
Sentinel™

Guia de instalação e configuração

Julho de 2018

Informações legais

Para obter detalhes sobre informações legais do NetIQ, isenções, garantias, exportação e outras restrições, direitos restringidos pelo Governo dos EUA, política de patentes e conformidade com FIPS, consulte <http://www.netiq.com/company/legal/>.

Copyright © 2018 NetIQ Corporation. Todos os direitos reservados.

Para obter informações sobre as marcas comerciais da NetIQ, consulte <http://www.netiq.com/company/legal/>. Todas as marcas registradas de terceiros pertencem aos seus respectivos proprietários.

Sobre este manual e a biblioteca	11
Parte I Compreendendo o Sentinel	13
1 O que é o Sentinel?	15
Desafios em proteger um ambiente de TI.	15
A solução fornecida pelo Sentinel.	16
2 Como o Sentinel funciona	19
Fontes de eventos	21
Evento do Sentinel	21
Serviço de Mapeamento	22
Transmitindo mapas.	23
Detecção de Exploração	23
Collector Manager.	23
Coletores	23
Conectores.	24
ArcSight SmartConnectors	24
Agent Manager	24
Roteamento e armazenamento de dados no Sentinel	24
Visualizações de eventos	25
Correlação.	25
Inteligência de Segurança.	26
Correção de incidente.	26
Fluxos de trabalho do iTrac.	26
Ações e integradores	26
Pesquisando	27
Relatórios	27
Monitoramento de identidade	27
Análise de eventos	27
Parte II Planejando a instalação do Sentinel	29
3 Lista de verificação da implementação	31
4 Compreendendo as informações da licença	33
Licenças do Sentinel.	35
Licença para Avaliação	35
Licença gratuita	35
Licenças corporativas.	35
5 Atendendo aos requisitos do sistema	37
Requisitos do sistema do Conector e do Coletor	37
Ambiente virtual	37
6 Considerações de implantação	39
Considerações sobre armazenamento de dados	39
Planejando o armazenamento tradicional	41
Planejando o armazenamento escalável	44

Estrutura de diretórios do Sentinel	46
Vantagens das implantações distribuídas	46
Vantagens de instâncias do Collector Manager adicionais	47
Vantagens das instâncias adicionais do Correlation Engine	47
Implantação multifuncional	48
Implantação distribuída de um nível	48
Implantação distribuída de um nível com alta disponibilidade	49
Implantação distribuída de dois e três níveis	50
Implantação de três níveis com armazenamento escalável	51
 7 Considerações da implantação para o modo FIPS140-2	 55
Implementação do FIPS no Sentinel	55
Pacotes RHEL NSS	55
Pacotes SLES NSS	56
Componentes ativados para FIPS no Sentinel	56
Conexões de dados afetadas pelo modo FIPS	57
Lista de verificação da implementação	57
Cenários de implantação	58
Cenário 1: Coleta de dados no modo FIPS 140-2 completo	58
Cenário 2: Coleta de dados no modo FIPS 140-2 parcial	59
 8 Portas usadas	 63
Portas do servidor do Sentinel	63
Portas locais	63
Portas de rede	63
Portas específicas da aplicação do Sentinel Server	65
Portas do Collector Manager	65
Portas de rede	65
Portas específicas da aplicação do Collector Manager	66
Portas do Correlation Engine	67
Portas de rede	67
Portas específicas da aplicação do Correlation Engine	67
Portas de armazenamento escalável	68
 9 Opções de instalação	 69
Instalação tradicional	69
Instalação da aplicação	70
 Parte III Instalando o Sentinel	 71
 10 Visão geral da instalação	 73
 11 Lista de verificação de instalação	 75
 12 Instalando e configurando o Elasticsearch	 77
Pré-requisitos	77
Instalando e configurando o Elasticsearch	77
Protegendo dados no Elasticsearch	79
Instalando o plug-in de segurança do Elasticsearch	80
Fornecendo acesso seguro a clientes adicionais do Elasticsearch	81

Atualizando a configuração do plug-in do Elasticsearch	82
Ajuste de desempenho para o Elasticsearch	83
Reimplantar o plug-in de segurança do Elasticsearch	84
13 Instalando e configurando o armazenamento escalável	87
Instalando e configurando o CDH	88
Pré-requisitos	88
Instalando e configurando o CDH	89
Habilitando o armazenamento escalável	89
14 Instalação tradicional	91
Executando instalações interativas	91
Instalação padrão do servidor do Sentinel	91
Instalação personalizada do servidor do Sentinel	92
Instalação do Collector Manager e Correlation Engine	95
Realizando uma instalação silenciosa	97
Instalando o Sentinel como um usuário não raiz	98
15 Instalação da aplicação	101
Pré-requisitos	101
Instalando a aplicação Sentinel ISO	101
Instalando o Sentinel	102
Instalando instâncias do Collector Manager e do Correlation Engine	103
Instalando a aplicação Sentinel OVF	104
Instalando o Sentinel	104
Instalando instâncias do Collector Manager e do Correlation Engine	105
Configuração pós-instalação para a aplicação	106
Registrando para receber atualizações	106
Criando partições para armazenamento tradicional	107
Configurando o armazenamento escalável	107
Configurando a aplicação com SMT	108
16 Instalando coletores e conectores adicionais	111
Instalando um Coletor	111
Instalando um Conector	111
17 Verificando a instalação	113
Parte IV Configurando o Sentinel	115
18 Configurando o horário	117
Entendendo o horário no Sentinel	117
Configurando o horário no Sentinel	119
Configurando o limite de tempo de atraso para eventos	119
Tratando fusos horários	119

19 Protegendo dados no Elasticsearch	121
20 Habilitando a visualização de eventos	123
Pré-requisitos	123
Habilitando a visualização de eventos	123
21 Modificando a configuração depois da instalação	125
22 Configurando plug-ins prontos para o uso	127
Visualizando os plug-ins pré-instalados	127
Configurando a coleta de dados	127
Configurando pacotes de soluções	127
Configurando ações e integradores	128
23 Ativando o modo FIPS 140-2 em uma instalação existente do Sentinel	129
Ativando o servidor do Sentinel para executar no Modo FIPS 140-2	129
Ativando o modo FIPS 140-2 nas instâncias remotas do Collector Manager e do Correlation Engine . . .	130
24 Operando o Sentinel no modo FIPS 140-2	131
Configurando o servido do Consultor em modo FIPS 140-2	131
Configurando a pesquisa distribuída em modo FIPS 140-2	131
Configurando a autenticação LDAP em modo FIPS 140-2	133
Atualizando certificados do servidor nas instâncias do Collector Manager e do Correlation Engine remotos	133
Configurando os plug-ins do Sentinel para execução em modo FIPS 140-2	134
Conector do Gerenciador de Agente	134
Conector de banco de dados (JDBC)	135
Conector do Link do Sentinel	135
Conector Syslog	136
Windows Event (WMI) Connector	137
Sentinel Link Integrator	138
LDAP Integrator	139
SMTP Integrator	139
Integrador Syslog	139
Usando conectores ativados não FIPS com o Sentinel no modo FIPS 140-2	140
Importando certificados para o banco de dados de keystore do FIPS	140
Revertendo o Sentinel para o modo não FIPS	141
Revertendo o servidor do Sentinel para o modo não FIPS	141
Revertendo as instâncias do Collector Manager e do Correlation Engine remotos para o modo não FIPS	142
25 Adicionando um banner de consentimento	143
Parte V Fazendo upgrade do Sentinel	145
26 Lista de verificação da implementação	147
27 Pré-requisitos	149
Gravando as informações de configuração personalizada	149
Gravando as Configurações do arquivo server.conf	149
Gravando as Configurações do arquivo jetty-ssl	149

Estendendo o Período de Retenção para Dados de Associações de Eventos	149
Configuração Pré-Upgrade para SSDM	150
Integração do Change Guardian.	150
28 Fazendo o upgrade da instalação tradicional do Sentinel	151
Fazendo upgrade do Sentinel.	151
Fazendo o upgrade do Sentinel como um usuário não root.	152
Fazendo o upgrade do Collector Manager ou do Correlation Engine.	154
Fazendo upgrade do sistema operacional	155
29 Fazendo upgrade da aplicação Sentinel	157
Fazendo upgrade do Sentinel.	157
Fazendo o upgrade do Sentinel por meio do Canal de Atualização da Aplicação.	157
Fazendo o upgrade do Sentinel usando o SMT.	159
Fazendo upgrade do sistema operacional	160
30 Configurações Pós-Upgrade	163
Protegendo dados no Elasticsearch	163
Configurando visualizações de eventos	163
Configurando coleta de dados de Fluxo de IP	164
Configuração Pós-Upgrade para o Gerente de Dados Escalável do Sentinel	165
Instalar o plug-in de segurança do Elasticsearch.	165
Atualizando Aplicativos do Spark no YARN	165
Habilitando Recursos do Sentinel	166
Atualizando painéis de controle e visualizações no Gerenciador de dados escaláveis do Sentinel	166
Adicionando o driver JDBC DB2.	167
Configurando propriedades de federação de dados na aplicação do Sentinel.	167
Registrando a aplicação do Sentinel atualizações	168
Atualizando bancos de dados externos para sincronização de dados	168
Reautenticando o Sentinel no Modo de Autenticação de Vários Fatores.	168
31 Fazendo upgrade de plug-ins do Sentinel	171
Parte VI Migrando dados do armazenamento tradicional	173
32 Migrando dados para o armazenamento escalável	175
Dados que você pode migrar	176
Migrando Dados de Configuração	177
Fazendo backup dos Dados no Servidor de Origem	177
Restaurando Dados no Servidor de Destino	178
Migrando Dados de Eventos e Dados Brutos.	179
Migrando Alertas e Dados do NetFlow	179
Atualizando Clientes do Sentinel	179
Importando a Configuração do ESM.	179

33 Migrando dados para o Elasticsearch	181
34 Migrando dados	183
Parte VII Implantando o Sentinel para alta disponibilidade	185
35 Conceitos	187
Sistemas externos	187
Armazenamento compartilhado	187
Monitoramento do serviço	188
Fencing	188
36 Requisitos do Sistema	189
37 Instalação e configuração	191
Configuração inicial	192
Configuração de armazenamento compartilhado	193
Configurando destinos iSCSI	194
Configurando iniciadores iSCSI	196
Instalação do Sentinel	197
Instalação no primeiro nó	197
Instalação do nó subsequente	199
Instalação do cluster	200
Configuração do Cluster	201
Configuração do recurso	204
Configuração do armazenamento secundário	206
38 Configurando o Sentinel de HA como SSDM	209
39 Fazendo o upgrade do Sentinel em alta disponibilidade	211
Pré-requisitos	211
Fazendo upgrade de instalações de HA tradicionais do Sentinel	211
Fazendo upgrade do Sentinel de HA	212
Fazendo upgrade do sistema operacional	213
Fazendo upgrade de instalações de aplicação de HA do Sentinel	217
Fazendo o upgrade da aplicação do Sentinel de HA usando o Zypper	217
40 Backup e recuperação	219
Backup	219
da PlateSpin	219
Falha temporária	219
Corrupção do nó	219
Configuração dos dados do cluster	220
Parte VIII Apêndices	221
A Solução de problemas	223
Falha na instalação devido a configuração de rede incorreta	223

O UUID não é criado para instâncias do Collector Manager em imagens nem para Correlation Engine. .	224
Após efetuar login, a interface principal do Sentinel ficará em branco no Internet Explorer	224
O Sentinel não inicia no Internet Explorer 11 no Windows Server 2012 R2	224
O Sentinel não pode executar relatórios locais com a licença EPS padrão.	225
É necessário iniciar a sincronização manualmente na Alta Disponibilidade do Sentinel após converter o nó ativo para o modo FIPS 140-2	225
A interface principal do Sentinel exibe uma página em branco após a conversão para o Gerenciador de dados escaláveis do Sentinel	225
O painel Campos de evento não é exibido na página Programar ao editar algumas pesquisas gravadas	226
O Sentinel não retorna nenhum evento correlacionado quando você pesquisa por eventos para a regra implantada com a pesquisa padrão de contagem de acionamentos	226
O painel de controle de inteligência de segurança exibe uma duração de linha de base inválida ao regenerar uma linha de base	226
O servidor do Sentinel desliga ao executar uma pesquisa quando há um número grande de eventos em uma única partição	226
Erro ao usar o script report_dev_setup.sh para configurar as portas do Sentinel de exceção do firewall em instalações com upgrade da aplicação do Sentinel.	227

B Desinstalando 229

Lista de verificação da desinstalação	229
Desinstalando o Sentinel	229
Desinstalando o Sentinel Server	229
Desinstalando o Collector Manager e o Correlation Engine	230
Desinstalando o NetFlow Collector Manager.	230
Tarefas pós-desinstalação	231

Sobre este manual e a biblioteca

O *Guia de instalação e configuração* fornece uma introdução ao Sentinel e explica como instalar e configurar o Sentinel.

Público-alvo

Este guia destina-se a administradores e consultores do Sentinel.

Outras informações na biblioteca

A biblioteca fornece os seguintes recursos informativos:

Guia de administração

Fornecer informações de administração e tarefas necessárias para gerenciar uma implantação do Sentinel.

Guia do usuário

Fornecer informações conceituais sobre o Sentinel. Este livro também fornece uma visão geral das interfaces do usuário e orientação passo a passo para diversas tarefas.

Compreendendo o Sentinel

Esta seção fornece informações detalhadas sobre o Sentinel e como ele fornece uma solução de gerenciamento de eventos para sua organização.

- ♦ [Capítulo 1, “O que é o Sentinel?” na página 15](#)
- ♦ [Capítulo 2, “Como o Sentinel funciona” na página 19](#)

1 O que é o Sentinel?

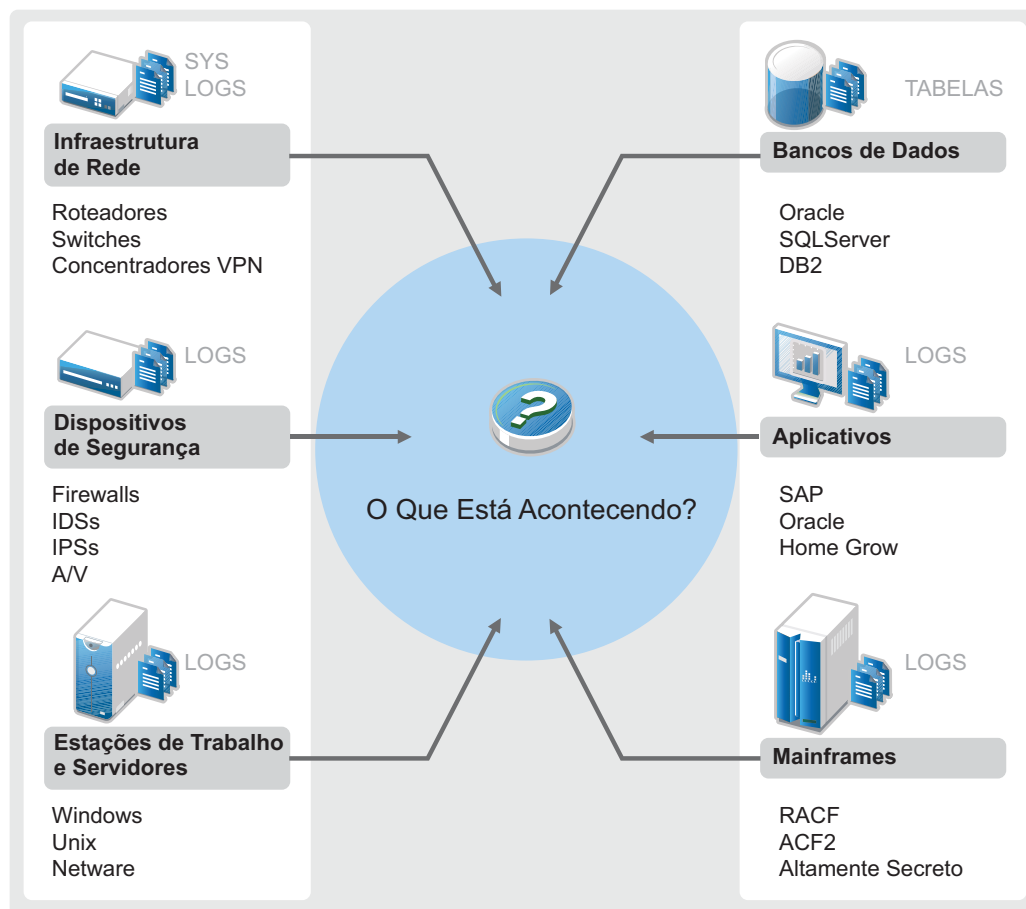
O Sentinel é uma solução de Gerenciamento de Segurança, Informações e Eventos (SIEM), além de uma solução de monitoramento de conformidade. Ele monitora automaticamente os ambientes de TI mais complexos e fornece a segurança necessária para proteger seu ambiente de TI.

- ♦ “Desafios em proteger um ambiente de TI” na página 15
- ♦ “A solução fornecida pelo Sentinel” na página 16

Desafios em proteger um ambiente de TI

A complexidade dos ambientes de TI geram grandes desafios para a segurança das informações. Normalmente, há diversos aplicativos, bancos de dados, mainframes, estações de trabalho e servidores em seu ambiente de TI, e todas essas entidades geram registros de eventos. Você também deve ter dispositivos de segurança e dispositivos de infraestrutura de rede que geram registros de eventos em seu ambiente de TI.

Figura 1-1 O que acontece no seu ambiente



Os desafios surgem porque:

- ♦ Há muitos dispositivos no seu ambiente de TI;
- ♦ Os registros estão em formatos diferentes;
- ♦ Os registros são armazenados em locais diferentes.
- ♦ O volume de informações capturadas nos arquivos de registro é grande.
- ♦ É impossível determinar acionadores de eventos sem analisar manualmente os arquivos de registro.

Para tornar as informações úteis nos registros, você deve ser capaz de:

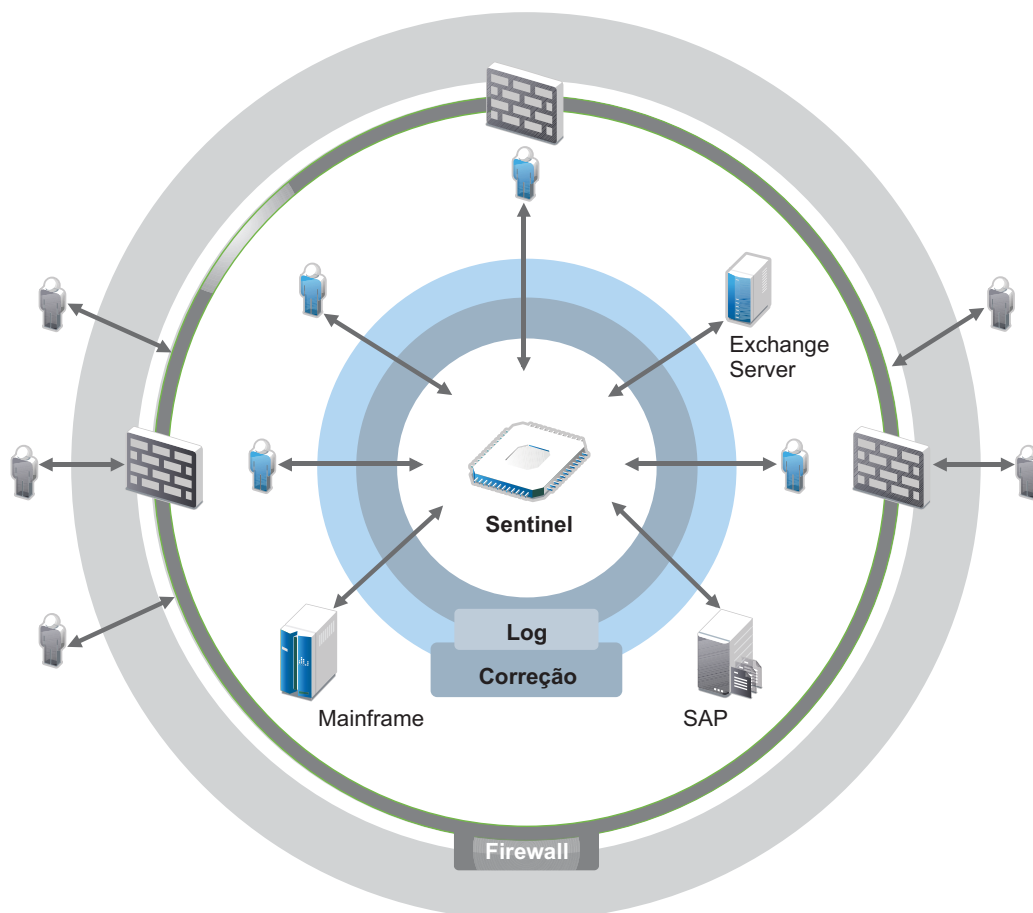
- ♦ Coletar dados;
- ♦ Consolidar dados;
- ♦ Normalizar dados distintos em eventos que possam ser facilmente comparados;
- ♦ Mapear eventos para normas padrão.
- ♦ Analisar os dados;
- ♦ Comparar eventos em diversos sistemas para determinar se há algum problema de segurança;
- ♦ Enviar notificações quando os dados não estão em conformidade com as normas.
- ♦ Impor ações sobre as notificações para cumprir com as políticas da empresa; e
- ♦ Gerar relatórios para comprovar a conformidade.

Após compreender os desafios para proteger seu ambiente de TI, é necessário determinar como proteger a empresa de e para usuários sem afetar a experiência do usuário. O Sentinel é a solução.

A solução fornecida pelo Sentinel

O Sentinel age como sistema nervoso central para a segurança empresarial. Ele retém dados de toda a infraestrutura: aplicativos, bancos de dados, servidores, armazenamento e dispositivos de segurança. Ele analisa e correlaciona os dados e torna os dados processáveis, seja manual ou automaticamente.

Figura 1-2 A solução fornecida pelo Sentinel



Com o Sentinel, você sabe o que está acontecendo no seu ambiente de TI a qualquer momento e consegue vincular as ações tomadas para os recursos às pessoas responsáveis por elas. Isso permite que você determine o comportamento do usuário e monitore eficientemente as atividades para evitar atividades mal-intencionadas.

O Sentinel consegue isso ao:

- ♦ Fornecer uma única solução que lida com controles de TI em diversas normas de segurança.
- ♦ Preencher a lacuna entre o que deveria acontecer e o que realmente acontece no seu ambiente de TI.
- ♦ Ajudar você a estar em conformidade com as normas de segurança.
- ♦ Fornecer monitoramento de conformidade e programas de relatórios prontos; e

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. Ele fornece monitoramento automático dos eventos de segurança e de conformidade, além dos controles de TI. Isso permite que você tome uma ação imediata se houver uma brecha de segurança ou ocorrer um evento em não conformidade. O Sentinel também permite que você reúna informações resumidas sobre seu ambiente e envie-as para seus principais acionistas.

2 Como o Sentinel funciona

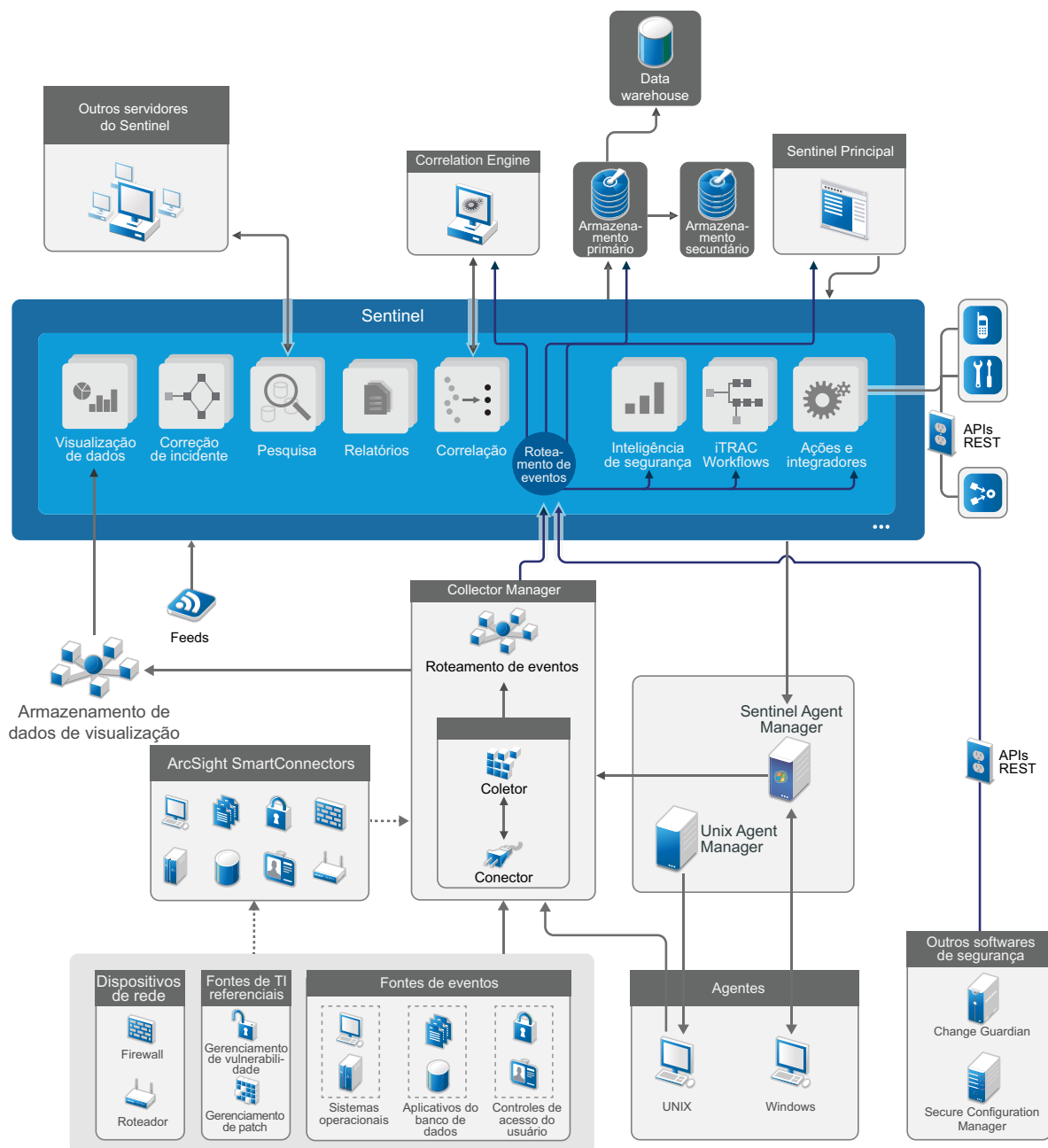
O Sentinel gerencia as informações e os eventos de segurança de forma contínua em todo o ambiente de TI para garantir uma solução de monitoramento completa.

O Sentinel faz o seguinte:

- ♦ Reúne informações de registros, eventos e segurança de diversas fontes de eventos presentes em seu ambiente de TI.
- ♦ Padroniza as informações de registros, eventos e segurança reunidas em um formato padrão do Sentinel.
- ♦ Armazena eventos em um armazenamento de dados com base no arquivo ou em um armazenamento escalável com base em Hadoop com políticas de retenção de dados flexíveis e personalizáveis.
- ♦ Coleta dados de Fluxo de IP e ajuda você a monitorar as atividades de rede em detalhes.
- ♦ Fornece a capacidade de vincular hierarquicamente vários sistemas Sentinel, incluindo o Sentinel Log Manager;
- ♦ Permite a você pesquisar eventos não apenas no seu servidor Sentinel local, mas também em outros servidores Sentinel distribuídos no mundo.
- ♦ Realiza uma análise estatística que permite definir uma linha de base e, depois, compará-la ao que está acontecendo a fim de determinar se há problemas que passaram despercebidos.
- ♦ Correlaciona um conjunto de eventos semelhantes ou comparáveis em uma duração específica para estabelecer um padrão.
- ♦ Organiza os eventos por incidente a fim de viabilizar gerenciamento de resposta e monitoramento eficientes; e
- ♦ Fornece relatórios com base em eventos em tempo real e históricos.

A figura a seguir ilustra como o Sentinel funciona, tendo o armazenamento tradicional como opção de armazenamento de dados:

Figura 2-1 Arquitetura do Sentinel



As seções a seguir descrevem os componentes do Sentinel em detalhes:

- ♦ “Fontes de eventos” na página 21
- ♦ “Evento do Sentinel” na página 21

- ♦ “Collector Manager” na página 23
- ♦ “ArcSight SmartConnectors” na página 24
- ♦ “Agent Manager” na página 24
- ♦ “Roteamento e armazenamento de dados no Sentinel” na página 24
- ♦ “Visualizações de eventos” na página 25
- ♦ “Correlação” na página 25
- ♦ “Inteligência de Segurança” na página 26
- ♦ “Correção de incidente” na página 26
- ♦ “Fluxos de trabalho do iTrac” na página 26
- ♦ “Ações e integradores” na página 26
- ♦ “Pesquisando” na página 27
- ♦ “Relatórios” na página 27
- ♦ “Monitoramento de identidade” na página 27
- ♦ “Análise de eventos” na página 27

Fontes de eventos

O Sentinel reúne informações de segurança e eventos de diversas fontes no seu ambiente de TI. Essas fontes são denominadas fontes de eventos. Normalmente, as seguintes são as fontes de evento em sua rede:

Perímetro de Segurança: Dispositivos de segurança, incluindo hardware e software usados para criar um perímetro de segurança para seu ambiente, como firewalls, IDS (Intrusion Detection System — Sistema de Detecção de Intrusão) e VPN (virtual private networks - redes privadas virtuais).

Sistemas Operacionais: Diversos sistemas operacionais executando na rede.

Fontes de TI Referenciais: o software usado para manter e monitorar bens, patches, configurações e vulnerabilidade.

Aplicativos: Diversos aplicativos instalados na rede.

Controle de Acesso de Usuário: Aplicativos ou dispositivos que permitem aos usuários acessar os recursos da empresa.

Para obter mais informações sobre a coleta de eventos de fontes de eventos, consulte “[Coletando e roteando dados de eventos](#)” no [Guia de Administração do Sentinel](#).

Evento do Sentinel

O Sentinel recebe informações de dispositivos, normaliza-as em uma estrutura chamada evento, categoriza o evento e, em seguida, envia-o para processamento.

Um evento representa um registro normalizado relatado ao Sentinel por um dispositivo de segurança, por uma rede ou dispositivo de aplicativo de terceiros ou por uma fonte interna do Sentinel. Existem vários tipos de eventos:

- ♦ Eventos externos (eventos recebidos de um dispositivo de segurança) como:
 - ♦ Um ataque detectado por um IDS (Intrusion Detection System — Sistema de Detecção de Intrusão)

- ♦ Um login bem-sucedido relatado por um sistema operacional
- ♦ Uma situação definida pelo cliente, como um usuário acessando um arquivo
- ♦ Eventos internos (eventos gerados pelo Sentinel), incluindo:
 - ♦ Uma regra de correlação sendo desativada
 - ♦ O preenchimento do banco de dados

O Sentinel adiciona informações de categoria (taxonomia) a eventos, para facilitar a comparação de eventos entre sistemas que relatam eventos de maneira diferente. Os eventos são processados pela exibição em tempo real, pelo mecanismo de correlação, por painéis e pelo servidor back end.

Um evento é composto por mais de 200 campos; campos de evento são de diferentes tipos e de diferentes finalidades. Alguns são predefinidos, como gravidade, importância, endereço IP de destino e porta de destino.

Há dois conjuntos de campos configuráveis:

- ♦ Campos reservados. Para uso interno do Sentinel para permitir a extensão de funcionalidade no futuro.
- ♦ Campos do cliente: De uso do cliente para permitir a personalização.

A fonte para um campo pode ser externa ou referencial:

- ♦ O valor de um campo externo é definido explicitamente pelo dispositivo ou o Coletor correspondente. Por exemplo, um campo pode ser definido como o código da construção que contém o bem mencionado como o endereço IP de destino de um evento.
- ♦ O valor de um campo referencial é computado como uma função de um ou mais campos que usam o serviço de mapeamento. Por exemplo, um campo pode ser computado pelo serviço de mapeamento por meio de um mapa definido pelo cliente usando o endereço IP de destino do evento.
- ♦ [“Serviço de Mapeamento” na página 22](#)
- ♦ [“Transmitindo mapas” na página 23](#)
- ♦ [“Detecção de Exploração” na página 23](#)

Serviço de Mapeamento

O Serviço de mapeamento propaga os dados de relevância dos negócios por todo o sistema. Esses dados podem enriquecer eventos com informações de referência.

Você pode aprimorar os dados de evento usando mapas para adicionar informações (como detalhes do host e da identidade) aos eventos recebidos de seus dispositivos de origem. O Sentinel pode usar essas informações adicionais para correlação e emissão avançadas de relatórios. O Sentinel suporta diversos mapas integrados e também mapas definidos pelo usuário.

Os mapas definidos no Sentinel são armazenados de duas formas:

- ♦ Os mapas integrados são armazenados no banco de dados, atualizados internamente e exportados automaticamente para o serviço de mapeamento.
- ♦ Os mapas personalizados são armazenados como arquivos CSV e podem ser atualizados no sistema de arquivos ou usando a Interface do Usuário da Configuração dos Dados do Mapa e, em seguida, carregados pelo serviço de Mapeamento.

Em ambos os casos, os arquivos CSV são mantidos no servidor central do Sentinel, mas as alterações feitas nos mapas são distribuídas para cada Collector Manager e aplicadas localmente. Esse processamento distribuído garante que a atividade de mapeamento não sobrecarregue o servidor principal.

Transmitindo mapas

O Serviço de Mapeamento emprega um modelo de atualização dinâmica e transmite os mapas de um ponto para outro, evitando o acúmulo de grandes mapas estáticos na memória dinâmica. Isso é relevante em um sistema em tempo real crítico ao sistema como o Sentinel onde uma movimentação de dados sólida, previsível e ágil independente de qualquer carga transitória no sistema seja necessária.

Detecção de Exploração

O Sentinel permite a referência cruzada entre as assinaturas dos dados de eventos e os dados do Vulnerability Scanner. O Sentinel notifica os usuários automática e imediatamente quando há uma tentativa de explorar um sistema vulnerável. O Sentinel realiza isso por meio das seguintes funções:

- ♦ A alimentação do Consultor;
- ♦ Detecção de intrusão;
- ♦ Verificação de vulnerabilidades; e
- ♦ Firewalls

O feed do Advisor contém informações sobre vulnerabilidades e ameaças, uma normalização de assinaturas de evento e plug-ins de vulnerabilidade. Ele fornece uma referência cruzada entre as assinaturas de dados do evento e os dados do verificador de vulnerabilidades. Para obter mais informações sobre o feed do Consultor, consulte [“Detectando vulnerabilidades e explorações”](#) no *Guia de administração do Sentinel*.

Collector Manager

O Collector Manager gerencia a coleta de dados, monitora as mensagens de status do sistema e executa a filtragem de eventos. As principais funções do Collector Manager incluem o que segue:

- ♦ Coleta de dados por meio do uso de Conectores.
- ♦ Análise e normalização de dados por meio do uso de Coletores.

Coletores

Coletores coletam as informações dos Conectores e as normalizam. Eles realizam as seguintes funções:

- ♦ Receber dados iniciais dos Conectores;
- ♦ Analisar e normalizar os dados:
 - ♦ Traduzir dados específicos da fonte de eventos para dados específicos do Sentinel.
 - ♦ Enriquecer eventos alterando as informações nos eventos em um formato que o Sentinel pode ler.
 - ♦ Filtrar eventos para a fonte de eventos.

- ♦ Adicionar relevância empresarial aos eventos por meio do serviço de mapeamento:
 - ♦ Mapear eventos para identificadores.
 - ♦ Mapear eventos para Bens.
- ♦ Rotear eventos;
- ♦ Passar os dados normalizados, analisados e formatados para o Collector Manager.
- ♦ Enviar mensagens de saúde ao servidor Sentinel.

Para obter mais informações sobre Coletores, consulte o [site de Plug-ins do Sentinel](#).

Conectores

Os Conectores fornecem a conexão entre as fontes de eventos e o sistema Sentinel.

Os Conectores fornecem as seguintes funcionalidades:

- ♦ Transporte dos dados de eventos iniciais das fontes de eventos para o Coletor.
- ♦ Filtragem específica da conexão.
- ♦ Gerenciamento de erros da conexão.

ArcSight SmartConnectors

O Sentinel utiliza o ArcSight SmartConnector para coletar eventos de vários tipos de fontes de eventos não suportados diretamente pelo Sentinel. Os SmartConnectors coletam eventos de dispositivos suportados, normalizam eventos no CEF (Common Event Format - Formato de Evento Comum) e os encaminham ao Sentinel por meio do Syslog Connector. O Connector, em seguida, encaminha os eventos para o Universal Common Event Format Collector para análise.

Para obter mais informações sobre como configurar o Sentinel com SmartConnectors, consulte a documentação do Universal Common Event Format Collector no [Site de plug-ins do Sentinel](#).

Agent Manager

O Gerenciador de agente possibilita a coleta de dados baseada em host, que complementa as coletas de dados sem agente permitindo que você realize as seguintes tarefas:

- ♦ Acessar registros que não estão disponíveis na rede.
- ♦ Opere em ambientes de rede rigidamente controlados.
- ♦ Melhore a postura de segurança limitando a superfície de ataque em servidores críticos.
- ♦ Forneça maior segurança de coleta de dados durante momento de interrupção de rede..

O Gerenciador de agente permite que você implante agentes e gerencie a configuração do agente, e também funciona como um ponto de coleta para eventos fluindo no Sentinel. Para obter mais informações sobre o Gerenciador de agente, consulte a [documentação do Gerenciador de agente](#).

Roteamento e armazenamento de dados no Sentinel

O Sentinel fornece várias opções para roteamento, armazenamento e extração de dados coletados. Por padrão, o Sentinel recebe os dados do evento analisados e os dados brutos das instâncias do Collector Manager. O Sentinel armazena os dados brutos para fornecer uma cadeia de evidências

segura e faz o roteamento dos dados de evento analisados de acordo com as regras que você definir. Você pode filtrar os dados do evento analisados, enviá-los para armazenamento ou para a análise em tempo real e encaminhá-los para sistemas externos. O Sentinel ainda compara todos os dados de eventos enviados ao armazenamento para políticas de retenção definidas pelo usuário. As políticas de retenção controlam quando os dados de evento devem ser apagados do sistema.

Dependendo da taxa de EPS (Events Per Second - Eventos Por Segundo) e dos requisitos de implantação, é possível optar por usar o armazenamento de dados tradicional com base no arquivo ou o armazenamento escalável com base em Hadoop como opção de armazenamento de dados. Para obter mais informações, consulte [“Considerações sobre armazenamento de dados” na página 39](#).

Visualizações de eventos

O Sentinel fornece visualizações de eventos que apresentam dados em gráficos, tabelas e mapas. Essas visualizações facilitam a visualização e a análise de grandes volumes de eventos, incluindo eventos de Fluxo de IP. Também é possível criar suas próprias visualizações e painéis de controle.

As visualizações de eventos estão disponíveis por padrão no Sentinel com armazenamento escalável. Em uma configuração de armazenamento tradicional, as visualizações de eventos estarão disponíveis somente se você tiver habilitado o armazenamento de dados de visualização (Elasticsearch) para armazenar e indexar dados. Para obter mais informações sobre como habilitar o Elasticsearch, consulte [“Configurando o armazenamento de dados de visualização” na página 43](#).

Correlação

Um único evento pode parecer trivial, mas, em combinação com outros eventos, ele pode avisá-lo de um possível problema. O Sentinel o ajuda a correlacionar tais eventos usando regras criadas por você e implantadas no Correlation Engine, e também a tomar as ações adequadas para minimizar qualquer problema.

A correlação agrega inteligência ao gerenciamento de eventos de segurança, automatizando a análise do fluxo de eventos de entrada para encontrar padrões relevantes. 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 sobre correlação, consulte a seção [“Correlacionando dados de eventos”](#) no *Guia do usuário do Sentinel*.

Para monitorar eventos de acordo com as Regras de correlação, é necessário implantar as regras no Correlation Engine. Quando um evento que atende aos critérios da regra ocorrer, o Correlation Engine gera um evento de correlação descrevendo o padrão. Para obter mais informações, consulte [“Correlation Engine”](#) no *Guia do usuário do Sentinel*.

Inteligência de Segurança

A capacidade de correlação do Sentinel fornece a você a possibilidade de buscar padrões conhecidos da atividade, que você pode analisar para segurança, conformidade ou outro motivo. O recurso Inteligência de Segurança procura atividades fora do comum e que possam ser maliciosas, mas que não correspondem a nenhum padrão conhecido.

O recurso Inteligência de Segurança do Sentinel concentra-se na análise estatística dos dados de séries cronológicas para permitir que os analistas identifiquem e analisem anomalias usando um mecanismo estatístico automático ou uma representação visual dos dados estatísticos para interpretação manual. Para obter mais informações, consulte [“Analisando tendências em dados”](#) no *Guia do Usuário do Sentinel*.

Correção de incidente

O Sentinel fornece um sistema de gerenciamento automatizado de resposta a incidentes que permite que você documente e formalize o processo de monitoramento, encaminhamento e resposta a incidentes e violações de política. Ele também fornece a integração bidirecional com sistemas de comunicação de problemas. O Sentinel permite que você reaja prontamente e resolva incidentes de forma eficiente. Para obter mais informações, consulte [“Configurando incidentes”](#) no *Guia do usuário do Sentinel*.

Fluxos de trabalho do iTrac

Os fluxos de dados iTRAC fornecem uma solução simples e flexível de automatização e monitoramento dos processos de resposta a incidentes em uma empresa. O iTRAC aproveita o sistema interno de incidentes do Sentinel para monitorar problemas de segurança ou do sistema desde a identificação (através de regras de correlação ou de identificação manual) até a resolução.

Você pode criar fluxos de trabalho usando etapas manuais e automatizadas. Os fluxos de trabalho iTrac suportam recursos avançados como ramificação, escalção com base em tempo e variáveis locais. A integração com scripts e plug-ins externos permite uma interação flexível com sistemas de terceiros. A geração de relatórios abrangente permite que os administradores compreendam e ajustem os processos de resposta a incidente. Para obter mais informações, consulte a seção [“Configurando fluxos de trabalho do iTRAC”](#) no *Guia do usuário do Sentinel*.

Ações e integradores

As ações executam manual ou automaticamente algum tipo de ação, como enviar um e-mail. Você pode acionar Ações por regras de roteamento, execução manual de um evento ou operação incidente, bem como por regras de correlação. O Sentinel fornece uma lista de Ações pré-configuradas. Você pode usar as ações padrões e reconfigurá-las conforme necessário, ou pode adicionar novas Ações. Para obter mais informações, consulte [“Configurando ações”](#) no *Guia de administração do Sentinel*.

Uma Ação pode ser executada por conta própria ou pode utilizar um instância de Integrador a partir de um plug-in de Integrador. Plug-ins do Integrador ampliam os recursos e a funcionalidade das ações de remediação do Sentinel. Os Integradores fornecem a capacidade de se conectar a um sistema externo, como um servidor SOAP, SMTP ou LDAP, para executar uma ação. Para obter mais informações, consulte [“Configurando integradores”](#) no *Guia de administração do Sentinel*.

Pesquisando

O Sentinel fornece a opção de execução de pesquisas em eventos. Com a configuração necessária, também é possível pesquisar eventos do sistema gerados pelo Sentinel e exibir os dados brutos de cada evento. Para obter mais informações, consulte [“Searching Events”](#) (Pesquisando eventos) no [Sentinel User Guide](#) (Guia do Usuário do NetIQ Sentinel).

Também é possível pesquisar nos servidores do Sentinel distribuídos em locais geográficos diferentes. Para obter mais informações, consulte a seção [“Configurando a federação de dados”](#) no [Guia de Administração do Sentinel](#).

Relatórios

O Sentinel fornece um recurso para executar relatórios nos dados coletados. O Sentinel é preparado com uma variedade de relatórios personalizáveis. Alguns desses relatórios são configuráveis para permitir que você especifique as colunas que devem ser exibidas nos resultados.

Você pode executar, programar e enviar por e-mail relatórios no formato PDF. Você também pode executar qualquer relatório como uma pesquisa e, depois, interagir com os resultados como faria com uma pesquisa, por exemplo, refinando a pesquisa ou executando ações com os resultados. Você também pode executar relatórios nos servidores Sentinel distribuídos em diferentes localizações geográficas. Para obter mais informações, consulte [“Geração de relatórios”](#) no [Guia do Usuário do Sentinel](#).

Monitoramento de identidade

O Sentinel fornece uma metodologia de integração para sistemas de gerenciamento de identidade para controlar as identidades para cada conta do usuário e que eventos essas identidades realizaram. O Sentinel fornece informações do usuário, como informações de contato, contas do usuário, eventos de autenticação recentes, eventos de acesso recentes, alterações de permissão, etc. Ao exibir informações sobre os usuários que iniciam uma ação específica ou os usuários afetados por uma ação, o Sentinel melhora o tempo de resposta a incidentes e permite a análise com base em comportamento. Para obter mais informações, consulte [“Aproveitando informações de identidade”](#) no [Guia do usuário do Sentinel](#).

Análise de eventos

O Sentinel fornece um conjunto de ferramentas avançadas para ajudar você a encontrar e analisar mais facilmente dados críticos de eventos. O Sentinel otimiza o sistema para a máxima eficiência em qualquer tipo de análise e fornece métodos para alternar de um tipo de análise para outro facilmente para uma transição perfeita.

A investigação de eventos no Sentinel geralmente começa com as Exibições de Eventos quase em tempo real. Embora ferramentas mais avançadas estejam disponíveis, as Exibições de Eventos exibem fluxos de evento filtrados juntamente com gráficos de resumo que podem ser usados para análises simples e rápidas de tendências de eventos, dados de evento, além de identificação de eventos específicos. Ao longo do tempo, você pode criar filtros ajustados para classes de dados específicas, como os resultados da correlação. É possível usar as Visualizações de Eventos como um painel de controle, mostrando uma postura geral operacional e de segurança.

Em seguida, você pode usar a pesquisa interativa para executar análises detalhadas de eventos. Isso permite que você pesquise e encontre de forma mais rápida e fácil dados relacionados a uma consulta específica, como a atividade de um usuário específico ou em sistema específico. Clicar nos dados do evento ou usar o painel de refinamento do lado esquerdo permite focar eventos de interesse específicos.

Ao analisar centenas de eventos, os recursos de relatório do Sentinel fornecem controle personalizado sobre o layout do evento e podem exibir volumes de dados maiores. O Sentinel facilita essa transição, permitindo que você transfira as pesquisas interativas incorporadas na interface da Pesquisa para um modelo de relatório. Isso cria instantaneamente um relatório que exibe os mesmos dados, mas em um formato mais bem adequado para uma quantidade maior de eventos.

O Sentinel inclui vários modelos de relatório para esse fim. Há dois tipos de modelos de relatórios:

- ♦ Modelos que são ajustados para exibir tipos particulares de informações, como dados de autenticação ou criação do usuário.
- ♦ Modelos de fins gerais que permitem que você personalize grupos e colunas no relatório interativamente.

Ao longo do tempo, você desenvolverá filtros e relatórios usados com frequência que facilitarão seus fluxos de trabalho. O Sentinel suporta o armazenamento e a distribuição dessas informações para as pessoas da sua empresa. Para obter mais informações, consulte o [Guia do usuário do Sentinel](#).



Planejando a instalação do Sentinel

Os seguintes capítulos o guiam pelo planejamento da instalação do seu Sentinel. Se você deseja instalar uma configuração que não está identificada nos capítulos que seguem ou se tiver quaisquer perguntas, entre em contato com o [Suporte técnico](#).

- ♦ Capítulo 3, “Lista de verificação da implementação” na página 31
- ♦ Capítulo 4, “Compreendendo as informações da licença” na página 33
- ♦ Capítulo 5, “Atendendo aos requisitos do sistema” na página 37
- ♦ Capítulo 6, “Considerações de implantação” na página 39
- ♦ Capítulo 7, “Considerações da implantação para o modo FIPS140-2” na página 55
- ♦ Capítulo 8, “Portas usadas” na página 63
- ♦ Capítulo 9, “Opções de instalação” na página 69

3 Lista de verificação da implementação

Use a seguinte lista de verificação para planejar, instalar e configurar o Sentinel.

Se você estiver atualizando de uma versão anterior do Sentinel, não use essa lista de verificação. Para obter informações sobre atualização, consulte o [Parte V, “Fazendo upgrade do Sentinel” na página 145](#).

<input type="checkbox"/> Tarefas	Consulte
<input type="checkbox"/> Revise as informações da arquitetura do produto para aprender sobre os componentes do Sentinel.	Parte I, “Compreendendo o Sentinel” na página 13.
<input type="checkbox"/> Revise as informações de licença do Sentinel para determinar se é necessário usar a licença de avaliação ou a licença empresarial do Sentinel.	Capítulo 4, “Compreendendo as informações da licença” na página 33.
<input type="checkbox"/> Avalie seu ambiente para determinar a configuração do hardware. Assegure que os computadores em que você instalará o Sentinel e seus componentes satisfaçam aos requisitos especificados.	Capítulo 5, “Atendendo aos requisitos do sistema” na página 37.
<input type="checkbox"/> Determine o tipo de implantação adequado ao seu ambiente com base nos eventos por segundo (EPS). Determine o número de instâncias do Collector Manager e do Correlation Engine que você precisa instalar para melhorar o desempenho e o equilíbrio de carga.	Capítulo 6, “Considerações de implantação” na página 39.
<input type="checkbox"/> Leia as notas de versão mais atuais do Sentinel para entender a nova funcionalidade e os problemas conhecidos.	Notas de versão do Sentinel
<input type="checkbox"/> Instale o Sentinel.	Parte III, “Instalando o Sentinel” na página 71.
<input type="checkbox"/> Configure o Sentinel.	Parte IV, “Configurando o Sentinel” na página 115.
<input type="checkbox"/> O Sentinel inclui regras de correlação prontas para uso. Algumas regras de correlação estão configuradas por padrão para executar uma ação que envia um e-mail quando a regra é acionada, como a ação Notificar Administrador de Segurança. Por isso, é necessário configurar as definições do servidor de correio eletrônico no servidor do Sentinel, configurando o Integrador SMTP e a ação Enviar E-mail.	Documentação de ação do SMTP Integrator e Enviar e-mail no site de Plug-ins do Sentinel .
<input type="checkbox"/> Instalando coletores e conectores adicionais no seu ambiente conforme necessário.	Capítulo 16, “Instalando coletores e conectores adicionais” na página 111.
<input type="checkbox"/> Instalando instâncias do Collector Manager e do Correlation Engine adicionais no seu ambiente conforme necessário.	Parte III, “Instalando o Sentinel” na página 71.

4 Compreendendo as informações da licença

O Sentinel é composto por uma ampla gama de funcionalidades, que atende a muitas necessidades de seus diversos clientes. Você pode escolher um modelo de licenciamento que atenda às suas necessidades.

A plataforma do Sentinel fornece os dois seguintes modelos de licenciamento:

- ♦ **Sentinel Enterprise:** Uma solução completa que possibilita todas as principais funções analíticas visuais em tempo real e diversos recursos adicionais. O Sentinel Enterprise foca em casos de uso de SIEM como detecção de ameaças, alertas e correções em tempo real.
- ♦ **Sentinel para Gerenciamento de registros:** Uma solução para casos de uso de gerenciamento de registros que permite coletar, armazenar, pesquisar e gerar relatórios com dados.

O Sentinel for Log Management representa um significativo upgrade em relação à funcionalidade oferecida no Sentinel Log Manager 1.2.2 e, em alguns casos, partes importantes da arquitetura sofreram alterações. Para planejar seu upgrade para o Sentinel para Gerenciamento de Registros, consulte a [Página de perguntas frequentes do Sentinel](#).

Dependendo das soluções e dos complementos adquiridos, é possível comprar as chaves de licença e os direitos apropriados para habilitar a funcionalidade correta no Sentinel. Embora as chaves de licença e direitos governem o acesso básico a recursos do produto e downloads, você deve consultar seu acordo de compra e o Acordo de licença por usuário final para termos e condições adicionais.

A tabela seguinte descreve os serviços e recursos específicos disponíveis em cada uma das soluções:

Tabela 4-1 Serviços e recursos do Sentinel

Serviços e recursos	Sentinel Enterprise	Sentinel for Log Management
Funcionalidade essencial	Sim	Sim
<ul style="list-style-type: none"> ♦ Coleta, análise e normalização de eventos, além de classificação taxonômica ♦ Coleta de dados não relacionados a eventos (dados de ativos, dados de vulnerabilidade e dados de identidade do usuário) ♦ Mapeamento contextual em linha ♦ Armazenamento de eventos com políticas de retenção e não repúdio ♦ Roteamento de eventos para armazenamento tradicional (interno e externo) ♦ Pesquisas e visualização de eventos ♦ Coleta, armazenamento e visualização de Fluxo de IP ♦ Gerador de relatórios ♦ Capacitação de Publicação de Normas de Processamento de Informações Federais 140-2 (FIPS 140-2) ♦ Ações desencadeadas manualmente ♦ Criação e gerenciamento manuais de incidentes 		
Link do Sentinel	Sim	Sim
Sincronização de dados	Sim	Sim
Restauração de dados do evento a partir do arquivo	Sim	Sim
Federação de dados (pesquisa distribuída)	Sim	Sim
Detecção de exploração (Assessor)*	Sim	Sim
Armazenamento escalável	Sim	Sim
Correlação	Sim	Não
<ul style="list-style-type: none"> ♦ Correlação de padrão de evento em tempo real ♦ Ações desencadeadas por regras de correlação ♦ Triagem de alertas ♦ Visualização de alerta 		
Inteligência de Segurança	Sim	Não
<ul style="list-style-type: none"> ♦ Regras de anomalia ♦ Análise estatística em tempo real 		

* O Advisor, fornecido pela Security Nexus, é um serviço complementar. Você precisa adquirir uma licença adicional para usar esse serviço.

