NetIQ Sentinel 7.1

Guia de instalação e configuração

June 2013

Informações legais

O NetIQ Sentinel está protegido pela patente americana nº 05829001.

ESTE DOCUMENTO E O SOFTWARE DESCRITO NESTE DOCUMENTO SÃO FORNECIDOS MEDIANTE E ESTÃO SUJEITOS AOS TERMOS DE UM CONTRATO DE LICENÇA OU DE UM CONTRATO DE NÃO DIVULGAÇÃO. EXCETO CONFORME EXPRESSAMENTE ESTABELECIDO NESTE CONTRATO DE LICENÇA OU CONTRATO DE NÃO DIVULGAÇÃO, A NETIQ CORPORATION FORNECE ESTE DOCUMENTO E O SOFTWARE DESCRITO NESTE DOCUMENTO NA FORMA EM QUE SE ENCONTRAM, SEM GARANTIAS DE QUALQUER TIPO, EXPRESSAS OU IMPLÍCITAS INCLUINDO, SEM LIMITAÇÃO, AS GARANTIAS IMPLÍCITAS DE COMERCIALIZAÇÃO OU ADEQUAÇÃO A UM FIM ESPECÍFICO. ALGUNS ESTADOS NÃO PERMITEM ISENÇÃO DE GARANTIAS EXPRESSAS OU IMPLÍCITAS EM DETERMINADAS TRANSAÇÕES; ASSIM, ESTA DECLARAÇÃO PODE NÃO SE APLICAR A VOCÊ.

Para fins de clareza, qualquer módulo, adaptador ou outro material semelhante ("Módulo"), está licenciado sob os termos e condições do Contrato de Licença do Usuário Final para a versão aplicável do produto ou software NetIQ ao qual esteja inter-relacionado e, ao acessar, copiar ou usar um Módulo, você aceita cumprir esses termos. Se você não aceitar os termos do Contrato de Licença do Usuário Final, não estará autorizado a usar, acessar ou copiar um Módulo e deverá destruir todas as cópias do Módulo, bem como entrar com contato com a NetIQ para obter mais instruções.

Este documento e o software descrito neste documento não podem ser emprestados, vendidos ou oferecidos sem a permissão prévia por escrito da NetIQ Corporation, exceto se de outra forma permitido por lei. Exceto conforme expressamente estabelecido neste contrato de licença ou de não divulgação, nenhuma parte deste documento ou do software descrito neste documento pode ser reproduzida, armazenada em um sistema de recuperação ou transmitida de qualquer forma ou por qualquer meio, seja eletrônico, mecânico ou de outro modo, sem o consentimento prévio por escrito da NetIQ Corporation. Algumas empresas, nomes e dados neste documento são usados para fins de ilustração e podem não representar empresas, indivíduos ou dados reais.

Este documento pode trazer imprecisões técnicas ou erros tipográficos. As informações contidas aqui sofrem alterações periodicamente. Essas alterações podem ser incorporadas em novas edições deste documento. A NetIQ Corporation pode fazer, a qualquer momento, melhorias ou alterações no software descrito neste documento.

Direitos restritos do Governo dos EUA: se o software e o documento estiverem sendo adquiridos por ou em nome do Governo dos EUA ou por um contratante principal ou subcontratante do Governo dos EUA (em qualquer nível), de acordo com 48 C.F.R. 227.7202-4 (para aquisições do Departamento de Defesa), 48 C.F.R. 2.101 e 12.212 (para aquisições não feitas pelo Departamento de Defesa), os direitos do governo sobre o software e a documentação, incluindo seu direito de usar, modificar, reproduzir, liberar, executar, mostrar ou divulgar o software ou documentação, estarão sujeitos em todos os aspectos aos direitos e restrições de licença comercial informados no contrato de licença.

Índice

Sobre este livro e a biblioteca

O *Guia de instalação e configuração* fornece uma introdução ao NetIQ 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.

Sobre a NetIQ Corporation

Nós somos uma empresa global de software corporativo com foco nos três desafios persistentes do seu ambiente: mudança, complexidade e risco, bem como de maneira podemos ajudá-lo e controlá-los.

