Guia de Instalação

Novell®
Sentinel 6.1 Rapid Deployment

SP2

Abril 2011

www.novell.com

Informações legais

A Novell, Inc., não faz nenhuma representação ou garantia com relação ao conteúdo ou uso desta documentação e especificamente se isenta de qualquer garantia expressa ou implícita de comercialização ou adequação a um propósito específico. Além disso, a Novel, Inc., se reserva o direito de revisar esta publicação e fazer mudanças no conteúdo, a qualquer momento, sem obrigação de notificar nenhum pessoa ou entidade sobre essas revisões ou mudanças.

A Novell, Inc., não faz nenhuma representação ou garantia com relação a nenhum software e especificamente se isenta de qualquer garantia expressa ou implícita de comercialização ou adequação a um propósito específico. Além disso, a Novell, Inc., se reserva o direito de fazer mudanças em qualquer ou todas as partes do software da Novell, a qualquer momento, sem nenhuma obrigação de notificar nenhuma pessoa ou entidade sobre essas mudanças.

Qualquer produto ou informação técnica fornecida sob este Contrato pode estar sujeita aos controles de exportação dos Estados Unidos e leis de comércio de outros países. Você concorda em atender a todos os regulamentos de controle de exportação e obter qualquer licença ou classificação necessária para exportar, reexportar ou importar produtos. 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. Veja a página da Web Novell International Trade Services (http://www.novell.com/info/exports/) para obter mais informações sobre exportação do software da Novell. A Novell não assume nenhuma responsabilidade por sua falha em obter quaisquer aprovações de exportação necessárias.

Novell, Inc.
404 Wyman Street, Suite 500
Waltham, MA 02451
E.U.A.
www.novell.com

Documentação Online: para acessar a documentação online mais recente deste e de outros produtos da Novell, consulte a página de Documentação da Novell na Web (http://www.novell.com/documentation).

Marcas registradas da Novell

Para ver marcas registradas da Novell, consulte a lista de Marcas Registradas e Marcas de Serviço da Novell (http://www.novell.com/company/legal/trademarks/tmlist.html).

Materiais de terceiros

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

Índice

Sobre este guia 7

1 Visão geral do produto 9

1.1 Visão geral do Sentinel 6.1 Rapid Deployment . . . 9
1.2 Configuração do Sentinel 6.1 Rapid Deployment . . . 11
1.3 Interfaces do usuário do Sentinel Rapid Deployment . . . 12
1.3.1 Interface da Web do Sentinel 6.1 Rapid Deployment . . . 13
1.3.2 Sentinel Control Center . . . 13
1.3.3 Gerenciador de Dados do Sentinel . . . 13
1.3.4 Designer de Soluções do Sentinel . . . 14
1.3.5 Sentinel Plug-in SDK . . . 14
1.4 Componentes do Sentinel Server . . . 14
1.4.1 Serviço de Acesso a Dados . . . 14
1.4.2 Barramento de mensagem . . . 15
1.4.3 Banco de Dados do Sentinel . . . 15
1.4.4 Gerenciador de Coletor do Sentinel . . . 15
1.4.5 Mecanismo de Correlação . . . 15
1.4.6 iTRAC . . . 15
1.4.7 Sentinel Advisor e Detecção de Exploração . . . 16
1.4.8 Servidor Web . . . 16
1.5 Plug-Ins do Sentinel . . . 16
1.5.1 Coletores . . . 16
1.5.2 Conectores e integradores . . . 17
1.5.3 Ações e regras de correlação . . . 17
1.5.4 Relatórios . . . 17
1.5.5 Workflows do iTRAC . . . 17
1.5.6 Pacotes de soluções . . . 18
1.6 Suporte de idiomas . . . 18

2 Requisitos do sistema 19

2.1 Plataformas Suportadas . . . 19
2.1.1 Sistemas operacionais suportados . . . 19
2.2 Requisitos de hardware . . . 20
2.3 Browsers da Web suportados . . . 23
2.4 Ambiente virtual . . . 23
2.5 Limites recomendados . . . 23
2.5.1 Limites do Gerenciador de Coletor . . . 23
2.5.2 Limites de relatórios . . . 24
2.6 Resultados do teste . . . 24

3 Instalação 27

3.1 Visão geral . . . 27
3.1.1 Componentes do servidor . . . 27
3.1.2 Aplicativos clientes . . . 28
3.2 Instalação no SUSE Linux Enterprise Server . . . 29
3.2.1 Pré-requisitos . . . 29
3.2.2 Instalando o Sentinel Rapid Deployment . . . 30

3.3 Instalando o Gerenciador de Coletor e os aplicativos clientes . . . 35
3.3.1 Fazendo download dos instaladores . . . 35
3.3.2 Números de portas para os componentes clientes do Sentinel Rapid Deployment . 36
3.3.3 Instalando os aplicativos clientes do Sentinel . . . 36
3.3.4 Instalando o Gerenciador de Coletor do Sentinel no SLES ou Windows . . . 38
3.4 Iniciando e interrompendo manualmente os serviços do Sentinel . . . 41
3.5 Upgrade manual do Java . . . 41
3.6 Configuração de pós-instalação . . . 42
3.6.1 Mudando as configurações de data e hora . . . 42
3.6.2 Configurando um integrador SMTP para enviar notificações do Sentinel . . . 42
3.6.3 Serviços do Gerenciador de Coletor . . . 43
3.6.4 Gerenciando o tempo . . . 44
3.7 Autenticação LDAP . . . 44
3.7.1 Visão geral . . . 44
3.7.2 Pré-requisitos . . . 45
3.7.3 Configurando o Sentinel Server para autenticação LDAP . . . 46
3.7.4 Configurando vários servidores LDAP para failover . . . 48
3.7.5 Configurando a autenticação LDAP para vários domínios do Active Directory . . . 50
3.7.6 Efetuando login com as credenciais de usuário LDAP . . . 51
3.8 Atualizando a classificação da chave de licença de chave de avaliação para chave de produção . . . 52

4 Fazendo upgrade do Sentinel Rapid Deployment 53

4.1 Pré-requisitos . . . 53
4.2 Instalando o patch no servidor . . . 53
4.3 Fazendo upgrade do Gerenciador de Coletor e dos aplicativos clientes . . . 54
4.3.1 Fazendo upgrade do Gerenciador de Coletor . . . 54
4.3.2 Fazendo upgrade dos aplicativos clientes . . . 55

5 Considerações de segurança do Sentinel Rapid Deployment 57

5.1 Proteção . . . 57
5.1.1 Proteção out-of-the-box . . . 57
5.1.2 Protegendo os dados do Sentinel Rapid Deployment . . . 58
5.2 Protegendo a comunicação na rede . . . 58
5.2.1 Comunicação entre processos do Sentinel Server . . . 58
5.2.2 Comunicação entre o Sentinel Server e os aplicativos clientes do Sentinel . . . 58
5.2.3 Comunicação entre o servidor e o banco de dados . . . 59
5.2.4 Comunicação entre os Gerenciadores de Coletor e as fontes de eventos . . . 60
5.2.5 Comunicação com os browsers da Web . . . 60
5.2.6 Comunicação entre o banco de dados e outros clientes . . . 60
5.3 Protegendo usuários e senhas . . . 60
5.3.1 Usuários do sistema operacional . . . 60
5.3.2 Usuários de bancos de dados e aplicativos do Sentinel . . . 61
5.3.3 Assegurando o uso obrigatório da política de senha pelos usuários . . . 62
5.4 Protegendo dados do Sentinel . . . 63
5.5 Fazendo backup de informações . . . 66
5.6 Protegendo o sistema operacional . . . 66
5.7 Vendo os eventos de auditoria do Sentinel . . . 67
5.8 Usando um certificado CA . . . 67

6 Testando as funcionalidades do Sentinel Rapid Deployment 69

6.1 Testando a instalação do Rapid Deployment . . . 69

6.2 Limpando após o teste 81
6.3 Usando dados reais 82

7 Desinstalando o Sentinel Rapid Deployment 83

7.1 Desinstalando o Sentinel Rapid Deployment Server 83
7.2 Desinstalando o Gerenciador de Coletor Remoto e os Aplicativos Clientes do Sentinel. 83
7.2.1 Linux 83
7.2.2 Windows 84
7.2.3 Procedimentos de pós-desinstalação 84

A Atualizando o nome de host do Sentinel Rapid Deployment 87

A.1 Servidor 87
A.2 Aplicativos clientes 87

B Dicas para solução de problemas 89

B.1 Falha na autenticação do banco de dados ao digitar credenciais inválidas 89
B.2 Falha ao inicializar interface da Web do Sentinel 89
B.3 O Gerenciador de Coletor Remoto gera uma exceção no Windows 2008 quando o UAC está habilitado 90
B.4 O UUID não é criado para Gerenciadores de Coletor com Imagens 91

C Melhores práticas de manutenção do banco de dados PostgreSQL 93

C.1 Modificando os parâmetros de configuração de memória 93
C.2 Reduzindo o impacto de E/S de Vacuum/Analyze 94

Sobre este guia

O objetivo deste guia é apresentar o Novell Sentinel 6.1 Rapid Deployment Service Pack 2 e descrever os procedimentos de instalação.

- Capítulo 1, “Visão geral do produto” na página 9
- Capítulo 2, “Requisitos do sistema” na página 19
- Capítulo 3, “Instalação” na página 27
- Capítulo 4, “Fazendo upgrade do Sentinel Rapid Deployment” na página 53
- Capítulo 5, “Considerações de segurança do Sentinel Rapid Deployment” na página 57
- Capítulo 6, “Testando as funcionalidades do Sentinel Rapid Deployment” na página 69
- Capítulo 7, “Desinstalando o Sentinel Rapid Deployment” na página 83
- Apêndice A, “Atualizando o nome de host do Sentinel Rapid Deployment” na página 87
- Apêndice B, “Dicas para solução de problemas” na página 89
- Apêndice C, “Melhores práticas de manutenção do banco de dados PostgreSQL” na página 93

Público

Essa documentação é destinada aos profissionais de segurança da informação.

Comentários

Gostaríamos de receber seus comentários e suas sugestões sobre este manual e sobre as outras documentações incluídas no produto. Use a função Comentários do Usuário, situada na parte inferior de cada página da documentação online e digite seus comentários.

Documentação adicional

A documentação técnica do Sentinel está dividida em diversos volumes. São eles:

- *Novell Sentinel Rapid Deployment Installation Guide* (http://www.novell.com/documentation/sentinel61rd/s61rd_install/data/index.html) (Guia de Instalação do Novell Sentinel 6.1 Rapid Deployment)
- *Novell Sentinel Rapid Deployment User Guide* (http://www.novell.com/documentation/sentinel61rd/s61rd_user/data/bookinfo.html) (Guia do Usuário do Novell Sentinel 6.1 Rapid Deployment)
- *Novell Sentinel Rapid Deployment Reference Guide* (http://www.novell.com/documentation/sentinel61rd/s61rd_reference/data/bookinfo.html) (Guia de Referência do Novell Sentinel 6.1 Rapid Deployment)
- *Guia de Instalação do Novell Sentinel* (http://www.novell.com/documentation/sentinel61/s61_install/?page=/documentation/sentinel61/s61_install/data/)
- *Novell Sentinel User Guide* (http://www.novell.com/documentation/sentinel61/s61_user/?page=/documentation/sentinel61/s61_user/data/) (Guia do Usuário do Novell Sentinel)

- *Novell Sentinel Reference Guide* (http://www.novell.com/documentation/sentinel61/s61_reference/?page=/documentation/sentinel61/s61_reference/data/) (Guia de Referência do Novell Sentinel)
- *Sentinel SDK* (http://www.novell.com/developer/develop_to_sentinel.html)

  O site do Sentinel SDK contém detalhes sobre desenvolvimento de Coletores (proprietários ou JavaScript) e ações de correlação do JavaScript.

Contatando a Novell

- *Site da Novell* (http://www.novell.com)
- *Suporte Técnico da Novell* (http://support.novell.com/phone.html?sourceidint=suplnav4_phonesup)
- *Auto-suporte da Novell* (http://support.novell.com/support_options.html?sourceidint=suplnav_supportprog)
- *Site de download de patches* (http://download.novell.com/index.jsp)
- *Suporte 24 horas da Novell* (http://www.novell.com/company/contact.html)
- *TIDS do Sentinel* (http://support.novell.com/products/sentinel)
- Fóruns de suporte da comunidade do Sentinel (http://forums.novell.com/novell-product-support-forums/sentinel/)
- Site de plug-ins do Sentinel (http://support.novell.com/products/sentinel/secure/sentinelplugins.html)
- Lista de E-mails de Notificação: Cadastre-se pelo site de plug-ins do Sentinel

Visão geral do produto

1

O Sentinel 6.1 Rapid Deployment é uma versão simplificada do Novell Sentinel que aproveita os componentes de código-fonte aberto PostgreSQL, activeMQ e JasperReports.

As seções a seguir ajudarão você a conhecer os principais componentes do sistema Sentinel 6.1 Rapid Deployment. Este *Guia de Instalação do Sentinel Rapid Deployment* contém informações detalhadas sobre os procedimentos de instalação e configuração. O *Sentinel Rapid Deployment User Guide* (http://www.novell.com/documentation/sentinel61rd/s61rd_user/?page=/documentation/sentinel61rd/s61rd_user/data/bookinfo.html) (Guia do Usuário do Sentinel Rapid Deployment) inclui os procedimentos detalhados de arquitetura, operação e administração.

- Seção 1.1, “Visão geral do Sentinel 6.1 Rapid Deployment” na página 9
- Seção 1.2, “Configuração do Sentinel 6.1 Rapid Deployment” na página 11
- Seção 1.3, “Interfaces do usuário do Sentinel Rapid Deployment” na página 12
- Seção 1.4, “Componentes do Sentinel Server” na página 14
- Seção 1.5, “Plug-Ins do Sentinel” na página 16
- Seção 1.6, “Suporte de idiomas” na página 18

1.1 Visão geral do Sentinel 6.1 Rapid Deployment

O Sentinel é uma solução de gerenciamento de eventos e informações de segurança que recebe dados de muitas fontes em toda a empresa e, em seguida, padroniza, prioriza e apresenta esses dados para que você tome decisões relacionadas a ameaças, riscos e políticas.

O Sentinel automatiza os processos de geração de relatórios, análise e coleta de registros para garantir que os controles de TI sejam eficazes no suporte à detecção de ameaças e aos requisitos de auditoria. O Sentinel substitui processos manuais muito trabalhosos por monitoração contínua e automatizada de eventos de conformidade e segurança e de controles de TI.

O Sentinel coleta e correlaciona informações de segurança e outros tipos de informação da infraestrutura em rede da organização, bem como de sistemas, dispositivos e aplicativos de terceiros. O Sentinel apresenta os dados coletados em uma interface gráfica do usuário, identifica problemas de conformidade ou segurança e monitora atividades de correção para aperfeiçoar processos sujeitos a erros e construir um programa de gerenciamento rigoroso e seguro.

O gerenciamento de respostas a incidentes automatizado permite que você documente e formalize o processo de monitoramento, encaminhamento e resposta a incidentes e violações de política, e fornece uma integração bidirecional com sistemas de comunicação de problemas. O Sentinel permite que você reaja prontamente e resolva incidentes de forma eficiente.

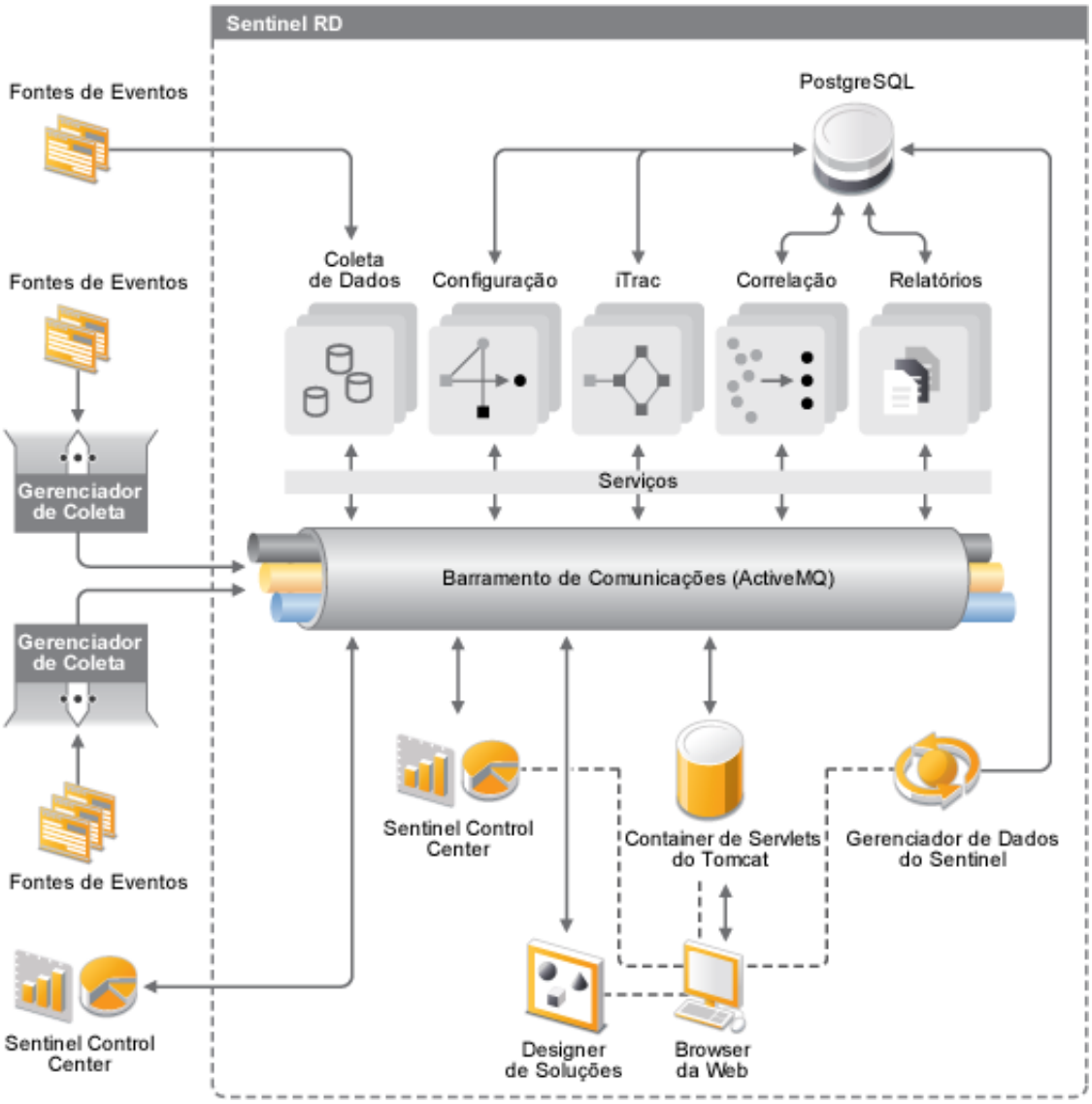
Os Pacotes de Soluções são uma maneira simples de distribuir e importar para controles regras de correlação, listas dinâmicas, mapas, relatórios e workflows do iTRAC no Sentinel. Esses controles podem ser criados para atender a requisitos regulatórios específicos, como o Payment Card Industry Data Security Standard, ou podem ser relacionados a determinada fonte de dados, como os eventos de autenticação do usuário de um banco de dados.

Com o Sentinel Rapid Deployment, você tem:

- Gerenciamento de segurança em tempo real automatizado e integrado e monitoramento de conformidade entre todos os sistemas e redes.
- Uma estrutura que permite que as políticas comerciais conduzam suas ações e sua política de TI.
- Geração automática de documentos e relatórios de segurança, sistemas e eventos de acesso em toda a empresa.
- Gerenciamento de incidentes e reparação incorporados.
- Capacidade de demonstrar e monitorar a conformidade com políticas internas e normas governamentais, como Sarbanes-Oxley, HIPAA, GLBA e FISMA. O conteúdo necessário para a implementação desses controles é distribuído e implementado por meio dos Pacotes de Soluções.

Veja a seguir uma arquitetura conceitual do Sentinel Rapid Deployment, que ilustra os componentes envolvidos na execução do gerenciamento de segurança e conformidade.

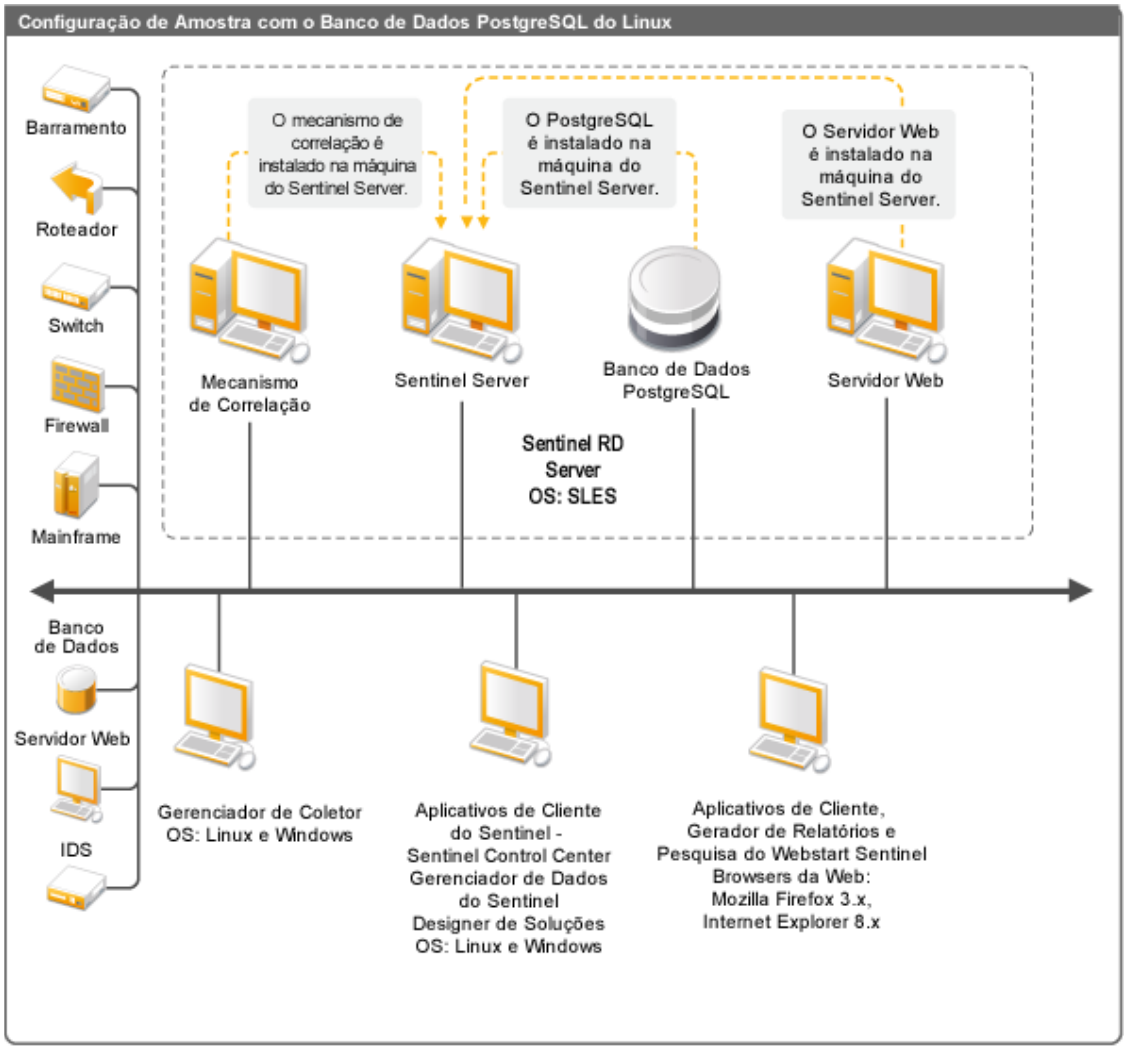
Figura 1-1 *Arquitetura conceitual do Sentinel*



1.2 Configuração do Sentinel 6.1 Rapid Deployment

A ilustração a seguir mostra a configuração do Sentinel 6.1 Rapid Deployment.

Figura 1-2 *Configuração do Sentinel 6.1 Rapid Deployment*



1.3 Interfaces do usuário do Sentinel Rapid Deployment

As interfaces do usuário do Sentinel, muito fáceis de usar, estão relacionadas a seguir:

- Interface da Web do Sentinel 6.1 Rapid Deployment
- Sentinel Control Center
- Gerenciador de Dados do Sentinel
- Designer de Soluções do Sentinel
- Sentinel Plug-in SDK

1.3.1 Interface da Web do Sentinel 6.1 Rapid Deployment

Na interface da Web do Novell Sentinel 6.1 Rapid Deployment, você pode gerenciar relatórios e iniciar o Sentinel Control Center (SCC), o Gerenciador de Dados do Sentinel e o Designer de Soluções. Além disso, você pode fazer download do instalador do Gerenciador de Coletor e do Cliente na página *Aplicativos* da interface da Web do Sentinel 6.1 Rapid Deployment.

Para obter mais informações, consulte "Managing Sentinel Rapid Deployment Through the Web Interface" (Gerenciando o Sentinel Rapid Deployment pela interface da Web) no *Sentinel Rapid Deployment User Guide* (Guia do Usuário do Sentinel Rapid Deployment).

1.3.2 Sentinel Control Center

O SCC dispõe de um painel de gerenciamento de segurança integrado que permite aos analistas identificar rapidamente novas tendências ou ataques, manipular e interagir com informações gráficas em tempo real e responder a incidentes.

Você pode iniciar o SCC como um aplicativo cliente ou usando o Java Webstart.

Os principais recursos do SCC incluem:

- **Telas Ativas:** Proporcionam análise e visualização em tempo real
- **Análise:** Executa e grava consultas offline
- **Incidentes:** Oferecem criação e gerenciamento de incidentes
- **Correlação:** Proporciona definição e gerenciamento de regras de correlação
- **iTRAC:** Fornece gerenciamento de processos para a documentação, a imposição e o monitoramento dos processos de resolução de incidentes
- **Gerador de Relatórios:** Dispõe de métricas e relatórios de histórico
- **Gerenciamento de Fonte de Eventos:** Proporciona a implantação e o monitoramento do coletor
- **Gerenciador de Soluções:** Instala, implementa e faz o teste do conteúdo do Pacote de Soluções

Para obter mais informações, consulte "Sentinel Control Center" no *Sentinel Rapid Deployment User Guide* (Guia do Usuário do Sentinel Rapid Deployment).

1.3.3 Gerenciador de Dados do Sentinel

O Gerenciador de Dados do Sentinel permite gerenciar o banco de dados do Sentinel. É possível realizar as seguintes operações no Gerenciador de Dados do Sentinel:

- Monitorar a utilização de espaço do banco de dados.
- Ver e gerenciar as partições de banco de dados.
- Gerenciar arquivos de bancos de dados.
- Importar dados arquivados de volta para o banco de dados.

Para obter mais informações, consulte "Sentinel Data Manager" (Gerenciador de Dados do Sentinel) no *Sentinel Rapid Deployment User Guide* (Guia do Usuário do Sentinel Rapid Deployment).