Licenças do Sentinel

Esta seção oferece informações sobre os tipos de licenças do Sentinel.

- ♦ “[Licença para Avaliação](#)” na página 35
- ♦ “[Licença gratuita](#)” na página 35
- ♦ “[Licenças corporativas](#)” na página 35

Licença para Avaliação

A licença para avaliação padrão permite usar todos os recursos do Sentinel Enterprise por um período de avaliação específico sem limite de EPS, de acordo com a capacidade do seu hardware. Para obter informações sobre os recursos disponíveis no Sentinel Enterprise, consulte [Tabela 4-1, “Serviços e recursos do Sentinel”](#) na página 34.

A data de expiração do sistema é baseada nos dados mais antigos do sistema. Se você restaurar eventos antigos para o sistema, o Sentinel atualizará a data de vencimento conforme apropriado.

Após o vencimento da licença de avaliação, o Sentinel será executado com uma licença básica gratuita que habilita um conjunto limitado de recursos e uma taxa limitada de eventos de 25 EPS. Isso se aplicará apenas se o Sentinel estiver configurado com armazenamento tradicional.

Em implantações de armazenamento escalável, o Sentinel não armazenará mais eventos e dados brutos quando a licença de avaliação expirar.

Uma vez que você faz o upgrade para uma licença empresarial, o Sentinel recupera toda sua funcionalidade. Para evitar qualquer interrupção na funcionalidade, é preciso fazer upgrade do sistema com uma licença empresarial antes de a licença de avaliação expirar.

Licença gratuita

A licença gratuita permite usar um conjunto limitado de recursos, com uma taxa de eventos limitada de 25 EPS. A licença gratuita é aplicável apenas ao Sentinel com armazenamento tradicional.

A licença gratuita permite coletar e armazenar eventos. Quando a taxa de EPS ultrapassa 25, o Sentinel armazena os eventos recebidos, mas não exibe os detalhes desses eventos nos resultados de pesquisa ou relatórios. O Sentinel sinaliza esses eventos com a tag `OverEPSLimit`.

A licença gratuita não oferece recursos em tempo real. É possível restaurar toda a funcionalidade fazendo o upgrade da licença para uma licença empresarial.

Observação: Suporte técnico e atualizações de produtos não estão disponíveis para a versão gratuita do Sentinel.

Licenças corporativas

Ao adquirir o Sentinel, você receberá uma chave de licença por meio do portal do cliente. Dependendo da licença adquirida, sua chave de licença ativará recursos, taxas de coleta de dados e fontes de evento. Pode haver termos de licença adicionais que não são impostos pela chave de licença, portanto, leia seu contrato de licença com bastante atenção.

Para fazer alterações no seu licenciamento, contate o gerente da sua conta.

Você pode adicionar a chave de licença empresarial durante a instalação ou posteriormente. Para adicionar a chave de licença, consulte “[Adicionando uma chave de licença](#)” no [Guia de administração do Sentinel](#).

5 Atendendo aos requisitos do sistema

Uma implantação do Sentinel pode variar de acordo com as necessidades do seu ambiente, assim recomenda-se que você consulte os [Serviços de consultoria](#) ou qualquer um dos parceiros do Sentinel antes de finalizar a arquitetura do Sentinel para seu ambiente.

Para obter informações sobre recomendações de hardware, sistemas operacionais suportados, plataformas de aplicações e browsers, consulte o [Site de informações técnicas do Sentinel](#).

- ♦ “Requisitos do sistema do Conector e do Coletor” na página 37
- ♦ “Ambiente virtual” na página 37

Requisitos do sistema do Conector e do Coletor

Cada Conector e Coletor tem seu próprio conjunto de requisitos de sistema e plataformas suportadas. Consulte a documentação do Conector e do Coletor no [site de Plug-ins do Sentinel](#).

Ambiente virtual

O Sentinel é suportado em servidores VMware ESX. Ao configurar um ambiente virtual, as máquinas virtuais devem ter duas ou mais CPUs. Para atingir resultados de desempenho iguais aos resultados de testes da máquina física no ESX ou em qualquer outro ambiente virtual, o ambiente virtual deve fornecer memória, CPUs, espaço em disco e E/S idênticos aos recomendados para a máquina física.

Para obter informações sobre recomendações de máquinas físicas, consulte o [site de Informações técnicas do Sentinel](#).

6 Considerações de implantação

O Sentinel tem uma arquitetura escalável que pode ser expandida para lidar com a carga que você precisa colocar nele. Este capítulo fornece uma visão geral das considerações mais importantes a fazer ao escalar uma implantação do Sentinel. Um profissional do [Suporte técnico](#) ou dos [Serviços de parceiro](#) pode trabalhar com você para projetar o sistema do Sentinel que seja adequado para seu ambiente de TI.

- ♦ “Considerações sobre armazenamento de dados” na página 39
- ♦ “Vantagens das implantações distribuídas” na página 46
- ♦ “Implantação multifuncional” na página 48
- ♦ “Implantação distribuída de um nível” na página 48
- ♦ “Implantação distribuída de um nível com alta disponibilidade” na página 49
- ♦ “Implantação distribuída de dois e três níveis” na página 50
- ♦ “Implantação de três níveis com armazenamento escalável” na página 51

Considerações sobre armazenamento de dados

Dependendo da taxa de EPS, é possível optar por usar o armazenamento tradicional ou o armazenamento escalável para armazenar e indexar seus dados do Sentinel. A implantação do Sentinel depende do tipo de armazenamento de dados que você escolher usar.

Tabela 6-1 Comparação entre armazenamento tradicional e armazenamento escalável

Armazenamento tradicional	Armazenamento escalável
<p>Por padrão, os dados são armazenados no armazenamento tradicional com base no arquivo e a indexação é feita localmente no servidor do Sentinel.</p> <p>Além do armazenamento de dados com base no arquivo, também é possível optar por armazenar e indexar eventos no Visualization Data Store para aproveitar os recursos de visualização de dados. Para obter mais informações, consulte “Configurando o armazenamento de dados de visualização” na página 43.</p> <p>Perfeitamente escalável até aproximadamente 20 mil EPS. Além disso, é preciso adicionar outros servidores do Sentinel para escalar verticalmente até uma taxa de EPS muito mais alta.</p> <p>A coleta de dados é balanceada por carga em vários servidores do Sentinel. Por isso, os dados são distribuídos entre diferentes servidores do Sentinel e devem ser gerenciados individualmente.</p> <p>Os dados são rotulados como encarregados, mas não são segregados desta forma no disco.</p> <p>A replicação e disponibilidade de dados devem ser feitas manualmente ou ao utilizar mecanismos de armazenamento caros, como o disco SAN.</p>	<p>Os dados são armazenados em um armazenamento escalável com base em Hadoop e usam mecanismo de indexação distribuída escalável para indexar dados.</p> <p>Perfeitamente escalável a uma taxa de EPS muito grande, como um milhão de eventos por segundo.</p> <p>A coleta de dados é gerenciada por um único servidor do Sentinel. Por isso, o gerenciamento de dados e o gerenciamento de recursos são centralizados em um único servidor do Sentinel.</p> <p>Os dados são rotulados e segregados no disco como encarregados.</p> <p>A replicação e a disponibilidade de dados são econômicas, já que o Hadoop é executado em hardware padrão.</p>

- ♦ [“Planejando o armazenamento tradicional” na página 41](#)
- ♦ [“Planejando o armazenamento escalável” na página 44](#)
- ♦ [“Estrutura de diretórios do Sentinel” na página 46](#)

Planejando o armazenamento tradicional

O armazenamento de dados com base no arquivo tem uma estrutura de três camadas:

Armazena mento online	Armazenamento primário, antes conhecido como armazenamento local.	Otimizado para gravação e recuperação rápida. Armazena os dados de eventos coletados mais recentemente e pesquisados mais frequentemente.
	Armazenamento secundário, antes conhecido como armazenamento de rede. (opcional)	Otimizado para reduzir o uso de espaço em armazenamento opcionalmente de menor custo, ao mesmo tempo dando suporte a recuperação rápida. O Sentinel automaticamente migra as partições de dados para o armazenamento secundário.
	Observação: O uso do armazenamento secundário é opcional. Políticas de retenção de dados, pesquisas e relatórios funcionam em partições de dados de evento independentemente de se residem em armazenamentos primários, secundários ou em ambos.	
Armazena mento offline	Armazenamento em arquivo-morto	Quando as partições são fechadas, você pode fazer backup da partição para qualquer serviço de armazenamento de arquivos, como o Amazon Glacier. Você pode importar novamente temporariamente as partições para uso em análise forense sempre que necessário.

Você também pode configurar o Sentinel para extrair dados de evento e resumos de dados de evento para um banco de dados externo usando políticas de sincronização de dados. Para obter mais informações, consulte [“Configurando a sincronização de dados”](#) no *Guia de Administração do Sentinel*.

Ao instalar o Sentinel, é necessário montar a partição de disco para o armazenamento primário no local em que o Sentinel será instalado, como padrão, o diretório `/var/opt/novell`.

Toda a estrutura de diretório em `/var/opt/novell/sentinel` precisa residir em uma única partição de disco para garantir que os cálculos de uso de disco sejam realizados corretamente. Caso contrário, as capacidades de gerenciamento automático de dados poderão apagar dados de eventos prematuramente. Para obter mais informações sobre o diretório do Sentinel, consulte [“Estrutura de diretórios do Sentinel”](#) na página 46.

Como prática recomendada, certifique-se de que o diretório de dados esteja localizado em uma partição de disco diferente daquela em que se encontram os arquivos do sistema operacional, arquivos de configuração e executáveis. Os benefícios de armazenar dados variáveis separadamente incluem mais facilidade para realizar backups de conjuntos de campos, mais simplicidade na recuperação em casos de corrupção e robustez adicional caso uma partição de disco fique cheia. Ele também melhora o desempenho geral de sistemas em que sistemas de arquivos menores são mais eficientes. Para obter mais informações, consulte [Particionamento de disco](#).

Observação: Há uma limitação nos sistemas de arquivos ext3 para armazenamento de arquivos, que evita que um diretório tenha mais de 32000 arquivos ou subdiretórios. Você poderá usar o sistema de arquivos XFS se tiver um grande número de políticas de retenção ou se for manter os dados por períodos mais longos, como um ano.

- ♦ [“Use partições nas instalações tradicionais”](#) na página 42
- ♦ [“Usando partições em instalações de aplicação”](#) na página 42

- ♦ [“Melhores práticas para o layout da partição” na página 42](#)
- ♦ [“Configurando o armazenamento de dados de visualização” na página 43](#)

Use partições nas instalações tradicionais

Nas instalações tradicionais, você pode modificar o layout da partição de disco do sistema operacional antes de instalar o Sentinel. O administrador deverá criar e montar as partições desejadas para os diretórios adequados com base na estrutura de diretório detalhada em [“Estrutura de diretórios do Sentinel” na página 46](#). Ao executar o instalador, o Sentinel é instalado nos diretórios pré-criados, resultando em uma instalação que abrange várias partições.

Observação:

- ♦ É possível usar a opção `--location` ao executar o instalador para especificar um local de nível superior diferente do diretório padrão para armazenar o arquivo. O valor passado para a opção `--location` é anexado aos caminhos do diretório. Por exemplo, se você especificar `--location=/foo`, o diretório de dados será `/foo/var/opt/novell/sentinel/data` e o diretório de configuração será `/foo/etc/opt/novell/sentinel/config`.
 - ♦ Não use os links do sistema de arquivos (por exemplo, soft links) para a opção `--location`.
-

Usando partições em instalações de aplicação

Ao usar o formato de aplicação ISO do DVD, você poderá configurar o particionamento do sistema de arquivos da aplicação durante a instalação seguindo as instruções nas telas do YaST. Por exemplo, você pode criar uma partição separada para o ponto de montagem `/var/opt/novell/sentinel` para colocar todos os dados em uma partição separada. No entanto, para outros formatos de aplicação, é possível configurar o particionamento somente após a instalação. É possível adicionar partições e mover um diretório para a nova partição usando a ferramenta de configuração de sistema SuSE YaST. Para obter informações sobre como criar partições após a instalação, consulte [“Criando partições para armazenamento tradicional” na página 107](#).

Melhores práticas para o layout da partição

Muitas organizações têm os próprios esquemas de layout de partição de práticas recomendadas documentados para qualquer sistema instalado. A seguinte proposta de partição é feita para conduzir as organizações sem qualquer política definida e considera o uso específico do Sentinel para o sistema de arquivos. Em geral, o Sentinel cumpre o [Padrão de hierarquia do sistema de arquivos](#), quando praticável.

Partição	Ponto de montagem	Tamanho	Notas
Root	/	100 GB	Contém arquivos do sistema operacional e binários/configuração do Sentinel.
Inicialização	/boot	150 MB	Partição de boot

Partição	Ponto de montagem	Tamanho	Notas
Armazenamento primário	/var/opt/novell/sentinel	Calcule usando as Informações de dimensionamento do sistema .	Essa área conterá os dados coletados primários do Sentinel, além de outros dados variáveis, como arquivos de registro. Essa partição pode ser compartilhada com outros sistemas.
Armazenamento secundário	Local baseado em tipo de armazenamento, NFS, CIFS ou SAN (Storage area network).	Calcule usando as Informações de dimensionamento do sistema .	Essa área de armazenamento secundária, que pode ser montada localmente, como mostrado, ou remotamente.
Armazenamento em arquivo-morto	Sistema remoto	Calcule usando as Informações de dimensionamento do sistema .	Este armazenamento é para dados arquivados.

Configurando o armazenamento de dados de visualização

O Sentinel fornece visualizações de eventos que apresentam dados em gráficos, tabelas e mapas. Essas visualizações facilitam visualizar e analisar grandes volumes de eventos. Também é possível criar suas próprias visualizações e painéis de controle.

O Sentinel utiliza o Kibana, um painel de controle de análise e pesquisa baseado em browser, que ajuda você a pesquisar e visualizar eventos. O Kibana acessa dados do armazenamento de dados de visualização (Elasticsearch) para apresentar eventos em painéis de controle. Por padrão, o Sentinel inclui um nó Elasticsearch que armazena e indexa apenas alertas. Você deve habilitar a visualização de eventos para armazenar e indexar eventos no Elasticsearch.

Quando você habilita o Elasticsearch para armazenar e indexar dados, o Sentinel indexa apenas alguns campos de eventos específicos necessários para visualizações e armazena os campos indexados no Elasticsearch. O Sentinel cria um índice dedicado para cada dia e usa o fuso horário UTC (meia-noite-meia-noite) para calcular a data do índice. O nome do índice está no formato `security.events.normalized_yyyyMMdd`. Por exemplo, o índice `security.events.normalized_20160101` contém todos os eventos de 1º de janeiro de 2016.

A configuração da visualização do armazenamento de dados envolve o seguinte:

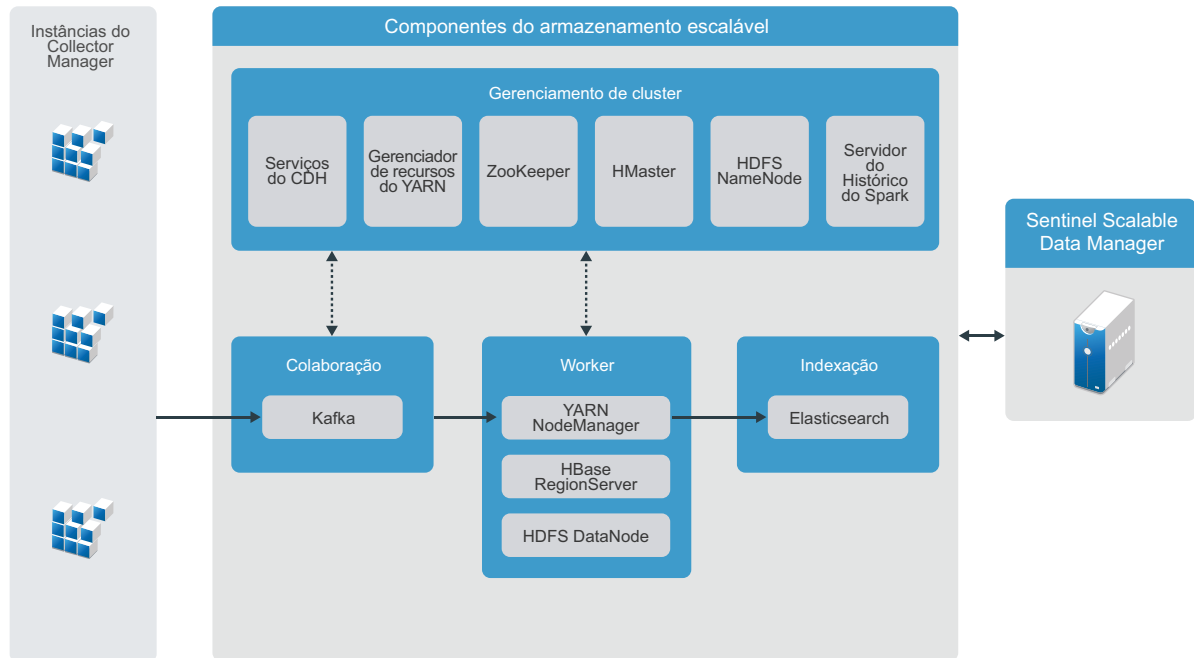
- ☐ **Instalar nós do Elasticsearch em um modo de cluster:** Por padrão, o Sentinel inclui um nó do Elasticsearch. Para obter o desempenho e a estabilidade ideais do servidor do Sentinel, é obrigatório instalar nós adicionais do Elasticsearch em um modo de cluster. Para obter mais informações, consulte [Capítulo 12, “Instalando e configurando o Elasticsearch”](#) na página 77.
- ☐ **Habilitar visualização de eventos:** A visualização de eventos está desabilitada por padrão. Para habilitar a visualização de eventos, consulte [Capítulo 20, “Habilitando a visualização de eventos”](#) na página 123.
- ☐ **Ajuste de desempenho:** O Sentinel configura automaticamente determinadas configurações do Elasticsearch para o desempenho ideal. É possível personalizar essas configurações conforme o necessário. Por exemplo, você pode modificar os campos de eventos que deseja que o Elasticsearch indexe. Para obter mais informações, consulte [“Ajuste de desempenho para o Elasticsearch”](#) na página 83.

Planejando o armazenamento escalável

O Sentinel usa a metodologia de Distribuição incluindo o Apache Hadoop (CDH) da Cloudera para armazenar e gerenciar grandes volumes de dados. Para indexar eventos, o Sentinel usa um mecanismo de indexação distribuída escalável chamado Elasticsearch do Elastic.

A ilustração seguinte explica os vários componentes usados em armazenamento escalável:

Figura 6-1 Arquitetura de armazenamento escalável



- ♦ **Colaboração:** O Sentinel usa o Apache Kafka como o sistema de mensagens escalável que recebe eventos normalizados e dados brutos das instâncias do Collector Manager. As instâncias do Collector Manager enviam dados brutos e dados de evento para clusters do Kafka.

Por padrão, o Sentinel cria os seguintes tópicos do Kafka:

- ♦ **security.events.normalized:** Armazena todos os dados de eventos processados e normalizados, incluindo eventos gerados pelo sistema e eventos internos.
- ♦ **security.events.raw:** Armazena todos os dados brutos das fontes de eventos.

Os dados de eventos e brutos seguem o esquema do Apache Avro. Para obter mais informações, consulte a [Documentação do Apache Avro](#). Os arquivos do esquema estão disponíveis no diretório `/etc/opt/novell/sentinel/scalablestore`.

- ♦ **Subordinado:** Esse nó hospeda tarefas de processamento e armazenamento em tempo real. O Apache Spark processa dados em larga escala em tempo real, por exemplo, segregando eventos com base em IDs de locatários, solicitando um grande volume de dados e armazenando dados no SOR (sistema de registro) e indexação escalável.

O Apache HBase é um armazenamento de dados distribuído e escalável com base em Hadoop. É usado como um SOR para eventos normalizados e dados brutos, segregados por IDs de arrendatários.

Baseado no ID de arrendatário, o Sentinel cria um namespace separado para cada arrendatário. Por exemplo, o namespace para o arrendatário padrão é 1. Em cada namespace, o Sentinel cria as seguintes tabelas e armazena dados com base no tempo do evento.

- ♦ **<ID_arrendatário>:security.events.normalized:** Armazena todos os dados de eventos processados e normalizados, incluindo eventos gerados pelo sistema e eventos internos.
- ♦ **<ID_arrendatário>:security.events.raw:** Armazena todos os dados brutos das fontes de eventos.
- ♦ **Gerenciamento de Cluster:** Esse nó hospeda todos os mestres e serviços de gerenciamento do cluster. O Apache ZooKeeper funciona como um serviço centralizado para manter informações de configuração, nomear serviços, fornecer sincronização distribuída e fornecer serviços de grupo.
- ♦ **Indexação:** O Sentinel usa o Elasticsearch como o mecanismo de indexação distribuída e escalável para eventos de indexação. É possível acessar dados do Elasticsearch para pesquisar e visualizar eventos.

O Sentinel cria um índice dedicado para cada dia e usa o fuso horário UTC (meia-noite-meia-noite) para calcular a data do índice. O nome do índice está no formato `security.events.normalized_yyyyMMdd`. Por exemplo, o índice `security.events.normalized_20160101` contém todos os eventos de 1º de janeiro de 2016. Para obter um desempenho ideal, o Sentinel indexa somente alguns campos de evento específicos. É possível modificar todos os campos de evento que você deseja que o Elasticsearch indexe. Para obter mais informações, consulte [“Ajuste de desempenho para o Elasticsearch” na página 83](#).

Configuração de armazenamento escalável

Quando você habilita o armazenamento escalável, a interface do usuário do servidor do Sentinel é reduzida para somente atender a alguns dos recursos do Sentinel, como coleta de dados, correlação, roteamento de eventos, pesquisa e visualização de eventos, além de executar certas atividades administrativas. Esta versão reduzida do Sentinel é referida como SSDM (Gerenciador de dados escaláveis do Sentinel). Para obter outros recursos do Sentinel, como Inteligência de Segurança, pesquisas convencionais e geração de relatórios, você deve instalar instâncias separadas do Sentinel com armazenamento tradicional e rotear os dados de eventos específicos do SSDM para o Sentinel usando o Sentinel Link.

A lista a seguir fornece informações sobre os serviços e os recursos não disponíveis no SSDM:

- ♦ Relatórios
- ♦ Inteligência de Segurança
- ♦ Executando operações de eventos durante a pesquisa
- ♦ Testando regras de correlação
- ♦ Criação e gerenciamento de incidentes
- ♦ Executando ações em eventos manualmente
- ♦ Sincronização de dados
- ♦ iTRAC Workflows
- ♦ Análise forense sobre os eventos que acionam o evento correlacionado
- ♦ Exibindo anexos de eventos para eventos do Secure Configuration Manager e do Guardiã de Mudanças

A habilitação do armazenamento escalável é uma configuração feita uma única vez, que não pode ser revertida. Se quiser desabilitar o armazenamento escalável e mudar para o armazenamento tradicional, você deverá reinstalar o Sentinel.

A lista de verificação seguinte fornece informações de alto nível sobre as tarefas que você precisa executar para configurar o armazenamento escalável:

Tabela 6-2 Lista de verificação da configuração de armazenamento escalável

Tarefas	Consulte
<input type="checkbox"/> Revise as informações de implantação para entender como implantar o Sentinel com armazenamento escalável.	“Implantação de três níveis com armazenamento escalável” na página 51
<input type="checkbox"/> Revise os pré-requisitos e conclua todas as tarefas solicitadas.	Capítulo 13, “Instalando e configurando o armazenamento escalável” na página 87.
<input type="checkbox"/> Habilite o armazenamento escalável. É possível habilitar o armazenamento escalável durante ou após a instalação. Nas instalações de upgrade, você pode habilitar o armazenamento escalável somente depois de fazer upgrade do Sentinel.	Para habilitar o armazenamento escalável durante a instalação, realize a instalação personalizada do Sentinel. Consulte a “Instalação personalizada do servidor do Sentinel” na página 92. Para habilitar o armazenamento escalável após a instalação ou o upgrade, consulte Habilitando o Armazenamento Escalável Pós-Instalação no Guia de Administração do Sentinel .
<input type="checkbox"/> Configure componentes do CDH e do Elasticsearch com o Sentinel.	Configurando o armazenamento escalável no Sentinel Administration Guide (Guia de Administração do Net IQ Sentinel).

Estrutura de diretórios do Sentinel

Por padrão, os diretórios do Sentinel estão nos seguintes locais:

- Os arquivos de dados ficam nos diretórios `/var/opt/novell/sentinel/data` e `/var/opt/novell/sentinel/3rdparty`.
- Os executáveis e as bibliotecas são armazenados no diretório `/opt/novell/sentinel`.
- Arquivos de registro estão no diretório `/var/opt/novell/sentinel/log`.
- Os arquivos temporários estão no diretório `/var/opt/novell/sentinel/tmp`.
- Arquivos de configuração estão no diretório `/etc/opt/novell/sentinel`.
- O arquivo de ID do processo (PID) está no diretório `/home/novell/sentinel/server.pid`.

Usando o PID, os administradores podem identificar o processo pai do servidor do Sentinel e monitorar ou encerra o processo.

Vantagens das implantações distribuídas

Por padrão, o servidor do Sentinel inclui os seguintes componentes:

- Collector Manager:** O Collector Manager oferece um ponto flexível para coleta de dados no Sentinel.

- ♦ **Correlation Engine:** O Correlation Engine processa eventos do fluxo de eventos em tempo real para determinar se eles devem acionar qualquer uma das regras de correlação.
- ♦ **Elasticsearch:** Um componente de armazenamento de dados opcional para armazenar e indexar dados. Por padrão, o Sentinel inclui um nó do Elasticsearch. Se você espera um EPS grande, mais de 2.500, deve implantar nós adicionais do Elasticsearch em um cluster.

Importante: Em ambientes de produção, você deve configurar uma implantação distribuída porque ela isola os componentes de coleta de dados em um computador separado, o que é importante para lidar com picos e outras anomalias com a máxima estabilidade do sistema.

Esta seção descreve as vantagens das implantações distribuídas.

- ♦ [“Vantagens de instâncias do Collector Manager adicionais” na página 47](#)
- ♦ [“Vantagens das instâncias adicionais do Correlation Engine” na página 47](#)

Vantagens de instâncias do Collector Manager adicionais

O servidor do Sentinel inclui um Collector Manager por padrão. No entanto, para ambientes de produção, instâncias do Collector Manager distribuídas fornecem um isolamento muito melhor quando grandes volumes de dados são recebidos. Nesse caso, um Collector Manager distribuído pode ficar sobrecarregado, mas o servidor do Sentinel continuará responsivo às solicitações dos usuários.

A instalação de mais de um Collector Manager em uma rede distribuída oferece as seguintes vantagens:

- ♦ **Melhor desempenho do sistema:** As instâncias do Collector Manager adicionais podem analisar e processar dados de eventos em um ambiente distribuído, o que aumenta o desempenho do sistema.
- ♦ **Segurança de dados adicional e menores requisitos de largura de banda de rede:** Se as instâncias do Collector Manager estiverem co-localizados com fontes de eventos, então a filtragem, criptografia e compactação de dados pode ser realizada na origem.
- ♦ **Cache de arquivos:** As instâncias do Collector Manager remotos podem fazer cache de grandes quantidades de dados enquanto o servidor está temporariamente ocupado arquivando eventos ou processando um pico de eventos. Esse recurso é uma vantagem para protocolos que, como o syslog, não suportam o cache de eventos de forma nativa.

Você pode instalar as instâncias do Collector Manager adicionais nos locais adequados na rede. Essas instâncias remotas do Collector Manager executam Conectores e Coletores e encaminham os dados coletados ao servidor do Sentinel para armazenamento e processamento. Para obter informações sobre a instalação de instâncias do Collector Manager adicionais, consulte [Parte III, “Instalando o Sentinel” na página 71](#).

Observação: Não é possível instalar mais do que um Collector Manager em um único sistema. Você pode instalar instâncias adicionais do Collector Manager nos sistemas remotos, e conectá-las ao servidor do Sentinel.

Vantagens das instâncias adicionais do Correlation Engine

Você pode implementar várias instâncias do Correlation Engine, cada qual em seu próprio servidor, sem precisar replicar configurações ou adicionar bancos de dados. Para ambientes com grandes números de regras de correlação ou taxas de evento extremamente altas, pode ser vantajoso

instalar mais de um Correlation Engine e reimplementar algumas regras no novo Correlation Engine. Várias instâncias do Correlation Engine fornecem a capacidade de escalar à medida que o sistema Sentinel incorpora fontes de dados adicionais ou à medida que as taxas de evento aumentam. Para obter informações sobre como instalar instâncias do Correlation Engine adicionais, veja [Parte III, “Instalando o Sentinel” na página 71](#).

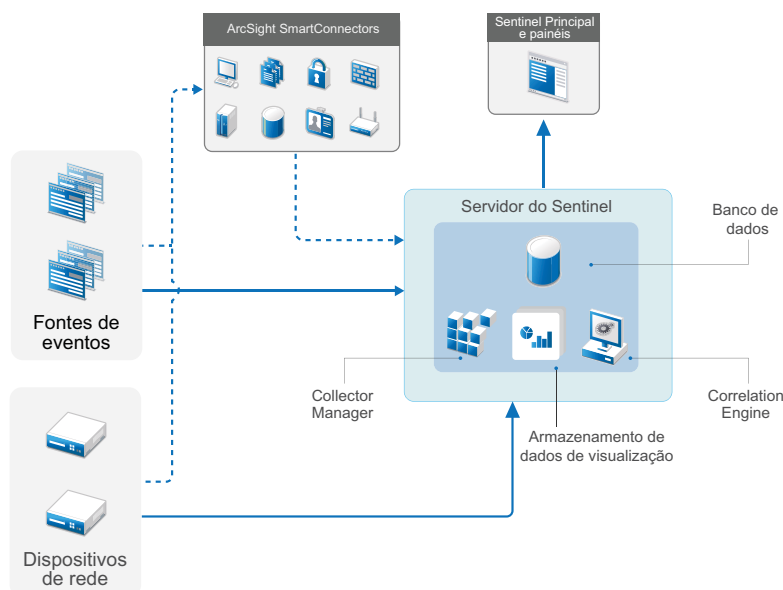
Observação: Não é possível instalar mais do que um Correlation Engine em um único sistema. Você pode instalar instâncias adicionais do Correlation Engine nos sistemas remotos, e conectá-los ao servidor do Sentinel.

Implantação multifuncional

A opção de implantação mais básica é um sistema multifuncional que contenha todos os componentes do Sentinel em um único computador. A implantação completa será adequada apenas se você estiver colocando uma parte relativamente pequena de carga no sistema e não precisar monitorar máquinas Windows. Em muitos ambientes, cargas imprevisíveis e flutuantes e conflitos de recurso entre os componentes podem causar problemas de desempenho.

Importante: Para ambientes de produção, você deve configurar uma implantação distribuída porque ela isola os componentes de coleta de dados em um computador separado, o que é importante para lidar com picos e outras anomalias com a máxima estabilidade do sistema.

Figura 6-2 Implantação multifuncional



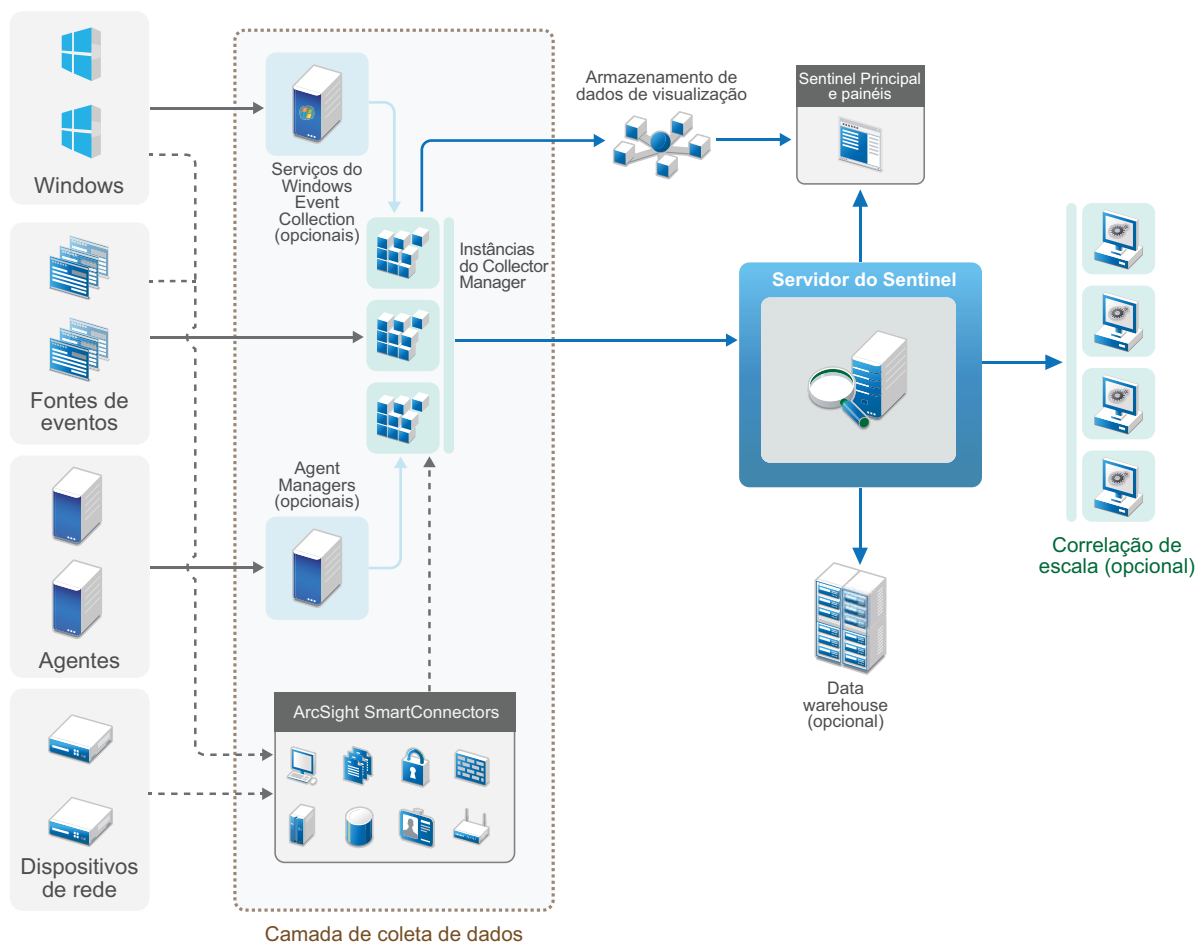
Implantação distribuída de um nível

A implantação em um nível adiciona a habilidade de monitorar máquinas Windows, bem como lidar com uma carga maior que a implantação multifuncional. É possível dimensionar a coleta e a correlação de dados adicionando os computadores do Collector Manager e Correlation Engine que descarregam o processamento do servidor central do Sentinel. Além de tratar a carga de regras de eventos e correlações, os Gerenciadores de Coletor e os Mecanismos de Correlação também

liberam recursos do servidor Sentinel central para atender outras solicitações, como armazenamento de evento e pesquisas. Conforme a carga aumenta no sistema, o servidor Sentinel central acabará se tornando um gargalo e você precisará de uma implantação com mais níveis para ampliar mais.

Opcionalmente, é possível configurar o Sentinel para copiar dados de evento para um data warehouse, que pode ser útil para descarregar relatório personalizado, análise e outros processamentos para outros sistemas.

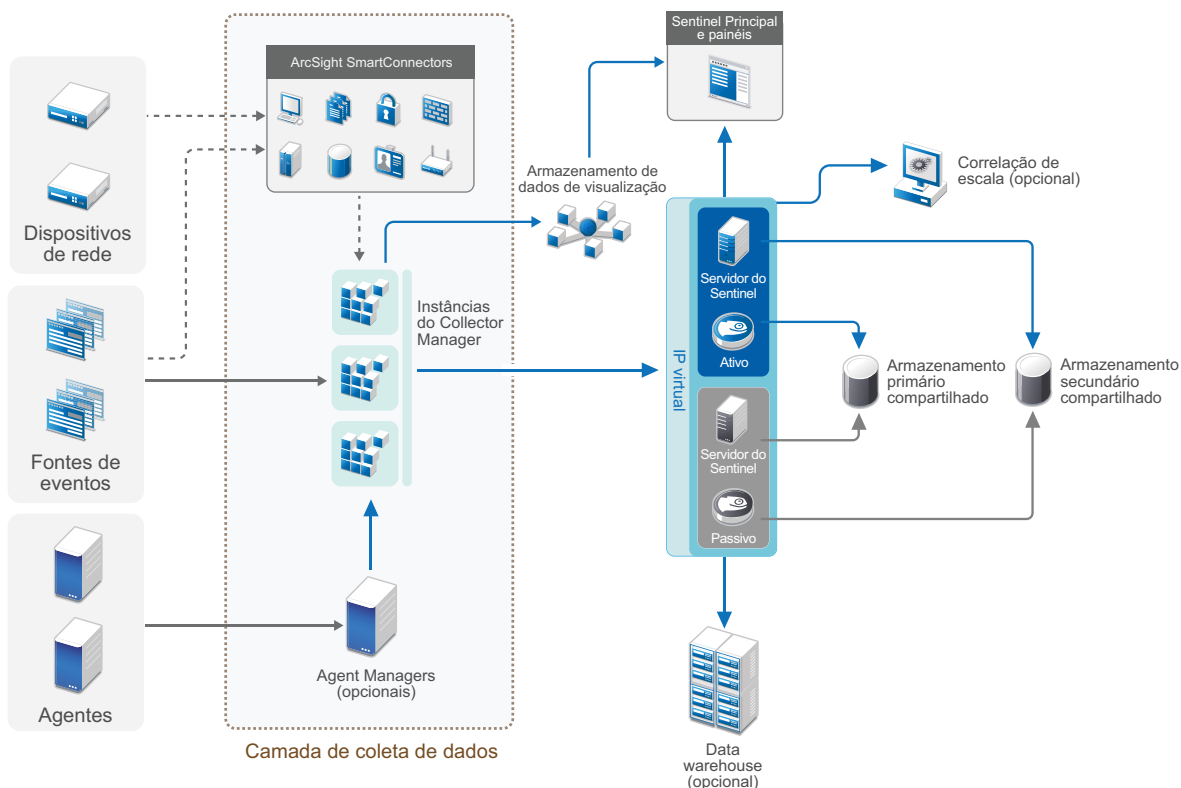
Figura 6-3 Implantação distribuída de um nível



Implantação distribuída de um nível com alta disponibilidade

A implantação distribuída em um nível mostra como pode ser transformado em um sistema altamente disponível com redundância de failover. Para obter mais informações sobre a implantação do Sentinel com alta disponibilidade, consulte [Parte VII, “Implantando o Sentinel para alta disponibilidade” na página 185](#).

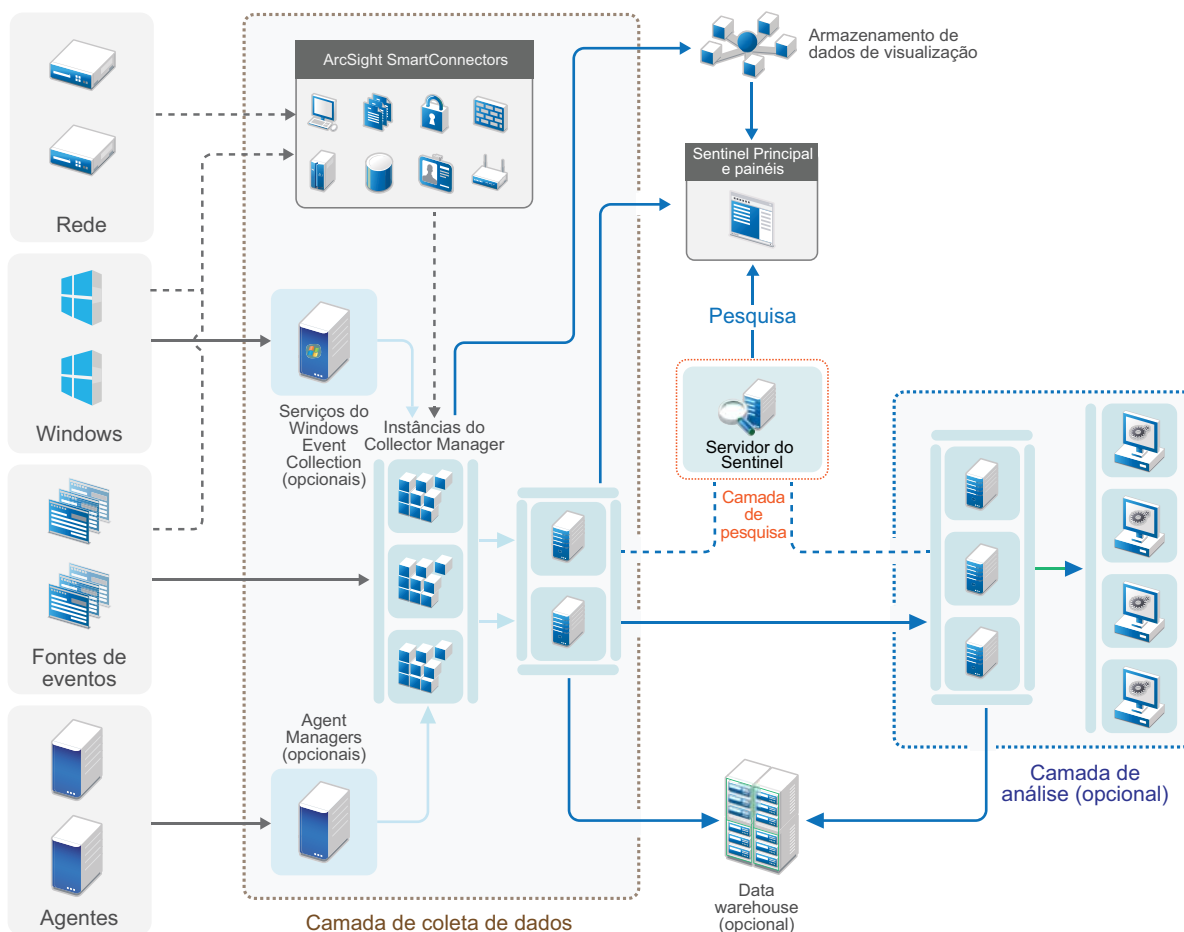
Figura 6-4 Implantação distribuída de um nível com alta disponibilidade



Implantação distribuída de dois e três níveis

Essa implantação permite que você supere as capacidades de tratamento de carga de um único servidor Sentinel central e compartilhe a carga de processamento entre várias instâncias do Sentinel aproveitando os recursos de Vínculo do Sentinel e Federação de dados do Sentinel. A coleta de dados tem carga balanceada através de vários servidores Sentinel, cada um com várias instâncias do Collector Manager, como mostrado no Nível de Coleta de Dados. Se você deseja realizar uma correlação de evento ou inteligência de segurança, pode encaminhar dados para o Nível de Análise usando o Link do Sentinel. O Nível de Pesquisa fornece um ponto de acesso único conveniente para pesquisar em todos os sistemas em todos os outros níveis usando a Federação de dados do Sentinel. Uma vez que a solicitação de pesquisa é federada em várias instâncias do Sentinel, essa implementação também tem propriedades de balanceamento de carga de pesquisa úteis em escala para lidar com uma carga de pesquisa pesada.

Figura 6-5 Implantação distribuída de dois e três níveis



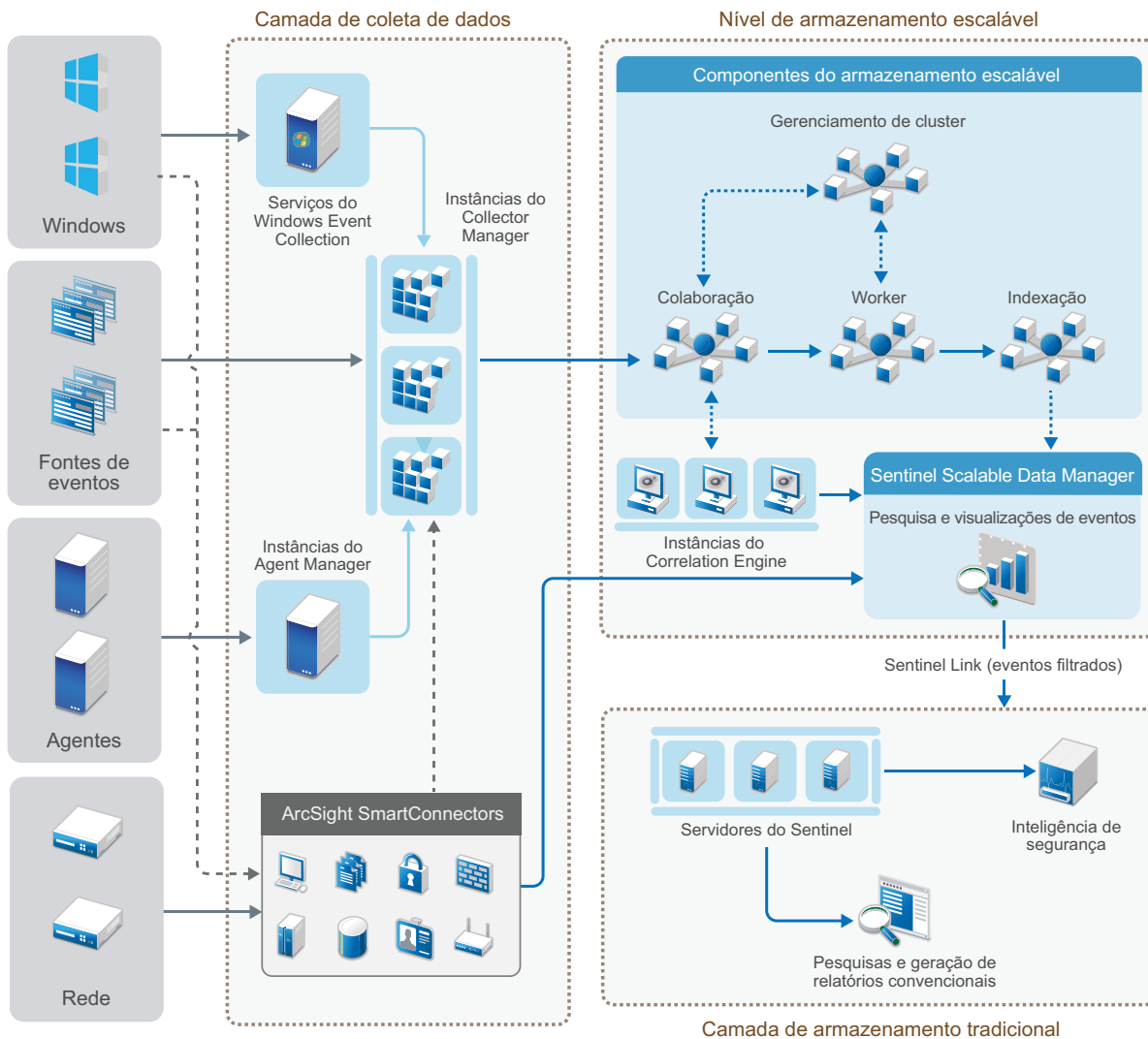
Implantação de três níveis com armazenamento escalável

Quando há necessidade de armazenamento de dados grandes e processamento de dados, e você não deseja distribuir eventos em vários servidores do Sentinel nem duplicar definições de configuração em várias instâncias, é possível configurar uma implantação distribuída de três níveis com armazenamento escalável. Essa implantação permite armazenar e gerenciar dados grandes usando um único servidor do Sentinel com armazenamento escalável, em vez de usar vários servidores do Sentinel.

Você pode configurar um novo servidor do Sentinel com armazenamento escalável ou fazer upgrade do servidor do Sentinel existente para habilitar o armazenamento escalável.

Dependendo dos recursos do Sentinel que você deseja usar, você pode determinar como deseja configurar a implantação do Sentinel.

Figura 6-6 Implantação de três níveis para armazenamento escalável



Esta implantação inclui os seguintes níveis:

- ♦ **Nível de coleta de dados:** Para coletar eventos de uma ampla faixa de fontes de eventos. Opcionalmente, se desejar manter a configuração de coleta de dados existente com o Sentinel de armazenamento tradicional e ainda aproveitar os recursos de armazenamento escaláveis, você poderá encaminhar os eventos desejados diretamente do armazenamento tradicional para o armazenamento escalável usando o script `data_uploader.sh`. Para obter mais informações, consulte [Capítulo 32, “Migrando dados para o armazenamento escalável”](#) na página 175.
- ♦ **Nível de armazenamento escalável:** Para armazenar, indexar e analisar grandes dados. O servidor do SSDM nessa camada habilita você a gerenciar a coleta e a correlação de dados e fornece outros recursos do SSDM. Para usar os recursos do Sentinel não disponíveis no SSDM, você pode configurar a camada de armazenamento tradicional. Você também pode encaminhar os dados coletados para qualquer outro sistema SIEM ou habilitar outras ferramentas de inteligência comercial para consultar os dados ou executar análises diretamente na sua distribuição Hadoop usando as APIs Hadoop, Kafka, Spark e Elasticsearch que têm amplo suporte.

- ♦ **Camada de armazenamento tradicional:** Para recursos do Sentinel, como Inteligência de Segurança, pesquisa convencional e geração de relatórios, você deve instalar instâncias separadas do Sentinel com armazenamento tradicional. Você pode configurar as regras de roteamento de eventos para encaminhar os eventos desejados do SSDM para o Sentinel usando o Sentinel Link.

Você pode realizar pesquisas e gerar relatórios usando qualquer um dos servidores do Sentinel no nível de armazenamento tradicional. Como opção, você pode configurar uma Camada de Pesquisa separada que forneça um ponto de acesso único conveniente para pesquisa e geração de relatórios em todos os servidores do Sentinel na camada de armazenamento tradicional. Para pesquisar eventos no armazenamento escalável, use a opção de pesquisa no SSDM.

Para obter mais informações sobre instalação e configuração do armazenamento escalável, consulte [Capítulo 13, “Instalando e configurando o armazenamento escalável” na página 87](#).

7 Considerações da implantação para o modo FIPS140-2

Opcionalmente, o Sentinel pode ser configurado para usar o Mozilla Network Security Services (NSS), que é um provedor criptográfico validado pelo FIPS 140-2, para sua criptografia interna e outras funções. A finalidade de fazer isso é assegurar que o Sentinel esteja "dentro do FIPS 140-2" e seja compatível com as políticas e os padrões de compra federais dos EUA.

Ativar o modo Sentinel FIPS 140-2 causa a comunicação entre o servidor do Sentinel, as instâncias remotas do Collector Manager do Sentinel, as instâncias remotas do Correlation Engine do Sentinel, a interface principal do Sentinel, o Sentinel Control Center e o serviço Sentinel Advisor para usar a criptografia validada pelo FIPS 140-2.

Importante: O modo FIPS é suportado apenas para o Sentinel. O Sentinel não será suportado se o sistema operacional estiver no modo FIPS.

- ♦ [“Implementação do FIPS no Sentinel” na página 55](#)
- ♦ [“Componentes ativados para FIPS no Sentinel” na página 56](#)
- ♦ [“Conexões de dados afetadas pelo modo FIPS” na página 57](#)
- ♦ [“Lista de verificação da implementação” na página 57](#)
- ♦ [“Cenários de implantação” na página 58](#)

Implementação do FIPS no Sentinel

O Sentinel usa as bibliotecas do Mozilla NSS que são fornecidas pelo sistema operacional. O RHEL (Red Hat Enterprise Linux) e o SLES (SUSE Linux Enterprise Server) têm conjuntos diferentes de pacotes NSS.

O módulo criptográfico NSS fornecido pelo RHEL 6.3 e posterior é validado pelo FIPS 140-2. O módulo criptográfico NSS incluído no SLES 11 ainda não foi oficialmente validado pelo FIPS 140-2, mas o trabalho está em andamento para validar o módulo SUSE pelo FIPS 140-2. Uma vez que a validação esteja disponível, nenhuma mudança necessária para o Sentinel é antecipada para disponibilizar "dentro do FIPS 140-2" na plataforma SUSE.

Para obter mais informações sobre o certificado RHEL FIPS 140-2, consulte <https://csrc.nist.gov/projects/cryptographic-module-validation-program/Certificate/2711> e <https://csrc.nist.gov/projects/cryptographic-module-validation-program/Certificate/1837>.

Pacotes RHEL NSS

O Sentinel requer os seguintes pacotes NSS de 64 bits para dar suporte ao modo FIPS 140-2:

- ♦ nspr-*
- ♦ nss-sysinit-*
- ♦ nss-util-*
- ♦ nss-softokn-freebl-*

- ♦ nss-softokn-*
- ♦ nss-*
- ♦ nss-tools-*

Se qualquer um desses pacotes não estiver instalado, instale-o antes de ativar o modo FIPS 140-2 no Sentinel.

Pacotes SLES NSS

O Sentinel requer os seguintes pacotes NSS de 64 bits para dar suporte ao modo FIPS 140-2:

- ♦ libfreebl3-*
- ♦ mozilla-nspr-*
- ♦ mozilla-nss-*
- ♦ mozilla-nss-tools-*

Se qualquer um desses pacotes não estiver instalado, instale-o antes de ativar o modo FIPS 140-2 no Sentinel.