Nosso ponto de vista

Adaptar-se a mudanças e gerenciar complexidades e riscos não são novidades

De fato, dentre todos os desafios que você enfrenta, estas são provavelmente as variáveis mais proeminentes, que impedem que você obtenha o controle de que precisa para gerenciar, monitorar e medir de forma segura seus ambientes de computação físicos, virtuais e em nuvem.

Habilitando serviços essenciais para empresas de forma mais rápida e eficiente

Nós acreditamos que fornecer o máximo possível de controle para organizações de TI é a única maneira de possibilitar uma entrega de serviços mais oportuna e econômica. Pressões persistentes como mudanças e complexidade só continuarão a aumentar conforme as organizações continuarem a mudar e as tecnologias necessárias para gerenciá-las se tornarem inerentemente mais complexas.

Nossa filosofia

Vender soluções inteligentes, não somente software

Visando providenciar um controle seguro, primeiro nos certificamos de que entendemos os cenários do mundo real, nos quais organizações de TI como a sua operam todos os dias. Somente dessa maneira podemos desenvolver soluções de TI práticas e inteligentes, que geram com sucesso resultados comprovados e mensuráveis. E isso é muito mais recompensador do que simplesmente vender software.

Promover seu sucesso é nossa paixão

O seu sucesso encontra-se no âmago de como fazemos negócios. Desde os primeiros esboços até a implantação de um produto, nós compreendemos que você precisa de soluções de TI que funcionem bem e se integrem perfeitamente com seus investimentos existentes, suporte contínuo e treinamento pós-implantação, bem como alguém com quem trabalhar seja verdadeiramente fácil, o que sabemos que não é muito comum. Em última análise, quando você é bem-sucedido, todos nós somos bem-sucedidos.

Nossas soluções

- Governança de acesso e identidade
- Gerenciamento de acesso
- Gerenciamento de segurança
- Gerenciamento de aplicativos e sistemas

- Gerenciamento de carga de trabalho
- Gerenciamento de serviços

Entrando em contato com o Suporte a vendas

Para esclarecer dúvidas sobre produtos, preços e recursos, entre em contato com seu parceiro local. Se não for possível entrar em contato com seu parceiro, entre em contato com nossa equipe de Suporte a vendas.

Mundial:	www.netiq.com/about_netiq/officelocations.asp
Estados Unidos e Canadá:	1-888-323-6768
E-mail:	info@netiq.com
Site na Web:	www.netiq.com

Entrando em contato com o Suporte técnico

Para questões sobre produtos específicos, entre em contato com nossa equipe de Suporte técnico.

Mundial:	www.netiq.com/support/contactinfo.asp
América do Norte e do Sul:	1-713-418-5555
Europa, Oriente Médio e África:	+353 (0) 91-782 677
E-mail:	support@netiq.com
Site na Web:	www.netiq.com/support

Entrando em contato com o Suporte de documentação

Nosso objetivo é fornecer uma documentação que atenda às suas necessidades. Se você tem sugestões de melhorias, clique em **Adicionar comentário** na parte inferior de qualquer página nas versões em HTML da documentação publicada em www.netiq.com/documentation. Você também pode enviar um e-mail para Documentation-Feedback@netiq.com. Nós valorizamos sua opinião e aguardamos seu contato.

Entrando em contato com a comunidade online de usuários

A Qmunity, a comunidade online da NetIQ, é um rede colaborativa que conecta você, seus colegas e os especialistas da NetIQ. Fornecendo mais informações imediatas, links para recursos úteis e acesso aos especialistas da NetIQ, a Qmunity ajuda a garantir que você domine os conhecimentos de que precisa para utilizar todo o potencial dos investimentos de TI dos quais depende. Para obter mais informações, visite http://community.netiq.com.

