Novell® Sentinel™

5.1.3

www.novell.com

Volume IV – GUIDA DI RIFERIMENTO DI SENTINEL

7 luglio 2006

Novell®

Note legali

Novell, Inc.
404 Wyman Street, Suite 500
Waltham, MA 02451
U.S.A.
www.novell.com

Documentazione in linea: Per accedere alla documentazione in linea per questo e altri prodotti Novell e per ottenere aggiornamenti, visitare il sito Novell all'indirizzo www.novell.com/documentation.

Marchi di fabbrica Novell

Per i marchi Novell, vedere l'elenco disponibile all'indirizzo (http://www.novell.com/company/legal/trademarks/tmlist.html).

Materiali di terze parti

Tutti i marchi di fabbrica di terze parti appartengono ai rispettivi proprietari.

Note legali di terze parti

In Sentinel 5 possono essere incluse le tecnologie di terze parti seguenti:

- Apache Axis e Apache Tomcat, Copyright © 1999-2005, Apache Software Foundation. Per ulteriori informazioni, esclusioni di garanzia e limitazioni, vedere http://www.apache.org/licenses/
- ANTLR. Per ulteriori informazioni, esclusioni di garanzia e limitazioni, vedere http://www.antlr.org
- Boost, Copyright © 1999, Boost.org.
- Bouncy Castle, Copyright © 2000-2004, the Legion of Bouncy Castle. Per ulteriori informazioni, esclusioni di garanzia e limitazioni, vedere http://www.bouncycastle.org.
- Checkpoint. Copyright © Check Point Software Technologies Ltd.
- Concurrent, pacchetto di utility. Copyright © Doug Lea. Utilizzato senza classi CopyOnWriteArrayList e ConcurrentReaderHashMap.
- Crypto++ Compilation. Copyright © 1995-2003, Wei Dai, con i materiali protetti da copyright seguenti: mars. cpp di Brian Gladman e Sean Woods. Per ulteriori informazioni, esclusioni di garanzia e limitazioni, vedere 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, concesso in licenza in base alla GNU Lesser General Public License. Per ulteriori informazioni, esclusioni di garanzia e limitazioni, vedere http://www.enterprisedt.com/products/edtftpj/purchase.html.
- Enhydra Shark, concesso in licenza in base alla Lesser General Public License disponibile all'indirizzo: 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/o Macrovision Europe Ltd.
- Java 2 Platform, Standard Edition. Copyright © Sun Microsystems, Inc. Per ulteriori informazioni, esclusioni di garanzia e limitazioni, visitare il sito Web all’indirizzo http://java.sun.com/j2se/1.4.2/j2re-1_4_2_10-license.txt (in lingua inglese).

  Java 2 Platform può inoltre includere i prodotti di terze parti seguenti:

  - CoolServlets © 1999
  - DES and 3xDES © 2000 by 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, marchio o marchio registrato di Bigelow e Holmes
- Taligent, Inc.
- IBM, alcuni componenti disponibili all'indirizzo: http://oss.software.ibm.com/icu4j/

Per ulteriori informazioni relative alle tecnologie di terze parti e le rispettive esclusioni di garanzia e limitazioni, vedere: http://java.sun.com/j2se/1.4.2/j2se-1_4_2-thirdpartylicensereadme.txt.

- JavaBeans Activation Framework (JAF). Copyright © Sun Microsystems, Inc. Per ulteriori informazioni, esclusioni di garanzia e limitazioni, visitare il sito Web all'indirizzo ://www.java.sun.com/products/javabeans/glasgow/jaf.htm (in lingua inglese) e fare clic sul collegamento per scaricare la licenza.
- JavaMail. Copyright © Sun Microsystems, Inc. Per ulteriori informazioni, esclusioni di garanzia e limitazioni, visitare il sito Web all'indirizzo ://www.java.sun.com/products/javabeans/glasgow/jaf.htm (in lingua inglese) e fare clic sul collegamento per scaricare la licenza.
- Java Ace, di Douglas C. Schmidt e il suo gruppo di ricerca presso la Washington University e Tao (con wrapper ACE) di Douglas C. Schmidt e il suo gruppo di ricerca presso la Washington University, University of California, Irvine e Vanderbilt University. Copyright © 1993-2005. Per ulteriori informazioni, esclusioni di garanzia e limitazioni, visitare i siti Web agli indirizzi http://www.cs.wustl.edu/~schmidt/ACE-copying.html e http://www.cs.wustl.edu/~pjain/java/ace/JACE-copying.html (in lingua inglese).
- Moduli Java Authentication e Authorization Service (JAAS), concessi in licenza in base alla Lesser General Public License. Per ulteriori informazioni, esclusioni di garanzia e limitazioni, vedere http://free.tagish.net/jaas/index.jsp.
- Java Network Launching Protocol (JNLP). Copyright © Sun Microsystems, Inc. Per ulteriori informazioni, esclusioni di garanzia e limitazioni, visitare il sito Web all'indirizzo ://www.java.sun.com/products/javabeans/glasgow/jaf.htm (in lingua inglese) e fare clic sul collegamento per scaricare la licenza.
- Java Service Wrapper. Componenti protetti da copyright come indicato di seguito: Copyright © 1999, 2004 Tanuki Software e Copyright © 2001 Silver Egg Technology. Per ulteriori informazioni, esclusioni di garanzia e limitazioni, vedere http://wrapper.tanukisoftware.org/doc/english/license.
- JIDE. Copyright © 2002-2005, JIDE Software, Inc.
- jTDS è concesso in licenza in base alla Lesser GNU Public License. Per ulteriori informazioni, esclusioni di garanzia e limitazioni, vedere http://jtds.sourceforge.net/.
- MDateSelector. Copyright © 2005, Martin Newstead, concesso in licenza in base a Lesser General Public License. Per ulteriori informazioni, esclusioni di garanzia e limitazioni, vedere http://web.ukonline.co.uk/mseries.
- Monarch Charts. Copyright © 2005, Singleton Labs.
- Net-SNMP. Parti di codice sono protette da copyright di diverse organizzazioni con tutti i diritti riservati. Copyright © 1989, 1991, 1992 di Carnegie Mellon University; Copyright © 1996, 1998-2000, the Regents of the University of California; Copyright © 2001-2003 Networks Associates Technology, Inc. ; Copyright © 2001-2003, Cambridge Broadband, Ltd. ; Copyright © 2003 Sun Microsystems, Inc. e Copyright © 2003-2004, Sparta, Inc. Per ulteriori informazioni, esclusioni di garanzia e limitazioni, visitare il sito Web all'indirizzo http://net-snmp.sourceforge.net (in lingua inglese).
- The OpenSSL Project. Copyright © 1998-2004. the Open SSL Project. Per ulteriori informazioni, esclusioni di garanzia e limitazioni, vedere http://www.openssl.org.
- Oracle Help for Java. Copyright © 1994-2006, Oracle Corporation.
- RoboHELP Office. Copyright © Adobe Systems Incorporated, precedentemente di Macromedia.
- Skin Look and Feel (SkinLF). Copyright © 2000-2006 L2FProd.com. Concesso in licenza in conformità ad Apache Software License. Per ulteriori informazioni, esclusioni di garanzia e limitazioni, vedere https://skinlf.dev.java.net/.
- Sonic Software Corporation. Copyright © 2003-2004. Il software SSC include software di sicurezza concesso in licenza da RSA Security, Inc.
- Tinyxml. Per ulteriori informazioni, esclusioni di garanzia e limitazioni, vedere http://grinninglizard.com/tinyxmldocs/index.html.

- SecurityNexus. Copyright © 2003-2006. SecurityNexus, LLC. Tutti i diritti riservati.
- Xalan e Xerces, entrambi concessi in licenza da Apache Software Foundation Copyright © 1999-2004. Per ulteriori informazioni, esclusioni di garanzia e limitazioni, visitare il sito Web all'indirizzo http://xml.apache.org/dist/LICENSE.txt (in lingua inglese).
- yWorks. Copyright © 2003-2006, yWorks.

NOTA: Al momento della pubblicazione della presente documentazione i collegamenti indicati sopra risultano attivi. Qualora i collegamenti risultassero non più validi o le relative pagine Web non più attive, contattare Security's Office of the Counsel at 404 Gallows Road, Vienna, VA 500. 703-852-8000.

Prefazione

La documentazione tecnica di Sentinel contiene informazioni generali sull'utilizzo e rappresenta una guida di riferimento. La presente documentazione è rivolta ai professionisti della protezione delle informazioni. Il testo contenuto nella presente documentazione è da considerarsi come documento di riferimento del sistema di gestione della protezione aziendale di Novell. Sul portale Web di Novell sono disponibili altri documenti.

La documentazione tecnica di Sentinel è suddivisa in cinque differenti volumi, ovvero:

- Volume I: Guida all'installazione di Sentinel™ 5
- Volume II: Guida dell'utente di Sentinel™ 5
- Volume III: Guida dell'utente di Sentinel™ 5
- Volume IV: Guida di riferimento dell'utente di Sentinel™
- Volume V: Guida all'integrazione con soluzioni di terze parti di Sentinel™

Volume I: Guida all'installazione di Sentinel 5

In questa guida viene descritto come installare i prodotti seguenti:

- Server Sentinel
- Console Sentinel
- Motore di correlazione di Sentinel
- Crystal Reports per Sentinel
- Generatore servizi di raccolta di Wizard
- Gestione servizi di raccolta di Wizard
- Advisor

Volume II: Guida dell'utente di Sentinel

In questa guida vengono descritti gli argomenti seguenti:

- Operazione della console Sentinel
- Funzioni di Sentinel
- Architettura di Sentinel
- Comunicazione di Sentinel
- Arresto/Avvio di Sentinel
- Valutazione delle vulnerabilità
- Monitoraggio degli eventi
- Filtro degli eventi
- Correlazione degli eventi
- Gestione dati Sentinel
- Configurazione eventi per rilevanza aziendale
- Servizio di mappatura
- Rapporti cronologici
- Gestione di host Wizard
- Casi
- Situazioni
- Gestione utenti
- Workflow

Volume III: Guida dell'utente di Wizard

In questa guida vengono descritti gli argomenti seguenti:

- Funzionamento di Generatore servizi di raccolta di Wizard
- Gestione servizi di raccolta di Wizard
- Servizi di raccolta
- Gestione di host Wizard
- Creazione e mantenimento di Servizi di raccolta

Volume IV: Guida di riferimento dell'utente di Sentinel

In questa guida vengono descritti gli argomenti seguenti:

- Linguaggio di script di Wizard
- Comandi di analisi sintattica di Wizard
- Funzioni dell'amministratore di Wizard
- Tag META di Wizard e Sentinel
- Autorizzazioni utente
- Motore di correlazione di Sentinel
- Opzioni della riga di comando di correlazione
- Schema database Sentinel

Volume V: Guida all'integrazione con soluzioni di terze parti di Sentinel

- Remedy
- HP OpenView Operations
- HP Service Desk

Sommario

1 Introduzione alla Guida di riferimento dell'utente di Sentinel™ 5

NOTA: Il termine agente è equivalente a servizio di raccolta. Si farà in seguito riferimento agli agenti come servizi di raccolta.

La Guida di riferimento dell'utente di Sentinel è il riferimento dell'utente per gli argomenti seguenti:

- Linguaggio di script di Wizard
- Comandi di analisi sintattica di Wizard
- Funzioni dell'amministratore di Wizard
- Tag META di Wizard e Sentinel
- Autorizzazioni utente della console Sentinel
- Motore di correlazione di Sentinel
- Opzioni della riga di comando di Sentinel
- Visualizzazioni database del server Sentinel

Questa guida presume che l'utente abbia familiarità con la sicurezza di rete, l'amministrazione dei database e i sistemi operativi UNIX.

Sommario

Questa guida contiene i capitoli seguenti:

Convenzioni utilizzate

Note e avvertenze

NOTA: le Note forniscono ulteriori informazioni che possono rivelarsi utili.

ATTENZIONE: le avvertenze forniscono ulteriori informazioni che possono essere utili per evitare danni al sistema o perdite di dati.

Comandi

I comandi sono visualizzati con il font courier. Ad esempio:

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

Altri riferimenti di Sentinel

Sono disponibili i manuali seguenti con i CD di installazione di Sentinel.

- Guida all'installazione di Sentinel™ 5
- Guida dell'utente di Sentinel™ 5
- Guida dell'utente di Sentinel™ 5 Wizard
- Guida di riferimento dell'utente di Sentinel™ 5
- Guida all'integrazione con soluzione di terze parti di Sentinel™5
- Note di rilascio

Come contattare Novell

- Sito Web: http://www.novell.com
- Supporto tecnico Novell: http://www.novell.com/support/index.html
- Supporto tecnico Novell internazionale: http://support.novell.com/phone.html?sourceidint=suplnav4_phonesup
- Supporto in autonomia: http://support.novell.com/support_options.html?sourceidint=suplnav_supportprog
- Per supporto 24x7, 800-858-4000

2 Linguaggio di script di Wizard

> **NOTA**: Il termine agente è equivalente a servizio di raccolta. Si farà in seguito riferimento agli agenti come servizi di raccolta.

Nel capitolo presente e nei capitoli successivi viene illustrato come utilizzare il linguaggio di script di Wizard per la creazione di script. Sono inoltre illustrati gli operatori delle varie stringhe e i comandi di analisi utilizzati nella creazione del Servizio di raccolta.

Sono illustrati gli argomenti seguenti:

Stringhe di decisione

Le stringhe prevedono la distinzione tra maiuscole e minuscole.

Durante il polling dei servizi di raccolta, vengono raccolte diverse informazioni nel buffer di ricezione interno. Le stringhe di tipo decisione specificano che verrà presa una decisione in relazione ai dati ricevuti e memorizzati nel buffer interno. Una stringa di decisione viene valutata come true o false. Se è presente un errore di sintassi o se la casella relativa al tipo di decisione è vuota, la decisione è false.

La stringa di decisione viene valutata solo se il tipo di decisione è impostato su stringa o dati.

Modifica del puntatore del buffer di ricezione

Ogni porta in Wizard dispone del proprio puntatore del buffer di ricezione. Il puntatore del buffer di ricezione fa riferimento a byte di dati nel buffer di ricezione. Prima di ogni stringa di decisione valutata, il puntatore del buffer di ricezione viene reimpostato sul valore di attesa, in genere zero, a meno che non venga modificato da una decisione in cui viene utilizzato l'operatore di ricerca (:).

- 0 non fa riferimento ad alcun byte del buffer di ricezione
- 1 fa riferimento al primo byte di dati, 2 al secondo byte di dati e così via

Formato

Una stringa di decisione ha il formato di una sequenza di operatori logici ed espressioni regolari.

Non è necessario che gli operatori logici e gli operatori delle stringhe siano presenti in ogni sequenza. Alcune regole relative al loro utilizzo sono:

- Gli operatori logici consentono di creare espressioni booleane (true o false) nelle stringhe di decisione e vengono valutati in base alla precedenza seguente:
  `~ Not`
  `& And`
- Un operatore di stringa specifica una stringa di caratteri da cercare nel buffer di ricezione. L'utilizzo dell'operatore delle stringhe consente di eseguire una ricerca byte per byte dalla posizione del puntatore del buffer di ricezione in avanti.

NOTA: Poiché il contenuto della casella relativa al tipo di decisione viene tagliato in corrispondenza dell'ultimo carattere stampabile, è necessario utilizzare l'equivalente esadecimale di uno spazio. L'operatore : non può essere utilizzato con l'operatore NULL.

Nomi dei parametri

Per specificare un parametro in una stringa di decisione, il nome del parametro deve essere racchiuso tra parentesi graffe ({ }). Quando viene creato lo script, il nome del parametro e le parentesi graffe vengono sostituite con il valore del parametro.

Se il nome del parametro specificato non esiste nel file di parametri dal quale viene creato lo script, l'espressione del nome del parametro e le parentesi graffe restano nei dati della stringa di decisione.

Le espressioni dei nomi dei parametri possono essere posizionate in qualsiasi punto della stringa di decisione. Non possono tuttavia essere nidificate (includendo un'altra espressione di nome di parametro in se stessa).

Gerarchia delle operazioni in una stringa di decisione

Ogni operazione in una stringa di decisione viene valutata come (1) o false (0). Le operazioni in una stringa di decisione sono sempre seguite nell'ordine indicato dalla sintassi dell'operatore logico.

- Quando viene utilizzata più di una operazione, le valutazioni della stringa vengono eseguite in ordine, da sinistra a destra.
- Quando vengono utilizzate le parentesi, viene valutato prima l'operatore logico in ogni serie di parentesi.
- Le successive operazioni logiche valutate sono not (~), e (&).

Viene inoltre seguito un ordine specifico di operazione quando si utilizza la sintassi dell'operatore di stringa:

- Viene valutato per primo il ripristino del puntatore del buffer di ricezione.
- Tutti gli altri caratteri della sintassi hanno la stessa precedenza e vengono valutati in ordine, da sinistra a destra.

Regole del puntatore del buffer di ricezione

Il puntatore del buffer di ricezione è gestito attraverso le regole seguenti:

- Quando la ricerca di una stringa di caratteri riesce, la ricerca è considerata true e il puntatore del buffer di ricezione è posizionato sul primo byte nella stringa trovata.

  Stringa di decisione: DE

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

- Quando la ricerca di una stringa di caratteri non riesce, la ricerca è considerata false e il puntatore del buffer di ricezione viene impostato sul valore di attesa.

  Stringa di decisione: DEJ

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

Ricerca di un buffer di ricezione vuoto

Per cercare un buffer di ricezione vuoto utilizzare la stringa di decisione seguente:

```
NULL
```

Esempio di valutazioni della stringa di decisione e dei risultati

Stringhe di decisione alfanumeriche

Le seguenti sono stringhe di decisione alfanumeriche per un buffer di ricezione di esempio:

```
ABCDEFGHIJKLMNO (line feed) YZ<[&
```

Stringa di decisione	Espressione logica	Risultato
A	1	1
P	0	0
\41\(valore esadecimale per A)	1	1
AB	1	1
\4142\(valore esadecimale per AB)	1	1
ABD	0	0
A&B	1 & 1	1
A&P	1 & 0	0
A+P	1 + 0	1
A\42\(valore esadecimale per 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\(valore esadecimale per avanzamento riga)	1	1
NULL *	0	0

Se nel buffer di ricezione non vengono trovati caratteri, il risultato è TRUE.

Stringhe di decisione esadecimali

Le seguenti sono stringhe di decisione esadecimali per un buffer di ricezione di esempio (HEX):

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

Stringa di decisione	Espressione logica	Risultato
\020A\&\FF\	1 & 1	1
\02\	0	0
\02\&\03\	1 & 1	1
\03\&\02\	1 & 0	0

Espressioni regolari

Nei modelli di scrittura per le espressioni regolari vengono utilizzati caratteri e sequenze di caratteri speciali.

Sentinel utilizza una libreria compatibile con POSIX (Portable Operating System Interface for UNIX) per le espressioni regolari. POSIX è il nome di un insieme di standard IEEE e ISO che contribuiscono ad assicurare la compatibilità fra una serie di sistemi operativi, tra cui la più ampia varietà di piattaforme UNIX.

Riepilogo dei caratteri speciali per le espressioni regolari

Nella tabella seguente sono riepilogati i caratteri speciali che è possibile utilizzare nelle espressioni regolari per le funzioni di ricerca e sostituzione.

Carattere	**Uso/Esempio**
\	Contrassegna il carattere successivo come speciale. n corrisponde al carattere "n." La sequenza \n corrisponde a un carattere di avanzamento riga o di nuova riga (fine riga), ma per passare "\" nell'analizzatore sintattico, è necessario farlo precedere dal carattere di eccezione "/"; quindi, per passare \n, è necessario utilizzare /\n.
^	Corrisponde all'inizio dell'input o della riga.
$	Corrisponde alla fine dell'input o della riga.
*	Corrisponde al carattere precedente zero o più volte: go* corrisponde a "g" o a "goo".
+	Corrisponde al carattere precedente una o più volte: go+ corrisponde a "goo" ma non a "g".
?	Corrisponde al carattere precedente zero o una volta: a?te? corrisponde a "te" in "eater".
.	Corrisponde a un carattere singolo con l'eccezione del carattere di nuova riga (fine riga).
x|y	Corrisponde a x o y. z|good? corrisponde a "goo" o "good" o "z".
{n}	n è un numero intero non negativo. Corrisponde esattamente a n volte. e{3} non corrisponde alla "e" in "Ted", ma corrisponde alle prime tre e in "greeeeeed".
{n,}	n è un numero intero non negativo. Corrisponde ad almeno n volte. e{3,} non corrisponde alla "e" in "Ted" e corrisponde a tutte le e in "greeeeeed". e{1,} equivale a e+.
{n,m}	m e n sono numeri interi non negativi. Corrisponde ad almeno n volte e al massimo a m volte. e{1,3} corrisponde alle prime tre e in "greeeeeed".
[xyz]	Una serie di caratteri. Corrisponde a uno dei caratteri racchiusi tra parentesi. [xyz] corrisponde alla "y" in "play".
[^xyz]	Una serie negativa di caratteri. Corrisponde a uno dei caratteri non racchiusi tra parentesi. [^xyz]/ corrisponde alla "v" in "vano".
[0-9]	Corrisponde a un carattere numerico.
[^0-9]	Corrisponde a un carattere non numerico.
[A-Za-z0-9_]	Corrisponde a un qualsiasi carattere, compreso il carattere di sottolineatura.
[^A-Za-z0-9_]	Corrisponde a un carattere non alfanumerico.
/n/	Corrisponde a n, dove n è un valore di escape ottale, esadecimale o decimale. Consente di incorporare codici ASCII in espressioni regolari.

Spazio vuoto nelle espressioni regolari

Nelle espressioni regolari, lo spazio vuoto è composto da uno o due spazi, che possono essere uno dei caratteri seguenti:

Nome simbolico	UCS	Descrizione
<tab>	<U0009>	CARATTERE DI TABULAZIONE (HT)
<ritorno a capo>	<U000D>	RITORNO A CAPO (CR)
<nuova riga>	<U000A>	AVANZAMENTO RIGA (LF)
<tabulazione verticale>	<U000B>	TABULAZIONE RIGA (VT)
<salto pagina>	<U000C>	SALTO PAGINA (FF)
<spazio>	<U0020>	SPAZIO

Comandi di analisi sintattica

Il linguaggio di analisi sintattica di Wizard è basato sulle funzioni. La maggior parte delle funzioni di analisi sintattica consente di modificare le variabili di Wizard e il relativo contenuto. Il linguaggio di analisi sintattica di Wizard supporta quattro tipi di variabili:

- Intere (il nome della variabile inizia con i)
- Mobili (Float, il nome della variabile inizia con f)
- Stringhe a lunghezza variabile (il nome della variabile inizia con un carattere diverso da i o f)
- Array di variabili (il nome della variabile finisce con [ ]). I tipi di variabili di array possono essere array di variabili intere, mobili o stringhe

Queste variabili sono locali per ogni porta di Wizard e non sono condivise su tutte le porte di Wizard. I comandi di analisi sintattica consentono di copiare dati dal buffer di ricezione in variabili stringa.

Il buffer di ricezione contiene i dati ricevuti dalla porta di comunicazione di Wizard, dalla porta del socket, dal file o dal processo.

La lunghezza dei byte da copiare, oltre alla posizione dalla quale copiare i byte, può essere controllata utilizzando i comandi di analisi sintattica seguenti:

- SEARCH()
- SKIP()
- SKIPWORD()
- NEGSEARCH()
- RESET()
- COPY()

I dati del buffer di ricezione possono essere aggiunti a una variabile stringa mediante il comando APPEND(). Il linguaggio di analisi sintattica di Wizard consente inoltre di copiare o aggiungere dati da variabili stringa in altre variabili stringa.

Tipi di dati semplici

di tipo numerico

I numeri possono essere preceduti solo da + o – nel caso del comando SKIP, SKIPWORD e SET. Ad esempio:

```
0, 10, 2.5
```

ivar (variabili intere)

Le variabili intere sono numeri con firma a 32 bit. Il nome della variabile deve iniziare con I o con i. Ad esempio:

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

La variabile intera i[55] è il 55° indice nell'array di interi i[]. L'indice in un array può anche essere una variabile intera.

fvar (variabili mobili)

Le variabili mobili sono numeri con virgola mobile a 32 bit. Il nome della variabile deve iniziare con F o con f. Ad esempio:

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

svar (variabili stringa)

Le variabili stringa contengono le stringhe di lunghezza delle variabili. I nomi delle variabili stringa non possono iniziare con I, i, F o f. Ad esempio:

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

array (array di variabili)

Gli array di variabili possono rappresentare array di variabili di tipo ivar, fvar e svar. Ad esempio:

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

Gli array possono essere indicizzati con qualsiasi indice numerico senza spreco di memoria. L'accesso a ivar[1000] non indica che la memoria sia allocata per 1.000 variabili intere.

Una variabile di array indicizzata viene considerata come qualsiasi altra variabile (ivar, svar e fvar)

La seguente sarebbe ad esempio la sintassi corretta per il comando POPUP:

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

Dati tra virgolette

I dati racchiusi tra virgolette sono sottoposti a scansione e analizzati nel modo seguente:

- /= Carattere di eccezione: include i byte che seguono / indipendentemente da significati speciali; per utilizzare uno dei caratteri speciali della stringa, è necessario inserire / prima del carattere. corp/\router è utilizzato ad esempio per corp\router
- \xx x xx\= Dati di tipo esadecimale (uno o due caratteri per byte): \0ad\, \0a0d\, \a d\,\0a 0d\, and \0a d\ all mean line feed/carriage return

Tutti gli altri caratteri sono specificati direttamente.

Tipi di dati derivati aggregati

Nella tabella seguente sono elencati i tipi di dati derivati aggregati:

Tipo	Descrizione
tutti	numero, ivar, fvar, svar, virgolette
di tipo numerico	numero, ivar, fvar, ivar[index], fvar[index]
stringa	svar, svar[index], virgolette

Tipo	Descrizione
variabile	ivar, fvar, svar, ivar[index], fvar[index], svar[index]
variabile numerica	ivar, fvar, ivar[index], fvar[index]
matrice	ivar[], fvar[], svar[]
matrice di variabili numeriche	ivar[], fvar[]
array di variabili stringa	svar[]

Regole speciali per le variabili

Le seguenti sono regole speciali per le variabili.

- I nomi delle variabili prevedono la distinzione tra maiuscole e minuscole.
- Quando si utilizza una variabile numvar per la prima volta, tranne in casi in cui il relativo valore deve essere impostato, la variabile è impostata su zero
- Quando si utilizza una variabile svar per la prima volta, tranne in casi in cui il relativo valore deve essere impostato, la variabile è impostata su null ("")
- Un array indicizzato viene considerato come qualsiasi altra variabile del relativo tipo, ivar, fvar o svar
- Per contrassegnare come commento uno o più comandi di analisi sintattica, o per inserire commenti nel testo dell'analisi, racchiudere i commenti tra /* */

Ad esempio:

```
/* questo è un commento */
/* questi sono comandi di analisi commentati
COPY(s: "test")
DISPLAY()
*/
```

3 Comandi di analisi sintattica di Wizard

NOTA: Il termine agente è equivalente a servizio di raccolta. Si farà in seguito riferimento agli agenti come servizi di raccolta**.**

In questo capitolo vengono elencati in ordine alfabetico i comandi di analisi sintattica utilizzati per la generazione dei servizi di raccolta. Di seguito è disponibile un elenco dei comandi di analisi sintattica in base alla funzione.

Funzione	**Comando di analisi sintattica**
Interazione con database	DBCLOSE DBDELETE DBGETROW DBINSERT DBOPEN DBSELECT
Debug	BREAKPOINT DISPLAY POPUP
Interazione con file	FILEA FILEL FILER FILEW

Operazioni logiche	COMPARE
	ELSE
	ENDFOR
	ENDIF
	ENDWHILE
	FOR
	IF
	LOOKUP
	WHILE

Interazione con rete	SOCKETW
Notifica	ALERT CLEARTAGS CONSTANTTAGS EVENT INDICATOR PAUSE

Funzione	Comando di analisi sintattica
Manipolazione dati non elaborati	BITFIELD BYTEFIELD CONVERT CRC DECODE DECODEMIME ENCODE ENCODEMIME HEXTONUM NUMTOHEX SETBYTES STRIP STRIP-ASCII-RANGE
Manipolazione di stringhe	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
Utility	DATE DATETIME PAUSE SHELL TBOSSETCOMMAND TBOSSETREQUEST TIME

Funzione	Comando di analisi sintattica
Gestione variabili	CLEAR DELETE GETCONFIG GETENV INC RESET RXBUFF SET SETCONFIG
Scansione vulnerabilità	INFO_CLEARTAGS INFO_CLOSE INFO_CONSTANTTAGS INFO_CREATE INFO_DUMP INFO_PUSH INFO_SEND INFO_SETTAG

Formato dei comandi e utilizzo di matrici

I formati dei comandi di analisi sintattica utilizzano determinati simboli per esprimere specifici significati. Di seguito sono disponibili alcuni esempi di tali simboli:

Esempio di simbolo utilizzato	Esempio di significato del simbolo
`[parameter]`	Le parentesi quadre indicano parametri facoltativi.
`<parameter>`	Le parentesi angolari indicano parametri che devono essere forniti dall'utente.
`a`	La lettera a deve essere digitata in questa posizione
`a|b`	Viene utilizzata a o b ma non entrambe
`<item> ::= <definition>`	item può essere sostituito da definition

`<varList>`
dove:
`<varList> ::= var [, <varList>]`
	Utilizzato per definizioni ricorsive per scrivere un elenco di variabili di cui almeno una obbligatoria

`...`	È consentito ripetere il parametro precedente.
`/`	La barra viene utilizzata come carattere di escape per consentire l'utilizzo di caratteri speciali, quali la barra rovesciata.

Le matrici sono consentite nelle espressioni, ad esempio:

Dato	Equivalente
`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]]`

Comandi

ALERT

Il comando ALERT inoltra messaggi sugli eventi a Sentinel.

- Il primo parametro obbligatorio definisce il nome della risorsa
- Il secondo parametro obbligatorio definisce il testo del messaggio sull'evento
- Il terzo parametro obbligatorio definisce la gravità dell'evento
- La data e l'ora del messaggio di evento possono essere definite come parametri facoltativi
  - Il parametro della data può essere utilizzato autonomamente
  - Il parametro dell'ora deve trovarsi combinato con il parametro data

Formato

```
ALERT(risorsa, messaggio, gravità)
```

oppure

```
ALERT(risorsa, messaggio, gravità[, data[, ora]]))
```

Non è possibile utilizzare il parametro ora se non in combinazione con il parametro della data.

NOTA: Utilizzare il comando STONUM per convertire la gravità da stringa a numero intero**.**

Tipi di dati

Argomento	Tipo	Descrizione
risorsa	stringa (INPUT)	La risorsa ed eventualmente la sottorisorsa a cui inviare un evento (ad esempio: xterm:tcp_retransmits).
stringa messaggio	(INPUT)	Il testo del messaggio relativo all'evento.
gravità	di tipo numerico (INPUT)	La rappresentazione numerica della priorità del messaggio di evento (0 -5). 0 = informativo 1 = indicazione 2 = avviso 3 = poco importante 4 = molto importante 5 = critico
stringa data	(INPUT) [FACOLTATIVO]	Imposta la data del messaggio di evento nel formato MM-GG-AAAA (ad esempio: “12-01-2002”) (default = data attuale).
stringa ora	(INPUT) [FACOLTATIVO]	Imposta l'ora del messaggio di evento nel formato HH:MM:SS (ad esempio: “15:14:34”) (default = ora corrente); deve essere utilizzato con il parametro della data.

Ad esempio:

```
ALERT("xterm:tcp_retransmits", mesg_txt,ivar[3])
ALERT("router_subnet_15", msg_txt, "c")
```

```
ALERT(resource, "Server not responding", iseverity)
ALERT("Mux184:card1", "C1 not funct. properly.", 4)
ALERT("Firewall", "Connection lost to Firewall.", 5)
ALERT("CB5", "Channel Bank 5 being serviced", "Maint")
ALERT(resource, message, isev, thedate, thetime)
ALERT("Switch3", oos_msg, 5, "07-30-1997", "07:03:23")
```

APPEND

Il comando APPEND aggiunge dati dal buffer di ricezione, una variabile di tipo stringa, una stringa o una stringa tra virgolette a una variabile stringa. Valgono le indicazioni seguenti:

- Tutti i parametri di APPEND sono facoltativi ad eccezione di quello della destinazione
- La destinazione dei dati (variabile stringa) può essere specificata con i parametri di APPEND
- È possibile specificare un offset nell'origine per controllare la posizione in cui i dati vengono copiati
- Il numero di byte da aggiungere alla variabile di destinazione può essere specificato con il parametro di lunghezza (ilen) oppure la lunghezza corrisponderà per default a quella dei dati di origine
- Oltre all'impostazione di un parametro di lunghezza numerico, è possibile utilizzare una stringa per definire la lunghezza
- Se si utilizza una stringa come parametro di lunghezza, il parametro di origine deve essere il buffer di ricezione oppure di tipo svar
- Se si utilizza una stringa come parametro di lunghezza, il motore del servizio di raccolta aggiunge i byte dei dati di origine (a partire dall'offset indicato) nella variabile di destinazione fino al primo carattere della stringa (se presente) escluso. Se la stringa non viene trovata, i byte non vengono aggiunti
- Se i parametri di offset e lunghezza sono esterni all'intervallo della variabile di origine, vengono aggiunti più byte possibile, fino alla fine dei dati di origine
- Se l'offset è maggiore o uguale alla lunghezza dei dati di origine, non vengono aggiunti byte alla variabile di destinazione. Se non viene specificato alcun offset, quest'ultimo verrà impostato per default su 0)

Formato

```
APPEND(<dest>: [source] [, [search] [, [ilen] [,
   [ioffset] ]]])
APPEND(<dest>: [source] [, [ilen] [, [ioffset] ]])
APPEND(<dest>: [ilen] [, [offset]])
```

Tipo di dati

Argomento	Tipo	Descrizione
dest	svar (OUTPUT)	La variabile della stringa di dati a cui aggiungere i byte.
source	stringa (INPUT)	La stringa in cui si trovano i byte da aggiungere che verranno aggiunti alla

Argomento	Tipo	Descrizione
	[FACOLTATIVO] oppure svar	stringa di destinazione. (default = buffer di ricezione) Se viene utilizzato il parametro search.
search	stringa (INPUT) [FACOLTATIVO]	Stringa utilizzata per specificare: copiare fino ai byte da ricercare nella stringa di origine.
ilen	di tipo numerico (INPUT) [FACOLTATIVO]	Il numero di byte dell'origine da aggiungere alla destinazione.
ioffset	di tipo numerico (INPUT) [FACOLTATIVO]	L'offset da considerare nell'origine in corrispondenza del quale iniziare l'aggiunta dei dati.

Negli esempi seguenti vengono aggiunti byte del buffer di ricezione a una svar di destinazione (dest). Il puntatore del buffer di ricezione viene aggiunto al valore di offset per specificare la posizione iniziale di aggiunta dei dati. Il simbolo ^ indica la posizione del puntatore del buffer di ricezione.

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

L'esempio illustrato sopra si base sui presupposti seguenti.

```
rxbuff="buffer di ricezione"
^ (posizione del puntatore del buffer di ricezione)
dest="stringa di destinazione"
source="Stringa di origine"
ilen=3
ioffset=3
```

Immettere quanto segue:

```
APPEND(dest:)
```

Risultato:

```
dest = "Buffer di ricezione stringa di destinazione"
```

Oppure se è stato immesso:

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

Risultato:

```
dest = "stringa di destinazione"
```

Oppure se è stato immesso:

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

Risultato:

```
dest = "Buffer di ricezione stringa di destinazione"
```

Negli esempi seguenti vengono aggiunti byte del buffer di ricezione fino alla stringa di ricerca esclusa a una svar di destinazione (dest). Se la stringa di ricerca non si trova nel buffer di ricezione (dopo la posizione del puntatore del buffer di ricezione + offset), non viene aggiunto alcun byte.

Immettere quanto segue:

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

Risultato:

```
dest = "stringa di destinazione"
```

Immettere quanto segue:

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

Risultato:

```
dest = "stringa di destinazione"
```

Negli esempi seguenti viene aggiunta una sottostringa del buffer di ricezione in base ai presupposti seguenti:

```
Buffer di ricezione = "Minor Alarm Firewall A"
```

Immettere quanto segue:

```
COPY(message:"Resource Name is: ")
APPEND(message:,6)
```

Risultato:

```
message = "Resource Name is: Alarm Firewall A"
```

BITFIELD

Il comando BITFIELD converte i byte in bit. Questo comando converte ogni byte in una stringa di lunghezza arbitraria in 8 bit (0 o 1) inserendoli in una matrice numero intero, una matrice decimale o una stringa.

ATTENZIONE: L'output è 8 volte maggiore dell'input, quindi il comando BITFIELD può determinare un eccessivo utilizzo della memoria, se utilizzato in modo inappropriato. Ad esempio, se si utilizzano stringhe di input contenenti un numero elevato di byte**.**

Formato

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

Tipi di dati

Argomento	Tipo	Descrizione
s_bytes	stringa (INPUT)	Qualsiasi numero di byte ASCII o esadecimali in una stringa.
dest_var	matrice di variabili numeriche (OUTPUT)	Matrice di numeri interi (impostata su 0 o 1). Il numero di bit corrisponde al numero di byte in s_bytes per 8 volte. Per ogni gruppo di 8 bit i bit vengono inseriti dal più significativo (MSB, Most Significant Bit) al meno significativo (LSB, Least Significant Bit). Ad esempio: idest_var[0] = MSB del byte 1 idest_var[1] = Successivo MSB del byte 1 idest_var[2] = Successivo MSB del byte 1 idest_var[3] = Successivo MSB del byte 1 idest_var[4] = Successivo MSB del byte 1 idest_var[5] = Successivo MSB del byte 1 idest_var[6] = Successivo MSB del byte 1 idest_var[7] = LSB di Byte 1 idest_var[8] = MSB del byte 2 idest_var[9] = Successivo MSB del byte 2 ... idest_var[n * 8 - 1] = LSB di Byte n Stringa che contiene un multiplo di 8 byte in cui ognuno di essi rappresenta un bit nei byte di output. I byte in questa stringa vengono sempre impostati su ASCII 0 o 1.
	Oppure svar (OUTPUT)	Per ogni 8 bit consecutivi rappresentati in ogni stringa, i valori ASCII (0 e 1) sono inseriti dallo MSB allo LSB. Ad esempio: Se s_bytes = “\5AFE\” Allora, dest_var= "0101101011111110"

NOTA: Il secondo parametro di BITFIELD (dest_var) deve essere una stringa (ad esempio, ivar[] o fvar[])**.**

Ad esempio:

```
BITFIELD("\00\", f_bit_array[])
BITFIELD(s_bytes, i_bit_array[])
BITFIELD(s_byte, string_out)
BITFIELD("This will work", i_bit_array[])
BITFIELD("\563F\", string_out)
```

Nell'esempio seguente, i byte della stringa sono impostati su un byte esadecimale e inviati al comando BITFIELD due volte (una volta per una matrice numero intero e una volta per una stringa).

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

Contenuto delle variabili di output correnti

```
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

Il comando BREAKPOINT interrompe l'esecuzione di uno script di analisi. Quando il debugger di script di Wizard è in esecuzione, il comando BREAKPOINT interrompe l'analisi in attesa dell'intervanto dell'utente. Ad esempio, nel pannello del debugger di Wizard, la selezione degli appositi pulsanti per riprendere il processo di debug.

Formato

```
BREAKPOINT()
```

BYTEFIELD

Il comando BYTEFIELD recupera una rappresentazione di byte in bit (0 or 1) e inserisce i byte in una variabile stringa.

L'input può risultare:

- stringa
- matrice numero intero
- matrice float

L'output è sempre una variabile stringa.

Formato

ATTENZIONE: Se il primo parametro è una matrice numero intero o float, non utilizzare valori maggiori di 100 per i_num_bytes, poiché la matrice verrà inizializzata sul numero di voci corrispondente, il che determina un eccessivo utilizzo di memoria.

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

NOTA: Il primo parametro di BYTEFIELD (`source_var`) deve essere svar, ivar[] o fvar[].

Tipi di dati

Argomento	Tipo	Descrizione
source_var	matrice di variabili numeriche (INPUT)	Matrice di numeri interi (impostata su 0 o 1). Il numero di bit corrisponde al numero di byte in s_bytes per 8 volte. Per ogni gruppo di 8 bit, i bit vengono inseriti dal più significativo (MSB, Most Significant Bit) al meno significativo (Least Significant Bit). Vedere gli esempi sotto questa tabella.
	svar (INPUT)	Stringa contenente un multiplo di 8 byte in cui ogni byte rappresenta un bit dei byte di input. I byte nella stringa devono essere sempre impostati su un valore ASCII 0 o 1. Per ogni 8 bit consecutivi rappresentati in ogni stringa, i valori ASCII (0 e 1) devono essere inseriti da MSB a LSB. Ad esempio: Se source_var = "0101101011111110", and i_num_bytes = 2, Allora, Se s_bytes = “\5AFE\”
s_bytes	stringa (OUTPUT)	Qualsiasi numero di byte ASCII o esadecimali in una stringa.
i_num_bytes	di tipo numerico (INPUT) [FACOLTATIVO]	Il numero di byte da inserire in _bytes. Poiché è facoltativo, il valore di default è 1 a meno che non venga utilizzato quando l'input è di tipo stringa. Se l'input è di tipo stringa, il valore di default corrisponde alle dimensioni della stringa diviso 8.

Esempi specifici relativi a source_var sono:

```
ISOURCE_VAR[0] = MSB del byte 1
ISOURCE_VAR[1] = Successivo MSB del byte 1
ISOURCE_VAR[2] = Successivo MSB del byte 1
ISOURCE_VAR[3] = Successivo MSB del byte 1
ISOURCE_VAR[4] = Successivo MSB del byte 1
ISOURCE_VAR[5] = Successivo MSB del byte 1
ISOURCE_VAR[6] = Successivo MSB del byte 1
ISOURCE_VAR[7] = LSB di Byte 1
ISOURCE_VAR[8] = MSB del byte 2
ISOURCE_VAR[9] = Successivo MSB del byte 2
...
```

```
ISOURCE_VAR[n * 8 - 1] = LSB di Byte n
```

Alcuni esempi di 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)
```

Nell'esempio seguente, la stringa, sbyte e la matrice numero intero ivar sono impostati su una rappresentazione di bit di un byte esadecimale e inviati al comando BITFIELD due volte (una volta per l'input della matrice numero intero e una volta per l'input di stringa).

```
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)
```

Contenuto delle variabili di output attuali:

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

CLEAR

Il comando CLEAR tronca le variabili stringa a byte zero o imposta variabili numero intero e float su zero. In un comando CLEAR possono essere specificate fino a 100 variabili.

Formato

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

Dove:

```
varlist ::= var [, <varlist>]
Var ::= variabile da cancellare (fvar, ivar o svar)
```

Numero massimo di variabili: 100

Tipi di dati

Argomento	Tipo	Descrizione
var1	variabile (INPUT/ OUTPUT)	Variabile da cancellare (fvar, ivar o svar).
var2	variabile (INPUT/ OUTPUT) [FACOLTATIVO]	Variabile da cancellare (fvar, ivar o svar).
var3	variabile (INPUT/ OUTPUT) [FACOLTATIVO]	Variabile da cancellare (fvar, ivar o svar).
...	variabile (INPUT/ OUTPUT) [FACOLTATIVO]	Altre variabili per CLEAR (fvar, ivar o svar).

Ad esempio:

```
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)
```

Negli esempi seguenti, I valori vengono assegnati alle variabili stringa, le quali vengono quindi utilizzate in un messaggio di evento e i suoi valori vengono cancellati.

```
COPY(res_var: "Firewall")
COPY(msg_var: "Firewall 116 Minor Alarm")
ALERT(res_var, msg_var, 4)
CLEAR(res_var, msg_var)
RISULTATO:
res_var = ""
msg_var = ""
```

CLEARTAGS

Il comando CLEARTAGS esegue un'operazione di cancellazione su tutte le variabili di tipo data e ora e riservate degli eventi protette mediante il comando CONSTANTTAGS.

È consigliabile chiamare questo comando nello stato di inizializzazione (stato 4 nel modello standard di Sentinel) del servizio di raccolta prima che qualsiasi input sia analizzato nelle variabili riservate.

Il comando CLEARTAGS funziona sulle variabili riservate degli eventi e sulle variabili riservate di date e ora. Il comando CLEARTAGS non ha parametri. Le variabili stringhe sono impostate su una stringa vuota "", ad esempio:

```
s_EVT and s_Sec.
```

La variabile numero intero i_Severity è impostata su zero.

Formato

```
CLEARTAGS ()
```

Ad esempio:

```
SET(i_Severity = 3)
COPY(s_BM:"Base Message")
COPY(s_Example:"Test")
CLEARTAGS ()
```

Risultato:

```
i_Severity = 0
s_BM = ""
s_Example = "Test"
```

NOTA: S_Example non è una variabile riservata di data e ora o di evento, pertanto non viene cancellata.

COMMENT

Questo comando ha un argomento facoltativo di tipo stringa. Si tratta di un metodo per immettere i commenti nel file del modello del servizio di raccolta. Ciò consente di immettere commenti dall'editor visivo senza passare all'editor di testo.

Formato

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

Ad esempio:

```
/* COLLECTOR INFORMATION
; ------------------------------------------------
Collector_Name:              Modello standard
Collector_Description:       Modello su cui basare i nuovi
   servizi di raccolta di Wizard
Collector_Manufacturer:      N/D
Collector_Product/Version:   N/D
Collector_Version:           versione 4.1
```

```
Collector_Date:                 Agosto 2003
; ------------------------------------------------*/
```

COMPARE

Il comando COMPARE esamina due argomenti e imposta una variabile a seconda del risultato. Il risultato del confronto di valori di tipo stringa e numerico può essere memorizzato in una variabile. Se la variabile è di tipo ivar, fvar o stringa conterrà il valore -1, 0 o 1.

- -1 viene utilizzato se arg1 è minore di arg2
- 0 viene utilizzato se arg1 è uguale a arg2
- 1 viene utilizzato se arg1 è maggiore di arg2

Formato

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

Tipi di dati

Argomento	Tipo	Descrizione
arg1	tutti (INPUT)	Dati Compare 1. Deve essere una stringa o un numero.
arg2	tutti (INPUT)	Dati Compare 2. Deve essere lo stesso di topo di Compare data 1.
dest	variabile (OUTPUT)	La variabile in cui verranno inseriti i risultati del confronto: svar = “-1”, “0” o “1” ivar = -1, 0 o 1 fvar = -1.0, 0.0 o 1.0

NOTA: I tipi di arg1 e arg2 devono essere entrambi di tipo stringa o numerico**.**

Ad esempio:

```
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])
```

Nell'esempio seguente, il testo viene confrontato con i contenuti di una variabile stringa e il risultato del confronto viene memorizzato in una variabile numero intero. Viene generato un evento se il testo non corrisponde al valore della variabile stringa.

```
COMPARE(s_data_var, "ALARM", i_compare_var)
IF(i_compare_var = 0)
ALERT(res_var, "Major ALARM", 5)
ENDIF()
```

NOTA: I comandi IF( ),ELSE( ) e ENDIF( ) eseguono la stessa funzione del comando COMPARE, ad eccezione del confronto di numeri negativi**.**

CONSTANTTAGS

Il comando CONSTANTTAGS utilizza un numero variabile di parametri di nomi di variabili riservate (evento e data/ora). Dichiarando una costante di variabile riservata, la variabile viene protetta dalla cancellazione mediante una chiamata al comando CLEARTAGS.

Un esempio di tale variabile è s_PN, contenente il nome del prodotto in elaborazione da parte del servizio di raccolta. La variabile s_PN deve essere dichiarata costante e imposta una volta nello stato di configurazione del servizio di raccolta.

È consigliabile chiamare questo comando nello stato di configurazione del servizio di raccolta (stato 1 nel modello standard 4.1) per le variabili riservate che non cambiano durante l'elaborazione degli eventi da parte del servizio di raccolta.

Il comando CONSTANTTAGS funziona sulle variabili riservate degli eventi e sulle variabili riservate di date e ora.

Formato

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

Tipi di dati

Argomento	Tipo	Descrizione
reserved_variable		L'elenco di variabili riservate che verranno impostate come costanti e non cancellate dal comando CLEARTAGS.

Ad esempio:

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

Risultato:

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

Delle tre variabili riservate di evento, s_BM non viene protetta da CLEARTAGS mediante CONSTANTTAGS e viene pertanto cancellata.

CONVERT

Il comando CONVERT trasforma un stringa di input di tipo binario, ottale, decimale, esadecimale o raw in una variabile stringa di output di tipo binario, ottale, decimale, esadecimale o raw.

Formato

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

Tipi di dati

Argomento	Tipo	Descrizione
string_in	Stringa (INPUT)	Stringa di input da convertire.
type_in	Elenco di selezione Stringa Variabile di tipo stringa (INPUT)	Il tipo della stringa di input (string_in): Binario = “B” o “b” Ottale = “O” o “o” Decimale = “D” o “d” Esadecimale = “H” o “h” Non elaborato = “R” o “r”
svar_out	svar (OUTPUT)	La variabile stringa contenente i dati della stringa da convertire.
type_out	Elenco di selezione Stringa Variabile di tipo stringa (INPUT)	Il tipo in cui convertire i dati (la stringa convertita verrà inserita in svar_out): Binario = “B” o “b” Ottale = “O” o “o” Decimale = “D” o “d” Esadecimale = “H” o “h” Non elaborato = “R” o “r”

Ad esempio:

```
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(data, "r", sdecimal, "d")
CONVERT(data, "o", shex, "H")
```

Nell'esempio seguente, il comando CONVERT viene chiamato per eseguire varie conversioni.

```
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")
```

I contenuti delle variabili di output attuali sono:

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

COPY

Il comando COPY duplica i dati dal buffer di ricezione o dalla stringa di origine, inserendoli in una variabile stringa o in una stringa tra virgolette per una variabile stringa. Il puntatore del buffer di ricezione non cambia quando si utilizza questo comando.

La destinazione dei dati (svar) può essere specificata con i parametri di COPY.

> **NOTA:** Nell'editor visuale del Generatore servizi di raccolta, COPY, COPY-FROM-RX-BUFF-UNTIL-SEARCH, COPY-FROM-RX-BUFF, COPY-FROM-STRING-TO-STRING-UNTIL-SEARCH and COPY-STRING-TO-STRING vengono elencati comandi separati. Corrispondono allo stesso comando. Vengono forniti come descrizioni delle diverse variazioni dello stesso comando. Per utilizzare eventuali variazioni del comando COPY nell'editor di testo, occorre immettere COPY.

Quando si utilizza questo comando:

- È possibile specificare un offset nell'origine per controllare la posizione in cui i dati vengono copiati dai dati di origine.
- Il numero di byte da copiare alla variabile di destinazione può essere specificato con il parametro di lunghezza (ilen) oppure la lunghezza può corrispondere per default a quella dei dati di origine
- Oltre all'impostazione di un parametro di lunghezza numerico, è possibile utilizzare una stringa. Se si utilizza una stringa, il motore del servizio di raccolta copia i byte dai dati di origine (a partire dall'offset indicato) nella variabile di destinazione fino al primo carattere della stringa (se presente). Se la stringa non viene trovata, i byte non vengono copiati.
- Se i parametri di offset (ioffset) o lunghezza (ilen) sono esterni all'intervallo della variabile di origine, vengono copiati più byte possibile, fino alla fine dei dati di origine.

  Se l'offset è maggiore o uguale alla lunghezza dei dati di origine, nella variabile di destinazione non verrà copiato alcun byte.

  Se non viene specificato alcun offset, il valore di quest'ultimo viene impostato su zero per default.

Formato

```
COPY(<dest>: [source] [, [search] [, [ilen] [,
   [ioffset] ]]])
COPY(<dest>: [source] [, [ilen] [, [ioffset] ]])
COPY(<dest>: [ilen] [, [offset]])
```

Tipi di dati

Argomento	Tipo	Descrizione
dest	svar (OUTPUT)	La variabile della stringa di dati in cui copiare i byte.

Argomento	Tipo	Descrizione
stringa di origine	(INPUT) [FACOLTATIVO] Oppure svar	La stringa da cui vengono copiati i byte (default = buffer di ricezione). Se viene utilizzato il parametro search.
search	stringa (INPUT) [FACOLTATIVO]	Stringa utilizzata per specificare: copiare fino ai byte da ricercare nella stringa di origine.
ilen	di tipo numerico (INPUT) [FACOLTATIVO]	Il numero di byte dell'origine da copiare nella destinazione.
ioffset	di tipo numerico (INPUT) [FACOLTATIVO]	L'offset nell'origine in corrispondenza del quale iniziare la copia dei dati, copia tutti i caratteri dal buffer di ricezione a quello di trasmissione.

Negli esempi seguenti vengono copiati byte del buffer di ricezione a una svar di destinazione (dest). Il puntatore del buffer di ricezione viene aggiunto al valore di offset per specificare la posizione iniziale di copia dei dati. Il simbolo ^ indica la posizione del puntatore del buffer di ricezione.

Si presuppone quanto segue:

```
rxbuff="buffer di ricezione"
^ (posizione del puntatore del buffer di ricezione)
dest=""
source="Stringa di origine"
ilen=3
ioffset=3
```

Comando	Risultato
`COPY(dest:)`	`dest = "receive buffer"`
`COPY(dest:5)`	`dest = "recei"`
`COPY(dest:0.5)`	`dest = "ve buffer"`

Negli esempi seguenti vengono copiati byte di una stringa di origine in una svar di destinazione (dest).

Comando	Risultato
`COPY(dest:source)`	`dest = "stringa di origine"`
`COPY(dest:source,5)`	`dest = "sou"`
`COPY(dest:source,5,6)`	`dest = "ce st"`

Negli esempi seguenti vengono copiati byte del buffer di ricezione fino alla stringa di ricerca esclusa in una variabile stringa. Se la stringa di ricerca non si trova nel buffer di ricezione (dopo la posizione del puntatore del buffer di ricezione + offset), non viene copiato alcun byte.

NOTA: per la sostituzione esadecimale, \0000\ termina una stringa. Pertanto, “xxxx\0000\yyyy” diventa “xxxx”.

Negli esempi seguenti vengono copiati byte del buffer di ricezione fino alla stringa di ricerca esclusa a una svar di destinazione (dest). Se la stringa di ricerca non si trova nel buffer di ricezione (dopo la posizione del puntatore del buffer di ricezione + offset), non viene copiato alcun byte.

Comando	Risultato
COPY(dest:,"buffer")	dest = "receive "
COPY(dest:,"receive")	dest = ""

Negli esempi seguenti vengono copiati byte di una stringa di origine (deve essere una variabile stringa) fino alla stringa di ricerca esclusa in una variabile stringa di destinazione (dest). Se la stringa di ricerca non si trova nel buffer di ricezione (dopo la posizione del puntatore del buffer di ricezione + offset), non viene copiato alcun byte.

Comando	Risultato
COPY(dest:source," string")	dest = "origine"
COPY(dest:source," string")	dest = ""

CRC

Il comando CRC calcola un controllo di ridondanza ciclica in una stringa di byte esadecimale o ASCII.

Formato

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

Tipo di dati

Argomento	Tipo	Descrizione
source_data	stringa (INPUT)	I dati della stringa su cui eseguire il comando CRC.
dest_crc	svar (OUTPUT)	La variabile stringa in cui il risultato a 2 byte di CRC viene memorizzato.

Ad esempio:

Nell'esempio seguente, il valore calcolato di CRC viene confrontato a un valore salvato. Se i due valori di CRC sono identici, viene generato un messaggio di evento.

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

NOTA: Per la sostituzione esadecimale, \0000\ termina una stringa; quindi, “xxxx\0000\yyyy” diventa “xxxx”.

DATE

Il comando DATE copia la data corrente nel formato MM-GG-AAAA in una variabile stringa. Può inoltre copiare il giorno corrente della settimana in una variabile di tipo stringa, numero intero o float.

Formato

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

Tipo di dati

Argomento	Tipo	Descrizione
date_string	svar (OUTPUT)	Variabile di tipo stringa in cui verrà memorizzata la data (ad esempio: svar = “11-18-2002”).
day_of_week	svar (OUTPUT) [FACOLTATIVO] ivar (OUTPUT) [FACOLTATIVO] Oppure fvar (OUTPUT) [FACOLTATIVO]	(Facoltativamente) Variabile di tipo stringa in cui verrà memorizzato il giorno della settimana; scritto nel formato nome giorno completo (ad esempio: svar = Sabato) (Facoltativamente) Variabile di tipo stringa o float in cui verrà memorizzato il giorno della settimana; scritto nel formato nome giorno completo nome = numero: Lunedì = 1 Martedì = 2 Mercoledì = 3 Giovedì = 4 Venerdì = 5 Sabato = 6 Domenica = 7 (ad esempio: lunedì corrisponde a ivar = 1)

Ad esempio:

Nell'esempio seguente, la data del sistema viene confrontata con una stringa di dati. Se le due date sono identiche, viene generato un messaggio di evento.

```
DATE(date_var, day_of_week)
IF(date_var = "11-18-2002")
ALERT(res, "Happy 23rd birthday!", 0)
ENDIF()
IF(day_of_week = "Saturday")
ALERT(res, "Time to go to the beach," 0)
ENDIF()
```

DATETIME

Il comando DATETIME converte una rappresentazione di tipo numero intero del numero di secondi trascorso dalla data 1 gennaio 1970 fino alle variabili stringa di data e ora. Può inoltre copiare il giorno corrente della settimana in una variabile di tipo stringa, numero intero o float.

Formato

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

Tipi di dati

Argomento	Tipo	Descrizione
itime_secs	di tipo numerico (INPUT)	Il numero intero contenente il numero di secondi trascorsi dal 1970.
svar_date	svar (OUTPUT)	Variabile di tipo stringa in cui verrà memorizzata la data (ad esempio: 02-19-96).
svar_time	svar (OUTPUT)	Variabile di tipo stringa in cui verrà memorizzata l'ora (ad esempio: 15:14:33).
day_of_week	svar (OUTPUT) [FACOLTATIVO] ivar (OUTPUT) [FACOLTATIVO] Oppure fvar (OUTPUT) [FACOLTATIVO]	(Facoltativamente) Variabile di tipo stringa in cui verrà memorizzato il giorno della settimana; scritto nel formato nome giorno completo (ad esempio: svar = Sabato) (Facoltativamente) Variabile di tipo stringa o float in cui verrà memorizzato il giorno della settimana; scritto nel formato nome giorno completo nome = numero: Lunedì = 1 Martedì = 2 Mercoledì = 3 Giovedì = 4 Venerdì = 5 Sabato = 6 Domenica = 7 (ad esempio: lunedì corrisponde a ivar = 1)

Ad esempio:

Nell'esempio seguente, il comando DATETIME converte il numero di secondi trascorsi dal 1970 in stringhe di data e ora:

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

Nell'esempio seguente, il comando DATETIME restituisce il giorno della settimana, nonché la data e l'ora:

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

Contenuto delle variabili di output correnti:

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

DBCLOSE

Il comando DBCLOSE chiude la connessione al database. I parametri obbligatori sono due.

- Il primo parametro obbligatorio è l'handle di database restituito dal comando DBOPEN. Si tratta di un numero intero o di una variabile di tipo numero intero.
- Il secondo parametro obbligatorio è lo stato di chiusura. Si tratta di una variabile di tipo numero intero o float. Se l'operazione ha esito positivo, verrà restituito un “1”.

Formato

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

DBDELETE

Il comando DBDELETE elimina righe dalla tabella selezionata in base a criteri di selezione.
I parametri obbligatori sono quattro.

- Il primo parametro obbligatorio è l'handle di database restituito dal comando DBOPEN. Si tratta di un numero intero o di una variabile di tipo numero intero.
- Il secondo parametro obbligatorio è lo stato di eliminazione. Si tratta di una variabile di tipo numero intero o float. Il numero di righe eliminate viene restituito in caso di esito positivo, anche se 0.
- Il terzo parametro obbligatorio è il nome della tabella da cui eliminare le righe. Può trattarsi di una stringa o di una variabile di tipo stringa.
- Il quarto parametro facoltativo è rappresentato dalla clausola WHERE. Consente agli utenti di filtrare i dati indesiderati mediante un criterio di selezione. Se vuota, verranno eliminate tutte le righe della tabella.

I codici di errore del comando DBDELETE sono i seguenti:

```
>0No error
0No rows deleted
-1DB handle is invalid
```

Formato

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

Ad esempio:

```
DBDELETE(i_dbhandle, i_deletestatus, "tablename")
DBDELETE(i_dbhandle, i_deletestatus, s_tablename, "where
   clause")
```

DBGETROW

Il comando DBGETROW funziona in combinazione con il comando DBSELECT. L'utente deve prima ottenere una selezione mediante DBSELECT, e quindi recuperare le righe con il comando DBGETROW. Questo comando recupera la riga disponibile successiva da una selezione, mantenendo un cursore aperto in modo che il comando possa essere chiamato in un ciclo per recuperare la riga successiva ad ogni chiamata. I parametri obbligatori sono quattro.

- Il primo parametro obbligatorio è l'handle di database restituito dal comando DBOPEN. Può trattarsi di un numero intero o di una variabile di tipo numero intero.
- Il secondo parametro obbligatorio è l'handle di selezione. Può trattarsi di una stringa o di una variabile di tipo stringa. Si tratta dello stesso handle assegnato durante il comando DBSELECT.
- Il terzo parametro obbligatorio è lo stato di recupero. Si tratta di una variabile di tipo numero intero o float. Se l'operazione ha esito positivo, verrà restituito un "1".
- Il quarto parametro obbligatorio e i successivi facoltativi sono i dati di colonna restituiti dal comando. Queste colonne possono essere variabili stringa, float o numero intero. I dati di colonna di un tipo diverso rispetto a quello del parametro vengono convertiti nel tipo corretto, se possibile. Quindi, se la tabella contiene una colonna float, ma il parametro è una stringa, i dati verranno convertiti in formato stringa. L'utente può includere fino a 48 parametri di questo tipo.

NOTA: il comando compilerà il minore dei parametri definiti e delle colonne effettive del database. Se il database ha 4 colonne ma si specificano 7 parametri, verranno compilati solo i primi 4**.**

I codici di errore del comando DBGETROW sono i seguenti:

```
1No Error
-1Error retrieving row
```

Formato

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

Ad esempio:

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

DBINSERT

Il comando DBINSERT inserisce una riga di dati nel database per la tabella selezionata. I parametri obbligatori sono quattro.

- Il primo parametro obbligatorio è l'handle di database restituito dal comando DBOPEN. Si tratta di un numero intero o di una variabile di tipo numero intero.

- Il secondo parametro obbligatorio è lo stato di inserimento. Si tratta di una variabile di tipo numero intero o float. Se l'operazione ha esito positivo, verrà restituito un “1”.
- Il terzo parametro obbligatorio è il nome della tabella in cui inserire i dati.
- Il quarto parametro obbligatorio e i successivi facoltativi sono i dati di colonna da inserire. Tali colonne possono essere di qualsiasi tipo. L'utente può includere fino a 48 parametri di questo tipo.

Il comando deve includere il numero esatto di parametri necessari per inserire una riga di dati. DBINSERT non aggiungerà un nuovo record se viene violato un vincolo univoco.

I codici di errore del comando DBINSERT sono i seguenti:

```
1 Nessun errore
-1 DB Handle is invalid / no row inserted
-2 Impossibile creare la richiesta dati
-7 Errore di esecuzione SQL
-16 Errore di sintassi SQL
```

Formato

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

Ad esempio:

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

DBOPEN

Il comando DBOPEN apre una connessione a un database supportato.

Solo nell'ambito del servizio di raccolta di Microsoft Windows NT, DBOPEN non funzionerà nel caso il nome del database venga configurato per fare riferimento a un'"unità mappata". Dal momento che il servizio di raccolta viene eseguito come un servizio, in genere, viene eseguito con l'account "system". Tale account non dispone delle autorizzazioni necessarie per accedere a condivisioni remote, comprese unità mappate. Ciò significa che qualsiasi connessione al database, anche attraverso OBDC, nel servizio di raccolta di Windows deve essere stabilita con un database locale.

I parametri obbligatori sono cinque.

- Il primo parametro obbligatorio è il tipo di database. Può essere selezionato mediante un elenco di selezione oppure utilizzando una stringa o una variabile di tipo stringa. Il valore accettabile per questo parametro è Oracle9i.
- Il secondo parametro obbligatorio è il nome del database con cui stabilire la connessione. Può trattarsi di una stringa o di una variabile di tipo stringa.

- Il terzo parametro obbligatorio è il nome utente del database. Può trattarsi di una stringa o di una variabile di tipo stringa. Questo campo può contenere qualsiasi testo, se gli utenti non lo hanno specificamente impostato per l'accesso al database.
- Il quarto parametro obbligatorio è la password dell'utente. Può trattarsi di una stringa o di una variabile di tipo stringa. Questo campo può contenere qualsiasi testo, se gli utenti non lo hanno specificamente impostato per l'accesso al database.
- Il quinto parametro obbligatorio è l'handle di database che viene restituito da questo comando nella variabile di tipo stringa o float. Se l'operazione ha esito positivo, il valore dell'handle di database sarà superiore a 0.

Formato

```
DBOPEN("oracle9i", "Database name", "username", "password",
   i_dbhandle)
```

Ad esempio:

```
DBOPEN(s_dbtype, s_dbname, s_username, s_password,
   i_dbhandle)
DBOPEN(s_dbtype, "dbname", s_username, "password",
   i_dbhandle)
```

DBSELECT

Il comando DBSELECT funziona in combinazione con il comando DBGETROW. Il comando DBSELECT apre un cursore di selezione nel database. In questo modo è possibile ottenere un'istantanea dei record correnti del database che soddisfano i criteri di selezione. I record immessi dopo il comando DBSELECT non verranno mostrati nel recupero dati fin quando non viene eseguito un altro comando DBSELECT per aggiornare la selezione.

I parametri obbligatori sono sette.

- Il primo parametro obbligatorio è l'handle di database restituito dal comando DBOPEN. Si tratta di un numero intero o di una variabile di tipo numero intero.
- Il secondo parametro obbligatorio è lo stato della selezione. Si tratta di una variabile di tipo numero intero o float. Se l'operazione ha esito positivo, verrà restituito un “1”.
- Il terzo parametro obbligatorio è l'identificatore di selezione. Può trattarsi di una stringa o di una variabile di tipo stringa. Questo parametro deve essere univoco qualora sia presente più di un comando DBSELECT.
- Il quarto parametro obbligatorio è il numero di righe da ignorare una volta effettuata la selezione. Ciò consente all'utente di posizionare il puntatore sul comando DBGETROW per i nuovi dati consentendo di ignorare i dati obsoleti. Potrebbe trattarsi di un numero intero o di una variabile di tipo numero intero.
- Il quinto parametro obbligatorio è la tabella da cui ottenere i dati. Può trattarsi sia di una stringa sia di una variabile di tipo stringa.
- Il sesto parametro facoltativo è rappresentato dalla clausola WHERE. Consente agli utenti di filtrare i dati indesiderati mediante un criterio di selezione. Se vuota, la selezione

conterrà tutte le righe della tabella. Il formato della clausola WHERE è: dove nome-colonna=’data’.

- Il settimo parametro facoltativo rappresenta le colonne restituite dal comando DBSELECT. Se vuota, la selezione conterrà tutte le colonne della tabella.

I codici di errore del comando DBSELECT sono i seguenti:

```
1 Nessun errore
-1 DB_Handle non valido
-2 Impossibile creare la richiesta dati
-3 Impostazione commit non riuscita
-4 Errore di allocazione della memoria
-5 Errore di sintassi SQL
-6 Errore di esecuzione SQL
```

Formato

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

Ad esempio:

```
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’", "FIRST, LAST,
   ADDRESS")
```

DEC

Il comando DEC riduce una variabile numerica di una unità. Quando si utilizza il comando DEC, è necessario specificare un ivar o un fvar.

Formato

```
DEC(i_numvar)
```

Tipi di dati

Argomento	Tipo	Descrizione
i_numvar	variabile numerica (INPUT/ OUTPUT)	La variabile da ridurre (ivar o fvar)

Ad esempio:

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

Risultato:

```
icounter = 0
```

DECODE

Il comando DECODE ripristina una stringa codificata per preservare l'identificazione del pacchetto. Questo comando identifica i byte di corrispondenza (o caratteri) e i byte di escape (o caratteri) al fine di rimuovere il carattere di escape. Consente di rimuovere ogni occorrenza della stringa di escape che precede i byte corrispondenti ogni volta che viene trovata nell'ambito dei dati.

Formato

```
DECODE(data_decode, match, escape)
```

Tipi di dati

Argomento	Tipo	Descrizione
data_decode	svar (INPUT/ OUTPUT)	La variabile della stringa di dati. Il risultato decodificato viene posizionato di nuovo nella variabile.
match	stringa (INPUT)	La stringa di byte che devono trovare corrispondenza nella variabile di tipo stringa data_decode.
escape	stringa (INPUT)	La stringa di escape da rimuovere dalla variabile data_decode.

Ad esempio:

Nell'esempio seguente una stringa viene codificata, copiata per salvare la versione codificata, quindi decodificata con gli stessi parametri.

```
COPY(svar:"This is just a test of decode")
ENCODE(svar, " ", "\00\")
COPY(svar_encode:svar)
DECODE(svar, " ", "\00\")
```

Contenuto delle variabili di output correnti:

```
svar = "This is just a test of decode"
svar_encode = "This\00\ is\00\ just\00\ a\00\ test\00\
   of\00\ decode"
```

DECODEMIME

Il comando DECODEMIME consente all'utente di decodificare una variabile di tipo stringa o una stringa codificata a base 64 e di memorizzare la stringa decodificata risultante in una variabile di tipo stringa. In caso di errore, la stringa di dati risultanti avrà una lunghezza pari a zero e la variabile numerica dell'esito facoltativa viene impostata su 0. Se la decodifica viene effettuata correttamente, la variabile numerica dell'esito viene impostata su 1.

Formato

```
DECODEMIME(encoded_data, data, success)
```

Tipi di dati

Argomento	Tipo	Descrizione
encoded_data	Stringa/Variabile di tipo stringa(INPUT)	Stringa codificata a base 64 da decodificare.
dati	Variabile di tipo stringa(OUTPUT)	Dati decodificati risultanti.
esito positivo	Variabile di tipo numero intero/Variabile di tipo float(OUTPUT) [FACOLTATIVO]	Verrà impostata su 1 se la decodifica viene effettuata correttamente. In caso contrario verrà impostata su zero.

Ad esempio:

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

Nell'esempio sopra riportato, il comando DECODEMIME decodifica la stringa tra virgolette utilizzando decodifica a base 64 e memorizza la stringa decodificata risultante in s_data. S_data viene popolata con quanto segue:

```
comando test encode64
```

In caso di decodifica corretta, 1 viene assegnato alla variabile numero intero i_success.

Fare riferimento anche al comando ENCODEMIME.

DELETE

Il comando DELETE rimuove variabili dal sistema per liberare la memoria allocata nelle aree di memorizzazione. Ciò è particolarmente utile per le variabili di tipo stringa.

È consigliabile eliminare variabili di tipo svar quando è necessario risparmiare capacità di memoria. In un comando DELETE possono essere specificate fino a 100 variabili.

Formato

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

Dove:

```
varlist ::= var [, <varlist>]
Var ::= variabile da cancellare (fvar, ivar o svar)
```

Numero massimo di variabili: 100

Tipi di dati

Argomento	Tipo	Descrizione
var1	variabile (INPUT/ OUTPUT)	La variabile da eliminare (fvar, ivar o svar).
var2	variabile (INPUT/ OUTPUT) [FACOLTATIVO]	La variabile da eliminare (fvar, ivar o svar).
var3	variabile (INPUT/ OUTPUT) [FACOLTATIVO]	La variabile da eliminare (fvar, ivar o svar).
...	variabile (INPUT/ OUTPUT) [FACOLTATIVO]	Altre variabili da eliminare (fvar, ivar o svar).

Ad esempio:

```
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

Il comando DISPLAY visualizza le variabili di script e i relativi valori correnti in una finestra a comparsa.

È possibile attenersi a una delle seguenti procedure:

- Utilizzare questo comando per il debug di script
- Se si passa una stringa come parametro, quest'ultimo visualizzerà il contenuto di tale stringa

- Le stringhe contenenti dati esadecimali vengono visualizzati in formato esadecimale, vale a dire stringa="\0a 0d\"

Il programma tenta, innanzitutto, di visualizzare la stringa in ASCII. Se la stringa contiene sia dati esadecimali stampabili che non stampabili, i caratteri esadecimali stampabili vengono visualizzati in formato ASCII e la stringa restante in formato esadecimale. per la sostituzione esadecimale, \0000\ termina una stringa; quindi, “xxxx\0000\yyyy” diventa “xxxx”.

Formato

```
DISPLAY(string_data)
```

Tipi di dati

Argomento	Tipo	Descrizione
string_data	stringa (INPUT) [FACOLTATIVO]	Una qualsiasi stringa da visualizzare. Se il comando non viene attivato, tutte le variabili vengono visualizzate (stringhe, numeri e matrici) per ogni script.

Ad esempio:

```
DISPLAY()
DISPLAY(sdata_var)
DISPLAY("Hello This is String Data")
DISPLAY(sdata_var)
```

ELSE

Il comando ELSE contrassegna la terminazione di una porzione TRUE del comando if() associato in precedenza. I comandi di analisi sintattica successivi al comando ELSE() vengono eseguiti se il risultato del comando IF() è FALSE. I comandi vengono eseguiti fino al comando ENDIF() successivo corrispondente

Formato

```
ELSE()
```

Ad esempio:

```
IF(i = 10)
ALERT("I is 10")
ELSE()
ALERT("I is not 10")
ENDIF()
```

Non è possibile eseguire un confronto diretto con un numero negativo. Per fare ciò, utilizzare uno dei due metodi seguenti:

- Utilizzare la funzione di analisi sintattica Compare
- Eseguire un confronto indiretto come segue:

```
SET(i_compare_val=-10)
IF(ivar > i_compare_val)
ALERT("ivar is greater than -10")
endif()
```

ENCODE

Utilizzare il comando ENCODE per preservare l'identificazione del pacchetto. Questo comando esegue la corrispondenza di byte o caratteri nei dati ed esegue l'escape o prefissi dei byte corrispondenti con una stringa di escape. La stringa di escape viene posizionata davanti ai byte corrispondenti ogni volta che tali caratteri vengono trovati nei dati.

Formato

```
ENCODE(data_encode, match, escape)
```

Tipi di dati

Argomento	Tipo	Descrizione
data_encode	svar (INPUT/ OUTPUT)	La variabile della stringa di dati da codificare. Il risultato codificato viene posizionato di nuovo nella variabile.
match	stringa (INPUT)	La stringa di byte che devono trovare corrispondenza nella variabile di tipo stringa data_encode.
escape	stringa (INPUT)	La stringa di escape da posizione davanti a ciascun byte corrispondente all'interno della variabile data_encode.

Ad esempio:

Nell'esempio seguente, due stringhe di dati vengono codificate per aggiungere a tutti gli spazi il prefisso “#” e un'altra per aggiungere a tutte le ‘t’ e le ‘h’ il prefisso “!!”.