Componentes ativados para FIPS no Sentinel

Os seguintes componentes do Sentinel fornecem o suporte do FIPS 140-2:

- ♦ Todos os componentes da plataforma Sentinel estão atualizados para suportar o modo FIPS 140-2.
- ♦ Os seguintes plug-ins do Sentinel que suportam criptografia estão atualizados para suportar o modo FIPS 140-2:
 - ♦ Agent Manager Connector 2011.1r1 e posterior;
 - ♦ Database (JDBC) Connector 2011.1r2 e posterior;
 - ♦ File Connector 2011.1r1 e mais recente (somente se o tipo de fonte de evento do arquivo for local ou NFS)
 - ♦ LDAP Integrator 2011.1r1 e posterior;
 - ♦ Sentinel Link Connector 2011.1r3 e posterior;
 - ♦ Sentinel Link Integrator 2011.1r2 e posterior;
 - ♦ SMTP Integrator 2011.1r1 e posterior;
 - ♦ Syslog Connector 2011.1r2 e posterior;
 - ♦ Windows Event (WMI) Connector 2011.1r2 e posterior.
 - ♦ Check Point (LEA) Connector 2011.1r2 e posterior
 - ♦ Syslog Integrator 2011.1r1 e posterior

Para obter mais informações sobre como configurar esses plug-ins do Sentinel para executar no modo FIPS 140-2, consulte [“Configurando os plug-ins do Sentinel para execução em modo FIPS 140-2” na página 134.](#)

Os seguintes Conectores do Sentinel que suportam criptografia opcional ainda não estão atualizados para dar suporte ao modo FIPS 140-2 no momento da liberação deste documento. No entanto, você pode continuar a coletar eventos usando esses Conectores. Para obter instruções sobre como usar esses Conectores com o Sentinel no modo FIPS 140-2, veja [“Usando conectores ativados não FIPS com o Sentinel no modo FIPS 140-2” na página 140.](#)

- ♦ Cisco SDEE Connector 2011.1r1
- ♦ File Connector 2011.1r1: as funcionalidades CIFS e SCP envolvem criptografia e não funcionarão no modo FIPS 140-2.
- ♦ Audit Connector 2011.1r1
- ♦ SNMP Connector 2011.1r1

Os seguintes Integradores do Sentinel que suportam SSL não estão atualizados para dar suporte ao modo FIPS 140-2 no momento da liberação deste documento. No entanto, é possível continuar a usar conexões não criptografadas quando esses Integradores são usados com o Sentinel no modo FIPS 140-2.

- ♦ Remedy Integrator 2011.1r1 ou posterior;
- ♦ SOAP Integrator 2011.1r1 ou posterior.

Quaisquer outros plug-ins do Sentinel que não estejam listados acima não usam criptografia nem são afetados pela ativação do modo FIPS 140-2 no Sentinel. Você não precisa executar nenhuma dessas etapas para usá-las com o Sentinel no modo FIPS 140-2.

Para obter mais informações sobre os plug-ins do Sentinel, consulte o [site de Plug-ins do Sentinel](#). Se você deseja solicitar que um dos plug-ins que ainda não foi atualizado seja disponibilizado com o suporte do FIPS, envie uma solicitação usando o [Bugzilla](#).

Conexões de dados afetadas pelo modo FIPS

Se o Sentinel estiver no modo FIPS 140-2, não será possível estabelecer conexões criptografadas com o Microsoft SQL Server. Essa consideração afeta os seguintes tipos de operações do Sentinel:

- ♦ Políticas de sincronização de dados para o SQL Server
- ♦ Servidor do Sentinel comunicando-se com o banco de dados do Agent Manager
- ♦ Conector de Banco de Dados coletando dados do SQL Server

Lista de verificação da implementação

A tabela a seguir fornece uma visão geral das tarefas necessárias para configurar o Sentinel para operação no modo FIPS 140-2.

Tarefas	Para obter mais informações, consulte...
Planejar a implantação.	“Cenários de implantação” na página 58.

Tarefas	Para obter mais informações, consulte...
Determine se você precisa habilitar o modo FIPS 140-2 durante a instalação do Sentinel ou se deseja ativá-lo no futuro. Para habilitar o Sentinel no modo FIPS 140-2 durante a instalação, você precisa selecionar o método de instalação, Personalizada ou Silenciosa, durante o processo de instalação.	“Instalação personalizada do servidor do Sentinel” na página 92. “Realizando uma instalação silenciosa” na página 97 Capítulo 23, “Ativando o modo FIPS 140-2 em uma instalação existente do Sentinel” na página 129
Configure os plug-ins do Sentinel para executar no Modo FIPS 140-2.	“Configurando os plug-ins do Sentinel para execução em modo FIPS 140-2” na página 134.
Importe certificados para o Sentinel FIPS Keystore.	“Importando certificados para o banco de dados de keystore do FIPS” na página 140

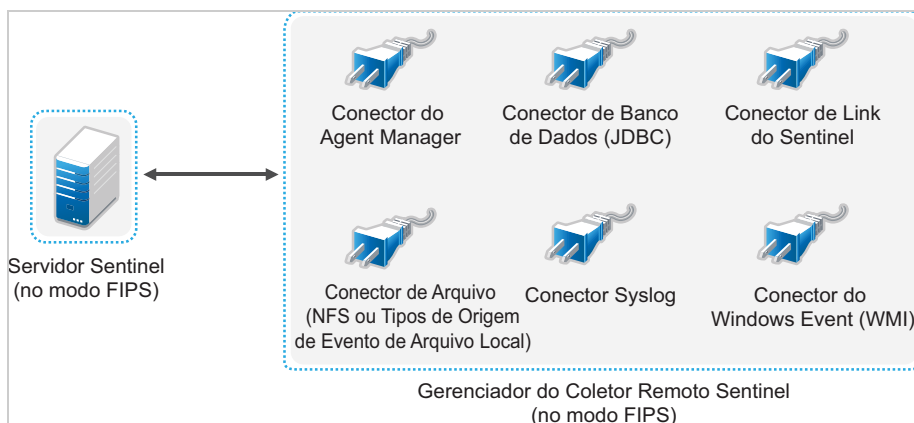
Observação: Faça o backup de seus sistemas Sentinel antes de iniciar a conversão para o modo FIPS. Se o servidor tiver de ser revertido para um modo não FIPS posteriormente, o único método suportado para fazer isso envolve a restauração de um backup. Para obter mais informações sobre a reversão para o modo não FIPS, consulte [“Revertendo o Sentinel para o modo não FIPS” na página 141.](#)

Cenários de implantação

Esta seção fornece informações sobre os cenários de implantação do Sentinel no modo FIPS 140-2.

Cenário 1: Coleta de dados no modo FIPS 140-2 completo

Neste cenário, a coleta de dados é feita apenas por meio de Conectores que suportam o modo FIPS 140-2. Presumiremos que esse ambiente envolve um servidor do Sentinel e os dados são coletados por meio de um Collector Manager remoto. Você pode ter um ou mais instâncias remotas do Collector Manager.



Execute o seguinte procedimento apenas se o seu ambiente envolver a coleta de dados das origens de evento usando Conectores que suportam o modo FIPS 140-2.

- 1 É necessário ter um servidor do Sentinel no modo FIPS 140-2.

Observação: Se o seu servidor do Sentinel (instalado ou atualizado recentemente) estiver no modo não FIPS, você deve habilitar o FIPS no servidor do Sentinel. Para obter mais informações, consulte [“Ativando o servidor do Sentinel para executar no Modo FIPS 140-2” na página 129.](#)

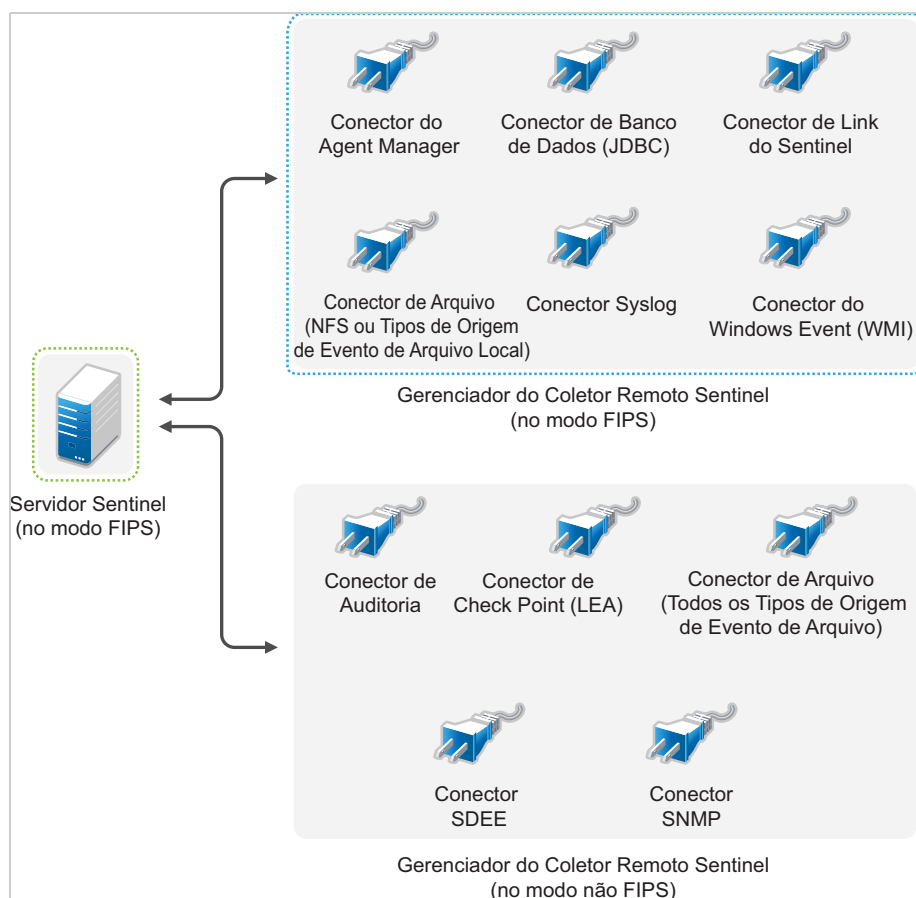
- 2 Um Collector Manager remoto do Sentinel deve estar em execução no modo FIPS 140-2.

Observação: Se o seu Collector Manager remoto (instalado ou atualizado recentemente) estiver executando no modo não FIPS, você deverá habilitar o FIPS no Collector Manager remoto. Para obter mais informações, consulte [“Ativando o modo FIPS 140-2 nas instâncias remotas do Collector Manager e do Correlation Engine” na página 130.](#)

- 3 Certifique-se de que o servidor FIPS e as instâncias remotas do Collector Manager comuniquem-se entre si.
- 4 Converta as instâncias remotas do Correlation Engine se algum deles estiver executando no modo FIPS. Para obter mais informações, consulte o [“Ativando o modo FIPS 140-2 nas instâncias remotas do Collector Manager e do Correlation Engine” na página 130.](#)
- 5 Configure os plug-ins do Sentinel para executar no Modo FIPS 140-2. Para obter mais informações, consulte [“Configurando os plug-ins do Sentinel para execução em modo FIPS 140-2” na página 134.](#)

Cenário 2: Coleta de dados no modo FIPS 140-2 parcial

Neste cenário, a coleta de dados é feita usando os Conectores que suportam o modo FIPS 140-2 e os Conectores que não suportam o modo FIPS 140-2. Presumimos que os dados sejam coletados por meio de um Collector Manager remoto. Você pode ter um ou mais instâncias remotas do Collector Manager.



Para manipular a coleta de dados usando Conectores que suportam e que não suportam o modo FIPS 140-2, você deve ter duas instâncias remotas do Collector Manager: um em execução no modo FIPS 140-2 para Conectores com suporte para FIPS e outro em execução no modo não FIPS (normal) para Conectores que não suportam o modo FIPS 140-2.

Você deve executar o procedimento a seguir se o seu ambiente envolver coleta de dados das origens de evento usando Conectores que suportam o FIPS 140-2 e Conectores que não suportam o modo FIPS 140-2.

- 1 É necessário ter um servidor do Sentinel no modo FIPS 140-2.

Observação: Se o seu servidor do Sentinel (instalado ou atualizado recentemente) estiver no modo não FIPS, você deve habilitar o FIPS no servidor do Sentinel. Para obter mais informações, consulte [“Ativando o servidor do Sentinel para executar no Modo FIPS 140-2” na página 129](#).

- 2 Certifique-se de que um Collector Manager remoto esteja sendo executando em modo FIPS 140-2 e outro Collector Manager remoto continue a ser executado no modo não FIPS.
 - 2a Se não tiver nenhum Collector Manager remoto ativado para o modo FIPS 140-2, você precisará habilitar o modo FIPS em um Collector Manager remoto. Para obter mais informações, consulte [“Ativando o modo FIPS 140-2 nas instâncias remotas do Collector Manager e do Correlation Engine” na página 130](#).
 - 2b Atualize o certificado do servidor no Collector Manager remoto não FIPS. Para obter mais informações, consulte [“Atualizando certificados do servidor nas instâncias do Collector Manager e do Correlation Engine remotos” na página 133](#).

- 3 Certifique-se de que duas instâncias remotas do Collector Manager se comuniquem com o servidor Sentinel ativado para o modo FIPS 140-2.
- 4 Configure as instâncias do Correlation Engine remotos se algum deles estiver executando no modo FIPS 140-2. Para obter mais informações, consulte [“Ativando o modo FIPS 140-2 nas instâncias remotas do Collector Manager e do Correlation Engine”](#) na página 130.
- 5 Configure os plug-ins do Sentinel para executar no modo FIPS 140-2. Para obter mais informações, consulte [“Configurando os plug-ins do Sentinel para execução em modo FIPS 140-2”](#) na página 134.
 - 5a Implante Conectores que suportam o modo FIPS 140-2 no Collector Manager remoto executando no modo FIPS.
 - 5b Distribua os Conectores que não suportam o modo FIPS 140-2 no Collector Manager remoto não FIPS.

8 Portas usadas

O Sentinel usa diversas portas para comunicação externa com outros componentes. Para a instalação da aplicação, as portas são abertas no firewall por padrão. No entanto, para a instalação tradicional, é preciso configurar o sistema operacional no qual o Sentinel está sendo instalado para abrir as portas no firewall.

- ♦ [“Portas do servidor do Sentinel” na página 63](#)
- ♦ [“Portas do Collector Manager” na página 65](#)
- ♦ [“Portas do Correlation Engine” na página 67](#)
- ♦ [“Portas de armazenamento escalável” na página 68](#)

Portas do servidor do Sentinel

O servidor Sentinel usa as seguintes portas para comunicações interna e externa.

Portas locais

O Sentinel usa as seguintes portas para comunicação interna com o banco de dados e outros processos internos:

Portas	Descrição
TCP 27017	Usado para o banco de dados de configuração de Inteligência de Segurança.
TCP 28017	Usado para o console da Web do banco de dados de Inteligência de Segurança.
TCP 32000	Usado para comunicação interna entre o processo do agrupador e o processo do servidor.
TCP 9200	Usada para comunicação com o serviço de indexação de alertas via REST.
TCP 9300	Usada para comunicação com o serviço de indexação de alertas via protocolo nativo.

Portas de rede

Para que o Sentinel funcione adequadamente, assegure-se de que as seguintes portas estejam abertas no firewall:

Portas	Direção	Necessária/ opcional	Descrição
TCP 5432	Interno	Opcional. Por padrão, esta porta escuta apenas a interface de loopback.	Usada pelo banco de dados PostgreSQL. Esta porta não precisa ser aberta por padrão. No entanto, você deve abrir esta porta ao desenvolver relatórios usando o Sentinel SDK. Para obter mais informações, consulte o Sentinel Plug-in SDK .

Portas	Direção	Necessária/ opcional	Descrição
TCP 1099 e 2000	Interno	Obrigatório	Usadas com ferramentas de monitoramento para se conectarem com o processo do servidor do Sentinel usando o JMX (Java Management Extensions).
TCP 1289	Interno	Opcional	Usada para conexões de auditoria.
UDP 1514	Interno	Opcional	Usada para mensagens syslog.
TCP 8443	Interno	Obrigatório	Usada para comunicação HTTPS.
TCP 1443	Interno	Opcional	Usada para mensagens syslog criptografadas por SSL.
TCP 61616	Interno	Opcional	Usada para conexões de entrada das instâncias do Collector Manager e do Correlation Engine.
TCP 10013	Interno	Obrigatório	Usadas pelo Sentinel Control Center e pelo Solution Designer.
TCP 1468	Interno	Opcional	Usada para mensagens syslog.
TCP 10014	Interno	Opcional	Usadas pelas instâncias remotas do Collector Manager para conectar ao servidor por meio do proxy SSL. No entanto, isso é incomum. Por padrão, as instâncias remotas do Collector Manager usam a porta SSL 61616 para conectar ao servidor.
TCP 443	Externo	Opcional	Se o Consultor for usado, a porta iniciará uma conexão ao serviço do Consultor pela Internet para a página de atualizações do Consultor .
TCP 8443	Externo	Opcional	Se a federação de dados for usada, a porta iniciará uma conexão para outros sistemas Sentinel, para executar a pesquisa distribuída.
TCP 389 ou 636	Externo	Opcional	Se a autenticação LDAP for usada, a porta iniciará uma conexão ao servidor LDAP.
TCP/UDP 111 e TCP/UDP 2049	Externo	Opcional	Se o armazenamento secundário estiver configurado para usar o NFS.
TCP 137, 138, 139, 445	Externo	Opcional	Se o armazenamento secundário estiver configurado para usar o CIFS.
TCP JDBC (dependente do banco de dados)	Externo	Opcional	Se a sincronização de dados for usada, a porta iniciará uma conexão para o banco de dados de destino usando JDBC. A porta usada depende do banco de dados de destino.
TCP 25	Externo	Opcional	Inicia uma conexão ao servidor de e-mail.
TCP 1290	Externo	Opcional	Quando o Sentinel encaminha eventos para outro sistema Sentinel, essa porta inicia uma conexão do Sentinel Link para esse sistema.
UDP 162	Externo	Opcional	Quando o Sentinel encaminha eventos para o sistema que está recebendo a detecção de SNMP, a porta envia um pacote para o receptor.
UDP 514 ou TCP 1468	Externo	Opcional	Essa porta é usada quando o Sentinel encaminha eventos para o sistema que está recebendo mensagens Syslog. Se a porta é UDP, ela envia um pacote para o receptor. Se a porta é TCP, ela inicia uma conexão ao receptor.

Portas	Direção	Necessária/ opcional	Descrição
TCP 9443	Interno	Opcional	Essa porta permite que um sistema Sentinel receba eventos de outro software SIEM, como o Guardião de Mudanças e o Gerenciador de Configuração Segura.

Portas específicas da aplicação do Sentinel Server

Em adição às portas acima, as seguintes portas estão abertas para a aplicação.

Portas	Direção	Necessária/ opcional	Descrição
TCP 22	Interno	Obrigatório	Usada para fornecer acesso seguro ao shell para a aplicação do Sentinel.
TCP 4984	Interno	Obrigatório	Também usada pelo serviço de atualização da aplicação do Sentinel.
TCP 289	Interno	Opcional	Encaminhada para 1289 para conexões de auditoria.
TCP 443	Interno	Opcional	Encaminhada para 8443 para comunicação HTTPS.
UDP 514	Interno	Opcional	Encaminhada para 1514 para mensagens syslog.
TCP 1290	Interno	Opcional	A porta do Sentinel Link que tem permissão para se conectar por meio do Firewall do SuSE.
UDP e TCP 40000 - 41000	Interno	Opcional	As portas podem ser usadas ao configurar servidores de coleta de dados, como o syslog. O Sentinel não se comunica nessas portas por padrão.
TCP 443 ou 80	Externo	Obrigatório	Inicia uma conexão ao repositório de atualização do software da aplicação na Internet ou um serviço SMT (Subscription Management Tool) na rede.
TCP 80	Externo	Opcional	Inicia uma conexão à SMT.
TCP 7630	Interno	Obrigatório	Usado pelo High Availability Web Konsole (Hawk).
TCP 9443	Interno	Obrigatório	Usado pelo Sentinel Appliance Management Console.
TCP 1098 e 2000	Interno	Obrigatório	Usadas com ferramentas de monitoramento para se conectarem com o processo do servidor do Sentinel usando o JMX (Java Management Extensions).

Portas do Collector Manager

O Collector Manager usa as seguintes portas para se comunicar com outros componentes.

Portas de rede

Para que o Collector Manager do Sentinel funcione adequadamente, assegure-se de que as seguintes portas estejam abertas no firewall:

Portas	Direção	Necessária/ opcional	Descrição
TCP 1289	Interno	Opcional	Usada para conexões de auditoria.
UDP 1514	Interno	Opcional	Usada para mensagens syslog.
TCP 1443	Interno	Opcional	Usada para mensagens syslog criptografadas por SSL.
TCP 1468	Interno	Opcional	Usada para mensagens syslog.
TCP 1099 e 2000	Interno	Obrigatório	Usadas com ferramentas de monitoramento para se conectarem com o processo do servidor do Sentinel usando o JMX (Java Management Extensions).
TCP 61616	Externo	Obrigatório	Inicia uma conexão para o servidor do Sentinel.
TCP 8443	Externo	Obrigatório	Inicie uma conexão com a porta do servidor Web do Sentinel.
			Deixe essa porta aberta somente durante a instalação e a configuração do Gerenciador de Coletor.

Portas específicas da aplicação do Collector Manager

Além das portas acima, as seguintes portas ficam abertas para a aplicação do Collector Manager do Sentinel.

Portas	Direção	Necessária/ opcional	Descrição
TCP 22	Interno	Obrigatório	Usada para fornecer acesso seguro ao shell para a aplicação do Sentinel.
TCP 4984	Interno	Obrigatório	Também usada pelo serviço de atualização da aplicação do Sentinel.
TCP 289	Interno	Opcional	Encaminhada para 1289 para conexões de auditoria.
UDP 514	Interno	Opcional	Encaminhada para 1514 para mensagens syslog.
TCP 1290	Interno	Opcional	Esta é a porta de vinculação do Sentinel que tem permissão para se conectar por meio do Firewall do SuSE.
UDP e TCP 40000 - 41000	Interno	Opcional	Usado ao configurar servidores de coleta de dados, como syslog. O Sentinel não se comunica nessas portas por padrão.
TCP 443	Externo	Obrigatório	Inicia uma conexão ao repositório de atualização do software da aplicação na Internet ou um serviço SMT (Subscription Management Tool) na rede.
TCP 80	Externo	Opcional	Inicia uma conexão à SMT.
TCP 9443	Interno	Obrigatório	Usado pelo Sentinel Appliance Management Console.
TCP 1098 e 2000	Interno	Obrigatório	Usadas com ferramentas de monitoramento para se conectarem com o processo do servidor do Sentinel usando o JMX (Java Management Extensions).

Portas do Correlation Engine

O Correlation Engine usa as seguintes portas para se comunicar com outros componentes.

Portas de rede

Para que o Sentinel Correlation Engine funcione adequadamente, assegure-se de que as seguintes portas estejam abertas no firewall:

Portas	Direção	Necessária/ opcional	Descrição
TCP 1099 e 2000	Interno	Obrigatório	Usadas com ferramentas de monitoramento para se conectarem com o processo do servidor do Sentinel usando o JMX (Java Management Extensions).
TCP 61616	Externo	Obrigatório	Inicia uma conexão para o servidor do Sentinel.
TCP 8443	Externo	Obrigatório	Inicie uma conexão com a porta do servidor Web do Sentinel. Deixe essa porta aberta somente durante a instalação e a configuração do Mecanismo de Correlação.

Portas específicas da aplicação do Correlation Engine

Além das portas acima, as seguintes portas ficam abertas na aplicação do Correlation Engine do Sentinel.

Portas	Direção	Necessária/ opcional	Descrição
TCP 22	Interno	Obrigatório	Usada para fornecer acesso seguro ao shell para a aplicação do Sentinel.
TCP 4984	Interno	Obrigatório	Também usada pelo serviço de atualização da aplicação do Sentinel.
TCP 443	Externo	Obrigatório	Inicia uma conexão ao repositório de atualização do software da aplicação na Internet ou um serviço SMT (Subscription Management Tool) na rede.
TCP 80	Externo	Opcional	Inicia uma conexão à SMT.
TCP 9443	Interno	Obrigatório	Usado pelo Sentinel Appliance Management Console.
TCP 1098 e 2000	Interno	Obrigatório	Usadas com ferramentas de monitoramento para se conectarem com o processo do servidor do Sentinel usando o JMX (Java Management Extensions).

Portas de armazenamento escalável

Para uma comunicação bem-sucedida do SSDM com o CDH e o Elasticsearch, verifique se as portas especificadas durante a configuração de armazenamento escalável estão abertas no firewall, além das portas exigidas pelo Cloudera e das portas listadas na seção [Portas do servidor do Sentinel](#).

9 Opções de instalação

Você pode executar uma instalação tradicional do Sentinel ou instalar a aplicação. Este capítulo fornece informações sobre as duas opções de instalação.

Instalação tradicional

A instalação tradicional instala o Sentinel em um sistema operacional existente usando o instalador do aplicativo. Você pode instalar o Sentinel das seguintes maneiras:

- ♦ **Interativo:** A instalação prossegue com entradas do usuário. Durante a instalação, você pode registrar as opções de instalação (entradas do usuário ou valores padrão) para um arquivo, que pode ser usado posteriormente em uma instalação silenciosa. É possível realizar tanto uma instalação padrão quanto uma instalação personalizada.

Instalação padrão	Instalação Personalizada
Usa os valores padrão para a configuração. A entrada do usuário só é obrigatória para a senha.	Solicita que você especifique os valores das opções de configuração. É possível selecionar os valores padrão ou especificar os valores necessários.
Instala com uma chave de avaliação padrão.	Permite instalar com a chave de licença de avaliação padrão ou com uma chave de licença válida.
Permite que você especifique a senha do administrador e use-a como senha padrão tanto para dbuser quanto para appuser.	Permite que você especifique a senha do administrador. Para dbauser e appuser, é possível especificar uma nova senha ou usar a senha do administrador.
Instala as portas padrão para todos os componentes.	Permite especificar portas para diferentes componentes.
Instala o Sentinel em modo não FIPS.	Permite que você instale o Sentinel em modo FIPS 140-2.
Usa o armazenamento tradicional para armazenar dados brutos e eventos.	Permite usar armazenamento escalável para armazenar dados brutos e eventos.
Autentica os usuários com o banco de dados interno.	Fornecer a opção de configuração da autenticação do LDAP para o Sentinel, em adição à autenticação do banco de dados. Quando o Sentinel é configurado para autenticação do LDAP, os usuários podem efetuar login no servidor usando suas credenciais do Novell eDirectory ou do Microsoft Active Directory.

Para obter mais informações sobre a instalação interativa, consulte [“Executando instalações interativas” na página 91](#).

- ♦ **Silencioso:** Se você deseja instalar diversos servidores Sentinel na sua implantação, poderá registrar as opções de instalação durante a instalação padrão ou personalizada em um arquivo de configuração e usá-lo para executar uma instalação autônoma. Para obter mais informações sobre a instalação silenciosa, veja [“Realizando uma instalação silenciosa” na página 97](#).

Instalação da aplicação

A instalação da aplicação instala o sistema operacional SLES 12 SP3 de 64 bits e o Sentinel.

A aplicação do Sentinel está disponível nos seguintes formatos:

- ♦ Uma imagem da aplicação OVF
- ♦ Uma imagem de aplicação ISO

Para obter mais informações sobre a instalação da aplicação, consulte [Capítulo 15, “Instalação da aplicação” na página 101](#).



Instalando o Sentinel

Esta seção fornece informações sobre a instalação do Sentinel e componentes adicionais.

- ♦ [Capítulo 10, “Visão geral da instalação” na página 73](#)
- ♦ [Capítulo 11, “Lista de verificação de instalação” na página 75](#)
- ♦ [Capítulo 12, “Instalando e configurando o Elasticsearch” na página 77](#)
- ♦ [Capítulo 13, “Instalando e configurando o armazenamento escalável” na página 87](#)
- ♦ [Capítulo 14, “Instalação tradicional” na página 91](#)
- ♦ [Capítulo 15, “Instalação da aplicação” na página 101](#)
- ♦ [Capítulo 16, “Instalando coletores e conectores adicionais” na página 111](#)
- ♦ [Capítulo 17, “Verificando a instalação” na página 113](#)

10 Visão geral da instalação

A instalação padrão do Sentinel instala os seguintes componentes no servidor do Sentinel:

- ♦ **Processos do servidor do Sentinel e do servidor web:** O processo do servidor do Sentinel processa solicitações de outros componentes do Sentinel e habilita a funcionalidade sem interrupções do sistema. O processo do servidor do Sentinel manipula solicitações, como filtragem de dados, processamento de consultas de pesquisa e gerenciamento de tarefas administrativas, que incluem a autenticação e autorização do usuário.

O Servidor Web do Sentinel permite uma conexão segura com a interface Principal do Sentinel.

- ♦ **Banco de dados PostgreSQL:** O Sentinel tem um banco de dados integrado que armazena informações de configuração do Sentinel, dados de ativos e vulnerabilidade, informações de identidade, status de incidente e workflow e assim por diante.
- ♦ **Banco de dados do MongoDB:** Armazena os dados de alertas e da Inteligência de Segurança.
- ♦ **Elasticsearch:** Indexa eventos e alertas para pesquisa e visualização.
- ♦ **Collector Manager:** O Collector Manager oferece um ponto flexível para coleta de dados no Sentinel. O instalador do Sentinel instala um Collector Manager por padrão durante a instalação.
- ♦ **Elasticsearch:** Um componente de armazenamento de dados opcional para armazenar e indexar dados. Por padrão, o Sentinel inclui um nó do Elasticsearch. Se você espera um EPS grande, mais de 2.500, deve implantar nós adicionais do Elasticsearch em um cluster.
- ♦ **Correlation Engine:** O Correlation Engine processa eventos do fluxo de eventos em tempo real para determinar se eles devem acionar qualquer uma das regras de correlação.
- ♦ **Advisor:** O Advisor, desenvolvido por Security Nexus, é um serviço de inscrição de dados opcional que fornece correlação no nível do dispositivo entre eventos em tempo real de detecções de intrusão e sistemas de prevenção e resultados de exploração de vulnerabilidades da empresa. Para obter mais informações sobre o Consultor, consulte “[Detectando vulnerabilidades e explorações](#)” no *Guia de administração do Sentinel*.
- ♦ **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. Você pode fazer download de plug-ins adicionais e atualizações no [site de Plug-ins do Sentinel](#). Os plug-ins do Sentinel incluem os que seguem:
 - ♦ Coletores
 - ♦ Conectores
 - ♦ Ações e regras de correlação;
 - ♦ Relatórios;
 - ♦ Fluxos de trabalho do iTRAC;
 - ♦ Solution Packs

11

Lista de verificação de instalação

Certifique-se de ter concluído as seguintes tarefas antes de iniciar a instalação:

- ☐ Verifique se o hardware e o software atendem aos requisitos de sistema listados em [Capítulo 5, “Atendendo aos requisitos do sistema” na página 37](#).
- ☐ Se houver uma instalação anterior do Sentinel, certifique-se de que não haja arquivos ou configurações de sistema restantes dessa instalação anterior. Para obter mais informações, consulte [Apêndice B, “Desinstalando” na página 229](#).
- ☐ Se você pretende instalar a versão licenciada, obtenha a chave de licença do [Centro de Atendimento ao Cliente](#).
- ☐ Confirme se as portas listadas em [Capítulo 8, “Portas usadas” na página 63](#) estão abertas no firewall.
- ☐ Para que o instalador do Sentinel funcione corretamente, o sistema deve ser capaz de retornar o nome do host ou um endereço IP válido. Para tal, adicione o nome do host ao arquivo `/etc/hosts` na linha contendo o endereço IP e insira `hostname -f` para garantir que o nome do host seja exibido adequadamente.
- ☐ Sincronize o horário usando o protocolo NTP (Network Time Protocol).
- ☐ Se planejar implantar o Sentinel com a configuração de armazenamento escalável, verifique se o CDH e o Elasticsearch estão instalados. Para obter mais informações sobre como implantar o Sentinel com armazenamento escalável, consulte [“Instalando e configurando o armazenamento escalável” na página 87](#).
- ☐ **Em sistemas RHEL:** Para obter o desempenho ideal, as configurações da memória devem ser definidas adequadamente para o banco de dados PostgreSQL. O parâmetro SHMMAX deve ser maior ou igual a 1073741824.

Para definir o valor adequado, anexe as seguintes informações ao arquivo `/etc/sysctl.conf`:

```
# for Sentinel Postgresql
kernel.shmmax=1073741824
```

☐ Para instalações tradicionais:

O sistema operacional do servidor do Sentinel deve incluir, pelo menos, os componentes do Servidor Base do servidor SLES ou do servidor RHEL 6. O Sentinel exige as versões de 64 bits dos seguintes RPMs:

- ♦ bash
- ♦ bc
- ♦ coreutils
- ♦ gettext
- ♦ glibc
- ♦ grep
- ♦ libgcc
- ♦ libstdc
- ♦ lsof

- ♦ net-tools
- ♦ openssl
- ♦ python-libs
- ♦ sed
- ♦ zlib

☐ **Para o Sentinel com armazenamento tradicional:**

Para ver as visualizações de eventos, defina a memória virtual adicionando a propriedade `vm.max_map_count=262144` ao arquivo `/etc/sysctl.conf`.

12 Instalando e configurando o Elasticsearch

Para indexação escalável e distribuída de eventos, você deve instalar o Elasticsearch em modo de cluster. O cluster Elasticsearch instalado para o Sentinel deve ser usado para indexar somente dados do Sentinel.

- ♦ “Pré-requisitos” na página 77
- ♦ “Instalando e configurando o Elasticsearch” na página 77
- ♦ “Protegendo dados no Elasticsearch” na página 79
- ♦ “Ajuste de desempenho para o Elasticsearch” na página 83
- ♦ “Reimplantar o plug-in de segurança do Elasticsearch” na página 84

Pré-requisitos

Conclua o seguinte pré-requisito antes de instalar o Elasticsearch:

- ♦ Com base na sua taxa de EPS, implante o Elasticsearch em um modo de cluster com o número de nós e o número de réplicas, conforme recomendado na página [Informações técnicas para o Sentinel](#).
- ♦ Defina os descritores de arquivos ao adicionar as seguintes propriedades no arquivo `/etc/security/limits.conf`:

```
elasticsearch hard nofile 65536
elasticsearch soft nofile 65536
elasticsearch soft as unlimited
```

Observação: Após concluir os pré-requisitos acima, execute o comando `sysctl -p` para recarregar as mudanças feitas nos arquivos.

Instalando e configurando o Elasticsearch

Você deve instalar o Elasticsearch e os plug-ins necessários em cada nó do cluster do Elasticsearch.

Para instalar e configurar o Elasticsearch:

- 1 Instale a versão do JDK suportada pelo Elasticsearch.
- 2 Faça download da versão certificada do Elasticsearch RPM. Para obter informações sobre a versão certificada do Elasticsearch e o URL de download, consulte a página [Technical Information for Sentinel](#) (Informações técnicas do Sentinel).
- 3 Instale o Elasticsearch:

```
rpm -i elasticsearch-<versão>.rpm
```
- 4 Conclua as tarefas conforme mencionado na tela nas instruções pós-instalação do RPM.
- 5 Verifique se o usuário do Elasticsearch tem acesso ao Java.

6 Configure o arquivo `/etc/elasticsearch/elasticsearch.yml` atualizando ou adicionando a seguinte informação:

Propriedade e valor	Notas
<code>cluster.name: <Elasticsearch_nome_do_cluster></code>	O nome do cluster que você especifica deve ser o mesmo para todos os nós.
<code>node.name: <nome_do_nó></code>	Cada nó deve ter um nome exclusivo.
<code>network.host: _<networkInterface>:ipv4_</code>	
<code>discovery.zen.ping.unicast.hosts: [<FQDN do nó elasticsearch no servidor do Sentinel>,<FQDN do nó1 do elasticsearch>, <FQDN do nó2 do elasticsearch> e assim por diante]</code>	
<code>thread_pool.bulk.queue_size: 300</code>	
<code>thread_pool.search.queue_size: 10000</code>	Uma vez que o tamanho da fila de pesquisa atinge seu limite, o Elasticsearch descarta todos os pedidos de pesquisa pendentes na fila. É possível aumentar o tamanho da fila de pesquisa com base no cálculo abaixo: <code>threadpool.search.queue_size =</code> Número médio de consultas de barra de rolagem por usuário para um painel de controle X número de fragmentos (por índice de dia) X número de dias (duração da pesquisa)
<code>index.codec: best_compression</code>	
<code>path.data: ["/<es1>", "/<es2>"]</code>	Distribua dados em vários locais ou discos independentes para reduzir a latência de E/S de disco. Configure vários caminhos para armazenar dados do Elasticsearch. Por exemplo <code>/es1</code> , <code>/es2</code> etc. Para obter melhor desempenho e gerenciabilidade, monte cada caminho em um disco físico separado (JBOD).

7 Atualize o tamanho do heap do Elasticsearch padrão no arquivo `/etc/elasticsearch/jvm.options`.

O tamanho do heap deve ser 50% da memória do servidor. Por exemplo, em um nó do Elasticsearch de 24 GB, aloque 12 GB como o tamanho do heap para obter o desempenho ideal.

8 Repita todas as etapas acima em cada nó do cluster do Elasticsearch.

- 9 No nó Elasticsearch do servidor Sentinel, configure o `/etc/opt/novell/sentinel/3rdparty/elasticsearch/elasticsearch.yml` conforme o seguinte:
- 9a Verifique se os valores de `cluster.name` e `discovery.zen.ping.unicast.hosts` no arquivo `elasticsearch.yml` são os mesmos que no arquivo `elasticsearch.yml` no nó Elasticsearch externo.
- 9b Especifique o endereço IP do host local seguido pelo endereço IP do nó local do Elasticsearch na propriedade `network.host` conforme segue:
- ```
network.host: ["127.0.0.1", "<Endereço IP do nó do Elasticsearch no Sentinel>"]
```
- 10 (Condicional) Para o Sentinel com armazenamento tradicional, adicione os endereços IP dos nós do Elasticsearch à propriedade `ServerList` no arquivo `/etc/opt/novell/sentinel/config/elasticsearch-index.properties`.
- Por exemplo: `ServerList=<IP1 do Elasticsearch>:<Porta>,<IP2 do Elasticsearch>:<Porta>`
- 11 Reinicie o Sentinel:
- ```
rcsentinel restart
```
- 12 Reinicie cada nó do Elasticsearch:
- ```
/etc/init.d/elasticsearch start
```
- 13 Para desempenho e estabilidade ideais do servidor do Sentinel, configure o nó do Elasticsearch no servidor do Sentinel como um nó elegível para master dedicado para que todos os dados de visualização de eventos sejam indexados em nós externos do Elasticsearch:
- 13a Efetue login no servidor do Sentinel como usuário novell.
- 13b Verifique se todos os dados de alerta existentes foram movidos para nós externos do Elasticsearch.
- 13c Abra o arquivo `/etc/opt/novell/sentinel/3rdparty/elasticsearch/elasticsearch.yml` e adicione as seguintes informações:
- ```
node.master: true
node.data: false
node.ingest: false
search.remote.connect: false
```
- 13d Reinicie o Elasticsearch:
- ```
rcsentinel stopSIdb
rcsentinel startSIdb
```
- 14 Avance para a [“Protegendo dados no Elasticsearch” na página 79](#).

## Protegendo dados no Elasticsearch

Os nós de cluster do Elasticsearch podem ser acessados por vários clientes, como os seguintes:

- Sentinel: para buscar e apresentar dados de eventos no painel de controle Visualização de Eventos.
- Tarefas do Spark em execução nos nós do NodeManager do YARN: para executar a indexação em massa dos eventos recebidos do Kafka. (para SSDM)

- ♦ Gerenciador de Coletor: para realizar a indexação em massa de eventos no Sentinel com o armazenamento tradicional.
- ♦ Outros clientes externos: para executar operações personalizadas, como análises personalizadas.

O Sentinel fornece um plug-in de segurança para o Elasticsearch denominado **elasticsearch-security-plugin**, que autentica e autoriza o acesso ao Elasticsearch.

O plug-in usa um token SAML ou uma lista de permissões para validação, dependendo de como os clientes se conectam:

- ♦ Quando um cliente envia um token SAML junto com a solicitação, o plug-in autentica o token no servidor de autenticação do Sentinel. Após a autenticação bem-sucedida, o plug-in permite acesso apenas aos eventos filtrados para os quais o cliente está autorizado.

Por exemplo, o painel de controle Visualização de Eventos (cliente) exibe apenas os eventos do Elasticsearch que uma função do usuário está autorizada a ver.

Para obter informações sobre funções e permissões, consulte “[Criando uma função](#)” no *Guia de Administração do Sentinel*.

- ♦ Quando um cliente não pode enviar um token SAML, o plug-in verifica sua lista de permissões de clientes legítimos. Após a validação bem-sucedida, o plug-in permite o acesso a todos os eventos sem filtragem.
- ♦ Quando um cliente não envia um token SAML válido ou não é permitido pela lista de permissões, o plug-in o considera um cliente ilegítimo e nega o acesso ao cliente.

Esta seção fornece informações sobre como instalar e configurar o plug-in de segurança do Elasticsearch:

- ♦ “[Instalando o plug-in de segurança do Elasticsearch](#)” na página 80
- ♦ “[Fornecendo acesso seguro a clientes adicionais do Elasticsearch](#)” na página 81
- ♦ “[Atualizando a configuração do plug-in do Elasticsearch](#)” na página 82

## Instalando o plug-in de segurança do Elasticsearch

Você deve instalar o plug-in de segurança do Elasticsearch em cada nó do cluster Elasticsearch e também no nó do Elasticsearch incluído no Sentinel.

**Para instalar o elasticsearch-security-plugin no nó do Elasticsearch incluído no Sentinel:**

- 1 Efetue login no servidor principal ou no servidor SSDM do Sentinel.
- 2 Defina o caminho para a variável de ambiente JAVA\_HOME da seguinte forma:

```
export JAVA_HOME=/<Sentinel_installation_path>/opt/novell/sentinel/jdk/
```

- 3 Instale o plug-in:

**Para Linux, efetue login como o usuário que o Elasticsearch está executando e execute o seguinte comando:**

```
<sentinel_installation_path>/opt/novell/sentinel/3rdparty/elasticsearch/bin/
elasticsearch-plugin install file://localhost/<Sentinel_installation_path>/
etc/opt/novell/sentinel/scalablestore/elasticsearch-security-plugin*.zip --
verbose
```

Quando solicitado a continuar com a instalação, digite *y*.

- 4 (Condicional) Se o Elasticsearch não estiver escutando na porta HTTP padrão (9200), você deverá atualizar o número da porta do Elasticsearch em cada entrada do arquivo `<caminho_de_instalação_do_Sentinel>/opt/novell/sentinel/3rdparty/elasticsearch/plugins/elasticsearch-security-plugin/elasticsearch-ip-whitelist.txt`.

Para obter mais informações, consulte [“Fornecendo acesso aos clientes do Elasticsearch com a lista de permissões” na página 82](#).

- 5 Reinicie os serviços de indexação no Sentinel usando o comando:

```
rcsentinel stopSldb
rcsentinel startSldb
```

### Para instalar o elasticsearch-security-plugin em nós externos do Elasticsearch:

Execute as etapas a seguir em cada nó no cluster do Elasticsearch:

- 1 Efetue login no servidor principal ou no servidor SSDM do Sentinel.
- 2 Copie o arquivo `<caminho_de_instalação_do_sentinel>/etc/opt/novell/sentinel/scalablestore/elasticsearch-security-plugin*.zip` para um local temporário em cada nó no cluster do Elasticsearch.

- 3 Instale o plug-in:

**Para Linux, efetue login como o usuário que o Elasticsearch está executando e execute o seguinte comando:**

```
<elasticsearch_install_directory>/bin/elasticsearch-plugin install file://
localhost/<full path of elasticsearch-security-plugin*.zip file> --verbose
```

Quando solicitado a continuar com a instalação, digite `y`.

- 4 (Condicional) Se o Elasticsearch não estiver escutando na porta HTTP padrão (9200), você deverá atualizar o número da porta do Elasticsearch em cada entrada do arquivo `<diretório_de_instalação_do_elasticsearch>/plugins/elasticsearch-security-plugin/elasticsearch-ip-whitelist.txt`.

Para obter mais informações, consulte [“Fornecendo acesso aos clientes do Elasticsearch com a lista de permissões” na página 82](#).

- 5 Reinicie o Elasticsearch.

## Fornecendo acesso seguro a clientes adicionais do Elasticsearch

Por padrão, os clientes confiáveis, como o servidor SSDM (para o painel de controle Visualização de Eventos) e o YRN NodeManagers, o servidor do Sentinel (para o painel de controle Visualização de Eventos) e o RCM têm acesso ao Elasticsearch. Se você quiser usar clientes adicionais do Elasticsearch, deverá fornecer acesso seguro a esses clientes adicionais usando o token SAML ou a lista de permissões.



## Fornecendo acesso aos clientes REST do Elasticsearch usando o token SAML

Se você estiver usando um cliente REST para acessar o Elasticsearch, será possível incluir um token SAML no cabeçalho da solicitação da seguinte maneira:

- 1 Obtenha um token SAML no servidor de autenticação do Sentinel. Para obter mais informações, consulte a documentação da API REST disponível no Sentinel.  
Clique em [Ajuda > APIs > Tutorial > Segurança de API > Obtendo um Token SAML \(Logon\)](#).
- 2 Use o token SAML nas solicitações REST subsequentes: inclua o token SAML no cabeçalho Autorização de cada solicitação feita pelo cliente REST. Especifique o nome do cabeçalho como `Autorização` e o valor do cabeçalho como o `<token SAML>` obtido na Etapa 1.

## Fornecendo acesso aos clientes do Elasticsearch com a lista de permissões

Por padrão, o Sentinel preenche automaticamente uma lista de permissões com os endereços IP dos clientes confiáveis do Elasticsearch, como o servidor SSDM (para o painel de controle Visualização de Eventos) e o YRN NodeManagers, o servidor do Sentinel (para o painel de controle Visualização de Eventos) e o RCM. O plug-in de segurança do Elasticsearch concede acesso ao Elasticsearch para todos os clientes listados em sua lista de permissões.

Para fornecer acesso a clientes adicionais que não enviam um token do Sentinel válido, você deve adicionar o endereço IP do cliente e o número da porta HTTP do servidor Elasticsearch à lista de permissões no formato `Endereço IP:porta`. Você deve verificar se os clientes externos adicionados à lista de permissões são legítimos e confiáveis para impedir qualquer acesso não autorizado.

### Para atualizar a lista de permissões:

- 1 Efetue login no servidor do Sentinel ou no nó do Elasticsearch como o usuário no qual o Elasticsearch está sendo executado.
- 2 Adicione a entrada  
`<IP_do_Cliente_do_Elasticsearch>:<Porta_HTTP_do_Elasticsearch_de_Destino>` ao arquivo:
  - ♦ `<caminho_de_instalação_do_Sentinel>/opt/novell/sentinel/3rdparty/elasticsearch/plugins/elasticsearch-security-plugin/elasticsearch-ip-whitelist.txt` para o nó do Elasticsearch incluído no Sentinel.
  - ♦ `<diretório_de_instalação_do_elasticsearch>/plugins/elasticsearch-security-plugin/elasticsearch-ip-whitelist.txt` para nós do Elasticsearch externos.Se houver várias entradas, adicione cada entrada em uma nova linha e grave o arquivo.
- 3 Repita as etapas acima em cada nó do cluster do Elasticsearch.

## Atualizando a configuração do plug-in do Elasticsearch

Nos casos em que você modificar o endereço IP/nome do host e o número da porta dos componentes de armazenamento escaláveis ou a versão e o número da porta do Elasticsearch, você deverá atualizar os arquivos de configuração do plug-in do Elasticsearch adequadamente.

### Execute as etapas a seguir em cada nó do cluster do Elasticsearch:

- 1 Efetue login no nó do Elasticsearch como o usuário no qual o Elasticsearch está sendo executado.

- 2 (Condicional) Se você modificou os endereços IP do NodeManager YARN, o endereço IP do servidor SSDM ou Sentinel, os endereços IP RCM ou o número da porta Elasticsearch, atualize a lista de permissões para verificar se o plug-in de segurança do Elasticsearch concede acesso aos clientes Elasticsearch.

Se você estiver configurando o SSDM ou o Sentinel no modo HA, adicione entradas para o endereço IP físico de cada nó ativo e nó passivo do cluster de alta disponibilidade.

Se você modificar o endereço IP físico de qualquer nó do cluster de alta disponibilidade ou adicionar um novo nó ao cluster de alta disponibilidade, atualize a lista de permissões com os endereços IP físicos dos nós modificados ou recém-adicionados.

Para obter mais informações, consulte [“Fornecendo acesso aos clientes do Elasticsearch com a lista de permissões” na página 82.](#)

- 3 (Condicional) Se você modificou o endereço IP do SSDM, o endereço IP do servidor do Sentinel ou o número da porta do servidor Web, atualize as propriedades `authServer.host` e `authServer.port` nos seguintes arquivos e reinicie o Elasticsearch:

- ♦ `<caminho_de_instalação_do_Sentinel>/opt/novell/sentinel/3rdparty/elasticsearch/plugins/elasticsearch-security-plugin/plugin-configuration.properties` para o nó do Elasticsearch incluído no Sentinel.
- ♦ `<diretório_de_instalação_do_elasticsearch>/plugins/elasticsearch-security-plugin/plugin-configuration.properties` para nós externos do Elasticsearch.

Se você estiver configurando o SSDM ou o Sentinel no modo HA, defina a propriedade `authServer.host` para o endereço IP virtual do cluster HA.

Se você modificar o endereço IP virtual do cluster de HA, atualize a propriedade `authServer.host` para o endereço IP virtual modificado.

- 4 (Condicional) Se você fez o upgrade do Elasticsearch para uma versão mais recente, atualize a propriedade `elasticsearch.version` nos seguintes arquivos e reinicie o Elasticsearch:
- ♦ `/opt/novell/sentinel/3rdparty/elasticsearch/plugins/elasticsearch-security-plugin/plugin-descriptor.properties` para o nó o Elasticsearch incluído no Sentinel.
  - ♦ `<diretório_de_instalação_do_elasticsearch>/plugins/elasticsearch-security-plugin/plugin-descriptor.properties` para nós externos do Elasticsearch.

## Ajuste de desempenho para o Elasticsearch

O Sentinel configura automaticamente as configurações do Elasticsearch descritas na tabela abaixo. É possível personalizar as configurações do Elasticsearch conforme necessário.

Para personalizar as configurações padrão:

**Para armazenamento tradicional:** Abra o arquivo `/etc/opt/novell/sentinel/config/elasticsearch-index.properties` e atualize as propriedades listadas na tabela conforme necessário.

**Para armazenamento escalável:** Na home page do SSDM, clique em **Armazenamento > Armazenamento Escalável > Propriedades Avançadas > Elasticsearch.**

**Tabela 12-1** Propriedades do Elasticsearch

| Propriedade                                      | Valor Padrão                                                                                                                                                                                                                                                                                                                                                                      | Notas                                                                                                                                                                                                                                                   |
|--------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| elasticsearch.events.lucen<br>efilter (opcional) |                                                                                                                                                                                                                                                                                                                                                                                   | Especifique um filtro para enviar apenas eventos específicos para o Elasticsearch para indexação. Por exemplo: Se você especificar o valor como sev:[3-5], somente os eventos com valores de gravidade entre 3 e 5 serão enviados para o Elasticsearch. |
| index.fields                                     | id,dt,rv171,msg,ei,evt,xda<br>staxname,xdasoutcomena<br>me,sev,vul,rv32,rv39,rv15<br>9,dhn,dip,rv98,dp,fn,rv199<br>,dun,tufname,rv84,rv158,s<br>hn,sip,rv76,sun,iufname,s<br>p,iudep,rv198,rv62,st,tid,sr<br>cgeo,destgeo,obsgeo,rv14<br>5,estz,estzmonth,estzdiy,e<br>stzdim,estzdiw,estzhour,es<br>tzmin,rv24,tudep,pn,xdasc<br>lass,xdasid,xdasreg,xdas<br>rov,iuident,tuident | Indica os campos de evento que você deseja que o Elasticsearch indexe.                                                                                                                                                                                  |
| es.num.shards                                    | 5                                                                                                                                                                                                                                                                                                                                                                                 | Indica o número de fragmentos primários por índice.<br><br>Você poderá aumentar esse valor padrão quando o tamanho do fragmento ultrapassar 50 GB.                                                                                                      |
| es.num.replicas                                  | 1                                                                                                                                                                                                                                                                                                                                                                                 | Indica o número de shards de réplica que cada shard primário deve ter.<br><br>É recomendado um cluster de pelo menos 2 nós considerando failover e alta disponibilidade.                                                                                |

## Reimplantar o plug-in de segurança do Elasticsearch

Você deve reimplantar; ou seja, desinstale e reinstale o plug-in de segurança Elasticsearch no nó Elasticsearch incluído no Sentinel e nos nós externos do Elasticsearch nos seguintes cenários:

- Adicionando ou modificando endereços IP remotos do Collector Manager.
- Desinstalando as instâncias do Collector Manager remotas.
- Habilitando a pós-instalação do armazenamento escalável.

