Sentinel™

Guia de instalação e configuração

Agosto de 2021

Informações legais

As únicas garantias para produtos e serviços da Micro Focus e suas afiliadas e licenciantes (“Micro Focus”) são apresentadas nas declarações de garantia expressas que acompanham tais produtos e serviços. Nada contido aqui deve ser interpretado como constituindo uma garantia adicional. A Micro Focus não será responsável por erros técnicos nem editoriais, tampouco por omissões aqui existentes. As informações aqui contidas estão sujeitas a mudanças sem aviso prévio.

Para obter informações adicionais, como marcas registradas e avisos relacionados à certificação, consulte http://www.microfocus.com/about/legal/.

Índice

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

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

Guia do usuário

Fornece 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.

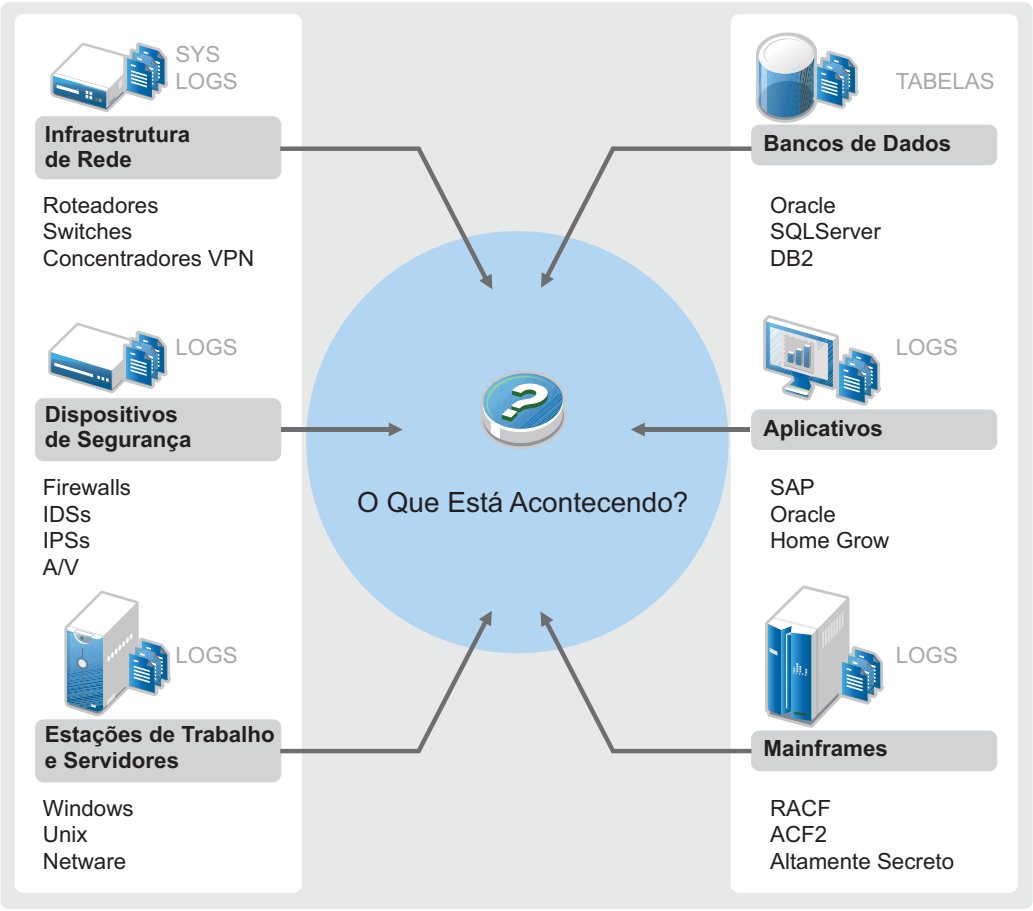
1 O que é o Sentinel?

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

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:

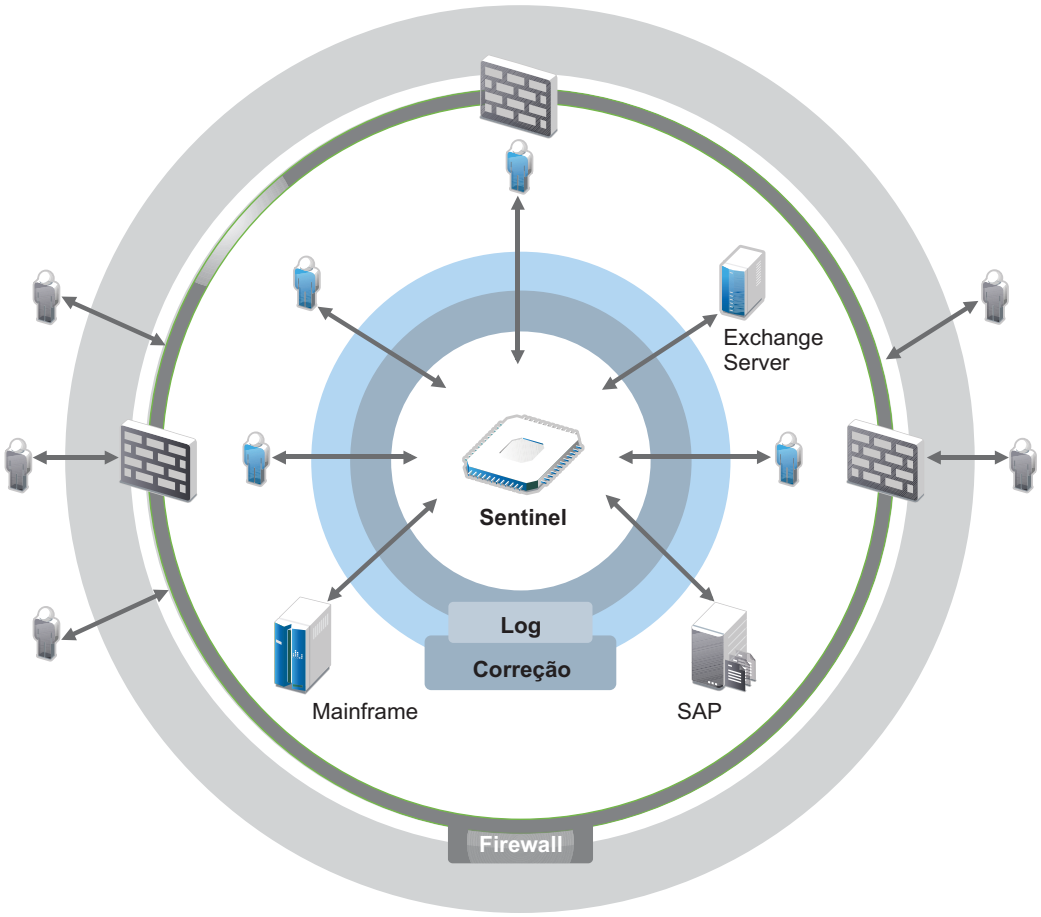
- Coletar dados;
- Consolidar dados;
- Normalizar dados distintos em eventos que possam ser facilmente comparados;
- Mapear eventos para normas padrão.
- Analisar os dados;
- Comparar eventos em diversos sistemas para determinar se há algum problema de segurança;
- Enviar notificações quando os dados 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 analise 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

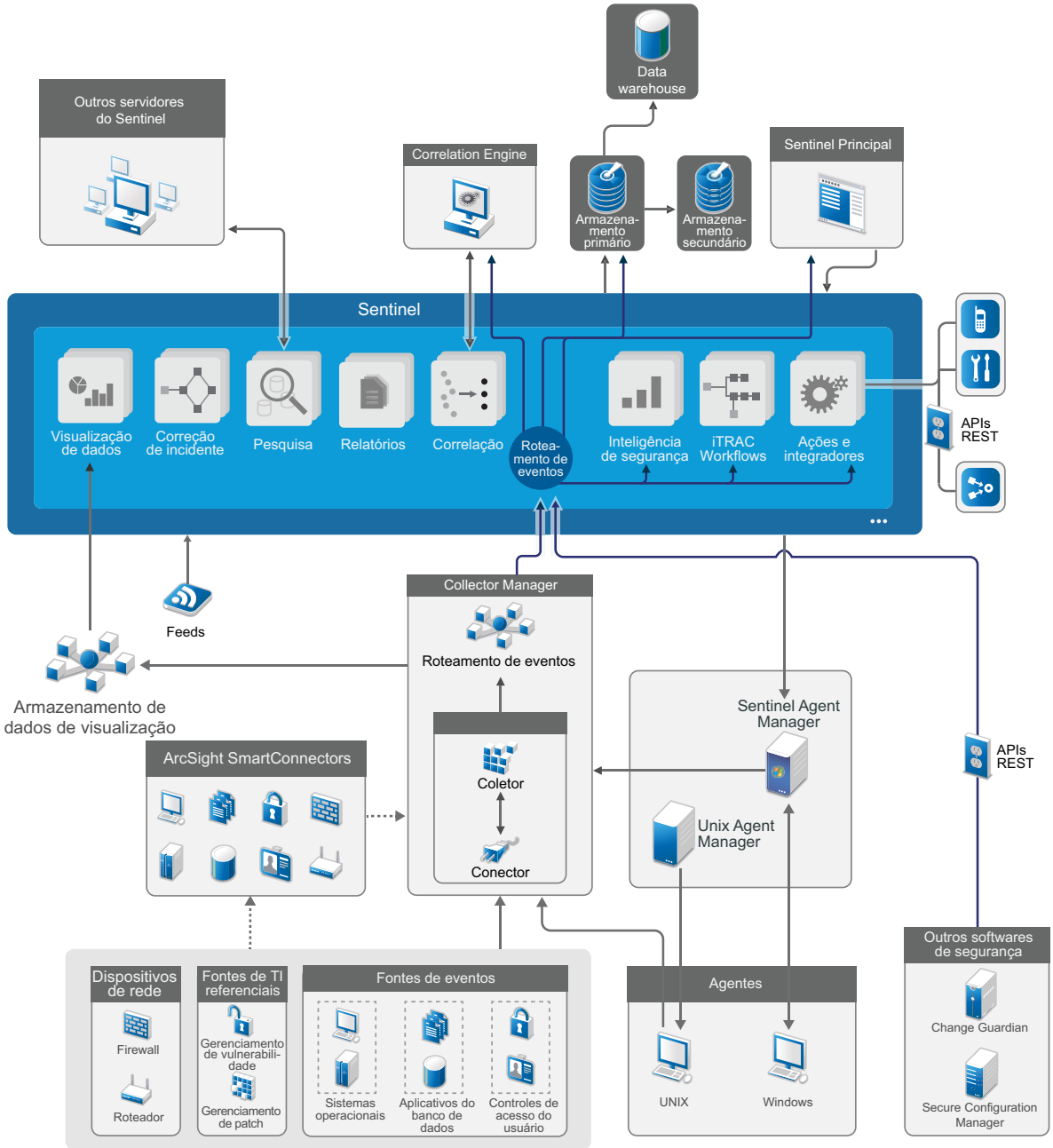
O Sentinel gerencia as informações e os eventos de segurança de forma contínua em todo o ambiente de TI para garantir uma solução de monitoramento completa.

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 com políticas flexíveis e personalizáveis de retenção de dados.
- 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

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 Correlation Engine, 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 23
- “Transmitindo mapas” 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.

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 brutos 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 brutos 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 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.

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 42.

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. Além disso, as regras de correlação agora estão associadas ao MITRE ATT&CK ID. 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 “Correlating Event Data” (Correlacionando dados de eventos) no *Sentinel User Guide* (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, escalação 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 facilmentepara 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 o 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 adeuqado 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*.

II Planejando a instalação do Sentinel

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

Observação: Todos os hosts usados para o servidor Sentinel e seus componentes devem ser configurados em ambiente de resolução DNS de duas vias (Hostname para IP e IP para Hostname).

---

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 149.

❒	Tarefas	Consulte
❒	Revise as informações da arquitetura do produto para aprender sobre os componentes do Sentinel.	Parte I, “Compreendendo o Sentinel” na página 13.
❒	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.
❒	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.
❒	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.
❒	Leia as notas de versão mais atuais do Sentinel para entender a nova funcionalidade e os problemas conhecidos.	Notas de versão do Sentinel
❒	Instale o Sentinel.	Parte III, “Instalando o Sentinel” na página 65.
❒	Configure o Sentinel.	Parte IV, “Configurando o Sentinel” na página 101.
❒	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.
❒	Instalando coletores e conectores adicionais no seu ambiente conforme necessário.	Capítulo 15, “Instalando coletores e conectores adicionais” na página 97.

❒	Tarefas	Consulte
❒	Instalando instâncias do Collector Manager e do Correlation Engine adicionais no seu ambiente conforme necessário.	Parte III, “Instalando o Sentinel” na página 65.

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
◆ 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
Correlação ◆ Correlação de padrão de evento em tempo real ◆ Ações desencadeadas por regras de correlação ◆ Triagem de alertas ◆ Visualização de alerta	Sim	Não
Inteligência de Segurança ◆ Regras de anomalia ◆ Análise estatística em tempo real	Sim	Não

Licenças do Sentinel

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

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.

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.

Observação

- Todos os hosts usados para o servidor Sentinel e seus componentes devem ser configurados em ambiente de resolução DNS de duas vias (Hostname para IP e IP para Hostname).
- Antes de instalar o Sentinel, verifique se o seu ambiente está seguro e em dia com as atualizações de segurança mais recentes.

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 Sentinel System Requirements (Requisitos do Sistema 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 parceiropode trabalhar com você para projetar o sistema do Sentinel que seja adequado para seu ambiente de TI.

Considerações sobre armazenamento de dados

Dependendo da taxa de EPS, é possível optar por usar o armazenamento tradicional para armazenar e indexar seus dados do Sentinel.

Tabela 6-1 *Armazenamento tradicional*

Armazenamento tradicional
Por padrão, os dados são armazenados no armazenamento tradicional com base no arquivo e a indexação é feita localmente no servidor do Sentinel. 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 42. Perfeitamente escalável até aproximadamente 20 mil EPS. Além disso, você deve adicionar outros servidores Sentinel para escalar verticalmente até uma taxa de EPS muito mais alta. 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. Os dados são rotulados de acordo com o locatário, mas não são segregados dessa forma no disco. A replicação e a disponibilidade dos dados devem ser feitas manualmente ou utilizando mecanismos de armazenamento caros, como o disco SAN (Storage area network).

Planejando o armazenamento tradicional

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

Armazenamento 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.	
Armazenamento 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 o 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 43.

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

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 43. 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 93.

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
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 o Elasticsearch” na página 71.
- ❒ **Habilitar visualização de eventos:** A visualização de eventos está desabilitada por padrão. Para habilitar a visualização de eventos, consulte Capítulo 18, “Configurando o Elasticsearch para visualização do evento” na página 109.
- ❒ **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 72.

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 44
- "Vantagens das instâncias adicionais do Correlation Engine" na página 44

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 65.

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 65.

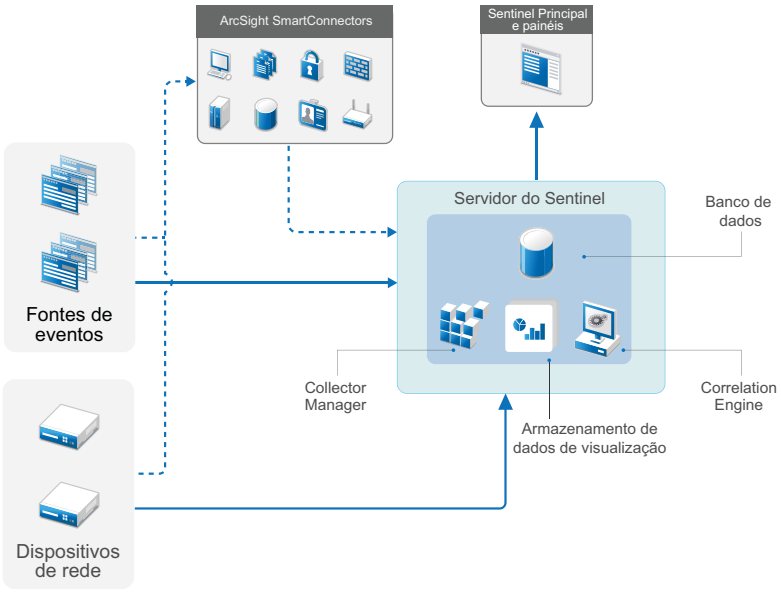
Observação: Não é possível instalar mais do que um Correlation Engine em um único sistema. Você pode instalar instâncias adicionais do Correlation Engine nos sistemas remotos, e conectá-los ao servidor do Sentinel.

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 6-1 *Implantação multifuncional*



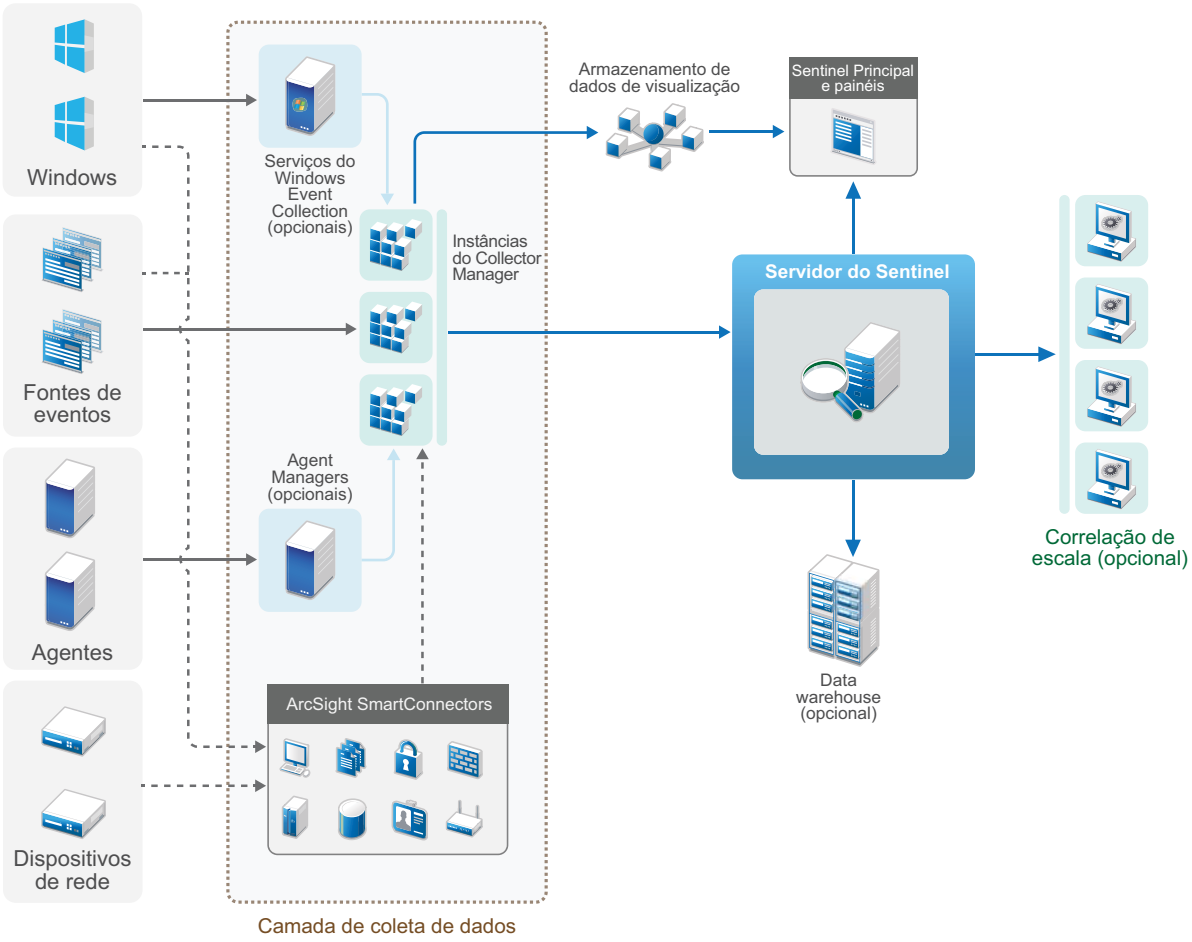
Implantação distribuída de um nível

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 Collector Managers e os Correlation Engines 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.

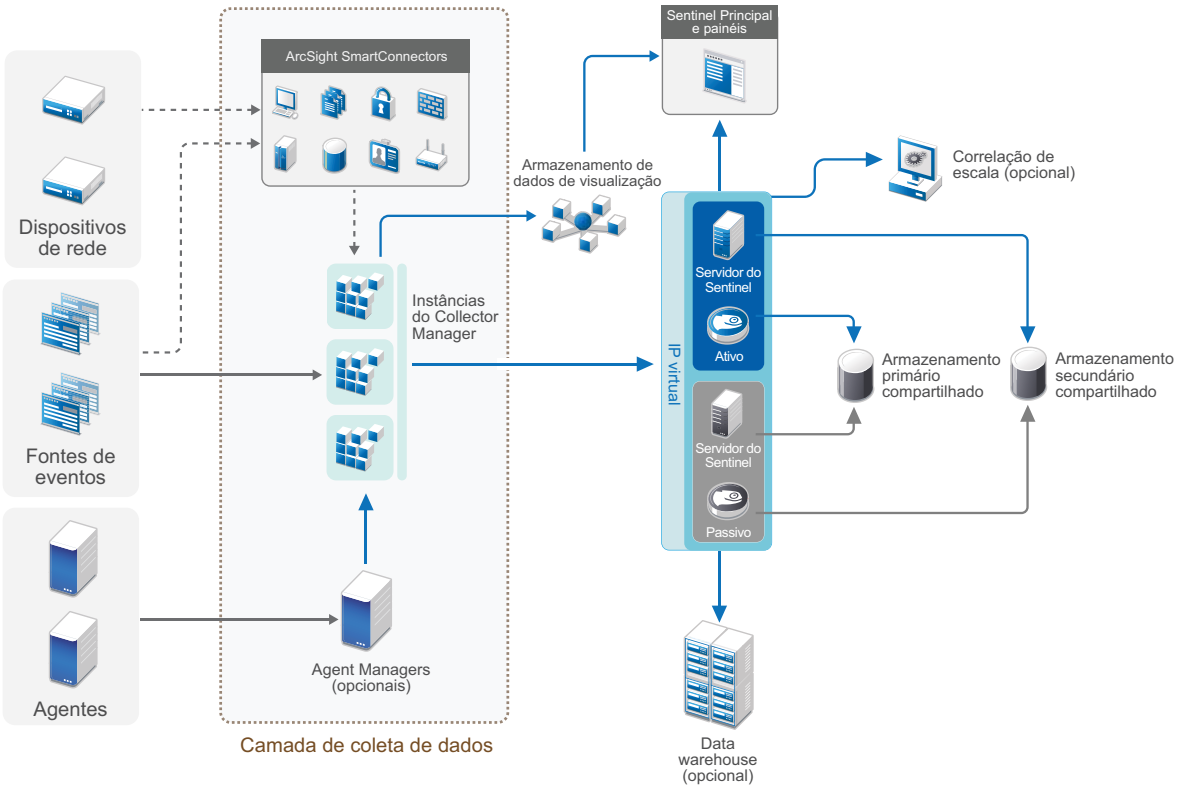
Figura 6-2 *Implantação distribuída de um nível*



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 199.

