Novell

Software per Open Enterprise™

Note di rilascio relative al prodotto

Sentinel™ 5.1.3 con iTRAC™

NOTA: per scaricare le versioni delle Note di rilascio in lingua tedesca, francese, italiana, spagnola o ortoghese, visitare il sito all'indirizzo http://www.novell.com/documentation/sentinel5.

Descrizione

Il presente prodotto costituisce una release completa di Sentinel 5.1.3 con iTRAC.

Questa release supporta i tipi di installazione seguenti:

- Nuova installazione di Sentinel 5.1.3 su Windows, Solaris e Linux (Novell SUSE Linux Enterprise Server 9 e RedHat).
- Upgrade con migrazione dei dati da Sentinel 4.2.x a Sentinel 5.1.3 su Windows e Solaris.
- Installazione di componenti aggiuntivi di Sentinel 5.1.3 in un'installazione esistente di Sentinel 5.1.3 su Windows, Solaris e Linux.

NOTA: se si dispone di un'installazione di Sentinel 5 precedente alla versione 5.1.3 e si desidera applicarvi una patch per eseguire l'upgrade alla versione 5.1.3, è necessario utilizzare a tale scopo un apposito programma di installazione di patch di Sentinel 5.1.3. Il programma di installazione di Sentinel 5.1.3 fornito con le presenti note di rilascio non consente l'installazione di patch. Per ottenere il programma di installazione delle patch di Sentinel 5.1.3, contattare il supporto tecnico.

Sistemi operativi e patch

Di seguito sono elencati i sistemi operativi e i database per le versioni localizzate di Sentinel 5.1.3. Le informazioni relative alla versione in lingua inglese si trovano nella Guida all'installazione.

- **Sistemi operativi server:**
  - SLES 9 SP3 (tedesco, francese, italiano, spagnolo, portoghese (Brasile))
  - Solaris 9 (tedesco, francese, italiano, spagnolo, portoghese (Brasile))
  - MS Windows Server 2003 SP1 (tedesco, francese, italiano, spagnolo, portoghese (Brasile))
  - MS Windows 2000 Server SP4 (tedesco, francese, italiano, spagnolo, portoghese (Brasile))

- **Sistemi operativi client:**
  - MS Windows 2000 Professional SP4 (tedesco, francese, italiano, spagnolo, portoghese (Brasile))
  - MS Windows XP Professional SP2 (tedesco, francese, italiano, spagnolo, portoghese (Brasile))
  - Solaris 9 (tedesco, francese, italiano, spagnolo, portoghese (Brasile))

- **Database:**
  - Oracle 9.2.0.7 (solo in lingua inglese)
  - MS SQL 2000 SP3a (solo in lingua inglese)

Installazione

Le istruzioni per l'installazione di questa release si trovano nella Guida all'installazione di Sentinel 5.1.3.

Per eseguire una nuova installazione di Sentinel, attenersi alle istruzioni fornite in uno dei capitoli seguenti, a seconda della piattaforma su cui verrà eseguito il programma.

- Capitolo 3: Installazione di Sentinel 5 per Oracle su Solaris
- Capitolo 4: Installazione di Sentinel 5 per Oracle su Linux
- Capitolo 5: Installazione di Sentinel 5 per MS SQL

Le operazioni seguenti devono essere eseguite nell'ambito delle attività preliminari all'installazione di Oracle su Linux. Questa modifica è relativa a Oracle Doc ID: Note:293988.1.

- In SUSE Linux Enterprise Server 9 SP2, aggiungere l'impostazione dei parametri del kernel seguente al file “etc/sysctl.conf”
  ```
  # Oracle requires MLOCK privilege for hugetlb memory.
  vm.disable_cap_mlock=1
  ```
- Eseguire il comando seguente per caricare le modifiche nel file “/etc/sysctl.conf”:
  ```
  sysctl -p
  ```

Per eseguire un upgrade con migrazione dei dati da un'installazione esistente di Sentinel 4.2.x a Sentinel 5.1.3, attenersi alle istruzioni fornite in uno dei capitoli seguenti, a seconda della piattaforma su cui verrà eseguito il programma.