Para reimplantar o plug-in de segurança do Elasticsearch:

- 1 Efetue login no servidor do Sentinel ou no nó do Elasticsearch como o usuário no qual o Elasticsearch está sendo executado.
- 2 Desinstale o plug-in usando o seguinte comando:
  - Para o Elasticsearch incluído no Sentinel: `<caminho_de_instalação_do_Sentinel>/opt/novell/sentinel/3rdparty/elasticsearch/bin/elasticsearch-plugin remove file://localhost/<caminho_de_instalação_do_Sentinel>/etc/opt/novell/sentinel/scalablestore/elasticsearchsecurity-plugin`
  - Para o Elasticsearch externo: `<diretório_de_instalação_do_elasticsearch> remove file://localhost/etc/opt/novell/sentinel/scalablestore/elasticsearchsecurity-plugin`

### 3 Reinstale o plug-in:

- ♦ Para o Elasticsearch incluído no Sentinel: `<caminho_de_instalação_do_Sentinel>/opt/novell/sentinel/3rdparty/elasticsearch/bin/elasticsearch-plugin install file://localhost/<caminho_de_instalação_do_Sentinel>/etc/opt/novell/sentinel/scalablestore/elasticsearchsecurity-plugin`
- ♦ Para o Elasticsearch externo: `<diretório_de_instalação_do_elasticsearch>/bin/elasticsearch-plugin install file://localhost/etc/opt/novell/sentinel/scalablestore/elasticsearchsecurity-plugin`

### 4 Reinicie o Elasticsearch usando o seguinte comando:

- ♦ Para o nó do Elasticsearch incluído no Sentinel:

```
rccsentinel stopSIdb
rccsentinel startSIdb
```

- ♦ Para nós externos do Elasticsearch:

```
sudo systemctl restart elasticsearch.service
```



# 13 Instalando e configurando o armazenamento escalável

Conclua os pré-requisitos listados na tabela a seguir para configurar o armazenamento escalável como opção de armazenamento de dados do Sentinel:

**Tabela 13-1** Pré-requisitos para habilitar o armazenamento escalável

| <input type="checkbox"/> Tarefas                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   | Consulte                                                                                                                                                                                       |
|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <input type="checkbox"/> Determine o número de nós de cluster de distribuição Hadoop e de nós de cluster Elasticsearch que você precisa configurar com base na taxa de EPS e no número necessário de réplicas.<br><br>Determine a versão certificada do CDH e do Elasticsearch.                                                                                                                                                                                                                                                                                                                                                                                    | <a href="#">Informações técnicas do Sentinel.</a>                                                                                                                                              |
| <input type="checkbox"/> O CDH, o Elasticsearch e o Sentinel têm sua própria matriz de suporte de plataforma. Revise a matriz de suporte da plataforma para cada um desses produtos e determine a plataforma que deseja usar.<br><br>Para o Elasticsearch, a instalação do RPM é recomendada porque o RPM inclui o script init. Isso instalará o Elasticsearch como um serviço e permitirá que ele automaticamente pare e inicie durante a reinicialização e upgrades, além de não sobregravar os arquivos de configuração.<br><br>A instalação do Elasticsearch RPM não é suportada no SLES 11. Portanto, determine uma plataforma adequada para o Elasticsearch. | <p>Matriz de suporte do CDH na documentação do Cloudera.</p> <p>Matriz de suporte do Elasticsearch na documentação do Elasticsearch.</p> <p><a href="#">Matriz de suporte do Sentinel.</a></p> |
| <input type="checkbox"/> Instale e configure o CDH em modo de cluster.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             | <a href="#">“Instalando e configurando o CDH” na página 88.</a>                                                                                                                                |
| <input type="checkbox"/> Instale e configure o Elasticsearch em modo de cluster.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   | <a href="#">“Instalando e configurando o Elasticsearch” na página 77.</a>                                                                                                                      |
| <input type="checkbox"/> Habilite o armazenamento escalável no Sentinel.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           | <a href="#">“Habilitando o armazenamento escalável” na página 89</a>                                                                                                                           |

# Instalando e configurando o CDH

Esta seção fornece informações sobre as configurações específicas solicitadas para instalar e configurar o CDH no Sentinel. Para obter informações detalhadas sobre a instalação e a configuração do CDH, consulte a versão certificada da documentação do Cloudera.

O Sentinel funciona com o Cloudera Express, a edição gratuita do CDH. O Sentinel também trabalha com o Cloudera Enterprise, que exige a compra de uma licença do Cloudera e inclui vários recursos não disponíveis na edição Cloudera Express. Se escolher começar com o Cloudera Express e mais tarde descobrir que precisa dos recursos disponíveis no Cloudera Enterprise, você poderá fazer upgrade do cluster após adquirir a licença do Cloudera.

- ♦ “Pré-requisitos” na página 88
- ♦ “Instalando e configurando o CDH” na página 89

## Pré-requisitos

Antes de instalar o CDH, você deve configurar os hosts de acordo com os seguintes pré-requisitos:

- ♦ Conclua os pré-requisitos mencionados na [documentação do Cloudera](#).
- ♦ Use o ext4 ou o sistema de arquivos XFS para obter melhor desempenho.
- ♦ O CDH precisa de alguns pacotes do sistema operacional que não são instalados por padrão. Portanto, você deve montar o respectivo DVD do sistema operacional. As instruções de instalação do Cloudera orientam sobre pacotes a serem instalados.
- ♦ Para sistemas operacionais do SLES, o CDH exige o pacote `python-psycopg2`. Instale o pacote `python-psycopg2`. Para obter mais informações, consulte a [documentação do openSUSE](#).
- ♦ Se você estiver usando máquinas virtuais, reserve o espaço em disco necessário no sistema de arquivos ao criar nós de máquinas virtuais. Por exemplo, no VMware, é possível usar o provisionamento significativo.
- ♦ Verifique se os nós de cluster do Sentinel e CDH estão no mesmo fuso horário.
- ♦ Defina a troca/transferência de todos os hosts como 1 no arquivo `/etc/sysctl.conf` adicionando a seguinte entrada:

```
vm.swappiness=1
```

Para aplicar essa configuração imediatamente, execute o comando a seguir:

```
sysctl -p
```

- ♦ A versão do JDK no CDH deve ser pelo menos a mesma versão do JDK usada no Sentinel. Se a versão do JDK disponível no CDH for inferior ao JDK do Sentinel, você deverá seguir as instruções para instalar o JDK manualmente em vez de instalar o JDK disponível no repositório do CDH.

Instale o JDK usando o arquivo binário (`.tar.gz`) porque a instalação de RPM do JDK causa problemas ao usar o script `manage_spark_jobs.sh` para enviar tarefas do Spark no YARN.

Para determinar a versão do JDK usada no Sentinel, consulte [Sentinel Release Notes](#) (Detalhes da versão do Sentinel).

## Instalando e configurando o CDH

Instale a versão certificada do CDH. Para obter mais informações sobre a versão certificada do CDH, consulte a página [Technical Information for Sentinel](#) (Informações técnicas do Sentinel). Consulte a versão certificada da [documentação do Cloudera](#) para obter instruções de instalação.

Enquanto instala o CDH, execute o seguinte:

- ♦ (Condicional) Se a instalação falhar durante a instalação do banco de dados PostgreSQL incorporado, execute as etapas a seguir:

```
mkdir -p /var/run/postgresql
```

```
sudo chown cloudera-scm:cloudera-scm /var/run/postgresql
```

- ♦ Ao escolher o tipo de instalação do software na janela **Selecionar Repositório**, verifique se a opção **Usar Pacotes** está marcada e selecione o Kafka em **Pacotes Adicionais**.
- ♦ Ao adicionar serviços, certifique-se de habilitar os seguintes serviços:
  - ♦ Cloudera Manager
  - ♦ ZooKeeper
  - ♦ HDFS
  - ♦ HBase
  - ♦ YARN
  - ♦ Spark
  - ♦ Kafka

---

**Observação:** O servidor de histórico Spark e o HDFS NameNode devem ser instalados no mesmo nó para garantir a confiabilidade do sistema. Para obter informações sobre a arquitetura do armazenamento escalável, consulte [“Planejando o armazenamento escalável” na página 44](#).

---

Ao ativar os serviços acima, configure a Alta Disponibilidade para os seguintes:

- ♦ HBase HMaster
- ♦ HDFS NameNode
- ♦ YARN ResourceManager
- ♦ (Condicional) Se o instalador não implantar a configuração do cliente devido à ausência de caminho Java, abra uma nova sessão do browser e atualize manualmente o caminho Java da seguinte maneira:

Clique em **Hosts > Todos os Hosts > Configuração** e especifique o caminho correto no campo **Diretório Pessoal do Java**.

## Habilitando o armazenamento escalável

É possível habilitar o armazenamento escalável durante ou após a instalação do Sentinel. Quando você habilita o armazenamento escalável durante a instalação, o Sentinel configura os componentes do CDH com valores padrão. Algumas dessas configurações são permanentes e não podem ser mudadas. Por exemplo, o número padrão de partições para tópicos do Kafka é 9 e esse valor não pode ser mudado.

Se desejar mudar os valores padrão, você deverá habilitar o armazenamento escalável após instalar o Sentinel e então definir as configurações para os componentes CDH como desejar.



Para instalações tradicionais, você pode habilitar o armazenamento escalável durante ou após a instalação do Sentinel. Para instalações de aplicação, é possível habilitar o armazenamento escalável somente após a instalação.

Nas instalações de upgrade, você pode habilitar o armazenamento escalável somente depois de fazer upgrade do Sentinel.

Antes de prosseguir com a habilitação do armazenamento escalável, tenha em mãos a lista de endereços IP ou nomes de host e números de portas Kafka, HDFS NameNode, YARN NodeManager, ZooKeeper e nós Elasticsearch. Você precisa dessa informação ao habilitar o armazenamento escalável.

Para habilitar o armazenamento escalável durante a instalação do Sentinel, consulte [“Instalação personalizada do servidor do Sentinel”](#) na página 92.

Para habilitar o armazenamento escalável após a instalação ou o upgrade do Sentinel, consulte [“Habilitando o Armazenamento Escalável Pós-Instalação”](#) no *Guia de Administração do Sentinel*.

# 14 Instalação tradicional

Este capítulo fornece informações sobre os diversos meios para instalar o Sentinel.

- ♦ “Executando instalações interativas” na página 91
- ♦ “Realizando uma instalação silenciosa” na página 97
- ♦ “Instalando o Sentinel como um usuário não raiz” na página 98

## Executando instalações interativas

Esta seção fornece informações sobre instalação padrão e personalizada.

- ♦ “Instalação padrão do servidor do Sentinel” na página 91
- ♦ “Instalação personalizada do servidor do Sentinel” na página 92
- ♦ “Instalação do Collector Manager e Correlation Engine” na página 95

## Instalação padrão do servidor do Sentinel

Use as seguintes etapas para executar uma instalação padrão:

- 1 Faça download do arquivo de instalação do Sentinel no [site de Downloads](#) da :
- 2 Especifique na linha de comando o seguinte comando para extrair o arquivo de instalação.

```
tar zxvf <install_filename>
```

Substitua <nome\_arquivo\_instalação> pelo nome real do arquivo de instalação.

- 3 Mude para o diretório no qual extraiu o instalador:

```
cd <directory_name>
```

- 4 Especifique o seguinte comando para instalar o Sentinel:

```
./install-sentinel
```

ou

Se desejar instalar o Sentinel em mais de um sistema, você pode registrar as opções de instalação em um arquivo. É possível usar esse arquivo para uma instalação independente do Sentinel em outros sistemas. Para registrar as opções de instalação, especifique o seguinte comando:

```
./install-sentinel -r <response_filename>
```

- 5 Especifique o número do idioma que deseja usar para a instalação e, em seguida, pressione Enter.

O contrato de licença de usuário final será exibido no idioma selecionado.

- 6 Pressione a barra de espaço para ler o contrato de licença.
- 7 Digite `sim` ou `s` para aceitar a licença e continuar a instalação.

A instalação poderá levar alguns segundos para carregar os pacotes de instalação e solicitar o tipo de configuração.

- 8 Quando solicitado, especifique 1 para prosseguir com a configuração padrão.

A instalação prossegue com a chave de licença de avaliação padrão incluída com o instalador. A qualquer momento durante ou após o período de avaliação, você pode substituir a licença de avaliação por uma chave de licença comprada.

- 9 Especifique a senha do usuário administrador `admin`.

- 10 Confirme a senha novamente.

Essa senha é usada por `admin`, `dbauser` e `appuser`.

A instalação do Sentinel é concluída e o servidor é iniciado. Poderá levar alguns minutos até que todos os serviços sejam iniciados depois da instalação, pois o sistema executa uma inicialização de uma única vez. Aguarde até que a instalação termine antes de efetuar login no servidor.

Para acessar a interface principal do Sentinel, especifique o seguinte URL em seu browser da web:

`https://IP_AddressOrDNS_Sentinel_server:8443/sentinel/views/main.html`

Em que `IP_AddressOrDNS_Sentinel_server` é o endereço IP ou o nome DNS do servidor do Sentinel e `8443` é a porta padrão do servidor do Sentinel.

## Instalação personalizada do servidor do Sentinel

Se estiver instalando o Sentinel com uma configuração personalizada, você poderá personalizar sua instalação do Sentinel especificando sua chave de licença, definindo uma senha diferente, especificando diferentes portas e assim por diante.

- 1 Se desejar habilitar o armazenamento escalável, conclua os pré-requisitos especificados em [Capítulo 13, “Instalando e configurando o armazenamento escalável” na página 87](#).
- 2 Faça download do arquivo de instalação do Sentinel no [site de Downloads da](#) :
- 3 Especifique na linha de comando o seguinte comando para extrair o arquivo de instalação.

```
tar zxvf <install_filename>
```

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

- 4 Especifique o seguinte comando na raiz do diretório extraído para instalar o Sentinel.

```
./install-sentinel
```

ou

Se desejar usar essa configuração padrão para instalar o Sentinel em mais de um sistema, você poderá gravar as opções de instalação em um arquivo. É possível usar esse arquivo para uma instalação independente do Sentinel em outros sistemas. Para registrar as opções de instalação, especifique o seguinte comando:

```
./install-sentinel -r <response_filename>
```

- 5 Especifique o número do idioma que deseja usar para a instalação e, em seguida, pressione Enter.  
O contrato de licença de usuário final será exibido no idioma selecionado.
- 6 Pressione a barra de espaço para ler o contrato de licença.
- 7 Digite `sim` ou `s` para aceitar o contrato de licença e prosseguir com a instalação.

A instalação poderá levar alguns segundos para carregar os pacotes de instalação e solicitar o tipo de configuração.

8 Especifique 2 para executar uma instalação personalizada do Sentinel.

9 Insira 1 para usar a chave de licença de avaliação padrão.

ou

Insira 2 para informar uma chave de licença adquirida do Sentinel.

10 Especifique a senha do usuário administrador `admin` e confirme a senha novamente.

11 Especifique a senha do usuário do banco de dados `dbauser` e confirme a senha novamente.

A conta `dbauser` é a identidade usada pelo Sentinel para interagir com o banco de dados. A senha inserida aqui pode ser usada para realizar tarefas de manutenção de banco de dados, incluindo a redefinição da senha do administrador, caso ela seja esquecida ou perdida.

12 Especifique a senha do usuário do aplicativo `appuser` e confirme a senha novamente.

13 Altere as atribuições de porta para os serviços do Sentinel inserindo o número desejado e, em seguida, especificando o novo número da porta.

14 Depois de alterar as portas, especifique 7 para concluir.

15 Insira 1 para autenticar os usuários usando somente o banco de dados interno.

ou

Se você configurou um diretório LDAP em seu domínio, insira 2 para autenticar os usuários usando a autenticação do diretório LDAP.

O valor padrão é 1.

16 **Se desejar habilitar o Sentinel no modo FIPS 140-2**, digite `s`.

16a Especifique uma senha forte para o banco de dados de keystore e confirme a senha novamente.

---

**Observação:** A senha deve ter, pelo menos, sete caracteres de comprimento. A senha deve conter, pelo menos, três das seguintes classes de caracteres: dígitos, letras ASCII minúsculas, letras ASCII maiúsculas, caracteres ASCII não alfanuméricos e caracteres não ASCII.

Se uma letra ASCII maiúscula for o primeiro caractere ou um dígito for o último caractere, eles não serão contados.

---

16b Se você deseja inserir certificados externos no banco de dados de keystore para estabelecer confiança, pressione `s` e especifique o caminho para o arquivo de certificado. Caso contrário, pressione `n`.

16c Conclua a configuração do modo FIPS 140-2 seguindo as tarefas mencionadas no [Capítulo 24, “Operando o Sentinel no modo FIPS 140-2” na página 131](#).

17 **Se desejar habilitar o armazenamento escalável**, digite `sim` ou `s` para habilitar o armazenamento escalável.

---

**Importante:** Depois de habilitar o armazenamento escalável, não será possível reverter a configuração, a menos que o Sentinel seja reinstalado.

---

- 17a** Especifique os endereços IP ou nomes de host e números de portas dos componentes do armazenamento escalável.
- 17b** (Condicional) Se desejar sair da configuração de armazenamento escalável e prosseguir com a instalação do Sentinel, digite `não` ou `n`.
- 17c** Após a conclusão da instalação do Sentinel, conclua a configuração de armazenamento escalável mencionada na seção [“Configuração pós-instalação para armazenamento escalável” na página 94](#).

A instalação do Sentinel é concluída e o servidor é iniciado. Poderá levar alguns minutos até que todos os serviços sejam iniciados depois da instalação, pois o sistema executa uma inicialização de uma única vez. Aguarde até que a instalação termine antes de efetuar login no servidor.

Para acessar a interface principal do Sentinel, especifique o seguinte URL em seu browser da web:

`https://IP_AddressOrDNS_Sentinel_server:8443/sentinel/views/main.html`

Em que `<IP_AddressOrDNS_Sentinel_server>` é o endereço IP ou o nome DNS do servidor do Sentinel e `8443` é a porta padrão do servidor do Sentinel.

## Configuração pós-instalação para armazenamento escalável

- 1 Efetue login no servidor SSDM.
- 2 Limpe o cache do seu browser para ver a versão do Sentinel que você instalou.
- 3 Para ver eventos e alertas, adicione o nó do Elasticsearch incluído no SSDM ao cluster do Elasticsearch que você configurou para armazenamento escalável:

No nó do Elasticsearch, abra o arquivo `/etc/opt/novell/sentinel/3rdparty/elasticsearch/elasticsearch.yml` e adicione as seguintes informações:

- ♦ `cluster.name: <Elasticsearch_nome_do_cluster>`
- ♦ `node.name: <nome_do_nó>`
- ♦ `discovery.zen.ping.unicast.hosts: [<FQDN do nó1 elasticsearch>, <FQDN do nó2 elasticsearch>]` e assim por diante]

Em todos os nós externos do Elasticsearch, abra `/etc/elasticsearch/elasticsearch.yml` e atualize

`discovery.zen.ping.unicast.hosts: [<FQDN do nó1 elasticsearch>, <FQDN do nó2 elasticsearch>]` e assim por diante]

---

**Observação:** Verifique se os valores dos parâmetros no arquivo local `elasticsearch.yml` e no arquivo `elasticsearch.yml` nos nós externos do Elasticsearch são os mesmos, exceto `network.host` e `node.name`, já que esses valores são exclusivos ao nó.

---

- 4 Reinicie os serviços de indexação usando o comando:

```
rcsentinel stopSldb
rcsentinel startSldb
```

- 5 Conclua a configuração de armazenamento escalável conforme mencionado nas seções a seguir:
  - ♦ [“Protegendo dados no Elasticsearch” na página 79](#)

- ♦ [Diretrizes de ajuste de desempenho](#) no *Guia de Administração do Sentinel*
- ♦ [Processando dados](#) no *Guia de Administração do Sentinel*

## Instalação do Collector Manager e Correlation Engine

Por padrão, o Sentinel instala um Collector Manager e um Correlation Engine. Para ambientes de produção, configure uma implantação distribuída porque ela isola os componentes de coleta de dados em uma máquina separada, o que é importante para lidar com picos e outras anomalias com a máxima estabilidade do sistema. Para obter informações sobre as vantagens da instalação de componentes adicionais, consulte [“Vantagens das implantações distribuídas”](#) na página 46.

---

**Importante:** Você deve instalar o Collector Manager ou o Correlation Engine adicional em sistemas separados: O Collector Manager ou o Correlation Engine não deve estar no mesmo sistema no qual o servidor do Sentinel está instalado.

---

**Lista de verificação de instalação:** Certifique-se de ter concluído as seguintes tarefas antes de iniciar a instalação.

- ♦ Certifique-se de que o hardware e o software atendem aos requisitos mínimos. Para obter mais informações, consulte [Capítulo 5, “Atendendo aos requisitos do sistema”](#) na página 37.
- ♦ Sincronize o horário usando o protocolo NTP (Network Time Protocol).
- ♦ O Collector Manager exige conectividade de rede na porta de barramento de mensagens (61616) no servidor do Sentinel. Antes de iniciar a instalação do Collector Manager, certifique-se de que todas as configurações do firewall e de rede podem se comunicar através dessa porta.

**Para instalar o Gerenciador de Coletor e o mecanismo de correlação, use as seguintes etapas:**

- 1 Inicie a interface principal do Sentinel especificando o seguinte URL em seu browser da web:

```
https://IP_AddressOrDNS_Sentinel_server:8443/sentinel/views/main.html
```

Em que `<IP_AddressOrDNS_Sentinel_server>` é o endereço IP ou o nome DNS do servidor do Sentinel e `8443` é a porta padrão do servidor do Sentinel.

Efetue login com o nome de usuário e senha especificados durante a instalação do servidor do Sentinel.

- 2 Na barra de ferramentas, clique em **Downloads**.
- 3 Clique em **Download do Instalador** na instalação desejada.
- 4 Clique em **Salvar Arquivo** para salvar o instalador no local desejado.
- 5 Especifique o seguinte comando para extrair o arquivo de instalação.

```
tar zxvf <install_filename>
```

Substitua `<nomearquivo_instalação>` pelo nome real do arquivo de instalação.

- 6 Mude para o diretório no qual extraiu o instalador.
- 7 Especifique o comando a seguir para instalar o Collector Manager ou o Correlation Engine

**Para o Collector Manager:**

```
./install-cm
```

**Para o Correlation Engine:**

```
./install-ce
```

ou

Se desejar instalar o Gerenciador de Coletor do Sentinel ou o Mecanismo de correlação em mais de um sistema, você pode registrar as opções de instalação em um arquivo. É possível usar esse arquivo para uma instalação independente do em outros sistemas. Para registrar as opções de instalação, especifique o seguinte comando:

**Para o Collector Manager:**

```
./install-cm -r <response_filename>
```

**Para o Correlation Engine:**

```
./install-ce -r <response_filename>
```

- 8 Especifique o número do idioma que deseja usar na instalação.

O contrato de licença de usuário final será exibido no idioma selecionado.

- 9 Pressione a barra de espaço para ler o contrato de licença.

- 10 Digite `sim` ou `s` para aceitar o contrato de licença e prosseguir com a instalação.

A instalação poderá levar alguns segundos para carregar os pacotes de instalação e solicitar o tipo de configuração.

- 11 Quando solicitado, especifique a opção adequada para prosseguir com a configuração Padrão ou Personalizada.

- 12 Digite o nome de host ou o endereço IP do servidor de comunicação da máquina na qual o Sentinel está instalado.

- 13 (Condicional) Se você selecionar a configuração Personalizada, especifique o seguinte:

**13a** Número da porta do canal de comunicação do servidor do Sentinel.

**13b** Número da porta do servidor da Web do Sentinel.

- 14 Quando solicitado a aceitar o certificado, verifique-o ao executar o seguinte comando no servidor do Sentinel:

Para modo FIPS:

```
/opt/novell/sentinel/jdk/jre/bin/keytool -list -keystore
/etc/opt/novell/sentinel/config/.activemqkeystore.jks
```

Para modo não FIPS:

```
/opt/novell/sentinel/jdk/jre/bin/keytool -list -keystore
/etc/opt/novell/sentinel/config/nonfips_backup/.activemqkeystore.jks
```

Compare a saída da certificação com a certificação de servidor do Sentinel exibida em [Etapa 12](#).

---

**Observação:** Se o certificado não corresponder, a instalação é interrompida. Execute a configuração da instalação novamente e verifique os certificados.

---

- 15 Aceite a certificação se a saída da certificação corresponder à certificação de servidor do Sentinel.

- 16 Especifique as credenciais de qualquer usuário na função de administrador. Digite o nome de usuário e a senha.

- 17 (Condicional) Se você selecionar a configuração Personalizada, digite `sim` ou `s` para ativar o modo FIPS 140-2 no Sentinel e continue com a configuração de FIPS.

- 18** (Condicional) Se seu ambiente usa autenticação forte ou multifator, você deve fornecer o ID do cliente do Sentinel e o segredo do cliente do Sentinel. Para obter mais informações sobre métodos de autenticação, consulte [“Métodos de autenticação”](#) no *Guia do Administrador do Sentinel*.

Para recuperar o ID do cliente do Sentinel e o segredo do cliente do Sentinel, vá para o seguinte URL:

```
https://Nome_de_host:porta/SentinelAuthServices/oauth/clients
```

Em que:

- ♦ *Nome\_de\_host* é o nome de host do servidor do Sentinel.
- ♦ *Porta* é a porta que o Sentinel usa (normalmente 8443).

O URL especificado usa sua sessão atual do Sentinel para recuperar o ID do cliente do Sentinel e o segredo do cliente do Sentinel.

- 19** (Condicional) Se você tiver habilitado a Visualização de eventos, deverá adicionar o Collector Manager à lista de permissões do Elasticsearch. Para obter mais informações, consulte [“Fornecendo acesso aos clientes do Elasticsearch com a lista de permissões”](#) na página 82.
- 20** Continue com a instalação, como solicitado, até que ela esteja concluída.

## Realizando uma instalação silenciosa

A instalação silenciosa ou autônoma será útil se for necessário instalar mais de um servidor do Sentinel, Gerenciador de Coletor ou Mecanismos de correlação em sua implantação. Em cenários como esse, você pode registrar os parâmetros de instalação durante a instalação interativa e depois executar o arquivo registrado nos outros servidores.

Para realizar a instalação silenciosa, você deve ter gravado os parâmetros de instalação em um arquivo. Para obter informações sobre a criação do arquivo de resposta, consulte [“Instalação padrão do servidor do Sentinel”](#) na página 91 ou [“Instalação personalizada do servidor do Sentinel”](#) na página 92 e [“Instalação do Collector Manager e Correlation Engine”](#) na página 95.

**Para habilitar o modo FIPS 140-2, certifique-se de que o arquivo de resposta inclua os seguintes parâmetros:**

- ♦ `ENABLE_FIPS_MODE`
- ♦ `NSS_DB_PASSWORD`

**Para executar uma instalação silenciosa, use as seguintes etapas:**

- 1 Faça download dos arquivos de instalação no [site de Downloads da](#) .
- 2 Faça login como `root` no servidor em que deseja instalar o Sentinel ou o Gerenciador de Coletor ou mecanismo de Correlação.
- 3 Especifique o seguinte comando para extrair os arquivos de instalação do arquivo tar:

```
tar -zxvf <install_filename>
```

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

- 4 Especifique o seguinte comando para instalar o Sentinel em modo silencioso:

Para servidor do Sentinel:

```
./install-sentinel -u <response_file>
```

Para o Collector Manager:



```
./install-cm -u <response_file>
```

Para o Correlation Engine:

```
./install-ce -u <response_file>
```

A instalação prossegue com os valores armazenados no arquivo de resposta.

Se você instalou um servidor do Sentinel, poderá levar alguns minutos até que todos os serviços sejam iniciados depois da instalação, pois o sistema executa uma inicialização de uma única vez. Aguarde até que a instalação termine antes de efetuar login no servidor.

- 5 (Condicional) se você selecionar ativar o modo FIPS 140-2 para o servidor do Sentinel,** conclua a configuração do modo FIPS 140-2 seguindo as tarefas mencionadas no [Capítulo 24, “Operando o Sentinel no modo FIPS 140-2”](#) na página 131.

## Instalando o Sentinel como um usuário não raiz

Se a sua política organizacional não permitir que você execute a instalação completa do Sentinel como usuário `root`, instale o Sentinel como um usuário não `root` ; ou seja, como o usuário `Novell`. Nessa instalação, algumas etapas são executadas como um usuário `root` e, em seguida, você prossegue para a instalação do Sentinel como um usuário `novell` criado pelo usuário `root`. Finalmente, o usuário `root` completa a instalação.

Ao instalar o Sentinel como um usuário não `root`, você deve instalar o Sentinel como o usuário `novell`. Não há suporte para instalações não raiz que não sejam o usuário `Novell`, embora a instalação prossiga com êxito.

---

**Observação:** Ao instalar o Sentinel em um diretório não padrão já existente, certifique-se de que o usuário tem permissões de propriedade no diretório. Execute o seguinte comando para atribuir as permissões de propriedade:

```
chown novell:novell <non-default installation directory>
```

---

- 1 Faça download dos arquivos de instalação no [site de Downloads da](#) .
- 2 Especifique o seguinte comando na linha de comando para extrair os arquivos de instalação do arquivo `tar`:

```
tar -zxvf <install_filename>
```

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

- 3 Efetue login como `root` no servidor em que você deseja instalar o Sentinel como `root`.
- 4 Especifique o seguinte comando:

```
./bin/root_install_prepare
```

Uma lista de comandos a serem executados com privilégios de `root` será exibida. Se você desejar que o usuário não raiz instale o Sentinel em um local que não seja o padrão, especifique a opção `--location` juntamente com o comando. Por exemplo:

```
./bin/root_install_prepare --location=/foo
```

O valor passado para a opção `--location foo` é anexado aos caminhos do diretório.

Isso também cria um grupo `novell` e um usuário `novell`, caso ainda não existam.

- 5 Aceite a lista de comandos.  
Os comandos exibidos serão executados.

- 6 Especifique o comando a seguir para mudar o usuário não root recém-criado, ou seja, o novell:
- ```
su novell
```
- 7 (Condicional) Para realizar uma instalação interativa:
- 7a Especifique o comando apropriado, dependendo do componente que você está instalando:

Componente	Comando
Servidor do Sentinel	Local padrão: <code>./install-sentinel</code> Local diferente do padrão: <code>./install-sentinel --location=/foo</code>
Collector Manager	Local padrão: <code>./install-cm</code> Local diferente do padrão: <code>./install-cm --location=/foo</code>
Correlation Engine	Local padrão: <code>./install-ce</code> Local diferente do padrão: <code>./install-cm --location=/foo</code>

7b Prossiga para a [Etapa 9](#).

- 8 (Condicional) Para realizar a instalação silenciosa, verifique se os parâmetros de instalação foram gravados em um arquivo. Para obter informações sobre a criação do arquivo de resposta, consulte “[Instalação padrão do servidor do Sentinel](#)” na página 91 ou “[Instalação personalizada do servidor do Sentinel](#)” na página 92.

Para realizar uma instalação silenciosa:

- 8a Especifique o comando apropriado, dependendo do componente que você está instalando:

Componente	Comando
Servidor do Sentinel	Local padrão: <code>./install-sentinel -u <arquivo_de_resposta></code> Local diferente do padrão: <code>./install-sentinel --location=/foo -u <arquivo_de_resposta></code>
Collector Manager	Local padrão: <code>./install-cm -u <arquivo_de_resposta></code> Local diferente do padrão: <code>./install-cm --location=/foo -u <arquivo_de_resposta></code>
Correlation Engine	Local padrão: <code>./install-ce -u <arquivo_de_resposta></code> Local diferente do padrão: <code>./install-ce --location=/foo -u <arquivo_de_resposta></code>

A instalação prossegue com os valores armazenados no arquivo de resposta.

8b Continue na [Etapa 12](#).

- 9 Especifique o número do idioma que deseja usar na instalação.

O contrato de licença de usuário final será exibido no idioma selecionado.

- 10 Leia a licença do usuário final e digite `sim` ou `s` para aceitar a licença e continuar com a instalação.

A instalação de todos os pacotes RPM será iniciada. A instalação pode levar alguns segundos para ser concluída.

- 11 Será solicitado que você especifique o modo de instalação.
- ♦ Se você escolher prosseguir com a instalação padrão, continue com [Etapa 8a](#) [Etapa 10](#) em “Instalação padrão do servidor do Sentinel” na página 91.
 - ♦ Se você escolher prosseguir com a instalação personalizada, continue com [Etapa 8a](#) [Etapa 15](#) em “Instalação personalizada do servidor do Sentinel” na página 92.
- 12 Efetue login como um usuário `root` e especifique o seguinte comando para concluir a instalação:

```
./bin/root_install_finish
```

A instalação do Sentinel é concluída e o servidor é iniciado. Poderá levar alguns minutos até que todos os serviços sejam iniciados depois da instalação, pois o sistema executa uma inicialização de uma única vez. Aguarde até que a instalação termine antes de efetuar login no servidor.

Para acessar a interface principal do Sentinel, especifique o seguinte URL em seu browser da web:

```
https://IP_AddressOrDNS_Sentinel_server:8443/sentinel/views/main.html
```

Em que *IP_AddressOrDNS_Sentinel_server* é o endereço IP ou o nome DNS do servidor do Sentinel e *8443* é a porta padrão do servidor do Sentinel.

15 Instalação da aplicação

A aplicação Sentinel é uma aplicação de software pronta para ser executada baseada no Micro Focus Common Appliance Framework. A aplicação combina um sistema operacional SLES 12 SP3 robusto com o serviço de atualização integrado do software Sentinel para fornecer uma experiência de usuário fácil e eficiente que permite que você aproveite investimentos existentes. A aplicação Sentinel fornece uma interface do usuário com base na Web para configurar e monitorar a aplicação.

A imagem da aplicação Sentinel é empacotada nos formatos ISO e OVF, que podem ser implantados em ambientes virtuais. Para obter informações sobre as plataformas de virtualização suportadas, consulte o [Website de informações técnicas do Sentinel](#).

- ♦ “Pré-requisitos” na página 101
- ♦ “Instalando a aplicação Sentinel ISO” na página 101
- ♦ “Instalando a aplicação Sentinel OVF” na página 104
- ♦ “Configuração pós-instalação para a aplicação” na página 106

Pré-requisitos

Verifique se o ambiente em que você vai instalar o Sentinel como aplicação ISO atende aos seguintes pré-requisitos:

- ♦ Antes de instalar a aplicação Sentinel, analise as novas funcionalidades e os problemas conhecidos nos [Detalhes da versão](#) certificadas do SLES.
- ♦ (Condicional) Se você estiver instalando a aplicação Sentinel ISO em um hardware completamente vazio, faça download da imagem em disco da aplicação ISO no site de suporte e crie um DVD.
- ♦ Garanta que o espaço mínimo em disco rígido seja de 50 GB para o instalador realizar a proposta de partição automática.
- ♦ Verifique se o seu sistema tem uma memória de pelo menos 4 GB para concluir a instalação. Se a memória for menor que 4 GB, a instalação não será concluída. Se a memória for maior que 4 GB, mas menor que o tamanho recomendado de 24 GB, a instalação exibirá uma mensagem informando que você tem menos memória do que o recomendado.

Instalando a aplicação Sentinel ISO

Esta seção oferece informações sobre a instalação do Sentinel, das instâncias do Collector Manager e do Correlation Engine usando a imagem da aplicação ISO. Esse formato permite gerar um formato da imagem completa em disco, que pode ser implantado diretamente no hardware, seja ele físico (completamente vazio) ou virtual (máquina virtual não instalada em um hipervisor), usando uma imagem ISO em um DVD inicializável.

- ♦ “Instalando o Sentinel” na página 102
- ♦ “Instalando instâncias do Collector Manager e do Correlation Engine” na página 103

Instalando o Sentinel

Para instalar a aplicação Sentinel ISO:

- 1 Faça download da imagem da aplicação virtual ISO no [Website de download da](#) .
- 2 (Condicional) Se você estiver usando um hipervisor:
Configure a máquina virtual usando a imagem da aplicação virtual ISO e ligue-a.
ou
Copie a imagem ISO em um DVD, use-o para configurar a máquina virtual e ligue-a.
- 3 (Condicional) Se você estiver instalando a ferramenta Sentinel em um hardware completamente vazio:
 - 3a Inicialize a máquina física a partir da unidade de DVD contendo o disco.
 - 3b Siga as instruções na tela do assistente de instalação.
 - 3c Selecione **Instalar servidor Sentinel <versão>**.
- 4 Selecione o idioma de sua escolha.
- 5 Selecione o layout do teclado.
- 6 Clique em **Avançar**.
- 7 Leia e aceite o Contrato de Licença do Software SUSE Enterprise Server. Clique em **Avançar**
- 8 Leia e aceite o contrato de licença da aplicação do servidor do Sentinel. Clique em **Avançar**
- 9 Defina as senhas, a configuração NTP e o fuso horário da aplicação Sentinel.
Defina as credenciais do usuário `vaadmin` para efetuar o logon no Sentinel Appliance Management Console.

Observação: Após a instalação, você poderá mudar a configuração NTP e o fuso horário das seguintes formas:

- ♦ Acesse o prompt de comando e digite `yast->Network Services->NTP Configuration`.
- ♦ Acesse o Sentinel Appliance Management Console e clique em **Hora**.

Se o horário estiver fora de sincronia imediatamente após a instalação, execute o seguinte comando para reiniciar o NTP:

```
rcntp restart
```

-
- 10 Na página Configurações de Rede da Aplicação do Servidor do Sentinel, especifique o nome do host e o nome do domínio. Selecione **Endereço IP Estático** ou **Endereço IP DHCP**.
 - 11 Clique em **Avançar**.
 - 12 (Condicional) Se você selecionou **Endereço IP Estático** na Etapa 10, especifique as configurações de conexão de rede.
 - 13 Clique em **Avançar**.
 - 14 Defina a senha para o usuário do Sentinel `admin`, depois clique em **Próximo**.
A aplicação está instalada.
 - 15 Anote o endereço IP da aplicação, exibido no console.
 - 16 Efetue login como usuário `root` no console para efetuar login na aplicação.
Digite o nome de usuário como `raiz` e digite a senha que você definiu em [Etapa 9](#).
 - 17 Avance para a [“Configuração pós-instalação para a aplicação”](#) na página 106.

Instalando instâncias do Collector Manager e do Correlation Engine

O procedimento para instalar um Collector Manager ou um Correlation Engine é semelhante ao procedimento para instalar o Sentinel, exceto que você precisa fazer download do arquivo da aplicação ISO apropriado no [Website de download](#).

- 1 Siga as Etapas 1 a 13 na [“Instalando o Sentinel” na página 102](#).

A instalação verifica a memória e o espaço em disco disponíveis. Se a memória disponível for menor do que 1 GB, a instalação não permitirá que você prossiga e o botão **Avançar** estará em cinza.

- 2 Especifique a configuração a seguir para instalar o Collector Manager ou o Correlation Engine:

- ♦ **Nome de host ou endereço IP do servidor do Sentinel:** Especifique o nome de host ou o endereço IP do servidor do Sentinel ao qual o Collector Manager ou o Correlation Engine deverá se conectar.
- ♦ **Porta de Canal de Comunicação do Sentinel:** Especifique o número da porta do canal de comunicação do servidor do Sentinel. O número da porta padrão é 61616.
- ♦ **Porta do Servidor Web do Sentinel:** Especifique a porta do Servidor Web do Sentinel. A porta padrão é 8443.
- ♦ **Nome de usuário com função de administrador:** Especifique o nome de usuário de qualquer usuário na função de Administrador.
- ♦ **Senha para usuário com função de administrador:** Especifique a senha para o nome de usuário determinado no campo acima.

- 3 (Condicional) Se seu ambiente usa autenticação forte ou multifator, você deve fornecer o ID do cliente do Sentinel e o segredo do cliente do Sentinel. Para obter mais informações sobre métodos de autenticação, consulte [“Métodos de autenticação”](#) no *Guia do Administrador do Sentinel*.

Para recuperar o ID do cliente do Sentinel e o segredo do cliente do Sentinel, vá para o seguinte URL:

`https://Nome_de_host:porta/SentinelAuthServices/oauth/clients`

Em que:

- ♦ *Nome_de_host* é o nome de host do servidor do Sentinel.
- ♦ *Porta* é a porta que o Sentinel usa (normalmente 8443).

O URL especificado usa sua sessão atual do Sentinel para recuperar o ID do cliente do Sentinel e o segredo do cliente do Sentinel.

- 4 Clique em **Avançar**.

- 5 Quando solicitado, aceite o certificado.

- 6 Anote o endereço IP da aplicação, exibido no console.

O console exibe uma mensagem indicando que essa aplicação é o Collector Manager do Sentinel ou o Correlation Engine do Sentinel, dependendo do que você escolheu instalar, junto com o endereço IP. O console também exibe o endereço IP da interface do usuário do servidor do Sentinel.

- 7 Conclua [Etapa 16](#) a [Etapa 17](#) em [“Instalando o Sentinel” na página 102](#).

Instalando a aplicação Sentinel OVF

Esta seção fornece informações sobre como instalar o Sentinel, o Collector Manager e o Correlation Engine como uma imagem da aplicação OVF.

O formato OVF é um formato de máquina virtual padrão compatível com a maioria dos hipervisores, seja diretamente ou por meio de uma conversão simples. O Sentinel é compatível com a aplicação OVF com dois hipervisores certificados, mas também é possível usá-lo com outros hipervisores.

- ♦ “[Instalando o Sentinel](#)” na página 104
- ♦ “[Instalando instâncias do Collector Manager e do Correlation Engine](#)” na página 105

Instalando o Sentinel

Para instalar a aplicação Sentinel OVF:

- 1 Faça download da imagem da aplicação virtual ISO no [Website de download da](#) .
- 2 No console de gerenciamento do seu hipervisor, importe o arquivo da imagem OFV como uma nova máquina virtual. Se for solicitado, permita que o hipervisor converta a imagem OVF para o formato nativo.
- 3 Revise os recursos do hardware virtual alocados à sua nova máquina virtual para assegurar que eles atendem aos requisitos do Sentinel.
- 4 Ligue a máquina virtual.
- 5 Selecione o idioma de sua escolha.
- 6 Selecione o layout do teclado.
- 7 Clique em **Avançar**.
- 8 Leia e aceite o Contrato de Licença do Software SUSE Enterprise Server. Clique em **Avançar**.
- 9 Leia e aceite o contrato de licença da aplicação do servidor do Sentinel. Clique em **Avançar**.
- 10 Defina as senhas, a configuração NTP e o fuso horário da aplicação Sentinel.

Defina as credenciais do usuário `vaadmin` para efetuar o logon no Sentinel Appliance Management Console.

Observação: Após a instalação, você poderá mudar a configuração NTP e o fuso horário das seguintes formas:

- ♦ Acesse o prompt de comando e digite `yast->Network Services->NTP Configuration`.
- ♦ Acesse o Sentinel Appliance Management Console e clique em **Hora**.

Se o horário estiver fora de sincronia imediatamente após a instalação, execute o seguinte comando para reiniciar o NTP:

```
rcntp restart
```

-
- 11 Na página Configurações de Rede da Aplicação do Servidor do Sentinel, especifique o nome do host e o nome do domínio. Selecione **Endereço IP Estático** ou **Endereço IP DHCP**.
 - 12 Clique em **Avançar**.
 - 13 (Condicional), Se você selecionou **Endereço IP Estático** na Etapa 11, especifique as configurações de conexão de rede.
 - 14 Clique em **Avançar**.
 - 15 Configure a senha do administrador do Sentinel e, em seguida, clique em **Avançar**.

Poderá levar alguns minutos até que todos os serviços sejam iniciados depois da instalação, pois o sistema executa uma inicialização por vez. Aguarde até que a instalação termine antes de efetuar login no servidor.

- 16 Anote o endereço IP da aplicação, exibido no console. Use o mesmo endereço IP para acessar a interface principal do Sentinel.

Instalando instâncias do Collector Manager e do Correlation Engine

Para instalar um Collector Manager ou um Correlation Engine em um servidor VMware ESX como uma imagem da aplicação OVF:

- 1 Siga as Etapas 1 a 14 na [“Instalando o Sentinel” na página 104](#).

A instalação verifica a memória e o espaço em disco disponíveis. Se a memória disponível for menor do que 1 GB, a instalação não permitirá que você prossiga e o botão **Avançar** estará em cinza.

- 2 Especifique o nome de host/endereço IP do servidor do Sentinel ao qual o Collector Manager deverá se conectar.
- 3 Especifique o número da porta do Servidor de Comunicação. A porta padrão é 61616.
- 4 Especifique as credenciais de qualquer usuário na função de administrador. Digite o nome de usuário e a senha.
- 5 (Condicional) Se seu ambiente usa autenticação forte ou multifator, você deve fornecer o ID do cliente do Sentinel e o segredo do cliente do Sentinel. Para obter mais informações sobre métodos de autenticação, consulte [“Métodos de autenticação”](#) no *Guia do Administrador do Sentinel*.

Para recuperar o ID do cliente do Sentinel e o segredo do cliente do Sentinel, vá para o seguinte URL:

`https://Nome_de_host:porta/SentinelAuthServices/oauth/clients`

Em que:

- ♦ *Nome_de_host* é o nome de host do servidor do Sentinel.
- ♦ *Porta* é a porta que o Sentinel usa (normalmente 8443).

O URL especificado usa sua sessão atual do Sentinel para recuperar o ID do cliente do Sentinel e o segredo do cliente do Sentinel.

- 6 Clique em **Avançar**.
- 7 Aceite o certificado.
- 8 Clique em **Avançar** para concluir a instalação.

Quando a instalação está concluída, o instalador exibe uma mensagem indicando que essa aplicação é o Collector Manager do Sentinel ou Correlation Engine do Sentinel dependendo do que você escolheu instalar, junto com o endereço IP. Ela também exibe o endereço IP da interface do usuário do servidor do Sentinel.

Configuração pós-instalação para a aplicação

Após instalar o Sentinel, você precisa executar a configuração adicional para que a aplicação funcione adequadamente.

- ♦ “[Registrando para receber atualizações](#)” na página 106
- ♦ “[Criando partições para armazenamento tradicional](#)” na página 107
- ♦ “[Configurando o armazenamento escalável](#)” na página 107
- ♦ “[Configurando a aplicação com SMT](#)” na página 108

Registrando para receber atualizações

Você deve registrar a aplicação Sentinel com o canal de atualização da aplicação para receber o Sentinel e as mais recentes atualizações do sistema operacional. Para registrar a aplicação, você deve obter o código de registro ou a chave de ativação da aplicação no [Centro de Atendimento ao Cliente](#).

Registrar usando o Sentinel Appliance Management Console

Se você estiver usando SLES 12 SP3, poderá se registrar para receber atualizações usando o Sentinel Appliance Management Console.

- 1 Inicie a aplicação Sentinel seguindo um destes procedimentos:
 - ♦ Efetue login no Sentinel e clique em **Sentinel Principal** > **Aplicação**.
 - ♦ Especifique o URL a seguir no browser da web: `https://<endereço_IP>:9443`.
- 2 Efetue login como `vaadmin` ou usuário `root`.
- 3 Clique em **Atualização Online** > **Registrar Agora**.
- 4 No campo **E-mail**, especifique o ID do e-mail no qual deseja receber atualizações.
- 5 No campo **Chave de Ativação**, digite o código de registro.
- 6 Clique em **Registrar** para concluir o registro.

Registrar usando comandos

Se você estiver usando o SLES 11 SP4 ou o SLES 12 SP3, poderá registrar usando comandos.

Para se registrar e receber atualizações

- 1 Efetue login no Sentinel Server como usuário `root`.
- 2 Especifique os seguintes comandos:
 - ♦ Para registrar o servidor, especifique `suse_register -a regcode-sentinel=<código_de_registro> -a email=<ID_de_e-mail>`
 - ♦ Para registrar o Collector Manager, especifique: `suse_register -a regcode-sentinel-collector=<código_de_registro> -a email=<ID_de_e-mail>`
 - ♦ Para registrar o Correlation Engine, especifique: `suse_register -a regcode-sentinel-correlation=<código_de_registro> -a email=<ID_de_e-mail>`
 - ♦ Para registrar o Sentinel em alta disponibilidade, especifique: `suse_register -a regcode-sentinel-ha=<código_de_registro> -a email=<ID_de_e-mail>`

Para o parâmetro de e-mail, especifique o ID do e-mail no qual deseja receber atualizações.

Criando partições para armazenamento tradicional

As informações nesta seção serão aplicáveis apenas se você desejar usar o armazenamento tradicional como opção de armazenamento de dados.

Como melhor prática, verifique se você criou partições diferentes para armazenar os arquivos executáveis, de configuração e do sistema operacional em uma partição separada dos dados do Sentinel. Os benefícios de armazenar dados variáveis separadamente incluem mais facilidade para realizar backups de conjuntos de campos, mais simplicidade na recuperação em casos de corrupção e robustez adicional caso uma partição de disco fique cheia. Para obter informações sobre como planejar suas partições, consulte a [“Planejando o armazenamento tradicional” na página 41](#). É possível adicionar partições à aplicação e mover um diretório para a nova partição usando a ferramenta YaST.

Use o procedimento a seguir para criar uma nova partição e mover os arquivos de dados de seu diretório para a partição recém-criada:

1 Efetue login no Sentinel como `root`.

2 Execute o seguinte comando para parar o Sentinel na aplicação:

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

3 Especifique o seguinte comando para mudar para o usuário `novell`:

```
su -novell
```

4 Mova o conteúdo do diretório em `/var/opt/novell/sentinel/` para um local temporário.

5 Mude para o usuário `root`.

6 Insira o seguinte comando para acessar o YaST2 Control Center:

```
yast
```

7 Selecione **Sistema > Particionador**.

8 Leia o aviso e selecione **Sim** para adicionar a nova partição não utilizada.

Para obter informações sobre a criação de partições, consulte [Usando o particionador do YaST na documentação do SLES 11](#).

9 Monte a nova partição em `/var/opt/novell/sentinel`.

10 Especifique o seguinte comando para mudar para o usuário `novell`:

```
su -novell
```

11 Mova o conteúdo do diretório de dados do local temporário (onde foi salvo em [Etapa 4](#)) de volta para `/var/opt/novell/sentinel/` na nova partição.

12 Execute o seguinte comando para reiniciar a aplicação do Sentinel:

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

Configurando o armazenamento escalável

Para habilitar e configurar o armazenamento escalável como opção de armazenamento de dados, consulte [“Configurando o armazenamento escalável” no *Sentinel Administration Guide \(Guia de Administração do NetIQ Sentinel\)*](#).

Configurando a aplicação com SMT

Em ambientes seguros onde a aplicação deva ser executada sem acesso direto à internet, você pode configurar a aplicação com a Subscription Management Tool (SMT), que permite atualizar a aplicação para as versões mais recentes do Sentinel à medida que são lançadas. A SMT é um sistema proxy de pacote que é integrado com o Atendimento ao Cliente e fornece os principais recursos do Atendimento ao Cliente.

- ♦ [“Pré-requisitos” na página 108](#)
- ♦ [“Configurando a aplicação” na página 109](#)
- ♦ [“Atualizando a aplicação” na página 109](#)

Pré-requisitos

Antes de configurar a aplicação com o SMT, verifique se você atende aos seguintes pré-requisitos:

- ♦ Obtenha as credenciais do Atendimento do Cliente para obter atualizações do Sentinel. Para obter mais informações sobre como obter as credenciais, entre em contato com o [Suporte técnico](#).
- ♦ Verifique se o SLES 11 SP3 está instalado com os seguintes pacotes no computador no qual deseja instalar a SMT:
 - ♦ `htmlDoc`
 - ♦ `perl-DBIx-Transaction`
 - ♦ `perl-File-Basename-Object`
 - ♦ `perl-DBIx-Migration-Director`
 - ♦ `perl-MIME-Lite`
 - ♦ `perl-Text-ASCIITable`
 - ♦ `yum-metadata-parser`
 - ♦ `createrepo`
 - ♦ `perl-DBI`
 - ♦ `apache2-prefork`
 - ♦ `libapr1`
 - ♦ `perl-Data-ShowTable`
 - ♦ `perl-Net-Daemon`
 - ♦ `perl-Tie-IxHash`
 - ♦ `fltk`
 - ♦ `libapr-util1`
 - ♦ `perl-PIRPC`
 - ♦ `apache2-mod_perl`
 - ♦ `apache2-utils`
 - ♦ `apache2`
 - ♦ `perl-DBD-mysql`
- ♦ Instale a SMT e configure o servidor da SMT. Para obter mais informações, consulte as seções a seguir na [documentação do SMT](#):
 - ♦ [Instalação da SMT](#)

- ♦ Configuração do servidor da SMT
- ♦ Espelhamento de instalação e atualização de repositórios com a SMT
- ♦ Instale o utilitário `wget` no computador da aplicação.

Configurando a aplicação

Execute as etapas a seguir para configurar a aplicação com a SMT:

- 1 Habilite os repositórios da aplicação executando os seguintes comandos no servidor SMT:

```
smt-repos -e Sentinel-Server-7.0-Updates sle-11-x86_64
```

```
smt-repos -e Sentinel-Collector-Manager-7.0-Updates sle-11-x86_64
```

```
smt-repos -e Sentinel-Correlation-Engine-7.0-Updates sle-11-x86_64
```

- 2 Configure a aplicação com o SMT ao executar as etapas da seção “[Configurando clientes para usar SMT](#)” na [documentação SMT](#).

Atualizando a aplicação

Para obter informações sobre a atualização da aplicação, veja “[Fazendo upgrade do Sentinel](#)” na [página 157](#)

16 Instalando coletores e conectores adicionais

Por padrão, todos os Coletores e Conectores lançados são instalados quando você instala o Sentinel. Se desejar instalar um novo Coletor ou Conector liberado após a versão do Sentinel, use as informações nas seções a seguir.

- ♦ “[Instalando um Coletor](#)” na página 111
- ♦ “[Instalando um Conector](#)” na página 111

Instalando um Coletor

Siga as etapas abaixo para instalar um Coletor:

- 1 Faça download do Coletor desejado no [site de Plug-ins do Sentinel](#).
- 2 Em **Principal do Sentinel**, clique no menu suspenso **admin** e, em seguida, em **Aplicativos**.
- 3 Clique em **Iniciar o Control Center** para iniciar o Sentinel Control Center.
- 4 Na barra de ferramentas, clique em **Gerenciamento de Fonte de Eventos > Tela Ativa** e, a seguir, clique em **Ferramentas > Importar plugin**.
- 5 Procure e selecione o arquivo do Coletor cujo download foi feito em [Etapa 1](#) e, em seguida, clique em **Avançar**.
- 6 Siga as instruções remanescentes e, em seguida, clique em **Concluir**.

