	
		Buffer_Overflow	
		Backdoor	
		Brute_Force	
		DoS	
	E-mail	Acesso	
		Buffer_Overflow	
		Backdoor	
		Brute_Force	
		DoS	
Probe	Arquivo	Excluir	App OS
		Executar	App OS
		Criar	App OS
		Modificar	App OS
		Acesso	App OS
	Serviço	Excluir	App OS
		Parar	App OS
		Iniciar	App OS

Ação – Nível1 (e.rv50)	Sistema – Nível2 (e.rv51)	Detalhe – Nível3 (e.rv52)	Resultados – Nível4 (e.rv53)
		Criar	App OS
		Acesso	App OS Arquivo ID E-mail Priv Rede Sistema
	Opção de	Excluir	App OS
		Modificar	App OS
		Criar	App OS
		Ativar	App OS
		Acesso	App OS
	Usuário	Criar	ID Auth Param Priv
		Modificar	ID Auth Param Priv
		Excluir	ID Auth Param Priv
		Acesso	Guest Root Outros
	Grupo	Criar	Membro Grupo
		Modificar	Membro Grupo
		Excluir	Membro Grupo
	Sistema	Informações	
		Memória	
		Depurar	
	Anomoly		
	Web	Acesso	
		Buffer_Overflow	

Ação – Nível1 (e.rv50)	Sistema – Nível2 (e.rv51)	Detalhe – Nível3 (e.rv52)	Resultados – Nível4 (e.rv53)
		Backdoor	
		Brute_Force	
		DoS	
	E-mail	Acesso	
		Buffer_Overflow	
		Backdoor	
		Brute_Force	
		DoS	
	Protocolo	IP	
		TCP	
		UDP	
		ICMP	
		HTTP	
		Rota	
		Talk	
		XFS	
		SSH	
		IGMP	
		Horário	
		Notícias	
		Windows	
		RIP	
		IDS	
		SNMP	
		BGP	

Correlação de saída

A estrutura de saída do Mecanismo de Correlação permite classificar, filtrar e relatar os dados gerados como parte de uma regra de Watchlist ou regra de correlação.

Estrutura da regra de correlação de saída

Os valores de saída padrão são:

- RES definido como "Correlação" se não for definido por usuário
- SubRes definido como "<rule>.<rulename> se não for definido por usuário
- Sev definido como 4 se não for definido por usuário
- ST (Sensor Type - Tipo de Sensor - C)
- El (padrão de regra - SIP=’1.2.3.4.’ ponto e vírgula, limite de regra no formato 3-2-m (contagem de 3 em 2 minutos, por exemplo)
- RT2 (nome da regra)

Parâmetros de script passados

Os parâmetros de script passados afetam tanto as Regras de Watchlist quanto as Regras de Correlação. Os parâmetros de script são especificados na caixa de entrada Executar Ação na guia Critérios de Ativação com formato %xyz% onde xyz é o nome do parâmetro. Os nomes dos parâmetros que representam meta-tags podem ser tanto um nome curto (como sip) ou longo (como SourceIP). Os nomes de parâmetros distinguem maiúsculas de minúsculas.

Parâmetros

Os primeiros onze parâmetros são parâmetros especiais. Eles não são tags META. Eles correspondem a eventos correlacionados. Os parâmetros doze a quarenta e seta são parâmetros de tags META.

1. `%RuleName%` - O nome da regra acionada (O formato é rule.rulename).
2. `%RuleType%` - O tipo de regra que foi acionada. C para correlação. W para Lista de Avisos.
3. `%RuleDescription%` - A descrição que foi digitada quando a regra foi criada.
4. `%RuleSeverity%` - O tipo de severidade da regra que foi acionada.
5. `%RuleResource%` - O nome do recurso da regra que foi acionada.
6. `%RuleSubResource%` - O nome do sub-recurso da regra que foi acionada.
7. `%RuleLg%` - A regra no idioma da regra do Mecanismo de Correlação (RuleLg).
8. `%RuleCount%` - A contagem da regra que foi acionada.
9. `%RuleDuration%` - A duração (em segundos) da regra que foi acionada.
10. `%RulePattern%` - Uma lista de todas as tags no idioma da regra e o valor da tag retirado do último evento que acionou a regra. O formato é tsn1='valor1='valor2'tsn3='valor3', onde:
    - tns1 é a abreviação da tag 1
    - tns2 é a abreviação da tag 2

    Por exemplo:

    ```
    sip='192.168.0.3'dip='2.168.0.2'
    ```
11. `%CorrelatedEventID%` - O identificador de eventos do evento correlacionado gerado pela regra acionada.
12. %MessageText% - O texto da mensagem da regra que foi acionada.
13. %EventName% - O nome do evento da regra que foi acionada.

As tags restantes correspondem ao campo do último evento que acionou o evento correlacionado.

14. %sev% - Gravidade: A gravidade normal do evento (0-5).
15. %vul% - Vulnerabilidade: A vulnerabilidade do bem identificado neste evento.
16. %crt% - Importância: A importância do bem identificado neste evento.
17. %dt% - Data/Hora: A data e a hora normalizadas do evento, conforme fornecido pelo Coletor..
18. %sip% - IP de Origem: O endereço IP de origem do qual o evento se originou.

19. %dip% - IP de Destino: O endereço IP de destino ao qual o evento era destinado.
20. %id% - ID do Evento: Identificador exclusivo (UUID) deste evento.
21. %src% - ID de Origem: Identificador exclusivo (UUID) para o processo do Sentinel que gerou este evento.
22. %port% - Porta do Assistente: Descrição de porta do Sentinel Collector .
23. %agent% - Coletor Assistente: Descrição de porta do Sentinel Collector .
24. %res% - Recurso: O nome do recurso.
25. %sres% - Sub-recurso: O nome do sub-recurso.
26. %evt% - Nome do Evento: o nome descritivo do evento, conforme relatado (ou fornecido) pelo sensor. Por exemplo: "Explorar Porta".
27. %sn% - Nome do Sensor: O nome do último detector do evento quando recebido em dados iniciais. Exemplo "FW1" para um firewall.
28. %st% - Tipo de Sensor: O único caractere determinador do tipo de sensor (N, H, O, V, C, W). H: baseado em host, N: baseado em rede, O: Outros, V: Antivírus, C: Correlação e W: Lista de Avisos.
29. %et% - Horário do Evento: A data normalizada do evento, conforme relatado pelo sensor, analisado no formato: A-M-D-H:M:S~AMPM24~TZ.
30. %prot% - Protocolo: O protocolo de rede do evento.
31. %shn% - Nome do Host de Origem: O nome do host de origem do qual o evento se originou.
32. %sp% - Porta de Origem: A porta de origem da qual o evento se originou.
33. %dhn% - Nome do Host de Destino: O nome do host de destino ao qual o evento era destinado.
34. %dp% - Porta de Destino: A porta de destino para a qual o evento era destinado.
35. %sun% - Nome do Usuário de Origem: O nome do usuário de origem usado para iniciar um evento. Exemplo "jdoe" durante uma tentativa para "su".
36. %dun% - Nome do Usuário de Destino: O nome do usuário de destino em que uma ação foi tentada. Por exemplo: Tentativa de redefinir a senha de raiz.
37. %fn% - Nome do Arquivo: O nome do programa executado ou do arquivo acessado, modificado ou afetado. Por exemplo: O nome de um arquivo infectado por vírus ou de um programa detectado por um IDS.
38. %ei% - Informações Estendidas: Armazena informações adicionais coletadas pelo Coletor. Os valores nessa variável são separados por ponto-e-vírgula (;).
Por exemplo: Um domínio para um ID ou nomes de arquivo.
39. %rn% - Nome do Relator: O nome do host ou o endereço IP do dispositivo para o qual um evento foi registrado ou do qual é enviada uma notificação do evento.
40. %pn% - Nome do Produto: Indica o tipo, o fornecedor e o nome de código de produto do sensor por meio do qual o evento foi gerado. Por exemplo: Check Point FireWall=CPFW.
41. %msg% - Mensagem: Texto de mensagem com formato livre para o evento.
42. %rt1% - Reservado pela Novell para expansão. Para uso com consultor (String).
43. %rt2% - Reservado pela Novell para expansão (string).
44. %ct1% -Reservado para uso de clientes, para dados específicos do cliente (string).

45. %ct2% -Reservado para uso de clientes, para dados específicos do cliente (string).
46. %rt3% - Reservado pela Novell para expansão (número).
47. %ct3% -Reservado para uso de clientes, para dados específicos do cliente (número).
48. Parâmetros 46 – 145

    %rv1% thru %rv100%

    Essas são tags META de eventos atuais representando variáveis reservadas.
49. Parâmetros 146 – 245

    %cv1% thru %cv100%

    Essas são tags META de eventos atuais representando variáveis do cliente.

NOTA: Para obter mais informações sobre Comandos e Parâmetros, consulte o Capítulo 5 – Assistente e tags META do Sentinel no Guia de Referência do Usuário e o Capítulo 9 – Guia Admin, Regras de Correlação no Guia do Usuário.

Quando usar o comando %all%:

- Se um valor de parâmetro for branco ou nulo, ele será E_NULL ou <tag absent>. Desse modo, haverá sempre 45 parâmetros independente de alguns campos estarem brancos.
- Ao configurar o mecanismo de correlação para iniciar o script de interface do HP OVO, você deve especificar o nome do script junto com a tag de parâmetro %all%:

  ```
  esec_ovo %all%
  ```

- Ao configurar o mecanismo de correlação para iniciar o script de interface BMC, você deve especificar o nome do script junto com o parâmetro %all%:

  ```
  bmc_interface.csh %all%
  ```

- Ao configurar o mecanismo de correlação para enviar um e-mail, você deve especificar o nome do script do e-mail junto com o parâmetro %all% e o endereço de e-mail e assunto (opcional):

  ```
  email_interface.csh %all% <name>@<domain name> "My
     Subject"
  ```

- Todos os scripts/aplicativos que o mecanismo de correlação podem executar tem que estar localizados no diretório $ESEC_HOME/sentinel/exec (UNIX) %ESEC_HOME%\sentinel\bin (Windows).
- Por padrão, o mecanismo de correlação NÃO passará nenhum parâmetro para os scripts que executar. Você tem que usar as %tags% descritas acima se quiser que os parâmetros sejam passados para os scripts.
- Ao especificar parâmetros para um script, você pode agrupá-los usando aspas. Aqui estão alguns exemplos:

  ```
  %sip% %dip% - seria tratado como dois parâmetros.

  "%sip% %dip%" – seria tratado como um parâmetro.

  "Hello World" %sip% - seria tratado como dois
     parâmetros.
  ```

"The message is %msg%" – seria tratado como um parâmetro.

%msg% - seria tratado como um parâmetro (mesmo que a mensagem possua espaços.)

"%msg%" – também seria tratado como um parâmetro (mesmo que a mensagem possua espaços.)

8 Opções da linha de comando de correlação do Sentinel

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

As opções da linha de comando devem ser usadas por usuários avançados. Usuários comuns não devem fazer modificações com base na utilização de tais opções. Para acessar as opções da linha de comando, vá para

Para UNIX:

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

Para Windows

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

Para executar a opção da linha de comando, digite

```
correlation_engine <correlation command line option>
```

Opção da linha de comando de correlação	**Descrição**
-debug	Modo de depuração (imprimir informações de depuração extensas)
-noErrorLogging	Desabilitar registro de erro no Registro de eventos do Windows.
-ruleFile <arquivo>	Especificar arquivo de texto contendo regras a serem processadas pela instância do Mecanismo de correlação.
-xmlruleFile <arquivo>	Especificar arquivo xml de configurações para armazenar uma cópia local das regras contidas no banco de dados. Padrão: startup_correlation_rules.xml
-inputChannel <string>	Especificar canal de entrada da camada de comunicação para o Mecanismo de correlação. Padrão: ewizard_binary_event
-outputChannel <string>	Especificar canal de saída da camada de comunicação para o Mecanismo de correlação. Padrão:correlation_binary_event.

Opção da linha de comando de correlação	Descrição
-outputUpdateChannel <string>	Especificar canal de atualização de saída da camada de comunicação para o mecanismo de correlação. Padrão: correlation_binary_event_update
-outputExecuteChannel <string>	Especificar canal de execução de saída da camada de comunicação para o Mecanismo de correlação. Padrão: execute
-outputIncidentChannel <string>	Especificar canal de incidente de saída da camada de comunicação para o Mecanismo de correlação. Padrão: app_incident_req
-service <string>	Especificar serviço de comunicação (parâmetro de configuração) para o Mecanismo de correlação. Padrão: correlation_engine
-mgmtInputChannel <string>	Especificar canal de entrada de gerenciamento da camada de comunicação para o Mecanismo de correlação. Padrão: correlation_mgmt_input_channel
-mgmtOutputChannel <string>	Especificar canal de gerenciamento de saída da camada de comunicação para o Mecanismo de correlação. Padrão: correlation_mgmt_output_channel
-mgmtService <string>	Especificar serviço de gerenciamento de comunicação (parâmetro de configuração) para o Mecanismo de correlação. adrão: correlation_engine_mgmt
-configurationFile <arquivo>	Especificar arquivo para substituir os parâmetros de inicialização de configuração padrão do Mecanismo de correlação. Padrão: + 30 segundos do tempo do Sentinel Server.
-noStartupRules	Definir Mecanismo de correlação para que seja executado sem recuperar regras armazenadas no banco de dados. A opção –ruleFile também ignora a recuperação do banco de dados.
-dbTimeout <tempo de espera em milissegundos>	Definir o valor de tempo de espera para recuperar as regras armazenadas no banco de dados. Padrão: 5.000 milissegundos

Opção da linha de comando de correlação	Descrição
-dbRetries <número>	Definir o número de repetições para entrar em contato com o banco de dados. Padrão: 6
-name <nome do mecanismo>	Define o nome do criador de relatório deste mecanismo de correlação. Padrão: Mecanismo de correlação
-affinityOneProcessor	Definir Mecanismo de correlação para ser executado somente em um processador.
-useEventTime	Para teste; não deve ser usado.
-useNullOutput	Para teste; não deve ser usado.
-logFile <nome do arquivo>	Direciona o status a um arquivo.
-logPeriod <segundos>	Controla a freqüência que o status é gravado no arquivo.
-version	Exibir a versão do build e sair.
-help	Exibir esta Ajuda e sair.

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

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

O processo do DAS é o serviço de persistência do Sentinel Server e fornece uma interface MOM (barramento de mensagem) para o banco de dados. Ele oferece ao banco de dados de backend acesso direcionado aos dados. Ele recebe um pedido XML de diferentes processos do Sentinel, o converte em uma consulta no banco de dados, processa o resultado do banco de dados e o converte de volta em uma resposta XML. Ele oferece suporte a solicitações para recuperar eventos para Consulta Rápida e Detalhamento de Eventos, para recuperar informações de vulnerabilidade e informações do consultor e para manipular informações de configuração. O DAS também lida com o registro de todos os eventos recebidos do Gerenciador do Coletor do Assistente e as solicitações para recuperar e armazenar informações de configuração.

Arquivos de container do DAS

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

- das_binary.xml: usado para a operação de inserção de eventos e eventos correlacionados
- das_query.xml: todas as outras operações de banco de dados;
- das_aggregation.xml: usado para a operação de agregação
- das_itrac.xml: usado para a execução e configuração do serviço da atividade e para a configuração do serviço de workflow
- das_rt.xml: usado para a configuração da função Telas Ativas no Console de Controle do Sentinel

AVISO: Não edite manualmente os arquivos xml. Use o utilitário dbconfig para mudar quaisquer valores dos arquivos xml.

Cada um desses processos tem um arquivo de registro de operação localizado em %ESEC_HOME%\Sentinel\log ou $ESEC_HOME/Sentinel/log. São eles:

- das_query0.*.log – Todos os registros das_query
- das_binary0.*.log – Todos os registros das_binary
- das_itrac0_*.log – registros de atividade e fluxo de trabalho
- das_aggregation0.*.log – registros de agregação
- das_rt0.*.log – registros da Tela Ativa

Os arquivos xml especificam:

- ConnectionManager
  - nome de usuário
  - senha
  - nome de host
  - número de porta
  - banco de dados (nome do banco de dados)
  - servidor (oracle ou mssql)
  - máximo de conexões
  - tamanho do lote
  - tamanho da carga
- DispatchManager — Especifica os canais no barramento de mensagens para escuta do DAS. Também especifica que classe java usar para converter solicitações xml em objetos java, e especifica para que gerenciador enviar o objeto java para processamento da mensagem. Por exemplo: uma solicitação de consulta de evento é convertida em um objeto java por meio do esecurity.cracker.QuickQueryRequestCracker O cracker o envia então ao gerenciador esecurity.event.request. O gerenciador o envia aos serviços, para execução.
- Além disso, outros componentes que fornecem serviços DAS relevantes.

Use o utilitário dbconfig para reconfigurar as propriedades de conexão do banco de dados para Windows.

Reconfigurando as propriedades de conexão do banco de dados

Esse procedimento deve ser executado para cada um dos nomes de arquivo de container a seguir (containerFilename)

- das_binary.xml
- das_query.xml
- das_rt.xml
- das_aggregation.xml
- das_itrac.xml

Reconfigurando as propriedades de conexão do banco de dados para Windows

NOTA: Em intervalos de 10 segundos, os arquivos de propriedade de registro serão verificados para determinar se ocorreram mudanças desde a última leitura. Se o arquivo tiver mudado, o LogManagerRefreshService lerá o arquivo de propriedades de registro novamente,

1. Quando o banco de dados for instalado, efetue login como usuário com direitos administrativos.
2. Vá para:

   Windows:

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

   Para UNIX:

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

3. Digite o seguinte comando:

```
dbconfig -n <containerFilename> [-u username] [-p
   password] [-h hostname] [-t port number] [-d
   database] [-s server(mssql ou oracle)] [-help]
   [-version]
```

Arquivos de Configuração do DAS

Estes arquivos são usados para configurar o registro do processo do DAS.

- das_query_log.prop
- das_binary_log.prop
- das_rt_log.prop
- das_itrac_log.prop
- das_aggregation_log.prop

Eles estão localizados em:

Para Windows:

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

Para UNIX:

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

Esses arquivos contêm informações de configuração para o gerenciador do console, que imprime mensagens em uma saída padrão, e para o gerenciador de arquivo, que imprime mensagens em um arquivo. A configuração de cada gerenciador permite a especificação de opções disponíveis para cada um deles. Esses arquivos permitem configurar quais mensagens de registro deverão ser impressas Os níveis são:

- DESATIVADO – desabilita todos os registros
- SEVERO (valor mais alto) – indicação de que um componente funciona mal ou de que há perda/corrupção de dados críticos.
- AVISO – se uma ação fizer com que um componente funcione mal no futuro ou se houver perda/corrupção de dados não-críticos.
- INFORMAÇÃO – Informações de auditoria
- CONFIGURAÇÃO
- BOM – para depuração
- ÓTIMO – para depuração
- MELHOR (valor menor) – para depuração
- TODOS – registrará todos os níveis

Quando um nível de registro é especificado, todas as mensagens de registro desse nível e dos superiores (da lista acima) são registradas. Por exemplo, se o nível INFORMAÇÃO for especificado, as mensagens de INFORMAÇÕES, AVISO e SEVERO serão registradas.

Se você mudar os arquivos, deverá reiniciar o DAS para que as mudanças tenham efeito.

O registro é gravado em:

Para Windows:

```
%ESEC_HOME%\sentinel\log\das_query_0.*.log
%ESEC_HOME%\sentinel\log\das_binary_0.*.log
```

```
%ESEC_HOME%\sentinel\log\das_itrac_0.*.log
%ESEC_HOME%\sentinel\log\das_aggregation0.*.log
```

Para UNIX:

```
$ESEC_HOME/sentinel/log/das_query0.*.log
$ESEC_HOME/sentinel/log/das_binary0.*.log
$ESEC_HOME/sentinel/log/das_itrac_0.*.log
$ESEC_HOME/sentinel/log/das_aggregation0.*.log
```

O * indica o número exclusivo para resolver conflitos e o número de geração para distinguir registros alternados. Por exemplo, das_query0.0.log é o registro com arquivo de índice 0 (primeiro) em um conjunto alternado de arquivos de registro para o processo do DAS.

Conectores nativos de BD para inserção de evento

Os conectores nativos de BD oferecem um desempenho de inserção de evento aprimorado. O conector a ser usado depende da plataforma de banco de dados usada.

Conector nativo de BD do MS SQL

Use o armazenamento de evento nativo ADO.Net.

Como configurar o conector nativo de BD do MS SQL

1. Na máquina em que o DAS foi instalado, instale a estrutura do .Net:
2. No arquivo das_binary.xml, mude a propriedade "insert.strategy" de EventStoreService > Persistor para:

```
esecurity.ccs.comp.event.jdbc.ADOLoadStrategy
```

Conector nativo de BD da Oracle

Use o armazenamento de evento nativo OCI. No mínimo, o cliente Oracle deve estar instalado na mesma máquina que o DAS.

Como configurar o conector nativo de BD da Oracle

1. Crie um arquivo ".profile" no diretório pessoal esecadm. Insira o texto a seguir no arquivo (modifique ORACLE_HOME para instalação):

```
ORACLE_HOME=/build/home/oracle/OraHome
export ORACLE_HOME
LD_LIBRARY_PATH=$LD_LIBRARY_PATH:$ORACLE_HOME/lib
export LD_LIBRARY_PATH
```

2. Em das_binary.xml, mude a propriedade "insert.strategy" de EventStoreService > Persistor para:

```
esecurity.ccs.comp.event.jdbc.OCILoadStrategy
```

10 Mudando as senhas de usuário padrão

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

Este capítulo aborda como mudar as senhas para usuários padrão do Sentinel:

Autenticação de Oracle e MS SQL:

- esecadm
- esecapp
- esecdba
- esecrpt

Autenticação do Windows:

- Administrador do Sentinel
- Usuário de BD de Aplicativo do Sentinel
- Administrador de BD do Sentinel
- Usuário de Relatório do Sentinel

Mudando senhas de usuário padrão para autenticação de Oracle e MS SQL

NOTA: Para mudar senhas, você deve ter direitos administrativos.

Mudando a senha de esecadm

Mudando a senha de esecadm

1. Efetue login no Console de Controle do Sentinel e clique na guia *Admin*.
2. Abra a janela *Gerenciador de Usuário*.
3. Clique duas vezes na conta de usuário esecadm ou clique o botão direito do mouse em > *Detalhes do Usuário*.
4. Modifique a senha da conta.
5. Clique em *OK*.

Mudando a senha de esecapp

Mudando a senha de esecadm

1. Para o MS SQL, use o MS SQL Enterprise Manager e mude a senha de esecapp.
2. Para Oracle, use o Oracle Enterprise Manager e mude a senha de esecapp.
3. Use o utilitário dbconfig para atualizar todos os arquivos xml de container. Isso é necessário porque os arquivos xml armazenam a senha (criptografada) de esecapp para permitir a conexão do DAS e do Consultor ao banco de dados.
   - das_binary.xml
   - das_query.xml
   - activity_container.xml
   - workflow_container.xml
   - das_rt.xml

Os arquivos xml de container estão nestes locais:

Windows:

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

Para Oracle:

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

Para obter mais informações sobre o uso do utilitário dbconfig, consulte o Guia de Referência do Sentinel, Capítulo 9 - Serviço de Acesso a Dados (DAS, Data Access Service) do Sentinel.

```
dbconfig –a <containerDirectory> -p <password>
```

Mudando a senha de esecdba

Mudando a senha de esecdba

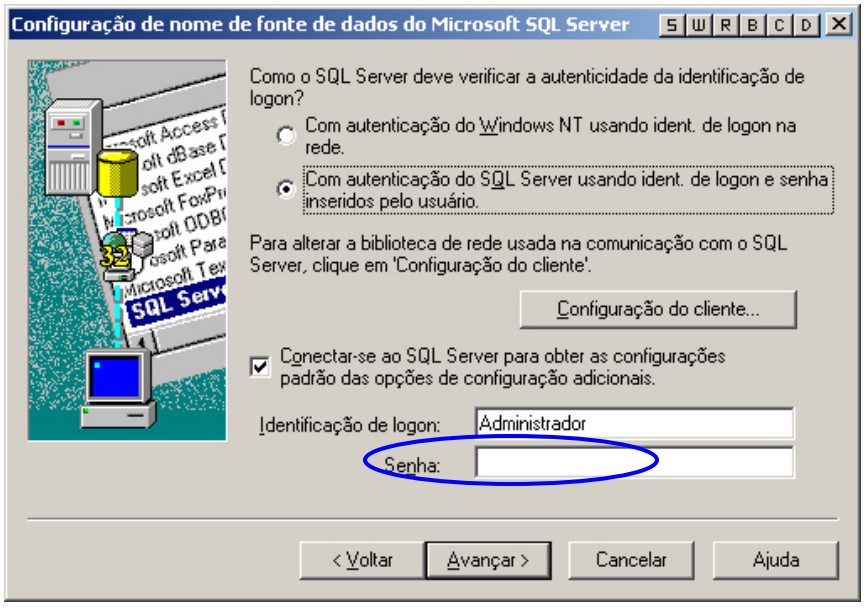
1. Para o MS SQL, use o MS SQL Enterprise Manager e mude a senha de esecdba.
2. Para Oracle, use o Oracle Enterprise Manager e mude a senha de esecdba.
3. Para que as tarefas SDM automatizadas continuem a funcionar (por ex.: adicionar partição, arquivar partição), atualize dbPass no arquivo sdm.connect com a nova senha de esecdba usando a GUI do SDM ou a linha de comando. Para obter mais informações, consulte o Guia do Usuário do Sentinel, Capítulo 10 – Gerenciador de Dados do Sentinel.

```
sdm -action saveConnection -server <oracle/mssql> -
   host <hostIp/hostName> -port <portnum> -database
   <databaseName/SID> [-driverProps <propertiesFile>]
   {-user <dbUser> -password <dbPass>} -connectFile
   <filenameToSaveConnection>
```

Mudando a senha de esecrpt

Mudando a senha de esecrpt

1. Para o banco de dados do MS SQL do Sentinel, use o MS SQL Enterprise Manager e mude a senha de esecrpt.
2. Para o banco de dados do Oracle do Sentinel, use o Oracle Enterprise Manager e mude a senha de esecrpt.
3. Crystal Server para MS SQL do Sentinel, se aplicável; na máquina do Crystal Server, atualize o ODBC DSN (*Painel de Controle* > *Ferramentas Administrativas* > *Origens de Dados (ODBC)*).
   a. Na guia DSN de Sistema, realce sentineldb e clique em *Configurar*.
   b. Clique em *Avançar*. Atualize a senha.
   c. Clique em *Avançar* até que seja exibido um botão Concluir. Clique em *Concluir*.



4. Crystal Server para Oracle do Sentinel: nenhuma mudança é necessária.

Mudando senhas de usuário padrão para autenticação do Windows

Mudando a senha do Administrador do Sentinel

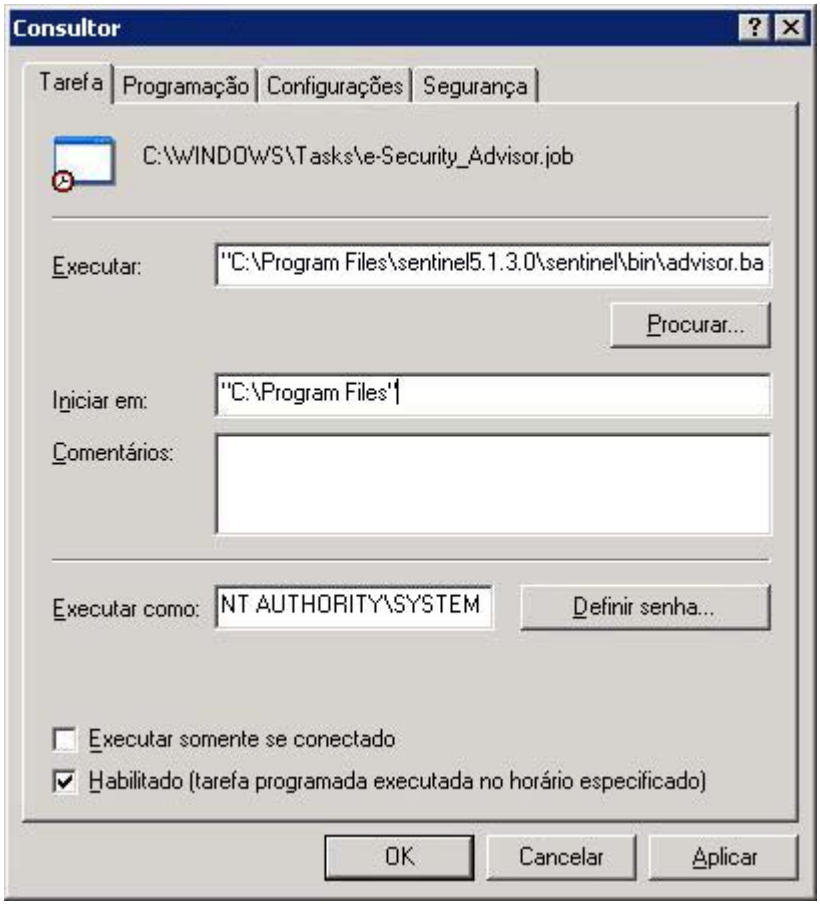
Mudando a senha do Administrador do Sentinel

1. Use o Sistema Operacional Windows para mudar a senha.

Mudando a senha do Administrador de BD do Sentinel

Mudando a senha do Administrador de BD do Sentinel

1. Use o Sistema Operacional Windows para mudar a senha.
2. Se estiver executando tarefas SDM programadas (por ex., para adicionar ou arquivar partições), você precisará atualizar a propriedade "Executar como" (*Painel de Controle >Tarefas Programadas > clique o botão direito do mouse em Propriedades*).

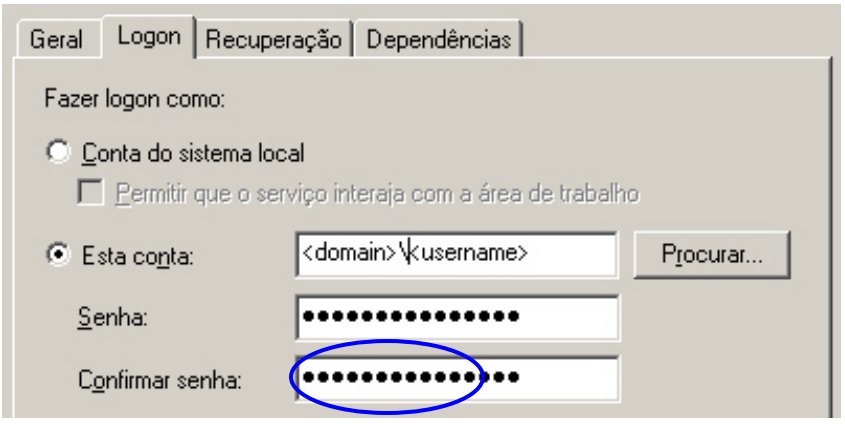


3. Clique em *Definir senha*. Digite a nova senha duas vezes e clique em *OK*. Clique em *Aplicar* e em *OK*.

Mudando a senha do Administrador de BD do Aplicativo do Sentinel

Mudando a senha do Administrador de BD do Sentinel

1. Use o Sistema Operacional Windows para mudar a senha.
2. Na máquina do DAS, abra os Serviços do Windows (*Painel de Controle* > *Ferramentas Administrativas* > *Serviços*).
3. Clique o botão direito do mouse em *Sentinel* > *Propriedades*. Clique na guia *Log On* (Logon) e atualize a senha de *logon as* (logon como). Clique em *Aplicar* e em *OK*.



4. Se tiver o Consultor instalado, você precisará atualizar a propriedade "Executar como" (*Painel de Controle >Tarefas Programadas > clique o botão direito do mouse em Propriedades*) da(s) tarefa(s) Programadas do Consultor.
5. Clique em *Definir senha*. Digite a nova senha duas vezes e clique em *OK*. Clique em *Aplicar* e em *OK*.

Mudando a senha do Usuário de Relatório do Sentinel

Mudando a senha do Usuário de Relatório do Sentinel

1. Use o Sistema Operacional Windows para mudar a senha.

11 Telas do banco de dados do Sentinel para Oracle

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

Este capítulo lista as Telas do Esquema do Sentinel para Oracle. As telas oferecem informações para a criação de relatórios próprios (Crystal Reports).

Telas

ADV_ALERT_CVE_RPT_V

A tela faz referência à tabela ADV_ALERT_CVE, que armazena o número de identificação de alerta do Consultor.

Nome da coluna	Tipo de dados	Comentário
ALERT_ID	número	Identificador de anotação - número de seqüência.
CVE	varchar2	
DATE_CREATED	data	Inserir data
DATE_MODIFIED	data	Data da última atualização
CREATED_BY	número	Por ID de usuário
MODIFIED_BY	número	Por ID de usuário

ADV_ALERT_PRODUCT_RPT_V

A tela faz referência à tabela ADV_ALERT_PRODUCT, que armazena informações sobre produtos do Consultor, como número de ID de service pack, versão e data de criação.

Nome da coluna	Tipo de dados	Comentário
ALERT_ID	número	Identificador de anotação - número de seqüência.
SERVICE_PACK_ID	número	
VENDOR	varchar2	
PRODUCT	varchar2	
VERSION	varchar2	Contém o número de versão
SERVICE_PACK_ID	varchar2	
PRIMARY_FLAG	número	
DATE_CREATED	data	Inserir data
DATE_MODIFIED	data	Data da última atualização
CREATED_BY	número	Por ID de usuário
MODIFIED_BY	número	Por ID de usuário

ADV_ALERT_RPT_V

A tela faz referência à tabela ADV_ALERT_PRODUCT, que armazena informações sobre alertas do Consultor, como nome, tipo de ameaça e data de publicação.

Nome da coluna	Tipo de dados	Comentário
ALERT_ID	número	Identificador de anotação - número de seqüência.
VERSION	número	Contém o número de versão
TEMPLATE_ID	número	
TEMPLATE_NAME	varchar2	
THREAT_CATEGORY_NAME	varchar2	
THREAT_TYPE_NAME	varchar2	
HEADLINE	clob	
FIRST_PUBLISHED	data	
LAST_PUBLISHED	data	
STATUS	varchar2	
URGENCY_ID	número	
CREDIBILITY_ID	número	
SEVERITY_ID	número	
SUMMARY	clob	
LEGAL_DISCLAIMER	clob	
COPYRIGHT	varchar2	
BEGIN_EFFECTIVE_DATE	data	
END_EFFECTIVE_DATE	data	
DATE_CREATED	data	Inserir data
DATE_MODIFIED	data	Data da última atualização
CREATED_BY	número	Por ID de usuário
MODIFIED_BY	número	Por ID de usuário

ADV_ATTACK_ALERT_RPT_V

A tela faz referência à tabela ADV_ATTACK_PRODUCT, que armazena informações sobre ataques do Consultor, como nome, tipo de ameaça e data de publicação.

Nome da coluna	Tipo de dados	Comentário
ATTACK_ID	número	
ALERT_ID	número	
DATE_CREATED	data	Inserir data
DATE_MODIFIED	data	Data da última atualização
CREATED_BY	número	Por ID de usuário
MODIFIED_BY	número	Por ID de usuário

ADV_ATTACK_CVE_RPT_V

A tela faz referência à tabela ADV_ATTACK_CVE, que armazena informações CVE do Consultor.

Nome da coluna	Tipo de dados	Comentário
ATTACK_ID	número	
CVE	varchar2	

Nome da coluna	Tipo de dados	Comentário
DATE_CREATED	data	Inserir data
DATE_MODIFIED	data	Data da última atualização
CREATED_BY	número	Por ID de usuário
MODIFIED_BY	número	Por ID de usuário

ADV_ATTACK_MAP_RPT_V

A tela faz referência à tabela ADV_ATTACK_MAP, que armazena informações sobre mapas do Consultor.

Nome da coluna	Tipo de dados	Comentário
ATTACK_KEY	número	
ATTACK_ID	número	
SERVICE_PACK_ID	número	
ATTACK_NAME	varchar2	
ATTACK_CODE	varchar2	
DATE_CREATED	data	Inserir data
DATE_MODIFIED	data	Data da última atualização
CREATED_BY	número	Por ID de usuário
MODIFIED_by	número	Por ID de usuário

ADV_ATTACK_PLUGIN_RPT_V

View references ADV_ATTACK_PLUGIN table that stores Advisor plug-in information.

Nome da coluna	Tipo de dados	Comentário
PLUGIN_KEY	número	
ATTACK_ID	número	
SERVICE_PACK_ID	número	
PLUGIN_ID	varchar2	
PLUGIN_NAME	varchar2	
DATE_CREATED	data	Inserir data
DATE_MODIFIED	data	Data da última atualização
CREATED_BY	número	Por ID de usuário
MODIFIED_BY	número	Por ID de usuário

ADV_ATTACK_RPT_V

A tela faz referência à tabela ADV_ATTACK, que armazena informações sobre ataques do Consultor.

Nome da coluna	Tipo de dados	Comentário
ALERT_ID	número	
TRUSECURE_ATTACK_NAME	número	
FEED_DATE_CREATED	data	
FEED_DATE_UPDATED	data	
ATTACK_CATEGORY	varchar2	
URGENCY_ID	número	
SEVERITY_ID	número	

Nome da coluna	Tipo de dados	Comentário
LOCAL	número	
REMOTE	número	
BEGIN_EFFECTIVE_DATE	data	
END_EFFECTIVE_DATE	data	
DESCRIPTION	clob	
SCENARIO	clob	
IMPACT	clob	
SAFEGUARDS	clob	
PATCHES	clob	
FALSE_POSITIVES	clob	
DATE_CREATED	data	Inserir data
DATE_MODIFIED	data	Data da última atualização
CREATED_BY	número	Por ID de usuário
MODIFIED_BY	número	Por ID de usuário

ADV_CREDIBILITY_RPT_V

A tela faz referência à tabela ADV_CREDIBILITY, que armazena informações sobre credibilidade do Consultor.