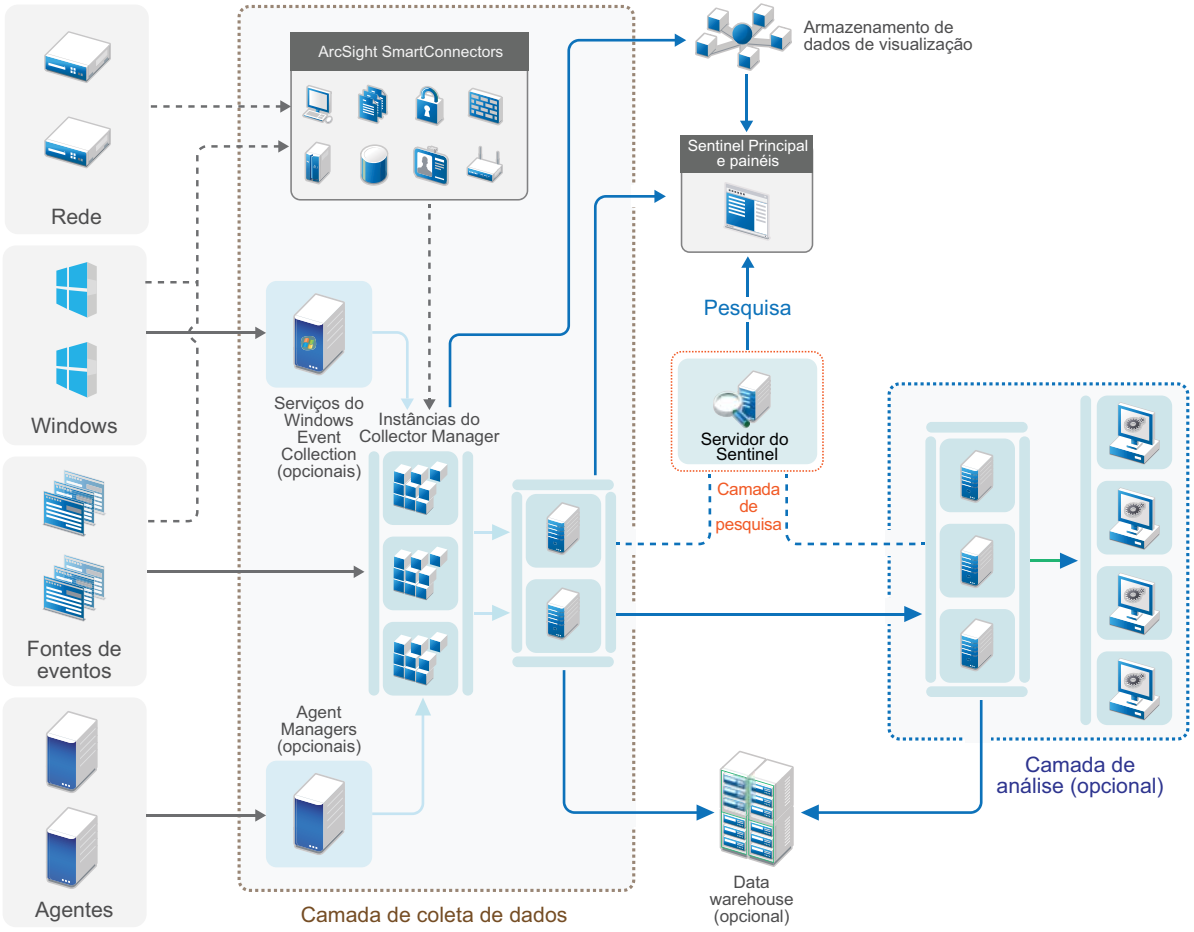
Figura 6-3 *Implantação distribuída de um nível com alta disponibilidade*



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 desejar 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 6-4 *Implantação distribuída de dois e três níveis*



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.

Habilitar o modo Sentinel FIPS 140-2 faz com que 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 e o Sentinel Control Center use 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

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 131.

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 138.

- 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 52.
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 76. “Realizando uma instalação silenciosa” na página 81 Capítulo 22, “Ativando o modo FIPS 140-2 em uma instalação existente do Sentinel” na página 125
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 131.
Importe certificados para o Sentinel FIPS Keystore.	“Importando certificados para o banco de dados de keystore do FIPS” na página 139

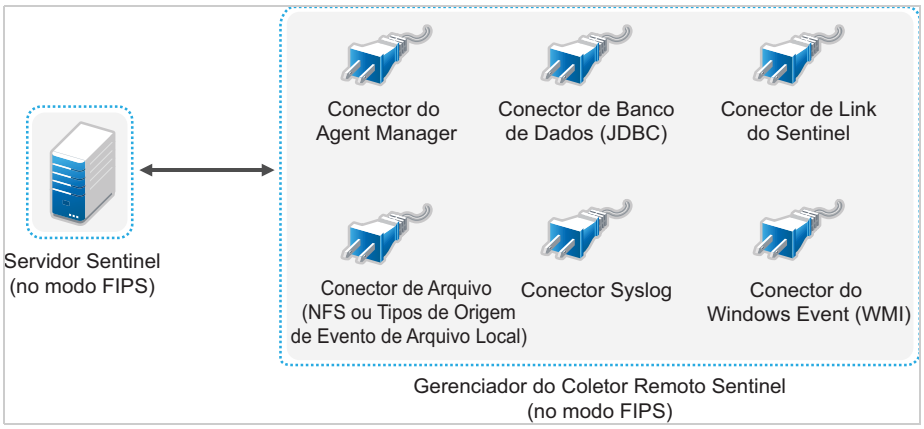
Observação: Faça o backup de seus sistemas Sentinel antes de iniciar a conversão para o modo FIPS. Se o servidore tiver de ser revertido para um modo não FIPS posteriormente, o único método suportado para fazer isso envolve a restauração de um backup. Para obter mais informações sobre a reversão para o modo não FIPS, consulte “Revertendo o Sentinel para o modo não FIPS” na página 139.

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 125.

---

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 127.

---

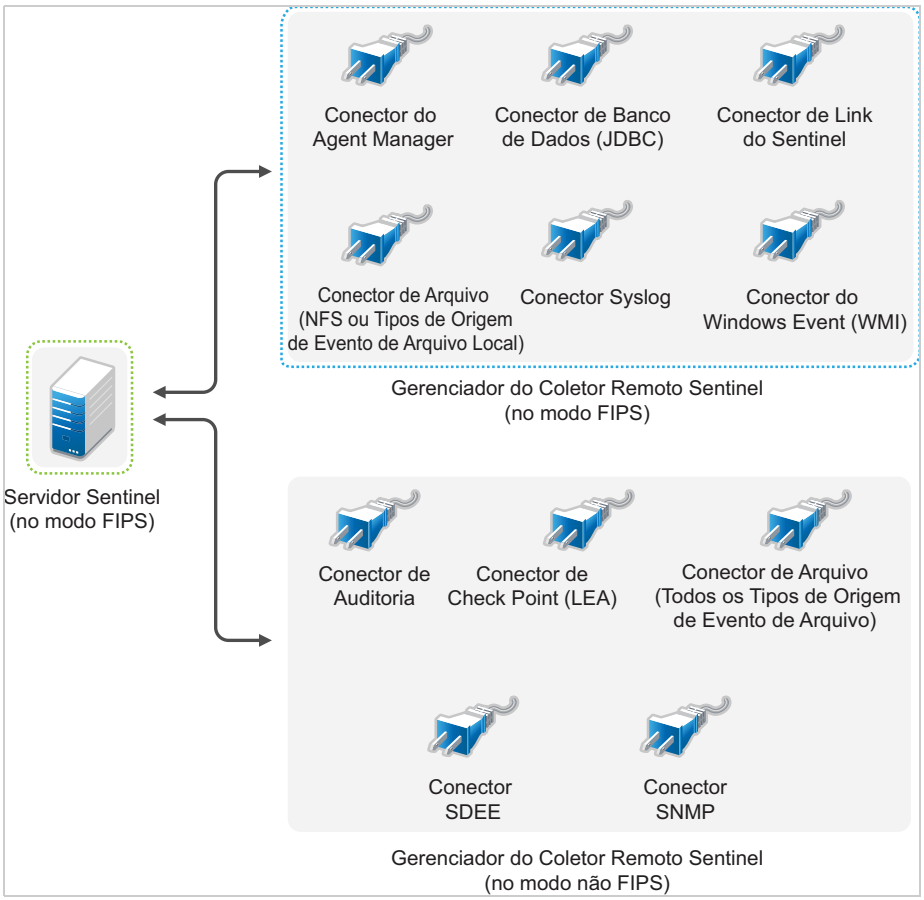
3 Certifique-se de que o servidor FIPS e as instâncias remotas do Collector Manager comuniquem-se entre si.

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 127.

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 131.

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 gerenciar a coleta de dados usando Conectores que suportam e que não suportam o modo FIPS 140-2, você deve ter duas instâncias remotas dos Collector Managers: uma em execução no modo FIPS 140-2 para Conectores com suporte para FIPS e outra 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 125.

---

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 127.

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 131.

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 127.

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 131.

   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

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.
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 criptografas 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 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.

Portas	Direção	Necessária/ opcional	Descrição
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.
TCP 7443	Interno	Opcional	Essa porta permite que um sistema Sentinel receba eventos de outro software SIEM, como o Change Guardian e o Secure Configuration Manager.

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).
TCP 7443	Interno	Obrigatório	Usada pelo Conector do Servidor HTTP.

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 criptografas 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 Collector Manager.
TCP 7443	Interno	Obrigatório	Usada pelo Conector do Servidor HTTP.

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.

Portas	Direção	Necessária/ opcional	Descrição
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).
TCP 7443	Interno	Obrigatório	Usada pelo Conector do Servidor HTTP.

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 Correlation Engine.

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).

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.
Autentica os usuários com o banco de dados interno.	Fornece 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 75.

- **Silencioso:** Se você deseja instalar vários servidores do Sentinel e instâncias do Collector Manager ou do Correlation Engine em sua implantação, pode registrar as opções de instalação durante a instalação padrão ou personalizada em um arquivo de configuração e usá-lo para executar uma instalação silenciosa. Para obter mais informações sobre a instalação silenciosa, veja “Realizando uma instalação silenciosa” na página 81.

Instalação da aplicação

A instalação da aplicação instala o sistema operacional SLES 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 14, “Instalação da aplicação” na página 87.

III Instalando o Sentinel

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

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 bens e de vulnerabilidade, informações de identidade, status de incidentes e de workflow, Inteligência de Segurança, dados de alertas e assim por diante.
- **Elasticsearch:** Indexa eventos e alertas para pesquisa e visualização. 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, acima de 2.500, deve implantar nós adicionais do Elasticsearch em um cluster
- **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.
- **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.
- **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 253.
- ❒ 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 57 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).
- ❒ **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. Portanto, verifique se os seguintes pacotes estão instalados antes de instalar o Sentinel:
    - `bc`
    - `bash`
    - `coreutils`
    - `gettext`
    - `glibc`
    - `grep`
    - `libgcc`
    - `libstdc`
    - `lsof`
    - `openssl`

- `sed`
- `insserv`
- `net-tools`
- `libX` (para RHEL 7.x)
- `zlib` (até SLES 12.x e RHEL 7.x, 8.x)
- `python-libs` (até SLES 12.x e RHEL 7.x)
- `netstat` (até SLES 12.x e RHEL 7.x) ou `ss` (para SLES 15 e posteriores)
- `pam-modules` (disponível apenas quando você instala o Legacy-Module no SLES 15.x)

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

Para ver as visualizações do evento, como usuário root, defina a propriedade `vm.max_map_count=262144` no arquivo `/etc/sysctl.conf`. Depois de adicionar a propriedade, execute `sysctl -p` para que as mudanças entrem em vigor.

12 Instalando 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

Preencha os seguintes pré-requisitos antes de instalar os nós externos do Elasticsearch:

- Se você instalou os nós externos do Elasticsearch 5.6.13 com as versões do Sentinel 8.3 ou anteriores, desinstale o Elasticsearch e instale o Elasticsearch 7.7.0. Para obter mais informações sobre a instalação, consulte Instalando 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 em Sentinel System Requirements (Requisitos do Sistema do Sentinel).

Instalando o Elasticsearch

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

Para instalar e configurar o Elasticsearch:

1. Instale a versão do JDK suportada pelo Elasticsearch.
2. Verifique se o usuário do Elasticsearch tem acesso ao Java.
3. Faça download da versão certificada do Elasticsearch RPM. Para obter informações sobre a versão certificada do Elasticsearch e o URL para download, consulte a página Sentinel System Requirements (Requisitos do Sistema do Sentinel).
4. Instale o Elasticsearch:

   ```
   rpm -ivh elasticsearch-<version>.rpm
   ```

5. Conclua as tarefas conforme mencionado na tela nas instruções pós-instalação do RPM.
6. 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 preencher os pré-requisitos acima, execute o comando `sysctl -p` para recarregar as mudanças feitas nos arquivos.

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 Reinicie o Elasticsearch.

9 Repita todas as etapas acima em cada nó externo do Elasticsearch do cluster 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 `<caminho_de_instalação_do_sentinel>/etc/opt/novell/sentinel/config/elasticsearch-index.properties` e atualize as propriedades listadas na tabela conforme necessário.

Tabela 12-1 *Propriedades do Elasticsearch*

Propriedade	Valor Padrão	Notas
elasticsearch.events.lucenefilter (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,xdastaxname,xdasoutcomename,sev,vul,rv32,rv39,rv159,dhn,dip,rv98,dp,fn,rv199,dun,tufname,rv84,rv158,shn,sip,rv76,sun,iufname,sp,iudep,rv198,rv62,st,tid,srcgeo,destgeo,obsgeo,rv145,estz,estzmonth,estzdiy,estzdim,estzdiw,estzhour,estzmin,rv24,tudep,pn,xdasclass,xdasid,xdasreg,xdasprov,iuident,tuident	Indica os campos de evento que você deseja que o Elasticsearch indexe.
es.num.shards	6	Indica o número de fragmentos primários por índice. Você poderá aumentar esse valor padrão quando o tamanho do fragmento ultrapassar 50 GB.

Propriedade	Valor Padrão	Notas
es.num.replicas	1	Indica o número de shards de réplica que cada shard primário deve ter. É recomendado um cluster de pelo menos 2 nós considerando failover e alta disponibilidade.

13 Instalação tradicional

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

Executando instalações interativas

Esta seção fornece informações sobre instalação padrão e personalizada.

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 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 Especifique o seguinte comando no root 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>`

4 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.

5 Pressione a barra de espaço para ler o contrato de licença.

6 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.

7 Especifique 2 para executar uma instalação personalizada do Sentinel.

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

ou

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

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

10 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.

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

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

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

14 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.

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

15a 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.

15b Insira certificados externos no banco de dados do keystore para estabelecer confiança, pressione `s` e especifique o caminho para o arquivo de certificado. Adicionar o caminho do certificado `http` do Elasticsearch `<caminho_de_instalação_do_sentinel>/opt/novell/sentinel/3rdparty/elasticsearch/config/http.pks` quando ele solicitar o certificado externo.

15c Conclua a configuração do modo FIPS 140-2 seguindo as tarefas mencionadas no Capítulo 23, “Operando o Sentinel no modo FIPS 140-2” na página 129.

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 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 43.

Você pode instalar mais de um Collector Manager ou Correlation Engine.

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.

Você pode registrar os parâmetros de instalação durante a instalação interativa e, em seguida, usar os arquivos registrados para uma instalação autônoma em outros sistemas. Você pode especificar os seguintes arquivos para registrar a instalação:

- <*Arquivo_de_resposta*>: Registra os parâmetros de instalação especificados durante a instalação.
- <*Arquivo_de_configuração*>: Especifique esse arquivo apenas se você tiver vários servidores do Sentinel. Você pode usar esse arquivo para conectar o Collector Manager e o Correlation Engine a um servidor do Sentinel diferente daquele registrado no arquivo de resposta. Durante a instalação interativa, ele cria marcadores para os detalhes do servidor do Sentinel. Posteriormente, você pode atualizar esse arquivo com os detalhes relevantes do servidor do Sentinel e usá-lo junto com o arquivo de resposta durante a instalação autônoma.

  Observação: Esta opção está disponível apenas no Sentinel 8.2 SP3 e posterior.

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 Collector Manager e o Correlation Engine, conclua 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 (Condicional) Para instalar sem registrar a instalação, especifique o seguinte comando:

- **Para o Collector Manager:**

  ```
  ./install-cm
  ```

- **Para o Correlation Engine:**

  ```
  ./install-ce
  ```

8 (Condicional) Para instalar e registrar a instalação, siga um dos seguintes procedimentos:

- (Condicional) Se você tiver um único servidor do Sentinel, especifique o seguinte comando:
  - **Para o Collector Manager:**

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

  - **Para o Correlation Engine:**

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

- (Condicional) Se você tiver vários servidores do Sentinel, especifique o seguinte comando:
  - **Para o Collector Manager:**

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

  - **Para o Correlation Engine:**

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

Para obter mais informações sobre como usar o arquivo de resposta ou o arquivo de configuração, consulte "Realizando uma instalação silenciosa" na página 81.

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

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

10 Pressione a barra de espaço para ler o contrato de licença.

11 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.

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

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

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

14a Número da porta do canal de comunicação do servidor do Sentinel.

14b Número da porta do servidor da Web do Sentinel.

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

Para modo FIPS:

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

Para modo não FIPS:

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

Compare a saída da certificação com a certificação de servidor do Sentinel exibida em Etapa 13.

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

---

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

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

18 (Condicional) Se a Lista de Revogação de Certificados estiver habilitada no servidor, selecione `Sim` quando solicitado e conclua as seguintes etapas:

18a Copie o certificado de <*CONFIG_HOME*>`/config/` do servidor para <*CONFIG_HOME*>`/config/` do Collector Manager ou do Correlation Engine. O valor padrão de <*CONFIG_HOME*> é `/etc/opt/novell/sentinel`.

18b Clique em `Sim` quando solicitado.

18c Especifique a senha do certificado do cliente.

19 (Condicional) Se você escolheu a configuração Personalizada, digite `yes` ou `y` para habilitar o modo FIPS 140-2 no Sentinel e adicione o caminho do certificado `http` do Elasticsearch `<caminho_de_instalação_do_sentinel>/opt/novell/sentinel/3rdparty/elasticsearch/config/http.pks` quando ele solicitar o certificado externo.

20 (Condicional) Se o 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 "Authentication Methods" (Métodos de autenticação) no *Sentinel Administration Guide* (Guia de Administração 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.

21 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, Collector Manager ou Correlation Engine em sua implantação. Você pode registrar os parâmetros de instalação durante a instalação interativa e, em seguida, executar em outros sistemas os arquivos registrados.

- Verifique se você registrou os parâmetros de instalação em um arquivo. Para obter mais informações sobre a criação do arquivo de resposta, consulte:
  - “Instalação padrão do servidor do Sentinel” na página 75
  - “Instalação personalizada do servidor do Sentinel” na página 76
  - “Instalação do Collector Manager e Correlation Engine” na página 78.

Observação: Para o Collector Manager e o Correlation Engine, use o arquivo de configuração para conectar o Collector Manager e o Correlation Engine a um servidor do Sentinel diferente daquele registrado no arquivo de resposta. Atualize esse arquivo com os detalhes relevantes do servidor do Sentinel e use-o junto com o arquivo de resposta durante a instalação autônoma.

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:

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 Collector Manager ou Correlation Engine.

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 (Condicional) Para instalar o servidor do Sentinel no modo silencioso, especifique o seguinte comando:

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

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) Para instalar instâncias do Collector Manager, especifique o seguinte comando:

- Para usar o arquivo de resposta:

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

- Para usar o arquivo de resposta e o arquivo de configuração:

  ```
  ./install-cm -u <response_filename> -i <configuration_filename>
  ```

6 (Condicional) Para instalar instâncias do Correlation Engine, especifique o seguinte comando:

- Para usar o arquivo de resposta:

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

- Para usar o arquivo de resposta e o arquivo de configuração:

  ```
  ./install-ce -u <response_filename> -i <configuration_filename>
  ```

7 (Condicional) Conclua a configuração do modo FIPS 140-2 seguindo as tarefas mencionadas em Capítulo 23, “Operando o Sentinel no modo FIPS 140-2” na página 129. Adicione o caminho do certificado `http` do Elasticsearch `<caminho_de_instalação_do_sentinel>/opt/novell/sentinel/3rdparty/elasticsearch/config/http.pks` quando ele solicitar o certificado externo.