Para configurar o Coletor, consulte a documentação do Coletor específico no [site de Plug-ins do Sentinel](#).

Instalando um Conector

Use as etapas abaixo para instalar um Conector:

- 1 Faça download do Conector desejado no [site de Plug-ins do Sentinel](#).
- 2 Em **Principal do Sentinel**, clique no menu suspenso **admin** e, em seguida, em **Aplicativos**.
- 3 Clique em **Iniciar o Control Center** para iniciar o Sentinel Control Center.
- 4 Na barra de ferramentas, selecione **Gerenciamento de Fonte de Eventos > Tela Ativa** e, em seguida, clique em **Ferramentas > Importar plugin**.
- 5 Procure e selecione o arquivo do Conector cujo download foi feito em [Etapa 1](#) e, em seguida, clique em **Avançar**.
- 6 Siga as instruções remanescentes e, em seguida, clique em **Concluir**.

Para configurar o Conector, consulte a documentação do Conector específico no [site de Plug-ins do Sentinel](#).

17 Verificando a instalação

É possível determinar se a instalação será bem-sucedida executando um dos seguintes procedimentos:

- ♦ Verifique a versão do Sentinel:

```
/etc/init.d/sentinel version
```

- ♦ Verifique se os serviços do Sentinel estão ativos e em execução e funcionando no modo FIPS e não FIPS:

```
/etc/init.d/sentinel status
```

- ♦ Verifique se os serviços web estão ativos e em execução:

```
netstat -an |grep 'LISTEN' |grep <HTTPS_port_number>
```

O número de porta padrão é 8443.

- ♦ Inicie o Sentinel:

1. Inicie um browser da Web compatível.
2. Especifique o URL do Sentinel:

```
https://IP_AddressOrDNS_Sentinel_server:8443
```

Em que *IP_AddressOrDNS_Sentinel_server* é o endereço IP ou o nome DNS do servidor do Sentinel e *8443* é a porta padrão do servidor do Sentinel.

3. Efetue login com o nome do administrador e senha especificados durante a instalação. O nome de usuário padrão é admin.

IV Configurando o Sentinel

Esta seção fornece informações sobre como configurar o Sentinel e os plug-ins prontos para o uso.

- ♦ [Capítulo 18, “Configurando o horário” na página 117](#)
- ♦ [Capítulo 19, “Protegendo dados no Elasticsearch” na página 121](#)
- ♦ [Capítulo 20, “Habilitando a visualização de eventos” na página 123](#)
- ♦ [Capítulo 21, “Modificando a configuração depois da instalação” na página 125](#)
- ♦ [Capítulo 22, “Configurando plug-ins prontos para o uso” na página 127](#)
- ♦ [Capítulo 23, “Ativando o modo FIPS 140-2 em uma instalação existente do Sentinel” na página 129](#)
- ♦ [Capítulo 24, “Operando o Sentinel no modo FIPS 140-2” na página 131](#)
- ♦ [Capítulo 25, “Adicionando um banner de consentimento” na página 143](#)

18 Configurando o horário

O horário de um evento é vital para seu processamento no Sentinel. É importante para fins de auditoria e geração de relatórios, bem como para o processamento em tempo real. Esta seção fornece informações sobre como compreender o tempo no Sentinel, como configurar o horário e como manipular os fusos horários.

- ♦ [“Entendendo o horário no Sentinel” na página 117](#)
- ♦ [“Configurando o horário no Sentinel” na página 119](#)
- ♦ [“Configurando o limite de tempo de atraso para eventos” na página 119](#)
- ♦ [“Tratando fusos horários” na página 119](#)

Entendendo o horário no Sentinel

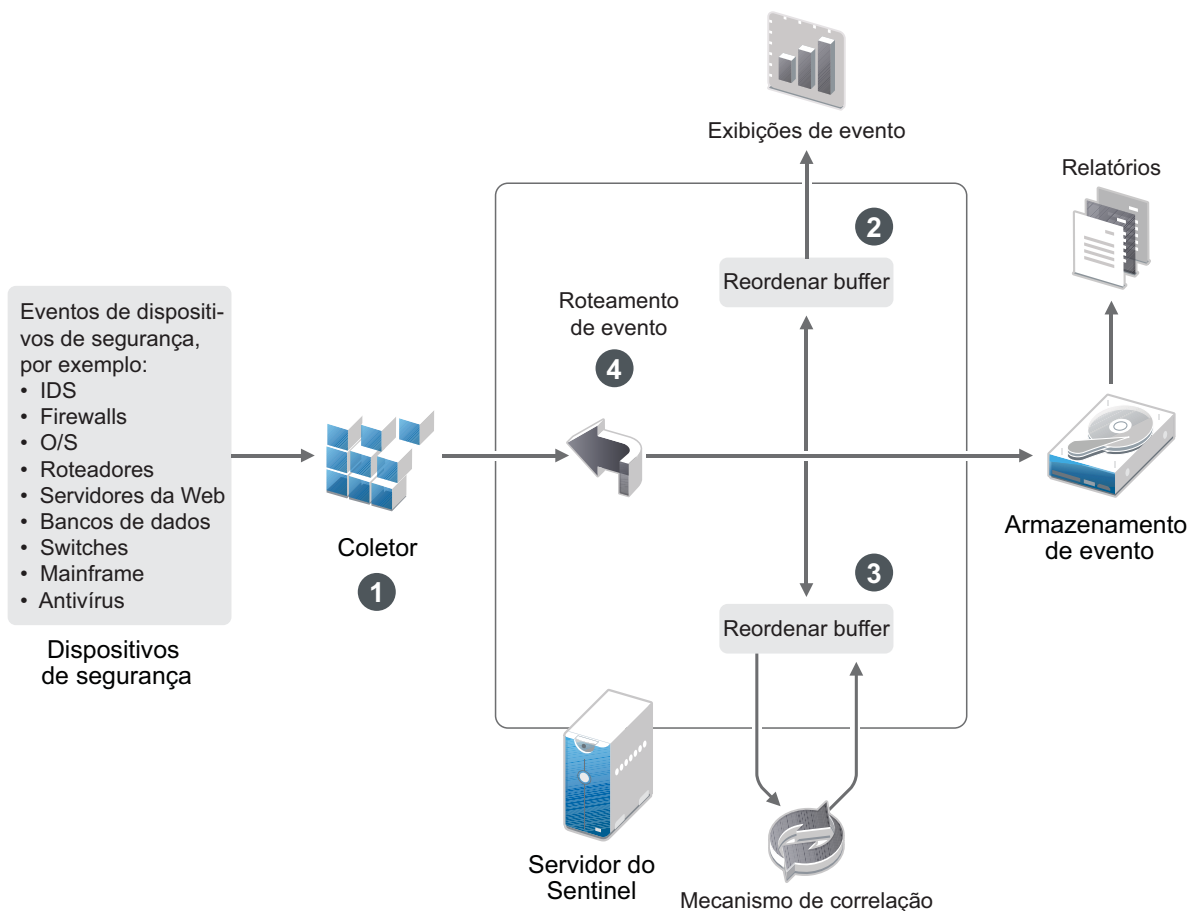
O Sentinel é um sistema distribuído, composto por vários processos distribuídos por toda a sua rede. Além disso, podem ocorrer certos atrasos introduzidos pela fonte de eventos. Para lidar com essa situação, os processos do Sentinel reordenam os eventos em um fluxo ordenado por horários antes de realizar o processamento.

Todo evento tem três campos de horário:

- ♦ **Horário do evento:** o horário de evento usado por todos os mecanismo de análise, pesquisa, relatórios, etc.
- ♦ **Horário de processamento do Sentinel:** o horário em que o Sentinel coleta os dados do dispositivo, obtido a partir do horário de sistema do Collector Manager.
- ♦ **Horário do evento do observador:** a marcação de horário que o dispositivo coloca nos dados. O dados nem sempre podem conter uma marcação de horário confiável e podem ser bem diferentes do Horário de processamento do Sentinel. Por exemplo, quando o dispositivo entrega dados em lotes.

A ilustração seguinte explica como o Sentinel faz isso em uma configuração de armazenamento tradicional:

Figura 18-1 Horário do Sentinel



1. Por padrão, o Horário do evento é definido para o Horário de processamento do Sentinel. O ideal, no entanto, é que o Horário do evento corresponda ao Horário do evento do observador, caso esse esteja disponível e seja confiável. É melhor configurar a coleta de dados para **Horário da fonte de eventos confiável** caso o horário do dispositivo estiver disponível, for preciso e devidamente analisado pelo Coletor. O Coletor ajusta o Horário do evento para corresponder ao Horário do evento do observador.
2. Os eventos que possuem Horários de evento com variações de até 5 minutos em relação ao horário do servidor (para passado ou futuro) são processados normalmente pelas Visualizações de Eventos. Os eventos que possuem Horários de evento com mais de 5 minutos no futuro não são exibidos nas Visualizações de Eventos, mas são inseridos no armazenamento de eventos. Eventos com Horários de evento mais de 5 minutos no futuro e menos de 24 horas no passado ainda são exibidos nos gráficos, mas não são exibidos nos dados de evento para o gráfico em questão. Uma operação de detalhamento é necessária para recuperar esses eventos do armazenamento de eventos.
3. Os eventos são organizados em intervalos de 30 segundos de modo que o Correlation Engine possa processá-los em ordem cronológica. Se o Horário do evento for mais de 30 segundos mais antigo do que o horário do servidor, o Correlation Engine não processará os eventos.
4. Se o Horário do evento estiver mais de 5 minutos atrás em relação ao horário do sistema do Gerenciador de Coletor, o Sentinel fará roteamento direto dos eventos para o armazenamento de eventos, ignorando sistemas em tempo real, como o Correlation Engine e a Inteligência de Segurança.

Configurando o horário no Sentinel

O Correlation Engine processa fluxos de eventos ordenados por horário e detecta padrões nos eventos, bem como padrões temporais no fluxo. No entanto, às vezes o dispositivo que gera o evento poderá não incluir o horário em suas mensagens do registro.

Para configurar o horário para que funcione corretamente com o Sentinel, há duas opções:

- Configure o NTP no Collector Manager e desmarque **Horário da Fonte de Eventos Confiável** na fonte de eventos, no Gerenciador de Fonte de Eventos. O Sentinel usa o Collector Manager como a origem de horário para os eventos.
- Selecione **Horário da Fonte de Eventos Confiável** na fonte de eventos no Gerenciador de Fonte de Eventos. O Sentinel usa o horário da mensagem do registro como o horário correto.

Para alterar essa configuração na fonte de eventos:

- 1 Efetue login no Gerenciamento de Fonte de Eventos.
Para obter mais informações, consulte [“Acessando o gerenciamento de fonte de eventos”](#) no [Guia de administração do Sentinel](#).
- 2 Clique com o botão direito do mouse na fonte de eventos para a qual alterar a configuração de horário e, em seguida, selecione **Editar**.
- 3 Marque ou desmarque a opção **Confiar na Fonte de Eventos** na parte inferior da guia **Geral**.
- 4 Clique em **OK** para gravar a mudança.

Configurando o limite de tempo de atraso para eventos

Quando o Sentinel recebe eventos de fontes de eventos, pode haver um atraso entre o horário que o evento foi gerado e o horário que o Sentinel processa o evento. O Sentinel armazena os eventos com atrasos grandes em partições separadas. A ocorrência de muitos eventos atrasados durante um longo período de tempo pode ser um indicador de uma fonte de eventos configurada incorretamente. Isso também pode diminuir o desempenho do Sentinel à medida que ele tenta lidar com os eventos atrasados. Como os eventos atrasados podem ser resultado de uma configuração incorreta e que, portanto, não devem ser armazenados, o Sentinel permite a configuração do limite de atraso aceitável para os eventos recebidos. O roteador de evento ignorará os eventos que excederem o limite de atraso. Especifique o limite de atraso na propriedade a seguir no arquivo `configuration.properties`:

```
esecurity.router.event.delayacceptthreshold = <time in milliseconds>
```

Você também pode registrar as fontes de eventos que enviaram eventos com atrasos superiores a um limite especificado no arquivo de registro do servidor do Sentinel. Para registrar essas informações, especifique o limite na propriedade a seguir no arquivo `configuration.properties`:

```
sentinel.indexedlog.eventdelay.reportthreshold= <time in milliseconds>
```

Tratando fusos horários

Tratar fusos horários pode se tornar muito complexo em um ambiente distribuído. Por exemplo, você pode ter uma fonte de eventos em um fuso horário, o Collector Manager em outro, o servidor backend do Sentinel em outro e o cliente que visualiza os dados em outro. Ao adicionar preocupações como horário de verão e as várias fontes de evento que não relatam para que fuso horário estão

configuradas (como todas as fontes de syslog), há muitos problemas possíveis que precisam ser tratados. O Sentinel é flexível, de forma que você possa representar adequadamente o horário quando os eventos ocorrem de fato, e comparar esses eventos a outros eventos de outras fontes em fusos horários iguais ou diferentes.

Em geral, há três diferentes cenários para como as fontes de evento relatam marcações de horário:

- ♦ A fonte de eventos informa o horário em UTC. Por exemplo, todos os eventos do log de eventos do Windows são sempre informados em UTC.
- ♦ A fonte de eventos informa o horário local, mas sempre inclui o fuso horário na marcação de horário. Por exemplo, qualquer fonte de eventos que siga a RFC3339 ao estruturar marcações de tempo incluem o fuso horário como deslocamento; outras fontes informam IDs longos de fuso horário, como América/Nova Iorque, ou IDs curtos de fuso horário, como EST, o que pode apresentar problemas por causa de conflitos e resoluções inadequadas.
- ♦ A fonte de eventos informa o horário local, mas não indica o fuso horário. Infelizmente, o formato do syslog, extremamente comum, segue esse modelo.

No primeiro cenário, é possível calcular o horário UTC absoluto em que um evento ocorreu (presumindo que um protocolo de sincronização de horário esteja em uso), para que você possa facilmente comparar o horário daquele evento a qualquer outra fonte de eventos no mundo. No entanto, não é possível determinar automaticamente qual era o horário local quando o evento ocorreu. Por esse motivo, o Sentinel permite que os clientes definam manualmente o fuso horário de uma fonte de evento adicionando o nó Fonte de Eventos no Gerenciador de Fontes de evento e especificando o fuso horário apropriado. Essa informação não afeta o cálculo de DeviceEventTime ou EventTime, mas é colocada no campo ObserverTZ e é usada para calcular os vários campos ObserverTZ, como ObserverTZHour. Esses campos são sempre expressos em horário local.

No segundo cenário, se os IDs de fuso horário em formato longo ou deslocamentos forem utilizados, será possível fazer a conversão para UTC e obter o horário canônico UTC absoluto (armazenado em DeviceEventTime), porém também é possível calcular os campos ObserverTZ de horário local. Se um ID em formato curto do fuso horário for usado, há algum potencial para conflitos.

O terceiro cenário requer que o administrador defina manualmente o fuso horário da fonte de evento para todas as fontes afetadas de modo que o Sentinel possa calcular corretamente o horário UTC. Se o fuso horário não for adequadamente especificado ao editar o nó da Fonte de Evento no Gerenciador de Fontes de Evento, então o DeviceEventTime (e provavelmente o EventTime) poderá estar incorreto; além disso, ObserverTZ e os campos associados poderão estar incorretos.

Em geral, o Coletor para um dado tipo de fonte de evento (como o Microsoft Windows) sabe como uma fonte de evento apresenta marcações de hora e faz os ajustes necessários. É sempre uma boa política definir manualmente o fuso horário para todos os nós de Fonte de Evento no Gerenciador de Fontes de Evento, a não ser que você saiba que a fonte de evento informa o horário local e sempre inclui o fuso horário na marcação de hora.

Processar a apresentação da marcação de horário da fonte de evento ocorre no Coletor e no Collector Manager. DeviceEventTime e EventTime são armazenados como UTC e os campos ObserverTZ são armazenados como strings definidos para o horário local da fonte de evento. Essas informações são enviadas do Collector Manager para o servidor Sentinel e ficam armazenadas no armazenamento de eventos. O fuso horário em que o Collector Manager e o servidor do Sentinel estão não deverá afetar esse processo ou os dados armazenados. No entanto, quando um cliente visualiza o evento em um browser da web, o Horário do evento em UTC é convertido para o horário local de acordo com o browser da web, portanto todos os eventos são apresentados aos clientes no fuso horário local. Se os usuários quiserem ver o horário local da fonte, poderão examinar os campos ObserverTZ para obter detalhes.

19 Protegendo dados no Elasticsearch

O Sentinel utiliza o Kibana, um painel de controle de análise e pesquisa baseado em browser, que ajuda você a visualizar eventos e alertas em painéis de controle. O Sentinel armazena e indexa alertas no Elasticsearch. É possível configurar o Sentinel para armazenar e indexar eventos no Elasticsearch para aproveitar os recursos de visualização de eventos. Os painéis de controle do Sentinel acessam dados do Elasticsearch para apresentar eventos e alertas em painéis de controle. Para verificar se os painéis de controle exibem somente os dados que a função de um usuário está autorizada a visualizar e impedir o acesso não autorizado a dados no Elasticsearch, instale o plug-in de segurança do Elasticsearch. Para obter mais informações, consulte [“Protegendo dados no Elasticsearch” na página 79](#).

20 Habilitando a visualização de eventos

Em uma configuração de armazenamento escalável, as visualizações de eventos estão disponíveis por padrão. Em uma configuração de armazenamento tradicional, as visualizações de eventos estarão disponíveis somente se você habilitar o armazenamento de dados de visualização (Elasticsearch) para armazenar e indexar dados.

- ♦ “Pré-requisitos” na página 123
- ♦ “Habilitando a visualização de eventos” na página 123

Pré-requisitos

Para indexação escalável e distribuída de eventos em ambientes de produção, você deve configurar nós adicionais do Elasticsearch em um modo de cluster. Para instalar e configurar o Elasticsearch em um modo de cluster, consulte [“Instalando e configurando o Elasticsearch” na página 77](#).

Habilitando a visualização de eventos

Para habilitar a visualização de eventos:

- 1 Efetue login no servidor do Sentinel como usuário Novell.
- 2 Abra o arquivo `/etc/opt/novell/sentinel/config/configuration.properties`.
- 3 Defina `eventvisualization.traditionalstorage.enabled` como `true`.
- 4 Atualize a interface do usuário após alguns minutos para ver as visualizações de eventos.
Agora você deve ver todos os painéis de controle habilitados na interface do usuário **Meu Sentinel**. Inicie qualquer painel de controle, o painel de controle de Busca por Ameaças, por exemplo, e clique em **Pesquisar**. O painel de controle exibe todos os eventos gerados na última hora.
- 5 (Opcional) Os painéis de controle visualização de eventos exibem apenas os eventos processados depois que você habilitou a visualização de eventos. Para ver os eventos existentes no armazenamento com base no arquivo, migre os dados do armazenamento com base no arquivo para o Elasticsearch. Para obter mais informações, consulte [Capítulo 33, “Migrando dados para o Elasticsearch” na página 181](#).

Observação: Habilitar ou desabilitar a visualização de eventos gera uma exceção, pois reinicia os serviços de indexação do Sentinel. Essa exceção é esperada e você pode ignorá-la.

21 Modificando a configuração depois da instalação

Depois de instalar o Sentinel, se você quiser inserir a chave de licença válida, alterar a senha ou modificar qualquer uma das portas atribuídas, poderá executar o script `configure.sh` para realizar essas modificações. O script está disponível na pasta `/opt/novell/sentinel/setup`.

- 1 Encerre o Sentinel usando o seguinte comando:

```
rcsentinel stop
```

- 2 Especifique o seguinte comando na linha de comando para executar o script `configure.sh`:

```
./configure.sh
```

- 3 Especifique 1 para realizar uma configuração padrão ou 2 para realizar uma configuração personalizada do Sentinel.

- 4 Pressione a barra de espaço para ler o contrato de licença.

- 5 Digite `sim` ou `s` para aceitar o contrato de licença e prosseguir com a instalação.

A instalação poderá levar alguns segundos para carregar os pacotes de instalação.

- 6 Insira 1 para usar a chave de licença de avaliação padrão.

ou

Insira 2 para informar uma chave de licença adquirida do Sentinel.

- 7 Decida se deseja manter a senha existente para o usuário administrador `admin`.

- ♦ Se desejar manter a senha existente, insira 1 e, em seguida, continue com [Etapa 8](#).
- ♦ Se desejar alterar a senha existente, insira 2, especifique a nova senha, confirme-a e, em seguida, continue com [Etapa 8](#).

O usuário `admin` é a identidade usada para realizar tarefas de administração através da interface principal do Sentinel, incluindo a criação de outras contas de usuário.

- 8 Decida se deseja manter a senha existente para o usuário do banco de dados `dbauser`.

- ♦ Se desejar manter a senha existente, insira 1 e, em seguida, continue com [Etapa 9](#).
- ♦ Se desejar alterar a senha existente, insira 2, especifique a nova senha, confirme-a e, em seguida, continue com [Etapa 9](#).

A conta `dbauser` é a identidade que o Sentinel usa para interagir com o banco de dados. A senha inserida aqui pode ser usada para realizar tarefas de manutenção de banco de dados, incluindo a redefinição da senha do administrador, caso ela seja esquecida ou perdida.

- 9 Decida se deseja manter a senha existente para o usuário do aplicativo `appuser`.

- ♦ Se desejar manter a senha existente, insira 1 e, em seguida, continue com [Etapa 10](#).
- ♦ Se desejar alterar a senha existente, insira 2, especifique a nova senha, confirme-a e, em seguida, continue com [Etapa 10](#).

A conta `appuser` é uma identidade interna que o processo java do Sentinel usa para estabelecer conexão e interagir com o banco de dados. A senha inserida aqui é usada para realizar tarefas do banco de dados.

- 10 Altere as atribuições de porta para os serviços do Sentinel inserindo o número desejado e, em seguida, especificando o novo número da porta.

11 Depois de alterar as portas, especifique 7 para concluir.

12 Insira 1 para autenticar os usuários usando somente o banco de dados interno.

ou

Se você configurou um diretório LDAP em seu domínio, insira 2 para autenticar os usuários usando a autenticação do diretório LDAP.

O valor padrão é 1.

22 Configurando plug-ins prontos para o uso

O Sentinel é pré-instalado com os plug-ins padrão do Sentinel disponíveis no momento do lançamento do Sentinel.

Este capítulo fornece informações sobre como configurar os plug-ins prontos para o uso.

- ♦ “Visualizando os plug-ins pré-instalados” na página 127
- ♦ “Configurando a coleta de dados” na página 127
- ♦ “Configurando pacotes de soluções” na página 127
- ♦ “Configurando ações e integradores” na página 128

Visualizando os plug-ins pré-instalados

Veja a lista de plug-ins pré-instalados no Sentinel. Você também pode ver as versões dos plug-ins e outros metadados, o que ajuda a determinar se você tem a versão mais recente de um plug-in.

Para ver os plug-ins instalados no servidor do Sentinel:

- 1 Efetue login como administrador na interface principal do Sentinel em `https://<Endereço IP>:8443`, em que 8443 é a porta padrão do servidor do Sentinel.
- 2 Clique em **Plug-ins** > **Catálogo**.

Configurando a coleta de dados

Para obter informações sobre como configurar o Sentinel para coleta de dados, consulte “Coleta e roteamento de dados de evento” no *Guia de administração do Sentinel*.

Configurando pacotes de soluções

O Sentinel acompanha uma ampla variedade de conteúdos úteis prontos para instalar que você pode usar imediatamente para atender suas necessidades de análise. Muito desse conteúdo vem do Sentinel Core Solution Pack e do Solution Pack for ISO 27000 Series pré-instalados. Para obter mais informações, consulte “Usando pacotes de solução” no *Guia de administração do Sentinel*.

Os Solution Packs permitem realizar a categorização e o agrupamento de conteúdos em controles ou conjuntos de políticas tratados como uma unidade. Os controles presentes nos Solution Packs são pré-instalados para fornecer conteúdo out-of-the-box, mas você deve formalmente implementar ou testar esses controles usando a interface principal do Sentinel.

Se for necessário mostrar que a implementação do Sentinel está funcionando como desejado, use o processo de atestação formal incorporado aos Solution Packs. Esse processo de atestado implementa e testa os controles do Solution Pack da mesma forma que você faria com qualquer outro Solution Pack. Como parte desse processo, o implementador e testador atestarão que eles

concluíram o trabalho; em seguida, essas atestações farão parte de uma trilha de auditoria que poderá ser examinada para demonstrar que qualquer controle específico foi corretamente implantado.

Você pode executar o processo de atestação usando o Solution Manager. Para obter mais informações sobre como implementar e testar os controles, consulte “[Instalando e gerenciando pacotes de solução](#)” no *Guia de administração do Sentinel*.

Configurando ações e integradores

Para obter informações sobre como configurar os plug-ins prontos para o uso, consulte a documentação específica de plug-in disponível no [site de Plug-ins do Sentinel](#).

23 Ativando o modo FIPS 140-2 em uma instalação existente do Sentinel

Este capítulo fornece informações sobre como ativar o modo do FIPS 140-2 em uma instalação existente do Sentinel.

Observação: Estas instruções presumem que o Sentinel está instalado no diretório `/opt/novell/sentinel`. Os comandos devem ser executados como o usuário `novell`.

- ♦ [“Ativando o servidor do Sentinel para executar no Modo FIPS 140-2” na página 129](#)
- ♦ [“Ativando o modo FIPS 140-2 nas instâncias remotas do Collector Manager e do Correlation Engine” na página 130](#)

Ativando o servidor do Sentinel para executar no Modo FIPS 140-2

Para ativar o servidor do Sentinel para execução em modo FIPS 140-2:

- 1 Efetue login no servidor do Sentinel.
- 2 Alterne para o usuário `novell` (`su novell`).
- 3 Navegue para o diretório `bin` do Sentinel.
- 4 Execute o script `convert_to_fips.sh` e siga as instruções na tela.
- 5 (Condicional) Se o ambiente usar autenticação multifator ou forte, você deverá executar o script `create_mfa_fips_keys.sh` e seguir as instruções na tela.

Observação: Enquanto o script está sendo executado, ele requer a senha do banco de dados `nss`.

- 6 (Condicional) Se seu ambiente usa autenticação forte ou multifator, você deve fornecer o ID do cliente do Sentinel e o segredo do cliente do Sentinel. Para obter mais informações sobre métodos de autenticação, consulte [“Métodos de autenticação”](#) no *Guia do Administrador do Sentinel*.

Para recuperar o ID do cliente do Sentinel e o segredo do cliente do Sentinel, vá para o seguinte URL:

`https://Nome_de_host:porta/SentinelAuthServices/oauth/clients`

Em que:

- ♦ *Nome_de_host* é o nome de host do servidor do Sentinel.
- ♦ *Porta* é a porta que o Sentinel usa (normalmente 8443).

O URL especificado usa sua sessão atual do Sentinel para recuperar o ID do cliente do Sentinel e o segredo do cliente do Sentinel.

- 7 Reinicie o servidor do Sentinel.
- 8 Conclua a configuração do modo FIPS 140-2 seguindo as tarefas mencionadas no [Capítulo 24, “Operando o Sentinel no modo FIPS 140-2” na página 131](#).

Ativando o modo FIPS 140-2 nas instâncias remotas do Collector Manager e do Correlation Engine

Você deve ativar o modo FIPS 140-2 no Collector Manager e Correlation Engine remotos se desejar usar as comunicações aprovadas do FIPS com o servidor do Sentinel executando no modo FIPS 140-2.

Para ativar um Collector Manager e Correlation Engine remotos para executar no modo FIPS 140-2:

- 1 Efetue login no sistema do Collector Manager ou Correlation Engine remotos.
- 2 Alterne para o usuário `novell` (`su novell`).
- 3 Navegue para o diretório `bin`. O local padrão é `/opt/novell/sentinel/bin`.
- 4 Execute o script `convert_to_fips.sh` e siga as instruções na tela.
- 5 Reinicie o Collector Manager ou o Correlation Engine.
- 6 Conclua a configuração do modo FIPS 140-2 seguindo as tarefas mencionadas no [Capítulo 24, “Operando o Sentinel no modo FIPS 140-2”](#) na página 131.

24 Operando o Sentinel no modo FIPS 140-2

Este capítulo fornece informações sobre a configuração e operação do Sentinel no modo FIPS 140-2.

- ♦ [“Configurando o servido do Consultor em modo FIPS 140-2” na página 131](#)
- ♦ [“Configurando a pesquisa distribuída em modo FIPS 140-2” na página 131](#)
- ♦ [“Configurando a autenticação LDAP em modo FIPS 140-2” na página 133](#)
- ♦ [“Atualizando certificados do servidor nas instâncias do Collector Manager e do Correlation Engine remotos” na página 133](#)
- ♦ [“Configurando os plug-ins do Sentinel para execução em modo FIPS 140-2” na página 134](#)
- ♦ [“Importando certificados para o banco de dados de keystore do FIPS” na página 140](#)
- ♦ [“Revertendo o Sentinel para o modo não FIPS” na página 141](#)

Configurando o servido do Consultor em modo FIPS 140-2

O serviço do Advisor usa uma conexão HTTPS segura para fazer download de seu feed do servidor do Advisor. O certificado usado pelo servidor para comunicação segura precisa ser adicionado ao banco de dados de keystore do Sentinel FIPS.

Para verificar o registro bem-sucedido com o banco de dados Resource Management:

- 1 Faça download do certificado no [servidor do Advisor](#) e salve o arquivo como `advisor.cer`.
- 2 Importe o certificado do servidor do Consultor para o keystore do Sentinel FIPS.

Para obter mais informações sobre como importar o certificado, veja [“Importando certificados para o banco de dados de keystore do FIPS” na página 140](#).

Configurando a pesquisa distribuída em modo FIPS 140-2

Esta seção fornece informações sobre como configurar a pesquisa distribuída em modo FIPS 140-2.

Cenário 1: tanto o servidor de destino quando de origem do Sentinel estão em modo FIPS 140-2

Para possibilitar pesquisas distribuídas em múltiplos servidores do Sentinel executados em modo FIPS 140-2, é preciso adicionar os certificados usados para a comunicação segura com a keystore do FIPS.

- 1 Efetue login no computador de origem da pesquisa distribuída.
- 2 Navegue até o diretório de certificados:

```
cd <sentinel_install_directory>/config
```

- 3 Copie o certificado de origem (`sentinel.cer`) para um local temporário no computador de destino.
- 4 Importe o certificado de origem para o keystore FIPS do Sentinel de destino.
Para obter mais informações sobre como importar o certificado, veja [“Importando certificados para o banco de dados de keystore do FIPS” na página 140](#).
- 5 Efetue login no computador de destino da pesquisa distribuída.
- 6 Navegue até o diretório de certificados:


```
cd /etc/opt/novell/sentinel/config
```
- 7 Copie o certificado de destino (`sentinel.cer`) para um local temporário no computador de origem.
- 8 Importe o certificado de destino para o keystore FIPS do Sentinel de origem.
- 9 Reinicie os serviços do Sentinel nos computadores de origem e destino.

Cenário 2: o servidor de origem do Sentinel está em modo não FIPS e o servidor de destino do Sentinel está em modo FIPS 140-2.

É preciso converter a keystore do servidor Web no computador de origem para o formato de certificado e então exportar o certificado para o computador de destino.

- 1 Efetue login no computador de origem da pesquisa distribuída.
- 2 Crie a keystore do servidor Web em formato de certificado (`.cer`):


```
<sentinel_install_directory>/jdk/jre/bin/keytool -export -alias webserver -  
keystore <sentinel_install_directory>/config/.webserverkeystore.jks -storepass  
password -file <certificate_name.cer>
```
- 3 Copie o certificado de origem (`sentinel.cer`) da pesquisa distribuída para um local temporário no computador de destino da pesquisa distribuída.
- 4 Efetue login no computador de destino da pesquisa distribuída.
- 5 Importe o certificado de origem para o keystore FIPS do Sentinel de destino.
Para obter mais informações sobre como importar o certificado, veja [“Importando certificados para o banco de dados de keystore do FIPS” na página 140](#).
- 6 Reinicie os serviços do Sentinel no computador de destino.

Cenário 3: o servidor de origem do Sentinel está em modo FIPS e o servidor de destino do Sentinel está em modo não FIPS.

- 1 Efetue login no computador de destino da pesquisa distribuída.
- 2 Crie a keystore do servidor Web em formato de certificado (`.cer`):


```
<sentinel_install_directory>/jdk/jre/bin/keytool -export -alias webserver -  
keystore <sentinel_install_directory>/config/.webserverkeystore.jks -storepass  
password -file <certificate_name.cer>
```
- 3 Copie o certificado para um local temporário no computador de origem da pesquisa distribuída.
- 4 Importe o certificado de destino para a keystore do FIPS do Sentinel de origem.
Para obter mais informações sobre como importar o certificado, veja [“Importando certificados para o banco de dados de keystore do FIPS” na página 140](#).
- 5 Reinicie os serviços do Sentinel no computador de origem.

Configurando a autenticação LDAP em modo FIPS 140-2

Para configurar a autenticação do LDAP dos servidores do Sentinel executando no modo FIPS 140-2:

- 1 Obtenha o certificado do servidor LDAP do administrador do LDAP ou use um comando. Por exemplo,

```
openssl s_client -connect <LDAP server IP>:636
```

e copiar o texto retornado (entre, sem incluir, as linhas BEGIN e END) em um arquivo.

- 2 Importe o certificado do servidor LDAP para o keystore do Sentinel FIPS.

Para obter mais informações sobre como importar o certificado, veja [“Importando certificados para o banco de dados de keystore do FIPS” na página 140.](#)

- 3 Navegue até a interface **Principal do Sentinel** como um usuário na função de administrador e prossiga com a autenticação do LDAP.

Para obter mais informações, consulte [“Autenticação LDAP com relação a um único servidor LDAP ou domínio” no Guia de Administração do Sentinel.](#)

Observação: Também é possível configurar a autenticação do LDAP para um servidor do Sentinel executando no modo FIPS 140-2 ao executar o script `ldap_auth_config.sh` no diretório `/opt/novell/sentinel/setup`.

Atualizando certificados do servidor nas instâncias do Collector Manager e do Correlation Engine remotos

Para configurar Gerenciadores de coletor e Mecanismos de correlação remotos para se comunicar com um servidor do Sentinel executado em modo FIPS 140-2, coloque o sistema remoto no modo FIPS 140-2 ou atualize o certificado do servidor do Sentinel para o sistema remoto e deixe o Collector Manager ou Correlation Engine em modo não FIPS. As instâncias do Collector Manager remotos no modo FIPS talvez não funcionem com origens de evento que não suportam o FIPS ou que requerem um dos Conectores do Sentinel que ainda não está ativado para FIPS.

Se você não pretende habilitar o modo FIPS 140-2 no Collector Manager ou Correlation Engine remotos, você precisa copiar o último certificado do servidor do Sentinel para o sistema remoto, de modo que o Collector Manager ou Correlation Engine possa se comunicar com o servidor do Sentinel.

Para atualizar o certificado do servidor do Sentinel no Collector Manager ou Correlation Engine remoto:

- 1 Efetue login no computador do Collector Manager ou Correlation Engine remotos.
- 2 Alterne para o usuário `novell` (`su novell`).
- 3 Navegue para o diretório `bin`. O local padrão é `/opt/novell/sentinel/bin`.
- 4 Execute o script `updateServerCert.sh` e siga as instruções na tela.

Configurando os plug-ins do Sentinel para execução em modo FIPS 140-2

Esta seção fornece informações sobre a configuração de diversos plug-ins do Sentinel no modo FIPS 140-2.

Observação: Essas instruções são fornecidas presumindo que você tenha instalado o Sentinel no diretório `/opt/novell/sentinel`. Execute todos os comandos como usuário do `novell`.

- ♦ [“Conector do Gerenciador de Agente” na página 134](#)
- ♦ [“Conector de banco de dados \(JDBC\)” na página 135](#)
- ♦ [“Conector do Link do Sentinel” na página 135](#)
- ♦ [“Conector Syslog” na página 136](#)
- ♦ [“Windows Event \(WMI\) Connector” na página 137](#)
- ♦ [“Sentinel Link Integrator” na página 138](#)
- ♦ [“LDAP Integrator” na página 139](#)
- ♦ [“SMTP Integrator” na página 139](#)
- ♦ [“Integrador Syslog” na página 139](#)
- ♦ [“Usando conectores ativados não FIPS com o Sentinel no modo FIPS 140-2” na página 140](#)

Conector do Gerenciador de Agente

Siga o procedimento abaixo apenas se você tiver selecionado a opção **Criptografado (HTTPS)** ao configurar as definições de rede do servidor de origem de evento do Gerenciador de agente.

Para configurar o Conector do Gerenciador de Agente para executar no modo FIPS 140-2:

- 1 Adicione ou edite o Servidor de Origem de Evento do Gerenciador de Agente. Avance pelas telas de configuração até que a janela Segurança seja exibida. Para obter mais informações, veja o *Guia do Conector do Gerenciador de Agente*.
- 2 Selecione uma das opções no campo *Client Authentication Type* (Tipo de autenticação do cliente). O tipo de autenticação do cliente determina estritamente como o Servidor de Origem de Evento do Gerenciador de Agente SSL verifica a identidade das Fontes de Evento do Gerenciador de Agente que estão tentando enviar dados.

- ♦ **Abrir:** Permite todas as conexões SSL provenientes dos agentes do Gerenciador de Agente. Não executa nenhuma validação ou autenticação de certificado de cliente.
- ♦ **Rígida:** Valida o certificado como um certificado X.509 válido e também verifica se o certificado do cliente é de confiança para o Servidor de Origem de Evento. Novas fontes precisarão ser explicitamente adicionadas ao Sentinel (isso evita que fontes fraudulentas enviem dados não autorizados).

Para a opção **Rígida**, você deve importar o certificado de cada novo cliente do Gerenciador de Agente para o keystore do Sentinel FIPS. Quando o Sentinel está executando no modo FIPS 140-2, não é possível importar o certificado do cliente usando a interface do Gerenciamento de Fonte de Eventos (ESM).

Para obter mais informações sobre como importar o certificado, veja [“Importando certificados para o banco de dados de keystore do FIPS” na página 140](#).

Observação: No modo FIPS 140-2, o servidor da Fonte de Evento do Gerenciador de Agente usa o par de chaves do servidor do Sentinel; não é necessário importar o par de chaves do servidor.

- 3 Se a autenticação de servidor estiver ativa nos agentes, os agentes também precisam ser configurados para confiar no servidor do Sentinel ou no certificado do Collector Manager remoto dependendo do local em que o Conector é implantado.

Localização do certificado do servidor do Sentinel: `/etc/opt/novell/sentinel/config/sentinel.cer`

Localização do certificado do Collector Manager remoto: `/etc/opt/novell/sentinel/config/rcm.cer`

Observação: Ao usar certificados personalizados que estejam assinados digitalmente por uma autoridade de certificação (CA), o agente do Gerenciador de Agente deverá confiar no arquivo de certificado apropriado.

Conector de banco de dados (JDBC)

Siga o procedimento abaixo apenas se tiver selecionado a opção SSL ao configurar a conexão do banco de dados.

Para configurar o Conector do Banco de Dados para executar no modo FIPS 140-2:

- 1 Antes de configurar o Conector, faça o download do certificado do servidor de banco de dados e salve-o como o arquivo `database.cert` no diretório `/etc/opt/novell/sentinel/config` do servidor do Sentinel.

Para obter mais informações, consulte a respectiva documentação do banco de dados.

- 2 Importe o certificado para o keystore do Sentinel FIPS.

Para obter mais informações sobre como importar o certificado, veja [“Importando certificados para o banco de dados de keystore do FIPS” na página 140](#).

- 3 Prossiga com a configuração do Conector.

Conector do Link do Sentinel

Siga o procedimento abaixo apenas se tiver selecionado a opção **Encrypted (HTTPS)** (Criptografado [HTTPS]) ao configurar as definições da rede do Servidor de Origem de Evento do Sentinel Link.

Para configurar o Sentinel Link Connector para executar no modo FIPS 140-2:

- 1 Adicione ou edite o Servidor de Origem de Evento do Sentinel Link. Avance pelas telas de configuração até que a janela Segurança seja exibida. Para obter mais informações, consulte *Guia do Sentinel Link Connector*.
- 2 Selecione uma das opções no campo *Client Authentication Type* (Tipo de autenticação do cliente). O tipo de autenticação do cliente determina com que rigidez o Servidor de Origem de Evento SSL Sentinel Link verifica a identidade das Fontes de Evento do Sentinel Link (Integradores de Sentinel Link) que estão tentando enviar dados.
 - ♦ **Abrir:** Permite todas as conexões SSL provenientes dos clientes (Sentinel Link Integrators). Não executa nenhuma validação ou autenticação de certificado do Integrator.
 - ♦ **Rígida:** Valida o certificado do Integrator como um certificado X.509 válido e também verifica se o certificado do Integrator é de confiança para o Servidor de Origem de Evento. Para obter mais informações, consulte a respectiva documentação do banco de dados.

Para a opção **Strict** (Rígida):

- ♦ Se o Sentinel Link Integrator estiver no modo FIPS 140-2, você deve copiar o arquivo `/etc/opt/novell/sentinel/config/sentinel.cer` da máquina Sentinel emissora à máquina Sentinel receptora. Importe esse certificado para o keystore do Sentinel FIPS receptor.

Observação: Ao usar certificados personalizados que estejam assinados digitalmente por uma autoridade de certificação (CA), você deve importar o arquivo de certificado personalizado adequado.

- ♦ Se o Sentinel Link Integrator estiver no modo não FIPS, você deve importar o certificado personalizado do Integrator para o keystores do Sentinel FIPS receptor.

Observação: Se o emissor for o Sentinel Log Manager (no modo não FIPS) e o receptor for o Sentinel no modo FIPS 140-2, o certificado do servidor a ser importado no emissor será o arquivo `/etc/opt/novell/sentinel/config/sentinel.cer` da máquina Sentinel receptora.

Quando o Sentinel está executando no modo FIPS 140-2, não é possível importar o certificado do cliente usando a interface do Gerenciamento de Fonte de Eventos (ESM). Para obter mais informações sobre como importar o certificado, veja [“Importando certificados para o banco de dados de keystore do FIPS” na página 140](#).

Observação: No modo FIPS 140-2, o servidor da Fonte de Evento do Sentinel Link usa o par de chaves do servidor do Sentinel. Não é necessário importar o par de chaves do servidor.

Conector Syslog

Siga o procedimento abaixo apenas se tiver selecionado o protocolo **SSL** ao configurar as definições da rede do Servidor de Origem de Evento Syslog.

Para configurar o Syslog Connector para executar no modo FIPS 140-2:

- 1 Adicione ou edite o Servidor de Origem de Evento do Syslog. Avance pelas telas de configuração até que a janela Networking (Rede) seja exibida. Para obter mais informações, consulte o *Guia do Syslog Connector*.
- 2 Clique em **Configurações**.
- 3 Selecione uma das opções no campo *Client Authentication Type* (Tipo de autenticação do cliente). O tipo de autenticação do cliente determina com que rigidez o Servidor de Origem de Evento do Syslog SSL verifica a identidade das Fontes de Evento do Syslog que estão tentando enviar dados.
 - ♦ **Abrir:** Permite todas as conexões SSL provenientes dos clientes (fontes de evento). Não executa nenhuma validação ou autenticação de certificado de cliente.
 - ♦ **Rígida:** Valida o certificado como um certificado X.509 válido e também verifica se o certificado do cliente é de confiança para o Servidor de Origem de Evento. Novas fontes terão que ser explicitamente adicionadas ao Sentinel (isso previne que fontes fraudulentas enviem dados para o Sentinel).

Para a opção **Rígida**, você deve importar o certificado cliente syslog para a keystore FIPS do Sentinel.

Quando o Sentinel está executando no modo FIPS 140-2, não é possível importar o certificado do cliente usando a interface do Gerenciamento de Fonte de Eventos (ESM).

Para obter mais informações sobre como importar o certificado, veja [“Importando certificados para o banco de dados de keystore do FIPS” na página 140.](#)

Observação: No modo FIPS 140-2, o Servidor de Origem de Evento do Syslog usa o par de chaves do servidor Sentinel. Não é necessário importar o par de chaves do servidor.

- 4 Se a autenticação de servidor estiver ativa no cliente syslog, o cliente precisa confiar no certificado do servidor do Sentinel ou no certificado do Collector Manager remoto dependendo do local em que o Conector é implantado.

O arquivo do certificado do servidor do Sentinel encontra-se em `/etc/opt/novell/sentinel/config/sentinel.cer`.

O arquivo do certificado do Gerenciador de coletor remoto encontra-se em `/etc/opt/novell/sentinel/config/rcm.cer`.

Observação: Ao usar certificados personalizados que estejam assinados digitalmente por uma autoridade de certificação (CA), o cliente deverá confiar no arquivo de certificado apropriado.

Windows Event (WMI) Connector

Para configurar o Windows Event (WMI) Connector para executar no modo FIPS 140-2:

- 1 Adicione ou edite o Windows Event Connector. Avance pelas telas de configuração até que a janela Segurança seja exibida. Para obter mais informações, consulte o *Guia do Windows Event (WMI) Connector*.
- 2 Clique em **Configurações**.
- 3 Selecione uma das opções no campo *Client Authentication Type* (Tipo de autenticação do cliente). O tipo de autenticação do cliente determina com que rigidez o Windows Event Connector verifica a identidade dos serviços do Windows Event Collection (WECS) cliente que estão tentando enviar os dados.
 - ♦ **Abrir:** permite todas as conexões SSL provenientes do WECS cliente. Não executa nenhuma validação ou autenticação de certificado de cliente.
 - ♦ **Rígida:** Valida o certificado como um certificado X.509 válido e verifica também se o certificado WECS cliente está assinado por uma CA. Novas fontes precisarão ser explicitamente adicionadas (isso previne que fontes fraudulentas enviem dados para o Sentinel).

Para a opção **Strict** (Rígida), você deve importar o certificado do WECS cliente para o keystore do Sentinel FIPS. Quando o Sentinel está executando no modo FIPS 140-2, não é possível importar o certificado do cliente usando a interface do Gerenciamento de Fonte de Eventos (ESM).

Para obter mais informações sobre como importar o certificado, veja [“Importando certificados para o banco de dados de keystore do FIPS” na página 140.](#)

Observação: No modo FIPS 140-2, o Windows Event Source Server usa o par de chaves do servidor do Sentinel. Não é necessário importar o par de chaves do servidor.

- 4 Se a autenticação de servidor estiver ativa no cliente Windows, o cliente precisa confiar no certificado do servidor do Sentinel ou no certificado do Collector Manager remoto dependendo do local em que o Conector é implantado.

O arquivo do certificado do servidor do Sentinel encontra-se em `/etc/opt/novell/sentinel/config/sentinel.cer`.

O arquivo do certificado do Collector Manager remoto encontra-se em `/etc/opt/novell/sentinel/config/rcm.cer`.

Observação: Ao usar certificados personalizados que estejam assinados digitalmente por uma autoridade de certificação (CA), o cliente deverá confiar no arquivo de certificado apropriado.

- 5 Se você deseja sincronizar automaticamente as fontes de evento ou preencher a lista de fontes de evento usando uma conexão do Active Directory, deverá importar o certificado do servidor Active Directory para o keystore do Sentinel FIPS.

Para obter mais informações sobre como importar o certificado, veja [“Importando certificados para o banco de dados de keystore do FIPS” na página 140](#).

Sentinel Link Integrator

Siga o procedimento abaixo apenas se tiver selecionado a opção **Encrypted (HTTPS)** (Criptografado [HTTPS]) ao configurar as definições da rede do Sentinel Link Integrator.

Para configurar o Sentinel Link Integrator para executar no modo FIPS 140-2:

- 1 Quando o Sentinel Link Integrator está no modo FIPS 140-2, a autenticação do servidor é obrigatória. Antes de configurar a instância do Integrador, importe o certificado do servidor de Link do Sentinel para a keystore FIPS do Sentinel:

- ♦ **Se o Conector do link do Sentinel estiver em modo FIPS 140-2:**

Se o Conector estiver implantado no servidor do Sentinel, você precisa copiar o arquivo `/etc/opt/novell/sentinel/config/sentinel.cer` da máquina Sentinel receptora para a máquina Sentinel emissora.

Se o Conector estiver implantado em um Collector Manager remoto, você precisa copiar o arquivo `/etc/opt/novell/sentinel/config/rcm.cer` da máquina receptora do Collector Manager remoto para a máquina receptora do Sentinel.

Importe esse certificado para o keystore do Sentinel FIPS emissor.

Observação: Ao usar certificados personalizados que estejam assinados digitalmente por uma autoridade de certificação (CA), você deve importar o arquivo de certificado personalizado adequado.

- ♦ **Se o Conector do link do Sentinel estiver em modo não FIPS:**

Importe o certificado do servidor de Link do Sentinel para a keystore FIPS do Sentinel emissor.

Observação: Quando o Sentinel Link Integrator está no modo FIPS 140-2 e o Sentinel Link Connector está no modo não FIPS, use o par de chaves personalizado do servidor no conector. Não use o par de chaves interno do servidor.

Para obter mais informações sobre como importar o certificado, veja [“Importando certificados para o banco de dados de keystore do FIPS” na página 140](#).

- 2 Prossiga com a configuração da instância do Integrator.

Observação: No modo FIPS 140-2, o Sentinel Link Integrator usa o par de chaves do servidor do Sentinel. Importar o par de chaves do Integrador não é necessário.

LDAP Integrator

Para configurar o LDAP Integrator para executar no modo FIPS 140-2:

- 1 Antes de configurar a instância do Integrator, faça o download do certificado do servidor LDAP e salve-o como arquivo `ldap.cert` para o diretório `/etc/opt/novell/sentinel/config` do servidor do Sentinel.

Por exemplo, usar

```
openssl s_client -connect <LDAP server IP>:636
```

e copiar o texto retornado (entre, sem incluir, as linhas BEGIN e END) em um arquivo.

- 2 Importe o certificado para o keystore do Sentinel FIPS.

Para obter mais informações sobre como importar o certificado, veja [“Importando certificados para o banco de dados de keystore do FIPS” na página 140](#).

- 3 Prossiga com a configuração da instância do Integrator.

SMTP Integrator

O Integrador SMTP suporta o modo FIPS 140-2 nas versões 2011.1r2 e mais recentes. Não é necessária nenhuma mudança de configuração.

Integrador Syslog

Realize o seguinte procedimento apenas se tiver selecionado a opção Criptografado (SSL) ao definir as configurações de rede do Syslog Integrator.

Para configurar o Syslog Integrator para executar no modo FIPS 140-2:

- 1 Quando o Syslog Integrator está no modo FIPS 140-2, a autenticação do servidor é obrigatória. Antes de configurar a instância do Integrator, importe o certificado do servidor Syslog para a keystore FIPS do Sentinel:

- ♦ **Se o Syslog Connector estiver no modo FIPS 140-2:** Se o Connector estiver implantado no servidor do Sentinel, você deverá copiar o arquivo `/etc/opt/novell/sentinel/config/sentinel.cert` do servidor do Sentinel receptor para o servidor do Sentinel emissor.

Se o Connector estiver implantado em um Collector Manager remoto, você deverá copiar o arquivo `/etc/opt/novell/sentinel/config/rcm.cert` do computador receptor do Collector Manager remoto para o computador receptor do Sentinel.

Importe esse certificado para o keystore do Sentinel FIPS emissor.

Observação: Ao usar certificados personalizados que estejam assinados digitalmente por uma autoridade de certificação (CA), você deve importar o arquivo de certificado personalizado adequado.

- ♦ **Se o Syslog Connector estiver em um modo não FIPS:** Será necessário importar o certificado personalizado do Syslog Server para o keystore do Sentinel FIPS remetente.

Observação: Quando o Syslog Integrator estiver no modo FIPS 140-2 e o Syslog Connector estiver no modo não FIPS, use o par de chaves personalizado do servidor no conector. Não use o par de chaves interno do servidor.

Para importar certificados para o banco de dados de keystore do FIPS:

1. Copie o arquivo de certificado para qualquer local temporário no servidor do Sentinel ou Collector Manager remoto.
2. Vá para o diretório `/opt/novell/sentinel/bin`.
3. Execute o comando a seguir para importar o certificado para o banco de dados da keystore do FIPS e siga as instruções na tela:

```
./convert_to_fips.sh -i <certificate file path>
```

4. Digite `sim` ou `s` quando solicitado a reiniciar o servidor do Sentinel ou o Collector Manager remoto.
2. Prossegue com a configuração da instância do Integrator.

Observação: No modo FIPS 140-2, o Syslog Integrator usa o par de chaves do servidor do Sentinel. Não é necessário importar o par de chaves do Integrator.

Usando conectores ativados não FIPS com o Sentinel no modo FIPS 140-2

Esta seção fornece informações sobre como usar Conectores ativados não FIPS com um servidor do Sentinel no modo FIPS 140-2. Recomendamos essa abordagem se você tiver fontes que não suportam FIPS ou se desejar coletar eventos dos Conectores não FIPS no seu ambiente.

Para usar conectores não FIPS com o Sentinel no modo FIPS 140-2:

1. Instale um Collector Manager no modo não FIPS para conectar ao servidor do Sentinel no modo FIPS 140-2.
Para obter mais informações, consulte [Parte III, “Instalando o Sentinel” na página 71](#).
2. Implemente os Conectores não FIPS especificamente para o Collector Manager remoto não FIPS.