1.3.4 Designer de Soluções do Sentinel

O Sentinel Solution Designer é usado para criar e modificar Pacotes de Soluções, que são conjuntos agrupados de conteúdo do Sentinel, como regras de correlação, ações, workflows do iTRAC e relatórios.

O conteúdo do Sentinel é a funcionalidade estendida do sistema Sentinel. Esse conteúdo inclui Ações do Sentinel, Integradores e plug-ins do Sentinel, como Coletores, Conectores e Pacotes de Soluções, que podem incluir vários outros tipos de plug-ins. Esses componentes modulares são usados para integração com sistemas de terceiros, instalação de uma solução completa de segurança baseada em controle e correção automatizada de incidentes detectados.

Para obter mais informações, consulte "Solution Packs " (Pacotes de soluções) no *Sentinel Rapid Deployment User Guide* (Guia do Usuário do Sentinel Rapid Deployment).

1.3.5 Sentinel Plug-in SDK

O Sentinel Plug-in SDK contém bibliotecas e códigos desenvolvidos pelo Novell Engineering, bem como o gabarito e o código de exemplo que você pode usar para desenvolver seus próprios projetos. Para obter mais informações, consulte o Sentinel SDK (http://www.novell.com/developer/develop_to_sentinel.html).

1.4 Componentes do Sentinel Server

O Sentinel é formado pelos seguintes componentes:

- Seção 1.4.1, "Serviço de Acesso a Dados" na página 14
- Seção 1.4.2, "Barramento de mensagem" na página 15
- Seção 1.4.3, "Banco de Dados do Sentinel" na página 15
- Seção 1.4.4, "Gerenciador de Coletor do Sentinel" na página 15
- Seção 1.4.5, "Mecanismo de Correlação" na página 15
- Seção 1.4.6, "iTRAC" na página 15
- Seção 1.4.7, "Sentinel Advisor e Detecção de Exploração" na página 16
- Seção 1.4.8, "Servidor Web" na página 16

1.4.1 Serviço de Acesso a Dados

O Serviço de Acesso a Dados do Sentinel é o principal componente usado na comunicação com o banco de dados do Sentinel. O Serviço de Acesso a Dados e outros componentes do servidor trabalham juntos para armazenar eventos recebidos dos Gerenciadores de Coletor no banco de dados, filtrar dados, processar telas do Active View, executar consultas de bancos de dados e processar resultados, e também gerenciar tarefas administrativas, como autorização e autenticação do usuário. Para obter mais informações, consulte "Data Access Service" (Serviço de Acesso a Dados) no *Sentinel Rapid Deployment Reference Guide* (Guia de Referência do Sentinel Rapid Deployment).

1.4.2 Barramento de mensagem

O Sentinel 6.1 Rapid Deployment usa o mediador de mensagens de código-fonte aberto chamado Apache Active MQ. O barramento de mensagem pode mover milhares de pacotes de mensagens em um segundo entre os componentes do Sentinel. A arquitetura do Apache Active MQ foi desenvolvida com base no Java Message Oriented Middleware (JMOM), que suporta chamadas assíncronas entre os aplicativos cliente e servidor. As filas de mensagens fornecem armazenamento temporário quando o programa de destino está ocupado ou não está conectado. Para obter mais informações, consulte "Communication Server" (Servidor de comunicação) no *Sentinel Rapid Deployment User Guide* (Guia do Usuário do Sentinel Rapid Deployment)

1.4.3 Banco de Dados do Sentinel

O Sentinel tem como base um banco de dados de back end que armazena eventos de segurança e todos os metadados do Sentinel. O Sentinel 6.1 Rapid Deployment suporta PostgreSQL. Os eventos são armazenados em um formato regularizado juntamente com dados de vulnerabilidade e de ativos, informações de identidade, status de incidente e de workflow e muitos outros tipos de dados. Para obter mais informações, consulte "Sentinel Data Manager" (Gerenciador de Dados do Sentinel) no *Sentinel Rapid Deployment User Guide* (Guia do Usuário do Sentinel Rapid Deployment).

1.4.4 Gerenciador de Coletor do Sentinel

O Gerenciador de Coletor do Sentinel gerencia coletas de dados, monitora mensagens de status do sistema e filtra eventos, conforme necessário. As principais funções do Gerenciador de Coletor incluem transformar eventos, adicionar relevância comercial aos eventos por meio de taxonomia, executar filtragem global nos eventos, rotear eventos e enviar mensagens sobre saúde ao Sentinel Server. O Gerenciador de Coletor do Sentinel conecta-se diretamente ao barramento de mensagem. Para obter mais informações, consulte "Collector Manager" (Gerenciador de Coletor) no *Sentinel Rapid Deployment User Guide* (Guia do Usuário do Sentinel Rapid Deployment).

1.4.5 Mecanismo de Correlação

O Mecanismo de Correlação agrega inteligência ao gerenciamento de eventos de segurança automatizando a análise do fluxo de eventos de entrada para localizar padrões de interesse. A correlação permite definir regras que identificam as ameaças importantes e padrões complexos de ataque, para que você consiga priorizar os eventos e iniciar o gerenciamento e a resposta eficazes aos incidentes. Para obter mais informações, consulte "Correlation Tab" (Guia Correlação) no *Sentinel Rapid Deployment User Guide* (Guia do Usuário do Sentinel Rapid Deployment).

1.4.6 iTRAC

O Sentinel fornece um sistema de gerenciamento de workflow do iTRAC para que você possa definir e automatizar processos de respostas a incidentes. Incidentes identificados no Sentinel, seja por uma regra de correlação ou manualmente, podem ser associados a um workflow do iTRAC. Para obter mais informações, consulte "iTRAC Workflows" (Workflows do iTRAC) no *Sentinel Rapid Deployment User Guide* (Guia do Usuário do Sentinel Rapid Deployment).

1.4.7 Sentinel Advisor e Detecção de Exploração

O Sentinel Advisor é um serviço opcional de inscrição de dados que inclui informações sobre ataques conhecidos, vulnerabilidades e correções. Esses dados, combinados com informações sobre vulnerabilidades conhecidas e sobre prevenção ou detecção de intrusão em tempo real no ambiente, fornecem uma detecção de exploração proativa e a capacidade de agir imediatamente quando um ataque ocorre em um sistema vulnerável.

Um instantâneo de dados do Advisor é instalado por padrão durante a instalação do Sentinel 6.1 Rapid Deployment. Você precisa de uma licença do Advisor para assinar as atualizações contínuas de dados do Advisor. Para obter mais informações, consulte "Advisor Usage and Maintenance" (Uso e manutenção do Advisor) no *Sentinel Rapid Deployment User Guide* (Guia do Usuário do Sentinel Rapid Deployment).

1.4.8 Servidor Web

O Sentinel Rapid Deployment usa o Apache Tomcat como seu servidor Web para conectar-se com segurança à interface da Web do Sentinel Rapid Deployment.

1.5 Plug-Ins do Sentinel

O Sentinel suporta vários plug-ins, o que permite expandir e aprimorar a funcionalidade do sistema. Alguns desses plug-ins estão pré-instalados. Plug-ins (e atualizações) adicionais estão disponíveis para download no site de plug-ins do Sentinel 6.1 (http://support.novell.com/products/sentinel/secure/sentinelplugins.html).

Alguns plug-ins, como o Remedy Integrator, o IBM Mainframe Connector e o Connector for SAP XAL, requerem uma licença adicional para download.

- Seção 1.5.1, "Coletores" na página 16
- Seção 1.5.2, "Conectores e integradores" na página 17
- Seção 1.5.3, "Ações e regras de correlação" na página 17
- Seção 1.5.4, "Relatórios" na página 17
- Seção 1.5.5, "Workflows do iTRAC" na página 17
- Seção 1.5.6, "Pacotes de soluções" na página 18

1.5.1 Coletores

O Sentinel coleta dados em dispositivos de origem e distribui um fluxo de eventos enriquecido aplicando taxonomia, detecção de exploração e relevância comercial ao fluxo de dados antes que os eventos sejam correlacionados, analisados e enviados para o banco de dados. Um fluxo de eventos enriquecido significa que os dados estão correlacionados ao contexto comercial necessário para identificar e resolver ameaças internas ou externas e violações às políticas.

Os Coletores do Sentinel podem analisar dados dos seguintes tipos de dispositivos e de muitos outros:

◆ Sistemas de detecção de intrusão (host)	◆ Sistemas de detecção antivírus
◆ Sistemas de detecção de intrusão (rede)	◆ Servidores da Web
◆ Firewalls	◆ Bancos de Dados
◆ Sistemas Operacionais	◆ Mainframe
◆ Monitoramento de políticas	◆ Sistemas de avaliação de vulnerabilidade
◆ Autenticação	◆ NDS
◆ Roteadores e switches	◆ Sistemas de gerenciamento de redes
◆ VPNs	◆ Sistemas proprietários

Os Coletores JavaScript podem ser gravados com as ferramentas de desenvolvimento padrão do JavaScript e com o SDK do Coletor.

1.5.2 Conectores e integradores

Os conectores fornecem conectividade entre o Gerenciador de Coletor e as fontes de eventos por meio de protocolos padrão, como JDBC e Syslog. Os eventos são passados do Conector ao Coletor para análise.

Os integradores permitem a execução de ações de correção em sistemas situados fora do Sentinel. Por exemplo, uma ação de correlação pode usar o Integrador SOAP para iniciar um workflow do Novell Identity Manager.

O Remedy AR Integrator opcional permite criar um ticket de correção a partir de incidentes ou eventos do Sentinel. Para obter mais informações, consulte "Action Manager and Integrator" (Gerenciador de ações e integrador) no *Sentinel Rapid Deployment User Guide* (Guia do Usuário do Sentinel Rapid Deployment).

1.5.3 Ações e regras de correlação

As regras de correlação identificam padrões importantes no fluxo de eventos. Quando acionada, a regra de correlação inicia ações de correlação, como o envio de notificações por e-mail, a inicialização de um workflow do iTRAC ou a execução de uma ação por meio de um Integrador. Para obter mais informações, consulte "Correlation Tab" (Guia Correlação) no *Sentinel Rapid Deployment User Guide* (Guia do Usuário do Sentinel Rapid Deployment).

1.5.4 Relatórios

Você pode executar uma grande variedade de relatórios operacionais e de painéis na interface da Web do Sentinel Rapid Deployment usando JasperReports. Geralmente, os relatórios são distribuídos por meio de Pacotes de Soluções.

1.5.5 Workflows do iTRAC

Os workflows do iTRAC fornecem processos consistentes e reutilizáveis para o gerenciamento de incidentes. Geralmente, os gabaritos de workflow são distribuídos por meio de Pacotes de Soluções. O iTRAC vem com um conjunto de gabaritos padrão que você pode modificar para atender aos seus requisitos. Para obter mais informações, consulte "iTRAC Workflows" (Workflows do iTRAC) no *Sentinel Rapid Deployment User Guide* (Guia do Usuário do Sentinel Rapid Deployment).

1.5.6 Pacotes de soluções

Os Pacotes de Soluções são conjuntos agrupados de conteúdo relacionado do Sentinel, como regras de correlação, ações, workflows do iTRAC e relatórios. A Novell fornece Pacotes de Soluções destinados a necessidades comerciais específicas, como o Pacote de Soluções PCI-DSS, que aborda a conformidade com o Payment Card Industry Data Security Standard. Além disso, a Novell cria pacotes de Coletor, que incluem conteúdo voltado a uma fonte de eventos específica, como o Windows Active Directory. Para obter mais informações, consulte "Solution Packs " (Pacotes de soluções) no *Sentinel Rapid Deployment User Guide* (Guia do Usuário do Sentinel Rapid Deployment).

1.6 Suporte de idiomas

Os componentes do Sentinel estão disponíveis nos seguintes idiomas:

- Tcheco
- Inglês
- Francês
- Alemão
- Italiano
- Japonês
- Holandês
- Polonês
- Português
- Chinês Simplificado
- Espanhol
- Chinês Tradicional

Requisitos do sistema

2

Para melhor desempenho e confiabilidade, instale os componentes do Sentinel Rapid Deployment em software e hardware aprovados, conforme listado nesta seção. Os requisitos mencionados nesta seção tiveram sua qualidade totalmente assegurada e certificada.

- Seção 2.1, “Plataformas Suportadas” na página 19
- Seção 2.2, “Requisitos de hardware” na página 20
- Seção 2.3, “Browsers da Web suportados” na página 23
- Seção 2.4, “Ambiente virtual” na página 23
- Seção 2.5, “Limites recomendados” na página 23
- Seção 2.6, “Resultados do teste” na página 24

2.1 Plataformas Suportadas

A Tabela 2-1 lista as combinações de software e sistema operacional certificadas ou suportadas pela Novell. As combinações certificadas foram testadas com a suíte completa de teste do Novell Engineering. As combinações suportadas devem ser totalmente funcionais.

2.1.1 Sistemas operacionais suportados

A Novell suporta a execução do Sentinel Rapid Deployment nas versões de sistema operacional descritas nesta seção. A Novell também suporta a execução em sistemas com atualizações secundárias nesses sistemas operacionais, como patches de segurança ou hotfixes. No entanto, a execução do Sentinel Rapid Deployment em sistemas com atualizações importantes ou secundárias nessas plataformas não é suportada enquanto a Novell não tiver testado e certificado essas atualizações.

Os componentes do servidor Sentinel Rapid Deployment incluem Servidor de Comunicação, Mecanismo de Correlação, Serviço de Acesso a Dados (DAS), servidor Web e serviço de inscrição de dados do Advisor.

Os aplicativos clientes do Sentinel incluem Sentinel Control Center (SCC), Gerenciador de Dados do Sentinel (SDM) e Sentinel Solution Designer (SSD).

O Gerenciador de Coletor tem requisitos de plataforma específicos.

Tabela 2-1 *Sistemas Operacionais Suportados e Certificados*

Plataformas	Componentes do servidor	Aplicativos clientes do Sentinel	Gerenciador de Coletor
SUSE Linux Enterprise Server (SLES) 11 SP1 (64 bits)	Certificado	Certificado	Certificado
SUSE Linux Enterprise Server (SLES) 11 SP1 (32 bits)	Não suportado	Suportado	Suportado

Plataformas	Componentes do servidor	Aplicativos clientes do Sentinel	Gerenciador de Coletor
SUSE Linux Enterprise Server (SLES) 10 SP3 (64 bits)	Certificado	Suportado	Suportado
SUSE Linux Enterprise Server (SLES) 10 SP3 (32 bits)	Suportado	Suportado	Suportado
Windows Server 2008 R2 (64 bits)	Não suportado	Certificado	Certificado
Windows Server 2003 R2 (64 bits)	Não suportado	Suportado	Suportado
Windows Server 2003 R2 (32 bits)	Não suportado	Suportado	Suportado
Windows XP SP3 (32 bits)	Não suportado	Suportado	Não suportado
Windows Vista SP2 (32 bits)	Não suportado	Suportado	Não suportado
Windows 7	Não suportado	Certificado	Não suportado

Siga estas diretrizes para atingir o desempenho, a estabilidade e a confiabilidade ideais:

- Para o SLES, o sistema operacional para a máquina do servidor Sentinel Rapid Deployment deve incluir no mínimo os componentes do Servidor Base e do X Window do SLES.
- Para o servidor Sentinel Rapid Deployment, use o sistema de arquivos ext3. Para obter mais informações sobre sistemas de arquivos, consulte Overview of File Systems in Linux (http://www.novell.com/documentation/sles11/stor_admin/data/filesystems.html) (Visão geral dos sistemas de arquivos no Linux) no *Storage Administration Guide* (Guia de Administração de Armazenamento).

Observação:

- O Sentinel Rapid Deployment não é suportado nas instalações do Open Enterprise Server no SLES.
- A versão de demonstração de 32 bits do servidor Sentinel 6.1 Rapid Deployment foi desenvolvida para ambientes de teste e demonstração em escala limitada, usando sistemas operacionais e hardware de 32 bits. Clientes ou parceiros com contrato de suporte do Sentinel 6.1 Rapid Deployment recebem suporte limitado nesta plataforma pelo Suporte Técnico da Novell para problemas que podem ser reproduzidos na plataforma de produção de 64 bits. Por causa das limitações inerentes ao hardware de 32 bits, o Suporte Técnico da Novell não soluciona problemas de desempenho ou escalabilidade da versão demo de 32 bits. As versões demo de 32 bits não têm suporte em um ambiente de produção.

2.2 Requisitos de hardware

Os componentes do servidor Sentinel Rapid Deployment são executados em hardware x86-64 (64 bits), com algumas exceções baseadas no sistema operacional, como descrito na Seção 2.1.1, “Sistemas operacionais suportados” na página 19. O Sentinel é certificado em hardware AMD Opteron e Intel Xeon. Servidores Itanium não são suportados.

Esta seção contém algumas recomendações gerais sobre hardware para design do sistema Sentinel. As recomendações de design são baseadas em faixas de taxas de eventos. No entanto, essas recomendações são baseadas nas seguintes suposições:

- A taxa de eventos está na extremidade alta da faixa de EPS (eventos por segundo).
- A média de tamanho dos eventos é de 1 KB.
- Todos eventos são armazenados no banco de dados (isto é, não há filtros para descartar eventos).
- Um volume de dados equivalente a noventa dias é armazenado online no banco de dados.
- O espaço de armazenamento para os dados do Advisor não está incluído nas especificações da Tabela 2-2 na página 22 nem da Tabela 2-3 na página 22.
- Por padrão, o Sentinel Server possui 5 GB de espaço em disco para armazenar em cache temporariamente os dados de eventos que não podem ser inseridos imediatamente no banco de dados.
- O Sentinel Server também possui por padrão 5 GB de espaço em disco para eventos que não podem ser inseridos imediatamente nos arquivos de eventos de agregação.
- A inscrição opcional do Advisor requer 1 GB de espaço em disco adicional no servidor.

As recomendações de hardware para uma implementação do Sentinel podem variar de acordo com cada implementação; portanto, é recomendável que você consulte o Novell Consulting Services ou qualquer um dos parceiros do Novell Sentinel antes de finalizar a arquitetura do Sentinel. As recomendações abaixo podem ser usadas como diretrizes.

Na versão SLES, o banco de dados está incorporado ao servidor Sentinel Rapid Deployment e é instalado na mesma máquina juntamente com o servidor.

Observação: Devido às altas cargas de eventos e ao cache local, o Sentinel Server precisa ter uma matriz de disco distribuída local ou compartilhada (RAID) com no mínimo 4 eixos de disco.

Tabela 2-2 *Configuração de Máquina Única (até 2000 eps)*

Componentes	RAM	Espaço em disco	CPU
Máquina 1: Sentinel Rapid Deployment Server ◆ Banco de dados PostgreSQL incorporado (3 GB) ◆ Gerenciador de Coletor (1228 MB) ◆ DAS_Core (1579 MB) ◆ DAS_Binary (1404 MB) ◆ Mecanismo de Correlação (1073 MB) ◆ 4 Coletores (Generic, Cisco, Snort e IBM, gerando 500 eps cada) ◆ 10 Regras de Correlação implantadas ◆ 10 Telas Ativas exclusivas ◆ 3 usuários simultâneos ◆ 2 mapas implantados	16 GB	Disco(s) rígido(s) SAS de 1 TB (15K rpm) Hardware RAID 10	Dell PowerEdge 2900,2 x Quad-Core Intel Xeon E5310 (1.6 GHz) com NIC Gigabit Ethernet

Tabela 2-3 *Configuração de Três Máquinas (até 5000 eps)*

Componentes	RAM	Espaço em disco	CPU
Máquina 1: Sentinel Rapid Deployment Server ◆ Banco de dados PostgreSQL incorporado (3 GB) ◆ Gerenciador de Coletor (1228 MB) ◆ DAS_Core (1579 MB) ◆ DAS_Binary (1404 MB) ◆ Mecanismo de Correlação (1073 MB) ◆ 4 Coletores (gerando 500 eps cada, 1500 EPS do Gerenciador de Coletor remoto 1 e 1500 EPS do Gerenciador de Coletor remoto 2.	16 GB	Disco(s) rígido(s) SAS de 1 TB (15K rpm) Hardware RAID 10	Dell PowerEdge 2900,2 x Quad-Core Intel Xeon E5310 (1.6 GHz) com NIC Gigabit Ethernet
Máquina 2: Gerenciador de Coletor ◆ Gerenciador de Coletor/Coletores ◆ 3 Coletores (gerando 500 eps cada)	4 GB	Disco rígido SATA de 300 GB (3 Gbit/s)	Intel Core 2 Duo E6750 (2.66 GHz) com NIC Gigabit Ethernet
Máquina 3: Gerenciador de Coletor ◆ Gerenciador de Coletor/Coletores ◆ 3 Coletores (gerando 500 eps cada)	4 GB	Disco rígido SATA de 300 GB (3 Gbit/s)	Intel Core 2 Duo E6750 (2.66 GHz) com NIC Gigabit Ethernet

2.3 Browsers da Web suportados

- Mozilla Firefox 3.*x*
- Internet Explorer 8.*x*

2.4 Ambiente virtual

O Sentinel Rapid Deployment foi amplamente testado no VMWare ESX Server, e a Novell oferece total suporte ao Sentinel Rapid Deployment nesse ambiente. Para atingir resultados de desempenho comparáveis aos resultados de teste de máquina física no ESX ou em qualquer outro ambiente virtual, o ambiente virtual deve ter as mesmas recomendações de memória, CPU, espaço em disco e E/S que a máquina física.

Para obter informações sobre as recomendações de máquina física para um sistema SLES, consulte a Seção 2.2, “Requisitos de hardware” na página 20

2.5 Limites recomendados

Os limites mencionados nesta seção são recomendações baseadas no teste de desempenho realizado no site da Novell ou do cliente. Eles não são limites de hardware. As recomendações são valores aproximados. Em sistemas altamente dinâmicos, vale a pena criar buffers e deixar espaço para crescimento.

- Seção 2.5.1, “Limites do Gerenciador de Coletor” na página 23
- Seção 2.5.2, “Limites de relatórios” na página 24

2.5.1 Limites do Gerenciador de Coletor

Exceto se especificado de outra forma, os limites do Gerenciador de Coletor levam em conta 4 núcleos de CPU com 2.2 GHz cada, 4 GB de RAM, em execução no SLES 11.

Tabela 2-4 *Números de Desempenho do Gerenciador de Coletor*

Atributo	Limite	Comentários
Número máximo de Gerenciadores de Coletor	20	Este limite considera que cada Gerenciador de Coletor esteja sendo executado a um EPS baixo (ex. menos de 100 EPS). O limite cai à medida que os eventos por segundo aumentam.
Número máximo de Conectores (totalmente utilizados) em um único Gerenciador de Coletor	1 por núcleo de CPU, com pelo menos 1 núcleo da CPU reservado para o sistema operacional e outro processamento	Um Conector totalmente utilizado é aquele que é executado com o maior EPS possível para seu tipo de Conector.
Número máximo de Coletores (totalmente utilizados) em um único Gerenciador de Coletor	1 por núcleo de CPU, com pelo menos 1 núcleo da CPU reservado para o sistema operacional e outro processamento	Um Coletor totalmente utilizado é aquele que é executado com o maior EPS possível para seu tipo de Coletor.

Atributo	Limite	Comentários
Número máximo de dispositivos em um único Gerenciador de Coletor	2000	O limite do servidor Sentinel Rapid Deployment também é 2000, logo, se 2000 dispositivos estiverem em um único Gerenciador de Coletor, o limite de dispositivos para todo o sistema Sentinel terá sido atingido nesse único Gerenciador de Coletor.
Número máximo de dispositivos no servidor Sentinel Rapid Deployment	2000	O limite de dispositivos no servidor Sentinel Rapid Deployment é de 2000.

2.5.2 Limites de relatórios

Tabela 2-5 *Números de Desempenho de Relatórios*

Atributo	Limite	Comentários
Número máximo de relatórios salvos	200	Esse limite pode aumentar ou diminuir de acordo com o tamanho dos relatórios e o espaço em disco disponível no servidor que não está sendo usado pelo restante do sistema.
Número máximo de relatórios em execução simultânea	3	O limite considera que o servidor ainda não esteja sendo totalmente utilizado na realização de coleta de dados nem de outras tarefas.

2.6 Resultados do teste

O Sentinel Rapid Deployment oferece diferentes configurações de acordo com as necessidades do ambiente. As informações de teste de desempenho a seguir são o resultado do teste da Novell para configurações específicas listadas nas tabelas abaixo.

As recomendações de hardware para uma implementação do Sentinel podem variar de acordo com cada implementação; portanto, recomendamos entrar em contato com o Novell Consulting Services ou com qualquer parceiro do Novell Sentinel antes de finalizar a arquitetura do Sentinel. As informações do teste a seguir podem ser usadas como orientação.

O teste do Linux foi realizado para expandir o máximo de EPS com um número diferente de dispositivos e para expandir o número máximo de dispositivos para um EPS específico. Foi usada a seguinte configuração de hardware:

- **Número de Núcleos da CPU:** 4
- **Modelo da CPU:** Intel Xeon CPU X5770 com 2.93 GHz
- **RAM:** 16 GB
- **Tamanho do Disco Rígido (Tipo de RAID e número de discos no RAID):** 1.7 TB (RAID 5, 6 discos)

Observação: Todos os testes foram realizados com fontes de eventos baseadas em syslog. Outros conectores podem oferecer um desempenho diferente.

A tabela a seguir mostra o máximo de EPS que é possível expandir com um número diferente de dispositivos no sistema SLES:

Tabela 2-6 *Máximo de EPS no Sistema SLES*

Configuração do Sistema	Dispositivos	Máximo de EPS
4 Gerenciadores de Coletor (um local e três remotos) com 10 Coletores, cada um gerando 500 EPS	25	5.000
4 Gerenciadores de Coletor (um local e três remotos) com 10 Coletores, cada um gerando 500 EPS	100	5.000
4 Gerenciadores de Coletor (um local e três remotos) com 10 Coletores, cada um gerando 500 EPS	1.000	5.000

A tabela a seguir mostra o máximo de dispositivos que é possível expandir em diferentes taxas de EPS no sistema SLES:

Tabela 2-7 *Máximo de Dispositivos no Sistema SLES*

Configuração do Sistema	EPS	Máximo de Dispositivos
1 Gerenciador de Coletor com 1 Coletor gerando 500 EPS	500	2.000
1 Gerenciador de Coletor com 2 Coletores gerando 500 EPS cada	1.000	2.000
1 Gerenciador de Coletor com 3 Coletores, cada um gerando 500 EPS	1.500	2.000

Observação:

- Para expandir mais EPS ou dispositivos, instale outros Gerenciadores de Coletor.
- Os limites máximos de dispositivos não são rígidos, mas são recomendações baseadas no teste de desempenho realizado pela Novell. Eles consideram uma taxa baixa da média de eventos por segundo por dispositivo (menor que 3 EPS). Taxas de EPS mais altas resultam em um número máximo de dispositivos sustentáveis menor. Você pode usar a equação (máximo de dispositivos) x (média de EPS por dispositivo) = taxa máxima de eventos para chegar aos limites aproximados para a sua taxa de EPS média específica ou o número de dispositivos, desde que o número máximo de dispositivos não exceda o limite indicado acima.