Instalando o Sentinel como um usuário não root

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.

Quando instalar o Sentinel como um usuário `não root`, você deve instalá-lo como o usuário `novell`. Não há suporte para instalações não root que não sejam o usuário `novell`, embora a instalação prossiga com êxito.

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 root insale 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 (Condicional) Se o local do diretório não padrão já existia antes de Etapa 4 na página 82, verifique se o usuário `novell` tem permissões de propriedade do diretório. Execute o seguinte comando para atribuir as permissões de propriedade:

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

7 Especifique o comando a seguir para mudar o usuário não root recém-criado, ou seja, o `novell`:

```
su novell
```

8 (Condicional) Para realizar uma instalação interativa:

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

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

8b Continue na Etapa 11.

9 (Condicional) Para executar a instalação silenciosa do servidor do Sentinel, verifique se você registrou 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 75 ou "Instalação personalizada do servidor do Sentinel" na página 76.

9a Para instalar, especifique o seguinte comando:

Local padrão: `./install-sentinel -u <nomedo_arquivo_de_resposta>`

Local diferente do padrão: `./install-sentinel --location=/foo -u <nome_do_arquivo_de_resposta>`

9b Continue na Etapa 14.

10 (Condicional) Para executar a instalação silenciosa do Collector Manager ou do Correlation Engine, verifique se você registrou os parâmetros de instalação em um arquivo.

Observação: Use o arquivo de configuração para conectar o Collector Manager e o Correlation Engine a um servidor do Sentinel diferente daquele registrado no arquivo de resposta. Atualize esse arquivo com os detalhes relevantes do servidor do Sentinel e use-o junto com o arquivo de resposta durante a instalação autônoma.

Para obter informações sobre como criar o arquivo de resposta ou o arquivo de configuração, consulte "Instalação do Collector Manager e Correlation Engine" na página 78

10a Especifique o comando apropriado, dependendo do componente que você está instalando:

Componente	Comando

Collector Manager	◆ Para usar o arquivo de resposta:
	◆ **Local padrão:** `./install-cm -u <`*nome*`do_arquivo_de_resposta>`
	◆ **Local diferente do padrão:** `./install-cm --location=/foo -u <`*nome*`do_arquivo_de_resposta>`
	◆ Para usar o arquivo de resposta e o arquivo de configuração:
	◆ **Local padrão:**
	`./install-cm -u <nome`*do_arquivo_de_resposta*`> -i <`*nomedoarquivo_de_configuração*`>`
	◆ **Local diferente do padrão:**
	`./install-cm --location=/foo -u <`*nome*`do_arquivo_de_resposta> -i <`*nome_do*`arquivo_de_configuração>`
	A instalação continua com os valores do servidor do Sentinel do arquivo de configuração e os outros valores dos parâmetros de instalação armazenados no arquivo de resposta.

Correlation Engine	◆ Para usar o arquivo de resposta:
	◆ **Local padrão:** `./install-ce -u <`*nome*`do_arquivo_de_resposta>`
	◆ **Local diferente do padrão:** `./install-ce --location=/foo -u <`*nome*`do_arquivo_de_resposta>`
	◆ Para usar o arquivo de resposta e o arquivo de configuração:
	◆ **Local padrão:**
	`./install-ce -u <`*nome_do*`arquivo_de_resposta> -i <`*nome_do_arquivo_de_configuração*`>`
	◆ Local diferente do padrão:
	`./install-ce --location=/foo -u <`*nome_do*`arquivo_de_resposta> -i <`*nome_do*`arquivo_de_configuração>`
	A instalação continua com os valores do servidor do Sentinel do arquivo de configuração e os outros valores dos parâmetros de instalação armazenados no arquivo de resposta.

10b Continue na Etapa 14.

11 Especifique o número do idioma que deseja usar na instalação.

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

12 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.

13 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 75.
   - Se você escolher prosseguir com a instalação personalizada, continue com Etapa 7a Etapa 14 em "Instalação personalizada do servidor do Sentinel" na página 76.

14 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.

14 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 robusto com o serviço de atualização integrado do software Sentinel para fornecer uma experiência do 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.

Dependendo da versão do Sentinel, o instalador da aplicação instala o sistema operacional SLES certificado:

- Para 8.2, o instalador da aplicação instala o SLES 12 SP3.
- Para 8.2 SP2, o instalador da aplicação instala o SLES 12 SP4.
- Para 8.3 SP1, o instalador da aplicação instala o SLES 12 SP5.

A imagem da aplicação Sentinel é empacotada nos formatos ISO e OVF, que podem ser implantados em ambientes virtuais. Para obter informações sobre plataformas de virtualização suportadas, consulte Sentinel System Requirements (Requisitos do Sistema do Sentinel).

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 88
- "Instalando instâncias do Collector Manager e do Correlation Engine" na página 89

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 `root` e digite a senha que você definiu em Etapa 9.

17 Avance para a "Configuração pós-instalação para a aplicação" na página 92.

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 88.

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:** Expecifique 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 o 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 "Authentication Methods" (Métodos de autenticação) no *Sentinel Administration Guide* (Guia de Administração 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 aEtapa 17 em "Instalando o Sentinel" na página 88.

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 90
- "Instalando instâncias do Collector Manager e do Correlation Engine" na página 91

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 90.

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 o 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 "Authentication Methods" (Métodos de autenticação) no *Sentinel Administration Guide* (Guia de Administração 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 92
- "Criando partições para armazenamento tradicional" na página 93
- "Configurando a aplicação com SMT" na página 94

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.

Com base no sistema operacional instalado, é possível registrar-se para atualizações das seguintes maneiras:

- Se você estiver usando o SLES 12 SP3 ou posterior, poderá se registrar usando o Sentinel Appliance Management Console.
- Se você estiver usando o SLES 12 SP3 ou posterior, poderá se registrar usando os comandos.

- "Registrar-se usando o Sentinel Appliance Management Console" na página 93
- "Registrar usando comandos" na página 93

Registrar-se usando o Sentinel Appliance Management Console

Para se registrar usando o Sentinel Appliance Management Console:

1. Inicie a aplicação do Sentinel seguindo um dos seguintes procedimentos:
   - Efetue login no Sentinel. Clique em **Sentinel Main** > **Appliance** (Principal do Sentinel > 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 **Online Update** > **Register Now** (Atualização Online > Registrar Agora).
4. No campo **Email** (E-mail), especifique o ID do e-mail no qual deseja receber atualizações.
5. No campo **Activation Key** (Chave de Ativação), digite o código de registro.
6. Clique em **Registrar** para concluir o registro.

Registrar usando comandos

Para registrar usando comandos:

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 40. 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 (no qual foi gravado 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 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 95
- “Configurando a aplicação” na página 95
- “Fazendo upgrade da aplicação” na página 96

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-8-OS-Updates sle-12-x86_64
smt-repos -e Sentinel-Server-8-Prod-Updates sle-12-x86_64
smt-repos -e Sentinel-Collector-Manager-8-OS-Updates sle-12-x86_64
smt-repos -e Sentinel-Collector-Manager-8-Prod-Updates sle-12-x86_64
smt-repos -e Sentinel-Correlation-Engine-8-OS-Updates sle-12-x86_64
smt-repos -e Sentinel-Correlation-Engine-8-Prod-Updates sle-12-x86_64
```

2 Configure a aplicação com o SMT seguindo as etapas na seção “Configuring Clients to Use SMT” (Configurando clientes para usar o SMT) da documentação do SMT.

Fazendo upgrade da aplicação

Para obter informações sobre a atualização da aplicação, veja “Fazendo upgrade da aplicação Sentinel” na página 163

15 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

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 segiur, 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.

16 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>`

  Observação: SLES15 em diante usa o seguinte comando:

  `ss -tln |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.

  Observação: Para cair na interface do usuário principal do Sentinel, execute as seguintes etapas:

  1. Acesse o diretório <pasta_de_instalação_do_sentinel>`/etc/opt/novell/sentinel/config/`
  2. Habilite o arquivo `sentinel.sentinel.redirection` em `Configuration.properties` mudando seu valor para `true`.
  3. Reinicie o Sentinel: `rcsentinel restart`.
  4. Efetue login no Sentinel usando o URL:

     `https://IP_AddressOrDNS_Sentinel_server:<port>/sentinel/`

IV Configurando o Sentinel

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

17 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

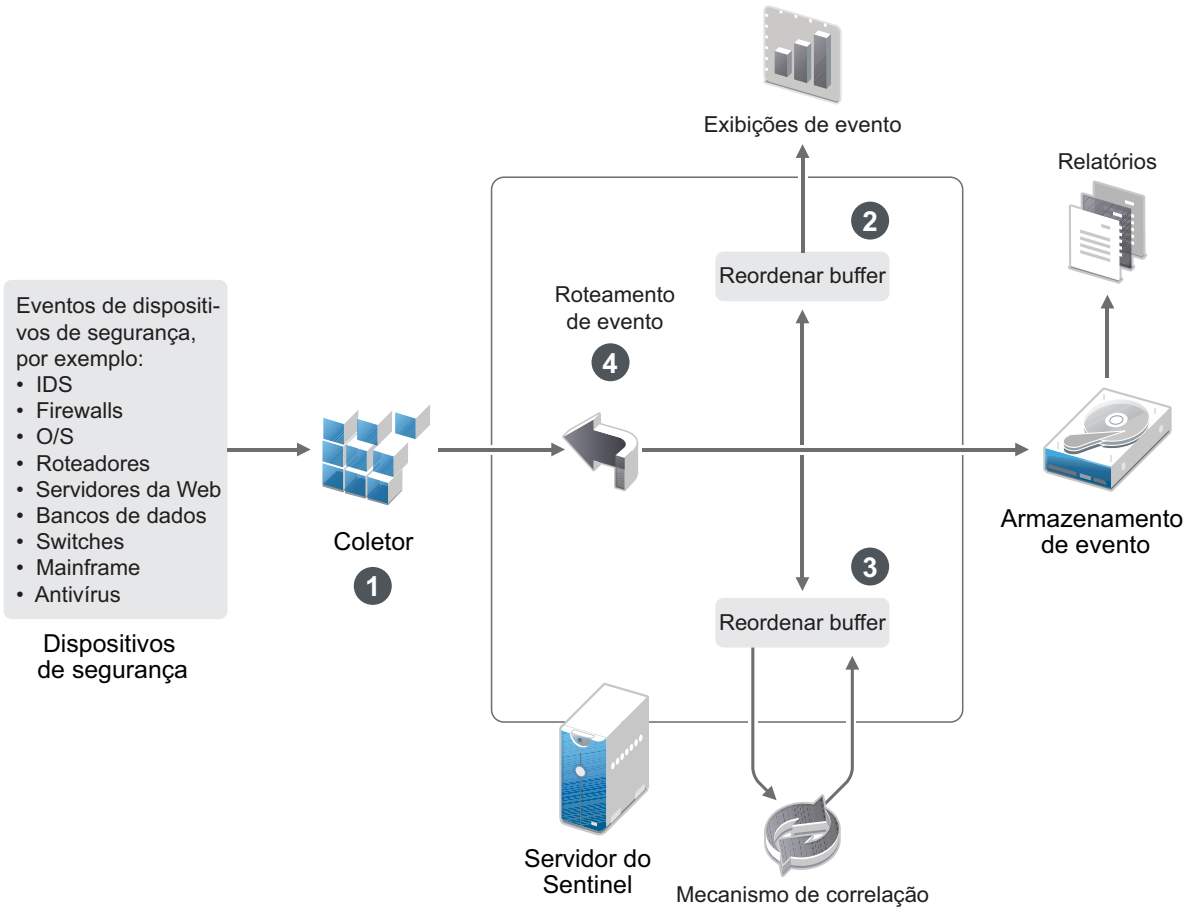
O Sentinel é um sistema distribuído, composto por vários processos distribuídos por toda a sua rede. Além disso, podem ocorrer certos atrasos introduzidos pela fonte de eventos. Para lidar com essa situação, os processos do Sentinel reordenam os eventos em um fluxo ordenado por horários antes de realizar 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 17-1 *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 Collector Manager, 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 completo em um ambiente ditribuido. Por exemplo, você pode ter uma fonte de eventos em um fuso horário, o Collector Manager em outro, o servidor back end 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 informaçõ̃es 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.

18 Configurando o Elasticsearch para visualização do evento

Embora a Elasticsearch exija muito pouca configuração, há uma série de configurações que precisam ser consideradas antes de entrar em produção.

Observação: Na configuração de cluster do Elasticsearch, com base na saúde dos nós, qualquer nó conectado/disponível primeiro é atualizado no arquivo `kibana.yml`. Ele foi projetado dessa forma para fornecer menos carga no nó do servidor Sentinel (para melhor desempenho). Este arquivo `kibana.yml` é atualizado via Sentinel com base na saúde do nó (que se conecta primeiro).

Habilitando a visualização do evento no Sentinel

1. Alterne para o usuário `novell`:

   ```
   su novell
   ```

   Execute as etapas 2 e 3, se a versão java for 292. Para encontrar a versão java no nível do OS, execute `java -version` no prompt de comando.

2. (Condicional) Defina JAVA_HOME como o JDK do Sentinel em "bundle":

   ```
   JAVA_HOME=/opt/novell/sentinel/jdk
   ```

3. (Condicional) Defina PATH para java como o local do JDK do Sentinel:

   ```
   PATH=$JAVA_HOME/bin:$PATH
   ```

4. Gere uma CA (Autoridade de Certificação) para o seu cluster no nó do Sentinel. Execute o seguinte comando no diretório pessoal do Elasticsearch `<caminho_de_instalação_do_sentinel>/opt/novell/sentinel/3rdparty/elasticsearch` do Sentinel:

   ```
   ./bin/elasticsearch-certutil ca
   ```

   São solicitados o nome do arquivo e uma senha do certificado CA. Aqui o nome do arquivo padrão é `elastic-stack-ca.p12`.

5. Gere os certificados e as chaves privadas para o nó do Elasticsearch pré-empacotado do Sentinel. Para isso, execute o seguinte comando no diretório pessoal do Elasticsearch `<caminho_de_instalação_do_sentinel>/opt/novell/sentinel/3rdparty/elasticsearch` do Sentinel:

   ```
   ./bin/elasticsearch-certutil cert --ca <CA certificate filename>.p12 --out config/certs/node-1.p12
   ```

É solicitada a senha do seu certificado CA. Você também precisa criar uma senha para o certificado gerado.

6 Adicione as seguintes configurações no arquivo `<caminho_de_instalação_do_sentinel>/opt/novell/sentinel/3rdparty/elasticsearch/config/elasticsearch.yml` no nó do Sentinel:

- `xpack.security.transport.ssl.enabled: true`
- `xpack.security.transport.ssl.keystore.path: certs/node-1.p12`
- `xpack.security.transport.ssl.truststore.path: certs/node-1.p12`
- `xpack.security.transport.ssl.verification_mode: certificate`

7 Armazene a senha do arquivo de certificado `truststore` e `keystore` gerado acima no keystore do Elasticsearch. Para isso, execute os seguintes comandos no diretório pessoal do Elasticsearch: `<caminho_de_instalação_do_sentinel>/opt/novell/sentinel/3rdparty/elasticsearch` do Sentinel:

```
./bin/elasticsearch-keystore add
xpack.security.transport.ssl.keystore.secure_password
```

```
./bin/elasticsearch-keystore add
xpack.security.transport.ssl.truststore.secure_password
```

8 Efetue login no servidor do Sentinel como usuário `novell`.

9 Abra o arquivo `/etc/opt/novell/sentinel/config/configuration.properties`.

10 (Condicional) Se você estiver usando o Sentinel no modo de Alta Disponibilidade (HA), verifique se a propriedade `sentinel.ha.cluster` está definida como `true` para todos os nós no cluster.

11 Defina `eventvisualization.traditionalstorage.enabled` como `true`.

12 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.

13 (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 35, “Migrando dados para o Elasticsearch” na página 195.

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.

Elasticsearch no modo cluster

1 Conclua as etapas na seção “Habilitando a visualização do evento no Sentinel” na página 109.

2 Configure o arquivo `/etc/elasticsearch/elasticsearch.yml` em cada nó externo do Elasticsearch atualizando ou adicionando as seguintes informações:

Propriedade e valor	Notas
discovery.seed_hosts: [<IP do nó master do elasticsearch elegível no cluster>,<IP do nó master do elasticsearch elegível no cluster>, <IP do nó master do elasticsearch elegível no cluster> e assim por diante]	
cluster.name: <*Elasticsearch _nome_do_cluster*>	O nome do cluster que você especifica deve ser o mesmo para todos os nós.
node.name: <*nome_do_nó*>	Cada nó deve ter um nome exclusivo.
network.host: _<*networkInterface*>:ipv4_	Se você estiver usando o nome de host em vez do endereço IP, verifique se o nome de host pode ser resolvido por todos os nós no cluster do Elasticsearch e no servidor Sentinel.
thread_pool.write.queue_size: 300	
thread_pool.search.queue_size: 10000	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: threadpool.search.queue_size = 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)
index.codec: best_compression	
path.data: ["/<*es1*>", "/<*es2*>"]	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 /es1, /es2 etc. Para obter melhor desempenho e gerenciabilidade, monte cada caminho em um disco físico separado (JBOD).

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

4 No nó do Elasticsearch do servidor Sentinel, configure <caminho_de_instalação_do_sentinel>/opt/novell/sentinel/3drparty/elasticsearch/config/elasticsearch.yml da seguinte maneira:

4a Verifique se os valores de `cluster.name` e `discovery.seed_hosts` no arquivo `elasticsearch.yml` são os mesmos que no arquivo `elasticsearch.yml` no nó externo do Elasticsearch.

5 (Condicional) Para o Sentinel com armazenamento tradicional, adicione os endereços IP dos nós do Elasticsearch à propriedade `ServerList` no arquivo <caminho_de_instalação_do_sentinel>/etc/opt/novell/sentinel/config/elasticsearch-index.properties.

Por exemplo: `ServerList=`*<IP1 do Elasticsearch>*`:`*<Porta>*`,`*<IP2 do Elasticsearch>*`:`*<Porta>*

6 **Habilitando a comunicação segura entre nós externos do Elasticsearch, bem como entre o Sentinel e o cluster do Elasticsearch se houver uma configuração de cluster externo do Elasticsearch**

A versão mais recente do Sentinel habilita a comunicação segura entre o servidor Sentinel e o cluster externo do Elasticsearch, bem como entre diferentes nós do cluster do Elasticsearch. Esta seção explica as etapas sobre como habilitar essas configurações seguras para casos em que você tem um cluster externo do Elasticsearch conectado ao servidor Sentinel.

Etapas a serem seguidas para garantir a comunicação dentro do cluster entre nós do Elasticsearch:

1. Gere os certificados para todos os nós externos do Elasticsearch no cluster. Você pode primeiro criar todos os certificados externos do Elasticsearch no próprio nó do Sentinel e, em seguida, copiá-los para os respectivos nós do Elasticsearch. Para isso, primeiro execute o seguinte comando no diretório pessoal do Elasticsearch <caminho_de_instalação_do_sentinel>/opt/novell/sentinel/3rdparty/elasticsearch do Sentinel:

   ```
   ./bin/elasticsearch-certutil cert --ca <CA certificate filename>.p12 --out config/certs/newNode.p12
   ```

   É solicitada a senha do seu certificado CA. Você também precisa criar uma senha para o certificado gerado.

2. Copie os certificados para os respectivos nós externos do Elasticsearch. Por exemplo, copie o arquivo `newNode.p12` no diretório `/etc/elasticsearch/certs/` do `newNode` do cluster externo do Elasticsearch. Forneça permissões de leitura e gravação para os certificados nas novas máquinas que usam o comando `chmod`.

   Observação: Se o diretório `certs` não estiver presente, você precisará criá-lo.

3. Depois de gerar e copiar os certificados para todos os nós externos do Elasticsearch, adicione as seguintes configurações no arquivo `/etc/elasticsearch/elasticsearch.yml` de todos os nós externos do Elasticsearch:

   - `xpack.security.enabled: true`
   - `xpack.security.transport.ssl.enabled: true`
   - `xpack.security.transport.ssl.keystore.path: certs/newNode.p12`

- `xpack.security.transport.ssl.truststore.path: certs/newNode.p12`
- `xpack.security.transport.ssl.verification_mode: certificate`

4. Em cada um dos nós externos do Elasticsearch, armazene a senha para o arquivo de certificado `keystore` e `truststore` gerado no keystore do Elasticsearch. Para isso, execute os seguintes comandos no diretório pessoal do Elasticsearch `/usr/share/elasticsearch` de todos os nós externos do Elasticsearch:

```
./bin/elasticsearch-keystore add
xpack.security.transport.ssl.keystore.secure_password
```

```
./bin/elasticsearch-keystore add
xpack.security.transport.ssl.truststore.secure_password
```

Etapas a serem seguidas para proteger as comunicações do Sentinel para o cluster do Elasticsearch:

1. Alterne para o usuário `novell`:

```
su novell
```

2. Execute o seguinte comando para gerar um certificado `http` para um nó externo do Elasticsearch da máquina Sentinel:

```
<sentinel_installation_path>/opt/novell/sentinel/bin/javacert.sh --
generateES <provide path where the http certificate should be
generated, example /opt/http.pks> <http certificate password>
<keyalias>
```

3. Copie o certificado `http` para o nó do Elasticsearch. Por exemplo, copie o arquivo `http.pks` no diretório `ES_PATH_CONF/certs/` no nó do Elasticsearch. Forneça permissões de leitura e gravação para os certificados das novas máquinas.

Observação: Se o diretório `certs` não estiver presente, você precisará criá-lo.

---

4. Adicione as seguintes configurações no arquivo `ES_PATH_CONF/elasticsearch.yml` em todos os nós externos do Elasticsearch:
   - `xpack.security.http.ssl.enabled: true`
   - `xpack.security.http.ssl.keystore.path: certs/http.pks`
5. Execute o seguinte comando no diretório pessoal do Elasticsearch `/usr/share/elasticsearch` de todos os nós externos do Elasticsearch para gravar a senha do certificado `http` no keystore do Elasticsearch:

```
./bin/elasticsearch-keystore add
xpack.security.http.ssl.keystore.secure_password
```

7 Reinicie o Sentinel:

```
rcsentinel restart
```

8 Reinicie cada nó externo do Elasticsearch:

```
/etc/init.d/elasticsearch restart
```

9 Verifique se o cluster do Elasticsearch foi formado, executando os seguintes comandos:

```
cd <sentinel_installation_path>/opt/novell/sentinel/bin
```

```
./elasticsearchRestClient.sh <sentinel_ip> <Port used for the
Elasticsearch> GET _cat/nodes
```

10 Verifique se todos os dados de alerta e de eventos existentes (se disponíveis) foram movidos para os nós externos do Elasticsearch.

11 Para desempenho e estabilidade ideais do servidor Sentinel, configure o nó do Elasticsearch no servidor Sentinel como um nó `elegível para master` dedicado, de modo que todos os dados de visualização do evento sejam indexados em nós externos do Elasticsearch:

11a Pare o nó interno (servidor Sentinel)

```
rcsentinel stopES
```

11b Defina os seguintes nós internos no arquivo `elasticsearch.yml`:

```
node.master: true
node.data: false
node.ingest: false
```

11c Execute `elasticsearch-node repurpose` para limpar todos os fragmentos

```
<sentinel_installation_path>/opt/novell/sentinel/3rdparty/
elasticsearch/bin/elasticsearch-node -v repurpose
```

11d Inicie o nó interno do Elasticsearch

```
rcsentinel startES
```

11e Reinicie cada nó externo do Elasticsearch:

```
/etc/init.d/elasticsearch restart
```

Importante: Sempre que um nó externo do Elasticsearch cai, o cluster do Elasticsearch é reiniciado automaticamente e, devido a isso, pode haver um problema temporário ao iniciar painéis de controle pelo Kibana e pela pesquisa de alerta.

Quando o servidor Sentinel for reiniciado, verifique se foram reiniciados também os nós externos do Elasticsearch.

---

19 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 inseerindo 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.

20 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

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.

21 Implementação da lista de revogação de certificados em uma instalação do Sentinel existente

Autenticação SSL mútua no Sentinel

O Sentinel é usado para padronizar protocolos de segurança em redes, servidores, computadores e design lógico para aumentar a segurança geral.

O Sentinel suporta Autenticação SSL mútua para fornecer um cache local de dados de revogação, implementando o recurso CRL (Certificate Revocation List – Lista de Revogação de Certificados). A CRL ajuda a bloquear um cliente comprometido mesmo quando o Sentinel não está conectado à Internet para validar as credenciais de certificado de um cliente revogado.

A CRL é uma lista de certificados digitais que foram revogados pela CA (Autoridade de Certificação) emissora antes da data de vencimento programada e não devem mais ser confiáveis. As CRLs são um tipo de lista negra e são usadas por vários endpoints, incluindo browsers da Web, para verificar se um certificado é válido e confiável.

Este capítulo fornece informações sobre o seguinte:

Habilitando a comunicação SSL mútua e a lista de revogação de certificados

Para habilitar a comunicação mútua de SSL e a CRL no servidor Sentinel:

1. Vá para o diretório <*caminho_de_instalação_do_sentinel*>/opt/novell/sentinel/bin.
2. Execute o comando a seguir como o usuário novell:

   ```
   ./createDefaultMutualCert.sh
   ```

3. (Condicional) Se o certificado for criado com o script antes de converter o servidor em modo FIPS, conclua as seguintes etapas:

   3a Vá para o diretório <*caminho_de_instalação_do_sentinel*>/opt/novell/sentinel/bin/.

   3b Execute o seguinte comando:

```
./convert_to_fips -i <sentinel_installation_path>
/etc/opt/novell/sentinel/config/
.defaultRestClient.p12
```

3c Reinicie o Sentinel:

```
rcsentinel restart
```

4 Acesse o diretório <*caminho_de_instalação_do_sentinel*>/opt/novell/sentinel/setup no Collector Manager e no Correlation Engine.

5 Execute o seguinte comando e siga as instruções na tela para tornar o Collector Manager e o Correlation Engine compatíveis com o servidor Sentinel:

```
./configure.sh
```

Observação: Se o Collector Manager e o Correlation Engine estiverem no modo CRL e não puderem se conectar com o servidor, faça upgrade da **versão cURL** na máquina para 7.60 ou posteriores.

Criando e importando um certificado personalizado

Para criar e importar um certificado personalizado:

1 Crie a chave privada e a pública usando o seguinte comando:

```
openssl req -new -text -out <public_key_name> -keyout
<private_key_name>
```

2 Crie um certificado X.509 autoassinado usando o seguinte comando:

```
openssl req -x509 -days 365 -in
 <public_key_name> -text -key
 <private_key_name> -out
 <certificate_name>
```

3 Importe o certificado gerado para o keystore do Sentinel:

```
<sentinel_installation_path>
/opt/novell/sentinel/bin/javacert.sh --import
 <sentinel_installation_path>
/etc/opt/novell/sentinel/config/.webserverkeystore.jks
 <password of the keystore>  <alias_name> <certificate_name>
```

4 Converta o certificado gerado para o formato p12:

```
openssl pkcs12 -inkey <private_key_name>  -in <certificate_name> -
export -out <certificate_name.p12>
```

5 Para ver a lista de certificados importados no Keystore, execute o seguinte comando:

```
<sentinel_installation_path>
/opt/novell/sentinel/jdk/jre/bin/keytool -list -keystore
/etc/opt/novell/sentinel/config/.webserverkeystore.jks
```

6 Reinicie o servidor Sentinel.

Iniciando o Sentinel por comunicação mútua SSL

Para iniciar o Sentinel por comunicação mútua SSL:

1. Faça download do arquivo de certificado .defaultRestClient.p12 criado em "Habilitando a comunicação SSL mútua e a lista de revogação de certificados" na página 119.

   Você também pode usar seu próprio certificado personalizado. Para obter mais informações sobre como criar um certificado personalizado, consulte "Criando e importando um certificado personalizado" na página 120.
2. Importe o certificado <*nome do certificado.p12*> para o browser do aplicativo do cliente.
3. Recarregue o browser do aplicativo do cliente.
4. Utilize o URL a seguir para iniciar o Sentinel:

   `https://<endereço_ip_do_sentinel>:<porta_do_sentinel>`
5. Selecione o certificado importado na etapa anterior e clique em **OK**.

Revogando o certificado e adicionando-o à CRL

Para revogar o certificado e adicioná-lo à CRL:

1. Crie um diretório para a CRL:

   `mkdir /etc/<CRL_directory>`
2. Alterne para o diretório criado:

   `cd /etc/<CRL_directory>`
3. Crie o arquivo de índice para a CRL:

   `touch index.txt`
4. Crie um arquivo de número temporário da CRL:

   `echo 00 > pulp_crl_number`
5. Edite o arquivo `openssl.cnf` presente no diretório `/etc/ssl/` (no SLES) ou `/etc/pki/tls/` (no RHEL).

   Observação: Se o caminho de arquivo não for conhecido, execute o comando `openssl version -a | grep OPENSSLDIR` para encontrar o diretório que contém o arquivo `openssl.cnf`.

   `database = /etc/<CRL_directory>/index.txt`

   `crlnumber = /etc/<CRL_directory>/pulp_crl_number`

   (Opcional) Você pode criar seu próprio arquivo config com a configuração necessária para a CRL.
6. Converta o certificado a ser revogado no formato `crt`:

   `openssl pkcs12 -in <certificate in p12 format> -clcerts -nokeys -out <certificate_name.crt>`

7 Revogue o certificado:

```
openssl ca -revoke <certificate_name.crt>
-keyfile <private_key> -cert
<X.509 certificate>
```

8 Gere o arquivo CRL para o certificado revogado:

```
openssl ca -gencrl -keyfile <private_key>
-cert <X.509 certificate> -out /etc/
<CRL_directory>/crl.pem
```

9 Adicione o certificado revogado ao arquivo CRL existente:

9a Execute o seguinte comando:

```
cat <sentinel_installation_path>/etc/opt/
novell/sentinel/config/<Sentinel CRL File Name>
/etc/<CRL_directory>/
crl.pem > temp.pem
```

9b Execute o seguinte comando:

```
mv temp.pem <sentinel_installation_path>/etc/opt/
novell/sentinel/config/<Sentinel CRL File Name>
```

O <nome do arquivo CRL do Sentinel> pode ser referido pela chave de propriedade `sentinel.webserver.crlfile`, que está disponível em `<caminho_de_instalação_do_sentinel>/etc/opt/novell/sentinel/config/configuration.properties`

10 (Condicional) Se houver mais de um certificado revogado, repita as etapas de 6 a 9 para cada um dos certificados.

11 Reinicie o servidor Sentinel.

Desabilitando o recurso CRL

Para desabilitar o recurso CRL:

1 Alterne para o diretório:

```
<sentinel_installation_path>/etc/opt/novell/sentinel/3rdparty/jetty
```

2 Execute o seguinte comando:

```
mv jetty-ssl-context.xml.crl.bkp jetty-ssl-context.xml
```

3 No arquivo `<caminho_de_instalação_do_sentinel>/etc/opt/novell/sentinel/config/configuration.properties`, remova as seguintes propriedades:

- `sentinel.client.cert.password=<cert.password>`
- `sentinel.validate.crl=true`
- `sentinel.webserver.crlfile=/config/pulp_crl.pem`

4 Reinicie o servidor Sentinel.

```
rcsentinel restart
```

5 Acesse o diretório <*caminho_de_instalação_do_sentinel*>/opt/novell/sentinel/setup no Collector Manager e no Correlation Engine.

6 Execute o seguinte comando e siga as instruções na tela para tornar o Collector Manager e o Correlation Engine compatíveis com o servidor Sentinel:

```
./configure.sh
```

Observação: Se o Collector Manager e o Correlation Engine estiverem no modo CRL e não puderem se conectar com o servidor, faça upgrade da **versão cURL** na máquina para 7.60 ou posteriores.

---

22 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

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.

   Adicione o caminho do certificado `http` do Elasticsearch `<caminho_de_instalação_do_sentinel>/opt/novell/sentinel/3rdparty/elasticsearch/config/http.pks` quando ele solicitar o certificado externo.

   (Condicional) Se o Elasticsearch estiver no modo cluster, copie todos os certificados `http` dos nós externos do Elasticsearch criados na seção "Configurações no Elasticsearch para comunicação segura de cluster" na página 180 para o servidor Sentinel. Adicione o caminho do certificado `http` do Elasticsearch copiado acima `<caminho dos certificados copiados acima>/<nome dos certificados>` quando ele solicitar o certificado externo. Repita esta etapa para garantir que todos os certificados do Elasticsearch externos sejam adicionados.

   (Condicional) Se estiver usando o recurso CRL, adicione o caminho do certificado do cliente `<caminho_de_instalação_do_sentinel>/etc/opt/novell/sentinel/config/.defaultRestClient.p12` quando ele solicitar o certificado externo.

   Você pode usar o certificado de cliente padrão (.defaultRestClient.p12) ou usar seu próprio certificado personalizado. Para obter mais informações sobre como criar um certificado personalizado, consulte "Criando e importando um certificado personalizado" na página 120.

5 (Condicional) Se o ambiente usar autenticação multifatorial ou forte:

5a Execute o script `create_mfa_fips_keys.sh` e siga as instruções na tela.

Observação: O script exige a senha para o banco de dados nss.

5b Forneça o ID do cliente do Sentinel e o segredo do cliente do Sentinel. Para obter mais informações sobre métodos de autenticação, consulte "Authentication Methods" (Métodos de autenticação) no Sentinel Administration Guide (Guia de Administração 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 Reinicie o servidor do Sentinel.

7 Conclua a configuração do modo FIPS 140-2 seguindo as tarefas mencionadas na Capítulo 23, "Operando o Sentinel no modo FIPS 140-2" na página 129.

Habilitando o modo FIPS na aplicação HA Tradicional/ Sentinel

1 No nó ativo:

1a Conclua as etapas mencionadas na seção "Ativando o servidor do Sentinel para executar no Modo FIPS 140-2" na página 125.

1b Execute o seguinte comando para sincronizar as propriedades de configuração de todos os nós passivos:

- `csync2 -x -v`

1c Verifique se a pasta está sincronizada com todos os nós passivos:

- `/etc/opt/novell/sentinel/3rdparty/nss`

1d (Condicional) Se a pasta `/etc/opt/novell/sentinel/3rdparty/nss` não estiver sincronizada, copie essa pasta manualmente do nó ativo para cada um dos nós passivos no cluster:

- `scp -pr /etc/opt/novell/sentinel/3rdparty/nss <ip do nó passivo ou nome do nó passivo>:/etc/opt/novell/sentinel/3rdparty/`

2 No nó passivo:

2a Verifique se a pasta `nss` tem permissão do usuário `novell` no nó passivo:

2a1 Efetue login no nó passivo.

2a2 Modifique a propriedade da pasta para o usuário `novell`:

- `chown -R novell:novell /etc/opt/novell/sentinel/3rdparty/nss`

2a3 Defina a permissão adequada para a pasta:

- `chmod –R 600 /etc/opt/novell/sentinel/3rdparty/nss`

2b Repita a etapa 2a em todos os nós passivos do cluster.

2c Execute repetidamente o seguinte comando do nó ativo, para garantir que todos os arquivos relacionados ao FIPS sejam atualizados em todos os nós passivos:

- `csync2 –x –v`

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.

   Copie o certificado `http` interno do Elasticsearch (`<caminho_de_instalação_do_sentinel>/opt/novell/sentinel/3rdparty/elasticsearch/config/http.pks` no servidor Sentinel) gerado durante a instalação do Sentinel e adicione o caminho do certificado `http` do Elasticsearch copiado acima `<caminho do certificado copiado acima>/<nome do certificado>` quando ele solicitar o certificado externo.

   (Condicional) Se o Elasticsearch estiver no modo cluster, copie todos os nós externos do certificado `http` do Elasticsearch criado na seção Configurações em Elasticsearch para a Comunicação Segura em Cluster para o Collector Manager Remoto. Adicione o caminho do certificado `http` do Elasticsearch copiado acima `<caminho dos certificados copiados acima>/<nome dos certificados>` quando ele solicitar o certificado externo. Repita esta etapa para garantir que todos os certificados do Elasticsearch externos sejam adicionados.
5. Reinicie o Collector Manager ou o Correlation Engine.
6. Conclua a configuração do modo FIPS 140-2 seguindo as tarefas mencionadas no Capítulo 23, “Operando o Sentinel no modo FIPS 140-2” na página 129.

23 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 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 139.
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 139.
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 139.
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 139.
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 Collector Managers e Correlation Engines 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`.

- "Sentinel Link Integrator" na página 136
- "LDAP Integrator" na página 137
- "SMTP Integrator" na página 137
- "Integrador Syslog" na página 137
- "Usando conectores ativados não FIPS com o Sentinel no modo FIPS 140-2" na página 138

Agent Manager Connector

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 Agent Manager.

Para configurar o Agent Manager Connector 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 Agent Manager Connector*.
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 139.

   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 139.

3. Prossiga com a configuração do Conector.

Conector do Link do Sentinel

Siga o procedimento abaixo apenas se você tiver selecionado a opção **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 139.

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 139.

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 139.

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 139.

Sentinel Link Integrator

Siga o procedimento abaixo apenas se você tiver selecionado a opção **Criptografado (HTTPS)** ao configurar as definições da rede do Integrador do Sentinel Link.

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 precisará 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 139.

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 139.

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 Integrador, 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.cer` 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.cer` 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 Prossiga 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 65.

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 8.5.

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 139
- "Revertendo as instâncias do Collector Manager e do Correlation Engine remotos para o modo não FIPS" na página 140

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-fips201301241911135903 4887.tar.gz` for o arquivo de backup, execute o seguinte comando:

   `./backup_util.sh -f non-fips201301241911135903 4887.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.

24 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.

---

25 Limitando o número de sessões ativas simultâneas

No Sentinel 8.2 SP3 ou posterior, você pode limitar o número de sessões ativas simultâneas que deseja permitir por usuário, locatário ou ambos. Limitar o número de sessões impede que os invasores iniciem sessões além do limite permitido, no caso de um ataque.

Se você limitar as sessões por usuário e locatário, os usuários não poderão iniciar sessões depois que o número total de sessões iniciadas por vários usuários atingir o limite permitido para o locatário.

O Sentinel não limita as sessões simultâneas, por padrão. Você deve configurar esse limite manualmente.

Observação: Este recurso está disponível apenas no modo não MFA.

Para limitar o número de sessões ativas simultâneas:

1. Efetue login no servidor do Sentinel.
2. Abra o arquivo `/<caminho_de_instalação_do_sentinel>/etc/opt/novell/sentinel/config/configuration.properties`.
3. (Condicional) Para configurar o limite por locatário, defina a propriedade `concurrent.overall.sessions` para um valor necessário.
4. (Condicional) Para configurar o limite por usuário, defina a propriedade `concurrent.per.user.sessions` para um valor necessário.
5. Grave o arquivo.
6. Reinicie o servidor do Sentinel.

26 Encerrando sessões inativas

No Sentinel 8.2 SP3 ou posterior, você poderá configurar o Sentinel para encerrar uma sessão se não houver atividade do usuário por um período especificado. O Sentinel exibe um aviso um minuto antes do término da duração especificada. Se um usuário mantiver uma sessão inativa até essa duração, ele será desconectado pelo Sentinel.

O Sentinel não monitora a inatividade do usuário, por padrão. Você deve configurar manualmente o Sentinel para encerrar sessões inativas.

Para definir o período de tempo de espera de inatividade:

1. Efetue login no servidor do Sentinel.
2. Abra o arquivo `/<caminho_de_instalação_do_sentinel>/etc/opt/novell/sentinel/config/ui-configuration.properties`.
3. Defina o valor desejado para a propriedade `user.inactivity.time` em milissegundos.
4. Atualize o browser com o qual você efetuou login no Sentinel.

27 Configurando coleta de dados de Fluxo de IP

O Sentinel utiliza os ArcSight SmartConnectors, que ajudam a monitorar sua rede corporativa pela coleta de dados do Fluxo de IP. Os SmartConnectors coletam dados de Fluxo de IP como eventos, o que permite:

- Use as instâncias do Collector Manager existentes para coletar dados do Fluxo de IP.
- 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.

Para configurar a coleta de dados do Fluxo de IP, você deve instalar e configurar 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.

V Fazendo upgrade do Sentinel

Esta seção fornece informações sobre a atualização do Sentinel e outros componentes.

Importante

- Depois de fazer upgrade do Sentinel 8.3 ou anterior para o Sentinel 8.4, os painéis de controle personalizados do Kibana existentes não serão exibidos. Recrie o painel de controle personalizado após fazer upgrade para o Sentinel 8.4.
- Se o parâmetro Definir para Expirar não estiver definido nas partições antes do upgrade, a opção não poderá ser definida na partição restaurada após fazer upgrade para o Sentinel 8.4.
- Depois de fazer upgrade para o Sentinel 8.4 do Sentinel 8.3.1 ou anteriores, como o upgrade também atualiza os formatos de dados subjacentes, os dados de eventos existentes não estarão disponíveis para operações do Sentinel, como funcionalidades de pesquisa ou relatório. Para permitir que os dados sejam pesquisados, você deve reindexar todas as partições de dados de eventos no sistema após o upgrade. Para obter mais informações, consulte Reindexando partições de dados de eventos no Sentinel Administration Guide (Guia de Administração do Sentinel).
- Quando você estiver fazendo upgrade do servidor Sentinel, faça upgrade também dos sistemas do Collector Manager, dos sistemas do Correlation Engine, do servidor Sentinel de destino no integrador de links do Sentinel e do servidor Sentinel de destino no integrador Syslog para a mesma versão do servidor Sentinel. Caso contrário, você poderá enfrentar alguns problemas no sistema.

28 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 28-1 *Lista de verificação da implementação*

❒	Tarefas	Consulte
❒	Assegure que os computadores em que você instalará o Sentinel e seus componentes satisfaçam aos requisitos especificados.	Detalhes da versão do Sentinel 8.5
❒	Analise as notas de versão do sistema operacional compatível para entender os problemas conhecidos.	Notas de versão do SUSE
❒	Leia as notas de versão do Sentinel para ver as novas funcionalidades e entender os problemas conhecidos.	Notas de versão do Sentinel
❒	Conclua as tarefas mencionadas nos pré-requisitos.	Capítulo 29, “Pré-requisitos” na página 153

29 Pré-requisitos

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

Se você fez qualquer modificação no 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. Você pode definir o período de retenção para um valor desejado adicionando uma propriedade no arquivo `configuration.properties`. Para obter mais informações, consulte “Configuring the Retention Period for the Event Associations Data” (Configurando o período de retenção para os dados de associações de eventos) no *Sentinel Administration Guide* (Guia de Administração do Sentinel).

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.

30 Fazendo o upgrade da instalação tradicional do Sentinel

Os procedimentos deste capítulo guiam você durante o upgrade do Sentinel.

É possível fazer upgrade do Sentinel 8.2 ou posterior.

Importante: Se você estiver fazendo upgrade de versões anteriores do Sentinel 8.3.0.0, as etapas abaixo se aplicarão.

Importante: Quando estiver fazendo upgrade do servidor Sentinel, faça upgrade também dos sistemas do Collector Manager e dos sistemas do Correlation Engine para a mesma versão do servidor Sentinel. Caso contrário, você poderá enfrentar alguns problemas no sistema.

O processo de upgrade faz o seguinte:

- Migra dados de Inteligência de Segurança e dados de alertas do MongoDB para o PostgreSQL.

  O Sentinel agora armazena dados de Inteligência de Segurança, dados de alertas e assim por diante no PostgreSQL, em vez de no MongoDB. O processo de upgrade primeiro migrará esses dados para o PostgreSQL e, se for bem-sucedido, prosseguirá automaticamente com o upgrade. Se a migração de dados não for bem-sucedida, você não poderá fazer upgrade do Sentinel.
- Gera um script de limpeza que você pode usar para remover dados e RPMs relacionados ao MongoDB.
- Os dados armazenados no MongoDB são mantidos como um backup.

- "Fazendo upgrade do Sentinel" na página 155
- "Fazendo o upgrade do Sentinel como um usuário não root" na página 157
- "Fazendo o upgrade do Collector Manager ou do Correlation Engine" na página 159
- "Fazendo upgrade do sistema operacional" na página 160

Fazendo upgrade do Sentinel

Use as etapas a seguir para fazer upgrade do servidor Sentinel:

Para fazer upgrade do servidor do 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 xfz <install_filename>
```

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

6 Acesse o local descompactado do instalador, por exemplo:

```
cd /opt/sentinel_server-<version>*
```

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 **Importante:** Se você estiver fazendo upgrade de versões anteriores do Sentinel 8.3.0.0, as etapas abaixo se aplicarão.