Nome da coluna	Tipo de dados	Comentário
CREDIBILITY_ID	número	
CREDIBILITY_RATING	varchar2	
CREDIBILITY_EXPLANATION	varchar2	
DATE_CREATED	data	Inserir data
DATE_MODIFIED	data	Data da última atualização
CREATED_BY	número	Por ID de usuário
MODIFIED_BY	número	Por ID de usuário

ADV_FEED_RPT_V

A tela faz referência à tabela ADV_FEED, que armazena informações sobre feeds do Consultor, como nome e data do feed.

Nome da coluna	Tipo de dados	Comentário
FEED_NAME	varchar2	
FEED_FILE	varchar2	
BEGIN_DATE	data	
END_DATE	data	
FEED_INSERT	número	
FEED_UPDATE	número	
FEED_EXPIRE	número	

ADV_PRODUCT_RPT_V

A tela faz referência à tabela ADV_PRODUCT, que armazena informações sobre produtos do Consultor, como fornecedor e ID do produto.

Nome da coluna	Tipo de dados	Comentário
PRODUCT_ID	número	
VENDOR_ID	número	
PRODUCT_CATEGORY_ID	número	
PRODUCT_CATEGORY_NAME	varchar2	
PRODUCT_TYPE-ID	número	
PRODUCT_TYPE_NAME	varchar2	
PRODUCT_NAME	varchar2	
PRODUCT_DESCRIPTION	varchar2	
FEED_DATE_CREATED	data	
FEED_DATE_UPDATED	data	
ACTIVE_FLAG	número	
DATE_CREATED	data	Inserir data
DATE_MODIFIED	data	Data da última atualização
CREATED_BY	número	Por ID de usuário
MODIFIED_BY	número	Por ID de usuário

ADV_PRODUCT_SERVICE_PACK_RPT_V

A tela faz referência à tabela ADV_PRODUCT_SERVICE _PACK, que armazena informações sobre service pack do Consultor, como nome do service pack, ID versão e data.

Nome da coluna	Tipo de dados	Comentário
SERVICE_PACK_ID	número	
VERSION_ID	número	Contém o número de ID de versão
SERVICE_PACK_NAME	varchar2	
FEED_DATE_CREATED	data	
FEED_DATE_UPDATED	data	
ACTIVE_FLAG	número	
BEGIN_EFFECTIVE_DATE	data	
END_EFFECTIVE_DATE	data	
DATE_CREATED	data	Inserir data
DATE_MODIFIED	data	Data da última atualização
CREATED_BY	número	Por ID de usuário
MODIFIED_BY	número	Por ID de usuário

ADV_PRODUCT_VERSION_RPT_V

A tela faz referência à tabela ADV_PRODUCT_VERSION, que armazena informações sobre versões de produtos do Consultor, como nome da versão, produto e ID da versão.

Nome da coluna	Tipo de dados	Comentário
VERSION_ID	número	Contém o número de ID de versão
PRODUCT_ID	número	
VERSION_NAME	varchar2	
FEED_DATE_CREATED	data	
FEED_DATE_UPDATED	data	
ACTIVE_FLAG	número	
DATE_CREATED	data	Inserir data
DATE_MODIFIED	número	Data da última atualização
CREATED_BY	número	Por ID de usuário
MODIFIED_BY	número	Por ID de usuário

ADV_SEVERITY_RPT_V

A tela faz referência à tabela ADV_SEVERITY, que armazena informações sobre classificação de gravidade do Consultor.

Nome da coluna	Tipo de dados	Comentário
SEVERITY_ID	número	
SEVERITY_RATING	varchar2	
SEVERITY_EXPLANATION	varchar2	
DATE_CREATED	data	Inserir data
DATE_MODIFIED	data	Data da última atualização
CREATED_BY	número	Por ID de usuário
MODIFIED_BY	número	Por ID de usuário

ADV_SUBALERT_RPT_V

A tela faz referência à tabela ADV_SUBALERT.

Nome da coluna	Tipo de dados	Comentário
ALERT_ID	número	
SUBALERT_ID	número	
CHANGED_SECTIONS	varchar2	
VARIANTS	clob	
VIRUS_NAME	clob	
DESCRIPTION	clob	
IMPACT	clob	
WARNING_INDICATORS	clob	
TECHNICAL_INFO	clob	
TRUSECURE_COMMENTS	clob	
VENDOR_ANNOUNCEMENTS	clob	
SAFEGUARDS	clob	

Nome da coluna	Tipo de dados	Comentário
PATCHES_SOFTWARE	clob	
ALERT_HISTORY	clob	
BACKGROUND_INFO	clob	
DATE_CREATED	data	Inserir data
DATE_MODIFIED	data	Data da última atualização
CREATED_BY	número	Por ID de usuário
MODIFIED_BY	número	Por ID de usuário

ADV_URGENCY_RPT_V

A tela faz referência à tabela ADV_URGENCY.

Nome da coluna	Tipo de dados	Comentário
URGENCY_ID	número	
URGENCY_RATING	varchar2	
URGENCY_EXPLANATION	varchar2	
DATE_CREATED	data	Inserir data
DATE_MODIFIED	data	Data da última atualização
CREATED_BY	número	Por ID de usuário
MODIFIED_BY	número	Por ID de usuário

ADV_VENDOR_RPT_V

A tela faz referência à tabela ADV_VENDOR, que armazena informações sobre endereços do Consultor.

Nome da coluna	Tipo de dados	Comentário
VENDOR_ID	número	
VENDOR_NAME	varchar2	
CONTACT_PERSON	varchar2	
ADDRESS_LINE_1	varchar2	
ADDRESS_LINE_2	varchar2	
ADDRESS_LINE_3	varchar2	
ADDRESS_LINE_4	varchar2	
CITY	varchar2	
STATE	varchar2	
COUNTRY	varchar2	
ZIP_CODE	varchar2	
URL	varchar2	
PHONE	varchar2	
FAX	varchar2	
EMAIL	varchar2	
PAGER	varchar2	
FEED_DATE_CREATED	data	
FEED_DATE_UPDATED	data	
ACTIVE_FLAG	número	

Nome da coluna	Tipo de dados	Comentário
DATE_CREATED	data	Inserir data
DATE_MODIFIED	data	Data da última atualização
CREATED_BY	número	Por ID de usuário
MODIFIED_BY	número	Por ID de usuário

ADV_VULN_PRODUCT_RPT_V

A tela faz referência à tabela ADV_VULN_PRODUCT, que armazena IDs de ataques a vulnerabilidades e IDs de service packs do Consultor.

Nome da coluna	Tipo de dados	Comentário
ATTACK_ID	número	
SERVICE_PACK_ID	número	
DATE_CREATED	data	Inserir data
DATE_MODIFIED	data	Data da última atualização
CREATED_BY	número	Por ID de usuário
MODIFIED_BY	número	Por ID de usuário

ANNOTATIONS_RPT_V

A tela faz referência à tabela ANNOTATIONS, que armazena documentação ou notas que podem ser associadas a objetos no sistema Sentinel, como incidentes.

Nome da coluna	Tipo de dados	Comentário
ANN_ID	NUMBER	Identificador de anotação - número de seqüência.
TEXT	VARCHAR2(4000)	Documentação ou notas.
DATE_CREATED	DATE	Inserir data
DATE_MODIFIED	DATE	Data da última atualização
MODIFIED_BY	NUMBER	ID do usuário que fez a última atualização
CREATED_BY	NUMBER	ID do usuário que fez a inserção
ACTION	varchar2	Ação

ASSET_CTGRY_RPT_V

A tela faz referência à tabela ASSET_CTGRY, que armazena informações sobre categorias de bens (por ex.: hardware, software, SO, banco de dados etc...).

Nome da coluna	Tipo de dados	Comentário
ASSET_CATAGORY_ID	número	Identificador de categoria de bem
ASSET_CATAGORY_NAME	varchar2(100)	Nome de categoria de bem
DATE_CREATED	data	Inserir data
DATE_MODIFIED	data	Data da última atualização
CREATED_BY	número	ID do usuário que fez a inserção
MODIFIED_BY	número	ID do usuário que fez a última atualização

ASSET_HOSTNAME_RPT_V

A tela faz referência à tabela ASSET_HOSTNAME, que armazena informações sobre nomes de hosts alternativos para bens.

Nome da coluna	Tipo de dados	Comentário
ASSET_HOSTNAME_ID	Varchar2(36)	Identificador de nome de host alternativo de bem
PHYSICAL_ASSET_ID	varchar2(36)	Identificador de bem físico
HOST_NAME	varchar2	Nome de host
CUSTOMER_ID	número	Identificador de cliente
DATE_CREATED	data	Data da última atualização
DATE_MODIFIED	data	ID do usuário que fez a última atualização
CREATED_BY	número	ID do usuário que fez a inserção
MODIFIED_BY	número	ID do usuário que fez a última atualização

ASSET_IP_RPT_V

A tela faz referência à tabela ASSET_IP, que armazena informações sobre endereços IP alternativos para bens.

Nome da coluna	Tipo de dados	Comentário
ASSET_IP_ID	Varchar2(36)	Identificador de IP alternativo de bem
PHYSICAL_ASSET_ID	varchar2(36)	Identificador de bem físico
IP_ADDRESS	número	Endereço IP de bem
CUSTOMER_ID	número	Identificador de cliente
DATE_CREATED	data	Inserir data
DATE_MODIFIED	data	Data da última atualização
CREATED_BY	número	ID do usuário que fez a inserção
MODIFIED_BY	número	ID do usuário que fez a última atualização

ASSET_LOCATION_RPT_V

A tela faz referência à tabela ASSET_LOC, que armazena informações sobre locais de bens.

Nome da coluna	Tipo de dados	Comentário
LOCATION_ID	número	Identificador de local
CUSTOMER_ID	número	Identificador de cliente
BUILDING_NAME	varchar2(255)	Nome do prédio
ADDRESS_LINE_1	varchar2(255)	Linha de endereço 1
ADDRESS_LINE_2	varchar2(255)	Linha de endereço 2
CITY	varchar2(100)	Cidade
STATE	varchar2(100)	Estado
COUNTRY	varchar2(100)	País
ZIP_CODE	varchar2(50)	CEP
DATE_CREATED	data	Inserir data
DATE_MODIFIED	data	Data da última atualização
CREATED_BY	número	ID do usuário que fez a inserção
MODIFIED_BY	número	ID do usuário que fez a última atualização

ASSET_RPT_V

A tela faz referência à tabela ASSET, que armazena informações sobre os bens físicos e intangíveis.

Nome da coluna	Tipo de dados	Comentário
ASSET_ID	varchar2(36)	Identificador do bem
CUSTOMER_ID	número	Identificador de cliente
ASSET_NAME	varchar2(255)	Nome do bem
PHYSICAL_ASSET_ID	varchar2(36)	Identificador de bem físico
PRDT_ID	número	Identificador de produtos
ASSET_CATEGORY_ID	número	Identificador de categoria de bem
ENVIRONMENT_IDENTITY_CD	varchar2(5)	Código de identidade do ambiente
PHYSICAL_ASSET_IND	número(1)	Indicador de bem físico
ASSET_VALUE_CODE	varchar2(5)	Código de valor do bem
CRITICALITY_CODE	varchar2(5)	Código de importância do bem
SENSITIVITY_CODE	varchar2(5)	Código de distinção do bem
DATE_CREATED	data	Inserir data
DATE_MODIFIED	data	Data da última atualização
CREATED_BY	número	ID do usuário que fez a inserção
MODIFIED_BY	número	ID do usuário que fez a última atualização

ASSET_VALUE_RPT_V

A tela faz referência à tabela ASSET_VAL_LKUP, que armazena informações sobre o valor do bem.

Nome da coluna	Tipo de dados	Comentário
ASSET_VALUE_CODE	varchar2(5)	Código de valor do bem
ASSET_VALUE_NAME	varchar2(50)	Nome do valor do bem
DATE_CREATED	data	Inserir data
DATE_MODIFIED	data	Data da última atualização
CREATED_BY	número	ID do usuário que fez a inserção
MODIFIED_BY	número	ID do usuário que fez a última atualização

ASSET_X_ENTITY_X_ROLE_RPT_V

A tela faz referência à tabela ASSET_X_ENTITY_X_ROLE, que associa uma pessoa ou uma organização a um bem.

Nome da coluna	Tipo de dados	Comentário
PERSON_ID	varchar2(36)	Identificador de pessoa
ORGANIZATION_ID	varchar2(36)	Identificador de organização
ROLE_CODE	varchar2(5)	Código de função
ASSET_ID	varchar2(36)	Identificador do bem
ENTITY_TYPE_CODE	varchar2(5)	Código de tipo de entidade
PERSON_ROLE_SEQUENCE	número	Ordem de pessoas em uma determinada função
DATE_CREATED	data	Inserir data
DATE_MODIFIED	data	Data da última atualização

Nome da coluna	Tipo de dados	Comentário
CREATED_BY	número	ID do usuário que fez a inserção
MODIFIED_BY	número	Usuário que fez a última atualização

ASSOCIATIONS_RPT_V

A tela faz referência à tabela ASSOCIATIONS, que associa usuários a incidentes, incidentes a anotações, etc.

Nome da coluna	Tipo de dados	Comentário
TABLE1	VARCHAR2(64)	Nome da tabela 1. Por exemplo, incidentes
ID1	VARCHAR2(36)	ID1. Por exemplo, ID do incidente.
TABLE2	VARCHAR2(64)	Nome da tabela 2. Por exemplo, usuários
ID2	VARCHAR2(36)	ID2. Por exemplo, ID do usuário.
DATE_CREATED	DATE	Inserir data.
DATE_MODIFIED	DATE	Data da última atualização
CREATED_BY	NUMBER	ID do usuário que fez a inserção
MODIFIED_BY	NUMBER	ID do usuário que fez a última atualização

ATTACHMENTS_RPT_V

A tela faz referência à tabela ATTACHMENTS, que armazena dados sobre anexos.

Nome da coluna	Tipo de dados	Comentário
ATTACHMENT_ID	número	Identificador do anexo
NAME	varchar2(255)	Nome do anexo
SOURCE_REFERENCE	varchar2(64)	Referência da fonte
TYPE	varchar2(32)	Tipo do anexo
SUB_TYPE	varchar2(32)	Subtipo do anexo
FILE_EXTENSION	varchar2(32)	Extensão do arquivo
ATTACHMENT_DESCRIPTION	varchar2(255)	Descrição do anexo
DATA	clob	Dados do anexo
DATE_CREATED	data	Inserir data
DATE_MODIFIED	data	Data da última atualização
CREATED_BY	número	ID do usuário que fez a inserção
MODIFIED_BY	número	ID do usuário que fez a última atualização

CONFIGS_RPT_V

A tela faz referência à tabela CONFIGS, que armazena informações sobre configuração geral do aplicativo.

Nome da coluna	Tipo de dados	Comentário
USR_ID	VARCHAR2(32)	Nome do usuário.
APPLICATION	VARCHAR2(255)	Identificador do aplicativo
UNIT	VARCHAR2(64)	Unidade do aplicativo
VALUE	VARCHAR2(255)	Valor de texto, se houver
DATA	CLOB	Dados XML

Nome da coluna	Tipo de dados	Comentário
DATE_CREATED	DATE	Inserir data.
DATE_MODIFIED	DATE	Data da última atualização.
CREATED_BY	NUMBER	ID do usuário que fez a inserção.
MODIFIED_BY	NUMBER	ID do usuário que fez a última atualização.

CONTACTS_RPT_V

A tela faz referência à tabela CONTACTS, que armazena informações de contato.

Nome da coluna	Tipo de dados	Comentário
CNT_ID	NUMBER	ID do contato – Número de seqüência
FIRST_NAME	VARCHAR2(20)	Nome do contato.
LAST_NAME	VARCHAR2(30)	Sobrenome do contato.
TITLE	VARCHAR2(128)	Título do contato
DEPARTMENT	VARCHAR2(128)	Departamento
PHONE	VARCHAR2(64)	Telefone do contato
EMAIL	VARCHAR2(255)	E-mail do contato
PAGER	VARCHAR2(64)	Pager do contato
CELL	VARCHAR2(64)	Telefone celular do contato
DATE_CREATED	DATE	Inserir data
DATE_MODIFIED	DATE	Data da última atualização
CREATED_BY	NUMBER	ID do usuário que fez a inserção
MODIFIED_BY	NUMBER	ID do usuário que fez a última atualização

CORRELATED_EVENTS_RPT_V

A tela faz referência à tabela CORRELATED_EVENTS_*, que armazena informações sobre eventos correlacionados.

Nome da coluna	Tipo de dados	Comentário
PARENT_EVT_ID	varchar2	Identificador Exclusivo Universal (UUID) do evento pai
CHILD_EVT_ID	varchar2	Identificador Exclusivo Universal (UUID) do evento filho
PARENT_EVT_TIME	DATE	Horário do evento pai
CHILD_EVT_TIME	DATE	Horário do evento filho
DATE_CREATED	DATE	Inserir data criada por DAS
DATE_MODIFIED	DATE	Data da última atualização
CREATED_BY	NUMBER	ID do usuário que fez a inserção
MODIFIED_BY	NUMBER	ID do usuário que fez a última atualização

CORRELATED_EVENTS_RPT_V1

A tela contém eventos atuais e históricos correlacionados (eventos correlacionados importados dos arquivos).

Nome da coluna	Tipo de dados	Comentário
PARENT_EVT_ID	varchar2	Identificador Exclusivo Universal (UUID) do evento pai
CHILD_EVT_ID	varchar2	Identificador Exclusivo Universal (UUID) do evento filho
PARENT_EVT_TIME	DATE	Horário do evento pai
CHILD_EVT_TIME	DATE	Horário do evento filho
DATE_CREATED	DATE	Inserir data criada por DAS
DATE_MODIFIED	DATE	Data da última atualização
CREATED_BY	NUMBER	ID do usuário que fez a inserção
MODIFIED_BY	NUMBER	ID do usuário que fez a última atualização

CRITICALITY_RPT_V

A tela faz referência à tabela CRIT_LKUP, que contém informações sobre a importância dos bens.

Nome da coluna	Tipo de dados	Comentário
CRITICALITY_CODE	varchar2(5)	Código de importância do bem
CRITICALITY_NAME	varchar2(50)	Nome da importância do bem
DATE_CREATED	data	Inserir data
DATE_MODIFIED	data	Data da última atualização
CREATED_BY	número	Por ID de usuário
MODIFIED_BY	número	Por ID de usuário

CUST_RPT_V

A tela faz referência à tabela CUST, que armazena informações de clientes para MSSPs.

Nome da coluna	Tipo de dados	Comentário
CUSTOMER_ID	número	Identificador de cliente
CUSTOMER_NAME	varchar2(255)	Nome do cliente
DATE_CREATED	data	Inserir data
DATE_MODIFIED	data	Data da última atualização
CREATED_BY	número	ID do usuário que fez a inserção
MODIFIED_BY	número	ID do usuário que fez a última atualização

ENTITY_TYPE_RPT_V

A tela faz referência à tabela ENTITY_TYP, que armazena informações sobre tipos de entidades (pessoa ou organização).

Nome da coluna	Tipo de dados	Comentário
ENTITY_TYPE_CODE	varchar2(5)	Código de tipo de entidade
ENTITY_TYPE_NAME	varchar2(50)	Nome do tipo de entidade

Nome da coluna	Tipo de dados	Comentário
DATE_CREATED	data	Inserir data
DATE_MODIFIED	data	Data da última atualização
CREATED_BY	número	ID do usuário que fez a inserção
MODIFIED_BY	número	ID do usuário que fez a última atualização

ENV_IDENTITY_RPT_V

A tela faz referência à tabela ENV_IDENTITY_LKUP, que armazena informações sobre a identidade do ambiente do bem.

Nome da coluna	Tipo de dados	Comentário
ENVIRONMENT_IDENTITY_CODE	varchar2(5)	Código de identidade do ambiente
ENVIRONMENT_IDENTITY_NAME	varchar2(255)	Nome da identidade do ambiente
DATE_CREATED	data	Inserir data
DATE_MODIFIED	data	Data da última atualização
CREATED_BY	número	ID do usuário que fez a inserção
MODIFIED_BY	número	ID do usuário que fez a última atualização

ESEC_DISPLAY_RPT_V

A tela faz referência à tabela ESEC_DISPLAY, que armazena propriedades de objetos que podem ser exibidas. Usada atualmente para renomear metatags. Usada com a Configuração de Eventos (Relevância Comercial).

Nome da coluna	Tipo de dados	Comentário
DISPLAY_OBJECT	VARCHAR2(32)	Objeto pai da propriedade
TAG	VARCHAR2(32)	Nome da tag nativa da propriedade
LABEL	VARCHAR2(32)	String de exibição da tag.
POSITION	NUMBER	Posição da tag na exibição.
WIDTH	NUMBER	Largura da coluna
ALIGNMENT	NUMBER	Alinhamento horizontal
FORMAT	NUMBER	Formatador enumerado para exibição da propriedade
ENABLED	VARCHAR2(1)	Indica se a tag é mostrada.
TYPE	NUMBER	Indica o tipo de dados da tag. 1 = string 2 = ulong 3 = data 4 = uuid 5 = ipv4
DESCRIPTION	VARCHAR2(255)	Descrição textual da tag
DATE_CREATED	DATE	Inserir data.
DATE_MODIFIED	DATE	Data da última atualização.
CREATED_BY	NUMBER	ID do usuário que fez a inserção.

Nome da coluna	Tipo de dados	Comentário
MODIFIED_BY	NUMBER	ID do usuário que fez a última atualização.
REF_CONFIG	VARCHAR2(4000)	Configuração de Dados Referenciais

ESEC_PORT_REFERENCE_RPT_V

A tela faz referência à tabela ESEC_PORT_REFERENCE, que armazena números de portas padrão atribuídas pela indústria.

Nome da coluna	Tipo de dados	Comentário
PORT_NUMBER	NUMBER	Em http://www.iana.org/assignments/port-numbers, a representação numérica da porta. Esse número de porta é geralmente associado ao nível de Protocolo de Transporte na pilha TCP/IP.
PROTOCOL_NUMBER	NUMBER	Em http://www.iana.org/assignments/protocol-numbers, os identificadores numéricos usados para representar protocolos encapsulados em um pacote IP.
PORT_KEYWORD	VARCHAR2(64)	Em http://www.iana.org/assignments/port-numbers, a representação de palavra-chave da porta.
PORT_DESCRIPTION	VARCHAR2(512)	Descrição da porta.
DATE_CREATED	DATE	Inserir data.
DATE_MODIFIED	DATE	Data da última atualização.
CREATED_BY	NUMBER	ID do usuário que fez a inserção.
MODIFIED_BY	NUMBER	ID do usuário que fez a última modificação.

ESEC_PROTOCOL_REFERENCE_RPT_V

A tela faz referência à tabela ESEC_PROTOCOL_REFERENCE, que armazena números de protocolo padrão atribuídos pela indústria.

Nome da coluna	Tipo de dados	Comentário
PROTOCOL_NUMBER	NUMBER	Em http://www.iana.org/assignments/protocol-numbers, os identificadores numéricos usados para representar protocolos encapsulados em um pacote IP.

Nome da coluna	Tipo de dados	Comentário
PROTOCOL_KEYWORD	VARCHAR2(64)	Em http://www.iana.org/assignments/protocol-numbers, as palavras-chave usadas para representar protocolos encapsulados em um pacote IP.
PROTOCOL_DESCRIPTION	VARCHAR2(512)	Descrição de protocolo de pacote IP.
DATE_CREATED	DATE	Inserir data.
DATE_MODIFIED	DATE	Data da última atualização.
CREATED_BY	NUMBER	ID do usuário que fez a inserção.
MODIFIED_BY	NUMBER	ID do usuário que fez a última atualização.

ESEC_SEQUENCE _RPT_V

A tela faz referência à tabela ESEC_SEQUENCE, que é usada para gerar números de seqüência de chave principal para tabelas do Sentinel.

Nome da coluna	Tipo de dados	Comentário
TABLE_NAME	VARCHAR2(32)	Nome da tabela.
COLUMN_NAME	VARCHAR2(32)	Nome da coluna
SEED	NUMBER	Valor atual do campo da chave principal.
DATE_CREATED	DATE	Inserir data.
DATE_MODIFIED	DATE	Data da última atualização.
CREATED_BY	NUMBER	ID do usuário que fez a inserção.
MODIFIED_BY	NUMBER	ID do usuário que fez a última atualização.

EVENTS_ALL_RPT_V (Fornecida para fins de compatibilidade retroativa)

A tela contém eventos atuais e históricos (eventos importados dos arquivos).

Nome da coluna	Tipo de dados	Comentário
EVENT_ID	varchar2	Identificador do evento
RESOURCE_NAME	varchar2(255)	Nome do recurso
SUB_RESOURCE	varchar2(255)	Nome do subrecurso
SEVERITY	número	Gravidade do evento
EVENT_PARSE_TIME	data	Horário do evento
EVENT_DATE_TIME	data	Horário do evento
BASE_MESSAGE	varchar2(4000)	Mensagem base
EVENT_NAME	varchar2(255)	Nome do evento conforme relatado pelo sensor
EVENT_TIME	varchar2(255)	Horário do evento conforme relatado pelo sensor
SENSOR_NAME	varchar2(255)	Nome do sensor

Nome da coluna	Tipo de dados	Comentário
SENSOR_TYPE	varchar2(5)	Tipo de sensor: H – baseado em host N – baseado em rede V – vírus O – outro
PROTOCOL	varchar2(255)	Nome do protocolo
SOURCE-IP	número	Endereço IP de origem em formato numérico
SOURCE_HOST_NAME	varchar2(255)	Nome do host de origem
SOURCE_PORT	varchar2(32)	Porta de origem
DESTINATION_IP	número	Endereço IP de destino em formato numérico
DESTINATION_HOST_NAME	varchar2(255)	Nome do host de destino
DESTINATION_PORT	varchar2(32)	Porta de destino
SOURCE_USER_NAME	varchar2(255)	Nome do usuário de origem
DESTINATION_USER_NAME	varchar2(255)	Nome do usuário de destino
FILE_NAME	varchar2(1000)	Nome do arquivo
EXTENDED_INFO	varchar2(1000)	Informações completas
REPORT_NAME	varchar2(255)	Nome do relator
PRODUCT_NAME	varchar2(255)	Nome de produto de relatórios
CUSTOM_TAG_1	varchar2(255)	Tag de Cliente 1
CUSTOM_TAG_2	varchar2(255)	Tag de Cliente 2
CUSTOM_TAG_3	número	Tag de Cliente 3
RESERVED_TAG_1	VARCHAR2(255)	Tag Reservada 1 Reservada para uso futuro da Novell. Campo usado para informações do Advisor sobre descrições de ataque.
RESERVED_TAG_2	varchar2(255)	Reservada para uso futuro da Novell. O uso desse campo para qualquer outra finalidade pode resultar em sobregravação de dados por uma funcionalidade futura.
RESERVED_TAG_3	número	Reservada para uso futuro da Novell. O uso desse campo para qualquer outra finalidade pode resultar em sobregravação de dados por uma funcionalidade futura.
SOURCE_UUID	varchar(36)	UUID de origem
PORT	varchar(64)	Porta do Coletor
AGENT	varchar2(64)	Nome do Coletor
VULNERABILITY_RATING	número	Classificação de vulnerabilidade
CRITICALITY_RATING	número	Classificação de importância
DATE_CREATED	data	Inserir data
DATE_MODIFIED	data	Data da última atualização
CREATED_BY	número	Por ID de usuário

Nome da coluna	Tipo de dados	Comentário
MODIFIED_BY	número	Por ID de usuário
RV01 - 10	NUMBER	Valores reservados de 1 a 10 Reservada para uso futuro da Novell. O uso desse campo para qualquer outra finalidade pode resultar em sobregravação de dados por uma funcionalidade futura.
RV11 - 20	DATE	Valores reservados de 11 a 20 Reservada para uso futuro da Novell. O uso desse campo para qualquer outra finalidade pode resultar em sobregravação de dados por uma funcionalidade futura.
RV21 - 25	varchar2	Valores reservados de 21 a 25 Reservada para uso futuro da Novell para o armazenamento de UUIDs. O uso desse campo para qualquer outra finalidade pode resultar em sobregravação de dados por uma funcionalidade futura.
RV26 - 31	VARCHAR2(255)	Valores reservados de 26 a 31 Reservada para uso futuro da Novell. O uso desse campo para qualquer outra finalidade pode resultar em sobregravação de dados por uma funcionalidade futura.
RV32	VARCHAR2(255)	Valor reservado - 32 Reservado para o DeviceCategory O uso desse campo para qualquer outra finalidade pode resultar em sobregravação de dados por uma funcionalidade futura.
RV33	VARCHAR2(255)	Valor reservado - 33 Reservado para o EventContex O uso desse campo para qualquer outra finalidade pode resultar em sobregravação de dados por uma funcionalidade futura.

Nome da coluna	Tipo de dados	Comentário
RV34	VARCHAR2(255)	Valor reservado - 34 Reservado para o SourceThreatLevel O uso desse campo para qualquer outra finalidade pode resultar em sobregravação de dados por uma funcionalidade futura.
RV35	VARCHAR2(255)	Valor reservado - 35 Reservado para o SourceUserContext. O uso desse campo para qualquer outra finalidade pode resultar em sobregravação de dados por uma funcionalidade futura.
RV36	VARCHAR2(255)	Valor reservado - 36 Reservado para o DataContext. O uso desse campo para qualquer outra finalidade pode resultar em sobregravação de dados por uma funcionalidade futura.
RV37	VARCHAR2(255)	Valor reservado - 37 Reservado para o SourceFunction. O uso desse campo para qualquer outra finalidade pode resultar em sobregravação de dados por uma funcionalidade futura.
RV38	VARCHAR2(255)	Valor reservado - 38 Reservado para o SourceOperationalContext. O uso desse campo para qualquer outra finalidade pode resultar em sobregravação de dados por uma funcionalidade futura.
RV39	VARCHAR2(255)	Valor reservado - 39 Reservado para o MSSPCustomerName. O uso desse campo para qualquer outra finalidade pode resultar em sobregravação de dados por uma funcionalidade futura.
RV40 - 43	VARCHAR2(255)	Valores reservados de 40 a 43 Reservada para uso futuro da Novell. O uso desse campo para qualquer outra finalidade pode resultar em sobregravação de dados por uma funcionalidade futura.

Nome da coluna	Tipo de dados	Comentário
RV44	VARCHAR2(255)	Valor reservado - 44 Reservado para o DestinationThreatLevel. O uso desse campo para qualquer outra finalidade pode resultar em sobregravação de dados por uma funcionalidade futura.
RV45	VARCHAR2(255)	Valor reservado - 45 Reservado para o DestinationUserContext. O uso desse campo para qualquer outra finalidade pode resultar em sobregravação de dados por uma funcionalidade futura.
RV46	VARCHAR2(255)	Valor reservado - 46 Reservado para o VirusStatus. O uso desse campo para qualquer outra finalidade pode resultar em sobregravação de dados por uma funcionalidade futura.
RV47	VARCHAR2(255)	Valor reservado - 47 Reservada para uso futuro da Novell. O uso desse campo para qualquer outra finalidade pode resultar em sobregravação de dados por uma funcionalidade futura.
RV48	VARCHAR2(255)	Valor reservado - 48 Reservado para o DestinationOperationalContext. O uso desse campo para qualquer outra finalidade pode resultar em sobregravação de dados por uma funcionalidade futura.
RV49	VARCHAR2(255)	Valor reservado - 49 Reservada para uso futuro da Novell. O uso desse campo para qualquer outra finalidade pode resultar em sobregravação de dados por uma funcionalidade futura.
RV50	VARCHAR2(255)	Nível de taxonomia 1
RV51	VARCHAR2(255)	Nível de taxonomia 2
RV52	VARCHAR2(255)	Nível de taxonomia 3
RV53	VARCHAR2(255)	Nível de taxonomia 4

Nome da coluna	Tipo de dados	Comentário
CV01 - 10	NUMBER	Valor personalizado de 1 a 10 Reservado para o uso do Cliente, geralmente para associação de dados de relevância para a empresa
CV11 - 20	DATE	Valor personalizado de 11 a 20 Reservado para o uso do Cliente, geralmente para associação de dados de relevância para a empresa
CV21 - 100	VARCHAR2(255)	Valor personalizado de 21 a 100 Reservado para o uso do Cliente, geralmente para associação de dados de relevância para a empresa

EVENTS_ALL_RPT_V1 (Fornecida para fins de compatibilidade retroativa)

A tela contém os eventos atuais. Possui as mesmas colunas que EVENT_ALL_RPT_V.

EVENTS_RPT_V (Fornecida para fins de compatibilidade retroativa)

A tela contém os eventos atuais e históricos. Possui as mesmas colunas que EVENT_ALL_RPT_V.

EVENTS_RPT_V1 (Fornecida para fins de compatibilidade retroativa)

A tela contém os eventos atuais. Possui as mesmas colunas que EVENT_ALL_RPT_V.

EVENTS_RPT_V2 (Todos os novos relatórios do Sentinel 5 devem usar essa tela)

A tela contém os eventos atuais e históricos.

Nome da coluna	Tipo de dados	Comentário
EVENT_ID	varchar2	Identificador do evento
RESOURCE_NAME	varchar2(255)	Nome do recurso
SUB_RESOURCE	varchar2(255)	Nome do subrecurso
SEVERITY	número	Gravidade do evento
EVENT_PARSE_TIME	data	Horário do evento
EVENT_DATETIME	data	Horário do evento
BASE_MESSAGE	varchar2(4000)	Mensagem base
EVENT_NAME	varchar2(255)	Nome do evento conforme relatado pelo sensor
EVENT_TIME	varchar2(255)	Horário do evento conforme relatado pelo sensor
TAXONOMY_ID	número	Identificador de taxonomia
PROTOCOL_ID	número	Identificador de protocolo

Nome da coluna	Tipo de dados	Comentário
AGENT_ID	número	Identificador de Coletor
SOURCE_IP	número	Endereço IP de origem em formato numérico
SOURCE_HOST_NAME	varchar2(255)	Nome do host de origem
SOURCE_PORT	varchar2(32)	Porta de origem
DESTINATION_IP	número	Endereço IP de destino em formato numérico
DESTINATION_HOST_NAME	varchar2(255)	Nome do host de destino
DESTINATION_PORT	varchar2(32)	Porta de destino
SOURCE_USER_NAME	varchar2(255)	Nome do usuário de origem
DESTINATION_USER_NAME	varchar2(255)	Nome do usuário de destino
FILE_NAME	varchar2(1000)	Nome do arquivo
EXTENDED_INFO	varchar2(1000)	Informações estendidas
CUSTOM_TAG_1	varchar2(255)	Tag de Cliente 1
CUSTOM_TAG 2	varchar2(255)	Tag de Cliente 2
CUSTOM_TAG 3	número	Tag de Cliente 3
RESERVED_TAG_1	VARCHAR2(255)	Tag Reservada 1 Reservada para uso futuro da Novell. Campo usado para informações do Advisor sobre descrições de ataque.
RESERVED_TAG_2	varchar2(255)	Reservada para uso futuro da Novell. O uso desse campo para qualquer outra finalidade pode resultar em sobregravação de dados por uma funcionalidade futura.
RESERVED_TAG_3	número	Reservada para uso futuro da Novell. O uso desse campo para qualquer outra finalidade pode resultar em sobregravação de dados por uma funcionalidade futura.
VULNERABILITY_RATING	número	Classificação de vulnerabilidade
CRITICALITY_RATING	número	Classificação de importância
DATE_CREATED	data	Inserir data
DATE_MODIFIED	data	Data da última atualização
CREATED_BY	número	ID do usuário que fez a inserção.
MODIFIED_BY	número	ID do usuário que fez a última atualização.
RV01 - 10	NUMBER	Valores reservados de 1 a 10 Reservada para uso futuro da Novell. O uso desse campo para qualquer outra finalidade pode resultar em sobregravação de dados por uma funcionalidade futura.

Nome da coluna	Tipo de dados	Comentário
RV11 - 20	DATE	Valores reservados de 1 a 31 Reservada para uso futuro da Novell. O uso desse campo para qualquer outra finalidade pode resultar em sobregravação de dados por uma funcionalidade futura.
RV21 - 25	varchar2	Valores reservados de 21 a 25 Reservada para uso futuro da Novell para o armazenamento de UUIDs. O uso desse campo para qualquer outra finalidade pode resultar em sobregravação de dados por uma funcionalidade futura.
RV26 - 31	VARCHAR2(255)	Valores reservados de 26 a 31 Reservada para uso futuro da Novell. O uso desse campo para qualquer outra finalidade pode resultar em sobregravação de dados por uma funcionalidade futura.
RV33	VARCHAR2(255)	Valor reservado - 33 Reservado para o EventContex O uso desse campo para qualquer outra finalidade pode resultar em sobregravação de dados por uma funcionalidade futura.
RV34	VARCHAR2(255)	Valor reservado - 34 Reservado para o SourceThreatLevel O uso desse campo para qualquer outra finalidade pode resultar em sobregravação de dados por uma funcionalidade futura.
RV35	VARCHAR2(255)	Valor reservado - 35 Reservado para o SourceUserContext. O uso desse campo para qualquer outra finalidade pode resultar em sobregravação de dados por uma funcionalidade futura.
RV36	VARCHAR2(255)	Valor reservado - 36 Reservado para o DataContext. O uso desse campo para qualquer outra finalidade pode resultar em sobregravação de dados por uma funcionalidade futura.