Compreendendo o Sentinel

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

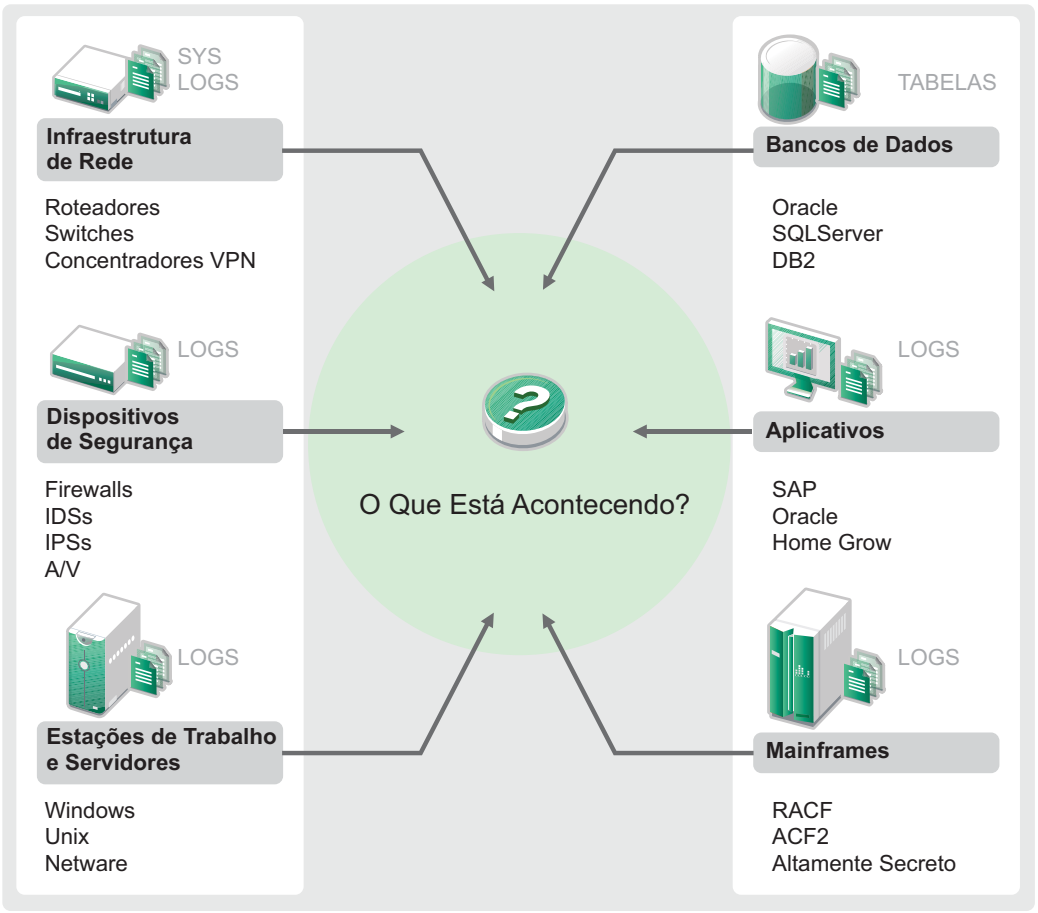
1 O que é o Sentinel?

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.

1.1 Desafios em proteger um ambiente de TI

A complexidade dos ambientes de TI geram grandes desafios para a segurança das informações. Existem diversos aplicativos, bancos de dados, mainframes, estações de trabalho e servidores, todos com registros de eventos. Você também possui dispositivos de segurança e de infraestrutura de rede, que também registram o que acontece no 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 estão armazenados em silos;
- À quantidade de informações geradas nos registros; e
- Não é possível identificar quem fez o que sem analisar manualmente todos os registros.