10a (Condicional) Selecione a opção de migração necessária. Ela migra dados de Inteligência de Segurança e dados de Alertas do MongoDB para o PostgreSQL.

Se você selecionar a opção **Only upgrade without migrating data** (Fazer upgrade somente sem migrar dados), o servidor Sentinel deverá estar em funcionamento.

Aviso: Verifique se você selecionou a opção apropriada, pois não será possível repetir este procedimento depois que o upgrade for bem-sucedido.

Se os seus dados forem migrados com sucesso, os dados armazenados no MongoDB serão retidos como um backup e, em seguida, o processo de upgrade do Sentinel prosseguirá automaticamente.

Pode levar vários minutos até que o upgrade seja concluído.

10b (Condicional) Se a migração de dados não for bem-sucedida:

10b1 Limpe os dados parcialmente migrados. Para obter mais informações, consulte "Limpando dados do PostgreSQL quando há falha na migração" na página 175.

10b2 Repita de Etapa 7 a Etapa 10 acima até fazer upgrade do Sentinel.

11 (Condicional) Antes do upgrade, se a visualização do evento estiver habilitada, após o upgrade para o Sentinel 8.4.0.0, o Elasticsearch parará, pois estará habilitado com o plug-in de segurança X-Pack. Para iniciar o Elasticsearch, siga o procedimento em "Configurações no Elasticsearch para comunicação segura de cluster" na página 180.

12 Limpe o cache do browser da web para ver a última versão do Sentinel.

13 (Condicional) Se o arquivo `delete_old_cluster.sh` estiver localizado na pasta bin (`/opt/novell/sentinel/3rdparty/postgresql/bin`), o que significa que o banco de dados PostgreSQL recebeu upgrade para uma versão importante (por exemplo, 8.0 para 9.0). Limpe os arquivos PostgreSQL antigos do banco de dados PostgreSQL. O caminho da pasta pode ser diferente em caso de instalações com caminhos personalizados.

Para limpar os arquivos PostgreSQL antigos:

13a Alterne para o usuário novell:

```
su novell
```

13b Procure a pasta `bin`:

```
cd /opt/novell/sentinel/3rdparty/postgresql/bin
```

13c Apague os arquivos PostgresSQL antigos usando o seguinte comando:

```
./delete_old_cluster.sh
```

14 Efetue login no Sentinel e verifique se você consegue ver dados migrados, como alertas, dados de Inteligência de Segurança e assim por diante.

15 Os dados no MongoDB agora são redundantes porque o Sentinel 8.3 e posterior armazenam dados apenas no PostgreSQL. Para limpar o espaço em disco, apague esses dados. Para obter mais informações, consulte "Removendo dados do MongoDB" na página 179.

16 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 159.

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 usuário `root` no servidor em que você deseja fazer upgrade do Sentinel.

- Acesse o local descompactado do instalador, por exemplo:

  ```
  cd /opt/sentinel_server-8.4.0.0*
  ```

6 Extraia o RPM `squashfs` dos arquivos de instalação do Sentinel.

7 Instale o `squashfs` no servidor do Sentinel.

```
rpm -Uvh <install_filename>
```

8 Alterne para o usuário `novell`:

```
su novell
```

9 (Condicional) Para realizar um upgrade interativo:

9a Acesse o diretório de instalação do Sentinel e execute o seguinte comando:

```
./bin/root_install_prepare
```

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.

---

13 **Importante:** Se você estiver fazendo upgrade de versões anteriores do Sentinel 8.3.0.0, as etapas abaixo se aplicarão.

13a (Condicional) Selecione a opção de migração. Ela migra dados de Inteligência de Segurança e dados de Alertas do MongoDB para o PostgreSQL.

Aviso: Verifique se você selecionou a opção apropriada, pois não será possível repetir este procedimento depois que o upgrade for bem-sucedido.

Se os seus dados forem migrados com sucesso, os dados armazenados no MongoDB serão retidos como um backup e, em seguida, o processo de upgrade do Sentinel prosseguirá automaticamente.

Pode levar vários minutos até que o upgrade seja concluído.

13b (Condicional) Se a migração de dados não for bem-sucedida:

13b1 Limpe os dados migrados. Para obter mais informações, consulte "Limpando dados do PostgreSQL quando há falha na migração" na página 175.

13b2 Repita de Etapa 7 a Etapa 13 acima até fazer upgrade do Sentinel.

14 (Condicional) Antes do upgrade, se a visualização do evento estiver habilitada, após o upgrade para o Sentinel 8.4.0.0, o Elasticsearch parará, pois estará habilitado com o plug-in de segurança X-Pack. Para iniciar o Elasticsearch, siga o procedimento em "Configurações no Elasticsearch para comunicação segura de cluster" na página 180.

15 Limpe o cache do browser da web para ver a última versão do Sentinel.

16 (Condicional) Se o arquivo `delete_old_cluster.sh` estiver localizado na pasta bin (`/opt/novell/sentinel/3rdparty/postgresql/bin`), o que significa que o banco de dados PostgreSQL recebeu upgrade para uma versão importante (por exemplo, 8.0 para 9.0). Limpe os arquivos PostgreSQL antigos do banco de dados PostgreSQL. O caminho da pasta pode ser diferente em caso de instalações com caminhos personalizados.

Para limpar os arquivos PostgreSQL antigos:

16a Mude para o usuário novell.

```
su novell
```

16b Procure a pasta `bin`:

```
cd /opt/novell/sentinel/3rdparty/postgresql/bin
```

16c Apague os arquivos PostgresSQL antigos usando o seguinte comando:

```
./delete_old_cluster.sh
```

17 Efetue login no Sentinel e verifique se você consegue ver dados migrados, como alertas, dados de Inteligência de Segurança e assim por diante.

18 Os dados no MongoDB agora são redundantes porque o Sentinel 8.3 e posterior armazenam dados apenas no PostgreSQL. Para limpar o espaço em disco, apague esses dados. Para obter mais informações, consulte "Removendo dados do MongoDB" na página 179.

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 a serem usados durante o procedimento de upgrade do sistema operacional. Esses comandos garantem que o Sentinel funcione corretamente após o upgrade do sistema operacional. Antes de fazer upgrade do Sentinel, consulte os requisitos do sistema para compatibilidade. Para obter informações, consulte Sentinel System Requirements (Requisitos do Sistema do Sentinel).

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 Como usuário root, defina a propriedade `vm.max_map_count=262144` no arquivo `/etc/sysctl.conf`. Depois de adicionar a propriedade, execute `sysctl -p` para que as mudanças entrem em vigor.

7 (Condicional) Ao fazer upgrade para o SLES 15 SP1 ou SLES 15 SP2, o seguinte aviso é exibido:

```
aviso: Versão não suportada da chave: V3
```

Você pode ignorar o aviso ou executar uma solução alternativa para impedir que o aviso seja exibido. Para obter mais informações sobre a solução alternativa, consulte a documentação do SLES.

8 (Condicional) Se você usar o NSS (Mozilla Network Security Services), não serão instalados dois arquivos RPM dependentes: `libfreebl3-hmac` e `libsoftokn3-hmac`. Instale manualmente os seguintes arquivos RPM: `libfreebl3-hmac` e `libsoftokn3-hmac`.

9 (Condicional) Se você estiver fazendo upgrade do SLES12SP4 para o SLES15SP1 ou o SLES15SP2 no modo FIPS, primeiro deverá fazer upgrade do sistema operacional SLES, aplicar os patches mais recentes do sistema operacional e depois iniciar o Sentinel.

10 (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`

10a 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`

10b Execute o comando mencionado na Etapa 7 para verificar se não há erros.

11 Repita esse procedimento no seguinte:

- Instâncias do Collector Manager
- Instâncias do Correlation Engine

12 Reinicie o serviço do Sentinel:

```
rcsentinel restart
```

Esta etapa não é aplicável ao Sentinel HA.

Dependência da versão do Python para upgrade do Sentinel

O Sentinel exige o uso de versões compatíveis da biblioteca do Python para que o processo de upgrade seja bem-sucedido. Isso se torna muito importante quando você está fazendo upgrade de uma versão mais antiga do OS para uma nova versão do OS. Por exemplo, de um Sentinel baseado em SLES 11 SP4 para uma versão do OS do Sentinel baseada em SLES 15 SP2. Será uma boa ideia verificar sua versão do Python antes de iniciar o processo de upgrade do Sentinel. Se a versão do Python da caixa do Sentinel existente mudar após um upgrade do OS, será obrigatório seguir as etapas mencionadas abaixo.

Considere um cenário de exemplo.

Cenário: Upgrade do Sentinel 8.2 (baseado em SLES 11 SP4) para o Sentinel 8.4 (baseado em SLES 15 SP2).

No cenário acima, a execução de `python –V` na caixa do SLES 11 SP4 mostrou que a versão do Python usada era a 2.6.x. Esperamos que, após um upgrade do OS, a versão do Python seja atualizada para 2.7.x. Essa diferença pode potencialmente causar um problema de compatibilidade, que é mencionado abaixo.

Após o upgrade do sistema operacional e antes do upgrade da versão do Sentinel:

Como primeira etapa do upgrade, faça upgrade do OS do SLES 11 SP4 para o SLES 15 SP2. Ao fazer um upgrade do OS, existe a possibilidade de que uma versão superior da biblioteca do Python, como o Python 2.7.x, tenha sido instalada na caixa. Então, agora, executar o comando `python –V` mostra a versão do Python como 2.7.x. Mas, apesar de a máquina mostrar essa versão do Python, há uma boa possibilidade de que o arquivo de objeto compartilhado do Python (`plpython2.so`) que foi instalado com a versão anterior do Sentinel ainda possa apontar para uma versão 2.6.x do Python.

Execute o seguinte comando:

```
ldd <sentinel_installation_path>/opt/novell/sentinel/3rdparty/postgresql/
lib/postgresql/plpython2.so
```

A saída deste comando pode nos dizer em qual versão do Python o arquivo `plpython2.so` foi construído. Por exemplo, `libpython2.6.so.1.0 => /usr/lib64/libpython2.6.so.1.0` como saída indica que este arquivo `.so` baseia-se na versão 2.6.x do Python e não funcionará com uma versão 2.7.x.

Esse conflito poderá resultar na falha no processo de upgrade. Para resolver isso, você deverá substituir a versão mais antiga do arquivo `plpython2.so` (com base em 2.6.x) por uma versão mais recente do arquivo `plpython2.so` (com base em 2.7.x), de acordo com o cenário dado. Há uma boa chance de que essas versões do Python sejam diferentes em suas configurações, e você deve usar esses comandos de acordo.

Para isso, siga as etapas abaixo:

1. Pare o Sentinel usando o comando abaixo:

   ```
   rcsentinel stop
   ```

2. Alterne para o diretório no qual está o arquivo `plpython2.so`:

   ```
   cd <sentinel_installation_path>/opt/novell/sentinel/3rdparty/
   postgresql/lib/postgresql
   ```

3. Remova o arquivo `.so` existente que está apontando para 2.6.x, usando o seguinte comando:

   ```
   rm plpython2.so
   ```

4. Descompacte o arquivo `2.7.x.so` do Python (ele deve estar no diretório `<caminho_de_instalação_do_sentinel>/opt/novell/sentinel/3rdparty/postgresql/lib/postgresql`):

   ```
   tar zxf plpython2.7.so.tar.gz
   ```

5. Defina a permissão de usuário `novell` para o arquivo:

   ```
   chown novell:novell plpython2.so
   ```

6. Verifique se o arquivo está apontando para a versão Python correta (a saída agora deve estar apontando para a versão 2.7.x) usando o comando abaixo:

   ```
   ldd <sentinel_installation_path>/opt/novell/sentinel/3rdparty/
   postgresql/lib/postgresql/plpython2.so
   ```

   Depois de concluir as etapas acima e garantir que o arquivo `plpython2.so` esteja apontando para a versão certa do Python, prossiga com o processo de upgrade do Sentinel.

31 Fazendo upgrade da aplicação Sentinel

Os procedimentos deste capítulo guiam você durante o upgrade da aplicação do Sentinel.

O Sentinel na versão 8.3.0.0 e posteriores usa o PostgreSQL em vez do MongoDB para armazenar dados de Inteligência de Segurança e dados de alertas. Você pode fazer upgrade da aplicação depois de migrar dados do MongoDB para o PostgreSQL com êxito.

Os dados armazenados no MongoDB serão mantidos como um backup e você poderá apagá-los após o upgrade do Sentinel.

Importante: Quando estiver fazendo upgrade do servidor Sentinel, faça upgrade também dos sistemas do Collector Manager e dos sistemas do Correlation Engine para a mesma versão do servidor Sentinel. Caso contrário, você poderá enfrentar alguns problemas no sistema.

Pré-requisitos para fazer upgrade da aplicação

Antes de fazer upgrade, você deve satisfazer os seguintes pré-requisitos:

1. Você precisa ter o Sentinel 8.2 ou posterior instalado.
2. Você precisa ter o SLES 12 SP3 ou SLES 12 SP4 instalado.
   a. (Condicional) Se você está no SLES 11 SP4 com o Sentinel 8.2.0.0, recomenda-se obter todas as atualizações do canal no SLES 11. Em seguida, faça upgrade do OS para SLES 12 SP3. Para obter mais informações sobre o upgrade do sistema operacional SLES, consulte "Upgrade do Sistema Operacional para SLES 12 SP3" na página 164. Faça download do utilitário pós-upgrade do site do Micro Focus Patch Finder e execute-o.
   b. (Condicional) Se você está no SLES 12 SP3 com o Sentinel 8.2.0.0 e executou o utilitário pós-upgrade `sentinel_sles_iso_os_post_upgrade-release-73.tar.gz`, então precisa fazer download do utilitário pós-upgrade `sentinel_sles_iso_os_post_upgrade-release-85.tar.gz` do site do Micro Focus Patch Finder e executá-lo.
   c. (Condicional) Se você está no SLES 12 SP3 com o Sentinel 8.2.0.0 e executou o utilitário pós-upgrade `sentinel_sles_iso_os_post_upgrade-release-85.tar.gz` do site do Micro Focus Patch Finder, siga as etapas de "Fazendo upgrade da aplicação" na página 167.

---

3. **Importante:** Se você está na versão com upgrade do Sentinel 8.3.0.0 ou na instalação recente de 8.3.0.0, siga as etapas de "Fazendo upgrade da aplicação" na página 167.

(Condicional) Migre dados de Inteligência de Segurança, dados de alertas e assim por diante do MongoDB para o PostgreSQL. Você poderá executar essa etapa somente após completar os pré-requisitos anteriores. Para mais informações sobre migração de dados, "Migrando dados do MongoDB para o PostgreSQL" na página 166.

Você precisará executar o script de migração mesmo quando não tiver dados para migrar, porque o script de migração gera um script de limpeza. Você poderá usar o script de limpeza para remover os dados do MongoDB que serão redundantes após o upgrade do Sentinel.

Upgrade do Sistema Operacional para SLES 12 SP3

Você precisa fazer upgrade do sistema operacional pelo seguinte motivo:

- O Sentinel agora está disponível apenas no canal do SLES 12. Portanto, para continuar recebendo as atualizações do sistema operacional e do Sentinel, você deve primeiro fazer upgrade do sistema operacional para SLES 12 SP3 antes de fazer upgrade do Sentinel.
- Você pode aproveitar os recursos do Sentinel Appliance Manager. O Sentinel Appliance Manager fornece uma interface do usuário simples com base na Web que ajuda você a configurar e gerenciar a aplicação.

Para fazer upgrade do sistema operacional e configurar a aplicação:

1. Pare os serviços do Sentinel:

   ```
   rcsentinel stop
   ```

2. (Condicional) Se o Sentinel estava no modo FIPS antes do upgrade do sistema operacional, é 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
   ```

3. (Condicional) Se você estiver usando 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`.
4. 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.
5. 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.

Importante: Você será solicitado a se registrar no SLES 12 SP3 durante o upgrade. Porém, ignore o processo de registro. O registro de atualizações nesta tela registrará apenas as atualizações do SLES 12 SP3 no SUSE Customer Channel, que não é suportado. Além disso, você não receberá atualizações do Sentinel. Portanto, registre-se para atualizações somente após concluir a Etapa 9 para receber as atualizações do Sentinel e do SLES 12 SP3 do canal de atualização da aplicação Sentinel.

6 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
```

7 (Condicional) Para o HA do Sentinel, conclua as etapas mencionadas nas seções a seguir:

- “Configurando destinos iSCSI” na página 231
- “Configurando iniciadores iSCSI” na página 233
- “Configurando o cluster de HA” na página 233

8 Para configurar a aplicação, execute o utilitário pós-upgrade no prompt de comando:

8a Descompacte o arquivo:

```
tar -xvf <post upgrade utility installer filename>.tar.gz
```

8b Mude para o diretório no qual extraiu o utilitário:

```
cd <post upgrade utility installer filename>
```

8c 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.

8d Siga as instruções na tela para concluir a configuração.

Este script reconfigura os pacotes instalados e configura os pacotes para gerenciar a aplicação.

9 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 “Registrando para receber atualizações” na página 92.

Migrando dados do MongoDB para o PostgreSQL

Você deve migrar os dados de Inteligência de Segurança, dados de alertas e assim por diante do MongoDB para o PostgreSQL executando o script de migração.

O script de migração faz o seguinte:

- Migra dados de Inteligência de Segurança e dados de alertas para o PostgreSQL.
- Gera um script de limpeza que você pode usar para remover dados e RPMs relacionados ao MongoDB do MongoDB.

Aviso: Após migrar os dados, você deverá fazer upgrade do Sentinel antes de iniciar ou reiniciar o Sentinel. Isso garante que não haja perda de dados no Sentinel.

Para migrar dados:

1. Faça download do `Mongo_To_PostgreSQL_Migration_Utility_8.3.0.0-5575.tar.gz` do Site de downloads.
2. Descompacte os arquivos.
3. Efetue login no console da aplicação como um usuário `novell`.

   Importante: Execute o script de migração do terminal da máquina. Não use um software de terminal de emulação como PuTty ou MobaXterm.

   ---

4. Execute o seguinte script: `mongo_to_pgsql_migration.sh`.
5. Selecione a opção de migração conforme seus requisitos.

   Aviso: Verifique se você selecionou a opção apropriada, porque você não poderá repetir este procedimento depois que a migração tiver sido bem-sucedida.

   Se seus dados forem migrados com sucesso, uma mensagem de confirmação será exibida na tela. Agora você pode fazer upgrade da aplicação.
6. (Condicional) Se a migração de dados não for bem-sucedida:
   - **6a** Limpe os dados migrados. Para obter mais informações, consulte “Limpando dados do PostgreSQL quando há falha na migração” na página 175.
   - **6b** Repita esse procedimento para migrar dados.

7 (Condicional) Se você vir o seguinte erro ao executar o script de migração, conclua as tarefas mencionadas em "Não é possível executar o script de migração" na página 176:

```
 8101server:/opt # su novell
novell@8101server:/opt>
novell@8101server:/opt> ./mongo_to_pgsql_migration.sh
./mongo_to_pgsql_migration.sh: line 25: /bin/setenv.sh: No such file or
directory
Cannot execute ./mongo_to_pgsql_migration.sh as novell
novell@8101server:/opt>
novell@8101server:/opt> exit
exit
8101server:/opt #
8101server:/opt # ./mongo_to_pgsql_migration.sh
./mongo_to_pgsql_migration.sh: line 25: /bin/setenv.sh: No such file or
directory
Cannot execute ./mongo_to_pgsql_migration.sh as root
```

Fazendo upgrade da aplicação

Você pode fazer upgrade do Sentinel e do sistema operacional SLES por meio do Canal de Atualização da Aplicação ou do SMT (Subscription Management Tool). Você deve primeiro satisfazer os pré-requisitos listados em "Pré-requisitos para fazer upgrade da aplicação" na página 163 e, então, fazer upgrade da aplicação.

- "Fazendo upgrade por meio do Canal de Atualização da Aplicação" na página 167
- "Fazendo upgrade por meio do SMT" na página 170
- "Executando atualizações offline" na página 171

Fazendo upgrade 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 upgrade da aplicação do prompt de comando:

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 Efetue login na máquina da aplicação e abra um prompt de comando como usuário `root`.

4 Execute os seguintes comandos no prompt de comando:

Importante: Ignore a mensagem/prompt de reinicialização até Etapa 6 na página 168. É importante iniciar o Sentinel (etapa 4c) antes de reinicializar a máquina.