Nome da coluna	Tipo de dados	Comentário
RV37	VARCHAR2(255)	Valor reservado - 37 Reservado para o SourceFunction. O uso desse campo para qualquer outra finalidade pode resultar em sobregravação de dados por uma funcionalidade futura.
RV38	VARCHAR2(255)	Valor reservado - 38 Reservado para o SourceOperationalContext. O uso desse campo para qualquer outra finalidade pode resultar em sobregravação de dados por uma funcionalidade futura.
RV40 - 43	VARCHAR2(255)	Valores reservados de 40 a 43 Reservada para uso futuro da Novell. O uso desse campo para qualquer outra finalidade pode resultar em sobregravação de dados por uma funcionalidade futura.
RV44	VARCHAR2(255)	Valor reservado - 44 Reservado para o DestinationThreatLevel. O uso desse campo para qualquer outra finalidade pode resultar em sobregravação de dados por uma funcionalidade futura.
RV45	VARCHAR2(255)	Valor reservado - 45 Reservado para o DestinationUserContext. O uso desse campo para qualquer outra finalidade pode resultar em sobregravação de dados por uma funcionalidade futura.
RV46	VARCHAR2(255)	Valor reservado - 46 Reservado para o VirusStatus. O uso desse campo para qualquer outra finalidade pode resultar em sobregravação de dados por uma funcionalidade futura.
RV47	VARCHAR2(255)	Valor reservado - 47 Reservada para uso futuro da Novell. O uso desse campo para qualquer outra finalidade pode resultar em sobregravação de dados por uma funcionalidade futura.

Nome da coluna	Tipo de dados	Comentário
RV48	VARCHAR2(255)	Valor reservado - 48 Reservado para o DestinationOperationalContext. O uso desse campo para qualquer outra finalidade pode resultar em sobregravação de dados por uma funcionalidade futura.
RV49	VARCHAR2(255)	Valor reservado - 49 Reservada para uso futuro da Novell. O uso desse campo para qualquer outra finalidade pode resultar em sobregravação de dados por uma funcionalidade futura.
REFERENCE_ID 01 - 20	número	Reservada para uso futuro da Novell. O uso desse campo para qualquer outra finalidade pode resultar em sobregravação de dados por uma funcionalidade futura.
CV01 - 10	NUMBER	Valor personalizado de 1 a 10 Reservado para o uso do Cliente, geralmente para associação de dados de relevância para a empresa
CV11 - 20	DATE	Valor personalizado de 11 a 20 Reservado para o uso do Cliente, geralmente para associação de dados de relevância para a empresa
CV21 - 100	VARCHAR2(255)	Valor personalizado de 21 a 100 - Reservado para o uso do Cliente, geralmente para associação de dados de relevância para a empresa

EVT_AGENT_RPT_V

A tela faz referência à tabela EVT_AGENT, que armazena informações sobre Coletores.

Nome da coluna	Tipo de dados	Comentário
AGENT_ID	número	Identificador de Coletor
AGENT	varchar2(64)	Nome do Coletor
PORT	varchar2(64)	Porta do Coletor
REPORT_NAME	varchar2(255)	Nome do relator
PRODUCT_NAME	varchar2(255)	Nome do produto
SENSOR_NAME	varchar2(255)	Nome do sensor

Nome da coluna	Tipo de dados	Comentário
SENSOR_TYPE	varchar2(5)	Tipo de sensor: H - baseado em host N - baseado em rede V - vírus O - outro
DEVICE_CTGRY	varchar2(255)	Categoria do dispositivo
SOURCE_UUID	varchar2	Identificador Exclusivo Universal (UUID) do componente de origem
DATE_CREATED	data	Inserir data
DATE_MODIFIED	data	Data da última atualização
CREATED_BY	número	ID do usuário que fez a inserção
MODIFIED_BY	número	ID do usuário que fez a última atualização

EVT_ASSET_RPT_V

A tela faz referência à tabela EVT_ASSET, que armazena informações sobre bens.

Nome da coluna	Tipo de dados	Comentário
EVENT_ASSET_ID	número	Identificador do bem do evento
ASSET_NAME	varchar2(255)	Nome do bem
PHYSICAL_ASSET_NAME	varchar2(255)	Nome do bem físico
REFERENCE_ASSET_ID	varchar2(100)	Identificador do bem de referência, que se vincula com o sistema de gerenciamento do bem de origem.
MAC_ADDRESS	varchar2(100)	Endereço MAC
RACK_NUMBER	varchar2(50)	Número do rack
ROOM_NAME	varchar2(100)	Nome da sala
BUILDING_NAME	varchar2(255)	Nome do prédio
CITY	varchar2(100)	Cidade
STATE	varchar2(100)	Estado
COUNTRY	varchar2(100)	País
ZIP_CODE	varchar2(50)	CEP
ASSET_CATEGORY_NAME	varchar2(100)	Nome de categoria de bem
NETWORK_IDENTITY_NAME	varchar2(255)	Nome da identidade da rede do bem
ENVIRONMENT_IDENTITY_NAME	varchar2(255)	Nome do ambiente
ASSET_VALUE_NAME	varchar2(50)	Nome do valor do bem
CRITICALITY_NAME	varchar2(50)	Nome da importância do bem
SENSITIVITY_NAME	varchar2(50)	Nome da distinção do bem
CONTACT_NAME_1	varchar2(255)	Nome da pessoa de contato/organização 1
CONTACT_NAME_2	varchar2(255)	Nome da pessoa de contato/organização 2
ORGANIZATION_NAME_1	varchar2(100)	Nível 1 da organização do proprietário do bem
ORGANIZATION_NAME_2	varchar2(100)	Nível 2 da organização do proprietário do bem

Nome da coluna	Tipo de dados	Comentário
ORGANIZATION_NAME_3	varchar2(100)	Nível 3 da organização do proprietário do bem
ORGANIZATION_NAME_4	varchar2(100)	Nível 4 da organização do proprietário do bem
DATE_CREATED	data	Inserir data
DATE_MODIFIED	data	Data da última atualização
CREATED_BY	número	ID do usuário que fez a inserção
MODIFIED_BY	número	ID do usuário que fez a última atualização

EVT_DEST_EVT_NAME_SMRY_1_RPT_V

Essa tela resume o total de eventos por destino, taxonomia, nome do evento, gravidade e horário do evento.

Nome da coluna	Tipo de dados	Comentário
DESTINATION_IP	número	Endereço IP de Destino
DESTINATION_EVENT_ASSET_ID	número	Identificador do bem do evento
TAXONOMY_ID	número	Identificador de taxonomia
EVENT_NAME_ID	número	Identificador do nome do evento
SEVERITY	número	Gravidade do evento
CUSTOMER_ID	número	Identificador de cliente
EVT_TIME	data	Horário do evento
EVT_COUNT	número	Total de Eventos
DATE_CREATED	data	Inserir data
DATE_MODIFIED	data	Data da última atualização
CREATED_BY	número	ID do usuário que fez a inserção
MODIFIED_BY	número	ID do usuário que fez a última atualização

EVT_DEST_SMRY_1_RPT_V

Essa tela contém informações de resumo de destino de eventos.

Nome da coluna	Tipo de dados	Comentário
DESTINATION_IP	número	Endereço IP de Destino
DESTINATION_EVENT_ASSET_ID	número	Identificador do bem do evento
DESTINATION_PORT	varchar2(32)	Porta de destino
DESTINATION_USR_ID	número	Identificador do usuário de destino
TAXONOMY_ID	número	Identificador de taxonomia
EVENT_NAME_ID	número	Identificador do nome do evento
RESOURCE_ID	número	Identificador do recurso
AGENT_ID	número	Identificador de Coletor
PROTOCOL_ID	número	Identificador de protocolo
SEVERITY	número	Gravidade do evento
CUSTOMER_ID	número	Identificador de cliente
EVENT_TIME	data	Horário do evento

Nome da coluna	Tipo de dados	Comentário
EVENT_CNT	número	Total de Eventos
DATE_CREATED	data	Inserir data
DATE_MODIFIED	data	Data da última atualização
CREATED_BY	número	ID do usuário que fez a inserção
MODIFIED_BY	número	ID do usuário que fez a última atualização

EVT_DEST_TXNMY_SMRY_1_RPT_V

Essa tela resume o total de eventos por destino, taxonomia, gravidade e horário do evento.

Nome da coluna	Tipo de dados	Comentário
DESTINATION_IP	número	Endereço IP de Destino
DESTINATION_EVENT_ASSET_ID	número	Identificador do bem do evento
TAXONOMY_ID	número	Identificador de taxonomia
SEVERITY	número	Gravidade do evento
CUSTOMER_ID	número	Identificador de cliente
EVENT_TIME	data	Horário do evento
EVENT_COUNT	número	Total de Eventos
DATE_CREATED	data	Inserir data
DATE_MODIFIED	data	Data da última atualização
CREATED_BY	número	ID do usuário que fez a inserção
MODIFIED_BY	número	ID do usuário que fez a última atualização

EVT_NAME_RPT_V

A tela faz referência à tabela EVT_NAME, que armazena informações sobre nomes de eventos.

Nome da coluna	Tipo de dados	Comentário
EVENT_NAME_ID	número	Identificador do nome do evento
EVENT_NAME	varchar2(255)	Nome do evento
DATE_CREATED	data	Inserir data
DATE_MODIFIED	data	Data da última atualização
CREATED_BY	número	ID do usuário que fez a inserção
MODIFIED_BY	número	ID do usuário que fez a última atualização

EVT_PORT_SMRY_1_RPT_V

Essa tela resume o total de eventos por porta de destino, gravidade e horário do evento.

Nome da coluna	Tipo de dados	Comentário
DESTINATION_PORT	Varchar2(32)	Porta de destino
SEVERITY	número	Gravidade do evento
CUSTOMER_ID	número	Identificador de cliente
EVENT_TIME	data	Horário do evento
EVENT_COUNT	número	Total de Eventos

Nome da coluna	Tipo de dados	Comentário
DATE_CREATED	data	Inserir data
DATE_MODIFIED	data	Data da última atualização
CREATED_BY	número	ID do usuário que fez a inserção
MODIFIED_BY	número	ID do usuário que fez a última atualização

EVT_PRTCL_RPT_V

A tela faz referência à tabela EVT_PRTCL, que armazena informações sobre protocolo.

Nome da coluna	Tipo de dados	Comentário
PROTOCOL_ID	número	Identificador de protocolo
PROTOCOL_NAME	varchar2(255)	Nome do protocolo
DATE_CREATED	data	Inserir data
DATE_MODIFIED	data	Data da última atualização
CREATED_BY	número	ID do usuário que fez a inserção
MODIFIED_BY	número	ID do usuário que fez a última atualização

EVT_RSRC_RPT_V

A tela faz referência à tabela EVT_RSRC, que armazena informações sobre recursos.

Nome da coluna	Tipo de dados	Comentário
RESOURCE_ID	número	Identificador do recurso
RESOURCE_NAME	varchar2(255)	Nome do recurso
SUBRESOURCE_NAME	varchar2(255)	Nome do subrecurso
DATE_CREATED	data	Inserir data
DATE_MODIFIED	data	Data da última atualização
CREATED_BY	número	ID do usuário que fez a inserção
MODIFIED_BY	número	ID do usuário que fez a última atualização

EVT_SEV_SMRY_1_RPT_V

Essa tela resume o total de eventos por gravidade e horário do evento.

Nome da coluna	Tipo de dados	Comentário
SEVERITY	número	Gravidade do evento
CUSTOMER_ID	número	Identificador de cliente
EVENT_TIME	data	Horário do evento
EVENT_COUNT	número	Total de Eventos
DATE_CREATED	data	Inserir data
DATE_MODIFIED	data	Data da última atualização
CREATED_BY	número	ID do usuário que fez a inserção
MODIFIED_BY	número	ID do usuário que fez a última atualização

EVT_SRC_SMRY_1_RPT_V

Essa tela contém informações de resumo de origem e destino de eventos.

Nome da coluna	Tipo de dados	Comentário
SOURCE_IP	número	Endereço IP de Origem
SOURCE_EVENT_ASSET_ID	número	Identificador do bem do evento de origem
SOURCE_PORT	varchar2(32)	Porta de origem
SOURCE_USER_ID	número	Identificador do usuário de origem
TAXONOMY_ID	número	Identificador de taxonomia
EVENT_NAME_ID	número	Identificador do nome do evento
RESOURCE_ID	número	Identificador do recurso
AGENT_ID	número	Identificador de Coletor
PROTOCOL_ID	número	Identificador de protocolo
SEVERITY	número	Gravidade do evento
CUSTOMER_ID	número	Identificador de cliente
EVENT_TIME	data	Horário do evento
EVENT_COUNT	número	Total de Eventos
DATE_CREATED	data	Inserir data
DATE_MODIFIED	data	Data da última atualização
CREATED_BY	número	ID do usuário que fez a inserção
MODIFIED_BY	número	ID do usuário que fez a última atualização

EVT_TXNMY_RPT_V

A tela faz referência à tabela EVT_TXNMY, que armazena informações sobre taxonomia.

Nome da coluna	Tipo de dados	Comentário
TAXONOMY_ID	número	Identificador de taxonomia
TAXONOMY_LEVEL_1	varchar2(100)	Nível de taxonomia 1
TAXONOMY_LEVEL_2	varchar2(100)	Nível de taxonomia 2
TAXONOMY_LEVEL_3	varchar2(100)	Nível de taxonomia 3
TAXONOMY_LEVEL_4	varchar2(100)	Nível de taxonomia 4
DATE_CREATED	data	Inserir data
DATE_MODIFIED	data	Data da última atualização
CREATED_BY	número	ID do usuário que fez a inserção
MODIFIED_BY	número	ID do usuário que fez a última atualização

EVT_USR_RPT_V

A tela faz referência à tabela EVT_USR, que armazena informações sobre usuários de eventos.

Nome da coluna	Tipo de dados	Comentário
USER_ID	número	Identificador do usuário
USER_NAME	varchar2(255)	Nome do usuário
DATE_CREATED	data	Inserir data
DATE_MODIFIED	data	Data da última atualização

Nome da coluna	Tipo de dados	Comentário
CREATED_BY	número	ID do usuário que fez a inserção
MODIFIED_BY	número	ID do usuário que fez a última atualização

EXTERNAL_DATA_RPT_V

A tela faz referência à tabela EXTERNAL_DATA, que armazena dados externos.

Nome da coluna	Tipo de dados	Comentário
EXTERNAL_DATA_ID	número	Identificador de dados externos
SOURCE_NAME	varchar2(50)	Nome de origem
SOURCE_DATA_ID	varchar2(255)	Identificador dos dados de origem
EXTERNAL_DATA	texto	Dados externos
EXTERNAL_DATA_TYPE	varchar2(10)	Tipo de dados externos
DATE_CREATED	data	Inserir data
DATE_MODIFIED	data	Data da última atualização
CREATED_BY	número	ID do usuário que fez a inserção
MODIFIED_BY	número	ID do usuário que fez a última atualização

HIST_ EVENTS_RPT_V

Ver eventos históricos (eventos restaurados dos arquivos).

HIST_ INCIDENTS_RPT_V

Ver eventos históricos (eventos restaurados dos arquivos).

IMAGES_RPT_V

A tela faz referência à tabela IMAGES, que armazena informações sobre imagens de visão geral do sistema.

Nome da coluna	Tipo de dados	Comentário
NAME	VARCHAR2(128)	Nome da imagem
TYPE	VARCHAR2(64)	Tipo de imagem
DATA	CLOB	Dados de imagem
DATE_CREATED	DATE	Inserir data
DATE_MODIFIED	DATE	Data da última atualização
CREATED_BY	NUMBER	ID do usuário que fez a inserção
MODIFIED_BY	NUMBER	ID do usuário que fez a última atualização

INCIDENTS_ASSETS_RPT_V

A tela faz referência à tabela INCIDENTS_ASSETS, que armazena informações sobre os bens que compõem incidentes criados no Console do Sentinel.

Nome da coluna	Tipo de dados	Comentário
INC_ID	NUMBER	Identificador de incidente – número de seqüência
ASSET_ID	varchar2	Identificador Exclusivo Universal (UUID) de bem
DATE_CREATED	DATE	Inserir data
DATE_MODIFIED	DATE	Data da última atualização
CREATED_BY	NUMBER	ID do usuário que fez a inserção
MODIFIED_BY	NUMBER	ID do usuário que fez a última atualização

INCIDENTS_EVENTS_RPT_V

A tela faz referência à tabela INCIDENTS_EVENTS, que armazena informações sobre os eventos que compõem incidentes criados no Console do Sentinel.

Nome da coluna	Tipo de dados	Comentário
INC_ID	NUMBER	Identificador de incidente – número de seqüência
EVT_ID	varchar2	Identificador Exclusivo Universal (UUID) de evento
EVT_TIME	DATE	Horário do evento
DATE_CREATED	DATE	Inserir data
DATE_MODIFIED	DATE	Data da última atualização
CREATED_BY	NUMBER	ID do usuário que fez a inserção
MODIFIED_BY	NUMBER	ID do usuário que fez a última atualização

INCIDENTS_RPT_V

A tela faz referência à tabela INCIDENTS, que armazena informações que descrevem os detalhes de incidentes criados no Console do Sentinel.

Nome da coluna	Tipo de dados	Comentário
INC_ID	NUMBER	Identificador de incidente – número de seqüência
NAME	VARCHAR2(255)	Nome do incidente
SEVERITY	NUMBER	Gravidade do incidente
STT_ID	NUMBER	ID de Estado do Incidente
SEVERITY_RATING	VARCHAR2(32)	Média de todas as gravidades de eventos que formam um incidente.

Nome da coluna	Tipo de dados	Comentário
VULNERABILITY_RATING	VARCHAR2(32)	Reservada para uso futuro da Novell. O uso desse campo para qualquer outra finalidade pode resultar em sobregravação de dados por uma funcionalidade futura.
CRITICALITY_RATING	VARCHAR2(32)	Reservada para uso futuro da Novell. O uso desse campo para qualquer outra finalidade pode resultar em sobregravação de dados por uma funcionalidade futura.
DATE_CREATED	DATE	Inserir data
DATE_MODIFIED	DATE	Data da última atualização
CREATED_BY	NUMBER	ID do usuário que fez a inserção
MODIFIED_BY	NUMBER	ID do usuário que fez a última atualização
INC_DESC	varchar2(4000)	Descrição do incidente
INC_PRIORITY	número	Prioridade do incidente
INC_CAT	varchar2(255)	Categoria do incidente
INC_RES	varchar2(4000)	Resolução do incidente

INCIDENTS_VULN_RPT_V

A tela faz referência à tabela INCIDENTS_VULN, que armazena informações sobre as vulnerabilidades que compõem incidentes criados no Console do Sentinel.

Nome da coluna	Tipo de dados	Comentário
INC_ID	NUMBER	Identificador de incidente – número de seqüência
VULN_ID	varchar2(36)	Identificador Exclusivo Universal (UUID) de vulnerabilidades
DATE_CREATED	DATE	Inserir data
DATE_MODIFIED	DATE	Data da última atualização
CREATED_BY	NUMBER	ID do usuário que fez a inserção
MODIFIED_BY	NUMBER	ID do usuário que fez a última atualização

L_STAT_RPT_V

A tela faz referência à tabela L_STAT, que armazena informações estatísticas.

Nome da coluna	Tipo de dados	Comentário
RES_NAME	VARCHAR2(32)	Nome do recurso
STATS_NAME	VARCHAR2(32)	Nome da estatística
STATS_VALUE	VARCHAR2(32)	Valor da estatística
OPEN_TOT_SECS	NUMERIC	Número de segundos desde 1970.

LOGS_RPT_V

A tela faz referência à tabela LOGS_RPT, que armazena informações sobre registro.

Tabela LOGS		
Nome da coluna	**Tipo de dados**	**Comentário**
LOG_ID	NUMBER	Número de seqüência
TIME	DATE	Data do Registro
MODULE	VARCHAR2(64)	O módulo ao qual o registro se destina
TEXT	VARCHAR2(4000)	Texto do registro

NETWORK_IDENTITY_RPT_V

A tela faz referência à tabela NETWORK_IDENTITY_LKUP, que armazena informações sobre a identidade da rede do bem.

Nome da coluna	**Tipo de dados**	**Comentário**
NETWORK_IDENTITY_CD	varchar2(5)	Código de identidade da rede
NETWORK_IDENTITY_NAME	varchar2(255)	Nome de identidade da rede
DATE_CREATED	data	Inserir data
DATE_MODIFIED	data	Data da última atualização
CREATED_BY	número	ID do usuário que fez a inserção
MODIFIED_BY	número	ID do usuário que fez a última atualização

ORGANIZATION_RPT_V

A tela faz referência à tabela ORGANIZATION, que armazena informações sobre organização (bem).

Nome da coluna	**Tipo de dados**	**Comentário**
ORGANIZATION_ID	varchar2	Identificador de organização
ORGANIZATION_NAME	varchar2(100)	Nome da organização
CUSTOMER_ID	número	Identificador de cliente
DATE_CREATED	data	Inserir data
DATE_MODIFIED	data	Data da última atualização
CREATED_BY	número	ID do usuário que fez a inserção
MODIFIED_BY	número	ID do usuário que fez a última atualização

PERSON_RPT_V

A tela faz referência à tabela PERSION, que armazena informações pessoais (bem).

Nome da coluna	**Tipo de dados**	**Comentário**
PERSON_ID	varchar2	Identificador de pessoa
FIRST_NAME	varchar2(255)	Nome
LAST_NAME	varchar2(255)	Sobrenome
CUSTOMER_ID	número	Identificador de cliente
PHONE_NUMBER	varchar2(50)	Número de telefone
EMAIL_ADDRESS	varchar2(255)	Endereço de e-mail
DATE_CREATED	data	Inserir data

Nome da coluna	Tipo de dados	Comentário
DATE_MODIFIED	data	Data da última atualização
CREATED_BY	número	ID do usuário que fez a inserção
MODIFIED_BY	número	ID do usuário que fez a última atualização

PHYSICAL_ASSET_RPT_V

A tela faz referência à tabela PHYSICAL_ASSET, que armazena informações sobre bens físicos.

Nome da coluna	Tipo de dados	Comentário
PHYSICAL_ASSET_ID	varchar2	Identificador de bem físico
CUSTOMER_ID	número	Identificador de cliente
LOCATION_ID	número	Identificador de local
HOST_NAME	varchar2(255)	Nome de host
IP_ADDRESS	número	Endereço IP
NETWORK_IDENTITY_CD	varchar2(5)	Código de identidade da rede
MAC_ADDRESS	varchar2(100)	Endereço MAC
RACK_NUMBER	varchar2(50)	Número do rack
ROOM_NAME	varchar2(100)	Nome da sala
DATE_CREATED	data	Inserir data
DATE_MODIFIED	data	Data da última atualização
CREATED_BY	número	ID do usuário que fez a inserção
MODIFIED_BY	número	ID do usuário que fez a última atualização

PRODUCT_RPT_V

A tela faz referência à tabela PRDT, que armazena informações sobre produtos de bens.

Nome da coluna	Tipo de dados	Comentário
PRODUCT_ID	número	Identificador de produtos
PRODUCT_NAME	varchar2(255)	Nome do produto
PRODUCT_VERSION	varchar2(100)	Versão do produto
VENDOR_ID	número	Identificador do fornecedor
DATE_CREATED	data	Inserir data
DATE_MODIFIED	data	Data da última atualização
CREATED_BY	número	ID do usuário que fez a inserção
MODIFIED_BY	número	ID do usuário que fez a última atualização

ROLE_RPT_V

A tela faz referência à tabela ROLE_LKUP, que armazena informações sobre a função do usuário (bem).

Nome da coluna	Tipo de dados	Comentário
ROLE_CODE	varchar2(5)	Código de função
ROLE_NAME	varchar2(255)	Nome da função
DATE_CREATED	data	Inserir data

Nome da coluna	Tipo de dados	Comentário
DATE_MODIFIED	data	Data da última atualização
CREATED_BY	número	ID do usuário que fez a inserção
MODIFIED_BY	número	ID do usuário que fez a última atualização

SENSITIVITY_RPT_V

A tela faz referência à tabela SENSITIVITY_LKUP, que armazena informações sobre sigilo de bens.

Nome da coluna	Tipo de dados	Comentário
SENSITIVITY_CODE	varchar2(5)	Código de distinção do bem
SENSITIVITY_NAME	varchar2(50)	Nome da distinção do bem
DATE_CREATED	data	Inserir data
DATE_MODIFIED	data	Data da última atualização
CREATED_BY	número	Por ID de usuário
MODIFIED_BY	número	Por ID de usuário

STATES_RPT_V

A tela faz referência à tabela STATES, que armazena definições de estados definidos por aplicativos ou contexto.

Nome da coluna	Tipo de dados	Comentário
STT_ID	NUMBER	ID do estado – número de seqüência
CONTEXT	VARCHAR2(64)	Contexto do estado. Trata-se de caso, incidente, usuário.
NAME	VARCHAR2(64)	Nome do estado.
TERMINAL_FLAG	VARCHAR2(1)	Indica se o estado do incidente é resolvido.
DATE_CREATED	DATE	Inserir data
DATE_MODIFIED	DATE	Data da última atualização
MODIFIED_BY	NUMBER	ID do usuário que fez a inserção
CREATED_BY	NUMBER	ID do usuário que fez a última atualização

Tela UNASSIGNED_INCIDENTS_RPT_V

A tela faz referência às tabelas CASES e INCIDENTS para relatar casos não atribuídos.

Nome	Tipo de dados
INC_ID	NUMBER
NAME	VARCHAR2(255)
SEVERITY	NUMBER
STT_ID	NUMBER
SEVERITY_RATING	VARCHAR2(32)
VULNERABILITY_RATING	VARCHAR2(32)
CRITICALITY_RATING	VARCHAR2(32)
DATE_CREATED	DATE
DATE_MODIFIED	DATE

Nome	Tipo de dados
CREATED_BY	NUMBER
MODIFIED_BY	NUMBER
INC_DESC	VARCHAR2(4000)
INC_PRIORITY	NUMBER
INC_CAT	VARCHAR2(255)
INC_RES	VARCHAR2(4000)

USERS_RPT_V

A tela faz referência à tabela USERS, que relaciona todos os usuários do aplicativo. Os usuários também serão criados como usuários do banco de dados para acomodar ferramentas de relatório de terceiros.

Nome da coluna	Tipo de dados	Comentário
USR_ID	NUMBER	Identificador de usuário – Número de seqüência
NAME	VARCHAR2(64)	Nome de usuário curto e exclusivo usado como login
CNT_ID	NUMBER	ID do contato – Número de seqüência
STT_ID	NUMBER	ID do estado. O status é ativo ou inativo.
DESCRIPTION	VARCHAR2(512)	Comentários
DATE_CREATED	DATE	Inserir data
DATE_MODIFIED	DATE	Data da última atualização
CREATED_BY	NUMBER	ID do usuário que fez a inserção
MODIFIED_BY	NUMBER	ID do usuário que fez a última atualização
PERMISSIONS	VARCHAR2(4000)	Permissões atualmente atribuídas ao usuário do Sentinel
FILTER	VARCHAR2(128)	Filtro de segurança atual atribuído ao usuário do Sentinel
UPPER_NAME	VARCHAR2(64)	Nome do usuário em maiúsculas
DOMAIN_AUTH_IND	NUMBER	Indicação de autenticação de domínio

VENDOR_RPT_V

A tela faz referência à tabela VNDR, que armazena informações sobre fornecedores de produtos de bens.

Nome da coluna	Tipo de dados	Comentário
VENDOR_ID	número	Identificador do fornecedor
VENDOR_NAME	varchar2(255)	Nome do fornecedor
DATE_CREATED	data	Inserir data
DATE_MODIFIED	data	Data da última atualização
CREATED_BY	número	ID do usuário que fez a inserção
MODIFIED_BY	número	ID do usuário que fez a última atualização

VULN_CALC_SEVERITY_RPT_V

A tela faz referência a VULN_RSRC e VULN para calcular a classificação de gravidade de vulnerabilidade do Sentinel com base nas vulnerabilidades atuais.

Nome da coluna	Tipo de dados
RSRC_ID	VARCHAR22(36)
IP	VARCHAR22(32)
HOST_NAME	VARCHAR22(255)
CRITICALITY	NUMBER
ASSIGNED_VULN_SEVERITY	NUMBER
VULN_COUNT	Total de Vulnerabilidades para o Recurso especificado
CALC_SEVERITY	Gravidade calculada com base em ASSIGNED_VULN_SEVERITY e CRITICALITY

VULN_CODE_RPT_V

A tela faz referência à tabela VULN_CODE, que armazena códigos de vulnerabilidade atribuídos pela indústria, como CVEs e CANs da Mitre.

Nome da coluna	Tipo de dados
VULN_CODE_ID	VARCHAR2(36)
VULN_ID	VARCHAR2(36)
VULN_CODE_TYPE	VARCHAR2(64)
VULN_CODE_VALUE	VARCHAR2(255)
URL	VARCHAR2(512)
DATE_CREATED	DATE
DATE_MODIFIED	DATE
CREATED_BY	NUMBER
MODIFIED_BY	NUMBER

VULN_INFO_RPT_V

A tela faz referência à tabela VULN_INFO, que armazena informações adicionais relatadas durante uma exploração.

Nome da coluna	Tipo de dados
VULN_INFO_ID	VARCHAR2(36)
VULN_ID	VARCHAR2(36)
VULN_INFO_TYPE	VARCHAR2(36)
VULN_INFO_VALUE	VARCHAR2(2000)
DATE_CREATED	DATE
DATE_MODIFIED	DATE
CREATED_BY	NUMBER
MODIFIED_BY	NUMBER

VULN_RPT_V

A tela faz referência à tabela VULN, que armazena informações sobre o sistema explorado. Cada scanner terá sua própria entrada para cada sistema.

Nome da coluna	Tipo de dados
VULN_ID	VARCHAR2(36)
RSRC_ID	VARCHAR2(36)
PORT_NAME	VARCHAR2(64)
PORT_NUMBER	NUMBER
NETWORK_PROTOCOL	NUMBER
APPLICATION_PROTOCOL	VARCHAR2(64)
ASSIGNED_VULN_SEVERITY	NUMBER
COMPUTED_VULN_SEVERITY	NUMBER
VULN_DESCRIPTION	CLOB
VULN_SOLUTION	CLOB
VULN_SUMMARY	VARCHAR2(1000)
BEGIN_EFFECTIVE_DATE	DATE
END_EFFECTIVE_DATE	DATE
DETECTED_OS	VARCHAR2(64)
DETECTED_OS_VERSION	VARCHAR2(64)
SCANNED_APP	VARCHAR2(64)
SCANNED_APP_VERSION	VARCHAR2(64)
VULN_USER_NAME	VARCHAR2(64)
VULN_USER_DOMAIN	VARCHAR2(64)
VULN_TAXONOMY	VARCHAR2(1000)
SCANNER_CLASSIFICATION	VARCHAR2(255)
VULN_NAME	VARCHAR2(300)
VULN_MODULE	VARCHAR2(64)
DATE_CREATED	DATE
DATE_MODIFIED	DATE
CREATED_BY	NUMBER
MODIFIED_BY	NUMBER

VULN_RSRC_RPT_V

A tela faz referência à tabela VULN_RSRC, que armazena cada recurso explorado de uma determinada exploração.

Nome da coluna	Tipo de dados
RSRC_ID	VARCHAR2(36)
SCANNER_ID	VARCHAR2(36)
IP	VARCHAR2(32)
HOST_NAME	VARCHAR2(255)
LOCATION	VARCHAR2(128)
DEPARTMENT	VARCHAR2(128)
BUSINESS_SYSTEM	VARCHAR2(128)
OPERATIONAL_ENVIRONMENT	VARCHAR2(64)
CRITICALITY	NUMBER
REGULATION	VARCHAR2(128)

Nome da coluna	Tipo de dados
REGULATION_RATING	VARCHAR2(64)
DATE_CREATED	DATE
DATE_MODIFIED	DATE
CREATED_BY	NUMBER
MODIFIED_BY	NUMBER

VULN_RSRC_SCAN_RPT_V

A tela faz referência à tabela VULN_RSRC_SCAN, que armazena cada recurso explorado de uma determinada exploração.

Nome da coluna	Tipo de dados
RSRC_ID	VARCHAR2(36)
SCAN_ID	VARCHAR2(36)
DATE_CREATED	DATE
DATE_MODIFIED	DATE
CREATED_BY	NUMBER
MODIFIED_BY	NUMBER

VULN_SCAN_RPT_V

A tela faz referência à tabela que armazena informações referentes a explorações.

Nome da coluna	Tipo de dados
SCAN_ID	VARCHAR2(36)
SCANNER_ID	VARCHAR2(36)
SCAN_TYPE	VARCHAR2(10)
SCAN_START_DATE	DATE
SCAN_END_DATE	DATE
CONSOLIDATION_SERVER	VARCHAR2(64)
DATE_CREATED	DATE
DATE_MODIFIED	DATE
CREATED_BY	NUMBER
MODIFIED_BY	NUMBER

VULN_SCAN_VULN_RPT_V

A tela faz referência à tabela VULN_SCAN_VULN, que armazena vulnerabilidades detectadas durante explorações.

Nome da coluna	Tipo de dados
SCAN_ID	VARCHAR2(36)
VULN_ID	VARCHAR2(36)
DATE_CREATED	DATE
DATE_MODIFIED	DATE
CREATED_BY	NUMBER
MODIFIED_BY	NUMBER

VULN_SCANNER_RPT_V

A tela faz referência à tabela VULN_SCANNER, que armazena informações sobre scanners de vulnerabilidades.

Nome da coluna	Tipo de dados
SCANNER_ID	VARCHAR2(36)
PRODUCT_NAME	VARCHAR2(100)
PRODUCT_VERSION	VARCHAR2(64)
SCANNER_TYPE	VARCHAR2(64)
VENDOR	VARCHAR2(100)
SCANNER_INSTANCE	VARCHAR2(64)
DATE_CREATED	DATE
DATE_MODIFIED	DATE
CREATED_BY	NUMBER
MODIFIED_BY	NUMBER

12 Telas do banco de dados do Sentinel para Microsoft SQL Server

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

Este capítulo relaciona as telas de Esquema do Sentinel para Microsoft SQL Server. As telas fornecem informações para o desenvolvimento de seus próprios relatórios (Crystal Reports).

Telas

ADV_ALERT_CVE_RPT_V

A tela faz referência à tabela ADV_ALERT_CVE, que armazena o número de identificação de alerta do Consultor.

Nome da coluna	Tipo de dados	Comentário
ALERT_ID	int	Identificador de anotação - número de seqüência
CVE	varchar	
DATE_CREATED	data/horário	Data de inserção
DATE_MODIFIED	data/horário	Data da última atualização
CREATED_BY	int	Por ID de usuário
MODIFIED_BY	int	Por ID de usuário

ADV_ALERT_PRODUCT_RPT_V

A tela faz referência à tabela ADV_ALERT_PRODUCT, que armazena informações sobre produtos do Consultor, como número de ID de service pack, versão e data de criação.

Nome da coluna	Tipo de dados	Comentário
ALERT_ID	int	Identificador de anotação - número de seqüência.
SERVICE_PACK_ID	int	
VENDOR	varchar	
PRODUCT	varchar	
VERSION	varchar	Contém o número de versão
SERVICE_PACK_ID	varchar	
PRIMARY_FLAG	int	
DATE_CREATED	data/horário	Data de inserção
DATE_MODIFIED	data/horário	Data da última atualização
CREATED_BY	int	Por ID de usuário
MODIFIED_BY	int	Por ID de usuário

ADV_ALERT_RPT_V

A tela faz referência à tabela ADV_ALERT_PRODUCT, que armazena informações sobre alertas do Consultor, como nome, tipo de ameaça e data de publicação.

Nome da coluna	Tipo de dados	Comentário
ALERT_ID	int	Identificador de anotação - número de seqüência
VERSION	int	Contém o número de versão
TEMPLATE_ID	int	
TEMPLATE_NAME	varchar	
THREAT_CATEGORY_NAME	varchar	
THREAT_TYPE_NAME	varchar	
HEADLINE	texto	
FIRST_PUBLISHED	data/horário	
LAST_PUBLISHED	data/horário	
STATUS	varchar	
URGENCY_ID	int	
CREDIBILITY_ID	int	
SEVERITY_ID	int	
SUMMARY	texto	
LEGAL_DISCLAIMER	texto	
COPYRIGHT	varchar	
BEGIN_EFFECTIVE_DATE	data/horário	
END_EFFECTIVE_DATE	data/horário	
DATE_CREATED	data/horário	Data de inserção
DATE_MODIFIED	data/horário	Data da última atualização
CREATED_BY	int	Por ID de usuário
MODIFIED_BY	int	Por ID de usuário

ADV_ATTACK_ALERT_RPT_V

A tela faz referência à tabela ADV_ATTACK_PRODUCT, que armazena informações sobre ataques do Consultor, como nome, tipo de ameaça e data de publicação.

Nome da coluna	Tipo de dados	Comentário
ATTACK_ID	int	
ALERT_ID	int	
DATE_CREATED	data/horário	Data de inserção
DATE_MODIFIED	data/horário	Data da última atualização
CREATED_BY	int	Por ID de usuário
MODIFIED_BY	int	Por ID de usuário

ADV_ATTACK_CVE_RPT_V

A tela faz referência à tabela ADV_ATTACK_CVE, que armazena informações CVE do Consultor.

Nome da coluna	Tipo de dados	Comentário
ATTACK_ID	int	
CVE	varchar	

Nome da coluna	Tipo de dados	Comentário
DATE_CREATED	data/horário	Data de inserção
DATE_MODIFIED	data/horário	Data da última atualização
CREATED_BY	int	Por ID de usuário
MODIFIED_BY	int	Por ID de usuário

ADV_ATTACK_MAP_RPT_V

A tela faz referência à tabela ADV_ATTACK_MAP, que armazena informações sobre mapas do Consultor.

Nome da coluna	Tipo de dados	Comentário
ATTACK_KEY	int	
ATTACK_ID	int	
SERVICE_PACK_ID	int	
ATTACK_NAME	varchar	
ATTACK_CODE	varchar	
DATE_CREATED	data/horário	Data de inserção
DATE_MODIFIED	data/horário	Data da última atualização
CREATED_BY	int	Por ID de usuário
MODIFIED_by	int	Por ID de usuário

ADV_ATTACK_PLUGIN_RPT_V

A tela faz referência à tabela ADV_ATTACK_PLUGIN, que armazena informações sobre plug-ins do Consultor.

