

Readme do Novell Sentinel 6.1 Rapid Deployment SP2

Abril de 2011

Novell®

O Sentinel Rapid Deployment é uma nova opção de pacote para o Gerenciamento de Segurança, Informações e Eventos do Sentinel, uma solução líder de mercado lançada pela Novell. O Sentinel Rapid Deployment inclui todas as funcionalidades do Sentinel e é ideal para organizações menores ou instalações locais.

O Sentinel 6.1 Rapid Deployment SP2 está disponível como instalador simples ou instalador de upgrade. O instalador de upgrade aplica as correções e melhorias mais recentes de software a uma instalação existente do Sentinel Rapid Deployment 6.1 SP1.

- ♦ [Seção 1, “O que há de novo” na página 1](#)
- ♦ [Seção 2, “Requisitos do sistema” na página 2](#)
- ♦ [Seção 3, “Instalando o Novell Sentinel Rapid Deployment” na página 2](#)
- ♦ [Seção 4, “Fazendo upgrade para o Sentinel Rapid Deployment SP2” na página 2](#)
- ♦ [Seção 5, “Acessando os arquivos de ajuda do Sentinel Rapid Deployment” na página 3](#)
- ♦ [Seção 6, “Defeitos corrigidos e aperfeiçoamentos” na página 4](#)
- ♦ [Seção 7, “Problemas conhecidos” na página 6](#)
- ♦ [Seção 8, “Documentação” na página 8](#)
- ♦ [Seção 9, “Informações legais” na página 8](#)

1 O que há de novo

- ♦ [Seção 1.1, “O que há de novo no Sentinel Rapid Deployment 6.1 SP2” na página 1](#)
- ♦ [Seção 1.2, “O que há de novo no Sentinel Rapid Deployment SP1” na página 2](#)

1.1 O que há de novo no Sentinel Rapid Deployment 6.1 SP2

- ♦ [“Suporte para SLES 11 SP1” na página 1](#)
- ♦ [“Limitações ao suporte do coletor Legacy” na página 1](#)
- ♦ [“Melhorias de segurança” na página 2](#)

1.1.1 Suporte para SLES 11 SP1

O Sentinel Rapid Deployment agora é suportado na plataforma SUSE Linux Enterprise Server (SLES) 11 SP1 de 64 bits.

1.1.2 Limitações ao suporte do coletor Legacy

A Novell está eliminando o suporte a Coletores Legacy na linha de produtos Sentinel. Nas versões anteriores do Sentinel Rapid Deployment, o sistema exibe um aviso quando você importa um Coletor Legacy. A partir da versão SP2, as instalações limpas do Sentinel Rapid Deployment e do

Gerenciador de Coletor não executam os Coletores Legacy. Porém, os sistemas Sentinel Rapid Deployment e os Gerenciadores de Coletor atualizados continuam a executar os Coletores Legacy como antes.

Observação: Os Coletores Legacy foram desenvolvidos usando o aplicativo Construtor de Coletores Legacy, que não é mais distribuído com os produtos Sentinel. Eles foram substituídos pelos Coletores JavaScript, desenvolvidos usando o Sentinel Plug-In SDK. Os Coletores JavaScript estão disponíveis no [site de plug-ins do Sentinel 6.1](http://support.novell.com/products/sentinel/secure/sentinel61.html) (<http://support.novell.com/products/sentinel/secure/sentinel61.html>).

1.1.3 Melhorias de segurança

O Sentinel Rapid Deployment 6.1 SP2 inclui diversas atualizações para melhorar a segurança do produto:

- ♦ O Java Runtime Environment (JRE) foi atualizado para a versão 1.6.0_24.
- ♦ O Apache Tomcat foi atualizado para a versão 6.0.29.
- ♦ O banco de dados PostgreSQL foi atualizado para a versão 8.3.12.

1.2 O que há de novo no Sentinel Rapid Deployment SP1

Para obter informações sobre as novidades do Sentinel Rapid Deployment 6.1 SP1, consulte o [“Readme do 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 Requisitos do sistema

Para obter informações detalhadas sobre os requisitos de hardware, os sistemas operacionais e os browsers suportados, consulte [“Requisitos do sistema”](#) no *Guia de Instalação do Sentinel Rapid Deployment*.

