

# Readme di Novell Sentinel 6.1 Rapid Deployment SP2

Aprile 2011

Novell®

Sentinel Rapid Deployment è una nuova opzione di packaging per la soluzione Novell Sentinel Security Information and Event Management leader del mercato. Sentinel Rapid Deployment include tutte le funzionalità di Sentinel ed è la soluzione ideale per organizzazioni di piccole dimensioni o per installazioni a livello regionale.

Sentinel 6.1 Rapid Deployment SP2 è disponibile sia come programma di installazione pulito, sia come programma di installazione dell'upgrade. Il programma di installazione dell'upgrade applica le correzioni e i miglioramenti software più recenti a un'installazione esistente di Sentinel Rapid Deployment 6.1 SP1.

- ♦ [Sezione 1, “Novità”, a pagina 1](#)
- ♦ [Sezione 2, “Requisiti di sistema”, a pagina 2](#)
- ♦ [Sezione 3, “Installazione di Novell Sentinel Rapid Deployment”, a pagina 2](#)
- ♦ [Sezione 4, “Upgrade a Sentinel Rapid Deployment SP2”, a pagina 3](#)
- ♦ [Sezione 5, “Accesso ai file della Guida di Sentinel Rapid Deployment”, a pagina 3](#)
- ♦ [Sezione 6, “Difetti corretti e miglioramenti”, a pagina 4](#)
- ♦ [Sezione 7, “Problemi noti”, a pagina 6](#)
- ♦ [Sezione 8, “Documentazione”, a pagina 8](#)
- ♦ [Sezione 9, “Note legali”, a pagina 8](#)

## 1 Novità

- ♦ [Sezione 1.1, “Novità di Sentinel Rapid Deployment 6.1 SP2”, a pagina 1](#)
- ♦ [Sezione 1.2, “Novità di Sentinel Rapid Deployment SP1”, a pagina 2](#)

### 1.1 Novità di Sentinel Rapid Deployment 6.1 SP2

- ♦ [“Supporto per SLES 11 SP1” a pagina 1](#)
- ♦ [“Limiti al supporto del servizio di raccolta esistente” a pagina 2](#)
- ♦ [“Miglioramenti alla sicurezza” a pagina 2](#)

#### 1.1.1 Supporto per SLES 11 SP1

Sentinel Rapid Deployment adesso è supportato sulla piattaforma SUSE Linux Enterprise Server (SLES) 11 SP1 a 64 bit.

### 1.1.2 Limiti al supporto del servizio di raccolta esistente

Novell è in processo di interrompere gradualmente il supporto al Servizio di raccolta esistente nella linea dei prodotti Sentinel. Nelle versioni precedenti di Sentinel Rapid Deployment, se si importa un servizio di raccolta esistente viene generato un avviso dal sistema. A partire dalla versione SP2, nelle installazioni pulite di Sentinel Rapid Deployment e Gestione servizi di raccolta non vengono eseguiti i servizi di raccolta esistenti. Tuttavia, i sistemi in cui è stato eseguito l'upgrade di Sentinel Rapid Deployment e Gestione servizi di raccolta continuano a eseguire i servizi di raccolta esistenti come prima.

---

**Nota:** i servizi di raccolta esistenti sono stati scritti utilizzando l'applicazione di generazione dei servizi di raccolta esistenti, che non viene più distribuita insieme ai prodotti Sentinel. I servizi di raccolta esistenti vengono sostituiti dai servizi di raccolta JavaScript che vengono scritti mediante Sentinel Plug-In SDK. I servizi di raccolta JavaScript sono disponibili nel [sito Web dei plug-in di Sentinel 6.1](http://support.novell.com/products/sentinel/secure/sentinel61.html) (<http://support.novell.com/products/sentinel/secure/sentinel61.html>).

---

### 1.1.3 Miglioramenti alla sicurezza

Sentinel Rapid Deployment 6.1 SP include diversi aggiornamenti volti a migliorare la sicurezza del prodotto:

- È stato eseguito l'upgrade di Java Runtime Environment (JRE) alla versione 1.6.0\_24.
- È stato eseguito l'upgrade di Apache Tomcat alla versione 6.0.29.
- È stato eseguito l'upgrade del database PostgreSQL alla versione 8.3.12.