Nome da coluna	Tipo de dados	Comentário
PLUGIN_KEY	int	
ATTACK_ID	int	
SERVICE_PACK_ID	int	
PLUGIN_ID	varchar	
PLUGIN_NAME	varchar	
DATE_CREATED	data/horário	Data de inserção
DATE_MODIFIED	data/horário	Data da última atualização
CREATED_BY	int	Por ID de usuário
MODIFIED_BY	int	Por ID de usuário

ADV_ATTACK_RPT_V

A tela faz referência à tabela ADV_ATTACK, que armazena informações sobre ataques do Consultor.

Nome da coluna	Tipo de dados	Comentário
ALERT_ID	int	
TRUSECURE_ATTACK_NAME	int	
FEED_DATE_CREATED	data/horário	
FEED_DATE_UPDATED	data/horário	
ATTACK_CATEGORY	varchar	
URGENCY_ID	int	

Nome da coluna	Tipo de dados	Comentário
SEVERITY_ID	int	
LOCAL	int	
REMOTE	int	
BEGIN_EFFECTIVE_DATE	data/horário	
END_EFFECTIVE_DATE	data/horário	
DESCRIPTION	texto	
SCENARIO	texto	
IMPACT	texto	
SAFEGUARDS	texto	
PATCHES	texto	
FALSE_POSITIVES	texto	
DATE_CREATED	data/horário	Data de inserção
DATE_MODIFIED	data/horário	Data da última atualização
CREATED_BY	int	Por ID de usuário
MODIFIED_BY	int	Por ID de usuário

ADV_CREDIBILITY_RPT_V

A tela faz referência à tabela ADV_CREDIBILITY, que armazena informações sobre credibilidade do Consultor.

Nome da coluna	Tipo de dados	Comentário
CREDIBILITY_ID	int	
CREDIBILITY_RATING	varchar	
CREDIBILITY_EXPLANATION	varchar	
DATE_CREATED	data/horário	Data de inserção
DATE_MODIFIED	data/horário	Data da última atualização
CREATED_BY	int	Por ID de usuário
MODIFIED_BY	int	Por ID de usuário

ADV_FEED_RPT_V

A tela faz referência à tabela ADV_FEED, que armazena informações sobre feeds do Consultor, como nome e data do feed.

Nome da coluna	Tipo de dados	Comentário
FEED_NAME	varchar	
FEED_FILE	varchar	
BEGIN_DATE	data/horário	
END_DATE	data/horário	
FEED_INSERT	int	
FEED_UPDATE	int	
FEED_EXPIRE	int	

ADV_PRODUCT_RPT_V

A tela faz referência à tabela ADV_PRODUCT, que armazena informações sobre produtos do Consultor, como fornecedor e ID do produto.

Nome da coluna	Tipo de dados	Comentário
PRODUCT_ID	int	
VENDOR_ID	int	
PRODUCT_CATEGORY_ID	int	
PRODUCT_CATEGORY_NAME	varchar	
PRODUCT_TYPE-ID	int	
PRODUCT_TYPE_NAME	varchar	
PRODUCT_NAME	varchar	
PRODUCT_DESCRIPTION	varchar	
FEED_DATE_CREATED	data/horário	
FEED_DATE_UPDATED	data/horário	
ACTIVE_FLAG	int	
DATE_CREATED	data/horário	Data de inserção
DATE_MODIFIED	data/horário	Data da última atualização
CREATED_BY	int	Por ID de usuário
MODIFIED_BY	int	Por ID de usuário

ADV_PRODUCT_SERVICE_PACK_RPT_V

A tela faz referência à tabela ADV_PRODUCT_SERVICE _PACK, que armazena informações sobre service pack do Consultor, como nome do service pack, ID versão e data.

Nome da coluna	Tipo de dados	Comentário
SERVICE_PACK_ID	int	
VERSION_ID	int	Contém o número de ID de versão
SERVICE_PACK_NAME	varchar	
FEED_DATE_CREATED	data/horário	
FEED_DATE_UPDATED	data/horário	
ACTIVE_FLAG	int	
BEGIN_EFFECTIVE_DATE	data/horário	
END_EFFECTIVE_DATE	data/horário	
DATE_CREATED	data/horário	Data de inserção
DATE_MODIFIED	data/horário	Data da última atualização
CREATED_BY	int	Por ID de usuário
MODIFIED_BY	int	Por ID de usuário

ADV_PRODUCT_VERSION_RPT_V

A tela faz referência à tabela ADV_PRODUCT_VERSION, que armazena informações sobre versões de produtos do Consultor, como nome da versão, produto e ID da versão.

Nome da coluna	Tipo de dados	Comentário
VERSION_ID	int	Contém o número de ID de versão
PRODUCT_ID	int	
VERSION_NAME	varchar	
FEED_DATE_CREATED	data/horário	
FEED_DATE_UPDATED	data/horário	
ACTIVE_FLAG	int	
DATE_CREATED	data/horário	Data de inserção
DATE_MODIFIED	int	Data da última atualização
CREATED_BY	int	Por ID de usuário
MODIFIED_BY	int	Por ID de usuário

ADV_SEVERITY_RPT_V

A tela faz referência à tabela ADV_SEVERITY, que armazena informações sobre classificação de gravidade do Consultor.

Nome da coluna	Tipo de dados	Comentário
SEVERITY_ID	int	
SEVERITY_RATING	varchar	
SEVERITY_EXPLANATION	varchar	
DATE_CREATED	data/horário	Data de inserção
DATE_MODIFIED	data/horário	Data da última atualização
CREATED_BY	int	Por ID de usuário
MODIFIED_BY	int	Por ID de usuário

ADV_SUBALERT_RPT_V

A tela faz referência à tabela ADV_SUBALERT.

Nome da coluna	Tipo de dados	Comentário
ALERT_ID	int	
SUBALERT_ID	int	
CHANGED_SECTIONS	varchar	
VARIANTS	texto	
VIRUS_NAME	texto	
DESCRIPTION	texto	
IMPACT	texto	
WARNING_INDICATORS	texto	
TECHNICAL_INFO	texto	
TRUSECURE_COMMENTS	texto	
VENDOR_ANNOUNCEMENTS	texto	

Nome da coluna	Tipo de dados	Comentário
SAFEGUARDS	texto	
PATCHES_SOFTWARE	texto	
ALERT_HISTORY	texto	
BACKGROUND_INFO	texto	
DATE_CREATED	data/horário	Data de inserção
DATE_MODIFIED	data/horário	Data da última atualização
CREATED_BY	int	Por ID de usuário
MODIFIED_BY	int	Por ID de usuário

ADV_URGENCY_RPT_V

A tela faz referência à tabela ADV_URGENCY.

Nome da coluna	Tipo de dados	Comentário
URGENCY_ID	int	
URGENCY_RATING	varchar	
URGENCY_EXPLANATION	varchar	
DATE_CREATED	data/horário	Data de inserção
DATE_MODIFIED	data/horário	Data da última atualização
CREATED_BY	int	Por ID de usuário
MODIFIED_BY	int	Por ID de usuário

ADV_VENDOR_RPT_V

A tela faz referência à tabela ADV_VENDOR, que armazena informações sobre endereços do Consultor.

Nome da coluna	Tipo de dados	Comentário
VENDOR_ID	int	
VENDOR_NAME	varchar	
CONTACT_PERSON	varchar	
ADDRESS_LINE_1	varchar	
ADDRESS_LINE_2	varchar	
ADDRESS_LINE_3	varchar	
ADDRESS_LINE_4	varchar	
CITY	varchar	
STATE	varchar	
COUNTRY	varchar	
ZIP_CODE	varchar	
URL	varchar	
PHONE	varchar	
FAX	varchar	
EMAIL	varchar	
PAGER	varchar	
FEED_DATE_CREATED	data/horário	
FEED_DATE_UPDATED	data/horário	

Nome da coluna	Tipo de dados	Comentário
ACTIVE_FLAG	int	
DATE_CREATED	data/horário	Data de inserção
DATE_MODIFIED	data/horário	Data da última atualização
CREATED_BY	int	Por ID de usuário
MODIFIED_BY	int	Por ID de usuário

ADV_VULN_PRODUCT_RPT_V

A tela faz referência à tabela ADV_VULN_PRODUCT, que armazena IDs de ataques a vulnerabilidades e IDs de service packs do Consultor.

Nome da coluna	Tipo de dados	Comentário
ATTACK_ID	int	
SERVICE_PACK_ID	int	
DATE_CREATED	data/horário	Data de inserção
DATE_MODIFIED	data/horário	Data da última atualização
CREATED_BY	int	Por ID de usuário
MODIFIED_BY	int	Por ID de usuário

ANNOTATIONS_RPT_V

A tela faz referência à tabela ANNOTATIONS, que armazena documentação ou notas que podem ser associadas a objetos no sistema Sentinel, como casos e incidentes.

Nome da coluna	Tipo de dados	Comentário
ANN_ID	INT	Identificador de anotação - número de seqüência
TEXT	VARCHAR(4000)	Documentação ou notas.
DATE_CREATED	DATETIME	Data de inserção
DATE_MODIFIED	DATETIME	Data da última atualização
MODIFIED_BY	INT	ID do usuário que fez a última atualização
CREATED_BY	INT	ID do usuário que fez a inserção
ACTION	Varchar(255)	Ação

ASSET_CTGRY_RPT_V

A tela faz referência à tabela ASSET_CTGRY, que armazena informações sobre categorias de bens (por ex.: hardware, software, SO, banco de dados etc...).

Nome da coluna	Tipo de dados	Comentário
ASSET_CATEGORY_ID	bigint	Identificador de categoria de bem
ASSET_CATEGORY_NAME	varchar(100)	Nome de categoria de bem
DATE_CREATED	data/horário	Data de inserção
DATE_MODIFIED	data/horário	Data da última atualização
CREATED_BY	int	ID do usuário que fez a inserção
MODIFIED_BY	int	ID do usuário que fez a última atualização

ASSET_HOSTNAME_RPT_V

A tela faz referência à tabela ASSET_HOSTNAME, que armazena informações sobre nomes de hosts alternativos para bens.

Nome da coluna	Tipo de dados	Comentário
ASSET_HOSTNAME_ID	Identificador exclusivo	Identificador de nome de host alternativo de bem
PHYSICAL_ASSET_ID	identificador exclusivo	Identificador de bem físico
HOST_NAME	Varchar(255)	Nome de host
CUSTOMER_ID	bigint	Identificador de cliente
DATE_CREATED	data/horário	Data da última atualização
DATE_MODIFIED	data/horário	ID do usuário que fez a última atualização
CREATED_BY	int	ID do usuário que fez a inserção
MODIFIED_BY	int	ID do usuário que fez a última atualização

ASSET_IP_RPT_V

A tela faz referência à tabela ASSET_IP, que armazena informações sobre endereços IP alternativos para bens.

Nome da coluna	Tipo de dados	Comentário
ASSET_IP_ID	Identificador exclusivo	Identificador de IP alternativo de bem
PHYSICAL_ASSET_ID	identificador exclusivo	Identificador de bem físico
IP_ADDRESS	int	Endereço IP de bem
CUSTOMER_ID	bigint	Identificador de cliente
DATE_CREATED	data/horário	Data de inserção
DATE_MODIFIED	data/horário	Data da última atualização
CREATED_BY	int	ID do usuário que fez a inserção
MODIFIED_BY	int	ID do usuário que fez a última atualização

ASSET_LOCATION_RPT_V

A tela faz referência à tabela ASSET_LOC, que armazena informações sobre locais de bens.

Nome da coluna	Tipo de dados	Comentário
LOCATION_ID	bigint	Identificador de local
CUSTOMER_ID	bigint	Identificador de cliente
BUILDING_NAME	varchar(255)	Nome do prédio
ADDRESS_LINE_1	varchar(255)	Linha de endereço 1
ADDRESS_LINE_2	varchar(255)	Linha de endereço 2
CITY	varchar(100)	Cidade
STATE	varchar(100)	Estado
COUNTRY	varchar(100)	País
ZIP_CODE	varchar(50)	CEP
DATE_CREATED	data/horário	Data de inserção

Nome da coluna	Tipo de dados	Comentário
DATE_MODIFIED	data/horário	Data da última atualização
CREATED_BY	int	ID do usuário que fez a inserção
MODIFIED_BY	int	ID do usuário que fez a última atualização

ASSET_RPT_V

A tela faz referência à tabela ASSET, que armazena informações sobre os bens físicos e intangíveis.

Nome da coluna	Tipo de dados	Comentário
ASSET_ID	identificador exclusivo	Identificador do bem
CUSTOMER_ID	bigint	Identificador de cliente
ASSET_NAME	varchar(255)	Nome do bem
PHYSICAL_ASSET_ID	identificador exclusivo	Identificador de bem físico
PRODUCT_ID	bigint	Identificador de produtos
ASSET_CATEGORY_ID	bigint	Identificador de categoria de bem
ENVIRONMENT_IDENTITY_CD	varchar(5)	Código de identidade do ambiente
PHYSICAL_ASSET_IND	bit	Indicador de bem físico
ASSET_VALUE_CD	varchar(5)	Código de valor do bem
CRITICALITY_CODE	varchar(5)	Código de importância do bem
SENSITIVITY_CODE	varchar(5)	Código de distinção do bem
DATE_CREATED	data/horário	Data de inserção
DATE_MODIFIED	data/horário	Data da última atualização
CREATED_BY	int	ID do usuário que fez a inserção
MODIFIED_BY	int	ID do usuário que fez a última atualização

ASSET_VALUE_RPT_V

A tela faz referência à tabela ASSET_VAL_LKUP, que armazena informações sobre o valor do bem.

Nome da coluna	Tipo de dados	Comentário
ASSET_VALUE_CODE	varchar(5)	Código de valor do bem
ASSET_VALUE_NAME	varchar(50)	Nome do valor do bem
DATE_CREATED	data/horário	Data de inserção
DATE_MODIFIED	data/horário	Data da última atualização
CREATED_BY	int	ID do usuário que fez a inserção
MODIFIED_BY	int	ID do usuário que fez a última atualização

ASSET_X_ENTITY_X_ROLE_RPT_V

A tela faz referência à tabela ASSET_X_ENTITY_X_ROLE, que associa uma pessoa ou uma organização a um bem.

Nome da coluna	Tipo de dados	Comentário
PERSON_ID	identificador exclusivo	Identificador de pessoa
ORGANIZATION_ID	identificador exclusivo	Identificador de organização
ROLE_CODE	varchar(5)	Código de função
ASSET_ID	identificador exclusivo	Identificador do bem
ENTITY_TYPE_CODE	varchar(5)	Código de tipo de entidade
PERSON_ROLE_SEQUENCE	int	Ordem de pessoas em uma determinada função
DATE_CREATED	data/horário	Data de inserção
DATE_MODIFIED	data/horário	Data da última atualização
CREATED_BY	int	ID do usuário que fez a inserção
MODIFIED_BY	int	ID do usuário que fez a última atualização

ASSOCIATIONS_RPT_V

A tela faz referência à tabela ASSOCIATIONS, que associa usuários a incidentes, incidentes a anotações, etc.

Nome da coluna	Tipo de dados	Comentário
TABLE1	VARCHAR(64)	Nome da tabela 1. Por exemplo, incidentes
ID1	VARCHAR(36)	ID1. Por exemplo, ID do incidente.
TABLE2	VARCHAR(64)	Nome da tabela 2. Por exemplo, usuários
ID2	VARCHAR(36)	ID2. Por exemplo, ID do usuário.
DATE_CREATED	DATETIME	Data de inserção.
DATE_MODIFIED	DATETIME	Data da última atualização
CREATED_BY	INT	ID do usuário que fez a inserção
MODIFIED_BY	INT	ID do usuário que fez a última atualização

ATTACHMENTS_RPT_V

A tela faz referência à tabela ATTACHMENTS, que armazena dados sobre anexos.

Nome da coluna	Tipo de dados	Comentário
ATTACHMENT_ID	int	Identificador do anexo
NAME	varchar(255)	Nome do anexo
SOURCE_REFERENCE	varchar(64)	Referência da fonte
TYPE	varchar(32)	Tipo do anexo
SUB_TYPE	varchar(32)	Subtipo do anexo
FILE_EXTENSION	varchar(32)	Extensão do arquivo
ATTACHMENT_DESCRIPTION	varchar(255)	Descrição do anexo

Nome da coluna	Tipo de dados	Comentário
DATA	clob	Dados do anexo
DATE_CREATED	data/horário	Data de inserção
DATE_MODIFIED	data/horário	Data da última atualização
CREATED_BY	int	ID do usuário que fez a inserção
MODIFIED_BY	int	ID do usuário que fez a última atualização

CONFIGS_RPT_V

A tela faz referência à tabela CONFIGS, que armazena informações sobre configuração geral do aplicativo.

Nome da coluna	Tipo de dados	Comentário
USR_ID	VARCHAR(32)	Nome do usuário.
APPLICATION	VARCHAR(255)	Identificador do aplicativo
UNIT	VARCHAR(64)	Unidade do aplicativo
VALUE	VARCHAR(255)	Valor de texto, se houver
DATA	TEXT	Dados XML
DATE_CREATED	DATETIME	Data de inserção.
DATE_MODIFIED	DATETIME	Data da última atualização.
CREATED_BY	INT	ID do usuário que fez a inserção.
MODIFIED_BY	INT	ID do usuário que fez a última atualização.

CONTACTS_RPT_V

A tela faz referência à tabela CONTACTS, que armazena informações de contato.

Nome da coluna	Tipo de dados	Comentário
CNT_ID	INT	ID do contato – Número de seqüência
FIRST_NAME	VARCHAR(20)	Nome do contato.
LAST_NAME	VARCHAR(30)	Sobrenome do contato.
TITLE	VARCHAR(128)	Título do contato
DEPARTMENT	VARCHAR(128)	Departamento
PHONE	VARCHAR(64)	Telefone do contato
EMAIL	VARCHAR(255)	E-mail do contato
PAGER	VARCHAR(64)	Pager do contato
CELL	VARCHAR(64)	Telefone celular do contato
DATE_CREATED	DATETIME	Data de inserção
DATE_MODIFIED	DATETIME	Data da última atualização
CREATED_BY	INT	ID do usuário que fez a inserção
MODIFIED_BY	INT	ID do usuário que fez a última atualização

CORRELATED_EVENTS_RPT_V

A tela faz referência à tabela CORRELATED_EVENTS_*, que armazena informações sobre eventos correlacionados.

Nome da coluna	Tipo de dados	Comentário
PARENT_EVT_ID	identificador exclusivo	Identificador Exclusivo Universal (UUID) do evento pai
CHILD_EVT_ID	identificador exclusivo	Identificador Exclusivo Universal (UUID) do evento filho
PARENT_EVT_TIME	DATETIME	Data de criação de evento pai
CHILD_EVT_TIME	DATETIME	Data de criação de evento filho
DATE_CREATED	DATE	Data de inserção gerada por DAS
DATE_MODIFIED	DATETIME	Data da última atualização
CREATED_BY	INT	ID do usuário que fez a inserção
MODIFIED_BY	INT	ID do usuário que fez a última atualização

CORRELATED_EVENTS_RPT_V1

A tela contém eventos atuais e históricos correlacionados (eventos correlacionados importados dos arquivos).

Nome da coluna	Tipo de dados	Comentário
PARENT_EVT_ID	identificador exclusivo	Identificador Exclusivo Universal (UUID) do evento pai
CHILD_EVT_ID	identificador exclusivo	Identificador Exclusivo Universal (UUID) do evento filho
PARENT_EVT_TIME	DATETIME	Horário do evento pai
CHILD_EVT_TIME	DATETIME	Horário do evento filho
DATE_CREATED	DATETIME	Data de inserção gerada por DAS
DATE_MODIFIED	DATETIME	Data da última atualização
CREATED_BY	INT	ID do usuário que fez a inserção
MODIFIED_BY	INT	ID do usuário que fez a última atualização

CRITICALITY_RPT_V

A tela faz referência à tabela CRIT_LKUP, que contém informações sobre a importância dos bens.

Nome da coluna	Tipo de dados	Comentário
CRITICALITY_CODE	varchar(5)	Código de importância do bem
CRITICALITY_NAME	varchar(50)	Nome da importância do bem
DATE_CREATED	data/horário	Data de inserção
DATE_MODIFIED	data/horário	Data da última atualização
CREATED_BY	int	Por ID de usuário
MODIFIED_BY	int	Por ID de usuário

CUST_RPT_V

A tela faz referência à tabela CUST, que armazena informações de clientes para MSSPs.

Nome da coluna	Tipo de dados	Comentário
CUSTOMER_ID	bigint	Identificador de cliente
CUSTOMER_NAME	varchar(255)	Nome do cliente
DATE_CREATED	data/horário	Data de inserção
DATE_MODIFIED	data/horário	Data da última atualização
CREATED_BY	int	ID do usuário que fez a inserção
MODIFIED_BY	int	ID do usuário que fez a última atualização

ENTITY_TYPE_RPT_V

A tela faz referência à tabela ENTITY_TYP, que armazena informações sobre tipos de entidades (pessoa ou organização).

Nome da coluna	Tipo de dados	Comentário
ENTITY_TYPE_CODE	varchar(5)	Código de tipo de entidade
ENTITY_TYPE_NAME	varchar(50)	Nome do tipo de entidade
DATE_CREATED	data/horário	Data de inserção
DATE_MODIFIED	data/horário	Data da última atualização
CREATED_BY	int	ID do usuário que fez a inserção
MODIFIED_BY	int	ID do usuário que fez a última atualização

ENV_IDENTITY_RPT_V

A tela faz referência à tabela ENV_IDENTITY_LKUP, que armazena informações sobre a identidade do ambiente do bem.

Nome da coluna	Tipo de dados	Comentário
ENVIRONMENT_IDENTITY_CODE	varchar(5)	Código de identidade do ambiente
ENVIRONMENT_IDENTITY_NAME	varchar(255)	Nome da identidade do ambiente
DATE_CREATED	data/horário	Data de inserção
DATE_MODIFIED	data/horário	Data da última atualização
CREATED_BY	int	ID do usuário que fez a inserção
MODIFIED_BY	int	ID do usuário que fez a última atualização

ESEC_DISPLAY_RPT_V

A tela faz referência à tabela ESEC_DISPLAY, que armazena propriedades de objetos que podem ser exibidas. Usada atualmente para renomear tags META. Usada com a Configuração de Eventos (Relevância Comercial).

Nome da coluna	Tipo de dados	Comentário
DISPLAY_OBJECT	VARCHAR(32)	O objeto pai da propriedade
TAG	VARCHAR(32)	O nome da tag nativa da propriedade
LABEL	VARCHAR(32)	A string de exibição da tag.
POSITION	INT	Posição da tag na exibição.

Nome da coluna	Tipo de dados	Comentário
WIDTH	INT	Largura da coluna
ALIGNMENT	INT	Alinhamento horizontal
FORMAT	INT	Formatador enumerado para exibição da propriedade
ENABLED	BIT	Indica se a tag é mostrada.
TYPE	INT	Indica o tipo de dados da tag. 1 = string 2 = ulong 3 = data 4 = uuid 5 = ipv4
DESCRIPTION	VARCHAR(255)	Descrição textual da tag
DATE_CREATED	DATETIME	Data de inserção.
DATE_MODIFIED	DATETIME	Data da última atualização.
CREATED_BY	INT	ID do usuário que fez a inserção.
MODIFIED_BY	INT	ID do usuário que fez a última atualização.
REF_CONFIG	VARCHAR(4000)	Configuração de Dados Referenciais

ESEC_PORT_REFERENCE_RPT_V

A tela faz referência à tabela ESEC_PORT_REFERENCE, que armazena números de portas padrão atribuídas pela indústria.

Nome da coluna	Tipo de dados	Comentário
PORT_NUMBER	INT	Em http://www.iana.org/assignments/port-numbers, a representação numérica da porta. Esse número de porta é geralmente associado ao nível de Protocolo de Transporte na pilha TCP/IP.
PROTOCOL_NUMBER	INT	Em http://www.iana.org/assignments/protocol-numbers, os identificadores numéricos usados para representar protocolos encapsulados em um pacote IP.
PORT_KEYWORD	VARCHAR(64)	Em http://www.iana.org/assignments/port-numbers, a representação de palavra-chave da porta.
PORT_DESCRIPTION	VARCHAR(512)	Descrição da porta.
DATE_CREATED	DATETIME	Data de inserção.
DATE_MODIFIED	DATETIME	Data da última atualização.
CREATED_BY	INT	ID do usuário que fez a inserção.
MODIFIED_BY	INT	ID do usuário que fez a última modificação.

ESEC_PROTOCOL_REFERENCE_RPT_V

A tela faz referência à tabela ESEC_PROTOCOL_REFERENCE, que armazena números de protocolo padrão atribuídos pela indústria.

Nome da coluna	Tipo de dados	Comentário
PROTOCOL_NUMBER	INT	Em http://www.iana.org/assignments/protocol-numbers, os identificadores numéricos usados para representar protocolos encapsulados em um pacote IP.
PROTOCOL_KEYWORD	VARCHAR(64)	Em http://www.iana.org/assignments/protocol-numbers, as palavras-chave usadas para representar protocolos encapsulados em um pacote IP.
PROTOCOL_DESCRIPTION	VARCHAR(512)	Descrição de protocolo de pacote IP.
DATE_CREATED	DATETIME	Data de inserção.
DATE_MODIFIED	DATETIME	Data da última atualização.
CREATED_BY	INT	ID do usuário que fez a inserção.
MODIFIED_BY	INT	ID do usuário que fez a última atualização.

ESEC_SEQUENCE _RPT_V

A tela faz referência à tabela ESEC_SEQUENCE, que é usada para gerar números de seqüência de chave principal para tabelas do Sentinel.

Nome da coluna	Tipo de dados	Comentário
TABLE_NAME	VARCHAR(32)	Nome da tabela.
COLUMN_NAME	VARCHAR(32)	Nome da coluna
SEED	INT	Valor atual do campo da chave principal.
DATE_CREATED	DATETIME	Data de inserção.
DATE_MODIFIED	DATETIME	Data da última atualização.
CREATED_BY	INT	ID do usuário que fez a inserção.
MODIFIED_BY	INT	ID do usuário que fez a última atualização.

EVENTS_ALL_RPT_V (Fornecida para fins de compatibilidade retroativa)

A tela contém eventos atuais e históricos (eventos importados dos arquivos).

Nome da coluna	Tipo de dados	Comentário
EVENT_ID	identificador exclusivo	Identificador do evento
RESOURCE_NAME	varchar(255)	Nome do recurso
SUB_RESOURCE	varchar(255)	Nome do sub-recurso
SEVERITY	int	Gravidade do evento
EVENT_PARSE_TIME	data/horário	Horário do evento
EVENT_DATETIME	data/horário	Horário do evento
BASE_MESSAGE	varchar(4000)	Mensagem base
EVENT_NAME	varchar(255)	Nome do evento conforme relatado pelo sensor
EVENT_TIME	varchar(255)	Horário do evento conforme relatado pelo sensor
SENSOR_NAME	varchar(255)	Nome do sensor
SENSOR_TYPE	varchar(5)	Tipo de sensor: H – baseado em host N – baseado em rede V – vírus O – outros
PROTOCOL	varchar(255)	Nome do protocolo
SOURCE_IP	int	Endereço IP de origem em formato numérico
SOURCE_HOST_NAME	varchar(255)	Nome do host de origem
SOURCE_PORT	varchar(32)	Porta de origem
DESTINATION_IP	int	Endereço IP de destino em formato numérico
DESTINATION_HOST_NAME	varchar(255)	Nome do host de destino
DESTINATION_PORT	varchar(32)	Porta de destino
SOURCE_USER_NAME	varchar(255)	Nome do usuário de origem
DESTINATION_USER_NAME	varchar(255)	Nome do usuário de destino
FILE_NAME	varchar(1000)	Nome do arquivo
EXTENDED_INFO	varchar(1000)	Informações estendidas
REPORT_NAME	varchar(255)	Nome do relator
PRODUCT_NAME	varchar(255)	Nome de produto de relatórios
CUSTOM_TAG_1	varchar(255)	Tag de Cliente 1
CUSTOM_TAG 2	varchar(255)	Tag de Cliente 2
CUSTOM_TAG 3	int	Tag de Cliente 3
RESERVED_TAG_1	VARCHAR(255)	Tag Reservada 1 Reservada para uso futuro do Sentinel. Campo usado para informações do Consultor sobre descrições de ataque.

Nome da coluna	Tipo de dados	Comentário
RESERVED_TAG_2	varchar(255)	Reservada para uso futuro do Sentinel. O uso desse campo para qualquer outra finalidade pode resultar em sobregravação de dados por uma funcionalidade futura.
RESERVED_TAG_3	int	Reservada para uso futuro do Sentinel. O uso desse campo para qualquer outra finalidade pode resultar em sobregravação de dados por uma funcionalidade futura.
SOURCE_UUID	identificador exclusivo	UUID de origem
PORT	varchar(64)	Porta do Coletor
AGENT	varchar(64)	Nome do Coletor
VULNERABILITY_RATING	int	Classificação de vulnerabilidade
CRITICALITY_RATING	int	Classificação de importância
DATE_CREATED	data/horário	Data de inserção
DATE_MODIFIED	data/horário	Data da última atualização
CREATED_BY	int	ID do usuário que fez a inserção.
MODIFIED_BY	int	ID do usuário que fez a última atualização.
RV01 - 10	INT	Valores reservados de 1 a 10 Reservada para uso futuro do Sentinel. O uso desse campo para qualquer outra finalidade pode resultar em sobregravação de dados por uma funcionalidade futura.
RV11 - 20	DATETIME	Valores reservados de 11 a 20 Reservada para uso futuro do Sentinel. O uso desse campo para qualquer outra finalidade pode resultar em sobregravação de dados por uma funcionalidade futura.
RV21 - 25	identificador exclusivo	Valores reservados de 21 a 25 Reservada para uso futuro do Sentinel para o armazenamento de UUIDs. O uso desse campo para qualquer outra finalidade pode resultar em sobregravação de dados por uma funcionalidade futura.

Nome da coluna	Tipo de dados	Comentário
RV26 - 31	VARCHAR(255)	Valores reservados de 26 a 31 Reservada para uso futuro do Sentinel. O uso desse campo para qualquer outra finalidade pode resultar em sobregravação de dados por uma funcionalidade futura.
RV32	VARCHAR(255)	Valor reservado - 32 Reservado para o DeviceCategory O uso desse campo para qualquer outra finalidade pode resultar em sobregravação de dados por uma funcionalidade futura.
RV33	VARCHAR(255)	Valor reservado - 33 Reservado para o EventContex O uso desse campo para qualquer outra finalidade pode resultar em sobregravação de dados por uma funcionalidade futura.
RV34	VARCHAR(255)	Valor reservado - 34 Reservado para o SourceThreatLevel O uso desse campo para qualquer outra finalidade pode resultar em sobregravação de dados por uma funcionalidade futura.
RV35	VARCHAR(255)	Valor reservado - 35 Reservado para o SourceUserContext. O uso desse campo para qualquer outra finalidade pode resultar em sobregravação de dados por uma funcionalidade futura.
RV36	VARCHAR(255)	Valor reservado - 36 Reservado para o DataContext. O uso desse campo para qualquer outra finalidade pode resultar em sobregravação de dados por uma funcionalidade futura.

Nome da coluna	Tipo de dados	Comentário
RV37	VARCHAR(255)	Valor reservado - 37 Reservado para o SourceFunction. O uso desse campo para qualquer outra finalidade pode resultar em sobregravação de dados por uma funcionalidade futura.
RV38	VARCHAR(255)	Valor reservado - 38 Reservado para o SourceOperationalContext. O uso desse campo para qualquer outra finalidade pode resultar em sobregravação de dados por uma funcionalidade futura.
RV39	VARCHAR(255)	Valor reservado - 39 Reservado para o MSSPCustomerName. O uso desse campo para qualquer outra finalidade pode resultar em sobregravação de dados por uma funcionalidade futura.
RV40 - 43	VARCHAR(255)	Valores reservados de 40 a 43 Reservada para uso futuro do Sentinel. O uso desse campo para qualquer outra finalidade pode resultar em sobregravação de dados por uma funcionalidade futura.
RV44	VARCHAR(255)	Valor reservado - 44 Reservado para o DestinationThreatLevel. O uso desse campo para qualquer outra finalidade pode resultar em sobregravação de dados por uma funcionalidade futura.
RV45	VARCHAR(255)	Valor reservado - 45 Reservado para o DestinationUserContext. O uso desse campo para qualquer outra finalidade pode resultar em sobregravação de dados por uma funcionalidade futura.

Nome da coluna	Tipo de dados	Comentário
RV46	VARCHAR(255)	Valor reservado - 46 Reservado para o VirusStatus. O uso desse campo para qualquer outra finalidade pode resultar em sobregravação de dados por uma funcionalidade futura.
RV47	VARCHAR(255)	Valor reservado - 47 Reservada para uso futuro do Sentinel. O uso desse campo para qualquer outra finalidade pode resultar em sobregravação de dados por uma funcionalidade futura.
RV48	VARCHAR(255)	Valor reservado - 48 Reservado para o DestinationOperationalContext. O uso desse campo para qualquer outra finalidade pode resultar em sobregravação de dados por uma funcionalidade futura.
RV49	VARCHAR(255)	Valor reservado - 49 Reservada para uso futuro do Sentinel. O uso desse campo para qualquer outra finalidade pode resultar em sobregravação de dados por uma funcionalidade futura.
RV50	VARCHAR(255)	Nível de taxonomia 1
RV51	VARCHAR(255)	Nível de taxonomia 2
RV52	VARCHAR(255)	Nível de taxonomia 3
RV53	VARCHAR(255)	Nível de taxonomia 4
CV01 - 10	INT	Valor personalizado de 1 a 10 Reservado para o uso do Cliente, geralmente para associação de dados de relevância para a empresa
CV11 - 20	DATETIME	Valor personalizado de 11 a 20 Reservado para o uso do Cliente, geralmente para associação de dados de relevância para a empresa
CV21 - 100	VARCHAR(255)	Valor personalizado de 21 a 100 Reservado para o uso do Cliente, geralmente para associação de dados de relevância para a empresa

EVENTS_ALL_RPT_V1 (Fornecida para fins de compatibilidade retroativa)

A tela contém os eventos atuais. Possui as mesmas colunas que EVENT_ALL_RPT_V.

EVENTS_RPT_V (Fornecida para fins de compatibilidade retroativa)

A tela contém os eventos atuais e históricos. Possui as mesmas colunas que EVENT_ALL_RPT_V.

EVENTS_RPT_V1 (Fornecida para fins de compatibilidade retroativa)

A tela contém os eventos atuais. Possui as mesmas colunas que EVENT_ALL_RPT_V.

EVENTS_RPT_V2 (Fornecida para fins de compatibilidade retroativa)

A tela contém os eventos atuais e históricos.

Nome da coluna	Tipo de dados	Comentário
EVENT_ID	identificador exclusivo	Identificador do evento
RESOURCE_NAME	varchar(255)	Nome do recurso
SUB_RESOURCE	varchar(255)	Nome do sub-recurso
SEVERITY	int	Gravidade do evento
EVENT_PARSE_TIME	data/horário	Horário do evento
EVENT_DATETIME	data/horário	Horário do evento
BASE_MESSAGE	varchar(4000)	Mensagem base
EVENT_NAME	varchar(255)	Nome do evento conforme relatado pelo sensor
EVENT_TIME	varchar(255)	Horário do evento conforme relatado pelo sensor
TAXONOMY_ID	bigint	Identificador de taxonomia
PROTOCOL_ID	bigint	Identificador de protocolo
AGENT_ID	bigint	Identificador de Coletor
SOURCE_IP	int	Endereço IP de origem em formato numérico
SOURCE_HOST_NAME	varchar(255)	Nome do host de origem
SOURCE_PORT	varchar(32)	Porta de origem
DESTINATION_IP	int	Endereço IP de destino em formato numérico
DESTINATION_HOST_NAME	varchar(255)	Nome do host de destino
DESTINATION_PORT	varchar(32)	Porta de destino
SOURCE_USER_NAME	varchar(255)	Nome do usuário de origem
DESTINATION_USER_NAME	varchar(255)	Nome do usuário de destino
FILE_NAME	varchar(1000)	Nome do arquivo
EXTENDED_INFO	varchar(1000)	Informações estendidas
CUSTOM_TAG_1	varchar(255)	Tag de Cliente 1
CUSTOM_TAG 2	varchar(255)	Tag de Cliente 2
CUSTOM_TAG 3	int	Tag de Cliente 3

Nome da coluna	Tipo de dados	Comentário
RESERVED_TAG_1	VARCHAR(255)	Tag Reservada 1 Reservada para uso futuro do Sentinel. Campo usado para informações do Consultor sobre descrições de ataque.
RESERVED_TAG_2	varchar(255)	Reservada para uso futuro do Sentinel. O uso desse campo para qualquer outra finalidade pode resultar em sobregravação de dados por uma funcionalidade futura.
RESERVED_TAG_3	int	Reservada para uso futuro do Sentinel. O uso desse campo para qualquer outra finalidade pode resultar em sobregravação de dados por uma funcionalidade futura.
VULNERABILITY_RATING	int	Classificação de vulnerabilidade
CRITICALITY_RATING	int	Classificação de importância
DATE_CREATED	data/horário	Data de inserção
DATE_MODIFIED	data/horário	Data da última atualização
CREATED_BY	int	ID do usuário que fez a inserção.
MODIFIED_BY	int	ID do usuário que fez a última atualização.
RV01 - 10	INT	Valores reservados de 1 a 10 Reservada para uso futuro do Sentinel. O uso desse campo para qualquer outra finalidade pode resultar em sobregravação de dados por uma funcionalidade futura.
RV11 - 20	DATETIME	Valores reservados de 1 a 31 Reservada para uso futuro do Sentinel. O uso desse campo para qualquer outra finalidade pode resultar em sobregravação de dados por uma funcionalidade futura.
RV21 - 25	identificador exclusivo	Valores reservados de 21 a 25 Reservada para uso futuro do Sentinel para o armazenamento de UUIDs. O uso desse campo para qualquer outra finalidade pode resultar em sobregravação de dados por uma funcionalidade futura.