3 Instalando o Novell Sentinel Rapid Deployment

A instalação foi simplificada e o nome do arquivo tar não é mais necessário como entrada. É possível fazer download do instalador, extraí-lo em um diretório e depois instalá-lo como usuário root ou não root apenas executando o script. É possível também especificar argumentos de linha de comando para criar apenas o usuário, instalar o servidor Rapid Deployment, criar serviço para iniciar automaticamente o Sentinel Rapid Deployment na inicialização do sistema ou instalar apenas o servidor Rapid Deployment sem criar usuário nem serviço.

Para instalar o Novell Sentinel Rapid Deployment 6.1 SP2, consulte [“Instalação”](#) no *Guia de Instalação do Sentinel Rapid Deployment*.

4 Fazendo upgrade para o Sentinel Rapid Deployment SP2

Antes de continuar com o upgrade, verifique se você instalou o Sentinel 6.1 Rapid Deployment SP1 no sistema em que vai instalar este service pack:

Para fazer upgrade para o Sentinel Rapid Deployment 6.1 SP2, consulte “[Fazendo upgrade do Sentinel Rapid Deployment](#)” no *Guia de Instalação do Sentinel Rapid Deployment*.

5 Acessando os arquivos de ajuda do Sentinel Rapid Deployment

É possível acessar o guia do Usuário online do Sentinel Rapid Deployment clicando em *Ajuda > Ajuda* no Sentinel Control Center. No entanto, se estiver trabalhando em um ambiente seguro no qual o acesso direto à Internet seja negado, você poderá fazer download e extrair o arquivo de Ajuda online para o servidor Sentinel Rapid Deployment como um procedimento único. Após a extração dos arquivos de ajuda em um local específico, você poderá acessar a documentação pelo servidor ou pelo sistema remoto. É possível ver os arquivos de ajuda em qualquer browser da Web.

Observação: Os arquivos de ajuda estão apenas em inglês.

Para fazer download da ajuda online:

- 1 Vá para o [site da documentação do Sentinel Rapid Deployment \(http://www.novell.com/documentation/sentinel61rd/\)](http://www.novell.com/documentation/sentinel61rd/).
- 2 Clique em *zip* na seção Downloadable User Guide Help (Ajuda do Guia do Usuário obtida por Download), depois grave o arquivo `s61rd_user_help.zip` na máquina local.
- 3 Use os seguintes comandos para copiar e extrair o arquivo obtido por download:

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

Importante: Não será possível acessar os arquivos de ajuda, exceto se você extrair o arquivo `s61rd_user_help.zip` no local especificado.

- 4 Execute um dos procedimentos a seguir para ver os arquivos de ajuda:
 - ♦ No Sentinel Control Center, clique em *Ajuda > Ajuda*.
 - ♦ Abra o arquivo `<Diretório_de_Instalação>/3rdparty/tomcat/webapps/ROOT/novellsiemdownloads/help/s61rd_user_help/index.html`.

O arquivo `Index.html` lista os tópicos no painel de navegação. Clique no tópico desejado para abrir a página de Ajuda desse tópico.

Observação: Se você fizer download e gravar os arquivos de ajuda no local especificado no servidor Sentinel Rapid Deployment, ao clicar no menu *Ajuda* no Sentinel Control Center, sempre aparecerá a lista do conteúdo de ajuda obtido por download disponível no servidor.

Para que o menu *Ajuda* leve você até o *Sentinel Rapid Deployment User Guide* (Guia do Usuário do Sentinel Rapid Deployment) disponível online, remova a pasta `s61rd_user_help` em `<Diretório_de_Instalação>/3rdparty/tomcat/webapps/ROOT/novellsiemdownloads/help` do servidor Sentinel Rapid Deployment.