Observação: Há alguns problemas conhecidos quando Conectores não FIPS, como o Conector de Auditoria e o Conector de Arquivo, são implementados em um Collector Manager remoto não FIPS conectado a um servidor do Sentinel no modo FIPS 140-2. Para obter mais informações sobre esses problemas conhecidos, veja os [Detalhes da versão do Sentinel](#).

Importando certificados para o banco de dados de keystore do FIPS

Você deve inserir certificados no banco de dados de keystore do Sentinel FIPS para estabelecer comunicações (SSL) seguras dos componentes que possuem esses certificados para o Sentinel. Não é possível fazer upload de certificados usando a interface do usuário do Sentinel quando o modo FIPS 140-2 está ativado. Você deve importar manualmente os certificados para o banco de dados de keystore do FIPS.

Para fontes de evento que estão usando Conectores implementados para um Collector Manager remoto, você deve importar os certificados para o banco de dados de keystore do FIPS do Collector Manager remoto em vez de para o servidor do Sentinel central.

Para importar certificados para o banco de dados de keystore do FIPS:

- 1 Copie o arquivo de certificado para qualquer local temporário no servidor do Sentinel ou Collector Manager remoto.
- 2 Navegue para o diretório bin do Sentinel. O local padrão é `/opt/novell/sentinel/bin`.
- 3 Execute o comando a seguir para importar o certificado para o banco de dados da keystore do FIPS e siga as instruções na tela:

```
./convert_to_fips.sh -i <certificate file path>
```

- 4 Digite `sim` ou `s` quando solicitado a reiniciar o servidor do Sentinel ou o Collector Manager remoto.

Revertendo o Sentinel para o modo não FIPS

Esta seção fornece informações sobre como reverter o Sentinel e seus componentes para o modo não FIPS.

- ♦ [“Revertendo o servidor do Sentinel para o modo não FIPS” na página 141](#)
- ♦ [“Revertendo as instâncias do Collector Manager e do Correlation Engine remotos para o modo não FIPS” na página 142](#)

Revertendo o servidor do Sentinel para o modo não FIPS

Você poderá reverter um servidor do Sentinel executando no modo FIPS 140-2 para o modo não FIPS apenas se tiver feito backup do servidor do Sentinel antes de convertê-lo para executar no modo FIPS 140-2.

Observação: Ao reverter um servidor do Sentinel para o modo não FIPS, você perderá os eventos, os dados de incidente e as mudanças de configuração feitas no servidor Sentinel após a conversão para execução no modo FIPS 140-2. O sistema do Sentinel será restaurado novamente para o último ponto de restauração do modo não FIPS. Você deve fazer um backup do sistema atual antes de reverter para o modo não FIPS para uso futuro.

Para reverter o servidor do Sentinel para o modo não FIPS:

- 1 Efetue login no Sentinel Server como usuário `root`.
- 2 Mude para o usuário `novell`.
- 3 Navegue para o diretório bin do Sentinel. O local padrão é `/opt/novell/sentinel/bin`.
- 4 Execute o comando a seguir para reverter o servidor Sentinel para o modo não FIPS e siga as instruções na tela:

```
./backup_util.sh -f <backup_file_name.tar.gz> -m 'restore'
```

Por exemplo, se `non-fips2013012419111359034887.tar.gz` for o arquivo de backup, execute o seguinte comando:

```
./backup_util.sh -f non-fips2013012419111359034887.tar.gz -m 'restore'
```

- 5 Reinicie o servidor do Sentinel.

Revertendo as instâncias do Collector Manager e do Correlation Engine remotos para o modo não FIPS

É possível reverter as instâncias remotas do Collector Manager e do Correlation Engine para o modo não FIPS

Para reverter instâncias remotas de um Collector Manager ou de um Correlation Engine para o modo não FIPS:

- 1 Efetue login no sistema do Collector Manager ou Correlation Engine remotos.
- 2 Alterne para o usuário `novell` (`su novell`).
- 3 Navegue para o diretório `bin`. O local padrão é `/opt/novell/sentinel/bin`.
- 4 Execute o script `revert_to_nonfips.sh` e siga as instruções na tela.
- 5 Reinicie o Collector Manager ou o Correlation Engine remotos.

25

Adicionando um banner de consentimento

O Sentinel permite que você exiba um banner de consentimento antes do login. É possível especificar o conteúdo do banner de acordo com seus requisitos. Depois de adicionar o banner de consentimento, você deve aceitar os termos no banner sempre que efetuar login no Sentinel.

Para adicionar um banner de consentimento:

- 1 Efetue login no servidor do Sentinel como usuário `novell`.
- 2 Procure por `/<caminho_de_instalação_do_Sentinel>/var/opt/novell/sentinel/3rdparty/jetty/webapps/ROOT/siemdownloads`.
- 3 Adicione um arquivo texto com o nome `USER_AGREEMENT.txt`.
- 4 Digite o texto de acordo do usuário.
- 5 Grave o arquivo.
- 6 Inicie o Sentinel para ver o banner de consentimento.

O Sentinel agora exibe o banner de consentimento na tela de login.

Observação: Você deve fazer o backup manual do arquivo `USER_AGREEMENT.txt` antes de fazer upgrade do Sentinel.

V Fazendo upgrade do Sentinel

Esta seção fornece informações sobre a atualização do Sentinel e outros componentes.

- ♦ [Capítulo 26, “Lista de verificação da implementação” na página 147](#)
- ♦ [Capítulo 27, “Pré-requisitos” na página 149](#)
- ♦ [Capítulo 28, “Fazendo o upgrade da instalação tradicional do Sentinel” na página 151](#)
- ♦ [Capítulo 29, “Fazendo upgrade da aplicação Sentinel” na página 157](#)
- ♦ [Capítulo 30, “Configurações Pós-Upgrade” na página 163](#)
- ♦ [Capítulo 31, “Fazendo upgrade de plug-ins do Sentinel” na página 171](#)

26

Lista de verificação da implementação

Antes de fazer o upgrade do Sentinel, analise a seguinte lista de verificação para garantir um upgrade bem-sucedido:

Tabela 26-1 Lista de verificação da implementação

<input type="checkbox"/>	Tarefas	Consulte
<input type="checkbox"/>	Assegure que os computadores em que você instalará o Sentinel e seus componentes satisfaçam aos requisitos especificados.	Site de informações técnicas do Sentinel
<input type="checkbox"/>	Analise as notas de versão do sistema operacional compatível para entender os problemas conhecidos.	Notas de versão do SUSE
<input type="checkbox"/>	Leia as notas de versão do Sentinel para ver as novas funcionalidades e entender os problemas conhecidos.	Notas de versão do Sentinel
<input type="checkbox"/>	Conclua as tarefas mencionadas nos pré-requisitos.	Capítulo 27, “Pré-requisitos” na página 149

27 Pré-requisitos

- ♦ “Gravando as informações de configuração personalizada” na página 149
- ♦ “Estendendo o Período de Retenção para Dados de Associações de Eventos” na página 149
- ♦ “Configuração Pré-Upgrade para SSDM” na página 150
- ♦ “Integração do Change Guardian” na página 150

Gravando as informações de configuração personalizada

Gravando as Configurações do arquivo `server.conf`

Se você configurou qualquer valor de parâmetro de configuração personalizada no arquivo `server.conf`, grave esses valores em arquivos separados antes do upgrade.

Para gravar suas informações de configuração personalizada:

- 1 Efetue login no Sentinel Server com o usuário `novell` e vá para o diretório `/etc/opt/novell/sentinel/config/`.
- 2 Crie um arquivo de configuração denominado `server-custom.conf` e adicione os parâmetros de configuração personalizados nesse arquivo.

O Sentinel aplica a configuração personalizada gravada nesses arquivos de configuração durante o upgrade.

Gravando as Configurações do arquivo `jetty-ssl`

O Sentinel 8.1 inclui uma versão atualizada do Jetty. A versão atualizada do Jetty inclui mudanças na estrutura de arquivos.

Se você fez qualquer mudança ao arquivo `/etc/opt/novell/sentinel/3rdparty/jetty/jetty-ssl.xml` em versões anteriores do Sentinel, como excluir cifras, grave essas mudanças em um arquivo separado antes do upgrade do Sentinel.

Após concluir o upgrade do Sentinel, copie essas mudanças para o arquivo `/etc/opt/novell/sentinel/3rdparty/jetty/jetty-ssl-context.xml` e reinicie o Sentinel.

Estendendo o Período de Retenção para Dados de Associações de Eventos

A partir do Sentinel 7.4.4, o período de retenção padrão para dados de associações de eventos é de 14 dias. Se você estiver fazendo upgrade de uma versão do Sentinel anterior à 7.4.4, o período de retenção que você definiu para os dados de associações de eventos será substituído para 14 dias após o upgrade. Para evitar isso, você pode definir o período de retenção para um valor desejado

adicionando uma propriedade no arquivo `configuration.properties`. Para obter mais informações, consulte “[Configurando o Período de Retenção para os Dados de Associações de Eventos](#)” no *Guia de Administração do Sentinel*.

Configuração Pré-Upgrade para SSDM

O processo de upgrade atualizará arquivos relacionados aos aplicativos do Spark. Para usar os arquivos atualizados, você deve reiniciar a tarefa do Spark e redefinir os pontos de verificação nos tópicos do Kafka. Para evitar a perda de dados devido à redefinição do ponto de verificação do tópico do Kafka, você deve pausar o encaminhamento de dados do Collector Manager para o Kafka antes de fazer upgrade do SSDM. Enquanto o encaminhamento de dados estiver pausado, os dados serão armazenados no Collector Manager até o encaminhamento de dados ser retomado. Uma vez que o aplicativo do Spark termina de processar os dados que foram encaminhados para o Kafka antes que o encaminhamento estivesse em pausa, o ponto de verificação pode ser redefinido com segurança sem perda de dados.

Para pausar o encaminhamento de eventos do Collector Manager para o Kafka:

- 1 Em Principal do Sentinel, clique em **Armazenamento** > **Armazenamento Escalável** > **Configurações Avançadas** > **Kafka**.
- 2 Adicione a propriedade a seguir e defina-a como verdadeira:
`pause.events.tokafka`
- 3 Clique em **Gravar**.

Integração do Change Guardian

O Sentinel é compatível com o Change Guardian 4.2 e posterior. Para receber eventos do Change Guardian, você deve primeiro fazer upgrade do servidor do Change Guardian, Agentes e editor de Política para a versão 4.2 ou posterior para garantir que o Sentinel continue recebendo eventos do Change Guardian após o upgrade.

28 Fazendo o upgrade da instalação tradicional do Sentinel

- ♦ “Fazendo upgrade do Sentinel” na página 151
- ♦ “Fazendo o upgrade do Sentinel como um usuário não root” na página 152
- ♦ “Fazendo o upgrade do Collector Manager ou do Correlation Engine” na página 154
- ♦ “Fazendo upgrade do sistema operacional” na página 155

Fazendo upgrade do Sentinel

Use as etapas a seguir para fazer upgrade do servidor Sentinel:

- 1 Faça o backup da sua configuração e, em seguida, crie a exportação ESM.
Para obter mais informações sobre como fazer backup de dados, consulte “[Fazendo backup e restaurando dados](#)” no *Guia de administração do Sentinel*.
- 2 (Condicional) Se você tiver personalizado as definições de configuração nos arquivos `server.xml`, `collector_mgr.xml` ou `correlation_engine.xml`, verifique se criou os arquivos de propriedades corretos nomeados com o ID obj-component, a fim de assegurar que as personalizações sejam mantidas após o upgrade. Para obter mais informações, consulte “[Mantendo configurações personalizadas em arquivos XML](#)” no *Guia de administração do Sentinel*.
- 3 Faça download do instalador mais recente do [Site de download](#).
- 4 Efetue login como `root` no servidor em que você deseja fazer upgrade do Sentinel.
- 5 Especifique o seguinte comando para extrair os arquivos de instalação do arquivo tar:

```
tar xzf <install_filename>
```


Substitua `<nome_arquivo_instalação>` pelo nome real do arquivo de instalação.
- 6 Altere para o diretório de onde o arquivo install foi extraído.
- 7 Especifique o seguinte comando para fazer upgrade do Sentinel:

```
./install-sentinel
```
- 8 Para prosseguir com o idioma de sua escolha, selecione o número ao lado de cada idioma.
O contrato de licença de usuário final será exibido no idioma selecionado.
- 9 Leia a licença do usuário final e digite `sim` ou `s` para aceitar a licença e continuar com a instalação.
- 10 O script de instalação detecta que uma versão mais antiga do produto já existe e solicita que você especifique se deseja fazer upgrade do produto. Para continuar com o upgrade, pressione `s`.
A instalação de todos os pacotes RPM será iniciada. A instalação pode levar alguns segundos para ser concluída.
- 11 Limpe o cache do browser da web para ver a última versão do Sentinel.

- 12 Limpe o cache do Java Web Start nos computadores cliente para usar a versão mais recente das aplicações Sentinel.
Você pode limpar o cache do Java Web Start usando o comando `javaws -clearcache` ou o Java Control Center. Para obter mais informações, consulte http://www.java.com/en/download/help/plugin_cache.xml.
- 13 (Condicional) Caso tenha ocorrido o upgrade do banco de dados PostgreSQL para uma versão mais recente (como 8.0 para 9.0 ou 9.0 para 9.1), limpe os arquivos do PostgreSQL antigo do banco de dados do PostgreSQL. Para obter informações sobre o upgrade do banco de dados PostgreSQL, consulte as Notas de versão do Sentinel.
 - 13a Mude para o usuário novell.

```
su novell
```
 - 13b Procure a pasta bin:

```
cd /opt/novell/sentinel/3rdparty/postgresql/bin
```
 - 13c Apague os arquivos PostgreSQL antigos usando o seguinte comando:

```
./delete_old_cluster.sh
```
- 14 Para fazer upgrade dos sistemas do Collector Manager e do Correlation Engine, consulte “Fazendo o upgrade do Collector Manager ou do Correlation Engine” na página 154.
- 15 (Condicional) Se você estiver usando a autenticação do Kerberos, habilite o AES256 no Java Runtime Environment, pois a pasta `java` é substituída por arquivos padrão durante o upgrade. Para habilitar o AES256 no Java Runtime Environment, conclua as etapas a seguir:
 - 15a Faça download do Java Cryptography Extension (JCE) 8 do seguinte local: <http://www.oracle.com/technetwork/java/javase/downloads/jce8-download-2133166.html>
 - 15b Extraia os dois arquivos *.jar e copie-os para `/opt/novell/sentinel/jdk/jre/lib/security` directory.
 - 15c (Condicional) Se você estiver executando o Sentinel em um ambiente de alta disponibilidade, repita essas etapas em todos os nós do cluster.
 - 15d Reinicie o Sentinel.

Fazendo o upgrade do Sentinel como um usuário não root

Se a política organizacional não permitir que você execute o upgrade completo do Sentinel como `root`, será possível fazer o upgrade como outro usuário. Nesse upgrade, algumas etapas são executadas como um usuário `root` e, em seguida, você prossegue para o upgrade do Sentinel como outro usuário criado pelo usuário `root`.

- 1 Faça o backup da sua configuração e, em seguida, crie a exportação ESM.
Para obter mais informações sobre como fazer backup de dados, consulte “Fazendo backup e restaurando dados” no *Guia de administração do Sentinel*.
- 2 (Condicional) Se você tiver personalizado as definições de configuração nos arquivos `server.xml`, `collector_mgr.xml` ou `correlation_engine.xml`, verifique se criou os arquivos de propriedades corretos nomeados com o ID obj-component, a fim de assegurar que as personalizações sejam mantidas após o upgrade. Para obter mais informações, consulte “Fazendo backup e restaurando dados” no *Guia de administração do Sentinel*.
- 3 Faça download dos arquivos de instalação no [site de downloads da](#) .

- 4 Especifique o seguinte comando na linha de comando para extrair os arquivos de instalação do arquivo tar:

```
tar -zxvf <install_filename>
```

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

- 5 Efetue login como `root` no servidor em que você deseja fazer upgrade do Sentinel.
- 6 Extraia o RPM `squashfs` dos arquivos de instalação do Sentinel.
- 7 Instale o `squashfs` no servidor do Sentinel.

```
rpm -Uvh <install_filename>
```

- 8 Especifique o seguinte comando para mudar o usuário não root `novell` recém-criado: `novell`:

```
su novell
```

- 9 (Condicional) Para realizar um upgrade interativo:

- 9a Especifique o seguinte comando:

```
./install-sentinel
```

Para fazer o upgrade do Sentinel em um local que não seja o padrão, especifique a opção `-location` juntamente com o comando. Por exemplo:

```
./install-sentinel --location=/foo
```

- 9b Continue na [Etapa 11](#).

- 10 (Condicional) Para fazer um upgrade silencioso, especifique o seguinte comando:

```
./install-sentinel -u <response_file>
```

A instalação prossegue com os valores armazenados no arquivo de resposta. O upgrade do Sentinel está concluído.

- 11 Especifique o número do idioma que deseja usar no upgrade.

O contrato de licença de usuário final será exibido no idioma selecionado.

- 12 Leia a licença por usuário final e digite `sim` ou `s` para aceitar a licença e continuar com o upgrade.

O upgrade de todos os pacotes RPM será iniciado. A instalação pode levar alguns segundos para ser concluída.

- 13 Limpe o cache do browser da web para ver a última versão do Sentinel.

- 14 Limpe o cache do Java Web Start nos computadores cliente para usar a versão mais recente das aplicações Sentinel.

Você pode limpar o cache do Java Web Start usando o comando `javaws -clearcache` ou o Java Control Center. Para obter mais informações, consulte http://www.java.com/en/download/help/plugin_cache.xml.

- 15 (Condicional) Caso tenha ocorrido o upgrade do banco de dados PostgreSQL para uma versão mais recente (como 8.0 para 9.0 ou 9.0 para 9.1), limpe os arquivos do PostgreSQL antigo do banco de dados do PostgreSQL. Para obter informações sobre o upgrade do banco de dados PostgreSQL, consulte as Notas de versão do Sentinel.

- 15a Alterne para o usuário da Novell.

```
su novell
```

- 15b Procure a pasta `bin`:

```
cd /opt/novell/sentinel/3rdparty/postgresql/bin
```

15c Apague os arquivos PostgreSQL antigos usando o seguinte comando:

```
./delete_old_cluster.sh
```

16 (Condicional) Se você estiver usando a autenticação do Kerberos, habilite o AES256 no Java Runtime Environment, pois a pasta `java` é substituída por arquivos padrão durante o upgrade. Para habilitar o AES256 no Java Runtime Environment, conclua as etapas a seguir:

16a Faça download do Java Cryptography Extension (JCE) 8 do seguinte local: <http://www.oracle.com/technetwork/java/javase/downloads/jce8-download-2133166.html>

16b Extraia os dois arquivos `*.jar` e copie-os para `/opt/novell/sentinel/jdk/jre/lib/security` directory.

16c (Condicional) Se você estiver executando o Sentinel em um ambiente de alta disponibilidade, repita essas etapas em todos os nós do cluster.

16d Reinicie o Sentinel.

Fazendo o upgrade do Collector Manager ou do Correlation Engine

Use as etapas a seguir para fazer a atualização do Collector Manager ou do Correlation Engine:

- 1 Faça o backup da sua configuração e crie a exportação ESM.
Para obter mais informações, consulte “[Fazendo backup e restaurando dados](#)” no *Guia de administração do Sentinel*.
- 2 Navegue até a interface **Principal do Sentinel** como um usuário na função de administrador.
- 3 Selecione **Downloads**.
- 4 Clique no **Download do Instalador** na seção Instalador do Collector Manager.
- 5 Grave o arquivo do instalador no respectivo servidor do Collector Manager ou Correlation Engine.
- 6 Copie o arquivo para um local temporário.
- 7 Extraia o conteúdo do arquivo.
- 8 Execute o script a seguir:

Para o Collector Manager:

```
./install-cm
```

Para o Correlation Engine:

```
./install-ce
```

- 9 Siga as instruções na tela para completar a instalação.
- 10 (Condicional) Para instalações personalizadas, execute o seguinte comando para sincronizar configurações entre o servidor do Sentinel, o Collector Manager e o Correlation Engine:

```
/opt/novell/sentinel/setup/configure.sh
```

Fazendo upgrade do sistema operacional

Esta versão do Sentinel inclui um conjunto de comandos para usar durante o procedimento de upgrade do sistema operacional. Estes comandos garantem que o Sentinel funcione corretamente após o upgrade do sistema operacional.

Observação: Você deve fazer upgrade do Sentinel antes de fazer upgrade do sistema operacional.

Use as etapas a seguir para fazer upgrade do seu sistema operacional:

- 1 No servidor do Sentinel escolhido para fazer upgrade do seu sistema operacional, efetue login como um dos seguintes:

- ♦ Usuário `root`
- ♦ Usuário não `root`

- 2 Abra um prompt de comando e mude para o diretório no qual o arquivo de instalação do Sentinel foi extraído.

- 3 Pare os serviços do Sentinel:

```
rcsentinel stop
```

- 4 (Condicional) Se o Sentinel estiver no modo FIPS antes do upgrade do sistema operacional, será preciso fazer upgrade dos arquivos do banco de dados do NSS manualmente executando o seguinte comando:

```
certutil -K -d sql:/etc/opt/novell/sentinel/3rdparty/nss -X
```

Siga as instruções na tela para fazer upgrade do banco de dados do NSS.

Dê permissões completas ao usuário `novell` para os seguintes arquivos:

```
cert9.db  
key4.db  
pkcs11.txt
```

- 5 Faça upgrade do seu sistema operacional.

- 6 (Condicional) Se você usar o NSS (Mozilla Network Security Services) 3.29, não serão instalados dois arquivos RPM dependentes `libfreebl3-hmac` e `libsoftokn3-hmac`. Instale manualmente os seguintes arquivos RPM: `libfreebl3-hmac` e `libsoftokn3-hmac`.

- 7 (Condicional) Para RHEL 7.x, execute o seguinte comando para verificar se há erros no banco de dados do RPM:

```
rpm -qa --dbpath <local_da_instalação>/rpm | grep novell
```

Exemplo: # `rpm -qa --dbpath /custom/rpm | grep novell`

- 7a Se houver qualquer erro, execute o seguinte comando para corrigir os erros:

```
rpm --rebuilddb --dbpath <local_da_instalação>/rpm
```

Exemplo: # `rpm --rebuilddb --dbpath /custom/rpm`

- 7b Execute o comando mencionado na Etapa 7 para verificar se não há erros.

- 8 Repita esse procedimento no seguinte:

- ♦ Instâncias do Collector Manager
- ♦ Instâncias do Correlation Engine
- ♦ Instâncias do NetFlow Collector Manager

- 9 Reinicie o serviço do Sentinel:


```
rcsentinel restart
```

Esta etapa não é aplicável ao Sentinel HA.

29 Fazendo upgrade da aplicação Sentinel

Os procedimentos deste capítulo guiam você durante o upgrade da aplicação do Sentinel. É possível fazer o upgrade do Sentinel sem fazer o upgrade do sistema operacional SLES, ou fazer o upgrade do Sentinel e do sistema operacional SLES. Como a aplicação Sentinel 8.2 inclui o SLES 12 SP3, o canal de atualizações do SLES 11 foi descontinuado e será removido quando o SUSE encerrar o suporte geral ao SLES 11. Portanto, é recomendável fazer upgrade para a aplicação Sentinel 8.2, que inclui o sistema operacional SLES 12 SP3 para continuar recebendo atualizações do sistema operacional. Você precisa fazer o upgrade do Sentinel antes de fazer o upgrade do sistema operacional.

- ♦ [“Fazendo upgrade do Sentinel” na página 157](#)
- ♦ [“Fazendo upgrade do sistema operacional” na página 160](#)

Fazendo upgrade do Sentinel

- ♦ [“Fazendo o upgrade do Sentinel por meio do Canal de Atualização da Aplicação” na página 157](#)
- ♦ [“Fazendo o upgrade do Sentinel usando o SMT” na página 159](#)

Fazendo o upgrade do Sentinel por meio do Canal de Atualização da Aplicação

Você pode fazer o upgrade do Sentinel usando Zypper. O Zypper é um gerente de pacotes de linha de comando que permite que você faça um upgrade interativo da aplicação. Em instâncias em que a interação do usuário é necessária para concluir o upgrade, como uma atualização de contrato de licença por usuário final, você deve fazer upgrade da aplicação do Sentinel usando o Zypper.

Para fazer o upgrade da aplicação pelo Canal de atualização da aplicação:

- 1 Faça o backup da sua configuração e, em seguida, crie a exportação ESM.
Para obter mais informações, consulte [“Fazendo backup e restaurando dados”](#) no *Guia de administração do Sentinel*.
- 2 (Condicional) Se você tiver personalizado as definições de configuração nos arquivos `server.xml`, `collector_mgr.xml` ou `correlation_engine.xml`, verifique se criou os arquivos de propriedades corretos nomeados com o ID obj-component, a fim de assegurar que as personalizações sejam mantidas após o upgrade. Para obter mais informações, consulte [“Mantendo configurações personalizadas em arquivos XML”](#) no *Guia de administração do Sentinel*.
- 3 Faça login no console de aplicativo como o usuário `root`.
- 4 Execute o seguinte comando:

```
/usr/bin/zypper patch
```
- 5 (Condicional) Se o instalador exibir uma mensagem informando que você deve resolver a dependência do pacote OpenSSH, digite a opção apropriada para instalar a versão menos eficiente do pacote OpenSSL.

- 6 (Condicional) Se o instalador exibir uma mensagem indicando mudança na arquitetura ncgOverlay, digite a opção apropriada para aceitar a mudança da arquitetura.
- 7 (Condicional) Se o instalador exibir uma mensagem informando que você deve resolver a dependência de alguns pacotes de aplicação, digite a opção apropriada para desinstalar os pacotes dependentes.
- 8 Digite `s` para continuar.
- 9 Digite `sim` para aceitar o contrato de licença.
- 10 Reinicie a aplicação Sentinel.
- 11 (Condicional) Se o Sentinel estiver instalado em uma porta personalizada ou se o Collector Manager ou o Correlation Engine estiver no modo FIPS, execute o seguinte comando:

```
/opt/novell/sentinel/setup/configure.sh
```

- 12 Limpe o cache do browser da web para ver a última versão do Sentinel.
- 13 Limpe o cache do Java Web Start nos computadores cliente para usar a versão mais recente das aplicações Sentinel.
Você pode limpar o cache do Java Web Start usando o comando `javaws -clearcache` ou o Java Control Center. Para obter mais informações, consulte http://www.java.com/en/download/help/plugin_cache.xml.
- 14 (Condicional) Caso tenha ocorrido o upgrade do banco de dados PostgreSQL para uma versão mais recente (como 8.0 para 9.0 ou 9.0 para 9.1), limpe os arquivos do PostgreSQL antigo do banco de dados do PostgreSQL. Para obter informações sobre o upgrade do banco de dados PostgreSQL, consulte as Notas de versão do Sentinel.

14a Alterne para o usuário da Novell.

```
su novell
```

14b Procure a pasta `bin`:

```
cd /opt/novell/sentinel/3rdparty/postgresql/bin
```

14c Apague os arquivos PostgreSQL antigos usando o seguinte comando:

```
./delete_old_cluster.sh
```

- 15 (Condicional) Para fazer o upgrade do Collector Manager ou do Correlation Engine, siga [Etapa 3](#) até [Etapa 11](#).
- 16 (Condicional) Se você estiver usando a autenticação do Kerberos, habilite o AES256 no Java Runtime Environment, pois a pasta `java` é substituída por arquivos padrão durante o upgrade. Para habilitar o AES256 no Java Runtime Environment, conclua as etapas a seguir:
 - 16a** Faça download do Java Cryptography Extension (JCE) 8 do seguinte local: <http://www.oracle.com/technetwork/java/javase/downloads/jce8-download-2133166.html>
 - 16b** Extraia os dois arquivos `*.jar` e copie-os para `/opt/novell/sentinel/jdk/jre/lib/security` directory.
 - 16c** Reinicie o Sentinel.
- 17 (Condicional) Se você estiver executando o Sentinel em um ambiente de alta disponibilidade, repita essas etapas em todos os nós do cluster.
- 18 (Condicional) Para fazer upgrade do sistema operacional, consulte ["Fazendo upgrade do sistema operacional"](#) na página 160
- 19 Reinicie o Sentinel.

Fazendo o upgrade do Sentinel usando o SMT

Em ambientes seguros, onde a aplicação deve ser executada sem acesso direto à internet, configure a aplicação com a Subscription Management Tool (SMT), que permite que você faça o upgrade da aplicação para as versões mais recentes disponíveis.

- 1 Certifique-se de que o aplicativo esteja configurado com SMT.

Para obter mais informações, consulte [“Configurando a aplicação com SMT”](#) na página 108.

- 2 Faça o backup da sua configuração e, em seguida, crie a exportação ESM.

Para obter mais informações, consulte [“Fazendo backup e restaurando dados”](#) no *Guia de administração do Sentinel*.

- 3 (Condicional) Se você tiver personalizado as definições de configuração nos arquivos `server.xml`, `collector_mgr.xml` ou `correlation_engine.xml`, verifique se criou os arquivos de propriedades corretos nomeados com o ID obj-component, a fim de assegurar que as personalizações sejam mantidas após o upgrade. Para obter mais informações, consulte [“Mantendo configurações personalizadas em arquivos XML”](#) no *Guia de administração do Sentinel*.

- 4 Faça login no console do aplicativo como o usuário `root`.

- 5 Atualize o repositório para atualização:

```
zypper ref -s
```

- 6 Verifique se o aplicativo está habilitado para atualização:

```
zypper lr
```

- 7 (Opcional) Verifique se há atualizações disponíveis para o aplicativo:

```
zypper lu
```

- 8 (Opcional) Verifique se há pacotes que incluem as atualizações disponíveis para o dispositivo:

```
zypper lp -r SMT-http_<smt_server_fqdn>:<package_name>
```

- 9 Atualize o aplicativo:

```
zypper up -t patch -r SMT-http_<smt_server_fqdn>:<package_name>
```

- 10 Reinicie o aplicativo.

```
rcsentinel restart
```

- 11 (Condicional) Se o Sentinel estiver instalado em uma porta personalizada ou se o Collector Manager ou o Correlation Engine estiver no modo FIPS, execute o seguinte comando:

```
/opt/novell/sentinel/setup/configure.sh
```

- 12 (Condicional) Para fazer o upgrade do Collector Manager ou do Correlation Engine, siga [Etapa 4](#) até [Etapa 11](#).

- 13 (Condicional) Se você estiver usando a autenticação do Kerberos, habilite o AES256 no Java Runtime Environment, pois a pasta `java` é substituída por arquivos padrão durante o upgrade. Para habilitar o AES256 no Java Runtime Environment, conclua as etapas a seguir:
 - 13a Faça download do Java Cryptography Extension (JCE) 8 do seguinte local: <http://www.oracle.com/technetwork/java/javase/downloads/jce8-download-2133166.html>
 - 13b Extraia os dois arquivos `*.jar` e copie-os para `/opt/novell/sentinel/jdk/jre/lib/security directory`.
 - 13c Reinicie o Sentinel.
- 14 (Condicional) Se você estiver executando o Sentinel em um ambiente de alta disponibilidade, repita essas etapas em todos os nós do cluster.
- 15 (Condicional) Para fazer upgrade do sistema operacional, consulte “Fazendo upgrade do sistema operacional” na página 160.
- 16 Reinicie o Sentinel.

Fazendo upgrade do sistema operacional

Você deve fazer upgrade do sistema operacional após fazer upgrade do Sentinel. Depois de fazer o upgrade do sistema operacional, você deve configurar a aplicação para promover os novos recursos do Gerenciador de Aplicação Sentinel. O Gerenciador de Aplicação Sentinel fornece uma interface do usuário simples com base na Web que ajuda você a configurar e gerenciar a aplicação. Ela substitui o recurso WebYast existente.

Para fazer upgrade do sistema operacional e configurar a aplicação:

- 1 Faça o upgrade do Sentinel. Para obter mais informações, consulte o “Fazendo upgrade do Sentinel” na página 157.
- 2 Pare os serviços do Sentinel:

```
rcsentinel stop
```
- 3 (Condicional) Se o Sentinel estiver no modo FIPS antes do upgrade do sistema operacional, será preciso fazer upgrade dos arquivos do banco de dados do NSS manualmente executando o seguinte comando:

```
certutil -K -d sql:/etc/opt/novell/sentinel/3rdparty/nss -X
```

Siga as instruções na tela para fazer upgrade do banco de dados do NSS.
Dê permissões completas ao usuário `novell` para os seguintes arquivos:

```
cert9.db
key4.db
pkcs11.txt
```
- 4 (Condicional) Se você estiver usando o NSS (Mozilla Network Security Services) 3.29, não serão instalados dois arquivos RPM dependentes `libfreebl3-hmac` e `libsoftoken3-hmac`. Instale manualmente os seguintes arquivos RPM: `libfreebl3-hmac` e `libsoftoken3-hmac`.
- 5 Faça download do instalador do SLES 12 SP3 e do utilitário de pós-upgrade do site do [Micro Focus Patch Finder](#). Para o HA do Sentinel, faça também o download do arquivo de HA do SLES 12 SP3.
- 6 Siga os prompts de instalação para fazer upgrade do sistema operacional. Para o HA do Sentinel, quando solicitado a instalar produtos complementares adicionais, selecione o local em que você fez o download do arquivo de HA do SLES 12 SP3 e prossiga com o upgrade.

Para obter mais informações sobre como fazer upgrade para o SLES 12 SP3, consulte [Documentação SLES](#).

- 7 Durante o processo de upgrade, o SLES renomeia o arquivo `/etc/sysctl.conf` para `/etc/sysctl.conf.rpmsave` como um backup e cria um novo arquivo `/etc/sysctl.conf`. Após fazer upgrade, copie o conteúdo do arquivo `/etc/sysctl.conf.rpmsave` para o arquivo `/etc/sysctl.conf`. Abra o arquivo `sysctl.conf` e pesquise `# Added by sentinel vm.max_map_count`. Mova esta configuração para a próxima linha da seguinte maneira:

Mudança

```
net.core.wmem_max = 67108864# Added by sentinel vm.max_map_count : 65530
vm.max_map_count = 262144
```

para

```
net.core.wmem_max = 67108864
# Added by sentinel vm.max_map_count : 65530
vm.max_map_count = 262144
```

- 8 (Condicional) Para o HA do Sentinel, conclua as etapas mencionadas nas seções a seguir:

- ♦ [“Configurando destinos iSCSI” na página 214](#)
- ♦ [“Configurando iniciadores iSCSI” na página 215](#)
- ♦ [“Configurando o cluster de HA” na página 216](#)

- 9 Para configurar a aplicação, execute o utilitário pós-upgrade no prompt de comando:

9a Descompacte o arquivo:

```
tar -xvf <nome do arquivo instalador do utilitário pós-upgrade>.tar.gz
```

9b Mude para o diretório no qual extraiu o utilitário:

```
cd <nome do arquivo instalador do utilitário pós-upgrade>
```

9c Para configurar a aplicação, execute o seguinte script:

```
./appliance_SLESISO_post_upgrade.sh
```

Observação: Não execute este script remotamente, pois ele envolve a reconfiguração da rede.

9d Siga as instruções na tela para concluir a configuração.

Este script reconfigura os pacotes instalados e configura os pacotes para gerenciar a aplicação.

- 10 Usando seu código de registro existente, registre-se novamente para receber o Sentinel e as atualizações mais recentes do sistema operacional. Para obter mais informações, consulte o [“Registrando para receber atualizações” na página 106](#).

30 Configurações Pós-Upgrade

Este capítulo inclui as configurações pós-upgrade.

- ♦ [“Protegendo dados no Elasticsearch” na página 163](#)
- ♦ [“Configurando visualizações de eventos” na página 163](#)
- ♦ [“Configurando coleta de dados de Fluxo de IP” na página 164](#)
- ♦ [“Configuração Pós-Upgrade para o Gerente de Dados Escalável do Sentinel” na página 165](#)
- ♦ [“Adicionando o driver JDBC DB2” na página 167](#)
- ♦ [“Configurando propriedades de federação de dados na aplicação do Sentinel” na página 167](#)
- ♦ [“Registrando a aplicação do Sentinel atualizações” na página 168](#)
- ♦ [“Atualizando bancos de dados externos para sincronização de dados” na página 168](#)
- ♦ [“Reautenticando o Sentinel no Modo de Autenticação de Vários Fatores” na página 168](#)

Protegendo dados no Elasticsearch

O Sentinel utiliza o Kibana, um painel de controle de análise e pesquisa baseado em browser, que ajuda você a visualizar eventos e alertas em painéis de controle. O Sentinel armazena e indexa alertas no Elasticsearch. É possível configurar o Sentinel para armazenar e indexar eventos no Elasticsearch para aproveitar os recursos de visualização de eventos. Os painéis de controle do Sentinel acessam dados do Elasticsearch para apresentar eventos e alertas em painéis de controle. Para verificar se os painéis de controle exibem somente os dados que a função de um usuário está autorizada a visualizar e impedir o acesso não autorizado a dados no Elasticsearch, instale o plug-in de segurança do Elasticsearch. Para obter mais informações, consulte [“Protegendo dados no Elasticsearch” na página 79](#).

Configurando visualizações de eventos

O Sentinel fornece visualizações de eventos que apresentam dados em gráficos, tabelas e mapas. Essas visualizações facilitam a visualização e a análise de grandes volumes de dados, como eventos, eventos de Fluxo de IP e alertas. Também é possível criar suas próprias visualizações e painéis de controle.

O Sentinel utiliza o Kibana, um painel de controle de análise e pesquisa baseado em browser, que ajuda você a pesquisar e visualizar eventos. O Kibana acessa dados do armazenamento de dados de visualização (Elasticsearch) para apresentar eventos em painéis de controle. Por padrão, o Sentinel inclui um nó do Elasticsearch. Você deve habilitar a visualização de eventos para armazenar e indexar eventos no Elasticsearch. Para obter mais informações, consulte [“Configurando o armazenamento de dados de visualização” na página 43](#).

Observação: Alguns dos painéis de controle do Sentinel que usam o Kibana não são carregados após o upgrade para o Sentinel 8.2. Esse problema ocorre porque foi feito o upgrade das versões do Elasticsearch e do Kibana no Sentinel 8.2 e o arquivo de índice do Kibana existente não é compatível com as versões com upgrade do Elasticsearch e do Kibana. Para corrigir esse problema,

você deve apagar manualmente o arquivo de índice do Kibana existente e recriar um novo arquivo de índice do Kibana. Para obter mais informações, consulte o [Artigo da Base de conhecimento 7022736](#).

Configurando coleta de dados de Fluxo de IP

O Sentinel agora aproveita os ArcSight SmartConnectors que ajudam você a monitorar sua rede corporativa, coletando dados de Fluxo de IP além dos dados do NetFlow. Os SmartConnectors coletam dados de Fluxo de IP como eventos, o que permite:

- ♦ Usar as instâncias do Collector Manager existentes para coletar dados do Fluxo de IP. Você não precisa mais das instâncias do NetFlow Collector Manager para coletar dados do NetFlow.
- ♦ Aproveite os dados do Fluxo de IP em várias áreas do Sentinel, como visualizações, roteamento de eventos, federação de dados, relatórios e correlação.
- ♦ Aplique políticas de retenção de dados aos dados do Fluxo de IP, que lhe permite armazenar esses dados pelo tempo que você quiser.

Depois de fazer upgrade do Sentinel, é possível continuar usando os recursos do NetFlow ou optar por configurar a coleta de dados do Fluxo de IP. No entanto, com a disponibilidade do recurso de visualização e coleta de dados do Fluxo de IP, os recursos do NetFlow anteriormente disponíveis, incluindo as visualizações do NetFlow, agora foram descontinuados e serão removidos no futuro para uma melhor experiência do usuário.

Depois de habilitar a coleta de dados do Fluxo de IP:

- ♦ Os dados de Fluxo de IP serão coletados como eventos e, portanto, serão considerados para contagem de EPS.
- ♦ Você perderá todos os dados do NetFlow coletados antes de habilitar o Fluxo de IP. O sistema NetFlow descontinuado tinha uma retenção máxima de 3 dias. Você pode manter os eventos de Fluxo de IP pelo tempo que precisar.
- ♦ Não é possível migrar os dados do NetFlow coletados antes de habilitar o Fluxo de IP no recurso de Fluxo de IP.
- ♦ Não será possível reverter a configuração, a menos que você reinstale o Sentinel.
- ♦ Você será desconectado do Sentinel Principal e precisará efetuar login novamente.

Para configurar a coleta de dados do Fluxo de IP:

- 1 Instale e configure o ArcSight SmartConnector. Ao configurar, verifique se você definiu os SmartConnectors relevantes que coletam dados de Fluxo de IP.

Para obter informações sobre como configurar SmartConnectors, consulte a documentação do Generic Universal CEF Collector no [site de plug-ins do Sentinel](#).

- 2 No **Sentinel Principal** > **Coleção** > **Fluxo de IP**, selecione **Coletar dados de Fluxo de IP** e clique em **Habilitar**.

Observação: Como os eventos de Fluxo de IP agora são enviados ao Collector Manager, você não precisa mais usar as instâncias do NetFlow Collector Manager. Portanto, é possível desinstalar quaisquer instâncias do NetFlow Collector Manager. Para obter mais informações, consulte [“Desinstalando o NetFlow Collector Manager” na página 230](#).

Configuração Pós-Upgrade para o Gerente de Dados Escalável do Sentinel

- ♦ [“Instalar o plug-in de segurança do Elasticsearch” na página 165](#)
- ♦ [“Atualizando Aplicativos do Spark no YARN” na página 165](#)
- ♦ [“Habilitando Recursos do Sentinel” na página 166](#)
- ♦ [“Atualizando painéis de controle e visualizações no Gerenciador de dados escaláveis do Sentinel” na página 166](#)

Instalar o plug-in de segurança do Elasticsearch

Além dos nós externos do Elasticsearch, o Sentinel agora inclui um nó do Elasticsearch local por padrão para visualização de dados. Portanto, você deve instalar um plug-in do Elasticsearch para o Elasticsearch local. Para obter mais informações, consulte [“Instalando o plug-in de segurança do Elasticsearch” na página 80](#).

Uma vez que é feito o upgrade do Elasticsearch e do Kibana usados no Sentinel, você deve reimplantar todos os plug-ins de segurança do Elasticsearch nos nós do Elasticsearch existentes. Para obter mais informações sobre como reimplantar o plug-in de segurança do Elasticsearch, consulte [“Reimplantar o plug-in de segurança do Elasticsearch” na página 84](#).

Atualizando Aplicativos do Spark no YARN

Durante o upgrade do Sentinel, alguns dos arquivos do aplicativo Spark também são atualizados. Você deve reenviar os aplicativos do Spark com esses arquivos atualizados executando as seguintes etapas:

- 1 Efetue login no servidor SSDM como o usuário `novell` e copie os arquivos para o servidor do histórico do Spark em que o NameNode HDFS está instalado:

```
cd /etc/opt/novell/sentinel/scalablestore
```

```
scp SparkApp-*.jar avroevent-*.avsc avrorawdata-*.avsc spark.properties  
log4j.properties manage_spark_jobs.sh root@<hdfs_node>:<destination_directory>
```

em que `<destination_directory>` é qualquer diretório em que você deseja colocar os arquivos copiados. Além disso, verifique se o usuário `hdfs` tem permissões completas para esse diretório.
- 2 Efetue login no servidor `<hdfs_node>` como o usuário `root` e mude a propriedade dos arquivos copiados para o usuário `hdfs`:

```
cd <destination_directory>
```

```
chown hdfs SparkApp-*.jar avroevent-*.avsc avrorawdata-*.avsc spark.properties  
log4j.properties manage_spark_jobs.sh
```

Atribua a permissão executável ao script `manage_spark_jobs.sh`.
- 3 Verifique se as tarefas do Spark concluíram o processamento de todos os dados:
Acesse a interface do usuário do ResourceManager Web do YARN e veja cada aplicativo Sentinel Spark. Os dados do aplicativo Spark Streaming mostrarão a queda da taxa de entrada para zero quando todos os dados forem processados no Kafka.
- 4 Execute o seguinte comando para parar o processamento de dados:

```
./manage_spark_jobs.sh stop
```
- 5 Limpe o ponto de verificação de processamento de dados:

```
sudo -u hdfs hadoop fs -rm -R -skipTrash /spark/checkpoint
```

em que `/spark/checkpoint` é o diretório do ponto de verificação.

- 6 Execute o script a seguir para reenviar as tarefas do Spark:

```
./manage_spark_jobs.sh start
```

O comando acima leva um tempo para concluir o processo de envio.

- 7 (Opcional) Execute o comando a seguir para verificar o status das tarefas do Spark enviadas:

```
./manage_spark_jobs.sh status
```

- 8 Continue o encaminhamento de eventos para o Kafka for Spark para começar a processar eventos:

8a Em Principal do Sentinel, clique em **Armazenamento > Armazenamento Escalável > Configurações Avançadas > Kafka**.

8b Defina a propriedade a seguir como falsa:

```
pause.events.tokafka
```

8c Clique em **Gravar**.

Habilitando Recursos do Sentinel

Ao fazer upgrade do SSDM 8.0.x.x, por padrão alguns dos recursos do Sentinel adicionados ao Sentinel 8.1 e posterior não estão disponíveis. Você deve habilitar manualmente esses recursos no arquivo `/etc/opt/novell/sentinel/config/ui-configuration.properties`.

- 1 Efetue login no servidor do Sentinel como usuário `novell`.
- 2 Abra o arquivo `/etc/opt/novell/sentinel/config/ui-configuration.properties`.
- 3 Mude as propriedades a seguir para falsas:

```
alerts.hideUI
solutionDesigner.launcher.hideUI
correlation.hideUI
scc.configurations.solutionPacks.hideUI
people.hideUI
permission.knowledgeBase.hideUI
scc.menuBarItem.toolsMenu.hideUI
scc.toolBarItem.peopleBrowser.hideUI
integration.hideUI
```

- 4 Atualize o browser do Sentinel.

Atualizando painéis de controle e visualizações no Gerenciador de dados escaláveis do Sentinel

Você deve atualizar painéis de controle e visualizações após o upgrade do SSDM para que os aprimoramentos incluídos na versão mais recente de painéis de controle e visualizações sejam aplicados.

Ao fazer upgrade do SSDM, os painéis de controle e as visualizações não são atualizados por padrão. No entanto, é possível atualizar manualmente após fazer o upgrade. É possível atualizar painéis de controle e visualizações apagando os painéis e visualizações existentes e executando o script `load_kibana_data.sh`, que instala painéis de controle e visualizações mais recentes.

Importante: As personalizações que você pode ter feito em painéis de controle e visualizações serão perdidas ao atualizá-los.

Para atualizar painéis de controle e visualizações:

- 1 Efetue login na interface da Web do SSCM e vá para Visualização de Eventos.
- 2 Em Visualização de Eventos, vá até **Configurações > Objetos > Painéis de controle**.
- 3 Selecione os painéis de controle que deseja atualizar e clique em **Apagar**.
- 4 Clique em **Visualizações**. Selecione as visualizações que deseja atualizar e clique em **Apagar**.
- 5 Efetue logout da interface da Web do SSDM.
- 6 Efetue login no servidor SSDM como usuário do novell.
- 7 Vá para o diretório `/opt/novell/sentinel/bin`.

- 8 Execute o `load_kibana_data.sh` usando o comando a seguir:

```
./load_kibana_data.sh http://<endereço ip>:<porta>> <alerts/events/misc>
```

Por exemplo:

```
./load_kibana_data.sh http://127.0.0.1:9200 alerts
```

```
./load_kibana_data.sh http://127.0.0.1:9200 events
```

- 9 Efetue login na interface da Web do SSDM e vá até Visualização de Eventos para ver as atualizações de painéis de controle e visualizações.

Adicionando o driver JDBC DB2

Após fazer o upgrade para o Sentinel, adicione o driver JDBC correto e configure-o para coleta e sincronização de dados seguindo as etapas a seguir:

- 1 Copie a versão correta do driver IBM DB2 JDBC (`db2jcc-*.jar`) para sua versão do banco de dados DB2 na pasta `/opt/novell/sentinel/lib`.
- 2 Verifique se você definiu a propriedade e as permissões necessárias para o arquivo do driver.
- 3 Configure esse driver para a coleta de dados. Para obter mais informações, consulte a documentação do [Conector do banco de dados](#).

Configurando propriedades de federação de dados na aplicação do Sentinel

Realize o seguinte procedimento após o upgrade da aplicação do Sentinel, para que a federação de dados não exiba nenhum erro no ambiente em que dois ou mais NICs estejam configurados:

- 1 No servidor do solicitante autorizado, adicione a seguinte propriedade no arquivo `/etc/opt/novell/sentinel/config/configuration.properties` da seguinte maneira:

```
sentinel.distsearch.console.ip=<um dos endereços IP do solicitante autorizado>
```
- 2 No servidor de origem de dados, adicione a seguinte propriedade no arquivo `/etc/opt/novell/sentinel/config/configuration.properties` da seguinte maneira:

```
sentinel.distsearch.target.ip=<um dos endereços IP da origem de dados>
```
- 3 Reinicie o Sentinel:

```
rcsentinel restart
```

- 4 Faça login no servidor do solicitante autorizado e clique em Integração. Se a origem de dados que deseja adicionar já estiver presente, apague-a e adicione-a novamente usando um dos endereços IP que você especificou na etapa 2.

Da mesma maneira, adicione os solicitantes autorizados usando os endereços IP que você especificou na etapa 1.

Registrando a aplicação do Sentinel atualizações

Se você fez o upgrade do sistema operacional, deverá registrar novamente a aplicação Sentinel para receber o Sentinel e as atualizações mais recentes do sistema operacional. Você pode usar sua chave de registro existente para se registrar novamente para receber atualizações. Para registrar a aplicação, consulte [“Registrando para receber atualizações” na página 106](#).

Atualizando bancos de dados externos para sincronização de dados

A partir do Sentinel 8.x, o tamanho do campo `Mensagem (msg)` de evento aumentou de 4.000 para 8.000 caracteres para acomodar mais informações.

Caso tenha criado uma política de sincronização de dados em versões anteriores do Sentinel que sincroniza o campo de evento `Mensagem (msg)` com um banco de dados externo, você deverá aumentar o tamanho da coluna mapeada apropriada no banco de dados externo de forma adequada.

Observação: A etapa acima será aplicável apenas se você estiver fazendo upgrade de versões anteriores do Sentinel para o 8.x.

Reautenticando o Sentinel no Modo de Autenticação de Vários Fatores

Quando você faz upgrade do servidor do Sentinel no modo MFA, as instâncias do NetFlow Collector Manager existentes não se reautenticam no servidor do Sentinel automaticamente. Você deve executar as seguintes etapas para reautenticar manualmente as instâncias do NetFlow Collector Manager para o servidor do Sentinel.

Para reautenticar o Sentinel no modo MFA:

- 1 Efetue login no computador do NetFlow Collector Manager.
- 2 Acesse `/opt/novell/sentinel/setup`.
- 3 Execute o script `configure.sh`.

Você será solicitado a efetuar login no servidor do Sentinel.

- 4 Especifique seu nome de usuário LDAP e a senha.
- 5 Forneça o ID do cliente do Sentinel e o segredo do cliente do Sentinel.

Para recuperar o ID do cliente do Sentinel e o segredo do cliente do Sentinel, vá para o seguinte URL:

`https://Sentinel_FQDN:port/SentinelAuthServices/oauth/clients`

Em que:

- ♦ `Sentinel_FQDN` é o nome de domínio completo e qualificado do servidor do Sentinel.

Por exemplo, `abc.netiq.com`

em que `abc` é o nome de host do servidor do Sentinel, `netiq.com` é o nome do domínio.

- ♦ `Porta` é a porta que o Sentinel usa (normalmente 8443).

O URL especificado usa sua sessão atual do Sentinel para recuperar o ID do cliente do Sentinel e o segredo do cliente do Sentinel.

31

Fazendo upgrade de plug-ins do Sentinel

O upgrade das instalações do Sentinel não atualiza os plug-ins, exceto se um plug-in específico não for compatível com a última versão do Sentinel.

Plug-ins novos e atualizados do Sentinel, incluindo Pacotes de solução, são frequentemente carregados para o [site de plug-ins do Sentinel](#). Para obter as correções de bug, atualizações de documentação e melhorias mais recentes para um plug-in, faça o download e instale a versão mais recente do plug-in. Para obter informações sobre como instalar um plug-in, consulte a documentação específica do plug-in.

VI

Migrando dados do armazenamento tradicional

A migração de dados do Sentinel com o armazenamento tradicional permite que você aproveite seus dados do Sentinel existentes e o tempo que você investiu. Para migrar dados do Sentinel com armazenamento tradicional, a versão do Sentinel nos servidores do Sentinel de origem e de destino deve ser a mesma. Por exemplo, se você quiser migrar dados do Sentinel 8.1 (origem) para o Sentinel 8.2 (destino), primeiro faça o upgrade do Sentinel 8.1 para o Sentinel 8.2 e inicie com o processo de migração de dados.

Esta seção fornece informações sobre como migrar dados existentes para o componente de armazenamento de dados desejado.

- ♦ [Capítulo 32, “Migrando dados para o armazenamento escalável” na página 175](#)
- ♦ [Capítulo 33, “Migrando dados para o Elasticsearch” na página 181](#)
- ♦ [Capítulo 34, “Migrando dados” na página 183](#)

32 Migrando dados para o armazenamento escalável

Você pode ter um único servidor do Sentinel ou vários servidores do Sentinel com armazenamento tradicional. O processo de migração de dados que você precisa seguir depende de como você deseja configurar e manter a implantação do Sentinel.

