Novell

Software for the Open Enterprise™

Notes de version du produit

Sentinel™ 5.1.3 avec iTRAC™

REMARQUE : Pour télécharger les notes de version en français, allemand, italien, espagnol ou portugais du Brésil, rendez-vous sur http://www.novell.com/documentation/sentinel5.

Description

Nouvelle version complète de Sentinel 5.1.3 avec iTRAC.

Cette version prend en charge les types d'installation suivants :

- Installation complète de Sentinel 5.1.3 sous Windows, Solaris et Linux (Novell SUSE Linux Enterprise Server 9 et Redhat).
- Mise à niveau et migration des données de Sentinel 4.2.x vers Sentinel 5.1.3 sous Windows et Solaris.
- Installation de composants supplémentaires de Sentinel 5.1.3 dans une installation existante de Sentinel 5.1.3 sous Windows, Solaris et Linux.

REMARQUE : Si vous disposez d'une installation de Sentinel 5 antérieure à la version 5.1.3 et si vous désirez lui appliquer un correctif pour passer à la version 5.1.3, vous devez utiliser un logiciel d'installation de correctifs Sentinel 5.1.3. Le programme d'installation de Sentinel 5.1.3 accompagnant ces notes de version n'est pas un programme d'installation de correctifs. Pour obtenir un programme d'installation de correctifs Sentinel 5.1.3, contactez l'assistance technique.

Systèmes d'exploitation et correctifs

La liste qui suit reprend les systèmes d'exploitation et les bases de données pris en charge par les versions localisées de Sentinel 5.1.3. Les informations relatives à la version anglaise figurent dans le guide d'installation.

- **Systèmes d'exploitation serveur :**
  - SLES 9 SP3 (allemand, français, italien, espagnol, portugais du Brésil)
  - Solaris 9 (allemand, français, italien, espagnol, portugais du Brésil)
  - MS Windows 2003 Serveur SP1 (allemand, français, italien, espagnol, portugais du Brésil)
  - MS Windows 2000 Serveur SP4 (allemand, français, italien, espagnol, portugais du Brésil)

- **Systèmes d'exploitation client :**
  - MS Windows 2000 Professionnel SP4 (allemand, français, italien, espagnol, portugais du Brésil)
  - MS Windows XP Professionnel SP2 (allemand, français, italien, espagnol, portugais du Brésil)
  - Solaris 9 (allemand, français, italien, espagnol, portugais du Brésil)

- **Base de données :**
  - Oracle 9.2.0.7 (anglais uniquement)
  - MS SQL 2000 SP3a (anglais uniquement)

Installation

Les instructions d'installation de cette version se trouvent dans le Guide d'installation de Sentinel pour Sentinel 5.1.3.

Pour une installation complète de Sentinel, suivez les instructions de l'un des chapitres suivants, selon la plate-forme sur laquelle s'effectue l'installation.

- Chapitre 3 : Installation de Sentinel 5 pour Oracle sous Solaris
- Chapitre 4 : Installation de Sentinel 5 pour Oracle sous Solaris
- Chapitre 5 : Installation de Sentinel 5 pour MS SQL

Les opérations suivantes doivent être effectuées dans le cadre de la pré-installation d'Oracle sous Linux. Ce changement concerne Oracle Doc ID: Note:293988.1.

- Sous SUSE Linux Enterprise Server 9 SP2, ajoutez la valeur de paramètre de noyau suivante au fichier « /etc/sysctl.conf » :
  ```
  # Oracle requires MLOCK privilege for hugetlb memory.
  vm.disable_cap_mlock=1
  ```
- Exécutez la commande suivante pour charger les modifications dans le fichier « /etc/sysctl.conf » :
  ```
  sysctl -p
  ```

Pour effectuer une mise à niveau et une migration de données de Sentinel 4.2.x vers Sentinel 5.1.3, suivez les instructions de l'un des chapitres suivants, selon la plate-forme sur laquelle s'effectue l'installation.