- Capitolo 6: Migrazione di dati e patch per Oracle su Solaris
- Capitolo 7: Migrazione di dati e patch per MS SQL

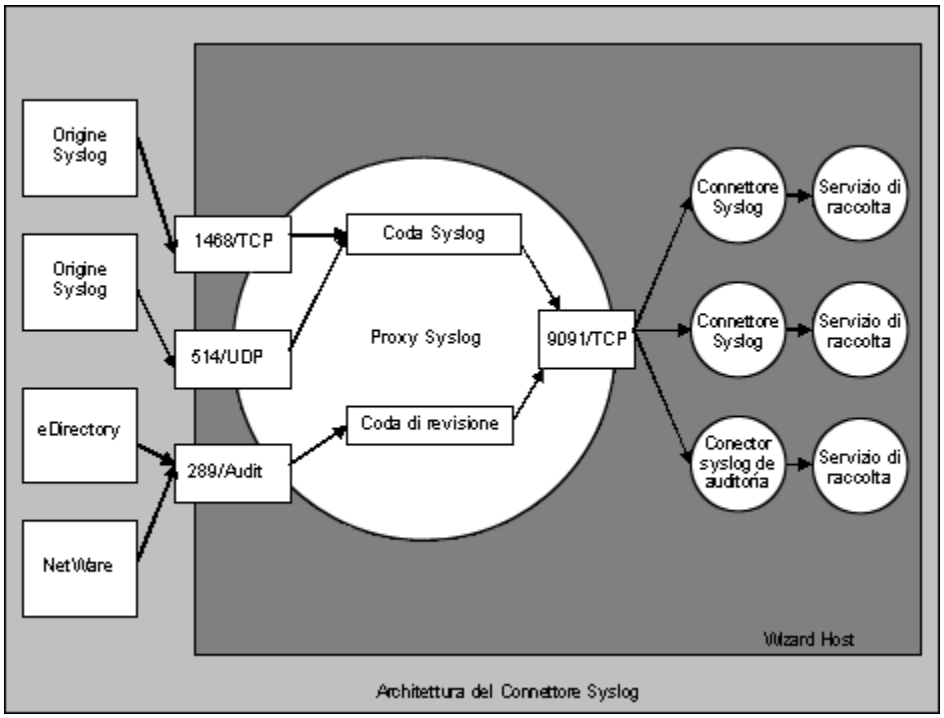
Per installare componenti aggiuntivi di Sentinel 5.1.3 in un'installazione esistente di Sentinel 5.1.3, attenersi alle istruzioni fornite nel capitolo seguente:

- Capitolo 14: Aggiunta di componenti a un’installazione esistente

Per installare componenti aggiuntivi di Sentinel 5.1.3 in un'installazione esistente di una versione precedente di Sentinel 5, applicare prima la patch per l'upgrade di Sentinel alla versione 5.1.3 mediante l'apposito programma di installazione, quindi seguire le istruzioni fornite nei capitoli indicati sopra.

Nuove funzioni

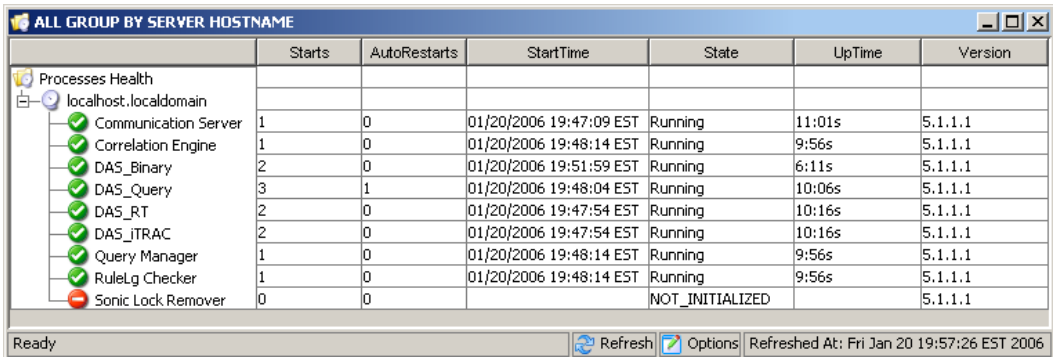
- In questa release è stato aggiunto il supporto per diverse lingue, tra cui portoghese (Brasile), francese, italiano, tedesco, spagnolo e inglese, alla console di controllo di Sentinel e a Gestione dati Sentinel.
- Il connettore syslog è stato migliorato per consentire la gestione delle applicazioni di strumentazione NAudit. A tale miglioramento si aggiunge un agente in grado di elaborare i dati NAudit in generale e in particolare per le applicazioni seguenti: eDirectory, Netware, Identity Manager, Secure Login e Access Manager. Altri miglioramenti sono:
  - Applicazione di filtri al corpo dei messaggi syslog mediante espressioni regolari.
  - Connettore del servizio di raccolta per la riconnessione automatica al server syslog.
  - Controllo di flusso per le connessioni TCP allo scopo di impedire la perdita di dati in seguito all'esaurimento della capacità del buffer dei messaggi. Questa funzione è relativa alle connessioni NAutid e TCP di syslog.