Instalação

3

Esta seção apresenta as informações sobre instalação do Sentinel Rapid Deployment e os componentes clientes.

- Seção 3.1, “Visão geral” na página 27
- Seção 3.2, “Instalação no SUSE Linux Enterprise Server” na página 29
- Seção 3.3, “Instalando o Gerenciador de Coletor e os aplicativos clientes” na página 35
- Seção 3.4, “Iniciando e interrompendo manualmente os serviços do Sentinel” na página 41
- Seção 3.5, “Upgrade manual do Java” na página 41
- Seção 3.6, “Configuração de pós-instalação” na página 42
- Seção 3.7, “Autenticação LDAP” na página 44
- Seção 3.8, “Atualizando a classificação da chave de licença de chave de avaliação para chave de produção” na página 52

3.1 Visão geral

O pacote de instalação do Sentinel inclui um instalador simplificado de servidor de única máquina para instalar tudo o que for necessário para execução do Sentinel Rapid Deployment. O instalador do servidor Sentinel Rapid Deployment instala os seguintes componentes:

- Seção 3.1.1, “Componentes do servidor” na página 27
- Seção 3.1.2, “Aplicativos clientes” na página 28

3.1.1 Componentes do servidor

Tabela 3-1 *Componentes e aplicativos do Sentinel Server*

Componente	Descrição
	O banco de dados do Sentinel armazena dados de configuração e eventos.
Barramento de mensagem	Um barramento de mensagem baseado em JMS gerencia a comunicação entre os componentes do sistema Sentinel.
Mecanismo de correlação	O mecanismo de correlação executa análises de eventos em tempo real.
Advisor	O Advisor fornece correlação em tempo real entre ataques IDS detectados e resultados da exploração de vulnerabilidades para indicar imediatamente se há aumento de risco para uma organização.
Serviço de Acesso a Dados	Inclui componentes de armazenamento de dados, consulta, exibição e processamento.
Servidor Web	Suporta a interface da Web do Sentinel Rapid Deployment.

Componente	Descrição
Gerenciador de Coletor	Um serviço que gerencia conexões com fontes de eventos, análise de dados, mapeamento, etc. Você pode distribuir o Gerenciador de Coletor para outros locais, outras máquinas e outros sistemas operacionais usando o instalador do Gerenciador de Coletor disponível na interface da Web do Sentinel Rapid Deployment. Por exemplo, você pode instalar um Gerenciador de Coletor adicional em uma máquina com o Windows para coletar eventos do Windows.
iTRAC	O Sentinel fornece um sistema de gerenciamento de workflow do iTRAC para que você possa definir e automatizar processos de respostas a incidentes. Incidentes identificados no Sentinel, seja por uma regra de correlação ou manualmente, podem ser associados a um workflow do iTRAC.

3.1.2 Aplicativos clientes

Os aplicativos clientes – o Sentinel Control Center, o Gerenciador de Dados do Sentinel e o Designer de Soluções são instalados por padrão no servidor Sentinel Rapid Deployment. Para iniciar os aplicativos clientes, você pode usar qualquer um dos seguintes métodos:

- Usando a interface da Web do Sentinel Rapid Deployment. Os sistemas clientes devem ter o Java 1.6.0_20 ou posterior instalado e o caminho JRE deve estar definido para iniciar os aplicativos do Sentinel pelo Webstart.

  Defina a variável de ambiente `JAVA_HOME` para apontar para o local da pasta `JRE 6`. Defina o caminho de exportação para apontar para a pasta `bin` no local do JRE 6.

- Usando o `<diretório_de_instalação>/bin` como o usuário que tem a propriedade dos arquivos de instalação do Sentinel Rapid Deployment. Por exemplo:

  `./bin/<client_application>.sh`

Tabela 3-2 *Aplicativos clientes do Sentinel*

Componente	Descrição
Sentinel Control Center	Console principal para analistas de segurança e conformidade.
Gerenciador de Dados do Sentinel	Utilitário de gerenciamento de banco de dados.
Designer de Soluções	Aplicativo usado para criar Pacotes de Soluções.
Gerenciador de Coletor do Sentinel	Esse serviço gerencia conexões com fontes de eventos, análise de dados, mapeamento, etc. Um Gerenciador de Coletor é instalado no Sentinel Server, mas Gerenciadores de Coletor adicionais podem ser instalados em máquinas Windows ou Linux remotas por meio de um instalador obtido por download.

3.2 Instalação no SUSE Linux Enterprise Server

- Seção 3.2.1, “Pré-requisitos” na página 29
- Seção 3.2.2, “Instalando o Sentinel Rapid Deployment” na página 30

3.2.1 Pré-requisitos

Verifique se os seguintes pré-requisitos são atendidos antes de instalar o Sentinel Rapid Deployment. Para obter mais informações sobre esses pré-requisitos (incluindo a lista de plataformas certificadas), consulte o Capítulo 2, “Requisitos do sistema” na página 19.

- “Servidor” na página 29
- “Cliente” na página 29
- “Consultor” na página 30

Importante: As instalações do Sentinel Rapid Deployment que usam o instalador completo devem ser sempre realizadas em um sistema limpo. Caso já tenha outras versões do Sentinel instaladas, como o Sentinel Classic ou o Sentinel Log Manager, em qualquer uma das máquinas, desinstale-as primeiro. Para obter informações sobre como desinstalar as versões anteriores do Sentinel, consulte os guias de Instalação relevantes:

- Para desinstalar o Sentinel Classic, consulte o capítulo “Uninstalling Sentinel” (Desinstalando o Sentinel) no Sentinel Installation Guide (http://www.novell.com/documentation/sentinel61/s61_install/?page=/documentation/sentinel61/s61_install/data/bgpq4la.html) (Guia de Instalação do Sentinel).
- Para desinstalar o Sentinel Log Manager, consulte o capítulo “Desinstalando o Sentinel Log Manager” no Guia de Instalação do Sentinel Log Manager 1.1 (http://www.novell.com/documentation/novelllogmanager11/log_manager_install/?page=/documentation/novelllogmanager11/log_manager_install/data/bor9aaf.html).

Servidor

- Verifique se todas as máquinas servidor atendem aos requisitos mínimos do sistema. Para obter mais informações sobre os requisitos do sistema, consulte o Capítulo 2, “Requisitos do sistema” na página 19.
- Configure o sistema operacional de maneira que o comando `hostname -f` retorne um nome de host válido.
- Instale e configure um servidor SMTP se desejar ter acesso ao recurso de enviar notificações por e-mail a partir do sistema Sentinel.

Cliente

- Verifique se todas as máquinas cliente atendem aos requisitos mínimos do sistema. Para obter mais informações sobre esses pré-requisitos, consulte o Capítulo 2, “Requisitos do sistema” na página 19.
- Crie um diretório que tenha apenas caracteres ASCII no nome (nenhum caractere especial) onde o instalador será executado.
- Quando instalar um Gerenciador de Coletor remoto ou aplicativos clientes em máquinas Linux, verifique se não há restrições no nível de pasta definidas na pasta `/tmp` para o usuário admin.

- Conceda privilégios de usuário Avançado ao Usuário de Domínio para o Gerenciador de Coletor no Windows, pois os direitos de usuário normal não são suficientes para a instalação do Gerenciador de Coletor.
- Se estiver instalando o Gerenciador de Coletor em uma máquina de 64 bits, verifique se as bibliotecas de 32 bits estão disponíveis. As bibliotecas de 32 bits são necessárias quando você executa um Coletor criado em seu idioma proprietário (que inclui quase todos os Coletores criados antes de junho de 2008), e também quando você executa determinados Conectores (como o Conector LEA). Coletores baseados em JavaScript e o restante do Sentinel são habilitados para 64 bits. Verificar se essas bibliotecas estão disponíveis é muito importante em plataformas Linux, que podem não as incluir por padrão.

Consultor

Para instalar o Advisor, adquira a Inscrição do Sentinel Exploit Detection e do Advisor Data. Após adquirir a inscrição, use o Novell eLogin para fazer download e atualizar os dados do Advisor. Para obter mais informações, consulte o capítulo "Advisor Usage and Maintenance" (Uso e manutenção do Advisor) no *Sentinel Rapid Deployment User Guide* (Guia do Usuário do Sentinel Rapid Deployment).

3.2.2 Instalando o Sentinel Rapid Deployment

É possível instalar o servidor Sentinel Rapid Deployment das seguintes maneiras:

- "Instalação de script único com privilégios root" na página 30
- "Instalação não root" na página 32

O script do instalador do Sentinel Rapid Deployment apresenta as seguintes opções durante a instalação:

- **-all:** Você deve ser usuário `root` para utilizar essa opção. Essa opção cria um usuário (padrão: `novell`), grupo de usuários, (padrão: `novell`) e instala o servidor Sentinel Rapid Deployment. Ela também executa os serviços do Sentinel Rapid Deployment automaticamente na inicialização do sistema.
- **-install:** Essa opção instala apenas o servidor Sentinel Rapid Deployment.
- **-createuser:** Você deve ser usuário `root` para utilizar essa opção. Essa opção cria apenas o usuário (padrão: `novell`) e o grupo de usuários (padrão: `novell`).
- **-createservice:** Você deve ser usuário `root` para utilizar essa opção. Essa opção apenas habilita a execução automática dos serviços do Sentinel Rapid Deployment na inicialização do sistema.
- **-help:** Essa opção exibe ajuda sobre como usar as opções de script de instalação.

Instalação de script único com privilégios root

1. Efetue login como usuário `root`.

   O usuário que está executando a instalação deve ter acesso de gravação ao diretório temporário em que os arquivos do instalador serão descarregados.
2. Faça download do instalador `sentinel6_rd_linux_x86-64.tar.gz` do site de download da Novell (http://download.novell.com/) em um diretório temporário.
3. Extraia o instalador:

   ```
   tar zxvf sentinel6_rd_linux_x86-64.tar.gz
   ```

4 Mude para o diretório no qual extraiu o instalador:

```
cd sentinel6_rd_linux_x86-64
```

5 Execute o script `install.sh` com a opção `-all`:

```
./install.sh -all
```

O script de instalação primeiro verifica a memória disponível e o espaço em disco. Se a memória disponível for menor que 1 GB, o script terminará a instalação automaticamente. Se a memória disponível for maior que 1 GB, mas menor que 4 GB, o script exibirá uma mensagem informando que você tem menos memória do que o recomendado. Ele também perguntará se você deseja continuar com a instalação. Digite `s` se quiser continuar com a instalação ou digite `n` se não quiser prosseguir.

6 Especifique o nome de usuário ou pressione Enter para selecionar o nome de usuário padrão. O nome de usuário padrão é `novell`.

Se o nome de usuário especificado já existir, o instalador exibirá uma mensagem de que o usuário existe e listará o grupo do usuário. Avance para a Etapa 8.

Se o nome de usuário especificado não existir, o instalador o criará. Avance para a Etapa 7.

7 Especifique o nome do grupo ou pressione Enter para selecionar o nome do grupo padrão. O nome do grupo padrão é `novell`.

Se o nome do grupo especificado já existir, o instalador continuará com a instalação. Se o nome do grupo especificado não existir, o instalador criará o grupo e exibirá uma mensagem informando que o nome de usuário inserido foi criado no grupo determinado.

O usuário e o grupo especificados obtêm a propriedade da instalação e dos processos em execução do Sentinel.

8 Especifique o caminho de instalação ou pressione Enter para selecionar o caminho padrão. O caminho padrão é `/opt/novell`.

O caminho de instalação especificado não deve conter espaço. Se houver espaço, o script de instalação solicitará o caminho de instalação sem espaço.

9 Escolha um dos idiomas a seguir. Para isso, digite o número correspondente:

Número de Série	Idioma
1	Tcheco
2	Inglês
3	Francês
4	Alemão
5	Italiano
6	Japonês
7	Holandês
8	Polonês
9	Português
10	Chinês Simplificado
11	Espanhol

Número de Série	Idioma
12	Chinês Tradicional

O Contrato de Licença de Usuário Final será exibido no idioma selecionado.

10 Leia o Contrato de Licença de Usuário Final e digite `1` se concordar com ele e quiser continuar com a instalação. Se quiser sair da instalação, digite `2`.

O instalador começa a extrair os arquivos e solicita a licença.

11 Digite `1` para usar a chave de licença de avaliação de 90 dias ou digite `2` para usar a chave de licença válida.

Se você digitar `2`, o instalador solicitará a chave de licença válida do Sentinel RD. Se a chave de licença especificada não for válida, o instalador solicitará novamente a chave de licença válida. Se a chave de licença especificada não for válida na segunda tentativa, a chave de licença de avaliação de 90 dias será instalada automaticamente. Você pode digitar a licença válida posteriormente.

O script carrega a licença de avaliação ou a licença válida.

12 Especifique uma senha para o usuário `dbauser` e especifique-a novamente para confirmar.

As credenciais do `dbauser` são usadas para criar tabelas e partições no banco de dados PostgreSQL.

13 Especifique uma senha para o usuário `admin` e especifique-a novamente para confirmar.

Quando for solicitado a especificar senhas para os usuários `admin` e `dbauser`, não use os caracteres de barra invertida (\) nem apóstrofo (‘) na senha, porque o banco de dados PostgreSQL não aceita esses caracteres.

O script de instalação instala o banco de dados PostgreSQL, cria tabelas e partições e, depois, instala o servidor Sentinel Rapid Deployment.

Após a instalação, você poderá:

- Inicie a interface da Web do Sentinel Rapid Deployment em `https://<IP_SERVIDOR>:8443/sentinel`. *<IP_SERVIDOR>* é o endereço IP da máquina na qual o Sentinel Rapid Deployment foi instalado.
- Inicie o Sentinel Control Center executando o `<diretório_de_instalação>/bin/control_center.sh` como o usuário criado na Etapa 6.

Instalação não root

Se a política organizacional proibir a execução do processo de instalação completo como `root`, a instalação poderá ser concluída em duas partes. A primeira parte do procedimento de instalação deve ser realizada com privilégios `root` e a segunda parte, como usuário administrativo do Sentinel (criado na primeira parte).

1 Efetue login no servidor onde você vai instalar o Sentinel Rapid Deployment.

O usuário que está executando a instalação deve ter acesso de gravação ao diretório temporário em que os arquivos do instalador serão descarregados.

2 Faça download do instalador `sentinel6_rd_linux_x86-64.tar.gz` do site de download da Novell (http://download.novell.com/) em um diretório temporário.

3 Extraia o instalador:

```
tar zxvf sentinel6_rd_linux_x86-64.tar.gz
```

4. Efetue login como usuário `root`.
5. Mude para o diretório no qual extraiu o instalador:

   ```
   cd sentinel6_rd_linux_x86-64
   ```

6. Execute o script `install.sh` com a opção `-createuser`:

   ```
   ./install.sh -createuser
   ```

7. Especifique o nome de usuário ou pressione Enter para selecionar o nome de usuário padrão. O nome de usuário padrão é `novell`.

   Se o nome de usuário especificado já existir, o instalador exibirá uma mensagem de que o usuário existe e listará o grupo do usuário. Avance para a Etapa 9.

   Se o nome de usuário especificado não existir, o instalador o criará. Avance para a Etapa 8.

8. Especifique o nome do grupo ou pressione Enter para selecionar o nome do grupo padrão. O nome do grupo padrão é `novell`.

   Se o nome do grupo especificado já existir, o instalador continuará com a instalação. Se o nome do grupo especificado não existir, o instalador criará o grupo e exibirá uma mensagem informando que o nome de usuário inserido foi criado no grupo determinado.

   O usuário e o grupo especificados obtêm a propriedade da instalação e dos processos em execução do Sentinel.

9. Especifique o caminho de instalação ou pressione Enter para selecionar o caminho padrão. O caminho padrão é `/opt/novell`.

   O caminho de instalação especificado não deve conter espaço. Se houver espaço, o script de instalação solicitará o caminho de instalação sem espaço.

10. Efetue login como usuário não root. Por exemplo.

    ```
    su - novell
    ```

11. Execute o script de instalação com a opção `-install`:

    ```
    ./install.sh -install
    ```

    O script de instalação primeiro verifica a memória disponível e o espaço em disco. Se a memória disponível for menor que 1 GB, o script terminará a instalação automaticamente. Se a memória disponível for maior que 1 GB, mas menor que 4 GB, o script exibirá uma mensagem informando que você tem menos memória do que o recomendado. Ele também perguntará se você deseja continuar com a instalação. Digite `s` se quiser continuar com a instalação ou digite `n` se não quiser prosseguir.

12. Especifique o caminho de instalação ou pressione Enter para selecionar o caminho padrão. O caminho padrão é `/opt/novell`.

    O caminho de instalação especificado não deve conter espaço. Se houver espaço, o script de instalação solicitará o caminho de instalação sem espaço.

13. Escolha um dos idiomas a seguir. Para isso, digite o número correspondente:

Número de Série	Idioma
1	Tcheco
2	Inglês
3	Francês

Número de Série	Idioma
4	Alemão
5	Italiano
6	Japonês
7	Holandês
8	Polonês
9	Português
10	Chinês Simplificado
11	Espanhol
12	Chinês Tradicional

O Contrato de Licença de Usuário Final será exibido no idioma selecionado.

14 Leia o Contrato de Licença de Usuário Final e digite `1` se concordar com ele e quiser continuar com a instalação. Se quiser sair da instalação, digite `2`.

O instalador começa a extrair os arquivos e solicita a licença.

15 Digite `1` para usar a chave de licença de avaliação de 90 dias ou digite `2` para usar a chave de licença válida.

Se você digitar `2`, o instalador solicitará a chave de licença válida do Sentinel RD. Se a chave de licença especificada não for válida, o instalador solicitará novamente a chave de licença válida. Se a chave de licença especificada não for válida na segunda tentativa, a chave de licença de avaliação de 90 dias será instalada automaticamente. Você pode digitar a licença válida posteriormente.

O script carrega a licença de avaliação ou a licença válida.

16 Especifique uma senha para o usuário `dbauser` e especifique-a novamente para confirmar.

As credenciais do `dbauser` são usadas para criar tabelas e partições no banco de dados PostgreSQL.

17 Especifique uma senha para o usuário `admin` e especifique-a novamente para confirmar.

Quando for solicitado a especificar senhas para os usuários `admin` e `dbauser`, não use os caracteres de barra invertida (\) nem apóstrofo (‘) na senha, porque o banco de dados PostgreSQL não aceita esses caracteres.

18 (Condicional) Quando a instalação é concluída, para executar os serviços do Sentinel Rapid Deployment automaticamente na inicialização do sistema, execute o script `install.sh` com a opção `-createservice` como usuário `root`:

```
./install.sh -createservice
```

Após a instalação, você poderá:

- Inicie a interface da Web do Sentinel Rapid Deployment em `https://<IP_SERVIDOR>:8443/sentinel`. *<IP_SERVIDOR>* é o endereço IP da máquina na qual o Sentinel Rapid Deployment foi instalado.
- Inicie o Sentinel Control Center executando o `<diretório_de_instalação>/bin/control_center.sh` como o usuário criado na Etapa 7 acima.

3.3 Instalando o Gerenciador de Coletor e os aplicativos clientes

Use a interface da Web do Novell Sentinel Rapid Deployment para fazer download do instalador do Gerenciador de Coletor e do instalador do Cliente.

- Seção 3.3.1, “Fazendo download dos instaladores” na página 35
- Seção 3.3.2, “Números de portas para os componentes clientes do Sentinel Rapid Deployment” na página 36
- Seção 3.3.3, “Instalando os aplicativos clientes do Sentinel” na página 36
- Seção 3.3.4, “Instalando o Gerenciador de Coletor do Sentinel no SLES ou Windows” na página 38

3.3.1 Fazendo download dos instaladores

1. Abra um browser da Web no seguinte URL:

   `https://<svrname.example.com>:8443/sentinel`

   Substitua `<nome_do_serv.exemplo.com>` pelo nome DNS ou endereço IP real do servidor em que o Sentinel está sendo executado. O URL diferencia maiúsculas de minúsculas.
2. Se for solicitado a verificar os certificados, confira as informações de certificado e, se elas forem válidas, clique em *Sim*.
3. Especifique o nome de usuário e a senha a serem usados para acessar a conta do Sentinel.
4. Use a lista suspensa *Idiomas* para selecionar o idioma.

   É o mesmo idioma do código de idioma do servidor Sentinel Rapid Deployment e do computador local. Verifique se a configuração de idiomas do browser está definida para suportar o idioma desejado.
5. Clique em *Entrar*.
6. Selecione *Aplicativos*.

   Você pode fazer download dos seguintes instaladores:

Opções	Descrição	Ação
Instalador do Gerenciador de Coletor	O Instalador do Gerenciador de Coletor permite instalar o Gerenciador de Coletor do Sentinel em plataformas Windows e Linux suportadas.	Clique em *Fazer download do instalador do Gerenciador de Coletor* e siga as instruções na tela.
Instalador do Cliente	O Instalador do Cliente permite instalar o Sentinel Control Center, o Sentinel Solution Designer e o Gerenciador de Dados do Sentinel em plataformas suportadas.	Clique em *Fazer download do instalador do Cliente* e siga as instruções na tela.

Para obter mais informações sobre como instalar o Gerenciador de Coletor, consulte a Seção 3.3.4, “Instalando o Gerenciador de Coletor do Sentinel no SLES ou Windows” na página 38, e sobre como instalar o instalador do Cliente, consulte a Seção 3.3.3, “Instalando os aplicativos clientes do Sentinel” na página 36.

3.3.2 Números de portas para os componentes clientes do Sentinel Rapid Deployment

Use as seguintes portas para configurar a definição de firewall para permitir acesso entre o servidor Sentinel Rapid Deployment e os componentes clientes.

Tabela 3-3 *Números de portas compatíveis para os componentes do Sentinel Rapid Deployment*

Número de porta	Descrição
61616	Os Gerenciadores de Coletor remotos usam esse número de porta para conectarem-se ao servidor Sentinel Rapid Deployment por meio do ActiveMQ.
10013	O Sentinel Control Center usa esse número de porta para conectar-se ao servidor Sentinel Rapid Deployment por meio de proxy.
5432	O Gerenciador de Dados do Sentinel usa esse número de porta para conectar-se ao banco de dados PostgreSQL.
8443	Os clientes Web usam esse número de porta para conectarem-se ao servidor Sentinel Rapid Deployment.

3.3.3 Instalando os aplicativos clientes do Sentinel

É possível instalar o aplicativo cliente do Sentinel em um sistema Linux ou Windows. Para instalar os aplicativos clientes:

1. Vá até a pasta na qual o instalador do cliente foi descarregado.
2. Extraia o script de instalação do arquivo:

Plataforma	Ação
Windows	Faça a descompactação do arquivo `client_installer.zip`. Os arquivos são descompactados em um diretório chamado `disk1`.
Linux	Execute o seguinte comando com privilégios root: `unzip client_installer.zip` Os arquivos são descompactados em um diretório chamado `disk1`.

3. Vá para o diretório de instalação e inicie a instalação:

Plataforma	Ação
Windows	Execute `disk1\setup.bat` **Observação:** Em uma máquina com Windows Vista, inicie o prompt de comando selecionando a opção *Executar como Administrador* no menu acessado com o botão direito do mouse.

Plataforma	Ação
Linux	◆ **Modo GUI:** `<diretório_de_instalação>/disk1/setup.sh` ◆ **Modo de console:** `<diretório_de_instalação>/disk1/setup.sh –console`

As etapas listadas a seguir são apenas para o modo GUI.

4 Clique na seta para baixo e selecione um dos idiomas.

5 Na tela de boas-vindas, clique em *Avançar*.

6 Leia e aceite o Contrato de Licença de Usuário Final. Clique em *Avançar*.

7 Aceite o diretório de instalação padrão ou clique em *Procurar* para especificar o local da instalação. Clique em *Avançar*.

Importante: Você não pode instalar em um diretório com caracteres especiais ou caracteres que não sejam ASCII no nome. Por exemplo, quando você instala o Sentinel Rapid Deployment no Windows x86-64, o caminho padrão é `C:\\Arquivos de Programas (x86)`. Mude esse caminho padrão para evitar caracteres especiais, como os parêntesis de (x86), para continuar com a instalação.

8 Selecione os aplicativos do Sentinel que quer instalar.

As seguintes opções estão disponíveis:

Componente	Descrição
Sentinel Control Center	O console principal para analistas de segurança e conformidade.
SDM (Gerenciador de Dados do Sentinel)	Usado para atividades manuais de gerenciamento de banco de dados.
Designer de Soluções	Ajuda a criar Pacotes de Soluções.

9 Se você optar por instalar o Sentinel Control Center, o instalador solicitará que o espaço em memória máximo seja alocado para o Sentinel Control Center. Especifique o tamanho de heap JVM máximo (MB) a ser usado somente pelo Sentinel Control Center.

A faixa permitida é 64-1024 MB.

Essa opção não estará disponível se houver algum aplicativo do Sentinel instalado.

10 Especifique o nome de usuário ou pressione Enter para selecionar o nome de usuário padrão. O nome de usuário padrão é `esecadm`.

É o nome de usuário do proprietário do Sentinel instalado. Se o usuário não existir, um usuário será criado com um diretório pessoal no diretório especificado.

11 Especifique o diretório pessoal do usuário ou pressione Enter para selecionar o diretório padrão. O diretório padrão é `/export/home`.

Se o nome de usuário for `esecadm`, o diretório pessoal correspondente será `/export/home/esecadm`.

12 Especifique a senha para o usuário para efetuar login como o usuário `esecadm`, caso tenha selecionado o nome de usuário padrão na Etapa 10. Do contrário, defina a senha para o usuário que você criou na Etapa 10.

13 Especifique as seguintes informações:

- **Porta de barramento de mensagem:** A porta de escuta do servidor de comunicação. Os componentes que se conectam diretamente ao servidor de comunicação usam essa porta. O número de porta padrão é 61616.
- **Porta proxy do Sentinel Control Center:** A porta na qual o servidor proxy SSL (Proxy do Servidor de Acesso a Dados) escuta para aceitar o nome de usuário e a senha. O servidor proxy SSL aceita as credenciais com base nas conexões autenticadas. O Sentinel Control Center usa essa porta para se conectar ao Sentinel Server. O número da porta padrão é `10013`.
- **Nome de host do Servidor de Comunicação:** O nome de host ou o endereço IP da máquina na qual o servidor Sentinel Rapid Deployment foi instalado.

Verifique se os números de portas são os mesmos do servidor Sentinel Rapid Deployment em`<diretório_de_instalação>/config/configuration.xml` para habilitar as comunicações. Anote essas portas para instalações futuras em outras máquinas. Para obter mais informações sobre números de portas, consulte a Seção 3.3.2, “Números de portas para os componentes clientes do Sentinel Rapid Deployment” na página 36.

14 Clique em *Next* (Avançar).

É exibido um resumo da instalação.

15 Clique em *Instalar*.

16 Clique em *Concluir* para concluir a instalação.

Observação: Quando efetuar login novamente, utilize o nome de usuário especificado na Etapa 10.

