

Fichier Lisezmoi de Novell Sentinel 6.1 Rapid Deployment SP2

Avril 2011

Novell®

Sentinel Rapid Deployment est une nouvelle option de paquetage pour la solution Novell de gestion des événements et des informations de sécurité Sentinel, leader sur le marché. Sentinel Rapid Deployment inclut l'ensemble des fonctionnalités Sentinel et constitue la solution idéale pour les petites entreprises ou les structures régionales.

Sentinel 6.1 Rapid Deployment SP2 est disponible sous forme de programme d'installation propre ou de mise à niveau. Le programme d'installation de la mise à niveau applique les derniers correctifs logiciels et améliorations à une installation existante de Sentinel Rapid Deployment 6.1 SP1.

- ♦ [Section 1, « Nouveautés », page 1](#)
- ♦ [Section 2, « Configuration système requise », page 2](#)
- ♦ [Section 3, « Installation de Novell Sentinel Rapid Deployment », page 2](#)
- ♦ [Section 4, « Mise à niveau vers Sentinel Rapid Deployment SP2 », page 3](#)
- ♦ [Section 5, « Accès aux fichiers d'aide de Sentinel Rapid Deployment », page 3](#)
- ♦ [Section 6, « Problèmes résolus et améliorations », page 4](#)
- ♦ [Section 7, « Problèmes connus », page 6](#)
- ♦ [Section 8, « Documentation », page 8](#)
- ♦ [Section 9, « Mentions légales », page 8](#)

1 Nouveautés

- ♦ [Section 1.1, « Nouveautés de Sentinel Rapid Deployment 6.1 SP2 », page 1](#)
- ♦ [Section 1.2, « Nouveautés de Sentinel Rapid Deployment SP1 », page 2](#)

1.1 Nouveautés de Sentinel Rapid Deployment 6.1 SP2

- ♦ [« Prise en charge par SLES 11 SP1 » page 1](#)
- ♦ [« Limites de prise en charge des collecteurs hérités » page 1](#)
- ♦ [« Optimisation de la sécurité » page 2](#)

1.1.1 Prise en charge par SLES 11 SP1

Sentinel Rapid Deployment est désormais pris en charge sur la plate-forme SUSE Linux Enterprise Server (SLES) 11 SP1 64 bits.

1.1.2 Limites de prise en charge des collecteurs hérités

Novell supprime progressivement de la gamme de produits Sentinel la prise en charge des collecteurs hérités. Dans les versions précédentes de Sentinel Rapid Deployment, le système affichait un avertissement si vous importiez un collecteur hérité. À partir de la version SP2, les

nouvelles installations de Sentinel Rapid Deployment et de Collector Manager n'exécutent pas les collecteurs hérités. En revanche, les systèmes Sentinel Rapid Deployment et Collector Manager mis à niveau continuent à les exécuter.

Remarque : les collecteurs hérités ont été écrits à l'aide de l'application Legacy Collector Builder qui n'est plus fournie avec les produits Sentinel. Les collecteurs hérités sont remplacés par les collecteurs JavaScript écrits à l'aide du kit de développement logiciel Sentinel Plug-In SDK. Les collecteurs JavaScript sont disponibles sur le [site Web des plug-ins Sentinel 6.1](http://support.novell.com/products/sentinel/secure/sentinel61.html) (<http://support.novell.com/products/sentinel/secure/sentinel61.html>).

1.1.3 Optimisation de la sécurité

Sentinel Rapid Deployment 6.1 SP2 comprend plusieurs mises à jour qui améliorent la sécurité du produit :

- ♦ Java Runtime Environment (JRE) a été mis à niveau vers la version 1.6.0_24.
- ♦ Apache Tomcat a été mis à niveau vers la version 6.0.29.
- ♦ La base de données PostgreSQL a été mise à niveau vers la version 8.3.12.

1.2 Nouveautés de Sentinel Rapid Deployment SP1

Pour obtenir des informations sur les nouveautés de Sentinel Rapid Deployment 6.1 SP1, consultez le « [fichier Lisezmoi de Sentinel Rapid Deployment SP1](http://www.novell.com/documentation/sentinel61rd/readme/data/s61rd_readme.html#bqtqd85) » (http://www.novell.com/documentation/sentinel61rd/readme/data/s61rd_readme.html#bqtqd85).

2 Configuration système requise

Pour obtenir des informations détaillées sur la configuration matérielle requise, les systèmes d'exploitation et les navigateurs pris en charge, reportez-vous à la section « [Configuration système requise](#) » du *Guide d'installation de Sentinel Rapid Deployment*.