```
COPY(data:"Preface all spaces with ‘#’")
ENCODE(data, " ", "#")
COPY(svar:"Preface ‘t’s and ‘h’s with ‘!!’")
ENCODE(svar, "th", "!!")
```

Risultato:

```
data = "Preface# all# spaces# with# ‘#’"
svar = "Preface ‘!!t’s and !!h’s wi!!t!!h ‘!!’"
```

ENCODEMIME

Il comando ENCODEMIME consente all'utente di codificare una variabile di tipo stringa o una stringa codificata a base 64 e di memorizzare la stringa codificata risultante in una variabile di tipo stringa.

Formato

```
ENCODEMIME(data, encoded_data)
```

Tipi di dati

Argomento	Tipo	Descrizione
dati	Stringa/variabile stringa (INPUT)	Stringa di dati da codificare.
encoded_data	Variabile di tipo stringa (OUTPUT)	Dati codificati risultanti.

Ad esempio:

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

Nell'esempio sopra riportato, il comando ENCODEMIME codifica la stringa della variabile s_data utilizzando decodifica a base 64 e memorizza la stringa codificata risultante in s_encd_data. S_encd_data viene popolata con quanto segue:

```
VGVzdGluZyBEYXRhIEVuY29kaW5n
```

Fare riferimento anche al comando DECODEMIME.

ENDFOR

Il comando ENDFOR contrassegna la terminazione del blocco for() precedente.

Formato

```
ENDFOR()
Esempio
FOR(i=0,i<3,i=i+1)
ALERT("Still in loop")
ENDFOR()
```

ENDIF

Il comando ENDFOR contrassegna la terminazione del blocco if() precedente.

Formato

```
ENDIF()
```

Ad esempio:

```
IF(i = 10)
ALERT("I is 10")
ELSE()
ALERT("I is not 10")
ENDIF()
```

Non è possibile eseguire un confronto diretto con un numero negativo. A questo scopo, utilizzare uno dei metodi seguenti:

- Utilizzare la funzione di analisi sintattica Compare
- Eseguire un confronto indiretto come segue:

```
SET(i_compare_val=-10)
IF(ivar > i_compare_val)
ALERT("ivar is greater than -10")
ENDIF()
```

ENDWHILE

Il comando ENDFOR contrassegna la terminazione del blocco while() precedente.

Formato

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

EVENT

Il comando EVENT crea e invia un messaggio di avviso. No recupera alcun parametro. Il comando EVENT crea automaticamente il messaggio di avviso utilizzando il contenuto delle variabili riservate.

La maggior parte delle variabili riservate eseguono direttamente la mappatura di meta-tag del modello Wizard v3.2. Vengono inviate soltanto le variabili utilizzate nello script non impostate su “”. Perchè possano essere elaborate da Gestione servizi di raccolta sono necessarie variabili quali i_Severity e s_Res per un messaggio di avviso.

Variabili riservate di evento

NOTA: Se un'etichetta è preceduta da ‘e.’, ad esempio e.crt, fa riferimento a eventi correnti. Se un'etichetta è preceduta da ‘w.’, ad esempio w.crt, fa riferimento a eventi cronologici.

Variabile	Breve descrizione	Esegue al mappatura di meta-tag (etichetta)
s_BM	Messaggio base	Messaggio (msg)
i_Severity	Gravità	Gravità (sev)
s_Res	Risorsa	Risorsa (res)
s_SubRes	SubResource	SubResource (sres)
s_ET	Ora dell'evento	EventTime (et)
s_P	Protocollo	Protocollo (prot)
s_DP	Porta di destinazione	DestinationPort (dp)
s_SP	Porta di origine	SourcePort (sp)
s_EVT	Nome dell'evento	EventName (evt)
s_SN	Nome del sensore	SensorName (sn)
s_SIP	Indirizzo IP di origine	Source IP (sip)
s_DIP	Indirizzo IP di destinazione	DestinationIP (dip)
s_SHN	Nome dell'host di origine	SourceHostName (shn)
s_DHN	Nome dell'host di destinazione	DestinationHostName (dhn)
s_SUN	Nome dell'utente di origine	SourceUserName (sun)
s_DUN	Nome dell'utente di destinazione	DestinationUserName (dun)
s_FN	Nome file	FileName (fn)
s_EI	Informazioni estese	ExtendedInformation (ei)
s_RN	Nome dell'autore del rapporto	ReporterName (rn)
s_ST	Tipo di sensore	Sensor Type (st)
s_PN	Nome del prodotto	ProductName (pn)
s_CRIT	Criticità	Criticality (crt)
s_VULN	Vulnerabilità	Vulnerability (vul)
s_CT1	Riservata dell'utente 1	Ct1 (ct1)
s_CT2	Riservata dell'utente 2	Ct2 (ct2)
s_CT3	Riservata dell'utente 3	Ct3 (ct3)
s_RT1	Nome attacco dispositivo (riservato per Sentinel 1)	Rt1 (rt1)
s_RT2	Riservata dell'utente 2	Rt2 (rt2)
s_RT3	Riservata dell'utente 3	Rt3 (rt3)
s_CV1 to s_CV100	Variabile utente da 1 a 100 **NOTA:** Da 1 a 10 è di tipo lungo numero) Da 11 a 20 è di tipo data Da 21 a 100 è di tipo stringa	Cv1 a Cv100 (cv1 a cv100)

Variabile	Breve descrizione	Esegue al mappatura di meta-tag (etichetta)
s_RV1 to s_RV29	Valore riservato da 1 a 29 **NOTA:** Riservato all'uso da parte di Novell**.**	Rv1 a Rv31 (rv1 a rv29)
s_RV30	AttackId	Rv30
s_RV31	DeviceName	Rv31
s_RV32	DeviceCategory	Rv32 (rv32)
s_RV33	EventContext	Rv33 (rv33)
s_RV34	SourceThreatLevel	Rv34 (rv34)
s_RV35	SourceUserContext	Rv35 (rv35)
s_RV36	DataContext	Rv36 (rv36)
s_RV37	SourceFunction	Rv37 (rv37)
s_RV38	SourceOperationalContext	Rv38 (rv38)
s_RV39	MSSPCustomerName	Rv39 (rv39)
s_RV40 a s_RV43	Valore riservato da 40 a 43 **NOTA:** Riservato all'uso da parte di Novell**.**	Rv40 a Rv43 (rv40 a rv43)
s_RV44	DestinationThreatLevel	Rv44 (rv44)
s_RV45	DestinationUserContext	Rv45 (rv45)
s_RV46	VirusStatus	Rv46 (rv46)
s_RV47	DestinationFunction	Rv47 (rv47)
s_RV48	DestinationOperationalContext	Rv48 (rv48)
s_RV49	ReservedVar49 **NOTA:** Riservato all'uso da parte di Novell .	Rv49 (rv49)
s_RV50	eSecTaxonomyLevel1	Rv50 (rv50)
s_RV51	eSecTaxonomyLevel2	Rv51 (rv51)
s_RV52	eSecTaxonomyLevel3	Rv52 (rv52)
s_RV53	eSecTaxonomyLevel4	Rv53 (rv53)
s_RV54 a s_RV100	Valore riservato da 54 a 100 **NOTA:** Riservato all'uso da parte di Novell.	Rv54 a Rv100 (rv54 a rv100)

Formattazione automatica

Le variabili riservate s_DP, s_SP e s_P sono impostate su lettere minuscole prima che il messaggio di evento venga inviato. Le variabili riservate s_ST e s_PN sono impostate su lettere maiuscole prima che il messaggio di evento venga inviato. Se lasciata vuota, la variabile temporale s_ET viene impostata sul formato dell'ora standard nel modo seguente:

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

È possibile ignorare questa funzione impostando la variabile s_ET con altre informazioni. Come minimo, sia s_Hour sia s_Month devono essere impostate per l'ET da creare. Tutti i campi vuoti verranno visualizzati nel campo ET come NULL.

Variabili riservate data/ora

Se la variabile temporale s_ET viene lasciata vuota mentre s_Hour e s_Month non lo sono, la variabile s_ET del meta-tag ET verrà popolata automaticamente. Le variabili riservare data/ora deve essere impostata su dei valori. Qualsiasi campo vuoto verrà visualizzato come NULL. Il campo s_Day ha un formato basata su valori a due cifre 01-09. L'autore dello script può scegliere di convertire il valore relativo al mese in un numero a due cifre utilizzando il comando TRANSLATE e il file months.csv. Di seguito vengono riportati i tag riservati:

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

Variabili riservate di controllo evento

Due variabili, s_SendEITag e s_SendETTag, vengono utilizzate per determinare se il comando EVENT include i campi EI e ET, rispettivamente, in un messaggio di avviso. Per disattivare l'invio dei campi, le variabili devono essere impostate su OFF.

Formato

```
EVENT ()
```

Ad esempio:

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

FILEA

Il comando FILEA aggiunge i contenuti di una stringa al termine di un file flat sul disco. Quando si utilizza questo comando:

- Specificare il nome file utilizzando una stringa
- Per Windows, il nome file fa riferimento al file come specificato se inizia con una lettera di unità, due punti e barra rovesciata (ad esempio c:\)
- È necessario specificare il percorso completo del file
- Se il file non esiste, verrà creato
- Qualora fosse impossibile creare il file, il comando FILEA non funzionerà correttamente
- Al termine dell'aggiunta dei dati al file, quest'ultimo viene chiuso

Se si sta scrivendo questo comando all'interno di uno script che dovrà essere eseguito mediante un servizio di raccolta, assicurarsi di utilizzare la sintassi corretta per il percorso, incluse le barre (/).

Quando si specifica il percorso, ricordarsi di inserire barre e barre rovesciate come sequenza di escape. Lo zero alla fine della stringa non viene scritto nel file.

Formato

```
FILEA("nome file", dati)
```

Tipi di dati

Argomento	Tipo	Descrizione
nome file	stringa (INPUT)	Il nome del file a cui i dati devono essere applicati.
dati	stringa (INPUT)	La stringa di dati da aggiungere al file.

Ad esempio:

Nell'esempio seguente, il file \temp\mux_data viene creato e i contenuti di s_variable vengono aggiunti al file:

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

Nell'esempio seguente, una stringa viene aggiunta alla fine del file di log di revisione:

```
COPY(audit_str: "Sent 20 severity 5 alerts.")
FILEA("h:/\temp/\audit.log", audit_str)
```

FILEL

Il comando FILEL ottiene la lunghezza, in byte, di un file flat e inserisce il valore nella variabile numerica. Quando si utilizza questo comando:

- Specificare il nome file utilizzando una stringa
- Per Windows, il nome file fa riferimento al file come specificato se inizia con una lettera di unità, due punti e barra rovesciata (ad esempio c:\)
- Se il file non esiste, il comando FILEL non funziona e il contenuto di numvar rimane invariato
- Al termine della lettura dei dati del file, quest'ultimo viene chiuso

Se si sta scrivendo questo comando all'interno di uno script che dovrà essere eseguito mediante un servizio di raccolta, assicurarsi di utilizzare la sintassi corretta per il percorso, incluse le barre (/). Quando si specifica il percorso, ricordarsi di inserire barre e barre rovesciate come sequenza di escape.

Formato

```
FILEL("nome file", i_length)
```

Tipi di dati

Argomento	Tipo	Descrizione
nome file	stringa (INPUT)	Il nome del file la cui lunghezza deve essere determinata.
i_length	variabile numerica (OUTPUT)	La lunghezza del file, in byte.

Ad esempio:

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

Restituisce la lunghezza del file infotron.log, in byte, ad esempio:

```
i_length = 2390
```

FILER

Il comando FILER copia il contenuto di un file flat sul disco in una variabile di tipo stringa. Quando si utilizza questo comando:

- Specificare il nome file utilizzando una stringa.
- Per Windows, il nome file fa riferimento al file come specificato se inizia con una lettera di unità, due punti e barra rovesciata (ad esempio c:\)
- Se il file non esiste, il comando FILER non funziona e il contenuto di svar rimane invariato
- Al termine della lettura dei dati del file, quest'ultimo viene chiuso
- Facoltativamente, immettere il numero massimo di byte da leggere. Non è possibile utilizzare il parametro max_bytes a meno che non sia accoppiato al parametro i_offset.

Se si sta scrivendo questo comando all'interno di uno script che dovrà essere eseguito mediante un servizio di raccolta, assicurarsi di utilizzare la sintassi corretta per il percorso, incluse le barre (/). Quando si specifica il percorso, ricordarsi di inserire barre e barre rovesciate come sequenza di escape.

Formato

```
FILER("filename", dest, [i_offset [, i_max_bytes]])
```

NOTA: Non è possibile utilizzare il parametro max_bytes a meno che non sia accoppiato al parametro i_offset.

Tipi di dati

Argomento	Tipo	Descrizione
nome file	stringa (INPUT)	Il nome del file in cui leggere la stringa di dati.
dati	svar	I dati letti dal file vengono inseriti nella variabile di tipo stringa.

Argomento	Tipo	Descrizione
	(OUTPUT)	
i_offset	intero (INPUT) [FACOLTATIVO]	Specifica un numero offset di caratteri da cui iniziare la lettura.
max_bytes	intero (INPUT) [FACOLTATIVO]	Facoltativamente, specificare il numero massimo di byte da leggere. **NOTA:** Quando si utilizza questo argomento, è necessario specificare l'argomento i_offset.

Ad esempio:

```
CLEAR(data)
FILER("filename", data, 0, 20)
if(data = "")
ALERT(s_res_var, "Data file doesn’t exist or is empty.", 0)
ENDIF()
```

FILEW

Il comando FILEW scrive il contenuto di una stringa in un file flat sul disco. Quando si utilizza questo comando:

- Il contenuto precedente del file viene sovrascritto
- Specificare il nome file utilizzando una stringa
- Per Windows, il nome file fa riferimento al file come specificato se inizia con una lettera di unità, due punti e barra rovesciata (ad esempio c:\)
- Se il file non esiste, verrà creato
- Qualora fosse impossibile creare il file, il comando FILEW non funzionerà correttamente
- Al termine della scrittura dei dati nel file, quest'ultimo viene chiuso

Se si sta scrivendo questo comando all'interno di uno script che dovrà essere eseguito mediante un servizio di raccolta, assicurarsi di utilizzare la sintassi corretta per il percorso, incluse le barre (/). Quando si specifica il percorso, ricordarsi di inserire barre e barre rovesciate come sequenza di escape.

Formato

```
FILEW("nome file", dati)
```

Tipi di dati

Argomento	Tipo	Descrizione
nome file	stringa (INPUT)	Il nome del file in cui scrivere la stringa di dati.
dati	svar (OUTPUT)	I dati da scrivere nel file.

Ad esempio:

```
FILEW("nome file", dati)
FILEW("h:/\tmp/\infotron.stat", "SUCCESSFUL EXEC")
```

FOR

Il comando FOR fornisce compatibilità per il flusso di controllo del ciclo. Quando si utilizza questo comando:

- L'istruzione di inizializzazione viene eseguita sempre
- Se il risultato dell'istruzione di confronto FOR() è TRUE, vengono eseguiti i comandi di analisi sintattica dopo FOR(), fino al successivo ENDFOR(). Viene quindi eseguita l'istruzione di incremento e il flusso di controllo viene restituito all'istruzione di confronto
- Se il risultato dell'istruzione di confronto FOR() è FALSE, non viene eseguito alcun comando di analisi sintattica tra FOR() e ENDFOR(). L'istruzione di incremento non viene eseguita
- Nonostante tutti i tipi di dati siano consentiti per ogni lato dell'istruzione di confronto for(), i valori numerici possono essere confrontati solo con i valori numerici e le stringhe con le stringhe
- L'operatore per l'istruzione di confronto FOR() può essere <, =, >, <=, >=, <>, &, + oppure ^

Non è possibile eseguire un confronto diretto con un numero negativo. A questo scopo, utilizzare uno dei metodi seguenti:

- Utilizzare la funzione di analisi sintattica COMPARE
- Eseguire un confronto indiretto come segue:

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

Formato

```
FOR(initialization, compare, increment)
```

Tipi di dati

Argomento	Tipo	Descrizione
inizializzazione	SET() parametro	Qualsiasi parametro valido che possa essere passato al comando SET(). Vedere la definizione del comando SET().
condizionale	IF() condizionale	Qualsiasi parametro valido che possa essere passato al comando IF(). Vedere la definizione del comando IF().
incremento	SET() parametro	Qualsiasi parametro valido che possa essere passato al comando SET(). Vedere la definizione del comando SET().

Ad esempio:

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

GETCONFIG

Recupera l'impostazione corrente per una proprietà di sistema. Questo comando viene utilizzato per recuperare le proprietà di sistema utilizzando il comando SETCONFIG. Tali comandi vengono utilizzati per impostare variabili e recuperare i valori correnti per le proprietà di sistema che possono cambiare periodicamente, ad esempio un file di log che viene rinominato quotidianamente utilizzando la data corrente.

Proprietà di sistema disponibili:

Proprietà di sistema	Esempi
▪ 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	elenco di indirizzi IP di questo host separati da un punto e virgola, ad esempio "172.163.3.45;172.45.2.1"

Vedere anche il comando SETCONFIG.

I parametri obbligatori sono due.

- Il primo parametro obbligatorio definisce l'opzione di configurazione (FileConnector.InputFile) o (FileConnector.OutputFile).
- Il secondo parametro obbligatorio definisce il valore di configurazione da recuperare.

Formato

```
GETCONFIG(Config Option, Value)
```

Tipi di dati

Argomento	Tipo	Descrizione
Config Opzione	stringa (INPUT)	Nome della variabile di configurazione da recuperare. File di input = “FileConnector.InputFile” File di output = “FileConnector.InputFile”
Valore	stringa (INPUT)	Impostazione di configurazione da recuperare.

Ad esempio:

```
GETCONFIG(“FileConnector.InputFile”, s_inputfilename)
GETCONFIG(“FileConnector.OutputFile”, s_outputfilename)
```

Contenuto delle variabili di output correnti

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

GETENV

Il comando GETENV recupera il valore di una variabile di ambiente.

Formato

```
GETENV(chiave di ambiente, variabile in cui memorizzare i dati)
```

Tipo di dati

Argomento	Tipo	Descrizione
Chiave di ambiente	stringa (INPUT)	Nome della variabile di ambiente.
Variabile in cui memorizzare i dati	stringa Var (INPUT)	Destinazione della variabile di ambiente.

Ad esempio:

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

HEXTONUM

Il comando HEXTONUM converte una stringa esadecimale con al massimo 4 byte di dati esadecimali in un numero decimale e colloca il numero decimale in una variabile di tipo numero intero o float. Oltre 4 byte risultano come dati non validi.

Formato

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

Tipi di dati

Argomento	Tipo	Descrizione
bytes_data	stringa (INPUT)	Stringa composta di un numero di byte compreso tra 1 e 4. (ad esempio: "\FF\", "\FF FF\", "\3C 4A F2\", "\43 76 F3 FF\", or "TEST"). Il numero esadecimale rappresentato da questi byte verrà convertito in un valore intero, i_val.
i_val	variabile numerica (OUTPUT)	L'equivalente decimale del numero esadecimale viene collocato in questa variabile, ivar o fvar.

Argomento	Tipo	Descrizione
i_len	di tipo numerico (INPUT) [FACOLTATIVO]	Numero di byte esadecimali da convertire in un intero (deve avere un intervallo di valori assoluti compresi tra 1 e 4). Se questo parametro non viene impostato, il valore predefinito sarà il numero di byte nella stringa di input, bytes_data, fino a 4 byte. Se i_len è positivo, i byte vengono interpretati da sinistra a destra (dal byte più significativo al meno significativo). Se i_len è negativo, i byte vengono interpretati da destra a sinistra (dal byte meno significativo al più significativo).
ioffset	di tipo numerico (INPUT) [FACOLTATIVO]	Il numero di offset di byte da ignorare in bytes_data.

Ad esempio:

Nell'esempio seguente, i dati nella stringa esadecimale "\5A32\" vengono convertiti in un valore intero, interpretati da MSB a LSB, quindi da LSB a MSB.

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

NOTA: Per la sostituzione esadecimale, \0000\ termina una stringa; quindi, “xxxx\0000\yyyy” diventa “xxxx”.

Contenuto delle variabili di output correnti:

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

IF

Il comando IF confronta due valori.

- Se il risultato dell'istruzione IF() è TRUE, vengono eseguiti i comandi di analisi sintattica dopo IF(), fino al successivo ELSE() o ENDIF().
- Se il risultato dell'istruzione IF() è FALSE, vengono eseguiti i comandi di analisi sintattica seguiti da ELSE() fino a ENDIF().
- Se non viene utilizzato alcun ELSE(), nessun comando di analisi sintattica viene eseguito tra IF() e ENDIF() quando il risultato dell'istruzione IF() è FALSE.
- Nonostante tutti i tipi di dati siano consentiti per ogni lato dell'istruzione IF(), i valori numerici possono essere confrontati solo con i valori numerici e le stringhe con le stringhe

- L'operatore per l'istruzione di confronto IF() può essere <, =, >, <=, >=, <>, &, + oppure ^ Non utilizzare l'operatore logico NOT (^) insieme a una variabile di tipo stringa. In caso contrario, verrà generato un errore di sintassi.

Non è possibile eseguire un confronto diretto con un numero negativo. A questo scopo, utilizzare uno dei metodi seguenti:

- Utilizzare la funzione di analisi sintattica COMPARE.
- Eseguire un confronto indiretto come segue:

```
SET(i_compare_val=-10)
IF(ivar > i_compare_val)
ALERT("ivar is greater than -10")
ENDIF()
```

Formato

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

Dove <expr> deve restituire un valore intero o float.

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

Dove entrambi i valori di <espr> devono restituire lo stesso tipo di dati.

Tipi di dati

Argomento	Tipo	Descrizione
dati1	variabile (INPUT)	I dati da confrontare con dati2. Se dati2 non viene utilizzato, diventa un'espressione logica (0 = false, altri valori = true).
operatore logico	< = > <= >= <> & + ^	Minore di Uguale a Maggiore di Minore o uguale a Maggiore o uguale a Diverso da AND logico OR logico NOT logico
dati2	tutti (INPUT) [FACOLTATIVO]	I dati da confrontare con dati1. Deve essere dello stesso tipo di data1.
…	come sopra	Utilizzare fino a 200 parametri singoli per creare espressioni logiche complesse.

Ad esempio:

```
IF(s = "test" & i_count < 5)
```

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

INC

Il comando INC incrementa una variabile numerica di 1. Quando si utilizza questo comando, è necessario specificare sia una variabile di tipo intero che una variabile di tipo float.

Formato

```
INC(i_counter)
```

Tipi di dati

Argomento	Tipo	Descrizione
i_counter	variabile numerica (INPUT/ OUTPUT)	La variabile numerica da incrementare di 1.

Ad esempio:

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

Risultato:

```
icounter = 2
```

INDICATOR

Il comando INDICATOR invia messaggi dell'indicatore a Sentinel. I messaggi contengono testo da visualizzare nell'ambito dell'indicatore specifico di Sentinel.

Formato

```
INDICATOR(nome, valore)
```

NOTA: Prima della versione v4.0, il comando INDICATOR aveva argomenti aggiuntivi che non vengono più utilizzati. Per compatibilità con i precedenti servizi di raccolta, questi argomenti hanno come etichetta "Non utilizzato" nella finestra editor dei comandi Wizard.

Tipi di dati

Argomento	Tipo	Descrizione
nome	stringa (INPUT)	Nome dell'indicatore
valore	stringa (INPUT)	Testo dell'indicatore da visualizzare nella console Sentinel. Ad esempio: STAMPANTE ACCESA

Ad esempio:

```
INDICATOR("memoria", "5 MB")
INDICATOR(nome, valore)
```

NOTA: Il nome dell'indicatore nel comando di analisi sintattica deve corrispondere al nome dell'indicatore in Sentinel; in caso contrario, l'indicatore non verrà aggiornato nella console di Sentinel.

INFO_CLEARTAGS

Questa funzione azzera, o annulla nel caso di stringhe, tutte le variabili che fanno parte del set del blocco di informazioni a cui fa riferimento l'handle. Utilizzare INFO_CONSTANTTAGS per evitare che ciò si verifichi in un subset di tali tag.

Formato

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

Tipi di dati

Argomento	Tipo	Descrizione
Handle IN	stringa (INPUT)	tipo di blocco di informazioni

INFO_CLOSE

Questo comando viene utilizzato per chiudere una sessione infoblock. Quando chiamato, invia innanzitutto qualsiasi infoblock non inviato come se si trattasse del comando INFO_SEND. Invia quindi un messaggio di chiusura della sessione infoblock impostando l'attributo EOD (End Of Data) dell'elemento infos su "TRUE". Dopo aver inviato il messaggio di chiusura, il numero di segmento ("segnum") viene incrementato di uno.

Formato

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

Tipi di dati

Argomento	Tipo	Descrizione
Handle IN	stringa (INPUT)	tipo di blocco di informazioni

INFO_CONSTANTTAGS

Utilizzare questo comando per denominare tag che non verranno annullate quando INFO_CLEARTAGS viene chiamato. Passare uno o più nomi di tag per creare un set di tag costante. Più chiamate a questa funzione reimpostano l'elenco dei tag costante.

Formato

```
INFO_CONSTANTTAGS(<IN handle>, [<IN tag name>, …])
```

Tipi di dati

Argomento	Tipo	Descrizione
Handle IN	stringa (INPUT)	tipo di blocco di informazioni
Nome tag IN	stringa (INPUT)	nome a cui handle IN deve fare riferimento

INFO_CREATE

Questo comando crea un nuovo set di blocchi di informazioni. È necessario passare un handle (che si utilizzerà in qualsiasi altro comando per influire su questo set di blocchi di informazioni). È anche necessario passare un tipo. Si tratta di una stringa scelta dall'utente ma che deve essere formalizzata (vedere INFO_SEND).

Se si chiama INFO_CREATE in un handle già esistente, il contenuto dell'handle viene annullato dal momento che si è avviato un nuovo handle. È necessario chiamare di nuovo INFO_SETTAG e INFO_CONSTANTTAGS.

Formato

```
INFO_CREATE(<OUT handle>,<IN type>)
```

Tipi di dati

Argomento	Tipo	Descrizione
Handle OUT	stringa (OUTPUT)	nome a cui tipo IN deve fare riferimento
Tipo IN	stringa (INPUT)	tipo di blocco di informazioni

INFO_DUMP

Questo comando fa persistere lo stato corrente del set di blocchi in informazioni in una variabile di tipo stringa. Ciò è stato incluso per facilitare la verifica ma può anche essere utilizzato per richiamare i set dei blocchi di informazioni o salvarli come file di testo o un altro tipo di file a scelta. È stato anche eliminato l'ulteriore effetto di INFO_SEND, ovvero l'eliminazione dello stato attuale.

Formato

```
INFO_DUMP(<IN handle>, <OUT string-variable>)
```

Tipi di dati

Argomento	Tipo	Descrizione
Handle IN	stringa (INPUT)	tipo di blocco di informazioni
OUT string-variable	stringa (OUTPUT)	variabile di tipo stringa a cui handle IN deve fare riferimento

INFO_PUSH

Ciò consente di contrassegnare i valori correnti di tutti i nomi di tag (mediante le variabili associate) e li colloca alla fine di un elenco di blocchi di informazioni a cui fa riferimento un handle. I blocchi continuano ad accumularsi nel set fin quando non viene chiamato il comando INFO_CREATE, INFO_SEND o INFO_CLOSE. Per INFO_CREATE, non viene effettuata alcuna azione.
Per INFO_SEND, i blocchi di informazioni vengono inviati a Gestione servizi di raccolta.
Per INFO_CLOSE, oltre ai blocchi di informazioni inviati a Gestione servizi di raccolta viene inviato anche un messaggio di chiusura del blocco di informazioni (EndOfData o EOD).

Formato

```
INFO_PUSH(<IN handle>)
```

Tipi di dati

Argomento	Tipo	Descrizione
Handle IN	stringa (INPUT)	tipo di blocco di informazioni

INFO_SEND

Questo sistema si basa sul set corrente di blocchi di informazioni e li invia a un canale di comunicazione specificato dal tipo utilizzato durante INFO_CREATE, incluso alla parola "infoblock.", punto incluso. Di conseguenza, se il tipo è "vulnerability", il nome del canale utilizzato per l'invio del messaggio sarà "infoblock.vulnerability".

Inoltre, questo comando annulla il set corrente di blocchi di informazioni e incrementa il numero di segmenti ("segnum") di uno.

Formato

```
INFO_SEND(<IN handle>)
```

Tipi di dati

Argomento	Tipo	Descrizione
Handle IN	stringa (INPUT)	tipo di blocco di informazioni

INFO_SETTAG

Questo comando associa una variabile di tipo script al nome di un attributo. Quando viene chiamato INFO_PUSH (vedere INFO_PUSH), tutte le variabili associate a questo comando verranno impostate come attributi nella voce del blocco.

Formato

```
INFO_SETTAG(<IN handle, IN tag name, IN variable)
```

Tipi di dati

Argomento	Tipo	Descrizione
Handle IN	stringa (INPUT)	tipo di blocco di informazioni
Nome tag IN	stringa (INPUT)	tipo di nome del tag
Variabile IN	stringa (INPUT)	tipo di variabile

Tag blocco informazioni di vulnerabilità

I seguenti sono tag blocco informazioni di vulnerabilità relativi al comando INFO_SETTAG. I tag contrassegnati come obbligatori devono essere impostati in modo che il blocco di informazioni venga memorizzato come una vulnerabilità. Anche se il blocco di informazioni non è memorizzato come una vulnerabilità, i tag contrassegnati come costante verranno ancora estratti dal blocco di informazioni. Se un tag impostato non è presente nell'elenco seguente, il backend della vulnerabilità ignorerà il tag.

Nome tag	Descrizione	Tipo	Costante	Obbligatorio
ScannerInstance	Il nome che l'utente dà all'istanza dello scanner. In genere impostato tra i parametri del servizio di raccolta.	Stringa	X	
ProductName	Nome dello scanner.	Stringa	X	

Nome tag	Descrizione	Tipo	Costante	Obbligatorio
ProductVersion	Versione dello scanner	Stringa	X	
ScannerType	Tipo di scanner.	Stringa	X	
Vendor	Nome del fornitore dello scanner.	Stringa	X	
ScanType	PARTIAL o FULL	Stringa	X	
ScanStartDate	Ora di inizio scansione	Stringa		
ScanEndDate	Ora di fine della scansione	Stringa		
IP	Indirizzo IP della risorsa	Stringa		X
HostName	Nome host della risorsa	Stringa		
Location	Percorso della risorsa	Stringa		
Reparto	Reparto della risorsa	Stringa		
BusinessSystem	Sistema aziendale della risorsa	Stringa		
OperationalEnvironment	Ambiente operativo della risorsa	Stringa		
Regulation	Regolazione della risorsa	Stringa		
RegulationRating	Livello di regolazione della risorsa	Stringa		
Criticità	Criticità della risorsa [1 - 25]	Numero		
VulnModule	Modulo utilizzato per rilevare la vulnerabilità	Stringa		
PortNumber	Numero di porta della vulnerabilità	Numero		
PortName	Nome della porta della vulnerabilità	Stringa		
NetworkProtocol	Protocollo di rete della vulnerabilità	Numero		
ApplicationProtocol	Protocollo applicativo della vulnerabilità	Stringa		
AssignedVulnSeverity	Gravità della vulnerabilità assegnata.	Numero		
ComputedVulnSeverity	Gravità della vulnerabilità calcolata.	Numero		
VulnDescription	Descrizione della vulnerabilità.	Stringa		
VulnSolution	Soluzione alla vulnerabilità	Stringa		
VulnSummary	Soluzione alla vulnerabilità	Stringa		
VulnCrossRefs	Elenco di codici della vulnerabilità.	Stringa		

Nome tag	Descrizione	Tipo	Costante	Obbligatorio
DetectedOs	Sistema operativo rilevato quando viene scoperta una vulnerabilità	Stringa		
DetectedOsVersion	Versione del sistema operativo rilevata quando viene scoperta una vulnerabilità.	Stringa		
ScannedApp	Applicazione rilevata quando viene scoperta una vulnerabilità	Stringa		
ScannedAppVersion	Versione dell'applicazione rilevata quando viene scoperta una vulnerabilità	Stringa		
VulnUserName	Nome utente della vulnerabilità.	Stringa		
VulnUserDomain	Dominio dell'utente della vulnerabilità.	Stringa		
VulnTaxonomy	Tassonomia della vulnerabilità.	Stringa		
ScannerClassification	Classificazione della vulnerabilità indicata dallo scanner.	Stringa		
ExtendedInformation	Informazioni estese da memorizzare insieme alla vulnerabilità	Stringa		
VulnName	Nome della vulnerabilità indicata dallo scanner.	Stringa		

Esempio di comando INFO_*

La vulnerabilità dei batch Sentinel viene analizzata in porzioni più piccole, sessioni di blocchi di informazioni, che possono essere elaborate più facilmente. Un sessione di questo tipo contiene più set di blocchi di informazioni, ciascuno con un numero di segmento crescente ("segnum") seguito da un messaggio di chiusura della sessione blocchi di informazioni. È possibile fare riferimento all'istanza di una sessione di questo tipo tramite l'"ID" univoco globale. Ogni volta che viene chiamato il comando INFO_SEND, verrà inviato un set di blocchi di informazioni con i valori "pushed" correnti e il numero di segmenti correnti ("segnum"). Subito dopo l'invio del set di blocchi di informazioni, il "segnum" viene aumentato di uno. Il comando INFO_SEND viene chiamato per ogni batch di dati, quindi viene chiamato il comando INFO_CLOSE per chiudere la sessione blocco di informazioni.
Il messaggio di chiusura blocco di informazioni consiste in un set di blocchi di informazioni con un attributo EOD impostato su "TRUE".

Ad esempio:

```
INFO_CREATE(h_vuln,"vulnerability")
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 is for apple")
COPY(s_gamma:"c is for coffee")
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 is for acorn")
COPY(s_gamma:"c is for carrot")
INFO_PUSH(h_vuln)
INFO_SEND(h_vuln)
INFO_CLOSE(h_vuln)
```

Risultati:

```
<?xml version="1.0" encoding="UTF-8"?>
<infos id="B008961E00CB1026B8F000065BBD13AB"
   type="vulnerability" segnum=”0” version=”4.2.0.0”
   EOD=”false”>
<info ALPHA="a is for apple" BETA="12345" DELTA="123456789"
   GAMMA="c is for coffee" _1EPSILON="1.234"/>
<info ALPHA="" BETA="0" DELTA="123456789" GAMMA="c is for
   coffee" _1EPSILON="1.234"/>
</infos>
<?xml version="1.0" encoding="UTF-8"?>
<infos id="B008961E00CB1026B8F000065BBD13AB"
   type="vulnerability" segnum=”1” version=”4.2.0.0”
   EOD=”false”>
```

```
<info ALPHA="a is for acorn" BETA="6789" DELTA="987654321"
   GAMMA="c is for carrot" _1EPSILON="3.1415926"/>
</infos>
<?xml version="1.0" encoding="UTF-8"?>
<infos id="B008961E00CB1026B8F000065BBD13AB"
   type="vulnerability" segnum=”2” version=”4.2.0.0”
   EOD=”true”>
</infos>
```

IPTONUM

Il comando IPTONUM converte la rappresentazione di stringhe di un indirizzo IPv4 in un numero intero e colloca quest'ultimo in una variabile di tipo intero. Questa funzione supporta solo indirizzi IPv4. Un indirizzo IPv4 che non rientra nell'intervallo valido comporterà dati non validi.

Formato

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

Tipi di dati

Argomento	Tipo	Descrizione
ip_address	svar(INPUT)	Indirizzo IPv4 di tipo stringa.
i_integer	numeric(OUTPUT)	Indirizzo IPv4 di tipo stringa viene convertito in un valore intero. Il valore intero viene collocato in questa variabile.
i_invalid	ivar(OUTPUT) [OPTIONAL}	Il valore 0 implica che l'indirizzo IP non è valido. Il valore 1 implica che l'indirizzo IP è valido.

Ad esempio:

Nell'esempio seguente, l'indirizzo IPv4 "10.10.10.255" viene convertito in un numero intero. i_valid viene impostato su 1, il che implica che il risultato è valido.

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

Contenuto delle variabili di output correnti:

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

Nell'esempio seguente, l'indirizzo IPv4 non valido "10.10.10.258" viene convertito in un numero intero 0. i_valid viene impostato su 0, il che implica che il risultato non è valido.

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

Contenuto delle variabili di output correnti:

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

Il comando NUMTOIP converte un numero in indirizzo IP. Per ulteriori informazioni, vedere NUMTOIP.

LENGTH o LENGTH-OPTION2

Il comando LENGTH imposta una variabile numerica dalla lunghezza in byte di una variabile di tipo stringa, senza tenere conto della terminazione zero.

> **NOTA**: Nell'ambito dell'editor visuale del Generatore servizi di raccolta, LENGTH e LENGTH-OPTION2 vengono elencati come comandi separati. Corrispondono allo stesso comando. Vengono forniti come descrizioni delle diverse variazioni dello stesso comando. Per utilizzare LENGTH-OPTION2 nell'editor di testo, sarà necessario immettere LENGTH.

Formato

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

Tipi di dati

Argomento	Tipo	Descrizione
s_variable	stringa (INPUT)	La stringa, in genere una variabile di tipo stringa, in cui viene calcolata la lunghezza.
i_length	variabile numerica (OUTPUT)	La lunghezza della variabile di tipo stringa, s_variable, viene collocata in questa variabile numerica.

Ad esempio:

```
LENGTH(i_length, source)
LENGTH(i_num_bytes, "It makes no sense to do this, as we
   know the string whose length we are checking")
```

Risultati:

```
i_num_bytes = 80
```

LOOKUP

Il comando LOOKUP corrisponde ai dati trovati nel buffer di ricezione o in una stringa con stringhe chiave di un file chiave di ricerca specificato.

Se un record corrisponde ai dati byte per byte, verranno elaborati i comandi di analisi sintattica nel record del file chiave di ricerca.

Se viene specificata una stringa come primo parametro del comando LOOKUP, il comando LOOKUP utilizza tale stringa durante la ricerca del file chiave di ricerca.

Vi sono cinque argomenti o parametri con questo comando.

- compare – Se come parametro viene specificato un valore numerico, il numero di byte (valore numerico) di dati dal buffer di ricezione, con inizio dalla posizione del puntatore del buffer Rx, viene utilizzato come stringa durante il confronto con le stringhe chiave del file di ricerca.
- lookup name – Questo parametro specifica il nome del file chiave di ricerca relativo alla directory WORKBENCH_HOME.
- imatch – Una variabile di tipo intero facoltativa che può essere specificata e che restituisce lo stato del comando LOOKUP. (0=nessuna corrispondenza trovata, 1=corrispondenza trovata).
- parameter file – Un parametro facoltativo che rappresenta il nome di un parametro da utilizzare al posto del file di parametri predefinito. Il nome del file di parametri predefinito è <Collector>.par. Questo nome file non deve includere il suffisso .par.
- column name – Un parametro opzionale è la colonna con il file di parametri da utilizzare per i valori di ricerca. Il nome colonna predefinito è il nome del modello. Se si specifica questo parametro, è anche necessario utilizzare un nome file di parametri.

Formato

```
LOOKUP(compare, lookup filename [, imatch] [, [parameter
   filename] [, column name]])
```

Tipi di dati

Argomento	Tipo	Descrizione
compare	stringa (INPUT) oppure di tipo numerico (INPUT)	I dati da utilizzare per il confronto con i campi nel file chiave di ricerca. Si tratta di un confronto byte per byte. Il numero dei byte dal buffer di ricezione, utilizzando la posizione del puntatore del buffer Rx, da utilizzare per il confronto con i campi del file chiave di ricerca. Si tratta di un confronto byte per byte. **NOTA:** Ciò funziona soltanto se rxbuff è stato utilizzato per impostare il buffer di ricezione.
lookup filename	stringa (INPUT)	Il nome del file chiave di ricerca
imatch	variabile numerica (OUTPUT) [FACOLTATIVO]	È stata trovata una corrispondenza. 0=No 1=Yes
parametro nome file	stringa (INPUT)	Nome file di parametri. Valore di default: Collector.par
column name	stringa (INPUT)	La colonna all'interno del file di parametri da utilizzare. Valore di default: Nome servizio di raccolta

Ad esempio:

```
LOOKUP(data, filename, imatch)
```

Nell'esempio seguente, il nome file key_01 viene determinato dal nome inserito nel file di parametri, non dal nome file chiave di ricerca.

```
LOOKUP(s_variable, {key_01})
LOOKUP(s_variable, {key_01}, imatch, "Send One Alert",
   "GeoElements")
```

Se nel file di ricerca vi sono definizioni dei parametri, è possibile individuarle nella colonna GeoElements del file dei parametri Send One Alert.

NEGSEARCH

Il comando NEGSEARCH esegue la ricerca indietro di una stringa nel buffer di ricezione. Questo comando richiede due parametri.

- search – La ricerca inizia dalla posizione del puntatore del buffer Rx corrente e continua all'indietro fino a trovare la stringa oppure fino all'inizio del buffer di ricezione. Se la ricerca trova una stringa, il puntatore del buffer Rx viene aggiornato in modo da puntare al primo byte della stringa di ricerca. Se la ricerca non trova la stringa, il puntatore del buffer Rx rimane invariato.
- ifound – Un parametro opzionale, è una variabile di tipo intero impostata su 1 se la ricerca trova la stringa e su zero se la ricerca non restituisce alcun risultato.

Formato

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

Tipi di dati

Argomento	Tipo	Descrizione
search	stringa (INPUT)	La stringa ricercata nel buffer di ricezione, con inizio dalla posizione del puntatore del buffer Rx corrente e la ricerca indietro.
ifound	variabile numerica (OUTPUT) (FACOLTATIVO)	Restituisce un valore che indica se la stringa di ricerca è stata trovata o meno. 0=non trovato 1=trovato

Ad esempio:

```
NEGSEARCH("MINOR ALARM")
NEGSEARCH(search_string)
```

Negli esempi seguenti viene eseguita la ricerca di un ritorno a capo e di un avanzamento riga:

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

Altro esempio:

La lettera con sottolineatura rappresenta la posizione del puntatore del buffer Rx corrente nell'esempio.

NOTA: Per la sostituzione esadecimale, \0000\ termina una stringa; quindi, “xxxx\0000\yyyy” diventa “xxxx”.

```
Buffer di ricezione = "Minor Alarm Radio A"
NEGSEARCH("Ala")
```

Risultato:

```
Buffer di ricezione = "Minor Alarm Radio A"
```

NUMTOHEX

Il comando NUMTOHEX converte un valore numerico in dati esadecimali e colloca gli esadecimali (fino a 4 byte) in una stringa.

Formato

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

Tipi di dati

Argomento	Tipo	Descrizione
i_decimal	di tipo numerico (INPUT)	Valore intero da convertire in dati esadecimali.
hex_data	svar (OUTPUT)	Stringa da 1 a 4 byte che sono byte esadecimali forniti dal valore numerico, i_decimal.

Ad esempio:

Nell'esempio seguente, il valore decimale 16777215 viene convertito in dati esadecimali.

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

Contenuto delle variabili di output correnti:

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

NUMTOIP

Il comando NUMTOIP converte un valore numerico in un indirizzo IPv4 e colloca l'indirizzo IP in una stringa.

Formato

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

Tipi di dati

Argomento	Tipo	Descrizione
i_integer	numeric(INPUT)	Valore intero da convertire in indirizzo IPv4.
ip_address	svar(OUTPUT)	Indirizzo IPv4 di tipo stringa

Ad esempio:

Nell'esempio seguente, il valore decimale 16777215 viene convertito in indirizzo IPv4.

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

Contenuto delle variabili di output correnti:

```
s = "10.0.0.1"
```

Il comando IPTONUM converte un indirizzo IP in un numero. Per ulteriori informazioni, vedere IPTONUM.

PARSER_ATTACHVARIABLE

Il comando PARSER_ATTACHVARIABLE consente di associare il nome della copia name-value a target_variable.

Nella maggior parte dei casi è consigliabile creare un analizzatore sintattico e collegare una variabile nello stato di inizializzazione all'esterno del ciclo. Sarà quindi possibile riutilizzare l'analizzatore sintattico in questione nel ciclo di analisi sintattica.

Per comandi di analisi sintattica correlati, vedere PARSER_CREATEBASIC e PARSER_PARSESTRING.

Analizzatore NVP (coppia Name-value)

Il seguente frammento di codice dimostra l'analizzatore NVP:

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

Parametri

I parametri seguenti vengono riconosciuti quando appaiono nel seguente formato:

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

<parameter> è uno degli elementi in basso e <value> è un valore appropriato per tale parametro.

- separator – il carattere utilizzato per separare il nome dal valore
- entry_separator – il carattere utilizzato per separare una coppia name-value dalla successiva
- name_quotes – il carattere utilizzato per racchiudere il nome (ad esempio " o ')
- value_quotes – il carattere utilizzato per racchiudere il valore

- name_quoted – impostare su Sì per consentire all'analizzatore NVP di osservare l'opzione name_quotes
- value_quoted - impostare su Sì per consentire all'analizzatore NVP di osservare l'opzione name_quotes
- name_quotes_optional – impostare su Sì per consentire l'inserimento di virgolette nel nome. Se è impostata su Sì e le virgolette vengono omesse, uno spazio vuoto facoltativo seguito dal separatore farà da terminazione al nome.
- value_quotes_optional – impostare su Sì per consentire l'inserimento di virgolette nel nome

Se è impostata su Sì e le virgolette vengono omesse, uno spazio vuoto facoltativo seguito da entry_separator farà da terminazione al nome.

Formato

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

Tipi di dati

Argomento	Tipo	Descrizione
parser_handle	variabile di tipo stringa (INPUT)	La variabile handle di un analizzatore sintattico creato.
nome	string (INPUT)	Il nome della coppia name-value.
target_variable	qualsiasi variabile (OUTPUT)	La variabile che verrà impostata al valore associato al nome della copia name-value.

Di seguito viene riportato un esempio di analizzatore sintattico dei punti di controllo.

```
COLLECTOR SETUP STATE:
PARSER_CREATEBASIC(h_nvp,"nvp", "separator==",
   "entry_separator= ", "value_quotes=/"",
   "value_quotes_optional=yes")
PARSER_ATTACHVARIABLE(h_nvp,"action", 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

Il comando PARSER_CREATEBASIC definisce un analizzatore e lo associa a parser_handle. Per ulteriori informazioni, vedere Analizzatore sintattico NVP (coppia nome-valore) in PARSER_ATTACHVARIABLE.

Nella maggior parte dei casi è consigliabile creare un analizzatore sintattico e collegare una variabile nello stato di inizializzazione all'esterno del ciclo. Sarà quindi possibile riutilizzare l'analizzatore sintattico in questione nel ciclo di analisi sintattica.

Per un altro comando di analisi sintattica correlato, vedere il comando PARSER_PARSESTRING.

Formato

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

Tipi di dati

Argomento	Tipo	Descrizione
parser_handle	variabile di tipo stringa (OUTPUT)	La variabile a cui l'analizzatore farà riferimento da questo punto in avanti.
parser_name	string (INPUT)	Il nome della stringa dell'analizzatore semplice da creare. **NOTA:** Al momento, viene riconosciuto solo l'analizzatore Nvp.
nvp	string (INPUT) (FACOLTATIVO)	La coppia name-value. Zero o più stringhe contenenti il nome di una proprietà, seguite da un segno di uguale, seguito da un valore. I parametri che vengono riconosciuti sono determinati dal parser_name scelto. **NOTA:** Quando il nome dell'analizzatore viene impostato su nvp, sarà necessario utilizzare i seguenti argomenti: "separator==" "entry_separator= " "value_quotes=/"" "value_quotes_optional=yes"
nvp1	string (INPUT) (FACOLTATIVO)	Coppia nome-valore 1.
nvp2	string (INPUT) (FACOLTATIVO)	Coppia nome-valore 2.
…	string (INPUT) (FACOLTATIVO)	Altre coppie name-value.

Per un esempio, vedere l'esempio di analizzatore sintattico dei punti di controllo in PARSER_ATTACHVARIABLE.

PARSER_NEXT

Il comando PARSER_NEXT fa avanzare l'analizzatore alla posizione successiva nella stringa di analisi inserendo le variabili impostate dal comando PARSER_ATTACHVARIABLE.

Formato

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

Tipo di dati

Argomento	Tipo	Descrizione
parser_handle	stringa variabile (INPUT)	La variabile handle di un analizzatore sintattico creato.
success_flag	variabile numerica (INPUT)	0: analisi non completata correttamente 1: analisi completata correttamente

PARSER_PARSESTRING

Il comando PARSER_PARSESTRING elabora string_to_parse utilizzando l'analizzatore creato a cui fa riferimento parser_handle. Ciò consente di creare eventuali stringhe arbitrarie per l'analisi, invece di continuare con una origine di flusso o con il buffer Rx.

Per ulteriori informazioni, vedere il comando PARSER_ATTACHVARIABLE e il comando PARSER_CREATEBASIC.

La variabile riservata s_RXBufferString può essere utilizzata come string_to_parse dopo che lo stato Ricezione analizza l'input di script. Per ulteriori informazioni, vedere Analizzatore sintattico NVP (coppia nome-valore) in PARSER_ATTACHVARIABLE.

Formato

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

Tipi di dati

Argomento	Tipo	Descrizione
parser_handle	stringa variabile (INPUT)	La variabile handle di un analizzatore sintattico creato.
string_to_parse	stringa (INPUT)	La singola stringa che verrà eseguita attraverso questo analizzatore.

Per un esempio, vedere l'esempio di analizzatore sintattico dei punti di controllo in PARSER_ATTACHVARIABLE.

PAUSE

il comando PAUSE consente di mettere immediatamente in pausa lo script corrente per "n" numero di secondi. Il comando PAUSE opera tra istruzioni in stato di analisi e tra stati. Il comando PAUSE è utile per impostare i tempi dei cicli di polling o per assicurare che il polling non venga eseguito troppo rapidamente, ad esempio il polling di un log di database.

È possibile specificare più comandi PAUSE durante l'analisi.

Formato

```
PAUSE(iseconds)
```

Argomento	Tipo	Descrizione
iseconds	di tipo numerico (INPUT)	Numero di secondi di pausa prima di passare allo stato successivo.

Ad esempio:

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

Oppure

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

POPUP

Il comando POPUP visualizza il contenuto di una stringa in una finestra di testo scorrevole.

Formato

```
POPUP(data [, title])
```

Tipi di dati

Argomento	Tipo	Descrizione
dati	stringa (INPUT)	Il messaggio della stringa di dati da collocare nella finestra di popup.
titolo	stringa (INPUT) [FACOLTATIVO]	La stringa da utilizzare come titolo della finestra di popup (impostazione di default = "Popup DATA").

Ad esempio:

```
POPUP(data)
POPUP("Hello World", "Title String")
POPUP(data, title)
```

PRINTF

Il comando PRINTF copia dati formattati in una variabile di tipo stringa (svar). Il comando PRINTF è un comando di analisi sintattica avanzato. Se non si ha familiarità con il linguaggio dei comandi di analisi sintattica, considerare l'utilizzo del comando COPY e del comando APPEND fin quando non si sia presa dimestichezza con il linguaggio.

Quando si utilizza questo comando:

- Specificare una variabile svar come stringa di destinazione.
- Specificare una stringa di formato.
- Specificare eventuali parametri aggiuntivi da analizzare in base alla stringa di formato.

Stringa di formato

Per utilizzare dati esadecimali nella stringa di formato, avvalersi della seguente convenzione:

```
\HX HX HX\
```

Se si desidera includere un avanzamento di riga alla fine della stringa di formato, quest'ultima dovrà avere l'aspetto della stringa seguente:

```
Format String\0a\
```

La stringa di formato per un ritorno a capo è \0d0a\, ad esempio:

```
PRINTF(message,"Voltage is %lf \0d0a\",f_volts)
```

La stringa di formato per una tabulazione è \09\, ad esempio:

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

Formato

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

dove:

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

Tipi di dati

Argomento	Tipo	Descrizione
dest	svar (OUTPUT)	La variabile di tipo stringa di destinazione in cui collocare la stringa formattata.
formato	stringa (INPUT)	Il formato di una stringa da copiare nella variabile di tipo stringa di destinazione. Simile al formato del comando C printf, ad esempio, "Looping %d in %s" (vedere % Caratteri di formato di output).
parm1	tutti (INPUT) [FACOLTATIVO]	Tutti i tipi di dati tranne le matrici. Deve corrispondere alla stringa di formato.
parm2	tutti (INPUT) [FACOLTATIVO]	Tutti i tipi di dati tranne le matrici. Deve corrispondere alla stringa di formato.

Argomento	Tipo	Descrizione
…	tutti (INPUT) [FACOLTATIVO]	Tutti i tipi di dati tranne le matrici. Deve corrispondere alla stringa di formato.

Formato

```
% Caratteri di formato di output
```

Carattere	Tipo	Formato di output
%d	intero	Intero decimale con segno.
%le	float	Valore con segno in formato [-]d.dddd e [sign]ddd ...dove d è costituito da una singola cifra decimale, dddd è costituito da una o più cifre decimali, ddd è costituito esattamente da tre cifre decimali e il segno è + o -.
%lf	float	Valore con segno in formato [-]dddd.dddd ...dove dddd è costituito da una o più cifre decimali. Il numero di cifre prima del punto decimale dipende dalla grandezza del numero e il numero di cifre dopo il punto decimale dipende dalla precisione richiesta.
%lg	float	Valore con segno stampato in formato f o e, quale dei due sia più compatto per un determinato valore e precisione. Il formato e viene utilizzato solo quando l'esponente del valore è minore di -4 o maggiore o uguale rispetto all'argomento di precisione. Gli zero finali sono troncati e il punto decimale è visibile solo se seguito da uno o più cifre.
%s	stringa	Stampare una variabile di tipo stringa.

Visualizzazione di cifre di precisione

Di default, il comando PRINTF visualizza un numero con virgola mobile in sei cifre di precisione. Le sei cifre di precisione di default sono applicabili anche ai numeri di precisione doppi.

Per visualizzare cifre di precisione aggiuntive, specificare un valore per il campo relativo alla precisione nel formato PRINTF():

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

Ad esempio:

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

Verrà prodotto come risultato: 22.012, che rappresenta 2 posizioni a sinistra del punto decimale e 3 posizioni a destra del punto decimale.

Gli esempi seguenti mostrano come passare variabile di tipo intero e di tipo stringa.

```
PRINTF(dest,format_string) PRINTF(mystring,
   "val of matrix[%d][%d] = %s",
   index_x, index_y, matrix[index_x][index_y])
```

```
PRINTF(dest,"Looping %d in state %s",iloop,state)
PRINTF(dest,"Formatted %s Data into %s","string","dest")
```

L'esempio seguente mostra come passare da una variabile di tipo float a una variabile di tipo stringa.

```
PRINTF(message,"Voltage is %lf",f_volts)
```

Per stampare numeri con virgola mobile, utilizzare %lf or %le.

REGEXPREPLACE

Il comando REGEXPREPLACE trova e sostituisce stringhe utilizzando espressioni regolari. Quando la ricerca trova la stringa, sostituisce la stringa regexpreplace. Il comando REGEXPREPLACE esegue una sostituzione globale, non sostituisce solo la prima occorrenza.

Formato

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

Tipi di dati

Argomento	Tipo	Descrizione
dest_string	svar (INPUT/ OUTPUT)	Variabile di tipo stringa in cui verranno sostituiti i byte.
search	stringa (INPUT) oppure svar (INPUT/ OUTPUT)	Stringa di ricerca da sostituire.
replace	stringa (INPUT) Oppure svar (INPUT/ OUTPUT)	La stringa di sostituzione può essere di lunghezza pari a zero per indicare una stringa NULL.

Ad esempio:

```
COPY(string:"La prima volta")
REGEXREPLACE(string, "1st", "2nd")
```

Risultato:

```
string = "La seconda volta"
```

NOTA: in questo esempio, è possibile sostituire un'espressione regolare per la

```
prima stringa ("1st").
```

Sostituzione con una stringa NULL

```
COPY(string:"La prima volta")
```

```
REGEXPREPLACE(string, "1st", "")
```

Risultato:

```
string="The time"
```

Per ulteriori informazioni sulle espressioni regolari e il set di caratteri di tipo "portable", vedere Espressioni regolari.

Sentinel utilizza una libreria compatibile con POSIX (Portable Operating System Interface for UNIX) per le espressioni regolari. POSIX è il nome di un insieme di standard IEEE e ISO che contribuiscono ad assicurare la compatibilità fra una serie di sistemi operativi, tra cui la più ampia varietà di piattaforme UNIX.

REGEXPSEARCH, REGEXPSEARCH_EXPLICIT o REGEXPSEARCH_STRING

Il comando REGEXPSEARCH esegue una ricerca in avanti nel buffer di ricezione (buffer Rx) o variabile di tipo stringa di input designata di una stringa utilizzando espressioni regolari. Supporta inoltre gruppi di espressioni.

NOTA: Nell'ambito dell'editor visuale del Generatore servizi di raccolta, REGEXPSEARCH, REGEXPSEARCH_EXPLICIT o REGEXPSEARCH_STRING vengono elencati come comandi separati. Corrispondono allo stesso comando. Vengono forniti come descrizioni delle diverse variazioni dello stesso comando. Per utilizzare REGEXPSEARCH_EXPLICIT o REGEXPSEARCH_STRING nell'editor di testo, sarà necessario immettere REGEXPSEARCH.

Buffer di ricezione

La ricerca all'interno del buffer di ricezione avviene secondo quanto segue:

- La ricerca inizia nella posizione corrente del puntatore del buffer di ricezione e continua in avanti fino all'individuazione della stringa o al raggiungimento della fine del buffer di ricezione.
- Se viene individuata la stringa, il puntatore del buffer di ricezione viene aggiornato per fare riferimento al primo byte della stringa ricercata. La posizione del puntatore del buffer Rx viene mantenuta durante la transizione tra stati a meno che non venga utilizzato il comando RESET.
- Se la ricerca non trova la stringa, il puntatore del buffer Rx non viene modificata.

Quando si utilizza questo comando per cercare il buffer di ricezione, il secondo parametro opzionale è una variabile di tipo intero impostata su 1 se la ricerca trova la stringa e impostata su 0 se la ricerca non trova la stringa.

Variabile di tipo stringa

Le variabili di tipo stringa non supportano il puntatore di analisi, di conseguenza le dinamiche di ricerca in una variabile di tipo stringa sono differenti. Lo schema delle espressioni regolari può corrispondere ad alcune o a tutte le stringhe di input. Se lo schema delle espressioni regolari è

configurato con gruppi di espressioni, il contenuto della stringa di input che corrisponde ai gruppo di espressioni può essere memorizzato in variabili di output. Vi sono due opzioni di output per il raggruppamento di espressioni. Una consiste nel popolare un elenco di variabili in base all'ordine dei gruppi di espressioni e l'altra consiste nel designare una matrice di stringhe.

Se l'espressione regolare corrisponde alla variabile di tipo stringa-input, un elenco designato di variabili o matrici di output viene impostato con il gruppo di valori e la variabile trovata viene impostata su un numero superiore rispetto al numero di gruppi o zero in base alla mancata corrispondenza.

Quando l'output dei valori di gruppo deve essere una matrice della stringa, il primo elemento indicizzato con "0" conterrà la stringa corrispondente. La stringa corrispondete contiene il contenuto che corrisponde all'intera espressione regolare indipendente o ai gruppi di espressioni. Di conseguenza, il contenuto del gruppo della prima espressione verrà memorizzato nella posizione di matrice indicizzata con "1". Durante il ciclo della matrice dell'output, tenere presente che il valore i_Found_Tokens è a compensazione del primo elemento che coincide con la stringa corrispondente ed è sempre maggiore rispetto al numero totale dei gruppi. Durante un ciclo, la condizione di interruzione è minore del valore i_Found_Tokens ancora in funzione, ma è possibile iniziare l'indice da "1" invece che da "0".

Al momento della designazione dei valori di gruppo da memorizzare in un elenco di variabili di output invece che in una matrice, il comando è in grado di eseguire la conversione dei tipi. Nonostante la stringa di input sia di tipo stringa, i componenti all'interno della stringa possono essere numerici. Se l'intento è di trattare tali numeri come valori interi o con virgola mobile, designando semplicemente le variabili di output con il tipo corretto verrà eseguita la conversione.

Corrispondenza REGEX semplice

Espressione	Descrizione
.	Qualsiasi carattere
\d	Qualsiasi cifra
\w	Qualsiasi carattere alfanumerico
\s	Qualsiasi spazio vuoto
+	1 o più dei precedenti
*	0 o più dei precedenti

Formato

Come buffer di ricezione:

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

Come variabile di tipo stringa:

```
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, ...)]
```

Tipi di dati

Argomento	Tipo	Descrizione
s_Input_String	Stringa o variabile di tipo stringa (INPUT) [FACOLTATIVO]	La stringa o la variabile di tipo stringa da ricercare per corrispondenze regex specificate in regex.
s_Regular_Exp_Pattern	Stringa (INPUT)	La stringa da ricercare nel buffer di ricezione (ricerca dalla posizione del puntatore del buffer Rx in avanti), variabile letterale di tipo stringa di input o una variabile di tipo stringa di input.
i_Found_Tokens	variabile numerica (OUTPUT) [FACOLTATIVO]	Restituisce un valore che indica se la stringa di ricerca è stata trovata o meno. 0: Lo schema delle espressioni regolari non corrisponde 1: Lo schema delle espressioni regolari corrisponde ma non è stato designato alcun gruppo di espressioni 2: Lo schema di espressioni regolari corrisponde al gruppo di espressioni 1 designato N+1: Lo schema di espressioni regolari corrisponde ai gruppi di espressione N designati **NOTA:** La variabile I_found_tokens può essere utilizzata come testo per le corrispondenze, dal momento che il valore sarà diverso da zero quando l'espressione regolare corrisponde.
s_Match	Stringa (OUTPUT) [CONDITIONAL]	Viene popolata solo su corrispondenza di schema e deve essere designata quando viene utilizzato un elenco di variabili di output di gruppi di espressioni. Quando i valori dei gruppi vengono memorizzati in una matrice di output, s_Match NON sarà un parametro valido.
Elenco di variabili OPPURE s_Output_Results[]	Tutte le variabili possibile (OUTPUT) [FACOLTATIVO] OPPURE Matrice di stringhe (OUTPUT) [FACOLTATIVO]	L'elenco delle variabili in cui collocare i valori dei gruppi. L'assegnazione del valore avviene in base ai valori dei gruppi designati in presenza delle seguenti regole di precedenza.

Negli esempi seguenti viene eseguita la ricerca di un ritorno a capo e di un avanzamento di riga nel buffer di ricezione:

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

Nell'esempio seguente viene eseguita la ricerca della parola "alarm" nel buffer di ricezione:

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

NOTA: Per la sostituzione esadecimale, \0000\ termina una stringa; quindi, "xxxx\0000\yyyy" diventa "xxxx".

Un esempio dettagliato della ricerca di uno schema nell'ambito di un valore di stringa letterale:

```
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)
```

Dove,

```
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
```

Per ulteriori informazioni sulle espressioni regolari e il set di caratteri di tipo "portable", vedere la sezione Espressioni regolari nel Capitolo 2.

Sentinel utilizza una libreria compatibile con POSIX (Portable Operating System Interface for UNIX) per le espressioni regolari. POSIX è il nome di un insieme di standard IEEE e ISO che contribuiscono ad assicurare la compatibilità fra una serie di sistemi operativi, tra cui la più ampia varietà di piattaforme UNIX.

REPLACE

Il comando REPLACE trova e sostituisce stringhe utilizzando espressioni regolari.

Quando la stringa viene individuata, viene sostituita con una stringa di sostituzione specificata. Il comando REPLACE effettua un sostituzione globale, non limitata alla prima occorrenza.

Formato

```
REPLACE(dest_string, search, replace)
```

Tipi di dati

Argomento	Tipo	Descrizione
dest_string	svar (INPUT/ OUTPUT)	Variabile di tipo stringa in cui verranno sostituiti i byte.
search	stringa (INPUT)	Stringa di ricerca da sostituire.

Argomento	Tipo	Descrizione
replace	stringa (INPUT)	La stringa di sostituzione.

Ad esempio:

```
COPY(string:"La prima volta")
REPLACE(string, "1st", "2nd")
```

Risultato:

```
string = "La seconda volta"
```

NOTA: In questo esempio, è possibile sostituire un'espressione regolare per la stringa "1st".

RESET

Il comando RESET reimposta il puntatore del buffer Rx su zero.

Formato

```
RESET()
```

Ad esempio, la posizione del puntatore del buffer è indicata dal simbolo ^.

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

Risultato:

```
"abcdefg"
 ^
```

RXBUFF

Il comando RXBUFF sovrascrivere il contenuto del buffer di ricezione con quello di una stringa o di una variabile stringa. I contenuti del buffer di ricezione verranno modificati immediatamente e il valore del puntatore del buffer Rx verrà reimpostato su zero.

Formato

```
RXBUFF(s_data)
```

Tipi di dati

Argomento	Tipo	Descrizione
s_data	stringa (INPUT)	La stringa di dati da scrivere nel buffer di ricezione. Questa stringa rappresenterà immediatamente la nuova stringa del buffer di ricezione.

Ad esempio:

Nell'esempio seguente, il comando FILER legge un file denominato alert.data e ne inserisce i contenuti in una variabile stringa denominata s_data. Ai fini di questo esempio si presuppone che:

```
alert.data: "Minor Alarm Xterminal A"
```

Quindi, il comando RXBUFF inserisce i dati nel buffer di ricezione, come se tali dati fossero stati ricevuti da una porta.

```
FILER("alert.data", s_data)
RXBUFF(s_data)
//copia i dati dal buffer Rx in S_Alarm_Priority,
   interrompendosi prima della stringa "Alarm")
COPY(S_Alarm_Priority:," Alarm")
```

Risultato:

```
S_Alarm_Priority= "Minor"
```

SEARCH

Il comando SEARCH esegue la ricerca in avanti di una stringa nel buffer di ricezione (buffer Rx).

La ricerca viene effettuata nel modo seguente:

- La ricerca inizia nella posizione corrente del puntatore del buffer di ricezione e continua in avanti fino all'individuazione della stringa o al raggiungimento della fine del buffer di ricezione.
- Se viene individuata la stringa, il puntatore del buffer di ricezione viene aggiornato per fare riferimento al primo byte della stringa ricercata. La posizione del puntatore del buffer Rx viene mantenuta al passaggio tra gli stati a meno che non venga modificata in modo esplicito mediante il comando RESET.
- Se la stringa non viene individuata, il puntatore del buffer Rx non viene spostato.

Quando si utilizza questo comando, il secondo parametro facoltativo è una variabile numero intero impostata su 1 se la ricerca trova la stringa e su 0 se invece la ricerca ha esito negativo.

Formato

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

Tipi di dati

Argomento	Tipo	Descrizione
search	stringa (INPUT)	La stringa da cercare nel buffer di ricezione a partire dalla posizione attuale del puntatore del buffer Rx).
ifound	variabile numerica (OUTPUT) [FACOLTATIVO]	Restituisce un valore che indica se la stringa di ricerca è stata trovata o meno. 0 = non trovata 1 = trovata

Ad esempio:

Negli esempi seguenti viene cercato un ritorno a capo e un avanzamento di riga.

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

L'esempio seguente consente di cercare la parola alarm:

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

NOTA: Per la sostituzione esadecimale, \0000\ termina una stringa; quindi, "xxxx\0000\yyyy" diventa "xxxx".

SET

Il comando SET elabora un'espressione matematica e aggiorna un valore numerico (numvar) con il risultato della valutazione.

Quando si utilizza questo comando:

- Specificare un numvar di destinazione seguito da un segno di uguale, a sua volta seguito da una combinazione di ( ) - + * / e variabili numeriche.
- È necessario specificare almeno un elemento numerico a destra del segno di uguale.
- Non vi sono limitazioni al numero di parentesi consentite.
- Tutti gli argomenti vengono convertiti in tipo float; il risultato viene convertito nel tipo (intero float) del numvar di destinazione.
- È possibile immettere fino a 98 voci dopo il segno di uguale, tra cui: (,), *, /, +, -, qualsiasi numero e variabile numerica.
- Quando le operazioni hanno lo stesso ordine del livello di operazione, vengono gestite da sinistra a destra. L'ordine delle operazioni è descritto nella tabella seguente.

Livello 1	:	()	ad esempio: parentesi
Livello 2	:	*/	ad esempio: moltiplicazione, divisione
Livello 3	:	+ -	ad esempio: addizione, sottrazione

Formato

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

Dove:

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

Tipo di dati

Argomento	Tipo	Descrizione
idest	variabile numerica (OUTPUT)	La variabile numerica (fvar o ivar) nel quale il valore verrà salvato.
inum1	di tipo numerico (INPUT)	Valore fvar, ivar o numerico.

Argomento	Tipo	Descrizione
inum2	di tipo numerico (INPUT) [FACOLTATIVO]	Valore fvar, ivar o numerico.
inum3	di tipo numerico (INPUT) [FACOLTATIVO]	Valore fvar, ivar o numerico.
…	di tipo numerico (INPUT) [FACOLTATIVO]	Valore fvar, ivar o numerico.

Ad esempio:

```
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

Il comando SETBYTES consente di impostare i byte all'interno di una variabile stringa su un determinato valore, passato come intero o come stringa. Se passato come intero, gli intervalli validi sono compresi tra 0 e 255. Se una stringa viene utilizzata come parametro di sostituzione, allora la string viene inserita all'inizio e della posizione di indice nella variabile stringa di destinazione.

Formato

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

Tipi di dati

Argomento	Tipo	Descrizione
dest_string	svar (INPUT/ OUTPUT)	Variabile di tipo stringa in cui verranno sostituiti i byte.
index	di tipo numerico (INPUT)	L'indice (conteggio dei byte a partire da 0 per il primo) in dest_string in cui i byte verranno utilizzati per la sostituzione.
replace	stringa (INPUT) Oppure intero (INPUT)	I byte stringa che verranno sovrascritti in dest_string. Il valore da impostare il byte numero # dell'indice nella stringa di destinazione.

Ad esempio:

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

Contenuto delle variabili di output correnti:

```
stringa = "Bandwidth Util. = 44%"
```

SETCONFIG

Questo comando imposta una proprietà di sistema. L'impostazione attuale della proprietà di sistema può essere recuperata mediante il comando GETCONFIG. Tali comandi vengono utilizzati per impostare le proprietà e recuperare i valori attuali delle proprietà di sistema che possono cambiare periodicamente, ad esempio un file di log rinominato quotidianamente con la data attuale.

Proprietà di sistema disponibili:

Proprietà di sistema	Esempi
▪ 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	elenco di indirizzi IP di questo host separati da un punto e virgola, ad esempio "172.163.3.45;172.45.2.1"

Vedere anche il comando GETCONFIG.

Questo comando richiede due parametri.

- Il primo parametro obbligatorio definisce l'opzione di configurazione (“FileConnector.InputFile” o “FileConnector.OutputFile”) da impostare.
- Il secondo parametro obbligatorio definisce il valore di configurazione da impostare.

Formato

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

Tipi di dati

Argomento	Tipo	Descrizione
Config Option	string (INPUT)	Nome della variabile di configurazione da impostare. File di input = “FileConnector.InputFile” File di output = “FileConnector.InputFile”
Valore	stringa svar (INPUT)	Impostazione di configurazione.

Ad esempio:

```
SETCONFIG(“FileConnector.InputFile”, s_inputfilename)
SETCONFIG(“FileConnector.OutputFile”, s_outputfilename)
```

Contenuto delle variabili di output correnti:

```
“C:/\test.dat”
```

SHELL

Il comando SHELL esegue uno script o un comando della shell.

Formato

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

Tipi di dati

Argomento	Tipo	Descrizione
comando	stringa (INPUT)	Il percorso e il nome file del comando da eseguire. Per default, viene utilizzata la variabile di ambiente PATH.
wait/no_wait	variabile numerica [FACOLTATIVO]	Consente al comando SHELL di attendere o non attendere il completamento dell'esecuzione del programma avviato prima di continuare l'elaborazione. 0 = no_wait (nessuna attesa) 1 = attesa del completamento del programma
return_status	variabile numerica [FACOLTATIVO]	Valore numerico quando si utilizzano le opzioni wait/no_wait. ESITO POSITIVO = 1 ESITO NEGATIVO = 0

L'esempio seguente avvia un file batch di PC o uno script di shell UNIX:

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

L'esempio seguente avvia Blocco note:

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

L'esempio seguente attende che venga completata l'esecuzione del comando clock:

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

L'esempio seguente attende il completamento dell'esecuzione di un file batch di PC o di uno script di shell UNIX e quindi ne recupera lo stato restituito:

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

L'esempio seguente esegue il processo clock e non ne attende il completamento:

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

SKIP

Il comando SKIP aggiunge un numero al valore del puntatore del buffer Rx.

Il numero può essere positivo o negativo. Se la posizione del puntatore del buffer Rx è minore di zero, il puntatore verrà comunque impostato su zero. Se la posizione del puntatore del buffer Rx

risultate supera la fine del buffer di ricezione, il puntatore viene spostato all'ultimo byte nel buffer di ricezione.

Formato

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

Tipi di dati

Argomento	Tipo	Descrizione
iskip_amount	di tipo numerico (INPUT)	Il numero di byte di cui spostare Rx.

Ad esempio:

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

Di seguito sono disponibile alcuni esempi che illustrano la posizione del puntatore del buffer di ricezione dopo un comando SKIP, per i dati:

```
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

Il comando SKIPWORD modifica il puntatore del buffer Rx in modo che punti all'inizio di una parola.

Questo comando considera una parola come una sequenza continua di byte stampabili sparati da almeno un byte non stampabile. I byte stampabili vengono definiti come ASCII e ASCII-0-255 estesi (per ISO 8859-1).

Utilizzando i valori positivi e negativi di passaggio, il puntatore del buffer Rx si sposta in avanti o indietro al primo o al successivo byte stampabile nel buffer di ricezione.

Il puntatore del buffer Rx non si sposterà oltre la fine del buffer o prima del suo inizio, anche se il comando SKIPWORD determinasse tale condizione.

Un valore pari a zero non determina alcuna modifica al puntatore del buffer Rx. Il comando SKIPWORD tratta tutti i caratteri inferiori a 33 e compresi tra 126 e 161 come spazi.

Formato

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

Tipi di dati

Argomento	Tipo	Descrizione
iwords	di tipo numerico (INPUT)	Il numero di parole di cui il puntatore deve spostarsi nel buffer di ricezione.

Ad esempio:

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

Di seguito sono disponibile alcuni esempi che illustrano la posizione del puntatore del buffer di ricezione dopo un comando SKIPWORD, per i dati:

```
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

Il comando SOCKETW esegue un'apertura, una connessione, una scrittura di dati in un socket (porta TCP e IP) di tipo NON-BLOCKING (socket STREAM di byte di rete) e quindi chiude il socket. Facoltativamente può restituire lo stato del tentativo di scrittura socket.

Formato

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

Tipi di dati

Argomento	Tipo	Descrizione
address	stringa (INPUT)	Indirizzo IP del socket.
i_port	di tipo numerico (INPUT)	Numero di porta TCP del socket.
data	stringa (INPUT)	Stringa di dati da scrivere sul socket.
istat	variabile numerica (OUTPUT)	Stato restituito (facoltativo). istat = numero di byte scritti > 0 (esito positivo) istat = 0 (esito negativo)

Esempi:

```
SOCKETW("192.168.15.25", 5051, "Data Write Socket")
SOCKETW("192.168.15.25", i_port, "Data to Socket\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

Il comando STONUM (string to number, da stringa a numero) converte una variabile stringa (svar) in variabile numerica (numvar).

ATTENZIONE: Variabili stringa costituite da elementi diversi dalla rappresentazione stringa di un valore di tipo intero o float possono produrre risultati imprevisti. tutti i valori interi sono limitati a 2147483647; i valori maggiori vengono troncati a 2147483647.

Formato

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

Tipi di dati

Argomento	Tipo	Descrizione
inum	variabile numerica (OUTPUT)	La variabile numerica in cui viene memorizzato il numero (ivar o fvar).
string	stringa (INPUT)	La rappresentazione stringa di un numero, ad esempio: “306”.

Ad esempio:

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

STRIP o STRIP-ASCII-RANGE


Il comando STRIP rimuove tutte le occorrenze della stringa o dell'intervallo ASCII da rimuovere dalla svar. Il comando STRIP esegue sempre operazioni di eliminazione multipasso finché la stringa o l'intervallo ASCII non si riduce a una lunghezza pari a quella della variabile stringa di destinazione.

Quando si utilizza questo comando, specificare la variabile stringa da cui i caratteri verranno rimossi. I parametri rimanenti possono essere valori di inizio e fine di una stringa o di un intervallo numerico.

NOTA: Nell'editor visivo di Generatore servizi di raccolta, STRIP e STRIP-ASCII-RANGE vengono elencati come comandi separati. Corrispondono allo stesso comando. Vengono forniti come descrizioni delle diverse variazioni dello stesso comando. Se si è tentato di utilizzare STRIP-ASCII-RANGE nell'editor di testo, occorre immettere STRIP.

Formato

```
STRIP(dest, strip)
STRIP(dest, start ASCII range, stop ASCII range)
```

Tipi di dati

Argomento	Tipo	Descrizione
dest	svar (INPUT/ OUTPUT)	La variabile stringa contenente i dati da cui rimuovere i byte in base al secondo argomento.
strip or start ASCII range	stringa o numerico (INPUT)	La stringa o il valore ASCII di inizio per la rimozione dalla stringa di destinazione.
stop ASCII range	di tipo numerico (INPUT [facoltativo])	Valore ASCII di interruzione **NOTA**: Se l'intervallo ASCII iniziale è specificato, questo parametro è obbligatorio.

Di seguito sono disponibili alcuni esempi di operazioni STRIP multipasso.

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

Dopo il comando STRIP(), la variabile test ha il valore di THE.

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

Dopo il comando STRIP(), la variabile test2 ha il valore di ABCEFGHTH.

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

Dopo il comando STRIP(), la variabile test3 ha il valore di ABCFGH.

TBOSSETCOMMAND

Il comando TBOSSETCOMMAND genera un pacchetto di comando TBOS a 3 byte che può essere trasmesso a un dispositivo tramite il protocollo TBOS.

Il numero visualizzato di TBOS, il numero del comando e il tipo vengono utilizzati per inserire il pacchetto di comando TBOS corretto (3 byte) nella variabile stringa di output. Il formato del pacchetto TBOS creato mediante questo comando di analisi sintattica viene descritto nelle tabelle relative alle richieste di comando remoto seguenti.

Carattere 1		
Numeri di bit	**Valore**	**Significato**
8 7	0 1	Codice dell'operazione: 01 = richiesta di comando remoto (carattere 1)
6 5 4	MSB LSB	Numero visualizzato: 000 = N. 1 001 = N. 2 ... 111 = N. 7
3	0	Nessun significato
2 1	MSB LSB	Tipo: 00 = momentary 01 = latch 10 = unlatch

Carattere 2		
Numeri di bit	**Valore**	**Significato**
8 7	1 0	Codice dell'operazione: 10 = richiesta di comando remoto (carattere 2)
6 5 4 3 2 1	MSB LSB	Numero di comando remoto: 000000 = No. 1 000001 = No. 2 ... 111111 = N. 63

Carattere 3		
Numeri di bit	**Valore**	**Significato**
8 7 6 5 4 3 2 1	1 1 0 0 1 1 0 0	Echo di carattere: La risposta del comando remoto corrisponde all'echo del byte restituito alla porta.

Formato

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

Tipi di dati

Argomento	Tipo	Descrizione
cmd_bytes	svar (OUTPUT)	I byte di dati esadecimali (3 byte totali) che verranno inseriti nella variabile stringa e che potrebbero essere utilizzati per trasmettere a un dispositivo TBOS nella postazione di trasmissione dello stato successiva.
idisp_num	di tipo numerico (INPUT)	Numero TBOS (o indirizzo) del dispositivo (1 - 8). **NOTA:** I valori validi per idisp_num sono compresi tra 1 e 8; se si utilizza qualsiasi altro valore, l'output (cmd_bytes) viene impostato su tutti zeri, “\00 00 00\”.
i_cmd_num	di tipo numerico (INPUT)	Il numero di comando TBOS (1 - 64). **NOTA:** I valori validi i_cmd_num sono compresi tra 1 e 64; se si utilizza qualsiasi altro valore, l'output (cmd_bytes) viene impostato su tutti zeri, “\00 00 00\”.

Argomento	Tipo	Descrizione
type	di tipo numerico (INPUT) Oppure stringa (INPUT)	Il tipo di comando TBOS (0 - 2). 0 = momentary 1 = latch 2 = unlatch **NOTA:** I valori validi per type sono solo compresi tra 0 e 2; se si utilizza qualsiasi altro valore, type verrà impostato su 0 = temporaneo per default. Il tipo di comando TBOS in formato stringa. “momentary” o “m” = momentary “latch” o “l” = latch “unlatch” o “u” = unlatch Per questa stringa non viene fatta distinzione tra maiuscole e minuscole.

Ad esempio:

```
TBOSSETCOMMAND(string_cmd_bytes, 1, 1, 0)
TBOSSETCOMMAND(s_bytes, 1, 1, "latch")
TBOSSETCOMMAND(s_bytes, i_display, i_cmd_num, "U")
TBOSSETCOMMAND(s_bytes, i_display, i_cmd_num, 2)
TBOSSETCOMMAND(s_bytes, 1, 1, "momentary")
TBOSSETCOMMAND(s_bytes, 1, 1, "latch")
```

Ricordare di verificare che il valore cmd_bytes di output sia impostato su "\00 00 00\" per poter controllare eventuali errori negli input esterni all'intervallo. Ad esempio:

```
TBOSSETCOMMAND(cmd_bytes, i_display, i_cmd_num, "M")
IF(cmd_bytes = "\00 00 00\") /* INPUTS OUT OF RANGE */
...
ENDIF()
```

L'esempio seguente genera un comando TBOS per il numero visualizzato 5, il numero di comando 33 e il tipo unlatched.