Caso se esqueça do nome de usuário definido, abra o console de terminal e digite o seguinte comando como usuário `root`:

```
env | grep ESEC_USER
```

Esse comando retornará o nome de usuário se o usuário já tiver sido criado e se as variáveis de ambiente já tiverem sido definidas.

3.3.4 Instalando o Gerenciador de Coletor do Sentinel no SLES ou Windows

O instalador do Gerenciador de Coletor do Sentinel está disponível para download na página Aplicativos da interface da Web do Sentinel Rapid Deployment. Para instalar o Gerenciador de Coletor:

1 Vá até a pasta na qual o instalador do Gerenciador de Coletor foi descarregado.

2 Extraia o script de instalação do arquivo:

Plataforma	Ação
Windows	Faça a descompactação do arquivo `scm_installer.zip`. Os arquivos são descompactados em um diretório chamado `disk1`.

Plataforma	Ação
Linux	Execute o seguinte comando com privilégios root: `unzip scm_installer.zip` Os arquivos são descompactados em um diretório chamado `disk1`.

3 Vá para o diretório `disk1` e comece a instalação:

Plataforma	Ação
Windows	Execute o seguinte comando: `disk1\setup.bat`
Linux	◆ **Modo GUI:** `<diretório_de_instalação>/disk1/setup.sh` ◆ **Modo de console:** `<diretório_de_instalação>/disk1/setup.sh –console`

4 Selecione o idioma para continuar com a instalação.

5 Leia a tela de boas-vindas e clique em *Avançar*.

6 Leia e aceite o Contrato de Licença de Usuário Final. Clique em *Avançar*.

7 Aceite o diretório de instalação padrão ou clique em *Procurar* para especificar o local da instalação e, em seguida, clique em *Avançar*.

Importante: Você não pode instalar em um diretório com caracteres especiais ou caracteres que não sejam ASCII no nome. Por exemplo, quando você instala o Sentinel no Windows x86-64, o caminho padrão é `C:\\Arquivos de Programas (x86)`. Mude esse caminho padrão para evitar caracteres especiais, como os parêntesis de (x86), para continuar com a instalação.

8 Especifique o nome de usuário do Administrador do Sentinel e o caminho para o diretório pessoal correspondente.

Essa opção não estará disponível se houver algum aplicativo do Sentinel instalado.

- **Nome de Usuário do Administrador do Sentinel no Sistema Operacional:** O padrão é `esecadm`.

  É o nome de usuário do proprietário do Sentinel instalado. Se o usuário ainda não existir, um usuário será criado com o diretório pessoal correspondente no diretório especificado.
- **Diretório Pessoal do Administrador do Sentinel no Sistema Operacional:** O padrão é `/export/home`. Se o nome de usuário for `esecadm`, o diretório pessoal correspondente será `/export/home/esecadm`.

Para efetuar login como o usuário `esecadm`, defina sua senha primeiro.

9 Especifique as seguintes informações:

- **Porta de barramento de mensagem:** A porta de escuta do servidor de comunicação. Os componentes que se conectam diretamente ao servidor de comunicação usam essa porta. O número de porta padrão é 61616.
- **Nome de host do Servidor de Comunicação:** O nome de host ou o IP da máquina em que o Sentinel Rapid Deployment Server está instalado.

Para habilitar comunicações, verifique se os números de porta são os mesmos em todas as máquinas do sistema Sentinel. Anote essas portas para instalações futuras em outras máquinas.

10 Clique em *Next* (Avançar).

11 Especifique as seguintes informações:

- **Configuração Automática de Memória:** Selecione o volume total de memória a ser alocado para o Gerenciador de Coletor. O instalador determina automaticamente a distribuição ideal de memória entre os componentes, levando em consideração o overhead estimado do sistema operacional e do banco de dados.

  Importante: Você pode modificar o valor -Xmx no arquivo `configuration.xml` para mudar a RAM alocada para o processo do Gerenciador de Coletor. O arquivo `configuration.xml` fica em `<diretório_de_instalação>/config` no Linux ou em `<diretório_de_instalação>\config` no Windows.

- **Configuração Personalizada de Memória:** Clique em *Configurar* para ajustar alocações de memória. Essa opção só estará disponível se houver memória suficiente na máquina.

12 Clique em *Next* (Avançar).

É exibida uma tela de resumo com os recursos selecionados para instalação.

13 Clique em *Instalar*.

14 Após o término da instalação, você será solicitado a inserir o nome de usuário e a senha usados pela estratégia JMS do ActiveMQ para estabelecer conexão com o controlador.

Utilize o nome de usuário `collectormanager` e sua senha correspondente que está disponível no arquivo `<diretório_de_instalação>/config/activemqusers.properties` no Sentinel Server.

Veja a seguir um exemplo das credenciais disponíveis no arquivo `activemqusers.properties`:

```
collectormanager=cefc76062c58e2835aa3d777778f9295
```

`collectormanager` é o nome de usuário e `cefc76062c58e2835aa3d777778f9295` é a senha correspondente.

Você deve utilizar o usuário collectormanager e a senha correspondente durante a instalação do serviço do Gerenciador de Coletor. Dessa forma, em operações do Gerenciador de Coletor, o usuário `collectormanager` só tem direitos de acesso nos canais de comunicação necessários.

Após o término da instalação, você será solicitado a reinicializar o sistema ou a efetuar login de novo e iniciar os serviços do Sentinel manualmente.

15 Clique em *Concluir* para reinicializar o sistema.

16 Efetue login novamente, utilizando o nome de usuário que você especificou na Etapa 8.

Se esquecer o nome de usuário, abra um console de terminal e digite o seguinte comando com credenciais `root`.

```
env | grep ESEC_USER
```

Esse comando retornará o nome de usuário se o usuário já tiver sido criado e se as variáveis de ambiente já tiverem sido definidas.

Observação: Há alguns problemas com a instalação do Gerenciador de Coletor na plataforma Windows 2008, e também nos Gerenciadores de Coletor com Imagens. Para obter informações sobre como solucionar esses problemas, consulte o Apêndice B, “Dicas para solução de problemas” na página 89.

3.4 Iniciando e interrompendo manualmente os serviços do Sentinel

Para iniciar os serviços do Sentinel manualmente, use os seguintes comandos:

Plataforma	Comando
Linux	`<diretório_de_instalação>/bin/sentinel.sh start`
Windows	`<diretório_de_instalação>/bin/sentinel.bat start`

Para parar os serviços do Sentinel manualmente, use os seguintes comandos:

Plataforma	Comando
Linux	`<diretório_de_instalação>/bin/sentinel.sh stop`
Windows	`<diretório_de_instalação>/bin/sentinel.bat stop`

É possível também usar o seguinte comando para iniciar ou parar os serviços do Sentinel.

```
/etc/init.d/sentinel.sh stop|start
```

3.5 Upgrade manual do Java

O Java versão 1.6.0_24 acompanha o instalador do servidor Sentinel Rapid Deployment e é instalado durante a instalação do servidor Sentinel Rapid Deployment. No entanto, se você fizer o upgrade do Java para a versão mais recente no servidor, vai precisar executar as etapas a seguir para que o Sentinel Rapid Deployment utilize a versão mais recente:

1. Faça download dos bundles do jre de acordo com o sistema operacional no qual o servidor Sentinel Rapid Deployment está instalado.

   O usuário que está fazendo o upgrade deve ter acesso de gravação ao diretório de instalação do Sentinel Rapid Deployment e também ao diretório no qual os arquivos de upgrade serão descarregados.

   - Se você instalou o Sentinel Rapid Deployment no SUSE Linux Enterprise Server, faça download dos bundles do jre de 32 bits e de 64 bits do site de download do Java (http://www.java.com/en/download/manual.jsp).

2. Renomeie as pastas `jre` e `jre64` no diretório de instalação do Sentinel Rapid Deployment para `jre_old` e `jre64_old`, respectivamente.

   ```
   cd <caminho_de_instalação>/sentinel_rd
   mv jre jre_old
   mv jre64 jre64_old
   ```

Observação: A renomeação é obrigatória para reverter para as versões mais antigas caso o upgrade do Java não funcione apropriadamente. É possível apagar as pastas renomeadas, se o Java funcionar bem após o upgrade.

3. Extraia os bundles do jre descarregados.
4. Renomeie a pasta de 32 bits para `jre` e o diretório de 64 bits para `jre64`.
5. Copie as pastas renomeadas `jre` e `jre64` para o diretório de instalação do Sentinel Rapid Deployment.

   ```
   copy jre <caminho_de_instalação>/sentinel_rd/
   copy jre64 <caminho_de_instalação>/sentinel_rd/
   ```

6. (Condicional) Verifique se você definiu a propriedade e as permissões necessárias das pastas `jre` e `jre64` para o usuário que está executando o servidor Sentinel Rapid Deployment.
7. Reinicie o servidor Sentinel Rapid Deployment, reinicie o browser e verifique se o Java foi instalado corretamente.

3.6 Configuração de pós-instalação

Esta seção ajudará você a compreender a configuração pós-instalação dos serviços do Sentinel Rapid Deployment.

- Seção 3.6.1, “Mudando as configurações de data e hora” na página 42
- Seção 3.6.2, “Configurando um integrador SMTP para enviar notificações do Sentinel” na página 42
- Seção 3.6.3, “Serviços do Gerenciador de Coletor” na página 43
- Seção 3.6.4, “Gerenciando o tempo” na página 44

3.6.1 Mudando as configurações de data e hora

É possível anular o formato de data e hora padrão do Sentinel Control Center. Para obter mais informações sobre como personalizar o formato de data e hora ao seu fuso horário local, consulte o site do Java na Web (http://java.sun.com/j2se/1.6.0/docs/api/java/text/SimpleDateFormat.html).

1. Edite o arquivo `SentinelPreferences.properties`.

   `<diretório_de_instalação>/config/SentinelPreferences.properties`

2. Remova o comentário da seguinte linha e personalize o formato de data e hora nos campos de data/hora de eventos do Sentinel Control Center:

   ```
   com.eSecurity.Sentinel.event.datetimeformat=yyyy-MM-dd'T'HH:mm:ss.SSSZ
   ```

3.6.2 Configurando um integrador SMTP para enviar notificações do Sentinel

No Sentinel Rapid Deployment, a ação SendEmail do JavaScript funciona com um integrador SMTP para enviar mensagens de vários contextos da interface do Sentinel para destinatários de e-mail. Para ele funcionar, configure o Integrador SMTP com informações de conexão válidas. Para obter mais informações, consulte “Sending an E-mail” (Enviando e-mail) no *Sentinel Rapid Deployment User Guide* (Guia do Usuário do Sentinel Rapid Deployment).

Uma única instância de ação do plug-in SendEmail é criada automaticamente em cada instalação do Sentinel. Não é necessária nenhuma configuração na ação SendEmail, exceto se os destinatários e o conteúdo da mensagem estiverem configurados nos parâmetros de ação.

Esta ação SendEmail é acionada internamente pelo Sentinel para enviar e-mails nas seguintes situações:

- Quando uma regra de Correlação é gerada, a ação SendEmail é acionada. SendEmail é a ação indicada pelo ícone de engrenagem, válida somente para correlação (diferente da ação SendEmail do JavaScript, indicada pelo ícone JS do JavaScript).
- Quando um workflow inclui uma Etapa de E-mail ou Atividade configurada para enviar e-mails.
- Quando um usuário abre um incidente e executa uma Atividade configurada para enviar e-mails.
- Quando um usuário clica o botão direito do mouse em um evento e seleciona *E-mail*.
- Quando um usuário abre um incidente e seleciona *Incidente de E-mail*.

3.6.3 Serviços do Gerenciador de Coletor

- “Instalando o Gerenciador de Coletor adicional” na página 43
- “Usando o coletor Generic” na página 44

Instalando o Gerenciador de Coletor adicional

Os Gerenciadores de Coletor gerenciam todos os processos de coleta e análise de dados. Ocasionalmente, pode ser necessário incluir um nó adicional do Gerenciador de Coletor em um ambiente do Sentinel para equilibrar a carga nas máquinas. Os Gerenciadores de Coletor remotos oferecem vários benefícios:

- Análise e processamento de eventos distribuídos para melhorar o desempenho do sistema.
- Filtragem, criptografia e compactação de dados no sistema de origem pela colocação com fontes de eventos. Isso reduz os requisitos de largura de banda de rede e aumenta a segurança dos dados.
- Instalação em sistemas operacionais adicionais. Por exemplo, a instalação de um nó do Gerenciador de Coletor no Microsoft Windows para habilitar a coleta de dados utilizando o protocolo WMI.
- Armazenamento de arquivos em cache, o que permite que o gerenciador de coletor remoto armazene em cache grandes volumes de dados enquanto o servidor está temporariamente ocupado executando arquivamentos ou processando um pico de eventos. Isso é uma vantagem para protocolos que, como o syslog, não suportam o cache de eventos de forma nativa.

Para efetuar o equilíbrio de carga nos componentes do Gerenciador de Coletor, instale instâncias desses componentes em máquinas adicionais. É possível instalar um Gerenciador de Coletor adicional executando o instalador em uma nova máquina. Para obter mais informações sobre a instalação do Gerenciador de Coletor, consulte a Seção 3.3.4, “Instalando o Gerenciador de Coletor do Sentinel no SLES ou Windows” na página 38.

Usando o coletor Generic

Durante a instalação do Sentinel Rapid Deployment Server, é configurado um Coletor chamado Generic. Por padrão, a taxa de criação de eventos é de 5 eventos por segundo (eps).

Para ter coletores adicionais no sistema, você pode fazer download deles pelo site da Novell na Web (http://support.novell.com/products/sentinel/collectors.html).

3.6.4 Gerenciando o tempo

Você deve conectar o Sentinel Server a um servidor Network Time Protocol (NTP) ou a outro tipo de servidor de horário. Se o horário do sistema não estiver sincronizado nas máquinas, o Mecanismo de Correlação do Sentinel e as Telas Ativas não funcionarão corretamente. Os eventos dos Gerenciadores de Coletor não são considerados eventos em tempo real e, portanto, não são enviados diretamente para o banco de dados do Sentinel, ignorando os Sentinel Control Centers e os Mecanismos de Correlação.

Por padrão, o limite de dados em tempo real é de 120 segundos. Para modificar esse padrão, mude o valor de `esecurity.router.event.realtime.expiration` no arquivo `event-router.properties`. O horário de eventos do Sentinel é preenchido de acordo com o Horário do Dispositivo de Confiança ou com o Horário do Gerenciador de Coletor. Você pode selecionar o Horário do Dispositivo de Confiança ao configurar um coletor. O Horário do Dispositivo de Confiança é o horário em que o registro foi gerado pelo dispositivo e o Horário do Gerenciador de Coletor é o horário local do sistema Gerenciador de Coletor.

3.7 Autenticação LDAP

O Sentinel Rapid Deployment suporta a autenticação LDAP além da autenticação de banco de dados. É possível habilitar os usuários a efetuarem login no Sentinel Rapid Deployment usando suas credenciais do Novell eDirectory ou do Microsoft Active Directory por meio da configuração de um servidor Sentinel Rapid Deployment para autenticação LDAP.

- Seção 3.7.1, “Visão geral” na página 44
- Seção 3.7.2, “Pré-requisitos” na página 45
- Seção 3.7.3, “Configurando o Sentinel Server para autenticação LDAP” na página 46
- Seção 3.7.4, “Configurando vários servidores LDAP para failover” na página 48
- Seção 3.7.5, “Configurando a autenticação LDAP para vários domínios do Active Directory” na página 50
- Seção 3.7.6, “Efetuando login com as credenciais de usuário LDAP” na página 51

3.7.1 Visão geral

É possível configurar o servidor Sentinel Rapid Deployment para autenticação LDAP por uma conexão SSL segura, usando ou não pesquisas anônimas no diretório LDAP.

Observação: Se a pesquisa anônima estiver desabilitada no diretório LDAP, não configure o servidor Sentinel Rapid Deployment para utilizar pesquisa anônima.

- **Pesquisa Anônima:** Ao criar contas de usuário LDAP do Sentinel Rapid Deployment, você deve especificar o nome de usuário do diretório, mas não precisa especificar o nome exclusivo (DN) do usuário.

  Quando o usuário LDAP efetua login no Sentinel Rapid Deployment, o servidor Sentinel Rapid Deployment realiza uma pesquisa anônima no diretório LDAP com base no nome de usuário especificado, encontra o DN correspondente e, na sequência, autentica o login do usuário no diretório LDAP usando o DN.
- **Pesquisa Não Anônima:** Ao criar contas de usuário LDAP do Sentinel Rapid Deployment, você deve especificar tanto o nome de usuário do diretório quanto o DN do usuário.

  Quando o usuário LDAP efetua login no Sentinel Rapid Deployment, o servidor Sentinel Rapid Deployment autentica o login do usuário no diretório LDAP usando o DN do usuário especificado e não realiza nenhuma pesquisa anônima no diretório LDAP.

  Existe uma outra abordagem que vale apenas para o Active Directory. Para obter mais informações, consulte Autenticação LDAP não anônima usando o atributo UserPrincipalName no Active Directory.

3.7.2 Pré-requisitos

- “Exportando o certificado CA do servidor LDAP” na página 45
- “Habilitando pesquisa anônima no diretório LDAP” na página 45

Exportando o certificado CA do servidor LDAP

A conexão SSL segura com o servidor LDAP requer o certificado CA do servidor LDAP, que você deve exportar para o arquivo codificado com base64.

- **eDirectory:** Consulte Exporting an Organizational CA's Self-Signed Certificate (http://www.novell.com/documentation/edir88/edir88/?page=/documentation/edir88/edir88/data/a7elxuq.html) (Exportando o certificado autoassinado de uma CA organizacional).

  Para exportar um certificado CA do eDirectory no iManager, os plug-ins do Servidor de Certificação da Novell devem ser instalados.
- **Active Directory:** Consulte Como habilitar LDAP sobre SSL com uma autoridade de certificação de terceiros (http://support.microsoft.com/kb/321051).

Habilitando pesquisa anônima no diretório LDAP

Para realizar a autenticação LDAP usando a pesquisa anônima, habilite a pesquisa anônima no diretório LDAP. Por padrão, a pesquisa anônima está habilitada no eDirectory e desabilitada no Active Directory.

Para habilitar a pesquisa anônima no diretório LDAP, consulte o seguinte:

- **eDirectory:** Consulte ldapBindRestrictions na seção Attributes on the LDAP Server Object (http://www.novell.com/documentation/edir88/edir88/?page=/documentation/edir88/edir88/data/agq8auc.html) (Atributos no objeto Servidor LDAP).

- **Active Directory:** O objeto Usuário LOGON ANÔNIMO deve ter a permissão de lista e o acesso de leitura apropriados para os atributos `sAMAccountName` e `objectclass`. Para obter mais informações, consulte Como configurar o Active Directory para permitir consultas anônimas (http://support.microsoft.com/kb/320528).

  Para o Windows Server 2003, você deve realizar uma configuração adicional. Para obter mais informações, consulte Configurando o Active Directory no Windows Server 2003 (http://support.microsoft.com/kb/326690/en-us).

3.7.3 Configurando o Sentinel Server para autenticação LDAP

1. Verifique se você atende aos pré-requisitos na Seção 3.7.2, “Pré-requisitos” na página 45.
2. Efetue login no servidor Sentinel Rapid Deployment como usuário `root`.
3. Copie o arquivo exportado do certificado CA do servidor LDAP para o diretório `<diretório_de_instalação>/config`.
4. Defina a propriedade e as permissões do arquivo de certificado como mostrado a seguir:

   ```
   chown novell:novell <diretório_de_instalação>/config/<arquivo-cert>
   chmod 700 <diretório_de_instalação>/config/<arquivo-cert>
   ```

5. Mude para o usuário `novell`:

   ```
   su - novell
   ```

6. Mude para o diretório `<diretório_de_instalação>/bin`.
7. Execute o script de configuração da autenticação LDAP:

   ```
   ./ldap_auth_config.sh
   ```

   O script faz backup dos arquivos de configuração `auth.login` e `configuration.xml` no diretório `config` como `auth.login.sav` e `configuration.xml.sav` antes de modificá-los para autenticação LDAP.
8. Especifique as seguintes informações:

   Pressione Enter para aceitar o valor padrão ou especifique um novo valor para anular o padrão.

   - **Local de instalação do Sentinel:** O diretório de instalação no Sentinel Server.
   - **Nome de host ou endereço IP do servidor LDAP:** O nome de host ou o endereço IP da máquina em que o servidor LDAP foi instalado. O valor padrão é localhost. Porém, você não deve instalar o servidor LDAP na mesma máquina que o servidor do Sentinel
   - **Porta do Servidor LDAP:** O número da porta para conexão LDAP segura. O número de porta padrão é 636.
   - **Pesquisas anônimas no diretório LDAP:** Especifique `y` para realizar pesquisas anônimas. Do contrário, especifique `n`. O valor padrão é `y`.

     Se você especificar `n`, conclua a configuração LDAP e execute as etapas mencionadas na seção “Autenticação LDAP sem realizar pesquisas anônimas” na página 47.
   - **Diretório LDAP usado:** Esse parâmetro é exibido apenas quando você especifica ‘y’ para pesquisas anônimas. Especifique 1 para Novell eDirectory ou 2 para Active Directory. O valor padrão é 1.

- **Subárvore LDAP para pesquisar usuários:** Esse parâmetro é exibido apenas quando você especifica ‘y’ para pesquisas anônimas. A subárvore no diretório que tem os objetos Usuário. Veja a seguir exemplos para especificar a subárvore no eDirectory e no Active Directory:
  - eDirectory:

    ```
    ou=users,o=novell
    ```

    Observação: Para o eDirectory, se nenhuma subárvore for especificada, a pesquisa será executada em todo o diretório.

  - Active Directory:

    ```
    CN=users,DC=TESTAD,DC=provo, DC=novell,DC=com
    ```

    Observação: Para o Active Directory, a subárvore não pode ficar em branco.

- **Nome de arquivo do certificado do servidor LDAP:** O nome de arquivo do certificado CA do eDirectory/Active Directory que você copiou na Etapa 3.

9 Digite uma das opções a seguir:

- `y` para aceitar os valores digitados
- `n` para digitar novos valores
- `q` para sair da configuração

Na configuração bem-sucedida:

- O certificado do servidor LDAP é adicionado a um keystore chamado `<diretório_de_instalação>/config/ldap_server.keystore`.
- Os arquivos de configuração `auth.login` e `configuration.xml` no diretório `<diretório_de_instalação>/config` são atualizados para habilitar a autenticação LDAP.

10 Digite `y` para reiniciar o serviço do Sentinel.

Importante: Se houver algum erro, reverta as mudanças feitas nos arquivos de configuração `auth.login` e `configuration.xml` no diretório `config`:

```
cp -p auth.login.sav auth.login
cp -p configuration.xml.sav configuration.xml
```

11 (Condicional) Se você especificou `n` para Pesquisas anônimas no diretório LDAP:, continue em “Autenticação LDAP sem realizar pesquisas anônimas” na página 47.

Autenticação LDAP sem realizar pesquisas anônimas

Durante a configuração do Sentinel Rapid Deployment para Autenticação LDAP, se você tiver especificado n para pesquisas Anônimas no diretório LDAP, a autenticação LDAP não realizará a pesquisa anônima.

Ao criar a conta de usuário LDAP utilizando o Sentinel Control Center, especifique o *DN de Usuário do LDAP* para autenticação LDAP não anônima. É possível usar essa abordagem tanto para o eDirectory quanto para o Active Directory.

Para obter mais informações, consulte “Creating an LDAP User Account for Sentinel” (Criando uma conta de usuário LDAP para o Sentinel) no *Sentinel Rapid Deployment User Guide* (Guia do Usuário do Sentinel Rapid Deployment).

Além disso, para o Active Directory, existe uma abordagem alternativa para realizar a autenticação LDAP sem pesquisas anônimas. Para obter mais informações, consulte Autenticação LDAP não anônima usando o atributo UserPrincipalName no Active Directory.

Autenticação LDAP não anônima usando o atributo UserPrincipalName no Active Directory

Para o Active Directory, é possível também executar a autenticação LDAP sem pesquisas anônimas, utilizando o atributo userPrinicipalName:

1. Verifique se o atributo userPrinicipalName está definido como <*sAMAccountName@domain*> para o usuário do Active Directory.

   Para obter mais informações, consulte o Atributo User-Principal-Name (http://msdn.microsoft.com/en-us/library/ms680857(VS.85).aspx).

2. Você deve ter realizado da Etapa 1 na página 46 a Etapa 10 na página 47, e especificado `n` para "Pesquisas anônimas no diretório LDAP:" na página 46.

3. No Sentinel Server, edite a seção `LdapLogin` no arquivo `<Diretório de Instalação>/config/auth.login` :

   ```
   LdapLogin {
    com.sun.security.auth.module.LdapLoginModule required
    userProvider="ldap://LDAP server IP:636/DN of the Container that contains the user objects"
    authIdentity="{USERNAME}@Domain Name"
    userFilter="(&(sAMAccountName={USERNAME})(objectclass=user))"
    useSSL=true;
    };
   ```

   Por exemplo:

   ```
   LdapLogin {
    com.sun.security.auth.module.LdapLoginModule required
    userProvider="ldap://137.65.151.12:636/DC=Test-AD,DC=provo,DC=novell,DC=com"
    authIdentity="{USERNAME}@Test-AD.provo.novell.com"
    userFilter="(&(sAMAccountName={USERNAME})(objectclass=user))"
    useSSL=true;
    };
   ```

4. Reinicie o serviço do Sentinel:

   ```
   /etc/init.d/sentinel stop
   ```

   ```
   /etc/init.d/sentinel start
   ```

3.7.4 Configurando vários servidores LDAP para failover

Para configurar um ou mais servidores LDAP como servidores de failover para autenticação LDAP:

1. Você deve ter seguido da Etapa 2 na página 46 a Etapa 10 na página 47 para configurar o Sentinel Server para autenticação LDAP no servidor LDAP principal.
2. Efetue login no Sentinel Server como usuário `novell`.
3. Pare o serviço do Sentinel.

   ```
   /etc/init.d/sentinel stop
   ```

4. Mude para o diretório `<diretório_de_instalação>/config`:

   ```
   cd <diretório_de_instalação>/config
   ```

5 Abra o arquivo `auth.login` para edição.

```
vi auth.login
```

6 Atualize o `userProvider` na seção LdapLogin para especificar vários URLs LDAP. Separe cada URL com um espaço.

Por exemplo:

```
userProvider="ldap://ldap-url1 ldap://ldap-url2"
```

Para o Active Directory, verifique se a subárvore no URL LDAP não está em branco.

Para obter mais informações sobre como especificar vários URLs LDAP, consulte a descrição da opção `userProvider` em Class LdapLogin Module (http://java.sun.com/javase/6/docs/jre/api/security/jaas/spec/com/sun/security/auth/module/LdapLoginModule.html).

7 Grave as mudanças.

8 Exporte o certificado de cada servidor LDAP de failover e copie o arquivo de certificado para o diretório `<diretório_de_instalação>/config` no Sentinel Server.

Para obter mais informações, consulte "Exportando o certificado CA do servidor LDAP" na página 45.