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

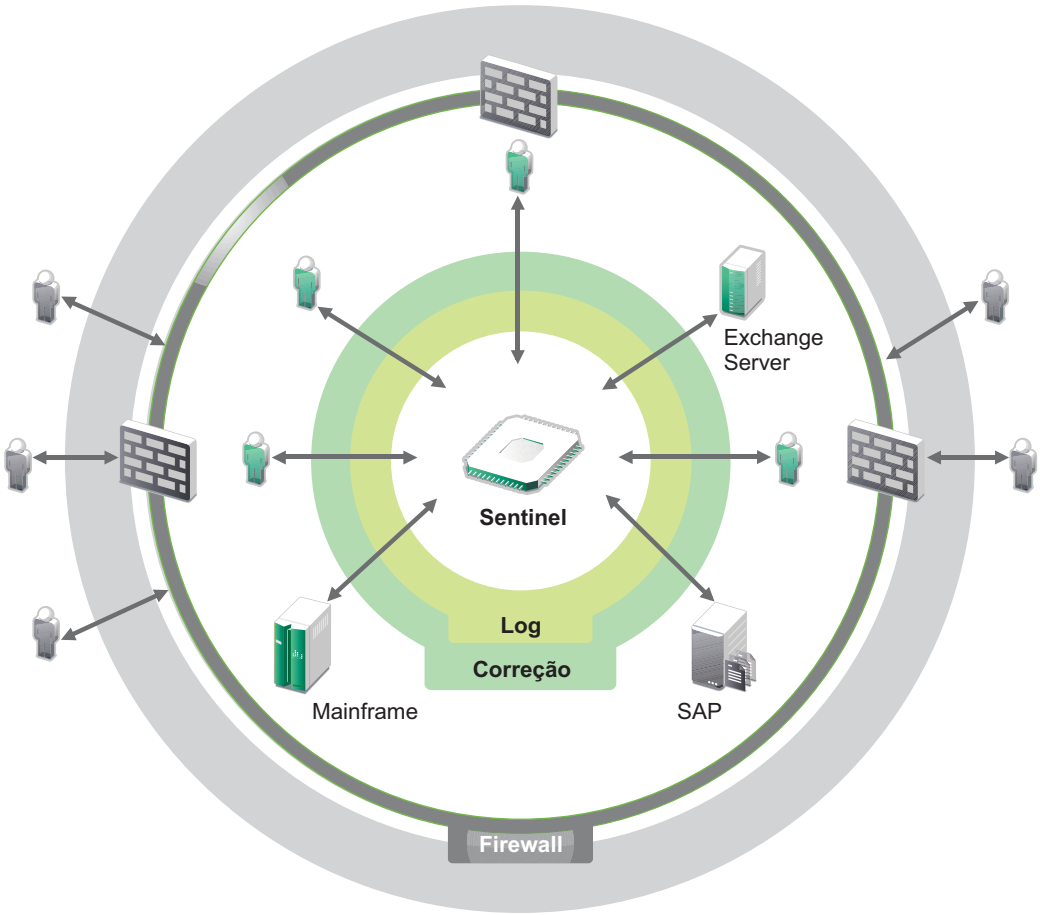
- Coletar dados;
- Consolidar dados;
- Normalizar dados distintos em eventos que possam ser facilmente comparados;
- Mapear eventos para normas padrão.
- Analisar os dados;
- Comparar eventos em diversos sistemas para determinar se há algum problema de segurança;
- Enviar notificações no caso de dados que não atendam às normas;
- Impor ações sobre as notificações para cumprir com as políticas da empresa; e
- Gerar relatórios para comprovar a conformidade.

Após identificar os desafios relacionados à segurança do ambiente de TI, será necessário determinar como proteger a empresa para os usuários e dos usuários sem tratá-los como usuários mal-intencionados ou sobrecarregá-los, impedindo-os de serem produtivos. O Sentinel é a solução.

1.2 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*



O resultado é que 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 determinar o comportamento dos usuários e também monitorar o controle de maneira eficiente. Independentemente se a pessoa está ligada diretamente ou não à empresa, é possível relacionar todas as ações tomadas por ela de modo que atividades não autorizadas sejam identificadas antes de causarem danos.

O Sentinel faz isso de maneira econômica ao:

- Fornecer uma única solução que lida com controles de TI em diversas normas;.
- Preencher a lacuna de conhecimento entre o que deveria acontecer e o que realmente acontece no seu ambiente em rede;
- Demonstrar aos auditores e às autoridades que sua empresa documenta, monitora e gera relatórios sobre controles de segurança;
- Fornecer monitoramento de conformidade e programas de relatórios prontos; e
- Gerar a visibilidade e o controle exigidos para avaliar continuamente o êxito dos programas de conformidade e de segurança da sua empresa.