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

Contenuto delle variabili di output correnti:

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

TBOSSETREQUEST

Il comando TBOSSETREQUEST genera una richiesta TBOS a 1 byte che può essere trasmessa a un dispositivo tramite il protocollo TBOS. Il numero visualizzato e il numero di richiesta TBOS vengono utilizzati per inserire il byte di richiesta di scansione TBOS nella variabile string di output. Il formato del pacchetto TBOS creato mediante questo comando di analisi sintattica viene descritto nelle tabelle relative alle richieste e alle risposte di scansione carattere seguenti.

Carattere 1 – Richiesta di scansione caratteri		
Numeri di bit	**Valore**	**Significato**
8 7	0 0	Codice dell'operazione: 00 = richiesta di scansione caratteri
6 5 4	MSB LSB	Numero visualizzato: 000 = N. 1 001 = N. 2 ... 111 = N. 3
3 2 1	MSB LSB	Tipo: 000 = N. 1 001 = N. 2 ... 111 = N. 8

Carattere 1 – Risposta di scansione caratteri		
Numeri di bit	**Valore**	**Significato**
8 7 6 5 4 3 2 1	MSB LSB	Ogni bit nel byte di risposta ha un significato speciale in base al numero di caratteri inviato (1-8) e al protocollo del dispositivo del numero visualizzato inviato (1-8).

Formato

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

Tipi di dati

Argomento	**Tipo**	**Descrizione**
cmd_bytes	svar (OUTPUT)	Il byte di dati esadecimale viene inserito nella variabile stringa e può essere utilizzato per trasmettere a un dispositivo TBOS nella postazione di trasmissione dello stato successiva.

Argomento	Tipo	Descrizione
idisp_num	di tipo numerico (INPUT)	Numero TBOS (o indirizzo) del dispositivo (1 - 8). **NOTA:** I valori validi per idisp_num sono compresi tra 1 e 8; se si utilizza qualsiasi altro valore, l'output (cmd_bytes) viene impostato su tutti zeri, "\00\".
irequest_num	di tipo numerico (INPUT)	Il numero di caratteri di scansione TBOS (1 - 8). **NOTA:** I valori validi per irequest_num sono compresi tra 1 e 8; se si utilizza qualsiasi altro valore, l'output (cmd_bytes) viene impostato su tutti zeri, "\00\".

Ad esempio:

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

L'esempio seguente genera un carattere di richiesta di scansione TBOS per il numero visualizzato 2 e il numero di richiesta 1.

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

Contenuto delle variabili di output correnti:

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

TIME

Il comando TIME copia l'ora corrente nel formato HH-MM-SS in una variabile stringa, ivar.

Formato

```
TIME(dest)
```

Tipi di dati

Argomento	Tipo	Descrizione
dest	svar (OUTPUT) variabile numerica (OUTPUT)	La rappresentazione stringa dell'ora viene inserita in questa variabile (ad esempio “23-11-55”). Il numero di secondi da 00:00:00 UTC, 1 gennaio 1970, viene inserito in questa variabile numerica (può essere fvar).

Ad esempio:

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

NOTA: Se si utilizza fvar, l'ora restituita risulterà precisa al microsecondo.

TOKENIZE

Il comando TOKENIZE copia ogni componente di una stringa tra i delimitatori in una matrice di tipo stringa. Ciò può risultare utile se si leggono dati delimitati in un file e dati di passaggio a uno script per l'esecuzione su richiesta.

Ogni carattere nella stringa viene considerato come un potenziale separatore token. Ad esempio, se si utilizza il separatore token "THE END", non si utilizza a tale scopo l'intera stringa. Verranno invece utilizzati singoli caratteri utilizzati come separatori potenziali:

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

Formato

```
TOKENIZE(data, delimiter, tokens[], itokens)
```

Tipi di dati

Argomento	Tipo	Descrizione
data	svar (INPUT)	I dati da sottoporre al comando TOKENIZED (ad esempio: “xterm|subres|33|50”).
delimiter	stringa (INPUT)	I delimitatori per separare i token.
token	matrice (OUTPUT)	La matrice di token trovata nei dati di input della stringa delimitata.
itokens	variabile numerica (OUTPUT)	Il numero di token inseriti nella matrice stringa di token.

Ad esempio:

```
COPY(data:"This|Data|Is|Tokenized")
TOKENIZE(data, "|",tokens[], inumtokens)
```

Contenuto delle variabili di output correnti:

```
inumtokens = 4
tokens[0]= "This"
tokens[1]= "Data"
tokens[2]= "Is"
tokens[3]= "Tokenized"
```

Nell'esempio seguente, i dati passati allo script sono:

```
"There#are|several*fields|in*this#string".
```

Sono presenti tra diversi separatori di token da utilizzare: #, | e *.

Contenuto delle variabili di output correnti:

```
i_tokens = 7
messages[0] = "There"
messages[1] = "are"
messages[2] = "several"
messages[3] = "fields"
messages[4] = "in"
messages[5] = "this"
messages[6] = "string"
```

Nell'esempio seguente, i dati nel buffer di ricezione sono:

```
"Firewall Alarm - Major;Denial of Service Alarm - Major;"
COPY(rxbuff:)
TOKENIZE(rxbuff,";",msgs[],i_msgs)
```

Contenuto delle variabili di output correnti:

```
i_msgs = 2
msgs[0] = "Firewall Alarm - Major"
msgs[1] = "Denial of Service Alarm - Major"
```

TOLOWER

Il comando TOLOWER converte i contenuti di una variabile stringa in caratteri minuscoli. I contenuti della variabile stringa passata tramite il comando vengono convertiti in lettere minuscole.

Formato

```
TOLOWER(stringvar)
```

Tipi di dati

Argomento	Tipo	Descrizione
stringvar	stringa (INPUT/ OUTPUT)	La variabile stringa contenente la stringa da convertire in caratteri minuscoli.

Ad esempio:

```
s_var = "This Is Lower Case"
TOLOWER(s_var)
```

Risultato:

```
s_var = "this is lower case"
```

TOUPPER

Il comando TOUPPER converte i contenuti di una variabile stringa in caratteri maiuscoli. I contenuti della variabile stringa passata tramite il comando vengono convertiti in lettere maiuscole.

Formato

```
TOUPPER(stringvar)
```

Tipi di dati

Argomento	Tipo	Descrizione
stringvar	stringa (INPUT/ OUTPUT)	La variabile stringa contenente la stringa da convertire in caratteri maiuscoli.

Ad esempio:

```
s_var = "This Is Upper Case"
toupper(s_var)
```

Risultato:

```
s_var = "THIS IS UPPER CASE"
```

TRANSLATE

Il comando TRANSLATE carica un file di valori separati da virgola (csv) in memoria consentendo di verificare rapidamente tramite una ricerca se la voce chiave vi è contenuta e di recuperare altri dati associati alla chiave.

Gli elementi seguenti sono correlati al comando TRANSLATE.

- Valori separati da virgola (CSV)
- Ricerche di chiavi senza distinzione tra maiuscole e minuscole
- Stato Trovato
- Variabili dati

File di valori separati da virgola (CSV)

Il file con estensione csv è relativo rispetto al percorso di una directory di script del servizio di raccolta. Generatore servizi di raccolta non supporta la modifica di tali file, pertanto è consigliabile generarli tramite Microsoft Excel. Il nome file può essere una stringa o una variabile.

Il formato di file csv è illustrato nell'esempio seguente relativo a un file denominato friends.csv utilizzato nell'esempio seguente:

```
key1,data1,data2,data3
Bob,blue,25,210
```

```
Alice,green,19,110
Pat,purple,36,145
```

Per trovare una determinata voce nel file, è possibile utilizzare il comando TRANSLATE nel modo seguente:

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

Oppure

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

Ricerche di chiavi senza distinzione tra maiuscole e minuscole

Il parametro chiave può essere una stringa o una variabile stringa. Inoltre, sono supportati un numero intero o una variabile. Poiché il file csv viene caricato in memoria, la chiave di ogni voce viene convertita in lettere minuscole. La chiave nel comando TRANSLATE viene inoltre impostata internamento in caratteri minuscoli per consentire la ricerca senza distinzione tra caratteri maiuscoli e minuscoli.

Nell'ambito dell'esempio di file csv precedente:

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

In questo modo sarà possibile trovare nel file csv anche Bob.

Stato Trovato

Lo stato trovato viene impostato su 1 se la chiave si trova nel file csv e su zero in caso contrario. È possibile utilizzare il comando TRANSLATE con un file csv contenente solo voci di chiave per determinare se la chiave si trova nel file. Per motivi di sicurezza, un file csv può contenere un elenco di indirizzi IP ostili noti oppure nomi utente valido con altre informazioni sulle norme, ad esempio autorizzazioni e tempi di accesso consentiti.

NOTA: Le chiavi che esprimono intervalli non sono supportate: indirizzi IP e intervalli numerici.

Variabili dati

Oltre a determinare l'eventuale presenta di una voce di chiave nel file csv, è possibile recuperare dati ad essa associati. È possibile utilizzare un numero variabile di variabili di script per indicare le variabili per la memorizzazione dei dati. Sono supportate variabili di tipo stringa, intero e float. Tutte le voci di dati vengono memorizzate come stringhe e convertite nel tipo di variabile specificata nel comando TRANSLATE.

Nell'ambito dell'esempio relativo al file friends.csv:

```
Bob,blue,25,210
Alice,green,19,110
Pat,purple,36,145
```

Si otterranno i dati associati a tali voci:

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

Dove:

- Se s_friend contiene Alice, allora i_found è uguale a 1, s_color a green, i_age a 19 e i_weight a 110.
- se la voce di chiave non viene trovata, allora le variabili non vengono modificate (s_color, i_age, i_weight).
- Se la voce per Alice è:
  `Alice,green,19,`

  Utilizzando lo stesso comando TRANSLATE, la variabile i_weight verrebbe eliminata (0 per interi, 0.0 per float e "" per le stringhe), s_color corrisponderebbe a green e i_age will a 19.
- Se la voce per Alice è:
  `Alice,green,,thin,Ford`

  Utilizzando lo stesso comando TRANSLATE, la variabile i_age verrebbe eliminata e thin verrebbe convertito in un intero (0) e inserito in i_weight, mentre s_color corrisponderebbe a green e Ford verrebbe ignorato.
- Se la voce per Alice è:
  `Alice,25,19,110`

  Utilizzando lo stesso comando TRANSLATE, la variabile s_color conterrebbe 25. i_age corrisponderebbe a 19 e i_weight a 110.

Formato

```
TRANSLATE(<key>, <csv_file>, <found_status>
   [, <variable>, ...])
```

Tipi di dati

Argomento	Tipo	Descrizione
key		Chiave da cercare nel file csv.
csv_file		Nome del file csv.
found_status		la variabile numero intero imposta su 1 se la chiave è nel file csv oppure su zero in caso non sia presente.
variable		elenco delle variabili in cui inserire i dati associati alla chiave.

TRIM

Rimuove tutti gli spazi vuoti alle estremità di una stringa e sostituisce più spazi contenuti in una stringa con spazi singoli. Gli spazi considerati vuoti includono i caratteri seguenti:

- <tab>
- <ritorno a capo>
- <nuova riga>
- <tabulazione verticale>
- <salto pagina>

- <spazio>

Formato

```
TRIM(svar)
```

Tipi di dati

Argomento	Tipo	Descrizione
stringa	svar (INPUT)	Stringa da cui rimuovere gli spazi. La stringa risultante viene memorizzata nella variabile di input.

Ad esempio:

```
COPY(s_var:" Hello    World  "
TRIM(s_var)
```

Contenuto delle variabili di output correnti:

```
s_var = " Hello World "
```

WHILE

Il comando WHILE offre funzionalità di ciclo del flusso di controllo.

Il funzionamento del comando WHILE è il seguente:

- Se il risultato dell'istruzione WHILE() è true, i comandi di analisi sintattica che lo seguono fino al successivo ENDWHILE() vengono eseguiti.
- Se il risultato di WHILE() è false, no vengono eseguiti i comandi di analisi sintattica compresi tra WHILE() e ENDWHILE().

Sebbene siano consentiti tutti i tipi di dati a entrambi i lati dell'operatore dell'istruzione WHILE(), è possibile confrontare solo valori dello stesso tipo, ovvero numeri con numeri e stringhe con stringhe.

L'operatore per WHILE() può essere <, =, >, <=, >=, <>, &, +, oppure ^.

ATTENZIONE: Non utilizzare l'operatore logico NOT (^) insieme a una variabile di tipo stringa. In caso contrario, verrà generato un errore di sintassi.

Non è possibile eseguire un confronto diretto con un numero negativo. Utilizzare uno dei metodi seguenti:

- Utilizzare la funzione di analisi sintattica COMPARE
- Eseguire un confronto indiretto come segue:

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

Formato

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

Dove:

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

Dove <expr> deve restituire un valore intero o float.

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

Dove entrambi i valori di <espr> devono restituire lo stesso tipo di dati.

Tipi di dati

Argomento	Tipo	Descrizione
data1	tutti (INPUT)	I dati da confrontare con data2. Se data2 non viene utilizzato, diventa un'espressione logica (0 = false, altri valori = true).
operatore logico	< = > <= >= <> & + ^	Minore di Uguale a Maggiore di Minore o uguale a Maggiore o uguale a Diverso da AND logico OR logico NOT logico
data2	tutti (INPUT) [FACOLTATIVO]	I dati da confrontare con dati1. Deve trattarsi dello stesso tipo di dati di data1.
…	come sopra	Utilizzare fino a 200 parametri singoli per creare espressioni logiche complesse.

Ad esempio:

```
WHILE(i<3)
SET(i=i+1)
ALERT("Still in loop")
ENDWHILE()
ALERT("Exited loop")
```

4 Funzioni dell'amministratore di Wizard

NOTA: Il termine agente è equivalente a servizio di raccolta. Si farà in seguito riferimento agli agenti come servizi di raccolta.

Questo capitolo è rivolto all'amministratore del sistema Wizard. Sono descritte diverse funzioni di amministrazione eseguite dall'amministratore di sistema e sono riportate informazioni relative ai processi in background di Wizard.

NOTA: Quando si esegue Generatore servizi di raccolta di Wizard per la prima volta, può essere visualizzato un messaggio indicante che la directory 'Collectors' non esiste e che verrà creata automaticamente. In questo caso è possibile che si verifichino perdite informazioni. Scegliere OK. La directory verrà creata e Generatore servizi di raccolta di Wizard verrà avviato. Se questo messaggio viene visualizzato anche successivamente alla prima volta in cui viene eseguito Generatore servizi di raccolta di Wizard, è possibile che la directory Collector sia stata eliminata inavvertitamente e sarà necessario verificare l'eventuale perdita di informazioni.

Utility e applicazioni di Wizard

In Wizard sono comprese un'interfaccia utente (Generatore servizi di raccolta) e diverse altre utility che funzionano con il Generatore di servizi di raccolta per eseguire il monitoraggio della rete.

Generatore servizi di raccolta

L'interfaccia utente di Wizard è Generatore servizi di raccolta, che consente di configurare i servizi di raccolta in rete oltre alle porte e agli script utilizzati per comunicare con gli host. Generatore servizi di raccolta viene eseguito solo in Windows.

NOTA: se si verificano problemi in relazione alla modalità di visualizzazione della finestra di Wizard dopo il trascinamento della finestra in un'altra posizione, verificare le impostazioni in Schermo nel Pannello di controllo di Microsoft Windows. Nella scheda Effetti, deselezionare Mostra contenuto della finestra durante l'operazione di trascinamento.

Porta

In Wizard, le porte consentono al Servizio di raccolta di individuare i dati degli eventi di sicurezza nella rete fornendo l’indirizzo IP e altre informazioni sull’origine (dispositivo di sicurezza [router, IDS, switch, e altri dati]). Ogni riga della tabella Configurazione porta esegue uno script del servizio di raccolta per un'origine eventi.

Gestione servizi di raccolta

Gestione servizi di raccolta consente di avviare e arrestare l'elaborazione delle porte.

Motore del servizio di correlazione

Motore servizi di raccolta elabora la logica dei modelli per ogni porta. Per ogni porta attiva viene eseguito un Motore servizi di raccolta.

popup.exe

L'utility popup.exe viene eseguita dal Motore servizi di raccolta per l'elaborazione comandi di analisi di popup o di visualizzazione.

popup.cfg

Il file popup.cfg è un file opzionale utilizzato per il controllo dei timeout dei comandi di analisi dei popup e della visualizzazione. Se non si dispone di un file popup.cfg non verrà eseguito il timeout dei comandi di analisi della visualizzazione e dei popup.

Per impostare un timeout per il comando di visualizzazione, immettere l'istruzione:

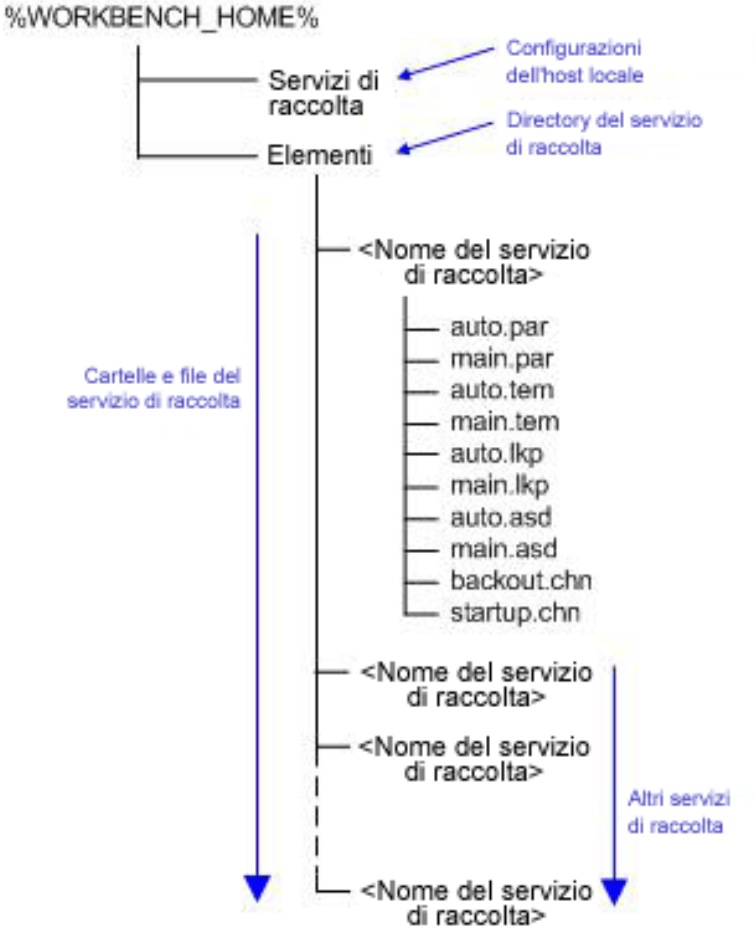
```
displaytimeout <true/false>.
```

Il timeout della visualizzazione è impostato su 20 secondi.

Per impostare un timeout per il comando di popup, immettere l'istruzione:

```
timeout <timeout in secondi>.
```

Struttura di directory di Wizard



Chiave

Servizi di raccolta	File di configurazione porte (host Wizard)
Elements	File del servizio di raccolta
.par	File dei parametri
.tem	File dei modelli
.lkp	File di ricerca
.asd	File di descrizione dello stato attivo
backout.chn	File di script di backout
startup.chn	File di script di avvio

5 Tag META di Wizard e Sentinel

NOTA: Il termine agente è equivalente a servizio di raccolta. Si farà in seguito riferimento agli agenti come servizi di raccolta.

NOTA: Per gli utenti di MS SQL 2000, la dimensione degli eventi non può superare gli 8 KB.

I tag META memorizzano metadati. I metadati sono informazioni sui dati, nomi variabili predefiniti per metadati. L'indirizzo IP di origine di un attacco viene memorizzato, ad esempio, nel tag META SourceIP. I nomi di prodotto vengono memorizzati nel tag META ProductName. I dati utilizzati per compilare i tag META vengono estratti dai dati di log dei dispositivi o impostati come parte dell'elaborazione del servizio di raccolta.

Per accedere alla configurazione degli eventi e alla funzione di mappatura in Gestione dati Sentinel, fare clic sulla scheda Eventi.

NOTA: Nel linguaggio delle regole di correlazione RuleLg in formato libero, quando un'etichetta è preceduta da una ‘e. ’, come e.crt, fa riferimento a eventi correnti. Se un'etichetta è preceduta da ‘w.’, ad esempio w.crt, fa riferimento a eventi cronologici.

Il valore della colonna Variabile servizio di raccolta corrisponde al nome della variabile del servizio di raccolta da impostare per compilare il tag META corrispondente. Per ulteriori informazioni sui comandi di analisi sintattica, vedere il capitolo 3 e la documentazione relativa a specifici servizi di raccolta disponibile in

```
%ESEC_HOME%\wizard\elements\<nome servizio di
   raccolta>\docs.
```

NOTA: nella tabella seguente, etichette e tag META vengono utilizzati in Sentinel Control Center. Le variabili servizio di raccolta vengono utilizzate nell'analisi sintattica del servizio di raccolta. Non a tutti i tag META è associata una variabile servizio di raccolta.

I tipi specificati nella colonna Tipo hanno le proprietà seguenti:

- stringa – massimo 255 caratteri (a meno che non sia diversamente specificato)
- intero – numero intero con segno a 32 bit
- UUID – stringa esadecimale di 36 caratteri (con trattini) o 32 caratteri (senza trattini) nel formato XXXXXXXX-XXXX-XXXX-XXXX-XXXXXXXXXXXX (ad esempio, 6A5349DA-7CBF-1028-9795-000BCDFFF482)
- data – la variabile servizio di raccolta deve essere impostata con la data espressa in millisecondi a partire dal primo gennaio 1970 00:00:00 GMT. Quando vengono visualizzati in Sentinel Control Center, i tag META di tipo data prevedono un formato data regolare.
- IPv4 – indirizzo IP in notazione decimale con punti (ad esempio, xxx.xxx.xxx.xxx)

Etichetta	Tag META	Tipo	Descrizione	Variabile servizio di raccolta
CorrelatedEventUuids	ceu	stringa	Elenco di UUID di evento associati all'evento correlato. Rilevante solo per gli eventi correlati.	
Criticality	crt	intero	Criticità della risorsa identificata nell'evento.	s_CRIT
Ct1 a Ct2 (Cliente riservato)	ct1 a ct2	stringa	Riservato all'uso da parte dei clienti per dati specifici del cliente (stringa).	s_CT1 e s_CT2
Ct3 (Cliente riservato)	ct3	intero	Riservato all'uso da parte dei clienti per dati specifici del cliente (di tipo numerico).	s_CT3
CustomerVar1 a CustomerVar10	cv1 a cv10	intero	Riservato all'uso da parte dei clienti per dati specifici del cliente (di tipo numerico).	s_CV1 a s_CV10
CustomerVar11 a CustomerVar20	cv11 a cv20	data	Riservato all'uso da parte dei clienti per dati specifici del cliente (data).	s_CV11 a s_CV20
CustomerVar21 a CustomerVar29	cv21 a cv29	stringa	Riservato all'uso da parte dei clienti per dati specifici del cliente (stringa).	s_CV21 a s_CV29
CustomerVar30 a CustomerVar34	cv30 a cv34	stringa	Riservato all'uso da parte dei clienti per dati specifici del cliente (stringa). Può gestire stringhe di lunghezza fino a 4000 caratteri.	s_CV30 a s_CV34
CustomerVar35 a CustomerVar89	cv35 a cv89	stringa	Riservato all'uso da parte dei clienti per dati specifici del cliente (stringa).	s_CV35 a s_CV89
SARBOX	cv90	stringa	Dati specifici Sarbanes Oxley.	s_CV90
HIPAA	cv91	stringa	Dati specifici HIPAA (Health Insurance Portability and Accountability Act).	s_CV91
GLBA	cv92	stringa	Dati specifici GLBA (Gramm-Leach-Bliley Act).	s_CV92
FISMA	cv93	stringa	Dati specifici FISMA (Federal Information Security Management Act).	s_CV93
NISPOM	cv94	stringa	Dati specifici NISPOM (National Industrial Security Program Operating Manual).	s_CV94
SIPCountry	cv95	stringa	Paese dell'IP di origine.	s_CV95
DIPCountry	cv96	stringa	Paese dell'IP di destinazione.	s_CV96

Etichetta	Tag META	Tipo	Descrizione	Variabile servizio di raccolta
CustomerVar97 a CustomerVar100	cv97 a cv100	stringa	Riservato all'uso da parte dei clienti per dati specifici del cliente (stringa).	s_CV97 a s_CV100
DateTime	dt	data	Data e ora normalizzate dell'evento, come indicate dal servizio di raccolta.	
DestinationHostName	dhn	stringa	Nome dell'host di destinazione a cui è destinato l'evento.	s_DHN
DestinationIP	dip	IPv4	Indirizzo IP di destinazione a cui è destinato l'evento.	s_DIP
DestinationPort	dp	stringa (32)	Porta di destinazione a cui è destinato l'evento.	s_DP
DestinationUserName	dun	stringa	Nome dell'utente di destinazione su cui è stata tentata l'azione. Esempio: tentativi eseguiti per reimpostare la password della radice.	s_DUN
EventID	id	UUID	Identificatore univoco dell'evento.	
EventTime	et	stringa	Ora normalizzata dell'evento, come indicato dal sensore; analizzata sintatticamente nel formato: A-M-G-H:M:S~AMPM24~TZ.	s_ET
EventName	evt	stringa	Nome descrittivo dell'evento, come riportato (o indicato) dal sensore. Esempio "Scansione porte".	s_EVT
ExtendedInformation	ei	stringa (1000)	Memorizza ulteriori informazioni raccolte dal servizio di raccolta. I valori all'interno di questa variabile sono separati da punti e virgola (;). Esempio: un dominio per ID o nomi file.	s_EI
FileName	fn	stringa (1000)	Nome del programma eseguito o del file aperto, modificato o interessato. Esempio: il nome di un file infetto da virus o un programma rilevato da un IDS.	s_FN

Etichetta	Tag META	Tipo	Descrizione	Variabile servizio di raccolta
Message	msg	stringa (4000)	Messaggio in formato libero per l'evento.	s_BM
Protocol	prot	stringa	Protocollo di rete dell'evento.	s_P
ProductName	pn	stringa	Indica tipo, fornitore e nome di prodotto in codice del sensore da cui è stato generato l'evento. Esempio: Check Point FireWall=CPFW.	s_PN
ReporterName	rn	stringa	Nome host o indirizzo IP del dispositivo in cui viene registrato un evento o da cui viene inviata una notifica dell'evento.	s_RN
ReservedVar1 a ReservedVar10	rv1 a rv10	intero	Riservato da Novell per l'espansione (di tipo numerico).	s_RV1 a s_RV10
ReservedVar11 a ReservedVar20	rv11 a rv20	data	Riservato da Novell all'espansione (data).	s_RV11 a s_RV20
ReservedVar21 a ReservedVar25	rv21 a rv25	UUID	Riservato da Novell all'espansione (UUID).	s_RV21 a s_RV25
ControlPack	rv26	stringa	Livello di classificazione dei controlli Sentinel 1	s_RV26
ControlMonitor	rv27	stringa	Livello di classificazione dei controlli Sentinel 2	s_RV27
ReservedVar28	rv28	stringa	Riservato da Novell per l'espansione (stringa).	s_RV28
SourceIPCountry	rv29	stringa	Paese dell'indirizzo IP di origine.	s_RV29
AttackID	rv30	stringa	ID dell'attacco normalizzato (ID attacco Advisor)	s_RV30
DeviceName	rv31	stringa	Nome del dispositivo di sicurezza	s_RV31
DeviceCategory	rv32	stringa	Categoria del dispositivo (AV, DB, ESEC, FW, IDS, OS). AV: Antivirus DB: Database ESEC: Evento di sistema FW: Firewall IDS: Rilevamento delle intrusioni OS: Sistema operativo	s_RV32

Etichetta	Tag META	Tipo	Descrizione	Variabile servizio di raccolta
EventContext	rv33	stringa	Contesto dell'evento (livello di minaccia).	s_RV33
SourceThreatLevel	rv34	stringa	Livello di minaccia di origine.	s_RV34
SourceUserContext	rv35	stringa	Contesto dell'utente di origine.	s_RV35
DataContext	rv36	stringa	Contesto dati.	s_RV36
SourceFunction	rv37	stringa	Funzione di origine.	s_RV37
SourceOperationalContext	rv38	stringa	Contesto operativo di origine.	s_RV38
MSSPCustomerName	rv39	stringa	Nome del cliente MSSP.	s_RV39
ReservedVar40 a ReservedVar43	rv40 a rv43	stringa	Riservato da Novell per l'espansione (stringa).	s_RV40 a s_RV43
DestinationThreatLevel	rv44	stringa	Livello di minaccia di destinazione.	s_RV44
DestinationUserContext	rv45	stringa	Contesto dell'utente di destinazione.	s_RV45
VirusStatus	rv46	stringa	Stato del virus.	s_RV46
DestinationFunction	rv47	stringa	Funzione di destinazione.	s_RV47
DestinationOperationalContext	rv48	stringa	Contesto operativo di destinazione.	s_RV48
ReservedVar49	rv49	stringa	Riservato da Novell per l'espansione (stringa).	s_RV49
eSecTaxonomyLevel1	rv50	stringa	Classificazione codici di evento Sentinel – livello 1	s_RV50
eSecTaxonomyLevel2	rv51	stringa	Classificazione codici di evento Sentinel – livello 2	s_RV51
eSecTaxonomyLevel3	rv52	stringa	Classificazione codici di evento Sentinel – livello 3	s_RV36
eSecTaxonomyLevel4	rv53	stringa	Classificazione codici di evento Sentinel – livello 4	s_RV53
ReservedVar54 a ReservedVar55	rv54 a rv55	stringa	Riservato da Novell per l'espansione (stringa).	s_RV54 a s_RV55
SourceAssetName	rv56	stringa	Nome della risorsa di origine (Gestione risorse)	s_RV56
SourceMacAddress	rv57	stringa	Indirizzo MAC di origine (Gestione risorse)	s_RV57
SourceNetworkIdentity	rv58	stringa	Identità di rete di origine (Gestione risorse)	s_RV58
SourceAssetCategory	rv59	stringa	Categoria della risorsa di origine (Gestione risorse)	s_RV59
SourceEnvironmentIdentity	rv60	stringa	Identità dell'ambiente di origine (Gestione risorse)	s_RV60

Etichetta	Tag META	Tipo	Descrizione	Variabile servizio di raccolta
SourceAssetValue	rv61	stringa	Valore della risorsa di origine (Gestione risorse)	s_RV61
SourceCriticality	rv62	stringa	Criticità di origine (Gestione risorse)	s_RV62
SourceSensitivity	rv63	stringa	Riservatezza di origine (Gestione risorse)	s_RV63
SourceBuilding	rv64	stringa	Edificio di origine (Gestione risorse)	s_RV64
SourceRoom	rv65	stringa	Stanza di origine (Gestione risorse)	s_RV65
SourceRackNumber	rv66	stringa	Numero del rack di origine (Gestione risorse)	s_RV66
SourceCity	rv67	stringa	Città di origine (Gestione risorse)	s_RV67
SourceState	rv68	stringa	Stato di origine (Gestione risorse)	s_RV68
SourceCountry	rv69	stringa	Paese di origine (Gestione risorse)	s_RV69
SourceZipCode	rv70	stringa	CAP di origine (Gestione risorse)	s_RV70
SourceAssetOwner	rv71	stringa	Proprietario della risorsa di origine (Gestione risorse)	s_RV71
SourceAssetMaintainer	rv72	stringa	Gestore della risorsa di origine (Gestione risorse)	s_RV72
SourceBusinessUnit	rv73	stringa	Unità aziendale di origine (Gestione risorse)	s_RV73
SourceLineOfBusiness	rv74	stringa	Settore d'attività di origine (Gestione risorse)	s_RV74
SourceDivision	rv75	stringa	Divisione di origine (Gestione risorse)	s_RV75
SourceDepartment	rv76	stringa	Reparto di origine (Gestione risorse)	s_RV76
SourceAssetId	rv77	stringa	ID risorsa di origine (Gestione risorse)	s_RV77
DestinationAssetName	rv78	stringa	Nome della risorsa di destinazione (Gestione risorse)	s_RV78
DestinationMacAddress	rv79	stringa	Indirizzo MAC di destinazione (Gestione risorse)	s_RV79
DestinationNetworkIdentity	rv80	stringa	Identità di rete di destinazione (Gestione risorse)	s_RV80
DestinationAssetCategory	rv81	stringa	Categoria della risorsa di destinazione (Gestione risorse)	s_RV81

Etichetta	Tag META	Tipo	Descrizione	Variabile servizio di raccolta
DestinationEnvironmentIdentity	rv82	stringa	Identità dell'ambiente di destinazione (Gestione risorse)	s_RV82
DestinationAssetValue	rv83	stringa	Valore della risorsa di destinazione (Gestione risorse)	s_RV83
DestinationCriticality	rv84	stringa	Criticità di destinazione (Gestione risorse)	s_RV84
DestinationSensitivity	rv85	stringa	Riservatezza di destinazione (Gestione risorse)	s_RV85
DestinationBuilding	rv86	stringa	Edificio di destinazione (Gestione risorse)	s_RV86
DestinationRoom	rv87	stringa	Stanza di destinazione (Gestione risorse)	s_RV87
DestinationRackNumber	rv88	stringa	Numero del rack di destinazione (Gestione risorse)	s_RV88
DestinationCity	rv89	stringa	Città di destinazione (Gestione risorse)	s_RV89
DestinationState	rv90	stringa	Stato di destinazione (Gestione risorse)	s_RV90
DestinationCountry	rv91	stringa	Paese di destinazione (Gestione risorse)	s_RV91
DestinationZipCode	rv92	stringa	CAP di destinazione (Gestione risorse)	s_RV92
DestinationAssetOwner	rv93	stringa	Proprietario della risorsa di destinazione (Gestione risorse)	s_RV93
DestinationAssetMaintainer	rv94	stringa	Gestore della risorsa di destinazione (Gestione risorse)	s_RV94
DestinationBusinessUnit	rv95	stringa	Unità aziendale di destinazione (Gestione risorse)	s_RV95
DestinationLineOfBusiness	rv96	stringa	Settore d'attività di destinazione (Gestione risorse)	s_RV96
DestinationDivision	rv97	stringa	Divisione di destinazione (Gestione risorse)	s_RV97
DestinationDepartment	rv98	stringa	Reparto di destinazione (Gestione risorse)	s_RV98
DestinationAssetId	rv99	stringa	ID della risorsa di destinazione (Gestione risorse)	s_RV99

Etichetta	Tag META	Tipo	Descrizione	Variabile servizio di raccolta
ReservedVar100	rv100	stringa	Riservato da Novell per l'espansione (stringa).	s_RV100
Resource	res	stringa	Nome della risorsa.	s_Res
DeviceAttackName	rt1	stringa	Per l'uso con Advisor. Nome dell'attacco indicato dal dispositivo di sicurezza.	s_RT1
Rt2	rt2	stringa	Compilato con il nome della regola di correlazione, quando viene generata una regola di correlazione da un evento.	s_RT2
Rt3	rt3	intero	Riservato da Novell per l'espansione (di tipo numerico).	s_RT3
SourceHostName	shn	stringa	Nome dell'host di origine da cui è originato l'evento.	s_SHN
SourceID	src	UUID	Identificatore univoco del processo di Sentinel che ha generato l'evento.	
SourceIP	sip	IPv4	Indirizzo IP di origine da cui è originato l'evento.	s_SIP
SensorName	sn	stringa	Nome del servizio di rilevamento definitivo dell'evento quando viene ricevuto in formato dati non elaborati. Esempio: "FW1" indica un firewall.	s_SN
Severity	sev	intero	Gravità normalizzata dell'evento (0-5).	i_Severity
SourcePort	sp	stringa (32)	Nome della porta di origine da cui è originato l'evento.	s_SP
SensorType	st	stringa (5)	Indicatore del tipo di sensore basato su un singolo carattere (N, H, I, O, P, V, C, W). C: Correlazione H: Basato sull'host I: Interno (evento di sistema) N: Basato sulla rete O: Altro P: Prestazioni (evento di sistema) V: Antivirus W: Watchlist	s_ST

Etichetta	Tag META	Tipo	Descrizione	Variabile servizio di raccolta
SourceUserName	sun	stringa	Nome dell'utente di origine utilizzato per avviare un evento. Esempio: "jdoe" durante un tentativo di "su".	s_SUN
SubResource	sres	stringa	Nome della sottorisorsa.	s_SubRes
Vulnerability	vul	intero	Vulnerabilità della risorsa identificata nell'evento.	s_VULN
WizardAgent	agent	stringa (64)	Servizio di raccolta Sentinel che ha generato l'evento. Per gli eventi di sistema, il servizio di raccolta sarà di tipo Prestazioni o Interno.	
WizardPort	port	stringa (64)	Descrizione della porta del servizio di raccolta Sentinel.	

6 Autorizzazioni utente di Sentinel Control Center

NOTA: Il termine agente è equivalente a servizio di raccolta. Si farà in seguito riferimento agli agenti come servizi di raccolta.

Le autorizzazioni utente sono suddivise come segue:

- Generale
  - Filtri pubblici
  - Filtri privati
  - Azioni di integrazione
- Active Views™
  - Voci di menu
  - Visualizzazioni di riepilogo
- iTRAC
  - Gestione dei modelli
  - Gestione dei processi
- Casi
- Gestione servizio di raccolta
- Analisi
- Advisor
- Amministrazione
  - Correlazione
  - Amministrazione - DAS
  - Informazioni su file di evento
  - Visualizzazioni server
  - Filtri globali
  - Gestione ruoli iTRAC
  - Configurazione menu
  - Gestione utenti
  - Gestione sessioni utente

Utenti di default

Il programma di installazione creerà gli utenti di default seguenti sul server Sentinel:

Autenticazione di Oracle e MS SQL :

- esecdba: proprietario dello schema (configurabile in fase di installazione).
- esecadm: utente amministratore di Sentinel (configurabile in fase di installazione).

NOTA: Per UNIX, il programma di installazione creerà anche l'utente del sistema operativo con gli stessi nome utente e password.

- esecrpt: utente autore rapporto, password dell'utente amministratore.
- ESEC_CORR: utenti del motore di correlazione, utilizzati per creare casi.
- esecapp: nome utente dell'applicazione Sentinel per la connessione al database.

Autenticazione di Windows:

- Amministratore DB Sentinel: proprietario dello schema (configurabile in fase di installazione).
- Amministratore Sentinel: utente amministratore di Sentinel (configurabile in fase di installazione).
- Utente rapporto Sentinel: utente autore rapporto, password dell'utente amministratore.
- Utente DB dell'applicazione Sentinel - nome utente dell'applicazione Sentinel per la connessione al database.

Generale

Autorizzazione	Descrizione
Salvataggio area di lavoro	Consente all'utente di salvare le preferenze. Se questa autorizzazione non è disponibile, all'utente non verrà mai richiesto di salvare le modifiche alle preferenze quando si disconnette o esce da Sentinel Control Center.
Gestione colonne	Consente all'utente di gestire le colonne nelle tabelle Active Views.
Istantanea	Consente all'utente di creare un'istantanea delle tabelle Active Views.

Generale – Filtri pubblici

Autorizzazione	Descrizione
Creazione filtri pubblici	Consente all'utente di creare un filtro con un ID proprietario PUBLIC. Se l'utente non dispone di questa autorizzazione, il valore PUBLIC non sarà elencato come uno degli ID proprietario per cui è possibile creare un filtro.
Modifica filtri pubblici	Consente all'utente di modificare un filtro pubblico.
Eliminazione filtri pubblici	Consente all'utente di eliminare un filtro pubblico.

Generale – Filtri privati

Autorizzazione	Descrizione
Creazione filtri privati	Consente all'utente di creare filtri privati per se stesso o per altri utenti.
Modifica filtri privati	Consente all'utente di modificare i propri filtri privati e quelli creati da altri utenti.
Eliminazione filtri privati	Consente all'utente di eliminare i propri filtri privati e quelli creati da altri utenti.
Visualizzazione/uso filtri privati	Consente all'utente di visualizzare i propri filtri privati e quelli creati da altri utenti.

Generale – Azioni di integrazione

Autorizzazione	Descrizione
Invio evento a HP Open View	Consente all'utente di inviare eventi, casi e oggetti associati a HP-OVO.
Invio evento a Service Desk	Consente all'utente di inviare eventi, casi e oggetti associati a HP Service Desk.
Invio a Remedy Help Desk	Consente all'utente di inviare eventi, casi e oggetti associati a Remedy.

Active Views

Autorizzazione	Descrizione
Visualizzazione scheda Active Views	Consente all'utente di visualizzare e utilizzare la scheda Active Views, il menu e altre funzioni correlate associate alla scheda Active Views.

Active Views – Voci di menu

Autorizzazione	Descrizione
Uso di voci di menu assegnate	Consente all'utente di utilizzare voci di menu assegnate nella tabella Eventi di Active Views (menu di scelta rapida).
Aggiunta di caso esistente	Consente all'utente di aggiungere eventi ai casi esistenti utilizzando la tabella Eventi di Active Views (menu di scelta rapida).
Rimozione da caso	Consente all'utente di rimuovere eventi da un caso esistente utilizzando la tabella Eventi di Active Views (menu di scelta rapida).
Invio eventi tramite e-mail	Consente all'utente di inviare eventi tramite e-mail utilizzando la tabella Eventi di Active Views (menu di scelta rapida).
Visualizzazione dati sugli attacchi di Advisor	Consente all'utente di visualizzare il flusso di dati sugli attacchi di Advisor.
Visualizzazione vulnerabilità	Consente all'utente di visualizzare l'output di una scansione Nessus.

Active Views – Visualizzazioni di riepilogo

Autorizzazione	Descrizione
Uso/visualizzazione riepiloghi	Consente all'utente di accedere ai grafici Active Views.

iTRAC

Autorizzazione	Descrizione
Visualizzazione scheda iTRAC	Consente all'utente di visualizzare e utilizzare la scheda iTRAC, il menu e altre funzioni correlate associate alla scheda iTRAC.
Gestione attività	Consente all'utente di accedere a Gestione attività.

Gestione modelli

Autorizzazione	Descrizione
Visualizzazione/uso di gestione modelli	Consente all'utente di accedere a Gestione modelli.
Creazione/modifica di modelli	Consente all'utente di creare e modificare modelli.

Gestione processi

Autorizzazione	Descrizione
Visualizzazione/uso di gestione processi	Consente all'utente di accedere a Gestione visualizzazione processi.
Controllo processi	Consente all'utente di utilizzare Gestione visualizzazione processi.

Casi

Autorizzazione	Descrizione
Visualizzazione scheda Casi	Consente all'utente di visualizzare e utilizzare la scheda Casi, il menu e altre funzioni correlate associate alla scheda Casi.
Amministrazione casi	Consente all'utente di modificare un caso.
Visualizzazione casi	Consente all'utente di visualizzare i dettagli di un caso. Se l'utente non dispone di questa autorizzazione, la finestra Dettagli caso non verrà visualizzata quando l'utente fa doppio clic su un caso nella finestra della barra di spostamento o nella relativa scheda Caso.
Creazione caso/i	Consente all'utente di creare casi nel menu Evento accessibile facendo clic con il pulsante destro del mouse su un evento.
Modifica caso/i	Consente all'utente di modificare un caso nella finestra Dettagli caso.
Eliminazione caso/i	Consente all'utente di eliminare casi.
Assegnazione caso/i	Consente all'utente di assegnare un caso nella finestra di modifica e creazione del caso.
Invio casi tramite e-mail	Consente all'utente di inviare casi di interesse tramite e-mail.
Azioni su casi	Consente all'utente di attivare/disattivare la configurazione/esecuzione di un'azione caso.

Gestione servizi di raccolta

Autorizzazione	Descrizione
Visualizzazione servizi di raccolta	▪ Consente di visualizzare la scheda "Servizi di raccolta" in Sentinel Control Center ▪ Consente di visualizzare la scheda "Host Wizard" in Generatore servizi di raccolta
Controllo servizi di raccolta	▪ Include tutte le funzionalità dell'autorizzazione di visualizzazione dei servizi di raccolta ▪ Consente il comando e il controllo dei servizi di raccolta da Sentinel Control Center ▪ Consente il comando e il controllo dei servizi di raccolta da Generatore servizi di raccolta di Wizard
Amministrazione servizi di raccolta	▪ Include tutte le funzionalità dell'autorizzazione di controllo dei servizi di raccolta ▪ In Generatore servizi di raccolta, modifica e distribuzione dei servizi di raccolta ▪ In Generatore servizi di raccolta, creazione, modifica, compilazione e debug dei servizi di raccolta ▪ In Generatore servizi di raccolta, caricamento e download dei servizi di raccolta ▪ In Generatore servizi di raccolta, esportazione di Host Wizard ▪ In Generatore servizi di raccolta, aggiunta, modifica ed eliminazione di porte ▪ In Generatore servizi di raccolta, impostazione delle opzioni Porta

Comando e controllo includono:

- avvio/interruzione di singole porte
- avvio/interruzione di tutte le porte
- riavvio di host
- ridenominazione di host

Analisi

Autorizzazione	Descrizione
Visualizzazione scheda Analisi	Consente all'utente di visualizzare e utilizzare la scheda Analisi, il menu e altre funzioni correlate associate alla scheda Panoramica di sistema.

Advisor

Autorizzazione	Descrizione
Visualizzazione scheda Advisor	Consente all'utente di visualizzare e utilizzare la scheda Advisor, il menu e altre funzioni correlate associate alla scheda Advisor.

Amministrazione

Autorizzazione	Descrizione
Visualizzazione scheda Amministrazione	Consente all'utente di visualizzare e utilizzare la scheda Amministrazione, il menu e altre funzioni correlate associate alla scheda Amministrazione.

Amministrazione - Correlazione

Autorizzazione	Descrizione
Uso/visualizzazione gestione motore di correlazione	Consente all'utente di visualizzare e utilizzare il motore di correlazione.
Uso/visualizzazione regole di correlazione	Consente all'utente di avviare o interrompere le regole di correlazione.

Amministrazione – Filtri globali

Autorizzazione	Descrizione
Visualizzazione/uso filtri globali	Consente all'utente di accedere alla finestra Configurazione filtri globali.
Modifica filtri globali	Consente all'utente di modificare la configurazione dei filtri globali. **NOTA:** Per accedere a questa funzione, è necessario che sia assegnata anche l'autorizzazione di visualizzazione dei filtri globali.

Amministrazione – Configurazione menu

Autorizzazione	Descrizione
Configurazione menu	Consente all'utente di accedere alla finestra Configurazione menu e di aggiungervi nuove opzioni che verranno visualizzate nel menu Evento quando si fa clic con il pulsante destro del mouse su un evento.

Amministrazione - Statistiche DAS

Autorizzazione	Descrizione
Statistiche DAS	Consente all'utente di visualizzare l'attività DAS (DAS_Binary e interrogazioni).

Amministrazione – Informazioni su file di evento

Autorizzazione	Descrizione
Informazioni su file di evento	Consente all'utente di visualizzare lo stato dei file di evento.

Amministrazione – Visualizzazioni server

Autorizzazione	Descrizione
Visualizzazione server	Consente all'utente di monitorare lo stato di tutti i processi.
Controllo server	Consente all'utente di avviare, riavviare e interrompere processi.

Amministrazione – Gestione utenti

Autorizzazione	Descrizione
Uso/visualizzazione conto utente	Consente all'utente di visualizzare e utilizzare conti utente.
Creazione conto utente	Consente all'utente di creare un conto utente. **NOTA:** Per accedere a questa funzione, è necessario che sia assegnata anche l'autorizzazione di visualizzazione/conto utente.
Modifica conto utente esistente	Consente all'utente di modificare un conto utente esistente. **NOTA:** Per accedere a questa funzione, è necessario che sia assegnata anche l'autorizzazione di visualizzazione/conto utente.
Eliminazione conto utente	Consente all'utente di eliminare un conto utente esistente. **NOTA:** per accedere a questa funzione, è necessario che sia assegnata anche l'autorizzazione di visualizzazione/conto utente.

Amministrazione – Gestione sessioni utente

Autorizzazione	Descrizione
Gestione sessioni utente	Consente all'utente di visualizzare, bloccare e terminare utenti attivi (login a Sentinel Control Center).

Amministrazione – Gestione ruoli iTRAC

Autorizzazione	Descrizione
Gestione ruoli iTRAC	Consente all'utente di visualizzare e utilizzare Gestione ruoli nella scheda Amministratore.

7 Motore di correlazione di Sentinel

NOTA: Il termine agente è equivalente a servizio di raccolta. Si farà in seguito riferimento agli agenti come servizi di raccolta.

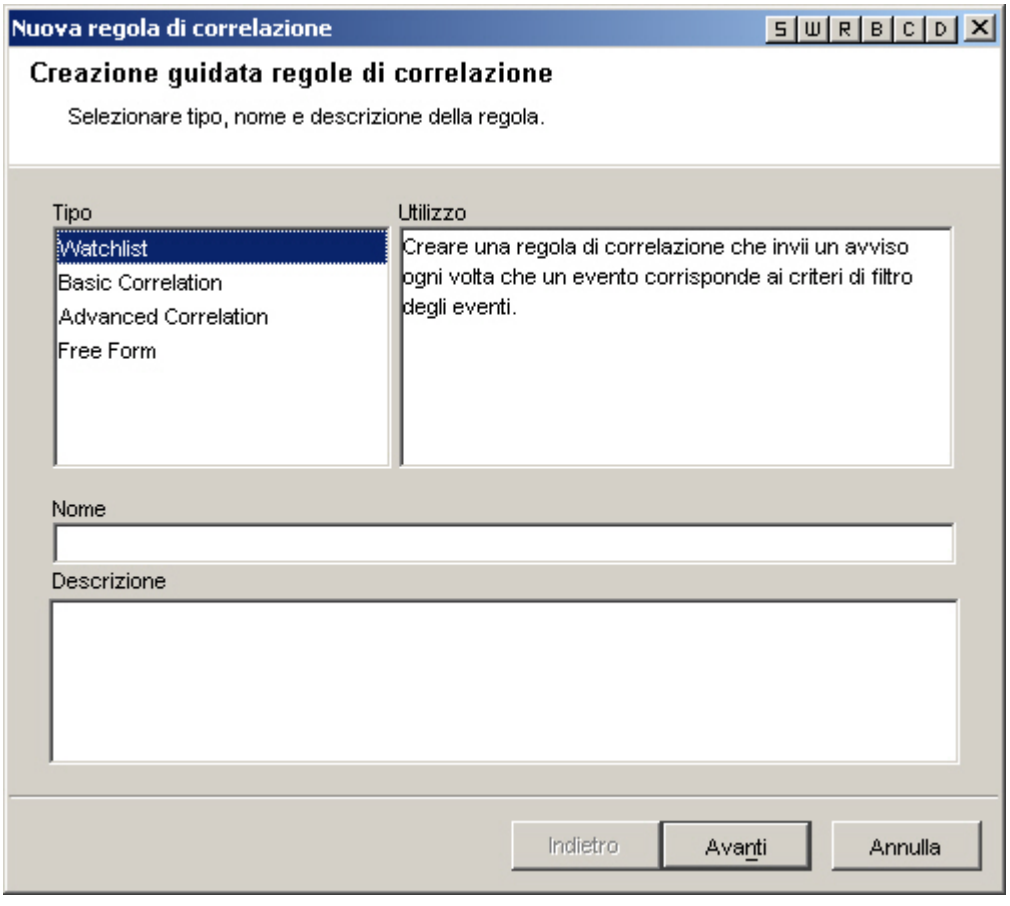
Il motore di correlazione di Sentinel è un'applicazione multithread residente in memoria. Il multithreading consente al motore di correlazione di sfruttare i vantaggi offerti dall'hardware multiprocessore, ad esempio computer SMP (Symmetric Multiprocessing).

Il motore di correlazione è progettato per ricevere dati da dispositivi di sicurezza, dispositivi di rete e altre origini di applicazioni e per cercare schemi significativi, in genere all'interno di intervalli di tempo specifici. Questi schemi possono indicare attacchi, intrusioni, usi impropri o errori. Se viene generato un evento correlato, il campo rt2 verrà compilato con il nome della regola di correlazione.

Il motore di correlazione di Sentinel garantisce una distribuzione scalabile. Questa architettura consente la distribuzione di una rete di motori di correlazione che lavorano insieme per eseguire correlazioni in tempo reale sui dati relativi alla sicurezza, ad esempio eventi di sicurezza monitorati in tempo reale, risultati di scansioni della vulnerabilità relativi a sistemi potenzialmente interessati nonché informazioni su risorse indicanti i processi di business critici per il sistema e la loro associazione con altri sistemi nell'organizzazione.

Il motore di correlazione di Sentinel è basato su regole. Tramite le regole create nell'editor regole di Sentinel Control Center, è possibile gestire l'elaborazione del motore di correlazione. L'editor regole è basato su un insieme di procedure guidate che offrono diverse opzioni per la creazione delle regole. Di seguito sono riportate le procedure guidate per la creazione delle regole:

- Watchlist
- Correlazione di base
- Correlazione avanzata
- RuleLg in formato libero



Tipi di filtri di correlazione

Per Watchlist, Correlazione di base e Correlazione avanzata è possibile scegliere tra quattro diversi tipi di filtri, ovvero:

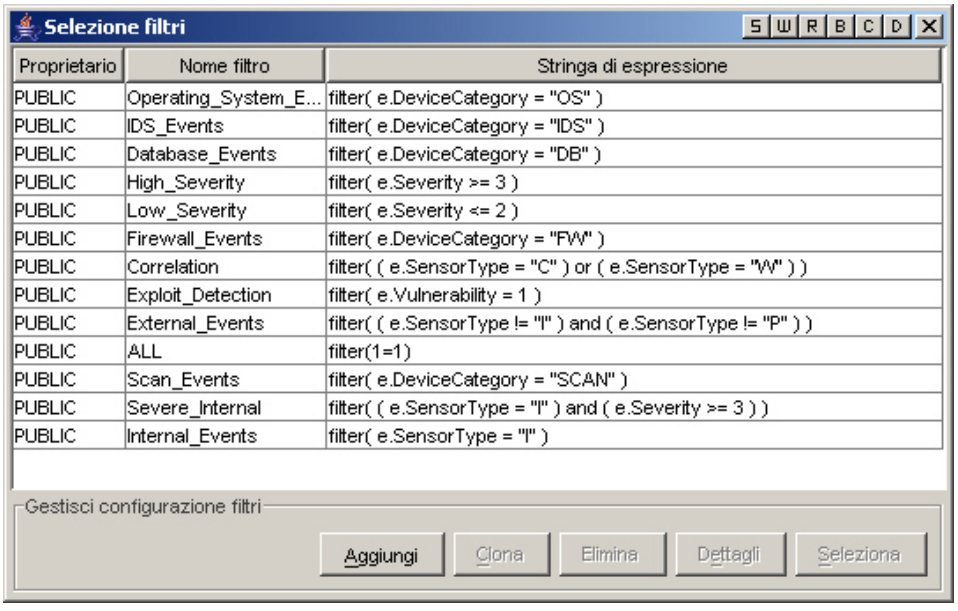
- Consenti tutto: equivalente all'esecuzione di un filtro con gravità maggiore o uguale a zero.
- Schema: qualsiasi espressione regolare con sintassi analoga a grep. Una regola è in grado di cercare un indirizzo IP di origine specifico di un pirata informatico e notificare l'utente ogni volta che l'indirizzo IP è presente in un messaggio di eventi.
- Gestione filtri: elenco a discesa che consente di selezionare o creare un nuovo filtro di Gestione filtri.
- Generatore: consente di creare criteri di inclusione ed esclusione degli eventi in base all'algebra booleana.

Filtro di correlazione di tipo schema

I filtri di correlazione di tipo schema utilizzano qualsiasi espressione regolare con sintassi analoga a grep. La corrispondenza con l'espressione regolare viene eseguita mediante la concatenazione di tutti i tag META presenti in ogni evento in entrata. Ad esempio, virusXYZ cercherà la stringa virusXYZ in tutti i tag META presenti in ogni evento in entrata.

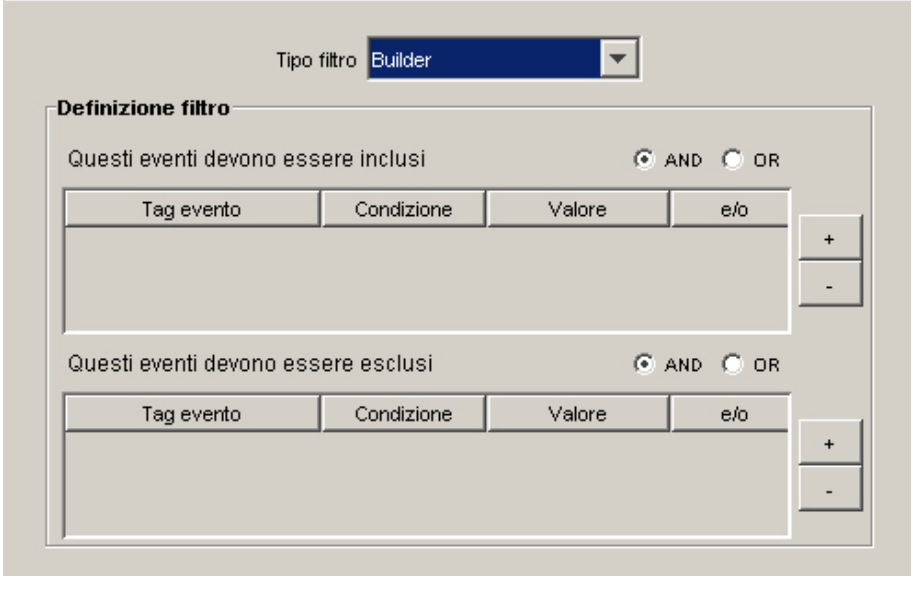
Filtro di correlazione di Gestione filtri

Questa opzione consente di selezionare un filtro esistente o creare un filtro da utilizzare nella propria correlazione tramite la finestra Gestione filtri.



Filtro di correlazione del generatore

Nel filtro di correlazione del generatore sono disponibili due parti, una con i criteri di inclusione (eventi che devono essere inclusi nella corrispondenza allo schema) e l'altra con quelli di esclusione (eventi che devono essere esclusi dalla corrispondenza allo schema).



- Gli eventi che devono essere inclusi nella corrispondenza allo schema. Utilizzare questa tabella per specificare le condizioni al fine di limitare gli eventi che attiveranno la correlazione.
  - Tag evento: la colonna Tag evento include un elenco a discesa dei tag di evento disponibili (noti inoltre come tag META) ai fini della correlazione.
  - Condizione: la colonna Condizione è un elenco a discesa di operatori utilizzati per la creazione di una condizione di correlazione.
  - Valore: la colonna Valore è un campo in formato libero utilizzabile per immettere valori se si scelgono le condizioni =, !=, <, >, <= o >=. Se nella colonna Condizione si seleziona =Meta-Tag o !=Meta-Tag, la colonna Valore conterrà un elenco a discesa di tag META disponibili da cui scegliere. È possibile immettere qualsiasi valore con le restrizioni seguenti:
    - Non è mai possibile immettere virgolette singole.
    - I caratteri jolly sono l'asterisco (*) e il punto (.) e possono essere inseriti in qualsiasi punto della stringa, se si utilizza regex.
    - Non sono disponibili caratteri di escape; ovvero, i caratteri jolly non possono essere ignorati.
  - and/or – Facendo clic su queste caselle è possibile passare da "and" a "or". Quando vengono specificate più condizioni in questa tabella, i pulsanti "and" e "or" consentono di indicare se è necessario soddisfare tutte le condizioni o solo una di esse. Scegliere "and" per indicare che è necessario soddisfare tutte le condizioni. Scegliere "or" per indicare che è necessario soddisfare solo una delle condizioni.

NOTA: La selezione effettuata diventa valida solo se la tabella contiene almeno una seconda riga. Tutte le righe della tabella vengono impostate di default sull'operatore logico scelto tranne l'ultima. Non sono possibili combinazioni di "and" e "or" tra le righe della tabella.

  - Pulsanti +/-: il pulsante + consente di aggiungere una riga supplementare alla fine della tabella. Il pulsante - consente di rimuovere la riga selezionata dalla tabella indipendentemente dalla posizione all'interno di quest'ultima.
- Gli eventi che devono essere esclusi dalla corrispondenza allo schema. Utilizzare questa tabella per specificare le condizioni al fine di limitare gli eventi che non attiveranno la regola di correlazione.
  - Tag evento: elenco di tag di evento disponibili ai fini della correlazione.
  - Condizione: la colonna Condizione è un elenco a discesa di operatori utilizzati per la creazione di una condizione di correlazione.
  - Valore: la colonna Valore è un campo in formato libero utilizzabile per immettere valori se si scelgono le condizioni =, !=, <, >, <= o >=. Se nella colonna Condizione si seleziona =Meta-Tag o !=Meta-Tag, la colonna Valore conterrà un elenco a discesa di tag META disponibili da cui scegliere. È possibile immettere qualsiasi valore con le restrizioni seguenti:
    - Non è mai possibile immettere virgolette singole.
    - I caratteri jolly sono l'asterisco (*) e il punto (.) e possono essere inseriti in qualsiasi punto della stringa, se si utilizza regex.
    - Non sono disponibili caratteri di escape; ovvero, i caratteri jolly non possono essere ignorati.
  - and/or – Facendo clic su queste caselle è possibile passare da "and" a "or". Quando vengono specificate più condizioni in questa tabella, i pulsanti "and" e "or" consentono di indicare se è necessario soddisfare tutte le condizioni o solo una di esse. Scegliere "and" per indicare che è necessario soddisfare tutte le condizioni. Scegliere "or" per indicare che è necessario soddisfare solo una delle condizioni.

NOTA: La selezione effettuata diventa valida solo se la tabella contiene almeno una seconda riga. Tutte le righe della tabella vengono impostate di default sull'operatore logico scelto tranne l'ultima. Non sono possibili combinazioni di "and" e "or" tra le righe della tabella.

- Pulsanti +/-: il pulsante + consente di aggiungere una riga supplementare alla fine della tabella. Il pulsante - consente di rimuovere la riga selezionata dalla tabella indipendentemente dalla posizione all'interno di quest'ultima.

Definizione di una regola di correlazione

Le procedure guidate per la creazione delle regole di correlazione, ovvero Watchlist, Correlazione base e Correlazione avanzata, consentono di aggiungere rapidamente un tipo di regola predefinito in base all'azione che si desidera eseguire. La procedura guidata per ogni tipo di regola consente di gestire la generazione della regola di correlazione nel linguaggio di origine per le regole del motore di correlazione. Ognuna di queste regole viene creata mediante l'utilizzo della finestra Regole di correlazione nella scheda Amministratore.

La procedura guidata per la creazione delle regole include un editor in formato libero che consente di utilizzare il linguaggio di definizione delle correlazioni RuleLg per aggiungere la regola direttamente nel linguaggio di origine delle regole del motore di correlazione.

Watchlist

È possibile scegliere fra quattro diversi tipi di filtro. ovvero:

- Consenti tutto: equivalente all'esecuzione di un filtro con gravità maggiore o uguale a zero.
- Schema: qualsiasi espressione regolare con sintassi analoga a grep.
- Gestione filtri: elenco a discesa che consente di selezionare o creare un nuovo filtro di Gestione filtri.
- Generatore: consente di creare criteri di inclusione ed esclusione degli eventi in base all'algebra booleana.

Per ulteriori informazioni, vedere Creazione di una regola watchlist.

Correlazione di base

È possibile scegliere fra quattro diversi tipi di filtro. ovvero:

- Consenti tutto: equivalente all'esecuzione di un filtro con gravità maggiore o uguale a zero.
- Schema: qualsiasi espressione regolare con sintassi analoga a grep.
- Gestione filtri: elenco a discesa che consente di selezionare o creare un nuovo filtro di Gestione filtri.
- Generatore: consente di creare criteri di inclusione ed esclusione degli eventi in base all'algebra booleana.

Questa regola consente di conteggiare il numero di volte in base al quale alcune condizioni vengono soddisfatte in un intervallo di tempo specifico.

Una regola di correlazione base consente, ad esempio, di cercare lo stesso indirizzo IP di origine segnalato cinque volte in cinque minuti, anche se gli eventi si riferiscono a prodotti differenti, come un sistema di rilevazione delle intrusioni (IDS) e un firewall.

Per ulteriori informazioni, vedere Creazione di una regola di correlazione di base.

Correlazione avanzata

È possibile scegliere fra quattro diversi tipi di filtro. ovvero:

- Consenti tutto: equivalente all'esecuzione di un filtro con gravità maggiore o uguale a zero.

- Schema: qualsiasi espressione regolare con sintassi analoga a grep.
- Gestione filtri: elenco a discesa che consente di selezionare o creare un nuovo filtro di Gestione filtri.
- Generatore: consente di creare criteri di inclusione ed esclusione degli eventi in base all'algebra booleana.

Questa regola consente quanto segue:

- Conteggiare il numero di volte in base al quale alcune condizioni vengono soddisfatte in un intervallo di tempo specifico.
- Incorporare tutte le funzioni della regola di correlazione semplice nonché valutare gli eventi rispetto ad eventi precedenti.
- Una regola di correlazione avanzata consente, ad esempio, di cercare eventi provenienti dallo stesso indirizzo IP di origine e diretti allo stesso indirizzo IP di destinazione, che abbiano lo stesso nome e che si verifichino sia all'interno che all'esterno di un firewall, ad indicare un attacco realizzato attraverso il firewall

Per ulteriori informazioni, vedere Creazione di una regola di correlazione avanzata.

Correlazione RuleLg in formato libero

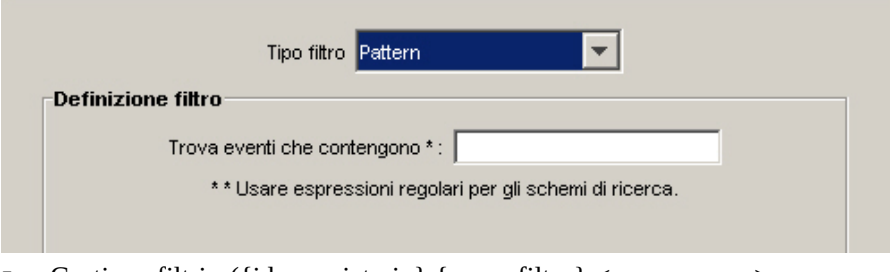
Il linguaggio di definizione delle regole di correlazione RuleLg consente di assumere il controllo completo ai fini della definizione delle regole di correlazione. Prima di utilizzare questo tipo di regola di correlazione, è consigliabile acquisire familiarità con il linguaggio di definizione delle regole di correlazione RuleLg.

Per ulteriori informazioni, vedere Creazione di una regola di correlazione RuleLg in formato libero.

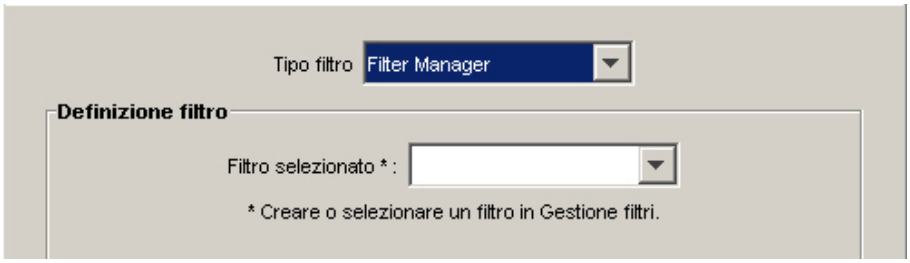
Creazione di una regola watchlist

Creare una regola watchlist quando si desidera specificare una stringa che verrà cercata dal motore di correlazione in ogni evento in entrata. Per creare una regola watchlist:

- Selezionare Regola watchlist nella prima finestra della Creazione guidata regole di correlazione. Completare le informazioni seguenti:
  - Nome regola - Nome che verrà visualizzato nell'elenco delle regole. È consentito un numero massimo di 255 caratteri senza punti. Non sono consentiti caratteri ASCII estesi. Il nome della regola prevede la distinzione tra maiuscole e minuscole.
  - Descrizione - Breve descrizione. La lunghezza massima del testo descrittivo è di 1.024 caratteri.
- Tipo di filtro
  - Consenti tutto:
  - Schema: consente di cercare gli eventi contenenti *



  - Gestione filtri - ({id proprietario}:{nome filtro}:<nome campo>

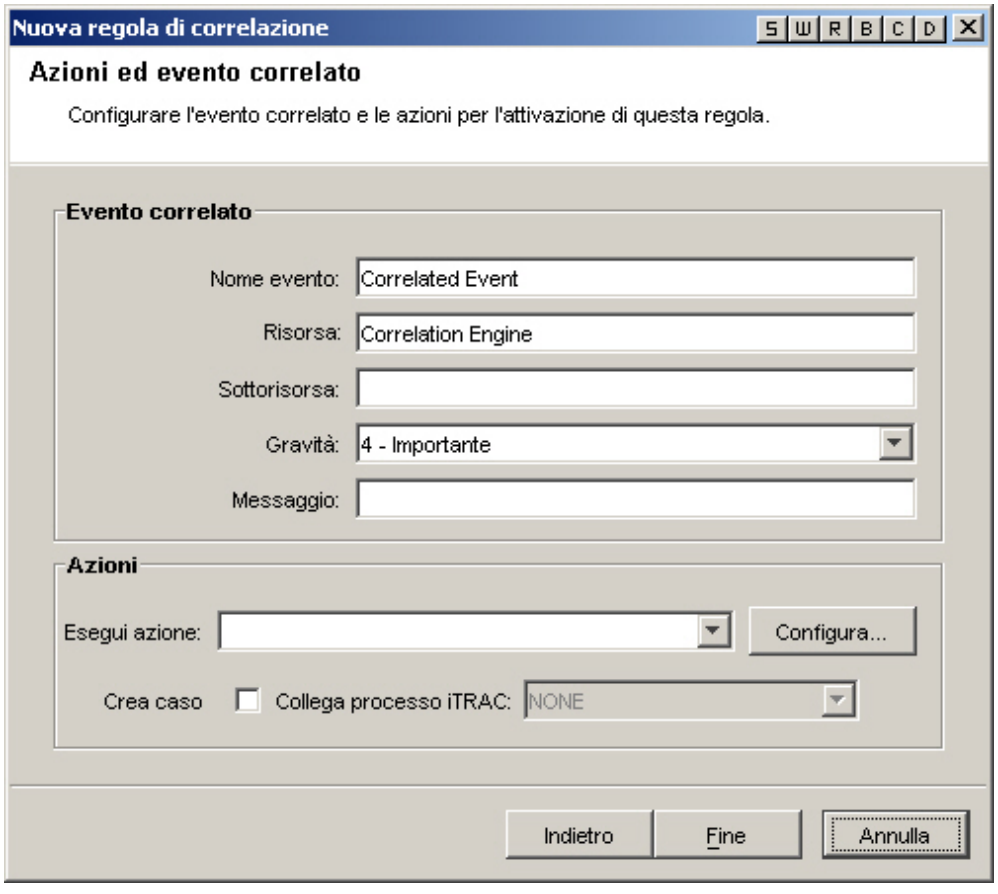


- Generatore

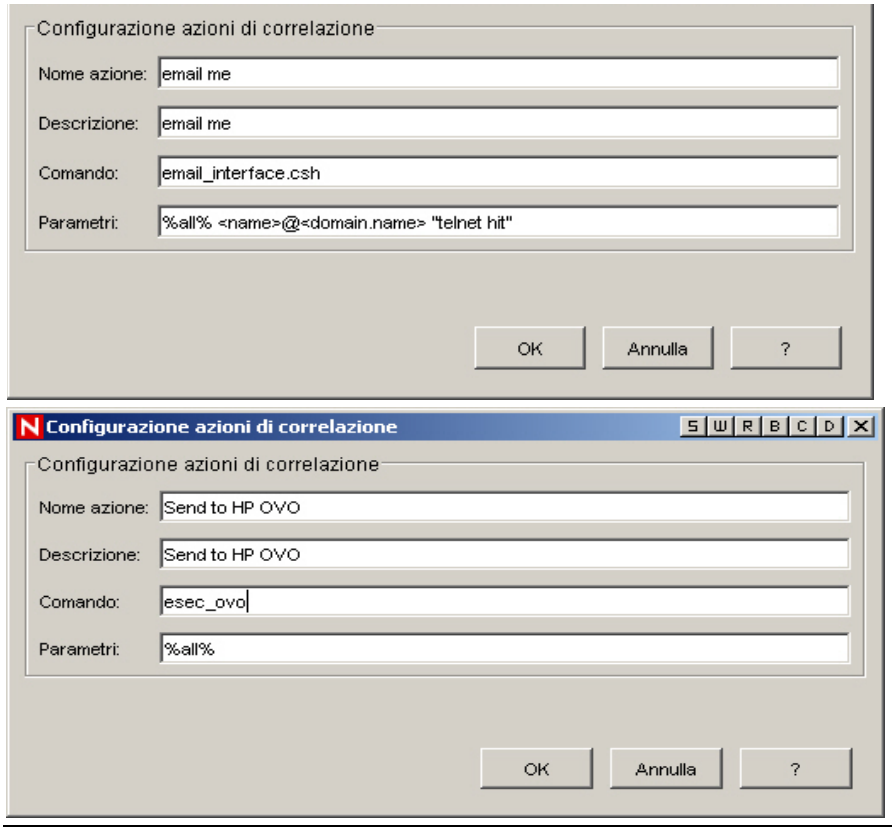
- Pagina Azioni ed evento correlato: questo pannello definisce quale azione verrà automaticamente intrapresa quando gli eventi soddisfano la regola di correlazione. L'unica voce obbligatoria è il livello di gravità, che di default è il 4.
  - Nome evento – Default: Evento correlato. Si tratta del nome in formato testo dell'evento correlato.
  - Risorsa - Default: Motore di correlazione. Si tratta del nome in formato testo di una risorsa del sistema.
  - Sottorisorsa - Default: <nessuno>. Si tratta del nome della sottorisorsa, per risorse con più sottorisorse.
  - Imposta livello di gravità su - Default: 4. Si tratta del livello di gravità assegnato all'evento. I valori validi sono 0, 1, 2, 3, 4 (default) e 5. È disponibile un elenco a discesa con i livelli di gravità validi.
  - Testo messaggio personalizzato - Default: <nessuno>. Si tratta del testo che verrà visualizzato insieme all'evento, utile per identificare la condizione che ha attivato la regola watchlist. È consentito un numero massimo di 4.000 caratteri. Il testo immesso in questa casella viene anteposto al testo dell'evento di correlazione con un separatore pipe. Ad esempio, l'input "Nuovo messaggio" produrrà il messaggio correlato "Nuovo messaggio|Tre istanze di....".
  - Esegui azione (solo Oracle) - Default: <nessuno>. Si tratta del nome di un file eseguibile che viene eseguito al momento dell'attivazione della regola watchlist. Il file deve trovarsi nella directory $ESEC_HOME/sentinel/exec ed essere eseguibile dall'utente esecadm. In questa casella di testo in formato libero non è prevista alcuna

convalida dell'input. È possibile specificare i tag META che si desidera inviare all'eseguibile.

- Esegui azione (solo MSSQL) - Default: <nessuno>. Si tratta del nome di un file eseguibile che viene eseguito al momento dell'attivazione della regola. Il file deve trovarsi nella directory %ESEC_HOME%\sentinel\bin ed essere eseguibile dall'utente esecadm. Non è prevista alcuna convalida dell'input. È possibile specificare i tag META che si desidera inviare all'eseguibile. Di seguito sono riportati due esempi di regola di correlazione, uno per l'invio di un messaggio e-mail e uno per l'invio dell'evento di correlazione a HP OVO.



La riga di comando e la riga dei parametri vengono compilate come stringhe. Nelle rispettive fasi di analisi vengono applicate le stesse regole in base alle quali la barra rovesciata (\) viene considerata un carattere di escape. Per le sequenze di escape è possibile utilizzare i caratteri \, % e “. Ad esempio, \%\”\\ equivale a %”\. Se è necessario un comando contenente una barra rovesciata, ad esempio per eseguire un comando Windows in una sottodirectory di sentinel\bin, immettere due barre rovesciate (\\) per ogni barra di directory. Per eseguire ad esempio un file batch denominato run.bat in %esec_home%\sentinel\bin\batchfiles\, sarà necessario immettere batchfiles\\run.bat. Tenere presente che tutti gli eseguibili devono trovarsi in %esec_home%\sentinel\bin\.



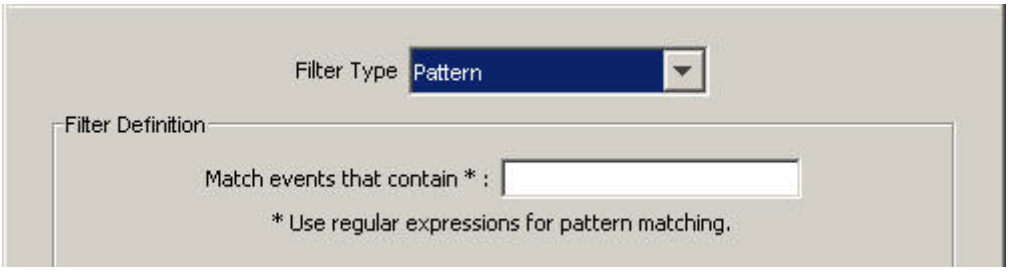
NOTA: Per ulteriori informazioni su comandi e parametri, vedere il capitolo 5 relativo ai tag META di Wizard e Sentinel, della Guida di riferimento dell'utente e la sezione sull'output di correlazione.

- Crea caso – Una delle azioni dell'evento correlato può essere la creazione di un caso.
- Collega processo iTrac – Il caso creato può essere collegato a un processo iTrac.