3 Installation de Novell Sentinel Rapid Deployment

Les installations sont désormais simplifiées et le nom du fichier tar n'est plus requis en tant qu'entrée. Il vous suffit d'exécuter le script pour télécharger le programme d'installation, l'extraire vers un répertoire et l'installer en tant qu'utilisateur `root` ou non-`root`. Vous pouvez également entrer des arguments de ligne de commande pour créer uniquement l'utilisateur, installer le serveur Rapid Deployment, créer un service permettant de lancer automatiquement Sentinel Rapid Deployment au démarrage du système ou installer uniquement le serveur Rapid Deployment sans créer d'utilisateur ni de service.

Pour installer Novell Sentinel Rapid Deployment 6.1 SP2, reportez-vous à la section « [Installation](#) » du *Guide d'installation de Sentinel Rapid Deployment*.

4 Mise à niveau vers Sentinel Rapid Deployment SP2

Avant de procéder à la mise à niveau, assurez-vous que vous avez installé Sentinel 6.1 Rapid Deployment SP1 sur le système sur lequel vous souhaitez installer ce service pack :

Pour exécuter une mise à niveau vers Sentinel Rapid Deployment 6.1 SP2, reportez-vous à la section « [Mise à niveau de Sentinel Rapid Deployment](#) » du *Guide d'installation de Sentinel Rapid Deployment*.

5 Accès aux fichiers d'aide de Sentinel Rapid Deployment

Vous pouvez accéder au Guide de l'utilisateur en ligne de Sentinel Rapid Deployment en cliquant sur *Aide* > *Aide* dans Sentinel Control Center. Toutefois, si vous travaillez dans un environnement sécurisé refusant l'accès direct à Internet, vous pouvez télécharger et extraire les fichiers d'aide en ligne sur le serveur Sentinel Rapid Deployment en une seule fois. Une fois les fichiers d'aide extraits vers un emplacement spécifique, vous pouvez accéder à la documentation à partir du serveur ou du système distant. Vous pouvez afficher les fichiers d'aide à partir de n'importe quel navigateur Web.

Remarque : les fichiers d'aide sont en anglais uniquement.

Pour télécharger les fichiers d'aide en ligne, procédez comme suit :

- 1 Accédez au [site Web de documentation de Sentinel Rapid Deployment \(http://www.novell.com/documentation/sentinel61rd/\)](http://www.novell.com/documentation/sentinel61rd/).
- 2 Cliquez sur *zip* dans la section Aide du Guide de l'utilisateur téléchargeable, puis enregistrez le fichier `s61rd_user_help.zip` sur votre machine locale.
- 3 Utilisez les commandes suivantes pour copier et extraire le fichier téléchargé :

```
cp s61rd_user_help.zip <répertoire_installation>/3rdparty/tomcat/webapps/ROOT/novellsiemdownloads/help
cd <répertoire_installation>/3rdparty/tomcat/webapps/ROOT/novellsiemdownloads/help
unzip s61rd_user_help.zip
```

Important : vous ne pouvez pas accéder aux fichiers d'aide si vous n'avez pas extrait le fichier `s61rd_user_help.zip` vers l'emplacement spécifié.

- 4 Exécutez l'une des tâches suivantes pour afficher les fichiers d'aide :
 - ♦ Dans le centre de contrôle Sentinel, cliquez sur *Aide* > *Aide*.
 - ♦ Ouvrez le fichier `<répertoire_installation>/3rdparty/tomcat/webapps/ROOT/novellsiemdownloads/help/s61rd_user_help/index.html`.

Le fichier `Index.html` répertorie les différentes sections du volet de navigation. Cliquez sur la section de votre choix pour ouvrir la page d'aide correspondante.

Remarque : si vous téléchargez et enregistrez les fichiers d'aide à l'emplacement spécifié sur le serveur Sentinel Rapid Deployment, le fait de cliquer sur le menu *Aide* dans le centre de contrôle Sentinel permet toujours d'afficher le contenu d'aide téléchargé disponible sur le serveur.

Si vous souhaitez que le menu *Aide* vous permette d'accéder au *Guide de l'utilisateur de Sentinel Rapid Deployment* disponible en ligne, supprimez `s61rd_user_help` à l'emplacement `<répertoire_installation>/3rdparty/tomcat/webapps/ROOT/novellssiemdownloads/help` du serveur Sentinel Rapid Deployment.