4a `zypper -v patch`

4b `zypper up`

4b1 Digite S para continuar.

4c (Condicional) Antes do upgrade, se a visualização do evento estiver habilitada, após o upgrade para o Sentinel 8.4.0.0, o Elasticsearch parará, pois estará habilitado com o plug-in de segurança X-Pack. Para iniciar o Elasticsearch, siga o procedimento em "Configurações no Elasticsearch para comunicação segura de cluster" na página 180.

4d `rcsentinel start`

5 Abra o arquivo `/etc/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
```

6 Reinicialize a aplicação.

7 (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
```

8 Limpe o cache do browser da web para ver a última versão do Sentinel.

9 (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.

9a Alterne para o usuário da Novell.

```
su novell
```

9b Procure a pasta `bin`:

```
cd /opt/novell/sentinel/3rdparty/postgresql/bin
```

9c Apague os arquivos postgresSQL antigos usando o seguinte comando:

```
./delete_old_cluster.sh
```

10 (Condicional) Para fazer o upgrade do Collector Manager ou do Correlation Engine, siga Etapa 3 até Etapa 7.

11 (Condicional) Se você estiver executando o Sentinel em um ambiente de alta disponibilidade, repita essas etapas em todos os nós do cluster.

12 Reinicie o Sentinel.

13 Efetue login no Sentinel e verifique se você consegue ver os dados migrados, como alertas, dados de Inteligência de Segurança e assim por diante.

14 Os dados no MongoDB agora são redundantes porque o Sentinel 8.3 e posterior armazenam dados apenas no PostgreSQL. Para limpar o espaço em disco, apague esses dados. Para obter mais informações, consulte "Removendo dados do MongoDB" na página 179.

Para fazer upgrade da aplicação por meio do Sentinel Appliance Manager:

1 Inicie a aplicação Sentinel fazendo um dos procedimentos a seguir:

- Efetue login no Sentinel. Clique em **Sentinel Main** > **Appliance** (Principal do Sentinel > Aplicação).
- Especifique o URL a seguir no browser da web: `https://<endereço_IP>:9443`.

2 Efetue login como um `vaadmin` ou um usuário `root`.

3 (Condicional) Registre-se para obter atualizações, caso ainda não tenha feito isso. Para obter mais informações, consulte "Registrando para receber atualizações" na página 92.

Observação: Para o Sentinel 8.3.1, além da etapa 4 e da etapa 5, é necessária uma etapa 6 adicional.

---

4 Clique em **Online Update** (Atualização Online).

Observação: Não reinicialize o sistema até que todas as etapas abaixo estejam concluídas.

---

5 Para instalar as atualizações exibidas, clique em **Update Now** > **OK** (Atualizar Agora > OK).

6 Execute o seguinte comando no prompt de comando:

Importante: Ignore a mensagem/prompt de reinicialização até a etapa 7. É importante iniciar o Sentinel antes de reinicializar a máquina.

- zypper up
- (Condicional) Antes do upgrade, se a visualização do evento estiver habilitada, após o upgrade para o Sentinel 8.4.0.0, o Elasticsearch parará, pois estará habilitado com o plug-in de segurança X-Pack. Para iniciar o Elasticsearch, siga o procedimento em "Configurações no Elasticsearch para comunicação segura de cluster" na página 180.
- rcsentinel start

7 Para aplicar as atualizações instaladas, clique em **Reinicializar**.

8 Efetue login no Sentinel e verifique se você consegue ver os dados migrados, como alertas, dados de Inteligência de Segurança e assim por diante.

9 Os dados no MongoDB agora são redundantes porque o Sentinel 8.3 e posterior armazenam dados apenas no PostgreSQL. Para limpar o espaço em disco, você pode apagar esses dados. Para obter mais informações, consulte "Removendo dados do MongoDB" na página 179.

Fazendo upgrade por meio do SMT

Em ambientes seguros, em que a aplicação deve ser executada sem acesso direto à Internet, configure a aplicação com o SMT (Subscription Management Tool), que permite que você faça upgrade da aplicação para as versões mais recentes disponíveis.

Para fazer upgrade da aplicação por meio do SMT:

1. Certifique-se de que o aplicativo esteja configurado com SMT.

   Para obter mais informações, consulte "Configurando a aplicação com SMT" na página 94.

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. (Condicional) Antes do upgrade, se a visualização do evento estiver habilitada, após o upgrade para o Sentinel 8.4.0.0, o Elasticsearch parará, pois estará habilitado com o plug-in de segurança X-Pack. Para iniciar o Elasticsearch, siga o procedimento em "Configurações no Elasticsearch para comunicação segura de cluster" na página 180.

11. Abra o arquivo `/etc/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
```

12 Reinicie a aplicação.

```
rcsentinel restart
```

13 (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
```

14 (Condicional) Para fazer o upgrade do Collector Manager ou do Correlation Engine, siga Etapa 4 até Etapa 13.

15 (Condicional) Se você estiver executando o Sentinel em um ambiente de alta disponibilidade, repita essas etapas em todos os nós do cluster.

16 Reinicie o Sentinel.

17 Efetue login no Sentinel e verifique se você consegue ver os dados migrados, como alertas, dados de Inteligência de Segurança e assim por diante.

18 Os dados no MongoDB agora são redundantes porque o Sentinel 8.3 e posterior armazenam dados apenas no PostgreSQL. Para liberar espaço em disco, você pode apagar esses dados. Para obter mais informações, consulte “Removendo dados do MongoDB” na página 179.

Executando atualizações offline

Você pode executar uma atualização offline fazendo download offline do Patch ISO para cada aplicação.

Atualização offline da aplicação em ambiente seguro

Ao aplicar o patch, se encontrar problemas de registro/repositório, você poderá tentar limpar as entradas de registro e do repositório em seu sistema.

Para limpar os detalhes do registro e do repositório na aplicação, execute as seguintes etapas:

1. Faça um backup dos arquivos antes de limpar as entradas do registro:
   a. Crie um diretório de backup. Por exemplo:

      ```
      mkdir /etc/zypp/backup
      ```

   b. Copie os seguintes arquivos de registro para o diretório de backup. Por exemplo:

      ```
      cp /etc/zypp/credentials.d /etc/zypp/backup
      cp /etc/zypp/repos.d/*     /etc/zypp/backup
      cp /etc/zypp/services.d/*  /etc/zypp/ backup
      ```

2. Apague os seguintes arquivos do registro:

   ```
   rm -fr /etc/zypp/credentials.d
   ```

```
rm -fr /etc/zypp/repos.d/*

rm -fr /etc/zypp/services.d/*
```

Aplicando o Patch ISO

Execute estas etapas:

1. Faça download do patch ISO para um diretório. Por exemplo: `<nome do diretório>/PatchCD-Sentinel-Server-<número do build da versão>-SLES12-SP5-<data e hora>.iso`
2. Crie um diretório para montar o patch ISO usando o seguinte comando. Por exemplo:

   ```
   mkdir -p /opt/trial
   ```

3. Monte o patch ISO usando o seguinte comando. Por exemplo:

   ```
   mount -o loop <directoryname>/PatchCD-Sentinel-Server-<version-build number>-SLES12-SP5-<datetime>.iso /opt/trial
   ```

4. Adicione os repositórios do produto e do sistema operacional. Por exemplo:

   ```
   zypper ar -c -t plaindir "/opt/trial/product-repo" "<product repository>"

   zypper ar -c -t plaindir "/opt/trial/osupdate-repo" "<operating system repository>"
   ```

5. (Opcional) Confirme se os repositórios foram adicionados com sucesso usando o seguinte comando:

   ```
   zypper repos
   ```

6. Verifique se os patches estão em bundle no patch ISO usando o seguinte comando:

   ```
   zypper lp
   ```

7. Aplique todas as atualizações usando os seguintes comandos:

   ```
   zypper -v patch

   zypper -v update
   ```

8. Limpe a lista de repositórios usando os seguintes comandos:

   ```
   zypper rr "<product repository>"

   zypper rr "<operating system repository>"
   ```

9. Após a conclusão da atualização, reinicialize a máquina usando o seguinte comando:

   ```
   reboot
   ```

Aplicando patches do sistema operacional

Para aplicar patches do sistema operacional:

1. Inicie a aplicação Sentinel fazendo um dos procedimentos a seguir:
   - Efetue login no Sentinel. Clique em **Sentinel Main** > **Appliance** (Principal do Sentinel > Aplicação).
   - Especifique o URL a seguir no browser da web: `https://<endereço_IP>:9443`.
2. Efetue login como um `vaadmin` ou um usuário `root`.
3. Clique em **Atualização Online**.
   - **3a** (Condicional) Registre-se para obter atualizações, caso ainda não tenha feito isso. Para obter mais informações, consulte "Registrando para receber atualizações" na página 92.
   - **3b** Para instalar as atualizações exibidas para o sistema operacional, clique em **Atualizar Agora** > **OK**.
4. Para aplicar as atualizações instaladas, clique em **Reinicializar**.

32 Solução de problemas

Limpando dados do PostgreSQL quando há falha na migração

Se a migração falhar, você deverá apagar os dados que foram parcialmente movidos para o banco de dados PostgreSQL e executar o script de migração novamente.

Aviso: Não execute esse procedimento se a migração for bem-sucedida. Este script apaga todos os dados migrados.

Para limpar os dados parcialmente migrados:

1. Verifique se o banco de dados PostgreSQL está ativo e em execução.
2. Efetue login no servidor do Sentinel como o usuário `novell`.
3. Vá para o local em que você extraiu o instalador do Sentinel ou o utilitário de migração.
4. Execute o script `./db_migration_failure_cleanup.sh` para apagar os dados parcialmente migrados.
5. Execute o comando `rm db_migration_failure_cleanup.sh` para apagar o arquivo `db_migration_failure_cleanup.sh`.

   Para continuar com o upgrade tradicional, consulte Capítulo 30, “Fazendo o upgrade da instalação tradicional do Sentinel” na página 155.

   Para continuar com o upgrade da aplicação, migre dados do MongoDB para o PostgreSQL. Para obter informações, veja “Migrando dados do MongoDB para o PostgreSQL” na página 166.

Não é possível executar o script de migração

Você pode ver o seguinte erro ao executar o script de migração para mover dados para o PostgreSQL:

```
8101server:/opt # su novell
novell@8101server:/opt>
novell@8101server:/opt> ./mongo_to_pgsql_migration.sh
./mongo_to_pgsql_migration.sh: line 25: /bin/setenv.sh: No such file or
directory
Cannot execute ./mongo_to_pgsql_migration.sh as novell
novell@8101server:/opt>
novell@8101server:/opt> exit
exit
8101server:/opt #
8101server:/opt # ./mongo_to_pgsql_migration.sh
./mongo_to_pgsql_migration.sh: line 25: /bin/setenv.sh: No such file or
directory
Cannot execute ./mongo_to_pgsql_migration.sh as root
```

Esse erro poderá ocorrer se você tiver feito upgrade da aplicação para o Sentinel 8.2 de uma versão anterior, pois o `bashrc` pode ter sido modificado durante um upgrade anterior.

Para evitar esse erro, você deve atualizar o arquivo `bashrc`.

Para atualizar o arquivo bashrc:

1. Abra o arquivo `bashrc`:

   `/home/novell/.bashrc`

2. (Condicional) Se o arquivo não incluir as seguintes propriedades, adicione-as:

   ```
   APP_HOME="/opt/novell/sentinel"
   export PATH="$APP_HOME/bin:$APP_HOME/bin/actions:$PATH"
   ```

3. Execute o script de migração novamente. Para obter mais informações, consulte “Migrando dados do MongoDB para o PostgreSQL” na página 166.

Não é possível conectar-se a servidores ou outros componentes por meio da aplicação

As instalações anteriores do Sentinel podem incluir o IP. endereço como 127.0.0.2 no arquivo `/etc/hosts` se você escolheu a opção **Atribuir nome do host ao endereço de loopback** durante a instalação. Isso pode causar problemas de comunicação com outros servidores ou componentes. Você deve editar o arquivo e remover este endereço IP.

Para remover o endereço IP:

1. Abra o arquivo `/etc/hosts`.
2. Comente a entrada do endereço IP 127.0.0.2.
3. Grave o arquivo.

Erro ao fazer upgrade da aplicação

Quando você estiver fazendo upgrade da aplicação e tiver feito upgrade de uma versão anterior para a 8.2 ou posterior, poderá ver o seguinte erro:

```
(104/134) Installing: kernel-default-4.12.14-95.45.1.x86_64
.....................................................................
.............[error]
Installation of kernel-default-4.12.14-95.45.1.x86_64 failed:
Error: Subprocess failed. Error: RPM failed:    installing package kernel-
default-4.12.14-95.45.1.x86_64 needs 4MB on the /boot filesystem
```

Esse é um problema conhecido no sistema operacional SUSE e não no Sentinel. Portanto, para resolver esse problema, siga a solução alternativa fornecida na documentação do SUSE.

Erro ao adicionar uma senha ao keystore do Elasticsearch na configuração do upgrade

A mensagem de erro `FileAlreadyExistsException` é exibida enquanto o comando abaixo é executado na configuração do upgrade:

```
./bin/elasticsearch-keystore add
xpack.security.transport.ssl.keystore.secure_password
```

Solução temporária:

1. Alterne para o usuário `novell`:

   ```
   su novell
   ```

2. Apague o arquivo `<caminho_de_instalação_do_sentinel>/opt/novell/sentinel/3rdparty/elasticsearch/config/elasticsearch.keystore.tmp`.
3. Apague o certificado `<caminho_de_instalação_do_sentinel>/opt/novell/sentinel/3rdparty/elasticsearch/config/http.pks` e execute o seguinte comando para regenerar o certificado:

   ```
   <sentinel_installation_path>/opt/novell/sentinel/bin/javacert.sh --
   generateES <sentinel_installation_path>/opt/novell/sentinel/3rdparty/
   elasticsearch/config/http.pks <password> <keyalias>
   ```

4. Execute o seguinte comando em `<caminho_de_instalação_do_sentinel>/opt/novell/sentinel/3rdparty/elasticsearch` para adicionar a senha do certificado criado na etapa acima ao keystore do Elasticsearch:

   ```
   ./bin/elasticsearch-keystore add
   xpack.security.http.ssl.keystore.secure_password
   ```

5. Consulte “Habilitando a visualização do evento no Sentinel” na página 109 e realize a etapa 5 até a etapa 11 para configurar o Elasticsearch.
6. Reinicie o Sentinel:

   ```
   rcsentinel restart
   ```

Não é possível ver alertas mais antigos no painel de controle nem visualizações de alerta após a configuração do Elasticsearch

Depois de configurar o Elasticsearch, o painel de controle de alerta e os gráficos na tela de alerta não atualizam ou exibem alertas antigos. No entanto, a tabela na tela de alerta exibe os alertas recém-gerados. Este problema pode acontecer por causa de um índice de alerta corrupto.

Solução temporária: Execute as seguintes etapas:

1. Vá para o diretório `<caminho_de_instalação_do_sentinel>/var/opt/novell/sentinel/bin`.
2. Para alternar para o usuário `novell`, execute o seguinte comando:

   ```
   su novell
   ```

3. Para iniciar o processo de sincronização de alerta, execute o seguinte comando:

   ```
   ./reSyncAlert.sh
   ```

33 Configurações Pós-Upgrade

Este capítulo inclui as configurações pós-upgrade.

Removendo dados do MongoDB

Depois de fazer upgrade do Sentinel, você não precisará dos dados armazenados no MongoDB. Você pode apagar esses dados para liberar espaço em disco.

Para liberar espaço do armazenamento:

1. Efetue login no servidor do Sentinel como usuário `root`.
2. Vá para `<caminho_de_instalação_do_sentinel>/opt/novell/sentinel/bin`.
3. Execute o script a seguir:

   `./mongoDB_cleanup.sh`

Sincronizando o arquivo postgresql.conf

Durante o upgrade, o arquivo `postgresql.conf` de uma versão anterior é renomeado como `postgresql.conf_old`. Um novo arquivo `postgresql.conf` é criado para 8.3. O novo arquivo `postgresql.conf` contém configurações para melhorar o desempenho do painel de controle de Inteligência de Segurança. Portanto, você precisa manter esse arquivo. Caso suas personalizações não estejam incluídas no novo arquivo, edite o novo arquivo `postgres.sql`. Os dois arquivos estão no seguinte local: `/var/opt/novell/sentinel/3rdparty/postgresql/data/`

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 42.

Configurações no Elasticsearch para comunicação segura de cluster

O Sentinel, nas versões 8.4.0.0 e acima, vem com recursos de segurança aprimorados de fábrica, para os quais são necessárias algumas configurações pós-instalação/upgrade. A partir da versão 8.4.0.0, o Sentinel comunica-se com o Elasticsearch de modo seguro (por SSL) e tem o plug-in X-Pack de Elasticsearch empacotado nele por padrão. Isso dará ao administrador do Sentinel a capacidade de configurar todas as comunicações do Elasticsearch **nó**-a-**nó** de modo seguro e por SSL. Isso abrirá a possibilidade de armazenar os dados nos nós do Elasticsearch entre geografias e ainda permitir que os dados sejam passados e visualizados com segurança por um servidor Sentinel. Ao utilizar esse recurso, um usuário agora pode ingressar em todos os seus clusters do Elasticsearch espalhados pelo mundo e ainda é capaz de ver e acumular os resultados com segurança de um único console de pesquisa do Sentinel.

Importante: Para que o processo de upgrade seja concluído, a execução das etapas abaixo é obrigatória. Os detalhes desta página só serão aplicáveis se o recurso de visualização do evento for habilitado antes do upgrade para as versões Sentinel 8.4 ou Sentinel 8.5 a partir de uma versão mais antiga do Sentinel.

Se você estiver fazendo upgrade do Sentinel 8.4 para o Sentinel 8.5, as etapas abaixo não deverão ser executadas.

Sem realizar as etapas abaixo, o upgrade para o Sentinel 8.4.0.0 ou superior de uma versão mais antiga estará incompleta e terá os seguintes problemas:

- O Elasticsearch não será iniciado automaticamente.
- Se o Elasticsearch não for reiniciado manualmente, alertas e eventos presentes nele não serão corretamente refletidos durante a pesquisa no Sentinel.

Habilitando a comunicação segura entre o Servidor Sentinel e o Elasticsearch pré-empacotado quando não houver configuração de cluster externo do Elasticsearch

Esta seção é necessária para casos em que você não tenha um cluster do Elasticsearch externo associado ao Sentinel. Nesse caso, você só precisa habilitar uma comunicação segura entre o Sentinel e o Elasticsearch pré-empacotado.

1. Pare o serviço interno do Elasticsearch usando o comando abaixo:

   ```
   rcsentinel stopES
   ```

2. Alterne para o usuário `novell`:

   ```
   su novell
   ```

   Execute as etapas 3 e 4 se a versão java for 292. Para encontrar a versão java no nível do OS, execute `java -version` no prompt de comando.

3. (Condicional) Defina JAVA_HOME como o JDK do Sentinel em “bundle”:

   ```
   JAVA_HOME=/opt/novell/sentinel/jdk
   ```

4. (Condicional) Defina PATH para java como o local do JDK do Sentinel:

   ```
   PATH=$JAVA_HOME/bin:$PATH
   ```

5. Gere uma CA (Autoridade de Certificação) para o seu cluster no nó do Sentinel. Execute o seguinte comando no diretório pessoal do Elasticsearch `<caminho_de_instalação_do_sentinel>/opt/novell/sentinel/3rdparty/elasticsearch` do Sentinel:

   ```
   ./bin/elasticsearch-certutil ca
   ```

   São solicitados o nome do arquivo e uma senha do certificado CA. Aqui o nome do arquivo padrão é `elastic-stack-ca.p12`.

6. Gere os certificados e as chaves privadas para o nó do Elasticsearch pré-empacotado do Sentinel. Para isso, execute o seguinte comando no diretório pessoal do Elasticsearch `<caminho_de_instalação_do_sentinel>/opt/novell/sentinel/3rdparty/elasticsearch` do Sentinel:

   ```
   ./bin/elasticsearch-certutil cert --ca <CA certificate filename>.p12 --out config/certs/node-1.p12
   ```

   É solicitada a senha do seu certificado CA. Você também precisa criar uma senha para o certificado gerado.

7. Adicione as seguintes configurações no arquivo `<caminho_de_instalação_do_sentinel>/opt/novell/sentinel/3rdparty/elasticsearch/config/elasticsearch.yml` no nó do Sentinel:

   - `xpack.security.transport.ssl.enabled: true`
   - `xpack.security.transport.ssl.keystore.path: certs/node-1.p12`
   - `xpack.security.transport.ssl.truststore.path: certs/node-1.p12`
   - `xpack.security.transport.ssl.verification_mode: certificate`

8 Armazene a senha do arquivo de certificado `truststore` e `keystore` gerado acima no keystore do Elasticsearch. Para isso, execute os seguintes comandos no diretório pessoal do Elasticsearch: `<caminho_de_instalação_do_sentinel>/opt/novell/sentinel/3rdparty/elasticsearch` do Sentinel:

```
./bin/elasticsearch-keystore add
xpack.security.transport.ssl.keystore.secure_password
```

```
./bin/elasticsearch-keystore add
xpack.security.transport.ssl.truststore.secure_password
```

9 Inicie o serviço do Elasticsearch usando o comando abaixo:

```
rcsentinel startES
```

Habilitando a comunicação segura entre nós externos do Elasticsearch, bem como entre o Sentinel e o cluster do Elasticsearch se houver uma configuração de cluster externo do Elasticsearch

A versão mais recente do Sentinel habilita a comunicação segura entre o servidor Sentinel e o cluster externo do Elasticsearch, bem como entre diferentes nós do cluster do Elasticsearch. Esta seção explica as etapas sobre como habilitar essas configurações seguras para casos em que você tem um cluster externo do Elasticsearch conectado ao servidor Sentinel.