Architettura del Connettore Syslog

- Il connettore syslog viene ora installato con script eseguibili su Windows e UNIX, nonché con file di configurazione migliorati. L'installazione del server proxy syslog come servizio è stata inoltre semplificata. Per installare il server proxy syslog come servizio con la configurazione di default, eseguire i comandi seguenti:
  - In Windows:
    1. Eseguire l'accesso come utente Administrator.
    2. Eseguire cd /d %ESEC_HOME%\wizard\syslog
    3. Eseguire .\syslog-server.bat install
  - In UNIX:
    4. Eseguire il login come utente radice.
    5. Eseguire cd $ESEC_HOME/wizard/syslog
    6. Eseguire ./syslog-server.sh install
- I nuovi comandi di script dell'agente encodemime e decodemime aggiungono capacità di codifica e decodifica in base 64.
- Il limite di lunghezza dei campi CV30-CV34 è stato esteso da 255 a 4000 caratteri.

- In questa release è stato aggiunto il supporto per l'installazione del database di Sentinel direttamente nel server di database MS SQL 2005.
- È stata aggiunta una nuova visualizzazione server alla scheda Amministrazione di Sentinel Control Center. Questa schermata offre le funzionalità seguenti:
  - Una visualizzazione dello stato di tutti i processi del server Sentinel nel sistema (richiede il privilegio Amministrazione > Visualizzazioni server > Visualizzazione server). È analoga alla visualizzazione esistente dei servizi di raccolta, tuttavia consente di visualizzare i processi del server Sentinel.
  - Consente di avviare, arrestare o riavviare i processi (richiede la visualizzazione con privilegi Amministrazione > Visualizzazioni server > Controllo server).



- I prompt delle password per i connettori dei processi di Wizard seguenti sono stati migliorati per tentare di mascherare la password durante la digitazione nella riga di comando.
  - dbconnector
  - rdep_client
- Il componente che genera il file di rilevamento degli exploit attackNormalization.csv è stato modificato affinché utilizzi una quantità inferiore di memoria. Ciò consente di ottenere prestazioni migliori su hardware dimostrativo.
- Ulteriori opzioni di configurazione relative ai processi nel file configuration.xml:
  - name [default: “Uknown”]: il nome dei processi. Si tratta di un nome descrittivo assegnato al processo affinché venga utilizzato nei file di log e nella visualizzazione server di Sentinel Control Center.
  - auto_restart_threshold [default: “5,10”]: il formato del valore è “<num. riavvii>,<num. minuti>”. Se il processo viene riavviato automaticamente (a causa, ad esempio, dell'arresto del processo in modo automatico o mediante un comando del sistema operativo), un numero di volte superiore al numero di riavvii specificato entro il numero di minuti impostato, il processo non verrà più riavviato. In questo modo è possibile impedire il riavvio continuo del processo nel caso di probabili errori di configurazione. In questi casi, viene generato un evento interno denominato “ProcessAutoRestartError”.
  - depends [default: <nessuna dipendenza>]: il formato del valore è un elenco separato da virgole di nomi di processi, come specificati dal nuovo attributo di processo “name”. I processi specificati nell'elenco devono essere eseguiti affinché questo processo possa essere eseguito correttamente.
  - type [default: “normal”]: i valori validi sono “normal” o “container”. Il valore “container” specifica che si tratta di un processo di container eSecurity, ovvero viene avviato mediante il file XML del container, il quale può essere arrestato senza problemi mediante l'invio di un messaggio di arresto al container stesso. Il valore “normal” indica tutti gli altri processi.