Creazione di una regola di correlazione di base

Creare una regola di correlazione base quando si desidera conteggiare il numero di volte in base al quale alcune condizioni vengono soddisfatte in un intervallo di tempo specifico. La procedura da seguire è la seguente:

- Selezionare Correlazione base nella prima finestra Creazione guidata regole di correlazione. Completare le informazioni seguenti:
  - Nome regola - Nome che verrà visualizzato nell'elenco delle regole. È consentito un numero massimo di 255 caratteri senza punti. Non sono consentiti caratteri ASCII estesi. Il nome della regola prevede la distinzione tra maiuscole e minuscole.
  - Descrizione - Breve descrizione. La lunghezza massima del testo descrittivo è di 1.024 caratteri.
- Tipo di filtro
  - Consenti tutto
  - Schema



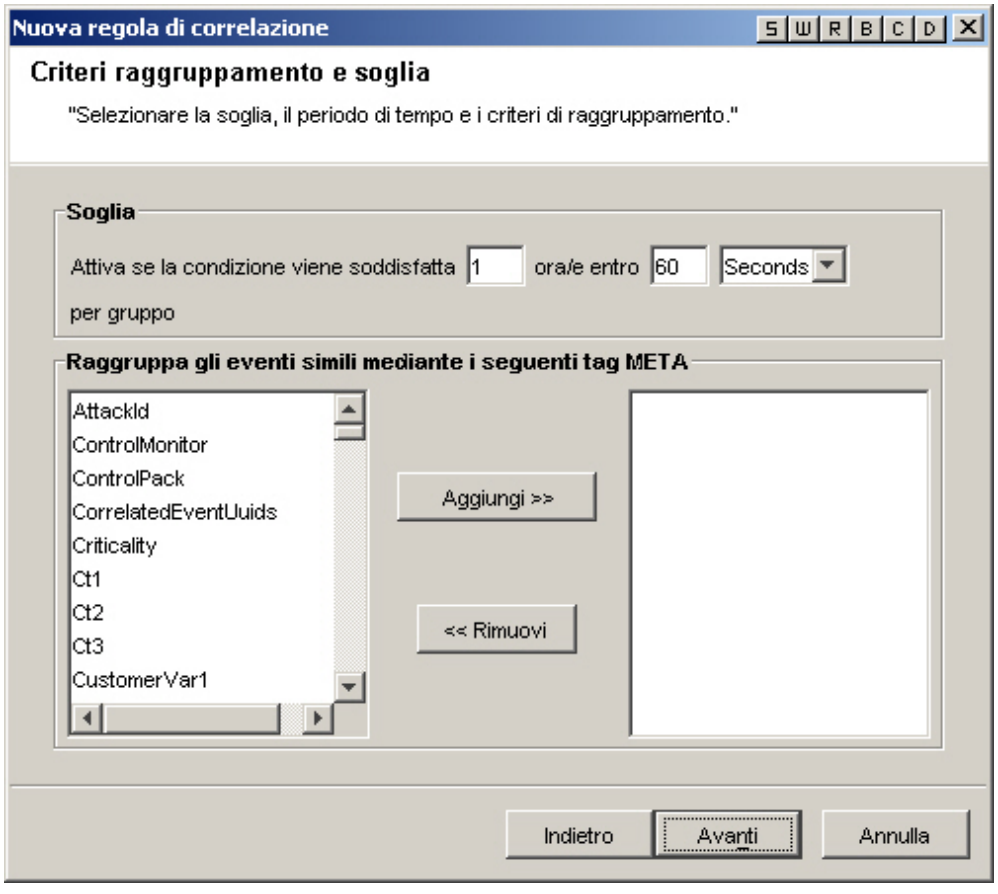
- Gestione filtri - ({id proprietario}:{nome filtro}:<nome campo>

- Generatore

- Criteri raggruppamento e soglia (metà superiore della finestra) – Attiva regola: Questa opzione consente di inserire criteri di corrispondenza per più eventi che accedono al sistema in un determinato periodo di tempo.
  - Quando la condizione viene soddisfatta _volte - Default: 1. Una regola viene attivata solo dopo essere stata rilevata il numero di volte specificato. L'intervallo di input validi per questa soglia include valori maggiori o uguali a 1.
  - entro (intervallo di tempo) - Default: 60 secondi. Questa impostazione consente di associare la condizione all'intervallo di tempo. Si tratta di un input variabile combinato e un elenco a discesa. L'elenco a discesa include le opzioni seguenti: secondi, minuti, ore e giorni.

NOTA: Se l'intervallo di tempo corrisponde a 0, il trigger viene considerato istantaneo. Per la correlazione di base, l'evento si verifica al massimo una volta per un intervallo di tempo pari a zero.

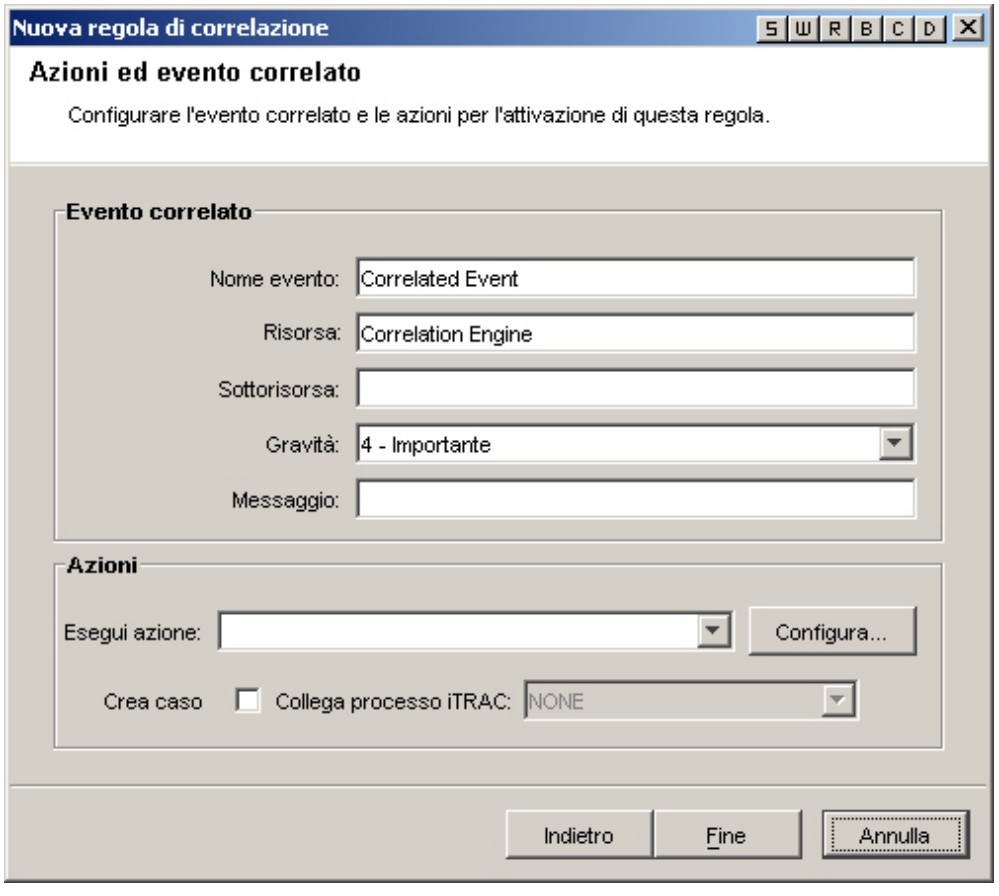
- Pagina Criteri raggruppamento e soglia (parte inferiore della finestra): consente la correlazione in base a combinazioni distinte dei seguenti tag META. Selezionare i tag META da utilizzare in combinazione ai fini della correlazione. Gli eventi vengono inseriti in gruppi sulla base dei tag META selezionati.

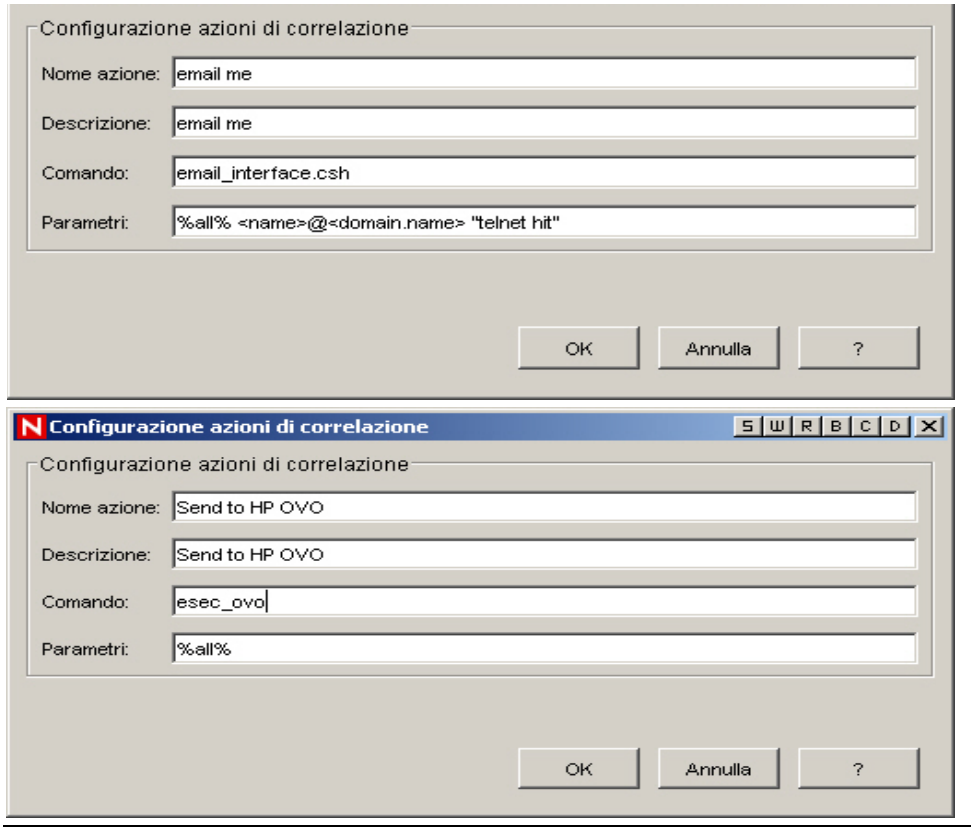


- Pagina Azioni ed evento correlato: questo pannello definisce quale azione verrà automaticamente intrapresa quando gli eventi soddisfano la regola di correlazione. L'unica voce obbligatoria è il livello di gravità, che di default è il 4.
  - Nome evento – Default: Evento correlato. Si tratta del nome in formato testo dell'evento correlato.
  - Risorsa - Default: Motore di correlazione. Si tratta del nome in formato testo di una risorsa del sistema.
  - Sottorisorsa - Default: <nessuno>. Si tratta del nome della sottorisorsa, per risorse con più sottorisorse
  - Imposta livello di gravità su - Default: 4. Si tratta del livello di gravità assegnato all'evento. I valori validi sono 0, 1, 2, 3, 4 (default) e 5. È disponibile un elenco a discesa con i livelli di gravità validi.
  - Testo messaggio personalizzato - Default: <nessuno>. Si tratta del testo che verrà visualizzato insieme all'evento, utile per identificare la condizione che ha attivato la regola watchlist. È consentito un numero massimo di 4.000 caratteri. Il testo

immesso in questa casella viene anteposto al testo dell'evento di correlazione con un separatore pipe. Ad esempio, l'input "Nuovo messaggio" produrrà il messaggio correlato "Nuovo messaggio|Tre istanze di....".

- Esegui il comando (solo Oracle) - Default: <nessuno>. Si tratta del nome di un file eseguibile che viene eseguito al momento dell'attivazione della regola watchlist. Il file deve trovarsi nella directory $ESEC_HOME/sentinel/exec ed essere eseguibile dall'utente esecadm. In questa casella di testo in formato libero non è prevista alcuna convalida dell'input. È possibile specificare i tag META che si desidera inviare all'eseguibile.
- Esegui azione (solo MSSQL) - Default: <nessuno>. Si tratta del nome di un file eseguibile che viene eseguito al momento dell'attivazione della regola. Il file deve trovarsi nella directory %ESEC_HOME%\sentinel\bin ed essere eseguibile dall'utente esecadm. Non è prevista alcuna convalida dell'input. È possibile specificare i tag META che si desidera inviare all'eseguibile. Di seguito sono riportati due esempi di regola di correlazione, uno per l'invio di un messaggio e-mail e uno per l'invio dell'evento di correlazione a HP OVO.





NOTA: Per ulteriori informazioni su comandi e parametri, vedere il capitolo 5 relativo ai tag META di Wizard e Sentinel, della Guida di riferimento dell'utente e la sezione sull'output di correlazione.

- Crea caso – Una delle azioni dell'evento correlato può essere la creazione di un caso.
- Collega processo iTrac: il caso creato può essere collegato a un processo iTrac.

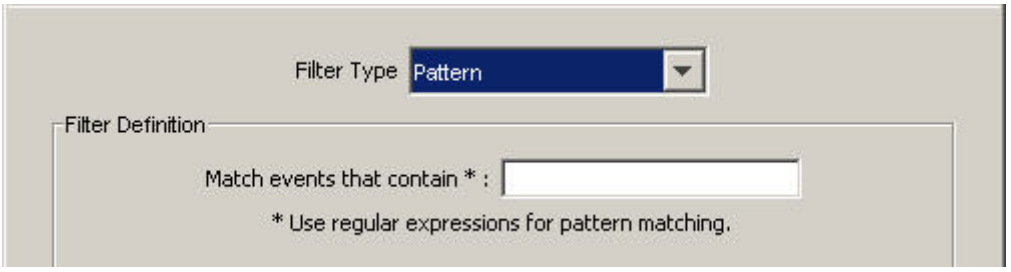
Creazione di una regola di correlazione avanzata

Una regola di correlazione avanzata consente di aumentare la complessità di una regola mediante l'aggiunta di una condizione supplementare nella finestra Criteri aggiuntivi, ovvero aggiungendo un livello di AND logico alla definizione della regola.

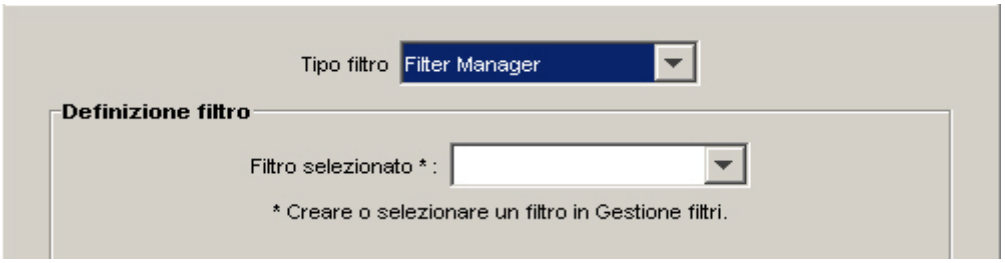
Creare una regola di correlazione avanzata quando si desidera non solo conteggiare il numero di volte in base al quale vengono soddisfatte alcune condizioni, ma anche per ricevere un avviso nel caso in cui gli eventi soddisfino criteri relativi a eventi precedenti. La procedura da seguire è la seguente:

- Selezionare Correlazione avanzata nella prima finestra Creazione guidata regole di correlazione. Completare le informazioni seguenti:
  - Nome regola - Nome che verrà visualizzato nell'elenco delle regole. È consentito un numero massimo di 255 caratteri senza punti. Non sono consentiti caratteri ASCII estesi. Il nome della regola prevede la distinzione tra maiuscole e minuscole.
  - Descrizione - Breve descrizione. La lunghezza massima del testo descrittivo è di 1.024 caratteri.

- Tipo di filtro
  - Consenti tutto
  - Schema



  - Gestione filtri - ({id proprietario}:{nome filtro}:<nome campo>



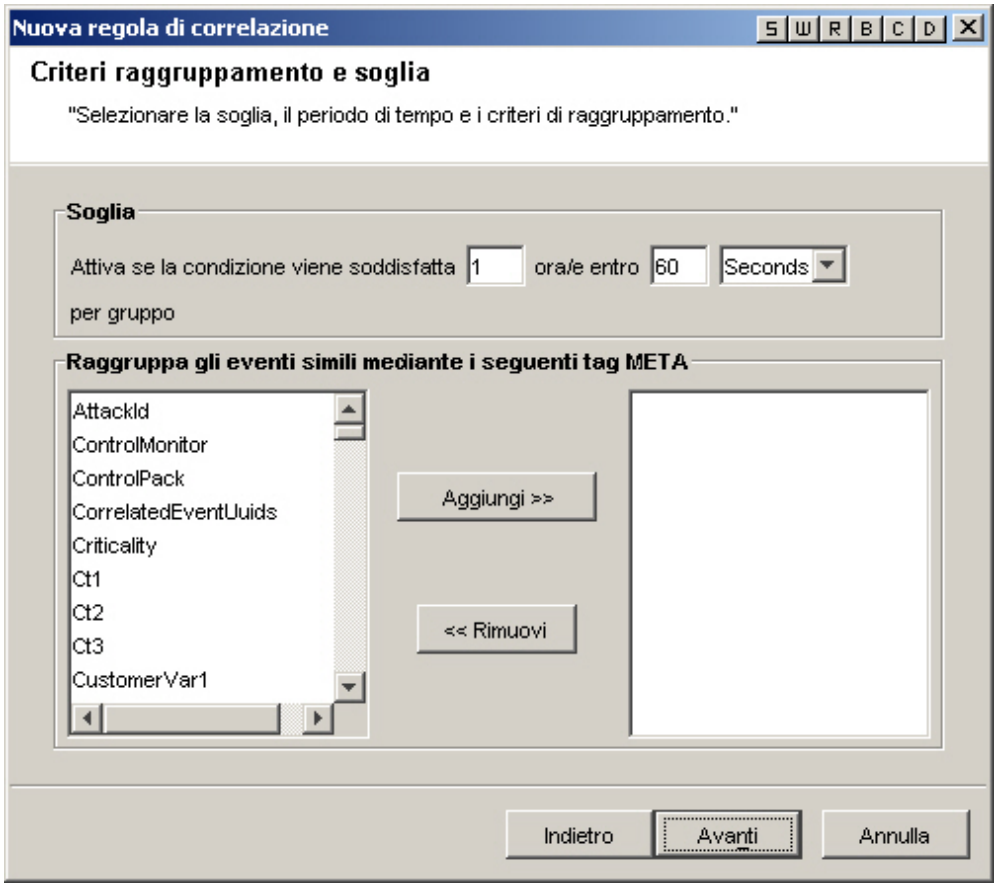
  - Generatore

- Criteri aggiuntivi: questa opzione consente di inserire criteri di corrispondenza per più eventi che accedono al sistema in un determinato periodo di tempo. Il periodo di default è 60 secondi. Si tratta di un input variabile combinato e un elenco a discesa. L'elenco a discesa include le opzioni seguenti: secondi, minuti, ore e giorni.
- Criteri raggruppamento e soglia (metà superiore della finestra) – Attiva regola: Questa opzione consente di inserire criteri di corrispondenza per più eventi che accedono al sistema in un determinato periodo di tempo.
  - Quando la condizione viene soddisfatta _volte - Default: 1. Una regola viene attivata solo dopo essere stata rilevata il numero di volte specificato. L'intervallo di input validi per questa soglia include valori maggiori o uguali a 1.

- entro (intervallo di tempo) - Default: 60 secondi. Questa impostazione consente di associare la condizione all'intervallo di tempo. Si tratta di un input variabile combinato e un elenco a discesa. L'elenco a discesa include le opzioni seguenti: secondi, minuti, ore e giorni.

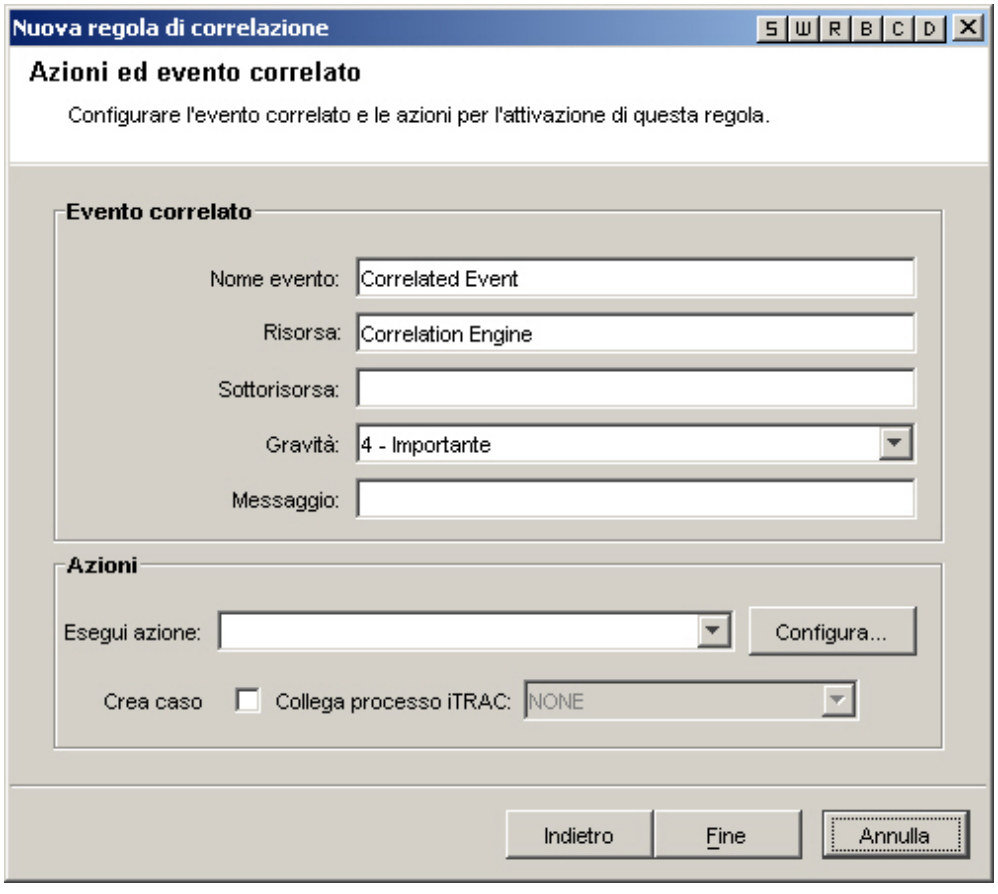
NOTA: Se l'intervallo di tempo corrisponde a 0, il trigger viene considerato istantaneo. Per la correlazione di base, l'evento si verifica al massimo una volta per un intervallo di tempo pari a zero.

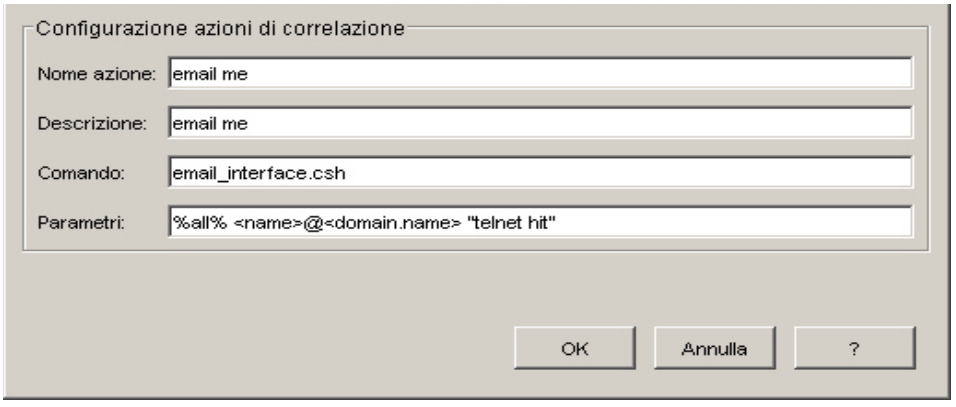
- Criteri raggruppamento e soglia (parte inferiore della finestra): consente la correlazione in base a combinazioni distinte dei seguenti tag META. Selezionare i tag META da utilizzare in combinazione ai fini della correlazione. Gli eventi vengono inseriti in gruppi sulla base dei tag META selezionati.

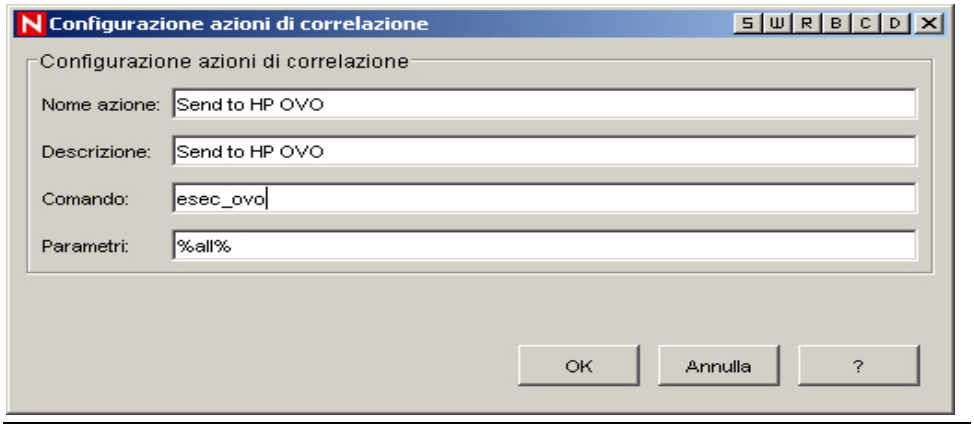


- Pagina Azioni ed evento correlato: questo pannello definisce quale azione verrà automaticamente intrapresa quando gli eventi soddisfano la regola di correlazione. L'unica voce obbligatoria è il livello di gravità, che di default è il 4.
  - Nome evento – Default: Evento correlato. Si tratta del nome in formato testo dell'evento correlato.
  - Risorsa - Default: Motore di correlazione. Si tratta del nome in formato testo di una risorsa del sistema.
  - Sottorisorsa - Default: <nessuno>. Si tratta del nome della sottorisorsa, per risorse con più sottorisorse

- Imposta livello di gravità su - Default: 4. Si tratta del livello di gravità assegnato all'evento. I valori validi sono 0, 1, 2, 3, 4 (default) e 5. È disponibile un elenco a discesa con i livelli di gravità validi.
- Testo messaggio personalizzato - Default: <nessuno>. Si tratta del testo che verrà visualizzato insieme all'evento, utile per identificare la condizione che ha attivato la regola watchlist. È consentito un numero massimo di 4.000 caratteri. Il testo immesso in questa casella viene anteposto al testo dell'evento di correlazione con un separatore pipe. Ad esempio, l'input "Nuovo messaggio" produrrà il messaggio correlato "Nuovo messaggio|Tre istanze di....".
- Esegui il comando (solo Oracle) - Default: <nessuno>. Si tratta del nome di un file eseguibile che viene eseguito al momento dell'attivazione della regola watchlist. Il file deve trovarsi nella directory $ESEC_HOME/sentinel/exec ed essere eseguibile dall'utente esecadm. In questa casella di testo in formato libero non è prevista alcuna convalida dell'input. È possibile specificare i tag META che si desidera inviare all'eseguibile.
- Esegui azione (solo MSSQL) - Default: <nessuno>. Si tratta del nome di un file eseguibile che viene eseguito al momento dell'attivazione della regola. Il file deve trovarsi nella directory %ESEC_HOME%\sentinel\bin ed essere eseguibile dall'utente esecadm. Non è prevista alcuna convalida dell'input. È possibile specificare i tag META che si desidera inviare all'eseguibile. Di seguito sono riportati due esempi di regola di correlazione, uno per l'invio di un messaggio e-mail e uno per l'invio dell'evento di correlazione a HP OVO.







NOTA: Per ulteriori informazioni su comandi e parametri, vedere il capitolo 5, Tag META di Wizard e Sentinel, nella Guida di riferimento dell'utente e nella sezione relativa all'output di correlazione.

- Crea caso – Una delle azioni dell'evento correlato può essere la creazione di un caso.
- Collega processo iTrac – Il caso creato può essere collegato a un processo iTrac.

Creazione di una regola di correlazione RuleLg in formato libero

Il motore di correlazione si basa su tre operazioni fondamentali. Queste operazioni sono combinate in modo da creare una regola per operatori di flusso, unione e intersezione. Le tre operazioni fondamentali sono le seguenti:

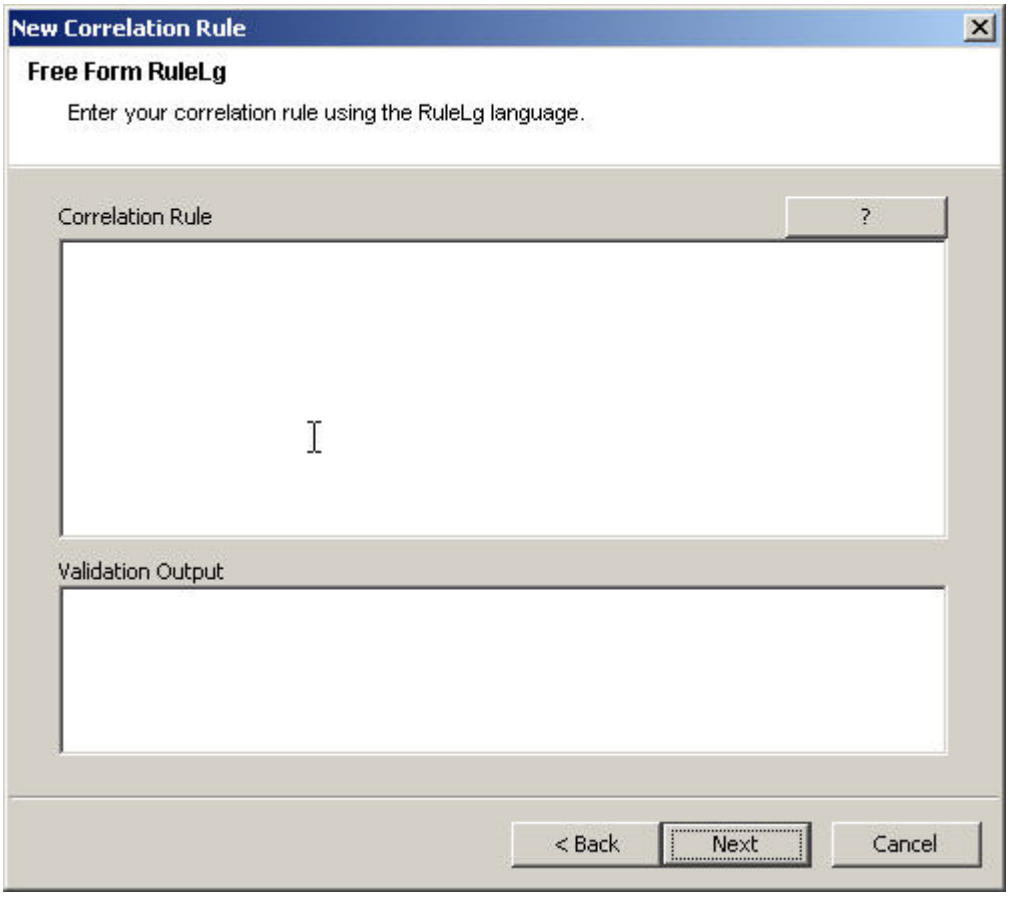
- Operazione filter
- Operazione window
- Operazione trigger

ATTENZIONE: Se si rinomina un tag, non utilizzare il nome originale per la creazione di una regola di correlazione.

Il linguaggio della regola riflette direttamente queste operazioni e indica come possono essere combinate in modo intuitivo per definire le regole di correlazione. Ogni operazione è progettata e implementata in modo specifico per garantire prestazioni elevate ed è basata su un gruppo di eventi, ovvero sulla ricezione di un gruppo di eventi come input e sulla restituzione di un gruppo di eventi. L'evento attuale elaborato da una regola spesso ha un significato speciale ai fini della semantica del

linguaggio. L'evento attuale fa sempre parte di un gruppo di eventi all'interno e all'esterno di un'operazione a meno che il gruppo non sia vuoto. Se un gruppo di input di un'operazione è vuoto, l'operazione stessa non viene valutata.

Per semplificare, le regole di correlazione elaborano in modo serializzato gli eventi in ingresso nel motore di correlazione, uno a uno. In realtà, il motore di correlazione è in grado di elaborare più eventi e di valutare contemporaneamente più regole relative a un evento.



Operazione filter

Le operazioni filter (espressione booleana) consentono di applicare un filtro in base al contenuto dell'evento attuale, ovvero in base ai valori dei tag META e all'espressione booleana specifica del filtro. L'output di un filtro può essere il gruppo vuoto (se l'evento attuale non soddisfa le condizioni del filtro) oppure un gruppo contenente l'evento attuale e tutti gli altri eventi del gruppo in ingresso.

- I filtri vengono applicati all'evento attuale per il quale viene valutata l'espressione booleana:
  - L'operazione filter restituisce il gruppo di input se l'espressione booleana restituisce il valore "true".
  - L'operazione filter restituisce il gruppo vuoto se l'espressione booleana restituisce il valore "false".
- Un'espressione booleana di filtro è costituita da istruzioni di confronto e corrispondenza con gli operatori booleani “and”, “or” e “not”.

Operazione filter - Precedenza e associatività degli operatori RuleLg

L'ordine di precedenza degli operatori booleani filter va dal primo (quello più in alto) all'ultimo (quello più in basso):

Operatore	Significato	Tipo di operatore	Associatività
not	operatore logico not	unario	nessuno
and	operatore logico and	binario	da sinistra a destra
or	operatore logico or	binario	da sinistra a destra

Valgono le indicazioni seguenti:

- Le istruzioni di confronto consentono di valutare i valori dei tag META in base ad altri valori di tag META o restrizioni.
- Gli operatori di confronto disponibili sono =, !=, >, <, >=, <=.
- Le istruzioni di corrispondenza disponibili sono rappresentate da espressioni regolari, ad esempio match regex() o match subnets, match subnet().
- Le istruzioni di confronto e corrispondenza possono essere nidificate nel numero di livelli desiderato mediante parentesi.
- I nomi dei tag META inclusi nelle istruzioni di confronto e corrispondenza devono essere sempre preceduti dall'elemento "e." per specificare l'evento attuale.
- Se l'applicazione di un filtro rappresenta l'ultima o l'unica operazione di una regola di correlazione, il gruppo di output del filtro viene utilizzato per generare un evento di correlazione. Si tratta del gruppo di eventi di output dell'operazione filter con l'evento attuale per primo.
- Se il filtro non costituisce l'ultima operazione di una regola di correlazione (ovvero è presente un operatore flow alla sua destra), il gruppo di output del filtro viene utilizzato come gruppo di input per le altre operazioni (tramite l'operatore flow).

Ad esempio: se l'evento attuale ha una gravità pari a 4 e il tag META della risorsa contiene un elemento "FW" o "Comm", viene inviato un evento correlato all'evento attuale (evento singolo) elencato come evento correlato.

```
filter(e.sev = 4 and (e.res match regex ("FW") or e.res
   match regex ("Comm")))
```

In un altro esempio, se uno dei tag META dell'evento attuale contiene un elemento "ABC", viene inviato un evento correlato all'evento attuale (evento singolo) elencato come evento correlato.

```
filter(e.all match regex("ABC"))
```

Operazione window

Le operazioni window (espressione booleana semplice [, espressione di filtro], int durata) vengono eseguite sull'evento attuale in relazione a un'operazione window di eventi precedenti. Questi ultimi vengono gestiti dall'operazione window stessa. L'output di un'operazione window può essere un gruppo vuoto (se l'evento attuale non corrisponde all'espressione booleana semplice) oppure un gruppo contenente l'evento attuale e tutti gli eventi precedenti per i quali l'espressione booleana semplice viene soddisfatta.

L'espressione booleana semplice può essere un'istruzione di confronto singola oppure un'istruzione di corrispondenza singola di un valore di tag META di un evento precedente con un valore di tag META attuale oppure una costante. Per le espressioni booleane:

- È necessario anteporre al nome del tag META l'elemento "e." per specificare l'evento attuale oppure "w." per specificare eventi precedenti
- Gli operatori di confronto disponibili sono =, !=, >, <, >=, <=, in e not in
- Le istruzioni di corrispondenza disponibili sono rappresentate da espressioni regolari, ad esempio match regex() o match subnets, match subnet()
- Nelle espressioni booleane semplici di un'operazione window deve essere presente un elemento w.[tag META]
- Se uno o più eventi precedenti soddisfano l'espressione booleana semplice rispetto all'evento attuale, il gruppo di output corrisponde all'evento in ingresso più tutte le corrispondenze nell'operazione window
- Se nessuno degli eventi nell'operazione window corrisponde all'evento attuale per l'espressione booleana semplice, viene restituito un gruppo vuoto come output

Gli eventi precedenti vengono gestiti per la durata specificata dell'operazione window.

Il parametro facoltativo dell'espressione di filtro di un'operazione window consente di determinare quali eventi devono essere gestiti dall'operazione window. È possibile utilizzare come espressione qualsiasi filtro valido.

- Tutti gli eventi in ingresso nel motore di correlazione che soddisfano le condizioni del filtro vengono inseriti nell'operazione window degli eventi precedenti.
- Se non è presente alcuna espressione di filtro tutti gli eventi in ingresso nel motore di correlazione vengono gestiti dall'operazione window.
- L'evento attuale non viene inserito nell'operazione window finché la valutazione dell'operazione window dell'evento attuale non viene completata.
- L'operazione window gestisce solo le parti pertinenti degli eventi precedenti allo scopo di ridurre l'utilizzo della memoria.

Se l'operazione window rappresenta l'ultima o l'unica operazione di una regola di correlazione, il gruppo di output dell'operazione viene utilizzato per generare un evento di correlazione. Si tratta del gruppo di eventi di output dell'operazione window con l'evento attuale per primo.

Esempio 1

```
window(e.sip = w.sip, filter(e.sip match subnet
   (<xxx.xxx.x.x/yy>)), 60)
```

Nell’esempio sopra riportato, se l’evento attuale include un indirizzo IP di origine nell’elemento specificato dall’indirizzo xxx.xxx.x.x/yy con maschera di sottorete CIDR e corrisponde a uno o più eventi verificatisi negli ultimi 60 secondi, viene inviato un evento correlato all'evento attuale e gli eventuali eventi precedenti vengono inviati come eventi correlati (evento attuale per primo).

Esempio 2

```
window(e.sip = w.dip, 3600) intersection
window(e.dp = w.dp, 3600) intersection
window(e.evt = w.evt, 3600)
```

Quello sopra riportato è un tipo di regola Domino. Un aggressore sfrutta la vulnerabilità di un sistema per utilizzare quest'ultimo come piattaforma d'attacco.

Esempio 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)
```

Nell'esempio sopra riportato viene illustrato un tipo di regola interno/esterno. La firma di un attacco è presente in due sistemi di rilevazione delle intrusioni, uno all'interno e l'altro all'esterno di un firewall, e la gravità dell'attacco è maggiore di 3.

Operazione trigger

Lo scopo principale di un'operazione trigger è il conteggio di un numero di eventi relativamente a una durata specificata. Se il totale indicato viene raggiunto entro la durata specificata, l'output sarà costituito da un gruppo di eventi contenente tutti gli eventi gestiti dall'operazione trigger. In caso contrario, verrà restituito un output vuoto.

- L'operazione trigger riceve come input un gruppo di eventi da restituire come parte del gruppo di eventi di output se il numero, la durata e i tag META dell'elemento "discriminator" dei gruppi di input precedenti e il gruppo di input attuale soddisfano i criteri definiti dall'operazione trigger.
- Il totale è un valore intero che specifica il numero di eventi che devono verificarsi entro la durata indicata al fine di restituire un gruppo di output non vuoto.
- La durata è un valore intero espresso in secondi indicante che gli eventi di durata vengono gestiti dall'operazione trigger.
- Se la durata è uguale a zero, l'operazione trigger confronta solo il numero di eventi nel gruppo di input con il totale e restituisce l'evento attuale se il numero è maggiore o uguale al totale.
- Se si riceve un nuovo gruppo di eventi di input, il trigger scarta innanzitutto gli eventi obsoleti, ovvero quelli che hanno superato la durata, e quindi inserisce l'evento attuale. Se il numero di eventi risultante è maggiore o uguale al totale specificato, l'output dell'operazione trigger corrisponde a un gruppo contenente tutti gli eventi.
- Se l'operazione trigger rappresenta l'ultima o l'unica operazione di una regola di correlazione, il gruppo di output dell'operazione viene utilizzato per generare un evento di correlazione. Si tratta del gruppo di eventi di output dell'operazione trigger con l'evento attuale per primo.
- Se il trigger non costituisce l'ultima operazione di una regola di correlazione (ovvero è presente un operatore flow alla sua destra), il gruppo di output del trigger viene utilizzato come gruppo di input per le altre operazioni (tramite l'operatore flow).
- Dopo la prima volta che i criteri dell'operazione di trigger vengono soddisfatti (e viene pertanto restituito un gruppo di eventi di output), se i criteri vengono nuovamente soddisfatti includendo almeno uno degli eventi di output precedenti e l'operazione trigger è l'ultima o l'unica operazione, il motore di correlazione non genera un nuovo evento correlato, bensì un aggiornamento dell'evento correlato precedente.
- L'elemento discriminator (elenco di tag META) include un elenco delimitato da virgole di tag META. Le operazioni trigger mantengono diversi totali per ogni combinazione distinta di tag META dell'elemento "discriminator".

Se ad esempio 5 eventi con il medesimo indirizzo IP di origine si verificano entro 10 secondi, viene inviato un evento correlato ai 5 eventi come eventi correlati (evento attuale per primo).

```
trigger(5,10,discriminator(e.sip))
```

Anche se l'opzione della regola in formato libero consente la creazione di espressioni di complessità illimitata, queste regole potrebbero non avere alcun senso. Il formato normale supportato di un'espressione RuleLg viene diviso in tre parti, ovvero la sezione filter, la sezione window e la sezione trigger. Le tre sezioni vengono connesse con un operatore flow.

La sezione filter può contenere più operazioni filter collegate.

Esempio:

```
(filter(e.sev = 5) union filter(e.sev =4))
(filter(e.sev = 5 or e.sev =4))
```

NOTA: Questa sezione è facoltativa. Se viene omessa equivale a filter(1=1).

La sezione window può contenere più operazioni window di intersezione.

Esempio:

(window(w.sev = e.sev,10) intersection window(w.sip = e.sip,10))

NOTA: Questa sezione è facoltativa.

La sezione trigger può contenere una sola operazione trigger.

Esempio

```
(trigger(5,10))
```

NOTA: Questa sezione è facoltativa. Se viene omessa la regola si comporta come se terminasse con trigger(1,0).

Combinazione di operatori e operazioni per la creazione di regole

Gli operatori che possono essere combinati a operazioni per la creazione di regole sono i seguenti:

- Operatore flow
- Operatore union
- Operatore intersection

L'ordine di precedenza degli operatori delle operazioni filter, window e trigger va dal primo (quello più in alto) all'ultimo (quello più in basso):

Operatore	Significato	Tipo di operatore	Associatività
flow	Il gruppo di output diventa gruppo di input	binario	da sinistra a destra
intersection	Intersezione dei gruppi (rimozione dei duplicati)	binario	da sinistra a destra

Operatore	Significato	Tipo di operatore	Associatività
union	Unione dei gruppi (rimozione dei duplicati)	binario	da sinistra a destra

Operatore flow

Il gruppo di eventi di output dell'operazione a sinistra rappresenta il gruppo di eventi di input dell'operazione a destra.

Ad esempio:

```
filter(e.sev = 5) flow trigger(3, 60)
```

L'output dell'operazione filter rappresenta l'input dell'operazione trigger. L'operazione trigger conteggia gli eventi con gravità pari a 5.

Operatore union

Indica l'unione del gruppo di output dell'operazione a sinistra con quello dell'operazione a destra. Il gruppo di output risultante contiene gli eventi sia del gruppo di output dell'operazione a sinistra sia quelli del gruppo di output dell'operazione a destra, ad eccezione dei duplicati.

Ad esempio:

```
filter(e.sev = 5) union filter(e.sip = 192.168.0.1)
```

equivale a

```
filter(e.sev = 5 or e.sip = 192.168.0.1)
```

Operatore intersection

Indica l'intersezione del gruppo di output dell'operazione a sinistra con quello dell'operazione a destra. Il gruppo di output risultante contiene gli eventi comuni al gruppo di output dell'operazione a sinistra e al gruppo di output dell'operazione a destra, ad eccezione dei duplicati.

Ad esempio:

```
filter(e.sev = 5) intersection filter(e.sip =
   192.17.16.32)
```

equivale a

```
filter(e.sev = 5 and e.sip = 192.17.16.32)
```

Regole di correlazione di esempio

In questo documento viene illustrato l'esempio di un gruppo di regole di correlazione basata su regole, insieme ai prerequisiti (requisiti) necessari per rendere effettive le regole. Le regole possono variare in base alla configurazione del sistema.

I tag da e.rv50 a e.rv53 inclusi negli esempi RuleLg corrispondono alle mappature impostate nei file di mappatura del servizio di raccolta. Se si apre ad esempio il file windows_v2000_mapv*.csv o snort_v20_mapv*.csv, è possibile verificare quanto segue:

- La colonna della lingua corrisponde a e.rv50
- Le colonne della comunità corrispondono a e.rv51
- La colonna della famiglia corrisponde a e.rv52
- La colonna dell'evento corrisponde a e.rv53

Ad esempio:

```
filter (e.rv52 = "Worm") flow trigger (3, 300)
```

Questa regola fa riferimento alla tassonomia NIDS. Se si controlla la colonna della famiglia nel file di mappatura snort, sarà possibile individuare più di 40 istanze della parola Worm. Questa regola verrà attivata per più di 40 diversi attacchi di worm se gli attacchi si verificano per tre volte in 5 minuti.

Di seguito sono riportate alcune regole di correlazione di esempio relative ad alcuni tipi di attacchi.

- Brute Force – stessa origine e destinazione
- Overflow del buffer - da stessa origine a stessa destinazione
- Overflow del buffer - interruzione del servizio
- Denial of Service
- Errore di login - da un'origine a una destinazione qualsiasi
- Errore di login - da una stessa origine a una stessa destinazione
- Microsoft - login anonimo
- Microsoft - autenticazione Windows generale
- Microsoft - IE
- Microsoft – IIS
- Microsoft - autenticazione LAN Manager
- Microsoft – MDAC
- Microsoft - accesso al registro remoto
- Microsoft– SQL Server
- Microsoft - NETBIOS
- Microsoft - scripting Windows
- Backdoor multipli – origini diverse
- Backdoor multipli – origine singola
- Trojan Horse
- UNIX - server Web Apache
- UNIX - BIND/DNS
- UNIX - FTP
- UNIX - UNIX generale
- UNIX - LPD (Line Printer Daemon)
- UNIX - chiamata di routine remota (RPC)
- UNIX - servizi remoti
- UNIX-Secure Shell.
- UNIX - sendmail
- UNIX – SNMP
- Presenza virus
- Presenza worm

Attacco di overflow del buffer e interruzione del servizio

Questa regola identificherà una potenziale violazione della sicurezza in seguito a un attacco di overflow del buffer. La regola attiverà un avviso se la destinazione di un attacco di overflow del buffer determina l'interruzione di un servizio entro 60 secondi dall'attacco. Un servizio di raccolta basato sull'host, HIDS/OS, è in grado di rilevare se un servizio viene interrotto. Gli attacchi di overflow del buffer possono essere rilevati dal servizio di raccolta NIDS, HIDS o OS.

Se un sistema viene interessato da un attacco di overflow del buffer, è necessario che tale evento venga controllato.

Frequenza della regola	Requisiti della regola	Tassonomia della regola
1 volta	Definire quanto segue prima di implementare la regola: ▪ Piattaforme IDS di rete convertibili dalla tassonomia di Sentinel (per ulteriori informazioni, consultare la tabella Tassonomia NIDS) ▪ Piattaforme IDS host convertibili dalla tassonomia di Sentinel (per ulteriori informazioni, consultare la tabella Tassonomia HIDS e OS)	NIDS HIDS/OS

RuleLg per questa regola

```
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)
```

Attacco Denial of Service e interruzione del servizio

Questa regola identificherà una potenziale violazione della sicurezza in seguito a un attacco Denial of Service. La regola attiverà un avviso se la destinazione di un attacco Denial of Service determina l'interruzione di un servizio entro 60 secondi dall'attacco. L'interruzione del servizio viene rilevata da un servizio di raccolta basato sull'host, ad esempio HIDS/OS. Gli attacchi di overflow del buffer possono essere rilevati dai servizi di raccolta NIDS, HIDS o OS.

Se un sistema viene interessato da un attacco Denial of Service, è necessario eseguire ulteriori controlli in merito.

Frequenza della regola	Requisiti della regola	Tassonomia della regola
1 volta	Definire quanto segue prima di implementare la regola: ▪ Piattaforme IDS di rete convertibili dalla tassonomia di Sentinel (per ulteriori informazioni, consultare la tabella Tassonomia NIDS) ▪ Piattaforme IDS host convertibili dalla tassonomia di Sentinel (per ulteriori informazioni, consultare la tabella Tassonomia HIDS e OS)	NIDS HIDS/OS

RuleLg per questa regola

```
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)
```

Rilevamento di virus

Questa regola identificherà i virus noti che attaccano un sistema all'interno di un'infrastruttura.

Quando vengono attaccati da un virus, i sistemi in genere subiscono effetti dannosi che richiedono il ricaricamento completo dei dati di applicazioni e sistemi o che comportano la perdita completa delle risorse aziendali. L'identificazione di un virus prima della sua diffusione consente di prevenire o di ridurre drasticamente eventuali danni.

Frequenza della regola	Requisiti della regola	Tassonomia della regola
3 volte in 5 minuti	Definire quanto segue prima di implementare la regola: ▪ Piattaforme IDS di rete convertibili dalla tassonomia di Sentinel (per ulteriori informazioni, consultare la tabella Tassonomia NIDS)	NIDS

RuleLg per questa regola

```
filter (e.rv52 ="Virus") flow trigger (3, 300)
```

Rilevamento di worm

Questa regola identificherà i worm noti che attaccano un sistema all'interno di un'infrastruttura.

Quando vengono attaccati da un worm, i sistemi in genere subiscono effetti dannosi che richiedono il ricaricamento completo dei dati di applicazioni e sistemi o che comportano la perdita completa delle risorse aziendali. L'identificazione di un worm prima della sua diffusione consente di ridurre drasticamente gli inconvenienti a cui è esposta la società.

Frequenza della regola	Requisiti della regola	Tassonomia della regola
3 volte in 5 minuti	Definire quanto segue prima di implementare la regola: ▪ Piattaforme IDS di rete convertibili dalla tassonomia di Sentinel (per ulteriori informazioni, consultare la tabella Tassonomia NIDS)	NIDS

RuleLg per questa regola

```
filter (e.rv52 = "Worm") flow trigger (3, 300)
```

Rilevamento di trojan horse

Questa regola identificherà i trojan horse noti insediati in un sistema all'interno dell'infrastruttura.

Quando un attacco trojan horse ha esito positivo, il sistema preso di mira può risultare completamente compromesso.

Frequenza della regola	Requisiti della regola	Tassonomia della regola
3 volte in 5 minuti	Definire quanto segue prima di implementare la regola: ▪ Piattaforme IDS di rete convertibili dalla tassonomia di Sentinel (per ulteriori informazioni, consultare la tabella Tassonomia NIDS) ▪ Piattaforme IDS host convertibili dalla tassonomia di Sentinel (per ulteriori informazioni, consultare la tabella Tassonomia HIDS e OS)	NIDS HIDS/OS

RuleLg per questa regola

```
filter (e.rv52 ="Trojan") flow trigger (3, 500)
```

Tentativi di backdoor multipli da una singola origine

Questa regola metterà in correlazione più tentativi di inserimento o esecuzione di un attacco backdoor da una singola origine.

I programmi Backdoor vengono in genere utilizzati per ottenere il controllo completo del sistema preso di mira e avviare quindi altri attacchi. In genere, questa regola identificherà i tentativi di intrusi alla ricerca di un sistema infetto o di un sistema da infettare.

Frequenza della regola	Requisiti della regola	Tassonomia della regola
5 volte in 2 minuti	Definire quanto segue prima di implementare la regola: ▪ Piattaforme IDS di rete convertibili dalla tassonomia di Sentinel (per ulteriori informazioni, consultare la tabella Tassonomia NIDS) ▪ Piattaforme IDS host convertibili dalla tassonomia di Sentinel (per ulteriori informazioni, consultare la tabella Tassonomia HIDS e OS)	NIDS HIDS/OS

RuleLg per questa regola

```
filter (e.rv50 = "Attack" and e.rv52 = "Backdoor" ) flow
   trigger(5, 120, discriminator (e.sip))
```

Tentativi di backdoor multipli da origini diverse

Questa regola metterà in correlazione più tentativi di inserimento o esecuzione di un attacco backdoor coordinato da diversi sistemi aventi una singola destinazione.

I programmi Backdoor vengono in genere utilizzati per ottenere il controllo completo del sistema preso di mira e avviare quindi altri attacchi. In genere, questa regola identifica quanto segue:

- il sistema di destinazione è compromesso
- l'aggressore sta tentando di sfruttare il sistema compromesso
- l'aggressore sta provando a nascondersi dietro un attacco coordinato
- oppure che l'aggressore ha ricevuto informazioni che la destinazione è vulnerabile a questo tipo di attacco. In questo caso, è possibile che l'aggressore abbia ricevuto informazioni da un'origine interna.

Frequenza della regola	Requisiti della regola	Tassonomia della regola
5 volte in 2 minuti	Definire quanto segue prima di implementare la regola: ▪ Piattaforme IDS di rete convertibili dalla tassonomia di Sentinel (per ulteriori informazioni, consultare la tabella Tassonomia NIDS) ▪ Piattaforme IDS host convertibili dalla tassonomia di Sentinel (per ulteriori informazioni, consultare la tabella Tassonomia HIDS e OS)	NIDS HIDS/OS

RuleLg per questa regola

```
filter (e.rv50 = "Attack" and e.rv52 = "Backdoor" ) flow
   trigger( 5, 120, discriminator(e.dip))
```

Errori di login multipli da un'origine a una destinazione qualsiasi

Questa regola identificherà gli errori di login relativi agli stessi tipi di sistemi.

Gli errori di login relativi allo stesso tipo di conto o sistema possono indicare che il responsabile dell'attacco ha una conoscenza pregressa della rete e dei sistemi critici presenti in essa. Questo dovrebbe suscitare allarme. Maggiori sono le informazioni in suo possesso, più alta sarà la probabilità che l'aggressore riesca a trovare un sistema vulnerabile.

Frequenza della regola	Requisiti della regola	Tassonomia della regola
5 volte in 2 minuti	Definire quanto segue prima di implementare la regola: ▪ Piattaforme IDS di rete convertibili dalla tassonomia di Sentinel (per ulteriori informazioni, consultare la tabella Tassonomia NIDS)	NIDS

RuleLg per questa regola

```
filter ((e.rv52 = "Access" or e.rv52 = "Brute_Force") and
   e.rv51 = "User" and e.rv50 = "Attack") flow trigger
   (5, 120)
```

Errori di login multipli da una stessa origine a una stessa destinazione

Questa regola identificherà più errori di login dalla stessa origine alla stessa destinazione.

Gli errori di login relativi allo stesso tipo di conto o sistema possono indicare che il responsabile dell'attacco ha una conoscenza pregressa della rete e dei sistemi critici presenti in essa. Questo dovrebbe suscitare allarme. Maggiori sono le informazioni in suo possesso, più alta sarà la probabilità che l'aggressore riesca a trovare un sistema vulnerabile.

Frequenza della regola	Requisiti della regola	Tassonomia della regola
3 volte in 5 minuti	Definire quanto segue prima di implementare la regola: ▪ Piattaforme IDS di rete convertibili dalla tassonomia di Sentinel (per ulteriori informazioni, consultare la tabella Tassonomia NIDS)	NIDS

RuleLg per questa regola

```
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))
```

Attacco di overflow del buffer da una stessa origine a una stessa destinazione

Questa regola identificherà un attacco di overflow del buffer dallo stesso indirizzo IP di origine allo stesso indirizzo IP di destinazione.

Gli attacchi di overflow del buffer sono gli attacchi più comuni sulla rete e vengono utilizzati per la disattivazione dei sistemi. Questi tipi di attacchi possono essere bloccati solo a livello perimetrale. L'identificazione di un attacco consente di bloccare il sistema in uso.

Frequenza della regola	Requisiti della regola	Tassonomia della regola
5 volte in 3 minuti	Definire quanto segue prima di implementare la regola: ▪ Piattaforme IDS di rete convertibili dalla tassonomia di Sentinel (per ulteriori informazioni, consultare la tabella Tassonomia NIDS) ▪ Piattaforme IDS host convertibili dalla tassonomia di Sentinel (per ulteriori informazioni, consultare la tabella Tassonomia HIDS e OS)	NIDS HIDS/OS

RuleLg per questa regola

```
filter (e.rv52 ="Buffer_Overflow" ) flow trigger (5, 180,
   discriminator (e.sip, e.dip))
```

Attacco Brute Force riuscito nel punto di corrispondenza tra origine e destinazione

Questa regola identificherà un sistema probabilmente compromesso in seguito alla violazione di una password.

Ripetuti tentativi di accesso mediante combinazioni di nomi utenti e password seguiti da un login riuscito possono indicare che l'aggressore ha ottenuto l'accesso tramite un attacco Brute Force. Se l'attacco riesce, è necessario che il conto utilizzato per l'accesso venga disattivato.

Frequenza della regola	Requisiti della regola	Tassonomia della regola
1 volta in 3 minuti	Definire quanto segue prima di implementare la regola: ▪ Piattaforme IDS di rete convertibili dalla tassonomia di Sentinel (per ulteriori informazioni, consultare la tabella Tassonomia NIDS) ▪ Piattaforme IDS host convertibili dalla tassonomia di Sentinel (per ulteriori informazioni, consultare la tabella Tassonomia HIDS e OS)	NIDS HIDS/OS

RuleLg per questa regola

```
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 - Verifica attacchi su IIS (Internet Information Services)

Questa regola supporta i 10 attacchi principali SANS Microsoft su IIS (Internet Information Service). L'esecuzione di un'applicazione Microsoft IIS può provocare una vulnerabilità a eventuali attacchi.

Frequenza della regola	Requisiti della regola	Tassonomia della regola
1 volta	Definire quanto segue prima di implementare la regola: ▪ Piattaforme IDS di rete convertibili dalla tassonomia di Sentinel (per ulteriori informazioni, consultare la tabella Tassonomia NIDS)	NIDS

RuleLg per questa regola

```
filter (e.rv53 = "Sans_MS_IIS") flow trigger(1,60)
```

Microsoft - Attacco su MDAC (Microsoft Data Access Connector) - Verifica attacchi su RDS (Remote Data Services)

Questa regola supporta i 10 attacchi principali SANS Microsoft su MDAC. L'utilizzo di prodotti Microsoft può provocare una vulnerabilità a eventuali attacchi. MDAC è uno strumento sottostante utilizzato per integrare alcuni prodotti Microsoft.

Frequenza della regola	Requisiti della regola	Tassonomia della regola
1 volta	Definire quanto segue prima di implementare la regola: ▪ Piattaforme IDS di rete convertibili dalla tassonomia di Sentinel (per ulteriori informazioni, consultare la tabella Tassonomia NIDS)	NIDS

RuleLg per questa regola

```
filter (e.rv53 = "Sans_MS_MDAC") flow trigger(1,60)
```

Microsoft – Attacchi su SQL Server – Verifica attacchi su SQL Server

Questa regola supporta i 10 attacchi principali SANS Microsoft su Microsoft SQL Server. L'utilizzo di Microsoft SQL Server può provocare una vulnerabilità a eventuali attacchi. Alcune vulnerabilità sono di una certa gravità e consentono agli utenti che effettuano attacchi remoti di ottenere informazioni riservate, inserire avvisi nel contenuto di database, compromettere server SQL e server host.

Frequenza della regola	Requisiti della regola	Tassonomia della regola
1 volta	Definire quanto segue prima di implementare la regola: ▪ Piattaforme IDS di rete convertibili dalla tassonomia di Sentinel (per ulteriori informazioni, consultare la tabella Tassonomia NIDS)	NIDS

RuleLg per questa regola

```
filter (e.rv53 = "Sans_MS_SQLServer") flow trigger(1,60)
```

Microsoft - NETBIOS - Verifica attacchi su condivisioni di rete Windows non protette

Questa regola supporta i 10 attacchi principali SANS Microsoft su NETBIOS. L'utilizzo di servizi di rete Microsoft con NETBIOS può provocare una vulnerabilità a eventuali attacchi. NETBIOS è un software Microsoft originale per le comunicazioni di rete. Le reti Microsoft attuali non si basano su NETBIOS come mezzo di trasporto.

Frequenza della regola	Requisiti della regola	Tassonomia della regola
1 volta	Definire quanto segue prima di implementare la regola: ▪ Piattaforme IDS di rete convertibili dalla tassonomia di Sentinel (per ulteriori informazioni, consultare la tabella Tassonomia NIDS)	NIDS

RuleLg per questa regola

```
filter (e.rv53 = "Sans_MS_NETBIOS") flow trigger(1,60)
```

Microsoft - Login anonimo - Verifica attacchi su sessioni null

Questa regola supporta i 10 attacchi principali SANS Microsoft su sessioni null. L'utilizzo di sessioni null Microsoft può provocare una vulnerabilità a eventuali attacchi. L'utente anonimo può recuperare informazioni sulla rete o connettersi senza alcuna autenticazione.

Frequenza della regola	Requisiti della regola	Tassonomia della regola
1 volta	Definire quanto segue prima di implementare la regola: ▪ Piattaforme IDS di rete convertibili dalla tassonomia di Sentinel (per ulteriori informazioni, consultare la tabella Tassonomia NIDS)	NIDS

RuleLg per questa regola

```
filter (e.rv53 = "Sans_MS_NullSessions") flow
   trigger(1,60)
```

Microsoft - Autenticazione LM (LAN Manager) - Verifica attacchi su hash LM vulnerabile

Questa regola supporta i 10 attacchi principali SANS Microsoft su hash LM vulnerabile. LM utilizza uno schema di cifratura molto più vulnerabile rispetto agli attuali protocolli di autenticazione Microsoft (NTLM e NTLMv2) e le password LM possono essere identificate in tempi brevi.

Frequenza della regola	Requisiti della regola	Tassonomia della regola
1 volta	Definire quanto segue prima di implementare la regola: ▪ Piattaforme IDS di rete convertibili dalla tassonomia di Sentinel (per ulteriori informazioni, consultare la tabella Tassonomia NIDS)	NIDS

RuleLg per questa regola

```
filter (e.rv53 = "Sans_MS_LM") flow trigger(1,60)
```

Microsoft - Verifica attacchi su autenticazione di Windows generale

Questa regola supporta i 10 attacchi principali SANS Microsoft su password. Se vengono rilevate password vulnerabili, è consigliabile modificarle.

Frequenza della regola	Requisiti della regola	Tassonomia della regola
1 volta	Definire quanto segue prima di implementare la regola: ▪ Piattaforme IDS di rete convertibili dalla tassonomia di Sentinel (per ulteriori informazioni, consultare la tabella Tassonomia NIDS)	NIDS

RuleLg per questa regola

```
filter (e.rv53 = "Sans_MS_WeakPasswords") flow
   trigger(1,60)
```

Microsoft - Verifica attacchi su IE (Internet Explorer)

Questa regola supporta i 10 attacchi principali SANS Microsoft su IE. Nelle versioni più recenti di Microsoft questa applicazione è incorporata nell'interfaccia utente del sistema operativo. Gli attacchi noti tramite IE possono compromettere qualsiasi ambiente Microsoft successivo a Windows 2000.

Frequenza della regola	Requisiti della regola	Tassonomia della regola
1 volta	Definire quanto segue prima di implementare la regola: ▪ Piattaforme IDS di rete convertibili dalla tassonomia di Sentinel (per ulteriori informazioni, consultare la tabella Tassonomia NIDS)	NIDS

RuleLg per questa regola

```
filter (e.rv53 = "Sans_MS_IE") flow trigger(1,60)
```

Microsoft - Verifica attacchi all'accesso del registro remoto

Questa regola supporta i 10 attacchi principali SANS Microsoft sul Registro di sistema Microsoft. Il registro di un sistema operativo Microsoft rappresenta l'ubicazione di tutte le variabili definite dal sistema. La possibilità di modificarlo o sostituirlo può seriamente compromettere il funzionamento o la sicurezza di una piattaforma Microsoft.

Frequenza della regola	Requisiti della regola	Tassonomia della regola
1 volta	Definire quanto segue prima di implementare la regola: ▪ Piattaforme IDS di rete convertibili dalla tassonomia di Sentinel (per ulteriori informazioni, consultare la tabella Tassonomia NIDS)	NIDS

RuleLg per questa regola

```
filter (e.rv53 = "Sans_MS_Registry") flow trigger(1,60)
```

Microsoft - Verifica attacchi su scripting Windows

Questa regola supporta i 10 attacchi principali SANS Microsoft su scripting Windows. Molte applicazioni Microsoft vengono create mediante l'utilizzo del linguaggio di programmazione Visual

Basic. La possibilità di eseguire comandi specificando uno script consente agli aggressori di accedere ai sistemi Microsoft e di assumerne il controllo.

Frequenza della regola	Requisiti della regola	Tassonomia della regola
1 volta	Definire quanto segue prima di implementare la regola: ▪ Piattaforme IDS di rete convertibili dalla tassonomia di Sentinel (per ulteriori informazioni, consultare la tabella Tassonomia NIDS)	NIDS

RuleLg per questa regola

```
filter (e.rv53 = "Sans_MS_Scripting") flow trigger(1,60)
```

UNIX - Verifica attacchi su chiamate di routine remote (RPC)

Questa regola supporta i 10 attacchi principali SANS UNIX su RPC. Le chiamate di routine remote (RPC) rappresentano un metodo che in ambiente UNIX consente di accedere o eseguire applicazioni o file su un sistema remoto senza alcuna autenticazione. Se una chiamata di routine remota viene lasciata aperta, gli utenti remoti potranno eseguire comandi privilegiati sul sistema senza alcuna autenticazione. Le chiamate di routine remote consentono attacchi remoti.

Frequenza della regola	Requisiti della regola	Tassonomia della regola
1 volta	Definire quanto segue prima di implementare la regola: ▪ Piattaforme IDS di rete convertibili dalla tassonomia di Sentinel (per ulteriori informazioni, consultare la tabella Tassonomia NIDS)	NIDS

RuleLg per questa regola

```
filter (e.rv53 = "Sans_Unix_RPC") flow trigger(1,60)
```

UNIX - Verifica attacchi su server Web Apache

Questa regola supporta i 10 attacchi principali SANS UNIX su server Web Apache. Il server Web Apache è un'applicazione gratuita che supporta i server Web. L'esecuzione di un server Web Apache può provocare una vulnerabilità a eventuali attacchi.

Frequenza della regola	Requisiti della regola	Tassonomia della regola
1 volta	Definire quanto segue prima di implementare la regola: ▪ Piattaforme IDS di rete convertibili dalla tassonomia di Sentinel (per ulteriori informazioni, consultare la tabella Tassonomia NIDS)	NIDS

RuleLg per questa regola

```
filter (e.rv53 = "Sans_Unix_Apache") flow trigger(1,60)
```

UNIX - Verifica attacchi su Secure Shell

Questa regola supporta i 10 attacchi principali SANS UNIX su Secure Shell. un protocollo per la cifratura del traffico tra due computer sviluppato per sopperire al gran numero di problemi rilevati con Telnet e FTP.. Questa applicazione consente il trasferimento di dati o l'interazione con sistemi

remoti tramite un metodo sicuro. Tuttavia, in alcune versioni dell'applicazione sono stati identificati diversi bug che consentono agli aggressori di assumere il controllo completo del sistema preso di mira.

Frequenza della regola	Requisiti della regola	Tassonomia della regola
1 volta	Definire quanto segue prima di implementare la regola: ▪ Piattaforme IDS di rete convertibili dalla tassonomia di Sentinel (per ulteriori informazioni, consultare la tabella Tassonomia NIDS)	NIDS

RuleLg per questa regola

```
filter (e.rv53 = "Sans_Unix_SSH") flow trigger(1,60)
```

UNIX – Verifica attacchi su SNMP (Simple Network Management Protocol)

Questa regola supporta i 10 attacchi principali SANS UNIX su SNMP. SNMP è stato originariamente progettato per la gestione dei nodi in una rete. In SNMP V 1.0 non sono mai state implementate funzioni di sicurezza e in SNMP V 3.0 ne sono state introdotte di minimali. Pertanto SNMP è soggetto a un gran numero di attacchi.

Frequenza della regola	Requisiti della regola	Tassonomia della regola
1 volta	Definire quanto segue prima di implementare la regola: ▪ Piattaforme IDS di rete convertibili dalla tassonomia di Sentinel (per ulteriori informazioni, consultare la tabella Tassonomia NIDS)	NIDS

RuleLg per questa regola

```
filter (e.rv53 = "Sans_Unix_SNMP") flow trigger(1,60)
```

UNIX - Verifica attacchi su FTP (File Transfer Protocol)

Questa regola supporta i 10 attacchi principali SANS UNIX su FTP. Il protocollo FTP rappresenta un elemento fondamentale delle comunicazioni su Internet. In quanto tale, quindi, è uno degli obiettivi principali degli aggressori per reindirizzare l'accesso in Internet.

Frequenza della regola	Requisiti della regola	Tassonomia della regola
1 volta	Definire quanto segue prima di implementare la regola: ▪ Piattaforme IDS di rete convertibili dalla tassonomia di Sentinel (per ulteriori informazioni, consultare la tabella Tassonomia NIDS)	NIDS

RuleLg per questa regola

```
filter (e.rv53 = "Sans_Unix_FTP") flow trigger(1,60)
```

UNIX - Verifica attacchi su servizi remoti

Questa regola supporta i 10 attacchi principali SANS UNIX su servizi remoti. I servizi remoti rappresentano un metodo che in ambiente UNIX consente di accedere o eseguire applicazioni o file

su un sistema remoto senza alcuna autenticazione. Se i servizi remoti vengono lasciati aperti, gli utenti remoti potranno eseguire comandi privilegiati su un sistema senza alcuna autenticazione. Ciò consente eventuali attacchi remoti.

Frequenza della regola	Requisiti della regola	Tassonomia della regola
1 volta	Definire quanto segue prima di implementare la regola: ▪ Piattaforme IDS di rete convertibili dalla tassonomia di Sentinel (per ulteriori informazioni, consultare la tabella Tassonomia NIDS)	NIDS

RuleLg per questa regola

```
filter (e.rv53 = "Sans_Unix_RemoteServices") flow
   trigger(1,60)
```

UNIX - Verifica attacchi su LPD (Line Printer Daemon)

Questa regola supporta i 10 attacchi principali su LPD (Line Printer Daemon). LPD rappresenta il meccanismo utilizzato da UNIX per eseguire la stampa dei file. Questa applicazione viene eseguita in ambiente UNIX nel conto radice. I molti bug trovati nell'applicazione consentono agli aggressori di assumere il controllo completo dell'ambiente UNIX.

Frequenza della regola	Requisiti della regola	Tassonomia della regola
1 volta	Definire quanto segue prima di implementare la regola: ▪ Piattaforme IDS di rete convertibili dalla tassonomia di Sentinel (per ulteriori informazioni, consultare la tabella Tassonomia NIDS)	NIDS

RuleLg per questa regola

```
filter (e.rv53 = "Sans_Unix_LPD") flow trigger(1,60)
```

UNIX - Verifica attacchi su Sendmail

Questa regola supporta i 10 attacchi principali SANS UNIX su Sendmail. L'applicazione Sendmail utilizza il protocollo SMTP (Simple Mail Transport Protocol) e rappresenta un elemento fondamentale delle comunicazioni su Internet. In quanto tale, quindi, è uno degli obiettivi principali degli aggressori per reindirizzare l'accesso in Internet.

Frequenza della regola	Requisiti della regola	Tassonomia della regola
1 volta	Definire quanto segue prima di implementare la regola: ▪ Piattaforme IDS di rete convertibili dalla tassonomia di Sentinel (per ulteriori informazioni, consultare la tabella Tassonomia NIDS)	NIDS

RuleLg per questa regola

```
filter (e.rv53 = "Sans_Unix_SendMail") flow trigger(1,60)
```

UNIX - Verifica attacchi su BIND/DNS

Questa regola supporta i 10 attacchi principali SANS UNIX su DNS. Il servizio DNS (Domain Name Service) rappresenta un elemento fondamentale delle comunicazioni su Internet. In quanto tale, quindi, è uno degli obiettivi principali degli aggressori per reindirizzare l'accesso in Internet.

Frequenza della regola	Requisiti della regola	Tassonomia della regola
1 volta	Definire quanto segue prima di implementare la regola: ▪ Piattaforme IDS di rete convertibili dalla tassonomia di Sentinel (per ulteriori informazioni, consultare la tabella Tassonomia NIDS)	NIDS

RuleLg per questa regola

```
filter (e.rv53 = "Sans_Unix_DNS") flow trigger(1,60)
```

UNIX - Verifica attacchi su autenticazione UNIX generale

Questa regola supporta i 10 attacchi principali SANS UNIX su password vulnerabili. Se vengono rilevate password vulnerabili, è consigliabile modificarle.

Frequenza della regola	Requisiti della regola	Tassonomia della regola
1 volta	Definire quanto segue prima di implementare la regola: ▪ Piattaforme IDS di rete convertibili dalla tassonomia di Sentinel (per ulteriori informazioni, consultare la tabella Tassonomia NIDS)	NIDS

RuleLg per questa regola

```
filter (e.rv53 = "Sans_Unix_WeakPasswords") flow
   trigger(1,60)
```

Tabelle di tassonomia

In questa sezione sono incluse due tabelle, ovvero:

- Tassonomia NIDS
- Tassonomia HIDS e OS

Nelle tabelle sono inclusi i diversi valori dei livelli da e.rv50 a e.rv53 relativi agli esempi RuleLg indicati.

Tabella tassonomia NIDS

Azione – Livello 1 (e.rv50)	Sistema – Livello 2 (e.rv51)	Dettaglio – Livello 3 (e.rv52)	Risultati – Livello 4 (e.rv53)
Attacco	Chat	Accesso	
		Overflow del buffer	
		Backdoor	
		Brute_Force	
		DoS	

Azione – Livello 1 (e.rv50)	**Sistema – Livello 2 (e.rv51)**	**Dettaglio – Livello 3 (e.rv52)**	**Risultati – Livello 4 (e.rv53)**
	DNS	Accesso	Sans_Unix_DNS
		Overflow del buffer	Sans_Unix_DNS
		Backdoor	
		Brute_Force	
		DoS	
	E-mail	Accesso	Sans_Unix_SendMail
		Overflow del buffer	Sans_Unix_SendMail Sans_MS_IE
		Backdoor	
		Brute_Force	
		DoS	
	Telnet	Accesso	
		Overflow del buffer	
		Backdoor	
		Brute_Force	
		DoS	
	File	Accesso	Sans_Unix_FTP Sans_MS_WeakPasswords Sans_MS_NETBIOS
		Overflow del buffer	Sans_Unix_FTP
		Backdoor	Sans_Unix_FTP
		Brute_Force	
		DoS	
	Web	Accesso	Sans_Unix_Apache Sans_MS_NETBIOS Sans_MS_WeakPasswords Sans_MS_IIS Sans_MS_Scripting Sans_MS_SQLServer Sans_MS_IE SANS_MS_MDAC
		Overflow del buffer	Sans_Unix_Apache Sans_MS_IIS
		Backdoor	
		Brute_Force	Sans_MS_IIS
		DoS	Sans_Unix_Apache Sans_MS_IIS
	PC	Virus	Sans_MS_IE Sans_MS_IIS
		Script	
		Worm	Sans_MS_SQLServer
		Trojan horse	
	Server	Accesso	Scan_MS_IIS Sans_MS_Registry Sans_MS_SQLServer Sans_MS_NETBIOS

Azione – Livello 1 (e.rv50)	Sistema – Livello 2 (e.rv51)	Dettaglio – Livello 3 (e.rv52)	Risultati – Livello 4 (e.rv53)
			Sans_Unix_remoteServices Sans_Unix_RPC Sans_Unix_SSH
		Overflow del buffer	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	
	Protocollo	IP	
		TCP	
		UDP	
		ICMP	
		HTTP	
		Route	
		Talk	
		XFS	
		SSH	
		IGMP	
		Ora	
		News	
		Windows	
		RIP	
		IDS	
		SNMP	Sans_Unix_SNMP
		BGP	
	Utente	Accesso	Sans_Unix_WeakPasswords Sans_Unix_RemoteServices
		Overflow del buffer	Sans_Unix_RemoteServices Sans_MS_NETBIOS
		Backdoor	
		Brute_Force	
		DoS	
Probe	Chat		
	DNS		
	E-mail		
	File		Sans_Unix_FTP
	Web		Sans_MS_IIS Sans_Unix_Apache
	PC		

Azione – Livello 1 (e.rv50)	**Sistema – Livello 2 (e.rv51)**	**Dettaglio – Livello 3 (e.rv52)**	**Risultati – Livello 4 (e.rv53)**
	Server		Sans_MS_NullSessions Sans_MS_Registry
	Protocollo	IP	
		TCP	
		RIP	
		SNMP	Sans_Unix_SNMP
		SSH	
		Talk	
		Ora	
		Windows	
		UDP	
		ICMP	
		DHCP	
	Scan		
	Telnet		Sans_MS_LM
	Utente		Sans_MS_LM
	IDS		
Policy	Porn		
Compromise	Chat	Accesso	
		Overflow del buffer	Sans_Unix_Weak_Passwords
		Backdoor	
		Brute_Force	
		DoS	
	DNS	Accesso	Sans_Unix_DNS
		Overflow del buffer	
		Backdoor	
		Brute_Force	
		DoS	
	E-mail	Accesso	
		Overflow del buffer	
		Backdoor	Sans_Unix_SendMail
		Brute_Force	
		DoS	
	Telnet	Accesso	
		Overflow del buffer	
		Backdoor	
		Brute_Force	
		DoS	
	File	Accesso	
		Overflow del buffer	
		Backdoor	
		Brute_Force	
		DoS	
	Web	Accesso	Sans_Unix_Apache
		Overflow del buffer	Sans_MS_IIS

Azione – Livello 1 (e.rv50)	Sistema – Livello 2 (e.rv51)	Dettaglio – Livello 3 (e.rv52)	Risultati – Livello 4 (e.rv53)
		Backdoor	Sans_Unix_Apache Sans_MS_Registry
		Brute_Force	
		DoS	
	PC	Virus	
		Script	
		Worm	
		Trojan horse	
	Server	Accesso	Sans_MS_SQLServer
		Overflow del buffer	Sans_Unix_RPC
		Backdoor	Sans_MS_WeakPasswords Sans_MS_Registry Sans_Unix_SNMP Sans_Unix_WeakPasswords
		Brute_Force	
		DoS	
	Utente	Accesso	
		Overflow del buffer	
		Backdoor	
		Brute_Force	
		DoS	

Tabella tassonomia HIDS e OS

Azione – Livello 1 (e.rv50)	Sistema – Livello 2 (e.rv51)	Dettaglio – Livello 3 (e.rv52)	Risultati – Livello 4 (e.rv53)
Attacco	File	Eliminazione	App SO
		Esecuzione	App SO
		Creazione	App SO
		Modifica	App SO
		Accesso	App SO
	Servizio	Eliminazione	App SO
		Interruzione	App SO
		Avvio	App SO
		Creazione	App SO
		Accesso	App SO Priv

Azione – Livello 1 (e.rv50)	**Sistema – Livello 2 (e.rv51)**	**Dettaglio – Livello 3 (e.rv52)**	**Risultati – Livello 4 (e.rv53)**
			E-mail ID Rete File Sistema
		Overflow del buffer	
		Backdoor	
		DoS	
	Config	Eliminazione	App SO
		Modifica	App SO
		Creazione	App SO
		Attivazione	App SO
		Accesso	App SO
	Utente	Creazione	ID Aut Param Priv
		Modifica	ID Aut Param Priv
		Eliminazione	ID Aut Param Priv
		Accesso	Guest Priv Radice Altro
	Gruppo	Creazione	Membro Gruppo
		Modifica	Membro Gruppo
		Eliminazione	Membro Gruppo
	Sistema	Informazioni	
		Memoria	
		Debug	
	Anomoly		
	Telnet	Accesso	
		Overflow del buffer	
		Backdoor	

Azione – Livello 1 (e.rv50)	**Sistema – Livello 2 (e.rv51)**	**Dettaglio – Livello 3 (e.rv52)**	**Risultati – Livello 4 (e.rv53)**
		Brute_Force	
		DoS	
	Web	Accesso	
		Overflow del buffer	
		Backdoor	
		Brute_Force	
		DoS	
	PC	Virus	
		Script	
		Backdoor	
		Worm	
		Trojan horse	
	DNS	Accesso	
		Overflow del buffer	
		Backdoor	
		Brute_Force	
		DoS	
	E-mail	Accesso	
		Overflow del buffer	
		Backdoor	
		Brute_Force	
		DoS	
Probe	File	Eliminazione	App SO
		Esecuzione	App SO
		Creazione	App SO
		Modifica	App SO
		Accesso	App SO
	Servizio	Eliminazione	App SO
		Interruzione	App SO
		Avvio	App SO
		Creazione	App SO
		Accesso	App SO File ID E-mail Priv Rete

Azione – Livello 1 (e.rv50)	Sistema – Livello 2 (e.rv51)	Dettaglio – Livello 3 (e.rv52)	Risultati – Livello 4 (e.rv53)
			Sistema
	Config	Eliminazione	App SO
		Modifica	App SO
		Creazione	App SO
		Attivazione	App SO
		Accesso	App SO
	Utente	Creazione	ID Aut Param Priv
		Modifica	ID Aut Param Priv
		Eliminazione	ID Aut Param Priv
		Accesso	Guest Radice Altro
	Gruppo	Creazione	Membro Gruppo
		Modifica	Membro Gruppo
		Eliminazione	Membro Gruppo
	Sistema	Informazioni	
		Memoria	
		Debug	
	Anomoly		
	Web	Accesso	
		Overflow del buffer	
		Backdoor	
		Brute_Force	
		DoS	
	E-mail	Accesso	
		Overflow del buffer	
		Backdoor	
		Brute_Force	
		DoS	
	Protocollo	IP	

Azione – Livello 1 (e.rv50)	Sistema – Livello 2 (e.rv51)	Dettaglio – Livello 3 (e.rv52)	Risultati – Livello 4 (e.rv53)
		TCP	
		UDP	
		ICMP	
		HTTP	
		Route	
		Talk	
		XFS	
		SSH	
		IGMP	
		Ora	
		News	
		Windows	
		RIP	
		IDS	
		SNMP	
		BGP	

Output di correlazione

La struttura di output del motore di correlazione consente di ordinare, filtrare ed eseguire rapporti sui dati generati come parte di una regola watchlist o di correlazione.