## 1.2 Novità di Sentinel Rapid Deployment SP1

Per informazioni sulle novità di Sentinel Rapid Deployment 6.1 SP1, vedere il “[Readme di 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](http://www.novell.com/documentation/sentinel61rd/readme/data/s61rd_readme.html#bqtqd85)).

## 2 Requisiti di sistema

Per informazioni dettagliate su requisiti hardware, sistemi operativi supportati e browser, vedere la sezione “[Requisiti di sistema](#)” nella *Guida all'installazione di Sentinel Rapid Deployment*.

## 3 Installazione di Novell Sentinel Rapid Deployment

Adesso il processo di installazione è più semplice e non è più necessario specificare il nome del file tar. È possibile effettuare il download del programma di installazione, estrarlo in una directory e installarlo come utente `root` o non radice semplicemente eseguendo lo script. È inoltre possibile specificare dalla riga di comando di creare solo l'utente, installare il server Rapid Deployment, creare il servizio di avvio automatico di Sentinel Rapid Deployment all'avvio del sistema o installare solo il server Rapid Deployment senza creare l'utente o il servizio.

Per installare Novell Sentinel Rapid Deployment 6.1 SP2, vedere la sezione “[Installazione](#)” nella *Guida all'installazione di Sentinel Rapid Deployment*.

## 4 Upgrade a Sentinel Rapid Deployment SP2

Prima di procedere con l'upgrade, assicurarsi che sul sistema in cui si desidera installare il service pack sia installato Sentinel 6.1 Rapid Deployment SP1:

Per eseguire l'upgrade a Sentinel Rapid Deployment 6.1 SP2, vedere la sezione “[Upgrade di Sentinel Rapid Deployment](#)” nella *Guida all'installazione di Sentinel Rapid Deployment*.

## 5 Accesso ai file della Guida di Sentinel Rapid Deployment

È possibile accedere alla Guida dell'utente online di Sentinel Rapid Deployment facendo clic su *Guida > Guida* in Sentinel Control Center. Tuttavia, se si utilizza un ambiente sicuro in cui l'accesso diretto a Internet è negato, è possibile effettuare il download ed estrarre il file della Guida online nel server Sentinel Rapid Deployment come procedura unica. Dopo l'estrazione dei file della Guida in un'ubicazione specifica, è possibile accedere alla documentazione tramite il server o il sistema remoto. È possibile visualizzare i file della Guida da qualsiasi browser Web.

---

**Nota:** i file della Guida sono unicamente in lingua inglese.

---

Per effettuare il download della Guida online:

- 1 Accedere al [sito relativo alla documentazione di Sentinel Rapid Deployment \(http://www.novell.com/documentation/sentinel61rd/\)](http://www.novell.com/documentation/sentinel61rd/).
- 2 Fare clic su *zip* nella sezione Downloadable User Guide Help, quindi salvare il file `s61rd_user_help.zip` sul computer locale.
- 3 Utilizzare i seguenti comandi per copiare ed estrarre il file di cui si è effettuato il download:

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

---

**Importante:** non è possibile accedere ai file della Guida se non si estrae il file `s61rd_user_help.zip` in un'ubicazione specificata.

---

- 4 Per visualizzare i file della Guida, eseguire una delle seguenti operazioni:
  - ♦ In Sentinel Control Center, fare clic su *Guida > Guida*.
  - ♦ Aprire il file `<Directory_di_installazione>/3rdparty/tomcat/webapps/ROOT/novellsiemdownloads/help/s61rd_user_help/index.html`.

Nel file `Index.html` sono elencati gli argomenti nel riquadro di navigazione. Fare clic sull'argomento desiderato per aprire la pagina della Guida corrispondente.

---

**Nota:** se si effettua il download e si salvano i file della Guida in un'ubicazione specificata sul server Sentinel Rapid Deployment, facendo clic sul menu *Guida* di Sentinel Control Center viene sempre visualizzato il contenuto della Guida di cui si è effettuato il download disponibile sul server.

---

Per essere ridiretti dal menu *Guida* alla *Sentinel Rapid Deployment User Guide* (in lingua inglese) disponibile online, rimuovere la cartella `s61rd_user_help` in `<Directory_di_installazione>/3rdparty/tomcat/webapps/ROOT/novellsiemdownloads/help` dal server Sentinel Rapid Deployment.