6 Defeitos corrigidos e aperfeiçoamentos

- ♦ [Seção 6.1, “Defeitos corrigidos” na página 4](#)
- ♦ [Seção 6.2, “Aperfeiçoamentos” na página 5](#)

6.1 Defeitos corrigidos

A tabela a seguir relaciona os números dos defeitos e as soluções fornecidas para esses defeitos no Sentinel Rapid Deployment 6.1 SP2:

Número do bug	Solução
451892	O aplicativo Sentinel WebStart faz download automaticamente das fontes requeridas, se necessário.
497131	O Coletor do eDirectory mais recente agora reconhece os caracteres japoneses de byte duplo no recurso de geração de relatórios.
531114	Quando é feito upload de arquivos que não são relatórios (.zip) por meio da interface de usuário da Web de Relatórios, o browser exibe este erro: <code>Error getting a PluginPackage from package.xml</code> (Erro ao obter um PluginPackage de package.xml).
556730	O Mecanismo de Correlação não armazena mais eventos futuros com mais de 30 segundos no futuro, portanto, ele não exibe um erro de falta de memória.
566973	A janela Gerenciador de Mecanismos de Correlação exibe agora a lista de Mecanismos de Correlação, mesmo se a lista estiver aberta na sessão do Sentinel Control Center que já foi gravada.
569849	O Sentinel Rapid Deployment agora vem com a versão mais recente do Apache Tomcat 6.0.29 para corrigir vulnerabilidades de segurança.
573181	Para os processos do Sentinel, a memória é alocada como porcentagens. Foi incluído também o suporte à substituição de alocações de memória do arquivo <code>memory.conf</code> .
600604	Foram feitas melhorias no desempenho, como o sistema não ficar sem memória enquanto executa grandes relatórios.
607145	Eventos de auditoria adicionais foram criados para monitorar as mudanças de configuração e as atividades administrativas do Sentinel no mapeamento de dados, nos filtros, nas regras de correlação, nas ações e no Gerenciamento de Fonte de Eventos (ESM).
621509	A janela <i>Novo Incidente</i> exibe os eventos quando um usuário seleciona os eventos e cria um incidente, e os eventos são gravados como parte do incidente.
623834	A mensagem <code>Diskspace usage reached upper threshold</code> (A utilização do espaço em disco atingiu o limite máximo) é exibida apenas quando o espaço de utilização atinge o valor do limite máximo calculado com base no espaço em disco real do sistema de arquivos.
625930	O nome da Regra no evento <code>RulePerformanceSummary</code> não aparece mais como nulo.
626402	Quando um Conector com várias fontes de eventos no ESM é reiniciado, não aparece mais uma exceção de tempo de espera.

Número do bug	Solução
629716	As instâncias do Sentinel Control Center (SCC) não ficam mais congeladas por causa de problemas de deadlock.
641087	O Sentinel Rapid Deployment agora vem com a versão mais recente do patch do PostgreSQL 8.3.12 para resolver as vulnerabilidades de segurança.
644821	O usuário com permissão de exibição no ESM não pode apagar os nós (Fontes de Eventos, Coletores, Gerenciador de Coletor) pressionando a tecla Delete do teclado.
648554	O arquivo de configuração do Gerenciador de Dados do Sentinel (SDM) é criado no diretório pessoal do usuário, e não no local de onde o SDM foi iniciado
651181	Um virtualizador do Jasper é usado na execução de relatórios grandes para diminuir o tempo de consulta.
651524	É possível agora fazer download dos arquivos de feed do Advisor usando um servidor proxy, e a senha de proxy é atualizada pelo gerenciador de download.
656595	A conexão com o banco de dados não deixa escapar nenhuma conexão, pois os bloqueios são liberados para as transações abertas que estão inativas por um longo período.
656715	Os dados transmitidos pelo ActiveMQ agora são compactados para melhorar a largura de banda da rede.
662213	O envio de e-mail a vários endereços de destinatários funciona na ação Enviar Eventos por E-mail e na ação Incidente de E-mail.
668443	É possível conectar-se ao banco de dados PostgreSQL por linha de comando, além do pgadmin.
672058	Quando você reinicia uma fonte de eventos configurada para emitir um alerta quando nenhum dado é recebido durante determinado período, a fonte de eventos não gera mais eventos duplicados (NoDataAlert) nem mensagens de registro.
682235	O Sentinel Rapid Deployment agora vem com a versão mais recente do Java 1.6.0_24 para corrigir vulnerabilidades de segurança.