Tabela 32-1 *Processo de Migração de Dados para Implantação do Sentinel*

Implantação do Sentinel	Processo de migração
Você tem um único servidor do Sentinel e planeja fazer upgrade do seu servidor Sentinel existente para armazenamento escalável.	Migre os dados do evento e os dados brutos do armazenamento tradicional para o armazenamento escalável depois de fazer upgrade do servidor do Sentinel e habilitar o armazenamento escalável. Para obter mais informações, consulte o Capítulo 34, “Migrando dados” na página 183.
Você tem um único servidor do Sentinel com armazenamento tradicional e deseja configurar outro servidor do Sentinel para armazenamento escalável para poder usar todos os recursos no Sentinel.	Use o utilitário de Backup e Restauração para migrar dados do Sentinel com armazenamento tradicional para o Sentinel com armazenamento escalável. Para obter informações sobre como usar o utilitário de backup e restauração, consulte “Restaurando e Fazendo Backup de Dados” no <i>Guia de Administração do Sentinel</i> .

Implantação do Sentinel	Processo de migração
<p>Você tem uma configuração multicamadas em que você tem vários servidores do Sentinel e planeja configurar um novo servidor do Sentinel ou usar um dos servidores existentes para o armazenamento escalável. É preciso migrar os dados de configuração para além dos dados de eventos e dos dados brutos.</p>	<p>Em uma configuração multicamadas, você pode identificar um dos servidores tradicionais do Sentinel que tem a maioria dos seus dados e, em seguida, usar o utilitário de backup e restauração para migrar os dados.</p> <p>Se você precisar fazer backup dos dados do restante dos seus servidores do Sentinel, você deverá migrar os dados de configuração, os dados de eventos e os dados brutos desses servidores usando uma abordagem diferente descrita mais adiante nesta seção. Você também deve recriar manualmente algumas das configurações.</p> <p>Não é possível usar o utilitário de backup e restauração para migrar seus dados de vários servidores porque o utilitário substitui dados existentes quando você restaura. Por exemplo, se você já restaurou dados do Servidor A e depois tenta restaurar dados do Servidor B, esse utilitário substitui os dados já restaurados do Servidor A.</p> <p>Portanto, para entender o processo de migração de dados envolvido, siga as instruções fornecidas nas seções a seguir na mesma ordem:</p> <ul style="list-style-type: none"> ♦ Dados que você pode migrar ♦ Migrando Dados de Configuração ♦ Migrando dados ♦ Migrando Alertas e Dados do NetFlow ♦ Atualizando Clientes do Sentinel ♦ Importando a Configuração do ESM

Dados que você pode migrar

Você pode migrar dados de eventos, dados brutos e alguns dos dados de configuração. Você deve recriar manualmente a inatividade da configuração, que não pode ser migrada.

Tabela 32-2 Configurações que você pode migrar e Configurações que você precisa recriar

Configurações que você pode migrar	Configurações que você precisa recriar
<ul style="list-style-type: none">♦ Regras de correlação♦ Ações♦ Mapas♦ Filtros♦ Feeds de Ameaças♦ Configuração do ESM♦ Alertas com exceção dos dados da Base de Conhecimento♦ NetFlow	<ul style="list-style-type: none">♦ Locatários, Funções, Usuários e Configuração LDAP♦ Regras de roteamento de alertas e eventos♦ Políticas de retenção de alertas e dados♦ Dashboards♦ Exibições em tempo real♦ Informações de identidade♦ Configurações de feeds♦ Configuração do plug-in de Ações e Integradores♦ Configuração de segurança

Migrando Dados de Configuração

Antes de migrar os dados de eventos, você deve primeiro migrar os dados de configuração para o servidor de destino do Sentinel. Você pode fazer backup de algumas das configurações usando o Solution Designer e as opções Exportar e Importar no ESM (Event Source Management - Gerenciamento de Fonte de Evento). Você deve recriar manualmente a inatividade dos dados de configuração, que não pode ser exportada ou copiada em backup.

- ♦ [“Fazendo backup dos Dados no Servidor de Origem” na página 177](#)
- ♦ [“Restaurando Dados no Servidor de Destino” na página 178](#)

Fazendo backup dos Dados no Servidor de Origem

Você deve fazer backup dos dados necessários usando várias opções no Sentinel.

- ♦ [“Usando Pacotes de Solução” na página 178](#)
- ♦ [“Usando a Opção Configuração de Exportar no ESM” na página 178](#)

Usando Pacotes de Solução

Faça o backup da configuração a seguir no servidor de origem usando o Solution Designer:

Tabela 32-3 Dados de configuração

Dados	Notas
<input type="checkbox"/> Regras de correlação	Crie controles separados para cada Correlation Engine para que você possa migrar as regras separadamente para instâncias do Correlation Engine específicas.
<input type="checkbox"/> Ações	Você pode fazer backup somente de ações de JavaScript e não de ações herdadas, como lista dinâmica e criar incidentes.
<input type="checkbox"/> Enriquecimento de Eventos	O Sentinel também faz backup dos mapas associados para os campos de eventos. Portanto, você não precisa recriar os mapas associados após restaurar dados de enriquecimento de eventos.
<input type="checkbox"/> Filtros	Faz backup de todos os filtros personalizados.
<input type="checkbox"/> Fontes	O Pacote de Solução faz backup dos plug-ins de Alimentação, mas não faz backup da configuração do plug-in.

Para obter informações sobre como fazer backup de dados no Solution Designer, consulte [“Criando Pacotes de Solução”](#) no *Guia de Administração do Sentinel*.

Usando a Opção Configuração de Exportar no ESM

Faça o backup da sua configuração de coleta de dados usando a opção de configuração Exportar no ESM. Para obter mais informações, consulte [“Exportando Configurações”](#) no *Guia de Administração do Sentinel*.

Restaurando Dados no Servidor de Destino

- ♦ [“Instalando Dados de Configuração do Pacote de Solução”](#) na página 178
- ♦ [“Recriando a configuração manualmente”](#) na página 178

Instalando Dados de Configuração do Pacote de Solução

Importe os dados de configuração dos quais você fez backup no servidor de origem usando o Solution Designer. Para obter mais informações, consulte [“Instalando Conteúdo de Pacotes de Solução”](#) no *Guia de Administração do Sentinel*.

Renomeie os nomes duplicados de objetos como Filtros, Ações e Regras de Correlação. Por padrão, todos os Filtros são Públicos quando você os importa no servidor de destino. Reatribua a permissão para cada filtro manualmente.

Recriando a configuração manualmente

Além dos dados de configuração que você importou do Pacote de Solução, você deve recriar manualmente todas as outras configurações. Para obter mais informações sobre as configurações que você precisa recriar manualmente, consulte [Tabela 32-2, “Configurações que você pode migrar e Configurações que você precisa recriar”](#) na página 177.

Migrando Dados de Eventos e Dados Brutos

Para migrar dados de eventos e dados brutos, consulte [Migrando dados](#).

Migrando Alertas e Dados do NetFlow

Você pode usar o utilitário de backup e restauração para migrar dados de Alertas e do NetFlow do servidor de origem para o servidor de destino. Para alertas, este utilitário restaura os eventos que acionaram o alerta. No entanto, isto não restaura a regra de correlação associada e a informação da base de conhecimento.

Use os seguintes comandos para fazer backup e restaurar dados do NetFlow e de Alertas:

```
For backing up:  
./backup_util.sh -i
```

```
For restore:  
./backup_util.sh -m restore -f <backup_file_path>
```

Para os dados do NetFlow e de Alertas, você tem uma opção para anular ou anexar a dados existentes. Escolha a opção desejada.

Embora o comando acima faça backup e restaure os dados da Inteligência de Segurança, você não pode usar esses dados porque a Inteligência de Segurança não está disponível no SSDM.

Para obter informações detalhadas sobre como usar o utilitário de backup e restauração, consulte “[Restaurando e Fazendo Backup de Dados](#)” no [Guia de Administração do Sentinel](#).

Atualizando Clientes do Sentinel

Você deve atualizar qualquer configuração existente das instâncias do Collector Manager, do Correlation Engine e do NetFlow Collector Manager de modo que eles comecem a se comunicar com o servidor de destino do Sentinel. Para obter mais informações, consulte “[Atualizando Clientes do Sentinel](#)” no [Guia de Administração do Sentinel](#).

Observação: Embora você já tenha migrado dados de eventos do servidor de origem, deve executar o script de migração de dados novamente para migrar quaisquer dados de evento que possam ter chegado durante ou após esse processo. Para obter mais informações, consulte o [Capítulo 34, “Migrando dados”](#) na [página 183](#).

Importando a Configuração do ESM

Importe a configuração de coleta de dados que você usou no servidor de origem usando a opção Importar Configuração na interface do usuário do ESM. Para obter mais informações, consulte “[Importando Configurações](#)” no [Guia de Administração do Sentinel](#).

33 Migrando dados para o Elasticsearch

O Sentinel armazena dados no armazenamento tradicional com base no arquivo e indexa os dados localmente no servidor do Sentinel por padrão. Quando você habilita a visualização de eventos, o Sentinel armazena e indexa os dados no Elasticsearch, além do armazenamento tradicional com base no arquivo. Os painéis de controle exibem apenas os eventos processados depois que você habilitou a visualização de eventos. Para ver os eventos existentes no armazenamento com base no arquivo, migre os dados do armazenamento com base no arquivo para o Elasticsearch. Para migrar dados para o Elasticsearch, consulte [Capítulo 34, “Migrando dados” na página 183](#).

34 Migrando dados

É possível usar o script `data_uploader.sh` para migrar dados para um dos seguintes componentes de armazenamento de dados:

- ♦ **Kafka:** É possível migrar dados brutos e de eventos para o Kafka. Execute o script individualmente para dados de eventos e dados brutos. O script migra os dados para os tópicos do Kafka.

É possível especificar personalizações, como compactar dados durante a migração, enviar dados em lotes e assim por diante. Para especificar essas personalizações, crie um arquivo de propriedades e adicione as propriedades necessárias no formato de chave-valor. Por exemplo, você pode adicionar propriedades da seguinte forma:

```
compression.type=lz4
```

```
batch.size=20000
```

Para obter mais informações sobre as propriedades do Kafka, consulte a [Documentação do Kafka](#). Defina as propriedades e os valores delas a seu critério, porque o script não valida essas propriedades.

Observação: Verifique se o servidor do Sentinel pode resolver todos os nomes de host do controlador Kafka para endereços IP válidos para todo o cluster Kafka. Se o DNS não estiver configurado para permitir isso, adicione os nomes de host do controlador Kafka ao arquivo `/etc/hosts` do servidor do Sentinel.

- ♦ **Elasticsearch:** É possível migrar apenas dados de eventos para o Elasticsearch. Antes de migrar os dados, verifique se você habilitou a visualização de eventos. Para obter mais informações, consulte [“Habilitando a visualização de eventos” na página 123](#).

O script transfere dados para a faixa de datas (de e para) que você especifica. Quando você executa o script, ele exibe os parâmetros obrigatórios e opcionais que você deve especificar para iniciar a migração de dados e também as informações sobre as propriedades relevantes a serem usadas para o componente de armazenamento de dados desejado.

O script deve ser executado como usuário `novell`. Portanto, verifique se os diretórios de dados e os arquivos que você especifica têm as permissões apropriadas para o usuário `novell`. Por padrão, o script migra dados do armazenamento primário. Se você quiser migrar dados do armazenamento secundário, especifique o caminho apropriado para o armazenamento secundário ao executar o script.

Para migrar dados:

- 1 Efetue login no servidor do Sentinel como o usuário `novell`.
- 2 Execute o script a seguir:

```
/opt/novell/sentinel/bin/data_uploader.sh
```
- 3 Siga as instruções na tela e execute o script novamente com os parâmetros necessários.

Os dados migrados terão o período de retenção conforme definido no servidor de destino.

Após a migração de dados estar concluída, o script registra o status, como partições migradas com êxito, partições que não foram migradas, número de eventos migrados e assim por diante. Para partições com data do dia anterior e do dia atual, o status da transferência de dados mostrará IN_PROGRESS considerando eventos que podem chegar atrasados.

Execute o script novamente em cenários em que a migração de dados não foi concluída com êxito ou em que o status de migração de dados para partições ainda indique IN_PROGRESS. Quando você executa novamente o script, ele primeiro verifica o arquivo de status para entender as partições que já foram migradas e continua a migrar apenas as restantes. O script mantém os logs no diretório `/var/opt/novell/sentinel/log/data_uploader.log` para fins de solução de problemas.

VII

Implantando o Sentinel para alta disponibilidade

Esta seção fornece informações sobre como instalar o Sentinel em um modo de alta disponibilidade ativo-passivo, o qual permite que o Sentinel faça o failover em um nó de cluster redundante, em caso de falha de hardware ou software. [Para obter mais informações sobre a implementação de alta disponibilidade e recuperação de desastre em seu ambiente Sentinel, entre em contato com o suporte técnico](#).

Observação: A configuração de Alta Disponibilidade (HA) tem suporte apenas no servidor do Sentinel. No entanto, as instâncias do Collector Manager e do Correlation Engine ainda podem se comunicar com o servidor de Alta Disponibilidade do Sentinel.

- ♦ [Capítulo 35, “Conceitos” na página 187](#)
- ♦ [Capítulo 36, “Requisitos do Sistema” na página 189](#)
- ♦ [Capítulo 37, “Instalação e configuração” na página 191](#)
- ♦ [Capítulo 38, “Configurando o Sentinel de HA como SSDM” na página 209](#)
- ♦ [Capítulo 39, “Fazendo o upgrade do Sentinel em alta disponibilidade” na página 211](#)
- ♦ [Capítulo 40, “Backup e recuperação” na página 219](#)

35 Conceitos

A alta disponibilidade se refere a uma metodologia de design que se destina a manter um sistema disponível para uso enquanto for prático. A intenção é minimizar as causas de tempo de espera, como falhas e manutenção do sistema, e minimizar o tempo que demorará para detectar e recuperar de eventos de tempo de espera ocorridos. Na prática, os meios automatizados de detecção e recuperação de eventos de tempo de espera tornam-se rapidamente necessários à medida que níveis mais altos de disponibilidade devem ser obtidos.

Para obter mais informações sobre a alta disponibilidade, consulte o [Guia de Alta Disponibilidade de SUSE](#).

- ♦ “Sistemas externos” na página 187
- ♦ “Armazenamento compartilhado” na página 187
- ♦ “Monitoramento do serviço” na página 188
- ♦ “Fencing” na página 188

Sistemas externos

O Sentinel é um aplicativo multicamadas complexo que depende de (e fornece) uma ampla variedade de serviços. Adicionalmente, ele se integra com vários sistemas de terceiros externos para coleção de dados, compartilhamento de dados e remediação de incidentes. A maioria das soluções de HA permite que os implementadores declarem as dependências entre os serviços que devem estar altamente disponíveis, mas isso se aplica apenas a serviços em execução no próprio cluster. Sistemas externos ao Sentinel, por exemplo, fontes de evento, devem ser configurados separadamente para estarem tão disponíveis quanto a organização necessita, e também devem ser configurados adequadamente para manipular situações quando o Sentinel estiver indisponível por algum período de tempo, como um evento de failover. Se os direitos de acesso estiverem firmemente restritos, por exemplo, se sessões autenticadas forem usadas para enviar e/ou receber dados entre o sistema de terceiros e o Sentinel, o sistema de terceiros deverá ser configurado para aceitar sessões de origem ou iniciar sessões para qualquer nó de cluster (o Sentinel deverá ser configurado com um endereço IP virtual para esse fim).

Armazenamento compartilhado

Todos os clusters de HA requerem algum formulário de armazenamento compartilhado de modo que os dados de aplicativo possam ser rapidamente movidos de um nó do cluster para outro, no caso de uma falha do nó de origem. O próprio armazenamento deve estar altamente disponível; isso é normalmente obtido usando a tecnologia SAN (Storage Area Network) conectada aos nós do cluster que usam uma rede Fibre Channel. Outros sistemas usam NAS (Network Attached Storage), iSCSI ou outras tecnologias que levam em conta a montagem remota do armazenamento compartilhado. O requisito fundamental do armazenamento compartilhado é que o cluster possa mover de forma limpa o armazenamento de um nó do cluster com falha para um novo nó do cluster.

Há duas abordagens básicas que o Sentinel pode usar para o armazenamento compartilhado. O primeiro localiza todos os componentes (binários de aplicativo, configuração e dados de evento) no armazenamento compartilhado. No failover, o armazenamento é desmontado do nó primário e movido para o nó de backup, que carrega o aplicativo inteiro e a configuração do armazenamento

compartilhado. A segunda abordagem armazena os dados do evento no armazenamento compartilhado, mas os binários de aplicativo e a configuração residem em cada nó do cluster. No failover, apenas os dados de evento são movidos para o nó de backup.

Cada abordagem tem benefícios e desvantagens, mas a segunda abordagem permite que a instalação do Sentinel use caminhos de instalação compatíveis com o FHS padrão, leve em consideração a verificação do pacote RPM, além do patch a quente e reconfiguração para minimizar o tempo de espera.

Essa solução lhe conduzirá por um exemplo de processo de instalação para um cluster que usa o armazenamento compartilhado iSCSI e localiza os binários de aplicativo/configuração em cada nó do cluster.

Monitoramento do serviço

Um componente principal de qualquer ambiente altamente disponível é um modo confiável e consistente de monitorar os recursos que devem ser altamente disponíveis, junto com quaisquer recursos dos quais sejam dependentes. O SLE HAE usa um componente chamado Agente de Recurso para executar esse monitoramento - o trabalho do Agente de Recurso deve fornecer o status de cada recurso, além de (quando perguntado) iniciar ou parar o recurso.

Os Agentes de Recurso devem fornecer um status confiável para recursos monitorados para prevenir tempo de espera desnecessário. Falsos positivos (quando um recurso é considerado como tendo falhado, mas pode, na verdade, recuperar-se por conta própria) podem causar a migração do serviço (e tempo de espera relacionado), quando não são, de fato, necessários; e falsos negativos (quando o Agente de Recurso reporta que um recurso está funcionando mas, na verdade, ele não está funcionando corretamente) podem impedir o uso adequado do serviço. Por outro lado, o monitoramento externo de um serviço pode ser um tanto difícil - uma porta de serviço da web pode responder a um simples ping, por exemplo, mas pode não fornecer dados corretos quando uma consulta real é emitida. Em muitos casos, a funcionalidade de autoteste deve estar integrada no próprio serviço para fornecer uma mediação verdadeiramente precisa.

Essa solução fornece um Agente de Recurso OCF para Sentinel que pode monitorar uma falha principal do hardware, sistema operacional ou sistema do Sentinel. A essa altura, os recursos de monitoramento externos do Sentinel estão baseados nas investigações de porta IP, e há algum potencial para leituras de falso positivo e falso negativo. Planejamos melhorar o Sentinel e o Agente de Recurso com o decorrer do tempo para aprimorar a precisão desse componente.

Fencing

Dentro de um cluster de alta disponibilidade, os serviços críticos são constantemente monitorados e reiniciados automaticamente em outros nós, no caso de falha. Essa automação pode introduzir problemas, no entanto, se ocorrer algum problema de comunicação com o nó primário, embora o serviço em execução nesse nó pareça estar inativo, na verdade, ele continua a executar e gravar dados no armazenamento compartilhado. Nesse caso, iniciar um novo conjunto de serviços em um nó de backup pode facilmente causar corrupção de dados.

Os clusters usam uma variedade de técnicas, coletivamente chamadas de fencing, para prevenir que isso aconteça, incluindo SBD (Detecção de split brain) e STONITH (Atirar na cabeça do outro nó). O primeiro objetivo é prevenir a corrupção de dados no armazenamento compartilhado.

36 Requisitos do Sistema

Ao alocar recursos de cluster para suportar uma instalação de alta disponibilidade (HA), considere os seguintes requisitos:

- ☐ (Condicional) Para instalações de aplicação de HA, verifique se a aplicação de HA do Sentinel está disponível com uma licença válida. A aplicação de HA do Sentinel é uma aplicação ISO que inclui os seguintes pacotes:
 - ♦ Sistema operacional: SLES 12 SP3
 - ♦ Pacote SLES HAE (SLES High Availability Extension)
 - ♦ Software Sentinel (incluindo RPM HA)
- ☐ (Condicional) Para instalações tradicionais de HA, verifique se os seguintes itens estão disponíveis:
 - ♦ Sistema operacional: SLES 11 SP4 ou SLES 12 SP1 ou posterior
 - ♦ Imagem ISO com licenças válidas do SLES HAE
 - ♦ Instalador do Sentinel (arquivo TAR)
- ☐ (Condicional) Se você estiver usando o sistema operacional SLES com a versão do kernel 3.0.101 ou posterior, será necessário carregar manualmente o driver de watchdog no computador. Para localizar o driver do watchdog adequado para o hardware do seu computador, entre em contato com o fornecedor do hardware. Para carregar o driver do watchdog, execute as etapas a seguir:
 1. No prompt de comandos, execute o seguinte comando para carregar o driver do watchdog na sessão atual:

```
/sbin/modprobe -v --ignore-install <watchdog driver name>
```
 2. No arquivo `/etc/init.d/boot.local`, adicione a seguinte linha para garantir que o computador carregue automaticamente o driver de watchdog em cada tempo de inicialização:

```
/sbin/modprobe -v --ignore-install <watchdog driver name>
```
- ☐ Verifique se cada nó do cluster que hospeda os serviços do Sentinel atende aos requisitos especificados no [Capítulo 5, “Atendendo aos requisitos do sistema” na página 37](#).
- ☐ Verifique se está disponível armazenamento compartilhado suficiente para os dados e aplicativo do Sentinel.
- ☐ Certifique-se de usar um endereço IP virtual dos serviços que podem ser migrados de nó a nó no failover.
- ☐ Verifique se seu dispositivo de armazenamento compartilhado atende aos requisitos de desempenho e às características de tamanho especificados no [Capítulo 5, “Atendendo aos requisitos do sistema” na página 37](#). Use uma máquina virtual SLES padrão configurada com destinos iSCSI como armazenamento compartilhado.

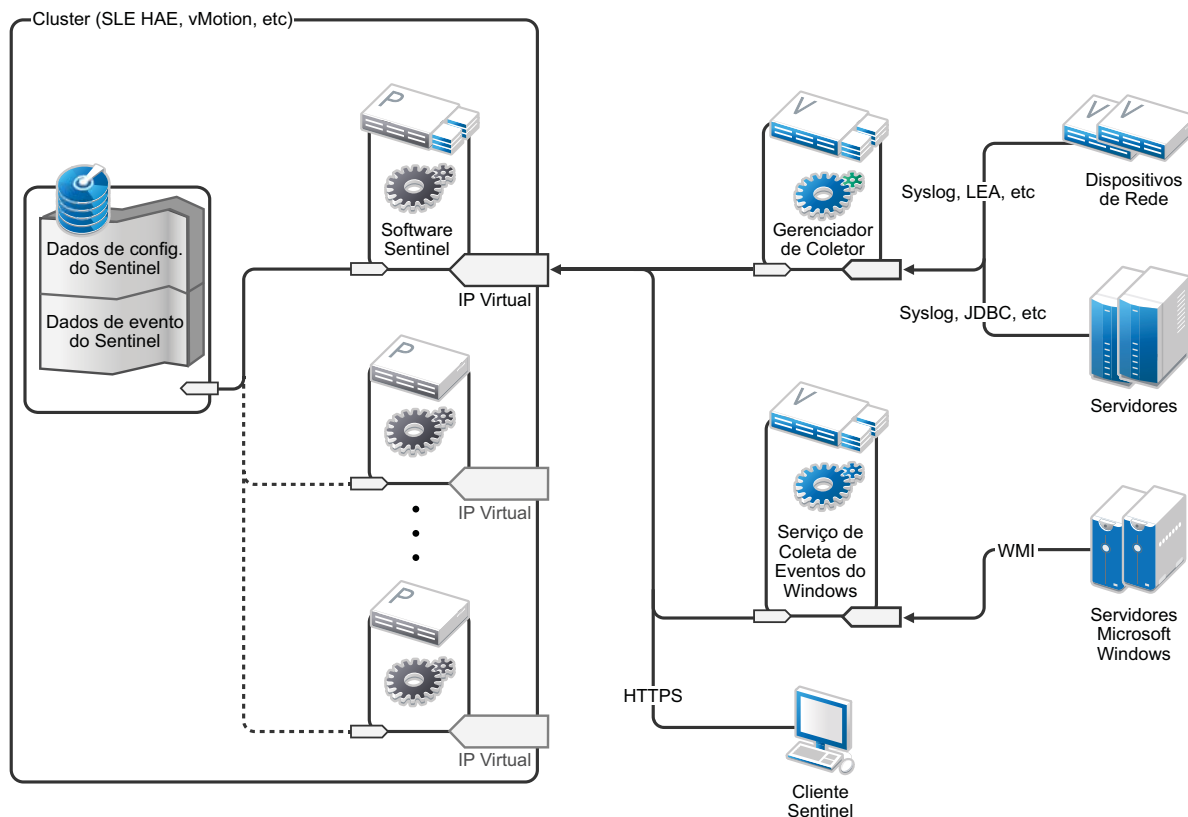
Para iSCSI, você precisa usar a maior Unidade de transferência de mensagem (MTU) suportada pelo hardware. MTUs maiores oferecem benefícios ao desempenho do armazenamento. O Sentinel pode apresentar problemas se a latência e a largura de banda para o armazenamento for mais lenta do que o recomendado.

- ☐ Verifique se há um mínimo de dois nós de cluster que atendem aos requisitos dos recursos para a execução do Sentinel no ambiente do cliente. Duas máquinas virtuais do SLES são recomendadas.
- ☐ Verifique se foi criado um método para que os nós do cluster se comuniquem com o armazenamento compartilhado, como o FibreChannel para uma SAN (Storage area network). Use um endereço IP dedicado para se conectar ao Destino iSCSI.
- ☐ Verifique se há um endereço IP virtual que pode ser migrado de um nó para outro em um cluster para servir como endereço IP externo do Sentinel.
- ☐ Verifique se há pelo menos um endereço IP por nó do cluster para comunicações internas do cluster. É possível usar um endereço IP simples de difusão ponto a ponto, mas o multicast é preferido para ambientes de produção.

37 Instalação e configuração

Esta seção fornece as etapas para instalação e configuração do Sentinel em um ambiente de alta disponibilidade (HA).

O diagrama a seguir representa uma arquitetura de HA ativo-passiva.



- ♦ “Configuração inicial” na página 192
- ♦ “Configuração de armazenamento compartilhado” na página 193
- ♦ “Instalação do Sentinel” na página 197
- ♦ “Instalação do cluster” na página 200
- ♦ “Configuração do Cluster” na página 201
- ♦ “Configuração do recurso” na página 204
- ♦ “Configuração do armazenamento secundário” na página 206

Configuração inicial

Configure o hardware do computador, hardware de rede, hardware de armazenamento, sistemas operacionais, contas de usuário e outros recursos básicos do sistema pelos requisitos documentados para o Sentinel e os requisitos do cliente local. Teste os sistemas para assegurar a função e estabilidade adequadas.

Use a seguinte lista de verificação para guiá-lo pela instalação e configuração inicial.

	Itens da Lista de verificação
<input type="checkbox"/>	As características de CPU, RAM e espaço em disco de cada nó do cluster devem satisfazer aos requisitos do sistema definidos no Capítulo 5, “Atendendo aos requisitos do sistema” na página 37 com base na taxa de eventos esperada.
<input type="checkbox"/>	As características de espaço em disco e E/S dos nós de armazenamento devem satisfazer aos requisitos do sistema definidos no Capítulo 5, “Atendendo aos requisitos do sistema” na página 37 com base na taxa de eventos esperada e nas políticas de retenção de dados para armazenamento primário e/ou secundário.
<input type="checkbox"/>	Para configurar os firewalls do sistema operacional de modo a restringir o acesso ao Sentinel e ao cluster, consulte o Capítulo 8, “Portas usadas” na página 63 para obter detalhes de quais portas devem estar disponíveis dependendo da configuração local e das origens que enviarão dados de evento.
<input type="checkbox"/>	Verifique se todos os nós do cluster são sincronizados em tempo. Use o NTP ou uma tecnologia semelhante para este propósito.
<input type="checkbox"/>	<ul style="list-style-type: none">♦ O cluster requer uma resolução do nome de host confiável. Digite todos os nomes do host de cluster internos no arquivo <code>/etc/hosts</code> para garantir a continuidade do cluster em caso de falha do DNS.♦ Verifique se não foi atribuído um nome de host a um endereço IP de loopback.♦ Ao configurar o nome de host e o nome de domínio durante a instalação do sistema operacional, anule a seleção Atribuir Nome de Host ao IP de Loopback.

Você pode usar a seguinte configuração:

- ♦ (Condicional) Para instalações de HA tradicionais:
 - ♦ Duas VMS de nós de cluster executando SLES 11 SP4, SLES 12 SP1 ou posterior.
 - ♦ (Condicional) Instale o Windows X se precisar de configuração GUI. Defina os scripts de inicialização para iniciar sem o X (nível de execução 3), para que você possa iniciá-los somente quando necessário.
- ♦ (Condicional) Para instalações de aplicações de HA: duas máquinas virtuais de nós de cluster com base em aplicações HA ISO. Para obter informações sobre a instalação da aplicação da ISO de HA, consulte a [“Instalando o Sentinel” na página 102](#).
- ♦ Os nós terão um NIC para acesso externo e um para comunicações iSCSI.
- ♦ Configure os NICs externos com os endereços IP que permitem acesso remoto por meio de SSH ou similar. Para este exemplo, utilizaremos 172.16.0.1 (node01 [nó 1]) e 172.16.0.2 (node02 [nó 2]).
- ♦ Cada nó deve ter disco suficiente para o sistema operacional, binários e dados de configuração do Sentinel, software do cluster, espaço temporário e assim por diante. Consulte os requisitos dos sistemas SLES e SLES HAE e do aplicativo do Sentinel.

- ♦ Uma máquina virtual executando SLES 11 SP4 ou SLES 12 SP1 ou posterior que está configurada com Destinos iSCSI para armazenamento compartilhado
 - ♦ (Condicional) Instale o Windows X se precisar de configuração GUI. Defina os scripts de inicialização para iniciar sem o X (nível de execução 3), para que você possa iniciá-los somente quando necessário.
 - ♦ O sistema terá dois NICs: um para acesso externo e um para comunicações iSCSI.
 - ♦ Configure o NIC externo com um endereço IP que permite acesso remoto por meio do SSH ou similar. Por exemplo, 172.16.0.3 (storage03).
 - ♦ O sistema deve ter espaço suficiente para o sistema operacional, espaço temporário, um grande volume de armazenamento compartilhado para manter os dados do Sentinel, e uma quantidade de espaço pequena para uma partição SBD. Consulte os requisitos do sistema SLES e do armazenamento de dados de evento do Sentinel.

Observação: Em um cluster de produção, é possível usar endereços IPs não roteáveis em NICs separados (possivelmente um par, para redundância) para comunicações internas do cluster.

Configuração de armazenamento compartilhado

Configure o armazenamento compartilhado e verifique se pode montá-lo em cada nó do cluster. Se você estiver usando o FibreChannel e uma SAN (Storage area network), pode ser necessário fornecer conexões físicas, bem como configuração adicional. O Sentinel usa esse armazenamento compartilhado para armazenar os bancos de dados e os dados do evento. Verifique se o armazenamento compartilhado está em conformidade com o tamanho apropriado com base nas políticas de retenção de dados e nas taxas de evento esperadas.

Considere o exemplo seguinte de uma configuração de armazenamento compartilhado:

Uma implementação típica pode usar uma SAN (Storage area network) rápida conectada via Fibre Channel a todos os nós do cluster, com uma matriz RAID grande para armazenar os dados de evento locais. Um nó NAS ou iSCSI separado pode ser usado pelo armazenamento secundário mais lento. Contudo que o nó do cluster possa montar o armazenamento primário como um dispositivo de blocos normal, ele pode ser usado pela solução. O armazenamento secundário também pode ser montado como um dispositivo de bloco ou pode ser um volume NFS ou CIFS.

Observação: Configure seu armazenamento compartilhado e teste a montagem em cada nó do cluster. No entanto, a configuração do cluster lidará com a montagem real do armazenamento.

Realize o seguinte procedimento para criar Destinos iSCSI hospedados em uma máquina virtual SLES:

- 1 Conecte-se ao `storage03`, a máquina virtual que você criou durante [Configuração inicial](#) e inicie uma sessão de console.
- 2 Execute o comando a seguir para criar um arquivo em branco de qualquer tamanho desejado para o armazenamento primário do Sentinel:

```
dd if=/dev/zero of=/localdata count=<tamanho do arquivo> bs=<tamanho de bit>
```

Por exemplo, execute o comando a seguir para criar um arquivo de 20 GB preenchido com zeros copiado do pseudodispositivo `/dev/zero`:

```
dd if=/dev/zero of=/localdata count=20480000 bs=1024
```

- 3 Repita as etapas 1 e 2 para criar um arquivo para o armazenamento secundário da mesma forma.

Por exemplo, execute o comando a seguir para o armazenamento secundário:

```
dd if=/dev/zero of=/networkdata count=20480000 bs=1024
```

Observação: Para este exemplo, você criou dois arquivos com as mesmas características de tamanho e desempenho para representar os dois discos. Para uma implantação de produção, crie o armazenamento primário em uma SAN (Storage area network) rápida e o armazenamento secundário em um volume iSCSI, NFS ou CIFS mais lento.

Execute as etapas apresentadas nas seções a seguir para configurar dispositivos iniciadores e de destino iSCSI:

- ♦ “Configurando destinos iSCSI” na página 194
- ♦ “Configurando iniciadores iSCSI” na página 196

Configurando destinos iSCSI

Realize o seguinte procedimento para configurar arquivos `localdata` e `networkdata` como Destinos iSCSI.

Para obter mais informações sobre como configurar destinos iSCSI, consulte [Creating iSCSI Targets with YaST](#) (Criando destinos iSCSI com o YaST) na documentação do SUSE.

- 1 Execute o YaST da linha de comandos (ou use a interface gráfica do usuário, se preferir):
`sbin/yast`
- 2 Selecione **Network Devices** (Dispositivos de Rede) > **Network Settings** (Configurações de Rede).
- 3 Certifique-se de que a guia **Overview** (Visão Geral) seja selecionada.
- 4 Selecione o NIC secundário na lista exibida, em seguida, pressione Tab e avance até Editar e pressione Enter
- 5 Na guia **Endereço**, atribua um endereço IP estático de 10.0.0.3. Esse será o endereço IP interno das comunicações iSCSI.
- 6 Clique em **Next** (Próximo) e, em seguida, clique em **OK**.
- 7 (Condicional) Na tela principal:
 - ♦ Se você estiver usando SLES 11 SP4, selecione **Serviços de Rede** > **Destino iSCSI**.
 - ♦ Se você estiver usando SLES 12 SP1 ou posterior, selecione **Serviços de Rede** > **Destino iSCSI LIO**.

Observação: Se não localizar essa opção, vá até **Software** > **Gerenciamento de Software** > **Servidor iSCSI LIO** e instale o pacote iSCSI LIO.

- 8 (Condicional) Se solicitado, instale o software necessário:
 - ♦ Para SLES 11 SP4: `iscsitarget RPM`
 - ♦ Para SLES 12 SP1 ou posterior: `iscsiliotarget RPM`
- 9 (Condicional) Se você estiver usando o SLES 12 SP1 ou posterior, execute as etapas a seguir em todos os nós do cluster:
 - 9a Execute o comando a seguir para abrir o arquivo que contém o nome do iniciador iSCSI:
`cat /etc/iscsi/initiatorname.iscsi`
 - 9b Observe o nome do iniciador que será usado para configurar os iniciadores iSCSI:

Por exemplo:

```
InitiatorName=iqn.1996-04.de.suse:01:441d6988994
```

Esses nomes de iniciador serão usados ao definir a Configuração de cliente do destino iSCSI.

- 10 Clique em **Service** (Serviço), selecione a opção **When Booting** (Ao Inicializar) para assegurar que o serviço inicie na inicialização do sistema operacional.
- 11 Selecione a guia **Global**, anule a seleção **Nenhuma Autenticação** para habilitar autenticações e, então, especifique as credenciais necessárias para autenticações recebidas e enviadas.
A opção **Nenhuma Autenticação** é habilitada por padrão. No entanto, você deve habilitar a autenticação para verificar se a configuração é segura.
- 12 Clique em **Targets** (Destinos) e **Add** (Adicionar) para incluir um novo destino.
O Destino iSCSI gerará automaticamente um ID e apresentará uma lista vazia de LUNs (unidades) que estão disponíveis.
- 13 Clique em **Add** (Adicionar) para incluir uma nova LUN.
- 14 Deixe o número de LUN como 0 e navegue na caixa de diálogo **Path** (Caminho) (debaixo de Type=fileio) e selecione o arquivo `/localdata` que você criou. Se você tiver um disco dedicado para armazenamento, especifique um dispositivo de blocos como `/dev/sdc`.
- 15 Repita as etapas 13 e 14, adicione LUN 1 e selecione `/networkdata` desta vez.
- 16 (Condicional) Se você estiver usando o SLES 11 SP4, execute as etapas a seguir:
 - 16a Deixe as outras opções com as configurações padrão, clique em **OK** e depois em **Próximo**.
 - 16b (Condicional) Caso tenha habilitado a autenticação na Etapa 11, forneça as credenciais de autenticação.
Selecione um cliente, selecione **Edit Auth (Editar Autenticação) > Incoming Authentication (Autenticação Recebida)** e especifique o nome de usuário e a senha.
- 17 (Condicional) Se você estiver usando o SLES 12 SP1 ou posterior, execute as etapas a seguir:
 - 17a Deixe as outras opções com as configurações padrão e clique em **Próximo**.
 - 17b Clique em **Adicionar**. Quando o Nome do Cliente for solicitado, especifique o nome do iniciador que você copiou na Etapa 9. Repita essa etapa para adicionar todos os nomes dos clientes ao especificar os nomes dos iniciadores.
A lista de nomes de clientes será exibida na Lista de Clientes.
 - 17c (Condicional) Caso tenha habilitado a autenticação na Etapa 11, forneça as credenciais de autenticação.
Selecione um cliente, selecione **Edit Auth (Editar Autenticação) > Incoming Authentication (Autenticação Recebida)** e especifique o nome de usuário e a senha. Repita isso para todos os clientes.
- 18 Clique em **Next** (Próximo) novamente para selecionar as opções de autenticação padrão, e em **Finish** (Terminar) para sair da configuração. Aceite, caso seja solicitado, reiniciar o iSCSI.
- 19 Saia do YaST.

Observação: Esse procedimento expõe dois Destinos iSCSI no servidor no endereço IP 10.0.0.3. Em cada nó do cluster, verifique se é possível montar o dispositivo de armazenamento dos dados locais compartilhados.

Configurando iniciadores iSCSI

Realize o seguinte procedimento para formatar os dispositivos do iniciador iSCSI.

Para obter mais informações sobre como configurar os iniciadores iSCSI, consulte [Configuring the iSCSI Initiator](#) (Configurando o iniciador iSCSI) na documentação do SUSE.

- 1 Conecte-se a um dos nós do cluster (node01) e inicie o YaST.
- 2 Selecione **Network Devices** (Dispositivos de Rede) > **Network Settings** (Configurações de Rede).
- 3 Certifique-se de que a guia **Overview** (Visão Geral) seja selecionada.
- 4 Selecione o NIC secundário na lista exibida, em seguida, pressione Tab e avance até Editar e pressione Enter
- 5 Clique em **Endereço**, atribua um endereço IP estático de 10.0.0.1. Esse será o endereço IP interno das comunicações do iSCSI.
- 6 Selecione **Next** (Próximo) e, em seguida, clique em **OK**.
- 7 Clique em **Network Services** (Serviços de Rede) > **iSCSI Initiator** (Iniciador iSCSI).
- 8 Se solicitado, instale o software necessário (RPM `iscsiclient`).
- 9 Clique em **Service** (Serviço), selecione **When Booting** (Ao Inicializar) para assegurar que o serviço iSCSI seja iniciado na inicialização.
- 10 Clique em **Discovered Targets** (Destinos Detectados) e selecione **Discovery** (Descoberta).
- 11 Especifique o endereço IP do Destino iSCSI (10.0.0.3).
(Condicional) Caso tenha habilitado a autenticação na Etapa 11 em “[Configurando destinos iSCSI](#)” na página 194, anule a seleção **Nenhuma Autenticação**. No campo **Autenticação Enviada**, digite o nome de usuário e a senha que você especificou durante a configuração de destino iSCSI.
Clique em **Avançar**.
- 12 Selecione o Destino iSCSI descoberto com o endereço IP 10.0.0.3 e selecione **Log In** (Efetuar Login).
- 13 Execute estas etapas:
 - 13a Alterne para Automático no menu suspenso de **Inicialização**.
 - 13b (Condicional) Caso tenha habilitado a autenticação, anule a seleção **Nenhuma Autenticação**.
O nome de usuário e a senha que você especificou na Etapa 11 deverão ser exibidos na seção **Autenticação Enviada**. Se essas credenciais não forem exibidas, digite as credenciais nesta seção.
 - 13c Clique em **Avançar**.
- 14 Alterne para a guia **Connected Targets** (Destinos Conectados) para assegurar que estejamos conectados ao destino.
- 15 Saia da configuração. Esse deve ter sido montado nos Destinos iSCSI como dispositivos de bloco no nó do cluster.
- 16 No menu principal do YaST, selecione **System** (Sistema) > **Partitioner** (Particionador).
- 17 Na Tela do sistema, você deverá ver novos discos rígidos dos seguintes tipos (como `/dev/sdb` e `/dev/sdc`) na lista:
 - ♦ No SLES 11 SP4: IET-VIRTUAL-DISK
 - ♦ No SLES 12 SP1 ou posterior: LIO-ORG-FILEIO

Pressione Tab para o primeiro item na lista (que deve ser o armazenamento primário), selecione o disco e pressione Enter.

- 18 Selecione **Add** (Adicionar) para incluir uma nova partição para o disco vazio. Formate o disco como uma partição primária, mas não a monte. Verifique se a opção **Não montar partição** está selecionada.
- 19 Selecione **Próximo** e **Terminar** após revisar as mudanças que serão feitas.
O disco formatado (como `/dev/sdb1`) deve estar pronto agora. É referido como `/dev/<SHARED1>` nas seguintes etapas desse procedimento.
- 20 Vá novamente para o **Particionador** e repita o processo de particionamento/formatação (etapas 16 a 19) para `/dev/sdc` ou qualquer dispositivo de blocos correspondente ao armazenamento secundário. Isso resultará em uma partição `/dev/sdc1` ou disco formatado similar (chamado como `/dev/<REDE1>` abaixo).
- 21 Saia do YaST.
- 22 (Condicional) Se estiver efetuando uma instalação de HA tradicional, crie um ponto de montagem e teste a montagem da partição local conforme mostrado a seguir (o nome exato do dispositivo pode depender da implementação específica):

```
# mkdir /var/opt/novell  
# mount /dev/<SHARED1> /var/opt/novell
```

Você deve ser capaz de criar arquivos na nova partição e ver os arquivos onde quer que a partição seja montada.
- 23 (Condicional) Se estiver efetuando uma instalação de HA tradicional, para efetuar a desmontagem:

```
# umount /var/opt/novell
```
- 24 (Condicional) Para instalações de aplicações de HA, repita as etapas de 1 a 15 para garantir que cada nó do cluster possa montar o armazenamento compartilhado local. Substitua o endereço IP do nó na etapa 5 com um endereço IP diferente para cada nó do cluster.
- 25 (Condicional) Para as instalações tradicionais de HA, repita as etapas de 1 a 15, 22 e 23 para garantir que cada nó do cluster possa montar o armazenamento compartilhado local. Substitua o endereço IP do nó na etapa 6 com um endereço IP diferente para cada nó do cluster.

Instalação do Sentinel

Há duas opções para instalar o Sentinel: instalar cada parte do Sentinel no armazenamento compartilhado usando a opção `--location` para redirecionar a instalação do Sentinel para o local em que você montou o armazenamento compartilhado ou instalar apenas os dados do aplicativo variáveis no armazenamento compartilhado.

Instale o Sentinel em cada nó do cluster que possa hospedá-lo. Depois de instalar o Sentinel pela primeira vez, você deve executar uma instalação completa, incluindo os binários do aplicativo, configuração e todos os armazenamentos de dados. Para instalações subsequentes nos outros nós do cluster, você instalará somente o aplicativo. Os dados do Sentinel estarão disponíveis após a montagem do armazenamento compartilhado.

Instalação no primeiro nó

- ♦ [“Instalação de HA tradicional” na página 198](#)
- ♦ [“Instalação da aplicação de HA do Sentinel” na página 198](#)

Instalação de HA tradicional

- 1 Conecte a um dos nós do cluster (node01) e abra uma janela de console.
- 2 Faça o download do instalador do Sentinel (um arquivo tar.gz) e o armazene em /tmp no nó do cluster.
- 3 Execute as etapas a seguir para iniciar a instalação:
 - 3a Execute os seguintes comandos:

```
mount /dev/<SHARED1> /var/opt/novell
cd /tmp
tar -xvzf sentinel_server*.tar.gz
cd sentinel_server*
./install-sentinel --record-unattended=/tmp/install.props
```
 - 3b Especifique 2 para selecionar a configuração personalizada quando solicitado a selecionar o método de configuração.
- 4 Execute a instalação, configurando o produto conforme apropriado.
- 5 Inicie o Sentinel e teste as funções básicas. Você pode usar o endereço IP do nó do cluster externo padrão para acessar o produto.
- 6 Encerre o Sentinel e desmonte o armazenamento compartilhado usando os seguintes comandos:

```
rcsentinel stop
```

```
umount /var/opt/novell
```

Esta etapa remove os scripts de autoinicialização de modo que o cluster possa gerenciar o produto.

```
cd /
```

```
insserv -r sentinel
```

Instalação da aplicação de HA do Sentinel

A aplicação de HA do Sentinel inclui o software Sentinel que já está instalado e configurado. Para configurar o software Sentinel para HA, execute as etapas a seguir:

- 1 Conecte a um dos nós do cluster (node01) e abra uma janela de console.
- 2 Navegue até o seguinte diretório:

```
cd /opt/novell/sentinel/setup
```

- 3 Registre a configuração:

- 3a Execute o seguinte comando:

```
./configure.sh --record-unattended=/tmp/install.props --no-start
```

Esta etapa grava a configuração no arquivo `install.props`, que é necessário para configurar os recursos do cluster usando o script `install-resources.sh`.

- 3b Especifique 2 para selecionar a configuração personalizada quando solicitado a selecionar o método de configuração.
 - 3c Quando a senha for solicitada, especifique 2 para digitar uma nova senha.
Se você especificar 1, o arquivo `install.props` não armazenará a senha.

- 4 Encerre o Sentinel usando o seguinte comando:

```
rcsentinel stop
```

Esta etapa remove os scripts de autoinicialização de modo que o cluster possa gerenciar o produto.

```
insserv -r sentinel
```

- 5 Mova a pasta de dados do Sentinel para o armazenamento compartilhado usando os comandos a seguir. Essa movimentação permite que os nós usem a pasta de dados do Sentinel por meio de um armazenamento compartilhado.

```
mkdir -p /tmp/new
```

```
mount /dev/<SHARED1> /tmp/new
```

```
mv /var/opt/novell/* /tmp/new
```

```
umount /tmp/new/
```

- 6 Verifique a movimentação da pasta de dados do Sentinel para o armazenamento compartilhado usando os seguintes comandos:

```
mount /dev/<SHARED1> /var/opt/novell/
```

```
umount /var/opt/novell/
```

Instalação do nó subsequente

- ♦ [“Instalação de HA tradicional” na página 199](#)
- ♦ [“Instalação da aplicação de HA do Sentinel” na página 200](#)

Repita a instalação em outros nós:

O instalador inicial do Sentinel cria uma conta do usuário para ser usada pelo produto, que usa o próximo ID de usuário disponível no momento da instalação. As instalações subsequentes no modo autônomo tentarão usar o mesmo ID de usuário para criação da conta, mas não existe a possibilidade de conflitos (se os nós do cluster não forem idênticos no momento da instalação). É altamente recomendado que você execute um dos seguintes procedimentos:

- ♦ Sincronize o banco de dados da conta do usuário entre nós do cluster (manualmente via LDAP ou similar), assegurando que a sincronização aconteça antes das instalações subsequentes. Neste caso, o instalador detectará a presença da conta do usuário e usará a existente.
- ♦ Assista a saída das instalações autônomas subsequentes - um aviso será emitido se a conta do usuário não puder ser criada com o mesmo ID de usuário.

Instalação de HA tradicional

- 1 Conecte-se a cada nó de cluster adicional (node02) e abra uma janela do console.
- 2 Execute os seguintes comandos:

```
cd /tmp
```

```
scp root@node01:/tmp/sentinel_server*.tar.gz .
```

```
scp root@node01:/tmp/install.props .
```

```
tar -xvzf sentinel_server*.tar.gz
```

```
cd sentinel_server*

./install-sentinel --no-start --cluster-node --unattended=/tmp/install.props

insserv -r sentinel
```

Instalação da aplicação de HA do Sentinel

- 1 Conecte-se a cada nó de cluster adicional (node02) e abra uma janela do console.
- 2 Execute o seguinte comando:

```
insserv -r sentinel
```

- 3 Pare os serviços do Sentinel.

```
rcsentinel stop
```

- 4 Remova o diretório Sentinel.

```
rm -rf /var/opt/novell/*
```

No fim deste processo, o Sentinel deverá estar instalado em todos os nós, mas provavelmente ele não funcionará corretamente em nenhum deles, exceto no primeiro, até que várias chaves sejam sincronizadas, o que acontecerá quando configurarmos os recursos do cluster.

Instalação do cluster

Você deve instalar o software de cluster somente para instalações tradicionais de alta disponibilidade (HA). A aplicação de HA do Sentinel inclui o software de cluster e não requer a instalação manual.

Use o procedimento a seguir para configurar a Extensão de alta disponibilidade do SLES com uma sobreposição de Agentes de recursos específicos do Sentinel:

- 1 Instale o software de cluster em cada nó.
- 2 Registre cada nó de cluster com o gerenciador de cluster.
- 3 Verifique se cada nó de cluster aparece no console de gerenciamento de cluster.

Observação: O Agente de Recurso OCF para Sentinel é um shell script simples que executa uma variedade de verificações para verificar se o Sentinel está funcional. Se não usar o Agente de Recurso OCF para monitorar o Sentinel, você deverá desenvolver uma solução de monitoramento similar para o ambiente do cluster local. Para desenvolver o seu próprio, reveja o Agente de Recursos existentes, armazenado no arquivo `Sentinelha.rpm` no pacote de download do Sentinel.

- 4 Instale o software principal SLE HAE de acordo com a [Documentação do SLE HAE](#). Para obter informações sobre a instalação dos complementos do SLES, veja o [Guia de Implementação](#).
- 5 Repita a etapa 4 em todos os nós do cluster. O complemento instalará o gerenciamento de cluster principal e o software de comunicações, assim como muitos Agentes de Recursos que são usados para monitorar os recursos do cluster.
- 6 Instale um RPM adicional para fornecer os Agentes de Recursos adicionais do cluster específico do Sentinel. O RPM de HA pode ser encontrado no arquivo `novell-Sentinelha-<versão_Sentinel>*.rpm`, armazenado no download padrão do Sentinel, que você descompacta para instalar o produto.
- 7 Em cada nó do cluster, copie o arquivo `novell-Sentinelha-<versão_Sentinel>*.rpm` para o diretório `/tmp`, em seguida, execute os seguintes comandos:

```
cd /tmp  
rpm -i novell-Sentinelha-<Sentinel_version>*.rpm
```

Configuração do Cluster

Você deve configurar o software do cluster para registrar cada nó do cluster como um membro do cluster. Como parte dessa configuração, você também pode configurar proteção e os recursos STONITH (Shoot The Other Node In The Head) para garantir a consistência do cluster.

Importante: Os procedimentos nesta seção usam os comandos `rcopenais` e `openais`, que funcionam somente com o SLES 11 SP4. Para o SLES 12 SP2 e posterior, use o comando `systemctl pacemaker.service`.

Por exemplo, para o comando `/etc/rc.d/openais start`, use o comando `systemctl start pacemaker.service`.

Use o procedimento a seguir para configuração de cluster:

Para esta solução, você deve usar endereços IP particulares para comunicações internas de cluster e usar unicast para minimizar a necessidade de solicitar um endereço multicast usando um administrador de rede. Você também deve usar um Destino iSCSI configurado na mesma máquina virtual SLES que hospeda o armazenamento compartilhado para funcionar como um dispositivo SBD (Split Brain Detector) para fins de proteção.

Configuração do SBD

- 1 Conecte-se ao `storage03` e inicie uma sessão de console. Execute o comando a seguir para criar um arquivo em branco de qualquer tamanho desejado:

```
dd if=/dev/zero of=/sbd count=<tamanho do arquivo> bs=<tamanho de bit>
```

Por exemplo, execute o comando a seguir para criar um arquivo de 1 MB preenchido com zeros copiado do pseudodispositivo `/dev/zero`:

```
dd if=/dev/zero of=/sbd count=1024 bs=1024
```

- 2 Execute o YaST da linha de comando ou da Interface Gráfica do Usuário: `/sbin/yast`
- 3 Selecione **Network Services** (Serviços de Rede) > **iSCSI Target** (Destino iSCSI).
- 4 Clique em **Targets** (Destinos) e selecione o destino existente.
- 5 Selecione **Edit** (Editar). A IU apresentará uma lista de LUNs (unidades) que estão disponíveis.
- 6 Selecione **Add** (Adicionar) para incluir uma nova LUN.
- 7 Deixe o número da LUN como 2. Navegue na caixa de diálogo **Path** (Caminho) e selecione o arquivo `/sbd` que você criou.
- 8 Deixe as outras opções com as configurações padrão e selecione **OK** e **Next** (Próximo) e clique em **Next** (Próximo) novamente para selecionar as opções de autenticação padrão.
- 9 Clique em **Finish** (Terminar) para sair da configuração. Reinicie os serviços, se necessário. Saia do YaST.