- Chapitre 6 : Migration de données et correctif pour Oracle sous Solaris
- Chapitre 7 : Migration de données et correctif pour MS SQL

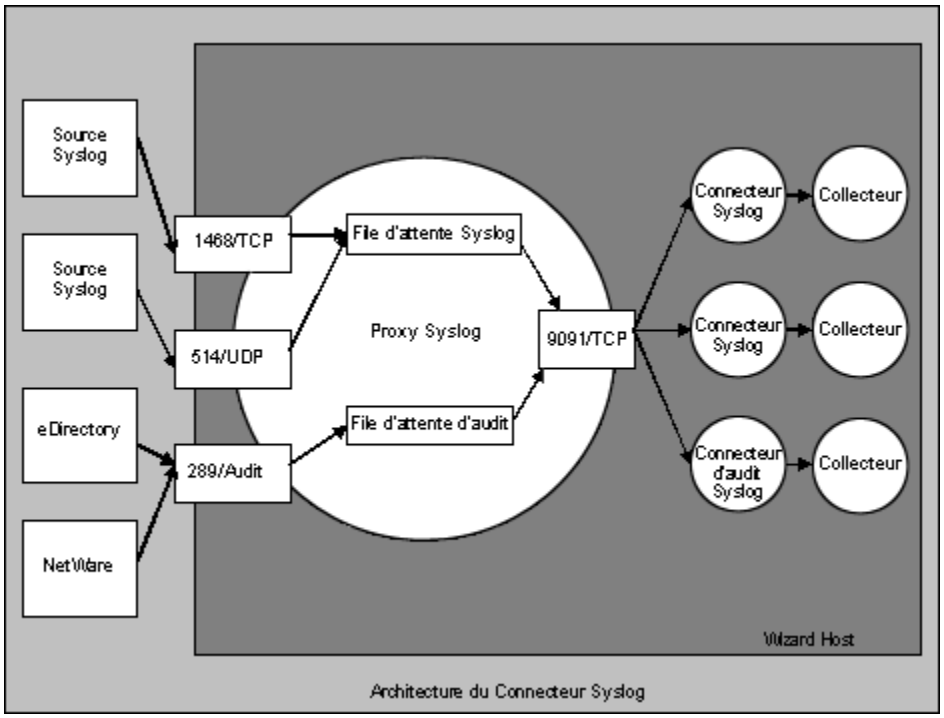
Pour installer des composants supplémentaires de Sentinel 5.1.3 dans une installation de Sentinel 5.1.3 existante, suivez les instructions du chapitre suivant :

- Chapitre 14 : Ajout de composants à une installation existante

Pour installer des composants supplémentaires de Sentinel 5.1.3 dans une installation existante ou une version antérieure de Sentinel 5, appliquez d'abord le correctif à l'installation de Sentinel version 5.1.3 à l'aide du programme d'installation de correctif approprié, puis suivez les instructions du chapitre spécifié ci-dessus.

Nouveautés

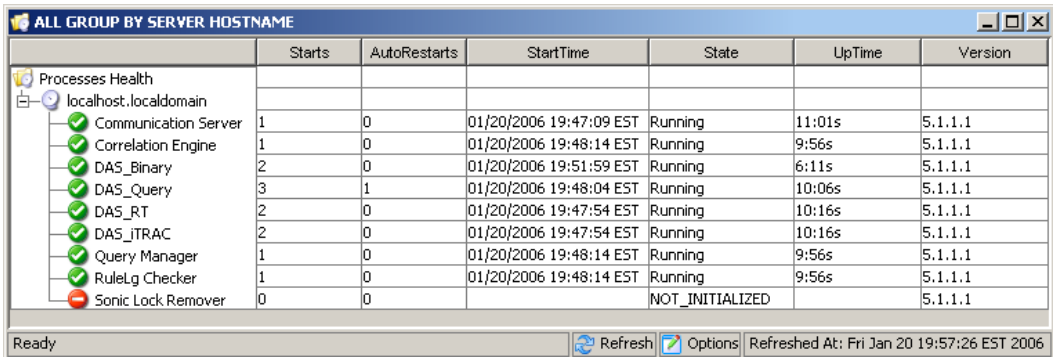
- Avec cette version, la console Sentinel et le gestionnaire de données Sentinel prennent en charge plusieurs langues, dont le portugais du Brésil, le français, l'italien, l'allemand, l'espagnol et l'anglais.
- Le connecteur syslog a été amélioré et peut désormais traiter les applications NAudit. Cette amélioration s'accompagne d'un agent qui traitera les données NAudit en général, mais plus particulièrement pour les applications suivantes : eDirectory, Netware, Identity Manager, Secure Login et Access Manager. Autres améliorations :
  - Filtrage du corps du message syslog à l'aide d'expressions régulières.
  - Reconnexion automatique du connecteur du collecteur au serveur syslog.
  - Contrôle du flux de connexions TCP pour éviter les pertes de données lorsque la mémoire tampon des messages est pleine. Cela s'applique aux connexions TCP syslog et NAudit.