9 Você deve ter definido a propriedade e as permissões necessárias do arquivo de certificado para cada servidor LDAP de failover.

```
chown novell:novell <diretório_de_instalação>/config/<arquivo-cert>
chmod 700 <diretório_de_instalação>/config/<arquivo-cert>
```

10 Adicione o certificado de cada servidor LDAP de failover ao keystore `ldap_server.keystore` criado na Etapa 8 da seção "Configurando o Sentinel Server para autenticação LDAP" na página 46.

```
<diretório_de_instalação>/jre64/bin/keytool -importcert -noprompt -
trustcacerts -file <arquivo-certificado> -alias <nome_álias> -keystore
ldap_server.keystore -storepass sentinel
```

Substitua `<arquivo-certificado>` pelo nome de arquivo do certificado LDAP em formato codificado com base64 e substitua `<nome_álias>` pelo nome do álias do certificado que será importado.

Importante: Você deve especificar o álias. Se nenhum álias for especificado, a ferramenta chave usará `mykey` como álias, por padrão. Quando você importa vários certificados para o keystore sem especificar um álias, a ferramenta chave relata um erro dizendo que o álias já existe.

---

11 Inicie o serviço do Sentinel.

```
/etc/init.d/sentinel start
```

O serviço não deverá se conectar ao servidor LDAP de failover se o Sentinel Server exceder o tempo de espera antes de reconhecer que o servidor LDAP principal está desativado. Para garantir a conexão do Sentinel Server com o servidor LDAP de failover sem exceder o tempo de espera:

1 Efetue login no Sentinel Server como usuário `root`.

2 Abra o arquivo `sysctl.conf` para edição:

```
vi /etc/sysctl.conf
```

3 Verifique se o valor `net.ipv4.tcp_syn_retries` está definido como 3. Se a entrada não existir, adicione-a. Grave o arquivo:

```
net.ipv4.tcp_syn_retries = 3
```

4 Execute o comando para que as mudanças entrem em vigor:

```
/sbin/sysctl -p
/sbin/sysctl -w net.ipv4.route.flush=1
```

5 Defina o valor de tempo de espera do Sentinel Server adicionando o parâmetro `-Desecurity.remote.timeout=60` a `control_center.sh` e `solution_designer.sh` no diretório `<diretório_de_instalação>/bin`:

control_center.sh:

```
"<diretório_de_instalação>/jre/bin/java" $MEMORY -
Dcom.esecurity.configurationfile=$ESEC_CONF_FILE -
Desecurity.cache.directory="<diretório_de_instalação>/data/
control_center.cache" -Desecurity.communication.service="sentinel_client"
-Dfile.encoding=UTF8 -Desecurity.dataobjects.config.file="/xml/
BaseMetaData.xml,/xml/WorkflowMetaData.xml,/xml/ActMetaData.xml" -
Djava.util.logging.config.file="<diretório_de_instalação>/config/
control_center_log.prop" -
Djava.security.auth.login.config="<diretório_de_instalação>/config/
auth.login" $SENTINEL_LANG_PROP $SENTINEL_CTRY_PROP -
Dice.pilots.html4.baseFontFamily="Arial Unicode MS" -
Desecurity.remote.timeout=60 -jar ../lib/console.jar
```

solution_designer.sh:

```
"<diretório_de_instalação>/jre/bin/java" -classpath $LOCAL_CLASSPATH
$MEMORY -Dcom.esecurity.configurationfile="$ESEC_CONF_FILE" -
Dsentinel.installer.jar.location="<diretório_de_instalação>/lib/
contentinstaller.jar" -Desecurity.communication.service="sentinel_client"
-Dfile.encoding=UTF8 -Desecurity.dataobjects.config.file="/xml/
BaseMetaData.xml,/xml/WorkflowMetaData.xml,/xml/ActMetaData.xml" -
Djava.util.logging.config.file="<diretório_de_instalação>/config/
solution_designer_log.prop" -
Djava.security.auth.login.config="<diretório_de_instalação>/config/
auth.login" $SENTINEL_LANG_PROP $SENTINEL_CTRY_PROP -
Desecurity.cache.directory=../data/solution_designer.cache -
Desecurity.remote.timeout=60
com.esecurity.content.exportUI.ContentPackBuilder
```

3.7.5 Configurando a autenticação LDAP para vários domínios do Active Directory

Se os usuários LDAP a serem autenticados estiverem em vários domínios do Active Directory, você poderá configurar o servidor Sentinel Rapid Deployment para autenticação LDAP da seguinte forma:

1 Verifique se você seguiu a Etapa 2 na página 46 até a Etapa 10 na página 47 para configurar o Sentinel Server para autenticação LDAP no controlador de domínio do Active Directory do primeiro domínio. Verifique também se você especificou `n` para "Pesquisas anônimas no diretório LDAP:" na página 46.

2 Efetue login no Sentinel Server como usuário `novell`.

3 Pare o serviço do Sentinel.

```
/etc/init.d/sentinel stop
```

4 Mude para o diretório `<diretório_de_instalação>/config`:

```
cd <diretório_de_instalação>/config
```

5 Abra o arquivo `auth.login` para edição.

```
vi auth.login
```

6 Edite a seção `LdapLogin` para especificar vários URLs LDAP, separando cada URL com um espaço em branco.

Por exemplo:

```
LdapLogin {
        com.sun.security.auth.module.LdapLoginModule required
        userProvider="ldap://<IP of the domain 1 domain controller>:636
ldap://<IP of the domain 2 domain controller>:636"
        authIdentity="{USERNAME}"
        useSSL=true;
};
```

Para obter mais informações sobre como especificar vários URLs LDAP, consulte a descrição da opção `userProvider` em Class LdapLogin Module (http://java.sun.com/javase/6/docs/jre/api/security/jaas/spec/com/sun/security/auth/module/LdapLoginModule.html).

7 Grave as mudanças.

8 Exporte o certificado do controlador de cada domínio e copie os arquivos de certificado para o diretório `<diretório_de_instalação>/config` no Sentinel Server.

Para obter mais informações, consulte "Exportando o certificado CA do servidor LDAP" na página 45.

9 Defina a propriedade e as permissões necessárias dos arquivos de certificado.

```
chown novell:novell <diretório_de_instalação>/config/<arquivo-cert>
```

```
chmod 700 <diretório_de_instalação>/config/<arquivo-cert>
```

10 Adicione cada certificado ao keystore `ldap_server.keystore` criado na Etapa 8 da seção "Configurando o Sentinel Server para autenticação LDAP" na página 46.

```
<diretório_de_instalação>/jre64/bin/keytool -importcert -noprompt -
trustcacerts -file <arquivo-certificado> -alias <nome_álias> -keystore
ldap_server.keystore -storepass sentinel
```

Substitua `<arquivo-certificado>` pelo nome de arquivo do certificado LDAP em formato codificado com base64 e substitua `<nome_álias>` pelo nome do álias do certificado que será importado.

Importante: Você deve especificar o álias. Se nenhum álias for especificado, a ferramenta chave usará `mykey` como álias, por padrão. Quando você importa vários certificados para o keystore sem especificar um álias, a ferramenta chave relata um erro dizendo que o álias já existe.

---

11 Inicie o serviço do Sentinel.

```
/etc/init.d/sentinel start
```

3.7.6 Efetuando login com as credenciais de usuário LDAP

Após configurar com êxito o Sentinel Server para autenticação LDAP, é possível criar contas de usuário LDAP do Sentinel no Sentinel Control Center. Para obter mais informações sobre como criar contas de usuário LDAP, consulte "Creating an LDAP User Account for Sentinel" (Criando uma conta de usuário LDAP para o Sentinel) no *Sentinel Rapid Deployment User Guide* (Guia do Usuário do Sentinel Rapid Deployment).

Após criar a conta de usuário LDAP, é possível efetuar login na interface do usuário da Web do Sentinel Rapid Deployment, no Sentinel Control Center e no Sentinel Solution Designer com o nome de usuário LDAP e a senha.

Observação: Para modificar uma configuração LDAP existente, execute o script `ldap_auth_config` novamente e especifique os novos valores para os parâmetros.

3.8 Atualizando a classificação da chave de licença de chave de avaliação para chave de produção

Se você adquirir o produto após a avaliação, siga o procedimento abaixo para atualizar sua chave de licença e evitar a reinstalação:

1. Efetue login na máquina em que o Sentinel Rapid Deployment está instalado como usuário do sistema operacional Administrador do Sentinel (o usuário padrão é `novell`).
2. No prompt de comando, mude o diretório para`<`*diretório_de_instalação*`>/bin`.
3. Digite o seguinte comando:

   ```
   ./softwarekey.sh
   ```

4. Especifique 1 para definir a chave primária. Pressione Enter.
5. Digite a nova chave de licença e siga as instruções na tela para sair após a atualização da chave de licença.

Fazendo upgrade do Sentinel Rapid Deployment

4

Esta seção apresenta informações sobre como fazer upgrade de uma versão existente do Sentinel Rapid Deployment para o patch mais recente.

Observação: Esse patch aplica-se apenas à instalação de 64 bits do Sentinel Rapid Deployment. A aplicação desse patch a um sistema demo de 32 bits faz com que a instalação não funcione.

- Seção 4.1, “Pré-requisitos” na página 53
- Seção 4.2, “Instalando o patch no servidor” na página 53
- Seção 4.3, “Fazendo upgrade do Gerenciador de Coletor e dos aplicativos clientes” na página 54

4.1 Pré-requisitos

- Verifique se o sistema que você está fazendo upgrade já tem instalado o Sentinel 6.1 Rapid Deployment SP1.
- Verifique se as tarefas do Gerenciador de Dados do Sentinel estão habilitadas para que a partição Online Atual nunca atinja P_MAX. Se ela atingir P_MAX e você adicionar as partições manualmente, o Sentinel Control Center não será iniciado com êxito.

4.2 Instalando o patch no servidor

1 Como usuário `novell`, efetue login no servidor em que o patch será instalado.

Antes de instalar o patch, faça backup do banco de dados do Sentinel, da pasta de configuração e da pasta de dados usando os seguintes comandos:

Banco de dados do Sentinel:

```
tar -cf backup.tar <diretório_de_instalação>/3rdparty/postgresql/
database_files
tar -cf backupdata.tar <diretório_de_instalação>/3rdparty/postgresql/data
```

Pasta de configuração:

```
tar -cf backupconfig.tar <diretório_de_instalação>/config
```

Pasta de dados:

```
tar -cf backupdata.tar <diretório_de_instalação>/data
```

Para obter mais informações sobre esses comandos, consulte File system level back up (http://www.postgresql.org/docs/8.1/static/backup-file.html) (Backup no nível do sistema de arquivos) no site do PostgreSQL na Web.

2 Faça backup da configuração do Gerenciamento de Fonte de Eventos (ESM) e crie uma exportação do ESM.

Para obter mais informações, consulte “Exporting a Configuration” (Exportando uma configuração) no *Sentinel Rapid Deployment User Guide* (Guia do Usuário do Sentinel Rapid Deployment).

3 Faça download do instalador de patch para o Sentinel Rapid Deployment a partir do Novell Patch Finder (http://download.novell.com/patch/finder/).

4 Copie o pacote do instalador descarregado para um diretório temporário.

5 Pare os serviços do Sentinel:

```
sentinel.sh stop
```

6 Especifique o seguinte comando para extrair os arquivos do pacote do instalador:

```
unzip <nome_de_arquivo_de_instalação>
```

Substitua <*nome_de_arquivo_de_instalação*> pelo nome real do arquivo do instalador.

7 Mude para o diretório no qual extraiu os arquivos do instalador:

```
cd <nome_diretório>
```

Substitua <*nome_diretório*> pelo nome real do diretório em que os arquivos foram extraídos.

8 Especifique o seguinte comando para aplicar o patch ao servidor, depois siga as instruções na tela:

```
./service_pack.sh
```

Após a instalação, os serviços do Sentinel são iniciados automaticamente.

9 Aplique o patch a todas as máquinas em que o Gerenciador de Coletor ou os Aplicativos Clientes (ou ambos) estiverem sendo executados.

4.3 Fazendo upgrade do Gerenciador de Coletor e dos aplicativos clientes

- Seção 4.3.1, “Fazendo upgrade do Gerenciador de Coletor” na página 54
- Seção 4.3.2, “Fazendo upgrade dos aplicativos clientes” na página 55

4.3.1 Fazendo upgrade do Gerenciador de Coletor

- “Linux” na página 54
- “Windows” na página 55

Linux

1 Efetue login na máquina do Gerenciador de Coletor do Sentinel Rapid Deployment como usuário `root`.

2 Faça download do instalador de patch para o Sentinel Rapid Deployment a partir do Novell Patch Finder (http://download.novell.com/patch/finder/).

3 Copie o arquivo do instalador descarregado para um diretório temporário.

4 Especifique o seguinte comando para extrair os arquivos do pacote zip do instalador:

```
unzip <nome_de_arquivo_de_instalação>
```

Substitua <*nome_arquivo_instalação*> pelo nome real do arquivo de instalação.

5 Mude para o diretório no qual extraiu os arquivos do instalador:

```
cd <nome_diretório>
```

Substitua <*nome_diretório*> pelo nome real do diretório em que os arquivos do instalador foram extraídos.

6 Pare os serviços do Gerenciador de Coletor.

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

7 Execute o instalador do service pack, depois siga as instruções na tela:

```
./service_pack.sh
```

Após a instalação, os serviços do Gerenciador de Coletor são iniciados automaticamente.

Windows

1 Efetue login na máquina do Gerenciador de Coletor do Sentinel Rapid Deployment como usuário admin.

2 Faça download do instalador de patch para o Sentinel Rapid Deployment a partir do Novell Patch Finder (http://download.novell.com/patch/finder/).

3 Copie o arquivo do instalador para um diretório temporário.

4 Extraia os arquivos do pacote do instalador.

5 Pare os serviços do Gerenciador de Coletor.

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

6 Navegue até o diretório no qual extraiu os arquivos do instalador.

7 Para executar o instalador, proceda de uma das seguintes maneiras:

- Clique duas vezes no arquivo `service_pack.bat`, depois siga as instruções na tela.
- No prompt de comando, execute o arquivo `service_pack.bat`, depois siga as instruções na tela.

Após a instalação, os serviços do Gerenciador de Coletor são iniciados automaticamente.

4.3.2 Fazendo upgrade dos aplicativos clientes

- “Linux” na página 55
- “Windows” na página 56

Linux

1 Como usuário `root`, efetue login na máquina em que os aplicativos Clientes do Novell Sentinel Rapid Deployment estão sendo executados.

2 Faça download do instalador de patch para o Sentinel Rapid Deployment a partir do Novell Patch Finder (http://download.novell.com/patch/finder/).

3 Copie o pacote do instalador descarregado para um diretório temporário.

4 Especifique o seguinte comando para extrair os arquivos do pacote do instalador:

```
unzip <nome_de_arquivo_de_instalação>
```

Substitua <*nome_arquivo_instalação*> pelo nome real do arquivo de instalação.

5 Mude para o diretório no qual extraiu os arquivos do instalador:

```
cd <nome_diretório>
```

Substitua <*nome_diretório*> pelo nome real do diretório em que os arquivos foram extraídos.

6 Execute o instalador, depois siga as instruções na tela:

```
./service_pack.sh
```

Windows

1. Efetue login como administrador na máquina em que os aplicativos Clientes do Novell Sentinel Rapid Deployment estão sendo executados.
2. Faça download do instalador de patch para o Sentinel Rapid Deployment a partir do Novell Patch Finder (http://download.novell.com/patch/finder/).
3. Copie o arquivo do instalador descarregado para um diretório temporário.
4. Extraia os arquivos do pacote do instalador.
5. Navegue até o diretório no qual extraiu os arquivos do instalador.
6. Para executar o instalador, proceda de uma das seguintes maneiras:
   - Clique duas vezes no arquivo `service_pack.bat`, depois siga as instruções na tela.
   - No prompt de comando, execute o arquivo `service_pack.bat`, depois siga as instruções na tela.

Considerações de segurança do Sentinel Rapid Deployment

5

Esta seção apresenta instruções específicas sobre como instalar, configurar e manter o Novell Sentinel Rapid Deployment de forma segura.

- Seção 5.1, “Proteção” na página 57
- Seção 5.2, “Protegendo a comunicação na rede” na página 58
- Seção 5.3, “Protegendo usuários e senhas” na página 60
- Seção 5.4, “Protegendo dados do Sentinel” na página 63
- Seção 5.5, “Fazendo backup de informações” na página 66
- Seção 5.6, “Protegendo o sistema operacional” na página 66
- Seção 5.7, “Vendo os eventos de auditoria do Sentinel” na página 67
- Seção 5.8, “Usando um certificado CA” na página 67

5.1 Proteção

- Seção 5.1.1, “Proteção out-of-the-box” na página 57
- Seção 5.1.2, “Protegendo os dados do Sentinel Rapid Deployment” na página 58

5.1.1 Proteção out-of-the-box

- Todas as portas desnecessárias são desativadas.
- Sempre que possível, uma porta de serviço escuta apenas as conexões locais e não permite conexões remotas.
- Os arquivos são instalados com o mínimo de privilégios para que apenas um pequeno número de usuários possa lê-los.
- Não são permitidas senhas padrão.
- Os relatórios no banco de dados são executados como um usuário que tenha apenas permissões selecionadas no banco de dados.
- Todas as interfaces da Web exigem HTTPS.
- Uma exploração de vulnerabilidade é executada no aplicativo, e todos os problemas potenciais de segurança são resolvidos.
- Por padrão, qualquer comunicação pela rede utiliza SSL e está configurada para autenticação.
- As senhas da conta do usuário são criptografadas por padrão quando armazenadas no sistema de arquivos ou no banco de dados.

5.1.2 Protegendo os dados do Sentinel Rapid Deployment

Devido à natureza altamente confidencial dos dados do Sentinel Rapid Deployment, você deve manter a máquina fisicamente protegida e em uma área segura da rede. Para coletar dados de fontes de eventos situadas fora da rede segura, use um Gerenciador de Coletor remoto. Para obter mais informações sobre Gerenciadores de Coletor remotos, consulte a “Seção 3.3, “Instalando o Gerenciador de Coletor e os aplicativos clientes” na página 35”.

5.2 Protegendo a comunicação na rede

A comunicação entre os diversos componentes do Sentinel Rapid Deployment é feita através da rede. Diferentes tipos de protocolos de comunicação são usados no sistema.

- Seção 5.2.1, “Comunicação entre processos do Sentinel Server” na página 58
- Seção 5.2.2, “Comunicação entre o Sentinel Server e os aplicativos clientes do Sentinel” na página 58
- Seção 5.2.3, “Comunicação entre o servidor e o banco de dados” na página 59
- Seção 5.2.4, “Comunicação entre os Gerenciadores de Coletor e as fontes de eventos” na página 60
- Seção 5.2.5, “Comunicação com os browsers da Web” na página 60
- Seção 5.2.6, “Comunicação entre o banco de dados e outros clientes” na página 60

5.2.1 Comunicação entre processos do Sentinel Server

Os processos do Sentinel Server incluem DAS Básico, DAS Binário, Mecanismo de Correlação, Gerenciador de Coletor e servidor Web. Esses processos se comunicam entre si por meio do ActiveMQ.

Por padrão, a comunicação entre esses processos do servidor é feita por SSL, por meio do barramento de mensagem do ActiveMQ. Para configurar o SSL, especifique as seguintes informações em `<Diretório_de_Instalação>/configuration.xml`:

```
<jms brokerURL="failover://(ssl://
localhost:61616?wireFormat.maxInactivityDuration=30000)?randomize=false"
interceptors="compression" keystore="../config/.activemqclientkeystore.jks"
keystorePassword="password" password="374d9f338b4dc4b50e45b3822fc6be12"
username="system"/>
```

Para mais informações sobre como configurar os certificados personalizados do cliente e do servidor, consulte “Processes” (Processos) no *Sentinel Rapid Deployment User Guide* (Guia do Usuário do Sentinel Rapid Deployment).

5.2.2 Comunicação entre o Sentinel Server e os aplicativos clientes do Sentinel

Os aplicativos Clientes do Sentinel, como o Sentinel Control Center (SCC), o Gerenciador de Dados do Sentinel (SDM) e o Designer de Soluções, por padrão, usam a comunicação SSL por meio do Servidor Proxy SSL.

Para habilitar a comunicação entre o Sentinel Server e o SCC, o SDM e o Designer de Soluções, quando são todos executados como aplicativos clientes no servidor, especifique as seguintes informações em <diretório_de_instalação>/configuration.xml:

```
<strategy active="yes" id="proxied_client"
location="com.esecurity.common.communication.strategy.proxystrategy.ProxiedCl
ientStrategyFactory">
   <transport type="ssl">
    <ssl host="localhost" keystore="<diretório_de_instalação>/config/
.proxyClientKeystore" port="10013" usecacerts="false"/>
   </transport>
  </strategy>
```

Para habilitar a comunicação entre o Sentinel Server e o SCC, o SDM e o Designer de Soluções executados no WebStart, a estratégia de comunicação é definida no servidor, no arquivo <*diretório_de_instalação*>/3rdparty/tomcat/webapps/ROOT/novellsiemdownloads/configuration.xml, conforme mostrado a seguir:

```
<strategy active="yes" id="proxied_client"
location="com.esecurity.common.communication.strategy.proxystrategy.ProxiedCl
ientStrategyFactory" >
   <transport type="ssl">
    <ssl host="127.0.0.1" port="10013" keystore="./.novell/sentinel/
.proxyClientKeystore" />
   </transport>
  </strategy>
```

Para mais informações sobre como configurar os certificados personalizados do cliente e do servidor, consulte "Processes" (Processos) no *Sentinel Rapid Deployment User Guide* (Guia do Usuário do Sentinel Rapid Deployment).

5.2.3 Comunicação entre o servidor e o banco de dados

O protocolo usado para a comunicação entre o servidor e o banco de dados é definido pelo driver JDBC. Alguns drivers são capazes de criptografar a comunicação com o banco de dados.

O Sentinel Rapid Deployment usa o driver PostgreSQL (postgresql-<versão>.jdbc3.jar) fornecido na Página de Download do PostgreSQL (http://jdbc.postgresql.org/download.html) para conectar-se ao banco de dados PostgreSQL, que é uma implementação do Java (Tipo IV). Esse driver suporta criptografia para comunicação de dados. Para configurar a criptografia para comunicação de dados, consulte as Opções de Criptografia do PostgreSQL (http://www.postgresql.org/docs/8.1/static/encryption-options.html).

Observação: A ativação da criptografia afeta o desempenho do sistema. Portanto, a comunicação do banco de dados não é criptografada por padrão. No entanto, isso não é uma preocupação de segurança, pois a comunicação entre o banco de dados e o servidor acontece pela interface de rede de loopback e não fica exposta à rede aberta.

5.2.4 Comunicação entre os Gerenciadores de Coletor e as fontes de eventos

É possível configurar o Sentinel Rapid Deployment para coletar dados com segurança de várias fontes de eventos. No entanto, a coleta de dados protegida é determinada por protocolos específicos suportados pela fonte de eventos. Por exemplo, o LEA de Ponto de Verificação, o Syslog e os Conectores de Auditoria podem ser configurados para criptografar sua comunicação com as fontes de eventos.

Para obter mais informações sobre os recursos de segurança que podem ser habilitados, consulte a documentação do fornecedor da fonte de eventos e do Conector que está no Site de Plug-ins do Novell Sentinel (http://support.novell.com/products/sentinel/secure/sentinelplugins.html).

5.2.5 Comunicação com os browsers da Web

Por padrão, o servidor Web é configurado para se comunicar via HTTPS. Para obter mais informações, consulte a documentação do Tomcat (http://tomcat.apache.org/tomcat-4.0-doc/ssl-howto.html).

5.2.6 Comunicação entre o banco de dados e outros clientes

Você pode configurar o banco de dados SIEM do PostgreSQL para conectar-se de qualquer máquina cliente usando o Gerenciador de Dados do Sentinel ou qualquer aplicativo de terceiros, como o Pgadmin.

Para permitir que o Gerenciador de Dados do Sentinel conecte-se de qualquer máquina cliente, adicione a seguinte linha ao arquivo `<Diretório_de_Instalação>/3rdparty/postgresql/data/pg_hba.conf`:

```
host    all         all         0.0.0.0/0             md5
```

Para limitar as conexões clientes que têm permissão para execução e conexão com o banco de dados pelo SDM, substitua a linha acima pelo endereço IP do host. A seguinte linha em `pg_hba.conf` indica ao PostgreSQL que as conexões da máquina local devem ser aceitas para que o Gerenciador de Dados do Sentinel tenha permissão para ser executado apenas no servidor.

```
host all all 127.0.0.1/32 md5
```

Para limitar as conexões de outras máquinas clientes, você pode incluir entradas `host` adicionais.

5.3 Protegendo usuários e senhas

- Seção 5.3.1, “Usuários do sistema operacional” na página 60
- Seção 5.3.2, “Usuários de bancos de dados e aplicativos do Sentinel” na página 61
- Seção 5.3.3, “Assegurando o uso obrigatório da política de senha pelos usuários” na página 62

5.3.1 Usuários do sistema operacional

- “Instalação do servidor” na página 61
- “Instalação do Gerenciador de Coletor” na página 61

Instalação do servidor

A instalação do servidor Sentinel Rapid Deployment cria um usuário e grupo de sistema que tem a propriedade dos arquivos instalados em *<diretório_de_instalação>*. Se o usuário não existir, ele será criado e o diretório pessoal será definido como *<diretório_de_instalação>*. Se um novo usuário for criado, sua senha não será definida por padrão, para aumentar a segurança. Para efetuar login no sistema como o usuário criado durante a instalação, defina uma senha para o usuário após a instalação.

Instalação do Gerenciador de Coletor

Os usuários do sistema podem variar de nível de segurança de acordo com o sistema operacional no qual foi instalado o Gerenciador de Coletor.

Linux: O instalador solicita que você especifique o nome do usuário do sistema que será o proprietário dos arquivos instalados, bem como a localização na qual será criado o diretório pessoal. Por padrão, o usuário do sistema é `esecadm`. No entanto, você pode mudar esse nome de usuário do sistema. Se o usuário não existir, ele será criado com seu respectivo diretório pessoal. Se um novo usuário for criado, sua senha não será definida durante a instalação, para aumentar a segurança. Para efetuar login no sistema como o usuário, defina uma senha para o usuário após a instalação. O grupo padrão é `esec`.

Durante a instalação do cliente, se o usuário já existir, o instalador não solicitará o usuário novamente. Esse comportamento é semelhante ao comportamento observado durante a desinstalação ou a reinstalação do software. No entanto, você pode fazer com que o instalador solicite o usuário novamente:

1. Apague o usuário e o grupo criados na primeira instalação
2. Limpe as variáveis do ambiente ESEC_USER de `/etc/profile`

Windows: Nenhum usuário é criado.

As políticas de senha dos usuários do sistema são definidas pelo sistema operacional que está sendo usado.