- Le funzionalità dei processi seguenti sono state riscritte in Java allo scopo di offrire prestazioni migliori o di ridurne la complessità:
  - sorveglianza
  - data_synchronizer (parte ora di DAS).
- Le funzioni dei servizi di base di Sentinel precedentemente disponibili tramite installazione separata sono state incorporate nell'installazione di DAS. I processi precedentemente attivati tramite l'installazione dei servizi Sentinel di base verranno ora attivati se si seleziona DAS per l'installazione. In questo modo è stato possibile ridurre la complessità del programma di installazione. L'installazione separata di questi componenti non offre infatti alcun vantaggio evidente.
- La verifica delle licenze è stata migliorata in modo da controllare il codice di licenza specificato dall'utente su tutte le schede di interfaccia di rete (NIC) disponibili. Se una qualsiasi delle schede NIC dispone dell'indirizzo MAC corretto, la verifica della licenza avrà esito positivo.

Correzione di bug

Sentinel

7424

Problema: assenza di alcuni dati durante la generazione di exploitDetection.csv.

Correzione: il generatore di rilevamento degli exploit è stato corretto in modo da aggiungere i dati mancanti al file exploitDetection.csv.

7460

Problema: in UNIX, non è possibile avviare automaticamente Communication Server se quest'ultimo viene installato separatamente. Il problema si verifica poiché in questo caso non viene installato il processo “watchdog” responsabile dell'avvio di Communication Server su UNIX.

Correzione: spostamento del componente Communication Server nella sezione del programma di installazione relativo ai servizi Sentinel per garantire l'installazione di “watchdog”.

7463

Problema: il generatore di rilevamento degli exploit avvia una seconda rigenerazione anche se non è in corso alcuna elaborazione, determinando in questo modo un ulteriore utilizzo della CPU per l'interrogazione di DAS.

Correzione: il generatore di rilevamento degli exploit elabora ora una sola rigenerazione alla volta.

SEN-2819

Problema: durante l'aggiunta delle partizioni, lo stato di Gestione dati Sentinel rimane allo 0%.

Correzione: il valore percentuale aumenta in base allo stato di completamento dell'attività di Gestione dati Sentinel.

SEN-3684

Problema: il tipo di argomento delle attività di comando dei casi non funzionano.

Correzione: tutti i parametri (None, Incident Output e Custom) come tipi di argomento ora funzionano.

SEN-3713

Problema: il rilevamento degli exploit rileva un solo attacco per ogni vulnerabilità.

Correzione: il rilevamento degli exploit rileva ora tutti gli attacchi collegati a una vulnerabilità nel feed di Advisor come exploit della vulnerabilità stessa, se quest'ultima è stata segnalata sul computer che subisce l'attacco.

SEN-3732

Problema: non è più possibile selezionare lo stato “Rifiutato” nella gestione dei casi dell'interfaccia utente grafica di Sentinel.

Correzione: lo stato “Rifiutato” è stato aggiunto alla gestione dei casi dell'interfaccia utente grafica di Sentinel.

SEN-3760

Problema: problema durante il passaggio di parametri contenenti spazi all'esecuzione di script tramite il menu di scelta rapida o le regole di correlazione.

Correzione: correzione dell'esecuzione tramite i comandi del menu di scelta rapida e delle regole di correlazione per consentire la corretta gestione degli spazi.

SEN-3763

Problema: il rilevamento degli exploit talvolta non funziona a causa della presenza di più ID di attacchi normalizzati per ogni nome di attacco al dispositivo.

Correzione: il rilevamento degli exploit rileva ora tutti gli attacchi collegati a una vulnerabilità nel feed di Advisor come exploit della vulnerabilità stessa, se quest'ultima è stata segnalata sul computer che subisce l'attacco.

SEN-3764

Problema: limite della frequenza con cui i dati di rilevamento degli exploit vengono rigenerati.

Correzione: la rigenerazione è ora limitata per default a una volta ogni 30 minuti. È possibile configurare il limite modificando il file das_query.xml.

SEN-3766

Problema: quando la chiamata DAS RT per il recupero delle preferenze utente ha esito negativo, vengono eliminati tutti i filtri permanenti.