1 **Etapas a serem seguidas para garantir a comunicação dentro do cluster entre nós do Elasticsearch:**

1. Pare o Elasticsearch em todos os nós.
2. Alterne para o usuário `novell`:

   ```
   su novell
   ```

   Execute as etapas 3 e 4 se a versão java for 292. Para encontrar a versão java no nível do OS, execute `java -version` no prompt de comando.
3. (Condicional) Defina JAVA_HOME como o JDK do Sentinel em “bundle”:

   ```
   JAVA_HOME=/opt/novell/sentinel/jdk
   ```
4. (Condicional) Defina PATH para java como o local do JDK do Sentinel:

   ```
   PATH=$JAVA_HOME/bin:$PATH
   ```
5. Gere uma CA (Autoridade de Certificação) para o seu cluster no nó do Sentinel. Execute o seguinte comando no diretório pessoal do Elasticsearch `<caminho_de_instalação_do_sentinel>/opt/novell/sentinel/3rdparty/elasticsearch` do Sentinel:

   ```
   ./bin/elasticsearch-certutil ca
   ```

   São solicitados o nome do arquivo e uma senha do certificado CA. Aqui o nome do arquivo padrão é `elastic-stack-ca.p12`.
6. Gere os certificados e as chaves privadas para o nó do Elasticsearch pré-empacotado do Sentinel. Para isso, execute o seguinte comando no diretório pessoal do Elasticsearch `<caminho_de_instalação_do_sentinel>/opt/novell/sentinel/3rdparty/elasticsearch` do Sentinel:

   ```
   ./bin/elasticsearch-certutil cert --ca <CA certificate
   filename>.p12 --out config/certs/node-1.p12
   ```

É solicitada a senha do seu certificado CA. Você também precisa criar uma senha para o certificado gerado.

7. Adicione as seguintes configurações no arquivo `<caminho_de_instalação_do_sentinel>/opt/novell/sentinel/3rdparty/elasticsearch/config/elasticsearch.yml` no nó do Sentinel:
   - `xpack.security.transport.ssl.enabled: true`
   - `xpack.security.transport.ssl.keystore.path: certs/node-1.p12`
   - `xpack.security.transport.ssl.truststore.path: certs/node-1.p12`
   - `xpack.security.transport.ssl.verification_mode: certificate`
8. Armazene a senha do arquivo de certificado `truststore` e `keystore` gerado acima no keystore do Elasticsearch. Para isso, execute os seguintes comandos no diretório pessoal do Elasticsearch: `<caminho_de_instalação_do_sentinel>/opt/novell/sentinel/3rdparty/elasticsearch` do Sentinel:

   ```
   ./bin/elasticsearch-keystore add
   xpack.security.transport.ssl.keystore.secure_password
   ```

   ```
   ./bin/elasticsearch-keystore add
   xpack.security.transport.ssl.truststore.secure_password
   ```

9. Gere os certificados para todos os nós externos do Elasticsearch no cluster. Você pode primeiro criar todos os certificados externos do Elasticsearch no próprio nó do Sentinel e, em seguida, copiá-los para os respectivos nós do Elasticsearch. Para isso, primeiro execute o seguinte comando no diretório pessoal do Elasticsearch `<caminho_de_instalação_do_sentinel>/opt/novell/sentinel/3rdparty/elasticsearch` do Sentinel:

   ```
   ./bin/elasticsearch-certutil cert --ca <CA certificate
   filename>.p12 --out config/certs/newNode.p12
   ```

   É solicitada a senha do seu certificado CA. Você também precisa criar uma senha para o certificado gerado.

10. Copie os certificados para os respectivos nós externos do Elasticsearch. Por exemplo, copie o arquivo `newNode.p12` no diretório `/etc/elasticsearch/certs/` do `newNode` do cluster externo do Elasticsearch. Forneça permissões de leitura e gravação para os certificados nas novas máquinas que usam o comando `chmod`.

Observação: Se o diretório `certs` não estiver presente, você precisará criá-lo.

---

11. Depois de gerar e copiar os certificados para todos os nós externos do Elasticsearch, adicione as seguintes configurações no arquivo `/etc/elasticsearch/elasticsearch.yml` de todos os nós externos do Elasticsearch:
    - `xpack.security.enabled: true`
    - `xpack.security.transport.ssl.enabled: true`
    - `xpack.security.transport.ssl.keystore.path: certs/newNode.p12`
    - `xpack.security.transport.ssl.truststore.path: certs/newNode.p12`
    - `xpack.security.transport.ssl.verification_mode: certificate`

12. Em cada um dos nós externos do Elasticsearch, armazene a senha para o arquivo de certificado `keystore` e `truststore` gerado no keystore do Elasticsearch. Para isso, execute os seguintes comandos no diretório pessoal do Elasticsearch `/usr/share/elasticsearch` de todos os nós externos do Elasticsearch:

    ```
    ./bin/elasticsearch-keystore add
    xpack.security.transport.ssl.keystore.secure_password
    ```

    ```
    ./bin/elasticsearch-keystore add
    xpack.security.transport.ssl.truststore.secure_password
    ```

2 Etapas a serem seguidas para proteger as comunicações do Sentinel para o cluster do Elasticsearch:

1. Alterne para o usuário `novell`:

    ```
    su novell
    ```

2. Execute o seguinte comando para gerar um certificado `http` para um nó externo do Elasticsearch da máquina Sentinel:

    ```
    <sentinel_installation_path>/opt/novell/sentinel/bin/javacert.sh --
    generateES <provide path where the http certificate should be
    generated, example /opt/http.pks> <http certificate password>
    <keyalias>
    ```

3. Copie o certificado `http` para o nó do Elasticsearch. Por exemplo, copie o arquivo `http.pks` no diretório ES_PATH_CONF`/certs/` no nó do Elasticsearch. Forneça permissões de leitura e gravação para os certificados das novas máquinas.

    Observação: Se o diretório `certs` não estiver presente, você precisará criá-lo.

    ---

4. Adicione as seguintes configurações no arquivo ES_PATH_CONF`/elasticsearch.yml` em todos os nós externos do Elasticsearch:
    - `xpack.security.http.ssl.enabled: true`
    - `xpack.security.http.ssl.keystore.path: certs/http.pks`
5. Execute o seguinte comando no diretório pessoal do Elasticsearch `/usr/share/elasticsearch` de todos os nós externos do Elasticsearch para gravar a senha do certificado `http` no keystore do Elasticsearch:

    ```
    ./bin/elasticsearch-keystore add
    xpack.security.http.ssl.keystore.secure_password
    ```

6. Inicie o serviço do Elasticsearch em cada um dos nós externos do Elasticsearch:

    ```
    /etc/init.d/elasticsearch start
    ```

3 (Condicional) Se você estiver no modo FIPS, depois de executar as duas etapas acima, precisará executar as etapas abaixo:

1. Adicione o certificado `http` interno do Elasticsearch gerado durante a instalação do Sentinel no keystore FIPS do servidor Sentinel usando o comando:

    ```
    ./convert_to_fips.sh -i <sentinel_installation_path>/opt/novell/
    sentinel/3rdparty/elasticsearch/config/http.pks
    ```

2. Após a etapa acima, haverá um prompt para reiniciar o Sentinel. Selecione **Não**.

3. Copie os certificados `http` de todos os nós externos do Elasticsearch gerados na etapa 2 e adicione-os ao keystore FIPS do servidor Sentinel usando o comando abaixo:

   ```
   ./convert_to_fips.sh -i <location of the copied http certificate>/
   <name of the certificate>
   ```

4. Verifique se todos os certificados `http` dos nós externos do Elasticsearch estão presentes no keystore FIPS do servidor Sentinel executando o comando:

   ```
   certutil -L -d sql:<sentinel_installation_path>/etc/opt/novell/
   sentinel/3rdparty/nss
   ```

5. Copie o certificado `http` interno do Elasticsearch (`<caminho_de_instalação_do_sentinel>/opt/novell/sentinel/3rdparty/elasticsearch/config/http.pks` no servidor Sentinel) gerado durante a instalação do Sentinel e adicione-o a todo o keystore FIPS do RCM (Collector Manager Remoto) usando o comando:

   ```
   ./convert_to_fips.sh -i <location of the copied http certificate>/
   http.pks
   ```

6. Após a etapa acima, haverá um prompt para reiniciar o Sentinel. Selecione **Não**.
7. Copie os certificados `http` de todos os nós externos do Elasticsearch gerados na etapa 2 e adicione-os ao keystore FIPS de todos os RCMs usando o comando abaixo:

   ```
   ./convert_to_fips.sh -i <location of the copied http certificate>/
   <name of the certificate>
   ```

8. Verifique se todos os certificados `http` dos nós externos do Elasticsearch estão presentes no keystore FIPS do RCM executando o seguinte comando:

   ```
   certutil -L -d sql:<rcm_installation_path>/etc/opt/novell/sentinel/
   3rdparty/nss
   ```

4 Reinicie o Sentinel e todos os RCMs:

```
rcsentinel restart
```

Adicionando o certificado http.pks no modo FIPS

A partir do Sentinel 8.4.0.0, a comunicação entre o Elasticsearch e o Sentinel é protegida, portanto o certificado `http` precisa ser adicionado ao keystore FIPS do servidor Sentinel e dos RCMs (Collector Managers Remotos).

Se a Visualização do Evento não estiver habilitada, execute as seguintes etapas:

1 Adicione o certificado `http` interno do Elasticsearch gerado durante a instalação do Sentinel ao keystore FIPS do servidor Sentinel usando o comando abaixo:

```
./convert_to_fips.sh -i <sentinel_installation_path>/opt/novell/
sentinel/3rdparty/elasticsearch/config/http.pks
```

2 Copie o certificado `http` interno do Elasticsearch (`<caminho_de_instalação_do_sentinel>/opt/novell/sentinel/3rdparty/elasticsearch/config/http.pks`) para todos os RCMs e importe-os para o keystore FIPS usando o comando abaixo:

```
./convert_to_fips.sh -i <path of the certificate copied above>/http.pks
```

Configurando coleta de dados de Fluxo de IP

O Sentinel utiliza os ArcSight SmartConnectors, que ajudam a monitorar sua rede corporativa pela coleta de dados do Fluxo de IP. Os SmartConnectors coletam dados do fluxo de IP como eventos e, portanto, são considerados para a contagem de EPS. Isso permite que você:

- Use as instâncias do Collector Manager existentes para coletar dados do Fluxo de IP.
- 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.

A funcionalidade de Fluxo de IP agora está habilitada por padrão. Você precisa instalar e configurar o ArcSight SmartConnector para coletar dados de Fluxo de IP.

O Sentinel não inclui mais recursos do NetFlow, incluindo exibições do NetFlow. Com o SmartConnectors coletando dados do Fluxo de IP como eventos, você pode usar as instâncias existentes do Collector Manager para coletar dados do NetFlow. Portanto, você não precisa mais das instâncias do NetFlow Collector Manager para coletar dados do NetFlow. Portanto, é possível desinstalar quaisquer instâncias existentes do NetFlow Collector Manager.

- “Configurando SmartConnectors que coletam dados do Fluxo de IP” na página 186
- “Desinstalando as instâncias existentes do NetFlow Collector Manager” na página 186

Configurando SmartConnectors que coletam dados do Fluxo de IP

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.

Desinstalando as instâncias existentes do NetFlow Collector Manager

Para desinstalar as instâncias existentes do NetFlow Collector Manager:

1 Efetue login no computador do NetFlow Collector Manager com a mesma permissão de usuário 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 interrompe o serviço e depois desinstala completamente o Collector Manager.

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 emIntegração. 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 92.

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.

Atualizando permissões para usuários que enviam dados de outros produtos integrados para o Sentinel

O Sentinel 8.2 SP1 e versões posteriores fornecem uma nova permissão, Enviar eventos e anexos, que permite que somente usuários designados enviem eventos e anexos do Change Guardian ou do Secure Configuration Manager para o Sentinel. Quando você faz upgrade para o Sentinel 8.2 SP1 e posterior, o Sentinel atribui automaticamente essa permissão aos usuários na função de Administrador. Para usuários não administradores que enviam eventos ou anexos ao Sentinel, você deve atribuir manualmente essa permissão. A menos que você atribua essa permissão, o Sentinel não receberá mais eventos ou anexos do Change Guardian nem do Secure Configuration Manager.

A atualização dessa permissão é aplicável apenas se o Sentinel está integrado ao Change Guardian ou ao Secure Configuration Manager. Para obter mais informações, consulte Creating Roles (Criando funções) no Sentinel Administration Guide (Guia de Administração do Sentinel).

Atualizando a senha de keystore

O script `chg_keystore_pass.sh` permite que você mude as senhas de keystore. Como uma melhor prática de segurança, mude as senhas de keystore imediatamente após fazer upgrade do Sentinel.

Observação: Não realize este procedimento se o servidor Sentinel estiver no modo FIPS.

Para mudar as senhas de keystore:

1. Efetue login no servidor Sentinel como usuário root.
2. Alterne de usuário para `novell`.
3. Vá para o diretório `/opt/novell/sentinel/bin`.
4. Execute o script `chg_keystore_pass.sh` e siga os prompts na tela para mudar as senhas de keystore.

34 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.

35 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 36, “Migrando dados” na página 197.

36 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 Capítulo 18, “Configurando o Elasticsearch para visualização do evento” na página 109.

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.

---

37 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

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.

38 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 SP5
  - Pacote SLES HAE (SLES High Availavility Extension)
  - Software Sentinel (incluindo RPM HA)
- ❒ (Condicional) Para instalações tradicionais de HA, verifique se os seguintes itens estão disponíveis:
  - Sistema operacional: SLES 12 SP5 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.

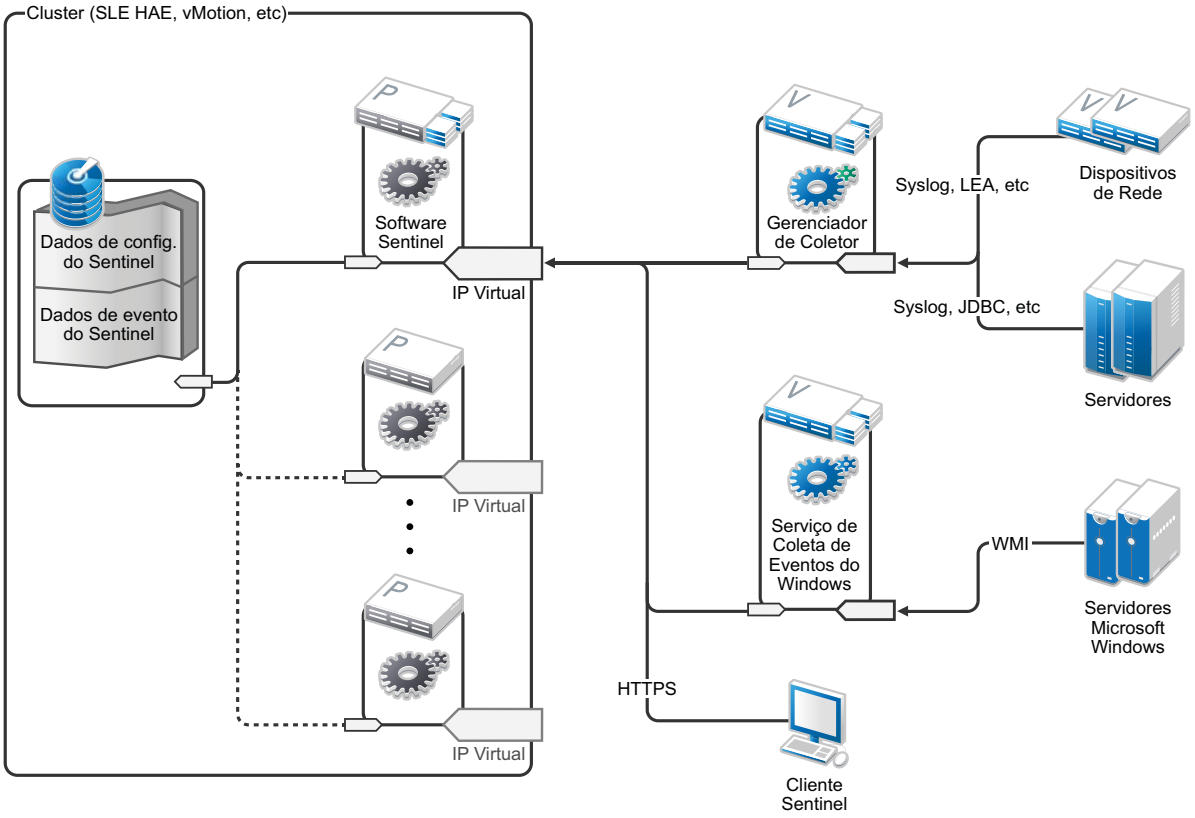
Para iSCSI, você precisa usar a maior Unidade de transferência de mensagem (MTU) suportada pelo hardware. MTUs maiores oferecem benefícios ao desempenho do armazenamento. O Sentinel pode apresentar problemas se a latência e a largura de banda para o armazenamento for mais lenta do que o recomendado.

- ❒ 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.

39 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

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
❑	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.
❑	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.
❑	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 57 para obter detalhes de quais portas devem estar disponíveis dependendo da configuração local e das origens que enviarão dados de evento.
❑	Verifique se todos os nós do cluster são sincronizados em tempo. Use o NTP ou uma tecnologia semelhante para este propósito.
❑	◆ O cluster requer uma resolução do nome de host confiável. Digite todos os nomes do host de cluster internos no arquivo `/etc/hosts` 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 88.
- 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. Contanto 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=<file size> bs=<bit size>
   ```

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 210
- "Configurando iniciadores iSCSI" na página 212

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 12 SP1 e posterior, selecione **Network Services** (Serviços de Rede) > **iSCSI LIO Target** (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 12 SP1 e posterior: `iscsiliotarget RPM`

9 (Condicional) Se você estiver usando o SLES 12, siga 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.

Observação: A Micro Focus recomenda que você use a senha diferente para o destino e o iniciador do iSCSI.

---

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 Deixe as outras opções com as configurações padrão e clique em **Próximo**.

17 (Condicional) Se você estiver usando o SLES 12, 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.

Você não precisa adicionar o nome do iniciador do cliente para o SLES 15 e posterior.

18 (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.

19 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.

20 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 clique em **OK**.
7. Clique em **Serviços de Rede** > **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 210, 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 de `/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 214
- "Instalação da aplicação de HA do Sentinel" na página 215

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.
   - **3c** Se você estiver habilitando o modo FIPS, adicione o caminho do certificado `http` do Elasticsearch `<caminho_de_instalação_do_sentinel>/opt/novell/sentinel/3rdparty/elasticsearch/config/http.pks` quando ele solicitar o certificado externo.
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`, o 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.
   - **3d** Se você estiver habilitando o modo FIPS, adicione o caminho do certificado `http` do Elasticsearch `<caminho_de_instalação_do_sentinel>/opt/novell/sentinel/3rdparty/elasticsearch/config/http.pks` quando ele solicitar o certificado externo.
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/sentinel/* /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/sentinel
```

```
umount /var/opt/novell/sentinel
```

Configurando a aplicação com SMT

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-HA-8-OS-Updates sle-12-x86_64
```

```
smt-repos -e Sentinel-Server-HA-8-Prod-Updates sle-12-x86_64
```

2 Configure a aplicação com o SMT seguindo as etapas na seção "Configuring Clients to Use SMT" (Configurando clientes para usar o SMT) da documentação do SMT.

Instalação do nó subsequente

- "Instalação de HA tradicional" na página 216
- "Instalação da aplicação de HA do Sentinel" na página 217

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/sentinel/*
   ```

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.

Conexão de RCM/RCE no modo HA

HA tradicional

Execute as seguintes etapas para conectar RCM/RCE no modo HA tradicional tanto para a configuração recente quanto para a existente:

1. Adicione um arquivo de entrada em `/etc/hosts` conforme dado abaixo na caixa RCM/RCE antes de instalar/configurar RCM/RCE.

   ```
   <virtual ip> <FQDN of first_scuccessful_activenode_host>
   <first_scuccessful_activenode_hostname>
   ```

   Por exemplo: 164.99.87.27 first_active_host.dom.name first_active_host

   ---

   Importante: Verifique sempre se essa entrada corresponde ao primeiro nome de host de nó ativo adequado bem-sucedido no ambiente HA especificado em `/etc/hosts` antes de executar `configure.sh`

   ---

2. Insira o IP virtual no prompt ao conectar RCM/RCE com o servidor.

   Importante: Embora o primeiro nó ativo bem-sucedido esteja desativado e o outro nó esteja ativo no momento, ainda use o primeiro nome de nó ativo bem-sucedido com IP virtual no arquivo `/etc/hosts`.

Aplicação HA

Execute as seguintes etapas para conectar RCM/RCE no modo HA da aplicação para uma nova configuração:

- Use apenas o nome de host do primeiro nó ativo bem-sucedido no cluster HA.

Execute as seguintes etapas para conectar RCM/RCE no modo HA da aplicação para a configuração existente:

1. Adicione um arquivo de entrada em `/etc/hosts` conforme dado abaixo na caixa RCM/RCE antes de instalar/configurar RCM/RCE.

   ```
   <virtual ip> <FQDN of first_scuccessful_activenode_host>
   <first_scuccessful_activenode_hostname>
   ```

   Por exemplo: 164.99.87.27 first_active_host.dom.name first_active_host

   ---

   Importante: Verifique sempre se essa entrada corresponde ao primeiro nome de host de nó ativo adequado bem-sucedido no ambiente HA especificado em `/etc/hosts` antes de executar `configure.sh`

   ---

2. Insira o IP virtual no prompt ao conectar RCM/RCE com o servidor.

   Importante: Embora o primeiro nó ativo bem-sucedido esteja desativado e o outro nó esteja ativo no momento, ainda use o primeiro nome de nó ativo bem-sucedido com IP virtual no arquivo `/etc/hosts`.