Architecture du Connecteur Syslog

- Le connecteur syslog est désormais installé avec des scripts qui fonctionnent sous Windows et UNIX, ainsi qu'avec des fichiers de configuration améliorés. En outre, l'installation du serveur proxy syslog en tant que service a été simplifiée. Pour installer le serveur proxy syslog en tant que service avec la configuration par défaut, exécutez les commandes suivantes :
  - Sous Windows :
    1. Connectez-vous en tant qu'administrateur.
    2. cd /d %ESEC_HOME%\wizard\syslog
    3. .\syslog-server.bat install
  - Sous UNIX :
    4. Connectez-vous sous l'ID d'utilisateur root.
    5. cd $ESEC_HOME/wizard/syslog
    6. ./syslog-server.sh install
- Les nouvelles commandes de script d'agent, encodemime et decodemime, apportent des capacités de codage et décodage en base 64.
- La limitation du nombre de caractères de CV30-CV34 passe de 255 à 4 000.

- Cette version prend désormais en charge l'installation de la base de données Sentinel directement sur un serveur de bases de données MS SQL 2005.
- Un nouvel écran « Vue du serveur » a été ajouté à l'onglet Admin du Centre de contrôle Sentinel. Cet écran donne accès aux fonctionnalités suivantes :
  - Affichage du statut de tous les processus du serveur Sentinel sur le système (privilège « Administration->Server Views->View Servers » requis). Cette fonction est similaire à la fonction existante Affichage des collecteurs, si ce n'est qu'elle affiche les processus du serveur Sentinel.
  - Il vous permet de démarrer, arrêter ou redémarrer des processus (privilèges d'affichage et « Administration->Server->Control Servers » requis).



- Les demandes de mot de passe pour les connecteurs de processus Wizard suivants ont été améliorées afin de tenter de masquer le mot de passe lors de sa saisie sur la ligne de commande :
  - dbconnector
  - rdep_client
- Le composant qui génère le fichier de détection d'exploitation attackNomarlization.csv a été modifié pour utiliser moins de mémoire. Cette modification améliorera les performances sur du matériel de démonstration.
- Le fichier configuration.xml contient des options de configuration supplémentaires pour les processus :
  - name [default: « Uknown »] : Nom des processus. Il s'agit d'un nom donné au processus et qui apparaîtra comme nom du processus dans les fichiers journaux et sur l'écran Vue du serveur du Centre de contrôle Sentinel.
  - auto_restart_threshold [default: « 5,10 »] : Le format de la valeur est « <#restarts>,<#minutes> ». Si le processus redémarre automatiquement (p. ex. parce que le processus s'arrête de lui-même ou est arrêté par une commande du système d'exploitation) plus de fois que le nombre de redémarrages spécifiés pendant le nombre de minutes indiqué, il ne redémarre plus automatiquement. L'objectif est d'éviter qu'un processus redémarre indéfiniment alors qu'une erreur de configuration est probable. Un événement interne « ProcessAutoRestartError » est envoyé lorsque cela se produit.
  - depends [default: <no dependencies>] : Le format de la valeur est une liste de noms de processus séparés par des virgules, tel que le spécifie le nouvel attribut de processus « name ». Les processus spécifiés dans la liste sont ceux qui doivent être exécutés avant que ce processus puisse être exécuté.
  - type [default: « normal »] – Seules les valeurs « normal » ou « container » sont acceptées. La valeur Container indique que le processus est un processus conteneur eSecurity (c.-à-d. lancé à l'aide d'un fichier XML conteneur) et peut être arrêté normalement en envoyant un message au conteneur pour qu'il s'arrête de lui-même. La valeur Normal s'applique à tous les autres processus.