## 6 Difetti corretti e miglioramenti

- ♦ [Sezione 6.1, “Difetti corretti”, a pagina 4](#)
- ♦ [Sezione 6.2, “Miglioramenti”, a pagina 5](#)

### 6.1 Difetti corretti

Nella tabella seguente sono elencati i numeri relativi ai difetti e le soluzioni fornite in Sentinel Rapid Deployment 6.1 SP2:

Numero bug	Soluzione
451892	L'applicazione Sentinel WebStart adesso effettua automaticamente il download dei font richiesti, se necessario.
497131	Il servizio di raccolta eDirectory più recente adesso è in grado di gestire i caratteri giapponesi a doppio byte nella funzione di generazione di rapporti.
531114	Quando si effettua l'upload di file non di rapporto (.zip) mediante l'uso dell'interfaccia utente Web dei rapporti, adesso nel browser viene visualizzato l'errore Si è verificato un errore durante l'ottenimento di un PluginPackage da package.xml.
556730	Gli eventi futuri di oltre 30 secondi non vengono più memorizzati nel motore di correlazione, pertanto non viene visualizzato alcun errore di memoria esaurita.
566973	Nella finestra Gestione motore di correlazione adesso viene visualizzato l'elenco dei motori di correlazione, anche se la finestra è aperta nella sessione di Sentinel Control Center precedentemente salvata.
569849	Sentinel Rapid Deployment adesso viene offerto con la versione più recente 6.0.29 di Apache Tomcat per correggere le vulnerabilità a livello di sicurezza.
573181	Per i processi di Sentinel, adesso la memoria viene allocata in percentuali. Viene altresì fornito ulteriore supporto per ignorare le allocazioni di memoria dal file <code>memory.conf</code> .
600604	Miglioramenti a livello di prestazioni in modo che la memoria di sistema non venga esaurita durante l'esecuzione di rapporti di grandi dimensioni.
607145	Adesso vengono creati eventi di revisione aggiuntivi per controllare l'attività amministrativa di Sentinel e le modifiche alla configurazione relative a mappatura dei dati, filtri, regole di correlazione, azioni e Gestione origine eventi (ESM).
621509	Adesso, quando un utente seleziona gli eventi e crea un caso, gli eventi salvati come parte del caso vengono visualizzati nella finestra <i>Nuovo caso</i> .
623834	Il messaggio Livello soglia superiore raggiunto dall'utilizzo dello spazio su disco viene visualizzato solo quando l'utilizzo dello spazio raggiunge il valore della soglia superiore, calcolato in base allo spazio su disco effettivo del file system.
625930	Il campo Nome regola nell'evento RulePerformanceSummary non è più nullo.

Numero bug	Soluzione
626402	Il riavvio di un servizio di raccolta con più origini eventi in Gestione origini eventi non genera più un'eccezione di timeout.
629716	Le istanze di Sentinel Control Center (SCC) non si bloccano più a causa dei problemi di stallo.
641087	Sentinel Rapid Deployment adesso viene offerto con la versione patch più recente 8.3.12 di PostgreSQL per risolvere le vulnerabilità a livello di sicurezza.
644821	L'utente dotato di autorizzazioni alla visualizzazione in Gestione origini eventi non può eliminare i nodi (Origini eventi, Servizi di raccolta, Gestione servizi di raccolta) premendo il pulsante Elimina sulla tastiera.
648554	Il file di configurazione di Gestione dati Sentinel (SDM) adesso viene creato nella home directory dell'utente e non nell'ubicazione di avvio di SDM.
651181	Per l'esecuzione di rapporti di grandi dimensioni viene utilizzato un virtualizzatore Jasper per ridurre i tempi di interrogazione.
651524	Adesso è possibile effettuare il download dei file feed di Advisor utilizzando un server proxy e la password del proxy viene aggiornata da Gestione download.
656595	La connessione al database rimane ininterrotta perché i blocchi vengono rilasciati per le transazioni aperte inattive da molto tempo.
656715	I dati trasmessi su ActiveMQ adesso sono compressi per migliorare la larghezza di banda della rete.
662213	L'invio di e-mail a più indirizzi del destinatario adesso funziona nelle azioni Invia eventi tramite e-mail e Invia caso tramite e-mail.
668443	Adesso è possibile connettersi al database PostgreSQL dalla riga di comando oltre che da Pgadmin.
672058	Quando si avvia un'origine evento configurata per avvisare l'utente della mancata ricezione dei dati per un periodo specificato, l'origine evento non genera più eventi duplicati (NoDataAlert) e messaggi di log.
682235	Sentinel Rapid Deployment adesso viene offerto con la versione più recente 1.6.0_24 di Java correggere le vulnerabilità a livello di sicurezza.