O Sentinel automatiza os processos de geração de relatórios, análise e coleta de registros para garantir que os controles de TI sejam eficazes no suporte à detecção de ameaças e aos requisitos de auditoria. O Sentinel fornece monitoramento automatizado de eventos de segurança, eventos de conformidade e controles de TI permitindo que você tome medidas imediatas quando ocorre violação na segurança ou eventos de não conformidade. Ele também permite que você colete informações resumidas sobre o seu ambiente para comunicar a situação geral da segurança aos principais acionistas.

2 Como o Sentinel funciona

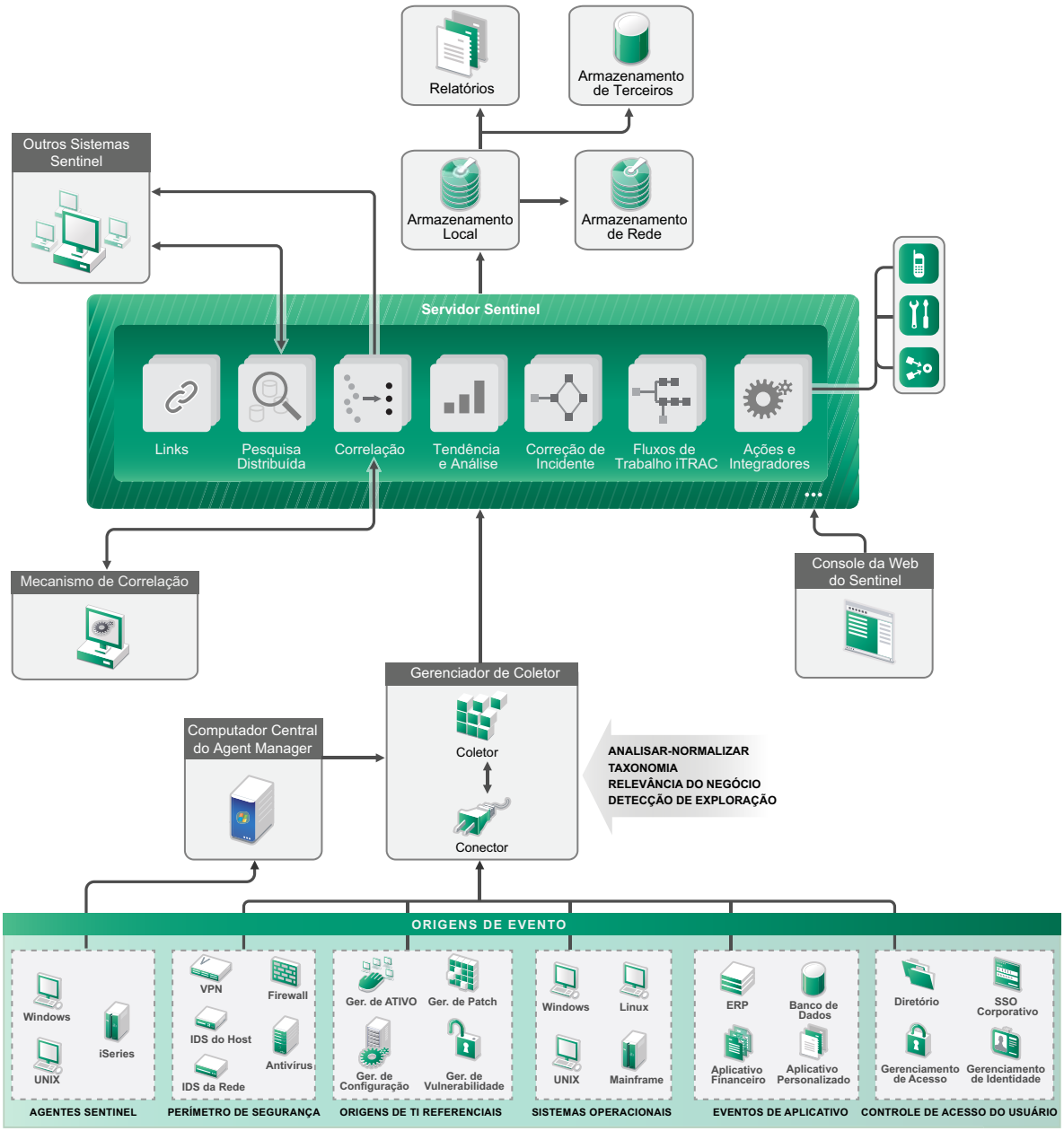
O Sentinel gerencia as informações e os eventos de segurança de forma contínua em todo o ambiente de TI para garantir uma solução de monitoramento completa.