5.3.2 Usuários de bancos de dados e aplicativos do Sentinel

Os usuários de todos os aplicativos do Sentinel Rapid Deployment são usuários de bancos de dados nativos e suas senhas são protegidas por meio de procedimentos seguidos pela plataforma do banco de dados nativo. Esses usuários têm acesso apenas leitura a determinadas tabelas do banco de dados para que possam executar consultas no banco de dados.

O instalador cria e configura um banco de dados PostgreSQL com os seguintes usuários:

- **admin:** O usuário admin é o usuário administrador para login em todos os aplicativos do Sentinel.
- **dbauser:** O dbauser é criado como um superusuário capaz de gerenciar o banco de dados. A senha de dbauser é definida no momento da instalação do servidor Sentinel Rapid Deployment. Essa senha é armazenada em `<diretório pessoal do usuário>/.pgpass`. O sistema segue as políticas de senha do banco de dados PostgreSQL. Para obter mais informações, consulte Seção 5.3.3, “Assegurando o uso obrigatório da política de senha pelos usuários” na página 62.

- **appuser:** O appuser (não superusuário) é usado pelos aplicativos do Sentinel para conexão com o banco de dados. Por padrão, o appuser utiliza uma senha gerada aleatoriamente durante a instalação, que é armazenada e criptografada nos arquivos XML (`das_core.xml`, `das_binary.xml` e `advisor_client.xml`) no diretório <*diretório_de_instalação*>/config. Para mudar a senha do appuser, use o utilitário `<diretório_de_instalação>/bin/dbconfig`. Para obter mais informações, consulte "DAS Container Files" (Arquivos do container DAS) no *Sentinel Rapid Deployment Reference Guide* (Guia de Referência do Sentinel Rapid Deployment).

Observação: Há também um usuário do banco de dados PostgreSQL que é o proprietário de todo o banco de dados, inclusive das tabelas de banco de dados do sistema. Por padrão, o usuário do banco de dados PostgreSQL é definido como NOLOGIN. Dessa forma, ninguém pode efetuar login como o usuário PostgreSQL.

5.3.3 Assegurando o uso obrigatório da política de senha pelos usuários

O Sentinel Rapid Deployment utiliza mecanismos baseados em padrões para facilitar o uso obrigatório das políticas de senha.

O instalador cria e configura um banco de dados PostgreSQL com os seguintes usuários:

dbauser: O proprietário do banco de dados (usuário administrador do banco de dados). A senha é definida durante o processo de instalação.

appuser: Este é o usuário do aplicativo utilizado para efetuar login no banco de dados do Sentinel Rapid Deployment. A senha é gerada aleatoriamente durante o processo de instalação e destina-se apenas ao uso interno.

admin: É possível usar as credenciais de administrador para efetuar login na interface da Web do Sentinel Rapid Deployment. A senha é definida durante o processo de instalação.

Por padrão, as senhas de usuário são armazenadas no banco de dados PostgreSQL embutido no Sentinel Rapid Deployment. O PostgreSQL dispõe de uma opção para utilizar vários mecanismos de autenticação baseados em padrões, conforme descrito na seção Client Authentication (http://www.postgresql.org/docs/8.3/static/client-authentication.html) (Autenticação de cliente) da documentação do PostgresSQL.

O uso desses mecanismos afeta todas as contas de usuário no Sentinel Rapid Deployment, incluindo os usuários de aplicativo Web e as contas usadas apenas por serviços de back end, como `dbauser` e `appuser`.

Uma opção mais simples é usar o diretório LDAP para autenticar os usuários de aplicativo Web. Para habilitar essa opção no servidor Sentinel Rapid Deployment, consulte a Seção 3.7, "Autenticação LDAP" na página 44. Essa opção não tem efeito sobre as contas usadas pelos serviços de back end, que continuam a autenticação pelo PostgreSQL, exceto se você mudar as configurações do PostgreSQL.

Usando esses mecanismos baseados em padrões e os mecanismos existentes em seu ambiente, como o diretório LDAP, você pode atingir um alto nível de imposição da política de senha do Sentinel Rapid Deployment.

5.4 Protegendo dados do Sentinel

Importante: Devido à natureza altamente confidencial dos dados do Sentinel Server, você deve manter a máquina fisicamente protegida e em uma área segura da rede. Para coletar dados de fontes de eventos situadas fora da rede segura, use um Gerenciador de Coletor remoto.

Para determinados componentes, as senhas devem ser armazenadas de modo que estejam disponíveis quando o sistema precisar se conectar a um recurso, como o banco de dados ou uma fonte de eventos. Nesse caso, a senha é criptografada antes de ser armazenada, para impedir acesso não autorizado à senha não criptografada.

Mesmo quando a senha está criptografada, é muito importante garantir que o acesso aos dados da senha armazenada esteja protegido para evitar a exposição da senha. Por exemplo, é possível garantir que as permissões para arquivos com dados confidenciais não possam ser lidas por usuários não autorizados.

ARQUIVOS

`advisor_client.xml`

Credenciais de banco de dados

As credenciais de banco de dados estão armazenadas no arquivo `<diretório_de_instalação>/config/server.xml`

```
<class>esecurity.base.ccs.comp.dataobject.ConnectionManager</class>
    <property name="username">appuser</property>
    <property name="password">7fA+ogBMeK7cRbJ+S6xJ/
InLBUi+sRVGK5qYycDxfIqGDHVX9FApWg==</property>
```

Credenciais do Advisor

```
<obj-component id="DownloadComponent">
          <class>esecurity.ccs.comp.advisor.feed.NewAdvClientDownload</class>
      <property name="advisor.downloadfrom.url">https://secure-www.novell.com/
sentinel/advisor/advisordata</property>
      <property name="username">admin</property>
      <!-- Set the password (encrypted) using the adv_change_password script -
->
      <property name="password">jqhlWIX8HD6GDHVX9FApWg==</property>
<property name="compression.enabled">true</property>
      <!--
        Set the following properties to connect through an HTTP proxy.
       Set the proxy password (encrypted) using the adv_change_password script
(make a
        copy of the script and add "-x" to the java cmd line to set the proxy
password
        instead of the advisor password.
      -->
```

```
      <!--
      <property name="proxy_host"></property>
      <property name="proxy_port"></property>
      <property name="proxy_username"></property>
      <property name="proxy_password"></property>
      -->
        </obj-component>
```

Configuration.xml

```
<strategy active="yes" id="jms"
location="com.esecurity.common.communication.strategy.jmsstrategy.activemq.Ac
tiveMQStrategyFactory" name="ActiveMQ">
<jms brokerURL="failover://(ssl://
localhost:61616?wireFormat.maxInactivityDuration=30000)?randomize=false"
interceptors="compression" keystore="../config/.activemqclientkeystore.jks"
keystorePassword="password" password="374d9f338b4dc4b50e45b3822fc6be12"
username="system"/>
    </strategy>
```

das_binary.xml

```
<class>esecurity.base.ccs.comp.dataobject.ConnectionManager</class>
    <property name="username">appuser</property>
    <property name="password">7fA+ogBMeK7cRbJ+S6xJ/
InLBUi+sRVGK5qYycDxfIqGDHVX9FApWg==</property>
```

das_core.xml

```
 <class>esecurity.base.ccs.comp.dataobject.ConnectionManager</class>
    <property name="username">appuser</property>
    <property name="password">7fA+ogBMeK7cRbJ+S6xJ/
InLBUi+sRVGK5qYycDxfIqGDHVX9FApWg==</property>
```

Algumas tabelas de banco de dados armazenam senhas e certificados. Esses dados confidenciais são criptografados e armazenados nas tabelas listadas a seguir. Você deve limitar o acesso a essas tabelas.

- **evt_src:** dados da coluna evt_src_config
- **evt_src_collector:** colunas: evt_src_collector_props
- **evt_src_grp (dúvida):** colunas: evt_src_default_config
- **md_config:** coluna: data
- **integrator_config:** coluna: integrator_properties
- **md_view_config:** coluna: view_data
- **esec_content:** coluna: content_context, content_hash
- **esec_content_grp_content:** colunas: content_hash
- **sentinel_plugin:** colunas: content_pkg, file_hash

O Sentinel Rapid Deployment armazena dados de configuração e dados de evento. Esses dados são armazenados nos seguintes locais:

Componentes	Local de Dados de Configuração	Local de Dados de Evento
Servidor Sentinel Rapid Deployment	Tabelas de banco de dados e o sistema de arquivos (*<diretório_de_instalação>*/config) Essas informações de configuração incluem o banco de dados criptografado, a fonte de eventos, os integradores e as senhas.	Banco de dados (tabelas EVENTS, CORRELATED_EVENTS e EVT_SMRY_, AUDIT_RECORD) e o sistema de arquivos em *<Diretório_de_Instalação>*/data/eventdata e <*Diretório_de_Instalação*>/data/raw data Os dados de eventos podem ser arquivados no sistema de arquivos como parte da tarefa de gerenciamento de partição.
Mecanismo de Correlação	Sistema de arquivos (*<Diretório_de_Instalação>*/config). A única informação de configuração confidencial é o par de chaves do cliente usado na conexão com o barramento de mensagem.	correlation_engine.cache
DAS Básico	*<Diretório_de_Instalação>*/config	das_core.cache
DAS Binário	*<Diretório_de_Instalação>*/config	Os dados de eventos poderão ser armazenados em cache se o banco de dados estiver desativado. das_binary.cache
Gerenciador de Coletor	Sistema de arquivos (*<Diretório_de_Instalação>*/config). A única informação confidencial de configuração é a senha do usuário do Gerenciador de Coletor utilizada para conexão com o barramento de mensagem.	Em condições de erro, os dados de eventos poderão ser armazenados em cache no sistema de arquivos; por exemplo, se o barramento de mensagem estiver desativado ou se houver overflow de eventos. Esses dados de eventos são armazenados no diretório *<Diretório_de_Instalação>*/data/collector_mgr.cache.
Aplicativos clientes	Sistema de arquivos (*diretório_de_instalação*/config). Os aplicativos clientes não armazenam informações confidenciais nos arquivos de configuração. Por exemplo, os aplicativos clientes podem exportar os dados do ESM para um sistema de arquivos local. O arquivo exportado conterá senhas criptografadas se essas senhas estiverem presentes na configuração das fontes de eventos exportadas. Embora as senhas sejam criptografadas, a permissão de exportação do ESM só deverá ser concedida a usuários confiáveis.	Nenhuma

5.5 Fazendo backup de informações

- Faça backup dos eventos regularmente. A mídia de backup deve ser armazenada em um local externo seguro.
- Faça backup dos dados do sistema. Para obter mais informações, consulte "Backup and Restore Utility" (Utilitário de backup e restauração) no *Sentinel Rapid Deployment User Guide* (Guia do Usuário do Sentinel Rapid Deployment).
- No caso de dados confidenciais, use um dos seguintes métodos para criptografar o backup de dados:
  - Criptografe os dados propriamente ditos se o aplicativo que cria os dados suportar criptografia. Por exemplo, produtos de bancos de dados e ferramentas de terceiros suportam criptografia de dados. Use um software de backup que seja capaz de criptografar dados à medida que você faz backup. Esse método apresenta verificações de desempenho e de capacidade de gerenciamento, especialmente para o gerenciamento de chaves criptografadas.
  - Use uma aplicação de criptografia que criptografe mídia de backup confidencial à medida que o backup dos dados é feito.
- Se você transportar e armazenar mídia externamente, use uma empresa que seja especializada em transportar e armazenar mídia. Verifique se suas fitas são monitoradas por códigos de barras, se são armazenadas em condições ambientais favoráveis e se são gerenciadas por uma empresa que seja conhecida por gerenciar mídias adequadamente.
- Carregue Certificados de Recuperação. Por padrão, o serviço do Novell Sentinel não é configurado para o Agente de recuperação. Durante a configuração do servidor realizada pelo YaST, verifique se o caminho do Agente de recuperação está configurado. Esse caminho deve conter a lista de certificados que podem ser carregados pelo serviço e selecionados pelos usuários.

  Para obter mais informações, consulte "Certificate Management for Sentinel 6.1 Rapid Deployment Server" (Gerenciamento de certificado para o Servidor Sentinel 6.1 Rapid Deployment) no *Sentinel Rapid Deployment Reference Guide* (Guia de Referência do Sentinel Rapid Deployment).

  O YaST inclui módulos para o gerenciamento básico dos certificados X.509, que envolvem principalmente a criação de CAs, sub-CAs e seus certificados. Para obter mais informações sobre como gerenciar e atualizar certificados, consulte Managing X.509 Certification (http://www.novell.com/documentation/sles10/sles_admin/data/cha_yast_ca.html) (Gerenciando certificações X.509) no *SUSE Linux Enterprise Server 10 Installation and Administration Guide* (http://www.novell.com/documentation/sles10/sles_admin/data/bookinfo_book_sles_admin.html) (Guia de Instalação e Administração do SUSE Linux Enterprise Server 10).

5.6 Protegendo o sistema operacional

- O Sentinel Rapid Deployment é suportado no SUSE Linux Enterprise Server (SLES) 10 SP3 ou posterior. Para obter mais informações sobre como proteger a máquina SLES, consulte a documentação do SuSE Linux Enterprise Server 10 (http://www.novell.com/documentation/sles10/sles_admin/data/part_security.html).
- Proteja o acesso ao Sentinel Rapid Deployment Server com um firewall. Se o Sentinel Server puder ser acessado de fora da rede corporativa, use um firewall para impedir que um intruso tenha acesso direto.

Habilite as seguintes portas do firewall:

Componentes	Porta
ActiveMQ	61616
PostgreSQL	5432
Tomcat	8443
Porta do Cliente Proxy do Sentinel Control Center	10013
Cliente confiável com proxy	10014
internal_gateway_server e internal_gateway Usados entre mecanismo e gerenciador	5556
internal_router_server and internal_router_client Usado entre o cliente e o servidor do roteador de evento	5558
Porta de escuta do evento configurada em `config/collector_mgr.properties` como "`esecurity.agentmanager.event.port`"	35000

Observação: As portas marcadas com asterisco poderão ser diferentes se já estiverem em uso na hora da instalação. Se as portas estavam em uso na hora da instalação, substitua os números de porta que foram solicitados na instalação.

Para obter mais informações sobre como habilitar um firewall no SLES 10, consulte Configuring Firewalls with YaST (http://www.novell.com/documentation/sles10/sles_admin/data/sec_fire_suse.html) (Configurando firewalls com o YaST) no *SLES 10 Administration Guide* (Guia de Administração do SLES 10).

5.7 Vendo os eventos de auditoria do Sentinel

O Sentinel Rapid Deployment gera eventos de auditoria para diversas ações realizadas pelos usuários e também para ações realizadas internamente para atividades do sistema. Esses eventos podem ser vistos nas Telas Ativas ou acessados por meio de uma pesquisa ou de um relatório. No entanto, você deve ter as permissões necessárias para ver os eventos do sistema.

Para obter mais informações, consulte "System Events for Sentinel" (Eventos de sistema do Sentinel) no *Sentinel Rapid Deployment User Guide* (Guia do Usuário do Sentinel Rapid Deployment).

5.8 Usando um certificado CA

Você pode substituir o certificado autoassinado por um certificado assinado por uma autoridade de certificação (CA) reconhecida, como VeriSign, Thawte ou Entrust. Você também pode substituir o certificado autoassinado por um certificado assinado por uma CA menos comum, como uma CA de sua empresa ou organização.

Para obter mais informações, consulte "Certificate Management for Sentinel 6.1 Rapid Deployment Server" (Gerenciamento de certificado para o Sentinel 6.1 Rapid Deployment Server) no *Sentinel Rapid Deployment Reference Guide* (Guia de Referência do Sentinel Rapid Deployment).

Testando as funcionalidades do Sentinel Rapid Deployment

6

O Sentinel Rapid Deployment é instalado com um Coletor Generic que pode ser usado para testar muitas das funções básicas do sistema. É possível usar esse Coletor para testar telas do Active View, criação de incidentes, regras de correlação e relatórios.

- Seção 6.1, “Testando a instalação do Rapid Deployment” na página 69
- Seção 6.2, “Limpando após o teste” na página 81
- Seção 6.3, “Usando dados reais” na página 82

6.1 Testando a instalação do Rapid Deployment

O procedimento a seguir descreve as etapas para testar o sistema Sentinel Rapid Deployment e os resultados esperados. Talvez você não veja os mesmos eventos, mas seus resultados deverão ser semelhantes aos resultados abaixo.

No nível básico, esses testes permitem que você verifique se:

- Os serviços do Sentinel estão ativos.
- Se a comunicação pelo barramento de mensagem é funcional.
- Se os eventos internos de auditoria estão sendo enviados.
- So os eventos podem ser enviados de um Gerenciador de Coletor.
- Os eventos são inseridos no banco de dados e podem ser recuperados por meio de um relatório.
- Se os Incidentes podem ser criados e vistos.
- As regras são eventos avaliados e correlacionados acionados pelo Mecanismo de Correlação.
- O Gerenciador de Dados do Sentinel está conectado ao banco de dados e consegue ler as informações de partição.

Se um desses testes falhar, revise o registro de instalação e outros arquivos de registro e entre em contato com o Suporte Técnico da Novell (http://support.novell.com/phone.html?sourceidint=suplnav4_phonesup), se necessário.

Para testar a instalação:

1. Efetue login em uma interface da Web do Sentinel Rapid Deployment.

   Para obter mais informações, consulte “Accessing the Novell Sentinel Web Interface” (Acessando a interface da Web do Novell Sentinel) no *Sentinel Rapid Deployment User Guide* (Guia do Usuário do Sentinel Rapid Deployment).
2. Selecione a página Pesquisa e pesquise um evento interno. Provavelmente, serão retornados um ou mais eventos.

   Por exemplo, para pesquisar eventos internos na faixa de gravidade 3-5, selecione *Incluir Eventos do Sistema* e depois digite *sev:[3 TO 5]* no campo *Pesquisar*.

Para obter mais informações sobre Pesquisa, consulte “Running an Event Search” (Executando uma pesquisa de eventos) no *Sentinel Rapid Deployment User Guide* (Guia do Usuário do Sentinel Rapid Deployment).

Por padrão, o recurso Pesquisar não está habilitado no SP2. No entanto, para habilitá-lo, consulte “Enabling the Search Option in Web User Interface” (Habilitando a opção de pesquisa na interface do usuário da Web) no *Sentinel Rapid Deployment User Guide* (Guia do Usuário do Sentinel Rapid Deployment).

3 Selecione a página Relatórios, especifique os parâmetros e execute um relatório.

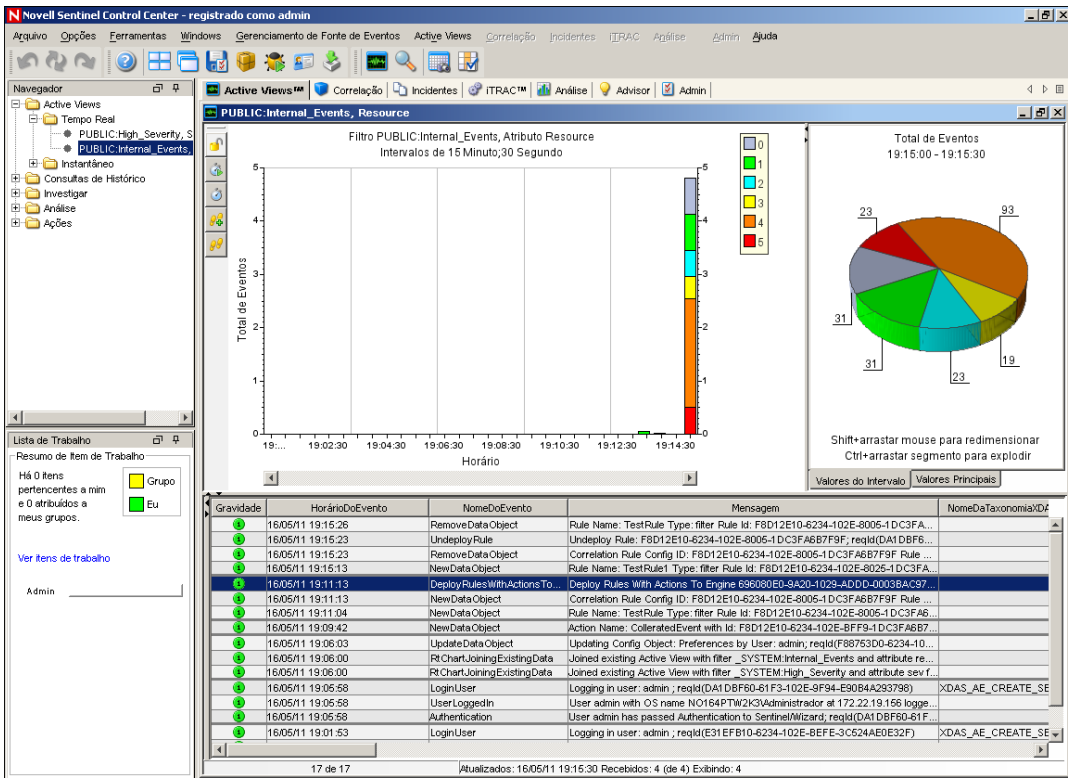
Por exemplo, clique no botão *Executar* ao lado da Configuração de Evento Básica do Sentinel, especifique os parâmetros desejados e clique em *Executar*.

Para obter mais informações, consulte “Running Reports” (Executando relatórios) no *Sentinel Rapid Deployment User Guide* (Guia do Usuário do Sentinel Rapid Deployment).

4 Na página Aplicativos, clique em *Iniciar o Sentinel Control Center*.

5 Efetue login no sistema utilizando o Usuário Administrativo do Sentinel especificado durante a instalação (o padrão é admin).

O Sentinel Control Center é aberto, e você pode ver a guia *Active Views* com os eventos filtrados pelos filtros públicos *Eventos_Internos* e *Gravidade_Alta*.



6 Vá para o menu *Gerenciamento de Fonte de Eventos* e selecione *Tela Ativa*.

7 Em Formato de Gráfico, clique o botão direito do mouse em *Fonte de Eventos de 5 eps* e selecione *Iniciar*.

8 Feche a janela Live View do Gerenciamento de Fonte de Eventos.

9 Clique na guia *Telas Ativas*.

É possível ver a janela Ativa intitulada PUBLIC: Gravidade_Alta, Gravidade. Pode levar algum tempo para que o Coletor seja iniciado e os dados sejam exibidos nessa janela.

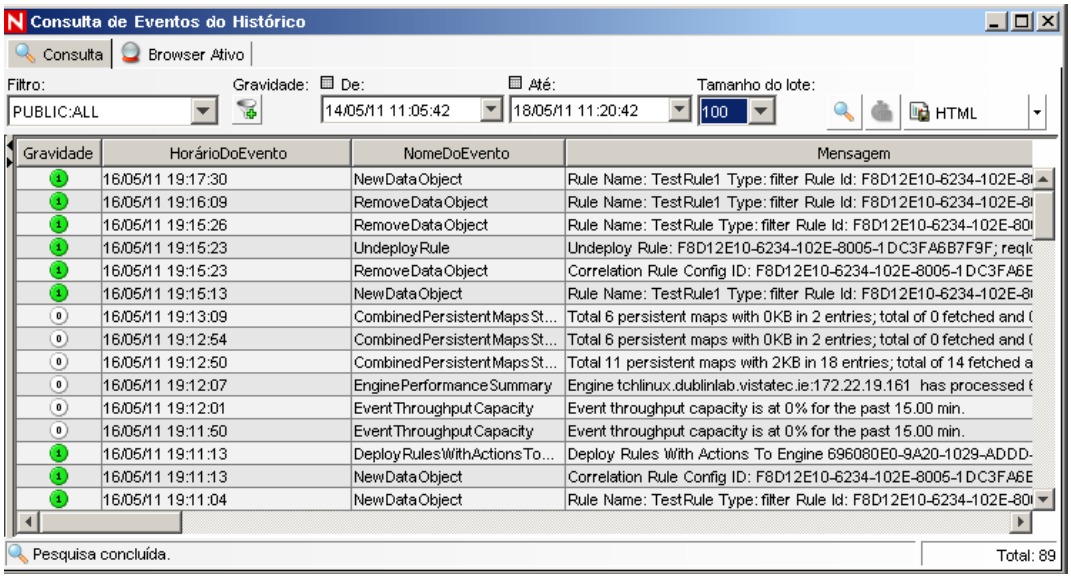
10 Clique no botão *Consulta de Eventos* na barra de ferramentas. A janela Consulta de Eventos do Histórico é exibida.

11 Na janela Consulta de Eventos do Histórico, clique na seta para baixo *Filtro* para selecionar o filtro. Selecione o filtro *Público: Todos*.

12 Selecione um período que abranja o horário em que o Coletor ficou ativo. Use as listas suspensas *De* e *Para* para selecionar a faixa de datas.

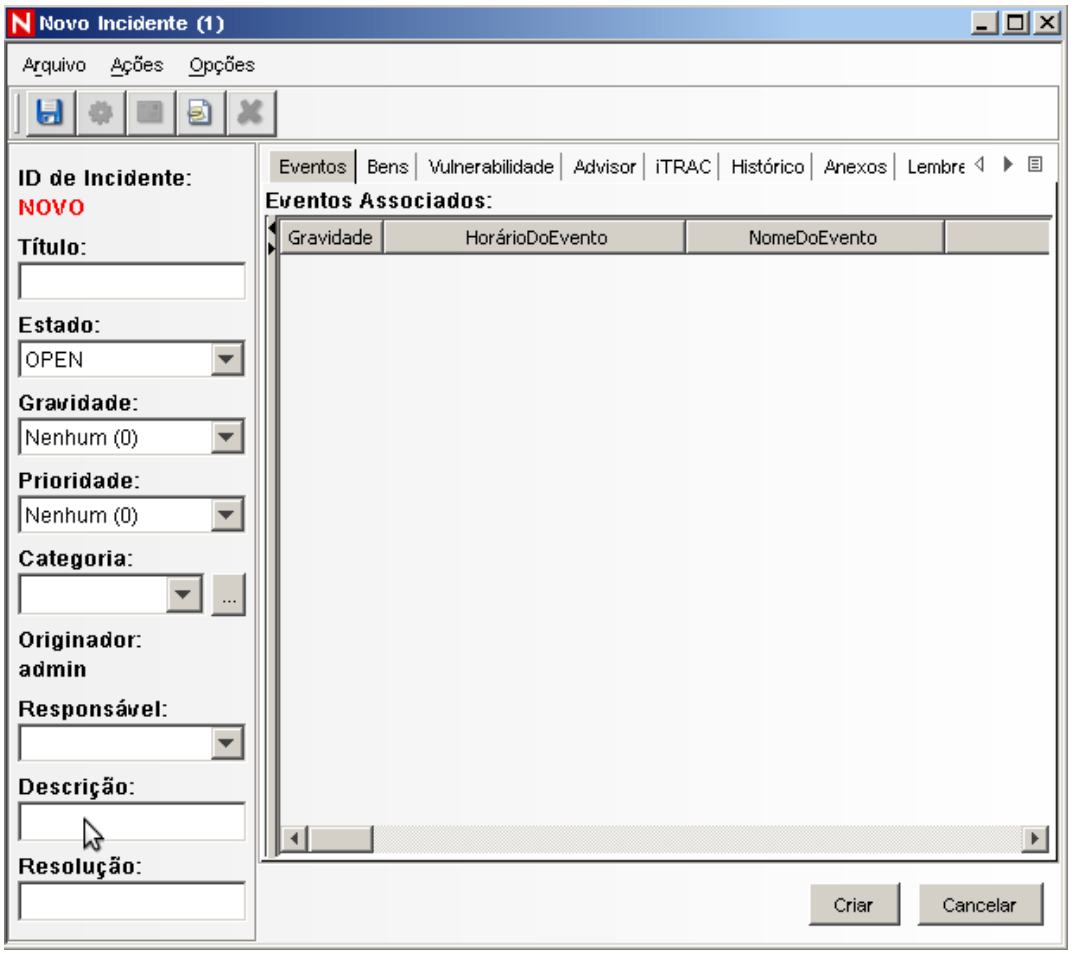
13 Selecione o tamanho do lote.