Correzione: la gestione degli errori è stata migliorata in modo che i filtri permanenti non vengano rimossi in caso di esito negativo del recupero delle preferenze utente.

SEN-3775 (miglioramento)

Problema: elaborazione delle trasformazioni di evento per servizi di mappatura con dipendenze cicliche.

Correzione: il servizio di mappatura tenterà di continuare l'elaborazione delle trasformazioni di evento anche in presenza di un dipendenza ciclica. Quest'ultima deve essere comunque corretta dall'utente. Tuttavia, questo miglioramento consente al sistema di funzionare nel miglior modo possibile nonostante si verifichi un problema di dipendenza ciclica.

SEN-3779

Problema: il processo JDBCLoadStrategy di DAS non inserisce i campi di evento RV37, RV38 e RV47-RV48 nel database.

Correzione: correzione di JDBCLoadStrategy per l'inserimento dei campi di evento mancanti.

SEN-3781

Problema: Advisor non è in grado di connettersi al server tramite un proxy.

Correzione: correzione del client di Advisor in modo che sia ora in grado di connettersi al server tramite un proxy su HTTPS.

SEN-3785

Problema: visualizzazione di un evento SummaryUpdateFailure in Sentinel Control Center.

Correzione: correzione dell'errore che genera questo evento.

SEN-3788

Problema: le regole di correlazione RuleLg “in” e “not in” non funzionano correttamente.

Correzione: correzione di tali aspetti di RuleLg.

SEN-3792

Problema: quando una regola di correlazione attiva i risultati in un comando in esecuzione e il parametro del comando è “%all%”, il 26° argomento passato al comando corrisponde al nome di evento impostato nella regola di correlazione (identico al 13° argomento), invece che al nome dell'evento effettivo che ha attivato la regola.

Correzione: il 13° e il 26° argomento corrispondono ora rispettivamente al nome di evento della regola di correlazione e al nome del primo evento, ovvero quello responsabile dell'attivazione dell'evento correlato.

SEN-3793

Problema: non viene visualizzato alcun evento nella sezione Eventi selezionati nella finestra dei risultati di vulnerabilità.

Correzione: gli eventi selezionati sono ora visualizzati nei risultati di vulnerabilità e nel grafico di vulnerabilità degli eventi.

SEN-3812

Problema: i file non vengono eliminati dalla cartella $ESEC_HOME/sentinel/bin/eventfiles/done anche se sono configurati per l'eliminazione al termine dell'elaborazione.

Correzione: i file verranno ora eliminati al termine dell'elaborazione.

SEN-3814 (miglioramento)

Problema: l'output di testo delle attività di comando dei casi dovrebbe restituire il testo in formato XML.

Correzione: aggiunta di tale funzionalità.

SEN-3835

Problema: se uno o più filtri salvati nelle preferenze di un utente non sono validi, tutte le visualizzazioni Active Views eventualmente provviste di filtri per qualsiasi utente verranno considerate non permanenti.

Correzione: la gestione degli errori è stata migliorata in modo da risolvere questo problema.

SEN-3851

Problema: non sono disponibili opzioni di salvataggio dei dati nelle interrogazioni rapide.

Correzione: aggiunta di due pulsanti al pannello delle interrogazioni rapide, i quali consentono rispettivamente di salvare i dati in un file HTML e CSV.

SEN-3877

Problema: gli eventi non vengono scritti nel database se il log delle transazioni è pieno.

Correzione: l'errore è stato corretto mediante l'aggiunta di componenti che ritentano di inserire gli eventi nel database in caso di errore di quest'ultimo. Tali componenti vengono abilitati per default in fase di installazione.

SEN-3880

Problema: il server di workflow viene eseguito senza essere connesso e si blocca dopo la creazione di numerosi processi tramite casi attivati dalla correlazione.

Correzione: il problema è stato corretto configurando le connessioni di workflow in modo che vengano chiuse dopo l'uso.

SEN-3914

Problema: la funzionalità responsabile dei tentativi di inserimento degli eventi non gestisce correttamente gli eventi correlati.

Correzione: la gestione degli eventi correlati da parte della funzionalità responsabile dell'inserimento degli eventi è stata corretta.