## 6.2 Miglioramenti

Nella seguente tabella sono elencati i miglioramenti apportati in Sentinel Rapid Deployment 6.1 SP2 per un utilizzo ottimale:

Numero bug	Descrizione
547390	Adesso è possibile configurare il limite di interrogazione offline impostando la proprietà relativa al numero massimo di eventi nel file <code>das_core.xml</code> .
642690	L'interrogazione offline è stata migliorata in modo da poter configurare il tempo di interrogazione dei sottointervalli nel file <code>das_core.xml</code> .
642691	Lo stato di aggiornamento delle informazioni sull'interrogazione offline adesso è memorizzato nel file di log <code>das_core</code> .

Numero bug	Descrizione
648108	Adesso nella finestra Stato Advisor vengono visualizzate le informazioni su tutti i file feed.
673362	Il file oggetto JasperPrint (ovvero, il file dei risultati non elaborato denominato results) non è più incluso nei risultati del rapporto. Questo file non è stato utilizzato da Sentinel e rimuoverlo consente di migliorare le prestazioni del rapporto e di salvare spazio su disco.
680054	In un server Sentinel Rapid Deployment, il supporto per gli indirizzi IP associati viene aggiunto come meccanismo di failover.

## 7 Problemi noti

Numero bug	Descrizione
486932	<p><b>Problema:</b> l'utente è in grado di eliminare un'attività associata a un processo iTRAC attivo.</p> <p><b>Soluzione:</b> nessuna.</p>
517568	<p><b>Problema:</b> l'installazione separata di Solution Designer risulta impossibile.</p> <p><b>Soluzione:</b> Installare Solution Designer con Sentinel Control Center o Gestione dati Sentinel.</p>
525334	<p><b>Problema:</b> nel Browser identità vengono visualizzati dati ridondanti per il dominio Active Directory.</p> <p><b>Soluzione:</b> nessuna.</p>
598473	<p><b>Problema:</b> quando si avvia l'interfaccia utente di Gestione origine eventi da un sistema in lingua diversa dall'inglese, il connettore file 6r9 non recupera i file remoti mediante l'uso del protocollo SCP come previsto.</p> <p><b>Soluzione:</b> nessuna. Questo problema sarà corretto nella versione 6r10 del connettore file.</p>
674008	<p><b>Problema:</b> l'icona e le informazioni sul copyright di Novell non sono visibili nella Procedura guidata Installshield su un computer Linux.</p> <p><b>Soluzione:</b> nessuna.</p>
674720	<p><b>Problema:</b> le informazioni su Generatore servizi di raccolta sono visualizzate nel contratto di licenza anche se il supporto per tale opzione non è incluso in Sentinel 6.1 Rapid Deployment SP2.</p> <p><b>Soluzione:</b> nessuna.</p>

---

Numero bug	Descrizione
------------	-------------

---

679830 **Problema:** in Generatore servizi di raccolta Windows, la funzionalità di mappatura talvolta non funziona come dovrebbe.

**Soluzione:** seguire la procedura indicata:

1. Interrompere Gestione servizi di raccolta:

```
<directory_di_installazione>/bin/sentinel.bat stop
```

2. Aprire il file di log `collector_mgr0.0.log` di Gestione servizi di raccolta nella directory `<directory_di_installazione>/log`.

3. Cercare un errore simile a quello riportato di seguito:

```
La directory temporanea del sistema (java.io.tmpdir property) di  
C:\Windows\system32\config\systemprofile\AppData\Local\Temp\  
sembra non valida.
```

4. Creare una cartella denominata Temp nell'ubicazione seguente:

**Sistemi Windows a 64 bit:**

```
C:\Windows\syswow64\config\systemprofile\AppData\Local\
```

**Sistemi Windows a 32 bit:**

```
C:\Windows\system32\config\systemprofile\AppData\Local\
```

5. Riavviare Gestione servizi di raccolta:

```
<directory_di_installazione>/bin/sentinel.bat start
```

680054 **Problema:** per il server Sentinel Rapid Deployment è impossibile determinare automaticamente l'indirizzo IP.

**Soluzione:** seguire la procedura indicata:

1. Creare un file `start_tomcat.properties` nella directory `<directory_di_installazione>/sentinel_rd/config`.

Assicurarsi che l'utente che esegue il server Sentinel Rapid Deployment sia il proprietario del file e che disponga delle autorizzazioni per l'esecuzione.