14 Clique no ícone da lupa para executar a consulta.



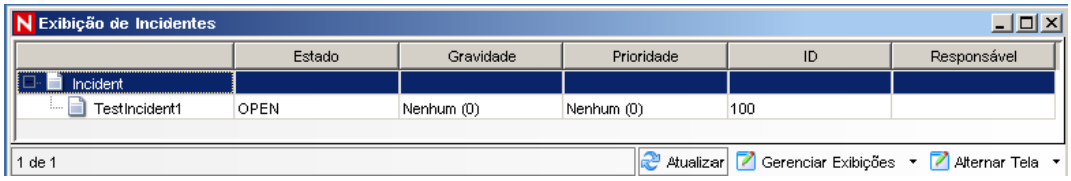
15 Mantenha a tecla Crtl ou Shift pressionada e selecione vários eventos na janela Consulta de Eventos do Histórico.

16 Clique o botão direito na janela e selecione *Criar Incidente* para exibir a janela Novo Incidente.

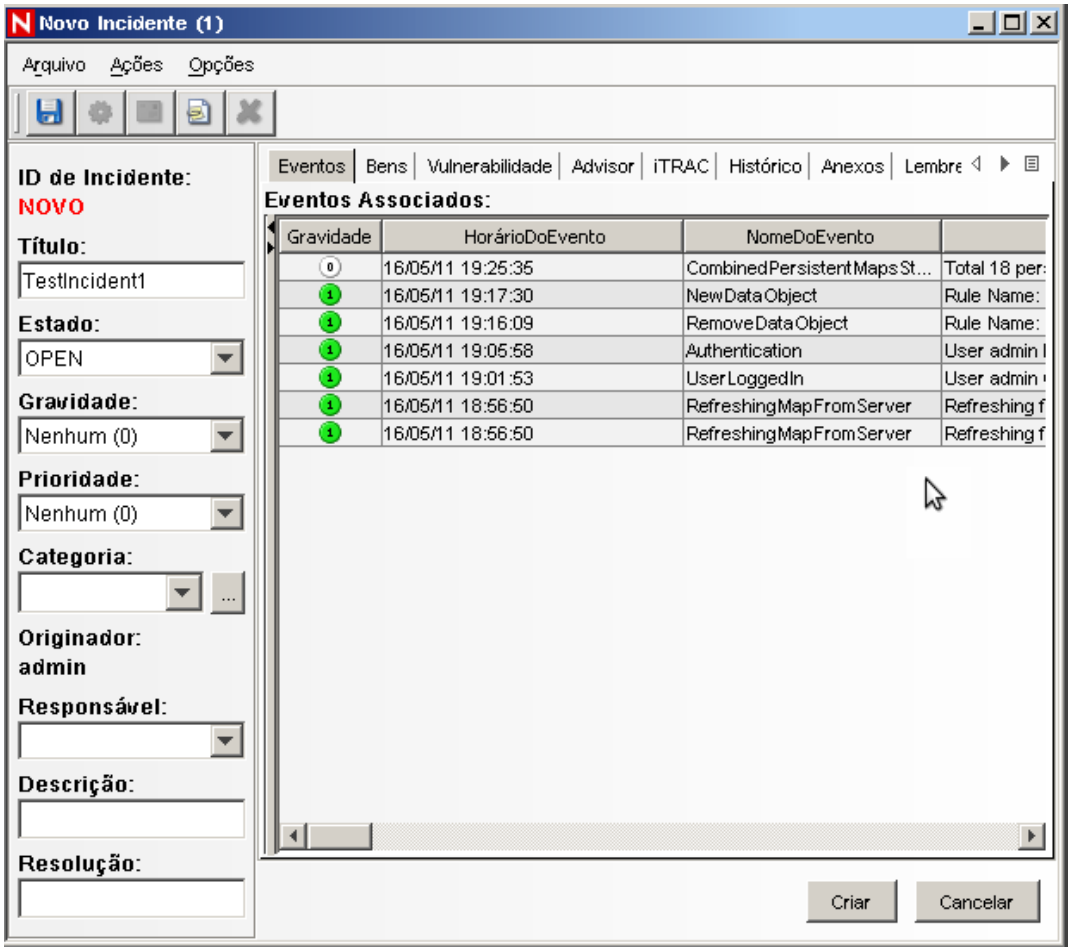


17 Nomeie o incidente como IncidentedeTeste1 e clique em *Criar*. Quando for exibida uma notificação de êxito, clique em *Gravar*.

18 Clique na guia *Incidente* para ver o incidente que você acabou de criar no Gerenciador de Tela de Incidente.



19 Clique duas vezes no incidente para exibir os eventos.



20 Feche a janela Incidente.

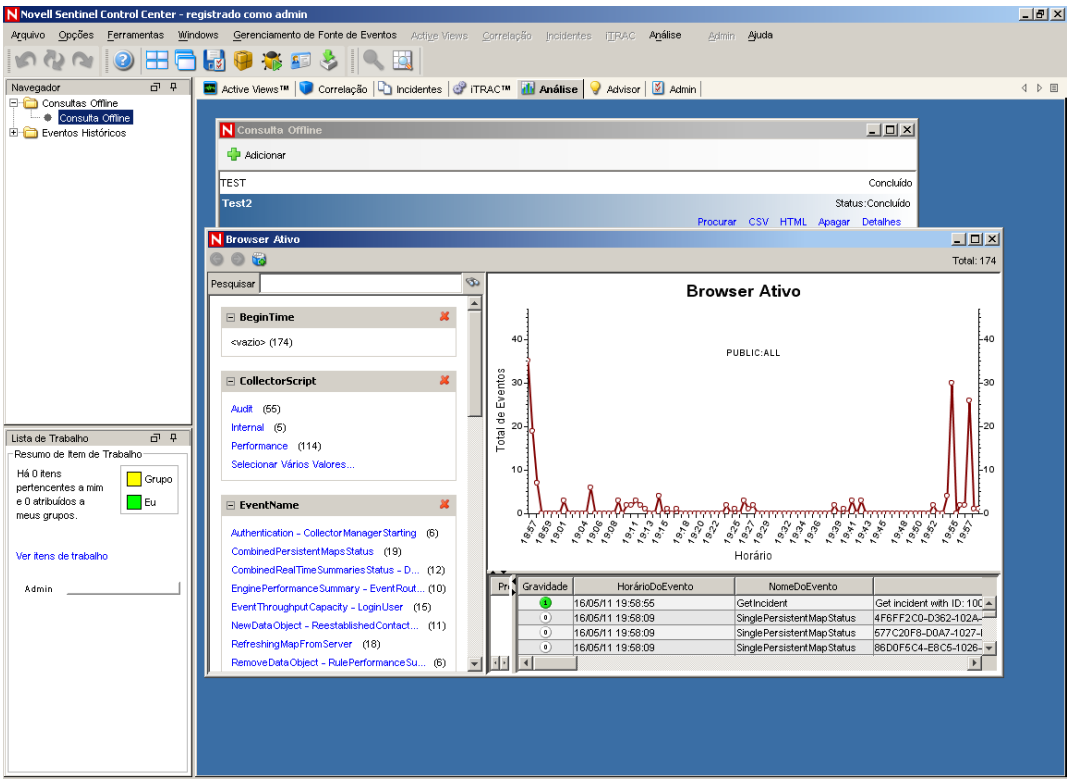
21 Clique na guia *Análise*.

22 Clique em *Consultas Offline* no menu *Análise* ou no Navegador.

23 Na janela Consulta Offline, clique em *Adicionar*.

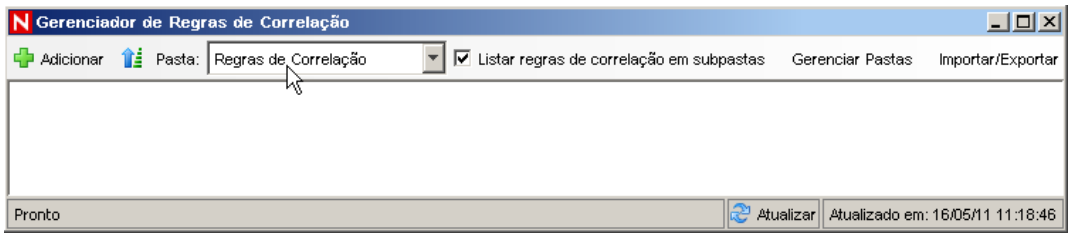
24 Especifique um nome, selecione um filtro, selecione um período e clique em *OK*.

25 Clique em *Procurar* para ver a lista de eventos e detalhes associados na janela Browser Ativo.



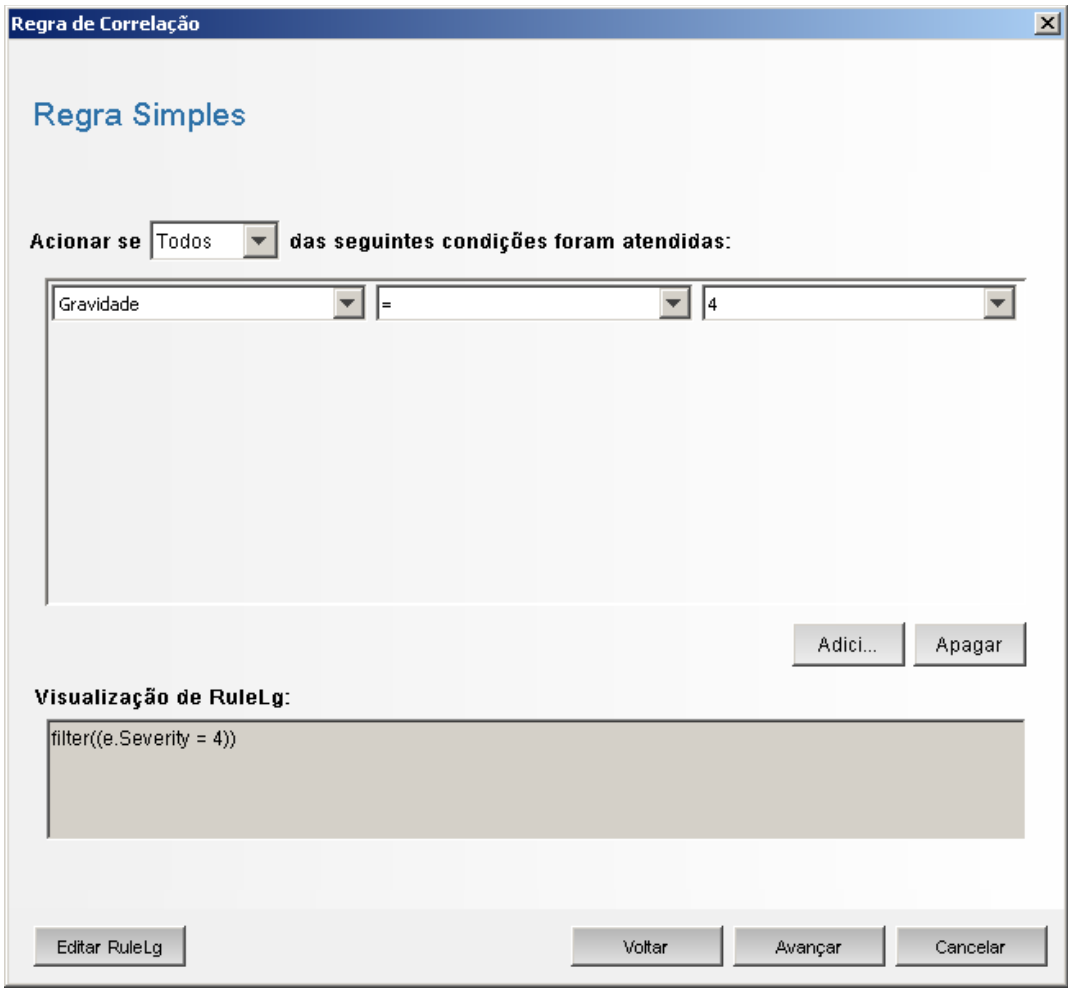
É possível ver detalhes como Coletor, IP de Destino, Gravidade, Porta de Serviço de Destino e Recurso.

26 Selecione a guia *Correlação*. O Gerenciador de Regras de Correlação é exibido.

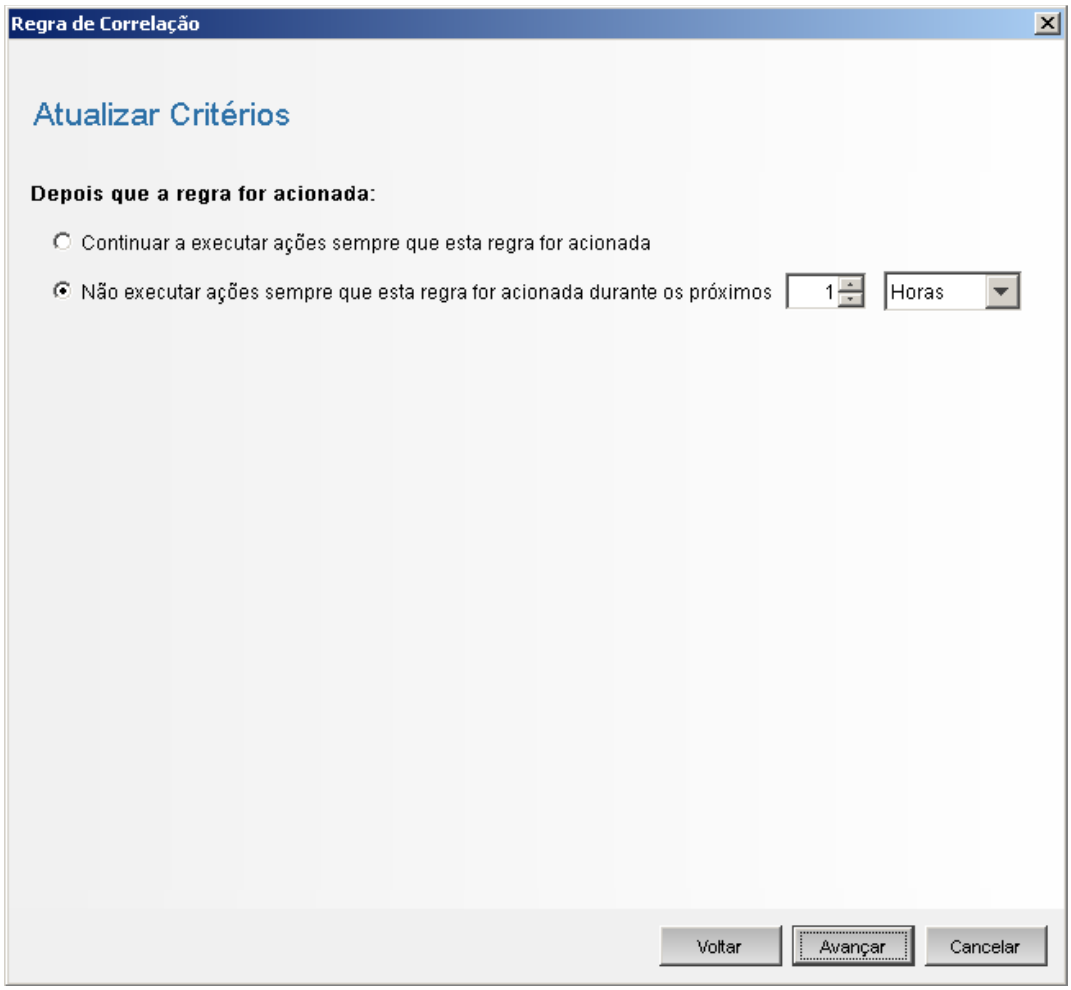


27 Clique em *Adicionar*. O Assistente de Regras de Correlação é exibido.

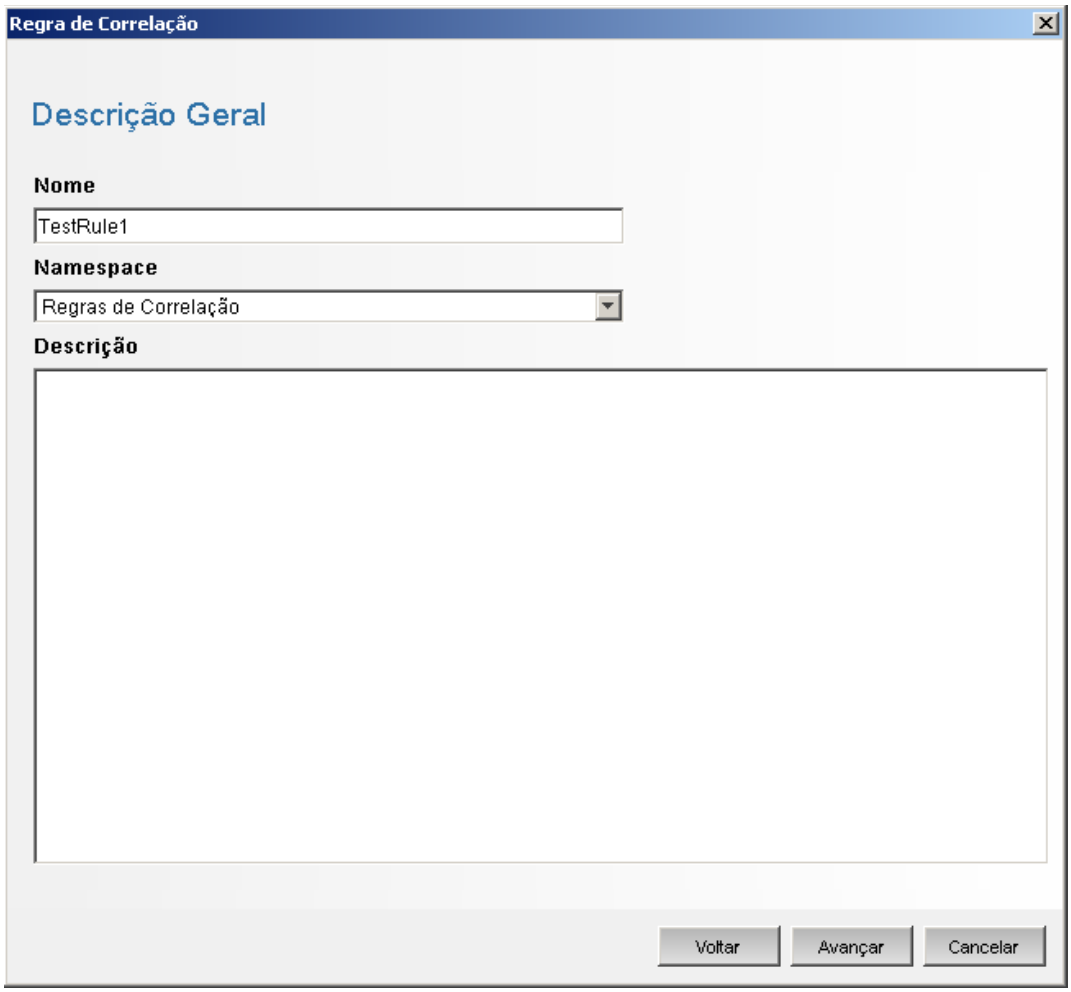
28 Clique em *Simples*. A janela Regra Simples é exibida.



29 Use os menus suspensos para definir os critérios como Gravidade=4, depois clique em *Avançar*. A janela Atualizar Critérios é exibida.



30 Selecione *Não executar ações sempre que esta regra for acionada durante os próximos*, use o menu suspenso para definir o período como 1 minuto, depois clique em *Avançar*. A janela Descrição Geral é exibida.



31 Nomeie a regra como *RegradeTeste1*, insira uma descrição e clique em *Avançar*.

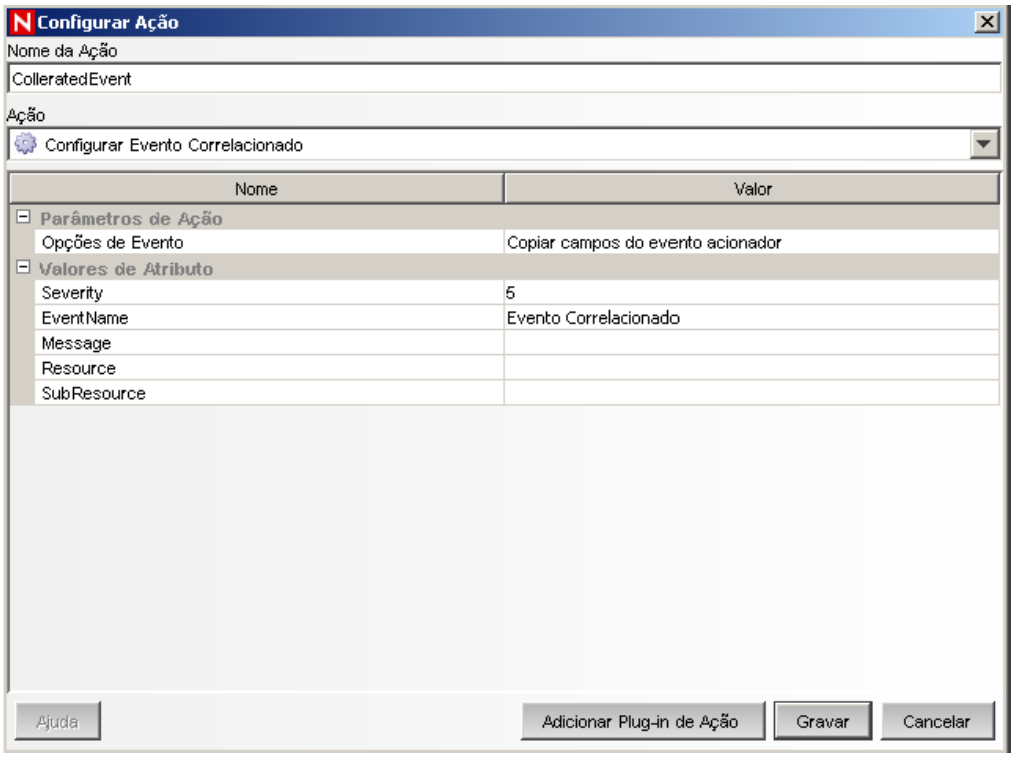
32 Selecione *Não, não criar outra regra* e clique em *Avançar*.

33 Crie uma ação para associar à regra criada:

33a Execute um dos seguintes procedimentos:

- Selecione *Ferramentas* > *Gerenciador de Ações* > *Adicionar*.
- Na janela Distribuir Regra, clique em *Adicionar Ação*. Para obter mais informações, consulte da Etapa 34 a Etapa 35 na página 79.

A janela Configurar Ação é exibida.



33b Na janela Configurar Ação, faça o seguinte:

- Especifique o nome da ação, como a Ação EventoCorrelacionado.
- Selecione *Configurar Evento Correlacionado* na lista suspensa *Ação*.
- Defina as *Opções de Evento*.
- Defina a *Gravidade* como 5.
- Especifique o *NomeDoEvento*, como EventoCorrelacionado.
- Especifique uma mensagem, se necessário.

Para obter mais informações sobre como criar uma ação, consulte "Creating Actions" (Criando ações) no *Sentinel Rapid Deployment User Guide* (Guia do Usuário do Sentinel Rapid Deployment).

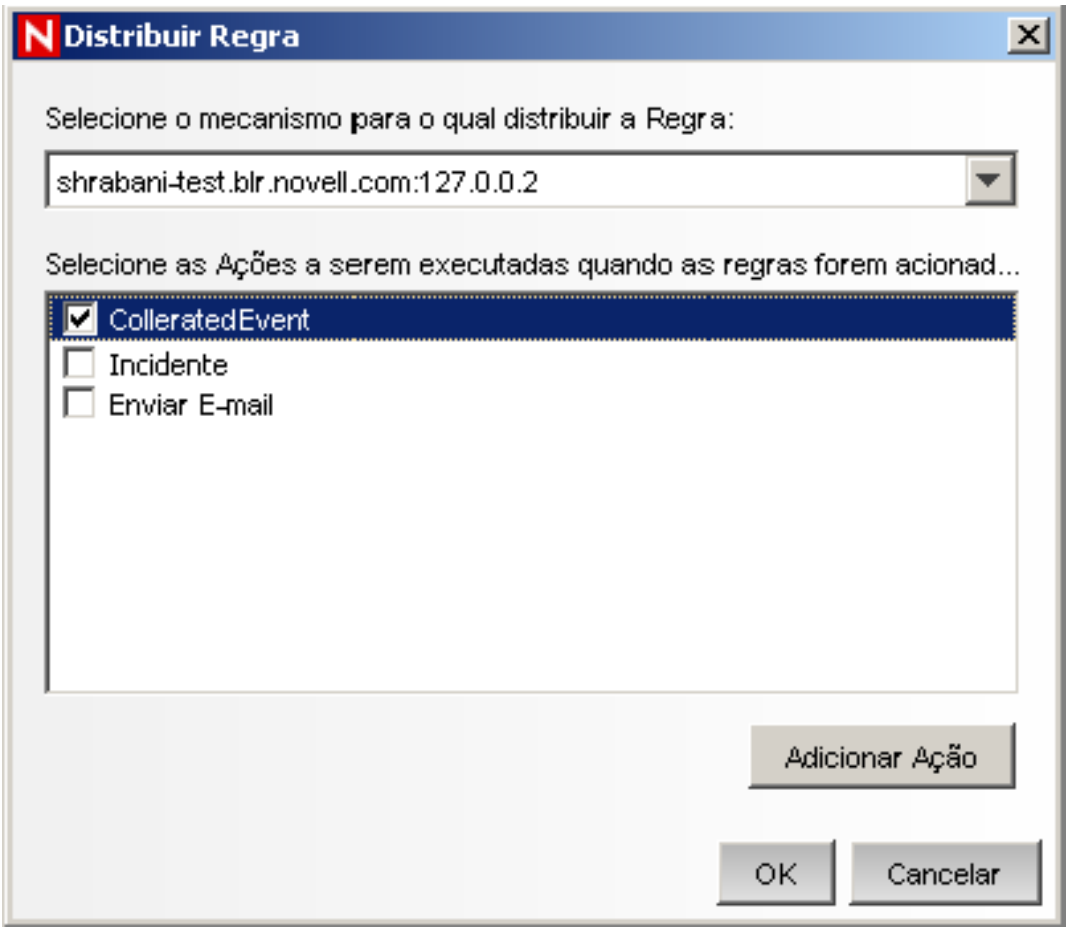
33c Clique em *Gravar*.