Struttura di output delle regole di correlazione

I valori di output di default sono i seguenti:

- RES impostato su "Correlazione" a meno che non viene impostato dall'utente
- SubRes impostato su "<regola>.<nomeregola> a meno che non viene impostato dall'utente
- Sev impostato su 4 a meno che non viene impostato dall'utente
- ST (tipo sensore - C)
- EI (schema regola - SIP='1.2.3.4.' quindi punto e virgola e soglia regola in formato 3-2-m (totale di 3 in 2 minuti, ad esempio)
- RT2 (nome regola)

Parametri script trasferiti

I parametri script trasferiti interessano sia le regole watchlist che le regole di correlazione. I parametri script vengono specificati nella casella di input Esegui azione della scheda Criteri di attivazione nel formato %xyz%, laddove xyz rappresenta il nome del parametro. I nomi dei parametri che rappresentano i tag META possono essere sia nomi brevi (ad esempio sip) sia nomi lunghi (ad esempio SourceIP). I nomi dei parametri prevedono la distinzione tra maiuscole e minuscole.

Parametri

I primi 11 parametri sono parametri speciali. Non si tratta di tag META e corrispondono a eventi correlati. I parametri da 12 a 47 sono parametri di tag META.

1. `%RuleName%` - Nome della regola attivata (il formato è regola.nomeregola).
2. `%RuleType%` - Tipo di regola attivata. C indica correlazione. W indica watchlist.
3. `%RuleDescription%` - Descrizione immessa alla creazione della regola.
4. `%RuleSeverity%` - Gravità della regola attivata.
5. `%RuleResource%` - Nome della risorsa della regola attivata.
6. `%RuleSubResource%` - Nome della sottorisorsa della regola attivata.
7. `%RuleLg%` - Regola nel linguaggio per le regole (RuleLg) del motore di correlazione.
8. `%RuleCount%` - Numero della regola attivata.
9. `%RuleDuration%` - Durata (in secondi) della regola attivata.
10. `%RulePattern%` - Elenco di tutti i tag nel linguaggio per le regole e del valore dei tag assunto dall'ultimo evento che ha attivato la regola. Il formato è tsn1='value1='value2'tsn3='value3', laddove:
    - tns1 rappresenta il nome breve del tag 1
    - tns2 rappresenta il nome breve del tag 2

    Ad esempio:

    ```
    sip='192.168.0.3'dip='2.168.0.2'
    ```
11. `%CorrelatedEventID%` - Identificatore dell'evento correlato generato dalla regola attivata.
12. %MessageText% - Testo del messaggio della regola attivata.
13. %EventName% - Nome dell'evento della regola attivata.

I tag restanti corrispondono al campo dell'ultimo evento che ha attivato l'evento correlato.

14. %sev% - Severity (gravità): gravità normalizzata dell'evento (0-5).
15. %vul% - Vulnerability (vulnerabilità): vulnerabilità della risorsa identificata nell'evento.
16. %crt% - Criticality (criticità): criticità della risorsa identificata nell'evento.
17. %dt% - DateTime (data/ora): data e ora normalizzate dell'evento, come indicate dal servizio di raccolta.
18. %sip% - SourceIP (IP di origine): indirizzo IP di origine da cui è originato l'evento.
19. %dip% - DestinationIP (IP di destinazione): indirizzo IP di destinazione a cui è destinato l'evento.
20. %id% - EventID (ID evento): identificatore univoco dell'evento.
21. %src% - SourceID (ID origine): identificatore univoco del processo di Sentinel che ha generato l'evento.
22. %port% - WizardPort (porta Wizard): descrizione della porta del servizio di raccolta di Sentinel.
23. %agent% - WizardCollector: descrizione della porta del servizio di raccolta di Sentinel.
24. %res% - Resource (risorsa): nome della risorsa.
25. %sres% - SubResource (sottorisorsa): nome della sottorisorsa.
26. %evt% - EventName (nome evento): nome descrittivo dell'evento, come riportato (o indicato) dal sensore. Esempio: "Scansione porte".

27. %sn% - SensorName (nome sensore): Nome del servizio di rilevamento definitivo dell'evento quando viene ricevuto in formato dati non elaborati. Esempio: "FW1" indica un firewall.
28. %st% - SensorType (tipo sensore): indicatore del tipo di sensore basato su un singolo carattere (N, H, O, V, C, W). H: basato sull'host, N: basato sulla rete, O: altro, V: Antivirus, C: correlazione e W: watchlist.
29. %et% - EventTime (ora evento): Ora normalizzata dell'evento, come indicato dal sensore; analizzata sintatticamente nel formato: Y-M-D-H:M:S~AMPM24~TZ.
30. %prot% - Protocol (protocollo): Protocollo di rete dell'evento.
31. %shn% - SourceHostName (nome host di origine): nome dell'host di origine da cui è originato l'evento.
32. %sp% - SourcePort (porta di origine): porta di origine da cui è originato l'evento.
33. %dhn% - DestinationHostName (nome host di destinazione): nome dell'host di destinazione a cui è destinato l'evento.
34. %dp% - DestinationPort (porta di destinazione): porta di destinazione a cui è destinato l'evento.
35. %sun% -1 SourceUserName (nome utente di origine): Nome dell'utente di origine utilizzato per avviare un evento. Esempio: "jdoe" durante un tentativo di "su".
36. %dun% - DestinationUserName (nome utente di destinazione): Nome dell'utente di destinazione su cui è stata tentata l'azione. Esempio: i tentativi eseguiti per reimpostare la password della radice.
37. %fn% - FileName: Nome del programma eseguito o del file aperto, modificato o interessato. Esempio: il nome di un file infetto da virus o un programma rilevato da un IDS.
38. %ei% - ExtendedInformation (informazioni estese): Memorizza ulteriori informazioni raccolte dal servizio di raccolta. I valori all'interno di questa variabile sono separati da punti e virgola (;). Esempio: un dominio per ID o nomi file.
39. %rn% - ReporterName (nome rapporto): nome host o indirizzo IP del dispositivo in cui viene registrato un evento o da cui viene inviata una notifica dell'evento.
40. %pn% - ProductName (nome prodotto): Indica tipo, fornitore e nome di prodotto in codice del sensore da cui è stato generato l'evento. Esempio: Check Point FireWall=CPFW.
41. %msg% - Message (messaggio): messaggio in formato libero per l'evento.
42. %rt1% - Riservato da Novell all'espansione. Per l'uso con Advisor (stringa).
43. %rt2% - Riservato da Novell all'espansione (stringa).
44. %ct% - Riservato all'uso da parte dei clienti per dati specifici del cliente (stringa).
45. %ct2% - Riservato all'uso da parte dei clienti per dati specifici del cliente (stringa).
46. %rt3% - Riservato da Novell all'espansione (numerica).
47. %ct3% - Riservato all'uso da parte dei clienti per dati specifici del cliente (numerica).
48. Parametri da 46 a 145

    Da %rv1% a %rv100%

    Si tratta di tag META di variabili riservate per la rappresentazione di eventi correnti.
49. Parametri da 146 a 245

    Da %cv1% a %cv100%

    Si tratta di tag META di variabili del cliente per la rappresentazione di eventi correnti.

NOTA: Per ulteriori informazioni su comandi e parametri, vedere il capitolo 5, Tag META di Wizard e Sentinel nella Guida di riferimento per gli utenti e la sezione relativa alle regole di correlazione nel capitolo 9, Scheda Amministratore della Guida dell'utente.

Quando si utilizza il comando %all%:

- Se un valore di parametro è vuoto o null, il valore del parametro sarà E_NULL o <tag absent>. In questo modo, saranno sempre presenti 45 parametri indipendentemente dal fatto che alcuni campi sono vuoti.
- Quando si configura il motore di correlazione per l'avvio dello script dell'interfaccia HP OVO, è necessario specificare il nome dello script insieme al tag del parametro %all%:

  ```
  esec_ovo %all%
  ```

- Quando si configura il motore di correlazione per l'avvio dello script dell'interfaccia BMC, è necessario specificare il nome dello script insieme al tag del parametro %all%:

  ```
  bmc_interface.csh %all%
  ```

- Quando si configura il motore di correlazione per l'invio di un'e-mail, è necessario specificare il nome dello script dell'e-mail insieme al parametro %all% nonché l'oggetto (facoltativo) e l'indirizzo e-mail:

  ```
  email_interface.csh %all% <nome>@<nome dominio>
     "Oggetto"
  ```

- Tutti gli script e/o le applicazioni che il motore di correlazione può eseguire devono trovarsi nella directory $ESEC_HOME/sentinel/exec (UNIX) %ESEC_HOME%\sentinel\bin (Windows).
- Per default, il motore di correlazione NON passerà alcun parametro agli script in esecuzione. Se si desidera che agli script vengano passati tutti i parametri, è necessario utilizzare i %tag% sopra riportati.
- Quando si specificano i parametri per uno script, è possibile raggrupparli mediante l'utilizzo di virgolette doppie. Di seguito sono riportati alcuni esempi:

  ```
  %sip% %dip% - (trattati come due parametri)

  "%sip% %dip%" – (trattati come un parametro)

  "Hello World" %sip% - (trattati come due
     parametri)

  "The message is %msg%" – (trattati come un
     parametro)

  %msg% - (trattato come un parametro, anche se
     il messaggio di sostituzione contiene spazi)

  "%msg%" – (tratto come un parametro, anche se il
     messaggio di sostituzione contiene spazi)
  ```

8 Opzioni della riga di comando del motore di correlazione di Sentinel

NOTA: Il termine agente è equivalente a servizio di raccolta. Si farà in seguito riferimento agli agenti come servizi di raccolta.

Le opzioni della riga di comando devono essere utilizzate dagli utenti avanzati. Gli utenti meno esperti non devono apportare modifiche basate sull'utilizzo di queste opzioni. Per accedere alle opzioni della riga di comando, passare a:

Per UNIX:

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

Per Windows

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

Per eseguire l'opzione della riga di comando, immettere:

```
correlation_engine <opzione della riga di comando di correlazione>
```

Opzione della riga di comando del motore di correlazione	**Descrizione**
-debug	Modalità di debug (stampa delle informazioni estese sul debug)
-noErrorLogging	Disabilita la registrazione degli errori nel registro eventi di Windows.
-ruleFile <file>	Specifica il file di testo che contiene le regole che devono essere elaborate dall'istanza del Motore di correlazione
-xmlruleFile <file>	Specifica il file delle configurazioni xml in cui memorizzare una copia locale delle regole contenute nel database. Valore di default: startup_correlation_rules.xml
-inputChannel <stringa>	Specifica il canale di input del livello di comunicazione per il Motore di correlazione. Valore di default: ewizard_binary_event
-outputChannel <stringa>	Specifica il canale di output del livello di comunicazione per il Motore di correlazione. Valore di default: correlation_binary_event.

Opzione della riga di comando del motore di correlazione	Descrizione
-outputUpdateChannel <stringa>	Specifica il canale di aggiornamento di output del livello di comunicazione per il Motore di correlazione. Valore di default: correlation_binary_event_update
-outputExecuteChannel <stringa>	Specifica il canale di esecuzione di output del livello di comunicazione per il Motore di correlazione. Valore di default: execute
-outputIncidentChannel <stringa>	Specifica il canale del caso di output del livello di comunicazione per il Motore di correlazione. Default: app_incident_req
-service <stringa>	Specifica il servizio di comunicazione (parametro di configurazione) per il Motore di correlazione. Valore di default: correlation_engine
-mgmtInputChannel <stringa>	Specifica il canale di input di gestione del livello di comunicazione per il Motore di correlazione. Valore di default: correlation_mgmt_input_channel
-mgmtOutputChannel <stringa>	Specifica il canale di output di gestione del livello di comunicazione per il Motore di correlazione. Valore di default: correlation_mgmt_output_channel
-mgmtService <stringa>	Specifica il servizio di gestione delle comunicazioni (parametro di configurazione) per il Motore di correlazione. Valore di default: correlation_engine_mgmt
-configurationFile <file>	Specifica il file che sovrascrive i parametri di avvio di default della configurazione del Motore di correlazione. Valore di default: ± 30 secondi rispetto all'ora del server Sentinel.
-noStartupRules	Imposta il motore di correlazione da eseguire senza il recupero delle regole memorizzate nel database. L'opzione -ruleFile ignora inoltre il recupero del database.
-dbTimeout <timeout in millisecondi>	Imposta il valore di timeout per il recupero delle regole memorizzate nel database. Valore di default: 5000 millisecondi.
-dbRetries <numero>	Imposta il numero di tentativi per contare il database. Valore di default: 6
-name <nome motore>	Imposta il nome del reporter del motore di correlazione. Valore di default: Motore di correlazione.
-affinityOneProcessor	Imposta l'esecuzione del motore di correlazione solo in un processore.
-useEventTime	Serve a scopo di test e non deve essere utilizzata.
-useNullOutput	Serve a scopo di test e non deve essere utilizzata.

Opzione della riga di comando del motore di correlazione	Descrizione
-logFile <nomefile>	Indirizza lo stato di un file.
-logPeriod <secondi>	Controlla la frequenza di scrittura dello stato nel file.
-version	Visualizza la versione della build ed esce.
-help	Visualizza la guida ed esce.

9 Servizio DAS (Data Access Service) di Sentinel

NOTA: Il termine agente è equivalente a servizio di raccolta. Si farà in seguito riferimento agli agenti come servizi di raccolta.

Il processo DAS (Data Access Service) è il servizio di persistenza del server Sentinel e fornisce un'interfaccia MOM (bus messaggi) al database. Garantisce l'accesso basato su dati al database backend. Riceve la richiesta XML dai diversi processi Sentinel, la converte in un'interrogazione sul database, elabora il risultato prodotto dal database e lo converte in una risposta XML. Supporta richieste di recupero di eventi per l'interrogazione rapida e il drill-down, di recupero di informazioni sulle vulnerabilità e su Advisor e di manipolazione delle informazioni di configurazione. DAS gestisce inoltre la registrazione di tutti gli eventi ricevuti da Gestione servizi di raccolta di Wizard e le richieste di recupero e memorizzazione delle informazioni di configurazione.

File container del servizio DAS

DAS è un container, composto da cinque processi differenti. Ogni processo è responsabile di differenti tipi di operazioni del database. Questi processi sono controllati dai file seguenti:

- das_binary.xml: utilizzato per gli eventi e le operazioni di inserimento di eventi correlati
- das_query.xml: tutte le altre operazioni di database
- das_aggregation.xml: utilizzato per le operazioni di aggregazione
- das_itrac.xml: utilizzato per l'esecuzione e la configurazione del servizio di attività e per la configurazione del servizio di workflow
- das_rt.xml: utilizzato per la configurazione della funzione Active Views all'interno della console di controllo di Sentinel

ATTENZIONE: Non modificare manualmente i file xml. Utilizzare l'utility dbconfig per modificare i valori all'interno dei file xml.

A ognuno di questi processi è associato un file di log che si trova in %ESEC_HOME%\Sentinel\log o $ESEC_HOME/Sentinel/log, ovvero:

- das_query0.*.log: tutti i log das_query
- das_binary0.*.log: tutti i log das_binary
- das_itrac0_*.log: log di attività e di workflow
- das_aggregation0.*.log: log di aggregazione
- das_rt0.*.log: log di Active Views

I file xml specificano:

- Gestore connessione
  - nome utente
  - password
  - nome host
  - numero porta
  - database (nome database)
  - server (oracle o mssql)
  - Connessioni massime
  - Dimensioni batch
  - Dimensioni carico

- Gestore invio — Specifica i canali nel bus messaggi che il servizio DAS deve ascoltare. Specifica inoltre la classe java da utilizzare per convertire le richieste xml in oggetti java e quale gestore inviare all'oggetto java per l'elaborazione del messaggio. Ad esempio: una richiesta di interrogazione evento viene convertita in un oggetto java mediante esecurity.cracker.QuickQueryRequestCracker. Il cracker lo invia quindi al gestore esecurity.event.request, il quale lo invia a uno dei servizi ai fini dell'elaborazione.
- Altri componenti che forniscono servizi DAS rilevanti.

Utilizzare l'utility dbconfig per la Riconfigurazione delle proprietà di connessione al database per Windows.

Riconfigurazione delle proprietà di connessione al database

La procedura deve essere eseguita per ognuno dei nomi di file container seguenti (containerFilename):

- das_binary.xml
- das_query.xml
- das_rt.xml
- das_aggregation.xml
- das_itrac.xml

Riconfigurazione delle proprietà di connessione al database per Windows

NOTA: A intervalli di 10 secondi, verrà eseguito il controllo del file delle proprietà di registrazione per verificare se sono state apportate modifiche dall'ultima visualizzazione. Se è il file è stato modificato, LogManagerRefreshService leggerà nuovamente il file delle proprietà di registrazione.

1. Eseguire il login come utente con diritti di amministrazione dove è installato il database.
2. Passare a:

   Per Windows:

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

   Per UNIX:

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

3. Immettere il comando seguente:

   ```
   dbconfig -n <nomeFilecontainer> [-u nome utente] [-p
      password] [-h nomehost] [-t numero porta] [-d
      database] [-s server(mssql oppure oracle)] [-help]
      [-versione]
   ```

File di configurazione del servizio DAS

I file seguenti sono utilizzati per configurare la registrazione del processo DAS:

- das_query_log.prop
- das_binary_log.prop
- das_rt_log.prop

- das_itrac_log.prop
- das_aggregation_log.prop

I file si trovano:

Per Windows:

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

Per UNIX:

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

In questi file sono contenute le informazioni di configurazione per il gestore della console, che stampa i messaggi in un output standard e per il gestore dei file, che stampa i messaggi in un file. La configurazione di ogni gestore consente di specificare le opzioni disponibili per ognuno di loro. I file consentono di specificare la configurazione dei messaggi di registrazione che dovrebbero essere stampati. I livelli disponibili sono:

- DISATTIVO: disattiva tutte le registrazioni
- GRAVE (valore più alto): indicazione di un errore di un componente o di una perdita/danneggiamento di dati critici
- AVVISO: un'azione potrebbe indurre in futuro un errore di esecuzione di un componente o si è verificata una perdita/un danneggiamento di dati non critici
- INFO: informazioni sulle revisioni
- CONFIG
- FINE: per l'esecuzione del debug
- PIÙ FINE: per l'esecuzione del debug
- FINISSIMO (valore più basso): per l'esecuzione del debug
- TUTTI: verranno registrati tutti i livelli di log

Quando si specifica un livello di registrazione, saranno registrati tutti i messaggi di log del livello e del livello superiore (come indicati nel precedente elenco). Ad esempio, se si specifica il livello INFO, saranno registrati tutti i messaggi di livello INFO, AVVISO e GRAVE.

Se si apportano modifiche ai file, è necessario riavviare il servizio DAS per renderle effettive.

La registrazione viene scritta in:

Per 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
```

Per 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
```

Il carattere * indica il numero univoco per risolvere i conflitti e il numero di generazione per distinguere i log sottoposti a rotazione. Ad esempio, das_query0.0.log è il log con file di indice 0 (primo) in una serie di file di log sottoposti a rotazione per il processo DAS.

Connettori del database nativi per l'inserimento di eventi

I connettori del database nativi garantiscono migliori prestazioni per l'inserimento di eventi. Il connettore da utilizzare dipende dalla piattaforma del database in uso.

Connettore del database nativo MS SQL

Utilizzare l'archivio degli eventi nativi ADO.Net.

Configurazione del connettore nativo MS SQL

1. Nel computer in cui è installato DAS, installare il framework .Net.
2. Nel file das_binary.xml, modificare la proprietà "insert.strategy" di EventStoreService > Persistore in:

```
esecurity.ccs.comp.event.jdbc.ADOLoadStrategy
```

Connettore del database nativo Oracle

Utilizzare l'archivio degli eventi nativi OCI. Sul computer del servizio DAS deve essere installato il client Oracle.

Configurazione del connettore nativo Oracle

1. Creare un file ".profile" nella home directory di esecadm. Inserirvi il teso seguente (modificare ORACLE_HOME in modo che sia conforme all'installazione in uso):

```
ORACLE_HOME=/build/home/oracle/OraHome
export ORACLE_HOME
LD_LIBRARY_PATH=$LD_LIBRARY_PATH:$ORACLE_HOME/lib
export LD_LIBRARY_PATH
```

2. Nel file das_binary.xml, modificare la proprietà "insert.strategy" di EventStoreService > Persistore in:

```
esecurity.ccs.comp.event.jdbc.OCILoadStrategy
```

10 Modifiche delle password utente di default

NOTA: Il termine agente è equivalente a servizio di raccolta. Si farà in seguito riferimento agli agenti come servizi di raccolta.

In questo capitolo viene descritto come modificare le password per gli utenti di default di Sentinel:

Autenticazione di Oracle e MS SQL:

- esecadm
- esecapp
- esecdba
- esecrpt

Autenticazione di Windows:

- Amministratore Sentinel
- Utente DB dell'applicazione Sentinel
- Amministratore DB Sentinel
- Utente rapporto Sentinel

Modifica delle password utente di default per l'autenticazione di Oracle e MS SQL

NOTA: Per modificare le password, è necessario disporre dei diritti di amministrazione.

Modifica della password di esecadm

Modifica della password di esecadm

1. Eseguire il login alla console di controllo Sentinel e fare clic sulla scheda Amministratore.
2. Aprire la finestra Gestione utenti.
3. Fare doppio clic sul conto utente esecadm oppure fare clic con il pulsante destro del mouse e scegliere Dettagli utente.
4. Modificare la password del conto.
5. Fare clic su *OK*.

Modifica della password di esecapp

Modifica della password di esecapp

1. Per MS SQL, utilizzare MS SQL Enterprise Manager e modificare la password di esecapp.
2. Per Oracle, utilizzare Oracle Enterprise Manager e modificare la password di esecapp.
3. Mediante l'utility dbconfig, aggiornare tutti i file xml container. Questa operazione è necessaria perché questi file xml memorizzano la password esecapp (cifrata) per consentire a DAS e Advisor la connessione al database.
   - das_binary.xml
   - das_query.xml
   - activity_container.xml
   - workflow_container.xml
   - das_rt.xml

I file xml container si trovano:

Per Windows:

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

Per Oracle:

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

Per ulteriori informazioni sull'uso dell'utility dbconfig, vedere il capitolo 9 - Servizio DAS (Data Access Service) di Sentinel della Guida di riferimento di Sentinel.

```
dbconfig –a <containerDirectory> -p <password>
```

Modifica della password di esecdba

Modifica della password di esecdba

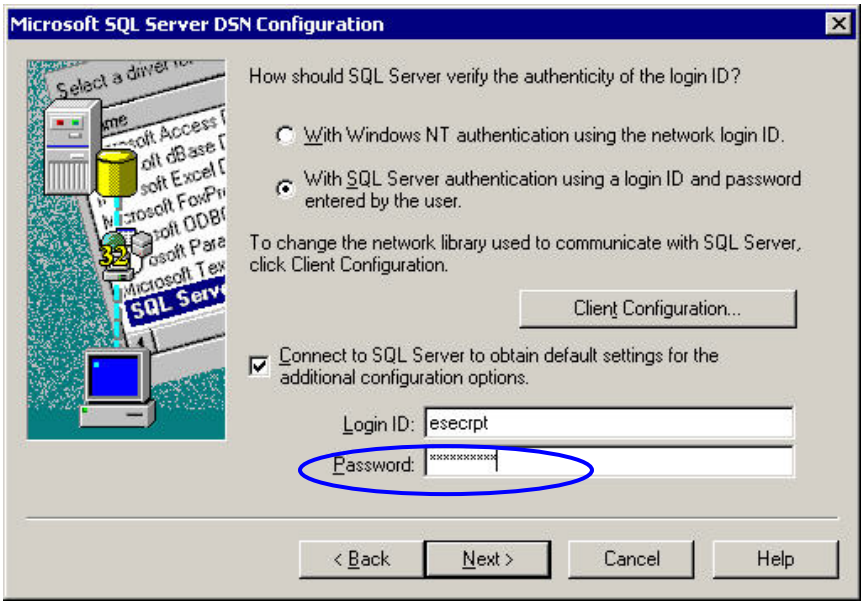
1. Per MS SQL, utilizzare MS SQL Enterprise Manager e modificare la password di esecdba.
2. Per Oracle, utilizzare Oracle Enterprise Manager e modificare la password di esecdba.
3. Perché i task automatici di SDM continuino a funzionare (ad esempio aggiunta di partizioni, archiviazione di partizioni) aggiornare dbPass nel file sdm.connect con la nuova password esecdba mediante l'interfaccia grafica utente di SDM o la riga di comando. Per ulteriori informazioni, vedere il capitolo 10 – Gestione dati Sentinel della Guida dell'utente di Sentinel.

```
sdm -action saveConnection -server <oracle/mssql> -
   host <IPHost/nomeHost> -port <numPorta> -database
   <nomeDatabase/SID> [-driverProps <fileProprietà>]
   {-user <utenteDb> -password <passDb>} -connectFile
   <nomefileSalvataggioConnessione>
```

Modifica della password di esecrpt

Modifica della password di esecdba

1. Per il database di MS SQL Sentinel, utilizzare MS SQL Enterprise Manager e modificare la password di esecrpt.
2. Per il database di Oracle Sentinel, utilizzare Oracle Enterprise Manager e modificare la password di esecrpt.
3. Per Crystal Server per Sentinel MS SQL, se applicabile, nel computer Crystal Server aggiornare il DSN di ODBC *(Pannello di controllo > Strumenti di amministrazione > Origine dati (ODBC)*).
   a. Nella scheda DSN di sistema evidenziare sentineldb e fare clic su *Configura*.
   b. Fare clic su *Avanti*. Aggiornare la password.
   c. Fare clic su *Avanti* fino a quando viene visualizzato il pulsante Fine. Fare clic su Fine.



4. Per Crystal Server per Oracle Sentinel non sono necessarie modifiche.

Modifica delle password utente di default per l'autenticazione di Windows

Modifica della password dell'Amministratore Sentinel

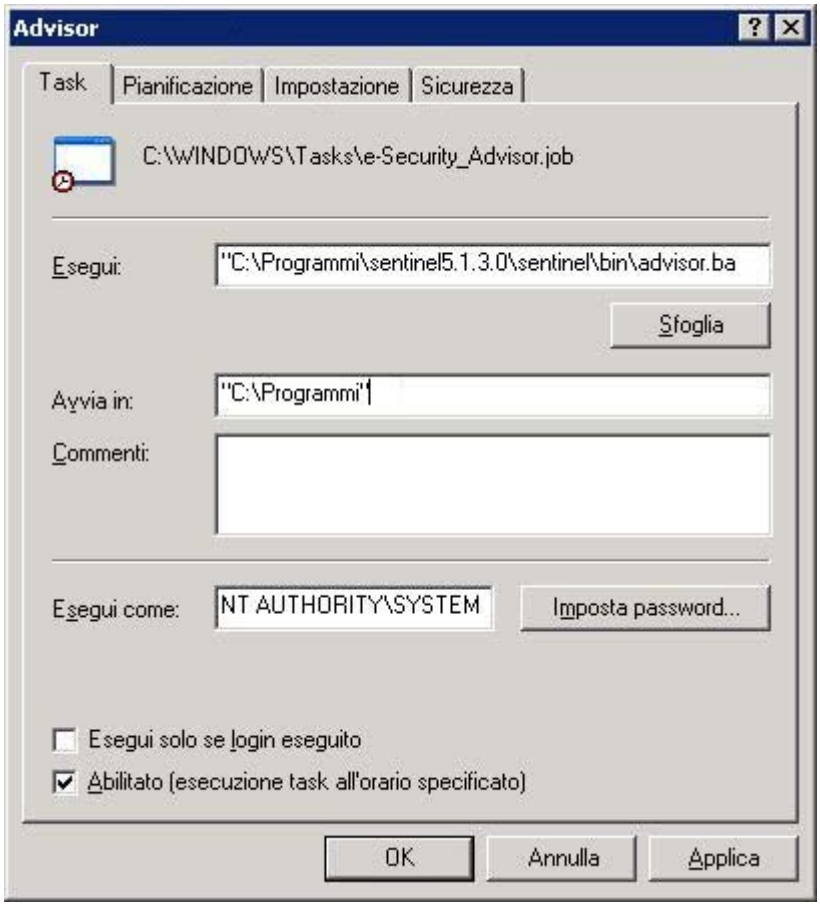
Modifica della password dell'Amministratore Sentinel

1. Utilizzare il sistema operativo Windows per modificare la password.

Modifica della password dell'Amministratore DB Sentinel

Modifica della password dell'Amministratore DB Sentinel

1. Utilizzare il sistema operativo Windows per modificare la password.
2. Se si stanno eseguendo task di Gestione dati Sentinel pianificati (ad esempio per l'aggiunta o l'archiviazione di partizioni), sarà necessario aggiornare la proprietà "Esegui come" *(Pannello di controllo > Operazioni pianificate > fare clic con il pulsante destro del mouse su Proprietà).*

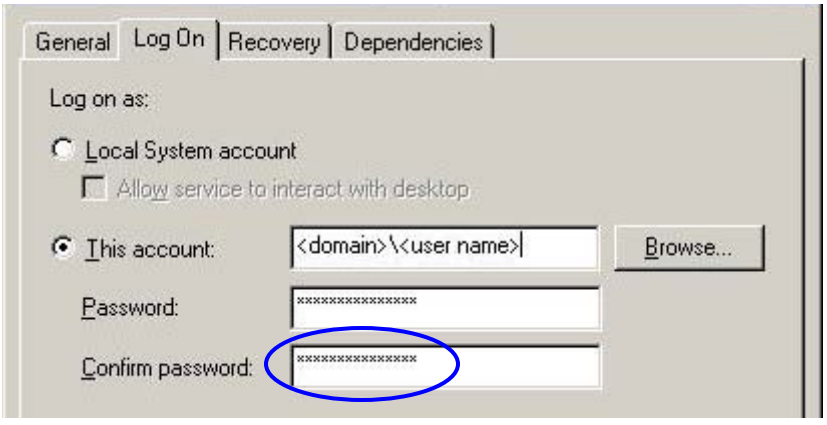


3. Fare clic su Imposta *password*. Immettere la nuova password due volte e fare clic su *OK*. Fare clic su *Applica* e quindi su *OK*.

Modifica della password dell'Amministratore DB applicazione Sentinel

Modifica della password dell'Amministratore DB applicazione Sentinel

1. Utilizzare il sistema operativo Windows per modificare la password.
2. Nel computer DAS avviare i Servizi di Windows *(Pannello di controllo > Strumenti di amministrazione > Servizi)*.
3. Fare clic con il pulsante destro del mouse su *Sentinel* quindi scegliere *Proprietà*. Fare clic sulla *scheda Logon* e aggiornare la password. Fare clic su *Applica* e quindi su *OK*.



4. Se si è installato Advisor, sarà necessario aggiornare la proprietà "Esegui come" *(Pannello di controllo > Operazioni pianificate > fare clic con il pulsante destro del mouse su Proprietà)* dei task pianificati di Advisor.
5. Fare clic su *Imposta password*. Immettere la nuova password due volte e quindi su *OK*. Fare clic su *Applica* e quindi su *OK*.

Modifica della password dell'Utente rapporto Sentinel

Modifica della password dell'Utente rapporto Sentinel

1. Utilizzare il sistema operativo Windows per modificare la password.

11 Viste database di Sentinel per Oracle

NOTA: Il termine agente è equivalente a servizio di raccolta. Si farà in seguito riferimento agli agenti come servizi di raccolta.

In questo capitolo sono riportate le viste dello schema di Sentinel per Oracle. Le viste forniscono informazioni per lo sviluppo di rapporti personalizzati (Crystal Reports).

Viste

ADV_ALERT_CVE_RPT_V

La vista fa riferimento alla tabella ADV_ALERT_CVE in cui è memorizzato il numero di identificazione dell'avviso di Advisor.

Nome colonna	Tipo di dati	Commento
ALERT_ID	di tipo numerico	Identificatore di annotazione – numero di sequenza
CVE	varchar2	
DATE_CREATED	data	Data di inserimento
DATE_MODIFIED	data	Data dell'ultimo aggiornamento
CREATED_BY	di tipo numerico	ID utente
MODIFIED_BY	di tipo numerico	ID utente

ADV_ALERT_PRODUCT_RPT_V

La vista fa riferimento alla tabella ADV_ALERT_PRODUCT in cui sono memorizzate le informazioni sul prodotto di Advisor, come il numero ID del Service Pack, la versione e la data di creazione.

Nome colonna	Tipo di dati	Commento
ALERT_ID	di tipo numerico	Identificatore di annotazione – numero di sequenza
SERVICE_PACK_ID	di tipo numerico	
VENDOR	varchar2	
PRODUCT	varchar2	
VERSION	varchar2	Contiene il numero di versione
SERVICE_PACK	varchar2	
PRIMARY_FLAG	di tipo numerico	
DATE_CREATED	data	Data di inserimento

Nome colonna	Tipo di dati	Commento
DATE_MODIFIED	data	Data dell'ultimo aggiornamento
CREATED_BY	di tipo numerico	ID utente
MODIFIED_BY	di tipo numerico	ID utente

ADV_ALERT_RPT_V

La vista fa riferimento alla tabella ADV_ALERT_PRODUCT in cui sono memorizzate le informazioni sull'avviso di Advisor, come il nome, il tipo di rischio e la data di pubblicazione.

Nome colonna	Tipo di dati	Commento
ALERT_ID	di tipo numerico	Identificatore di annotazione – numero di sequenza
VERSION	di tipo numerico	Contiene il numero di versione
TEMPLATE_ID	di tipo numerico	
TEMPLATE_NAME	varchar2	
THREAT_CATEGORY_NAME	varchar2	
THREAT_TYPE_NAME	varchar2	
HEADLINE	clob	
FIRST_PUBLISHED	data	
LAST_PUBLISHED	data	
STATUS	varchar2	
URGENCY_ID	di tipo numerico	
CREDIBILITY_ID	di tipo numerico	
SEVERITY_ID	di tipo numerico	
SUMMARY	clob	
LEGAL_DISCLAIMER	clob	
COPYRIGHT	varchar2	
BEGIN_EFFECTIVE_DATE	data	
END_EFFECTIVE_DATE	data	
DATE_CREATED	data	Data di inserimento
DATE_MODIFIED	data	Data dell'ultimo aggiornamento
CREATED_BY	di tipo numerico	ID utente
MODIFIED_BY	di tipo numerico	ID utente

ADV_ATTACK_ALERT_RPT_V

La vista fa riferimento alla tabella ADV_ATTACK_ALERT in cui sono memorizzate le informazioni sull'attacco di Advisor, come il nome, il tipo di rischio e la data di pubblicazione.

Nome colonna	Tipo di dati	Commento
ATTACK_ID	di tipo numerico	
ALERT_ID	di tipo numerico	
DATE_CREATED	data	Data di inserimento
DATE_MODIFIED	data	Data dell'ultimo aggiornamento
CREATED_BY	di tipo numerico	ID utente
MODIFIED_BY	di tipo numerico	ID utente

ADV_ATTACK_CVE_RPT_V

La vista fa riferimento alla tabella ADV_ATTACK_CVE in cui sono memorizzate le informazioni CVE di Advisor.

Nome colonna	Tipo di dati	Commento
ATTACK_ID	di tipo numerico	
CVE	varchar2	
DATE_CREATED	data	Data di inserimento
DATE_MODIFIED	data	Data dell'ultimo aggiornamento
CREATED_BY	di tipo numerico	ID utente
MODIFIED_BY	di tipo numerico	ID utente

ADV_ATTACK_MAP_RPT_V

La vista fa riferimento alla tabella ADV_ATTACK_MAP in cui sono memorizzate le informazioni di mappatura di Advisor.

Nome colonna	Tipo di dati	Commento
ATTACK_KEY	di tipo numerico	
ATTACK_ID	di tipo numerico	
SERVICE_PACK_ID	di tipo numerico	
ATTACK_NAME	varchar2	
ATTACK_CODE	varchar2	
DATE_CREATED	data	Data di inserimento
DATE_MODIFIED	data	Data dell'ultimo aggiornamento
CREATED_BY	di tipo numerico	ID utente
MODIFIED_by	di tipo numerico	ID utente

ADV_ATTACK_PLUGIN_RPT_V

La vista fa riferimento alla tabella ADV_ATTACK_PLUGIN in cui sono memorizzate le informazioni sul plug-in di Advisor.

Nome colonna	Tipo di dati	Commento
PLUGIN_KEY	di tipo numerico	
ATTACK_ID	di tipo numerico	
SERVICE_PACK_ID	di tipo numerico	
PLUGIN_ID	varchar2	
PLUGIN_NAME	varchar2	
DATE_CREATED	data	Data di inserimento
DATE_MODIFIED	data	Data dell'ultimo aggiornamento
CREATED_BY	di tipo numerico	ID utente
MODIFIED_BY	di tipo numerico	ID utente

ADV_ATTACK_RPT_V

La vista fa riferimento alla tabella ADV_ATTACK in cui sono memorizzate le informazioni sull'attacco di Advisor.

Nome colonna	Tipo di dati	Commento
ALERT_ID	di tipo numerico	
TRUSECURE_ATTACK_NAME	di tipo numerico	
FEED_DATE_CREATED	data	
FEED_DATE_UPDATED	data	
ATTACK_CATEGORY	varchar2	
URGENCY_ID	di tipo numerico	
SEVERITY_ID	di tipo numerico	
LOCAL	di tipo numerico	
REMOTE	di tipo numerico	
BEGIN_EFFECTIVE_DATE	data	
END_EFFECTIVE_DATE	data	
DESCRIPTION	clob	
SCENARIO	clob	
IMPACT	clob	
SAFEGUARDS	clob	
PATCHES	clob	
FALSE_POSITIVES	clob	
DATE_CREATED	data	Data di inserimento
DATE_MODIFIED	data	Data dell'ultimo aggiornamento
CREATED_BY	di tipo numerico	ID utente
MODIFIED_BY	di tipo numerico	ID utente

ADV_CREDIBILITY_RPT_V

La vista fa riferimento alla tabella ADV_CREDIBILITY in cui sono memorizzate le informazioni sulla credibilità di Advisor.

Nome colonna	Tipo di dati	Commento
CREDIBILITY_ID	di tipo numerico	
CREDIBILITY_RATING	varchar2	
CREDIBILITY_EXPLANATION	varchar2	
DATE_CREATED	data	Data di inserimento
DATE_MODIFIED	data	Data dell'ultimo aggiornamento
CREATED_BY	di tipo numerico	ID utente
MODIFIED_BY	di tipo numerico	ID utente

ADV_FEED_RPT_V

La vista fa riferimento alla tabella ADV_FEED in cui sono memorizzate le informazioni sul feed di Advisor, come il nome e la data.

Nome colonna	Tipo di dati	Commento
FEED_NAME	varchar2	
FEED_FILE	varchar2	
BEGIN_DATE	data	
END_DATE	data	
FEED_INSERT	di tipo numerico	

Nome colonna	Tipo di dati	Commento
FEED_UPDATE	di tipo numerico	
FEED_EXPIRE	di tipo numerico	

ADV_PRODUCT_RPT_V

La vista fa riferimento alla tabella ADV_PRODUCT in cui sono memorizzate le informazioni sul prodotto di Advisor, come il fornitore e l'ID.

Nome colonna	Tipo di dati	Commento
PRODUCT_ID	di tipo numerico	
VENDOR_ID	di tipo numerico	
PRODUCT_CATEGORY_ID	di tipo numerico	
PRODUCT_CATEGORY_NAME	varchar2	
PRODUCT_TYPE-ID	di tipo numerico	
PRODUCT_TYPE_NAME	varchar2	
PRODUCT_NAME	varchar2	
PRODUCT_DESCRIPTION	varchar2	
FEED_DATE_CREATED	data	
FEED_DATE_UPDATED	data	
ACTIVE_FLAG	di tipo numerico	
DATE_CREATED	data	Data di inserimento
DATE_MODIFIED	data	Data dell'ultimo aggiornamento
CREATED_BY	di tipo numerico	ID utente
MODIFIED_BY	di tipo numerico	ID utente

ADV_PRODUCT_SERVICE_PACK_RPT_V

La vista fa riferimento alla tabella ADV_PRODUCT_SERVICE _PACK in cui sono memorizzate le informazioni sul Service Pack di Advisor, come il nome, l'ID della versione e la data.

Nome colonna	Tipo di dati	Commento
SERVICE_PACK_ID	di tipo numerico	
VERSION_ID	di tipo numerico	Contiene il numero ID della versione
SERVICE_PACK_NAME	varchar2	
FEED_DATE_CREATED	data	
FEED_DATE_UPDATED	data	
ACTIVE_FLAG	di tipo numerico	
BEGIN_EFFECTIVE_DATE	data	
END_EFFECTIVE_DATE	data	
DATE_CREATED	data	Data di inserimento
DATE_MODIFIED	data	Data dell'ultimo aggiornamento
CREATED_BY	di tipo numerico	ID utente
MODIFIED_BY	di tipo numerico	ID utente

ADV_PRODUCT_VERSION_RPT_V

La vista fa riferimento alla tabella ADV_PRODUCT_VERSION in cui sono memorizzate le informazioni sul prodotto di Advisor, come il nome della versione e l'ID del prodotto e della versione.

Nome colonna	Tipo di dati	Commento
VERSION_ID	di tipo numerico	Contiene il numero ID della versione
PRODUCT_ID	di tipo numerico	
VERSION_NAME	varchar2	
FEED_DATE_CREATED	data	
FEED_DATE_UPDATED	data	
ACTIVE_FLAG	di tipo numerico	
DATE_CREATED	data	Data di inserimento
DATE_MODIFIED	di tipo numerico	Data dell'ultimo aggiornamento
CREATED_BY	di tipo numerico	ID utente
MODIFIED_BY	di tipo numerico	ID utente

ADV_SEVERITY_RPT_V

La vista fa riferimento alla tabella ADV_SEVERITY in cui sono memorizzate le informazioni di classificazione della gravità di Advisor.

Nome colonna	Tipo di dati	Commento
SEVERITY_ID	di tipo numerico	
SEVERITY_RATING	varchar2	
SEVERITY_EXPLANATION	varchar2	
DATE_CREATED	data	Data di inserimento
DATE_MODIFIED	data	Data dell'ultimo aggiornamento
CREATED_BY	di tipo numerico	ID utente
MODIFIED_BY	di tipo numerico	ID utente

ADV_SUBALERT_RPT_V

La vista fa riferimento alla tabella ADV_SUBALERT.

Nome colonna	Tipo di dati	Commento
ALERT_ID	di tipo numerico	
SUBALERT_ID	di tipo numerico	
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	
PATCHES_SOFTWARE	clob	

Nome colonna	Tipo di dati	Commento
ALERT_HISTORY	clob	
BACKGROUND_INFO	clob	
DATE_CREATED	data	Data di inserimento
DATE_MODIFIED	data	Data dell'ultimo aggiornamento
CREATED_BY	di tipo numerico	ID utente
MODIFIED_BY	di tipo numerico	ID utente

ADV_URGENCY_RPT_V

La vista fa riferimento alla tabella ADV_URGENCY.

Nome colonna	Tipo di dati	Commento
URGENCY_ID	di tipo numerico	
URGENCY_RATING	varchar2	
URGENCY_EXPLANATION	varchar2	
DATE_CREATED	data	Data di inserimento
DATE_MODIFIED	data	Data dell'ultimo aggiornamento
CREATED_BY	di tipo numerico	ID utente
MODIFIED_BY	di tipo numerico	ID utente

ADV_VENDOR_RPT_V

La vista fa riferimento alla tabella ADV_VENDOR in cui sono memorizzate le informazioni sull'indirizzo di Advisor.

Nome colonna	Tipo di dati	Commento
VENDOR_ID	di tipo numerico	
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	di tipo numerico	
DATE_CREATED	data	Data di inserimento
DATE_MODIFIED	data	Data dell'ultimo aggiornamento
CREATED_BY	di tipo numerico	ID utente
MODIFIED_BY	di tipo numerico	ID utente

ADV_VULN_PRODUCT_RPT_V

La vista fa riferimento alla tabella ADV_VULN_PRODUCT in cui sono memorizzate le informazioni sull'ID dell'attacco alla vulnerabilità e l'ID del Service Pack di Advisor.

Nome colonna	Tipo di dati	Commento
ATTACK_ID	di tipo numerico	
SERVICE_PACK_ID	di tipo numerico	
DATE_CREATED	data	Data di inserimento
DATE_MODIFIED	data	Data dell'ultimo aggiornamento
CREATED_BY	di tipo numerico	ID utente
MODIFIED_BY	di tipo numerico	ID utente

ANNOTATIONS_RPT_V

La visualizzazione fa riferimento alla tabella ANNOTAZIONI in cui sono memorizzate le note o la documentazione che è possibile associare a oggetti del sistema Sentinel quali i casi.

Nome colonna	Tipo di dati	Commento
ANN_ID	NUMBER	Identificatore di annotazione – numero di sequenza
TEXT	VARCHAR2(4000)	Documentazione o note
DATE_CREATED	DATE	Data di inserimento
DATE_MODIFIED	DATE	Data dell'ultimo aggiornamento
MODIFIED_BY	NUMBER	ID dell'utente che ha eseguito l'ultimo aggiornamento
CREATED_BY	NUMBER	ID dell'utente che ha eseguito l'inserimento
ACTION	Varchar2(255)	Azione

ASSET_CTGRY_RPT_V

La vista fa riferimento alla tabella ASSET_CTGRY in cui sono memorizzate informazioni sulle categorie di risorse, ad esempio hardware, software, sistema operativo, database e così via.

Nome colonna	Tipo di dati	Commento
ASSET_CATEGORY_ID	di tipo numerico	Identificatore della categoria della risorsa
ASSET_CATEGORY_NAME	varchar2(100)	Nome della categoria della risorsa
DATE_CREATED	data	Data di inserimento
DATE_MODIFIED	data	Data dell'ultimo aggiornamento
CREATED_BY	di tipo numerico	ID dell'utente che ha eseguito l'inserimento
MODIFIED_BY	di tipo numerico	ID dell'utente che ha eseguito l'ultimo aggiornamento

ASSET_HOSTNAME_RPT_V

La vista fa riferimento alla tabella ASSET_HOSTNAME in cui sono memorizzate informazioni sui nomi host alternativi delle risorse.

Nome colonna	Tipo di dati	Commento
ASSET_HOSTNAME_ID	Varchar2(36)	Identificatore del nome host alternativo della risorsa
PHYSICAL_ASSET_ID	varchar2(36)	Identificatore della risorsa fisica
HOST_NAME	Varchar2(255)	Nome host
CUSTOMER_ID	di tipo numerico	Identificatore del cliente
DATE_CREATED	data	Data dell'ultimo aggiornamento
DATE_MODIFIED	data	ID dell'utente che ha eseguito l'ultimo aggiornamento
CREATED_BY	di tipo numerico	ID dell'utente che ha eseguito l'inserimento
MODIFIED_BY	di tipo numerico	ID dell'utente che ha eseguito l'ultimo aggiornamento

ASSET_IP_RPT_V

La vista fa riferimento alla tabella ASSET_IP in cui sono memorizzate informazioni sugli indirizzi IP alternativi delle risorse.

Nome colonna	Tipo di dati	Commento
ASSET_IP_ID	Varchar2(36)	Identificatore dell'indirizzo IP alternativo della risorsa
PHYSICAL_ASSET_ID	varchar2(36)	Identificatore della risorsa fisica
IP_ADDRESS	di tipo numerico	Indirizzo IP della risorsa
CUSTOMER_ID	di tipo numerico	Identificatore del cliente
DATE_CREATED	data	Data di inserimento
DATE_MODIFIED	data	Data dell'ultimo aggiornamento
CREATED_BY	di tipo numerico	ID dell'utente che ha eseguito l'inserimento
MODIFIED_BY	di tipo numerico	ID dell'utente che ha eseguito l'ultimo aggiornamento

ASSET_LOCATION_RPT_V

La vista fa riferimento alla tabella ASSET_LOC in cui sono memorizzate informazioni sulle ubicazioni delle risorse.

Nome colonna	Tipo di dati	Commento
LOCATION_ID	di tipo numerico	Identificatore dell'ubicazione
CUSTOMER_ID	di tipo numerico	Identificatore del cliente
BUILDING_NAME	varchar2(255)	Nome dell'edificio
ADDRESS_LINE_1	varchar2(255)	Riga indirizzo 1
ADDRESS_LINE_2	varchar2(255)	Riga indirizzo 2
CITY	varchar2(100)	Città
STATE	varchar2(100)	Stato
COUNTRY	varchar2(100)	Paese
ZIP_CODE	varchar2(50)	CAP
DATE_CREATED	data	Data di inserimento
DATE_MODIFIED	data	Data dell'ultimo aggiornamento
CREATED_BY	di tipo numerico	ID dell'utente che ha eseguito l'inserimento
MODIFIED_BY	di tipo numerico	ID dell'utente che ha eseguito l'ultimo aggiornamento

ASSET_RPT_V

La vista fa riferimento alla tabella ASSET in cui sono memorizzate informazioni sulle risorse fisiche e software.

Nome colonna	Tipo di dati	Commento
ASSET_ID	varchar2(36)	Identificatore della risorsa
CUSTOMER_ID	di tipo numerico	Identificatore del cliente
ASSET_NAME	varchar2(255)	Nome della risorsa
PHYSICAL_ASSET_ID	varchar2(36)	Identificatore della risorsa fisica
PRDT_ID	di tipo numerico	Identificatore del prodotto
ASSET_CATEGORY_ID	di tipo numerico	Identificatore della categoria della risorsa
ENVIRONMENT_IDENTITY_CD	varchar2(5)	Codice di identificazione dell'ambiente
PHYSICAL_ASSET_IND	di tipo numerico(1)	Indicatore della risorsa fisica
ASSET_VALUE_CODE	varchar2(5)	Codice del valore della risorsa
CRITICALITY_CODE	varchar2(5)	Codice della criticità della risorsa
SENSITIVITY_CODE	varchar2(5)	Codice della riservatezza della risorsa
DATE_CREATED	data	Data di inserimento
DATE_MODIFIED	data	Data dell'ultimo aggiornamento
CREATED_BY	di tipo numerico	ID dell'utente che ha eseguito l'inserimento
MODIFIED_BY	di tipo numerico	ID dell'utente che ha eseguito l'ultimo aggiornamento

ASSET_VALUE_RPT_V

La vista fa riferimento alla tabella ASSET_VAL_LKUP in cui sono memorizzate informazioni sul valore delle risorse.

Nome colonna	Tipo di dati	Commento
ASSET_VALUE_CODE	varchar2(5)	Codice del valore della risorsa
ASSET_VALUE_NAME	varchar2(50)	Nome del valore della risorsa
DATE_CREATED	data	Data di inserimento
DATE_MODIFIED	data	Data dell'ultimo aggiornamento
CREATED_BY	di tipo numerico	ID dell'utente che ha eseguito l'inserimento
MODIFIED_BY	di tipo numerico	ID dell'utente che ha eseguito l'ultimo aggiornamento

ASSET_X_ENTITY_X_ROLE_RPT_V

La vista fa riferimento alla tabella ASSET_X_ENTITY_X_ROLE che associa una persona o un'organizzazione a una risorsa.

Nome colonna	Tipo di dati	Commento
PERSON_ID	varchar2(36)	Identificatore della persona
ORGANIZATION_ID	varchar2(36)	Identificatore dell'organizzazione
ROLE_CODE	varchar2(5)	Codice del ruolo

Nome colonna	Tipo di dati	Commento
ASSET_ID	varchar2(36)	Identificatore della risorsa
ENTITY_TYPE_CODE	varchar2(5)	Codice del tipo di entità
PERSON_ROLE_SEQUENCE	di tipo numerico	Ordine di persone con un particolare ruolo
DATE_CREATED	data	Data di inserimento
DATE_MODIFIED	data	Data dell'ultimo aggiornamento
CREATED_BY	di tipo numerico	ID dell'utente che ha eseguito l'inserimento
MODIFIED_BY	di tipo numerico	Utente che ha eseguito l'ultimo aggiornamento

ASSOCIATIONS_RPT_V

La vista fa riferimento alla tabella ASSOCIATIONS che associa utenti a casi, casi ad annotazioni e così via.

Nome colonna	Tipo di dati	Commento
TABLE1	VARCHAR2(64)	Nome tabella 1. Ad esempio, casi
ID1	VARCHAR2(36)	ID1. Ad esempio, ID caso.
TABLE2	VARCHAR2(64)	Nome tabella 2. Ad esempio, utenti
ID2	VARCHAR2(36)	ID2. Ad esempio ID utente.
DATE_CREATED	DATE	Data di inserimento.
DATE_MODIFIED	DATE	Data dell'ultimo aggiornamento
CREATED_BY	NUMBER	ID dell'utente che ha eseguito l'inserimento
MODIFIED_BY	NUMBER	ID dell'utente che ha eseguito l'ultimo aggiornamento

ATTACHMENTS_RPT_V

La vista fa riferimento alla tabella ATTACHMENTS in cui sono memorizzati dati sugli allegati.

Nome colonna	Tipo di dati	Commento
ATTACHMENT_ID	di tipo numerico	Identificatore dell'allegato
NAME	varchar2(255)	Nome dell'allegato
SOURCE_REFERENCE	varchar2(64)	Informazioni sull'origine
TYPE	varchar2(32)	Tipo di allegato
SUB_TYPE	varchar2(32)	Sottotipo di allegato
FILE_EXTENSION	varchar2(32)	Estensione file
ATTACHMENT_DESCRIPTION	varchar2(255)	Descrizione dell'allegato
DATA	clob	Dati dell'allegato
DATE_CREATED	data	Data di inserimento
DATE_MODIFIED	data	Data dell'ultimo aggiornamento
CREATED_BY	di tipo numerico	ID di chi ha eseguito l'inserimento
MODIFIED_BY	di tipo numerico	ID dell'utente che ha eseguito l'ultimo aggiornamento

CONFIGS_RPT_V

La vista fa riferimento alla tabella CONFIGS in cui sono memorizzate le informazioni di configurazione generali dell'applicazione.

Nome colonna	Tipo di dati	Commento
USR_ID	VARCHAR2(32)	Nome utente.
APPLICATION	VARCHAR2(255)	Identificatore dell'applicazione
UNIT	VARCHAR2(64)	Unità dell'applicazione
VALUE	VARCHAR2(255)	Valore testuale, se disponibile
DATA	CLOB	Dati XML
DATE_CREATED	DATE	Data di inserimento.
DATE_MODIFIED	DATE	Data dell'ultimo aggiornamento.
CREATED_BY	NUMBER	ID dell'utente che ha eseguito l'inserimento.
MODIFIED_BY	NUMBER	ID dell'utente che ha eseguito l'ultimo aggiornamento.

CONTACTS_RPT_V

La vista fa riferimento alla tabella CONTACTS in cui sono memorizzate informazioni sui contatti.

Nome colonna	Tipo di dati	Commento
CNT_ID	NUMBER	ID del contatto – numero di sequenza
FIRST_NAME	VARCHAR2(20)	Nome del contatto.
LAST_NAME	VARCHAR2(30)	Cognome del contatto.
TITLE	VARCHAR2(128)	Titolo del contatto
DEPARTMENT	VARCHAR2(128)	Reparto
PHONE	VARCHAR2(64)	Numero di telefono del contatto
EMAIL	VARCHAR2(255)	Indirizzo e-mail del contatto
PAGER	VARCHAR2(64)	Numero del cercapersone del contatto
CELL	VARCHAR2(64)	Numero del cellulare del contatto
DATE_CREATED	DATE	Data di inserimento
DATE_MODIFIED	DATE	Data dell'ultimo aggiornamento
CREATED_BY	NUMBER	ID dell'utente che ha eseguito l'inserimento
MODIFIED_BY	NUMBER	ID dell'utente che ha eseguito l'ultimo aggiornamento

CORRELATED_EVENTS_RPT_V

La vista fa riferimento alle tabelle CORRELATED_EVENTS_* in cui sono memorizzate informazioni sugli eventi correlati.

Nome colonna	Tipo di dati	Commento
PARENT_EVT_ID	varchar2	UUID (Event Universal Unique Identifier) dell'evento di livello superiore
CHILD_EVT_ID	varchar2	UUID (Event Universal Unique Identifier) dell'evento secondario
PARENT_EVT_TIME	DATE	Ora dell'evento di livello superiore
CHILD_EVT_TIME	DATE	Ora dell'evento secondario

Nome colonna	Tipo di dati	Commento
DATE_CREATED	DATE	Data di inserimento creata da DAS
DATE_MODIFIED	DATE	Data dell'ultimo aggiornamento
CREATED_BY	NUMBER	ID dell'utente che ha eseguito l'inserimento
MODIFIED_BY	NUMBER	ID dell'utente che ha eseguito l'ultimo aggiornamento

CORRELATED_EVENTS_RPT_V1

La vista contiene eventi correlati presenti e passati (importati da archivi).

Nome colonna	Tipo di dati	Commento
PARENT_EVT_ID	varchar2	UUID (Event Universal Unique Identifier) dell'evento di livello superiore
CHILD_EVT_ID	varchar2	UUID (Event Universal Unique Identifier) dell'evento secondario
PARENT_EVT_TIME	DATE	Ora dell'evento di livello superiore
CHILD_EVT_TIME	DATE	Ora dell'evento secondario
DATE_CREATED	DATE	Data di inserimento creata da DAS
DATE_MODIFIED	DATE	Data dell'ultimo aggiornamento
CREATED_BY	NUMBER	ID dell'utente che ha eseguito l'inserimento
MODIFIED_BY	NUMBER	ID dell'utente che ha eseguito l'ultimo aggiornamento

CRITICALITY_RPT_V

La vista fa riferimento alla tabella CRIT_LKUP in cui sono contenute informazioni sulla criticità delle risorse.

Nome colonna	Tipo di dati	Commento
CRITICALITY_CODE	varchar2(5)	Codice della criticità della risorsa
CRITICALITY_NAME	varchar2(50)	Nome della criticità della risorsa
DATE_CREATED	data	Data di inserimento
DATE_MODIFIED	data	Data dell'ultimo aggiornamento
CREATED_BY	di tipo numerico	ID utente
MODIFIED_BY	di tipo numerico	ID utente

CUST_RPT_V

La vista fa riferimento alla tabella CUST in cui sono memorizzate informazioni sui clienti per MSSP.

Nome colonna	Tipo di dati	Commento
CUSTOMER_ID	di tipo numerico	Identificatore del cliente
CUSTOMER_NAME	varchar2(255)	Nome del cliente
DATE_CREATED	data	Data di inserimento
DATE_MODIFIED	data	Data dell'ultimo aggiornamento
CREATED_BY	di tipo numerico	ID dell'utente che ha eseguito l'inserimento

Nome colonna	Tipo di dati	Commento
MODIFIED_BY	di tipo numerico	ID dell'utente che ha eseguito l'ultimo aggiornamento

ENTITY_TYPE_RPT_V

La vista fa riferimento alla tabella ENTITY_TYP in cui sono memorizzate informazioni sui tipi di entità (persona, organizzazione).

Nome colonna	Tipo di dati	Commento
ENTITY_TYPE_CODE	varchar2(5)	Codice del tipo di entità
ENTITY_TYPE_NAME	varchar2(50)	Nome del tipo di entità
DATE_CREATED	data	Data di inserimento
DATE_MODIFIED	data	Data dell'ultimo aggiornamento
CREATED_BY	di tipo numerico	ID dell'utente che ha eseguito l'inserimento.
MODIFIED_BY	di tipo numerico	ID dell'utente che ha eseguito l'ultimo aggiornamento

ENV_IDENTITY_RPT_V

La vista fa riferimento alla tabella ENV_IDENTITY_LKUP in cui sono memorizzate informazioni sull'identità dell'ambiente delle risorse.

Nome colonna	Tipo di dati	Commento
ENVIRONMENT_IDENTITY_CODE	varchar2(5)	Codice di identità dell'ambiente
ENVIRONMENT_IDENTITY_NAME	varchar2(255)	Nome dell'identità dell'ambiente
DATE_CREATED	data	Data di inserimento
DATE_MODIFIED	data	Data dell'ultimo aggiornamento
CREATED_BY	di tipo numerico	ID dell'utente che ha eseguito l'inserimento
MODIFIED_BY	di tipo numerico	ID dell'utente che ha eseguito l'ultimo aggiornamento

ESEC_DISPLAY_RPT_V

La vista fa riferimento alla tabella ESEC_DISPLAY in cui sono memorizzate le proprietà visualizzabili degli oggetti. Viene attualmente utilizzata per la ridenominazione dei tag META. Viene utilizzata con la configurazione eventi (rilevanza aziendale).

Nome colonna	Tipo di dati	Commento
DISPLAY_OBJECT	VARCHAR2(32)	Oggetto di livello superiore della proprietà
TAG	VARCHAR2(32)	Nome tag nativo della proprietà
LABEL	VARCHAR2(32)	Stringa visualizzata del tag.
POSITION	NUMBER	Posizione del tag nella visualizzazione.
WIDTH	NUMBER	Larghezza della colonna
ALIGNMENT	NUMBER	Allineamento orizzontale
FORMAT	NUMBER	Formattatore enumerato per la visualizzazione della proprietà
ENABLED	VARCHAR2(1)	Indica se il tag è visualizzato.

Nome colonna	Tipo di dati	Commento
TYPE	NUMBER	Indica il tipo di dati del tag. 1 = string 2 = ulong 3 = date 4 = uuid 5 = ipv4
DESCRIPTION	VARCHAR2(255)	Descrizione testuale del tag
DATE_CREATED	DATE	Data di inserimento.
DATE_MODIFIED	DATE	Data dell'ultimo aggiornamento.
CREATED_BY	NUMBER	ID dell'utente che ha eseguito l'inserimento.
MODIFIED_BY	NUMBER	ID dell'utente che ha eseguito l'ultimo aggiornamento.
REF_CONFIG	VARCHAR2(4000)	Configurazione dei dati di riferimento

ESEC_PORT_REFERENCE_RPT_V

La vista fa riferimento alla tabella ESEC_PORT_REFERENCE in cui sono memorizzati i numeri di porta assegnati in base a standard di settore.

Nome colonna	Tipo di dati	Commento
PORT_NUMBER	NUMBER	Per http://www.iana.org/assignments/port-numbers, rappresentazione numerica della porta. Questo numero di porta viene normalmente associato al livello del protocollo di trasporto nello stack TCP/IP.
PROTOCOL_NUMBER	NUMBER	Per http://www.iana.org/assignments/protocol-numbers, identificatori numerici utilizzati per rappresentare i protocolli incapsulati in un pacchetto IP.
PORT_KEYWORD	VARCHAR2(64)	Per http://www.iana.org/assignments/port-numbers, rappresentazione con parola chiave della porta.
PORT_DESCRIPTION	VARCHAR2(512)	Descrizione della porta.
DATE_CREATED	DATE	Data di inserimento.
DATE_MODIFIED	DATE	Data dell'ultimo aggiornamento.
CREATED_BY	NUMBER	ID dell'utente che ha eseguito l'inserimento.
MODIFIED_BY	NUMBER	ID dell'utente che ha eseguito l'ultimo aggiornamento.

ESEC_PROTOCOL_REFERENCE_RPT_V

La vista fa riferimento alla tabella ESEC_PROTOCOL_REFERENCE in cui sono memorizzati i numeri di protocollo assegnati in base a standard di settore.

Nome colonna	Tipo di dati	Commento
PROTOCOL_NUMBER	NUMBER	Per http://www.iana.org/assignments/protocol-numbers, identificatori numerici utilizzati per rappresentare i protocolli incapsulati in un pacchetto IP.
PROTOCOL_KEYWORD	VARCHAR2(64)	Per http://www.iana.org/assignments/protocol-numbers, parola chiave utilizzata per rappresentare i protocolli incapsulati in un pacchetto IP.
PROTOCOL_DESCRIPTION	VARCHAR2(512)	Descrizione del protocollo del pacchetto IP.
DATE_CREATED	DATE	Data di inserimento.
DATE_MODIFIED	DATE	Data dell'ultimo aggiornamento.
CREATED_BY	NUMBER	ID dell'utente che ha eseguito l'inserimento.
MODIFIED_BY	NUMBER	ID dell'utente che ha eseguito l'ultimo aggiornamento.

ESEC_SEQUENCE _RPT_V

La vista fa riferimento alla tabella ESEC_SEQUENCE, utilizzata per generare numeri di sequenza con chiave primaria per le tabelle di Sentinel.

Nome colonna	Tipo di dati	Commento
TABLE_NAME	VARCHAR2(32)	Nome della tabella.
COLUMN_NAME	VARCHAR2(32)	Nome della colonna
SEED	NUMBER	Valore corrente del campo chiave primaria.
DATE_CREATED	DATE	Data di inserimento.
DATE_MODIFIED	DATE	Data dell'ultimo aggiornamento.
CREATED_BY	NUMBER	ID dell'utente che ha eseguito l'inserimento.
MODIFIED_BY	NUMBER	ID dell'utente che ha eseguito l'ultimo aggiornamento.

EVENTS_ALL_RPT_V (fornita a scopo di compatibilità con versioni precedenti)

La vista contiene eventi presenti e passati (importati da archivi).

Nome colonna	Tipo di dati	Commento
EVENT_ID	varchar2	Identificatore dell'evento
RESOURCE_NAME	varchar2(255)	Nome della risorsa
SUB_RESOURCE	varchar2(255)	Nome della sottorisorsa
SEVERITY	di tipo numerico	Gravità dell'evento
EVENT_PARSE_TIME	data	Ora dell'evento
EVENT_DATE_TIME	data	Ora dell'evento
BASE_MESSAGE	varchar2(4000)	Messaggio base
EVENT_NAME	varchar2(255)	Nome dell'evento riportato dal sensore
EVENT_TIME	varchar2(255)	Ora dell'evento riportata dal sensore
SENSOR_NAME	varchar2(255)	Nome del sensore
SENSOR_TYPE	varchar2(5)	Tipo di sensore: H – basato sull'host N – basato sulla rete V – virus O – altro
PROTOCOL	varchar2(255)	Nome del protocollo
SOURCE-IP	di tipo numerico	Indirizzo IP di origine in formato numerico
SOURCE_HOST_NAME	varchar2(255)	Nome dell'host di origine
SOURCE_PORT	varchar2(32)	Porta di origine
DESTINATION_IP	di tipo numerico	Indirizzo IP di destinazione in formato numerico
DESTINATION_HOST_NAME	varchar2(255)	Nome dell'host di destinazione
DESTINATION_PORT	varchar2(32)	Porta di destinazione
SOURCE_USER_NAME	varchar2(255)	Nome dell'utente di origine
DESTINATION_USER_NAME	varchar2(255)	Nome dell'utente di destinazione
FILE_NAME	varchar2(1000)	Nome file
EXTENDED_INFO	varchar2(1000)	Informazioni estese
REPORT_NAME	varchar2(255)	Nome dell'autore del rapporto
PRODUCT_NAME	varchar2(255)	Nome del prodotto per la generazione di rapporti
CUSTOM_TAG_1	varchar2(255)	Tag cliente 1
CUSTOM_TAG_2	varchar2(255)	Tag cliente 2
CUSTOM_TAG_3	di tipo numerico	Tag cliente 3
RESERVED_TAG_1	VARCHAR2(255)	Tag riservato 1 Riservato all'uso futuro da parte di Novell. Questo campo viene utilizzato per le informazioni di Advisor relative alle descrizioni degli attacchi.
RESERVED_TAG_2	varchar2(255)	Riservato all'uso futuro da parte di Novell. L'uso di questo campo per qualsiasi altro scopo può causare la sovrascrittura dei dati da parte di funzionalità future.

Nome colonna	Tipo di dati	Commento
RESERVED_TAG_3	di tipo numerico	Riservato all'uso futuro da parte di Novell. L'uso di questo campo per qualsiasi altro scopo può causare la sovrascrittura dei dati da parte di funzionalità future.
SOURCE_UUID	varchar(36)	UUID di origine
PORT	varchar(64)	Porta del servizio di raccolta
AGENT	varchar2(64)	Nome servizio di raccolta
VULNERABILITY_RATING	di tipo numerico	Classificazione della vulnerabilità
CRITICALITY_RATING	di tipo numerico	Classificazione della criticità
DATE_CREATED	data	Data di inserimento
DATE_MODIFIED	data	Data dell'ultimo aggiornamento
CREATED_BY	di tipo numerico	ID utente
MODIFIED_BY	di tipo numerico	ID utente
RV01 - 10	NUMBER	Valore riservato 1 - 10 Riservato all'uso futuro da parte di Novell. L'uso di questo campo per qualsiasi altro scopo può causare la sovrascrittura dei dati da parte di funzionalità future.
RV11 - 20	DATE	Valore riservato 11 - 20 Riservato all'uso futuro da parte di Novell. L'uso di questo campo per qualsiasi altro scopo può causare la sovrascrittura dei dati da parte di funzionalità future.
RV21 - 25	varchar2	Valore riservato 21 - 25 Riservato all'uso futuro da parte di Novell per la memorizzazione di UUID. L'uso di questo campo per qualsiasi altro scopo può causare la sovrascrittura dei dati da parte di funzionalità future.
RV26 - 31	VARCHAR2(255)	Valore riservato 26 - 31 Riservato all'uso futuro da parte di Novell. L'uso di questo campo per qualsiasi altro scopo può causare la sovrascrittura dei dati da parte di funzionalità future.
RV32	VARCHAR2(255)	Valore riservato 32 Riservato a DeviceCategory L'uso di questo campo per qualsiasi altro scopo può causare la sovrascrittura dei dati da parte di funzionalità future.

Nome colonna	Tipo di dati	Commento
RV33	VARCHAR2(255)	Valore riservato 33 Riservato a EventContex L'uso di questo campo per qualsiasi altro scopo può causare la sovrascrittura dei dati da parte di funzionalità future.
RV34	VARCHAR2(255)	Valore riservato 34 Riservato a SourceThreatLevel L'uso di questo campo per qualsiasi altro scopo può causare la sovrascrittura dei dati da parte di funzionalità future.
RV35	VARCHAR2(255)	Valore riservato 35 Riservato a SourceUserContext. L'uso di questo campo per qualsiasi altro scopo può causare la sovrascrittura dei dati da parte di funzionalità future.
RV36	VARCHAR2(255)	Valore riservato 36 Riservato a DataContext. L'uso di questo campo per qualsiasi altro scopo può causare la sovrascrittura dei dati da parte di funzionalità future.
RV37	VARCHAR2(255)	Valore riservato 37 Riservato a SourceFunction. L'uso di questo campo per qualsiasi altro scopo può causare la sovrascrittura dei dati da parte di funzionalità future.
RV38	VARCHAR2(255)	Valore riservato 38 Riservato a SourceOperationalContext. L'uso di questo campo per qualsiasi altro scopo può causare la sovrascrittura dei dati da parte di funzionalità future.
RV39	VARCHAR2(255)	Valore riservato 39 Riservato a MSSPCustomerName. L'uso di questo campo per qualsiasi altro scopo può causare la sovrascrittura dei dati da parte di funzionalità future.

Nome colonna	Tipo di dati	Commento
RV40 - 43	VARCHAR2(255)	Valore riservato 40 - 43 Riservato all'uso futuro da parte di Novell. L'uso di questo campo per qualsiasi altro scopo può causare la sovrascrittura dei dati da parte di funzionalità future.
RV44	VARCHAR2(255)	Valore riservato 44 Riservato a DestinationThreatLevel. L'uso di questo campo per qualsiasi altro scopo può causare la sovrascrittura dei dati da parte di funzionalità future.
RV45	VARCHAR2(255)	Valore riservato 45 Riservato a DestinationUserContext. L'uso di questo campo per qualsiasi altro scopo può causare la sovrascrittura dei dati da parte di funzionalità future.
RV46	VARCHAR2(255)	Valore riservato 46 Riservato a VirusStatus. L'uso di questo campo per qualsiasi altro scopo può causare la sovrascrittura dei dati da parte di funzionalità future.
RV47	VARCHAR2(255)	Valore riservato 47 Riservato all'uso futuro da parte di Novell. L'uso di questo campo per qualsiasi altro scopo può causare la sovrascrittura dei dati da parte di funzionalità future.
RV48	VARCHAR2(255)	Valore riservato 48 Riservato a DestinationOperationalContext. L'uso di questo campo per qualsiasi altro scopo può causare la sovrascrittura dei dati da parte di funzionalità future.
RV49	VARCHAR2(255)	Valore riservato 49 Riservato all'uso futuro da parte di Novell. L'uso di questo campo per qualsiasi altro scopo può causare la sovrascrittura dei dati da parte di funzionalità future.
RV50	VARCHAR2(255)	Livello di tassonomia 1
RV51	VARCHAR2(255)	Livello di tassonomia 2
RV52	VARCHAR2(255)	Livello di tassonomia 3

Nome colonna	Tipo di dati	Commento
RV53	VARCHAR2(255)	Livello di tassonomia 4
CV01 - 10	NUMBER	Valore personalizzato 1 - 10 Riservato all'uso da parte del cliente, in genere per l'associazione di dati aziendali rilevanti
CV11 - 20	DATE	Valore personalizzato 11 - 20 Riservato all'uso da parte del cliente, in genere per l'associazione di dati aziendali rilevanti
CV21 - 100	VARCHAR2(255)	Valore personalizzato 21 – 100 Riservato all'uso da parte del cliente, in genere per l'associazione di dati aziendali rilevanti

EVENTS_ALL_RPT_V1 (fornita a scopo di compatibilità con versioni precedenti)

La vista contiene eventi correnti. Include le stesse colonne di EVENT_ALL_RPT_V.

EVENTS_RPT_V (fornita a scopo di compatibilità con versioni precedenti)

La vista contiene eventi presenti e passati. Include le stesse colonne di EVENT_ALL_RPT_V.

EVENTS_RPT_V1 (fornita a scopo di compatibilità con versioni precedenti)

La vista contiene eventi correnti. Include le stesse colonne di EVENT_ALL_RPT_V.

EVENTS_RPT_V2 (questa visualizzazione dovrebbe essere utilizzata da tutti i nuovi rapporti di Sentinel 5)

La vista contiene eventi presenti e passati.