Observação: As etapas a seguir requerem que cada nó do cluster possa resolver o nome do host de todos os outros nós do cluster (o serviço de sincronização de arquivo `csync2` falhará se esse não for o caso). Se o DND não estiver configurado ou disponível, adicione entradas para cada host ao

arquivo `/etc/hosts` que lista cada endereço IP em seu nome de host (como relatado pelo comando de nome de host). Além disso, verifique se não foi atribuído um nome de host a um endereço IP de loopback.

Execute as etapas a seguir para expor um Destino iSCSI ao dispositivo SBD no servidor no endereço IP 10.0.0.3 (storage03).

Node Configuration (Configuração do nó)

Conecte a um nó do cluster (node01) e abra um console:

- 1 Execute o YaST.
- 2 Abra **Network Services** (Serviços de Rede) > **iSCSI Initiator** (Iniciador iSCSI).
- 3 Selecione **Connected Targets**(Destinos Conectados) e, em seguida, o iSCSI Target (Destino iSCSI) que você configurou acima.
- 4 Selecione a opção **Log Out** (Efetuar logout) e efetue logout do Destino.
- 5 Alterne para a guia **Destinos Descobertos**, selecione o **Destino** e efetue login novamente para atualizar a lista de dispositivos (deixe a opção de inicialização **automática** e anule a seleção **Nenhuma Autenticação**).
- 6 Selecione **OK** para sair da ferramenta Iniciador iSCSI.
- 7 Abra **System** (Sistema) > **Partitioner** (Particionador) e identifique o dispositivo SBD como o IET-VIRTUAL-DISK de 1 MB. Ele será listado como `/dev/sdd` ou similar - anote qual.
- 8 Saia do YaST.
- 9 Execute o comando `ls -l /dev/disk/by-id/` e anote o ID do dispositivo que está vinculado ao nome do dispositivo localizado acima.
- 10 (Condicional) Execute um dos seguintes comandos:
 - ♦ Se você estiver usando SLES 11 SP4:
`sleha-init`
 - ♦ Se você estiver usando SLES 12 SP1 ou posterior:
`ha-cluster-init`
- 11 Quando solicitado o endereço de rede ao qual vincular, especifique o endereço IP externo do NIC (172.16.0.1).
- 12 Aceite o endereço e a porta padrão do multicast. Nós os anularemos mais tarde.
- 13 Digite `s` para habilitar o SBD e especifique o `/dev/disk/by-id/<id de dispositivo>`, no qual `<id de dispositivo>` é o ID que você localizou acima (é possível usar Tab para preencher automaticamente o caminho).
- 14 (Condicional) Digite `N` quando for solicitado com o seguinte:

`Do you wish to configure an administration IP? [y/N]`

Para configurar um endereço IP de administração, forneça o endereço IP virtual durante **“Configuração do recurso” na página 204**
- 15 Conclua o assistente e certifique-se de que nenhum erro seja informado.
- 16 Inicie o YaST.
- 17 Selecione **High Availability** (Alta Disponibilidade) > **Cluster** (ou apenas Cluster em alguns sistemas).
- 18 Na caixa à esquerda, certifique-se de que **Communication Channels** (Canais de Comunicação) esteja selecionado.

- 19 Pressione Tab até a linha superior da configuração e mude a seleção **udp** para **udpu** (isso desativa o multicast e seleciona o unicast).
- 20 Selecione **Add a Member Address** (Adicionar um Endereço de Membro) e especifique esse nó (172.16.0.1), em seguida, repita e adicione o(s) outro(s) nó(s) do cluster: 172.16.0.2.
- 21 Selecione **Finish** (Terminar) para completar a configuração.
- 22 Saia do YaST.
- 23 Execute o comando de reiniciação `/etc/rc.d/openais` para reiniciar os serviços do cluster com o novo protocolo de sincronização.

Conecte-se a cada nó de cluster adicional (node02) e abra um console:

- 1 Execute o YaST.
- 2 Abra **Network Services** (Serviços de Rede) > **iSCSI Initiator** (Iniciador iSCSI).
- 3 Selecione **Connected Targets** (Destinos Conectados) e, em seguida, o iSCSI Target (Destino iSCSI) que você configurou acima.
- 4 Selecione a opção **Log Out** (Efetuar logout) e efetue logout do Destino.
- 5 Alterne para a guia **Destinos Descobertos**, selecione o **Destino** e efetue login novamente para atualizar a lista de dispositivos (deixe a opção de inicialização **automática** e anule a seleção **Nenhuma Autenticação**).
- 6 Selecione **OK** para sair da ferramenta Iniciador iSCSI.
- 7 (Condicional) Execute um dos seguintes comandos:
 - ♦ Se você estiver usando SLES 11 SP4:


```
sleha-join
```
 - ♦ Se você estiver usando SLES 12 SP1 ou posterior:


```
ha-cluster-join
```
- 8 Insira o endereço IP do primeiro nó do cluster.

(Condicional) Se o cluster não for iniciado corretamente, execute as seguintes etapas:

- 1 Execute o comando `crm status` para verificar se os nós estão unidos. Se os nós não estiverem unidos, reinicie todos os nós no cluster.
- 2 Copie, manualmente, o arquivo `/etc/corosync/corosync.conf` de node01 para node02, ou execute o `csync2 -x -v` em node01, ou defina manualmente o cluster no node02 pelo YaST.
- 3 (Condicional) Se o comando `csync2 -x -v` executado na Etapa 1 falhar ao sincronizar todos os arquivos, realize o procedimento a seguir:
 - 3a Limpe o banco de dados `csync2` no diretório `/var/lib/csync2` em todos os nós.
 - 3b Em todos os nós, atualize o banco de dados do `csync2` para que ele corresponda ao sistema de arquivos sem marcar nada que precise ser sincronizado com outros servidores:


```
csync2 -cIr /
```
 - 3c No nó ativo, execute o seguinte:
 - 3c1 Encontre todas as diferenças entre nós ativos e passivos e marque essas diferenças para sincronização:


```
csync2 -TUXI
```
 - 3c2 Redefina o banco de dados para forçar o nó ativo a anular qualquer conflito:


```
csync2 -fr /
```

3c3 Inicie a sincronização para todos os outros nós:

```
csync2 -xr /
```

3d Em todos os nós, verifique se todos os arquivos estão sincronizados:

```
csync2 -T
```

Este comando listará apenas os arquivos que não estão sincronizados.

4 Execute o seguinte comando em `node02`:

Para SLES 11 SP4:

```
/etc/rc.d/openais start
```

Para SLES 12 SP1 e posterior:

```
systemctl start pacemaker.service
```

(Condicional) Se o serviço `xinetd` não adicionar corretamente o novo serviço `csync2`, o script não funcionará corretamente. O serviço `xinetd` é necessário para que o outro nó possa sincronizar os arquivos de configuração do cluster para este nó. Se você vir erros como `csync2 run failed` (execução de `csync2` com falha), talvez haja um problema.

Para resolver esse problema, execute o comando `kill -HUP `cat /var/run/xinetd.init.pid`` e, em seguida, execute novamente o script `sleha-join`.

5 Execute `crm_mon` em cada nó de cluster para verificar se o cluster está funcionando corretamente. Você também pode usar "hawk", o console da web, para verificar o cluster. O nome de login padrão é `hacluster`, e a senha é `linux`.

(Condicional) Dependendo do seu ambiente, realize as seguintes tarefas para modificar os parâmetros adicionais:

1 Para garantir que todo o cluster não seja parado inesperadamente em caso de falha em um nó único no cluster de dois nós, defina a opção global de cluster `no-quorum-policy` para `ignore`:

```
crm configure property no-quorum-policy=ignore
```

Observação: Se o cluster contiver mais de dois nós, não defina esta opção.

2 Para garantir que o gerenciador de recursos permita que os recursos sejam executados no local e em movimento, defina a opção global de cluster `default-resource-stickiness` como 1:

```
crm configure property default-resource-stickiness=1.
```

Configuração do recurso

Os Agentes de Recursos são fornecidos por padrão com SLE HAE. Se você não quiser usar o SLE HAE, será preciso monitorar esses recursos adicionais usando uma tecnologia alternativa:

- ♦ Um recurso Filesystem (sistema de arquivos) correspondente para o armazenamento compartilhado que o software usa;
- ♦ Um recurso de endereço IP correspondente ao endereço IP virtual pelo qual os serviços serão acessados.
- ♦ O software de banco de dados PostgreSQL que armazena metadados de evento e configuração.

Use o seguinte procedimento para configuração de recursos:

O script `crm` ajuda você na configuração de cluster. O script extrai variáveis de configuração relevantes do arquivo de configuração autônomo gerado como parte da instalação do Sentinel. Se você não gerou o arquivo de configuração ou se deseja mudar a configuração dos recursos, é possível usar o seguinte procedimento para editar o script em conformidade.

- 1 Conecte-se ao nó original no qual você instalou o Sentinel.

Observação: Ele deve ser o nó no qual você executou a instalação completa do Sentinel.

- 2 Edite o script para que ele apareça da seguinte forma, em que `<SHARED1>` é o volume compartilhado criado anteriormente:

```
mount /dev/<SHARED1> /var/opt/novell
cd /usr/lib/ocf/resource.d/novell
./install-resources.sh
```

- 3 (Condicional) Você pode ter problemas com os novos recursos que chegam ao cluster. Se você tiver esse problema, execute o seguinte comando no `node02`:

Para SLES 11 SP4:

```
/etc/rc.d/openais start
```

Para SLES 12 SP1:

```
systemctl start pacemaker.service
```

- 4 O script `install-resources.sh` solicitará alguns valores, isto é, o endereço IP virtual que você deseja que as pessoas usem para acessar o Sentinel e o nome do dispositivo do armazenamento compartilhado e, então, criará automaticamente os recursos do cluster necessários. Observe que o script requer que o volume compartilhado já esteja montado, e também requer que o arquivo de instalação autônomo criado durante a instalação do Sentinel esteja presente (`/tmp/install.props`). Você não precisa executar esse script em nenhum outro nó, exceto no primeiro nó instalado; todos os arquivos de configuração relevantes serão automaticamente sincronizados para os outros nós.
- 5 Se o seu ambiente for diferente da solução recomendada pela , edite o arquivo `resources.cli` (no mesmo diretório) e modifique as definições primitivas lá. Por exemplo, a solução recomendada usa um recurso simples do Sistema de arquivos; você pode desejar usar um recurso CLVM que reconhece mais clusters.
- 6 Após executar o shell script, você poderá emitir um comando de `status crm` e a saída se parecerá com esta:

```
crm status
```

```
Last updated: Thu Jul 26 16:34:34 2012
Last change: Thu Jul 26 16:28:52 2012 by hacluster via crmd on node01
Stack: openais
Current DC: node01 - partition with quorum
Version: 1.1.6-b988976485d15cb702c9307df55512d323831a5e
2 Nodes configured, 2 expected votes
5 Resources configured.
```

```
Online: [ node01, node02 ]
stonith-sbd (stonith:external/sbd): Started node01
Resource Group: sentinelgrp
  sentinelip (ocf::heartbeat:IPaddr2): Started node01
  sentinelfs (ocf::heartbeat:Filesystem): Started node01
  sentineldb (ocf::novell:pgsql): Started node01
  sentinelserver (ocf::novell:sentinel): Started node01
```

- 7 A esta altura, os recursos relevantes do Sentinel devem estar configurados no cluster. Você pode examinar como eles estão configurados e agrupados na ferramenta de gerenciamento do cluster, por exemplo, executando o status do crm.

Configuração do armazenamento secundário

Execute as seguintes etapas para configurar o armazenamento secundário para que Sentinel possa migrar partições de eventos para um armazenamento mais barato:

Observação: Este processo é opcional, e a alta disponibilidade do armazenamento secundário não precisa ser igual à alta disponibilidade que você configurou no resto do sistema. Use qualquer diretório, montado de uma SAN (Storage area network) ou não, NFS ou volume CIFS.

- 1 Na interface principal do Sentinel, na barra de menu superior, clique em **Armazenamento**.
- 2 Selecione **Configuração**.
- 3 Selecione um dos botões de opção no Armazenamento secundário não configurado

Use um Destino iSCSI simples como um local de armazenamento compartilhado de rede com uma configuração muito semelhante à do armazenamento primário. Em seu ambiente de produção, suas tecnologias de armazenamento podem ser diferentes.

Use o procedimento a seguir para configurar o armazenamento secundário a ser usado pelo Sentinel:

Observação: Para o Destino iSCSI, o destino será montado como um diretório para uso como armazenamento secundário. Você deve configurar a montagem como um recurso de sistema de arquivos semelhante ao modo como o sistema de arquivos de armazenamento primário está configurado. Ele não foi configurado automaticamente como parte do script de instalação de recursos uma vez que existem outras variações possíveis.

- 1 Examine as etapas acima para determinar que partição foi criada para ser usada como armazenamento secundário (`/dev/<REDE1>`, ou algo como `/dev/sdc1`). Se necessário, crie um diretório vazio em que a partição possa ser montada (por exemplo, `/var/opt/netdata`).
- 2 Configure o sistema de arquivos de rede como um recurso de cluster: use a interface principal do Sentinel ou execute o comando:

```
crm configure primitive sentinelnetfs ocf::heartbeat:Filesystem params device="/dev/<NETWORK1>" directory="<PATH>" fstype="ext3" op monitor interval=60s
```

em que `/dev/<REDE1>` é a partição que foi criada na seção Configuração do armazenamento compartilhado acima, e `<CAMINHO>` é qualquer diretório local em que ele possa ser montado.

- 3 Adicione o novo recurso ao grupo de recursos gerenciados:

```
crm resource stop sentinelgrp
crm configure delete sentinelgrp
crm configure group sentinelgrp sentinelip sentinelifs sentinelnetfs sentinelldb
sentinelserver
crm resource start sentinelgrp
```

- 4 Você pode se conectar ao nó que hospeda atualmente os recursos (usar `crm status` ou Hawk) e assegurar que o armazenamento secundário esteja devidamente montado (usar o comando `mount`).
- 5 Efetue login na interface principal do Sentinel.
- 6 Selecione **Storage** (Armazenamento) e **Configuration** (Configuração), e selecione **SAN (Storage area network) (locally mounted)** (SAN [localmente montada]) abaixo do armazenamento secundário não configurado.
- 7 Digite o caminho no qual o armazenamento secundário está montado, por exemplo, `/var/opt/netdata`.

Use versões simples dos recursos necessários, como o Agente de Recursos do Sistema de Arquivos simples. Você pode optar por usar mais recursos de cluster sofisticados como cLVM (uma versão de volume lógico do sistema de arquivos), se necessário.

38 Configurando o Sentinel de HA como SSDM

Este capítulo fornece informações sobre como definir a configuração do Sentinel de HA como SSDM. Essas instruções são aplicáveis a instalações tradicionais e instalações de aplicação.

Para definir a configuração do Sentinel de HA como SSDM:

- 1 Instale e configure o armazenamento escalável para o Sentinel. Para obter mais informações, consulte o [Capítulo 13, “Instalando e configurando o armazenamento escalável” na página 87](#).
- 2 Habilite o armazenamento escalável no nó ativo. Para obter mais informações, consulte [“Enabling Scalable Storage Post-Installation”](#) (Habilitando o armazenamento escalável pós-instalação) no [Sentinel Administration Guide](#) (Guia de Administração do NetIQ Sentinel).
- 3 Execute o seguinte comando no nó ativo:

```
csync2 -x -v
```

Isto sincroniza a configuração SSDM com todos os nós passivos.

- 4 (Condicional) Se o comando `csync2 -x -v` executado na Etapa 3 falhar ao sincronizar todos os arquivos, realize as etapas a seguir:

4a Limpe o banco de dados `csync2` (no diretório `/var/lib/csync2`) em todos os nós.

4b Execute o comando a seguir em todos os servidores para atualizar o banco de dados `csync2` para corresponder ao sistema de arquivos, mas sem marcar nada como sincronização necessária com outros servidores:

```
csync2 -cIr /
```

4c Execute o comando a seguir para localizar todas as diferenças entre o servidor oficial e os servidores remotos e, então, marque para sincronização:

```
csync2 -TUXI
```

4d Execute o comando a seguir para redefinir o banco de dados para forçar o servidor atual a ser vencedor em quaisquer conflitos:

```
csync2 -fr /
```

4e Execute o comando a seguir para iniciar a sincronização em todos os outros servidores:

```
csync2 -xr /
```

4f Execute o comando a seguir para verificar se todos os arquivos estão sincronizados:

```
csync2 -T
```

Esse comando não listará nenhum arquivo se a sincronização tiver sido bem-sucedida.

39 Fazendo o upgrade do Sentinel em alta disponibilidade

Ao fazer o upgrade do Sentinel em um ambiente de HA, primeiro faça o upgrade dos nós passivos no cluster e depois do nó ativo.

- ♦ “Pré-requisitos” na página 211
- ♦ “Fazendo upgrade de instalações de HA tradicionais do Sentinel” na página 211
- ♦ “Fazendo upgrade de instalações de aplicação de HA do Sentinel” na página 217

Pré-requisitos

- ♦ Faça o download do instalador mais recente do [site Downloads](#).
- ♦ Se você estiver usando o sistema operacional SLES com a versão do kernel 3.0.101 ou posterior, será necessário carregar manualmente o driver do watchdog no computador. Para localizar o driver do watchdog adequado para o hardware do seu computador, entre em contato com o fornecedor do hardware. Para carregar o driver do watchdog, execute as etapas a seguir:
 1. No prompt de comandos, execute o seguinte comando para carregar o driver do watchdog na sessão atual:

```
/sbin/modprobe -v --ignore-install <nome do driver watchdog>
```
 2. Adicione a seguinte linha ao arquivo `/etc/init.d/boot.local` para assegurar que o computador carregue automaticamente o driver do watchdog sempre que for inicializado:

```
/sbin/modprobe -v --ignore-install <nome do driver watchdog>
```

Fazendo upgrade de instalações de HA tradicionais do Sentinel

Esta seção fornece informações sobre como fazer upgrade de uma instalação tradicional do Sentinel, e também sobre como fazer upgrade do sistema operacional em uma instalação tradicional do Sentinel.

Importante: Os procedimentos nesta seção usam os comandos `rcopenais` e `openais`, que funcionam somente com o SLES 11 SP4. Para o SLES 12 SP2 e posterior, use o comando `systemctl pacemaker.service`.

Por exemplo, para o comando `/etc/rc.d/openais start`, use o comando `systemctl start pacemaker.service`.

- ♦ “Fazendo upgrade do Sentinel de HA” na página 212
- ♦ “Fazendo upgrade do sistema operacional” na página 213

Fazendo upgrade do Sentinel de HA

- 1 Habilite o modo de manutenção no cluster:

```
crm configure property maintenance-mode=true
```

O modo de manutenção ajuda a evitar quaisquer interrupções nos recursos do cluster em execução durante a atualização do Sentinel. É possível executar este comando em qualquer nó de cluster.

- 2 Verifique se o modo de manutenção está ativo:

```
crm status
```

Os recursos do cluster devem aparecer no estado não gerenciado.

- 3 Faça upgrade do nó passivo de cluster:

- 3a Interrompa a pilha do cluster:

```
rcopenais stop
```

A interrupção da pilha do cluster garante que os recursos do cluster permaneçam acessíveis e evita o confinamento dos nós.

- 3b Efetue login como `root` no servidor em que você deseja fazer upgrade do Sentinel.

- 3c Extraia os arquivos de instalação do arquivo tar:

```
tar xfz <nome_arquivo_instalação>
```

- 3d Execute o seguinte comando no diretório em que você extraiu os arquivos de instalação:

```
./install-sentinel --cluster-node
```

- 3e Quando o upgrade for concluído, reinicie a pilha do cluster:

```
rcopenais start
```

Repita [Etapa 3](#) para todos os nós do cluster passivos.

- 3f Remova os scripts de inicialização automática para que o cluster possa gerenciar o produto.

```
cd /
```

```
insserv -r sentinel
```

- 4 Faça upgrade do nó ativo de cluster:

- 4a Faça o backup da sua configuração e, em seguida, crie a exportação ESM.

Para obter mais informações sobre como fazer backup de dados, consulte [“Fazendo backup e restaurando dados”](#) no *Guia de administração do Sentinel*.

- 4b Interrompa a pilha do cluster:

```
rcopenais stop
```

A interrupção da pilha do cluster garante que os recursos do cluster permaneçam acessíveis e evita o confinamento dos nós.

- 4c Efetue login como `root` no servidor em que você deseja fazer upgrade do Sentinel.

- 4d Execute o seguinte comando para extrair os arquivos de instalação do arquivo tar:

```
tar xfz <nome_arquivo_instalação>
```

- 4e Execute o seguinte comando no diretório em que você extraiu os arquivos de instalação:

```
./install-sentinel
```

- 4f Quando o upgrade for concluído, inicie a pilha do cluster:

```
rcopenais start
```


- 4g** Remova os scripts de inicialização automática para que o cluster possa gerenciar o produto.

```
cd /  
insserv -r sentinel
```

- 4h** Execute o seguinte comando para sincronizar quaisquer mudanças nos arquivos de configuração:

```
csync2 -x -v
```

- 5** Desative o modo de manutenção no cluster:

```
crm configure property maintenance-mode=false
```

É possível executar este comando em qualquer nó de cluster.

- 6** Verifique se o modo de manutenção está inativo:

```
crm status
```

Os recursos do cluster devem aparecer no estado iniciado.

- 7** Opcional: verifique se o upgrade do Sentinel foi bem-sucedido:

```
rcsentinel version
```

Fazendo upgrade do sistema operacional

Esta seção fornece informações sobre como fazer upgrade do sistema operacional para uma versão principal, como fazer upgrade de SLES 11 para SLES 12 em um cluster do Sentinel HA. Ao fazer upgrade do sistema operacional, você deve executar algumas tarefas de configuração para garantir que o Sentinel HA funcione perfeitamente após o upgrade do sistema operacional.

Execute as etapas como descrito nas seções a seguir:

- ♦ [“Fazendo upgrade do sistema operacional” na página 213](#)
- ♦ [“Configurando destinos iSCSI” na página 214](#)
- ♦ [“Configurando iniciadores iSCSI” na página 215](#)
- ♦ [“Configurando o cluster de HA” na página 216](#)

Fazendo upgrade do sistema operacional

Para fazer upgrade do sistema operacional:

- 1** Efetue login como usuário `root` em qualquer nó do cluster do Sentinel HA.
- 2** Execute o comando a seguir para habilitar o modo de manutenção no cluster:

```
crm configure property maintenance-mode=true
```

O modo de manutenção ajuda a evitar qualquer interrupção nos recursos do cluster em execução durante o upgrade do sistema operacional.
- 3** Execute o seguinte comando para verificar se o modo de manutenção está ativo:

```
crm status
```

Os recursos do cluster devem aparecer no estado não gerenciado.
- 4** Verifique se você atualizou o Sentinel para a versão 8.2 ou posterior em todos os nós do cluster.
- 5** Verifique se todos os nós no cluster estão registrados com SLES e SLESHA.

- 6 Execute as etapas a seguir para fazer upgrade do sistema operacional no nó do cluster passivo:
 - 6a Execute o comando a seguir para parar a pilha de cluster:


```
rcopenais stop
```

A interrupção da pilha do cluster garante que os recursos do cluster permaneçam inacessíveis e evita o confinamento dos nós.
 - 6b Faça upgrade do sistema operacional. Para obter mais informações, consulte [Fazendo upgrade do sistema operacional](#).
- 7 Repita a etapa 6 em todos os nós passivos para fazer upgrade do sistema operacional.
- 8 Repita a etapa 6 no nó ativo para fazer upgrade do sistema operacional nele.
- 9 Repita a etapa 6b para fazer upgrade do sistema operacional no armazenamento compartilhado.
- 10 Verifique se o sistema operacional está atualizado para SLES 12 SP3 em todos os nós do cluster.

Configurando destinos iSCSI

Para configurar destinos iSCSI:

- 1 No armazenamento compartilhado, verifique se o pacote iSCSI LIO está instalado. Se ainda não estiver instalado, vá até o Gerenciador de Software YaST2 e instale o pacote iSCSI LIO do (RPM `iscsiliotarget`).
- 2 Execute as etapas a seguir em todos os nós do cluster:
 - 2a Execute o comando a seguir para abrir o arquivo que contém o nome do iniciador iSCSI:


```
cat /etc/iscsi/initiatorname.iscsi
```
 - 2b Observe o nome do iniciador que será usado para configurar os iniciadores iSCSI:

Por exemplo:

```
InitiatorName=iqn.1996-04.de.suse:01:441d6988994
```

Esses nomes de iniciador serão usados ao definir a Configuração de cliente do destino iSCSI.
- 3 Clique em **Serviço**, selecione a opção **Ao Inicializar** para assegurar que o serviço seja iniciado quando o sistema operacional inicializar.
- 4 Selecione a guia **Global**, anule a seleção **Nenhuma Autenticação** para habilitar autenticações e, então, especifique o nome de usuário e a senha para autenticações recebidas e enviadas.

A opção **Nenhuma Autenticação** é habilitada por padrão. No entanto, você deve habilitar a autenticação para verificar se a configuração é segura.
- 5 Clique em **Destinos** e em **Adicionar** para incluir um novo destino.
- 6 Clique em **Add** (Adicionar) para incluir uma nova LUN.
- 7 Deixe o número de LUN como 0, procure na caixa de diálogo **Caminho** (debaixo de Type=fileio) e selecione o arquivo `/localdata` criado. Se você tiver um disco dedicado para armazenamento, especifique um dispositivo de blocos como `/dev/sdc`.
- 8 Repita as etapas 6 e 7, adicione LUN 1 e selecione `/networkdata` desta vez.
- 9 Repita as etapas 6 e 7, adicione LUN 2 e selecione `/sbd` desta vez.
- 10 Deixe as outras opções com os valores padrão. Clique em **Avançar**.
- 11 Clique em **Adicionar**. Quando o Nome do Cliente for solicitado, especifique o nome do iniciador que você copiou na Etapa 2. Repita essa etapa para adicionar todos os nomes dos clientes ao especificar os nomes dos iniciadores.

A lista de nomes de clientes será exibida na Lista de Clientes.

- 12 (Condicional) Se você tiver habilitado a autenticação na Etapa 4, forneça as credenciais de autenticação especificadas na Etapa 4.
Selecione um cliente, selecione **Edit Auth (Editar Autenticação)** > **Incoming Authentication (Autenticação Recebida)** e especifique o nome de usuário e a senha. Repita isso para todos os clientes.
- 13 Clique em **Próximo** para selecionar as opções de autenticação padrão e clique em **Terminar** para sair da configuração. Se solicitado, reinicie o iSCSI.
- 14 Saia do YaST.

Configurando iniciadores iSCSI

Para configurar iniciadores iSCSI:

- 1 Conecte-se a um dos nós do cluster (node01) e inicie o YaST.
- 2 Clique em **Serviços de Rede > Iniciador iSCSI**.
- 3 Se solicitado, instale o software necessário (RPM `iscsiclient`).
- 4 Clique em **Serviço**, selecione **Ao Inicializar** para assegurar que o serviço iSCSI seja iniciado na inicialização.
- 5 Clique em **Destinos Detectados**.

Observação: Se quaisquer destinos iSCSI existentes anteriormente forem exibidos, apague esses destinos.

Selecione **Descoberta** para adicionar um novo destino iSCSI.

- 6 Especifique o endereço IP do Destino iSCSI (10.0.0.3).
(Condicional) Caso tenha habilitado a autenticação na Etapa 4 em **“Configurando destinos iSCSI” na página 214**, anule a seleção **Nenhuma Autenticação**. Na seção **Autenticação Enviada**, digite as credenciais de autenticação que você especificou durante a configuração dos destinos iSCSI.
Clique em **Avançar**.
- 7 Selecione o Destino iSCSI descoberto com o endereço IP 10.0.0.3 e selecione **Efetuar Login**.
- 8 Execute estas etapas:
 - 8a Alterne para Automático no menu suspenso de **Inicialização**.
 - 8b (Condicional) Caso tenha habilitado a autenticação, anule a seleção **Nenhuma Autenticação**.
O nome de usuário e a senha que você especificou deverão ser exibidos na seção **Autenticação Enviada**. Se essas credenciais não forem exibidas, digite as credenciais nesta seção.
 - 8c Clique em **Avançar**.
- 9 Alterne para a guia **Destinos Conectados** para verificar se você está conectado ao destino.
- 10 Saia da configuração. Esse deve ter sido montado nos Destinos iSCSI como dispositivos de bloco no nó do cluster.
- 11 No menu principal do YaST, selecione **System (Sistema) > Partitioner (Particionador)**.

- 12 Na Tela do Sistema, você deverá ver novos discos rígidos do tipo LIO-ORG-FILEIO (como /dev/sdb e /dev/sdc) na lista, além de discos já formatados (como /dev/sdb1 ou /dev/<SHARED1).
- 13 Repita as etapas de 1 a 12 em todos os nós.

Configurando o cluster de HA

Para configurar o cluster de HA:

- 1 Inicie o YaST2 e vá para **Alta Disponibilidade > Cluster**.
- 2 Se solicitado, instale o pacote de HA e resolva as dependências.
Após a instalação do pacote de HA, Cluster — Canais de Comunicação é exibido.
- 3 Verifique se o **Unicast** está selecionado como opção de Transporte.
- 4 Selecione **Adicionar um Endereço de Membro**, especifique o endereço IP do nó e, então, repita essa ação para adicionar todos os outros endereços IP de nós do cluster.
- 5 Verifique se a opção **Gerar Automaticamente ID de Nó** está selecionada.
- 6 Verifique se o serviço HAWK está habilitado em todos os nós. Caso não esteja, execute o seguinte comando para habilitá-lo:

```
service hawk start
```
- 7 Execute o seguinte comando:

```
ls -l /dev/disk/by-id/
```

O ID da partição SBD é exibido. Por exemplo, `scsi-1LIO-ORG_FILEIO:33caaa5a-a0bc-4d90-b21b-2ef33030cc53`.

Copie o ID.
- 8 Abra o arquivo `sbd (/etc/sysconfig/sbd)` e substitua o ID do `SBD_DEVICE` pelo ID que você copiou na etapa 7.
- 9 Execute o seguinte comando para reiniciar o serviço de pacemaker:

```
rcpacemaker restart
```
- 10 Execute o seguinte comando para remover os scripts de início automático, para que o cluster possa gerenciar o produto.

```
cd /
```

```
insserv -r sentinel
```
- 11 Repita as etapas de 1 a 10 em todos os nós do cluster.
- 12 Execute o seguinte comando para sincronizar quaisquer mudanças nos arquivos de configuração:

```
csync2 -x -v
```
- 13 Execute o comando a seguir para desabilitar o modo de manutenção no cluster:

```
crm configure property maintenance-mode=false
```

É possível executar este comando em qualquer nó de cluster.
- 14 Execute o seguinte comando para verificar se o modo de manutenção está inativo:

```
crm status
```

Os recursos do cluster devem aparecer no estado iniciado.

Fazendo upgrade de instalações de aplicação de HA do Sentinel

É possível fazer upgrade de uma instalação da aplicação do Sentinel de alta disponibilidade usando o patch Zypper.

Importante: Os procedimentos nesta seção usam os comandos `rcopenais` e `openais`, que funcionam somente com o SLES 11 SP4. Para o SLES 12 SP2 e posterior, use o comando `systemctl pacemaker.service`.

Por exemplo, para o comando `/etc/rc.d/openais start`, use o comando `systemctl start pacemaker.service`.

- ♦ [“Fazendo o upgrade da aplicação do Sentinel de HA usando o Zypper” na página 217](#)

Fazendo o upgrade da aplicação do Sentinel de HA usando o Zypper

Você deve registrar todos os nós da aplicação por meio do Gerenciador de Aplicação Sentinel antes do upgrade. Para obter mais informações, consulte [“Registrando para receber atualizações” na página 106](#). Se você não registrar a aplicação, o Sentinel exibirá um aviso amarelo.

- 1 Habilite o modo de manutenção no cluster.

```
crm configure property maintenance-mode=true
```

O modo de manutenção ajuda a evitar quaisquer interrupções nos recursos do cluster em execução durante a atualização do software do Sentinel. É possível executar este comando em qualquer nó de cluster.

- 2 Verifique se o modo de manutenção está ativo.

```
crm status
```

Os recursos do cluster devem aparecer no estado não gerenciado.

- 3 Faça upgrade do nó passivo de cluster:

- 3a Interrompa a pilha do cluster.

```
rcopenais stop
```

A interrupção da pilha do cluster garante que os recursos do cluster permaneçam inacessíveis e evita o confinamento dos nós.

- 3b Faça o download das atualizações da aplicação de HA do Sentinel.

```
zypper -v patch
```

- 3c (Condicional) Se o instalador exibir uma mensagem informando que você deve resolver a dependência do pacote OpenSSH, digite a opção apropriada para instalar a versão menos eficiente do pacote OpenSSL.

- 3d (Condicional) Se o instalador exibir uma mensagem indicando mudança na arquitetura ncgOverlay, digite a opção apropriada para aceitar a mudança da arquitetura.

- 3e (Condicional) Se o instalador exibir uma mensagem informando que você deve resolver a dependência de alguns pacotes de aplicação, digite a opção apropriada para desinstalar os pacotes dependentes.

- 3f Quando o upgrade for concluído, inicie a pilha do cluster.

```
rcopenais start
```

- 4 Repita a Etapa 3 para todos os nós passivos do cluster.
- 5 Faça upgrade do nó ativo de cluster:
 - 5a Faça o backup da sua configuração e, em seguida, crie a exportação ESM.
Para obter mais informações sobre como fazer backup de dados, consulte [“Fazendo backup e restaurando dados”](#) no *Guia de administração do Sentinel*.
 - 5b Interrompa a pilha do cluster.

```
rcopenais stop
```


A interrupção da pilha do cluster garante que os recursos do cluster permaneçam inacessíveis e evita o confinamento dos nós.
 - 5c Faça o download das atualizações da aplicação de HA do Sentinel.

```
zypper -v patch
```
 - 5d (Condicional) Se o instalador exibir uma mensagem informando que você deve resolver a dependência do pacote OpenSSH, digite a opção apropriada para instalar a versão menos eficiente do pacote OpenSSL.
 - 5e (Condicional) Se o instalador exibir uma mensagem indicando mudança na arquitetura ncgOverlay, digite a opção apropriada para aceitar a mudança da arquitetura.
 - 5f (Condicional) Se o instalador exibir uma mensagem informando que você deve resolver a dependência de alguns pacotes de aplicação, digite a opção apropriada para desinstalar os pacotes dependentes.
 - 5g Quando o upgrade for concluído, inicie a pilha do cluster.

```
rcopenais start
```
 - 5h Execute o seguinte comando para sincronizar quaisquer mudanças nos arquivos de configuração:

```
csync2 -x -v
```
- 6 Desative o modo de manutenção no cluster.

```
crm configure property maintenance-mode=false
```


É possível executar este comando em qualquer nó de cluster.
- 7 Verifique se o modo de manutenção está inativo.

```
crm status
```


Os recursos do cluster devem aparecer no estado iniciado.
- 8 Opcional: verifique se o upgrade do Sentinel foi bem-sucedido:

```
rcsentinel version
```
- 9 (Condicional) Para fazer upgrade do sistema operacional, consulte [“Fazendo upgrade do sistema operacional”](#) na página 160.

40 Backup e recuperação

O cluster de failover altamente disponível neste documento fornece um nível de redundância, assim, se o serviço falhar em um nó no cluster, ele automaticamente alternará e será recuperado no outro nó no cluster. Quando um evento como esse acontece, é importante recolocar o nó com falha em um estado operacional de modo que a redundância no sistema possa ser restaurada e haja proteção no caso de outra falha. Esta seção fala sobre como restaurar o nó com falha em uma variedade de condições de falha.

- ♦ [“Backup” na página 219](#)
- ♦ [“da PlateSpin” na página 219](#)

Backup

Ao passo que um cluster de failover altamente disponível como o descrito neste documento fornece uma camada de redundância, mesmo assim, é importante fazer regularmente um backup tradicional da configuração e dos dados, que não poderiam ser facilmente recuperados em caso de perda ou corrupção. A seção [“Fazendo backup e restauração de dados”](#) no *Guia de administração do Sentinel* descreve como usar as ferramentas integradas do Sentinel para criar um backup. Essas ferramentas devem ser usadas no nó ativo no cluster, porque o nó passivo no cluster não terá o acesso necessário para o dispositivo de armazenamento compartilhado. Outras ferramentas de backup comercialmente disponíveis podem ser usadas em vez disso e podem ter requisitos diferentes do nó em que podem ser usadas.

da PlateSpin

- ♦ [“Falha temporária” na página 219](#)
- ♦ [“Corrupção do nó” na página 219](#)
- ♦ [“Configuração dos dados do cluster” na página 220](#)

Falha temporária

Se a falha for temporária e não houver nenhuma corrupção aparente no aplicativo, software do sistema operacional e configuração, então basta limpar a falha temporária e, por exemplo, reinicializar o nó, que restaurará o nó para um estado operacional. A interface do usuário de gerenciamento do cluster pode ser usada para efetuar o failback do serviço em execução novamente para o nó do cluster original, se desejado.

Corrupção do nó

Se a falha tiver causado uma corrupção no aplicativo ou software do sistema operacional ou configuração que está presente no sistema de armazenamento do nó, então, o software corrompido precisará ser reinstalado. Repetir as etapas para adicionar um nó no cluster descrito anteriormente neste documento restaurará o nó para um estado operacional. A interface do usuário de gerenciamento do cluster pode ser usada para efetuar o failback do serviço em execução novamente para o nó do cluster original, se desejado.

Configuração dos dados do cluster

Se ocorrer corrupção de dados no dispositivo de armazenamento compartilhado de forma que o dispositivo de armazenamento compartilhado não possa se recuperar, isso resultará em corrupção que afetará todo o cluster de maneira que não poderá ser automaticamente recuperado pelo uso do cluster de failover altamente disponível descrito neste documento. A seção “[Fazendo backup e restauração de dados](#)” no *Guia de administração do Sentinel* descreve como usar as ferramentas integradas do Sentinel para restaurar a partir de um backup. Essas ferramentas devem ser usadas no nó ativo no cluster, porque o nó passivo no cluster não terá o acesso necessário para o dispositivo de armazenamento compartilhado. Outras ferramentas de backup e restauração comercialmente disponíveis podem ser usadas como alternativa e podem ter requisitos diferentes quanto ao nó em que podem ser usadas.

VIII Apêndices

- ♦ [Apêndice A, “Solução de problemas” na página 223](#)
- ♦ [Apêndice B, “Desinstalando” na página 229](#)

A Solução de problemas

Esta seção contém alguns dos problemas que podem ocorrer durante a instalação e as ações para solucioná-los.

- ♦ “Falha na instalação devido a configuração de rede incorreta” na página 223
- ♦ “O UUID não é criado para instâncias do Collector Manager em imagens nem para Correlation Engine” na página 224
- ♦ “Após efetuar login, a interface principal do Sentinel ficará em branco no Internet Explorer” na página 224
- ♦ “O Sentinel não inicia no Internet Explorer 11 no Windows Server 2012 R2” na página 224
- ♦ “O Sentinel não pode executar relatórios locais com a licença EPS padrão” na página 225
- ♦ “É necessário iniciar a sincronização manualmente na Alta Disponibilidade do Sentinel após converter o nó ativo para o modo FIPS 140-2” na página 225
- ♦ “A interface principal do Sentinel exibe uma página em branco após a conversão para o Gerenciador de dados escaláveis do Sentinel” na página 225
- ♦ “O painel Campos de evento não é exibido na página Programar ao editar algumas pesquisas gravadas” na página 226
- ♦ “O Sentinel não retorna nenhum evento correlacionado quando você pesquisa por eventos para a regra implantada com a pesquisa padrão de contagem de acionamentos” na página 226
- ♦ “O painel de controle de inteligência de segurança exibe uma duração de linha de base inválida ao regenerar uma linha de base” na página 226
- ♦ “O servidor do Sentinel desliga ao executar uma pesquisa quando há um número grande de eventos em uma única partição” na página 226
- ♦ “Erro ao usar o script `report_dev_setup.sh` para configurar as portas do Sentinel de exceção do firewall em instalações com upgrade da aplicação do Sentinel” na página 227

Falha na instalação devido a configuração de rede incorreta

Durante a primeira inicialização, uma mensagem de erro é exibida se o instalador determinar que as configurações de rede estão incorretas. Se a rede estiver indisponível, a instalação do Sentinel na aplicação falhará.

Para resolver esse problema, defina corretamente as configurações de rede. Para verificar a configuração, use o comando `ipconfig` para retornar o endereço IP válido e o comando `hostname -f` para retornar o nome do host válido.

O UUID não é criado para instâncias do Collector Manager em imagens nem para Correlation Engine

Se você cria uma imagem de um servidor Collector Manager (por exemplo, usando o ZENworks Imaging) e restaura as imagens em diferentes máquinas, o Sentinel não identifica exclusivamente as novas instâncias do Collector Manager. Isso ocorre por causa de UUIDs duplicados.

É preciso gerar um novo UUID executando as seguintes etapas nos sistemas em que acabou de instalar o Collector Manager:

- 1 Exclua o arquivo `host.id` ou `sentinel.id` que está localizado na pasta `/var/opt/novell/sentinel/data`.
- 2 Reinicie o Collector Manager.
O Collector Manager gera automaticamente o UUID.

Após efetuar login, a interface principal do Sentinel ficará em branco no Internet Explorer

Se o Nível de Segurança da Internet for definido como Alto, uma página em branco será exibida após o login no Sentinel e a janela pop-up de download do arquivo poderá ser bloqueada pelo browser. Para resolver esse problema, é necessário primeiro definir o nível de segurança para Médio-alto e, em seguida, alterar para Nível personalizado da seguinte forma:

1. Navegue até **Ferramentas > Opções da Internet > Segurança** e defina o nível de segurança como **Médio-alto**.
2. Certifique-se de que a opção **Ferramentas > Modo de Exibição de Compatibilidade** não está selecionada.
3. Navegue até **Ferramentas > Opções da Internet > guia Segurança > Nível personalizado** e, em seguida mova a barra de rolagem para baixo até a seção **Downloads** e selecione **Habilitar** na opção **Aviso automático para downloads de arquivo**.

O Sentinel não inicia no Internet Explorer 11 no Windows Server 2012 R2

Quando você usa o Windows Server 2012 R2, o Sentinel não inicia no Internet Explorer 11 devido às configurações de segurança padrão do Internet Explorer 11. Você deve adicionar manualmente o Sentinel à lista de sites confiáveis antes de iniciá-lo.

Para adicionar o Sentinel à lista de sites confiáveis

- 1 Abra o Internet Explorer 11.
- 2 Clique no ícone **Configurações > Opções de Internet > guia Segurança > Sites Confiáveis > Sites**
- 3 Adicione o host do Sentinel à lista de sites confiáveis.

O Sentinel não pode executar relatórios locais com a licença EPS padrão

Se seu ambiente tiver a licença padrão de 25 EPS e você executar um relatório, o relatório falhará com o seguinte erro: Licença para o recurso de Pesquisa Distribuída expirada

Para executar relatórios na mesma JVM que o Sentinel, conclua as seguintes etapas:

- 1 Efetue login no servidor do Sentinel e abra o arquivo `/etc/opt/novell/sentinel/config/obj-component.JasperReportingComponent.properties`.
- 2 Localize a propriedade `reporting.process.oktorunstandalone`.
- 3 (Condicional) Se a propriedade não estiver no arquivo, adicione-a.
- 4 Defina a propriedade como `false`. Por exemplo:
`reporting.process.oktorunstandalone=false`
- 5 Reinicie o Sentinel.

É necessário iniciar a sincronização manualmente na Alta Disponibilidade do Sentinel após converter o nó ativo para o modo FIPS 140-2

Problema: Quando você converte o nó ativo para o modo FIPS 140-2 no Sentinel de Alta Disponibilidade, a sincronização para converter todos os nós passivos para o modo FIPS 140-2 não é completamente executada. Você deve iniciar a sincronização manualmente.

Solução temporária: Sincronize manualmente todos os nós passivos para o modo FIPS 140-2 da seguinte maneira:

- 1 Efetue login como o usuário root no nó ativo.
- 2 Abra o arquivo `/etc/csync2/csync2.cfg`.
- 3 Mude a linha a seguir:
`include /etc/opt/novell/sentinel/3rdparty/nss/*;`
para
`include /etc/opt/novell/sentinel/3rdparty/nss/*;`
- 4 Grave o arquivo `csync2.cfg`.
- 5 Inicie a sincronização manualmente executando o seguinte comando:
`csync2 -x -v`

A interface principal do Sentinel exibe uma página em branco após a conversão para o Gerenciador de dados escaláveis do Sentinel

Problema: Após habilitar o SSDM, quando você efetuar login na interface principal do Sentinel, o browser exibirá uma página em branco.

Solução temporária: Feche o seu browser e efetue login novamente na interface principal do Sentinel. Esse problema acontece somente uma vez, ao efetuar login na interface principal do Sentinel pela primeira vez após habilitar o SSDM.

O painel Campos de evento não é exibido na página Programar ao editar algumas pesquisas gravadas

Problema: Ao editar uma pesquisa gravada atualizada do Sentinel 7.2 para uma versão posterior, o painel **Campos de evento**, usado para especificar os campos de saída no arquivo CSV de relatório de pesquisa, não é exibido na página Programar.

Solução temporária: Após fazer o upgrade do Sentinel, recrie e re programe a pesquisa para exibir o painel **Campos de evento** na página Programar.

O Sentinel não retorna nenhum evento correlacionado quando você pesquisa por eventos para a regra implantada com a pesquisa padrão de contagem de acionamentos

Problema: O Sentinel não retorna nenhum evento correlacionado quando você pesquisa por todos os eventos correlacionados que foram gerados após a regra ser implantada ou habilitada, clicando no ícone ao lado de **Contagem Acionada** no painel **Estatísticas de atividade** na página Resumo da Correlação da regra.

Solução temporária: Mude o valor no campo **De** na página Pesquisa de evento para um horário anterior ao horário preenchido no campo e clique em **Pesquisar** novamente.

O painel de controle de inteligência de segurança exibe uma duração de linha de base inválida ao regenerar uma linha de base

Problema: Durante a regeneração da linha de base de Inteligência de Segurança, as datas de início e de fim da linha de base são exibidas incorretamente como 1/1/1970.

Solução temporária: As datas corretas são atualizadas após a conclusão da regeneração da linha de base.

O servidor do Sentinel desliga ao executar uma pesquisa quando há um número grande de eventos em uma única partição

Problema: O servidor do Sentinel desliga ao executar uma pesquisa quando há um número grande de eventos indexado em uma única partição.

Solução temporária: Crie políticas de retenção de forma que haja pelo menos duas partições abertas em um dia. Ter mais de uma partição aberta ajuda a reduzir o número de eventos indexados nas partições.

Você pode criar políticas de retenção que filtrem eventos com base no campo `estzhour`, que controla a hora do dia. Dessa forma, é possível criar uma política de retenção com `estzhour:[0 TO 11]` como o filtro e outra política de retenção com `estzhour:[12 TO 23]` como o filtro.

Para obter mais informações, consulte [“Configuring Data Retention Policies \(Configurando políticas de retenção de dados\)”](#) no *Sentinel Administration Guide (Guia de Administração do NetIQ Sentinel)*.

Erro ao usar o script `report_dev_setup.sh` para configurar as portas do Sentinel de exceção do firewall em instalações com upgrade da aplicação do Sentinel

Problema: O Sentinel exibe um erro quando o script `report_dev_setup.sh` é usado para configurar as portas do Sentinel de exceção do firewall.

Solução temporária: Configure as portas do Sentinel de exceção do firewall com as etapas a seguir:

1 Abra o arquivo `/etc/sysconfig/SuSEfirewall2`.

2 Mude a linha a seguir:

```
FW_SERVICES_EXT_TCP=" 443 8443 4984 22 61616 10013 289 1289 1468 1443  
40000:41000 1290 1099 2000 1024 1590"
```

para

```
FW_SERVICES_EXT_TCP=" 443 8443 4984 22 61616 10013 289 1289 1468 1443  
40000:41000 1290 1099 2000 1024 1590 5432"
```

3 Reinicie o Sentinel.

B Desinstalando

Este apêndice fornece informações sobre como desinstalar o Sentinel e as tarefas pós-desinstalação.

- ♦ “Lista de verificação da desinstalação” na página 229
- ♦ “Desinstalando o Sentinel” na página 229
- ♦ “Tarefas pós-desinstalação” na página 231

Lista de verificação da desinstalação

Use a lista de verificação a seguir para desinstalar o Sentinel:

- ☐ Desinstale o servidor do Sentinel.
- ☐ Desinstale o Collector Manager e o Correlation Engine, se houver.
- ☐ Execute as tarefas de pós-desinstalação para concluir a desinstalação do Sentinel.

Desinstalando o Sentinel

Um script de desinstalação está disponível para ajudá-lo a remover uma instalação do Sentinel. Antes de realizar uma nova instalação, você deverá executar todas as etapas a seguir para verificar se não restaram arquivos ou configurações do sistema de uma instalação anterior.

Aviso: Essas instruções envolvem a modificação de configurações e arquivos do sistema operacional. Se você não estiver familiarizado com a modificação dessas configurações e arquivos do sistema, contate o administrador do sistema.

Desinstalando o Sentinel Server

Use as etapas a seguir para desinstalar o servidor Sentinel:

- 1 Efetue login no servidor do Sentinel como `root`.

Observação: Você não pode desinstalar o servidor do Sentinel como usuário não root quando a instalação é realizada como usuário `root`. No entanto, o usuário não root pode desinstalar o servidor do Sentinel quando a instalação tiver sido executada pelo usuário não root.

- 2 Acesse o seguinte diretório:

```
<sentinel_installation_path>/opt/novell/sentinel/setup/
```

- 3 Execute o seguinte comando:

```
./uninstall-sentinel
```

- 4 Quando for solicitado que você confirme novamente que deseja prosseguir com a desinstalação, pressione **s**.

O script primeiro para o serviço e, em seguida, remove-o completamente.

Desinstalando o Collector Manager e o Correlation Engine

Use as etapas a seguir para desinstalar o Collector Manager e o Correlation Engine:

- 1 Efetue login como `root` no computador do Collector Manager e do Correlation Engine.

Observação: Você não poderá desinstalar o Collector Manager remoto nem o Correlation Engine remoto como um usuário não root se a instalação foi executada como um usuário `root`. No entanto, o usuário não root poderá efetuar a desinstalação se a instalação foi executada por um usuário não root.

- 2 Vá para o seguinte local:

```
/opt/novell/sentinel/setup
```

- 3 Execute o seguinte comando:

```
./uninstall-sentinel
```

O script exibe um aviso informando que o Collector Manager ou o Correlation Engine e todos os dados associados serão completamente removidos.

- 4 Insira **s** para remover o Collector Manager ou o Correlation Engine.

O script primeiro para o serviço e, em seguida, remove-o completamente. No entanto, o ícone do Collector Manager e do Correlation Engine ainda é exibido no estado inativo na interface principal do Sentinel.

- 5 (Condicional) Se você tiver habilitado a Visualização de eventos, deverá reimplantar o plug-in de segurança do Elasticsearch. Para obter mais informações, consulte [“Reimplantar o plug-in de segurança do Elasticsearch” na página 84](#).

- 6 Realize as seguintes etapas adicionais para apagar manualmente o Collector Manager e o Correlation Engine da interface principal do Sentinel:

Collector Manager:

1. Clique em **Gerenciamento de Fonte de Eventos > Tela Ativa**.
2. Clique com o botão direito do mouse no Collector Manager que deseja apagar e clique em **Apagar**.

Correlation Engine:

1. Navegue até a interface **Principal do Sentinel** como um administrador.
2. Expanda **Correlation** e, em seguida, selecione o Correlation Engine que deseja apagar.
3. Clique no botão **Apagar** (ícone da lixeira).

Desinstalando o NetFlow Collector Manager

Use as etapas a seguir para desinstalar o NetFlow Collector Manager:

- 1 Efetue login no computador do NetFlow Collector Manager.

Observação: Efetue login com a mesma permissão de usuário que foi usada para instalar o NetFlow Collector Manager.

- 2 Mude para o seguinte diretório:

```
/opt/novell/sentinel/setup
```

- 3 Execute o seguinte comando:

```
./uninstall-sentinel
```

- 4 Digite `s` para desinstalar o Collector Manager.

O script primeiro para o serviço e, em seguida, desinstala-o completamente.

Tarefas pós-desinstalação

A desinstalação do servidor do Sentinel não remove do sistema operacional o Usuário Administrador do Sentinel. É preciso remover manualmente o usuário.

Depois de desinstalar o Sentinel, certas configurações dos sistemas permanecerão. Essas configurações deverão ser removidas antes de realizar uma instalação "limpa" do Sentinel, particularmente se a desinstalação do Sentinel encontrou erros.

Para limpar manualmente as configurações do sistema Sentinel:

- 1 Efetue login como `root`.
- 2 Verifique se todos os processos do Sentinel foram parados.
- 3 Remova o conteúdo de `/opt/novell/sentinel` ou do local onde o software Sentinel foi instalado.
- 4 Assegure-se de que ninguém está conectado ao sistema operacional como Administrador do Sentinel (o padrão é `novell`). Em seguida, remova o usuário, o diretório pessoal e o grupo.

```
userdel -r novell
```

```
groupdel novell
```
- 5 Reinicie o sistema operacional.