- Les processus suivants ont été réécrits en Java pour en accroître la fonctionnalité et en réduire la complexité :
  - watchdog
  - data_synchronizer (désormais partie de DAS).
- La fonction Base Sentinel Services qui pouvait auparavant être installée séparément a été intégrée à la fonction d'installation DAS. Les processus précédemment activés lors de la sélection de l'installation de Base Sentinel Services seront dorénavant activés lors de la sélection de l'installation DAS. L'objectif est de réduire la complexité du programme d'installation. La possibilité d'installation séparée offerte précédemment ne présentait aucun avantage connu en termes de performances.
- La procédure de vérification de la licence a été améliorée afin de comparer la clé de licence spécifiée par l'utilisateur à toutes les cartes d'interface réseau (NIC) disponibles. Si une de celles-ci a l'adresse MAC correcte, la vérification de la licence réussit.

Corrections de bogues

Sentinel

7424

Problème : Il manque des données pour générer exploitDetection.csv.

Solution : Le générateur de détection d'exploitation a été corrigé pour ajouter les données manquantes au fichier exploitDetection.csv.

7460

Problème : Sous UNIX, si le serveur de communication a été installé seul, il ne démarre jamais automatiquement. Il en est ainsi parce que le programme d'installation n'installe pas « watchdog », qui assure le démarrage du serveur de communication sous UNIX.

Solution : La fonction Serveur de communication a été déplacée sous Services Sentinel dans le programme d'installation afin de garantir également l'installation de « watchdog ».

7463

Problème : Le générateur de détection d'exploitation démarre une seconde régénération, même s'il y en a déjà une en cours, ce qui provoque une utilisation supplémentaire du processeur sur la requête DAS.

Solution : Le générateur de détection d'exploitation n'autorise plus qu'un seul processus de régénération à la fois.

SEN-2819

Problème : SDM % n'affiche pas l'état de progression lors de l'ajout de partitions. Il reste à 0%.

Solution : Le pourcentage augmente continuellement en fonction de l'état d'achèvement de l'activité SDM.

SEN-3684

Problème : Le type d'argument dans Activité de commande d'incident ne fonctionne pas.

Solution : Tous les paramètres (None, Incident Output et Custom) comme type d'argument fonctionnent désormais.

SEN-3713

Problème : La détection d'exploitation ne détecte qu'une seule attaque pour chaque vulnérabilité.

Solution : La détection d'exploitation détecte désormais toutes les attaques qui sont liées à une vulnérabilité du flux Advisor comme une exploitation de cette vulnérabilité si cette dernière a été signalée sur la machine attaquée.

SEN-3732

Problème : Il n'est plus possible de sélectionner le statut « Rejeté » dans le gestionnaire d'incidents de l'interface utilisateur graphique Sentinel

Solution : Le statut « Rejeté » a été ajouté au gestionnaire d'incidents de l'interface utilisateur graphique Sentinel.

SEN-3760

Problème : Problème de transmission de paramètres contenant des espaces lors de l'exécution de scripts à partir du menu contextuel ou de règles de corrélation.

Solution : L'exécuteur des commandes du menu contextuel et des règles de corrélation a été corrigé pour gérer correctement les espaces présents dans les paramètres.

SEN-3763

Problème : Il peut arriver que détection d'exploitation ne fonctionne pas du fait de l'existence de multiples ID d'attaque normalisés multiples pour chaque nom d'attaque de périphérique.

Solution : La détection d'exploitation détecte désormais toutes les attaques qui sont liées à une vulnérabilité du flux Advisor comme une exploitation de cette vulnérabilité si cette dernière à été signalée sur la machine attaquée.

SEN-3764

Problème : La fréquence à laquelle les données de détection d'exploitation sont régénérées est limitée.

Solution : La régénération est désormais limitée par défaut à une fois toutes les 30 minutes. Cette fréquence peut être configurée en modifiant le fichier das_query.xml.