6 Problèmes résolus et améliorations

- ♦ [Section 6.1, « Problèmes résolus », page 4](#)
- ♦ [Section 6.2, « Améliorations », page 5](#)

6.1 Problèmes résolus

Le tableau suivant répertorie les problèmes identifiés dans Sentinel Rapid Deployment 6.1 SP2 par numéro, ainsi que les solutions proposées pour les résoudre :

Numéro de bogue	Solution
451892	Si nécessaire, l'application Sentinel WebStart télécharge désormais automatiquement les polices requises.
497131	Le dernier collecteur eDirectory prend en charge les caractères japonais double octet dans la fonctionnalité de création de rapport.
531114	Si des fichiers hors rapports (.zip) sont chargés à l'aide de l'interface utilisateur Web de rapport, le navigateur affiche désormais un message indiquant qu'une erreur est survenue lors de la récupération d'un paquetage PluginPackage depuis package.xml.
556730	Le moteur de corrélation ne stocke plus les événements futurs au-delà de 30 secondes. Il n'affiche ainsi plus d'erreur de mémoire insuffisante.
566973	La fenêtre du gestionnaire des moteurs de corrélation affiche maintenant la liste des moteurs de corrélation même si elle est ouverte dans la session Sentinel Control Center précédemment enregistrée.
569849	Sentinel Rapid Deployment a été regroupé avec la dernière version Apache Tomcat 6.0.29 pour résoudre les vulnérabilités de sécurité.
573181	Pour les processus Sentinel, la mémoire est désormais allouée sous forme de pourcentage. Par ailleurs, le remplacement des allocations de mémoire depuis le fichier <code>memory.conf</code> est maintenant pris en charge.
600604	Des améliorations ont été apportées concernant les performances afin que le système ne soit pas confronté à des problèmes de mémoire insuffisante lors de la création de rapports volumineux.
607145	Des événements d'audit supplémentaires ont été créés pour surveiller les activités administratives et les modifications de configuration de Sentinel sur l'assignation des données, les filtres, les règles de corrélation, les actions et la gestion de sources d'événements.
621509	La fenêtre <i>Nouvel incident</i> fait maintenant apparaître les événements quand un utilisateur sélectionne les événements et crée un incident. Les événements sont enregistrés dans l'incident.
623834	Le message indiquant que l'espace disque a atteint son seuil maximum d'utilisation s'affiche uniquement si l'espace utilisé a atteint la valeur de seuil maximum calculée en fonction de l'espace disque du système de fichiers réel.

Numéro de bogue	Solution
625930	Le nom de règle ne fait plus apparaître une valeur nulle dans l'événement RulePerformanceSummary.
626402	Le redémarrage d'un connecteur présentant plusieurs sources d'événements dans la gestion de sources d'événements n'entraîne plus une exception de timeout.
629716	Les instances Sentinel Control Center (SCC) ne s'arrêtent plus en raison de problèmes de blocage.
641087	Sentinel Rapid Deployment a été regroupé avec la dernière version de patch PostgreSQL 8.3.12 pour résoudre les vulnérabilités de sécurité.
644821	Les utilisateurs disposant d'autorisations d'affichage dans la gestion de sources d'événements ne peuvent pas supprimer les nœuds (sources d'événements, collecteurs, gestionnaire des collecteurs) en appuyant sur le bouton Suppr de leur clavier.
648554	Le fichier de configuration Sentinel Data Manager (SDM) est maintenant créé dans le répertoire privé de l'utilisateur et non à l'emplacement depuis lequel SDM est lancé.
651181	Un outil de virtualisation Jasper est utilisé lors de la création de rapports volumineux pour réduire le délai d'interrogation.
651524	Les fichiers de flux Advisor peuvent désormais être téléchargés à l'aide d'un serveur proxy dont le mot de passe est mis à jour via le gestionnaire de téléchargements.
656595	La connexion à la base de données ne permet plus de fuite de connexions car les verrouillages sont débloqués pour les transactions ouvertes inactives pendant une longue période.
656715	Les données transmises via ActiveMQ font maintenant l'objet d'une compression pour améliorer la bande passante du réseau.
662213	L'envoi d'un message électronique à plusieurs adresses de destinataires fonctionne désormais dans les actions d'événements et d'incidents de messagerie électronique.
668443	Vous pouvez maintenant vous connecter à la base de données PostgreSQL via la ligne de commande en plus de la connexion via pgadmin.
672058	Lorsque vous redémarrez une source d'événements configurée pour émettre une alerte en cas de non-réception de données pour une période spécifique, la source d'événements ne génère plus d'événements (NoDataAlert) et de messages de journal en double.
682235	Sentinel Rapid Deployment a été regroupé avec la dernière version Java 1.6.0_24 pour résoudre les vulnérabilités de sécurité.