6.2 Aperfeiçoamentos

A tabela a seguir lista os aperfeiçoamentos feitos no Sentinel Rapid Deployment 6.1 SP2 para melhorar sua usabilidade:

Número do bug	Descrição
547390	É possível configurar o limite de consulta offline definindo a propriedade de eventos máximos no arquivo <code>das_core.xml</code> .
642690	A consulta offline foi aprimorada para tornar o tempo de consulta de subintervalo configurável no arquivo <code>das_core.xml</code> .
642691	O status de atualização das informações da consulta offline agora é armazenado no arquivo de registro <code>das_core</code> .
648108	A janela Status do Advisor mostra as informações sobre todos os arquivos de feed.

Número do bug	Descrição
673362	O arquivo de objeto do JasperPrint (isto é, o arquivo inicial de resultados chamado resultados) não aparece mais nos resultados do relatório. Esse arquivo não era usado pelo Sentinel, e sua remoção aprimora o desempenho do relatório e economiza espaço em disco.
680054	No servidor Sentinel Rapid Deployment, foi incluído o suporte aos endereços IP vinculados como um mecanismo de failover.

7 Problemas conhecidos

Número do bug	Descrição
486932	<p>Problema: Um usuário pode apagar uma atividade associada a um processo ativo do iTRAC.</p> <p>Solução temporária: Nenhuma.</p>
517568	<p>Problema: Quando você tenta instalar o Designer de Soluções separadamente, ele não é instalado.</p> <p>Solução: Instale o Designer de Soluções com o Sentinel Control Center ou com o Gerenciador de Dados do Sentinel.</p>
525334	<p>Problema: O Browser de Identidade exibe dados redundantes para o domínio do Active Directory.</p> <p>Solução temporária: Nenhuma.</p>
598473	<p>Problema: Quando a interface de usuário do ESM é iniciada em sistemas com idioma diferente do inglês, o Conector de Arquivos 6r9 não recupera os arquivos remotos usando o protocolo SCP, conforme esperado.</p> <p>Solução temporária: Nenhuma. Isso será corrigido no Conector de Arquivos versão 6r10.</p>
674008	<p>Problema: O ícone e as informações de copyright da Novell não ficam visíveis no Assistente do InstallShield em uma máquina Linux.</p> <p>Solução temporária: Nenhuma.</p>
674720	<p>Problema: As informações do Construtor de Coletor são exibidas no contrato de licença mesmo quando o suporte para a opção do Construtor de Coletor não está incluído no Sentinel 6.1 Rapid Deployment SP2.</p> <p>Solução temporária: Nenhuma.</p>

Número do bug **Descrição**

679830

Problema: No Gerenciador de Coletor para Windows, a funcionalidade de mapeamento pode não funcionar conforme esperado.

Solução: Siga estas etapas:

1. Pare o Gerenciador de Coletor:

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

2. Abra o arquivo de registro do Gerenciador de Coletor `collector_mgr0.0.log` do diretório `<diretório_de_instalação>/log`.

3. Pesquise por um erro semelhante a este:

```
System temporary directory (java.io.tmpdir property) of  
C:\Windows\system32\config\systemprofile\AppData\Local\Temp\  
appears to be invalid (O diretório temporário do sistema (java.io.tmpdir  
property) de C:\Windows\system32\config\systemprofile\AppData\Local\Temp\  
parece ser inválido.)
```

4. Crie uma pasta chamada `Temp` no seguinte local:

Sistemas Windows de 64 bits:

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

Sistemas Windows de 32 bits:

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

5. Reinicie o Gerenciador de Coletor:

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

680054

Problema: O servidor Sentinel Rapid Deployment não consegue determinar automaticamente o endereço IP.

Solução: Siga estas etapas:

1. Crie um arquivo `start_tomcat.properties` no diretório `<diretório_de_instalação>/sentinel_rd/config`.

Verifique se o usuário que executa o servidor Sentinel Rapid Deployment tem a propriedade desse arquivo e as permissões de execução.