SEN-3766

Problème : Lorsque l'appel effectué par DAS RT pour obtenir les préférences utilisateur échoue, il supprime tous les filtres permanents.

Solution : Le traitement des erreurs a été amélioré pour ne plus effacer tous les filtres permanents si l'obtention des préférences utilisateur échoue.

SEN-3775 (amélioration)

Problème : Traitement des transformations d'événements pour le service d'assignation en cas de dépendances cycliques.

Solution : Le service d'assignation s'efforcera de continuer à traiter les transformations d'événements, même en cas de dépendance cyclique. C'est encore à l'utilisateur qu'il revient de corriger la dépendance cyclique, mais cette amélioration permet au système de fonctionner aussi bien que possible même en cas de problème de dépendance cyclique.

SEN-3779

Problème : Le DAS JDBCLoadStrategy n'insère pas les champs d'événements RV37, RV38 et RV47-48 dans la base de données.

Solution : Le JDBCLoadStrategy corrigé insère désormais les champs d'événements manquants.

SEN-3781

Problème : Advisor ne peut pas se connecter au serveur via un serveur proxy.

Solution : Le client Advisor a été corrigé pour qu'il puisse désormais se connecter au serveur via un serveur proxy sur une connexion https.

SEN-3785

Problème : Un événement SummaryUpdateFailure apparaît dans le SCC.

Solution : L'erreur à l'origine de cet événement a été corrigée.

SEN-3788

Problème : La règle de corrélation « in » et « not in » de RuleLg ne fonctionne pas bien.

Solution : Les problèmes liés à ces aspects de RuleLg ont été corrigés.

SEN-3792

Problème : Lorsque le déclenchement d'une règle de corrélation provoque l'exécution d'une commande et que le paramètre de la commande est « %all% », le 26^{e} argument transmis à la commande est le nom de l'événement défini dans la règle de corrélation (identique au 13^{e} argument) plutôt que celui de l'événement qui a effectivement déclenché la règle.

Solution : Désormais, les 13^{e} et 26^{e} arguments sont, respectivement, le « nom d'événement » de la règle de corrélation et le nom du premier événement (celui qui a déclenché l'événement corrélé).

SEN-3793

Problème : Aucun événement ne s'affiche dans la section des événements sélectionnés de la fenêtre des résultats de vulnérabilité.

Solution : Les événements sélectionnés s'affichent désormais dans les résultats de vulnérabilité et dans Événement du graphique de vulnérabilité.

SEN-3812

Problème : Les fichiers ne sont pas effacés du dossier $ESEC_HOME/sentinel/bin/eventfiles/done, même s'ils sont configurés de manière à être effacés après leur traitement.

Solution : Le fichier sera désormais effacé après son traitement.

SEN-3814 (amélioration)

Problème : Les activités de commande d'incident devraient renvoyer le texte en XML.

Solution : Fonctionnalité ajoutée.

SEN-3835

Problème : Si un filtre enregistré dans les préférences d'un utilisateur n'est pas valide, toutes les vues actives avec un filtre pour un utilisateur sont traitées comme des vues actives non permanentes.

Solution : Le traitement des erreurs a été amélioré pour résoudre ce problème.

SEN-3851

Problème : Une requête rapide n'offre aucune option d'enregistrement des données.

Solution : Deux boutons ont été ajoutés au volet Requête rapide. L'un sert à enregistrer les données dans un fichier HTML, l'autre dans un fichier CSV.

SEN-3877

Problème : Les événements ne sont pas écrits dans la boîte de dialogue si le journal des transactions est plein.

Solution : Problème résolu en ajoutant des composants qui tenteront de nouveau d'insérer les événements dans la base de données en cas d'erreur de base de données. Ces composants sont activés par défaut par ce programme d'installation.

SEN-3880

Problème : Le serveur de flux de travail est à court de connexions et se bloque après la création de nombreux processus via des incidents déclenchés par corrélation.

Solution : Problème corrigé en veillant à ce que les connexions des flux de travail soient fermées après utilisation.