6.2 Améliorations

Le tableau suivant répertorie les améliorations apportées à Sentinel Rapid Deployment 6.1 SP2 pour optimiser le confort d'utilisation :

Numéro de bogue	Description
547390	Il est désormais possible de configurer la limite d'interrogation hors ligne en définissant la propriété des événements maximum dans le fichier <code>das_core.xml</code> .

Numéro de bogue	Description
642690	L'interrogation hors ligne a été optimisée grâce à la possibilité de configurer un sous-intervalle de temps d'interrogation dans le fichier <code>das_core.xml</code> .
642691	L'état de mise à jour des informations d'interrogation hors ligne est maintenant stocké dans le fichier journal <code>das_core</code> .
648108	La fenêtre d'état Advisor affiche désormais les informations relatives à tous les fichiers de flux.
673362	Le fichier d'objet JasperPrint (c'est-à-dire le fichier de résultat brut) ne fait plus partie des résultats de rapport. Ce fichier n'était pas utilisé par Sentinel. Sa suppression permet d'améliorer les performances de rapport et de libérer de l'espace disque.
680054	La prise en charge des adresses IP liées a été ajoutée comme mécanisme de basculement sur un serveur Sentinel Rapid Deployment.

7 Problèmes connus

Numéro de bogue	Description
486932	<p>Problème : un utilisateur peut supprimer une activité associée à un processus iTRAC actif.</p> <p>Solution : aucune.</p>
517568	<p>Problème : lorsque vous essayez d'installer Solution Designer séparément, le processus échoue.</p> <p>Solution : installez Solution Designer avec Sentinel Control Center ou Sentinel Data Manager.</p>
525334	<p>Problème : l'outil Identity Browser affiche des données redondantes pour le domaine Active Directory.</p> <p>Solution : aucune.</p>
598473	<p>Problème : lorsque l'interface utilisateur de gestion de sources d'événements est lancée depuis des systèmes non anglais, le Connecteur de fichiers 6r9 ne récupère pas les fichiers distants à l'aide du protocole SCP comme prévu.</p> <p>Solution : aucune. Ce problème sera résolu dans la version du Connecteur de fichiers 6r10.</p>
674008	<p>Problème : l'icône Novell et les informations de copyright ne sont pas visibles dans l'assistant Installshield Wizard sur une machine Linux.</p> <p>Solution : aucune.</p>
674720	<p>Problème : les informations concernant le générateur des collecteurs s'affichent dans l'accord de licence même si la prise en charge de l'option de générateur des collecteurs n'est pas incluse dans Sentinel 6.1 Rapid Deployment SP2.</p> <p>Solution : aucune.</p>

Numéro de bogue	Description
679830	<p>Problème : dans le gestionnaire des collecteurs Windows, la fonctionnalité d'assignation ne fonctionne pas toujours comme elle devrait.</p> <p>Solution : procédez comme suit :</p> <ol style="list-style-type: none"> 1. Arrêtez le gestionnaire des collecteurs. <pre data-bbox="456 474 1130 495"><répertoire_installation>/bin/sentinel.bat stop</pre> 2. Ouvrez le fichier journal du gestionnaire des collecteurs <code>collector_mgr0.0.log</code> depuis le répertoire <code><répertoire_installation>/log</code>. 3. Recherchez une erreur identique à celle indiquée ci-dessous. <pre data-bbox="456 625 1341 705">Le répertoire système temporaire (propriété java.io.tmpdir) de C:\Windows\system32\config\systemprofile\AppData\Local\Temp\ semble non valide.</pre> 4. Créez un dossier <code>Temp</code> à l'emplacement suivant : <p>Systèmes Windows 64 bits :</p> <pre data-bbox="456 806 1243 827">C:\Windows\syzow64\config\systemprofile\AppData\Local\</pre> <p>Systèmes Windows 32 bits :</p> <pre data-bbox="456 890 1243 911">C:\Windows\system32\config\systemprofile\AppData\Local\</pre> 5. Redémarrez le gestionnaire des collecteurs : <pre data-bbox="456 974 1146 995"><répertoire_installation>/bin/sentinel.bat start</pre>
680054	<p>Problème : le serveur Sentinel Rapid Deployment ne parvient pas à déterminer automatiquement l'adresse IP.</p> <p>Solution : procédez comme suit :</p> <ol style="list-style-type: none"> 1. Créez un fichier <code>start_tomcat.properties</code> sous le répertoire <code><répertoire_installation>/sentinel_rd/config</code>. <p>Assurez-vous que l'utilisateur exécutant le serveur Sentinel Rapid Deployment dispose de ce fichier et des autorisations d'exécution nécessaires.</p> 2. Indiquez l'adresse IP dans le nouveau fichier en ajoutant la ligne suivante : <pre data-bbox="456 1352 854 1373">SERVER_IP=<ip_address_value></pre> 3. Enregistrez le fichier. 4. Loguez-vous en tant qu'utilisateur propriétaire des fichiers d'installation Sentinel et redémarrez le serveur en utilisant la commande suivante : <pre data-bbox="456 1499 724 1520">sentinel.sh restart</pre> 5. Vérifiez l'adresse IP à l'emplacement suivant pour voir si l'adresse IP remplacée est utilisée : <pre data-bbox="456 1604 1308 1663">fichiers jnlp sous %ESEC_HOME/3rdparty/tomcat/webapps/ROOT/novellsiemdownloads</pre>
680154	<p>Problème : l'onglet d'<i>espace de table</i> sur Sentinel Data Manager affiche des données incorrectes pour l'espace utilisé/disponible. L'espace utilisé/disponible est calculé en fonction de l'espace de table <code>sendata1</code> au lieu de l'espace disque réel.</p> <p>Solution : aucune.</p>