SEN-3916

Problema: la tassonomia nella documentazione relativa alla correlazione e nei dati di generazione delle regole di correlazione non è aggiornata.

Correzione: le regole di correlazione installate nell'ambito dei dati di generazione sono state aggiornate coerentemente con la tassonomia successiva. Il capitolo 7 della Guida di riferimento è stato inoltre aggiornato in base alla nuova tassonomia e alle nuove regole di correlazione.

SEN-3800

Problema: un rapporto pianificato determina un problema nella visualizzazione della gerarchia di cartelle dei rapporti in Sentinel.

Correzione: il file GetReports.asp/GetReports.jsp è stato modificato in modo da adeguare la modalità di recupero della gerarchia di cartelle dall'archivio.

SEN-3832

Problema: l'interrogazione rapida non funziona per le espressioni di corrispondenza sottorete.

Correzione: l'interrogazione eseguita per l'espressione di corrispondenza sottorete è stata aggiornata in modo da riflettere le modifiche apportate all'archiviazione degli indirizzi IP nel database.

SEN-3924

Problema: il motore di correlazione si arresta in modo anomalo (operazione di stringa window con !=).

Correzione: il confronto di una stringa letterale mediante la valutazione != nell'operazione window causa una violazione di segmentazione. Il problema è stato corretto. Ad esempio window(e.evt!= “bob”,10).

SEN-3933

Problema: in seguito al drill-down, il grafico a torta non restituisce il numero corretto di eventi nell'interrogazione rapida, mentre la suddivisione in porzioni del grafico a torta non restituisce alcun risultato.

Correzione: il problema corretto è relativo a un'etichetta vuota. Poiché RuleLg non è in grado di supportare operazioni isnull, le etichette vuote vengono rimosse dall'interrogazione. Ciò influisce tuttavia sugli indici producendo quindi risultati errati. Se tuttavia si seleziona solo l'etichetta vuota e si effettua un drill-down, verranno restituiti tutti gli eventi relativi al periodo di tempo, non solo quelli con l'etichetta vuota. Ciò è dovuto a una limitazione di RuleLg.

SEN-3999 (miglioramento)

Problema: aumento della lunghezza dei campi compresi tra cv30 e cv34 da 255 a 4000 caratteri

Correzione: questi campi possono contenere una quantità maggiore di dati stringa.

SEN-4056

Problema: problema relativo alle autorizzazioni di workflow/utente

Correzione: la creazione di un utente con il servizio di workflow non disponibile risulta eseguita solo parzialmente in uno dei due database contenenti le informazioni sugli utenti. In questo modo, l'utente verrà lasciato in uno stato non valido irreversibile. Il problema è stato risolto perfezionando il processo di creazione dell'utente come transazione.

SEN-4087

Problema: NON viene visualizzato un messaggio di conferma appropriato quando si fa clic sul pulsante Rimuovi nella scheda Advisor per un caso.

Correzione: il messaggio di conferma è stato modificato affinché vengano visualizzate le informazioni appropriate per l'eliminazione di un attacco nella scheda Advisor.

SEN-4094

Problema: le configurazioni dei menu non vengono avviate nel browser interno se non è selezionata l'opzione “Usa browser esterno”.

Correzione: l'avvio del browser è stato corretto.

SEN-4302

Problema: i file UpgradePortCfgFile devono essere aggiunti all'installazione completa.

Correzione: i file sono stati aggiunti all'installazione.

Wizard

7414 (HD 101689)

Problema: blocco di Generatore servizi di raccolta alla schermata di login a causa dell'inizializzazione non corretta di variabili.

Correzione: il processo di inizializzazione delle variabili è stato corretto.

WIZ-1649

Problema: Gestione servizi di raccolta tronca i dati di trap SNMP se un valore di trap supera i 57 caratteri. Ciò causa la perdita dell'intero trap.

Correzione: Il troncamento dei trap è stato corretto in modo da consentire l'utilizzo di valori di lunghezza notevolmente superiore a 57 caratteri.

WIZ-1651

Problema: il supporto per SNMP di Gestione servizi di raccolta gestisce solo trap di comunità pubblici.

Correzione: in Gestione servizi di raccolta sono ora supportati anche i trap di comunità non pubblici.