Nome da coluna	Tipo de dados	Comentário
RV26 - 31	VARCHAR(255)	Valores reservados de 26 a 31 Reservada para uso futuro do Sentinel. O uso desse campo para qualquer outra finalidade pode resultar em sobregravação de dados por uma funcionalidade futura.
RV33	VARCHAR(255)	Valor reservado - 33 Reservado para o EventContex O uso desse campo para qualquer outra finalidade pode resultar em sobregravação de dados por uma funcionalidade futura.
RV34	VARCHAR(255)	Valor reservado - 34 Reservado para o SourceThreatLevel O uso desse campo para qualquer outra finalidade pode resultar em sobregravação de dados por uma funcionalidade futura.
RV35	VARCHAR(255)	Valor reservado - 35 Reservado para o SourceUserContext. O uso desse campo para qualquer outra finalidade pode resultar em sobregravação de dados por uma funcionalidade futura.
RV36	VARCHAR(255)	Valor reservado - 36 Reservado para o DataContext. O uso desse campo para qualquer outra finalidade pode resultar em sobregravação de dados por uma funcionalidade futura.
RV37	VARCHAR(255)	Valor reservado - 37 Reservado para o SourceFunction. O uso desse campo para qualquer outra finalidade pode resultar em sobregravação de dados por uma funcionalidade futura.
RV38	VARCHAR(255)	Valor reservado - 38 Reservado para o SourceOperationalContext. O uso desse campo para qualquer outra finalidade pode resultar em sobregravação de dados por uma funcionalidade futura.

Nome da coluna	Tipo de dados	Comentário
RV40 - 43	VARCHAR(255)	Valores reservados de 40 a 43 Reservada para uso futuro do Sentinel. O uso desse campo para qualquer outra finalidade pode resultar em sobregravação de dados por uma funcionalidade futura.
RV44	VARCHAR(255)	Valor reservado - 44 Reservado para o DestinationThreatLevel. O uso desse campo para qualquer outra finalidade pode resultar em sobregravação de dados por uma funcionalidade futura.
RV45	VARCHAR(255)	Valor reservado - 45 Reservado para o DestinationUserContext. O uso desse campo para qualquer outra finalidade pode resultar em sobregravação de dados por uma funcionalidade futura.
RV46	VARCHAR(255)	Valor reservado - 46 Reservado para o VirusStatus. O uso desse campo para qualquer outra finalidade pode resultar em sobregravação de dados por uma funcionalidade futura.
RV47	VARCHAR(255)	Valor reservado - 47 Reservada para uso futuro do Sentinel. O uso desse campo para qualquer outra finalidade pode resultar em sobregravação de dados por uma funcionalidade futura.
RV48	VARCHAR(255)	Valor reservado - 48 Reservado para o DestinationOperationalContext. O uso desse campo para qualquer outra finalidade pode resultar em sobregravação de dados por uma funcionalidade futura.
RV49	VARCHAR(255)	Valor reservado - 49 Reservada para uso futuro do Sentinel. O uso desse campo para qualquer outra finalidade pode resultar em sobregravação de dados por uma funcionalidade futura.

Nome da coluna	Tipo de dados	Comentário
REFERENCE_ID 01 - 20	BIGINT	Reservada para uso futuro do Sentinel. O uso desse campo para qualquer outra finalidade pode resultar em sobregravação de dados por uma funcionalidade futura.
CV01 - 10	INT	Valor personalizado de 1 a 10 Reservado para o uso do Cliente, geralmente para associação de dados de relevância para a empresa
CV11 - 20	DATETIME	Valor personalizado de 11 a 20 Reservado para o uso do Cliente, geralmente para associação de dados de relevância para a empresa
CV21 - 100	VARCHAR(255)	Valor personalizado de 21 a 100 Reservado para o uso do Cliente, geralmente para associação de dados de relevância para a empresa

EVT_AGENT_RPT_V

A tela faz referência à tabela EVT_AGENT, que armazena informações sobre Coletores.

Nome da coluna	Tipo de dados	Comentário
AGENT_ID	bigint	Identificador de Coletor
AGENT	varchar(64)	Nome do Coletor
PORT	varchar(64)	Porta do Coletor
REPORT_NAME	varchar(255)	Nome do relator
PRODUCT_NAME	varchar(255)	Nome do produto
SENSOR_NAME	varchar(255)	Nome do sensor
SENSOR_TYPE	varchar(5)	Tipo de sensor: H - baseado em host N - baseado em rede V - vírus O - outro
DEVICE_CTGRY	varchar(255)	Categoria do dispositivo
SOURCE_UUID	identificador exclusivo	Identificador Exclusivo Universal (UUID) do componente de origem
DATE_CREATED	data/horário	Data de inserção
DATE_MODIFIED	data/horário	Data da última atualização
CREATED_BY	int	ID do usuário que fez a inserção.
MODIFIED_BY	int	ID do usuário que fez a última atualização.

EVT_ASSET_RPT_V

A tela faz referência à tabela EVT_ASSET, que armazena informações sobre bens.

Nome da coluna	Tipo de dados	Comentário
EVENT_ASSET_ID	bigint	Identificador do bem do evento
ASSET_NAME	varchar(255)	Nome do bem
PHYSICAL_ASSET_NAME	varchar(255)	Nome do bem físico
REFERENCE_ASSET_ID	varchar(100)	Identificador do bem de referência, que se vincula com o sistema de gerenciamento do bem de origem.
MAC_ADDRESS	varchar(100)	Endereço MAC
RACK_NUMBER	varchar(50)	Número do rack
ROOM_NAME	varchar(100)	Nome da sala
BUILDING_NAME	varchar(255)	Nome do prédio
CITY	varchar(100)	Cidade
STATE	varchar(100)	Estado
COUNTRY	varchar(100)	País
ZIP_CODE	varchar(50)	CEP
ASSET_CATEGORY_NAME	varchar(100)	Nome de categoria de bem
NETWORK_IDENTITY_NAME	varchar(255)	Nome da identidade da rede do bem
ENVIRONMENT_IDENTITY_NAME	varchar(255)	Nome do ambiente
ASSET_VALUE_NAME	varchar(50)	Nome do valor do bem
CRITICALITY_NAME	varchar(50)	Nome da importância do bem
SENSITIVITY_NAME	varchar(50)	Nome da distinção do bem
CONTACT_NAME_1	varchar(255)	Nome da pessoa de contato/organização 1
CONTACT_NAME_2	varchar(255)	Nome da pessoa de contato/organização 2
ORGANIZATION_NAME_1	varchar(100)	Nível 1 da organização do proprietário do bem
ORGANIZATION_NAME_2	varchar(100)	Nível 2 da organização do proprietário do bem
ORGANIZATION_NAME_3	varchar(100)	Nível 3 da organização do proprietário do bem
ORGANIZATION_NAME_4	varchar(100)	Nível 4 da organização do proprietário do bem
DATE_CREATED	data/horário	Data de inserção
DATE_MODIFIED	data/horário	Data da última atualização
CREATED_BY	int	ID do usuário que fez a inserção.
MODIFIED_BY	int	ID do usuário que fez a última atualização.

EVT_DEST_EVT_NAME_SMRY_1_RPT_V

Essa tela resume o total de eventos por destino, taxonomia, nome do evento, gravidade e horário do evento.

Nome da coluna	Tipo de dados	Comentário
DESTINATION_IP	int	Endereço IP de Destino
DESTINATION_EVENT_ASSET_ID	bigint	Identificador do bem do evento
TAXONOMY_ID	bigint	Identificador de taxonomia
EVENT_NAME_ID	bigint	Identificador do nome do evento
SEVERITY	int	Gravidade do evento
CUSTOMER_ID	bigint	Identificador de cliente
EVT_TIME	data/horário	Horário do evento
EVT_COUNT	int	Total de Eventos
DATE_CREATED	data/horário	Data de inserção
DATE_MODIFIED	data/horário	Data da última atualização
CREATED_BY	int	ID do usuário que fez a inserção.
MODIFIED_BY	int	ID do usuário que fez a última atualização.

EVT_DEST_SMRY_1_RPT_V

Essa tela contém informações de resumo de destino de eventos.

Nome da coluna	Tipo de dados	Comentário
DESTINATION_IP	int	Endereço IP de Destino
DESTINATION_EVENT_ASSET_ID	bigint	Identificador do bem do evento
DESTINATION_PORT	varchar(32)	Porta de destino
DESTINATION_USR_ID	bigint	Identificador do usuário de destino
TAXONOMY_ID	bigint	Identificador de taxonomia
EVENT_NAME_ID	bigint	Identificador do nome do evento
RESOURCE_ID	bigint	Identificador do recurso
AGENT_ID	bigint	Identificador de Coletor
PROTOCOL_ID	bigint	Identificador de protocolo
SEVERITY	int	Gravidade do evento
CUSTOMER_ID	bigint	Identificador de cliente
EVENT_TIME	data/horário	Horário do evento
EVENT_COUNT	int	Total de Eventos
DATE_CREATED	data/horário	Data de inserção
DATE_MODIFIED	data/horário	Data da última atualização
CREATED_BY	int	ID do usuário que fez a inserção.
MODIFIED_BY	int	ID do usuário que fez a última atualização.

EVT_DEST_TXNMY_SMRY_1_RPT_V

Essa tela resume o total de eventos por destino, taxonomia, gravidade e horário do evento.

Nome da coluna	Tipo de dados	Comentário
DESTINATION_IP	int	Endereço IP de Destino
DESTINATION_EVENT_ASSET_ID	bigint	Identificador do bem do evento
TAXONOMY_ID	bigint	Identificador de taxonomia
SEVERITY	int	Gravidade do evento
CUSTOMER_ID	bigint	Identificador de cliente
EVENT_TIME	data/horário	Horário do evento
EVENT_COUNT	int	Total de Eventos
DATE_CREATED	data/horário	Data de inserção
DATE_MODIFIED	data/horário	Data da última atualização
CREATED_BY	int	ID do usuário que fez a inserção.
MODIFIED_BY	int	ID do usuário que fez a última atualização.

EVT_NAME_RPT_V

A tela faz referência à tabela EVT_NAME, que armazena informações sobre nomes de eventos.

Nome da coluna	Tipo de dados	Comentário
EVENT_NAME_ID	bigint	Identificador do nome do evento
EVENT_NAME	varchar(255)	Nome do evento
DATE_CREATED	data/horário	Data de inserção
DATE_MODIFIED	data/horário	Data da última atualização
CREATED_BY	int	ID do usuário que fez a inserção.
MODIFIED_BY	int	ID do usuário que fez a última atualização.

EVT_PORT_SMRY_1_RPT_V

Essa tela resume o total de eventos por porta de destino, gravidade e horário do evento.

Nome da coluna	Tipo de dados	Comentário
DESTINATION_PORT	Varchar(32)	Porta de destino
SEVERITY	int	Gravidade do evento
CUSTOMER_ID	bigint	Identificador de cliente
EVENT_TIME	data/horário	Horário do evento
EVENT_COUNT	int	Total de Eventos
DATE_CREATED	data/horário	Data de inserção
DATE_MODIFIED	data/horário	Data da última atualização
CREATED_BY	int	ID do usuário que fez a inserção.
MODIFIED_BY	int	ID do usuário que fez a última atualização.

EVT_PRTCL_RPT_V

A tela faz referência à tabela EVT_PRTCL, que armazena informações sobre protocolo.

Nome da coluna	Tipo de dados	Comentário
PROTOCOL_ID	bigint	Identificador de protocolo
PROTOCOL_NAME	varchar(255)	Nome do protocolo
DATE_CREATED	data/horário	Data de inserção
DATE_MODIFIED	data/horário	Data da última atualização
CREATED_BY	int	ID do usuário que fez a inserção.
MODIFIED_BY	int	ID do usuário que fez a última atualização.

EVT_RSRC_RPT_V

A tela faz referência à tabela EVT_RSRC, que armazena informações sobre recursos.

Nome da coluna	Tipo de dados	Comentário
RESOURCE_ID	bigint	Identificador do recurso
RESOURCE_NAME	varchar(255)	Nome do recurso
SUB_RESOURCE_NAME	varchar(255)	Nome do sub-recurso
DATE_CREATED	data/horário	Data de inserção
DATE_MODIFIED	data/horário	Data da última atualização
CREATED_BY	int	ID do usuário que fez a inserção.
MODIFIED_BY	int	ID do usuário que fez a última atualização.

EVT_SEV_SMRY_1_RPT_V

Essa tela resume o total de eventos por gravidade e horário do evento.

Nome da coluna	Tipo de dados	Comentário
SEVERITY	int	Gravidade do evento
CUSTOMER_ID	bigint	Identificador de cliente
EVENT_TIME	data/horário	Horário do evento
EVENT_COUNT	int	Total de Eventos
DATE_CREATED	data/horário	Data de inserção
DATE_MODIFIED	data/horário	Data da última atualização
CREATED_BY	int	ID do usuário que fez a inserção.
MODIFIED_BY	int	ID do usuário que fez a última atualização.

EVT_SRC_SMRY_1_RPT_V

Essa tela contém informações de resumo de origem e destino de eventos.

Nome da coluna	Tipo de dados	Comentário
SOURCE_IP	int	Endereço IP de Origem
SOURCE_EVENT_ASSET_ID	bigint	Identificador do bem do evento
SOURCE_PORT	varchar(32)	Porta de origem
SOURCE_USER_ID	bigint	Identificador do usuário
TAXONOMY _ID	bigint	Identificador de taxonomia

Nome da coluna	Tipo de dados	Comentário
EVENT_NAME_ID	bigint	Identificador do nome do evento
RESOURCE_ID	bigint	Identificador do recurso
AGENT_ID	bigint	Identificador de Coletor
PROTOCOL _ID	bigint	Identificador de protocolo
SEVERITY	int	Gravidade do evento
CUSTOMER_ID	bigint	Identificador de cliente
EVENT_TIME	data/horário	Horário do evento
EVENT_COUNT	int	Total de Eventos
DATE_CREATED	data/horário	Data de inserção
DATE_MODIFIED	data/horário	Data da última atualização
CREATED_BY	int	ID do usuário que fez a inserção.
MODIFIED_BY	int	ID do usuário que fez a última atualização.

EVT_TXNMY_RPT_V

A tela faz referência à tabela EVT_TXNMY, que armazena informações sobre taxonomia.

Nome da coluna	Tipo de dados	Comentário
TAXONOMY _ID	bigint	Identificador de taxonomia
TAXONOMY _ LEVEL _1	varchar(100)	Nível de taxonomia 1
TAXONOMY _ LEVEL _2	varchar(100)	Nível de taxonomia 2
TAXONOMY _ LEVEL _3	varchar(100)	Nível de taxonomia 3
TAXONOMY _ LEVEL _4	varchar(100)	Nível de taxonomia 4
DATE_CREATED	data/horário	Data de inserção
DATE_MODIFIED	data/horário	Data da última atualização
CREATED_BY	int	ID do usuário que fez a inserção.
MODIFIED_BY	int	ID do usuário que fez a última atualização.
TAXONOMY _ID	bigint	Identificador de taxonomia

EVT_USR_RPT_V

A tela faz referência à tabela EVT_USR, que armazena informações sobre usuários de eventos.

Nome da coluna	Tipo de dados	Comentário
USER_ID	bigint	Identificador do usuário
USER_NAME	varchar(255)	Nome do usuário
DATE_CREATED	data/horário	Data de inserção
DATE_MODIFIED	data/horário	Data da última atualização
CREATED_BY	int	ID do usuário que fez a inserção.
MODIFIED_BY	int	ID do usuário que fez a última atualização.
USER_ID	bigint	Identificador do usuário

EXTERNAL_DATA_RPT_V

A tela faz referência à tabela EXTERNAL_DATA, que armazena dados externos.

Nome da coluna	Tipo de dados	Comentário
EXTERNAL_DATA_ID	int	Identificador de dados externos
SOURCE_NAME	varchar(50)	Nome de origem
SOURCE_DATA_ID	varchar(255)	Identificador de dados de origem
EXTERNAL_DATA	texto	Dados externos
EXTERNAL_DATA_TYPE	varchar(10)	Tipo de dados externos
DATE_CREATED	data/horário	Data de inserção
DATE_MODIFIED	data/horário	Data da última atualização
CREATED_BY	int	ID do usuário que fez a inserção.
MODIFIED_BY	int	ID do usuário que fez a última atualização.

HIST_EVENTS_RPT_V

Ver eventos históricos (eventos restaurados dos arquivos).

HIST_INCIDENTS_RPT_V

Ver incidentes históricos (incidentes restaurados dos arquivos).

IMAGES_RPT_V

A tela faz referência à tabela IMAGES, que armazena informações sobre imagens de visão geral do sistema.

Nome da coluna	Tipo de dados	Comentário
NAME	VARCHAR(128)	Nome da imagem
TYPE	VARCHAR(64)	Tipo de imagem
DATA	TEXT	Dados de imagem
DATE_CREATED	DATETIME	Data de inserção
DATE_MODIFIED	DATETIME	Data da última atualização
CREATED_BY	INT	ID do usuário que fez a inserção
MODIFIED_BY	INT	ID do usuário que fez a última atualização

INCIDENTS_ASSETS_RPT_V

A tela faz referência à tabela INCIDENTS_ASSETS, que armazena informações sobre os bens que formam incidentes criados no Console do Sentinel.

Nome da coluna	Tipo de dados	Comentário
INC_ID	INT	Identificador de incidente – número de seqüência
ASSET_ID	identificador exclusivo	Identificador Exclusivo Universal (UUID) de bem
DATE_CREATED	DATETIME	Data de inserção
DATE_MODIFIED	DATETIME	Data da última atualização

Nome da coluna	Tipo de dados	Comentário
CREATED_BY	INT	ID do usuário que fez a inserção
MODIFIED_BY	INT	ID do usuário que fez a última atualização

INCIDENTS_EVENTS_RPT_V

A tela faz referência à tabela INCIDENTS_EVENTS, que armazena informações sobre os eventos que compõem incidentes criados no Console do Sentinel.

Nome da coluna	Tipo de dados	Comentário
INC_ID	INT	Identificador de incidente – número de seqüência
EVT_ID	identificador exclusivo	Identificador Exclusivo Universal (UUID) de evento
EVT_TIME	DATETIME	Horário do evento
DATE_CREATED	DATETIME	Data de inserção
DATE_MODIFIED	DATETIME	Data da última atualização
CREATED_BY	INT	ID do usuário que fez a inserção
MODIFIED_BY	INT	ID do usuário que fez a última atualização

INCIDENTS_RPT_V

A tela faz referência à tabela INCIDENTS, que armazena informações que descrevem os detalhes de incidentes criados no Console do Sentinel.

Nome da coluna	Tipo de dados	Comentário
INC_ID	INT	Identificador de incidente – número de seqüência
NAME	VARCHAR(255)	Nome do incidente
SEVERITY	INT	Gravidade do incidente
STT_ID	INT	ID de Estado do Incidente
SEVERITY_RATING	VARCHAR(32)	Média de todas as gravidades de eventos que formam um incidente.
VULNERABILITY_RATING	VARCHAR(32)	Reservada para uso futuro do Sentinel. O uso desse campo para qualquer outra finalidade pode resultar em sobregravação de dados por uma funcionalidade futura.
CRITICALITY_RATING	VARCHAR(32)	Reservada para uso futuro do Sentinel. O uso desse campo para qualquer outra finalidade pode resultar em sobregravação de dados por uma funcionalidade futura.
DATE_CREATED	DATETIME	Data de inserção
DATE_MODIFIED	DATETIME	Data da última atualização
CREATED_BY	INT	ID do usuário que fez a inserção
MODIFIED_BY	INT	ID do usuário que fez a última atualização
INC_DESC	varchar(4000)	Descrição do incidente

Nome da coluna	Tipo de dados	Comentário
INC_PRIORITY	int	Prioridade do incidente
INC_CAT	varchar(255)	Categoria do incidente
INC_RES	varchar(4000)	Resolução do incidente

INCIDENTS_VULN_RPT_V

A tela faz referência à tabela INCIDENTS_VULN, que armazena informações sobre as vulnerabilidades que compõem incidentes criados no Console do Sentinel.

Nome da coluna	Tipo de dados	Comentário
INC_ID	INT	Identificador de incidente – número de seqüência
VULN_ID	identificador exclusivo	Identificador Exclusivo Universal (UUID) de vulnerabilidade
DATE_CREATED	DATETIME	Data de inserção
DATE_MODIFIED	DATETIME	Data da última atualização
CREATED_BY	INT	ID do usuário que fez a inserção
MODIFIED_BY	INT	ID do usuário que fez a última atualização

L_STAT_RPT_V

A tela faz referência à tabela L_STAT, que armazena informações estatísticas.

Nome da coluna	Tipo de dados	Comentário
RES_NAME	VARCHAR(32)	Nome do recurso
STATS_NAME	VARCHAR(32)	Nome da estatística
STATS_VALUE	VARCHAR(32)	Valor da estatística
OPEN_TOT_SECS	NUMERIC	Número de segundos desde 1970.

LOGS_RPT_V

A tela faz referência à tabela LOGS_RPT, que armazena informações sobre registro.

Tabela LOGS		
Nome da coluna	**Tipo de dados**	**Comentário**
LOG_ID	NÚMERO	Número de seqüência
TIME	DATE	Data do Registro
MODULE	VARCHAR(64)	O módulo ao qual o registro se destina
TEXT	VARCHAR(4000)	Texto do registro

NETWORK_IDENTITY_RPT_V

A tela faz referência à tabela NETWORK_IDENTITY_LKUP, que armazena informações sobre a identidade da rede do bem.

Nome da coluna	Tipo de dados	Comentário
NETWORK_IDENTITY_CD	varchar(5)	Código de identidade da rede
NETWORK_IDENTITY_NAME	varchar(255)	Nome de identidade da rede
DATE_CREATED	data/horário	Data de inserção
DATE_MODIFIED	data/horário	Data da última atualização

Nome da coluna	Tipo de dados	Comentário
CREATED_BY	int	ID do usuário que fez a inserção
MODIFIED_BY	int	ID do usuário que fez a última atualização

ORGANIZATION_RPT_V

A tela faz referência à tabela ORGANIZATION, que armazena informações sobre organização (bem).

Nome da coluna	Tipo de dados	Comentário
ORGANIZATION_ID	identificador exclusivo	Identificador de organização
ORGANIZATION_NAME	varchar(100)	Nome da organização
CUSTOMER_ID	bigint	Identificador de cliente
DATE_CREATED	data/horário	Data de inserção
DATE_MODIFIED	data/horário	Data da última atualização
CREATED_BY	int	ID do usuário que fez a inserção
MODIFIED_BY	int	ID do usuário que fez a última atualização

PERSON_RPT_V

A tela faz referência à tabela PERSION, que armazena informações pessoais (bem).

Nome da coluna	Tipo de dados	Comentário
PERSON_ID	identificador exclusivo	Identificador de pessoa
FIRST_NAME	varchar(255)	Nome
LAST_NAME	varchar(255)	Sobrenome
CUSTOMER_ID	bigint	Identificador de cliente
PHONE_NUMBER	varchar(50)	Número de telefone
EMAIL_ADDRESS	varchar(255)	Endereço de e-mail
DATE_CREATED	data/horário	Data de inserção
DATE_MODIFIED	data/horário	Data da última atualização
CREATED_BY	int	ID do usuário que fez a inserção
MODIFIED_BY	int	ID do usuário que fez a última atualização

PHYSICAL_ASSET_RPT_V

A tela faz referência à tabela PHYSICAL_ASSET, que armazena informações físicas sobre bens.

Nome da coluna	Tipo de dados	Comentário
PHYSICAL_ASSET_ID	identificador exclusivo	Identificador de bem físico
CUSTOMER_ID	int	Identificador de cliente
LOCATION_ID	bigint	Identificador de local
HOST_NAME	varchar(255)	Nome de host
IP_ADDRESS	int	Endereço IP

Nome da coluna	Tipo de dados	Comentário
NETWORK_IDENTITY_CD	varchar(5)	Código de identidade da rede
MAC_ADDRESS	varchar(100)	Endereço MAC
RACK_NUMBER	varchar(50)	Número do rack
ROOM_NAME	varchar(100)	Nome da sala
DATE_CREATED	data/horário	Data de inserção
DATE_MODIFIED	data/horário	Data da última atualização
CREATED_BY	int	ID do usuário que fez a inserção
MODIFIED_BY	int	ID do usuário que fez a última atualização

PRODUCT_RPT_V

A tela faz referência à tabela PRDT, que armazena informações sobre produtos de bens.

Nome da coluna	Tipo de dados	Comentário
PRODUCT _ID	bigint	Identificador de produtos
PRODUCT _NAME	varchar(255)	Nome do produto
PRODUCT _VERSION	varchar(100)	Versão do produto
VENDOR _ID	bigint	Identificador do fornecedor
DATE_CREATED	data/horário	Data de inserção
DATE_MODIFIED	data/horário	Data da última atualização
CREATED_BY	int	ID do usuário que fez a inserção
MODIFIED_BY	int	ID do usuário que fez a última atualização

ROLE_RPT_V

A tela faz referência à tabela ROLE_LKUP, que armazena informações sobre a função do usuário (bem).

Nome da coluna	Tipo de dados	Comentário
ROLE_CODE	varchar(5)	Código de função
ROLE_NAME	varchar(255)	Nome da função
DATE_CREATED	data/horário	Data de inserção
DATE_MODIFIED	data/horário	Data da última atualização
CREATED_BY	int	ID do usuário que fez a inserção
MODIFIED_BY	int	ID do usuário que fez a última atualização

SENSITIVITY_RPT_V

A tela faz referência à tabela SENSITIVITY_LKUP, que armazena informações sobre sigilo de bens.

Nome da coluna	Tipo de dados	Comentário
SENSITIVITY_CODE	varchar(5)	Código de distinção do bem
SENSITIVITY_NAME	varchar(50)	Nome da distinção do bem
DATE_CREATED	data/horário	Data de inserção
DATE_MODIFIED	data/horário	Data da última atualização

Nome da coluna	Tipo de dados	Comentário
CREATED_BY	int	Por ID de usuário
MODIFIED_BY	int	Por ID de usuário

STATES_RPT_V

A tela faz referência à tabela STATES, que armazena definições de estados definidos por aplicativos ou contexto.

Nome da coluna	Tipo de dados	Comentário
STT_ID	INT	ID do estado – número de seqüência
CONTEXT	VARCHAR(64)	Contexto do estado. Trata-se de caso, incidente, usuário.
NAME	VARCHAR(64)	Nome do estado.
TERMINAL_FLAG	VARCHAR(1)	Indica se o estado do incidente é resolvido.
DATE_CREATED	DATETIME	Data de inserção
DATE_MODIFIED	DATETIME	Data da última atualização
MODIFIED_BY	INT	ID do usuário que fez a inserção
CREATED_BY	INT	ID do usuário que fez a última atualização

Tela UNASSIGNED_INCIDENTS_RPT_V

A tela faz referência às tabelas CASES e INCIDENTS para relatar casos não atribuídos.

Nome	Tipo de dados
INC_ID	INT
NAME	VARCHAR(255)
SEVERITY	INT
STT_ID	INT
SEVERITY_RATING	VARCHAR(32)
VULNERABILITY_RATING	VARCHAR(32)
CRITICALITY_RATING	VARCHAR(32)
DATE_CREATED	DATETIME
DATE_MODIFIED	DATETIME
CREATED_BY	INT
MODIFIED_BY	INT
INC_DESC	VARCHAR(4000)
INC_PRIORITY	INT
INC_CAT	VARCHAR(255)
INC_RES	VARCHAR(4000)

USERS_RPT_V

A tela faz referência à tabela USERS, que relaciona todos os usuários do aplicativo. Os usuários também serão criados como usuários do banco de dados para acomodar ferramentas de relatório de terceiros.

Nome da coluna	Tipo de dados	Comentário
USR_ID	INT	Identificador de usuário – Número de seqüência
NAME	VARCHAR(64)	Nome de usuário curto e exclusivo usado como login
CNT_ID	INT	ID do contato – Número de seqüência
STT_ID	INT	ID do estado. O status é ativo ou inativo.
DESCRIPTION	VARCHAR(512)	Comentários
DATE_CREATED	DATETIME	Data de inserção
DATE_MODIFIED	DATETIME	Data da última atualização
CREATED_BY	INT	ID do usuário que fez a inserção
MODIFIED_BY	INT	ID do usuário que fez a última atualização
PERMISSIONS	VARCHAR(4000)	Permissões atualmente atribuídas ao usuário do Sentinel
FILTER	VARCHAR(128)	Filtro de segurança atual atribuído ao usuário do Sentinel
UPPER_NAME	VARCHAR(64)	Nome do usuário em maiúsculas
DOMAIN_AUTH_IND	Bit	Indicação de autenticação de domínio

VENDOR_RPT_V

A tela faz referência à tabela VNDR, que armazena informações sobre fornecedores de produtos de bens.

Nome da coluna	Tipo de dados	Comentário
VENDOR_ID	bigint	Identificador do fornecedor
VENDOR_NAME	varchar(255)	Nome do fornecedor
DATE_CREATED	data/horário	Data de inserção
DATE_MODIFIED	data/horário	Data da última atualização
CREATED_BY	int	ID do usuário que fez a inserção
MODIFIED_BY	int	ID do usuário que fez a última atualização

VULN_CALC_SEVERITY_RPT_V

A tela faz referência a VULN_RSRC e VULN para calcular a classificação de gravidade de vulnerabilidade do eSecurity com base nas vulnerabilidades atuais.

Nome da coluna	Tipo de dados
RSRC_ID	identificador exclusivo
IP	VARCHAR(32)
HOST_NAME	VARCHAR(255)
CRITICALITY	int
ASSIGNED_VULN_SEVERITY	int

Nome da coluna	Tipo de dados
VULN_COUNT	Total de Vulnerabilidades para o Recurso especificado
CALC_SEVERITY	Gravidade calculada com base em ASSIGNED_VULN_SEVERITY e CRITICALITY

VULN_CODE_RPT_V

A tela faz referência à tabela VULN_CODE, que armazena códigos de vulnerabilidade atribuídos pela indústria, como CVEs e CANs da Mitre.

Nome da coluna	Tipo de dados
VULN_CODE_ID	VARCHAR(36)
VULN_ID	VARCHAR(36)
VULN_CODE_TYPE	VARCHAR(64)
VULN_CODE_VALUE	VARCHAR(255)
URL	VARCHAR(512)
DATE_CREATED	DATETIME
DATE_MODIFIED	DATETIME
CREATED_BY	INT
MODIFIED_BY	INT

VULN_INFO_RPT_V

A tela faz referência à tabela VULN_INFO, que armazena informações adicionais relatadas durante uma exploração.

Nome da coluna	Tipo de dados
VULN_INFO_ID	VARCHAR(36)
VULN_ID	VARCHAR(36)
VULN_INFO_TYPE	VARCHAR(36)
VULN_INFO_VALUE	VARCHAR(2000)
DATE_CREATED	DATETIME
DATE_MODIFIED	DATETIME
CREATED_BY	INT
MODIFIED_BY	INT

VULN_RPT_V

A tela faz referência à tabela VULN, que armazena informações sobre o sistema explorado. Cada scanner terá sua própria entrada para cada sistema.

Nome da coluna	Tipo de dados
VULN_ID	VARCHAR(36)
RSRC_ID	VARCHAR(36)
PORT_NAME	VARCHAR(64)
PORT_NUMBER	INT
NETWORK_PROTOCOL	INT
APPLICATION_PROTOCOL	VARCHAR(64)
ASSIGNED_VULN_SEVERITY	INT

Nome da coluna	Tipo de dados
COMPUTED_VULN_SEVERITY	INT
VULN_DESCRIPTION	CLOB
VULN_SOLUTION	CLOB
VULN_SUMMARY	VARCHAR(1000)
BEGIN_EFFECTIVE_DATE	DATETIME
END_EFFECTIVE_DATE	DATETIME
DETECTED_OS	VARCHAR(64)
DETECTED_OS_VERSION	VARCHAR(64)
SCANNED_APP	VARCHAR(64)
SCANNED_APP_VERSION	VARCHAR(64)
VULN_USER_NAME	VARCHAR(64)
VULN_USER_DOMAIN	VARCHAR(64)
VULN_TAXONOMY	VARCHAR(1000)
SCANNER_CLASSIFICATION	VARCHAR(255)
VULN_NAME	VARCHAR(300)
VULN_MODULE	VARCHAR(64)
DATE_CREATED	DATETIME
DATE_MODIFIED	DATETIME
CREATED_BY	INT
MODIFIED_BY	INT

VULN_RSRC_RPT_V

A tela faz referência à tabela VULN_RSRC, que armazena cada recurso explorado de uma determinada exploração.

Nome da coluna	Tipo de dados
RSRC_ID	VARCHAR(36)
SCANNER_ID	VARCHAR(36)
IP	VARCHAR(32)
HOST_NAME	VARCHAR(255)
LOCATION	VARCHAR(128)
DEPARTMENT	VARCHAR(128)
BUSINESS_SYSTEM	VARCHAR(128)
OPERATIONAL_ENVIRONMENT	VARCHAR(64)
CRITICALITY	INT
REGULATION	VARCHAR(128)
REGULATION_RATING	VARCHAR(64)
DATE_CREATED	DATETIME
DATE_MODIFIED	DATETIME
CREATED_BY	INT
MODIFIED_BY	INT

VULN_RSRC_SCAN_RPT_V

A tela faz referência à tabela VULN_RSRC_SCAN, que armazena cada recurso explorado de uma determinada exploração.

Nome da coluna	Tipo de dados
RSRC_ID	VARCHAR(36)
SCAN_ID	VARCHAR(36)
DATE_CREATED	DATETIME
DATE_MODIFIED	DATETIME
CREATED_BY	INT
MODIFIED_BY	INT

VULN_SCAN_RPT_V

A tela faz referência à tabela que armazena informações referentes a explorações.

Nome da coluna	Tipo de dados
SCAN_ID	VARCHAR(36)
SCANNER_ID	VARCHAR(36)
SCAN_TYPE	VARCHAR(10)
SCAN_START_DATE	DATETIME
SCAN_END_DATE	DATETIME
CONSOLIDATION_SERVER	VARCHAR(64)
DATE_CREATED	DATETIME
DATE_MODIFIED	DATETIME
CREATED_BY	INT
MODIFIED_BY	INT

VULN_SCAN_VULN_RPT_V

A tela faz referência à tabela VULN_SCAN_VULN, que armazena vulnerabilidades detectadas durante explorações.

Nome da coluna	Tipo de dados
SCAN_ID	VARCHAR(36)
VULN_ID	VARCHAR(36)
DATE_CREATED	DATETIME
DATE_MODIFIED	DATETIME
CREATED_BY	INT
MODIFIED_BY	INT

VULN_SCANNER_RPT_V

A tela faz referência à tabela VULN_SCANNER, que armazena informações sobre scanners de vulnerabilidades.

Nome da coluna	Tipo de dados
SCANNER_ID	VARCHAR(36)
PRODUCT_NAME	VARCHAR(100)
PRODUCT_VERSION	VARCHAR(64)
SCANNER_TYPE	VARCHAR(64)

Nome da coluna	Tipo de dados
VENDOR	VARCHAR(100)
SCANNER_INSTANCE	VARCHAR(64)
DATE_CREATED	DATETIME
DATE_MODIFIED	DATETIME
CREATED_BY	INT
MODIFIED_BY	INT

A Lista de verificação de solução de problemas do Sentinel

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

Esta lista de verificação é fornecida para ajudar no diagnóstico de problemas. Preencher a lista de verificação ajuda a resolver com mais rapidez a maioria dos problemas comuns. Os problemas que exigirem mais tempo para serem resolvidos já terão as informações de diagnóstico coletadas, eliminando o trabalho de diagnóstico redundante.

Item da lista de verificação	**Informações**	**Exemplo**
Versão da Novell:		v5.1.3
Plataforma Novell e versão do SO:		Win2003 Server sp1
Plataforma do banco de dados e versão do SO:		MS SQL 2000 sp3a
Configuração de hardware do Sentinel Server ▪ Processador ▪ Memória ▪ Outros		5 GB RAM 4 CPU 3.0 GHz
Configuração de hardware do servidor do banco de dados ▪ Processador ▪ Memória ▪ Outro (se Caixa separada)		8 GB RAM 4 CPU 3.0 GHz
Configuração de armazenamento do banco de dados (NAS, SAN, Local etc.		Local, com backup remoto
SO e configuração do servidor de relatórios (Crystal Server)		Crystal XI Win2003 Server sp1 Autenticação de janela

NOTA: Dependendo de como o seu sistema Sentinel está configurado (distribuído), talvez seja necessário ampliar a tabela acima. Por exemplo, informações adicionais podem ser necessárias para o DAS, o Consultor, o Sentinel Control Center, o Construtor de Coletores e para a camada de comunicação.

1. Verifique o portal do suporte técnico para obter informações sobre o seu problema em particular:
   - Ele é um problema conhecido com solução?
   - Esse problema foi resolvido na última versão de patch ou hot-fix?
   - A solução desse problema está atualmente programada para uma versão futura?
2. Determine a natureza do problema.
   - Ele pode ser reproduzido? É possível enumerar as etapas para reproduzir o problema?
   - Qual ação do usuário, se houver, causará o problema?
   - Esse problema é periódico por natureza?
3. Determine a gravidade desse problema.
   - O sistema ainda pode ser usado?
4. Entenda o ambiente e os sistemas envolvidos.
   - Quais plataformas e versões de produto estão envolvidas?
   - Existe algum componente fora do padrão ou personalizado envolvido?
   - É um ambiente com alta taxa de eventos?
   - Qual é a taxa de eventos sendo coletada?
   - Qual é a taxa de inserção de eventos no banco de dados?
   - Quantos usuários simultâneos existem?
   - São usados relatórios Crystal Reports? Quando os relatórios são executados?
   - É usada a correlação? Quantas regras são distribuídas?