2. Especifique o endereço IP no arquivo recém-criado adicionando a seguinte linha:

```
SERVER_IP=<valor_do_endereço_IP>
```

3. Grave o arquivo.

4. Efetue login como o usuário que tem a propriedade dos arquivos de instalação do Sentinel e reinicie o servidor usando o seguinte comando:

```
sentinel.sh restart
```

5. Verifique o endereço IP no local a seguir para confirmar se o endereço IP substituído foi usado:

```
jnlp files under %ESEC_HOME/3rdparty/tomcat/webapps/ROOT/  
novellsiemdownloads
```

680154

Problema: A guia *Tablespace* no Gerenciador de Dados do Sentinel mostra os espaços livre e usado incorretos. Os espaços livre e usado são calculados com base no *tablespace sendata1*, e não no espaço em disco real.

Solução temporária: Nenhuma.

Número do bug	Descrição
685187	<p>Problema: Quando você tenta instalar o Gerenciador de Coletor remoto por meio do modo de console, há uma falha na instalação ao importar o certificado do controlador do servidor.</p> <p>Solução: É possível instalar o Gerenciador de Coletor no modo de console em um sistema remoto usando <code>ssh</code> no modo gráfico para conectar-se ao sistema. Por exemplo, <code>ssh -x <IP_do_sistema></code>.</p>

8 Documentação

A documentação e as notas de versão atualizadas estão disponíveis no [site da documentação do Sentinel Rapid Deployment](http://www.novell.com/documentation/sentinel61rd/index.html) (<http://www.novell.com/documentation/sentinel61rd/index.html>).

9 Informações legais

A Novell, Inc. não faz representações ou garantias com relação ao conteúdo ou uso desta documentação e, particularmente, não se responsabiliza por quaisquer garantias expressas ou implícitas de comerciabilidade ou adequação a qualquer finalidade específica. Além disso, a Novell, Inc. reserva-se o direito de revisar esta publicação e fazer mudanças em seu conteúdo, a qualquer momento, sem a obrigação de notificar qualquer pessoa ou entidade de tais revisões ou mudanças.

Ainda, a Novell, Inc. não faz declarações nem garantias com relação a qualquer software e, particularmente, não se responsabiliza por quaisquer garantias expressas ou implícitas de adequação comercial ou adequação a qualquer finalidade específica. Por fim, a Novell, Inc. reserva-se o direito de fazer mudanças em qualquer uma ou todas as partes do software da Novell, a qualquer momento, sem a obrigação de notificar qualquer pessoa ou entidade de tais mudanças.

Quaisquer informações técnicas ou sobre produtos fornecidas segundo os termos do presente Contrato estão sujeitas aos controles de exportação dos EUA e às leis comerciais de outros países. Você concorda em cumprir todos os regulamentos do controle de exportação e em obter as licenças ou a classificação necessárias para exportar, reexportar ou importar produtos finais. Você concorda em não exportar ou reexportar para entidades nas listas de exclusão de exportação dos Estados Unidos atuais ou para países terroristas ou com embargo conforme especificado nas leis de exportação dos Estados Unidos. Você concorda em não usar produtos para fins proibidos relacionados a armas nucleares, biológicas e químicas ou mísseis. Consulte a página da Web [Novell International Trade Services](http://www.novell.com/info/exports/) (<http://www.novell.com/info/exports/>) para obter mais informações sobre a exportação de software da Novell. A Novell não se responsabiliza pela falha na aquisição de quaisquer aprovações necessárias para exportação.

Copyright © 2011 Novell, Inc. Todos os direitos reservados. Nenhuma parte desta publicação poderá ser reproduzida, fotocopiada, armazenada em um sistema de recuperação ou transmitida sem o consentimento expresso por escrito do editor.

Para as marcas registradas da Novel, consulte [a lista de marcas registradas e marcas de serviço da Novell](http://www.novell.com/company/legal/trademarks/tmlist.html) (<http://www.novell.com/company/legal/trademarks/tmlist.html>).

Todas as marcas registradas de terceiros pertencem aos seus respectivos proprietários.