WIZ-1656

Problema: Gestione servizi di raccolta gestisce solo trap SNMP v1 e v3. In particolare, non vengono gestiti i trap SNMP v2 e v2c.

Correzione: in Gestione servizi di raccolta è stato aggiunto il supporto per trap SNMP v2 e v2c.

WIZ-1661

Problema: se si impostano le variabili s_VULN e s_CRIT del servizio di raccolta durante l'utilizzo del comando EVENT, i campi dei tag Vulnerability e Criticality risulteranno vuoti.

Correzione: tali campi vengono ora impostati correttamente se si utilizza il comando EVENT.

WIZ-1664

Problema: se il delimitatore si trova all'inizio di un nuovo blocco di dati letto dall'origine (ad esempio un file), verrà ignorato dallo stato Rx.

Correzione: l'errore è stato corretto.

WIZ-1665

Problema: se il delimitatore è di lunghezza superiore a 1 carattere e si trova in corrispondenza del limite di un blocco, verrà ignorato dallo stato Rx.

Correzione: l'errore è stato corretto.

WIZ-1675

Problema: Gestione servizi di raccolta entra talvolta in uno stato quando la CPU viene utilizzata quasi al 100%, benché non sia in elaborazione alcun evento e il motore del servizio di raccolta sia in esecuzione.

Correzione: l'errore responsabile di questa situazione è stato corretto.

WIZ-1676

Problema: memoria insufficiente quando si utilizza il comando Alert.

Correzione: il problema di insufficienza della memoria è stato corretto.

WIZ-1682

Problema: il connettore del database viene eseguito in un ciclo infinito se l'interrogazione contiene un nome di tabella inesistente nel database.

Correzione: il problema è stato corretto mediante l'inizializzazione corretta della variabile del set di risultati.

WIZ-1699

Problema: rimozione del comando di script exportvar e degli elementi di interfaccia utente grafica relativi al generatore di servizi di raccolta.

Correzione: il comando è stato rimosso.

WIZ-1713

Problema: l'analizzatore NVP non gestisce l'analisi sintattica di valori a 32 bit senza segno in valori a 32 bit con segno/il comando stonum non consente la conversione del massimo numero intero positivo con segno.

Correzione: questi comandi di script sono stati modificati in modo da accettare numeri senza segno grandi a 32 bit. Tutti gli interi di script sono valori a 32 bit con segno. Un numero grande a 32 bit senza segno produce una variabile di script che rappresenta il valore a 32 bit (con il set di bit più significativo) come valore negativo.

Database

DAT-145

Problema: quando si abbandonano le partizioni, Gestione dati Sentinel non è in grado di rinominare la partizione di indice P_TEMP in P_MIN.

Correzione: la ridenominazione della partizione di indice P_TEMP in P_MIN da parte di Gestione dati Sentinel durante l'abbandono delle partizioni viene ora eseguita correttamente.

DAT-147

Problema: SERVICE_PACK_ID mancante in ADV_ATTACK_PLUGIN_RPT_V

Correzione: la colonna SERVICE_PACK_ID si trova ora nella visualizzazione di ADV_ATTACK_PLUGIN_RPT_V.

DAT-151

Problema: l'installazione del database ha esito negativo se l'utente imposta TNS_ADMIN e il file tnsnames.ora si trova in una directory diversa da $ORACLE_HOME/network/admin/.

Correzione: la procedura di installazione del database è stata corretta in modo da gestire in modo appropriato tale situazione.

DAT-157

Problema: Gestione dati Sentinel non è in grado di archiviare EVT_DEST_SMRY_1.

Correzione: sono stati corretti due casi che determinano l'esito negativo dell'archiviazione di EVT_DEST_SMRY_1 da parte di Gestione dati Sentinel. Si tratta in un caso del fatto che il vincolo univoco determinato da ARCH_SEQ è troppo breve, nell'altro che l'accesso a Gestione dati Sentinel da parte di MSSQL viene effettuato mediante l'autenticazione di Windows. Questo problema è relativo a tutte le tabelle di evento e di riepilogo di evento.

DAT-161 (miglioramento)

Problema: separazione delle partizioni di archiviazione ed eliminazione della tabella di riepilogo dalle tabelle degli eventi.