34 Abra a janela do Gerenciador da Regra de Correlação.

35 Selecione uma regra e clique no link *Distribuir Regras*. A janela Distribuir Regra é exibida.

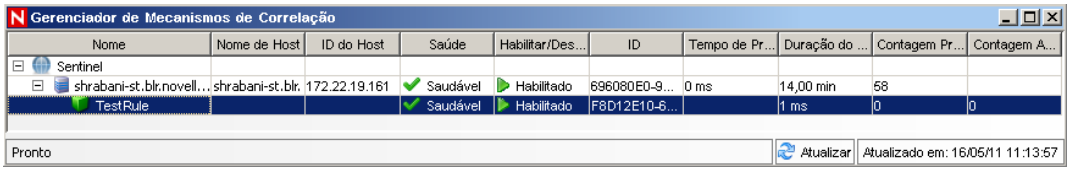
36 Na janela Distribuir Regra, selecione um Mecanismo para implantar a regra.

37 Selecione a ação que você criou na Etapa 33 na página 78 para associar à regra, depois clique em *OK*.



38 Selecione *Gerenciador de Mecanismos de Correlação*.

Em Mecanismo de Correlação, você vê a regra implantada e habilitada.



39 Acione um evento de gravidade 4, como uma autenticação com falha, para disparar a regra de correlação implantada.

Por exemplo, abra a janela de login do Sentinel Control Center e especifique credenciais de usuário incorretas para gerar um evento desse tipo.

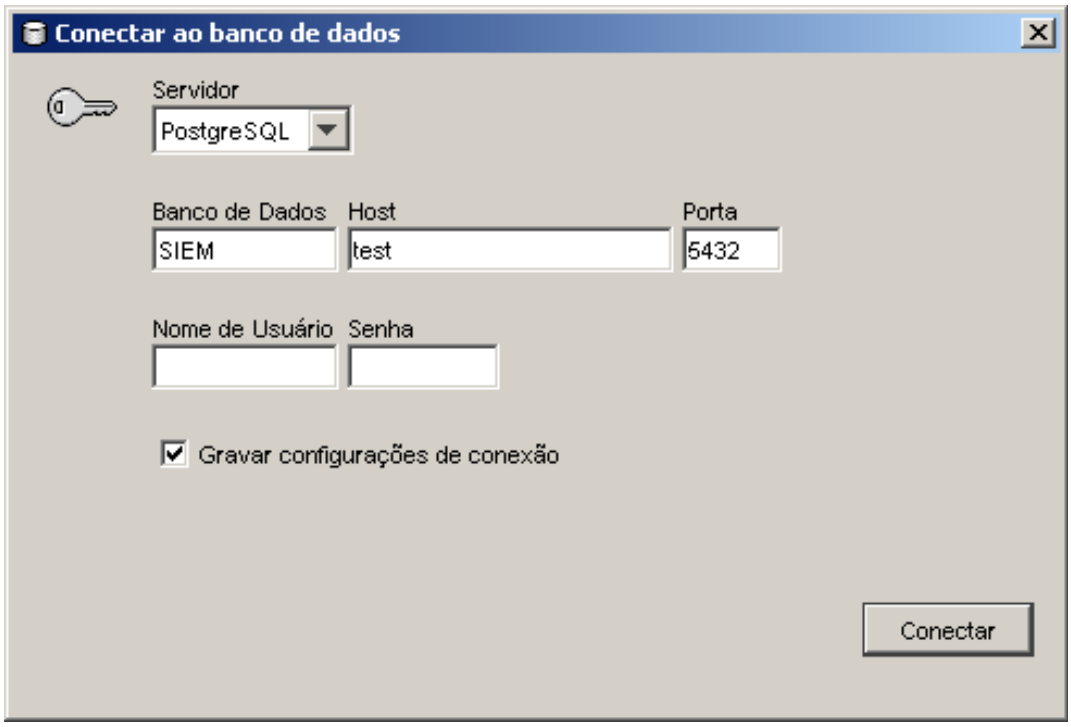
40 Clique na guia *Active Views* e verifique se o Evento Correlacionado foi gerado.

Gravidade	HorárioDoEvento	NomeDoEvento	Mensagem	NomeDaTaxonomiaXDAST
1	16/05/11 19:01:53	LoginUser	Logging in user: admin ; reqId(E31EFB10-6234-102E-BEFE-3C524AE0E32F)	XDAS_AE_CREATE_SESSI..
1	16/05/11 19:01:53	UserLoggedIn	User admin with OS name null at null logged in; currently 1 active users; reqId(E...	
1	16/05/11 19:01:53	Authentication	User admin has passed Authentication to SentinelWizard; reqId(E31EFB10-623...	

41 Feche o Sentinel Control Center.

42 Na página Aplicativos, clique em *Iniciar o Gerenciador de Dados do Sentinel*.

43 Efetue login no Gerenciador de Dados do Sentinel usando o Usuário Administrativo de Banco de Dados especificado durante a instalação (por padrão, dbauser).



44 Clique em cada guia para verificar se você pode acessá-la.

45 Feche o Gerenciador de Dados do Sentinel.

Se puder executar todas essas etapas sem erros, você concluiu uma verificação básica da instalação do sistema Sentinel.

6.2 Limpando após o teste

Depois de concluir a verificação do sistema, você deve remover os objetos criados para os testes.

1 Efetue login no sistema utilizando o Usuário Administrativo do Sentinel especificado durante a instalação (o padrão é admin).

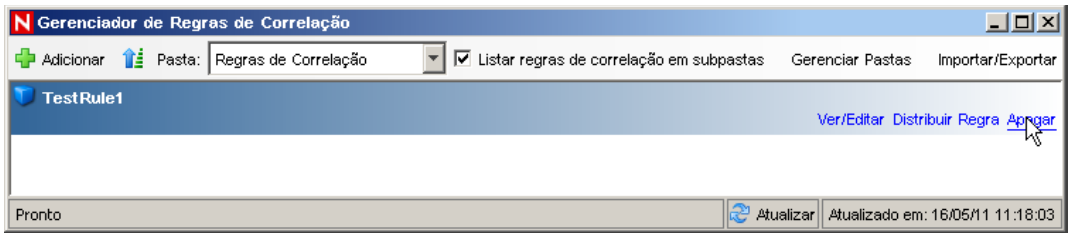
2 Selecione a guia *Correlação*.

3 Abra o Gerenciador do Mecanismo de Correlação.

4 Clique o botão direito do mouse em *RegradeTeste1* no Gerenciador de Mecanismos de Correlação, depois selecione *Desabilitar*.

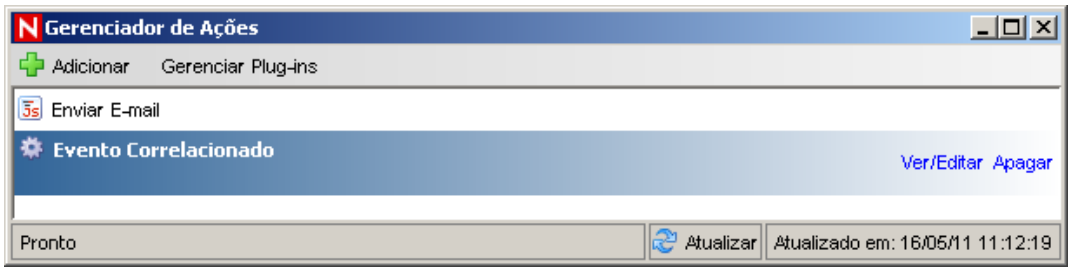
5 Abra o Gerenciador do Mecanismo de Correlação.

6 Selecione *RegradeTeste1* e clique em *Apagar*.



7 Selecione *Ferramentas* > *Gerenciador de Ações* para exibir a janela Gerenciador de Ações.

8 Selecione a ação *EventoCorrelacionado*, clique em *Apagar* e depois em *Sim* para confirmar a exclusão.



9 Selecione o menu *Gerenciamento de Fonte de Eventos* e depois selecione *Tela Ativa*.

10 Na hierarquia gráfica de fontes de eventos, clique o botão direito do mouse em *Coletor Geral*, depois selecione *Parar*.

11 Feche a janela Gerenciamento de Fonte de Eventos.

12 Clique na guia *Incidentes*.

13 Abra o Gerenciador da Tela Incidente.

14 Selecione *IncidentedeTeste1*, clique o botão direito do mouse e selecione *Apagar*.

6.3 Usando dados reais

Para começar a utilizar dados reais, você precisa importar e configurar os Coletores apropriados para seu ambiente, configurar suas próprias regras, criar workflows do iTRAC, e assim por diante. Para obter mais informações, consulte o *Sentinel Rapid Deployment User Guide* (Guia do Usuário do Sentinel Rapid Deployment). Os Sentinel Solution Packs podem ajudar você a começar rapidamente. Consulte a Página de Conteúdo do Sentinel (http://support.novell.com/products/sentinel/sentinel61.html) para ver mais detalhes.

Desinstalando o Sentinel Rapid Deployment 7

- Seção 7.1, “Desinstalando o Sentinel Rapid Deployment Server” na página 83
- Seção 7.2, “Desinstalando o Gerenciador de Coletor Remoto e os Aplicativos Clientes do Sentinel” na página 83

7.1 Desinstalando o Sentinel Rapid Deployment Server

1. Efetue login como usuário `root`.
2. Mude para o diretório `setup`.

   `cd <diretório_de_instalação>/setup`
3. Execute o script `uninstall.sh` para desinstalar o servidor Sentinel Rapid Deployment:

   `./uninstall.sh`

   O script exibe uma mensagem informando que o Sentinel Rapid Deployment será completamente removido.
4. Especifique se vai manter ou remover o usuário durante a desinstalação do servidor Sentinel Rapid Deployment. Pressione `y` para remover o usuário ou `n` para mantê-lo.
5. Especifique se vai manter ou remover o grupo durante a desinstalação do servidor Sentinel Rapid Deployment. Pressione `y` para remover o grupo ou `n` para mantê-lo.
6. Digite `y` para desinstalar ou `n` para sair da desinstalação.

7.2 Desinstalando o Gerenciador de Coletor Remoto e os Aplicativos Clientes do Sentinel

- Seção 7.2.1, “Linux” na página 83
- Seção 7.2.2, “Windows” na página 84
- Seção 7.2.3, “Procedimentos de pós-desinstalação” na página 84

7.2.1 Linux

1. Efetue login como `root`.
2. (Condicional) Se estiver desinstalando o Gerenciador de Coletor, pare os serviços do Sentinel Rapid Deployment:

   `<diretório_de_instalação>/bin/sentinel.sh stop`
3. Vá para o seguinte local:

   `<diretório_de_instalação>/_uninst`
4. Proceda de uma das seguintes maneiras:

Modo	Comando
GUI	`./uninstall.bin` Continue na Etapa 5 na página 84.
Console	`./uninstall.bin -console` Continue seguindo as instruções na tela.

5 Selecione um idioma e clique em *OK*.

6 No Assistente do Sentinel UninstallShield, clique em *Avançar*.

7 Selecione os componentes a serem desinstalados e clique em *Avançar*.

8 Pare todos os aplicativos do Sentinel que estiverem em execução e clique em *Avançar*.

Será exibido um resumo dos recursos selecionados para desinstalação.

9 Clique em *Desinstalar*.

10 Clique em *Concluir*.

7.2.2 Windows

1 Efetue login como usuário Administrador.

2 (Condicional) Se estiver desinstalando o Gerenciador de Coletor, pare os serviços do Sentinel Rapid Deployment:

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

3 Execute um destes procedimentos:

- Selecione *Iniciar* > *Todos os Programas* > *Sentinel* > *Desinstalar Sentinel*.
- Selecione *Iniciar* > *Executar*, digite `<diretório_de_instalação>\_uninst`, depois clique duas vezes em `uninstall.exe`.

4 Selecione um idioma e clique em *OK*.

O Assistente UninstallShield do Sentinel Rapid Deployment é exibido.

5 Clique em *Avançar*.

6 Selecione os componentes a serem desinstalados e clique em *Avançar*.

7 Pare todos os aplicativos do Sentinel que estiverem em execução e clique em *Avançar*.

Será exibido um resumo dos recursos selecionados para desinstalação.

8 Clique em *Desinstalar*.

9 Reinicialize o sistema e clique em *Concluir*.

7.2.3 Procedimentos de pós-desinstalação

Depois que você desinstalar os aplicativos, algumas configurações do sistema permanecerão e deverão ser removidas manualmente. Remova essas configurações antes de executar uma instalação limpa do Sentinel, particularmente se ocorrerem erros na desinstalação do programa.

Observação: No Linux, a desinstalação do Gerenciador de Coletor e dos Aplicativos Clientes não remove o Usuário Administrador do Sentinel do sistema operacional. Se desejar remover esse usuário, você deverá fazê-lo manualmente.

- "Linux" na página 85
- "Windows" na página 85

Linux

1. Efetue login como `root`.
2. Remova o conteúdo de `<diretório_de_instalação>` no qual o software do Sentinel está instalado.
3. Remova os seguintes arquivos do diretório `/etc/init.d`, caso eles existam:

   `sentinel`

   Isso só será aplicável se o Gerenciador de Coletor estiver instalado.
4. Garanta que não haja ninguém registrado como Administrador do Sentinel (o padrão é esecadm). Em seguida, remova o usuário, o diretório pessoal e o grupo esec:
   - Execute `userdel -r esecadm`
   - Execute `groupdel esec`
5. Remova o diretório `/root/InstallShield`.
6. Remova a seção InstallShield de `/etc/profile`.
7. Reinicie a máquina.

Windows

1. Apague a pasta `%CommonProgramFiles%\InstallShield\Universal` e todo o seu conteúdo.
2. Apague a pasta `<diretório_de_instalação>` (por padrão: `C:\Arquivos de Programas\Novell\Sentinel6`).
3. Clique o botão direito do mouse em *Meu Computador* > *Propriedades* > *guia Avançado*.
4. Clique no botão *Variáveis de Ambiente*.
5. Exclua as seguintes variáveis, se elas existirem:
   - ESEC_HOME
   - ESEC_VERSION
   - ESEC_JAVA_HOME
   - ESEC_CONF_FILE
   - WORKBENCH_HOME
6. Remova quaisquer entradas na variável de ambiente CAMINHO que apontam para a instalação do Sentinel.
7. Apague todos os atalhos do Sentinel da área de trabalho.
8. Apague a pasta de atalhos *Iniciar* > *Programas* > *Sentinel* do menu *Iniciar*.
9. Reinicie a máquina.

Atualizando o nome de host do Sentinel Rapid Deployment

A

- Seção A.1, “Servidor” na página 87
- Seção A.2, “Aplicativos clientes” na página 87

A.1 Servidor

No Sentinel Server, as mudanças feitas no nome de host são atualizadas automaticamente no tempo de execução ou durante a instalação. Se o servidor não funcionar corretamente depois de uma atualização de nome de host, verifique manualmente se:

- Todos os arquivos `jnlp` e o arquivo `configuration.xml` foram atualizados no reinício do Sentinel.
- A entrada do nome de host na tabela de banco de dados `sentinel_host` foi atualizada.
- Todas as referências ao loop local (localhost ou 127.0.0.1) do arquivo `<diretório_de_instalação>/config/configuration.xml` permanecem inalteradas.

A.2 Aplicativos clientes

Em aplicativos clientes, você deve mudar manualmente o nome de host ou o endereço IP do servidor nos seguintes locais para apontar para o servidor correto:

- `<diretório_de_instalação>/config/configuration.xml`.

  O Sentinel Control Center e o Designer de Soluções usam essas informações.
- O URL da Ajuda que consta no arquivo `<diretório_de_instalação>/config/SentinelPreferences.properties`.
- Execute o seguinte comando para atualizar o nome de host no arquivo `sdm.connect`:

  ```
  sdm -action saveConnection -server <postgresql> -host <hostIpaddress/
  hostName> -port <portnum> -database <databaseName/SID> [-driverProps
  <propertiesFile] {-user <dbUser> -password <dbPass> | -winAuth} -
  connectFile <filenameToSaveConnection>
  ```

Dicas para solução de problemas

B

Esta seção contém uma lista de sugestões de solução de problemas que poderá ajudar você a resolver alguns dos problemas de instalação do Sentinel Rapid Deployment.

- Seção B.1, “Falha na autenticação do banco de dados ao digitar credenciais inválidas” na página 89
- Seção B.2, “Falha ao inicializar interface da Web do Sentinel” na página 89
- Seção B.3, “O Gerenciador de Coletor Remoto gera uma exceção no Windows 2008 quando o UAC está habilitado” na página 90
- Seção B.4, “O UUID não é criado para Gerenciadores de Coletor com Imagens” na página 91

B.1 Falha na autenticação do banco de dados ao digitar credenciais inválidas

Causa Comum: A autenticação no banco de dados falha se um nome de host ou endereço IP inválido do servidor LDAP for digitado durante a configuração do servidor Sentinel Rapid Deployment para autenticação LDAP.

Ação: Digite um nome de host ou endereço IP válido do servidor LDAP.

B.2 Falha ao inicializar interface da Web do Sentinel

Causa Comum: Você instalou o Sentinel Rapid Deployment em uma máquina em que o processo do Identity Audit está sendo executado, ou o Identity Audit não foi completamente desinstalado.

Ação: Impossível instalar o Sentinel Rapid Deployment e o Novell Identity Audit na mesma máquina. Antes de instalar o Sentinel Rapid Deployment na máquina que tem o Identity Audit instalado, desinstale o Identity Audit completamente.

Se os processos do Identity Audit não forem totalmente interrompidos, sua desinstalação não poderá ser concluída com êxito. Nesse caso, é possível que ocorram conflitos na instalação do Sentinel Rapid Deployment ou na inicialização de seus aplicativos.

1. Execute o seguinte comando para encerrar os serviços do Identity Audit:

   ```
   /etc/init.d/identity_audit stop
   ```

2. Execute o seguinte comando para garantir que todos os processos do Identity Audit tenham parado de funcionar:

   ```
   ps -ef | grep novell
   ```

3. Se necessário, interrompa os processos restantes manualmente.

   ```
   kill -9 pid
   ```

4. Desinstale o Identity Audit com as permissões `root` necessárias.

   Para obter mais informações, consulte o Guia do Identity Audit (http://www.novell.com/documentation/identityaudit/identityaudit10guide/data/).

B.3 O Gerenciador de Coletor Remoto gera uma exceção no Windows 2008 quando o UAC está habilitado

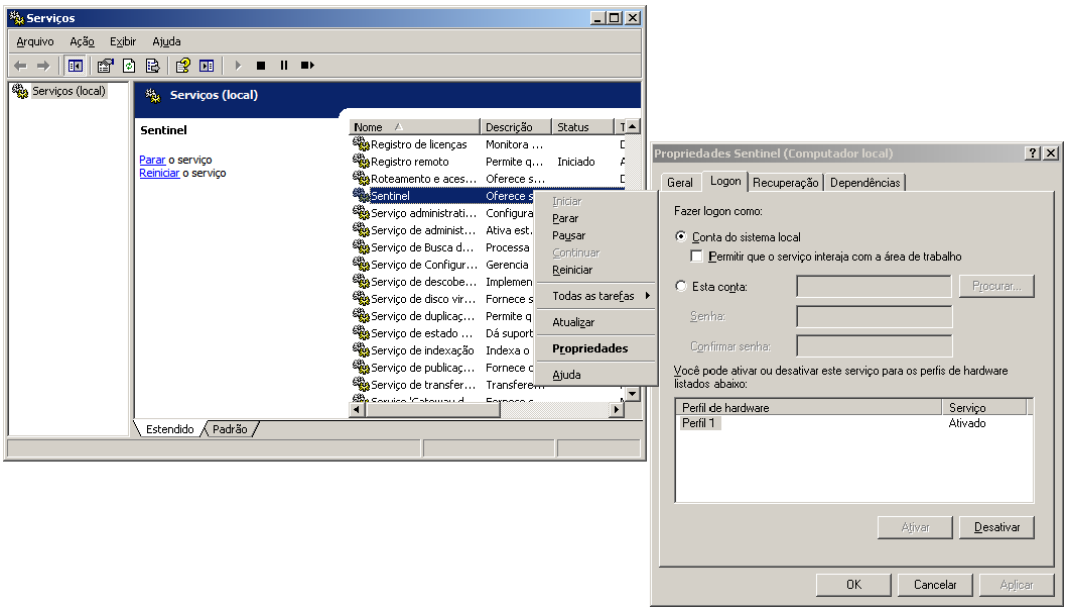
Problema: Efetue login como qualquer usuário que pertença ao grupo Administrador. Execute o comando `setup.bat` em um prompt de terminal para instalar o Gerenciador de Coletor. Reinicie o sistema ou inicie os serviços do Gerenciador de Coletor manualmente e, em seguida, efetue login com as mesmas credenciais de usuário. As exceções são registradas em `collector_manager0.0.log`. Elas impactam as seguintes funcionalidades do Gerenciador de Coletor:

- Os mapas não são inicializados.
- Você não pode escolher nenhum arquivo de fonte de eventos no sistema de arquivos da máquina do Gerenciador de Coletor (Win2008) usando o Conector de Arquivos.

Causa Comum: Você instalou o Gerenciador de Coletor em um Windows 2008 SP1 standard edition de 64 bits. Por padrão, a máquina tem o Controle de Acesso de Usuário (UAC) definido como *Habilitado*.

Ação: Mude o proprietário de *Logon* dos serviços do Sentinel Rapid Deployment para o usuário atual. Por padrão, o proprietário de *Logon* está definido como *Conta Sistema Local*. Para mudar a opção padrão:

1. Execute `services.msc` para abrir a janela *Serviços*.
2. Clique o botão direito do mouse em Sentinel e selecione *Propriedades*.



3. Na janela Propriedade do Sentinel, selecione a guia *Login*.
4. Selecione *Esta Conta* e forneça as credenciais do usuário atual que foram usadas para instalar o Gerenciador de Coletor.

B.4 O UUID não é criado para Gerenciadores de Coletor com Imagens

Se você cria uma imagem de um servidor Gerenciador de Coletor (por exemplo, usando o ZenWorks Imaging) e restaura as imagens em diferentes máquinas, o Sentinel Rapid Deployment não identifica exclusivamente as novas instâncias do Gerenciador de Coletor. Isso acontece por causa dos UUIDs duplicados.

Gere o UUID executando as seguintes etapas nos sistemas em que acabou de instalar o Gerenciador de Coletor:

1. Apague o arquivo `host.id` ou `sentinel.id` localizado na pasta `<diretório_de_instalação>/data`.
2. Reinicie o Gerenciador de Coletor.

   O Gerenciador de Coletor gera automaticamente o UUID.

Melhores práticas de manutenção do banco de dados PostgreSQL

C

É possível ajustar o banco de dados para aprimorar o desempenho do servidor de banco de dados. Os limites mencionados nesta seção são recomendações aproximadas. Não são limites exatos. Entretanto, em sistemas altamente dinâmicos, vale a pena criar buffers e deixar espaço para crescimento.

- Seção C.1, “Modificando os parâmetros de configuração de memória” na página 93
- Seção C.2, “Reduzindo o impacto de E/S de Vacuum/Analyze” na página 94

C.1 Modificando os parâmetros de configuração de memória

Para ajustar o servidor de banco de dados PostgreSQL, modifique os seguintes parâmetros de configuração de memória no arquivo `<dir_de_instalação>/3rd party/postgresql/data/postgresql.conf`:

- **buffers_compartilhados:** Determina a quantidade de memória dedicada ao PostgreSQL para armazenamento dos dados em cache. Para melhor desempenho, é possível definir esse valor de parâmetro como 1/4 da RAM disponível.
- **effective_cache_size:** Determina a quantidade de memória disponível para armazenamento do disco em cache pelo sistema operacional e no banco de dados. É possível estimar o tamanho desse parâmetro levando em consideração o que é usado pelo sistema operacional e por outros aplicativos. Você pode alocar metade da memória total disponível no sistema para esse parâmetro.
- **work_mem:** Determina a quantidade de memória usada pelas operações internas de classificação e tabelas de Hashing antes de alternar para os arquivos de disco temporários. O valor é especificado em kilobytes. O valor padrão é 1024 kilobytes (1 MB).

  Para uma consulta complexa, uma variedade de operações de Hashing pode estar em execução paralelamente. Cada operação usa a mesma quantidade de memória que o valor especificado para work_mem, antes que seja iniciada a colocação de dados nos arquivos de disco temporários. Se você estiver programando mais relatórios no sistema Sentinel Rapid Deployment, defina esse valor entre 500 MB e 1GB.
- **maintenance_work_mem:** Determina a quantidade máxima de memória que será usada nas operações de manutenção do banco de dados, como VACUUM, CREATE INDEX e ALTER TABLE ADD FOREIGN KEY. O valor é especificado em kilobytes. O valor padrão é 16384 kilobytes (16 MB).

  Configurações maiores podem melhorar o desempenho da limpeza e restauração dos dumps de banco de dados. Não modifique esse parâmetro, pois o valor padrão é suficiente para as operações do Sentinel Rapid Deployment.

C.2 Reduzindo o impacto de E/S de Vacuum/ Analyze

É possível melhorar o desempenho do banco de dados PostgreSQL de várias maneiras.

- Os dois parâmetros a seguir controlam as operações automáticas de vacuum e, por padrão, esses parâmetros são comentados durante a instalação do servidor Sentinel Rapid Deployment, e você tem que remover o comentário e definir os valores.
  - **vacuum_cost_delay:** Determina por quanto tempo o processo vai ficar adormecido quando o limite de custo for excedido. Por exemplo, é possível definir esse valor como 100.
  - **vacuum_cost_limit:** Determina o custo acumulado que vai fazer com que o processo de vacuum adormeça. Por exemplo, é possível definir esse valor como 10000.

    Se você definir o valor desses parâmetros diferente de zero, o impacto de E/S do comando vacuum e analyze será reduzido na atividade do banco de dados normal. Eles podem ter um impacto insignificante no desempenho durante a execução dos relatórios, já que o vacuum vai levar mais tempo do que antes.
- Por padrão, o processo de `autolimpeza` está definido como verdadeiro e é executado periodicamente para recuperar o espaço em disco e atualizar as estatísticas do planejador. Quando o tamanho do banco de dados aumenta, a `autolimpeza` não consegue manter todos os objetos do banco de dados. Nesses casos, se o desempenho for lento, execute o script `AnalyzePartitions.sh` como uma tarefa cron. Essa tarefa cron deve ser definida pelo usuário proprietário dos processos do Sentinel Rapid Deployment.

  Por exemplo:

  ```
  30 11 * * * $ESEC_HOME/bin/AnalyzePartitions.sh
  ```

  Onde:

  - `30` é o tempo em minutos.
  - `11` é o tempo em horas.
  - `ESEC_HOME` é o caminho absoluto do banco de dados.

  Nesse exemplo, o script é executado diariamente às 11:30.
- Evite programar o arquivamento para ocorrer durante a geração do relatório. Se você programar os dois processos juntos, a geração do relatório entrará em um estado de espera, por causa dos bugs do PostgreSQL, e iniciará o processamento dos dados após o término da tarefa de arquivamento. Essa mudança afeta o desempenho do banco de dados.