O Sentinel faz o seguinte:

- Reúne informações de registros, eventos e segurança de todas as diferentes fontes de eventos presentes em seu ambiente de TI.
- Padroniza as informações de registros, eventos e segurança reunidas em um formato comum.
- Armazena eventos em um repositório de dados baseado em arquivo com políticas flexíveis e personalizáveis de retenção de dados.
- Fornece a capacidade de vincular hierarquicamente vários sistemas Sentinel, incluindo o Sentinel Log Manager;
- Permite pesquisar eventos não apenas no 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 determinado período 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 o funcionamento do Sentinel:

Figura 2-1 *Arquitetura do Sentinel*



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

2.1 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. As fontes de eventos podem representar inúmeros itens distintos na sua rede.

Perímetro de Segurança: Dispositivos de segurança, incluindo hardware e software usados para criar um perímetro de segurança para o seu ambiente, como firewalls, IDS e VPNs.

Sistemas Operacionais: eventos dos diferentes sistemas operacionais que são executados na rede.

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

Eventos do Aplicativo: eventos gerados nos aplicativos instalados na rede.

Controle de Acesso de Usuário: eventos gerados nos aplicativos ou dispositivos que permitem aos usuários acessar os recursos da empresa.

2.2 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. Adicionar informações de categoria (taxonomia) aos eventos facilita a comparação deles em sistemas que relatam eventos de forma diferente. Por exemplo, falhas na autenticação. Os eventos são processados pela exibição em tempo real, pelo mecanismo de correlação, por painéis e pelo servidor back end.

Um evento consiste em mais de 200 campos. Os campos do evento têm tipos e finalidades diferentes. Alguns são predefinidos, como gravidade, importância, IP de destino e porta de destino. Há dois conjuntos de campos configuráveis: os campos reservados são de uso interno da Novell para permitir futuras expansões, enquanto que os campos de Cliente são para extensões de clientes.

Para mudar a finalidade de um campo, basta renomeá-lo. A origem de um campo pode ser referencial ou externa, a qual é definida explicitamente pelo dispositivo ou pelo Coletor correspondente. 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 definido como o código da construção que contém o bem mencionado como o IP de destino de um evento. Por exemplo, um campo pode ser computado pelo serviço de mapeamento por meio de um mapa definido pelo cliente usando o IP de destino do evento.

2.2.1 Serviço de Mapeamento

O Serviço de Mapeamento permite que um mecanismo sofisticado propague dados comerciais importantes por todo o sistema. Esses dados podem aprimorar eventos com informações referenciais que fornecem contexto, permitindo que os analistas tomem melhores decisões, escrevam relatórios mais úteis e regras de correlação melhor definidas.

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. Essas informações adicionais podem ser usadas para correlação avançada e geração de relatórios. O sistema suporta vários mapas integrados e também mapas personalizados definidos pelo usuário

Os mapas definidos no Sentinel são armazenados de duas formas:

- Os mapas integrados são armazenados no banco de dados, atualizados com o APIs no código do Coletor 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 via IU de Configuração de Dados de 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 Gerenciador de Coletor e aplicadas localmente. Esse processamento distribuído garante que a atividade de mapeamento não sobrecarregue o servidor principal.