SEN-3914

Problème : La fonctionnalité permettant une nouvelle tentative d'insertion d'événements ne traite pas correctement les événements corrélés.

Solution : Fonctionnalité d'insertion d'événements corrigée pour traiter correctement les événements corrélés.

SEN-3916

Problème : La taxonomie est périmée dans la documentation de corrélation et dans les données de base des règles de corrélation.

Solution : Les règles de corrélation installées comme partie intégrante des données de base ont été mises à jour de manière à être cohérentes avec la taxonomie suivante. En outre, le chapitre 7 du guide de référence a été mis à jour pour correspondre à la nouvelle taxonomie et aux nouvelles règles de corrélation.

SEN-3800

Problème : Un rapport planifié générera des problèmes d'affichage de la hiérarchie des dossiers de rapports dans Sentinel.

Solution : GetReports.asp/GetReports.jsp a été modifié afin de changer la manière de récupérer la hiérarchie des dossiers dans le référentiel.

SEN-3832

Problème : Les requêtes rapides ne fonctionnent pas pour les expressions de mise en correspondance de sous-réseaux.

Solution : La requête qui est émise pour l'expression de mise en correspondance de sous-réseaux a été mise à jour afin de refléter les modifications du stockage des adresses IP des bases de données.

SEN-3924

Problème : Le moteur de corrélations se bloque (opération de chaîne Window avec !=)

Solution : La comparaison d'une chaîne littérale avec l'évaluation != dans l'opération Window a généré une violation de la segmentation. Problème résolu. Par exemple : window(e.evt != « jean »,10).

SEN-3933

Problème : Piechart ne renvoie pas le bon nombre d'événements lors de la requête rapide d'analyse approfondie et une partie de piechart ne renvoie rien lors de l'analyse approfondie.

Solution : Le problème corrigé est dû à une étiquette vide. RuleLg ne prenant pas en charge l'opération insull, les étiquettes vides sont supprimées de la requête. Toutefois, la suppression des étiquettes vides entraîne celle des indices, ce qui provoque des résultats incorrects. En ne sélectionnant que l'étiquette vide et en faisant une analyse approfondie, vous obtiendrez tous les événements de la période et non les seuls événements avec l'étiquette vide. Ce problème est dû à une limitation de RuleLg.

SEN 3999 (amélioration)

Problème : La longueur des champs de cv30 à cv34 a été portée de 255 à 4 000.

Solution : Ces champs peuvent contenir davantage de données de type chaîne.

SEN-4056

Problème : Problèmes d'autorisations flux de travail/utilisateur

Solution : Lorsqu'un utilisateur est créé avec le service de flux de travail indisponible, il est créé partiellement dans l'une des deux bases de données contenant les informations utilisateur. Cette opération génère un statut d'utilisateur incorrect et irrécupérable.
Ce problème a été résolu en faisant en sorte que la création d'un utilisateur ne se résume pas qu'à une transaction.

SEN-4087

Problème : AUCUN message de confirmation pertinent N'EST affiché lors d'un clic sur le bouton Supprimer de l'onglet Advisor d'un incident

Solution : Le message de confirmation a été modifié pour afficher les informations correctes lors de la suppression d'une attaque dans l'onglet Advisor.

SEN-4094

Problème : Les configurations de menu ne sont pas lancées dans le navigateur interne lorsque l'option « Utiliser le navigateur externe » n'est pas sélectionnée.

Solution : Lancement du navigateur corrigé.

SEN-4302

Problème : Les fichiers UpgradePortCfgFile doivent être ajoutés au programme d'installation COMPLETE.

Solution : Fichiers ajoutés au programme d'installation.

Assistant

7414 (HD 101689)

Problème : Le générateur de collecteurs se bloque à l'écran de connexion en raison d'une mauvaise initialisation de variables.

Solution : Les variables sont correctement initialisées.

WIZ-1649

Problème : Le gestionnaire de collecteurs tronque les données des trappes SNMP lorsqu'une valeur de trappe a une longueur supérieure à 57 caractères. Cela entraîne une perte de toute la trappe.

Solution : La troncation des trappes a été corrigée par l'acception de valeurs de trappes plus grandes (largement supérieures à 57 caractères).