Numéro de bogue	Description
685187	<p>Problème : lorsque vous essayez d'installer le gestionnaire des collecteurs à distance en mode console, le programme d'installation ne parvient pas à importer le certificat de courtier depuis le serveur.</p> <p>Solution : vous pouvez installer le gestionnaire des collecteurs en mode console sur un système à distance en utilisant <code>ssh</code> en mode graphique pour vous connecter au système. Par exemple, <code>ssh -x <IP_système></code>.</p>

8 Documentation

Les notes de version et la documentation mises à jour sont disponibles sur le [site Web de documentation de Sentinel Rapid Deployment \(http://www.novell.com/documentation/sentinel61rd/index.html\)](http://www.novell.com/documentation/sentinel61rd/index.html).

9 Mentions légales

Novell, Inc. exclut toute garantie relative au contenu ou à l'utilisation de cette documentation. En particulier, Novell ne garantit pas que cette documentation est exhaustive ni exempte d'erreurs. Novell, Inc. se réserve en outre le droit de réviser cette publication à tout moment et sans préavis.

Par ailleurs, Novell exclut toute garantie relative à tout logiciel, notamment toute garantie, expresse ou implicite, que le logiciel présenterait des qualités spécifiques ou qu'il conviendrait à un usage particulier. Novell se réserve en outre le droit de modifier à tout moment tout ou partie des logiciels Novell, sans notification préalable de ces modifications à quiconque.

Tous les produits ou informations techniques fournis dans le cadre de ce contrat peuvent être soumis à des contrôles d'exportation aux États-Unis et à la législation commerciale d'autres pays. Vous acceptez de vous conformer à toutes les réglementations de contrôle des exportations et à vous procurer les licences requises ou la classification permettant d'exporter, de réexporter ou d'importer des biens de consommation. Vous acceptez de ne pas procéder à des exportations ou à des réexportations vers des entités figurant sur les listes noires d'exportation en vigueur aux États-Unis ou vers des pays terroristes ou soumis à un embargo par la législation américaine en matière d'exportations. Vous acceptez de ne pas utiliser les produits livrables pour le développement prohibé d'armes nucléaires, de missiles ou chimiques et biologiques. Reportez-vous à la [page Web des services de commerce international de Novell \(http://www.novell.com/info/exports/\)](http://www.novell.com/info/exports/) pour plus d'informations sur l'exportation des logiciels Novell. Novell décline toute responsabilité dans le cas où vous n'obtiendriez pas les approbations d'exportation nécessaires.

Copyright © 2011 Novell, Inc. Tous droits réservés. Cette publication ne peut être reproduite, photocopiée, stockée sur un système de recherche documentaire ou transmise, même en partie, sans le consentement écrit explicite préalable de l'éditeur.

Pour connaître les marques commerciales de Novell, reportez-vous à la [liste des marques commerciales et des marques de service de Novell \(http://www.novell.com/company/legal/trademarks/tmlist.html\)](http://www.novell.com/company/legal/trademarks/tmlist.html).

Toutes les marques commerciales de fabricants tiers appartiennent à leur propriétaire respectif.