Correzione: le partizioni della tabella di riepilogo vengono ora abbandonate contestualmente all'abbandono delle partizioni delle tabelle degli eventi.

Problemi noti

Installazione

- Se si tenta di acquisire un'immagine del programma di installazione premendo Alt+Stamp, l'aspetto del programma risulterà alterato. Ciò è dovuto a un problema di InstallShield. La soluzione alternativa per questo problema consiste nel premere solo Stamp.

Sentinel

- Il workflow verrà interrotto all'inizio del processo di estirpazione se si tenta di eseguire il comando arp -a. Per risolvere questo problema:
  1. Eseguire il login al computer che esegue il componente DAS come utente esecadm.
  2. Aprire il file “bash_profile” nella home directory dell'utente esecadm e modificarlo in modo che la variabile di ambiente PATH includa la directory “/usr/sbin”.
  3. Modificare l'attività del modello in modo che esegua un'altra attività.
- Quando si imposta un filtro nelle opzioni di visualizzazione relative ai casi, ai servizi di raccolta, alle istanze di Gestione servizi di raccolta o a iTRAC, i campi degli attributi contenenti date potrebbero non funzionare se inclusi nel filtro:
- In Sentinel Control Center > scheda Amministrazione, in Sessioni utente attive verrà temporaneamente indicata una sessione di un utente che ha effettuato il login a Generatore servizi di raccolta.

- Se il ruolo di analisi è vuoto (come per default all'installazione del prodotto) e viene creata un'istanza di un workflow di risposta automatica, al ruolo verrà assegnato _WORKFLOW_SERVER. Tuttavia, se in seguito si aggiunge un utente a tale ruolo, le assegnazioni non verranno ricalcolate e il nuovo utente non potrà ottenere gli elementi di lavoro associati al processo. Le soluzioni a questo problema sono le seguenti:
  - Prima di avviare qualsiasi processo di workflow, verificare che tutti i gruppi assegnati abbiano almeno un utente. Ciò impedirà che si verifichi il problema descritto sopra.
  - Se è stata creata un'istanza di un processo iTRAC senza aggiungere almeno un utente a un gruppo assegnato, eseguire le operazioni seguenti:
    - Aggiungere un utente al gruppo in questione.
    - Modificare il modello corrispondente e salvarlo. Ai fini di questa operazione non è necessaria alcuna modifica effettiva al modello. È sufficiente fare doppio clic sull'attività manuale per visualizzare la finestra di dialogo per la personalizzazione, riselezionare la stessa risorsa e fare clic su OK per salvare il modello.

      In questo modo verrà forzato il ricalcolo delle assegnazioni degli elementi di lavoro. Gli utenti del gruppo di analisi saranno quindi in grado di visualizzare gli elementi di lavoro per l'attività.
- Non è possibile apportare modifiche durante la creazione di un modello definito dall'utente nella stessa finestra di personalizzazione dopo che ne è stato eseguito il salvataggio. Per risolvere questo problema, dopo aver salvato il nuovo modello, chiuderne la finestra e quindi riaprirla per apportarvi le modifiche desiderate.

Wizard

- Se si utilizza la funzionalità di popolamento rete in Generatore servizi di raccolta, gli UUID non vengono reimpostati nelle configurazioni di porta copiate. In questo modo gli eventi delle configurazioni di porta copiate avranno lo stesso ID di origine.
  - [WIZ-1684] Se si esegue il debug di un servizio di raccolta mediante Generatore servizi di raccolta, quest'ultimo potrebbe essere chiuso in modo imprevisto. Ciò si verifica raramente se si fa clic lentamente (meno di una volta ogni due secondi) sui pulsanti di debug del Generatore servizi di raccolta per l'esecuzione di un comando e la ripresa di un comando.

Supporto tecnico 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

Esclusioni di garanzia

La Fonte delle presenti informazioni può essere interna o esterna a Novell. Novell si impegna a verificare le informazioni con la massima cura ragionevole. Le informazioni fornite nel presente documento vengono tuttavia offerte a solo scopo di riferimento per l'utente. Novell non offre garanzie esplicite o implicite relativamente alla validità di tali informazioni.

Tutti i marchi di fabbrica citati nel presente documento appartengono ai rispettivi proprietari. Consultare i manuali del prodotto per informazioni complete sui marchi di fabbrica.