Nome colonna	Tipo di dati	Commento
EVENT_ID	varchar2	Identificatore dell'evento
RESOURCE_NAME	varchar2(255)	Nome della risorsa
SUB_RESOURCE	varchar2(255)	Nome della sottorisorsa
SEVERITY	di tipo numerico	Gravità dell'evento
EVENT_PARSE_TIME	data	Ora dell'evento
EVENT_DATETIME	data	Ora dell'evento
BASE_MESSAGE	varchar2(4000)	Messaggio base
EVENT_NAME	varchar2(255)	Nome dell'evento riportato dal sensore

Nome colonna	Tipo di dati	Commento
EVENT_TIME	varchar2(255)	Ora dell'evento riportata dal sensore
TAXONOMY_ID	di tipo numerico	Identificatore della tassonomia
PROTOCOL_ID	di tipo numerico	Identificatore del prodotto
AGENT_ID	di tipo numerico	Identificatore del servizio di raccolta
SOURCE_IP	di tipo numerico	Indirizzo IP di origine in formato numerico
SOURCE_HOST_NAME	varchar2(255)	Nome dell'host di origine
SOURCE_PORT	varchar2(32)	Porta di origine
DESTINATION_IP	di tipo numerico	Indirizzo IP di destinazione in formato numerico
DESTINATION_HOST_NAME	varchar2(255)	Nome dell'host di destinazione
DESTINATION_PORT	varchar2(32)	Porta di destinazione
SOURCE_USER_NAME	varchar2(255)	Nome dell'utente di origine
DESTINATION_USER_NAME	varchar2(255)	Nome dell'utente di destinazione
FILE_NAME	varchar2(1000)	Nome file
EXTENDED_INFO	varchar2(1000)	Informazioni estese
CUSTOM_TAG_1	varchar2(255)	Tag cliente 1
CUSTOM_TAG 2	varchar2(255)	Tag cliente 2
CUSTOM_TAG 3	di tipo numerico	Tag cliente 3
RESERVED_TAG_1	VARCHAR2(255)	Tag riservato 1 Riservato all'uso futuro da parte di Novell. Questo campo viene utilizzato per le informazioni di Advisor relative alle descrizioni degli attacchi.
RESERVED_TAG_2	varchar2(255)	Riservato all'uso futuro da parte di Novell. L'uso di questo campo per qualsiasi altro scopo può causare la sovrascrittura dei dati da parte di funzionalità future.
RESERVED_TAG_3	di tipo numerico	Riservato all'uso futuro da parte di Novell. L'uso di questo campo per qualsiasi altro scopo può causare la sovrascrittura dei dati da parte di funzionalità future.
VULNERABILITY_RATING	di tipo numerico	Classificazione della vulnerabilità
CRITICALITY_RATING	di tipo numerico	Classificazione della criticità
DATE_CREATED	data	Data di inserimento
DATE_MODIFIED	data	Data dell'ultimo aggiornamento
CREATED_BY	di tipo numerico	ID dell'utente che ha eseguito l'inserimento.
MODIFIED_BY	di tipo numerico	ID dell'utente che ha eseguito l'ultimo aggiornamento.

Nome colonna	Tipo di dati	Commento
RV01 - 10	NUMBER	Valore riservato 1 - 10 Riservato all'uso futuro da parte di Novell. L'uso di questo campo per qualsiasi altro scopo può causare la sovrascrittura dei dati da parte di funzionalità future.
RV11 - 20	DATE	Valore riservato 1 - 31 Riservato all'uso futuro da parte di Novell. L'uso di questo campo per qualsiasi altro scopo può causare la sovrascrittura dei dati da parte di funzionalità future.
RV21 - 25	varchar2	Valore riservato 21 - 25 Riservato all'uso futuro da parte di Novell per la memorizzazione di UUID. L'uso di questo campo per qualsiasi altro scopo può causare la sovrascrittura dei dati da parte di funzionalità future.
RV26 - 31	VARCHAR2(255)	Valore riservato 26 - 31 Riservato all'uso futuro da parte di Novell. L'uso di questo campo per qualsiasi altro scopo può causare la sovrascrittura dei dati da parte di funzionalità future.
RV33	VARCHAR2(255)	Valore riservato 33 Riservato a EventContex L'uso di questo campo per qualsiasi altro scopo può causare la sovrascrittura dei dati da parte di funzionalità future.
RV34	VARCHAR2(255)	Valore riservato 34 Riservato a SourceThreatLevel L'uso di questo campo per qualsiasi altro scopo può causare la sovrascrittura dei dati da parte di funzionalità future.
RV35	VARCHAR2(255)	Valore riservato 35 Riservato a SourceUserContext. L'uso di questo campo per qualsiasi altro scopo può causare la sovrascrittura dei dati da parte di funzionalità future.
RV36	VARCHAR2(255)	Valore riservato 36 Riservato a DataContext. L'uso di questo campo per qualsiasi altro scopo può causare la sovrascrittura dei dati da parte di funzionalità future.

Nome colonna	Tipo di dati	Commento
RV37	VARCHAR2(255)	Valore riservato 37 Riservato a SourceFunction. L'uso di questo campo per qualsiasi altro scopo può causare la sovrascrittura dei dati da parte di funzionalità future.
RV38	VARCHAR2(255)	Valore riservato 38 Riservato a SourceOperationalContext. L'uso di questo campo per qualsiasi altro scopo può causare la sovrascrittura dei dati da parte di funzionalità future.
RV40 - 43	VARCHAR2(255)	Valore riservato 40 - 43 Riservato all'uso futuro da parte di Novell. L'uso di questo campo per qualsiasi altro scopo può causare la sovrascrittura dei dati da parte di funzionalità future.
RV44	VARCHAR2(255)	Valore riservato 44 Riservato a DestinationThreatLevel. L'uso di questo campo per qualsiasi altro scopo può causare la sovrascrittura dei dati da parte di funzionalità future.
RV45	VARCHAR2(255)	Valore riservato 45 Riservato a DestinationUserContext. L'uso di questo campo per qualsiasi altro scopo può causare la sovrascrittura dei dati da parte di funzionalità future.
RV46	VARCHAR2(255)	Valore riservato 46 Riservato a VirusStatus. L'uso di questo campo per qualsiasi altro scopo può causare la sovrascrittura dei dati da parte di funzionalità future.
RV47	VARCHAR2(255)	Valore riservato 47 Riservato all'uso futuro da parte di Novell. L'uso di questo campo per qualsiasi altro scopo può causare la sovrascrittura dei dati da parte di funzionalità future.

Nome colonna	Tipo di dati	Commento
RV48	VARCHAR2(255)	Valore riservato 48 Riservato a DestinationOperationalContext. L'uso di questo campo per qualsiasi altro scopo può causare la sovrascrittura dei dati da parte di funzionalità future.
RV49	VARCHAR2(255)	Valore riservato 49 Riservato all'uso futuro da parte di Novell. L'uso di questo campo per qualsiasi altro scopo può causare la sovrascrittura dei dati da parte di funzionalità future.
REFERENCE_ID 01 - 20	di tipo numerico	Riservato all'uso futuro da parte di Novell. L'uso di questo campo per qualsiasi altro scopo può causare la sovrascrittura dei dati da parte di funzionalità future.
CV01 - 10	NUMBER	Valore personalizzato 1 - 10 Riservato all'uso da parte del cliente, in genere per l'associazione di dati aziendali rilevanti
CV11 - 20	DATE	Valore personalizzato 11 - 20 Riservato all'uso da parte del cliente, in genere per l'associazione di dati aziendali rilevanti
CV21 - 100	VARCHAR2(255)	Valore personalizzato 21 – 100 Riservato all'uso da parte del cliente, in genere per l'associazione di dati aziendali rilevanti

EVT_AGENT_RPT_V

La vista fa riferimento alla tabella EVT_AGENT in cui sono memorizzate informazioni sui servizi di raccolta.

Nome colonna	Tipo di dati	Commento
AGENT_ID	di tipo numerico	Identificatore del servizio di raccolta
AGENT	varchar2(64)	Nome servizio di raccolta
PORT	varchar2(64)	Porta del servizio di raccolta
REPORT_NAME	varchar2(255)	Nome dell'autore del rapporto
PRODUCT_NAME	varchar2(255)	Nome del prodotto
SENSOR_NAME	varchar2(255)	Nome del sensore

Nome colonna	Tipo di dati	Commento
SENSOR_TYPE	varchar2(5)	Tipo di sensore: H - basato sull'host N - basato sulla rete V - virus O - altro
DEVICE_CTGRY	varchar2(255)	Categoria del dispositivo
SOURCE_UUID	varchar2	UUID (Universal Unique Identifier) del componente di origine
DATE_CREATED	data	Data di inserimento
DATE_MODIFIED	data	Data dell'ultimo aggiornamento
CREATED_BY	di tipo numerico	ID dell'utente che ha eseguito l'inserimento
MODIFIED_BY	di tipo numerico	ID dell'utente che ha eseguito l'ultimo aggiornamento

EVT_ASSET_RPT_V

La vista fa riferimento alla tabella EVT_ASSET in cui sono memorizzate informazioni sulle risorse.

Nome colonna	Tipo di dati	Commento
EVENT_ASSET_ID	di tipo numerico	Identificatore della risorsa dell'evento
ASSET_NAME	varchar2(255)	Nome della risorsa
PHYSICAL_ASSET_NAME	varchar2(255)	Nome della risorsa fisica
REFERENCE_ASSET_ID	varchar2(100)	Identificatore della risorsa di riferimento, collega al sistema di gestione delle risorse di origine.
MAC_ADDRESS	varchar2(100)	Indirizzo MAC
RACK_NUMBER	varchar2(50)	Numero del rack
ROOM_NAME	varchar2(100)	Nome della stanza
BUILDING_NAME	varchar2(255)	Nome dell'edificio
CITY	varchar2(100)	Città
STATE	varchar2(100)	Stato
COUNTRY	varchar2(100)	Paese
ZIP_CODE	varchar2(50)	CAP
ASSET_CATEGORY_NAME	varchar2(100)	Nome della categoria della risorsa
NETWORK_IDENTITY_NAME	varchar2(255)	Nome dell'identità di rete della risorsa
ENVIRONMENT_IDENTITY_ NAME	varchar2(255)	Nome dell'ambiente
ASSET_VALUE_NAME	varchar2(50)	Nome del valore della risorsa
CRITICALITY_NAME	varchar2(50)	Nome della criticità della risorsa
SENSITIVITY_NAME	varchar2(50)	Nome della riservatezza della risorsa
CONTACT_NAME_1	varchar2(255)	Nome della persona/organizzazione di contatto 1

Nome colonna	Tipo di dati	Commento
CONTACT_NAME_2	varchar2(255)	Nome della persona/organizzazione di contatto 2
ORGANIZATION_NAME_1	varchar2(100)	Livello dell'organizzazione proprietaria delle risorse 1
ORGANIZATION_NAME_2	varchar2(100)	Livello dell'organizzazione proprietaria delle risorse 2
ORGANIZATION_NAME_3	varchar2(100)	Livello dell'organizzazione proprietaria delle risorse 3
ORGANIZATION_NAME_4	varchar2(100)	Livello dell'organizzazione proprietaria delle risorse 4
DATE_CREATED	data	Data di inserimento
DATE_MODIFIED	data	Data dell'ultimo aggiornamento
CREATED_BY	di tipo numerico	ID dell'utente che ha eseguito l'inserimento
MODIFIED_BY	di tipo numerico	ID dell'utente che ha eseguito l'ultimo aggiornamento

EVT_DEST_EVT_NAME_SMRY_1_RPT_V

La vista riepiloga il numero di eventi per destinazione, tassonomia, gravità, nome e ora dell'evento.

Nome colonna	Tipo di dati	Commento
DESTINATION_IP	di tipo numerico	Indirizzo IP di destinazione
DESTINATION_EVENT_ ASSET_ID	di tipo numerico	Identificatore della risorsa dell'evento
TAXONOMY_ID	di tipo numerico	Identificatore della tassonomia
EVENT_NAME_ID	di tipo numerico	Identificatore del nome dell'evento
SEVERITY	di tipo numerico	Gravità dell'evento
CUSTOMER_ID	di tipo numerico	Identificatore del cliente
EVT_TIME	data	Ora dell'evento
EVT_COUNT	di tipo numerico	Numero di eventi
DATE_CREATED	data	Data di inserimento
DATE_MODIFIED	data	Data dell'ultimo aggiornamento
CREATED_BY	di tipo numerico	ID dell'utente che ha eseguito l'inserimento
MODIFIED_BY	di tipo numerico	ID dell'utente che ha eseguito l'ultimo aggiornamento

EVT_DEST_SMRY_1_RPT_V

La vista contiene informazioni di riepilogo sulle destinazioni degli eventi.

Nome colonna	Tipo di dati	Commento
DESTINATION_IP	di tipo numerico	Indirizzo IP di destinazione
DESTINATION_EVENT_ ASSET_ID	di tipo numerico	Identificatore della risorsa dell'evento
DESTINATION_PORT	varchar2(32)	Porta di destinazione

Nome colonna	Tipo di dati	Commento
DESTINATION_USR_ID	di tipo numerico	Identificatore dell'utente di destinazione
TAXONOMY_ID	di tipo numerico	Identificatore della tassonomia
EVENT_NAME_ID	di tipo numerico	Identificatore del nome dell'evento
RESOURCE_ID	di tipo numerico	Identificatore della risorsa
AGENT_ID	di tipo numerico	Identificatore del servizio di raccolta
PROTOCOL_ID	di tipo numerico	Identificatore del prodotto
SEVERITY	di tipo numerico	Gravità dell'evento
CUSTOMER_ID	di tipo numerico	Identificatore del cliente
EVENT_TIME	data	Ora dell'evento
EVENT_CNT	di tipo numerico	Numero di eventi
DATE_CREATED	data	Data di inserimento
DATE_MODIFIED	data	Data dell'ultimo aggiornamento
CREATED_BY	di tipo numerico	ID dell'utente che ha eseguito l'inserimento
MODIFIED_BY	di tipo numerico	ID dell'utente che ha eseguito l'ultimo aggiornamento

EVT_DEST_TXNMY_SMRY_1_RPT_V

La vista riepiloga il numero di eventi per destinazione, tassonomia, gravità e ora dell'evento.

Nome colonna	Tipo di dati	Commento
DESTINATION_IP	di tipo numerico	Indirizzo IP di destinazione
DESTINATION_EVENT_ ASSET_ID	di tipo numerico	Identificatore della risorsa dell'evento
TAXONOMY_ID	di tipo numerico	Identificatore della tassonomia
SEVERITY	di tipo numerico	Gravità dell'evento
CUSTOMER_ID	di tipo numerico	Identificatore del cliente
EVENT_TIME	data	Ora dell'evento
EVENT_COUNT	di tipo numerico	Numero di eventi
DATE_CREATED	data	Data di inserimento
DATE_MODIFIED	data	Data dell'ultimo aggiornamento
CREATED_BY	di tipo numerico	ID dell'utente che ha eseguito l'inserimento
MODIFIED_BY	di tipo numerico	ID dell'utente che ha eseguito l'ultimo aggiornamento

EVT_NAME_RPT_V

La vista fa riferimento alla tabella EVT_NAME in cui sono memorizzate informazioni sui nomi degli eventi.

Nome colonna	Tipo di dati	Commento
EVENT_NAME_ID	di tipo numerico	Identificatore del nome dell'evento
EVENT_NAME	varchar2(255)	Nome dell'evento
DATE_CREATED	data	Data di inserimento
DATE_MODIFIED	data	Data dell'ultimo aggiornamento

Nome colonna	Tipo di dati	Commento
CREATED_BY	di tipo numerico	ID dell'utente che ha eseguito l'inserimento
MODIFIED_BY	di tipo numerico	ID dell'utente che ha eseguito l'ultimo aggiornamento

EVT_PORT_SMRY_1_RPT_V

La vista riepiloga il numero di eventi per porta di destinazione, gravità e ora dell'evento.

Nome colonna	Tipo di dati	Commento
DESTINATION_PORT	Varchar2(32)	Porta di destinazione
SEVERITY	di tipo numerico	Gravità dell'evento
CUSTOMER_ID	di tipo numerico	Identificatore del cliente
EVENT_TIME	data	Ora dell'evento
EVENT_COUNT	di tipo numerico	Numero di eventi
DATE_CREATED	data	Data di inserimento
DATE_MODIFIED	data	Data dell'ultimo aggiornamento
CREATED_BY	di tipo numerico	ID dell'utente che ha eseguito l'inserimento
MODIFIED_BY	di tipo numerico	ID dell'utente che ha eseguito l'ultimo aggiornamento

EVT_PRTCL_RPT_V

La vista fa riferimento alla tabella EVT_PRTCL in cui sono memorizzate informazioni sui protocolli degli eventi.

Nome colonna	Tipo di dati	Commento
PROTOCOL_ID	di tipo numerico	Identificatore del prodotto
PROTOCOL_NAME	varchar2(255)	Nome del protocollo
DATE_CREATED	data	Data di inserimento
DATE_MODIFIED	data	Data dell'ultimo aggiornamento
CREATED_BY	di tipo numerico	ID dell'utente che ha eseguito l'inserimento
MODIFIED_BY	di tipo numerico	ID dell'utente che ha eseguito l'ultimo aggiornamento

EVT_RSRC_RPT_V

La vista fa riferimento alla tabella EVT_RSRC in cui sono memorizzate informazioni sulle risorse degli eventi.

Nome colonna	Tipo di dati	Commento
RESOURCE_ID	di tipo numerico	Identificatore della risorsa
RESOURCE_NAME	varchar2(255)	Nome della risorsa
SUBRESOURCE_NAME	varchar2(255)	Nome della sottorisorsa
DATE_CREATED	data	Data di inserimento
DATE_MODIFIED	data	Data dell'ultimo aggiornamento
CREATED_BY	di tipo numerico	ID dell'utente che ha eseguito l'inserimento

Nome colonna	Tipo di dati	Commento
MODIFIED_BY	di tipo numerico	ID dell'utente che ha eseguito l'ultimo aggiornamento

EVT_SEV_SMRY_1_RPT_V

La vista riepiloga il numero di eventi per gravità e ora dell'evento.

Nome colonna	Tipo di dati	Commento
SEVERITY	di tipo numerico	Gravità dell'evento
CUSTOMER_ID	di tipo numerico	Identificatore del cliente
EVENT_TIME	data	Ora dell'evento
EVENT_COUNT	di tipo numerico	Numero di eventi
DATE_CREATED	data	Data di inserimento
DATE_MODIFIED	data	Data dell'ultimo aggiornamento
CREATED_BY	di tipo numerico	ID dell'utente che ha eseguito l'inserimento
MODIFIED_BY	di tipo numerico	ID dell'utente che ha eseguito l'ultimo aggiornamento

EVT_SRC_SMRY_1_RPT_V

La vista contiene informazioni di riepilogo sulle destinazioni e le origini degli eventi.

Nome colonna	Tipo di dati	Commento
SOURCE_IP	di tipo numerico	Indirizzo IP di origine
SOURCE_EVENT_ASSET_ID	di tipo numerico	Identificatore della risorsa dell'evento di origine
SOURCE_PORT	varchar2(32)	Porta di origine
SOURCE_USER_ID	di tipo numerico	Identificatore dell'utente di origine
TAXONOMY_ID	di tipo numerico	Identificatore della tassonomia
EVENT_NAME_ID	di tipo numerico	Identificatore del nome dell'evento
RESOURCE_ID	di tipo numerico	Identificatore della risorsa
AGENT_ID	di tipo numerico	Identificatore del servizio di raccolta
PROTOCOL_ID	di tipo numerico	Identificatore del prodotto
SEVERITY	di tipo numerico	Gravità dell'evento
CUSTOMER_ID	di tipo numerico	Identificatore del cliente
EVENT_TIME	data	Ora dell'evento
EVENT_COUNT	di tipo numerico	Numero di eventi
DATE_CREATED	data	Data di inserimento
DATE_MODIFIED	data	Data dell'ultimo aggiornamento
CREATED_BY	di tipo numerico	ID dell'utente che ha eseguito l'inserimento
MODIFIED_BY	di tipo numerico	ID dell'utente che ha eseguito l'ultimo aggiornamento

EVT_TXNMY_RPT_V

La vista fa riferimento alla tabella EVT_TXNMY in cui sono memorizzate informazioni sulla tassonomia degli eventi.

Nome colonna	Tipo di dati	Commento
TAXONOMY_ID	di tipo numerico	Identificatore della tassonomia
TAXONOMY_LEVEL_1	varchar2(100)	Livello di tassonomia 1
TAXONOMY_LEVEL_2	varchar2(100)	Livello di tassonomia 2
TAXONOMY_LEVEL_3	varchar2(100)	Livello di tassonomia 3
TAXONOMY_LEVEL_4	varchar2(100)	Livello di tassonomia 4
DATE_CREATED	data	Data di inserimento
DATE_MODIFIED	data	Data dell'ultimo aggiornamento
CREATED_BY	di tipo numerico	ID dell'utente che ha eseguito l'inserimento
MODIFIED_BY	di tipo numerico	ID dell'utente che ha eseguito l'ultimo aggiornamento

EVT_USR_RPT_V

La vista fa riferimento alla tabella EVT_USR in cui sono memorizzate informazioni sugli utenti degli eventi.

Nome colonna	Tipo di dati	Commento
USER_ID	di tipo numerico	Identificatore dell'utente
USER_NAME	varchar2(255)	Nome utente
DATE_CREATED	data	Data di inserimento
DATE_MODIFIED	data	Data dell'ultimo aggiornamento
CREATED_BY	di tipo numerico	ID dell'utente che ha eseguito l'inserimento
MODIFIED_BY	di tipo numerico	ID dell'utente che ha eseguito l'ultimo aggiornamento

EXTERNAL_DATA_RPT_V

La vista fa riferimento alla tabella EXTERNAL_DATA in cui sono memorizzati dati esterni.

Nome colonna	Tipo di dati	Commento
EXTERNAL_DATA_ID	di tipo numerico	Identificatore dei dati esterni
SOURCE_NAME	varchar2(50)	Nome dell'origine
SOURCE_DATA_ID	varchar2(255)	Identificatore dei dati di origine
EXTERNAL_DATA	testo	Dati esterni
EXTERNAL_DATA_TYPE	varchar2(10)	Tipo dei dati esterni
DATE_CREATED	data	Data di inserimento
DATE_MODIFIED	data	Data dell'ultimo aggiornamento
CREATED_BY	di tipo numerico	ID dell'utente che ha eseguito l'inserimento
MODIFIED_BY	di tipo numerico	ID dell'utente che ha eseguito l'ultimo aggiornamento

HIST_EVENTS_RPT_V

Vista di eventi cronologici (ripristinati da archivi).

HIST_ INCIDENTS_RPT_V

Vista di eventi cronologici (ripristinati da archivi).

IMAGES_RPT_V

La vista fa riferimento alla tabella IMAGES in cui sono memorizzate informazioni sulle immagini di panoramica del sistema.

Nome colonna	Tipo di dati	Commento
NAME	VARCHAR2(128)	Nome dell'immagine
TYPE	VARCHAR2(64)	Tipo di immagine
DATA	CLOB	Data dell'immagine
DATE_CREATED	DATE	Data di inserimento
DATE_MODIFIED	DATE	Data dell'ultimo aggiornamento
CREATED_BY	NUMBER	ID dell'utente che ha eseguito l'inserimento
MODIFIED_BY	NUMBER	ID dell'utente che ha eseguito l'ultimo aggiornamento

INCIDENTS_ASSETS_RPT_V

La vista fa riferimento alla tabella INCIDENTS_ASSETS in cui sono memorizzate informazioni sulle risorse che costituiscono casi creati nella console Sentinel.

Nome colonna	Tipo di dati	Commento
INC_ID	NUMBER	Identificatore del caso – numero di sequenza
ASSET_ID	varchar2	UUID (Universal Unique Identifier) della risorsa
DATE_CREATED	DATE	Data di inserimento
DATE_MODIFIED	DATE	Data dell'ultimo aggiornamento
CREATED_BY	NUMBER	ID dell'utente che ha eseguito l'inserimento
MODIFIED_BY	NUMBER	ID dell'utente che ha eseguito l'ultimo aggiornamento

INCIDENTS_EVENTS_RPT_V

La vista fa riferimento alla tabella INCIDENTS_EVENTS in cui sono memorizzate informazioni sugli eventi che costituiscono casi creati nella console Sentinel.

Nome colonna	Tipo di dati	Commento
INC_ID	NUMBER	Identificatore del caso – numero di sequenza
EVT_ID	varchar2	UUID (Universal Unique Identifier) dell'evento
EVT_TIME	DATE	Ora dell'evento
DATE_CREATED	DATE	Data di inserimento
DATE_MODIFIED	DATE	Data dell'ultimo aggiornamento

Nome colonna	Tipo di dati	Commento
CREATED_BY	NUMBER	ID dell'utente che ha eseguito l'inserimento
MODIFIED_BY	NUMBER	ID dell'utente che ha eseguito l'ultimo aggiornamento

INCIDENTS_RPT_V

La vista fa riferimento alla tabella INCIDENTS in cui sono memorizzate informazioni che descrivono i dettagli dei casi creati nella console Sentinel.

Nome colonna	Tipo di dati	Commento
INC_ID	NUMBER	Identificatore del caso – numero di sequenza
NAME	VARCHAR2(255)	Nome del caso
SEVERITY	NUMBER	Gravità del caso
STT_ID	NUMBER	ID dello stato del caso
SEVERITY_RATING	VARCHAR2(32)	Media di tutte le gravità degli eventi che compongono un caso.
VULNERABILITY_RATING	VARCHAR2(32)	Riservato all'uso futuro da parte di Novell. L'uso di questo campo per qualsiasi altro scopo può causare la sovrascrittura dei dati da parte di funzionalità future.
CRITICALITY_RATING	VARCHAR2(32)	Riservato all'uso futuro da parte di Novell. L'uso di questo campo per qualsiasi altro scopo può causare la sovrascrittura dei dati da parte di funzionalità future.
DATE_CREATED	DATE	Data di inserimento
DATE_MODIFIED	DATE	Data dell'ultimo aggiornamento
CREATED_BY	NUMBER	ID dell'utente che ha eseguito l'inserimento
MODIFIED_BY	NUMBER	ID dell'utente che ha eseguito l'ultimo aggiornamento
INC_DESC	varchar2(4000)	Descrizione del caso
INC_PRIORITY	di tipo numerico	Priorità del caso
INC_CAT	varchar2(255)	Categoria del caso
INC_RES	varchar2(4000)	Risoluzione del caso

INCIDENTS_VULN_RPT_V

La vista fa riferimento alla tabella INCIDENTS_VULN in cui sono memorizzate informazioni sulle vulnerabilità che costituiscono casi creati nella console Sentinel.

Nome colonna	Tipo di dati	Commento
INC_ID	NUMBER	Identificatore del caso – numero di sequenza
VULN_ID	varchar2(36)	UUID (Universal Unique Identifier) della vulnerabilità

Nome colonna	Tipo di dati	Commento
DATE_CREATED	DATE	Data di inserimento
DATE_MODIFIED	DATE	Data dell'ultimo aggiornamento
CREATED_BY	NUMBER	ID dell'utente che ha eseguito l'inserimento
MODIFIED_BY	NUMBER	ID dell'utente che ha eseguito l'ultimo aggiornamento

L_STAT_RPT_V

La vista fa riferimento alla tabella L_STAT in cui sono memorizzate informazioni statistiche.

Nome colonna	Tipo di dati	Commento
RES_NAME	VARCHAR2(32)	Nome della risorsa
STATS_NAME	VARCHAR2(32)	Nome della statistica
STATS_VALUE	VARCHAR2(32)	Valore della statistica
OPEN_TOT_SECS	NUMERIC	Numero di secondi a partire dal 1970.

LOGS_RPT_V

La vista fa riferimento alla tabella LOGS_RPT in cui sono memorizzate informazioni di registrazione.

Tabella LOGS		
Nome colonna	**Tipo di dati**	**Commento**
LOG_ID	NUMBER	Numero di sequenza
TIME	DATE	Data del log
MODULE	VARCHAR2(64)	Modulo a cui si riferisce il log
TEXT	VARCHAR2(4000)	Testo del log

NETWORK_IDENTITY_RPT_V

La vista fa riferimento alla tabella NETWORK_IDENTITY_LKUP in cui sono memorizzate informazioni sull'identità di rete delle risorse.

Nome colonna	Tipo di dati	Commento
NETWORK_IDENTITY_CD	varchar2(5)	Codice dell'identità di rete
NETWORK_IDENTITY_NAME	varchar2(255)	Nome di identificazione della rete
DATE_CREATED	data	Data di inserimento
DATE_MODIFIED	data	Data dell'ultimo aggiornamento
CREATED_BY	di tipo numerico	ID dell'utente che ha eseguito l'inserimento
MODIFIED_BY	di tipo numerico	ID dell'utente che ha eseguito l'ultimo aggiornamento

ORGANIZATION_RPT_V

La vista fa riferimento alla tabella ORGANIZATION in cui sono memorizzate informazioni sull'organizzazione (risorsa).

Nome colonna	Tipo di dati	Commento
ORGANIZATION_ID	varchar2	Identificatore dell'organizzazione

Nome colonna	Tipo di dati	Commento
ORGANIZATION_NAME	varchar2(100)	Nome dell'organizzazione
CUSTOMER_ID	di tipo numerico	Identificatore del cliente
DATE_CREATED	data	Data di inserimento
DATE_MODIFIED	data	Data dell'ultimo aggiornamento
CREATED_BY	di tipo numerico	ID dell'utente che ha eseguito l'inserimento
MODIFIED_BY	di tipo numerico	ID dell'utente che ha eseguito l'ultimo aggiornamento

PERSON_RPT_V

La vista fa riferimento alla tabella PERSION in cui sono memorizzate informazioni personali (risorsa).

Nome colonna	Tipo di dati	Commento
PERSON_ID	varchar2	Identificatore della persona
FIRST_NAME	varchar2(255)	Nome
LAST_NAME	varchar2(255)	Cognome
CUSTOMER_ID	di tipo numerico	Identificatore del cliente
PHONE_NUMBER	varchar2(50)	Numero di telefono
EMAIL_ADDRESS	varchar2(255)	Indirizzo e-mail
DATE_CREATED	data	Data di inserimento
DATE_MODIFIED	data	Data dell'ultimo aggiornamento
CREATED_BY	di tipo numerico	ID dell'utente che ha eseguito l'inserimento
MODIFIED_BY	di tipo numerico	ID dell'utente che ha eseguito l'ultimo aggiornamento

PHYSICAL_ASSET_RPT_V

La vista fa riferimento alla tabella PHYSICAL_ASSET in cui sono memorizzate informazioni sulle risorse fisiche.

Nome colonna	Tipo di dati	Commento
PHYSICAL_ASSET_ID	varchar2	Identificatore della risorsa fisica
CUSTOMER_ID	di tipo numerico	Identificatore del cliente
LOCATION_ID	di tipo numerico	Identificatore dell'ubicazione
HOST_NAME	varchar2(255)	Nome host
IP_ADDRESS	di tipo numerico	Indirizzo IP
NETWORK_IDENTITY_CD	varchar2(5)	Codice dell'identità di rete
MAC_ADDRESS	varchar2(100)	Indirizzo MAC
RACK_NUMBER	varchar2(50)	Numero del rack
ROOM_NAME	varchar2(100)	Nome della stanza
DATE_CREATED	data	Data di inserimento
DATE_MODIFIED	data	Data dell'ultimo aggiornamento
CREATED_BY	di tipo numerico	ID dell'utente che ha eseguito l'inserimento
MODIFIED_BY	di tipo numerico	ID dell'utente che ha eseguito l'ultimo aggiornamento

PRODUCT_RPT_V

La vista fa riferimento alla tabella PRDT in cui sono memorizzate informazioni sui prodotti delle risorse.

Nome colonna	Tipo di dati	Commento
PRODUCT_ID	di tipo numerico	Identificatore del prodotto
PRODUCT_NAME	varchar2(255)	Nome del prodotto
PRODUCT_VERSION	varchar2(100)	Versione del prodotto
VENDOR_ID	di tipo numerico	Identificatore del produttore
DATE_CREATED	data	Data di inserimento
DATE_MODIFIED	data	Data dell'ultimo aggiornamento
CREATED_BY	di tipo numerico	ID dell'utente che ha eseguito l'inserimento
MODIFIED_BY	di tipo numerico	ID dell'utente che ha eseguito l'ultimo aggiornamento

ROLE_RPT_V

La vista fa riferimento alla tabella ROLE_LKUP in cui sono memorizzate informazioni sui ruoli utente (risorsa).

Nome colonna	Tipo di dati	Commento
ROLE_CODE	varchar2(5)	Codice del ruolo
ROLE_NAME	varchar2(255)	Nome del ruolo
DATE_CREATED	data	Data di inserimento
DATE_MODIFIED	data	Data dell'ultimo aggiornamento
CREATED_BY	di tipo numerico	ID dell'utente che ha eseguito l'inserimento
MODIFIED_BY	di tipo numerico	ID dell'utente che ha eseguito l'ultimo aggiornamento

SENSITIVITY_RPT_V

La vista fa riferimento alla tabella SENSITIVITY_LKUP in cui sono memorizzate informazioni sulla riservatezza delle risorse

Nome colonna	Tipo di dati	Commento
SENSITIVITY_CODE	varchar2(5)	Codice della riservatezza della risorsa
SENSITIVITY_NAME	varchar2(50)	Nome della riservatezza della risorsa
DATE_CREATED	data	Data di inserimento
DATE_MODIFIED	data	Data dell'ultimo aggiornamento
CREATED_BY	di tipo numerico	ID utente
MODIFIED_BY	di tipo numerico	ID utente

STATES_RPT_V

La vista fa riferimento alla tabella STATES in cui sono memorizzate le definizioni degli stati definiti dalle applicazioni o dal contesto.

Nome colonna	Tipo di dati	Commento
STT_ID	NUMBER	ID dello stato – numero di sequenza
CONTEXT	VARCHAR2(64)	Contesto dello stato, ovvero situazione, caso, utente.
NAME	VARCHAR2(64)	Nome dello stato.
TERMINAL_FLAG	VARCHAR2(1)	Indica se lo stato del caso è risolto.
DATE_CREATED	DATE	Data di inserimento
DATE_MODIFIED	DATE	Data dell'ultimo aggiornamento
MODIFIED_BY	NUMBER	ID dell'utente che ha eseguito l'inserimento
CREATED_BY	NUMBER	ID dell'utente che ha eseguito l'ultimo aggiornamento

UNASSIGNED_INCIDENTS_RPT_V

La vista fa riferimento alle tabelle CASES e INCIDENTS per generare report relative a situazioni e casi non assegnati.

Nome	Tipo di dati
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
CREATED_BY	NUMBER
MODIFIED_BY	NUMBER
INC_DESC	VARCHAR2(4000)
INC_PRIORITY	NUMBER
INC_CAT	VARCHAR2(255)
INC_RES	VARCHAR2(4000)

USERS_RPT_V

La vista fa riferimento alla tabella USERS in cui sono elencati tutti gli utenti dell'applicazione. Gli utenti verranno creati anche come utenti di database per adattarsi agli strumenti di generazione di rapporti di terze parti.

Nome colonna	Tipo di dati	Commento
USR_ID	NUMBER	Identificatore dell'utente – numero di sequenza
NAME	VARCHAR2(64)	Breve nome utente univoco utilizzato come login
CNT_ID	NUMBER	ID del contatto – numero di sequenza
STT_ID	NUMBER	ID dello stato. Lo stato è attivo o inattivo.
DESCRIPTION	VARCHAR2(512)	Commenti

Nome colonna	Tipo di dati	Commento
DATE_CREATED	DATE	Data di inserimento
DATE_MODIFIED	DATE	Data dell'ultimo aggiornamento
CREATED_BY	NUMBER	ID dell'utente che ha eseguito l'inserimento
MODIFIED_BY	NUMBER	ID dell'utente che ha eseguito l'ultimo aggiornamento
PERMISSIONS	VARCHAR2(4000)	Autorizzazioni attualmente assegnate all'utente Sentinel
FILTER	VARCHAR2(128)	Filtro di sicurezza corrente assegnato all'utente Sentinel
UPPER_NAME	VARCHAR2(64)	Nome utente al maiuscolo
DOMAIN_AUTH_IND	NUMBER	Indicazione dell'autenticazione di dominio

VENDOR_RPT_V

La vista fa riferimento alla tabella VNDR in cui sono memorizzate informazioni sui fornitori dei prodotti delle risorse.

Nome colonna	Tipo di dati	Commento
VENDOR_ID	di tipo numerico	Identificatore del produttore
VENDOR_NAME	varchar2(255)	Nome del fornitore
DATE_CREATED	data	Data di inserimento
DATE_MODIFIED	data	Data dell'ultimo aggiornamento
CREATED_BY	di tipo numerico	ID dell'utente che ha eseguito l'inserimento
MODIFIED_BY	di tipo numerico	ID dell'utente che ha eseguito l'ultimo aggiornamento

VULN_CALC_SEVERITY_RPT_V

La vista fa riferimento a VULN_RSRC e VULN per calcolare la classificazione della gravità della vulnerabilità di eSecurity in base alle vulnerabilità correnti.

Nome colonna	Tipo di dati
RSRC_ID	VARCHAR22(36)
IP	VARCHAR22(32)
HOST_NAME	VARCHAR22(255)
CRITICALITY	NUMBER
ASSIGNED_VULN_SEVERITY	NUMBER
VULN_COUNT	Numero di vulnerabilità per la risorsa specificata
CALC_SEVERITY	Gravità calcolata in base a ASSIGNED_VULN_SEVERITY e CRITICALITY

VULN_CODE_RPT_V

La vista fa riferimento alla tabella VULN_CODE in cui sono memorizzati i codici delle vulnerabilità assegnati in base a standard di settore.

Nome colonna	Tipo di dati
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

La vista fa riferimento alla tabella VULN_INFO in cui sono memorizzate informazioni aggiuntive riportate durante una scansione.

Nome colonna	Tipo di dati
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

La vista fa riferimento alla tabella VULN in cui sono memorizzate le informazioni del sistema sottoposto a scansione. Ogni scanner avrà una voce propria per ciascun sistema.

Nome colonna	Tipo di dati
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)

Nome colonna	Tipo di dati
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

La vista fa riferimento alla tabella VULN_RSRC in cui sono memorizzate tutte le risorse su cui è stata eseguita una particolare scansione.

Nome colonna	Tipo di dati
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)
REGULATION_RATING	VARCHAR2(64)
DATE_CREATED	DATE
DATE_MODIFIED	DATE
CREATED_BY	NUMBER
MODIFIED_BY	NUMBER

VULN_RSRC_SCAN_RPT_V

La vista fa riferimento alla tabella VULN_RSRC_SCAN in cui sono memorizzate tutte le risorse su cui è stata eseguita una particolare scansione.

Nome colonna	Tipo di dati
RSRC_ID	VARCHAR2(36)
SCAN_ID	VARCHAR2(36)
DATE_CREATED	DATE
DATE_MODIFIED	DATE
CREATED_BY	NUMBER
MODIFIED_BY	NUMBER

VULN_SCAN_RPT_V

La vista fa riferimento alla tabella in cui sono memorizzate le informazioni relative alle scansioni.

Nome colonna	Tipo di dati
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

La vista fa riferimento alla tabella VULN_SCAN_VULN in cui sono memorizzate le vulnerabilità rilevate durante le scansioni.

Nome colonna	Tipo di dati
SCAN_ID	VARCHAR2(36)
VULN_ID	VARCHAR2(36)
DATE_CREATED	DATE
DATE_MODIFIED	DATE
CREATED_BY	NUMBER
MODIFIED_BY	NUMBER

VULN_SCANNER_RPT_V

La vista fa riferimento alla tabella VULN_SCANNER in cui sono memorizzate informazioni sugli scanner delle vulnerabilità.

Nome colonna	Tipo di dati
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 Viste del database di Sentinel per Microsoft SQL Server

NOTA: Il termine agente è equivalente a servizio di raccolta. Si farà in seguito riferimento agli agenti come servizi di raccolta.

In questo capitolo vengono indicate le viste dello scherma Sentinel per Microsoft SQL Server. Le viste forniscono informazioni per lo sviluppo di rapporti personalizzati (Crystal Reports).

Viste

ADV_ALERT_CVE_RPT_V

La vista fa riferimento alla tabella ADV_ALERT_CVE in cui è memorizzato il numero di identificazione dell'avviso di Advisor.

Nome colonna	Tipo di dati	Commento
ALERT_ID	int	Identificatore di annotazione – numero di sequenza.
CVE	varchar	
DATE_CREATED	datetime	Data di inserimento
DATE_MODIFIED	datetime	Data dell'ultimo aggiornamento
CREATED_BY	int	ID utente
MODIFIED_BY	int	ID utente

ADV_ALERT_PRODUCT_RPT_V

La vista fa riferimento alla tabella ADV_ALERT_PRODUCT in cui sono memorizzate le informazioni sul prodotto di Advisor, come il numero ID del Service Pack, la versione e la data di creazione.

Nome colonna	Tipo di dati	Commento
ALERT_ID	int	Identificatore di annotazione – numero di sequenza
SERVICE_PACK_ID	int	
VENDOR	varchar	
PRODUCT	varchar	
VERSION	varchar	Contiene il numero di versione
SERVICE_PACK	varchar	
PRIMARY_FLAG	int	
DATE_CREATED	datetime	Data di inserimento
DATE_MODIFIED	datetime	Data dell'ultimo aggiornamento
CREATED_BY	int	ID utente
MODIFIED_BY	int	ID utente

ADV_ALERT_RPT_V

La vista fa riferimento alla tabella ADV_ALERT_PRODUCT in cui sono memorizzate le informazioni sull'avviso di Advisor, come il nome, il tipo di rischio e la data di pubblicazione.

Nome colonna	Tipo di dati	Commento
ALERT_ID	int	Identificatore di annotazione – numero di sequenza.
VERSION	int	Contiene il numero di versione
TEMPLATE_ID	int	
TEMPLATE_NAME	varchar	
THREAT_CATEGORY_NAME	varchar	
THREAT_TYPE_NAME	varchar	
HEADLINE	testo	
FIRST_PUBLISHED	datetime	
LAST_PUBLISHED	datetime	
STATUS	varchar	
URGENCY_ID	int	
CREDIBILITY_ID	int	
SEVERITY_ID	int	
SUMMARY	testo	
LEGAL_DISCLAIMER	testo	
COPYRIGHT	varchar	
BEGIN_EFFECTIVE_DATE	datetime	
END_EFFECTIVE_DATE	datetime	
DATE_CREATED	datetime	Data di inserimento
DATE_MODIFIED	datetime	Data dell'ultimo aggiornamento
CREATED_BY	int	ID utente
MODIFIED_BY	int	ID utente

ADV_ATTACK_ALERT_RPT_V

La vista fa riferimento alla tabella ADV_ATTACK_ALERT in cui sono memorizzate le informazioni sull'attacco di Advisor, come il nome, il tipo di rischio e la data di pubblicazione.

Nome colonna	Tipo di dati	Commento
ATTACK_ID	int	
ALERT_ID	int	
DATE_CREATED	datetime	Data di inserimento
DATE_MODIFIED	datetime	Data dell'ultimo aggiornamento
CREATED_BY	int	ID utente
MODIFIED_BY	int	ID utente

ADV_ATTACK_CVE_RPT_V

La vista fa riferimento alla tabella ADV_ATTACK_CVE in cui sono memorizzate le informazioni CVE di Advisor.

Nome colonna	Tipo di dati	Commento
ATTACK_ID	int	
CVE	varchar	
DATE_CREATED	datetime	Data di inserimento
DATE_MODIFIED	datetime	Data dell'ultimo aggiornamento
CREATED_BY	int	ID utente
MODIFIED_BY	int	ID utente

ADV_ATTACK_MAP_RPT_V

La vista fa riferimento alla tabella ADV_ATTACK_MAP in cui sono memorizzate le informazioni di mappatura di Advisor.

Nome colonna	Tipo di dati	Commento
ATTACK_KEY	int	
ATTACK_ID	int	
SERVICE_PACK_ID	int	
ATTACK_NAME	varchar	
ATTACK_CODE	varchar	
DATE_CREATED	datetime	Data di inserimento
DATE_MODIFIED	datetime	Data dell'ultimo aggiornamento
CREATED_BY	int	ID utente
MODIFIED_by	int	ID utente

ADV_ATTACK_PLUGIN_RPT_V

La vista fa riferimento alla tabella ADV_ATTACK_PLUGIN in cui sono memorizzate le informazioni sul plug-in di Advisor.

Nome colonna	Tipo di dati	Commento
PLUGIN_KEY	int	
ATTACK_ID	int	
SERVICE_PACK_ID	int	
PLUGIN_ID	varchar	
PLUGIN_NAME	varchar	
DATE_CREATED	datetime	Data di inserimento
DATE_MODIFIED	datetime	Data dell'ultimo aggiornamento
CREATED_BY	int	ID utente
MODIFIED_BY	int	ID utente

ADV_ATTACK_RPT_V

La vista fa riferimento alla tabella ADV_ATTACK in cui sono memorizzate le informazioni sull'attacco di Advisor.

Nome colonna	Tipo di dati	Commento
ALERT_ID	int	
TRUSECURE_ATTACK_ NAME	int	
FEED_DATE_CREATED	datetime	
FEED_DATE_UPDATED	datetime	

Nome colonna	Tipo di dati	Commento
ATTACK_CATEGORY	varchar	
URGENCY_ID	int	
SEVERITY_ID	int	
LOCAL	int	
REMOTE	int	
BEGIN_EFFECTIVE_DATE	datetime	
END_EFFECTIVE_DATE	datetime	
DESCRIPTION	testo	
SCENARIO	testo	
IMPACT	testo	
SAFEGUARDS	testo	
PATCHES	testo	
FALSE_POSITIVES	testo	
DATE_CREATED	datetime	Data di inserimento
DATE_MODIFIED	datetime	Data dell'ultimo aggiornamento
CREATED_BY	int	ID utente
MODIFIED_BY	int	ID utente

ADV_CREDIBILITY_RPT_V

La vista fa riferimento alla tabella ADV_CREDIBILITY in cui sono memorizzate le informazioni sulla credibilità di Advisor.

Nome colonna	Tipo di dati	Commento
CREDIBILITY_ID	int	
CREDIBILITY_RATING	varchar	
CREDIBILITY_EXPLANATION	varchar	
DATE_CREATED	datetime	Data di inserimento
DATE_MODIFIED	datetime	Data dell'ultimo aggiornamento
CREATED_BY	int	ID utente
MODIFIED_BY	int	ID utente

ADV_FEED_RPT_V

La vista fa riferimento alla tabella ADV_FEED in cui sono memorizzate le informazioni sul feed di Advisor, come il nome e la data.

Nome colonna	Tipo di dati	Commento
FEED_NAME	varchar	
FEED_FILE	varchar	
BEGIN_DATE	datetime	
END_DATE	datetime	
FEED_INSERT	int	
FEED_UPDATE	int	
FEED_EXPIRE	int	

ADV_PRODUCT_RPT_V

La vista fa riferimento alla tabella ADV_PRODUCT in cui sono memorizzate le informazioni sul prodotto di Advisor, come il fornitore e l'ID.

Nome colonna	Tipo di dati	Commento
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	datetime	
FEED_DATE_UPDATED	datetime	
ACTIVE_FLAG	int	
DATE_CREATED	datetime	Data di inserimento
DATE_MODIFIED	datetime	Data dell'ultimo aggiornamento
CREATED_BY	int	ID utente
MODIFIED_BY	int	ID utente

ADV_PRODUCT_SERVICE_PACK_RPT_V

La vista fa riferimento alla tabella ADV_PRODUCT_SERVICE _PACK in cui sono memorizzate le informazioni sul Service Pack di Advisor, come il nome, l'ID della versione e la data.

Nome colonna	Tipo di dati	Commento
SERVICE_PACK_ID	int	
VERSION_ID	int	Contiene il numero ID della versione
SERVICE_PACK_NAME	varchar	
FEED_DATE_CREATED	datetime	
FEED_DATE_UPDATED	datetime	
ACTIVE_FLAG	int	
BEGIN_EFFECTIVE_DATE	datetime	
END_EFFECTIVE_DATE	datetime	
DATE_CREATED	datetime	Data di inserimento
DATE_MODIFIED	datetime	Data dell'ultimo aggiornamento
CREATED_BY	int	ID utente
MODIFIED_BY	int	ID utente

ADV_PRODUCT_VERSION_RPT_V

La vista fa riferimento alla tabella ADV_PRODUCT_VERSION in cui sono memorizzate le informazioni sul prodotto di Advisor, come il nome della versione e l'ID del prodotto e della versione.

Nome colonna	Tipo di dati	Commento
VERSION_ID	int	Contiene il numero ID della versione
PRODUCT_ID	int	
VERSION_NAME	varchar	

Nome colonna	Tipo di dati	Commento
FEED_DATE_CREATED	datetime	
FEED_DATE_UPDATED	datetime	
ACTIVE_FLAG	int	
DATE_CREATED	datetime	Data di inserimento
DATE_MODIFIED	int	Data dell'ultimo aggiornamento
CREATED_BY	int	ID utente
MODIFIED_BY	int	ID utente

ADV_SEVERITY_RPT_V

La vista fa riferimento alla tabella ADV_SEVERITY in cui sono memorizzate le informazioni di classificazione della gravità di Advisor.

Nome colonna	Tipo di dati	Commento
SEVERITY_ID	int	
SEVERITY_RATING	varchar	
SEVERITY_EXPLANATION	varchar	
DATE_CREATED	datetime	Data di inserimento
DATE_MODIFIED	datetime	Data dell'ultimo aggiornamento
CREATED_BY	int	ID utente
MODIFIED_BY	int	ID utente

ADV_SUBALERT_RPT_V

La vista fa riferimento alla tabella ADV_SUBALERT.

Nome colonna	Tipo di dati	Commento
ALERT_ID	int	
SUBALERT_ID	int	
CHANGED_SECTIONS	varchar	
VARIANTS	testo	
VIRUS_NAME	testo	
DESCRIPTION	testo	
IMPACT	testo	
WARNING_INDICATORS	testo	
TECHNICAL_INFO	testo	
TRUSECURE_COMMENTS	testo	
VENDOR_ANNOUNCEMENTS	testo	
SAFEGUARDS	testo	
PATCHES_SOFTWARE	testo	
ALERT_HISTORY	testo	
BACKGROUND_INFO	testo	
DATE_CREATED	datetime	Data di inserimento
DATE_MODIFIED	datetime	Data dell'ultimo aggiornamento
CREATED_BY	int	ID utente
MODIFIED_BY	int	ID utente

ADV_URGENCY_RPT_V

La vista fa riferimento alla tabella ADV_URGENCY.

Nome colonna	Tipo di dati	Commento
URGENCY_ID	int	
URGENCY_RATING	varchar	
URGENCY_EXPLANATION	varchar	
DATE_CREATED	datetime	Data di inserimento
DATE_MODIFIED	datetime	Data dell'ultimo aggiornamento
CREATED_BY	int	ID utente
MODIFIED_BY	int	ID utente

ADV_VENDOR_RPT_V

La vista fa riferimento alla tabella ADV_VENDOR in cui sono memorizzate le informazioni sull'indirizzo di Advisor.

Nome colonna	Tipo di dati	Commento
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	datetime	
FEED_DATE_UPDATED	datetime	
ACTIVE_FLAG	int	
DATE_CREATED	datetime	Data di inserimento
DATE_MODIFIED	datetime	Data dell'ultimo aggiornamento
CREATED_BY	int	ID utente
MODIFIED_BY	int	ID utente

ADV_VULN_PRODUCT_RPT_V

La vista fa riferimento alla tabella ADV_VULN_PRODUCT in cui sono memorizzate le informazioni sull'ID dell'attacco alla vulnerabilità e l'ID del Service Pack di Advisor.

Nome colonna	Tipo di dati	Commento
ATTACK_ID	int	
SERVICE_PACK_ID	int	

Nome colonna	Tipo di dati	Commento
DATE_CREATED	datetime	Data di inserimento
DATE_MODIFIED	datetime	Data dell'ultimo aggiornamento
CREATED_BY	int	ID utente
MODIFIED_BY	int	ID utente

ANNOTATIONS_RPT_V

La vista fa riferimento alla tabella ANNOTATIONS in cui sono archiviate documentazione e note che possono essere associate ad oggetti del sistema Sentinel, ad esempio ai casi.

Nome colonna	Tipo di dati	Commento
ANN_ID	INT	Identificatore di annotazione – numero di sequenza.
TEXT	VARCHAR(4000)	Documentazione o note
DATE_CREATED	DATETIME	Data di inserimento
DATE_MODIFIED	DATETIME	Data dell'ultimo aggiornamento
MODIFIED_BY	INT	ID dell'utente che ha eseguito l'ultimo aggiornamento
CREATED_BY	INT	ID dell'utente che ha eseguito l'inserimento
ACTION	Varchar(255)	Azione

ASSET_CTGRY_RPT_V

La vista fa riferimento alla tabella ASSET_CTGRY in cui sono memorizzate informazioni sulle categorie di risorse, ad esempio hardware, software, sistema operativo, database e così via.

Nome colonna	Tipo di dati	Commento
ASSET_CATEGORY_ID	bigint	Identificatore della categoria della risorsa
ASSET_CATEGORY_NAME	varchar(100)	Nome della categoria della risorsa
DATE_CREATED	datetime	Data di inserimento
DATE_MODIFIED	datetime	Data dell'ultimo aggiornamento
CREATED_BY	int	ID dell'utente che ha eseguito l'inserimento
MODIFIED_BY	int	ID dell'utente che ha eseguito l'ultimo aggiornamento

ASSET_HOSTNAME_RPT_V

La vista fa riferimento alla tabella ASSET_HOSTNAME in cui sono memorizzate informazioni sui nomi host alternativi delle risorse.

Nome colonna	Tipo di dati	Commento
ASSET_HOSTNAME_ID	Uniqueidentifier	Identificatore del nome host alternativo della risorsa
PHYSICAL_ASSET_ID	uniqueidentifier	Identificatore della risorsa fisica
HOST_NAME	Varchar(255)	Nome host
CUSTOMER_ID	bigint	Identificatore del cliente
DATE_CREATED	datetime	Data dell'ultimo aggiornamento
DATE_MODIFIED	datetime	ID dell'utente che ha eseguito l'ultimo aggiornamento

Nome colonna	Tipo di dati	Commento
ASSET_HOSTNAME_ID	Uniqueidentifier	Identificatore del nome host alternativo della risorsa
CREATED_BY	int	ID dell'utente che ha eseguito l'inserimento
MODIFIED_BY	int	ID dell'utente che ha eseguito l'ultimo aggiornamento

ASSET_IP_RPT_V

La vista fa riferimento alla tabella ASSET_IP in cui sono memorizzate informazioni sugli indirizzi IP alternativi delle risorse.

Nome colonna	Tipo di dati	Commento
ASSET_IP_ID	Uniqueidentifier	Identificatore dell'indirizzo IP alternativo della risorsa
PHYSICAL_ASSET_ID	uniqueidentifier	Identificatore della risorsa fisica
IP_ADDRESS	int	Indirizzo IP della risorsa
CUSTOMER_ID	bigint	Identificatore del cliente
DATE_CREATED	datetime	Data di inserimento
DATE_MODIFIED	datetime	Data dell'ultimo aggiornamento
CREATED_BY	int	ID dell'utente che ha eseguito l'inserimento
MODIFIED_BY	int	ID dell'utente che ha eseguito l'ultimo aggiornamento

ASSET_LOCATION_RPT_V

La vista fa riferimento alla tabella ASSET_LOC in cui sono memorizzate informazioni sulle ubicazioni delle risorse.

Nome colonna	Tipo di dati	Commento
LOCATION_ID	bigint	Identificatore dell'ubicazione
CUSTOMER_ID	bigint	Identificatore del cliente
BUILDING_NAME	varchar(255)	Nome dell'edificio
ADDRESS_LINE_1	varchar(255)	Riga indirizzo 1
ADDRESS_LINE_2	varchar(255)	Riga indirizzo 2
CITY	varchar(100)	Città
STATE	varchar(100)	Stato
COUNTRY	varchar(100)	Paese
ZIP_CODE	varchar(50)	CAP
DATE_CREATED	datetime	Data di inserimento
DATE_MODIFIED	datetime	Data dell'ultimo aggiornamento
CREATED_BY	int	ID dell'utente che ha eseguito l'inserimento
MODIFIED_BY	int	ID dell'utente che ha eseguito l'ultimo aggiornamento

ASSET_RPT_V

La vista fa riferimento alla tabella ASSET in cui sono memorizzate informazioni sulle risorse fisiche e software.

Nome colonna	Tipo di dati	Commento
ASSET_ID	uniqueidentifier	Identificatore della risorsa
CUSTOMER_ID	bigint	Identificatore del cliente
ASSET_NAME	varchar(255)	Nome della risorsa
PHYSICAL_ASSET_ID	uniqueidentifier	Identificatore della risorsa fisica
PRODUCT_ID	bigint	Identificatore del prodotto
ASSET_CATEGORY_ID	bigint	Identificatore della categoria della risorsa
ENVIRONMENT_IDENTITY_CD	varchar(5)	Codice di identificazione dell'ambiente
PHYSICAL_ASSET_IND	bit	Indicatore della risorsa fisica
ASSET_VALUE_CD	varchar(5)	Codice del valore della risorsa
CRITICALITY_CODE	varchar(5)	Codice della criticità della risorsa
SENSITIVITY_CODE	varchar(5)	Codice della riservatezza della risorsa
DATE_CREATED	datetime	Data di inserimento
DATE_MODIFIED	datetime	Data dell'ultimo aggiornamento
CREATED_BY	int	ID dell'utente che ha eseguito l'inserimento
MODIFIED_BY	int	ID dell'utente che ha eseguito l'ultimo aggiornamento

ASSET_VALUE_RPT_V

La vista fa riferimento alla tabella ASSET_VAL_LKUP in cui sono memorizzate informazioni sul valore delle risorse.

Nome colonna	Tipo di dati	Commento
ASSET_VALUE_CODE	varchar(5)	Codice del valore della risorsa
ASSET_VALUE_NAME	varchar(50)	Nome del valore della risorsa
DATE_CREATED	datetime	Data di inserimento
DATE_MODIFIED	datetime	Data dell'ultimo aggiornamento
CREATED_BY	int	ID dell'utente che ha eseguito l'inserimento
MODIFIED_BY	int	ID dell'utente che ha eseguito l'ultimo aggiornamento

ASSET_X_ENTITY_X_ROLE_RPT_V

La vista fa riferimento alla tabella ASSET_X_ENTITY_X_ROLE che associa una persona o un'organizzazione a una risorsa.

Nome colonna	Tipo di dati	Commento
PERSON_ID	uniqueidentifier	Identificatore della persona
ORGANIZATION_ID	uniqueidentifier	Identificatore dell'organizzazione
ROLE_CODE	varchar(5)	Codice del ruolo
ASSET_ID	uniqueidentifier	Identificatore della risorsa
ENTITY_TYPE_CODE	varchar(5)	Codice del tipo di entità
PERSON_ROLE_SEQUENCE	int	Ordine di persone con un particolare ruolo

Nome colonna	Tipo di dati	Commento
DATE_CREATED	datetime	Data di inserimento
DATE_MODIFIED	datetime	Data dell'ultimo aggiornamento
CREATED_BY	int	ID dell'utente che ha eseguito l'inserimento
MODIFIED_BY	int	ID dell'utente che ha eseguito l'ultimo aggiornamento

ASSOCIATIONS_RPT_V

La vista fa riferimento alla tabella ASSOCIATIONS che associa utenti a casi, casi ad annotazioni e così via.

Nome colonna	Tipo di dati	Commento
TABLE1	VARCHAR(64)	Nome tabella 1. Ad esempio, casi
ID1	VARCHAR(36)	ID1. Ad esempio, ID caso.
TABLE2	VARCHAR(64)	Nome tabella 2. Ad esempio, utenti.
ID2	VARCHAR(36)	ID2. Ad esempio, ID utente.
DATE_CREATED	DATETIME	Data di inserimento.
DATE_MODIFIED	DATETIME	Data dell'ultimo aggiornamento
CREATED_BY	INT	ID dell'utente che ha eseguito l'inserimento
MODIFIED_BY	INT	ID dell'utente che ha eseguito l'ultimo aggiornamento

ATTACHMENTS_RPT_V

La vista fa riferimento alla tabella ATTACHMENTS in cui sono memorizzati dati sugli allegati.

Nome colonna	Tipo di dati	Commento
ATTACHMENT_ID	int	Identificatore dell'allegato
NAME	varchar(255)	Nome dell'allegato
SOURCE_REFERENCE	varchar(64)	Informazioni sull'origine
TYPE	varchar(32)	Tipo di allegato
SUB_TYPE	varchar(32)	Sottotipo di allegato
FILE_EXTENSION	varchar(32)	Estensione file
ATTACHMENT_DESCRIPTION	varchar(255)	Descrizione dell'allegato
DATA	clob	Dati dell'allegato
DATE_CREATED	datetime	Data di inserimento
DATE_MODIFIED	datetime	Data dell'ultimo aggiornamento
CREATED_BY	int	ID dell'utente che ha eseguito l'inserimento
MODIFIED_BY	int	ID dell'utente che ha eseguito l'ultimo aggiornamento

CONFIGS_RPT_V

La vista fa riferimento alla tabella CONFIGS in cui sono memorizzate le informazioni di configurazione generali dell'applicazione.

Nome colonna	Tipo di dati	Commento
USR_ID	VARCHAR(32)	Nome utente.
APPLICATION	VARCHAR(255)	Identificatore dell'applicazione
UNIT	VARCHAR(64)	Unità dell'applicazione
VALUE	VARCHAR(255)	Valore testuale, se disponibile
DATA	TEXT	Dati XML
DATE_CREATED	DATETIME	Data di inserimento.
DATE_MODIFIED	DATETIME	Data dell'ultimo aggiornamento.
CREATED_BY	INT	ID dell'utente che ha eseguito l'inserimento.
MODIFIED_BY	INT	ID dell'utente che ha eseguito l'ultimo aggiornamento.

CONTACTS_RPT_V

La vista fa riferimento alla tabella CONTACTS in cui sono memorizzate informazioni sui contatti.

Nome colonna	Tipo di dati	Commento
CNT_ID	INT	ID del contatto - numero di sequenza
FIRST_NAME	VARCHAR(20)	Nome del contatto.
LAST_NAME	VARCHAR(30)	Cognome del contatto.
TITLE	VARCHAR(128)	Titolo del contatto
DEPARTMENT	VARCHAR(128)	Reparto
PHONE	VARCHAR(64)	Numero di telefono del contatto
EMAIL	VARCHAR(255)	Indirizzo e-mail del contatto
PAGER	VARCHAR(64)	Numero del cercapersone del contatto
CELL	VARCHAR(64)	Numero del cellulare del contatto
DATE_CREATED	DATETIME	Data di inserimento
DATE_MODIFIED	DATETIME	Data dell'ultimo aggiornamento
CREATED_BY	INT	ID dell'utente che ha eseguito l'inserimento
MODIFIED_BY	INT	ID dell'utente che ha eseguito l'ultimo aggiornamento

CORRELATED_EVENTS_RPT_V

La vista fa riferimento alle tabelle CORRELATED_EVENTS_* in cui sono memorizzate informazioni sugli eventi correlati.

Nome colonna	Tipo di dati	Commento
PARENT_EVT_ID	uniqueidentifier	UUID (Event Universal Unique Identifier) dell'evento di livello superiore
CHILD_EVT_ID	uniqueidentifier	UUID (Event Universal Unique Identifier) dell'evento secondario
PARENT_EVT_TIME	DATETIME	Data di creazione dell'evento principale
CHILD_EVT_TIME	DATETIME	Data di creazione dell'evento secondario
DATE_CREATED	DATE	Data di inserimento generata da DAS
DATE_MODIFIED	DATETIME	Data dell'ultimo aggiornamento
CREATED_BY	INT	ID dell'utente che ha eseguito l'inserimento

Nome colonna	Tipo di dati	Commento
MODIFIED_BY	INT	ID dell'utente che ha eseguito l'ultimo aggiornamento

CORRELATED_EVENTS_RPT_V1

La vista contiene eventi correlati presenti e passati (importati da archivi).

Nome colonna	Tipo di dati	Commento
PARENT_EVT_ID	uniqueidentifier	UUID (Event Universal Unique Identifier) dell'evento di livello superiore
CHILD_EVT_ID	uniqueidentifier	UUID (Event Universal Unique Identifier) dell'evento secondario
PARENT_EVT_TIME	DATETIME	Ora dell'evento di livello superiore
CHILD_EVT_TIME	DATETIME	Ora dell'evento secondario
DATE_CREATED	DATETIME	Data di inserimento generata da DAS
DATE_MODIFIED	DATETIME	Data dell'ultimo aggiornamento
CREATED_BY	INT	ID dell'utente che ha eseguito l'inserimento
MODIFIED_BY	INT	ID dell'utente che ha eseguito l'ultimo aggiornamento

CRITICALITY_RPT_V

La vista fa riferimento alla tabella CRIT_LKUP in cui sono contenute informazioni sulla criticità delle risorse.

Nome colonna	Tipo di dati	Commento
CRITICALITY_CODE	varchar(5)	Codice della criticità della risorsa
CRITICALITY_NAME	varchar(50)	Nome della criticità della risorsa
DATE_CREATED	datetime	Data di inserimento
DATE_MODIFIED	datetime	Data dell'ultimo aggiornamento
CREATED_BY	int	ID utente
MODIFIED_BY	int	ID utente

CUST_RPT_V

La vista fa riferimento alla tabella CUST in cui sono memorizzate informazioni sui clienti per MSSP.

Nome colonna	Tipo di dati	Commento
CUSTOMER_ID	bigint	Identificatore del cliente
CUSTOMER_NAME	varchar(255)	Nome del cliente
DATE_CREATED	datetime	Data di inserimento
DATE_MODIFIED	datetime	Data dell'ultimo aggiornamento
CREATED_BY	int	ID dell'utente che ha eseguito l'inserimento
MODIFIED_BY	int	ID dell'utente che ha eseguito l'ultimo aggiornamento

ENTITY_TYPE_RPT_V

La vista fa riferimento alla tabella ENTITY_TYP in cui sono memorizzate informazioni sui tipi di entità (persona, organizzazione).

Nome colonna	Tipo di dati	Commento
ENTITY_TYPE_CODE	varchar(5)	Codice del tipo di entità
ENTITY_TYPE_NAME	varchar(50)	Nome del tipo di entità
DATE_CREATED	datetime	Data di inserimento
DATE_MODIFIED	datetime	Data dell'ultimo aggiornamento
CREATED_BY	int	ID dell'utente che ha eseguito l'inserimento
MODIFIED_BY	int	ID dell'utente che ha eseguito l'ultimo aggiornamento

ENV_IDENTITY_RPT_V

La vista fa riferimento alla tabella ENV_IDENTITY_LKUP in cui sono memorizzate informazioni sull'identità dell'ambiente delle risorse.

Nome colonna	Tipo di dati	Commento
ENVIRONMENT_IDENTITY_CODE	varchar(5)	Codice di identità dell'ambiente
ENVIRONMENT_IDENTITY_NAME	varchar(255)	Nome dell'identità dell'ambiente
DATE_CREATED	datetime	Data di inserimento
DATE_MODIFIED	datetime	Data dell'ultimo aggiornamento
CREATED_BY	int	ID dell'utente che ha eseguito l'inserimento
MODIFIED_BY	int	ID dell'utente che ha eseguito l'ultimo aggiornamento

ESEC_DISPLAY_RPT_V

La vista fa riferimento alla tabella ESEC_DISPLAY in cui sono memorizzate le proprietà visualizzabili degli oggetti. Viene attualmente utilizzata per la ridenominazione dei tag META. Viene utilizzata con la configurazione eventi (rilevanza aziendale).

Nome colonna	Tipo di dati	Commento
DISPLAY_OBJECT	VARCHAR(32)	Oggetto di livello superiore della proprietà
TAG	VARCHAR(32)	Nome tag nativo della proprietà
LABEL	VARCHAR(32)	Stringa visualizzata del tag.
POSITION	INT	Posizione del tag nella visualizzazione.
WIDTH	INT	Larghezza della colonna
ALIGNMENT	INT	Allineamento orizzontale
FORMAT	INT	Formattatore enumerato per la visualizzazione della proprietà
ENABLED	BIT	Indica se il tag è visualizzato.
TYPE	INT	Indica il tipo di dati del tag. 1 = string 2 = ulong 3 = date

Nome colonna	Tipo di dati	Commento
		4 = uuid 5 = ipv4
DESCRIPTION	VARCHAR(255)	Descrizione testuale del tag
DATE_CREATED	DATETIME	Data di inserimento.
DATE_MODIFIED	DATETIME	Data dell'ultimo aggiornamento.
CREATED_BY	INT	ID dell'utente che ha eseguito l'inserimento.
MODIFIED_BY	INT	ID dell'utente che ha eseguito l'ultimo aggiornamento.
REF_CONFIG	VARCHAR(4000)	Configurazione dei dati di riferimento

ESEC_PORT_REFERENCE_RPT_V

La vista fa riferimento alla tabella ESEC_PORT_REFERENCE in cui sono memorizzati i numeri di porta assegnati in base a standard di settore.

Nome colonna	Tipo di dati	Commento
PORT_NUMBER	INT	Per http://www.iana.org/assignments/port-numbers, rappresentazione numerica della porta. Questo numero di porta viene normalmente associato al livello del protocollo di trasporto nello stack TCP/IP.
PROTOCOL_NUMBER	INT	Per http://www.iana.org/assignments/protocol-numbers, identificatori numerici utilizzati per rappresentare i protocolli incapsulati in un pacchetto IP.
PORT_KEYWORD	VARCHAR(64)	Per http://www.iana.org/assignments/port-numbers, rappresentazione con parola chiave della porta.
PORT_DESCRIPTION	VARCHAR(512)	Descrizione della porta.
DATE_CREATED	DATETIME	Data di inserimento.
DATE_MODIFIED	DATETIME	Data dell'ultimo aggiornamento.
CREATED_BY	INT	ID dell'utente che ha eseguito l'inserimento.
MODIFIED_BY	INT	ID dell'utente che ha eseguito l'ultimo aggiornamento.

ESEC_PROTOCOL_REFERENCE_RPT_V

La vista fa riferimento alla tabella ESEC_PROTOCOL_REFERENCE in cui sono memorizzati i numeri di protocollo assegnati in base a standard di settore.

Nome colonna	Tipo di dati	Commento
PROTOCOL_NUMBER	INT	Per http://www.iana.org/assignments/protocol-numbers, identificatori numerici utilizzati per rappresentare i protocolli incapsulati in un pacchetto IP.
PROTOCOL_KEYWORD	VARCHAR(64)	Per http://www.iana.org/assignments/protocol-numbers, parola chiave utilizzata per rappresentare i protocolli incapsulati in un pacchetto IP.
PROTOCOL_DESCRIPTION	VARCHAR(512)	Descrizione del protocollo del pacchetto IP.
DATE_CREATED	DATETIME	Data di inserimento.
DATE_MODIFIED	DATETIME	Data dell'ultimo aggiornamento.
CREATED_BY	INT	ID dell'utente che ha eseguito l'inserimento.
MODIFIED_BY	INT	ID dell'utente che ha eseguito l'ultimo aggiornamento.

ESEC_SEQUENCE _RPT_V

La vista fa riferimento alla tabella ESEC_SEQUENCE, utilizzata per generare numeri di sequenza con chiave primaria per le tabelle di Sentinel.

Nome colonna	Tipo di dati	Commento
TABLE_NAME	VARCHAR(32)	Nome della tabella.
COLUMN_NAME	VARCHAR(32)	Nome della colonna
SEED	INT	Valore corrente del campo chiave primaria.
DATE_CREATED	DATETIME	Data di inserimento.
DATE_MODIFIED	DATETIME	Data dell'ultimo aggiornamento.
CREATED_BY	INT	ID dell'utente che ha eseguito l'inserimento.
MODIFIED_BY	INT	ID dell'utente che ha eseguito l'ultimo aggiornamento.

EVENTS_ALL_RPT_V (fornita a scopo di compatibilità con versioni precedenti)

La vista contiene eventi presenti e passati (importati da archivi).

Nome colonna	Tipo di dati	Commento
EVENT_ID	uniqueidentifier	Identificatore dell'evento
RESOURCE_NAME	varchar(255)	Nome della risorsa
SUB_RESOURCE	varchar(255)	Nome della sottorisorsa
SEVERITY	int	Gravità dell'evento

Nome colonna	Tipo di dati	Commento
EVENT_PARSE_TIME	datetime	Ora dell'evento
EVENT_DATETIME	datetime	Ora dell'evento
BASE_MESSAGE	varchar(4000)	Messaggio base
EVENT_NAME	varchar(255)	Nome dell'evento riportato dal sensore
EVENT_TIME	varchar(255)	Ora dell'evento riportata dal sensore
SENSOR_NAME	varchar(255)	Nome del sensore
SENSOR_TYPE	varchar(5)	Tipo di sensore: H – basato sull'host N – basato sulla rete V – virus O – altro
PROTOCOL	varchar(255)	Nome del protocollo
SOURCE_IP	int	Indirizzo IP di origine in formato numerico
SOURCE_HOST_NAME	varchar(255)	Nome dell'host di origine
SOURCE_PORT	varchar(32)	Porta di origine
DESTINATION_IP	int	Indirizzo IP di destinazione in formato numerico
DESTINATION_HOST_NAME	varchar(255)	Nome dell'host di destinazione
DESTINATION_PORT	varchar(32)	Porta di destinazione
SOURCE_USER_NAME	varchar(255)	Nome dell'utente di origine
DESTINATION_USER_NAME	varchar(255)	Nome dell'utente di destinazione
FILE_NAME	varchar(1000)	Nome file
EXTENDED_INFO	varchar(1000)	Informazioni estese
REPORT_NAME	varchar(255)	Nome dell'autore del rapporto
PRODUCT_NAME	varchar(255)	Nome del prodotto per la generazione di rapporti
CUSTOM_TAG_1	varchar(255)	Tag cliente 1
CUSTOM_TAG 2	varchar(255)	Tag cliente 2
CUSTOM_TAG 3	int	Tag cliente 3
RESERVED_TAG_1	VARCHAR(255)	Tag riservato 1 Riservato all'uso futuro da parte di Sentinel. Questo campo viene utilizzato per le informazioni di Advisor relative alle descrizioni degli attacchi.
RESERVED_TAG_2	varchar(255)	Riservato all'uso futuro da parte di Sentinel. L'uso di questo campo per qualsiasi altro scopo può causare la sovrascrittura dei dati da parte di funzionalità future.

Nome colonna	Tipo di dati	Commento
RESERVED_TAG_3	int	Riservato all'uso futuro da parte di Sentinel. L'uso di questo campo per qualsiasi altro scopo può causare la sovrascrittura dei dati da parte di funzionalità future.
SOURCE_UUID	uniqueidentifier	UUID di origine
PORT	varchar(64)	Porta del servizio di raccolta
AGENT	varchar(64)	Nome servizio di raccolta
VULNERABILITY_RATING	int	Classificazione della vulnerabilità
CRITICALITY_RATING	int	Classificazione della criticità
DATE_CREATED	datetime	Data di inserimento
DATE_MODIFIED	datetime	Data dell'ultimo aggiornamento
CREATED_BY	int	ID dell'utente che ha eseguito l'inserimento.
MODIFIED_BY	int	ID dell'utente che ha eseguito l'ultimo aggiornamento.
RV01 - 10	INT	Valore riservato 1 - 10 Riservato all'uso futuro da parte di Sentinel. L'uso di questo campo per qualsiasi altro scopo può causare la sovrascrittura dei dati da parte di funzionalità future.
RV11 - 20	DATETIME	Valore riservato 11 - 20 Riservato all'uso futuro da parte di Sentinel. L'uso di questo campo per qualsiasi altro scopo può causare la sovrascrittura dei dati da parte di funzionalità future.
RV21 - 25	uniqueidentifier	Valore riservato 21 - 25 Riservato all'uso futuro da parte di Sentinel per la memorizzazione di UUID. L'uso di questo campo per qualsiasi altro scopo può causare la sovrascrittura dei dati da parte di funzionalità future.
RV26 - 31	VARCHAR(255)	Valore riservato 26 - 31 Riservato all'uso futuro da parte di Sentinel. L'uso di questo campo per qualsiasi altro scopo può causare la sovrascrittura dei dati da parte di funzionalità future.

Nome colonna	Tipo di dati	Commento
RV32	VARCHAR(255)	Valore riservato 32 Riservato a DeviceCategory L'uso di questo campo per qualsiasi altro scopo può causare la sovrascrittura dei dati da parte di funzionalità future.
RV33	VARCHAR(255)	Valore riservato 33 Riservato a EventContex L'uso di questo campo per qualsiasi altro scopo può causare la sovrascrittura dei dati da parte di funzionalità future.
RV34	VARCHAR(255)	Valore riservato 34 Riservato a SourceThreatLevel L'uso di questo campo per qualsiasi altro scopo può causare la sovrascrittura dei dati da parte di funzionalità future.
RV35	VARCHAR(255)	Valore riservato 35 Riservato a SourceUserContext. L'uso di questo campo per qualsiasi altro scopo può causare la sovrascrittura dei dati da parte di funzionalità future.
RV36	VARCHAR(255)	Valore riservato 36 Riservato a DataContext. L'uso di questo campo per qualsiasi altro scopo può causare la sovrascrittura dei dati da parte di funzionalità future.
RV37	VARCHAR(255)	Valore riservato 37 Riservato a SourceFunction. L'uso di questo campo per qualsiasi altro scopo può causare la sovrascrittura dei dati da parte di funzionalità future.

Nome colonna	Tipo di dati	Commento
RV38	VARCHAR(255)	Valore riservato 38 Riservato a SourceOperationalContext. L'uso di questo campo per qualsiasi altro scopo può causare la sovrascrittura dei dati da parte di funzionalità future.
RV39	VARCHAR(255)	Valore riservato 39 Riservato a MSSPCustomerName. L'uso di questo campo per qualsiasi altro scopo può causare la sovrascrittura dei dati da parte di funzionalità future.
RV40 - 43	VARCHAR(255)	Valore riservato 40 - 43 Riservato all'uso futuro da parte di Sentinel. L'uso di questo campo per qualsiasi altro scopo può causare la sovrascrittura dei dati da parte di funzionalità future.
RV44	VARCHAR(255)	Valore riservato 44 Riservato a DestinationThreatLevel. L'uso di questo campo per qualsiasi altro scopo può causare la sovrascrittura dei dati da parte di funzionalità future.
RV45	VARCHAR(255)	Valore riservato 45 Riservato a DestinationUserContext. L'uso di questo campo per qualsiasi altro scopo può causare la sovrascrittura dei dati da parte di funzionalità future.
RV46	VARCHAR(255)	Valore riservato 46 Riservato a VirusStatus. L'uso di questo campo per qualsiasi altro scopo può causare la sovrascrittura dei dati da parte di funzionalità future.