2. Specificare l'indirizzo IP nel file appena creato aggiungendo la seguente riga:

```
SERVER_IP=<ip_address_value>
```

3. Salvare il file.

4. Eseguire il login come utente proprietario dei file di installazione Sentinel e riavviare il server utilizzando il seguente comando:

```
sentinel.sh restart
```

5. Verificare che nell'ubicazione seguente sia stato utilizzato l'indirizzo IP prioritario:

```
file jnlp in $ESEC_HOME/3rdparty/tomcat/webapps/ROOT/  
novellsiemdownloads
```

680154 **Problema:** lo spazio utilizzato e quello libero visualizzati nella scheda *Spazi delle tabelle* di Gestione dati Sentinel sono errati. Lo spazio utilizzato e quello libero vengono calcolati in base allo spazio della tabella `sendata1` al posto dello spazio su disco effettivo.

**Soluzione:** nessuna.

---

---

Numero bug	Descrizione
685187	<p><b>Problema:</b> quando si tenta di installare Gestione servizi di raccolta remoto dalla modalità console, è impossibile importare il certificato broker dal server.</p> <p><b>Soluzione:</b> è possibile installare Gestione servizi di raccolta in modalità console su un sistema remoto utilizzando <code>ssh</code> in modalità grafica per connettersi al sistema. Ad esempio, <code>ssh -x &lt;IP_sistema&gt;</code>.</p>

---

## 8 Documentazione

La documentazione aggiornata e le note sulla versione sono disponibili nel [sito relativo alla documentazione di Sentinel Rapid Deployment \(http://www.novell.com/documentation/sentinel61rd/index.html\)](http://www.novell.com/documentation/sentinel61rd/index.html).

## 9 Note legali

Novell, Inc. non rilascia dichiarazioni o garanzie in merito a contenuto o utilizzo di questa documentazione e in particolare declina qualsiasi garanzia espressa o implicita di commerciabilità o idoneità a scopo particolare. Novell, Inc. inoltre si riserva il diritto di aggiornare la presente pubblicazione e di modificarne il contenuto in qualsiasi momento, senza alcun obbligo di notificare tali revisioni o modifiche ad alcuna persona fisica o entità.

Novell, Inc. non rilascia dichiarazioni o garanzie in merito a software e in modo specifico declina qualsiasi garanzia espressa o implicita di commerciabilità o idoneità a scopo particolare. Novell, Inc. inoltre si riserva il diritto di modificare parti del software Novell in qualsiasi momento, senza alcun obbligo di notificare tali modifiche ad alcuna persona fisica o entità.

Qualsiasi informazione tecnica o prodotto fornito con il presente Contratto può essere soggetto ai controlli statunitensi relativi alle esportazioni e alla normativa del commercio in vigore in altri paesi. L'utente acconsente a conformarsi a tutte le norme che controllano le esportazioni e a ottenere le eventuali licenze o autorizzazioni necessarie per l'esportazione, la riesportazione o l'importazione di prodotti. L'utente si impegna inoltre a non esportare o riesportare verso entità incluse negli elenchi di esclusione delle esportazioni statunitensi o a qualsiasi paese sottoposto a embargo o che sostiene azioni terroristiche, come specificato nella legislazione statunitense che regola le esportazioni. L'utente accetta infine di non utilizzare i prodotti a fini proibiti correlati all'uso di armi nucleari, missilistiche o biochimiche. Per ulteriori informazioni sull'esportazione del software Novell, vedere la [pagina Web dei servizi commerciali internazionali di Novell \(http://www.novell.com/info/exports/\)](http://www.novell.com/info/exports/). Novell non si assume alcuna responsabilità relativa al mancato ottenimento, da parte dell'utente, delle autorizzazioni necessarie all'esportazione.

Copyright © 2011 Novell, Inc. Tutti i diritti riservati. È vietato riprodurre, fotocopiare, memorizzare su un sistema di recupero o trasmettere la presente pubblicazione o parti di essa senza l'espresso consenso scritto dell'editore.

Per informazioni sui marchi di fabbrica di Novell, vedere [l'elenco dei marchi di fabbrica e di servizio di Novell \(http://www.novell.com/company/legal/trademarks/tmlist.html\)](http://www.novell.com/company/legal/trademarks/tmlist.html).

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