   Arquivos de configuração de coleta, arquivos de registro e informações do sistema. Reúna essas informações para possível transferência futura de conhecimento. Para obter informações sobre a localização dos arquivos de registro, consulte o Guia de Instalação do Sentinel – Capítulo 2 – As melhores práticas.
5. Verifique a saúde do sistema.
   - Você pode se conectar ao Console do Sentinel?
   - Os eventos estão sendo gerados e inseridos no banco de dados? (se ainda estiver configurado, execute SendOneEvent e procure os eventos)
   - Os eventos podem ser vistos no console do Sentinel?
   - Os eventos podem ser recuperados do banco de dados usando a consulta rápida?
   - Verifique o uso da RAM e da CPU, o espaço em disco, a atividade do processo e a conectividade de rede dos hosts envolvidos.
   - Verifique se todos os processos esperados do Sentinel estão sendo executados. Scripts como o hp_checkprocess no Solaris listarão nossos processos e seus status. O gerenciador de tarefas da Microsoft pode ser usado em um ambiente Windows.
   - Verifique os dumps de memória em qualquer um dos subdiretórios do ESEC_HOME. Descubra qual processo realizou dump de memória. (cd $ESEC_HOME, find . –name core –print)

- Verifique o acesso de rede sqlplus. Verifique as tabelas.
- Verifique se o controlador Sonic está em execução. A conectividade pode ser verificada utilizando-se o console de gerenciamento do Sonic. Verifique se todas as várias conexões estão ativas para os processos da Novell. Certifique-se de que o arquivo de bloqueio não esteja impedindo a inicialização do Sonic. Opcionalmente, faça telnet com aquele servidor na porta do sonic (ex.: telnet sentinel.company.com 10012)
- Verifique se o watchdog está em execução no servidor. (ps –ef | grep watchdog)
- Verifique se os processos do Assistente estão funcionando. O Gerenciador do Coletor está em execução? O Gerenciador do Coletor aparece ativo no Construtor de Coletor ou no Console do Sentinel? Os Coletores estão em execução? Quantos por máquina? Quais conectores estão sendo usados (arquivo, processo, registro do sistema, firewall, registro de evento, etc.)? Qual o consumo de recursos do SO deles?

6. Existe algum problema com o banco de dados?
   - Com o sqlplus, você consegue se conectar ao banco de dados?
   - O banco de dados permite a conexão sqlplus utilizando a conta dba da Novell no esquema ESEV?
     - A pesquisa em uma das tabelas foi realizada com êxito?
   - Uma declaração selecionar em uma tabela de banco de dados foi realizada com êxito?
   - Verifique os drivers JDBC, sua localização e configurações de caminho
   - de classe.
   - No caso da Oracle, o Particionamento foi instalado (digite "select * from v$version;") e usado?
   - O banco de dados está sendo mantido por um administrador? Por alguém?
   - O banco de dados foi modificado pelo administrador?
   - O SDM está sendo usado para manter as partições e arquivar/apagar as partições para criar mais espaço no banco de dados?
   - Utilizando o SDM, qual é a partição atual? É o PMAX?
7. Verifique se as configurações de ambiente de produto estão corretas.
   - Verifique o equilíbrio dos scripts de shell de conexão de usuário, as variáveis de ambiente, configurações, configurações pessoais Java.
   - O conjunto de variáveis de ambiente executam o jvm correto?
   - Verifique as permissões apropriadas nas pastas para o produto instalado.
   - Verifique se alguma tarefa cron está configurada, causando interferência com a funcionalidade de nosso produto.
   - Se o produto estiver instalado em montagens NFS, verifique o equilíbrio das montagens NFS e dos serviços NFS/NIS.

8. Existe um possível vazamento de memória?
   - Obtenha as estatísticas sobre a rapidez de consumo da memória e por quais processos ela está sendo consumida.
   - Reúna as métricas dos eventos throughput por Coletor.
   - Execute o comando prstat no Solaris. Isso dará estatísticas de tempo de execução ao processo.
   - No Windows, você pode verificar o tamanho do processo e lidar com a contagem no gerenciador de tarefas.

   Esse problema, se não for resolvido, está agora preparado para expansão. Possíveis resultados da expansão:
   - Aperfeiçoamentos;
   - Hot fixes;
   - Soluções temporárias.

B Configurando a conta de conexão de serviço do Sentinel como NT AUTHORITY/ NetworkService

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

O propósito deste documento é descrever detalhadamente como configurar a conta de conexão do serviço do Sentinel como NT AUTHORITY\NetworkService, em vez da conta de usuário de Domínio. Foi provado que este processo funciona somente com a plataforma Windows 2003.

Um serviço deve efetuar logon com uma conta para acessar recursos e objetos no sistema operacional. Se você selecionar uma conta que não tenha permissão de logon como um serviço, o snap-in de serviços concederá automaticamente àquela conta os direitos de usuário que são necessários para a conexão como um serviço no computador que você estiver gerenciando. Isso não garante, porém, que o serviço será iniciado. É recomendado que as contas do usuário usadas para conexão como serviço tenham a caixa de seleção **Senha nunca expira** marcada em suas caixas de diálogo de propriedades e que possuam senhas avançadas. Se a política de bloqueio de conta estiver habilitada e a conta estiver bloqueada, o serviço não funcionará corretamente.

A tabela a seguir descreve as contas de conexão de serviço e como elas são usadas.

Conta de conexão	Descrição
Conta de Sistema Local	A conta de Sistema Local é uma conta poderosa que tem acesso completo ao sistema, incluindo o serviço de diretório nos controladores de domínio. Se um serviço fizer a conexão na conta de Sistema Local em um controlador de domínio, tal serviço terá acesso a todo o domínio. Alguns serviços são configurados por padrão para fazer a conexão na conta de Sistema Local. Não mude a configuração padrão de serviço. A conta de Sistema Local é uma conta local predefinida, usada para iniciar um serviço e fornecer o contexto de segurança para tal serviço. O nome da conta é NT AUTHORITY\System. Essa conta não tem uma senha e qualquer informação de senha fornecida por você será ignorada. A conta de Sistema Local é uma conta que tem acesso completo ao sistema, incluindo o serviço de diretório nos controladores de domínio. Como a conta de Sistema Local funciona como um computador na rede, ela tem acesso a recursos de rede.

Conta de conexão	Descrição
Conta de Serviço Local	A conta de Serviço Local é uma conta embutida especial, semelhante a uma conta de usuário autenticada. A conta de Serviço Local tem o mesmo nível de acesso aos recursos e objetos que os membros do grupo Usuários. Esse acesso limitado ajuda a proteger o seu sistema se serviços ou processos individuais forem aceitos. Os serviços executados como a conta de Serviço Local acessam recursos da rede, como uma sessão nula, sem credenciais. A conta de Serviço Local é uma conta local predefinida, usada para iniciar um serviço e fornecer o contexto de segurança para tal serviço. O nome da conta é NT AUTHORITY\LocalService. A conta de Serviço Local tem acesso limitado ao computador local e acesso Anônimo aos recursos de rede.
Conta de Serviço de Rede	A conta de Serviço de Rede é uma conta especial, embutida, semelhante a uma conta de usuário autenticada. A conta de Serviço de Rede tem o mesmo nível de acesso aos recursos e objetos que os membros do grupo Usuários. Esse acesso limitado ajuda a proteger o seu sistema se serviços ou processos individuais forem aceitos. Os serviços executados como a conta de Serviço de Rede acessam recursos da rede usando as credenciais da conta do computador. A conta de Serviço de Rede é uma conta local predefinida, usada para iniciar um serviço e fornecer o contexto de segurança para tal serviço. O nome da conta é NT AUTHORITY\NetworkService. A conta de Serviço de Rede tem acesso limitado ao computador local e acesso autenticado (como a conta do computador) aos recursos de rede.

A execução de um serviço no contexto de uma conta de conexão de usuário tem as seguintes desvantagens:

1. A conta deve ser criada antes que o serviço possa ser executado. Se o programa de configuração para o serviço criar a conta, a Configuração deverá ser executada de uma conta com credenciais administrativas suficientes para criar contas no serviço de diretório.
2. Os nomes e as senhas de contas de serviço são armazenados nos computadores nos quais o serviço é instalado. Se a senha de uma conta de serviço em um computador for mudada ou expirar, o serviço não poderá ser iniciado naquele computador até que a senha seja definida para a nova senha daquele serviço. A recomendação é usar o Serviço Local e o Serviço de Rede em vez de usar uma conta que exija senha: isso simplifica o gerenciamento de senhas
3. Se a conta de serviço for renomeada, bloqueada, desabilitada ou apagada, o serviço não poderá ser iniciado naquele computador até que a conta seja redefinida.

Devido às desvantagens descritas acima, a Novell tentou executar o serviço do Sentinel sob uma conta NT AUTHORITY\NetworkService. A conta NT AUTHORITY\LocalService não possui privilégios suficientes para esse propósito, já que os processos do DAS precisam se comunicar com o servidor do banco de dados na rede.

Para configurar o NT AUTHORITY\NetworkService como a conta de conexão de serviço do Sentinel

Para configurar o NT AUTHORITY\NetworkService como a conta de conexão de serviço do Sentinel, você terá que executar as seguintes etapas:

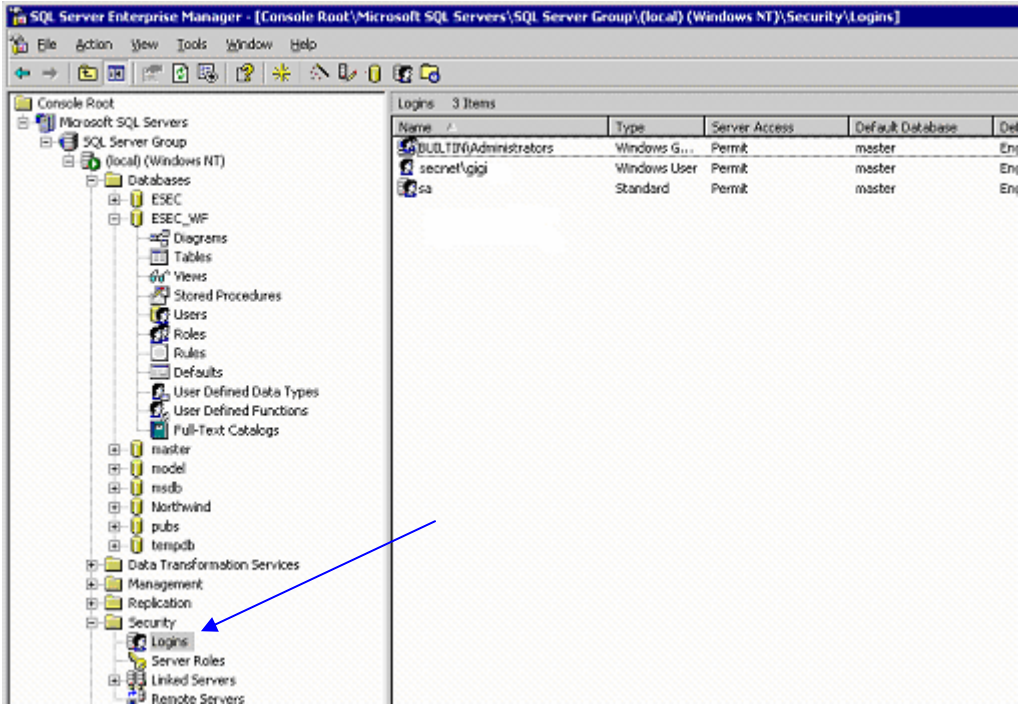
- Adicionar a máquina que executa o Serviço do Sentinel como uma conta de conexão para as instâncias de banco de dados ESEC e ESEC_WF (executada na máquina do banco de dados)
- Mudar a conta de conexão para o serviço do Sentinel para NT AUTHORITY\NetworkService (executado na máquina remota)
- Configurar a inicialização do eSecurity (executada na máquina remota)

Adicionando o Serviço do Sentinel como uma conta de conexão a instâncias ESEC e ESEC_WF DB

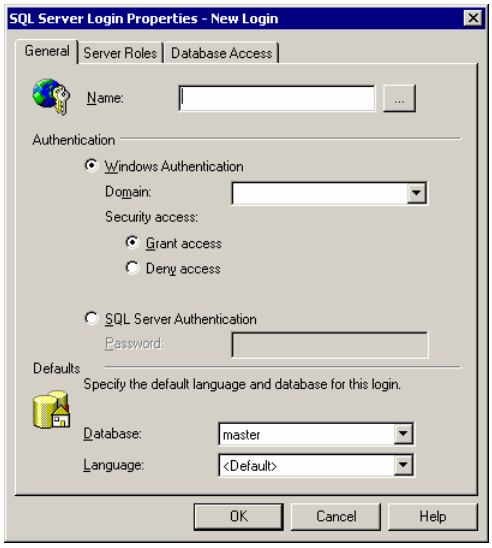
Adicionando uma conexão de uma máquina remota ao servidor de banco de dados

NOTA: Como exemplo, apresentamos a seguir as etapas para adicionar secnet\case1 como uma conexão ao servidor de banco de dados.

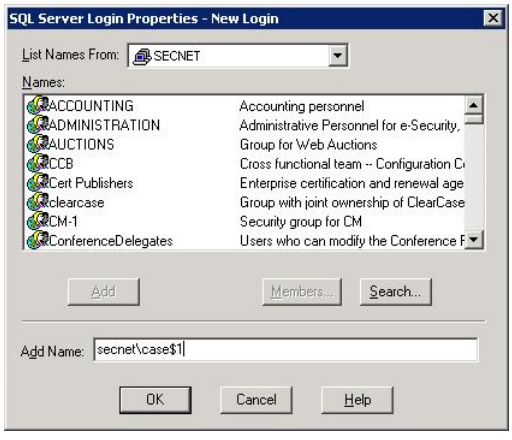
1. Em sua máquina de banco de dados, abra o SQL Server Enterprise Manager. No painel de navegação, em SQL Server Group (Grupo de Servidor SQL), expanda a pasta Security (Segurança) e realce Logins (Conexões).



2. Clique o botão direito do mouse em *Logins* > *New login*... (Novo Login...)

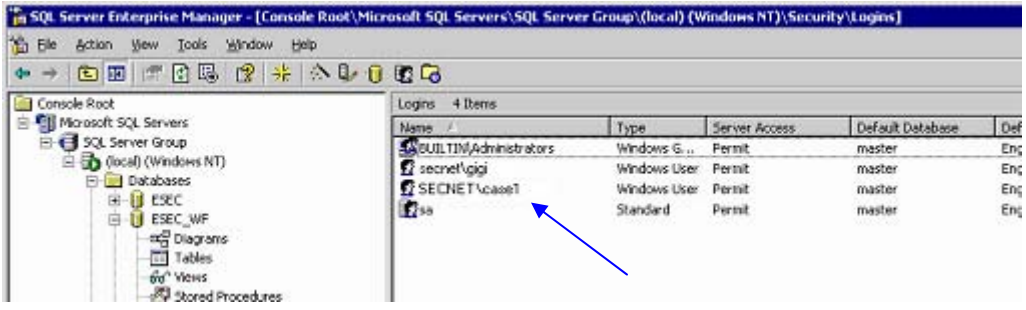


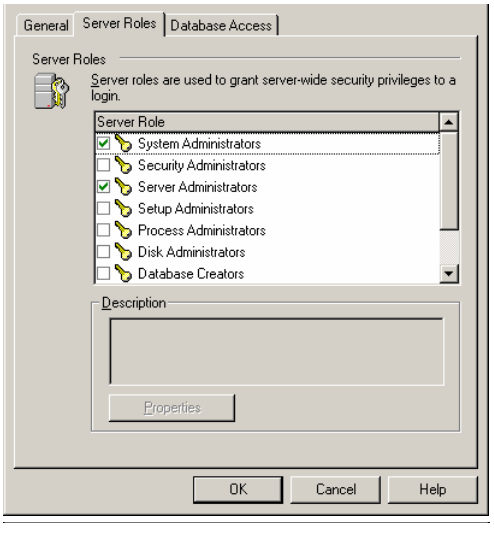
3. Clique no botão procurar pelo campo Name (Nome) e a seguinte tela será mostrada.

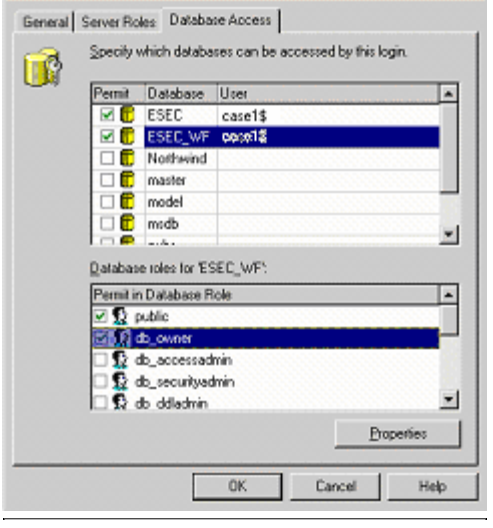


No campo Add Name (Adicionar Nome), digite um nome de domínio e um nome de usuário (secnet\case1$ é fornecido como exemplo). Esta é a máquina <nome de domínio>\<nome da máquina>$ que você está adicionando como uma conexão para o servidor de banco de dados. Clique em *OK*.

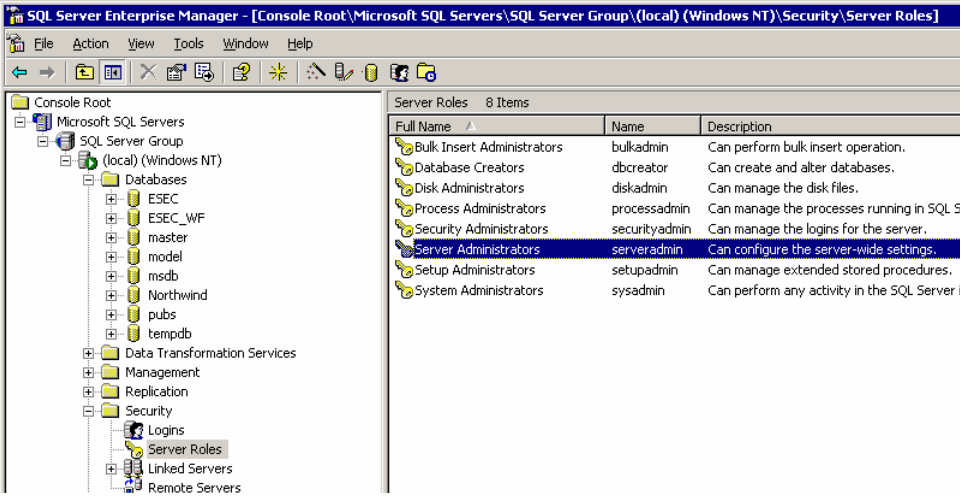
4. Clique o botão direito do mouse em Propriedades no nome (a máquina <nome de domínio>\<nome da máquina>$ que você está adicionando como uma conexão ao servidor de banco de dados) para mudar as funções do servidor e o acesso ao banco de dados. Selecione System Administrators (Administradores do Sistema) e Server Administrators (Administradores do Servidor) como as Funções do Servidor. Selecione o acesso ao ESEC como 'public' e 'db_owner'. Selecione o acesso ao ESEC_WF como 'public' e 'db_owner'.

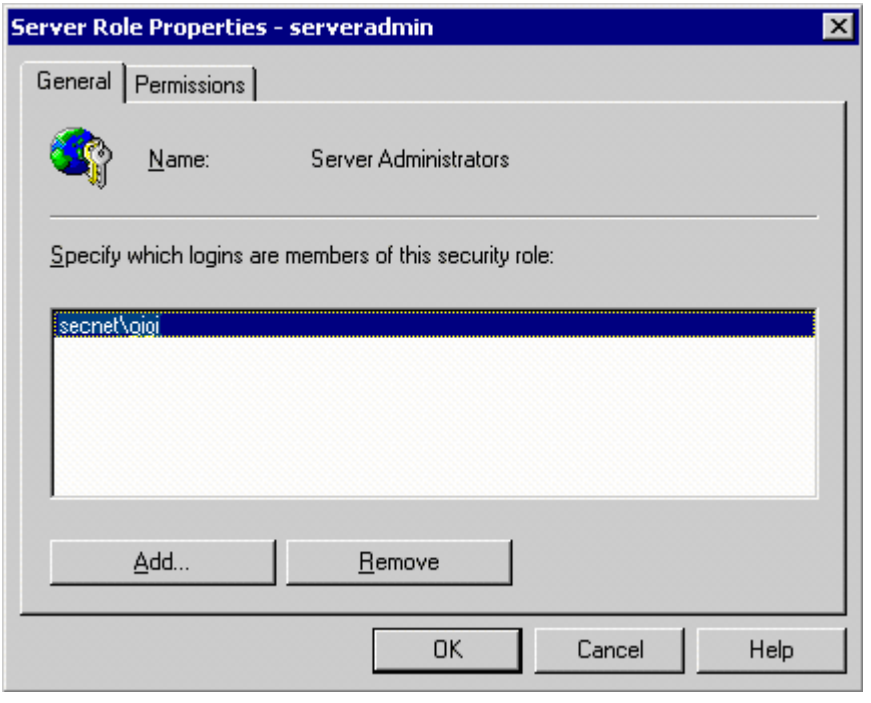




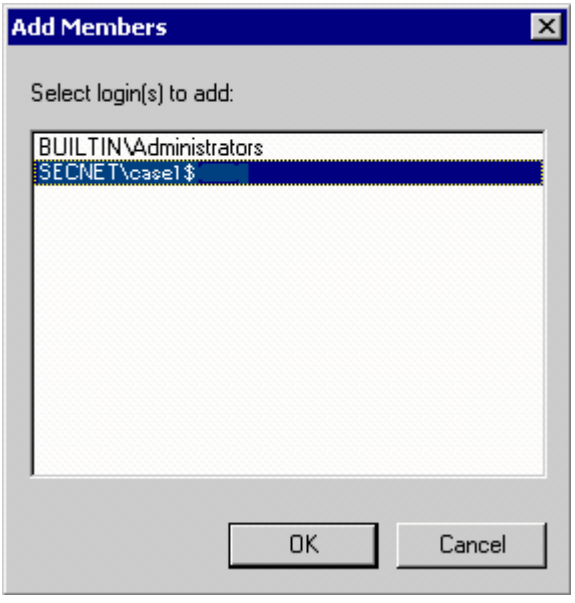


5. Em Server Roles (Funções do Servidor), realce Server Administrators (Administradores do Servidor), clique o botão direito do mouse em > *Properties* (Propriedades).





6. Clique no botão *Adicionar*.

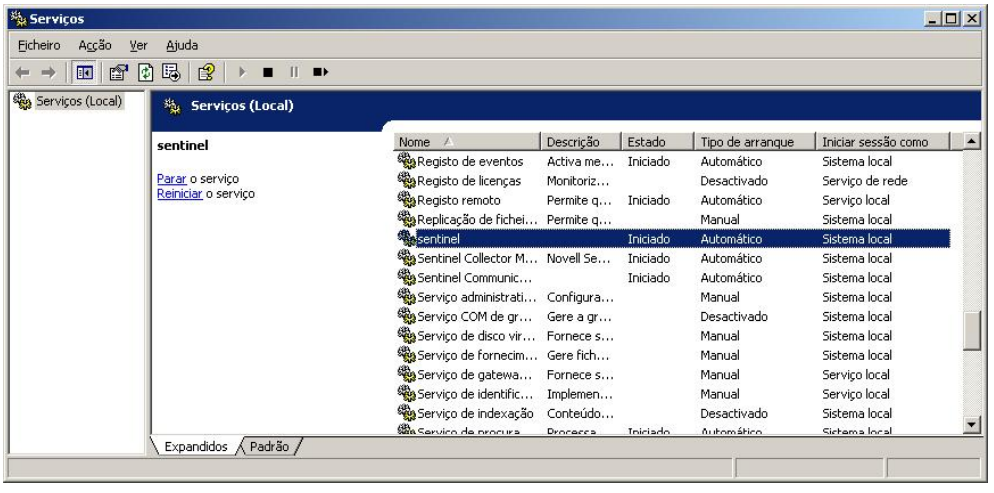


Clique em OK, Secnet\case1$ é adicionado.

Mudando a conta de conexão do serviço do Sentinel para NT AUTHORITY\NetworkService

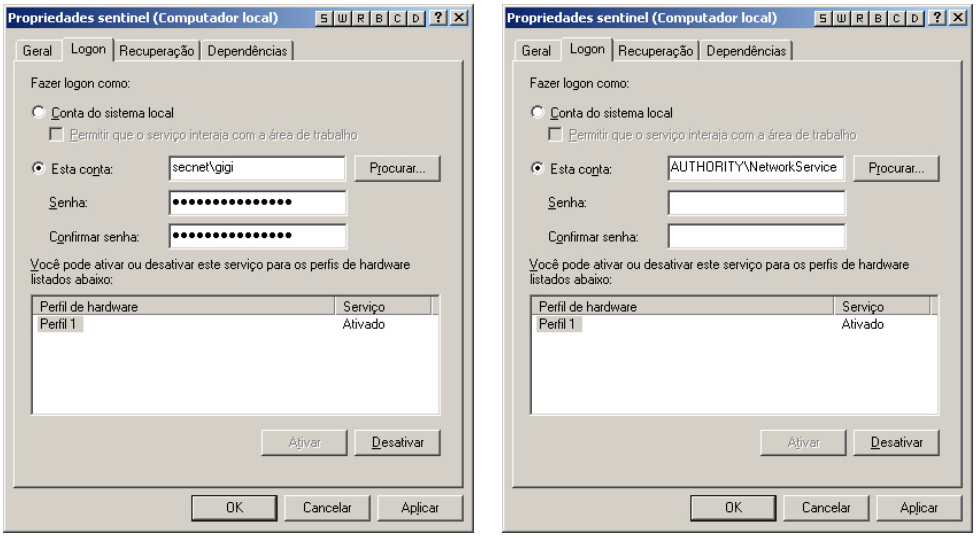
Mudando a conexão do Serviço do Sentinel para NT AUTHORITY\NetworkService

1. Na máquina remota onde estiver se conectando ao banco de dados, clique em *Iniciar* > *Programas* > *Ferramentas Administrativas*> *Serviços*.

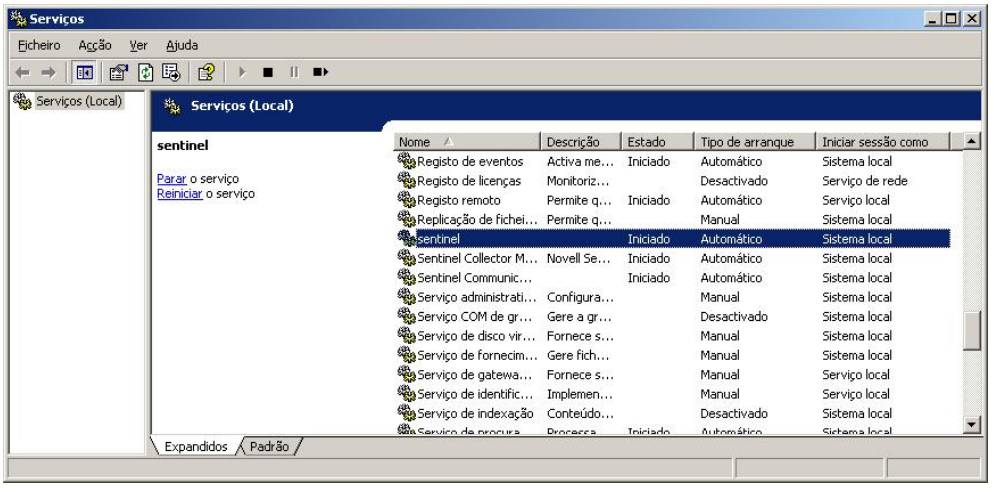


2. Pare o serviço do Sentinel, clique o botão direito do mouse em > *propriedades* > guia *Logon*.

3. Clique em 'Esta conta' e no campo digite 'NT AUTHORITY\NetworkService'. Limpe os campos 'Senha' e 'Confirmar senha'.



Clique em *OK*. A janela Serviços para o Serviço do Sentinel deve indicar 'Serviço de Rede' na coluna 'Fazer Logon Como'.



Configurando o Serviço do Sentinel para iniciar com êxito.

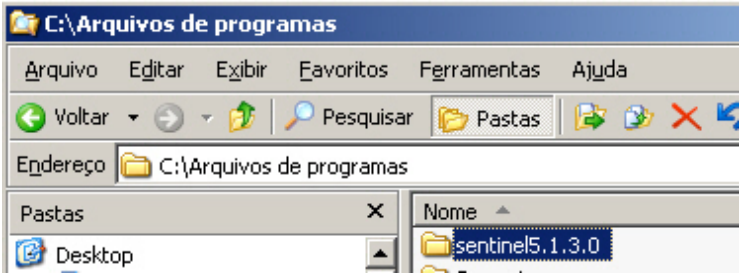
Para que o Serviço do Sentinel inicie com êxito, a conta NT AUTHORITY\NetworkService deve ter permissão de gravação para %ESEC_HOME%. De acordo com a documentação da Microsoft, a conta Serviço de Rede tem os seguintes privilégios:

- SE_AUDIT_NAME
- SE_CHANGE_NOTIFY_NAME
- SE_UNDOCK_NAME
- Quaisquer privilégios designados a usuários e a usuários autenticados

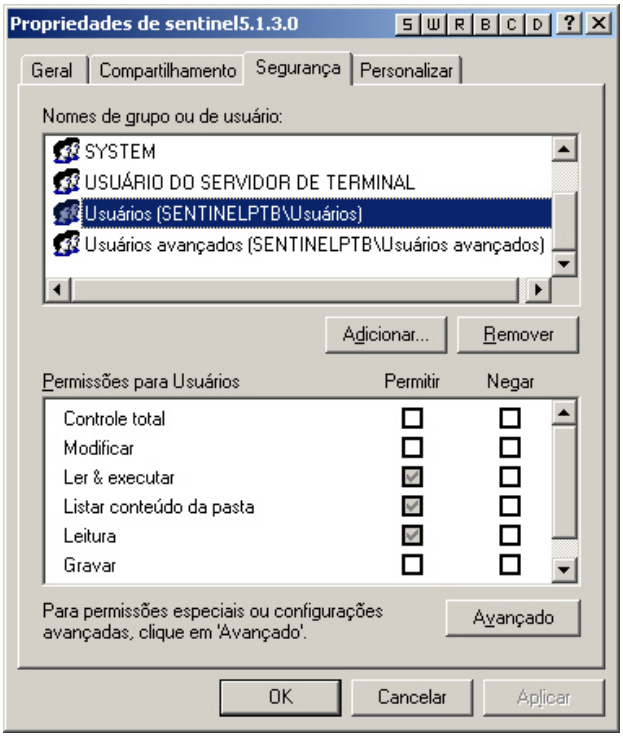
Você terá que conceder ao grupo Usuários acesso de gravação em %ESEC_HOME%.

Configurando o Serviço do Sentinel para iniciar com êxito

1. Abra o Explorer do Windows e navegue para %ESEC_HOME%.
2. Clique o botão direito do mouse na pasta pai (normalmente chamada sentinel5.1.3) > *Propriedades* > guia *Segurança*.



3. Realce o grupo Usuários. Conceda permissão ler&executar, conteúdo de pasta de lista, leitura e gravação.



Clique em *OK*.

4. Na janela Serviços, reinicie o serviço do Sentinel.

C Usuários, funções e permissões de acesso de banco de dados do Sentinel

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

O propósito deste documento é fornecer uma explicação detalhada dos usuários, das funções e suas permissões de acesso do banco de dados do Sentinel.

Instância do banco de dados do Sentinel

ESEC

Usuários:

- esecadm
- esecapp
- esecdba
- esecrpt
- outros usuários

NOTA: Os usuários acima são criados pelo Gerenciador do Usuário. Consulte a seção Usuários de banco de dados do Sentinel para obter permissões de acesso detalhadas.

Funções:

- ESEC_APP – A mesma permissão de db_owner
- ESEC_ETL – Essa função não está atualmente em uso, ela está reservada para atualização futura. Consulte a seção Funções do banco de dados do Sentinel para obter permissões de acesso detalhadas.
- ESEC_USER – Consulte a seção Funções do banco de dados do Sentinel para obter permissões de acesso detalhadas.

ESEC_WF

- Usuários: esecapp – Consulte a seção Funções do banco de dados do Sentinel para obter permissões de acesso detalhadas.
- Funções: ESEC_APP – Consulte a seção Funções do banco de dados do Sentinel para obter permissões de acesso detalhadas.

Usuários do banco de dados do Sentinel

Resumo

Nome do usuário	Nome do grupo	Nome de login	Nome do BD padrão
esecadm	ESEC_USER	esecadm	ESEC
esecapp	ESEC_APP	esecapp	ESEC
esecapp	ESEC_ETL	esecapp	ESEC

esecdba	db_owner	esecdba	ESEC
esecrpt	ESEC_USER	esecrpt	ESEC

esecadm

Nome de login	Nome do BD	Nome do usuário	Usuário do álias
esecadm	ESEC	ESEC_USER	MembroDe
esecadm	ESEC	esecadm	Usuário

esecapp

Nome de login	Nome do BD	Nome do usuário	Usuário do álias
esecapp	ESEC	ESEC_APP	MembroDe
esecapp	ESEC	ESEC_ETL	MembroDe
esecapp	ESEC	esecapp	Usuário
esecapp	ESEC_WF	ESEC_APP	MembroDe
esecapp	ESEC_WF	esecapp	Usuário

esecdba

Nome de login	Nome do BD	Nome do usuário	Usuário do álias
esecdba	ESEC	db_owner	MembroDe
esecdba	ESEC	esecdba	Usuário

esecrpt

Nome de login	Nome do BD	Nome do usuário	Usuário do álias
esecrpt	ESEC	ESEC_USER	MembroDe
esecrpt	ESEC	esecrpt	Usuário

Funções do banco de dados do Sentinel

Resumo

- ESEC_APP – É uma função de banco de dados para ESEC e ESEC_WF. Ela tem a mesma permissão de db_owner para a instância ESEC. Consulte a seção ESEC_APP para obter detalhes sobre permissões.
- ESEC_ETL – É uma função de banco de dados para instância ESEC. Essa função não está atualmente em uso e está reservada para desenvolvimento futuro. Consulte a seção Funções do banco de dados do Sentinel para obter permissões de acesso detalhadas.
- ESEC_USER – Uma função para instância ESEC. Consulte a seção Funções do banco de dados do Sentinel para obter permissões de acesso detalhadas.

ESEC_APP

Para a instância ESEC, a ESEC_APP tem a mesma permissão de db_owner. A função ESEC_APP realiza as mesmas atividades de todas as funções de banco de dados, assim como outras atividades de manutenção e configuração no banco de dados. As permissões dessa função segmentam todas as outras funções fixas de banco de dados.

Para a instância ESEC_WF, essa é a permissão para a função ESEC_APP.