Nome colonna	Tipo di dati	Commento
RV47	VARCHAR(255)	Valore riservato 47 Riservato all'uso futuro da parte di Sentinel. L'uso di questo campo per qualsiasi altro scopo può causare la sovrascrittura dei dati da parte di funzionalità future.
RV48	VARCHAR(255)	Valore riservato 48 Riservato a DestinationOperationalContext. L'uso di questo campo per qualsiasi altro scopo può causare la sovrascrittura dei dati da parte di funzionalità future.
RV49	VARCHAR(255)	Valore riservato 49 Riservato all'uso futuro da parte di Sentinel. L'uso di questo campo per qualsiasi altro scopo può causare la sovrascrittura dei dati da parte di funzionalità future.
RV50	VARCHAR(255)	Livello di tassonomia 1
RV51	VARCHAR(255)	Livello di tassonomia 2
RV52	VARCHAR(255)	Livello di tassonomia 3
RV53	VARCHAR(255)	Livello di tassonomia 4
CV01 - 10	INT	Valore personalizzato 1 - 10 Riservato all'uso da parte del cliente, in genere per l'associazione di dati aziendali rilevanti
CV11 - 20	DATETIME	Valore personalizzato 11 - 20 Riservato all'uso da parte del cliente, in genere per l'associazione di dati aziendali rilevanti
CV21 - 100	VARCHAR(255)	Valore personalizzato 21 - 100 Riservato all'uso da parte del cliente, in genere per l'associazione di dati aziendali rilevanti

EVENTS_ALL_RPT_V1 (fornita a scopo di compatibilità con versioni precedenti)

La vista contiene eventi correnti. Include le stesse colonne di EVENT_ALL_RPT_V.

EVENTS_RPT_V (fornita a scopo di compatibilità con versioni precedenti)

La vista contiene eventi presenti e passati. Include le stesse colonne di EVENT_ALL_RPT_V.

EVENTS_RPT_V1 (fornita a scopo di compatibilità con versioni precedenti)

La vista contiene eventi correnti. Include le stesse colonne di EVENT_ALL_RPT_V.

EVENTS_RPT_V2 (fornita a scopo di compatibilità con versioni precedenti)

La vista contiene eventi presenti e passati.

Nome colonna	Tipo di dati	Commento
EVENT_ID	uniqueidentifier	Identificatore dell'evento
RESOURCE_NAME	varchar(255)	Nome della risorsa
SUB_RESOURCE	varchar(255)	Nome della sottorisorsa
SEVERITY	int	Gravità dell'evento
EVENT_PARSE_TIME	datetime	Ora dell'evento
EVENT_DATETIME	datetime	Ora dell'evento
BASE_MESSAGE	varchar(4000)	Messaggio base
EVENT_NAME	varchar(255)	Nome dell'evento riportato dal sensore
EVENT_TIME	varchar(255)	Ora dell'evento riportata dal sensore
TAXONOMY_ID	bigint	Identificatore della tassonomia
PROTOCOL_ID	bigint	Identificatore del prodotto
AGENT_ID	bigint	Identificatore del servizio di raccolta
SOURCE_IP	int	Indirizzo IP di origine in formato numerico
SOURCE_HOST_NAME	varchar(255)	Nome dell'host di origine
SOURCE_PORT	varchar(32)	Porta di origine
DESTINATION_IP	int	Indirizzo IP di destinazione in formato numerico
DESTINATION_HOST_NAME	varchar(255)	Nome dell'host di destinazione
DESTINATION_PORT	varchar(32)	Porta di destinazione
SOURCE_USER_NAME	varchar(255)	Nome dell'utente di origine
DESTINATION_USER_NAME	varchar(255)	Nome dell'utente di destinazione
FILE_NAME	varchar(1000)	Nome file
EXTENDED_INFO	varchar(1000)	Informazioni estese
CUSTOM_TAG_1	varchar(255)	Tag cliente 1
CUSTOM_TAG 2	varchar(255)	Tag cliente 2
CUSTOM_TAG 3	int	Tag cliente 3

Nome colonna	Tipo di dati	Commento
RESERVED_TAG_1	VARCHAR(255)	Tag riservato 1 Riservato all'uso futuro da parte di Sentinel. Questo campo viene utilizzato per le informazioni di Advisor relative alle descrizioni degli attacchi.
RESERVED_TAG_2	varchar(255)	Riservato all'uso futuro da parte di Sentinel. L'uso di questo campo per qualsiasi altro scopo può causare la sovrascrittura dei dati da parte di funzionalità future.
RESERVED_TAG_3	int	Riservato all'uso futuro da parte di Sentinel. L'uso di questo campo per qualsiasi altro scopo può causare la sovrascrittura dei dati da parte di funzionalità future.
VULNERABILITY_RATING	int	Classificazione della vulnerabilità
CRITICALITY_RATING	int	Classificazione della criticità
DATE_CREATED	datetime	Data di inserimento
DATE_MODIFIED	datetime	Data dell'ultimo aggiornamento
CREATED_BY	int	ID dell'utente che ha eseguito l'inserimento.
MODIFIED_BY	int	ID dell'utente che ha eseguito l'ultimo aggiornamento.
RV01 - 10	INT	Valore riservato 1 - 10 Riservato all'uso futuro da parte di Sentinel. L'uso di questo campo per qualsiasi altro scopo può causare la sovrascrittura dei dati da parte di funzionalità future.
RV11 - 20	DATETIME	Valore riservato 1 - 31 Riservato all'uso futuro da parte di Sentinel. L'uso di questo campo per qualsiasi altro scopo può causare la sovrascrittura dei dati da parte di funzionalità future.
RV21 - 25	uniqueidentifier	Valore riservato 21 - 25 Riservato all'uso futuro da parte di Sentinel per la memorizzazione di UUID. L'uso di questo campo per qualsiasi altro scopo può causare la sovrascrittura dei dati da parte di funzionalità future.

Nome colonna	Tipo di dati	Commento
RV26 - 31	VARCHAR(255)	Valore riservato 26 - 31 Riservato all'uso futuro da parte di Sentinel. L'uso di questo campo per qualsiasi altro scopo può causare la sovrascrittura dei dati da parte di funzionalità future.
RV33	VARCHAR(255)	Valore riservato 33 Riservato a EventContex L'uso di questo campo per qualsiasi altro scopo può causare la sovrascrittura dei dati da parte di funzionalità future.
RV34	VARCHAR(255)	Valore riservato 34 Riservato a SourceThreatLevel L'uso di questo campo per qualsiasi altro scopo può causare la sovrascrittura dei dati da parte di funzionalità future.
RV35	VARCHAR(255)	Valore riservato 35 Riservato a SourceUserContext. L'uso di questo campo per qualsiasi altro scopo può causare la sovrascrittura dei dati da parte di funzionalità future.
RV36	VARCHAR(255)	Valore riservato 36 Riservato a DataContext. L'uso di questo campo per qualsiasi altro scopo può causare la sovrascrittura dei dati da parte di funzionalità future.
RV37	VARCHAR(255)	Valore riservato 37 Riservato a SourceFunction. L'uso di questo campo per qualsiasi altro scopo può causare la sovrascrittura dei dati da parte di funzionalità future.
RV38	VARCHAR(255)	Valore riservato 38 Riservato a SourceOperationalContext. L'uso di questo campo per qualsiasi altro scopo può causare la sovrascrittura dei dati da parte di funzionalità future.

Nome colonna	Tipo di dati	Commento
RV40 - 43	VARCHAR(255)	Valore riservato 40 - 43 Riservato all'uso futuro da parte di Sentinel. L'uso di questo campo per qualsiasi altro scopo può causare la sovrascrittura dei dati da parte di funzionalità future.
RV44	VARCHAR(255)	Valore riservato 44 Riservato a DestinationThreatLevel. L'uso di questo campo per qualsiasi altro scopo può causare la sovrascrittura dei dati da parte di funzionalità future.
RV45	VARCHAR(255)	Valore riservato 45 Riservato a DestinationUserContext. L'uso di questo campo per qualsiasi altro scopo può causare la sovrascrittura dei dati da parte di funzionalità future.
RV46	VARCHAR(255)	Valore riservato 46 Riservato a VirusStatus. L'uso di questo campo per qualsiasi altro scopo può causare la sovrascrittura dei dati da parte di funzionalità future.
RV47	VARCHAR(255)	Valore riservato 47 Riservato all'uso futuro da parte di Sentinel. L'uso di questo campo per qualsiasi altro scopo può causare la sovrascrittura dei dati da parte di funzionalità future.
RV48	VARCHAR(255)	Valore riservato 48 Riservato a DestinationOperationalContext. L'uso di questo campo per qualsiasi altro scopo può causare la sovrascrittura dei dati da parte di funzionalità future.
RV49	VARCHAR(255)	Valore riservato 49 Riservato all'uso futuro da parte di Sentinel. L'uso di questo campo per qualsiasi altro scopo può causare la sovrascrittura dei dati da parte di funzionalità future.

Nome colonna	Tipo di dati	Commento
REFERENCE_ID 01 - 20	BIGINT	Riservato all'uso futuro da parte di Sentinel. L'uso di questo campo per qualsiasi altro scopo può causare la sovrascrittura dei dati da parte di funzionalità future.
CV01 - 10	INT	Valore personalizzato 1 - 10 Riservato all'uso da parte del cliente, in genere per l'associazione di dati aziendali rilevanti
CV11 - 20	DATETIME	Valore personalizzato 11 - 20 Riservato all'uso da parte del cliente, in genere per l'associazione di dati aziendali rilevanti
CV21 - 100	VARCHAR(255)	Valore personalizzato 21 - 100 Riservato all'uso da parte del cliente, in genere per l'associazione di dati aziendali rilevanti

EVT_AGENT_RPT_V

La vista fa riferimento alla tabella EVT_AGENT in cui sono memorizzate informazioni sui servizi di raccolta.

Nome colonna	Tipo di dati	Commento
AGENT_ID	bigint	Identificatore del servizio di raccolta
AGENT	varchar(64)	Nome servizio di raccolta
PORT	varchar(64)	Porta del servizio di raccolta
REPORT_NAME	varchar(255)	Nome dell'autore del rapporto
PRODUCT_NAME	varchar(255)	Nome del prodotto
SENSOR_NAME	varchar(255)	Nome del sensore
SENSOR_TYPE	varchar(5)	Tipo di sensore: H - basato sull'host N - basato sulla rete V - virus O - altro
DEVICE_CTGRY	varchar(255)	Categoria del dispositivo
SOURCE_UUID	uniqueidentifier	UUID (Universal Unique Identifier) del componente di origine
DATE_CREATED	datetime	Data di inserimento
DATE_MODIFIED	datetime	Data dell'ultimo aggiornamento
CREATED_BY	int	ID dell'utente che ha eseguito l'inserimento.
MODIFIED_BY	int	ID dell'utente che ha eseguito l'ultimo aggiornamento.

EVT_ASSET_RPT_V

La vista fa riferimento alla tabella EVT_ASSET in cui sono memorizzate informazioni sulle risorse.

Nome colonna	Tipo di dati	Commento
EVENT_ASSET_ID	bigint	Identificatore della risorsa dell'evento
ASSET_NAME	varchar(255)	Nome della risorsa
PHYSICAL_ASSET_NAME	varchar(255)	Nome della risorsa fisica
REFERENCE_ASSET_ID	varchar(100)	Identificatore della risorsa di riferimento, collega al sistema di gestione delle risorse di origine.
MAC_ADDRESS	varchar(100)	Indirizzo MAC
RACK_NUMBER	varchar(50)	Numero del rack
ROOM_NAME	varchar(100)	Nome della stanza
BUILDING_NAME	varchar(255)	Nome dell'edificio
CITY	varchar(100)	Città
STATE	varchar(100)	Stato
COUNTRY	varchar(100)	Paese
ZIP_CODE	varchar(50)	CAP
ASSET_CATEGORY_NAME	varchar(100)	Nome della categoria della risorsa
NETWORK_IDENTITY_NAME	varchar(255)	Nome dell'identità di rete della risorsa
ENVIRONMENT_IDENTITY_ NAME	varchar(255)	Nome dell'ambiente
ASSET_VALUE_NAME	varchar(50)	Nome del valore della risorsa
CRITICALITY_NAME	varchar(50)	Nome della criticità della risorsa
SENSITIVITY_NAME	varchar(50)	Nome della riservatezza della risorsa
CONTACT_NAME_1	varchar(255)	Nome della persona/organizzazione di contatto 1
CONTACT_NAME_2	varchar(255)	Nome della persona/organizzazione di contatto 2
ORGANIZATION_NAME_1	varchar(100)	Livello dell'organizzazione proprietaria delle risorse 1
ORGANIZATION_NAME_2	varchar(100)	Livello dell'organizzazione proprietaria delle risorse 2
ORGANIZATION_NAME_3	varchar(100)	Livello dell'organizzazione proprietaria delle risorse 3
ORGANIZATION_NAME_4	varchar(100)	Livello dell'organizzazione proprietaria delle risorse 4
DATE_CREATED	datetime	Data di inserimento
DATE_MODIFIED	datetime	Data dell'ultimo aggiornamento
CREATED_BY	int	ID dell'utente che ha eseguito l'inserimento.
MODIFIED_BY	int	ID dell'utente che ha eseguito l'ultimo aggiornamento.

EVT_DEST_EVT_NAME_SMRY_1_RPT_V

La vista riepiloga il numero di eventi per destinazione, tassonomia, gravità, nome e ora dell'evento.

Nome colonna	Tipo di dati	Commento
DESTINATION_IP	int	Indirizzo IP di destinazione
DESTINATION_EVENT_ASSET_ID	bigint	Identificatore della risorsa dell'evento
TAXONOMY_ID	bigint	Identificatore della tassonomia
EVENT_NAME_ID	bigint	Identificatore del nome dell'evento
SEVERITY	int	Gravità dell'evento
CUSTOMER_ID	bigint	Identificatore del cliente
EVT_TIME	datetime	Ora dell'evento
EVT_COUNT	int	Numero di eventi
DATE_CREATED	datetime	Data di inserimento
DATE_MODIFIED	datetime	Data dell'ultimo aggiornamento
CREATED_BY	int	ID dell'utente che ha eseguito l'inserimento.
MODIFIED_BY	int	ID dell'utente che ha eseguito l'ultimo aggiornamento.

EVT_DEST_SMRY_1_RPT_V

La vista contiene informazioni di riepilogo sulle destinazioni degli eventi.

Nome colonna	Tipo di dati	Commento
DESTINATION_IP	int	Indirizzo IP di destinazione
DESTINATION_EVENT_ASSET_ID	bigint	Identificatore della risorsa dell'evento
DESTINATION_PORT	varchar(32)	Porta di destinazione
DESTINATION_USR_ID	bigint	Identificatore dell'utente di destinazione
TAXONOMY_ID	bigint	Identificatore della tassonomia
EVENT_NAME_ID	bigint	Identificatore del nome dell'evento
RESOURCE_ID	bigint	Identificatore della risorsa
AGENT_ID	bigint	Identificatore del servizio di raccolta
PROTOCOL_ID	bigint	Identificatore del prodotto
SEVERITY	int	Gravità dell'evento
CUSTOMER_ID	bigint	Identificatore del cliente
EVENT_TIME	datetime	Ora dell'evento
EVENT_COUNT	int	Numero di eventi
DATE_CREATED	datetime	Data di inserimento
DATE_MODIFIED	datetime	Data dell'ultimo aggiornamento
CREATED_BY	int	ID dell'utente che ha eseguito l'inserimento.
MODIFIED_BY	int	ID dell'utente che ha eseguito l'ultimo aggiornamento.

EVT_DEST_TXNMY_SMRY_1_RPT_V

La vista riepiloga il numero di eventi per destinazione, tassonomia, gravità e ora dell'evento.

Nome colonna	Tipo di dati	Commento
DESTINATION_IP	int	Indirizzo IP di destinazione
DESTINATION_EVENT_ASSET_ID	bigint	Identificatore della risorsa dell'evento
TAXONOMY_ID	bigint	Identificatore della tassonomia
SEVERITY	int	Gravità dell'evento
CUSTOMER_ID	bigint	Identificatore del cliente
EVENT_TIME	datetime	Ora dell'evento
EVENT_COUNT	int	Numero di eventi
DATE_CREATED	datetime	Data di inserimento
DATE_MODIFIED	datetime	Data dell'ultimo aggiornamento
CREATED_BY	int	ID dell'utente che ha eseguito l'inserimento.
MODIFIED_BY	int	ID dell'utente che ha eseguito l'ultimo aggiornamento.

EVT_NAME_RPT_V

La vista fa riferimento alla tabella EVT_NAME in cui sono memorizzate informazioni sui nomi degli eventi.

Nome colonna	Tipo di dati	Commento
EVENT_NAME_ID	bigint	Identificatore del nome dell'evento
EVENT_NAME	varchar(255)	Nome dell'evento
DATE_CREATED	datetime	Data di inserimento
DATE_MODIFIED	datetime	Data dell'ultimo aggiornamento
CREATED_BY	int	ID dell'utente che ha eseguito l'inserimento.
MODIFIED_BY	int	ID dell'utente che ha eseguito l'ultimo aggiornamento.

EVT_PORT_SMRY_1_RPT_V

La vista riepiloga il numero di eventi per porta di destinazione, gravità e ora dell'evento.

Nome colonna	Tipo di dati	Commento
DESTINATION_PORT	Varchar(32)	Porta di destinazione
SEVERITY	int	Gravità dell'evento
CUSTOMER_ID	bigint	Identificatore del cliente
EVENT_TIME	datetime	Ora dell'evento
EVENT_COUNT	int	Numero di eventi
DATE_CREATED	datetime	Data di inserimento
DATE_MODIFIED	datetime	Data dell'ultimo aggiornamento
CREATED_BY	int	ID dell'utente che ha eseguito l'inserimento.
MODIFIED_BY	int	ID dell'utente che ha eseguito l'ultimo aggiornamento.

EVT_PRTCL_RPT_V

La vista fa riferimento alla tabella EVT_PRTCL in cui sono memorizzate informazioni sui protocolli degli eventi.

Nome colonna	Tipo di dati	Commento
PROTOCOL_ID	bigint	Identificatore del prodotto
PROTOCOL_NAME	varchar(255)	Nome del protocollo
DATE_CREATED	datetime	Data di inserimento
DATE_MODIFIED	datetime	Data dell'ultimo aggiornamento
CREATED_BY	int	ID dell'utente che ha eseguito l'inserimento.
MODIFIED_BY	int	ID dell'utente che ha eseguito l'ultimo aggiornamento.

EVT_RSRC_RPT_V

La vista fa riferimento alla tabella EVT_RSRC in cui sono memorizzate informazioni sulle risorse degli eventi.

Nome colonna	Tipo di dati	Commento
RESOURCE_ID	bigint	Identificatore della risorsa
RESOURCE_NAME	varchar(255)	Nome della risorsa
SUB_RESOURCE_NAME	varchar(255)	Nome della sottorisorsa
DATE_CREATED	datetime	Data di inserimento
DATE_MODIFIED	datetime	Data dell'ultimo aggiornamento
CREATED_BY	int	ID dell'utente che ha eseguito l'inserimento.
MODIFIED_BY	int	ID dell'utente che ha eseguito l'ultimo aggiornamento.

EVT_SEV_SMRY_1_RPT_V

La vista riepiloga il numero di eventi per gravità e ora dell'evento.

Nome colonna	Tipo di dati	Commento
SEVERITY	int	Gravità dell'evento
CUSTOMER_ID	bigint	Identificatore del cliente
EVENT_TIME	datetime	Ora dell'evento
EVENT_COUNT	int	Numero di eventi
DATE_CREATED	datetime	Data di inserimento
DATE_MODIFIED	datetime	Data dell'ultimo aggiornamento
CREATED_BY	int	ID dell'utente che ha eseguito l'inserimento.
MODIFIED_BY	int	ID dell'utente che ha eseguito l'ultimo aggiornamento.

EVT_SRC_SMRY_1_RPT_V

La vista contiene informazioni di riepilogo sulle destinazioni e le origini degli eventi.

Nome colonna	Tipo di dati	Commento
SOURCE_IP	int	Indirizzo IP di origine
SOURCE_EVENT_ASSET_ID	bigint	Identificatore della risorsa dell'evento
SOURCE_PORT	varchar(32)	Porta di origine
SOURCE_USER_ID	bigint	Identificatore dell'utente
TAXONOMY_ID	bigint	Identificatore della tassonomia
EVENT_NAME_ID	bigint	Identificatore del nome dell'evento
RESOURCE_ID	bigint	Identificatore della risorsa
AGENT_ID	bigint	Identificatore del servizio di raccolta
PROTOCOL _ID	bigint	Identificatore del prodotto
SEVERITY	int	Gravità dell'evento
CUSTOMER_ID	bigint	Identificatore del cliente
EVENT_TIME	datetime	Ora dell'evento
EVENT_COUNT	int	Numero di eventi
DATE_CREATED	datetime	Data di inserimento
DATE_MODIFIED	datetime	Data dell'ultimo aggiornamento
CREATED_BY	int	ID dell'utente che ha eseguito l'inserimento.
MODIFIED_BY	int	ID dell'utente che ha eseguito l'ultimo aggiornamento.

EVT_TXNMY_RPT_V

La vista fa riferimento alla tabella EVT_TXNMY in cui sono memorizzate informazioni sulla tassonomia degli eventi.

Nome colonna	Tipo di dati	Commento
TAXONOMY_ID	bigint	Identificatore della tassonomia
TAXONOMY _ LEVEL _1	varchar(100)	Livello di tassonomia 1
TAXONOMY _ LEVEL _2	varchar(100)	Livello di tassonomia 2
TAXONOMY _ LEVEL _3	varchar(100)	Livello di tassonomia 3
TAXONOMY _ LEVEL _4	varchar(100)	Livello di tassonomia 4
DATE_CREATED	datetime	Data di inserimento
DATE_MODIFIED	datetime	Data dell'ultimo aggiornamento
CREATED_BY	int	ID dell'utente che ha eseguito l'inserimento.
MODIFIED_BY	int	ID dell'utente che ha eseguito l'ultimo aggiornamento.
TAXONOMY_ID	bigint	Identificatore della tassonomia

EVT_USR_RPT_V

La vista fa riferimento alla tabella EVT_USR in cui sono memorizzate informazioni sugli utenti degli eventi.

Nome colonna	Tipo di dati	Commento
USER_ID	bigint	Identificatore dell'utente
USER_NAME	varchar(255)	Nome utente
DATE_CREATED	datetime	Data di inserimento

Nome colonna	Tipo di dati	Commento
DATE_MODIFIED	datetime	Data dell'ultimo aggiornamento
CREATED_BY	int	ID dell'utente che ha eseguito l'inserimento.
MODIFIED_BY	int	ID dell'utente che ha eseguito l'ultimo aggiornamento.
USER_ID	bigint	Identificatore dell'utente

EXTERNAL_DATA_RPT_V

La vista fa riferimento alla tabella EXTERNAL_DATA in cui sono memorizzati dati esterni.

Nome colonna	Tipo di dati	Commento
EXTERNAL_DATA_ID	int	Identificatore dei dati esterni
SOURCE_NAME	varchar(50)	Nome dell'origine
SOURCE_DATA_ID	varchar(255)	Identificatore dei dati di origine
EXTERNAL_DATA	testo	Dati esterni
EXTERNAL_DATA_TYPE	varchar(10)	Tipo dei dati esterni
DATE_CREATED	datetime	Data di inserimento
DATE_MODIFIED	datetime	Data dell'ultimo aggiornamento
CREATED_BY	int	ID dell'utente che ha eseguito l'inserimento.
MODIFIED_BY	int	ID dell'utente che ha eseguito l'ultimo aggiornamento.

HIST_EVENTS_RPT_V

Vista di eventi cronologici (ripristinati da archivi).

HIST_INCIDENTS_RPT_V

Vista di casi cronologici (ripristinati da archivi).

IMAGES_RPT_V

La vista fa riferimento alla tabella IMAGES in cui sono memorizzate informazioni sulle immagini di panoramica del sistema.

Nome colonna	Tipo di dati	Commento
NAME	VARCHAR(128)	Nome dell'immagine
TYPE	VARCHAR(64)	Tipo di immagine
DATA	TEXT	Data dell'immagine
DATE_CREATED	DATETIME	Data di inserimento
DATE_MODIFIED	DATETIME	Data dell'ultimo aggiornamento
CREATED_BY	INT	ID dell'utente che ha eseguito l'inserimento
MODIFIED_BY	INT	ID dell'utente che ha eseguito l'ultimo aggiornamento

INCIDENTS_ASSETS_RPT_V

La vista fa riferimento alla tabella INCIDENTS_ASSETS in cui sono memorizzate informazioni sulle risorse che costituiscono casi creati nella console Sentinel.

Nome colonna	Tipo di dati	Commento
INC_ID	INT	Identificatore del caso – numero di sequenza
ASSET_ID	uniqueidentifier	UUID (Universal Unique Identifier) della risorsa
DATE_CREATED	DATETIME	Data di inserimento
DATE_MODIFIED	DATETIME	Data dell'ultimo aggiornamento
CREATED_BY	INT	ID dell'utente che ha eseguito l'inserimento
MODIFIED_BY	INT	ID dell'utente che ha eseguito l'ultimo aggiornamento

INCIDENTS_EVENTS_RPT_V

La vista fa riferimento alla tabella INCIDENTS_EVENTS in cui sono memorizzate informazioni sugli eventi che costituiscono casi creati nella console Sentinel.

Nome colonna	Tipo di dati	Commento
INC_ID	INT	Identificatore del caso – numero di sequenza
EVT_ID	uniqueidentifier	UUID (Universal Unique Identifier) dell'evento
EVT_TIME	DATETIME	Ora dell'evento
DATE_CREATED	DATETIME	Data di inserimento
DATE_MODIFIED	DATETIME	Data dell'ultimo aggiornamento
CREATED_BY	INT	ID dell'utente che ha eseguito l'inserimento
MODIFIED_BY	INT	ID dell'utente che ha eseguito l'ultimo aggiornamento

INCIDENTS_RPT_V

La vista fa riferimento alla tabella INCIDENTS in cui sono memorizzate informazioni che descrivono i dettagli dei casi creati nella console Sentinel.

Nome colonna	Tipo di dati	Commento
INC_ID	INT	Identificatore del caso – numero di sequenza
NAME	VARCHAR(255)	Nome del caso
SEVERITY	INT	Gravità del caso
STT_ID	INT	ID dello stato del caso
SEVERITY_RATING	VARCHAR(32)	Media di tutte le gravità degli eventi che compongono un caso.

Nome colonna	Tipo di dati	Commento
VULNERABILITY_RATING	VARCHAR(32)	Riservato all'uso futuro da parte di Sentinel. L'uso di questo campo per qualsiasi altro scopo può causare la sovrascrittura dei dati da parte di funzionalità future.
CRITICALITY_RATING	VARCHAR(32)	Riservato all'uso futuro da parte di Sentinel. L'uso di questo campo per qualsiasi altro scopo può causare la sovrascrittura dei dati da parte di funzionalità future.
DATE_CREATED	DATETIME	Data di inserimento
DATE_MODIFIED	DATETIME	Data dell'ultimo aggiornamento
CREATED_BY	INT	ID dell'utente che ha eseguito l'inserimento
MODIFIED_BY	INT	ID dell'utente che ha eseguito l'ultimo aggiornamento
INC_DESC	varchar(4000)	Descrizione del caso
INC_PRIORITY	int	Priorità del caso
INC_CAT	varchar(255)	Categoria del caso
INC_RES	varchar(4000)	Risoluzione del caso

INCIDENTS_VULN_RPT_V

La vista fa riferimento alla tabella INCIDENTS_VULN in cui sono memorizzate informazioni sulle vulnerabilità che costituiscono casi creati nella console Sentinel.

Nome colonna	Tipo di dati	Commento
INC_ID	INT	Identificatore del caso – numero di sequenza
VULN_ID	uniqueidentifier	UUID (Universal Unique Identifier) della vulnerabilità
DATE_CREATED	DATETIME	Data di inserimento
DATE_MODIFIED	DATETIME	Data dell'ultimo aggiornamento
CREATED_BY	INT	ID dell'utente che ha eseguito l'inserimento
MODIFIED_BY	INT	ID dell'utente che ha eseguito l'ultimo aggiornamento

L_STAT_RPT_V

La vista fa riferimento alla tabella L_STAT in cui sono memorizzate informazioni statistiche.

Nome colonna	Tipo di dati	Commento
RES_NAME	VARCHAR(32)	Nome della risorsa
STATS_NAME	VARCHAR(32)	Nome della statistica
STATS_VALUE	VARCHAR(32)	Valore della statistica
OPEN_TOT_SECS	NUMERIC	Numero di secondi a partire dal 1970.

LOGS_RPT_V

La vista fa riferimento alla tabella LOGS_RPT in cui sono memorizzate informazioni di registrazione.

Tabella LOGS		
Nome colonna	**Tipo di dati**	**Commento**
LOG_ID	NUMBER	Numero di sequenza
TIME	DATE	Data del log
MODULE	VARCHAR(64)	Modulo a cui si riferisce il log
TEXT	VARCHAR(4000)	Testo del log

NETWORK_IDENTITY_RPT_V

La vista fa riferimento alla tabella NETWORK_IDENTITY_LKUP in cui sono memorizzate informazioni sull'identità di rete delle risorse.

Nome colonna	Tipo di dati	Commento
NETWORK_IDENTITY_CD	varchar(5)	Codice dell'identità di rete
NETWORK_IDENTITY_NAME	varchar(255)	Nome di identificazione della rete
DATE_CREATED	datetime	Data di inserimento
DATE_MODIFIED	datetime	Data dell'ultimo aggiornamento
CREATED_BY	int	ID dell'utente che ha eseguito l'inserimento
MODIFIED_BY	int	ID dell'utente che ha eseguito l'ultimo aggiornamento

ORGANIZATION_RPT_V

La vista fa riferimento alla tabella ORGANIZATION in cui sono memorizzate informazioni sull'organizzazione (risorsa).

Nome colonna	Tipo di dati	Commento
ORGANIZATION_ID	uniqueidentifier	Identificatore dell'organizzazione
ORGANIZATION_NAME	varchar(100)	Nome dell'organizzazione
CUSTOMER_ID	bigint	Identificatore del cliente
DATE_CREATED	datetime	Data di inserimento
DATE_MODIFIED	datetime	Data dell'ultimo aggiornamento
CREATED_BY	int	ID dell'utente che ha eseguito l'inserimento
MODIFIED_BY	int	ID dell'utente che ha eseguito l'ultimo aggiornamento

PERSON_RPT_V

La vista fa riferimento alla tabella PERSION in cui sono memorizzate informazioni personali (risorsa).

Nome colonna	Tipo di dati	Commento
PERSON_ID	uniqueidentifier	Identificatore della persona
FIRST_NAME	varchar(255)	Nome
LAST_NAME	varchar(255)	Cognome
CUSTOMER_ID	bigint	Identificatore del cliente

Nome colonna	Tipo di dati	Commento
PHONE_NUMBER	varchar(50)	Numero di telefono
EMAIL_ADDRESS	varchar(255)	Indirizzo e-mail
DATE_CREATED	datetime	Data di inserimento
DATE_MODIFIED	datetime	Data dell'ultimo aggiornamento
CREATED_BY	int	ID dell'utente che ha eseguito l'inserimento
MODIFIED_BY	int	ID dell'utente che ha eseguito l'ultimo aggiornamento

PHYSICAL_ASSET_RPT_V

La vista fa riferimento alla tabella PHYSICAL_ASSET in cui sono memorizzate informazioni sulle risorse fisiche.

Nome colonna	Tipo di dati	Commento
PHYSICAL_ASSET_ID	uniqueidentifier	Identificatore della risorsa fisica
CUSTOMER_ID	int	Identificatore del cliente
LOCATION_ID	bigint	Identificatore dell'ubicazione
HOST_NAME	varchar(255)	Nome host
IP_ADDRESS	int	Indirizzo IP
NETWORK_IDENTITY_CD	varchar(5)	Codice dell'identità di rete
MAC_ADDRESS	varchar(100)	Indirizzo MAC
RACK_NUMBER	varchar(50)	Numero del rack
ROOM_NAME	varchar(100)	Nome della stanza
DATE_CREATED	datetime	Data di inserimento
DATE_MODIFIED	datetime	Data dell'ultimo aggiornamento
CREATED_BY	int	ID dell'utente che ha eseguito l'inserimento
MODIFIED_BY	int	ID dell'utente che ha eseguito l'ultimo aggiornamento

PRODUCT_RPT_V

La vista fa riferimento alla tabella PRDT in cui sono memorizzate informazioni sui prodotti delle risorse.

Nome colonna	Tipo di dati	Commento
PRODUCT _ID	bigint	Identificatore del prodotto
PRODUCT _NAME	varchar(255)	Nome del prodotto
PRODUCT _VERSION	varchar(100)	Versione del prodotto
VENDOR _ID	bigint	Identificatore del produttore
DATE_CREATED	datetime	Data di inserimento
DATE_MODIFIED	datetime	Data dell'ultimo aggiornamento
CREATED_BY	int	ID dell'utente che ha eseguito l'inserimento
MODIFIED_BY	int	ID dell'utente che ha eseguito l'ultimo aggiornamento

ROLE_RPT_V

La vista fa riferimento alla tabella ROLE_LKUP in cui sono memorizzate informazioni sui ruoli utente (risorsa).

Nome colonna	Tipo di dati	Commento
ROLE_CODE	varchar(5)	Codice del ruolo
ROLE_NAME	varchar(255)	Nome del ruolo
DATE_CREATED	datetime	Data di inserimento
DATE_MODIFIED	datetime	Data dell'ultimo aggiornamento
CREATED_BY	int	ID dell'utente che ha eseguito l'inserimento
MODIFIED_BY	int	ID dell'utente che ha eseguito l'ultimo aggiornamento

SENSITIVITY_RPT_V

La vista fa riferimento alla tabella SENSITIVITY_LKUP in cui sono memorizzate informazioni sulla riservatezza delle risorse.

Nome colonna	Tipo di dati	Commento
SENSITIVITY_CODE	varchar(5)	Codice della riservatezza della risorsa
SENSITIVITY_NAME	varchar(50)	Nome della riservatezza della risorsa
DATE_CREATED	datetime	Data di inserimento
DATE_MODIFIED	datetime	Data dell'ultimo aggiornamento
CREATED_BY	int	ID utente
MODIFIED_BY	int	ID utente

STATES_RPT_V

La vista fa riferimento alla tabella STATES in cui sono memorizzate le definizioni degli stati definiti dalle applicazioni o dal contesto.

Nome colonna	Tipo di dati	Commento
STT_ID	INT	ID dello stato – numero di sequenza
CONTEXT	VARCHAR(64)	Contesto dello stato, ovvero situazione, caso, utente.
NAME	VARCHAR(64)	Nome dello stato.
TERMINAL_FLAG	VARCHAR(1)	Indica se lo stato del caso è risolto.
DATE_CREATED	DATETIME	Data di inserimento
DATE_MODIFIED	DATETIME	Data dell'ultimo aggiornamento
MODIFIED_BY	INT	ID dell'utente che ha eseguito l'inserimento
CREATED_BY	INT	ID dell'utente che ha eseguito l'ultimo aggiornamento

UNASSIGNED_INCIDENTS_RPT_V

La vista fa riferimento alle tabelle CASES e INCIDENTS per generare report relative a situazioni e casi non assegnati.

Nome	Tipo di dati
INC_ID	INT
NAME	VARCHAR(255)
SEVERITY	INT
STT_ID	INT
SEVERITY_RATING	VARCHAR(32)

Nome	Tipo di dati
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

La vista fa riferimento alla tabella USERS in cui sono elencati tutti gli utenti dell'applicazione. Gli utenti verranno creati anche come utenti di database per adattarsi agli strumenti di generazione di rapporti di terze parti.

Nome colonna	Tipo di dati	Commento
USR_ID	INT	Identificatore dell'utente – numero di sequenza
NAME	VARCHAR(64)	Breve nome utente univoco utilizzato come login
CNT_ID	INT	ID del contatto – numero di sequenza
STT_ID	INT	ID dello stato. Lo stato è attivo o inattivo.
DESCRIPTION	VARCHAR(512)	Commenti
DATE_CREATED	DATETIME	Data di inserimento
DATE_MODIFIED	DATETIME	Data dell'ultimo aggiornamento
CREATED_BY	INT	ID dell'utente che ha eseguito l'inserimento
MODIFIED_BY	INT	ID dell'utente che ha eseguito l'ultimo aggiornamento
PERMISSIONS	VARCHAR(4000)	Autorizzazioni attualmente assegnate all'utente Sentinel
FILTER	VARCHAR(128)	Filtro di sicurezza corrente assegnato all'utente Sentinel
UPPER_NAME	VARCHAR(64)	Nome utente al maiuscolo
DOMAIN_AUTH_IND	Bit	Indicazione dell'autenticazione di dominio

VENDOR_RPT_V

La vista fa riferimento alla tabella VNDR in cui sono memorizzate informazioni sui fornitori dei prodotti delle risorse.

Nome colonna	Tipo di dati	Commento
VENDOR_ID	bigint	Identificatore del produttore
VENDOR_NAME	varchar(255)	Nome del fornitore
DATE_CREATED	datetime	Data di inserimento
DATE_MODIFIED	datetime	Data dell'ultimo aggiornamento

Nome colonna	Tipo di dati	Commento
CREATED_BY	int	ID dell'utente che ha eseguito l'inserimento
MODIFIED_BY	int	ID dell'utente che ha eseguito l'ultimo aggiornamento

VULN_CALC_SEVERITY_RPT_V

La vista fa riferimento a VULN_RSRC e VULN per calcolare la classificazione della gravità della vulnerabilità di eSecurity in base alle vulnerabilità correnti.

Nome colonna	Tipo di dati
RSRC_ID	uniqueidentifier
IP	VARCHAR(32)
HOST_NAME	VARCHAR(255)
CRITICALITY	int
ASSIGNED_VULN_SEVERITY	int
VULN_COUNT	Numero di vulnerabilità per la risorsa specificata
CALC_SEVERITY	Gravità calcolata in base a ASSIGNED_VULN_SEVERITY e CRITICALITY

VULN_CODE_RPT_V

La vista fa riferimento alla tabella VULN_CODE in cui sono memorizzati i codici delle vulnerabilità assegnati in base a standard di settore.

Nome colonna	Tipo di dati
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

La vista fa riferimento alla tabella VULN_INFO in cui sono memorizzate informazioni aggiuntive riportate durante una scansione.

Nome colonna	Tipo di dati
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

La vista fa riferimento alla tabella VULN in cui sono memorizzate le informazioni del sistema sottoposto a scansione. Ogni scanner avrà una voce propria per ciascun sistema.

Nome colonna	Tipo di dati
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
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

La vista fa riferimento alla tabella VULN_RSRC in cui sono memorizzate tutte le risorse su cui è stata eseguita una particolare scansione.

Nome colonna	Tipo di dati
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

Nome colonna	Tipo di dati
REGULATION	VARCHAR(128)
REGULATION_RATING	VARCHAR(64)
DATE_CREATED	DATETIME
DATE_MODIFIED	DATETIME
CREATED_BY	INT
MODIFIED_BY	INT

VULN_RSRC_SCAN_RPT_V

La vista fa riferimento alla tabella VULN_RSRC_SCAN in cui sono memorizzate tutte le risorse su cui è stata eseguita una particolare scansione.

Nome colonna	Tipo di dati
RSRC_ID	VARCHAR(36)
SCAN_ID	VARCHAR(36)
DATE_CREATED	DATETIME
DATE_MODIFIED	DATETIME
CREATED_BY	INT
MODIFIED_BY	INT

VULN_SCAN_RPT_V

La vista fa riferimento alla tabella in cui sono memorizzate le informazioni relative alle scansioni.

Nome colonna	Tipo di dati
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

La vista fa riferimento alla tabella VULN_SCAN_VULN in cui sono memorizzate le vulnerabilità rilevate durante le scansioni.

Nome colonna	Tipo di dati
SCAN_ID	VARCHAR(36)
VULN_ID	VARCHAR(36)
DATE_CREATED	DATETIME
DATE_MODIFIED	DATETIME
CREATED_BY	INT
MODIFIED_BY	INT

VULN_SCANNER_RPT_V

La vista fa riferimento alla tabella VULN_SCANNER in cui sono memorizzate informazioni sugli scanner delle vulnerabilità.

Nome colonna	Tipo di dati
SCANNER_ID	VARCHAR(36)
PRODUCT_NAME	VARCHAR(100)
PRODUCT_VERSION	VARCHAR(64)
SCANNER_TYPE	VARCHAR(64)
VENDOR	VARCHAR(100)
SCANNER_INSTANCE	VARCHAR(64)
DATE_CREATED	DATETIME
DATE_MODIFIED	DATETIME
CREATED_BY	INT
MODIFIED_BY	INT

A Elenco di controllo per la soluzione dei problemi di Sentinel

NOTA: Il termine agente è equivalente a servizio di raccolta. Si farà in seguito riferimento agli agenti come servizi di raccolta.

L'elenco di controllo è un valido strumento per la diagnosi dei problemi. Una volta compilato, l'elenco consente di risolvere velocemente la maggior parte dei problemi più frequenti. Per i problemi la cui risoluzione richiede più tempo, l'elenco consentirà di raggruppare tutte le informazioni necessarie alla diagnosi del problema evitando così di perdere tempo in inutili ricerche.

Elemento	Informazioni	Esempio
Versione di Novell:		v5.1.3
Piattaforma Novell e versione del sistema operativo:		Win2003 Server sp1
Piattaforma database e versione del sistema operativo:		MS SQL 2000 SP3a
Configurazione hardware del server Sentinel ▪ Processore ▪ Memoria ▪ Altro		5 GB di RAM 4 CPU 3.0 GHz
Configurazione hardware del server del database ▪ Processore ▪ Memoria ▪ Altro (se postazione indipendente)		8 GB di RAM 4 CPU 3.0 GHz
Configurazione per la memorizzazione del database (NAS, SAN, locale, ecc.)		Locale con backup offsite
Sistema operativo e configurazione del server dei rapporti (Crystal Server)		Crystal XI Win2003 Server sp1 Autenticazione di Windows

NOTA: Potrà essere necessario aggiungere ulteriori informazioni se la configurazione (distribuzione) del sistema Sentinel lo richiede (ad esempio per DAS, Advisor, Sentinel Control Center, il Generatore servizi di raccolta e il livello di comunicazione).

1. Cercare nel portale del Supporto clienti le risposte alle domande seguenti:
   - Si tratta di un problema noto con una soluzione alternativa?
   - Il problema è stato risolto nell'ultima patch o nell'ultimo hot-fix rilasciato?
   - Il problema verrà risolto in una futura versione del prodotto?
2. Stabilire la natura del problema.

- Il problema può essere riprodotto? I passaggi per la riproduzione del problema possono essere enumerati?
- Quali comportamenti dell'utente possono causare il problema?
- Il problema si verifica periodicamente?

3. Stabilire la gravità del problema.
   - Il sistema è ancora utilizzabile?
4. Capire l'ambiente e i sistemi interessati.
   - Quali sono le piattaforme e le versioni di prodotto interessate?
   - Sono coinvolti componenti non standard o personalizzati?
   - Si tratta di un ambiente a elevata frequenza di eventi?
   - Con quale frequenza gli eventi vengono raccolti?
   - Con quale frequenza gli eventi vengono inseriti nel database?
   - Quanti sono gli utenti collegati?
   - Viene utilizzato Crystal Reporting? Quando vengono eseguiti i rapporti?
   - Viene utilizzata la correlazione? Quante sono le regole che vengono distribuite?

   Raccogliere i file di configurazione, i file di log e le informazioni sul sistema per poterle così trasferire quando necessario. Per informazioni su come trovare i file di log, consultare il Capitolo 2 relativo alle procedure consigliate della Guida all'installazione di Sentinel.
5. Controllare lo stato del sistema.
   - È possibile collegarsi alla Console Sentinel?
   - Gli eventi vengono generati e inseriti nel database? (Se ancora configurato, eseguire SendOneEvent e cercare gli eventi.)
   - È possibile visualizzare gli eventi nella Console Sentinel?
   - Gli eventi possono essere recuperati dal database tramite interrogazioni veloci?
   - Verificare l'utilizzo della RAM, lo spazio su disco, i processi in corso, l'utilizzo della CPU e la connessione alla rete degli host interessati.
   - Controllare che tutti i processi di Sentinel che dovrebbero essere in esecuzione lo siano veramente. Script di Solaris come hp_checkprocess consentono di elencare i processi in esecuzione e il relativo stato. Il task manager di Microsoft può essere utilizzato in un ambiente Windows.
   - Cercare i dump della memoria in tutte le sottodirectory di ESEC_HOME. Individuare per quali processi sono stati effettuati dei dump della memoria. (passare alla directory $ESEC_HOME, find . –name core –print)
   - Controllare l'accesso alla rete di SQLPlus. Controllare gli spazi delle tabelle.
   - Verificare che Sonic Broker sia in esecuzione. La connettività può essere controllata utilizzando la console di gestione Sonic. Utilizzare i processi di Novell per verificare che le varie connessioni siano attive. Controllare che l'avvio di Sonic non sia ostacolato da un file di lock. Utilizzare eventualmente Telnet per accedere al server dalla porta Sonic (ad esempio: telnet sentinel.company.com 10012)
   - Verificare che Watchdog sia in esecuzione sul server (ps –ef | grep watchdog).
   - Verificare che i processi di Wizard siano in esecuzione. Gestione servizi di raccolta è in esecuzione? Gestione servizi di raccolta appare attivo nel Generatore servizi di raccolta o nella console Sentinel? I Servizi di raccolta sono

in esecuzione? Quanti ce ne sono per macchina? Quali connettori vengono utilizzati (file, processi, syslog, firewall, log degli eventi e così via)? Quante risorse del sistema operativo utilizzano?

6. C'è qualche problema con il database?
   - È possibile connettersi al database mediante SQL*Plus?
   - Il database consente di connettersi da SQL*Plus allo schema ESEC utilizzando l'account DBA di Novell?
     - È possibile eseguire l'interrogazione di una delle tabelle?
   - È possibile eseguire un'istruzione SELECT in una tabella del database?
   - Controllare i driver JDBC, la relativa ubicazione e la relativa impostazione del percorso di classe.
   - Viene utilizzato Partitioning di Oracle (immettere “select * da v$version;”)?
   - Il database viene gestito da un amministratore? Da qualcun altro?
   - Il database è stato modificato dall'amministratore?
   - SDM viene utilizzato per gestire le partizioni nonché per archiviare o eliminare le partizioni al fine di creare spazio nel database?
   - In SDM qual è la partizione corrente? È PMAX?
7. Controllare che le impostazioni di ambiente dei prodotti siano corrette.
   - Controllare il funzionamento degli script della shell di login utente, le variabili di ambiente, le configurazioni nonché le impostazioni di Java Home.
   - Le variabili di ambiente sono impostate in modo che eseguano la giusta jvm?
   - Verificare che nelle cartelle del prodotto installato ci siano le giuste autorizzazioni.
   - Controllare se sono presenti processi cron che interferiscono con la funzionalità del prodotto.
   - Se il prodotto è installato su volumi NFS, controllare il funzionamento dei volumi NFS e dei servizi NFS/NIS.
8. Potrebbe esserci un problema di memoria?
   - Procurarsi le statistiche sulla velocità di consumo della memoria e sui processi che la consumano.
   - Procurarsi i volumi di eventi generati per ogni Servizio di raccolta.
   - Eseguire il comando prstat in Solaris per ottenere le statistiche di runtime dei processi.
   - Controllare le dimensioni dei processi e il numero totale di Handle in Task Manager Windows.

   Se il problema persiste, procedere a una escalation.:
   - Miglioramenti
   - Hot-fix
   - Soluzioni alternative temporanee

B Impostazione del conto di login del servizio e Security come NT AUTHORITY\NetworkService

NOTA: Il termine agente è equivalente a servizio di raccolta. Si farà in seguito riferimento agli agenti come servizi di raccolta.

In questo capitolo viene descritto dettagliatamente come configurare il conto di login del servizio Sentinel come NT AUTHORITY\NetworkService anziché come conte utente di dominio. È stato dimostrato che questo conto funziona solo con la piattaforma Windows 2003.

Per accedere alle risorse e agli oggetti nel sistema operativo, un servizio deve effettuare il login a un conto. Se si seleziona un conto che non dispone dell'autorizzazione di login come servizio, lo snap-in dei servizi concede automaticamente al conto i diritti utente necessari per effettuare il login come servizio nel computer che si sta gestendo. Questa operazione non garantisce tuttavia l'avvio del servizio. Per i conti utente utilizzati per eseguire il login come servizio è consigliabile selezionare la casella di controllo **Nessuna scadenza password** nella finestra di dialogo delle proprietà e specificare password complesse. Se è abilitata la norma di blocco del conto e il conto è bloccato, il servizio non funzionerà correttamente

Nella tabella seguente sono elencati i conti di login di servizio e la relativa modalità di utilizzo.

Conto di login	Descrizione
Conto del sistema locale	Il conto del sistema locale rappresenta un conto efficace che dispone dell'accesso completo al sistema, incluso il servizio di directory nei controller di dominio. Se un servizio esegue il login al conto del sistema locale in un controller di dominio, questo servizio dispone dell'accesso all'intero dominio. Alcuni servizi vengono configurati di default per eseguire il login al conto del sistema locale. Non modificare l'impostazione di default del servizio. Il conto del sistema locale rappresenta un conto locale predefinito utilizzato per avviare un servizio e fornire l'apposito contesto di sicurezza. Il nome del conto è NT AUTHORITY\System. Questo conto non dispone di alcuna password e tutte le informazioni fornite sulla password vengono ignorate. Il conto del sistema locale dispone dell'accesso completo al sistema, incluso il servizio di directory nei controller di dominio. Poiché il conto del sistema locale funziona come un computer in rete, dispone dell'accesso alle risorse di rete.

Conto di login	Descrizione
Conto del servizio locale	Il conto del servizio locale rappresenta uno speciale conto integrato simile a un conto utente autenticato. Il conto del servizio locale dispone dello stesso livello di accesso a risorse e oggetti di quello dei membri del gruppo Utenti. Questo accesso limitato consente di salvaguardare il sistema in caso di compromissione di singoli servizi o processi. I servizi in esecuzione come conto del servizio locale accedono alle risorse di rete come una sessione nulla senza credenziali. Il conto del servizio locale rappresenta un conto locale predefinito utilizzato per avviare un servizio e fornire l'apposito contesto di sicurezza. Il nome del conto è NT°AUTHORITY\LocalService. Il conto del servizio locale dispone dell'accesso limitato al computer locale e dell'accesso anonimo alle risorse di rete.
Conto del servizio di rete	Il conto del servizio di rete rappresenta uno speciale conto integrato simile a un conto utente autenticato. Il conto del servizio di rete dispone dello stesso livello di accesso a risorse e oggetti di quello dei membri del gruppo Utenti. Questo accesso limitato consente di salvaguardare il sistema in caso di compromissione di singoli servizi o processi. I servizi in esecuzione come conto del servizio di rete accedono alle risorse di rete utilizzando le credenziali del conto del computer. Il conto del servizio di rete rappresenta un conto locale predefinito utilizzato per avviare un servizio e fornire l'apposito contesto di sicurezza. Il nome del conto è NT°AUTHORITY\NetworkService. Il conto del servizio di rete dispone dell'accesso limitato al computer locale e dell'accesso autenticato (come conto del computer) alle risorse di rete.

L'esecuzione di un servizio con un conto di login utente comporta gli svantaggi seguenti:

1. È necessario creare il conto prima di poter eseguire il servizio. Se il conto viene creato dal programma di installazione del servizio, è necessario effettuare l'installazione da un conto che dispone di credenziali di amministrazione sufficienti per la creazione di conti nel servizio di directory.
2. I nomi e le password del conto del servizio vengono memorizzati in ogni computer in cui è installato il servizio. Se la password di un conto del servizio viene modificata o scade in un computer, non sarà possibile avviare il servizio in tale computer finché non si imposta la nuova password per il servizio in questione. È consigliabile utilizzare un servizio locale o un servizio di rete anziché un conto che necessita della password: ciò semplifica la gestione delle password.
3. Se si rinomina, si blocca, si disabilita o si elimina un conto di servizio, non sarà possibile avviare il servizio sul computer in questione finché non si reimposta il conto.

A causa degli svantaggi sopra menzionati, Novell ha testato l'esecuzione del servizio Sentinel nel conto NT AUTHORITY\NetworkService. Il conto NT AUTHORITY\LocalService non dispone dei privilegi sufficienti per questo scopo perché i processi DAS devono comunicare con il server del database in rete.

Per impostare NT AUTHORITY\NetworkService come conto di login per il servizio Sentinel

Per impostare NT AUTHORITY\NetworkService come conto di login per il servizio Sentinel, è necessario eseguire le operazioni seguenti

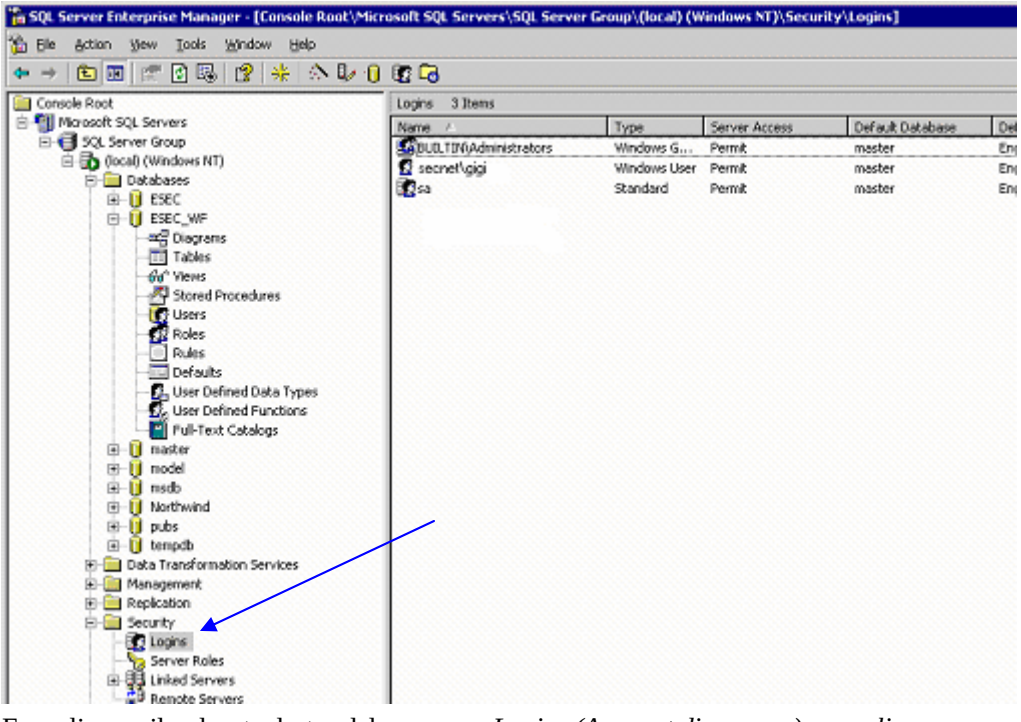
- Aggiungere il computer che esegue il servizio Sentinel come conto di login nelle istanze del database ESEC e ESEC_WF (eseguite nel computer del database)
- Modificare il conto di login per il servizio Sentinel su NT AUTHORITY\NetworkService (eseguito nel computer remoto)
- Impostare l'avvio di Sentinel (eseguito nel computer remoto)

Aggiunta del servizio Sentinel come conto di login alle istanze del database ESEC e ESEC_WF

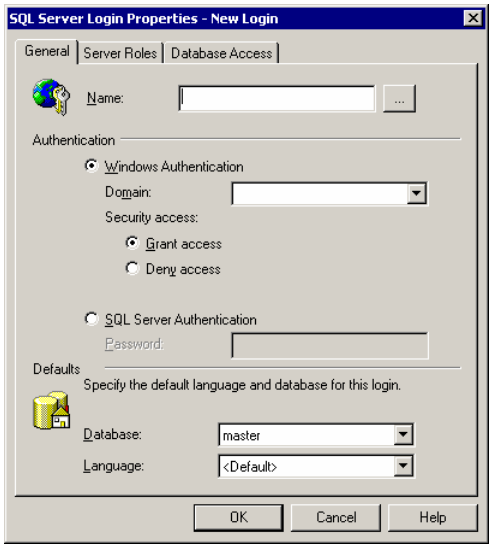
Aggiunta di un login di un computer remoto al server del database

NOTA: Come esempio, nei passaggi seguenti viene aggiunto secnet\case1 come login al server del database.

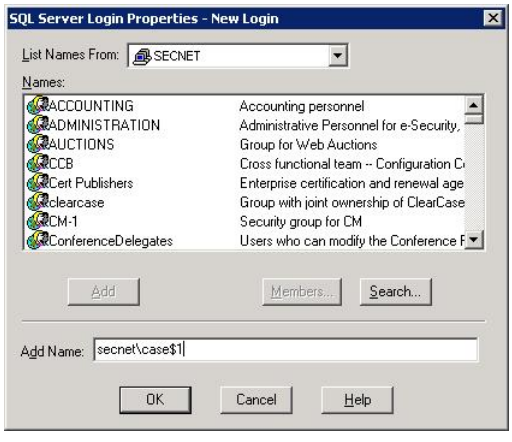
1. Nel computer del database aprire SQL Server Enterprise Manager. Nella sezione SQL Server Group (Gruppo di SQL Server) del riquadro di navigazione espandere la cartella Security (Sicurezza) ed evidenziare Logins (Login).



2. Fare clic con il pulsante destro del mouse su *Logins (Account di accesso) e scegliere New Login (Nuovo account di accesso).*

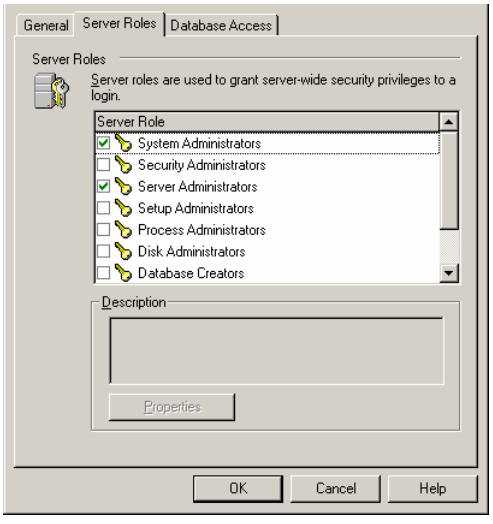


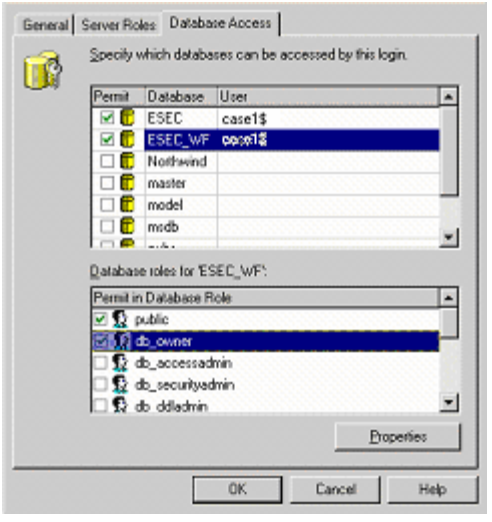
3. Fare clic sul pulsante di esplorazione accanto al campo Name (Nome). Verrà visualizzata la finestra seguente.



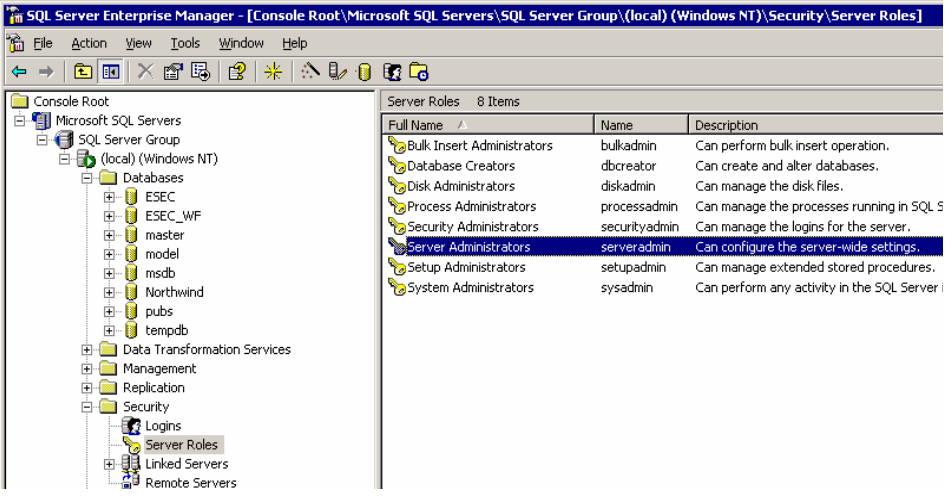
Nel campo Add Name (Aggiungi nome) immettere un nome di dominio e un nome utente (come esempio è stato immesso secnet\case1$). Questo è il computer <nome dominio>\<nome del computer>$ che viene aggiunto come login al server del database. Fare clic su *OK*.

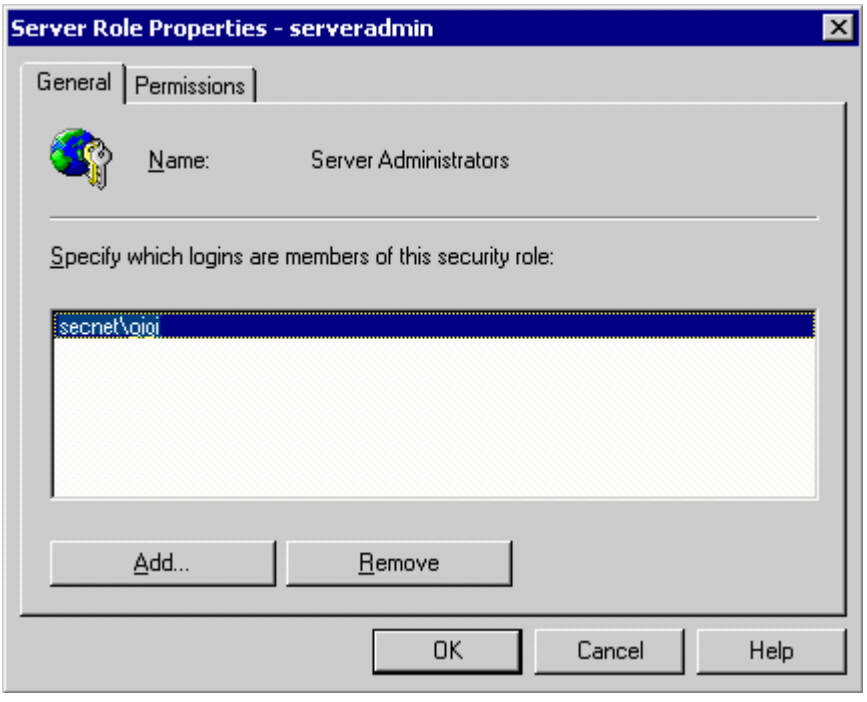
4. Per modificare il ruoli del server e l'accesso al database, fare clic con il pulsante destro del mouse su Properties on the name (Proprietà nel nome) (il computer [<nome dominio>\<nome del computer>$] che viene aggiunto come login al server del database). Per i ruoli del server scegliere System Administrators (Amministratori di sistema) e Server Administrators (Amministratori del server). Per ESEC selezionare il tipo di accesso pubblico e db_owner. Per ESEC_WF selezionare il tipo di accesso pubblico e db_owner.



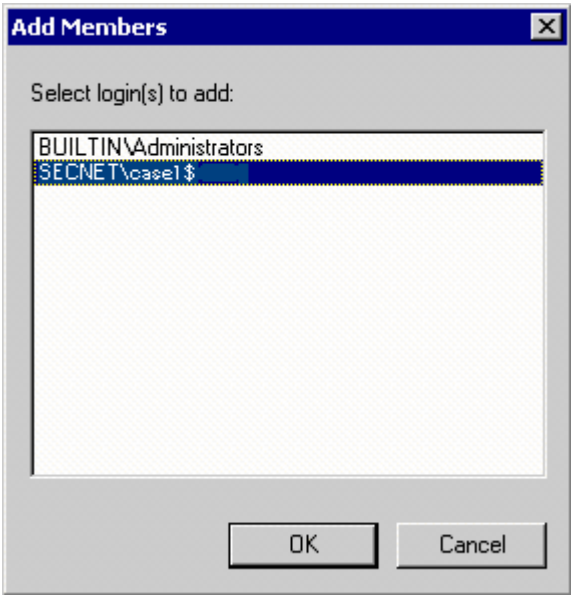


5. In Server Roles (Ruoli server), evidenziare Server Administrators (Amministratori del server), fare clic con il pulsante destro del mouse quindi scegliere *Properties (Proprietà)*.





6. Fare clic sul pulsante *Aggiungi*.

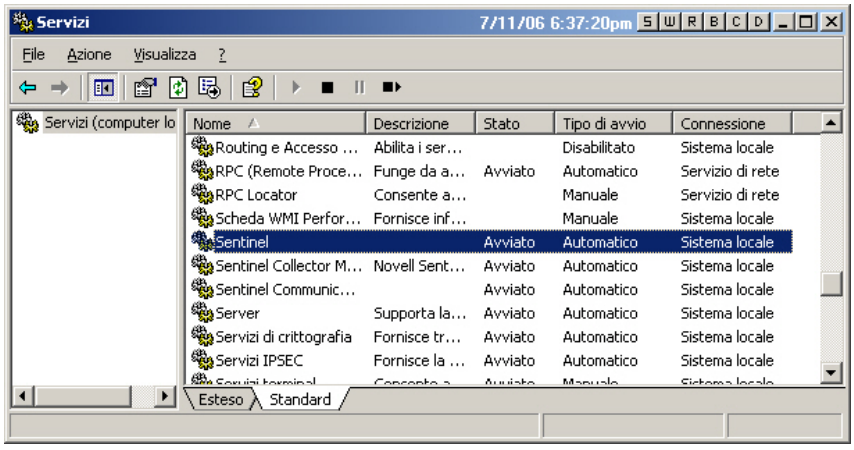


Fare clic su OK. Verrà aggiunto Secnet\case1$.

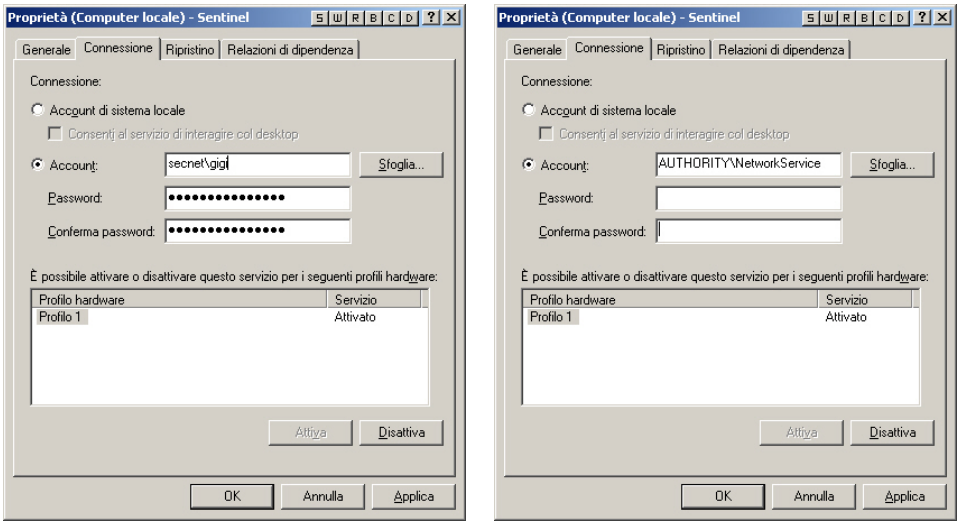
Modifica del conto di login del servizio Sentinel su NT AUTHORITY\NetworkService

Modifica del conto di login del servizio Sentinel per NT AUTHORITY\NetworkService

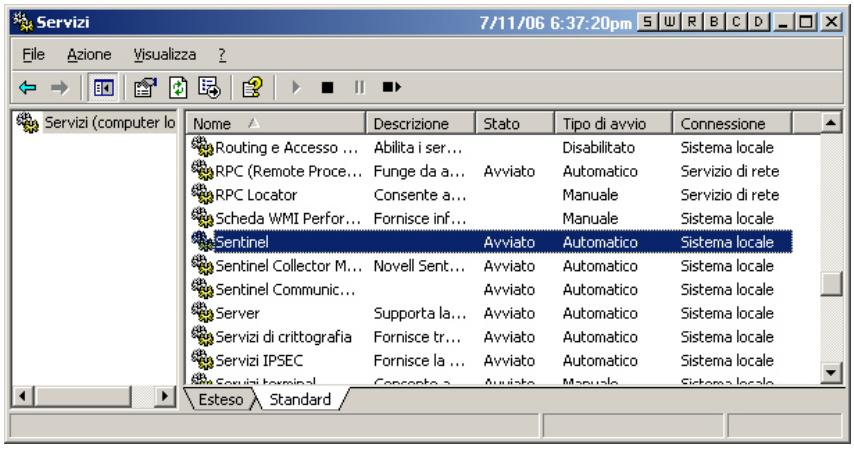
1. Nel computer remoto che si sta collegando al database, fare clic su *Start* > *Programmi* > *Strumenti di amministrazione* > *Servizi.*



2. Arrestare il servizio Sentinel, fare clic con il pulsante destro del mouse quindi scegliere *Proprietà > scheda Login*.
3. Fare clic su Account, quindi immettere NT AUTHORITY\NetworkService nel campo. Annullare i campi Password e Conferma password.



Fare clic su *OK*. Nella finestra Servizi del servizio Sentinel verrà visualizzato Servizi di rete nella colonna Accedi come.



Impostazione del servizio Sentinel per garantirne l'avvio

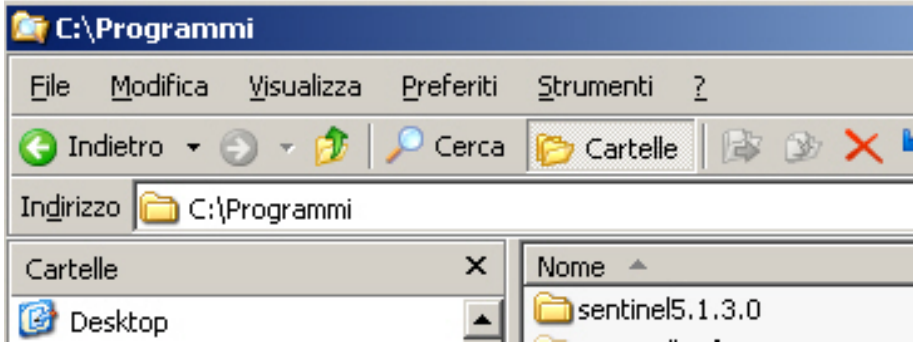
Per garantire l'avvio del servizio Sentinel, è necessario che il conto NT AUTHORITY\NetworkService disponga dei diritti di scrittura per %ESEC_HOME%. In base alla documentazione Microsoft il conto NetworkService dispone dei privilegi seguenti:

- SE_AUDIT_NAME
- SE_CHANGE_NOTIFY_NAME
- SE_UNDOCK_NAME
- Tutti i privilegi assegnati agli utenti e agli utenti autenticati

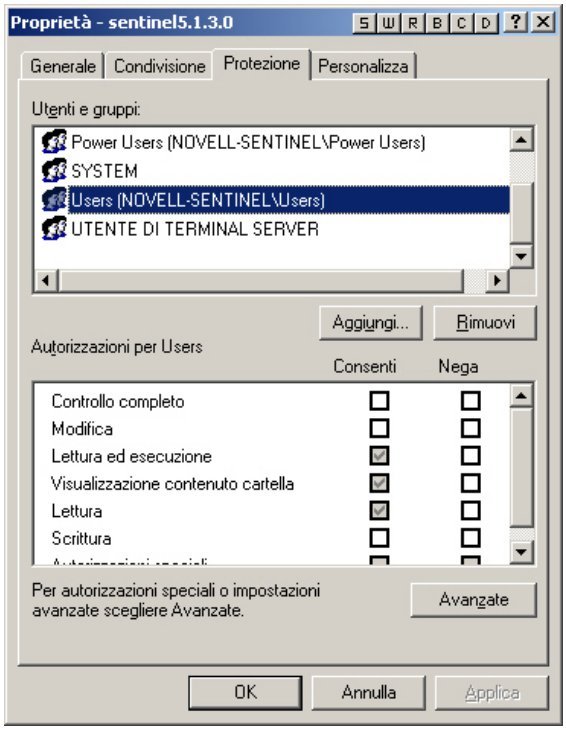
È necessario concedere l'accesso in scrittura al gruppo Utenti per %ESEC_HOME%.

Impostazione per l'avvio corretto del servizio Sentinel

1. Aprire Windows Explorer e individuare %ESEC_HOME%.
2. Fare clic on il pulsante destro del mouse sulla cartella superiore di Sentinel (in genere denominata sentinel5.1.3), quindi scegliere > *Proprietà* > *scheda Sicurezza*.



3. Evidenziare il gruppo Utenti. Concedere le autorizzazioni di lettura ed esecuzione, visualizzazione del contenuto delle cartelle, lettura e scrittura.



Fare clic su *OK*.

4. Nella finestra Servizi riavviare il servizio Sentinel.

C Utenti, ruoli e autorizzazioni di accesso al database di Sentinel

NOTA: Il termine agente è equivalente a servizio di raccolta. Si farà in seguito riferimento agli agenti come servizi di raccolta

In questo documento viene fornita un'analisi dettagliata degli utenti di Sentinel e dei relativi ruoli e autorizzazioni di accesso.

Istanza del database Sentinel

ESEC

Utenti:

- esecadm
- esecapp
- esecdba
- esecrpt
- altri utenti

NOTA: Gli utenti nella tabella precedente vengono creati mediante Gestione utenti. Per un elenco dettagliato delle autorizzazioni di accesso, vedere la sezione Utenti del database di Sentinel.

Ruoli:

- ESEC_APP: la stessa autorizzazione di db_owner
- ESEC_ETL: questo ruolo non è attualmente utilizzato ed è riservato agli aggiornamenti futuri. Per un elenco dettagliato delle autorizzazioni di accesso, vedere la sezione Ruoli del database di Sentinel.
- ESEC_USER: per un elenco dettagliato delle autorizzazioni di accesso, vedere la sezione Ruoli del database di Sentinel.

ESEC_WF

- Utenti: esecapp: per un elenco dettagliato delle autorizzazioni di accesso, vedere la sezione Ruoli del database di Sentinel.
- Ruoli: ESEC_APP: per un elenco dettagliato delle autorizzazioni di accesso, vedere la sezione Ruoli del database di Sentinel.

Utenti del database di Sentinel

Riepilogo

Nome utente	Nome gruppo…	Nome di login	Nome di default del database
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 di login	Nome DB	Nome utente	Utente di Alias
esecadm	ESEC	ESEC_USER	MemberOf
esecadm	ESEC	esecadm	Utente

esecapp

Nome di login	Nome DB	Nome utente	Utente di Alias
esecapp	ESEC	ESEC_APP	MemberOf
esecapp	ESEC	ESEC_ETL	MemberOf
esecapp	ESEC	esecapp	Utente
esecapp	ESEC_WF	ESEC_APP	MemberOf
esecapp	ESEC_WF	esecapp	Utente

esecdba

Nome di login	Nome DB	Nome utente	Utente di Alias
esecdba	ESEC	db_owner	MemberOf
esecdba	ESEC	esecdba	Utente

esecrpt

Nome di login	Nome DB	Nome utente	Utente di Alias
esecrpt	ESEC	ESEC_USER	MemberOf
esecrpt	ESEC	esecrpt	Utente

Ruoli del database di Sentinel

Riepilogo

- ESEC_APP: è un ruolo del database per ESEC e ESEC_WF. Dispone della stessa autorizzazione di db_owner per l'istanza ESEC. Per un elenco dettagliato delle autorizzazioni di accesso, vedere la sezione Ruoli del database di Sentinel.
- ESEC_ETL: è un ruolo del database per l'istanza di ESEC. Attualmente non viene utilizzato ed è riservato per lo sviluppo futuro. Per un elenco dettagliato delle autorizzazioni di accesso, vedere la sezione Ruoli del database di Sentinel.
- ESEC_USER: è un ruolo del database per l'istanza di ESEC. Per un elenco dettagliato delle autorizzazioni di accesso, vedere la sezione Ruoli del database di Sentinel.

ESEC_APP

Nel caso dell'istanza ESEC, ESEC_APP dispone della stessa autorizzazione di db_owner. ESEC_APP esegue le attività di tutti i ruoli del database nonché altre attività di manutenzione e configurazione nel database. Le autorizzazioni di questo ruolo comprendono tutti gli altri ruoli fissi del database.

Nel caso dell'istanza ESEC_WF, questa è l'autorizzazione per il ruolo ESEC_APP.