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`, depois 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 iSCI 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** > **iSCSI Initiator** (Serviços de Rede > 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 223

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), especifique esse nó (172.16.0.1) e, então, repita e adicione os outros nós do cluster: 172.16.0.2.

21 (Condicional) Se você não tiver habilitado a autenticação, selecione **Security** (Segurança) no painel esquerdo e desmarque **Enable Security Auth** (Habilitar Autenticação de Segurança).

22 Selecione **Finish** (Terminar) para completar a configuração.

23 Saia do YaST.

24 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** > **iSCSI Initiator** (Serviços de Rede > 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 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 clusterno`-quorum-policy` para `ignore`:

```
crm configure property no-quorum-policy=ignore
```

Observação: Se o cluster contiver mais de dois nós, não defina esta opção.

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 dessa solução recomendada, 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 sentinelfs sentinelnetfs
   sentineldb 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.

40 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

- 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 <watchdog driver name>`

Fazendo upgrade do HA do Sentinel Tradicional

O procedimento nesta seção orienta você através do upgrade do HA do Sentinel tradicional e do Sistema Operacional.

O Sentinel na versão 8.3.0.0 e posteriores usa o PostgreSQL em vez do MongoDB para armazenar dados de Inteligência de Segurança e dados de alertas.

Importante: Se você estiver fazendo upgrade de versões anteriores do Sentinel 8.3.0.0, as etapas abaixo se aplicarão.

No nó ativo, o processo de upgrade faz o seguinte:

- Migra dados de Inteligência de Segurança, dados de alertas e assim por diante, do MongoDB para o PostgreSQL.

O Sentinel agora armazena dados de Inteligência de Segurança e dados de alertas no PostgreSQL, em vez de no MongoDB. O processo de upgrade primeiro migrará esses dados para o PostgreSQL e, se for bem-sucedido, prosseguirá automaticamente com o upgrade. Se a migração de dados não for bem-sucedida, você não poderá fazer upgrade do Sentinel.

- Gera um script de limpeza que você pode usar para remover dados e RPMs relacionados ao MongoDB.

Os dados armazenados no MongoDB serão mantidos como um backup e você poderá apagá-los após o upgrade do Sentinel.

- "Fazendo upgrade do Sentinel de HA" na página 228
- "Fazendo upgrade do sistema operacional" na página 230

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:

   ```
   rcpacemaker 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 <install_filename>
   ```

   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:

   ```
   rcpacemaker start
   ```

   Repita Etapa 3a na página 228 a Etapa 3e na página 228 para todos os nós passivos do cluster.

   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 Pare a pilha do cluster:

```
rcpacemaker 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 <install_filename>
```

4e Execute o seguinte comando no diretório em que você extraiu os arquivos de instalação:

```
./install-sentinel
```

4f **Importante:** Se você estiver fazendo upgrade de versões anteriores do Sentinel 8.3.0.0, as etapas abaixo se aplicarão.

4f1 Selecione a opção de migração desejada.

Aviso: Verifique se você selecionou a opção apropriada, pois não será possível repetir este procedimento depois que o upgrade for bem-sucedido.

Se os seus dados forem migrados com êxito, o processo de upgrade continuará automaticamente.

O processo de upgrade mantém os dados que foram armazenados no MongoDB como um backup.

4f2 (Condicional) Se a migração de dados não for bem-sucedida:

4f2a Limpe os dados migrados sem sucesso. Para obter mais informações, consulte "Limpando dados do PostgreSQL quando há falha na migração" na página 175

4f2b (Condicional) Se o Sentinel não for iniciado automaticamente, inicie-o:

```
rcsentinel start
```

4f2c (Condicional) Antes do upgrade, se a visualização do evento estiver habilitada, após o upgrade para o Sentinel 8.4.0.0, o Elasticsearch parará, pois estará habilitado com o plug-in de segurança X-Pack. Para iniciar o Elasticsearch, siga o procedimento em "Configurações no Elasticsearch para comunicação segura de cluster" na página 180.

4g Depois que o upgrade for concluído, inicie a pilha do cluster:

```
rcpacemaker start
```

4h Remova os scripts de inicialização automática para que o cluster possa gerenciar o produto.

```
cd /
```

```
insserv -r sentinel
```

4i 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
```

8 Efetue login no Sentinel e verifique se você consegue ver os dados migrados, como alertas, dados de Inteligência de Segurança e assim por diante.

9 Os dados no MongoDB agora são redundantes porque o Sentinel 8.3 e posterior armazenam dados apenas no PostgreSQL. Para limpar o espaço em disco, apague esses dados. Para obter mais informações, consulte “Removendo dados do MongoDB” na página 179.

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 230
- “Configurando destinos iSCSI” na página 231
- “Configurando iniciadores iSCSI” na página 233
- “Configurando o cluster de HA” na página 233

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 interromper a pilha de cluster:

```
rcpacemaker 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 é o mesmo em todos os nós do cluster.

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.

Para configurar destinos iSCSI:

1 Execute o YaST da linha de comando (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:

- Selecione **Network Services** > **iSCSI LIO Target** (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:

iscsiliotarget RPM

9 (Condicional) 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 **Serviço**, selecione a opção **Ao Inicializar** para assegurar que o serviço seja iniciado quando o sistema operacional inicializar.

11 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 envidas.

A opção **Nenhuma Autenticação** é habilitada por padrão. No entanto, você deve habilitar a autenticação para verificar se a configuração é segura.

Observação: A Micro Focus recomenda que você use a senha diferente para o destino e o iniciador do iSCSI.

12 Clique em **Destinos** e em **Adicionar** para incluir um novo destino.

13 Clique em **Add** (Adicionar) para incluir uma nova LUN.

14 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`.

15 Repita as etapas 13 e 14, adicione LUN 1 e selecione `/networkdata` desta vez.

16 Deixe as outras opções com os valores padrão. Clique em **Avançar**.

17 (Condicional) Se você estiver usando o SLES 12, 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.

Você não precisa adicionar o nome do iniciador do cliente para o SLES 15 e posterior.

18 (Condicional) Caso tenha habilitado a autenticação na etapa 11, forneça as credenciais de autenticação.

Selecione um cliente, selecione **Edit Auth** > **Incoming Authentication** (Editar Autenticação > Autenticação Recebida) e especifique o nome de usuário e a senha. Repita isso para todos os clientes.

19 Clique em **Próximo** para selecionar as opções de autenticação padrão e clique em **Terminar** para sair da configuração. Se solicitado, reinicie o iSCSI.

20 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 231, 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 do Sentinel 8.2 ou posterior. Você pode fazer upgrade do Sentinel e do sistema operacional SLES por meio do Sentinel Appliance Manager ou Zypper (Canal de Atualização da Aplicação).

O Sentinel na versão 8.3.0.0 e posteriores usa o PostgreSQL em vez do MongoDB para armazenar dados de Inteligência de Segurança e dados de alertas. Antes de fazer upgrade da aplicação no nó ativo, você deve migrar seus dados do MongoDB para o PostgreSQL. Você poderá fazer upgrade da aplicação apenas se tiver migrado com sucesso seus dados para o PostgreSQL.

- Você precisa ter o SLES 12 SP3 ou SLES 12 SP4 instalado.
    1. (Condicional) Se você está no SLES 11 SP4 com o Sentinel 8.2.0.0, recomenda-se obter todas as atualizações do canal no SLES 11. Em seguida, faça upgrade do OS para SLES 12 SP3. Para obter mais informações sobre o upgrade do sistema operacional SLES, consulte “Upgrade do Sistema Operacional para SLES 12 SP3” na página 164. Faça download do utilitário pós-upgrade do site do Micro Focus Patch Finder e execute-o.
    2. (Condicional) Se você está no SLES 12 SP3 com o Sentinel 8.2.0.0 e executou o utilitário pós-upgrade `sentinel_sles_iso_os_post_upgrade-release-73.tar.gz`, então precisa fazer download do utilitário pós-upgrade `sentinel_sles_iso_os_post_upgrade-release-85.tar.gz` do site do Micro Focus Patch Finder e executá-lo.
    3. (Condicional) Se você está no SLES 12 SP3 com o Sentinel 8.2.0.0 e executou o utilitário pós-upgrade `sentinel_sles_iso_os_post_upgrade-release-85.tar.gz` do site do Micro Focus Patch Finder, siga as etapas de “Fazendo upgrade da aplicação” na página 167.
- “Fazendo upgrade por meio do patch do Zypper” na página 235
- “Fazendo upgrade por meio do Sentinel Appliance Management Console” na página 237

Fazendo upgrade por meio do patch do 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 92. 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 Pare a pilha do cluster.

```
rcpacemaker stop
```

A interrupção da pilha do cluster garante que os recursos do cluster permaneçam inacessíveis e evita o confinamento dos nós.

3b Satisfaça os pré-requisitos 1 e 2 listados em "Pré-requisitos para fazer upgrade da aplicação" na página 163

3c Faça download das atualizações do Sentinel:

Observação: Para o Sentinel 8.3.1, os comandos `zypper -v patch` e `zypper up` são necessários, pois tanto o rpm atualizado quanto o novo rpm são necessários para a aplicação.

- `zypper -v patch`

  Observação: Após o patch, é exibida a mensagem para reinicializar o sistema. Ignore a reinicialização até que a próxima etapa `zypper up` esteja concluída.

- `zypper up`

3d Depois que o upgrade for concluído, inicie a pilha do cluster.

```
rcpacemaker 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 Pare a pilha do cluster.

```
rcpacemaker stop
```

A interrupção da pilha do cluster garante que os recursos do cluster permaneçam inacessíveis e evita o confinamento dos nós.

5c Satisfaça os pré-requisitos listados em "Pré-requisitos para fazer upgrade da aplicação" na página 163.

5d Faça download das atualizações do Sentinel.

Para fazer upgrade do Sentinel, execute os seguintes comandos do prompt de comando:

- `zypper -v patch`

  Observação: Depois de executar o comando acima, é exibida a mensagem para reinicializar o sistema. Ignore a reinicialização até que Etapa 8 na página 237 esteja concluída.

- `zypper up`
- (Condicional) Antes do upgrade, se a visualização do evento estiver habilitada, após o upgrade para o Sentinel 8.4.0.0, o Elasticsearch parará, pois estará habilitado com o plug-in de segurança X-Pack. Para iniciar o Elasticsearch, siga o procedimento em "Configurações no Elasticsearch para comunicação segura de cluster" na página 180.

5e Após a conclusão do upgrade:

- (Condicional) Se o Sentinel não for iniciado automaticamente, inicie o banco de dados do Sentinel:

  ```
  rcsentinel startdb
  ```

- Inicie a pilha do cluster:

  ```
  rcpacemaker start
  ```

5f 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 foi bem-sucedido:

```
rcsentinel version
```

9 Reinicialize o sistema conforme a mensagem `zypper patch` mostrada na etapa 5d.

10 Efetue login no Sentinel e verifique se você consegue ver os dados migrados, como alertas, painéis de controle de Inteligência de Segurança e assim por diante.

11 Os dados no MongoDB agora são redundantes porque o Sentinel 8.3 e posterior armazenam dados apenas no PostgreSQL. Para limpar o espaço em disco, apague esses dados. Para obter mais informações, consulte "Removendo dados do MongoDB" na página 179.

Fazendo upgrade por meio do Sentinel Appliance Management Console

Para fazer upgrade por meio do Sentinel Appliance Management Console:

1 Execute o seguinte comando no nó ativo ou em um nó passivo no cluster, para habilitar o modo de manutenção:

```
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.

2 Execute o seguinte comando para verificar se o modo de manutenção está ativo:

```
crm status
```

Os recursos do cluster devem ser exibidos no estado não gerenciado.

3 Faça upgrade de todos os nós do cluster passivo primeiro:

3a Execute o comando a seguir para interromper a pilha de cluster:

```
rcpacemaker stop
```

A interrupção da pilha do cluster garante que os recursos do cluster permaneçam inacessíveis e evita o confinamento dos nós.

3b Execute o seguinte comando para verificar se a porta 9443 está escutando no nó ativo para acessar a aplicação:

```
netstat –na | grep 9443
```

3c (Condicional) Execute o seguinte comando se a porta 9443 não estiver escutando:

```
systemctl restart vabase vabase-jetty vabase-datamodel
```

3d Satisfaça os pré-requisitos 1 e 2 listados em "Pré-requisitos para fazer upgrade da aplicação" na página 163

3e Inicie a aplicação realizando um dos procedimentos a seguir:

- Efetue login no Sentinel. Clique em **Sentinel Main** > **Appliance** (Principal do Sentinel > Aplicação).
- Especifique o URL a seguir no browser da web: `https://<endereço_IP>:9443`.

3f (Condicional) Se você não conseguir iniciar o Sentinel Appliance Management Console:

3f1 Vá para `/var/opt/novell` no nó ativo e copie os seguintes arquivos para `/var/opt/novell/` em cada nó passivo:

- `datamodel-service`
- `ganglia`
- `jetty`
- `python`
- `va`

3f2 Em cada nó passivo, defina a permissão de arquivo como `vabase-jetty` para os arquivos na pasta `jetty`:

1. Acesse `/var/opt/novell/jetty`.
2. Execute o seguinte comando:

```
chown -R vabase-jetty:vabase-jetty *
```

3f3 Execute o seguinte comando para reiniciar os serviços do vabase:

```
systemctl start vabase-jetty vabase-datamodel vabase
```

3f4 Execute o seguinte comando para verificar se a porta 9443 está escutando em todos os nós disponíveis:

```
netstat -na | grep 9443
```

3g Efetue login como `vaadmin`.

3h Clique em **Atualização Online**.

3h1 (Condicional) Registre-se para obter atualizações, caso ainda não tenha feito isso. Para obter mais informações, consulte "Registrando para receber atualizações" na página 92.

Observação: É exibida uma mensagem para reinicializar o sistema após a etapa 5h2, mas ignore-a até que a etapa 5h3 seja concluída.

3h2 Para instalar as atualizações exibidas para o Sentinel e o sistema operacional, clique em **Update Now** > **OK** (Atualizar Agora > OK).

3h3 **Observação:** Para o Sentinel 8.3.1, além da etapa 5h2, o comando `zypper up` também é necessário, pois tanto o rpm atualizado quanto o novo rpm são necessários para a aplicação.

Execute o seguinte comando do prompt de comando para fazer upgrade completo do rpm:

```
zypper up
```

3h4 Para aplicar as atualizações instaladas, clique em **Reinicializar**.

3h5 Após a reinicialização, confira a versão no canto superior direito da tela para verificar se o upgrade foi bem-sucedido.

3i Quando o upgrade for concluído, reinicie a pilha do cluster.

```
rcpacemaker start
```

4 Faça upgrade do nó ativo de cluster.

4a Satisfaça os pré-requisitos listados em "Pré-requisitos para fazer upgrade da aplicação" na página 163.

4b Repita as etapas 5h1 a 5h3 para o nó de cluster ativo.

4c (Condicional) Se o Sentinel não for iniciado automaticamente, inicie o Sentinel:

```
rcsentinel start
```

4d Quando o upgrade for concluído, reinicie a pilha do cluster:

```
rcpacemaker start
```

5 Execute o seguinte comando no nó ativo ou em um nó passivo no cluster para desabilitar o modo de manutenção:

```
crm configure property maintenance-mode=false
```

6 Execute o seguinte comando no nó ativo ou em um nó passivo no cluster para verificar se o modo de manutenção não está ativo:

```
crm status
```

7 (Condicional) Antes do upgrade, se a visualização do evento estiver habilitada, após o upgrade para o Sentinel 8.4.0.0, o Elasticsearch parará, pois estará habilitado com o plug-in de segurança X-Pack. Para iniciar o Elasticsearch, siga o procedimento em "Configurações no Elasticsearch para comunicação segura de cluster" na página 180.

8 Agora reinicialize o sistema conforme a mensagem `zypper patch` mostrada na etapa 5h2.

9 Após a reinicialização, confira a versão no canto superior direito da tela para verificar se o upgrade foi bem-sucedido.

10 Efetue login no Sentinel e verifique se você consegue ver os dados migrados, como alertas, painéis de controle de Inteligência de Segurança e assim por diante.

11 Os dados no MongoDB agora são redundantes porque o Sentinel 8.3 e posterior armazenam dados apenas no PostgreSQL. Para limpar o espaço em disco, apague esses dados. Para obter mais informações, consulte "Removendo dados do MongoDB" na página 179.

41 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

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

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

A Solução de problemas

Esta seção contém alguns dos problemas que podem ocorrer durante a instalação e as ações para solucioná-los.

A propriedade do cluster Default-Resource-Stickiness foi descontinuada

Problema: O uso do comando `crm` para definir ou modificar a propriedade de configuração (por exemplo: `crm configure property maintenance-mode=true`) mostra a seguinte mensagem:

```
ERROR: DEBUG: Cluster properties: cib-bootstrap-options-default-resource-
stickiness: moving default-resource-stickiness under rsc_defaults as
resource-stickiness unless already defined there
WARNING: cib-bootstrap-options: unknown attribute 'default-resource-
stickiness'
```

Correção: A mensagem acima será exibida se for feito upgrade da versão mais antiga do SLE HAE para a nova versão do produto SLE HAE no Sentinel, tipicamente de SLES 12 SP3 para SLES 12 SP5 ou uma versão superior. Nenhum impacto de funcionalidade é causado por essa mudança. Para obter mais informações, consulte o artigo do SUSE KB.

Não é possível configurar RCM/RCE usando IP virtual na configuração HA

Problema:

Não é possível configurar o RCM/RCE usando IP virtual. O host não pode ser acessado pelo nome de host.

Correção:

HA tradicional

Execute as seguintes etapas para conectar RCM/RCE no modo HA tradicional tanto para a configuração recente quanto para a existente:

1. Adicione um arquivo de entrada em `/etc/hosts` conforme dado abaixo na caixa RCM/RCE antes de instalar/configurar RCM/RCE.

   ```
   <virtual ip> <FQDN of first_scuccessful_activenode_host>
   <first_scuccessful_activenode_hostname>
   ```

   Por exemplo: 164.99.87.27 first_active_host.dom.name first_active_host

   ---

   Importante: Verifique sempre se essa entrada corresponde ao primeiro nome de host de nó ativo adequado bem-sucedido no ambiente HA especificado em `/etc/hosts` antes de executar `configure.sh`

   ---

2. Insira o IP virtual no prompt ao conectar RCM/RCE com o servidor.

   Importante: Embora o primeiro nó ativo bem-sucedido esteja desativado e o outro nó esteja ativo no momento, ainda use o primeiro nome de nó ativo bem-sucedido com IP virtual no arquivo `/etc/hosts`.

Aplicação HA

Execute as seguintes etapas para conectar RCM/RCE no modo HA da aplicação para uma nova configuração:

- Use apenas o nome de host do primeiro nó ativo bem-sucedido no cluster HA.

Execute as seguintes etapas para conectar RCM/RCE no modo HA da aplicação para a configuração existente:

1. Adicione um arquivo de entrada em `/etc/hosts` conforme dado abaixo na caixa RCM/RCE antes de instalar/configurar RCM/RCE.

   ```
   <virtual ip> <FQDN of first_scuccessful_activenode_host>
   <first_scuccessful_activenode_hostname>
   ```

   Por exemplo: 164.99.87.27 first_active_host.dom.name first_active_host

   ---

   Importante: Verifique sempre se essa entrada corresponde ao primeiro nome de host de nó ativo adequado bem-sucedido no ambiente HA especificado em `/etc/hosts` antes de executar `configure.sh`

   ---

2. Insira o IP virtual no prompt ao conectar RCM/RCE com o servidor.

   Importante: Embora o primeiro nó ativo bem-sucedido esteja desativado e o outro nó esteja ativo no momento, ainda use o primeiro nome de nó ativo bem-sucedido com IP virtual no arquivo `/etc/hosts`.

No ambiente DHCP, o ícone da interface do usuário web do servidor Sentinel da página da aplicação do servidor Sentinel está redirecionando para uma página em branco

Problema: O ícone da interface do usuário web do servidor Sentinel da página da aplicação do servidor Sentinel está sendo iniciado como uma página bloqueada em branco no ambiente DHCP.

Solução temporária: Execute estas etapas:

1. Acesse o menu **YaST**.
2. Navegue até **System > Network Settings > IPv6 protocol Setting** (Sistema > Configurações de rede > Configuração do protocolo IPv6).
3. Desabilite o IPv6 e grave.
4. Reinicialize o sistema.

Não é possível se conectar com o hub de transformação (T-Hub) depois de dar o endereço IP/nome de host correto

Caso o servidor Sentinel não consiga se comunicar com o T-Hub, mesmo que o T-Hub seja acessível e todos os certificados T-Hub sejam copiados para o servidor Sentinel, execute as seguintes etapas:

1. Navegue até o diretório `/etc/opt/novell/sentinel/intelligence` no servidor Sentinel.
2. Apague o arquivo `avro-schema-file-V1.json`
3. Reinicie o servidor Sentinel:

   ```
   rcsentinel restart
   ```

Reiniciar o servidor Sentinel regenera o arquivo de esquema e o usuário deve ser capaz de estabelecer uma conexão bem-sucedida com o T-Hub.

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 **Tools > Internet Options > Security** (Ferramentas > Opções da Internet > Segurança) e defina o nível de segurança como **Medium-high** (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 **Settings** > **Internet Options** > guia **Security** > **Trusted Sites** > **Sites** (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 mesmo 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
   ```

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 reprograme 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 para desinstalar o Sentinel

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 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).

Tarefas após desinstalar o Sentinel

A desinstalação do servidor Sentinel não remove do sistema operacional o Usuário Administrador do Sentinel. É preciso remover manualmente o usuário.

Depois de desinstalar o Sentinel, certas configurações de sistema permanecem. Você deve remover as configurações antes de realizar uma nova instalação do Sentinel, especialmente se ocorreram erros ao desinstalar o Sentinel.

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.