Nome da função	Nome do objeto	Ação	Tipo
		193	Tabela de
ESEC_APP	Activities	SELECIONAR	Usuário U
			Tabela de
ESEC_APP	Activities	195 INSERIR	Usuário U
			Tabela de
ESEC_APP	Activities	196 APAGAR	Usuário U
		197	Tabela de
ESEC_APP	Activities	ATUALIZAR	Usuário U
		193	Tabela de
ESEC_APP	ActivityData	SELECIONAR	Usuário U
			Tabela de
ESEC_APP	ActivityData	195 INSERIR	Usuário U
			Tabela de
ESEC_APP	ActivityData	196 APAGAR	Usuário U
		197	Tabela de
ESEC_APP	ActivityData	ATUALIZAR	Usuário U
		193	Tabela de
ESEC_APP	ActivityStateEventAudits	SELECIONAR	Usuário U
			Tabela de
ESEC_APP	ActivityStateEventAudits	195 INSERIR	Usuário U
			Tabela de
ESEC_APP	ActivityStateEventAudits	196 APAGAR	Usuário U
		197	Tabela de
ESEC_APP	ActivityStateEventAudits	ATUALIZAR	Usuário U
		193	Tabela de
ESEC_APP	ActivityStates	SELECIONAR	Usuário U
			Tabela de
ESEC_APP	ActivityStates	195 INSERIR	Usuário U
			Tabela de
ESEC_APP	ActivityStates	196 APAGAR	Usuário U
		197	Tabela de
ESEC_APP	ActivityStates	ATUALIZAR	Usuário U
		193	Tabela de
ESEC_APP	AndJoinTable	SELECIONAR	Usuário U
			Tabela de
ESEC_APP	AndJoinTable	195 INSERIR	Usuário U
			Tabela de
ESEC_APP	AndJoinTable	196 APAGAR	Usuário U
		197	Tabela de
ESEC_APP	AndJoinTable	ATUALIZAR	Usuário U
		193	Tabela de
ESEC_APP	AssignmentEventAudits	SELECIONAR	Usuário U
			Tabela de
ESEC_APP	AssignmentEventAudits	195 INSERIR	Usuário U
			Tabela de
ESEC_APP	AssignmentEventAudits	196 APAGAR	Usuário U

Nome da função	Nome do objeto	Ação	Tipo
		197	Tabela de
ESEC_APP	AssignmentEventAudits	ATUALIZAR	Usuário U
		193	Tabela de
ESEC_APP	AssignmentsTable	SELECIONAR	Usuário U
			Tabela de
ESEC_APP	AssignmentsTable	195 INSERIR	Usuário U
			Tabela de
ESEC_APP	AssignmentsTable	196 APAGAR	Usuário U
		197	Tabela de
ESEC_APP	AssignmentsTable	ATUALIZAR	Usuário U
		193	Tabela de
ESEC_APP	Counters	SELECIONAR	Usuário U
			Tabela de
ESEC_APP	Counters	195 INSERIR	Usuário U
			Tabela de
ESEC_APP	Counters	196 APAGAR	Usuário U
		197	Tabela de
ESEC_APP	Counters	ATUALIZAR	Usuário U
		193	Tabela de
ESEC_APP	CreateProcessEventAudits	SELECIONAR	Usuário U
			Tabela de
ESEC_APP	CreateProcessEventAudits	195 INSERIR	Usuário U
			Tabela de
ESEC_APP	CreateProcessEventAudits	196 APAGAR	Usuário U
		197	Tabela de
ESEC_APP	CreateProcessEventAudits	ATUALIZAR	Usuário U
		193	Tabela de
ESEC_APP	DataEventAudits	SELECIONAR	Usuário U
			Tabela de
ESEC_APP	DataEventAudits	195 INSERIR	Usuário U
			Tabela de
ESEC_APP	DataEventAudits	196 APAGAR	Usuário U
		197	Tabela de
ESEC_APP	DataEventAudits	ATUALIZAR	Usuário U
		193	Tabela de
ESEC_APP	Deadlines	SELECIONAR	Usuário U
			Tabela de
ESEC_APP	Deadlines	195 INSERIR	Usuário U
			Tabela de
ESEC_APP	Deadlines	196 APAGAR	Usuário U
		197	Tabela de
ESEC_APP	Deadlines	ATUALIZAR	Usuário U
		193	Tabela de
ESEC_APP	EventTypes	SELECIONAR	Usuário U
			Tabela de
ESEC_APP	EventTypes	195 INSERIR	Usuário U
			Tabela de
ESEC_APP	EventTypes	196 APAGAR	Usuário U

Nome da função	Nome do objeto	Ação	Tipo
		197	Tabela de
ESEC_APP	EventTypes	ATUALIZAR	Usuário U
		193	Tabela de
ESEC_APP	GroupGroupTable	SELECIONAR	Usuário U
			Tabela de
ESEC_APP	GroupGroupTable	195 INSERIR	Usuário U
			Tabela de
ESEC_APP	GroupGroupTable	196 APAGAR	Usuário U
		197	Tabela de
ESEC_APP	GroupGroupTable	ATUALIZAR	Usuário U
		193	Tabela de
ESEC_APP	GroupTable	SELECIONAR	Usuário U
			Tabela de
ESEC_APP	GroupTable	195 INSERIR	Usuário U
			Tabela de
ESEC_APP	GroupTable	196 APAGAR	Usuário U
		197	Tabela de
ESEC_APP	GroupTable	ATUALIZAR	Usuário U
		193	Tabela de
ESEC_APP	GroupUser	SELECIONAR	Usuário U
			Tabela de
ESEC_APP	GroupUser	195 INSERIR	Usuário U
			Tabela de
ESEC_APP	GroupUser	196 APAGAR	Usuário U
		197	Tabela de
ESEC_APP	GroupUser	ATUALIZAR	Usuário U
		193	Tabela de
ESEC_APP	GroupUserPackLevelParticipant	SELECIONAR	Usuário U
			Tabela de
ESEC_APP	GroupUserPackLevelParticipant	195 INSERIR	Usuário U
			Tabela de
ESEC_APP	GroupUserPackLevelParticipant	196 APAGAR	Usuário U
		197	Tabela de
ESEC_APP	GroupUserPackLevelParticipant	ATUALIZAR	Usuário U
		193	Tabela de
ESEC_APP	GroupUserProcLevelParticipant	SELECIONAR	Usuário U
			Tabela de
ESEC_APP	GroupUserProcLevelParticipant	195 INSERIR	Usuário U
			Tabela de
ESEC_APP	GroupUserProcLevelParticipant	196 APAGAR	Usuário U
		197	Tabela de
ESEC_APP	GroupUserProcLevelParticipant	ATUALIZAR	Usuário U
		193	Tabela de
ESEC_APP	LockTable	SELECIONAR	Usuário U
			Tabela de
ESEC_APP	LockTable	195 INSERIR	Usuário U
			Tabela de
ESEC_APP	LockTable	196 APAGAR	Usuário U

Nome da função	Nome do objeto	Ação	Tipo
		197	Tabela de
ESEC_APP	LockTable	ATUALIZAR	Usuário U
		193	Tabela de
ESEC_APP	NewEventAuditData	SELECIONAR	Usuário U
			Tabela de
ESEC_APP	NewEventAuditData	195 INSERIR	Usuário U
			Tabela de
ESEC_APP	NewEventAuditData	196 APAGAR	Usuário U
		197	Tabela de
ESEC_APP	NewEventAuditData	ATUALIZAR	Usuário U
		193	Tabela de
ESEC_APP	NextXPDLVersions	SELECIONAR	Usuário U
			Tabela de
ESEC_APP	NextXPDLVersions	195 INSERIR	Usuário U
			Tabela de
ESEC_APP	NextXPDLVersions	196 APAGAR	Usuário U
		197	Tabela de
ESEC_APP	NextXPDLVersions	ATUALIZAR	Usuário U
		193	Tabela de
ESEC_APP	NormalUser	SELECIONAR	Usuário U
			Tabela de
ESEC_APP	NormalUser	195 INSERIR	Usuário U
			Tabela de
ESEC_APP	NormalUser	196 APAGAR	Usuário U
		197	Tabela de
ESEC_APP	NormalUser	ATUALIZAR	Usuário U
		193	Tabela de
ESEC_APP	ObjectId	SELECIONAR	Usuário U
			Tabela de
ESEC_APP	ObjectId	195 INSERIR	Usuário U
			Tabela de
ESEC_APP	ObjectId	196 APAGAR	Usuário U
		197	Tabela de
ESEC_APP	ObjectId	ATUALIZAR	Usuário U
		193	Tabela de
ESEC_APP	OldEventAuditData	SELECIONAR	Usuário U
			Tabela de
ESEC_APP	OldEventAuditData	195 INSERIR	Usuário U
			Tabela de
ESEC_APP	OldEventAuditData	196 APAGAR	Usuário U
		197	Tabela de
ESEC_APP	OldEventAuditData	ATUALIZAR	Usuário U
		193	Tabela de
ESEC_APP	PackLevelParticipant	SELECIONAR	Usuário U
			Tabela de
ESEC_APP	PackLevelParticipant	195 INSERIR	Usuário U
			Tabela de
ESEC_APP	PackLevelParticipant	196 APAGAR	Usuário U

Nome da função	Nome do objeto	Ação	Tipo
ESEC_APP	PackLevelParticipant	197 ATUALIZAR	Tabela de Usuário U
ESEC_APP	PackLevelXPDLApp	193 SELECIONAR	Tabela de Usuário U
ESEC_APP	PackLevelXPDLApp	195 INSERIR	Tabela de Usuário U
ESEC_APP	PackLevelXPDLApp	196 APAGAR	Tabela de Usuário U
ESEC_APP	PackLevelXPDLApp	197 ATUALIZAR	Tabela de Usuário U
ESEC_APP	PackLevelXPDLAppTAAppDetail	193 SELECIONAR	Tabela de Usuário U
ESEC_APP	PackLevelXPDLAppTAAppDetail	195 INSERIR	Tabela de Usuário U
ESEC_APP	PackLevelXPDLAppTAAppDetail	196 APAGAR	Tabela de Usuário U
ESEC_APP	PackLevelXPDLAppTAAppDetail	197 ATUALIZAR	Tabela de Usuário U
ESEC_APP	PackLevelXPDLAppTAAppDetailUsr	193 SELECIONAR	Tabela de Usuário U
ESEC_APP	PackLevelXPDLAppTAAppDetailUsr	195 INSERIR	Tabela de Usuário U
ESEC_APP	PackLevelXPDLAppTAAppDetailUsr	196 APAGAR	Tabela de Usuário U
ESEC_APP	PackLevelXPDLAppTAAppDetailUsr	197 ATUALIZAR	Tabela de Usuário U
ESEC_APP	PackLevelXPDLAppTAAppUser	193 SELECIONAR	Tabela de Usuário U
ESEC_APP	PackLevelXPDLAppTAAppUser	195 INSERIR	Tabela de Usuário U
ESEC_APP	PackLevelXPDLAppTAAppUser	196 APAGAR	Tabela de Usuário U
ESEC_APP	PackLevelXPDLAppTAAppUser	197 ATUALIZAR	Tabela de Usuário U
ESEC_APP	PackLevelXPDLAppToolAgentApp	193 SELECIONAR	Tabela de Usuário U
ESEC_APP	PackLevelXPDLAppToolAgentApp	195 INSERIR	Tabela de Usuário U
ESEC_APP	PackLevelXPDLAppToolAgentApp	196 APAGAR	Tabela de Usuário U
ESEC_APP	PackLevelXPDLAppToolAgentApp	197 ATUALIZAR	Tabela de Usuário U
ESEC_APP	ProcessData	193 SELECIONAR	Tabela de Usuário U
ESEC_APP	ProcessData	195 INSERIR	Tabela de Usuário U
ESEC_APP	ProcessData	196 APAGAR	Tabela de Usuário U

Nome da função	Nome do objeto	Ação	Tipo
ESEC_APP	ProcessData	197 ATUALIZAR	Tabela de Usuário U
ESEC_APP	ProcessDefinitions	193 SELECIONAR	Tabela de Usuário U
ESEC_APP	ProcessDefinitions	195 INSERIR	Tabela de Usuário U
ESEC_APP	ProcessDefinitions	196 APAGAR	Tabela de Usuário U
ESEC_APP	ProcessDefinitions	197 ATUALIZAR	Tabela de Usuário U
ESEC_APP	Processos	193 SELECIONAR	Tabela de Usuário U
ESEC_APP	Processos	195 INSERIR	Tabela de Usuário U
ESEC_APP	Processos	196 APAGAR	Tabela de Usuário U
ESEC_APP	Processos	197 ATUALIZAR	Tabela de Usuário U
ESEC_APP	ProcessRequesters	193 SELECIONAR	Tabela de Usuário U
ESEC_APP	ProcessRequesters	195 INSERIR	Tabela de Usuário U
ESEC_APP	ProcessRequesters	196 APAGAR	Tabela de Usuário U
ESEC_APP	ProcessRequesters	197 ATUALIZAR	Tabela de Usuário U
ESEC_APP	ProcessStateEventAudits	193 SELECIONAR	Tabela de Usuário U
ESEC_APP	ProcessStateEventAudits	195 INSERIR	Tabela de Usuário U
ESEC_APP	ProcessStateEventAudits	196 APAGAR	Tabela de Usuário U
ESEC_APP	ProcessStateEventAudits	197 ATUALIZAR	Tabela de Usuário U
ESEC_APP	ProcessStates	193 SELECIONAR	Tabela de Usuário U
ESEC_APP	ProcessStates	195 INSERIR	Tabela de Usuário U
ESEC_APP	ProcessStates	196 APAGAR	Tabela de Usuário U
ESEC_APP	ProcessStates	197 ATUALIZAR	Tabela de Usuário U
ESEC_APP	ProcLevelParticipant	193 SELECIONAR	Tabela de Usuário U
ESEC_APP	ProcLevelParticipant	195 INSERIR	Tabela de Usuário U
ESEC_APP	ProcLevelParticipant	196 APAGAR	Tabela de Usuário U

Nome da função	Nome do objeto	Ação	Tipo
		197	Tabela de
ESEC_APP	ProcLevelParticipant	ATUALIZAR	Usuário U
		193	Tabela de
ESEC_APP	ProcLevelXPDLApp	SELECIONAR	Usuário U
			Tabela de
ESEC_APP	ProcLevelXPDLApp	195 INSERIR	Usuário U
			Tabela de
ESEC_APP	ProcLevelXPDLApp	196 APAGAR	Usuário U
		197	Tabela de
ESEC_APP	ProcLevelXPDLApp	ATUALIZAR	Usuário U
		193	Tabela de
ESEC_APP	ProcLevelXPDLAppTAAppDetail	SELECIONAR	Usuário U
			Tabela de
ESEC_APP	ProcLevelXPDLAppTAAppDetail	195 INSERIR	Usuário U
			Tabela de
ESEC_APP	ProcLevelXPDLAppTAAppDetail	196 APAGAR	Usuário U
		197	Tabela de
ESEC_APP	ProcLevelXPDLAppTAAppDetail	ATUALIZAR	Usuário U
		193	Tabela de
ESEC_APP	ProcLevelXPDLAppTAAppDetailUsr	SELECIONAR	Usuário U
			Tabela de
ESEC_APP	ProcLevelXPDLAppTAAppDetailUsr	195 INSERIR	Usuário U
			Tabela de
ESEC_APP	ProcLevelXPDLAppTAAppDetailUsr	196 APAGAR	Usuário U
		197	Tabela de
ESEC_APP	ProcLevelXPDLAppTAAppDetailUsr	ATUALIZAR	Usuário U
		193	Tabela de
ESEC_APP	ProcLevelXPDLAppTAAppUser	SELECIONAR	Usuário U
			Tabela de
ESEC_APP	ProcLevelXPDLAppTAAppUser	195 INSERIR	Usuário U
			Tabela de
ESEC_APP	ProcLevelXPDLAppTAAppUser	196 APAGAR	Usuário U
		197	Tabela de
ESEC_APP	ProcLevelXPDLAppTAAppUser	ATUALIZAR	Usuário U
		193	Tabela de
ESEC_APP	ProcLevelXPDLAppToolAgentApp	SELECIONAR	Usuário U
			Tabela de
ESEC_APP	ProcLevelXPDLAppToolAgentApp	195 INSERIR	Usuário U
			Tabela de
ESEC_APP	ProcLevelXPDLAppToolAgentApp	196 APAGAR	Usuário U
		197	Tabela de
ESEC_APP	ProcLevelXPDLAppToolAgentApp	ATUALIZAR	Usuário U
		193	Tabela de
ESEC_APP	ResourcesTable	SELECIONAR	Usuário U
			Tabela de
ESEC_APP	ResourcesTable	195 INSERIR	Usuário U
			Tabela de
ESEC_APP	ResourcesTable	196 APAGAR	Usuário U

Nome da função	Nome do objeto	Ação	Tipo
ESEC_APP	ResourcesTable	197 ATUALIZAR	Tabela de Usuário U
ESEC_APP	StateEventAudits	193 SELECIONAR	Tabela de Usuário U
ESEC_APP	StateEventAudits	195 INSERIR	Tabela de Usuário U
ESEC_APP	StateEventAudits	196 APAGAR	Tabela de Usuário U
ESEC_APP	StateEventAudits	197 ATUALIZAR	Tabela de Usuário U
ESEC_APP	ToolAgentApp	193 SELECIONAR	Tabela de Usuário U
ESEC_APP	ToolAgentApp	195 INSERIR	Tabela de Usuário U
ESEC_APP	ToolAgentApp	196 APAGAR	Tabela de Usuário U
ESEC_APP	ToolAgentApp	197 ATUALIZAR	Tabela de Usuário U
ESEC_APP	ToolAgentAppDetail	193 SELECIONAR	Tabela de Usuário U
ESEC_APP	ToolAgentAppDetail	195 INSERIR	Tabela de Usuário U
ESEC_APP	ToolAgentAppDetail	196 APAGAR	Tabela de Usuário U
ESEC_APP	ToolAgentAppDetail	197 ATUALIZAR	Tabela de Usuário U
ESEC_APP	ToolAgentAppDetailUser	193 SELECIONAR	Tabela de Usuário U
ESEC_APP	ToolAgentAppDetailUser	195 INSERIR	Tabela de Usuário U
ESEC_APP	ToolAgentAppDetailUser	196 APAGAR	Tabela de Usuário U
ESEC_APP	ToolAgentAppDetailUser	197 ATUALIZAR	Tabela de Usuário U
ESEC_APP	ToolAgentAppUser	193 SELECIONAR	Tabela de Usuário U
ESEC_APP	ToolAgentAppUser	195 INSERIR	Tabela de Usuário U
ESEC_APP	ToolAgentAppUser	196 APAGAR	Tabela de Usuário U
ESEC_APP	ToolAgentAppUser	197 ATUALIZAR	Tabela de Usuário U
ESEC_APP	ToolAgentUser	193 SELECIONAR	Tabela de Usuário U
ESEC_APP	ToolAgentUser	195 INSERIR	Tabela de Usuário U
ESEC_APP	ToolAgentUser	196 APAGAR	Tabela de Usuário U

Nome da função	Nome do objeto	Ação	Tipo
		197	Tabela de
ESEC_APP	ToolAgentUser	ATUALIZAR	Usuário U
		193	Tabela de
ESEC_APP	UserGroupTable	SELECIONAR	Usuário U
			Tabela de
ESEC_APP	UserGroupTable	195 INSERIR	Usuário U
			Tabela de
ESEC_APP	UserGroupTable	196 APAGAR	Usuário U
		197	Tabela de
ESEC_APP	UserGroupTable	ATUALIZAR	Usuário U
		193	Tabela de
ESEC_APP	UserPackLevelParticipant	SELECIONAR	Usuário U
			Tabela de
ESEC_APP	UserPackLevelParticipant	195 INSERIR	Usuário U
			Tabela de
ESEC_APP	UserPackLevelParticipant	196 APAGAR	Usuário U
		197	Tabela de
ESEC_APP	UserPackLevelParticipant	ATUALIZAR	Usuário U
		193	Tabela de
ESEC_APP	UserProcLevelParticipant	SELECIONAR	Usuário U
			Tabela de
ESEC_APP	UserProcLevelParticipant	195 INSERIR	Usuário U
			Tabela de
ESEC_APP	UserProcLevelParticipant	196 APAGAR	Usuário U
		197	Tabela de
ESEC_APP	UserProcLevelParticipant	ATUALIZAR	Usuário U
		193	Tabela de
ESEC_APP	UserTable	SELECIONAR	Usuário U
			Tabela de
ESEC_APP	UserTable	195 INSERIR	Usuário U
			Tabela de
ESEC_APP	UserTable	196 APAGAR	Usuário U
		197	Tabela de
ESEC_APP	UserTable	ATUALIZAR	Usuário U
		193	Tabela de
ESEC_APP	XPDLApplicationPackage	SELECIONAR	Usuário U
			Tabela de
ESEC_APP	XPDLApplicationPackage	195 INSERIR	Usuário U
			Tabela de
ESEC_APP	XPDLApplicationPackage	196 APAGAR	Usuário U
		197	Tabela de
ESEC_APP	XPDLApplicationPackage	ATUALIZAR	Usuário U
		193	Tabela de
ESEC_APP	XPDLApplicationProcess	SELECIONAR	Usuário U
			Tabela de
ESEC_APP	XPDLApplicationProcess	195 INSERIR	Usuário U
			Tabela de
ESEC_APP	XPDLApplicationProcess	196 APAGAR	Usuário U

Nome da função	Nome do objeto	Ação	Tipo
		197	Tabela de
ESEC_APP	XPDLApplicationProcess	ATUALIZAR	Usuário U
		193	Tabela de
ESEC_APP	XPDLData	SELECIONAR	Usuário U
			Tabela de
ESEC_APP	XPDLData	195 INSERIR	Usuário U
			Tabela de
ESEC_APP	XPDLData	196 APAGAR	Usuário U
		197	Tabela de
ESEC_APP	XPDLData	ATUALIZAR	Usuário U
		193	Tabela de
ESEC_APP	XPDLHistory	SELECIONAR	Usuário U
			Tabela de
ESEC_APP	XPDLHistory	195 INSERIR	Usuário U
			Tabela de
ESEC_APP	XPDLHistory	196 APAGAR	Usuário U
		197	Tabela de
ESEC_APP	XPDLHistory	ATUALIZAR	Usuário U
		193	Tabela de
ESEC_APP	XPDLHistoryData	SELECIONAR	Usuário U
			Tabela de
ESEC_APP	XPDLHistoryData	195 INSERIR	Usuário U
			Tabela de
ESEC_APP	XPDLHistoryData	196 APAGAR	Usuário U
		197	Tabela de
ESEC_APP	XPDLHistoryData	ATUALIZAR	Usuário U
		193	Tabela de
ESEC_APP	XPDLParticipantPackage	SELECIONAR	Usuário U
			Tabela de
ESEC_APP	XPDLParticipantPackage	195 INSERIR	Usuário U
			Tabela de
ESEC_APP	XPDLParticipantPackage	196 APAGAR	Usuário U
		197	Tabela de
ESEC_APP	XPDLParticipantPackage	ATUALIZAR	Usuário U
		193	Tabela de
ESEC_APP	XPDLParticipantProcess	SELECIONAR	Usuário U
			Tabela de
ESEC_APP	XPDLParticipantProcess	195 INSERIR	Usuário U
			Tabela de
ESEC_APP	XPDLParticipantProcess	196 APAGAR	Usuário U
		197	Tabela de
ESEC_APP	XPDLParticipantProcess	ATUALIZAR	Usuário U
		193	Tabela de
ESEC_APP	XPDLReferences	SELECIONAR	Usuário U
			Tabela de
ESEC_APP	XPDLReferences	195 INSERIR	Usuário U
			Tabela de
ESEC_APP	XPDLReferences	196 APAGAR	Usuário U

Nome da função	Nome do objeto	Ação	Tipo
ESEC_APP	XPDLReferences	197 ATUALIZAR	Tabela de Usuário U
ESEC_APP	XPDLS	193 SELECIONAR	Tabela de Usuário U
ESEC_APP	XPDLS	195 INSERIR	Tabela de Usuário U
ESEC_APP	XPDLS	196 APAGAR	Tabela de Usuário U
ESEC_APP	XPDLS	197 ATUALIZAR	Tabela de Usuário U

ESEC_ETL

Nome da função	Nome do objeto	Ação	Tipo
ESEC_ETL	ACTVY	193 SELECIONAR	Tabela de Usuário U
ESEC_ETL	ACTVY_NAMESPACE	193 SELECIONAR	Tabela de Usuário U
ESEC_ETL	ACTVY_PARM	193 SELECIONAR	Tabela de Usuário U
ESEC_ETL	ACTVY_REF	193 SELECIONAR	Tabela de Usuário U
ESEC_ETL	ACTVY_REF_PARM_VAL	193 SELECIONAR	Tabela de Usuário U
ESEC_ETL	ADV_ALERT	193 SELECIONAR	Tabela de Usuário U
ESEC_ETL	ADV_ALERT_CVE	193 SELECIONAR	Tabela de Usuário U
ESEC_ETL	ADV_ALERT_PRODUCT	193 SELECIONAR	Tabela de Usuário U
ESEC_ETL	ADV_ATTACK	193 SELECIONAR	Tabela de Usuário U
ESEC_ETL	ADV_ATTACK_ALERT	193 SELECIONAR	Tabela de Usuário U
ESEC_ETL	ADV_ATTACK_CVE	193 SELECIONAR	Tabela de Usuário U
ESEC_ETL	ADV_ATTACK_MAP	193 SELECIONAR	Tabela de Usuário U
ESEC_ETL	ADV_ATTACK_PLUGIN	193 SELECIONAR	Tabela de Usuário U
ESEC_ETL	ADV_CREDIBILITY	193 SELECIONAR	Tabela de Usuário U
ESEC_ETL	ADV_FEED	193 SELECIONAR	Tabela de Usuário U
ESEC_ETL	ADV_PRODUCT	193 SELECIONAR	Tabela de Usuário U
ESEC_ETL	ADV_PRODUCT_SERVICE_PACK	193 SELECIONAR	Tabela de Usuário U

Nome da função	Nome do objeto	Ação	Tipo
ESEC_ETL	ADV_PRODUCT_VERSION	193 SELECIONAR	Tabela de Usuário U
ESEC_ETL	ADV_SEVERITY	193 SELECIONAR	Tabela de Usuário U
ESEC_ETL	ADV_SUBALERT	193 SELECIONAR	Tabela de Usuário U
ESEC_ETL	ADV_URGENCY	193 SELECIONAR	Tabela de Usuário U
ESEC_ETL	ADV_VENDOR	193 SELECIONAR	Tabela de Usuário U
ESEC_ETL	ADV_VULN_PRODUCT	193 SELECIONAR	Tabela de Usuário U
ESEC_ETL	ANNOTATIONS	193 SELECIONAR	Tabela de Usuário U
ESEC_ETL	ASSET	193 SELECIONAR	Tabela de Usuário U
ESEC_ETL	ASSET_CTGRY	193 SELECIONAR	Tabela de Usuário U
ESEC_ETL	ASSET_HOSTNAME	193 SELECIONAR	Tabela de Usuário U
ESEC_ETL	ASSET_IP	193 SELECIONAR	Tabela de Usuário U
ESEC_ETL	ASSET_LOC	193 SELECIONAR	Tabela de Usuário U
ESEC_ETL	ASSET_VAL_LKUP	193 SELECIONAR	Tabela de Usuário U
ESEC_ETL	ASSET_X_ENTITY_X_ROLE	193 SELECIONAR	Tabela de Usuário U
ESEC_ETL	ASSOCIATIONS	193 SELECIONAR	Tabela de Usuário U
ESEC_ETL	ATTACHMENTS	193 SELECIONAR	Tabela de Usuário U
ESEC_ETL	CONFIGS	193 SELECIONAR	Tabela de Usuário U
ESEC_ETL	CONTACTS	193 SELECIONAR	Tabela de Usuário U
ESEC_ETL	CORRELATED_EVENTS_P_MAX	193 SELECIONAR	Tabela de Usuário U
ESEC_ETL	CORRELATED_EVENTS_P_MIN	193 SELECIONAR	Tabela de Usuário U
ESEC_ETL	CRIT_LKUP	193 SELECIONAR	Tabela de Usuário U
ESEC_ETL	CUST	193 SELECIONAR	Tabela de Usuário U
ESEC_ETL	ENTITY_TYP_LKUP	193 SELECIONAR	Tabela de Usuário U
ESEC_ETL	ENV_IDENTITY_LKUP	SELECIONAR	Usuário U

Nome da função	Nome do objeto	Ação	Tipo
ESEC_ETL	ESEC_ARCHIVE_CONFIG	193 SELECIONAR	Tabela de Usuário U
ESEC_ETL	ESEC_ARCHIVE_LOG_FILES	193 SELECIONAR	Tabela de Usuário U
ESEC_ETL	ESEC_ARCHIVE_LOGS	193 SELECIONAR	Tabela de Usuário U
ESEC_ETL	ESEC_DB_PATCHES	193 SELECIONAR	Tabela de Usuário U
ESEC_ETL	ESEC_DB_VERSION	193 SELECIONAR	Tabela de Usuário U
ESEC_ETL	ESEC_DISPLAY	193 SELECIONAR	Tabela de Usuário U
ESEC_ETL	ESEC_PARTITION_CONFIG	193 SELECIONAR	Tabela de Usuário U
ESEC_ETL	ESEC_PARTITIONS_TEMP	193 SELECIONAR	Tabela de Usuário U
ESEC_ETL	ESEC_PORT_REFERENCE	193 SELECIONAR	Tabela de Usuário U
ESEC_ETL	ESEC_PROTOCOL_REFERENCE	193 SELECIONAR	Tabela de Usuário U
ESEC_ETL	ESEC_SDM_LOCK	193 SELECIONAR	Tabela de Usuário U
ESEC_ETL	ESEC_SEQUENCE	193 SELECIONAR	Tabela de Usuário U
ESEC_ETL	EVENTS_P_MAX	193 SELECIONAR	Tabela de Usuário U
ESEC_ETL	EVENTS_P_MIN	193 SELECIONAR	Tabela de Usuário U
ESEC_ETL	EVT_AGENT	193 SELECIONAR	Tabela de Usuário U
ESEC_ETL	EVT_ASSET	193 SELECIONAR	Tabela de Usuário U
ESEC_ETL	EVT_DEST_EVT_NAME_SMRY_1_P_MAX	SELECIONAR	Tabela de Usuário U
ESEC_ETL	EVT_DEST_EVT_NAME_SMRY_1_P_MAX	195 INSERIR	Tabela de Usuário U
ESEC_ETL	EVT_DEST_EVT_NAME_SMRY_1_P_MAX	196 APAGAR	Tabela de Usuário U
ESEC_ETL	EVT_DEST_EVT_NAME_SMRY_1_P_MAX	197 ATUALIZAR	Tabela de Usuário U
ESEC_ETL	EVT_DEST_EVT_NAME_SMRY_1_P_MIN	193 SELECIONAR	Tabela de Usuário U
ESEC_ETL	EVT_DEST_SMRY_1_P_MAX	SELECIONAR	Tabela de Usuário U
ESEC_ETL	EVT_DEST_SMRY_1_P_MAX	195 INSERIR	Tabela de Usuário U
ESEC_ETL	EVT_DEST_SMRY_1_P_MAX	196 APAGAR	Tabela de Usuário U

Nome da função	Nome do objeto	Ação	Tipo
ESEC_ETL	EVT_DEST_SMRY_1_P_MAX	197 ATUALIZAR	Tabela de Usuário U
ESEC_ETL	EVT_DEST_SMRY_1_P_MIN	193 SELECIONAR	Tabela de Usuário U
ESEC_ETL	EVT_DEST_TXNMY_SMRY_1_P_MAX	193 SELECIONAR	Tabela de Usuário U
ESEC_ETL	EVT_DEST_TXNMY_SMRY_1_P_MAX	195 INSERIR	Tabela de Usuário U
ESEC_ETL	EVT_DEST_TXNMY_SMRY_1_P_MAX	196 APAGAR	Tabela de Usuário U
ESEC_ETL	EVT_DEST_TXNMY_SMRY_1_P_MAX	197 ATUALIZAR	Tabela de Usuário U
ESEC_ETL	EVT_DEST_TXNMY_SMRY_1_P_MIN	193 SELECIONAR	Tabela de Usuário U
ESEC_ETL	EVT_NAME	193 SELECIONAR	Tabela de Usuário U
ESEC_ETL	EVT_NAME	195 INSERIR	Tabela de Usuário U
ESEC_ETL	EVT_NAME	196 APAGAR	Tabela de Usuário U
ESEC_ETL	EVT_NAME	197 ATUALIZAR	Tabela de Usuário U
ESEC_ETL	EVT_PORT_SMRY_1_P_MAX	193 SELECIONAR	Tabela de Usuário U
ESEC_ETL	EVT_PORT_SMRY_1_P_MAX	195 INSERIR	Tabela de Usuário U
ESEC_ETL	EVT_PORT_SMRY_1_P_MAX	196 APAGAR	Tabela de Usuário U
ESEC_ETL	EVT_PORT_SMRY_1_P_MAX	197 ATUALIZAR	Tabela de Usuário U
ESEC_ETL	EVT_PORT_SMRY_1_P_MIN	193 SELECIONAR	Tabela de Usuário U
ESEC_ETL	EVT_PRTCL	193 SELECIONAR	Tabela de Usuário U
ESEC_ETL	EVT_RSRC	193 SELECIONAR	Tabela de Usuário U
ESEC_ETL	EVT_SEV_SMRY_1_P_MAX	193 SELECIONAR	Tabela de Usuário U
ESEC_ETL	EVT_SEV_SMRY_1_P_MAX	195 INSERIR	Tabela de Usuário U
ESEC_ETL	EVT_SEV_SMRY_1_P_MAX	196 APAGAR	Tabela de Usuário U
ESEC_ETL	EVT_SEV_SMRY_1_P_MAX	197 ATUALIZAR	Tabela de Usuário U
ESEC_ETL	EVT_SEV_SMRY_1_P_MIN	193 SELECIONAR	Tabela de Usuário U
ESEC_ETL	EVT_SRC_SMRY_1_P_MAX	193 SELECIONAR	Tabela de Usuário U

Nome da função	Nome do objeto	Ação	Tipo
ESEC_ETL	EVT_SRC_SMRY_1_P_MAX	195 INSERIR	Tabela de Usuário U
ESEC_ETL	EVT_SRC_SMRY_1_P_MAX	196 APAGAR	Tabela de Usuário U
ESEC_ETL	EVT_SRC_SMRY_1_P_MAX	197 ATUALIZAR	Tabela de Usuário U
ESEC_ETL	EVT_SRC_SMRY_1_P_MIN	193 SELECIONAR	Tabela de Usuário U
ESEC_ETL	EVT_TXNMY	193 SELECIONAR	Tabela de Usuário U
ESEC_ETL	EVT_USR	193 SELECIONAR	Tabela de Usuário U
ESEC_ETL	EVT_USR	195 INSERIR	Tabela de Usuário U
ESEC_ETL	EVT_USR	196 APAGAR	Tabela de Usuário U
ESEC_ETL	EVT_USR	197 ATUALIZAR	Tabela de Usuário U
ESEC_ETL	EXT_DATA	193 SELECIONAR	Tabela de Usuário U
ESEC_ETL	HIST_CORRELATED_EVENTS_P_MAX	193 SELECIONAR	Tabela de Usuário U
ESEC_ETL	HIST_EVENTS_P_MAX	193 SELECIONAR	Tabela de Usuário U
ESEC_ETL	IMAGES	193 SELECIONAR	Tabela de Usuário U
ESEC_ETL	INCIDENTS	193 SELECIONAR	Tabela de Usuário U
ESEC_ETL	INCIDENTS_ASSETS	193 SELECIONAR	Tabela de Usuário U
ESEC_ETL	INCIDENTS_EVENTS	193 SELECIONAR	Tabela de Usuário U
ESEC_ETL	INCIDENTS_VULN	193 SELECIONAR	Tabela de Usuário U
ESEC_ETL	L_STAT	193 SELECIONAR	Tabela de Usuário U
ESEC_ETL	LOGS	193 SELECIONAR	Tabela de Usuário U
ESEC_ETL	MD_CONFIG	193 SELECIONAR	Tabela de Usuário U
ESEC_ETL	MD_EVT_FILE_STS	SELECIONAR	Tabela de Usuário U
ESEC_ETL	MD_EVT_FILE_STS	195 INSERIR	Tabela de Usuário U
ESEC_ETL	MD_EVT_FILE_STS	196 APAGAR	Tabela de Usuário U
ESEC_ETL	MD_EVT_FILE_STS	197 ATUALIZAR	Tabela de Usuário U

Nome da função	Nome do objeto	Ação	Tipo
ESEC_ETL	MD_SMRY_STS	193 SELECIONAR	Tabela de Usuário U
ESEC_ETL	MD_SMRY_STS	195 INSERIR	Tabela de Usuário U
ESEC_ETL	MD_SMRY_STS	196 APAGAR	Tabela de Usuário U
ESEC_ETL	MD_SMRY_STS	197 ATUALIZAR	Tabela de Usuário U
ESEC_ETL	MD_VIEW_CONFIG	193 SELECIONAR	Tabela de Usuário U
ESEC_ETL	NETWORK_IDENTITY_LKUP	193 SELECIONAR	Tabela de Usuário U
ESEC_ETL	OBJ_STORE	193 SELECIONAR	Tabela de Usuário U
ESEC_ETL	ORGANIZATION	193 SELECIONAR	Tabela de Usuário U
ESEC_ETL	PERSON	193 SELECIONAR	Tabela de Usuário U
ESEC_ETL	PHYSICAL_ASSET	193 SELECIONAR	Tabela de Usuário U
ESEC_ETL	PRDT	193 SELECIONAR	Tabela de Usuário U
ESEC_ETL	ROLE_LKUP	193 SELECIONAR	Tabela de Usuário U
ESEC_ETL	SENSITIVITY_LKUP	193 SELECIONAR	Tabela de Usuário U
ESEC_ETL	STATES	193 SELECIONAR	Tabela de Usuário U
ESEC_ETL	USERS	193 SELECIONAR	Tabela de Usuário U
ESEC_ETL	VNDR	193 SELECIONAR	Tabela de Usuário U
ESEC_ETL	VULN	193 SELECIONAR	Tabela de Usuário U
ESEC_ETL	VULN_CODE	193 SELECIONAR	Tabela de Usuário U
ESEC_ETL	VULN_INFO	193 SELECIONAR	Tabela de Usuário U
ESEC_ETL	VULN_RSRC	193 SELECIONAR	Tabela de Usuário U
ESEC_ETL	VULN_RSRC_SCAN	193 SELECIONAR	Tabela de Usuário U
ESEC_ETL	VULN_SCAN	193 SELECIONAR	Tabela de Usuário U
ESEC_ETL	VULN_SCAN_VULN	193 SELECIONAR	Tabela de Usuário U
ESEC_ETL	VULN_SCANNER	SELECIONAR	Tabela de Usuário U

Nome da função	Nome do objeto	Ação	Tipo
ESEC_ETL	WORKFLOW_DEF	193 SELECIONAR	Tabela de Usuário U
ESEC_ETL	WORKFLOW_INFO	193 SELECIONAR	Tabela de Usuário U

ESEC_USER

Nome da função	Nome do objeto	Ação	Tipo
ESEC_USER	ADV_ALERT_CVE_RPT_V	193 SELECIONAR	Tela V
ESEC_USER	ADV_ALERT_PRODUCT_RPT_V	193 SELECIONAR	Tela V
ESEC_USER	ADV_ALERT_RPT_V	193 SELECIONAR	Tela V
ESEC_USER	ADV_ATTACK_ALERT_RPT_V	193 SELECIONAR	Tela V
ESEC_USER	ADV_ATTACK_CVE_RPT_V	193 SELECIONAR	Tela V
ESEC_USER	ADV_ATTACK_MAP_RPT_V	193 SELECIONAR	Tela V
ESEC_USER	ADV_ATTACK_PLUGIN_RPT_V	193 SELECIONAR	Tela V
ESEC_USER	ADV_ATTACK_RPT_V	193 SELECIONAR	Tela V
ESEC_USER	ADV_CREDIBILITY_RPT_V	193 SELECIONAR	Tela V
ESEC_USER	ADV_FEED_RPT_V	193 SELECIONAR	Tela V
ESEC_USER	ADV_PRODUCT_RPT_V	193 SELECIONAR	Tela V
ESEC_USER	ADV_PRODUCT_SERVICE_PACK_RPT_V	193 SELECIONAR	Tela V
ESEC_USER	ADV_PRODUCT_VERSION_RPT_V	193 SELECIONAR	Tela V
ESEC_USER	ADV_SEVERITY_RPT_V	193 SELECIONAR	Tela V
ESEC_USER	ADV_SUBALERT_RPT_V	193 SELECIONAR	Tela V
ESEC_USER	ADV_URGENCY_RPT_V	193 SELECIONAR	Tela V
ESEC_USER	ADV_VENDOR_RPT_V	193 SELECIONAR	Tela V
ESEC_USER	ADV_VULN_PRODUCT_RPT_V	193 SELECIONAR	Tela V
ESEC_USER	ANNOTATIONS_RPT_V	193 SELECIONAR	Tela V
ESEC_USER	ASSET_CATEGORY_RPT_V	SELECIONAR	Tela V