Nome ruolo	Nome oggetto	Azione	Tipo
ESEC_APP	Attività	193 SELECT	U Tabella utente
ESEC_APP	Attività	195 INSERT	U Tabella utente
ESEC_APP	Attività	196 DELETE	U Tabella utente

Nome ruolo	Nome oggetto	Azione	Tipo
ESEC_APP	Attività	197 UPDATE	U Tabella utente
ESEC_APP	ActivityData	193 SELECT	U Tabella utente
ESEC_APP	ActivityData	195 INSERT	U Tabella utente
ESEC_APP	ActivityData	196 DELETE	U Tabella utente
ESEC_APP	ActivityData	197 UPDATE	U Tabella utente
ESEC_APP	ActivityStateEventAudits	193 SELECT	U Tabella utente
ESEC_APP	ActivityStateEventAudits	195 INSERT	U Tabella utente
ESEC_APP	ActivityStateEventAudits	196 DELETE	U Tabella utente
ESEC_APP	ActivityStateEventAudits	197 UPDATE	U Tabella utente
ESEC_APP	ActivityStates	193 SELECT	U Tabella utente
ESEC_APP	ActivityStates	195 INSERT	U Tabella utente
ESEC_APP	ActivityStates	196 DELETE	U Tabella utente
ESEC_APP	ActivityStates	197 UPDATE	U Tabella utente
ESEC_APP	AndJoinTable	193 SELECT	U Tabella utente
ESEC_APP	AndJoinTable	195 INSERT	U Tabella utente
ESEC_APP	AndJoinTable	196 DELETE	U Tabella utente
ESEC_APP	AndJoinTable	197 UPDATE	U Tabella utente
ESEC_APP	AssignmentEventAudits	193 SELECT	U Tabella utente
ESEC_APP	AssignmentEventAudits	195 INSERT	U Tabella utente
ESEC_APP	AssignmentEventAudits	196 DELETE	U Tabella utente
ESEC_APP	AssignmentEventAudits	197 UPDATE	U Tabella utente
ESEC_APP	AssignmentsTable	193 SELECT	U Tabella utente
ESEC_APP	AssignmentsTable	195 INSERT	U Tabella utente
ESEC_APP	AssignmentsTable	196 DELETE	U Tabella utente
ESEC_APP	AssignmentsTable	197 UPDATE	U Tabella utente
ESEC_APP	Contatori	193 SELECT	U Tabella utente
ESEC_APP	Contatori	195 INSERT	U Tabella utente
ESEC_APP	Contatori	196 DELETE	U Tabella utente
ESEC_APP	Contatori	197 UPDATE	U Tabella utente
ESEC_APP	CreateProcessEventAudits	193 SELECT	U Tabella utente
ESEC_APP	CreateProcessEventAudits	195 INSERT	U Tabella utente
ESEC_APP	CreateProcessEventAudits	196 DELETE	U Tabella utente
ESEC_APP	CreateProcessEventAudits	197 UPDATE	U Tabella utente
ESEC_APP	DataEventAudits	193 SELECT	U Tabella utente
ESEC_APP	DataEventAudits	195 INSERT	U Tabella utente
ESEC_APP	DataEventAudits	196 DELETE	U Tabella utente
ESEC_APP	DataEventAudits	197 UPDATE	U Tabella utente
ESEC_APP	Scadenze	193 SELECT	U Tabella utente
ESEC_APP	Scadenze	195 INSERT	U Tabella utente
ESEC_APP	Scadenze	196 DELETE	U Tabella utente
ESEC_APP	Scadenze	197 UPDATE	U Tabella utente
ESEC_APP	EventTypes	193 SELECT	U Tabella utente
ESEC_APP	EventTypes	195 INSERT	U Tabella utente
ESEC_APP	EventTypes	196 DELETE	U Tabella utente
ESEC_APP	EventTypes	197 UPDATE	U Tabella utente
ESEC_APP	GroupGroupTable	193 SELECT	U Tabella utente

Nome ruolo	Nome oggetto	Azione	Tipo
ESEC_APP	GroupGroupTable	195 INSERT	U Tabella utente
ESEC_APP	GroupGroupTable	196 DELETE	U Tabella utente
ESEC_APP	GroupGroupTable	197 UPDATE	U Tabella utente
ESEC_APP	GroupTable	193 SELECT	U Tabella utente
ESEC_APP	GroupTable	195 INSERT	U Tabella utente
ESEC_APP	GroupTable	196 DELETE	U Tabella utente
ESEC_APP	GroupTable	197 UPDATE	U Tabella utente
ESEC_APP	GroupUser	193 SELECT	U Tabella utente
ESEC_APP	GroupUser	195 INSERT	U Tabella utente
ESEC_APP	GroupUser	196 DELETE	U Tabella utente
ESEC_APP	GroupUser	197 UPDATE	U Tabella utente
ESEC_APP	GroupUserPackLevelParticipant	193 SELECT	U Tabella utente
ESEC_APP	GroupUserPackLevelParticipant	195 INSERT	U Tabella utente
ESEC_APP	GroupUserPackLevelParticipant	196 DELETE	U Tabella utente
ESEC_APP	GroupUserPackLevelParticipant	197 UPDATE	U Tabella utente
ESEC_APP	GroupUserProcLevelParticipant	193 SELECT	U Tabella utente
ESEC_APP	GroupUserProcLevelParticipant	195 INSERT	U Tabella utente
ESEC_APP	GroupUserProcLevelParticipant	196 DELETE	U Tabella utente
ESEC_APP	GroupUserProcLevelParticipant	197 UPDATE	U Tabella utente
ESEC_APP	LockTable	193 SELECT	U Tabella utente
ESEC_APP	LockTable	195 INSERT	U Tabella utente
ESEC_APP	LockTable	196 DELETE	U Tabella utente
ESEC_APP	LockTable	197 UPDATE	U Tabella utente
ESEC_APP	NewEventAuditData	193 SELECT	U Tabella utente
ESEC_APP	NewEventAuditData	195 INSERT	U Tabella utente
ESEC_APP	NewEventAuditData	196 DELETE	U Tabella utente
ESEC_APP	NewEventAuditData	197 UPDATE	U Tabella utente
ESEC_APP	NextXPDLVersions	193 SELECT	U Tabella utente
ESEC_APP	NextXPDLVersions	195 INSERT	U Tabella utente
ESEC_APP	NextXPDLVersions	196 DELETE	U Tabella utente
ESEC_APP	NextXPDLVersions	197 UPDATE	U Tabella utente
ESEC_APP	NormalUser	193 SELECT	U Tabella utente
ESEC_APP	NormalUser	195 INSERT	U Tabella utente
ESEC_APP	NormalUser	196 DELETE	U Tabella utente
ESEC_APP	NormalUser	197 UPDATE	U Tabella utente
ESEC_APP	ObjectId	193 SELECT	U Tabella utente
ESEC_APP	ObjectId	195 INSERT	U Tabella utente
ESEC_APP	ObjectId	196 DELETE	U Tabella utente
ESEC_APP	ObjectId	197 UPDATE	U Tabella utente
ESEC_APP	OldEventAuditData	193 SELECT	U Tabella utente
ESEC_APP	OldEventAuditData	195 INSERT	U Tabella utente
ESEC_APP	OldEventAuditData	196 DELETE	U Tabella utente
ESEC_APP	OldEventAuditData	197 UPDATE	U Tabella utente
ESEC_APP	PackLevelParticipant	193 SELECT	U Tabella utente
ESEC_APP	PackLevelParticipant	195 INSERT	U Tabella utente
ESEC_APP	PackLevelParticipant	196 DELETE	U Tabella utente

Nome ruolo	Nome oggetto	Azione	Tipo
ESEC_APP	PackLevelParticipant	197 UPDATE	U Tabella utente
ESEC_APP	PackLevelXPDLApp	193 SELECT	U Tabella utente
ESEC_APP	PackLevelXPDLApp	195 INSERT	U Tabella utente
ESEC_APP	PackLevelXPDLApp	196 DELETE	U Tabella utente
ESEC_APP	PackLevelXPDLApp	197 UPDATE	U Tabella utente
ESEC_APP	PackLevelXPDLAppTAAppDetail	193 SELECT	U Tabella utente
ESEC_APP	PackLevelXPDLAppTAAppDetail	195 INSERT	U Tabella utente
ESEC_APP	PackLevelXPDLAppTAAppDetail	196 DELETE	U Tabella utente
ESEC_APP	PackLevelXPDLAppTAAppDetail	197 UPDATE	U Tabella utente
ESEC_APP	PackLevelXPDLAppTAAppDetailUsr	193 SELECT	U Tabella utente
ESEC_APP	PackLevelXPDLAppTAAppDetailUsr	195 INSERT	U Tabella utente
ESEC_APP	PackLevelXPDLAppTAAppDetailUsr	196 DELETE	U Tabella utente
ESEC_APP	PackLevelXPDLAppTAAppDetailUsr	197 UPDATE	U Tabella utente
ESEC_APP	PackLevelXPDLAppTAAppUser	193 SELECT	U Tabella utente
ESEC_APP	PackLevelXPDLAppTAAppUser	195 INSERT	U Tabella utente
ESEC_APP	PackLevelXPDLAppTAAppUser	196 DELETE	U Tabella utente
ESEC_APP	PackLevelXPDLAppTAAppUser	197 UPDATE	U Tabella utente
ESEC_APP	PackLevelXPDLAppToolAgentApp	193 SELECT	U Tabella utente
ESEC_APP	PackLevelXPDLAppToolAgentApp	195 INSERT	U Tabella utente
ESEC_APP	PackLevelXPDLAppToolAgentApp	196 DELETE	U Tabella utente
ESEC_APP	PackLevelXPDLAppToolAgentApp	197 UPDATE	U Tabella utente
ESEC_APP	ProcessData	193 SELECT	U Tabella utente
ESEC_APP	ProcessData	195 INSERT	U Tabella utente
ESEC_APP	ProcessData	196 DELETE	U Tabella utente
ESEC_APP	ProcessData	197 UPDATE	U Tabella utente
ESEC_APP	ProcessDefinitions	193 SELECT	U Tabella utente
ESEC_APP	ProcessDefinitions	195 INSERT	U Tabella utente
ESEC_APP	ProcessDefinitions	196 DELETE	U Tabella utente
ESEC_APP	ProcessDefinitions	197 UPDATE	U Tabella utente
ESEC_APP	Processi	193 SELECT	U Tabella utente
ESEC_APP	Processi	195 INSERT	U Tabella utente
ESEC_APP	Processi	196 DELETE	U Tabella utente
ESEC_APP	Processi	197 UPDATE	U Tabella utente
ESEC_APP	ProcessRequesters	193 SELECT	U Tabella utente
ESEC_APP	ProcessRequesters	195 INSERT	U Tabella utente
ESEC_APP	ProcessRequesters	196 DELETE	U Tabella utente
ESEC_APP	ProcessRequesters	197 UPDATE	U Tabella utente
ESEC_APP	ProcessStateEventAudits	193 SELECT	U Tabella utente
ESEC_APP	ProcessStateEventAudits	195 INSERT	U Tabella utente
ESEC_APP	ProcessStateEventAudits	196 DELETE	U Tabella utente
ESEC_APP	ProcessStateEventAudits	197 UPDATE	U Tabella utente
ESEC_APP	ProcessStates	193 SELECT	U Tabella utente
ESEC_APP	ProcessStates	195 INSERT	U Tabella utente
ESEC_APP	ProcessStates	196 DELETE	U Tabella utente
ESEC_APP	ProcessStates	197 UPDATE	U Tabella utente
ESEC_APP	ProcLevelParticipant	193 SELECT	U Tabella utente
ESEC_APP	ProcLevelParticipant	195 INSERT	U Tabella utente

Nome ruolo	Nome oggetto	Azione	Tipo
ESEC_APP	ProcLevelParticipant	196 DELETE	U Tabella utente
ESEC_APP	ProcLevelParticipant	197 UPDATE	U Tabella utente
ESEC_APP	ProcLevelXPDLApp	193 SELECT	U Tabella utente
ESEC_APP	ProcLevelXPDLApp	195 INSERT	U Tabella utente
ESEC_APP	ProcLevelXPDLApp	196 DELETE	U Tabella utente
ESEC_APP	ProcLevelXPDLApp	197 UPDATE	U Tabella utente
ESEC_APP	ProcLevelXPDLAppTAAppDetail	193 SELECT	U Tabella utente
ESEC_APP	ProcLevelXPDLAppTAAppDetail	195 INSERT	U Tabella utente
ESEC_APP	ProcLevelXPDLAppTAAppDetail	196 DELETE	U Tabella utente
ESEC_APP	ProcLevelXPDLAppTAAppDetail	197 UPDATE	U Tabella utente
ESEC_APP	ProcLevelXPDLAppTAAppDetailUsr	193 SELECT	U Tabella utente
ESEC_APP	ProcLevelXPDLAppTAAppDetailUsr	195 INSERT	U Tabella utente
ESEC_APP	ProcLevelXPDLAppTAAppDetailUsr	196 DELETE	U Tabella utente
ESEC_APP	ProcLevelXPDLAppTAAppDetailUsr	197 UPDATE	U Tabella utente
ESEC_APP	ProcLevelXPDLAppTAAppUser	193 SELECT	U Tabella utente
ESEC_APP	ProcLevelXPDLAppTAAppUser	195 INSERT	U Tabella utente
ESEC_APP	ProcLevelXPDLAppTAAppUser	196 DELETE	U Tabella utente
ESEC_APP	ProcLevelXPDLAppTAAppUser	197 UPDATE	U Tabella utente
ESEC_APP	ProcLevelXPDLAppToolAgentApp	193 SELECT	U Tabella utente
ESEC_APP	ProcLevelXPDLAppToolAgentApp	195 INSERT	U Tabella utente
ESEC_APP	ProcLevelXPDLAppToolAgentApp	196 DELETE	U Tabella utente
ESEC_APP	ProcLevelXPDLAppToolAgentApp	197 UPDATE	U Tabella utente
ESEC_APP	ResourcesTable	193 SELECT	U Tabella utente
ESEC_APP	ResourcesTable	195 INSERT	U Tabella utente
ESEC_APP	ResourcesTable	196 DELETE	U Tabella utente
ESEC_APP	ResourcesTable	197 UPDATE	U Tabella utente
ESEC_APP	StateEventAudits	193 SELECT	U Tabella utente
ESEC_APP	StateEventAudits	195 INSERT	U Tabella utente
ESEC_APP	StateEventAudits	196 DELETE	U Tabella utente
ESEC_APP	StateEventAudits	197 UPDATE	U Tabella utente
ESEC_APP	ToolAgentApp	193 SELECT	U Tabella utente
ESEC_APP	ToolAgentApp	195 INSERT	U Tabella utente
ESEC_APP	ToolAgentApp	196 DELETE	U Tabella utente
ESEC_APP	ToolAgentApp	197 UPDATE	U Tabella utente
ESEC_APP	ToolAgentAppDetail	193 SELECT	U Tabella utente
ESEC_APP	ToolAgentAppDetail	195 INSERT	U Tabella utente
ESEC_APP	ToolAgentAppDetail	196 DELETE	U Tabella utente
ESEC_APP	ToolAgentAppDetail	197 UPDATE	U Tabella utente
ESEC_APP	ToolAgentAppDetailUser	193 SELECT	U Tabella utente
ESEC_APP	ToolAgentAppDetailUser	195 INSERT	U Tabella utente
ESEC_APP	ToolAgentAppDetailUser	196 DELETE	U Tabella utente
ESEC_APP	ToolAgentAppDetailUser	197 UPDATE	U Tabella utente
ESEC_APP	ToolAgentAppUser	193 SELECT	U Tabella utente
ESEC_APP	ToolAgentAppUser	195 INSERT	U Tabella utente
ESEC_APP	ToolAgentAppUser	196 DELETE	U Tabella utente
ESEC_APP	ToolAgentAppUser	197 UPDATE	U Tabella utente
ESEC_APP	ToolAgentUser	193 SELECT	U Tabella utente

Nome ruolo	Nome oggetto	Azione	Tipo
ESEC_APP	ToolAgentUser	195 INSERT	U Tabella utente
ESEC_APP	ToolAgentUser	196 DELETE	U Tabella utente
ESEC_APP	ToolAgentUser	197 UPDATE	U Tabella utente
ESEC_APP	UserGroupTable	193 SELECT	U Tabella utente
ESEC_APP	UserGroupTable	195 INSERT	U Tabella utente
ESEC_APP	UserGroupTable	196 DELETE	U Tabella utente
ESEC_APP	UserGroupTable	197 UPDATE	U Tabella utente
ESEC_APP	UserPackLevelParticipant	193 SELECT	U Tabella utente
ESEC_APP	UserPackLevelParticipant	195 INSERT	U Tabella utente
ESEC_APP	UserPackLevelParticipant	196 DELETE	U Tabella utente
ESEC_APP	UserPackLevelParticipant	197 UPDATE	U Tabella utente
ESEC_APP	UserProcLevelParticipant	193 SELECT	U Tabella utente
ESEC_APP	UserProcLevelParticipant	195 INSERT	U Tabella utente
ESEC_APP	UserProcLevelParticipant	196 DELETE	U Tabella utente
ESEC_APP	UserProcLevelParticipant	197 UPDATE	U Tabella utente
ESEC_APP	UserTable	193 SELECT	U Tabella utente
ESEC_APP	UserTable	195 INSERT	U Tabella utente
ESEC_APP	UserTable	196 DELETE	U Tabella utente
ESEC_APP	UserTable	197 UPDATE	U Tabella utente
ESEC_APP	XPDLApplicationPackage	193 SELECT	U Tabella utente
ESEC_APP	XPDLApplicationPackage	195 INSERT	U Tabella utente
ESEC_APP	XPDLApplicationPackage	196 DELETE	U Tabella utente
ESEC_APP	XPDLApplicationPackage	197 UPDATE	U Tabella utente
ESEC_APP	XPDLApplicationProcess	193 SELECT	U Tabella utente
ESEC_APP	XPDLApplicationProcess	195 INSERT	U Tabella utente
ESEC_APP	XPDLApplicationProcess	196 DELETE	U Tabella utente
ESEC_APP	XPDLApplicationProcess	197 UPDATE	U Tabella utente
ESEC_APP	XPDLData	193 SELECT	U Tabella utente
ESEC_APP	XPDLData	195 INSERT	U Tabella utente
ESEC_APP	XPDLData	196 DELETE	U Tabella utente
ESEC_APP	XPDLData	197 UPDATE	U Tabella utente
ESEC_APP	XPDLHistory	193 SELECT	U Tabella utente
ESEC_APP	XPDLHistory	195 INSERT	U Tabella utente
ESEC_APP	XPDLHistory	196 DELETE	U Tabella utente
ESEC_APP	XPDLHistory	197 UPDATE	U Tabella utente
ESEC_APP	XPDLHistoryData	193 SELECT	U Tabella utente
ESEC_APP	XPDLHistoryData	195 INSERT	U Tabella utente
ESEC_APP	XPDLHistoryData	196 DELETE	U Tabella utente
ESEC_APP	XPDLHistoryData	197 UPDATE	U Tabella utente
ESEC_APP	XPDLParticipantPackage	193 SELECT	U Tabella utente
ESEC_APP	XPDLParticipantPackage	195 INSERT	U Tabella utente
ESEC_APP	XPDLParticipantPackage	196 DELETE	U Tabella utente
ESEC_APP	XPDLParticipantPackage	197 UPDATE	U Tabella utente
ESEC_APP	XPDLParticipantProcess	193 SELECT	U Tabella utente
ESEC_APP	XPDLParticipantProcess	195 INSERT	U Tabella utente
ESEC_APP	XPDLParticipantProcess	196 DELETE	U Tabella utente
ESEC_APP	XPDLParticipantProcess	197 UPDATE	U Tabella utente

Nome ruolo	Nome oggetto	Azione	Tipo
ESEC_APP	XPDLReferences	193 SELECT	U Tabella utente
ESEC_APP	XPDLReferences	195 INSERT	U Tabella utente
ESEC_APP	XPDLReferences	196 DELETE	U Tabella utente
ESEC_APP	XPDLReferences	197 UPDATE	U Tabella utente
ESEC_APP	XPDLS	193 SELECT	U Tabella utente
ESEC_APP	XPDLS	195 INSERT	U Tabella utente
ESEC_APP	XPDLS	196 DELETE	U Tabella utente
ESEC_APP	XPDLS	197 UPDATE	U Tabella utente

ESEC_ETL

Nome ruolo	Nome oggetto	Azione	Tipo
ESEC_ETL	ACTVY	193 SELECT	U Tabella utente
ESEC_ETL	ACTVY_NAMESPACE	193 SELECT	U Tabella utente
ESEC_ETL	ACTVY_PARM	193 SELECT	U Tabella utente
ESEC_ETL	ACTVY_REF	193 SELECT	U Tabella utente
ESEC_ETL	ACTVY_REF_PARM_VAL	193 SELECT	U Tabella utente
ESEC_ETL	ADV_ALERT	193 SELECT	U Tabella utente
ESEC_ETL	ADV_ALERT_CVE	193 SELECT	U Tabella utente
ESEC_ETL	ADV_ALERT_PRODUCT	193 SELECT	U Tabella utente
ESEC_ETL	ADV_ATTACK	193 SELECT	U Tabella utente
ESEC_ETL	ADV_ATTACK_ALERT	193 SELECT	U Tabella utente
ESEC_ETL	ADV_ATTACK_CVE	193 SELECT	U Tabella utente
ESEC_ETL	ADV_ATTACK_MAP	193 SELECT	U Tabella utente
ESEC_ETL	ADV_ATTACK_PLUGIN	193 SELECT	U Tabella utente
ESEC_ETL	ADV_CREDIBILITY	193 SELECT	U Tabella utente
ESEC_ETL	ADV_FEED	193 SELECT	U Tabella utente
ESEC_ETL	ADV_PRODUCT	193 SELECT	U Tabella utente
ESEC_ETL	ADV_PRODUCT_SERVICE_PACK	193 SELECT	U Tabella utente
ESEC_ETL	ADV_PRODUCT_VERSION	193 SELECT	U Tabella utente
ESEC_ETL	ADV_SEVERITY	193 SELECT	U Tabella utente
ESEC_ETL	ADV_SUBALERT	193 SELECT	U Tabella utente
ESEC_ETL	ADV_URGENCY	193 SELECT	U Tabella utente
ESEC_ETL	ADV_VENDOR	193 SELECT	U Tabella utente
ESEC_ETL	ADV_VULN_PRODUCT	193 SELECT	U Tabella utente
ESEC_ETL	ANNOTATIONS	193 SELECT	U Tabella utente
ESEC_ETL	ASSET	193 SELECT	U Tabella utente
ESEC_ETL	ASSET_CTGRY	193 SELECT	U Tabella utente
ESEC_ETL	ASSET_HOSTNAME	193 SELECT	U Tabella utente
ESEC_ETL	ASSET_IP	193 SELECT	U Tabella utente
ESEC_ETL	ASSET_LOC	193 SELECT	U Tabella utente
ESEC_ETL	ASSET_VAL_LKUP	193 SELECT	U Tabella utente
ESEC_ETL	ASSET_X_ENTITY_X_ROLE	193 SELECT	U Tabella utente
ESEC_ETL	ASSOCIATIONS	193 SELECT	U Tabella utente
ESEC_ETL	ATTACHMENTS	193 SELECT	U Tabella utente
ESEC_ETL	CONFIGS	193 SELECT	U Tabella utente
ESEC_ETL	CONTACTS	193 SELECT	U Tabella utente

Nome ruolo	Nome oggetto	Azione	Tipo
ESEC_ETL	CORRELATED_EVENTS_P_MAX	193 SELECT	U Tabella utente
ESEC_ETL	CORRELATED_EVENTS_P_MIN	193 SELECT	U Tabella utente
ESEC_ETL	CRIT_LKUP	193 SELECT	U Tabella utente
ESEC_ETL	CUST	193 SELECT	U Tabella utente
ESEC_ETL	ENTITY_TYP_LKUP	193 SELECT	U Tabella utente
ESEC_ETL	ENV_IDENTITY_LKUP	193 SELECT	U Tabella utente
ESEC_ETL	ESEC_ARCHIVE_CONFIG	193 SELECT	U Tabella utente
ESEC_ETL	ESEC_ARCHIVE_LOG_FILES	193 SELECT	U Tabella utente
ESEC_ETL	ESEC_ARCHIVE_LOGS	193 SELECT	U Tabella utente
ESEC_ETL	ESEC_DB_PATCHES	193 SELECT	U Tabella utente
ESEC_ETL	ESEC_DB_VERSION	193 SELECT	U Tabella utente
ESEC_ETL	ESEC_DISPLAY	193 SELECT	U Tabella utente
ESEC_ETL	ESEC_PARTITION_CONFIG	193 SELECT	U Tabella utente
ESEC_ETL	ESEC_PARTITIONS_TEMP	193 SELECT	U Tabella utente
ESEC_ETL	ESEC_PORT_REFERENCE	193 SELECT	U Tabella utente
ESEC_ETL	ESEC_PROTOCOL_REFERENCE	193 SELECT	U Tabella utente
ESEC_ETL	ESEC_SDM_LOCK	193 SELECT	U Tabella utente
ESEC_ETL	ESEC_SEQUENCE	193 SELECT	U Tabella utente
ESEC_ETL	EVENTS_P_MAX	193 SELECT	U Tabella utente
ESEC_ETL	EVENTS_P_MIN	193 SELECT	U Tabella utente
ESEC_ETL	EVT_AGENT	193 SELECT	U Tabella utente
ESEC_ETL	EVT_ASSET	193 SELECT	U Tabella utente
ESEC_ETL	EVT_DEST_EVT_NAME_SMRY_1_P_MAX	193 SELECT	U Tabella utente
ESEC_ETL	EVT_DEST_EVT_NAME_SMRY_1_P_MAX	195 INSERT	U Tabella utente
ESEC_ETL	EVT_DEST_EVT_NAME_SMRY_1_P_MAX	196 DELETE	U Tabella utente
ESEC_ETL	EVT_DEST_EVT_NAME_SMRY_1_P_MAX	197 UPDATE	U Tabella utente
ESEC_ETL	EVT_DEST_EVT_NAME_SMRY_1_P_MIN	193 SELECT	U Tabella utente
ESEC_ETL	EVT_DEST_SMRY_1_P_MAX	193 SELECT	U Tabella utente
ESEC_ETL	EVT_DEST_SMRY_1_P_MAX	195 INSERT	U Tabella utente
ESEC_ETL	EVT_DEST_SMRY_1_P_MAX	196 DELETE	U Tabella utente
ESEC_ETL	EVT_DEST_SMRY_1_P_MAX	197 UPDATE	U Tabella utente
ESEC_ETL	EVT_DEST_SMRY_1_P_MIN	193 SELECT	U Tabella utente
ESEC_ETL	EVT_DEST_TXNMY_SMRY_1_P_MAX	193 SELECT	U Tabella utente
ESEC_ETL	EVT_DEST_TXNMY_SMRY_1_P_MAX	195 INSERT	U Tabella utente
ESEC_ETL	EVT_DEST_TXNMY_SMRY_1_P_MAX	196 DELETE	U Tabella utente
ESEC_ETL	EVT_DEST_TXNMY_SMRY_1_P_MAX	197 UPDATE	U Tabella utente
ESEC_ETL	EVT_DEST_TXNMY_SMRY_1_P_MIN	193 SELECT	U Tabella utente
ESEC_ETL	EVT_NAME	193 SELECT	U Tabella utente
ESEC_ETL	EVT_NAME	195 INSERT	U Tabella utente
ESEC_ETL	EVT_NAME	196 DELETE	U Tabella utente
ESEC_ETL	EVT_NAME	197 UPDATE	U Tabella utente
ESEC_ETL	EVT_PORT_SMRY_1_P_MAX	193 SELECT	U Tabella utente
ESEC_ETL	EVT_PORT_SMRY_1_P_MAX	195 INSERT	U Tabella utente
ESEC_ETL	EVT_PORT_SMRY_1_P_MAX	196 DELETE	U Tabella utente
ESEC_ETL	EVT_PORT_SMRY_1_P_MAX	197 UPDATE	U Tabella utente
ESEC_ETL	EVT_PORT_SMRY_1_P_MIN	193 SELECT	U Tabella utente
ESEC_ETL	EVT_PRTCL	193 SELECT	U Tabella utente

Nome ruolo	Nome oggetto	Azione	Tipo
ESEC_ETL	EVT_RSRC	193 SELECT	U Tabella utente
ESEC_ETL	EVT_SEV_SMRY_1_P_MAX	193 SELECT	U Tabella utente
ESEC_ETL	EVT_SEV_SMRY_1_P_MAX	195 INSERT	U Tabella utente
ESEC_ETL	EVT_SEV_SMRY_1_P_MAX	196 DELETE	U Tabella utente
ESEC_ETL	EVT_SEV_SMRY_1_P_MAX	197 UPDATE	U Tabella utente
ESEC_ETL	EVT_SEV_SMRY_1_P_MIN	193 SELECT	U Tabella utente
ESEC_ETL	EVT_SRC_SMRY_1_P_MAX	193 SELECT	U Tabella utente
ESEC_ETL	EVT_SRC_SMRY_1_P_MAX	195 INSERT	U Tabella utente
ESEC_ETL	EVT_SRC_SMRY_1_P_MAX	196 DELETE	U Tabella utente
ESEC_ETL	EVT_SRC_SMRY_1_P_MAX	197 UPDATE	U Tabella utente
ESEC_ETL	EVT_SRC_SMRY_1_P_MIN	193 SELECT	U Tabella utente
ESEC_ETL	EVT_TXNMY	193 SELECT	U Tabella utente
ESEC_ETL	EVT_USR	193 SELECT	U Tabella utente
ESEC_ETL	EVT_USR	195 INSERT	U Tabella utente
ESEC_ETL	EVT_USR	196 DELETE	U Tabella utente
ESEC_ETL	EVT_USR	197 UPDATE	U Tabella utente
ESEC_ETL	EXT_DATA	193 SELECT	U Tabella utente
ESEC_ETL	HIST_CORRELATED_EVENTS_P_MAX	193 SELECT	U Tabella utente
ESEC_ETL	HIST_EVENTS_P_MAX	193 SELECT	U Tabella utente
ESEC_ETL	IMAGES	193 SELECT	U Tabella utente
ESEC_ETL	INCIDENTS	193 SELECT	U Tabella utente
ESEC_ETL	INCIDENTS_ASSETS	193 SELECT	U Tabella utente
ESEC_ETL	INCIDENTS_EVENTS	193 SELECT	U Tabella utente
ESEC_ETL	INCIDENTS_VULN	193 SELECT	U Tabella utente
ESEC_ETL	L_STAT	193 SELECT	U Tabella utente
ESEC_ETL	LOGS	193 SELECT	U Tabella utente
ESEC_ETL	MD_CONFIG	193 SELECT	U Tabella utente
ESEC_ETL	MD_EVT_FILE_STS	193 SELECT	U Tabella utente
ESEC_ETL	MD_EVT_FILE_STS	195 INSERT	U Tabella utente
ESEC_ETL	MD_EVT_FILE_STS	196 DELETE	U Tabella utente
ESEC_ETL	MD_EVT_FILE_STS	197 UPDATE	U Tabella utente
ESEC_ETL	MD_SMRY_STS	193 SELECT	U Tabella utente
ESEC_ETL	MD_SMRY_STS	195 INSERT	U Tabella utente
ESEC_ETL	MD_SMRY_STS	196 DELETE	U Tabella utente
ESEC_ETL	MD_SMRY_STS	197 UPDATE	U Tabella utente
ESEC_ETL	MD_VIEW_CONFIG	193 SELECT	U Tabella utente
ESEC_ETL	NETWORK_IDENTITY_LKUP	193 SELECT	U Tabella utente
ESEC_ETL	OBJ_STORE	193 SELECT	U Tabella utente
ESEC_ETL	ORGANIZATION	193 SELECT	U Tabella utente
ESEC_ETL	PERSON	193 SELECT	U Tabella utente
ESEC_ETL	PHYSICAL_ASSET	193 SELECT	U Tabella utente
ESEC_ETL	PRDT	193 SELECT	U Tabella utente
ESEC_ETL	ROLE_LKUP	193 SELECT	U Tabella utente
ESEC_ETL	SENSITIVITY_LKUP	193 SELECT	U Tabella utente
ESEC_ETL	STATES	193 SELECT	U Tabella utente
ESEC_ETL	USERS	193 SELECT	U Tabella utente
ESEC_ETL	VNDR	193 SELECT	U Tabella utente

Nome ruolo	Nome oggetto	Azione	Tipo
ESEC_ETL	VULN	193 SELECT	U Tabella utente
ESEC_ETL	VULN_CODE	193 SELECT	U Tabella utente
ESEC_ETL	VULN_INFO	193 SELECT	U Tabella utente
ESEC_ETL	VULN_RSRC	193 SELECT	U Tabella utente
ESEC_ETL	VULN_RSRC_SCAN	193 SELECT	U Tabella utente
ESEC_ETL	VULN_SCAN	193 SELECT	U Tabella utente
ESEC_ETL	VULN_SCAN_VULN	193 SELECT	U Tabella utente
ESEC_ETL	VULN_SCANNER	193 SELECT	U Tabella utente
ESEC_ETL	WORKFLOW_DEF	193 SELECT	U Tabella utente
ESEC_ETL	WORKFLOW_INFO	193 SELECT	U Tabella utente

ESEC_USER

Nome ruolo	Nome oggetto	Azione	Tipo
ESEC_USER	ADV_ALERT_CVE_RPT_V	193 SELECT	V Visualizzazione
ESEC_USER	ADV_ALERT_PRODUCT_RPT_V	193 SELECT	V Visualizzazione
ESEC_USER	ADV_ALERT_RPT_V	193 SELECT	V Visualizzazione
ESEC_USER	ADV_ATTACK_ALERT_RPT_V	193 SELECT	V Visualizzazione
ESEC_USER	ADV_ATTACK_CVE_RPT_V	193 SELECT	V Visualizzazione
ESEC_USER	ADV_ATTACK_MAP_RPT_V	193 SELECT	V Visualizzazione
ESEC_USER	ADV_ATTACK_PLUGIN_RPT_V	193 SELECT	V Visualizzazione
ESEC_USER	ADV_ATTACK_RPT_V	193 SELECT	V Visualizzazione
ESEC_USER	ADV_CREDIBILITY_RPT_V	193 SELECT	V Visualizzazione
ESEC_USER	ADV_FEED_RPT_V	193 SELECT	V Visualizzazione
ESEC_USER	ADV_PRODUCT_RPT_V	193 SELECT	V Visualizzazione
ESEC_USER	ADV_PRODUCT_SERVICE_PACK_RPT_V	193 SELECT	V Visualizzazione
ESEC_USER	ADV_PRODUCT_VERSION_RPT_V	193 SELECT	V Visualizzazione
ESEC_USER	ADV_SEVERITY_RPT_V	193 SELECT	V Visualizzazione
ESEC_USER	ADV_SUBALERT_RPT_V	193 SELECT	V Visualizzazione
ESEC_USER	ADV_URGENCY_RPT_V	193 SELECT	V Visualizzazione
ESEC_USER	ADV_VENDOR_RPT_V	193 SELECT	V Visualizzazione
ESEC_USER	ADV_VULN_PRODUCT_RPT_V	193 SELECT	V Visualizzazione
ESEC_USER	ANNOTATIONS_RPT_V	193 SELECT	V Visualizzazione
ESEC_USER	ASSET_CATEGORY_RPT_V	193 SELECT	V Visualizzazione
ESEC_USER	ASSET_HOSTNAME_RPT_V	193 SELECT	V Visualizzazione
ESEC_USER	ASSET_IP_RPT_V	193 SELECT	V Visualizzazione
ESEC_USER	ASSET_LOCATION_RPT_V	193 SELECT	V Visualizzazione
ESEC_USER	ASSET_RPT_V	193 SELECT	V Visualizzazione
ESEC_USER	ASSET_VALUE_RPT_V	193 SELECT	V Visualizzazione
ESEC_USER	ASSET_X_ENTITY_X_ROLE_RPT_V	193 SELECT	V Visualizzazione
ESEC_USER	ASSOCIATIONS_RPT_V	193 SELECT	V Visualizzazione
ESEC_USER	ATTACHMENTS_RPT_V	193 SELECT	V Visualizzazione
ESEC_USER	CONFIGS_RPT_V	193 SELECT	V Visualizzazione
ESEC_USER	CONTACTS_RPT_V	193 SELECT	V Visualizzazione
ESEC_USER	CORRELATED_EVENTS	193 SELECT	V Visualizzazione
ESEC_USER	CORRELATED_EVENTS_RPT_V	193 SELECT	V Visualizzazione
ESEC_USER	CORRELATED_EVENTS_RPT_V1	193 SELECT	V Visualizzazione

Nome ruolo	Nome oggetto	Azione	Tipo
ESEC_USER	CRITICALITY_RPT_V	193 SELECT	V Visualizzazione
ESEC_USER	CUST_RPT_V	193 SELECT	V Visualizzazione
ESEC_USER	ENTITY_TYPE_RPT_V	193 SELECT	V Visualizzazione
ESEC_USER	ENV_IDENTITY_RPT_V	193 SELECT	V Visualizzazione
ESEC_USER	ESEC_DISPLAY_RPT_V	193 SELECT	V Visualizzazione
ESEC_USER	ESEC_PORT_REFERENCE_RPT_V	193 SELECT	V Visualizzazione
ESEC_USER	ESEC_PROTOCOL_REFERENCE_RPT_V	193 SELECT	V Visualizzazione
ESEC_USER	ESEC_SEQUENCE_RPT_V	193 SELECT	V Visualizzazione
ESEC_USER	esec_toBase	224 EXECUTE	NULL
ESEC_USER	esec_toDecimal	224 EXECUTE	NULL
ESEC_USER	esec_toIpChar	224 EXECUTE	NULL
ESEC_USER	EVENTS	193 SELECT	V Visualizzazione
ESEC_USER	EVENTS_ALL_RPT_V	193 SELECT	V Visualizzazione
ESEC_USER	EVENTS_ALL_RPT_V1	193 SELECT	V Visualizzazione
ESEC_USER	EVENTS_ALL_V	193 SELECT	V Visualizzazione
ESEC_USER	EVENTS_RPT_V	193 SELECT	V Visualizzazione
ESEC_USER	EVENTS_RPT_V1	193 SELECT	V Visualizzazione
ESEC_USER	EVENTS_RPT_V2	193 SELECT	V Visualizzazione
ESEC_USER	EVT_AGENT_RPT_V	193 SELECT	V Visualizzazione
ESEC_USER	EVT_ASSET_RPT_V	193 SELECT	V Visualizzazione
ESEC_USER	EVT_DEST_EVT_NAME_SMRY_1	193 SELECT	V Visualizzazione
ESEC_USER	EVT_DEST_EVT_NAME_SMRY_1_RPT_V	193 SELECT	V Visualizzazione
ESEC_USER	EVT_DEST_SMRY_1	193 SELECT	V Visualizzazione
ESEC_USER	EVT_DEST_SMRY_1_RPT_V	193 SELECT	V Visualizzazione
ESEC_USER	EVT_DEST_TXNMY_SMRY_1	193 SELECT	V Visualizzazione
ESEC_USER	EVT_DEST_TXNMY_SMRY_1_RPT_V	193 SELECT	V Visualizzazione
ESEC_USER	EVT_NAME_RPT_V	193 SELECT	V Visualizzazione
ESEC_USER	EVT_PORT_SMRY_1	193 SELECT	V Visualizzazione
ESEC_USER	EVT_PORT_SMRY_1_RPT_V	193 SELECT	V Visualizzazione
ESEC_USER	EVT_PRTCL_RPT_V	193 SELECT	V Visualizzazione
ESEC_USER	EVT_RSRC_RPT_V	193 SELECT	V Visualizzazione
ESEC_USER	EVT_SEV_SMRY_1	193 SELECT	V Visualizzazione
ESEC_USER	EVT_SEV_SMRY_1_RPT_V	193 SELECT	V Visualizzazione
ESEC_USER	EVT_SRC_SMRY_1	193 SELECT	V Visualizzazione
ESEC_USER	EVT_SRC_SMRY_1_RPT_V	193 SELECT	V Visualizzazione
ESEC_USER	EVT_TXNMY_RPT_V	193 SELECT	V Visualizzazione
ESEC_USER	EVT_USR_RPT_V	193 SELECT	V Visualizzazione
ESEC_USER	EXTERNAL_DATA_RPT_V	193 SELECT	V Visualizzazione
ESEC_USER	HIST_CORRELATED_EVENTS	193 SELECT	V Visualizzazione
ESEC_USER	HIST_CORRELATED_EVENTS_RPT_V	193 SELECT	V Visualizzazione
ESEC_USER	HIST_EVENTS	193 SELECT	V Visualizzazione
ESEC_USER	HIST_EVENTS_RPT_V	193 SELECT	V Visualizzazione
ESEC_USER	IMAGES_RPT_V	193 SELECT	V Visualizzazione
ESEC_USER	INCIDENTS_ASSETS_RPT_V	193 SELECT	V Visualizzazione
ESEC_USER	INCIDENTS_EVENTS_RPT_V	193 SELECT	V Visualizzazione
ESEC_USER	INCIDENTS_RPT_V	193 SELECT	V Visualizzazione
ESEC_USER	INCIDENTS_VULN_RPT_V	193 SELECT	V Visualizzazione

Nome ruolo	Nome oggetto	Azione	Tipo
ESEC_USER	L_STAT_RPT_V	193 SELECT	V Visualizzazione
ESEC_USER	LOGS_RPT_V	193 SELECT	V Visualizzazione
ESEC_USER	NETWORK_IDENTITY_RPT_V	193 SELECT	V Visualizzazione
ESEC_USER	ORGANIZATION_RPT_V	193 SELECT	V Visualizzazione
ESEC_USER	PERSON_RPT_V	193 SELECT	V Visualizzazione
ESEC_USER	PHYSICAL_ASSET_RPT_V	193 SELECT	V Visualizzazione
ESEC_USER	PRODUCT_RPT_V	193 SELECT	V Visualizzazione
ESEC_USER	ROLE_RPT_V	193 SELECT	V Visualizzazione
ESEC_USER	SENSITIVITY_RPT_V	193 SELECT	V Visualizzazione
ESEC_USER	STATES_RPT_V	193 SELECT	V Visualizzazione
ESEC_USER	UNASSIGNED_INCIDENTS_RPT_V	193 SELECT	V Visualizzazione
ESEC_USER	USERS_RPT_V	193 SELECT	V Visualizzazione
ESEC_USER	VENDOR_RPT_V	193 SELECT	V Visualizzazione
ESEC_USER	VULN_CALC_SEVERITY_RPT_V	193 SELECT	V Visualizzazione
ESEC_USER	VULN_CODE_RPT_V	193 SELECT	V Visualizzazione
ESEC_USER	VULN_INFO_RPT_V	193 SELECT	V Visualizzazione
ESEC_USER	VULN_RPT_V	193 SELECT	V Visualizzazione
ESEC_USER	VULN_RSRC_RPT_V	193 SELECT	V Visualizzazione
ESEC_USER	VULN_RSRC_SCAN_RPT_V	193 SELECT	V Visualizzazione
ESEC_USER	VULN_SCAN_RPT_V	193 SELECT	V Visualizzazione
ESEC_USER	VULN_SCAN_VULN_RPT_V	193 SELECT	V Visualizzazione
ESEC_USER	VULN_SCANNER_RPT_V	193 SELECT	V Visualizzazione

Ruoli del server di Sentinel

Ruolo del server	Descrizione	Utente di Sentinel
sysadmin	Amministratori del sistema	esecdba
securityadmin	Amministratori della sicurezza	esecapp
serveradmin	Amministratori del server	esecdba
setupadmin	Amministratori della configurazione	
processadmin	Amministratori dei processi	
diskadmin	Amministratori dei dischi	
dbcreator	Creatori di database	
bulkadmin	Amministratori di inserimenti di massa	

Utenti e autorizzazioni di accesso ai database con autenticazione del dominio di Windows

Agli utenti esecadm, esecapp, esecdba e esecrpt viene associato un dominio utente in base alle opzioni specificate in fase di installazione. Gli utenti di questi domini dispongono degli stessi privilegi di quelli specificati nelle sezioni precedenti.

D Tabelle delle autorizzazioni dei servizi Sentinel

NOTA: Il termine agente è equivalente a servizio di raccolta. Si farà in seguito riferimento agli agenti come servizi di raccolta.

Server Sentinel (Motore di correlazione)

Componenti di Sentinel	Applicazione di Sentinel	Servizio di Sentinel	Processo di Sentinel	Riepilogo delle funzioni	Autorizzazioni necessarie	Descrizione delle autorizzazioni
Server Sentinel	-	Sentinel / WatchDog.exe	correlation_engine.exe	Il processo del motore di correlazione (correlation_engine) riceve eventi da Gestione servizi di raccolta di Wizard e pubblica eventi correlati in base a regole di correlazione definite dall'utente.	Accesso alla rete, accesso in lettura ai file di configurazione modificati.	Comunica con Sonic per i processi di configurazione e degli eventi e per la generazione di eventi correlati. Se si utilizza un file di configurazione modificato, necessita dell’autorizzazione di accesso al file.

Gestione servizi di raccolta

Componenti di Sentinel	Applicazione di Sentinel	Servizio di Sentinel	Processo di Sentinel	Riepilogo delle funzioni	Tipo di connettore	Autorizzazioni necessarie	Descrizione delle autorizzazioni
Sentinel Wizard / Gestione servizi di raccolta	-	Gestione servizi di raccolta	agentengine.exe	Il processo di Gestione servizi di raccolta gestisce i motori dei servizi di raccolta (genera i processi del motore dei servizi di raccolta), pubblica i messaggi di stato del sistema, esegue il filtraggio degli eventi e le mappature di riferimento. Il Motore servizi di raccolta esegue uno script del Servizio di raccolta che normalizza gli eventi non elaborati nei dispositivi e sistemi di sicurezza.	**NOTA:** gestione servizi di raccolta necessita di diverse autorizzazioni in base al tipo di connessione.		
					Seriale: lettura di dati da una porta seriale RS-232C	Autorizzazione di lettura/scrittura per una porta seriale	Autorizzazione di lettura/scrittura del Motore servizi di raccolta per una porta seriale
					Socket: una connessione socket TCP	Accesso di rete: lettura/scrittura dal socket di rete - Autorizzazione all'avvio di una connessione	Il Motore servizi di raccolta avvia una connessione a un endpoint di rete e concede le autorizzazioni di lettura/scrittura al socket in questione
					Nuovi nel file nuovo: legge solo i dati degli eventi di sicurezza che vengono aggiunti al file dopo l'avvio dello script (legge a partire dalla fine del file)	Accesso in lettura/scrittura ai file	Il motore del servizio di raccolta legge dal primo file specificato e scrive nel secondo file specificato
					Tutti nel file tutti: legge tutti i dati degli eventi di sicurezza inclusi in un file	Accesso in lettura/scrittura ai file	Il motore del servizio di raccolta legge dal primo file specificato e scrive nel secondo file specificato

Componenti di Sentinel	Applicazione di Sentinel	Servizio di Sentinel	Processo di Sentinel	Riepilogo delle funzioni	Tipo di connettore	Autorizzazioni necessarie	Descrizione delle autorizzazioni
					Processo persistente: avvia un processo persistente al momento dell'avvio della porta, comunica con il Servizio di raccolta assegnato alla porta e con un'applicazione esterna ricevendo e trasmettendo gli stati, continua a eseguire il processo per l'intero esercizio della porta.	Autorizzazione di esecuzione del processo persistente definita. (Nota: Se si utilizza EventLog.exe come processo persistente per raccogliere il log NT mediante WMI, per Gestione servizi di raccolta è necessaria l'autorizzazione di accesso a WMI).	Il motore del servizio di raccolta esegue il processo definito al livello di autorizzazione corrente
					Processo transitorio: comunica con il Servizio di raccolta assegnato alla porta e con un'applicazione esterna ricevendo e trasmettendo gli stati. I processi transitori possono venire avviati più volte.	Autorizzazione di esecuzione del processo transitorio definita.	Il motore del servizio di raccolta esegue il processo definito al livello di autorizzazione corrente
					SNMP: riceve i trap SNMP v1, v2 e v3	Accesso alla rete-Lettura/scrittura dal socket di rete	Gestione servizi di raccolta invia e/o riceve i trap SNMP
					Nessuno	N/D	N/D

Componenti di Sentinel	Applicazione di Sentinel	Servizio di Sentinel	Processo di Sentinel	Riepilogo delle funzioni	Tipo di connettore	Autorizzazioni necessarie	Descrizione delle autorizzazioni
Sentinel Wizard / Generatore servizi di raccolta	Generatore servizi di raccolta	-	agentbuilder.exe	Un'interfaccia utente grafica che consente di creare, configurare e controllare i Servizi di raccolta. L'interfaccia utente grafica può essere utilizzata per eseguire i servizi di raccolta locali o controllare i servizi di raccolta nell'istanza locale di Wizard.	Accesso in lettura/scrittura ai file		Generatore servizi di raccolta dispone dei diritti in lettura/scrittura per gli script di Servizi di raccolta in %WORKBENCH_HOME%/Elements
					Accesso in lettura/scrittura ai file		Generatore servizi di raccolta dispone dei diritti in lettura/scrittura per il file di configurazione della porta in %WORKBENCH_HOME%/Agents
					Accesso in lettura/scrittura ai file		Generatore servizi di raccolta dispone dell'autorizzazione di accesso per %ESEC_HOME%/.uuid
					Accesso di rete: lettura/scrittura dal socket di rete - Autorizzazione all'avvio di una connessione		Generatore servizio di raccolta per caricamento/scaricamento di servizi di raccolta e messaggi sullo stato di Gestione servizi di raccolta ricevuti

Sentinel Communication

Componenti di Sentinel	Applicazione di Sentinel	Servizio di Sentinel	Processo di Sentinel	Riepilogo delle funzioni	Autorizzazioni necessarie	Descrizione delle autorizzazioni
iSCALE / MOM	SonicMQ	Comunicazione di Sentinel	sonicmf.exe	Per Windows, Sentinel Communication rappresenta un servizio e viene chiamato iSCALE, ovvero un middleware di messagistica (Message Oriented Middleware, MOM). Il componente iSCALE fornisce un framework JMS (Java Message Service) per la comunicazione tra processi. I processi comunicano attraverso un broker, responsabile dell'instradamento e della memorizzazione nel buffer dei messaggi. Più broker possono comunicare tra di loro ai fini del passaggio attraverso i firewall e del bilanciamento del carico. I processi di Sentinel utilizzano un meccanismo basato su produttore/sottoscrittore per comunicare tra di loro. Ciò consente a un processo di pubblicare un messaggio su un canale di argomenti usufruibile da più produttori, senza utilizzare il processo produttore che conosce il processo che lo sottoscrive. I sottoscrittori possono ricevere i messaggi pubblicati dai produttori senza conoscere i produttori disponibili. Ciò riduce al minimo la configurazione e aumenta la stabilità e la scalabilità del sistema. Se ad esempio si aggiunge una nuova istanza di Wizard al sistema, non sono necessarie operazioni di configurazione in Sentinel. Il processo del produttore pubblica i messaggi negli argomenti (canale) e i processi del sottoscrittore attivano la sottoscrizione agli argomenti. Il broker dei messaggi instrada i messaggi dai produttori ai sottoscrittori in base agli argomenti registrati.	Autorizzazioni di accesso al proprio database incorporato, alla directory di installazione (%ESEC_HOME%\3rdparty\SonicMQ) e ai file	Sonic consente l'accesso al proprio database incorporato, alla directory di installazione (%ESEC_HOME%\3rdparty\SonicMQ) e ai file

Server di database (senza DAS)

Componenti di Sentinel	Applicazione di Sentinel	Servizio di Sentinel	Processo di Sentinel	Riepilogo delle funzioni	Autorizzazioni necessarie	Descrizione delle autorizzazioni
-	-	-	-	Configurazione del database di Sentinel	-	Richiede che il driver ODBC o Oracle faccia riferimento al database di Sentinel

Server di database (con DAS)

Per un riepilogo e/o un’analisi delle autorizzazioni di accesso al database di Sentinel, vedere i dettagli nella documentazione seguente:
Appendice A: Utenti, ruoli e autorizzazioni di accesso al database di Sentinel

Componenti di Sentinel	Applicazione di Sentinel	Servizio di Sentinel	Processo di Sentinel	Riepilogo delle funzioni	Autorizzazioni necessarie	Descrizione delle autorizzazioni
-	-	-	-	Configurazione del database di Sentinel	-	Richiede che il driver ODBC o Oracle faccia riferimento al database di Sentinel
Server Sentinel	-	Sentinel / WatchDog.exe	das_binary	eventi e operazioni di inserimento di eventi correlati.	Accesso alla rete: necessario l'accesso al DB per l'istanza ESEC come ESECAPP	Comunica con Sonic. Comunica con il database tramite JDBC per il recupero dati e ADO per l'inserimento degli eventi se è impostata la strategia di caricamento ADO.
			das_query	tutte le altre operazioni di database	Accesso alla rete: necessario l'accesso al DB per l'istanza ESEC come ESECAPP; necessaria l'autorizzazione per l'esecuzione di processi	Comunica con Sonic. Comunica con il database tramite JDBC per il recupero dei dati.
			activity_container	esecuzione e configurazione del servizio di attività	Accesso alla rete: necessario l'accesso al DB per l'istanza ESEC come ESECAPP; necessaria l'autorizzazione per l'esecuzione di processi	Comunica con Sonic. Comunica con il database tramite JDBC per il recupero e l'inserimento dei dati.

Per un riepilogo e/o un’analisi delle autorizzazioni di accesso al database di Sentinel, vedere i dettagli nella documentazione seguente:
Appendice A: Utenti, ruoli e autorizzazioni di accesso al database di Sentinel

Componenti di Sentinel	Applicazione di Sentinel	Servizio di Sentinel	Processo di Sentinel	Riepilogo delle funzioni	Autorizzazioni necessarie	Descrizione delle autorizzazioni
			workflow_container	configurazione del servizio di workflow (iTRAC)	Accesso alla rete; necessaria l’autorizzazione di accesso al database per l'istanza ESEC_WF come ESECAPP; necessaria l'autorizzazione per l'esecuzione di processi	Comunica con Sonic. Comunica con il database tramite JDBC per il recupero e l'inserimento dei dati.
			das_rt	configurazione per la funzione Active Views all’interno della console Sentinel Control.	Accesso alla rete: necessario l'accesso al DB per l'istanza ESEC come ESECAPP	Comunica con Sonic. Comunica con il database tramite JDBC per il recupero dei dati.

Server dei rapporti

Componenti di Sentinel	Applicazione di Sentinel	Servizio di Sentinel	Processo di Sentinel	Riepilogo delle funzioni	Autorizzazioni necessarie	Descrizione delle autorizzazioni
-	-	-	-	Crystal Reports XI o Crystal Enterprise 9 Standard è uno degli strumenti per la generazione di rapporti che si integra con Sentinel.	-	Richiede che il driver ODBC o Oracle faccia riferimento al database di Sentinel

Glossario

NOTA: Il termine agente è equivalente a servizio di raccolta. Si farà in seguito riferimento agli agenti come servizi di raccolta.

Advisor

Sistema integrato che include il database delle vulnerabilità SecurityNexus per fornire riferimenti incrociati tra eventi in tempo reale e vulnerabilità note.

Agente

Vedere Servizio di raccolta

Aggregazione e normalizzazione degli eventi

L'aggregazione è il processo che prevede la combinazione di singoli elementi poco rilevanti, con la conseguente creazione di un elemento di grande importanza. Le singole parti di un evento, quali il nome e la data, l'IP di origine, l'IP di destinazione, l'UUID, il tipo di sensore e così via, di per sé non sono particolarmente significative. Se messe insieme, però, possono generare un evento di rilievo che potrebbe attaccare la rete e sfruttarne le risorse.
Il salvataggio di un intero evento comporta la memorizzazione di informazioni doppie. Ad esempio, in un sistema non aggregato di dieci eventi identici, ad eccezione della data, ogni evento viene salvato dieci volte, con gli stessi elementi (nome, tipo di sensore e così via). Con l'aggregazione, gli elementi identici vengono memorizzati una sola volta e si tiene traccia delle operazioni in esecuzione per un'ora.

I dati degli eventi vengono trasformati, riassunti e memorizzati in tabelle riepilogative. I rapporti di riepilogo vengono eseguiti in riepiloghi pre-elaborati, e questo facilita l'esecuzione delle interrogazioni nelle tabelle di eventi in tempo reale. Il motore di aggregazione degli eventi consente di acquisire i dati di eventi binari, trasformarli in una struttura di eventi normalizzata e riassumerli sulla base di un set predefinito di definizioni di riepilogo. Il motore di aggregazione degli eventi consente l'elaborazione degli eventi quasi in tempo reale con un overhead minimo rispetto al sistema Sentinel in tempo reale.

Analisi

Sentinel Control Center consente di eseguire rapporti cronologici. I rapporti cronologici e sulle vulnerabilità sono pubblicati su un server Web Crystal®, vengono eseguiti direttamente sul database e sono visualizzati nelle schede Analisi e Advisor della barra di spostamento in Sentinel Control Center.

Buffer di ricezione

Fa parte di Gestione servizi di raccolta e per default contiene 50.000 eventi. Il buffer di ricezione è un parametro modificabile, che ha una dimensione minima di 5.000 eventi.

Casi

Si tratta di una funzione molto utile per raggruppare una serie di eventi che rappresenti un interesse comune (gruppo di eventi analoghi o serie di differenti eventi che indicano uno schema di interesse, ad esempio un attacco).

Comando di analisi

È un'interfaccia di script di alto livello che in Wizard consente di manipolare i dati. Il processo di analisi prevede la suddivisione di un evento in più parti.

Configurazione di eventi

La configurazione degli eventi (parte del servizio di mappatura) consente:

- il monitoraggio della conformità alle normative di legge
- la conformità ai criteri
- la prioritizzazione delle risposte
- l'analisi dei dati di sicurezza relativi alle attività aziendali
- L'ottimizzazione della contabilità

Tramite la configurazione di eventi, è possibile assegnare un nome alle etichette esistenti. È possibile ad esempio rinominare Ct2 con City. Le modifiche sono applicate ai filtri e alle regole di correlazione.

Controller di dati

Vedere Processo di sincronizzazione dei dati.

CorrelatedEventUUID (UUID eventi correlati)

Identificatore dell'evento correlato generato dalla regola attivata.

Correlazione

Il processo di analisi degli eventi di sicurezza per identificare le potenziali relazioni tra due o più eventi. Tramite la correlazione, è possibile eseguire una rapida associazione degli attacchi di priorità sulla base degli elementi comuni dei dati di eventi. Utilizzando la correlazione, è possibile identificare in modo più efficace le tendenze o i pattern tra gli eventi di livello inferiore progettati per funzionare al di sotto delle soglie di sicurezza.

Sentinel fornisce cinque tipi di regole di correlazione, ovvero:

- Watchlist
- Correlazione di base
- Correlazione avanzata
- RuleLg in formato libero

das_aggregation.xml

Utilizzato per le operazioni di aggregazione.

das_binary.xml

Utilizzato per gli eventi e le operazioni di inserimento di eventi correlati.

das_itrac.xml

Utilizzato per eseguire e configurare il servizio di attività e per configurare il servizio di workflow.

das_query.xml

Specifica i parametri di configurazione per il servizio DAS (Data Access Service), un componente del database di Sentinel.

das_rt.xml

Specifica la configurazione per la funzione Active Views all'interno della console di controllo di Sentinel.

Eventi di sistema

Gli eventi interni o di sistema consentono di fornire rapporti sullo stato del sistema e sulle modifiche a esso apportate. Il sistema può generare due tipi di eventi, ovvero:

- Eventi interni
- Eventi di prestazioni

Gli eventi interni sono informativi e descrivono un singolo stato o una modifica allo stato del sistema. Segnalano inoltre quando un utente effettua il login o non riesce a completare l'autenticazione e indicano l'avvio di un processo o l'attivazione di una regola di correlazione. Gli eventi di prestazioni sono generati periodicamente e descrivono le risorse mediamente utilizzate dai diversi componenti del sistema.

Eventi interni

Vedere Eventi di sistema.

Evento

Per evento s'intende un'azione o un'occorrenza rilevata da un dispositivo di sicurezza (evento esterno) o da processo (evento interno). Gli eventi possono essere legati alla sicurezza, alle prestazioni o alle informazioni. Un evento esterno, ad esempio, potrebbe essere un attacco rilevato da un sistema di rilevamento delle intrusioni (IDS), un login avvenuto correttamente rilevato da un sistema operativo o da una situazione definita da un cliente, come ad esempio l'apertura di un file da parte di un utente. Gli eventi legati alle informazioni sono eventi interni. Questo tipo di eventi indica un cambiamento nello stato di un processo, come ad esempio la chiusura di una porta.

File dei modelli

Per i Servizi di raccolta, è possibile creare, modificare, eliminare e aggiungere stati ai modelli. I modelli determinano il modo in cui i record vengono elaborati. La maggior parte delle decisioni relative ai modelli dipende dal tipo di record utilizzato e dal relativo formato. È disponibile un file di modelli equivalente con estensione .tem,

I file dei modelli si basano sugli stati. Uno stato è un punto di decisione all'interno del flusso o del percorso logico di un modello. Ogni punto (stato) contiene informazioni che indicano il processo successivo da eseguire. Gli stati contengono parametri e, quando il modello viene unito a un file di parametri, i valori specifici sostituiscono i parametri stessi. In questo caso, vengono creati uno o più file di script.

Quando uno stato viene inserito in un modello, gli viene assegnato un numero che rimarrà invariato, indipendentemente dalla posizione nella quale esso viene spostato all'interno del modello.

File dei parametri

Per i Servizi di raccolta, i file dei parametri (file .par) corrispondono a tabelle utilizzate per definire i nomi dei parametri nei file di script da eseguire associati. Essi sono utilizzati quando il codice di analisi contiene riferimenti I parametri sono equivalenti alle variabili e sono memorizzati come stringhe. È necessario convertire i valori numerici in stringhe affinché sia possibile utilizzarli. Quando vengono immessi nuovi valori per i parametri, essi diventano effettivi dopo la creazione dello script e, durante questo processo, vengono uniti al file dei modelli.

I nomi dei file di script da eseguire sono visualizzati nella prima riga della tabella, mentre i nomi dei parametri o etichette sono riportati nella prima colonna. La seconda riga della tabella è utilizzata per definire le icone visualizzate nell'albero del Servizio di raccolta. L'altra riga si riferisce allo script in questione e definisce le variabili o i valori dei parametri da utilizzare come parametri.

I file dei parametri contengono i valori seguenti:

- Tag META, informazioni e commenti: sono disponibili oltre 200 tag META, di cui 100 possono essere configurati dall'utente e gli altri sono riservati.
- Regola: i nomi dei file delle serie sono visualizzati nella riga di intestazione della tabella, mentre i parametri sono riportati nella prima colonna.
- Bitmap: la seconda riga della tabella definisce le bitmap utilizzate per il file in questione, visualizzate nell'elenco Servizi di raccolta.

File di mappatura

Per i Servizi di raccolta, i file di mappatura sono file opzionali (.csv) che consentono di eseguire una ricerca rapida delle voci chiave. Il file .csv è il percorso relativo di una directory di script del Servizio di raccolta. Attualmente questi file non possono essere modificati all'interno di Generatore servizi di raccolta, bensì utilizzando Excel.

File di ricerca

Per i Servizi di raccolta, i file di ricerca sono tabelle facoltative (file .lkp) sulle quali vengono confrontati i valori ricevuti per determinare quali azioni intraprendere, se necessario, in risposta agli eventi di sicurezza. I file di ricerca contengono clausole match utilizzate per confrontare le singole stringhe. Sulla base delle clausole match di un file di ricerca specifico e i dati ricevuti dai sensori, il comando LOOKUP determina se la stringa di ricerca è presente o assente.

I comandi di analisi possono eventualmente essere associati alla stringa match. I comandi di analisi vengono eseguiti se si trova una corrispondenza.

File di script

In Wizard, è un file compilato (*.asd) composto dai file dei modelli, dei parametri, di ricerca e di mappatura di Servizio di raccolta.

Generatore agenti

Vedere Generatore servizi di raccolta

Generatore servizi di raccolta

Interfaccia utente grafica che consente di creare Servizi di raccolta basati su regole per raccogliere, filtrare e normalizzare i dati provenienti da fonti diverse e comunicare in maniera sicura al server Sentinel le informazioni di rilievo che possono essere impiegate per monitorare il traffico.

Gestione agenti

Gestione servizi di raccolta

Gestione delle interrogazioni (query_manager)

Il servizio di gestione delle interrogazioni (query_manager) riceve richieste di interrogazioni rapide e di drill down da Sentinel Control Center e le invia al database tramite DAS. Le richieste ricevute da Sentinel Control Center definiscono gli eventi necessari per mezzo di criteri o filtri. Se si utilizza un filtro, il servizio di gestione delle interrogazioni ne recupera la definizione e lo converte in un criterio xml. Il servizio di gestione delle interrogazioni poi invia la richiesta al database. Non è possibile convertire completamente tutti i filtri in criteri xml. Se un filtro viene convertito interamente, il servizio di gestione delle interrogazioni indica a DAS di inviare la risposta direttamente a Sentinel Control Center. Se il filtro contiene espressioni regolari che non possono essere convertite in criteri xml, il servizio di gestione delle interrogazioni effettua le conversioni possibili e genera un criterio xml conservativo che restituisce un superset degli eventi richiesti. In tal caso, DAS viene istruito a restituire il risultato al servizio di gestione delle interrogazioni. Una volta ricevuta la risposta, il servizio di gestione delle interrogazioni la filtra nella memoria e invia gli eventi che soddisfano le condizioni di filtro a Sentinel Control Center.

Gestione delle risorse

La funzione di gestione delle risorse ha lo scopo di collegare uno o più eventi alle risorse e alle informazioni sulle vulnerabilità per creare un metodo che consenta di proteggere in modo efficiente le risorse di un’organizzazione. Le risorse possono essere fisiche e software. Le risorse fisiche sono rappresentate da componenti hardware mentre le risorse software sono servizi e applicazioni.

Gestione filtri

I filtri di Sentinel consentono di elaborare i dati sulla base di criteri specifici sia per gli eventi in ingresso nel sistema sia per gli utenti del sistema. Esistono filtri di livelli diversi:

- Servizio di raccolta: eseguito tramite lo script che utilizza Generatore servizi di raccolta
- Filtro globale: applicato in eguale misura a tutti gli eventi generati da tutte le istanze di Wizard del sistema. Solo gli eventi che superano i filtri globali vengono inviati a tutti i processi di Sentinel.
- Filtro di sicurezza: assegnato agli utenti attivi. Questo filtro limita gli eventi che un utente attivo può osservare ed è assegnato dall'amministratore.
- Filtro di visualizzazione: applicato all'interfaccia. Questo filtro consente di definire le finestre degli eventi per l'analisi in tempo reale e deve essere applicato da ogni utente.

Esistono due tipi di filtri:

- Pubblici, ovvero di proprietà del sistema. I filtri pubblici possono essere utilizzati come filtri di sicurezza o filtri di visualizzazione. I filtri di sicurezza sono basati sulle autorizzazioni utente. I filtri di visualizzazione determinano gli eventi che sono illustrati nelle tabelle di eventi in tempo reale e nei grafici.
- Privati, ovvero di proprietà dell'utente. Si tratta di filtri di visualizzazione che possono essere condivisi se si dispone dell'autorizzazione a visualizzarli.

Gestione servizi di raccolta

Il back end di Wizard che gestisce i Servizi di raccolta e i messaggi sullo stato del sistema.

Host Wizard

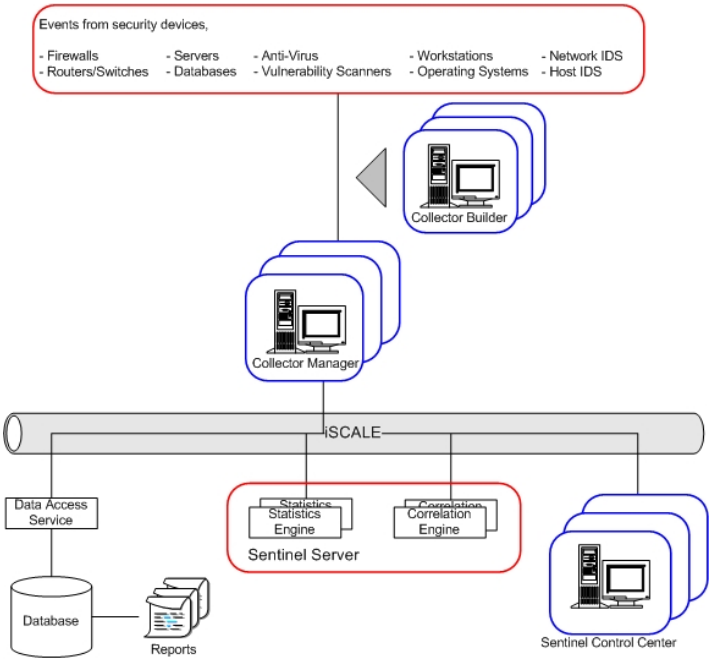
Una macchina in cui è installato il software Gestione servizi di raccolta.

Interrogazione rapida

Vedere Gestione delle interrogazioni.

iSCALE™

Il bus messaggi fornisce un framework JMS (Java Message Service) per la comunicazione tra processi. I processi comunicano attraverso un broker, responsabile dell'instradamento e della memorizzazione nel buffer dei messaggi. Più broker possono comunicare tra di loro ai fini del passaggio attraverso i firewall e del bilanciamento del carico.



I processi seguenti comunicano tra loro tramite il bus messaggi.

- Sorveglianza
- Prestazioni evento (Motore filtri)
- Numero eventi nel tempo (motore di statistiche)
- Sincronizzazione dei dati (controller di dati)
- Motore di correlazione
- Verifica RuleLg (verifica di regole di correlazione)
- Servizio DAS (Data Access Service)
- Gestione delle interrogazioni

iTRAC™

iTRAC consente di automatizzare le procedure e rispondere agli eventi indesiderati. Sentinel fornisce un sistema di gestione del workflow che consente l'automazione procedurale del processo di gestione degli eventi indesiderati SANS. I componenti principali di iTRAC sono:

- Azioni elenco di lavoro: applicazione utilizzata per spostarsi da un'attività a un'altra.
- Generatore attività: applicazione utilizzata per creare una versione personalizzata di iTRAC.
- Monitoraggio processo: consente il monitoraggio delle attività (passaggi) svolte per completare un processo.

Metadati

I metadati sono informazioni sui dati, nomi variabili predefiniti per metadati. L'indirizzo IP di origine di un attacco viene memorizzato, ad esempio, nel tag META SourceIP. I nomi di prodotti vengono memorizzati nel tag META ProductName. I dati utilizzati per compilare i tag META vengono estratti dai dati degli eventi o impostati come parte dell'elaborazione del Servizio di raccolta.

Middleware orientato ai messaggi

Vedere iSCALE™.

MOM

Vedere iSCALE™.

Motore agenti

Vedere Motore servizi di raccolta

Motore del servizio di correlazione

Consente di elaborare la logica dei modelli per ogni porta. Ogni Motore servizi di raccolta gestisce la propria porta.

Motore di correlazione

Il Motore di correlazione effettua l'analisi degli eventi in ingresso per individuare pattern di rilievo ed esegue il drill-down su eventi di correlazione per determinare quali dettagli abbiano attivato una regola.

Motore di statistiche

Vedere il processo Numero eventi nel tempo.

Motore filtri

Vedere la sezione relativa all'elaborazione delle prestazioni degli eventi.

Motore filtri

Vedere la sezione relativa all'elaborazione delle prestazioni degli eventi.

Normalizzazione eventi

Vedere Aggregazione

Numero ID evento

Un numero assegnato a un evento.

Porta

In Wizard, le porte consentono al Servizio di raccolta di individuare i dati degli eventi di sicurezza nella rete fornendo l'indirizzo IP e altre informazioni sull'origine (dispositivo di sicurezza [router, IDS, switch, e altri dati]). Ogni riga della tabella Configurazione porta esegue uno script del servizio di raccolta per un'origine eventi.

Processo DAS (Data Access Service)

Il processo DAS (Data Access Service) è il servizio di persistenza del server Sentinel che fornisce un'interfaccia bus messaggi (iSCALE) al database. Garantisce l'accesso basato su dati al database backend. Riceve la richiesta XML dai diversi processi Sentinel, la converte in un'interrogazione sul database, elabora il risultato prodotto dal database e lo converte in una risposta XML. Supporta richieste di recupero di eventi per l'interrogazione rapida e il drill-down, di recupero di informazioni sulle vulnerabilità e su Advisor e di manipolazione delle informazioni di configurazione. DAS gestisce inoltre la registrazione di tutti gli eventi ricevuti da Gestione servizi di raccolta di Wizard e le richieste di recupero e memorizzazione delle informazioni di configurazione.

Processo del motore di correlazione (correlation_engine)

Il processo del motore di correlazione (correlation_engine) riceve eventi da Gestione servizi di raccolta di Wizard e pubblica eventi correlati in base a regole di correlazione definite dall'utente.

Processo di sincronizzazione dei dati (controller di dati)

Il processo di sincronizzazione dei dati (data_synchronizer) gestisce la modifica dei dati di configurazione da parte di più utenti. Quando un utente richiede di modificare i dati tramite Sentinel Control Center, il record dei dati viene bloccato da data_synchronizer. I dettagli di chi ha bloccato i dati sono pubblicati su altri Sentinel Control Center attivi, e nessun altro utente può modificare quei dati. Se un Sentinel Control Center viene chiuso prima che i dati in esso contenuti vengano sbloccati, i dispositivi di bloccaggio non saranno più validi.

Processo di verifica RuleLg (rulelg_checker)

Il processo di verifica RuleLg (rulelg_checker) consente di convalidare le espressioni dei filtri e delle regole di correlazione. Sentinel Control Center utilizza questi risultati per stabilire se sia possibile salvare un filtro o una regola di correlazione.

Processo watchdog

Il processo watchdog di Sentinel consente la gestione di tutti gli altri processi del server. Se si interrompe un altro processo, il servizio di sorveglianza lo riavvia.

Puntatore del buffer di ricezione

Il puntatore del buffer di ricezione fa riferimento a byte di dati nel buffer di ricezione. Prima di ogni stringa di decisione valutata, il puntatore del buffer di ricezione viene reimpostato sul valore di attesa, in genere zero.

Regola di correlazione avanzata

Consente di creare una regola di correlazione che includa tutte le funzioni di una regola di correlazione semplice, nonché inviare un evento quando in un set di eventi i valori dei tag META sono differenti, ad esempio quando un sensore è all’interno o all’esterno del firewall. Una regola di correlazione avanzata consente, ad esempio, di cercare eventi provenienti dallo stesso indirizzo IP di origine e diretti allo stesso indirizzo IP di destinazione, che abbiano lo stesso nome e che si verifichino sia all'interno che all'esterno di un firewall, ad indicare un attacco realizzato attraverso il firewall.

Regola di correlazione base

Consente di selezionare uno dei tag META per creare una regola di correlazione che permetta di conteggiare il numero di volte in base al quale alcune condizioni vengono soddisfatte in un intervallo di tempo specifico. Una regola di correlazione base consente, ad esempio, di cercare lo stesso indirizzo IP di origine segnalato cinque volte in cinque minuti, anche se gli eventi si riferiscono a prodotti differenti, come un sistema di rilevazione delle intrusioni (IDS) e un firewall.

Regola di correlazione watchlist

Consente di specificare una stringa di testo che verrà cercata dal motore di correlazione in ogni tag META per ogni evento in entrata. Una regola watchlist, ad esempio, è in grado di cercare un indirizzo IP di origine specifico di un pirata informatico e inviare una notifica all'utente ogni volta che l'indirizzo IP è presente in un messaggio di eventi.

Rilevamento degli exploit

Vedere Servizio di mappatura.

Rilevanza aziendale

Vedere Servizio di mappatura.

Router eventi

Router eventi esegue la trasformazione e il filtraggio della mappatura degli eventi.

Sentinel Control Center

Sentinel Control Center è la console di gestione centrale in cui è possibile visualizzare riepiloghi e rapporti cronologici, filtrare eventi in tempo reale e creare casi. Sentinel Control Center consente la visualizzazione in tempo reale di eventi, fornisce una panoramica di sistema delle modifiche apportate alle attività determinate dalle impostazioni dei Servizi di raccolta, consente l'amministrazione di filtri, la creazione di rapporti, l'impiego di regole correlate e filtri globali e la gestione degli eventi di sicurezza tramite casi.

Sequenze (avvio e backout)

Le sequenze di avvio e backout vengono assegnate a una porta, che esegue la serie di script al suo interno quando viene avviata o arrestata. Per essere utilizzato da una porta, lo script deve essere incluso in una sequenza di avvio o di backout. Le porte consentono ai Servizi di raccolta di individuare gli host di Wizard all'interno della rete grazie all'indirizzo IP o al nome degli host in questione. Esse forniscono inoltre a Sentinel le informazioni relative alla posizione dei sensori e al Servizio di raccolta utilizzato per gestire i dati provenienti da questi ultimi. È possibile configurare le opzioni seguenti per le porte:

- Tipo di connessione
- Nome del processo
- Informazioni sul socket
- Informazioni SNMP
- Nomi dei file di input/output
- Nome servizio di raccolta

Sequenze di avvio

Vedere Sequenze.

Sequenze di backout

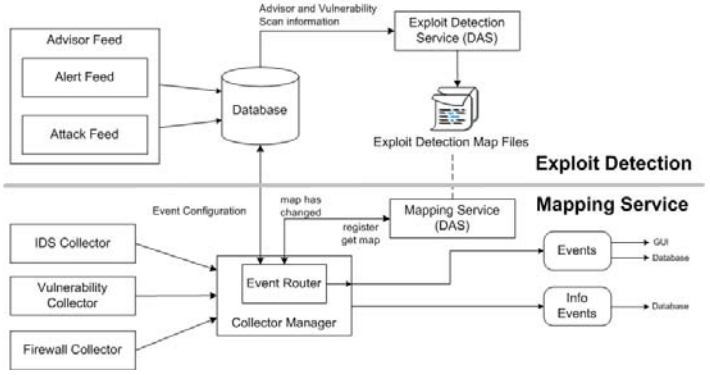
Vedere Sequenze.

Server Sentinel

Il server Sentinel riceve da Gestione servizi di raccolta di Wizard le informazioni sugli eventi normalizzati reperite dai Servizi di raccolta. Il server Sentinel collega tali eventi per individuare pattern e identificare eventuali minacce e crea rapporti su dati in tempo reale e informazioni sulla cronologia che è possibile visualizzare in Sentinel Control Center.

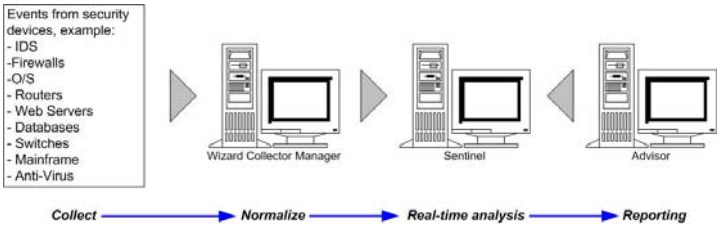
Servizio di mappatura

Il servizio di mappatura di Sentinel consente la notifica immediata e processabile degli attacchi ai sistemi vulnerabili. Fornisce un collegamento in tempo reale tra gli eventi e i risultati di scansione delle vulnerabilità, in modo che gli utenti ricevano una notifica automatica e immediata di un tentativo di attacco rivolto a sfruttare un sistema vulnerabile. Ciò consente di rispondere agli eventi indesiderati in modo più efficace, aumentando così la disponibilità dei sistemi critici e fornendo una sicurezza più efficiente in termini di costi.



Servizio di raccolta

Un Servizio di raccolta raccoglie e normalizza gli eventi non elaborati da programmi e dispositivi di sicurezza e fornisce in output eventi normalizzati che possano essere correlati, segnalati e utilizzati per rispondere ai casi.



Esistono tre livelli di Servizi di raccolta, ovvero:

- Servizi di raccolta supportati (L1)
- Servizi di raccolta documentati (L2)
- Servizi di raccolta di esempio (L3)

I Servizi di raccolta sono composti da:

- file dei modelli
- file dei parametri
- file di ricerca
- file di mappatura

Tag META

I tag META memorizzano metadati.

Tempo reale evento

Fornisce la possibilità di monitorare gli eventi che si verificano mediante interrogazioni. Il monitoraggio degli eventi può essere eseguito in una tabella oppure attraverso una rappresentazione grafica 3-D.

Visualizzazione delle vulnerabilità

Rappresentazione grafica dei dati di eventi in tempo reale sui sistemi vulnerabili che consente di evidenziare le vulnerabilità correnti e di tempo.

Wizard

Generatore servizi di raccolta e Gestione servizi di raccolta.

Workflow

Vedere iTRAC™.