WIZ-1651

Problème : La prise en charge SNMP par le gestionnaire de collecteurs ne gère que les trappes communautaires « publiques ».

Solution : Les trappes communautaires non publiques sont désormais également gérées par le gestionnaire de collecteurs.

WIZ-1656

Problème : Le gestionnaire de collecteurs ne gère que les trappes SNMP v1 et v3. Plus spécifiquement, il ne gère pas les trappes SNMP v2 et v2c.

Solution : La prise en charge des trappes SNMP v2 et v2c a été ajoutée dans le gestionnaire de collecteurs.

WIZ-1661

Problème : La définition des variables Collector s_VULN et s_CRIT en utilisant la commande EVENT se traduit par des étiquettes de champs Vulnerability et Criticality vides.

Solution : Ces champs sont désormais correctement définis lors de l'utilisation de la commande EVENT.

WIZ-1664

Problème : Si le séparateur se trouve au début d'un nouveau bloc de données lues dans la source (c.-à-d. fichier), il est ignoré par le statut Rx.

Solution : Erreur corrigée.

WIZ-1665

Problème : Si la taille du séparateur est supérieure à 1 caractère et si ce séparateur apparaît à la limite d'un bloc, le statut Rx ignore le séparateur.

Solution : Erreur corrigée.

WIZ-1675

Problème : Il arrive que le gestionnaire de collecteurs passe dans un état dans lequel il utilise pratiquement 100 % du processeur alors qu'il ne traite aucun événement, même si Collectorengine est en service.

Solution : L'erreur à l'origine de ce scénario a été corrigée.

WIZ-1676

Problème : Fuite de mémoire lors de l'utilisation de la commande Alert.

Solution : Fuite de mémoire corrigée.

WIZ-1682

Problème : Le connecteur de base de données entre dans une boucle infinie lorsque la requête contient un nom de table inexistant dans la base de données.

Solution : La variable de définition du résultat a été initialisée correctement.

WIZ-1699

Problème : Suppression de la commande de script exportvar et des éléments d'interface utilisateur graphique du générateur de collecteurs.

Solution : Cette commande a été supprimée.

WIZ-1713

Problème : L'analyseur NVP ne gère pas l'analyse non signé 32 bits en signé 32 bits. Stonum ne permet pas de convertir plus que l'entier positif signé maximum.

Solution : Ces commandes de scripts ont été modifiées de manière à accepter de grands nombres non signés 32 bits Tous les entiers des scripts sont des valeurs signées 32 bits. Un grand nombre non signé 32 bits se traduit par une variable de script représentant la valeur 32 bits (avec le bit le plus significatif à 1) sous la forme d'une valeur négative.

Base de données

DAT-145

Problème : Lors de la suppression de partitions, SDM ne parvient pas à renommer la partition d'index P_TEMP en P_MIN.

Solution : Lorsqu'il supprime des partitions, SDM renomme désormais la partition d'index P_TEMP en P_MIN.

DAT-147

Problème : Le SERVICE_PACK_ID est manquant dans ADV_ATTACK_PLUGIN_RPT_V.

Solution : La colonne SERVICE_PACK_ID est désormais présente dans la vue ADV_ATTACK_PLUGIN_RPT_V.

DAT-151

Problème : Le programme d'installation de la base de données échoue si l'utilisateur a activé TNS_ADMIN et si le fichier tnsnames.ora se trouve dans un répertoire autre que $ORACLE_HOME/network/admin.

Solution : Le programme d'installation de la base de données a été corrigé de manière à gérer correctement cette situation.

DAT-157

Problème : SDM ne parvient pas à archiver EVT_DEST_SMRY_1

Solution : Deux cas provoquant l'échec de l'archivage d'EVT_DEST_SMRY_1 par SDM ont été résolus. L'un est une contrainte unique, causée par la taille insuffisante de la colonne ARCH_SEQ, et l'autre est dû à la connexion de MSSQL à SDM à l'aide de l'authentification Windows. Cela touche toutes les tables d'événements et de récapitulatifs d'événements.

DAT-161 (amélioration)

Problème : Archivage séparé et suppression des partitions de la table de récapitulatifs des tables d'événements.