Nome da função	Nome do objeto	Ação	Tipo
		193	
ESEC_USER	ASSET_HOSTNAME_RPT_V	SELECIONAR	Tela V
		193	
ESEC_USER	ASSET_IP_RPT_V	SELECIONAR	Tela V
		193	
ESEC_USER	ASSET_LOCATION_RPT_V	SELECIONAR	Tela V
		193	
ESEC_USER	ASSET_RPT_V	SELECIONAR	Tela V
		193	
ESEC_USER	ASSET_VALUE_RPT_V	SELECIONAR	Tela V
		193	
ESEC_USER	ASSET_X_ENTITY_X_ROLE_RPT_V	SELECIONAR	Tela V
		193	
ESEC_USER	ASSOCIATIONS_RPT_V	SELECIONAR	Tela V
		193	
ESEC_USER	ATTACHMENTS_RPT_V	SELECIONAR	Tela V
		193	
ESEC_USER	CONFIGS_RPT_V	SELECIONAR	Tela V
		193	
ESEC_USER	CONTACTS_RPT_V	SELECIONAR	Tela V
		193	
ESEC_USER	CORRELATED_EVENTS	SELECIONAR	Tela V
		193	
ESEC_USER	CORRELATED_EVENTS_RPT_V	SELECIONAR	Tela V
		193	
ESEC_USER	CORRELATED_EVENTS_RPT_V1	SELECIONAR	Tela V
		193	
ESEC_USER	CRITICALITY_RPT_V	SELECIONAR	Tela V
		193	
ESEC_USER	CUST_RPT_V	SELECIONAR	Tela V
		193	
ESEC_USER	ENTITY_TYPE_RPT_V	SELECIONAR	Tela V
		193	
ESEC_USER	ENV_IDENTITY_RPT_V	SELECIONAR	Tela V
		193	
ESEC_USER	ESEC_DISPLAY_RPT_V	SELECIONAR	Tela V
		193	
ESEC_USER	ESEC_PORT_REFERENCE_RPT_V	SELECIONAR	Tela V
		193	
ESEC_USER	ESEC_PROTOCOL_REFERENCE_RPT_V	SELECIONAR	Tela V
		193	
ESEC_USER	ESEC_SEQUENCE_RPT_V	SELECIONAR	Tela V
		224	
ESEC_USER	esec_toBase	EXECUTAR	NULL
		224	
ESEC_USER	esec_toDecimal	EXECUTAR	NULL
		224	
ESEC_USER	esec_toIpChar	EXECUTAR	NULL

Nome da função	Nome do objeto	Ação	Tipo
		193	
ESEC_USER	EVENTS	SELECIONAR	Tela V
		193	
ESEC_USER	EVENTS_ALL_RPT_V	SELECIONAR	Tela V
		193	
ESEC_USER	EVENTS_ALL_RPT_V1	SELECIONAR	Tela V
		193	
ESEC_USER	EVENTS_ALL_V	SELECIONAR	Tela V
		193	
ESEC_USER	EVENTS_RPT_V	SELECIONAR	Tela V
		193	
ESEC_USER	EVENTS_RPT_V1	SELECIONAR	Tela V
		193	
ESEC_USER	EVENTS_RPT_V2	SELECIONAR	Tela V
		193	
ESEC_USER	EVT_AGENT_RPT_V	SELECIONAR	Tela V
		193	
ESEC_USER	EVT_ASSET_RPT_V	SELECIONAR	Tela V
		193	
ESEC_USER	EVT_DEST_EVT_NAME_SMRY_1	SELECIONAR	Tela V
		193	
ESEC_USER	EVT_DEST_EVT_NAME_SMRY_1_RPT_V	SELECIONAR	Tela V
		193	
ESEC_USER	EVT_DEST_SMRY_1	SELECIONAR	Tela V
		193	
ESEC_USER	EVT_DEST_SMRY_1_RPT_V	SELECIONAR	Tela V
		193	
ESEC_USER	EVT_DEST_TXNMY_SMRY_1	SELECIONAR	Tela V
		193	
ESEC_USER	EVT_DEST_TXNMY_SMRY_1_RPT_V	SELECIONAR	Tela V
		193	
ESEC_USER	EVT_NAME_RPT_V	SELECIONAR	Tela V
		193	
ESEC_USER	EVT_PORT_SMRY_1	SELECIONAR	Tela V
		193	
ESEC_USER	EVT_PORT_SMRY_1_RPT_V	SELECIONAR	Tela V
		193	
ESEC_USER	EVT_PRTCL_RPT_V	SELECIONAR	Tela V
		193	
ESEC_USER	EVT_RSRC_RPT_V	SELECIONAR	Tela V
		193	
ESEC_USER	EVT_SEV_SMRY_1	SELECIONAR	Tela V
		193	
ESEC_USER	EVT_SEV_SMRY_1_RPT_V	SELECIONAR	Tela V
		193	
ESEC_USER	EVT_SRC_SMRY_1	SELECIONAR	Tela V
		193	
ESEC_USER	EVT_SRC_SMRY_1_RPT_V	SELECIONAR	Tela V

Nome da função	Nome do objeto	Ação	Tipo
		193	
ESEC_USER	EVT_TXNMY_RPT_V	SELECIONAR	Tela V
		193	
ESEC_USER	EVT_USR_RPT_V	SELECIONAR	Tela V
		193	
ESEC_USER	EXTERNAL_DATA_RPT_V	SELECIONAR	Tela V
		193	
ESEC_USER	HIST_CORRELATED_EVENTS	SELECIONAR	Tela V
		193	
ESEC_USER	HIST_CORRELATED_EVENTS_RPT_V	SELECIONAR	Tela V
		193	
ESEC_USER	HIST_EVENTS	SELECIONAR	Tela V
		193	
ESEC_USER	HIST_EVENTS_RPT_V	SELECIONAR	Tela V
		193	
ESEC_USER	IMAGES_RPT_V	SELECIONAR	Tela V
		193	
ESEC_USER	INCIDENTS_ASSETS_RPT_V	SELECIONAR	Tela V
		193	
ESEC_USER	INCIDENTS_EVENTS_RPT_V	SELECIONAR	Tela V
		193	
ESEC_USER	INCIDENTS_RPT_V	SELECIONAR	Tela V
		193	
ESEC_USER	INCIDENTS_VULN_RPT_V	SELECIONAR	Tela V
		193	
ESEC_USER	L_STAT_RPT_V	SELECIONAR	Tela V
		193	
ESEC_USER	LOGS_RPT_V	SELECIONAR	Tela V
		193	
ESEC_USER	NETWORK_IDENTITY_RPT_V	SELECIONAR	Tela V
		193	
ESEC_USER	ORGANIZATION_RPT_V	SELECIONAR	Tela V
		193	
ESEC_USER	PERSON_RPT_V	SELECIONAR	Tela V
		193	
ESEC_USER	PHYSICAL_ASSET_RPT_V	SELECIONAR	Tela V
		193	
ESEC_USER	PRODUCT_RPT_V	SELECIONAR	Tela V
		193	
ESEC_USER	ROLE_RPT_V	SELECIONAR	Tela V
		193	
ESEC_USER	SENSITIVITY_RPT_V	SELECIONAR	Tela V
		193	
ESEC_USER	STATES_RPT_V	SELECIONAR	Tela V
		193	
ESEC_USER	UNASSIGNED_INCIDENTS_RPT_V	SELECIONAR	Tela V
		193	
ESEC_USER	USERS_RPT_V	SELECIONAR	Tela V

Nome da função	Nome do objeto	Ação	Tipo
		193	
ESEC_USER	VENDOR_RPT_V	SELECIONAR	Tela V
		193	
ESEC_USER	VULN_CALC_SEVERITY_RPT_V	SELECIONAR	Tela V
		193	
ESEC_USER	VULN_CODE_RPT_V	SELECIONAR	Tela V
		193	
ESEC_USER	VULN_INFO_RPT_V	SELECIONAR	Tela V
		193	
ESEC_USER	VULN_RPT_V	SELECIONAR	Tela V
		193	
ESEC_USER	VULN_RSRC_RPT_V	SELECIONAR	Tela V
		193	
ESEC_USER	VULN_RSRC_SCAN_RPT_V	SELECIONAR	Tela V
		193	
ESEC_USER	VULN_SCAN_RPT_V	SELECIONAR	Tela V
		193	
ESEC_USER	VULN_SCAN_VULN_RPT_V	SELECIONAR	Tela V
		193	
ESEC_USER	VULN_SCANNER_RPT_V	SELECIONAR	Tela V

Funções do Sentinel Server

Função do servidor	Descrição	Usuário do Sentinel
sysadmin	Administradores de Sistema	esecdba
securityadmin	Administradores de Segurança	esecapp
serveradmin	Administradores de Servidor	esecdba
setupadmin	Administradores de Configuração	
processadmin	Administradores de Processo	
diskadmin	Administradores de Disco	
dbcreator	Criadores de banco de dados	
bulkadmin	Administradores de Inserção de Bulk	

Usuários e permissões de banco de dados de autenticação de domínio do Windows

Um usuário de domínio será associado com usuário esecadm, esecapp, esecdba e esecrpt, de acordo com a configuração no momento da instalação. Esses usuários de domínio terão os mesmos privilégios especificados nas seções anteriores.

D Tabelas de permissão de serviço do Sentinel

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

Sentinel Server (Mecanismo de correlação)

Componente do Sentinel	Aplicativo do Sentinel	Serviço do Sentinel	Processo do Sentinel	Resumo da função	Permissões necessárias	Explicação da permissão
Sentinel Server	-	Sentinel / WatchDog.exe	correlation_engine.exe	O processo do Mecanismo de Correlação (correlation_engine) recebe eventos do Gerenciador do Coletor Assistente e publica eventos correlacionados com base em regras de correlação definidas pelo usuário.	Acesso a rede; acesso de leitura para arquivos de configuração modificados.	Ele se comunica com o Sonic para configuração e processo de evento e geração de evento correlacionado. Precisará de acesso de arquivo se você usar um arquivo de configuração modificado.

Gerenciador de Coletor do Windows

Componente do Sentinel	Aplicativo do Sentinel	Serviço do Sentinel	Processo do Sentinel	Resumo da função	Tipo de conector	Permissões necessárias	Explicação da permissão
Assistente do Sentinel / Gerenciador de Coletor	-	Gerenciador de Coletores	agentengine.exe	O processo do Gerenciador de Coletor gerencia os Mecanismos do Coletor (gera os processos do Mecanismo do Coletor), publica mensagens de status do sistema, realiza a filtragem global de eventos e mapeamentos referenciais. O processo do Mecanismo do Coletor executa scripts de um Coletor, que normaliza eventos não processados (iniciais) de dispositivos e sistemas de segurança.	**NOTA:** Dependendo dos tipos de conexão, o Gerenciador de Coletor precisará de permissões diferentes.		
					Serial – dados lidos de uma porta serial RS-232C	Permissão de leitura/gravação em uma porta serial	Leitura/gravação do Mecanismo do Coletor para uma porta serial
					Soquete – uma conexão de s oquete TCP	Acesso a rede – leitura/gravação do soquete da rede; permissão para iniciar uma conexão	O Mecanismo do Coletor inicia uma conexão com um ponto final de rede e leitura/gravação neste soquete
					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)	Acesso de leitura/gravação de arquivo	O Mecanismo do Coletor faz a leitura do primeiro arquivo especificado e grava no segundo arquivo especificado
					Arquivo todos – lê todos os dados de evento de segurança em um arquivo	Acesso de leitura/gravação de arquivo	O Mecanismo do Coletor faz a leitura do primeiro arquivo especificado e grava no segundo arquivo especificado

Componente do Sentinel	Aplicativo do Sentinel	Serviço do Sentinel	Processo do Sentinel	Resumo da função	Tipo de conector	Permissões necessárias	Explicação da permissão
					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.	Permissão para executar o processo persistente definido. (Nota: se estiver usando EventLog.exe como o processo persistente para coletar registro NT usando o WMI, o Gerenciador do Coletor precisará de permissão para acessar o WMI)	O Mecanismo do Coletor executa o processo definido no nível de permissão atual
					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.	Permissão para executar o processo transitório definido	O Mecanismo do Coletor executa o processo definido no nível de permissão atual

Componente do Sentinel	Aplicativo do Sentinel	Serviço do Sentinel	Processo do Sentinel	Resumo da função	Tipo de conector	Permissões necessárias	Explicação da permissão
					SNMP – recebe detecções de SNMP v1, v2 e v3	Acesso a rede – leitura/gravação do soquete da rede	O Gerenciador do Coletor envia/recebe detecções SNMP
					Nenhum	NA	NA
Assistente do Sentinel / Construtor de Coletor	Construtor de Coletor	-	agentbuilder.exe	Uma GUI que possibilita que você construa, configure e controle Coletores. A GUI pode ser usada para executar Coletores locais ou controlar Coletores nos sistemas do Assistente remoto.	Acesso de leitura/gravação de arquivo		%WORKBENCH_HOME%/Elements – contém os scripts do Coletor de leitura/gravação do Construtor de Coletor.
					Acesso de leitura/gravação de arquivo		%WORKBENCH_HOME%/Agents – contém o arquivo de configuração de porta de leitura/gravação do Construtor de Coletor.
					Acesso de leitura/gravação de arquivo		%ESEC_HOME%/.uuid de acesso do Construtor de Coletor
					Acesso a rede – leitura/gravação do soquete da rede; permissão para iniciar uma conexão		Coletores de upload/download do Construtor de Coletor e mensagens recebidas sobre a saúde do Gerenciador de Coletor

Comunicação do Sentinel

Componente do Sentinel	Aplicativo do Sentinel	Serviço do Sentinel	Processo do Sentinel	Resumo da função	Permissões necessárias	Explicação da permissão
iSCALE / MOM	SonicMQ	Comunicação do Sentinel	sonicmf.exe	No Windows, a Comunicação do Sentinel é um serviço e é chamado de iSCALE – um MOM (Message-Oriented Middleware - Middleware Orientado por Mensagem). O componente do iSCALE que fornece um sistema Java Message Service (JMS) para comunicação dentro do processo. Os processos comunicam-se através de um controlador que é responsável por rotear as mensagens e armazená-las no buffer. Vários controladores podem se comunicar entre si para atravessar firewalls ou para equilibrar carga. Os processos do Sentinel usam um mecanismo editor/subscritor para se comunicarem uns com os outros. Isso permite que um processo publique uma mensagem em um canal tópico consumido por vários assinantes, sem que o processo de publicação saiba qual processo está subscrito a ele. Os assinantes podem receber mensagens publicadas dos editores sem saber quais editores estão disponíveis. Esse processo minimiza a configuração e aumenta a estabilidade e a escalabilidade do sistema. Por exemplo, quando um novo Assistente é adicionado ao sistema, não é necessário fazer nenhuma configuração no lado do Sentinel. O processo do editor publica as mensagens em tópicos (canais) e os processos de assinante assinam os tópicos. O controlador de mensagens direciona as mensagens dos editores para os assinantes com base nos tópicos nos quais foram registrados.	Permissões para acessar o seu próprio banco de dados embutido, instalar diretório (%ESEC_HOME%\3rdparty \SonicMQ) e arquivos	O Sonic acessa o seu próprio banco de dados embutido e instala o diretório (%ESEC_HOME%\3rdparty \SonicMQ) e os arquivos

Servidor de banco de dados (diferente de DAS)

Componente do Sentinel	Aplicativo do Sentinel	Serviço do Sentinel	Processo do Sentinel	Resumo da função	Permissões necessárias	Explicação da permissão
-	-	-	-	Configuração do banco de dados do Sentinel	-	Precisa ter driver odbc ou driver oracle apontando para o bd do sentinel

Servidor de banco de dados (com DAS)

Para obter um resumo / um detalhamento da permissão de acesso do banco de dados do Sentinel, consulte a seguinte documentação:
Apêndice A – Usuários, funções e permissões de acesso de banco de dados do Sentinel

Componente do Sentinel	Aplicativo do Sentinel	Serviço do Sentinel	Processo do Sentinel	Resumo da função	Permissões necessárias	Explicação da permissão
-	-	-	-	Configuração do banco de dados do Sentinel	-	Precisa ter driver odbc ou driver oracle apontando para o bd do sentinel
Sentinel Server	-	Sentinel / WatchDog.exe	das_binary	operações de inserção de evento e evento correlacionado	Acesso a rede; precisa de acesso ao BD para instância ESEC como ESECAPP	Comunica-se com o Sonic. Comunica-se com o BD via JDBC para recuperação de dados e ADO para inserção de evento se a estratégia de carregamento ADO for configurada
			das_query	todas as outras operações de banco de dados	Acesso a rede; precisa de acesso ao BD para instância ESEC como ESECAPP; precisa de permissão para executar processos	Comunica-se com o Sonic. Comunica-se com BD via JDBC para recuperação de dados
			activity_container	execução e configuração do serviço de atividade	Acesso a rede; precisa de acesso ao BD para instância ESEC como ESECAPP; precisa de permissão para executar processos	Comunica-se com o Sonic. Comunica-se com BD via JDBC para recuperação e inserção de dados

Para obter um resumo / um detalhamento da permissão de acesso do banco de dados do Sentinel, consulte a seguinte documentação:
Apêndice A – Usuários, funções e permissões de acesso de banco de dados do Sentinel

Componente do Sentinel	Aplicativo do Sentinel	Serviço do Sentinel	Processo do Sentinel	Resumo da função	Permissões necessárias	Explicação da permissão
			workflow_container	configuração do serviço de workflow (iTRAC)	Acesso a rede; precisa de acesso ao BD para instância ESEC_WF como ESECAPP; precisa de permissão para executar processos	Comunica-se com o Sonic. Comunica-se com BD via JDBC para recuperação e inserção de dados
			das_rt	configuração da função dos Active Views dentro do Console de Controle do Sentinel.	Acesso a rede; precisa de acesso ao BD para instância ESEC como ESECAPP	Comunica-se com o Sonic. Comunica-se com BD via JDBC para recuperação de dados

Reporting Server

Componente do Sentinel	Aplicativo do Sentinel	Serviço do Sentinel	Processo do Sentinel	Resumo da função	Permissões necessárias	Explicação da permissão
-	-	-	-	Crystal Reports XI ou Crystal Enterprise 9 Standard é uma das ferramentas de geração de relatórios que se integram ao Sentinel.	-	Precisa ter driver odbc ou driver oracle apontando para o bd do sentinel

Glossário

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

Agente

Consulte Coletor

Agregação e Normalização de Eventos

Agregação é o processo de combinar itens de dados individuais de baixa relevância, resultando em um item de dados que pode ser de alta importância. As partes individuais do evento em si, como nome do evento, data do evento, IP de origem, IP de destino, UUID, tipo de sensor e assim por diante, podem não ter muita importância. Contudo, basta juntá-los, e é criado um evento que pode ser de interesse como, por exemplo, um ataque na rede, resultando em uma possível exploração de bem. A gravação de um evento inteiro causa o armazenamento de informações duplicadas. Por exemplo, em um sistema não agregado para dez eventos idênticos, com exceção da data do evento, serão armazenados todos os eventos, resultando em itens de dados idênticos (nome do evento, tipo de sensor etc...) sendo gravados dez vezes. A agregação armazenará os itens de dados idênticos somente uma vez e, em seguida, manterá uma conta em execução por uma hora.

Os dados do evento são transformados, resumidos e armazenados em tabelas de resumo. Os relatórios de resumo podem, então, ser executados em relação aos resumos pré-calculados, o que torna as consultas menos disputadas nas tabelas de eventos em tempo real. O mecanismo de agregação de eventos captura os dados do evento binário, transforma-o em uma estrutura de evento normalizada e o resume com base em um conjunto predefinido de definições de resumo. O mecanismo de agregação de eventos processa os eventos em um modo quase em tempo real, com overhead mínimo para o sistema em tempo real do Sentinel.

Análise

No Sentinel Control Center, é permitida a geração de relatórios de histórico. Os relatórios de histórico e de vulnerabilidade são publicados em um servidor web Crystal®. Depois, são executados diretamente no banco de dados e aparecem nas guias Análise e Consultor da barra Navegador do Sentinel Control Center.

arquivo de script

No Assistente, um arquivo compilado (*.asd) formado pelos seguintes arquivos: de gabarito do Coletor, de parâmetro, de pesquisa e de mapeamento.

Arquivos de gabarito

Para os Coletores, você pode criar, editar e apagar gabaritos, assim como adicionar estados a estes. 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.

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 próximo processamento a ser realizado. Os estados incluem 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.

Arquivos de Mapeamento

Para os Coletores, 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 é feita no Construtor de Coletor, mas eles podem ser editados no Excel.

Arquivos de Parâmetro

Para os Coletores, os arquivos de Parâmetro (arquivos .par) são tabelas usadas para definir nomes de parâmetros nos arquivos de script de execução associados. Eles são usados quando mencionados no código de análise. Os parâmetros equivalem a variáveis 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

Para os Coletores, 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 sensores, 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.

Assistente

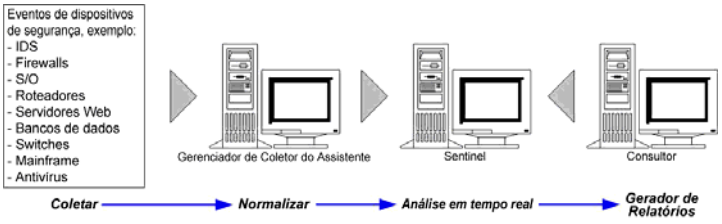
O Construtor de Coletor e o Gerenciador de Coletor.

Buffer Rx

Parte do Gerenciador do Coletor, seu tamanho padrão é de 50.000 eventos. O buffer de recebimento é um parâmetro editável. O tamanho mínimo é 5.000.

Coletor

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.



Existem três níveis de Coletores, mostrados a seguir:

- Coletores Aceitos (T1)
- Coletores Documentados (T2)
- Coletores de Exemplo (T3)

Os coletores são constituídos de:

- arquivos de gabarito
- arquivos de parâmetros
- arquivos de pesquisa
- arquivos de mapeamento

comando de análise

No Assistente, uma interface de criação de scripts de alto nível que permite a manipulação de dados. A análise é o processo de dividir um evento em seus componentes.

Configuração de Evento

A configuração de evento (Parte do Serviço de Mapeamento) permite:

- Habilitar o monitoramento de Conformidade Normativa
- Habilitar a Conformidade com Políticas
- Habilitar a priorização de resposta
- Habilitar a análise de dados de segurança relacionados a operações comerciais
- Aperfeiçoar a responsabilidade

A configuração de evento é a atribuição de nomes a etiquetas existentes. Por exemplo, renomear Ct2 para City. As mudanças propagam-se para os filtros e regras de correlação.

Construtor de Agentes

Consulte Construtor de Coletor

Construtor de Coletor

Uma GUI que permite que você crie Coletores baseados em regras para coletar, filtrar e normalizar dados de várias fontes e comunique com segurança informações relevantes ao Sentinel Server que podem ser usadas para monitorar o tráfego.

Consulta Rápida

Consulte Gerenciador de Consultas.

Consultor

Um sistema integrado com o banco de dados de vulnerabilidades da SecurityNexus destinado a estabelecer uma referência cruzada entre eventos em tempo real e vulnerabilidades conhecidas.

Controlador de Dados

Consulte Processo do Sincronizador de Dados.

Correlação	O processo de analisar eventos de segurança para identificar relacionamentos em potencial entre dois ou mais eventos. A correlação permite uma rápida associação de ataques prioritários com base em elementos comuns de dados do evento. Tendências ou padrões entre eventos de nível inferior que são desenvolvidos para operar abaixo dos limites de segurança podem ser identificados com mais eficiência usando a correlação. O Sentinel oferece cinco tipos de regras de correlação. São elas: ▪ Lista de Avisos ▪ Correlação Básica ▪ Correlação Avançada ▪ RuleLg de Formato Livre
das_aggregation.xml	Usado para operação de agregação
das_binary.xml	Usado para a operação de inserção de evento e evento correlacionado.
das_itrac.xml	Usado para a execução e a configuração do serviço ativo e para a configuração do serviço de workflow.
das_query.xml	Especifica os parâmetros de configuração para o DAS (Data Access Service - Serviço de Acesso a Dados), um componente do Banco de Dados do Sentinel.
das_rt.xml	Especifica a configuração para a função do Active Views dentro do Console de Controle do Sentinel.
Detecção de Exploração	Consulte Serviço de mapeamento

evento

Evento é uma ação ou ocorrência detectada por um dispositivo de segurança (evento externo) ou processo (interno). Os eventos podem ser relacionados a segurança, desempenho ou informações. Por exemplo, um evento externo pode ser um ataque detectado pelo IDS (Intrusion Detection System - Sistema de Detecção de Intrusão), um login bem-sucedido detectado por um sistema operacional ou uma situação definida pelo cliente, como um usuário acessando um arquivo. Os eventos relacionados a informações são eventos internos. Os eventos internos indicam uma mudança no estado de um processo. Por exemplo, a interrupção de uma porta.

Eventos do sistema

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

- Eventos internos
- Eventos de desempenho

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

Eventos Internos

Consulte Eventos do sistema

Filtros

Os filtros do Sentinel permitem o processamento de dados com base em um critério específico para ambos os eventos que entram no sistema e os usuários do sistema. Existem vários níveis de filtragem:

- Coletor – feito através do script usando o Construtor de Coletor.
- filtro global – aplicado igualmente a todos os eventos gerados por todos os Assistentes no sistema. Somente os eventos que passam pelos Filtros Globais são enviados para todos os processos do Sentinel.
- filtro de segurança – aplicado a todos os Usuários ativos. Esses filtros restringem os eventos que um usuário ativo pode observar. Esses filtros são atribuídos pelo Administrador.
- filtro de exibição – aplicado a telas de interface. Esses filtros permitem que o usuário defina suas janelas de eventos para análise em tempo real. Esses filtros são aplicados pelos usuários, individualmente.

Existem dois tipos de filtros:

- público – os filtros públicos são de propriedade do sistema. Os filtros públicos podem ser usados como filtros de segurança ou filtros de exibição. Os filtros de segurança são baseados em permissões do usuário. Os filtros de exibição determinam quais eventos são descritos nas tabelas e nos gráficos de eventos em tempo real.
- privado – os filtros particulares são de propriedade do usuário. Os filtros particulares são filtros de exibição e poderão ser compartilhados se você tiver a permissão Ver Filtros Particulares.

Gerenciador de Agentes

Gerenciador de Coletores

Gerenciador de Coletores

O assistente de backend que gerencia Coletores e mensagens de status do sistema.

Gerenciamento de Bens

O propósito do Gerenciamento de Bens é vincular um ou mais eventos a bens e a informações sobre vulnerabilidade para aplicar um método para proteger os bens da organização de maneira eficiente. Existem dois tipos de bens: físicos e flexíveis. Os Bens Físicos são o hardware e os Bens Flexíveis são os serviços e os aplicativos.

Host do assistente

Qualquer máquina que tenha o software Gerenciador de Coletores instalado.

Incidentes

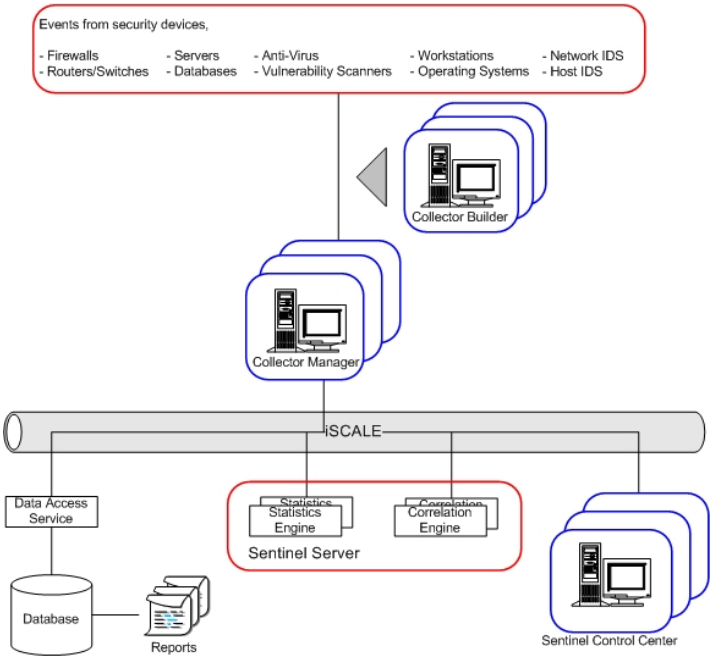
Agrupamento de um conjunto de eventos reunidos como um todo, representando algo de interesse (um grupo de eventos semelhantes ou um conjunto de eventos diferentes que indicam um padrão de interesse, como um ataque).

Indicador de Buffer Rx

O indicador do Buffer de Recebimento indica os bytes de dados no Buffer de Recebimento. Antes de cada string conclusiva avaliada, o indicador do Buffer de Recebimento é redefinido para o seu valor mantido (normalmente zero).

iSCALE™

O Barramento de Mensagens fornece um sistema JMS (Java Message Service - Serviço de Mensagens Java) para comunicação entre processos. Os processos comunicam-se através de um controlador que é responsável por rotear as mensagens e armazená-las no buffer. Vários controladores podem se comunicar entre si para atravessar firewalls e para equilibrar a carga.



Os processos a seguir comunicam-se entre si através do Barramento de Mensagens.

- Watchdog
- Desempenho de Evento (Mecanismo de Filtro)
- Total de Eventos ao Longo do Tempo (Mecanismo de Estatísticas)
- Sincronizador de Dados (Controlador de Dados)
- Mecanismo de Correlação
- Verificador RuleLg (Verificador de Regra de Correlação)
- DAS (Data Access Service - Serviço de Acesso a Dados)
- Gerenciador de Consultas

iTRAC™

O iTRAC envolve a automação de procedimentos, a capacidade de responder a incidentes. O Sentinel fornece um sistema de gerenciamento de workflow que oferece automação de procedimentos do processo Gestão de Incidentes do SANS. As partes principais do iTRAC são:

- Gerenciador de Listas de Trabalho – aplicativo usado para mover-se de uma atividade para outra.
- Construtor de Atividades – aplicativo usado para criar o seu próprio iTRAC personalizado
- Monitor de Processos – Monitora as atividades (etapas) realizadas para concluir um processo.

Mecanismo de Coletor

Processa a lógica de gabarito para cada porta. Um mecanismo de Coletor executa uma porta correspondente.

Mecanismo de Correlação

O Mecanismo de Correlação realiza a análise de eventos recebidos para encontrar padrões de interesse e investiga os eventos de correlação para determinar os detalhes que acionaram uma regra.

Mecanismo de Estatística

Consulte Total de Eventos ao Longo do Tempo.

Mecanismo de Filtro

Consulte Processo de Desempenho de Evento.

Mecanismo de Filtro

Consulte Processo de Desempenho de Evento.

Mecanismo do Agente

Consulte Mecanismo de Coletor

metadados

Os metadados são informações sobre dados, nomes variáveis predefinidos para metadados. Por exemplo, o IP de origem de um ataque é armazenado na tag META SourceIP. Nomes de produtos são armazenados na tag META ProductName. Os dados usados para preencher tags META são extraídos de dados de eventos ou definidos como parte do processamento do Coletor.

Middleware Baseado em Mensagens

Consulte iSCALE™.

MOM

Consulte iSCALE™.

Normalização de Eventos

Consulte Agregação

número de ID de evento

Um número atribuído a um evento.

Porta

No Assistente, as portas possibilitam que um Coletor localize os dados do evento de segurança na rede, fornecendo o endereço IP e outras informações sobre a origem (dispositivo de segurança [roteador, IDS, switch, etc…]). Cada linha na tabela de Configuração de Portas executa um script de Coletor para uma origem de evento.

Processo do Gerenciador de Consultas (query_manager)

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

Processo do Mecanismo de Correlação (correlation_engine)

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

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

O processo do DAS é o serviço de persistência do Sentinel Server e fornece uma interface de barramento (iSCALE) de mensagens para o banco de dados. Ele concede acesso baseado em dados para o banco de dados de backend. Ele recebe um pedido XML de diferentes processos do Sentinel, o converte em uma consulta no banco de dados, processa o resultado do banco de dados e o converte de volta em uma resposta XML. Ele oferece suporte a solicitações para recuperar eventos para Consulta Rápida e Detalhamento de Eventos, para recuperar informações de vulnerabilidade e informações do consultor e para manipular informações de configuração. O DAS também gerencia o registro de todos os eventos recebidos do Gerenciador do Coletor Assistente e pede a recuperação e o armazenamento das informações de configuração.

Processo do Sincronizador de Dados (Controlador de Dados)

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

Processo do Verificador de RuleLg (rulelg_checker)

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

Processo Watchdog

O Watchdog é um Processo do Sentinel que gerencia todos os outros Processos desse programa. Se um processo que não seja o Watchdog parar, o Watchdog reiniciará esse processo.

Regra de Correlação Avançada

Permite criar uma regra de correlação que incorpore todos os recursos da regra de correlação simples, assim como enviar um evento quando um conjunto de eventos possuir valores de tags META diferentes, como um sensor dentro ou fora do firewall. Por exemplo, uma regra de Correlação Avançada pode procurar por eventos do mesmo endereço IP fonte para o mesmo endereço de destino com o mesmo nome de evento que ocorre tanto dentro quanto fora de um firewall (o que quer dizer que o ataque ocorreu através do firewall).

Regra de Correlação Básica

Permite selecionar qualquer meta-tag para criar uma regra de correlação que permite contar o número de vezes que certas condições são atendidas dentro de determinado espaço de tempo. Por exemplo, uma regra de Correlação Básica pode procurar pelo mesmo endereço IP relatado cinco vezes em cinco minutos, mesmo que os eventos sejam relatados de diferentes produtos, como um sistema de detecção de invasão (IDS) e um firewall.

Regra de Correlação de Lista de Avisos

Permite que você especifique uma string de texto que o Mecanismo de Correlação assistirá em cada tag META para cada evento recebido. Por exemplo, uma regra de lista de avisos pode procurar por um endereço IP de origem específico de um hacker e notificá-lo todas as vezes que esse endereço IP for visto em qualquer mensagem de evento.

Relevância Comercial

Consulte Serviço de Mapeamento.

Roteador de Eventos

O Roteador de Eventos faz a transformação e a filtragem do mapeamento de eventos.

Sentinel Control Center

O Sentinel Control Center é o console de gerenciamento central para visualizar exibições de resumo, relatórios de histórico e eventos de filtro em tempo real, bem como para criar incidentes. O Sentinel Control Center oferece exibição em tempo real de eventos, visão geral do sistema de mudanças em atividade acionado por conjuntos de configurações nos Coletores, administração dos filtros, geração de relatórios, regras correlacionadas e filtros globais e gerenciamento de eventos de segurança através de incidentes.

Sentinel Server

O Sentinel Server recebe informações de evento normalizado reunidas pelos Coletores do Gerenciador do Coletor Assistente. O Sentinel Server correlaciona esses eventos para encontrar padrões e identificar ameaças e relatórios em dados e informações de histórico em tempo real que podem ser vistos no Sentinel Control Center.

Seqüências (inicialização e 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 Assistentes na rede, fornecendo o endereço IP ou nome de arquivo sobre o host. 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
- Nome do processo
- Informações sobre soquete
- Informações sobre SNMP
- Nomes de arquivos de entrada/saída
- Nome do Coletor

Seqüências de Backout

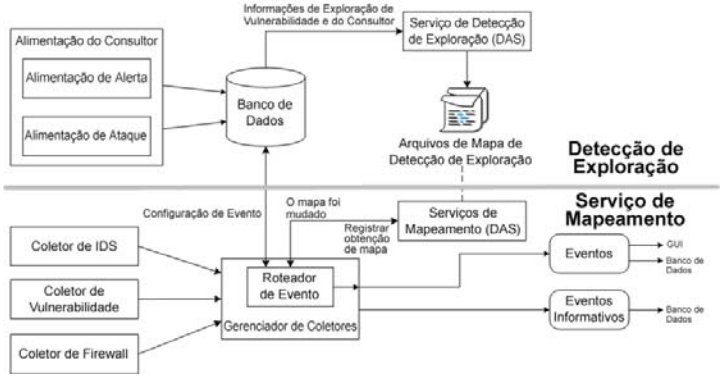
Consulte Seqüências.

Seqüências de Inicialização

Consulte Seqüências.

Serviço de Mapeamento

O Serviço de Mapeamento do Sentinel possibilita a notificação imediata e processável de ataques em sistemas vulneráveis. Ele fornece um vínculo em tempo real entre os eventos e os resultados de exploração de vulnerabilidades, para que os usuários sejam notificados de forma automática e imediata quando um ataque estiver tentando explorar um sistema vulnerável. Isso melhora a eficiência e a efetividade da resposta a incidentes, resultando em maior disponibilidade de sistemas críticos e em segurança mais econômica.



tag META

As tags META armazenam metadados.

Tempo Real de Evento

Capacidade de monitorar a ocorrência de eventos e de realizar consultas nesses eventos. Você pode monitorá-los em forma de tabela ou por meio de uma representação gráfica em 3D.

Uuids de Eventos Correlacionados

O identificador do evento correlacionado gerado pela regra acionada.

Visualização de Vulnerabilidade

Uma representação gráfica de dados de evento em tempo real em relação a sistemas vulneráveis e que fica disponível em um evento para vulnerabilidade atual e no momento do evento.

workflow

Consulte iTRAC™.