Solution : Les partitions de la table de récapitulatifs ne sont désormais plus supprimées lors de la suppression des partitions de tables d'événements.

Problèmes connus

Programme d'installation

- Une tentative de capture d'écran du programme d'installation à l'aide de la combinaison de touches Alt+Impr. écran entraîne la déformation des images du programme d'installation. Ce problème est dû à un bogue d'InstallShield. La solution consiste à utiliser la touche Impr. écran seule.

Sentinel

- Le flux de travail ne va pas au-delà du processus Start Eradication lorsqu'il tente d'exécuter la commande arp –a. La solution consiste à effectuer les opérations suivantes :
  1. Se connecter à la machine exécutant le composant DAS en tant qu'utilisateur esecadm.
  2. Ouvrir le fichier « .bash_profile » sous le répertoire principal de l'utilisateur et le modifier de sorte que la variable d'environnement PATH englobe le répertoire /usr/sbin.
  3. Modifier l'activité du modèle de manière à exécuter une autre activité.
- Lors de la définition d'un filtre dans les options d'affichage des incidents, collecteurs, gestionnaires de collecteurs ou iTrac, les champs d'attribut qui contiennent des dates risquent de ne pas fonctionner correctement s'ils sont inclus dans le filtre.
- Dans le Centre de contrôle Sentinel > onglet Admin, les sessions utilisateur actives afficheront temporairement une session pour un utilisateur qui s'est connecté au générateur de collecteurs.
- Si le rôle Analyst est vide (il est vide pendant l'installation du produit) et qu'un flux de travail de réponse automatique est instancié, le serveur assigne _WORKFLOW_SERVER. Mais lorsque l'utilisateur est ajouté ultérieurement au rôle Analyst, les assignations ne sont pas recalculées et le nouvel utilisateur ne reçoit pas les éléments de travail associés à ce processus. Les solutions sont les suivantes :
  - Avant de démarrer un processus de flux de travail, assurez-vous que tous les groupes assignés ont au moins un utilisateur. Cela évitera le problèmes décrit ci-dessus.

- Si un processus iTRAC a été instancié sans groupe assigné avec au moins un utilisateur, respectez la procédure suivante pour résoudre le problème :
  - Ajoutez un utilisateur au groupe affecté.
  - Modifiez le modèle correspondant et enregistrez-le. Aucune modification du modèle n'est nécessaire. Il vous suffit de double-cliquer sur l'activité manuelle pour ouvrir la boîte de dialogue de personnalisation, puis de sélectionner les mêmes ressources, avant de cliquer sur OK et d'enregistrer le modèle.

    Cela forcera un nouveau calcul des assignations des éléments de travail. Les utilisateurs du groupe Analyst verront alors les éléments de travail de cette activité.

- Après avoir créé et enregistré un modèle défini par l'utilisateur, il est impossible de le modifier dans le même personnalisateur de modèles. La solution consiste, après avoir enregistré le nouveau modèle, à effectuer les modifications dans le modèle, à fermer sa fenêtre et à l'ouvrir à nouveau.

Assistant

- Lors de l'utilisation de « Populate Network » dans le générateur de collecteurs, les UUID ne sont pas redéfinies dans les configurations de port copiées. Les événements provenant des configurations de port copiées ont le même ID source.
  - [WIZ-1684] Pendant le débogage d'un collecteur à l'aide du générateur de collecteurs, ce dernier peut se fermer de manière inattendue. Ce problème est moins susceptible de survenir si vous cliquez lentement sur les boutons de débogage « Execute One Command » et « Resume Command Execution » du générateur de collecteurs (moins d'une fois toutes les deux secondes).

Assistance technique Novell

Site Web : http://www.novell.com

- Assistance technique Novell : http://www.novell.com/support/index.html
- Assistance technique Novell (international) : http://support.novell.com/phone.html?sourceidint=suplnav4_phonesup
- Auto-assistance : http://support.novell.com/support_options.html?sourceidint=suplnav_supportprog
- Pour une assistance 24 heures sur 24, 7 jours sur 7, appelez le 800-858-4000