2.2.2 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. A importância desse recurso de transmissão é especialmente relevante em um sistema em tempo real que seja vital para os negócios, como o Sentinel, no qual é preciso haver uma movimentação de dados constante, previsível e ágil, qualquer que seja a carga transiente no sistema.

2.2.3 Detecção de exploração (serviço de mapeamento)

O Sentinel permite a referência cruzada entre as assinaturas dos dados de eventos e os dados do Vulnerability Scanner. Os usuários são notificados de forma automática e imediata em caso de tentativa de ataque para explorar um sistema vulnerável. Isso é possível graças à:

- Alimentação do Consultor;
- Detecção de intrusão;
- Verificação de vulnerabilidades; e
- Firewalls

O Consultor fornece uma referência cruzada entre as assinaturas de dados do evento e os dados do verificador de vulnerabilidades. O feed do Advisor contém informações sobre vulnerabilidades e ameaças, uma normalização de assinaturas de evento e plug-ins de vulnerabilidade. Para obter mais informações sobre o Consultor, consulte “Configurando o Consultor” no *Guia de administração do NetIQ Sentinel 7.1*.

2.3 Gerenciador de Coletor

O Gerenciador de Coletor do gerencia coletas de dados, monitora mensagens de status do sistema e filtra eventos, conforme necessário. As principais funções do Gerenciador de Coletor incluem o que segue:

- Transformar eventos;
- Adicionar relevância empresarial aos eventos por meio do serviço de mapeamento.
- Realizar filtragem global do eventos;
- Rotear eventos;
- Determinar dados em tempo real, de vulnerabilidade, de bens e não tempo real; e
- Enviar mensagens de saúde ao servidor Sentinel.

2.3.1 Coletores

Os Coletores normalizam e coletam informações dos Conectores. Os coletores são gravados em Javascript e definem a lógica do que segue:

- Receber dados iniciais dos Conectores;
- Analisar e normalizar os dados;
- Aplicar lógica repetida aos dados;
- Traduzir dados específicos do dispositivo em dados específicos do Sentinel;
- Formatar os eventos;
- Passar os dados normalizados, analisados e formatados para o Gerenciador de Coletor.
- Filtragem de eventos específica de dispositivo.

2.3.2 Conectores

Os Conectores fornecem a conexão entre as fontes de eventos e o sistema Sentinel. Os conectores usam protocolos padrão de mercado para obter eventos, como syslog, JBDC para ler das tabelas de bancos de dados, WMI para ler dos registros de eventos do Windows e assim por diante. Os conectores fornecem:

- Transporte dos dados de eventos iniciais das fontes de eventos para o Coletor.
- Filtro específico para conexão; e
- Gerenciamento de erros da conexão.

2.4 Gerenciador de agente

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

- Acesse registros não 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 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.

2.5 Correlação

Um único evento pode parecer comum, mas quando combinado com outros eventos, ele pode informar você sobre um problema potencial. O Sentinel ajuda você a correlacionar os eventos em questão usando as regras que você cria e implementa no Mecanismo de correlação e toma a medida necessária para reduzir os problemas.

A correlação agrega inteligência ao gerenciamento de eventos de segurança, automatizando a análise do fluxo de eventos de entrada para encontrar padrões relevantes. A correlação permite definir regras que identificam as ameaças importantes e padrões complexos de ataque, para que você consiga priorizar os eventos e iniciar o gerenciamento e a resposta eficazes aos incidentes. Para obter mais informações, consulte a seção "Correlacionando dados de eventos" no *Guia do usuário do NetIQ Sentinel 7.1*.

Para monitorar eventos de acordo com as Regras de correlação, é necessário implantar as regras no Mecanismo de correlação. Quando um evento que atende aos critérios da regra ocorrer, o Mecanismo de correlação gera um evento de correlação descrevendo o padrão. Para obter mais informações, consulte "Mecanismo de correlação" no *Guia do usuário do NetIQ Sentinel 7.1*.

2.6 Inteligência de segurança

O recurso de correlação do Sentinel fornece a capacidade de conhecer padrões de atividade, sejam eles para segurança, conformidade ou outros fins. O recurso Security Intelligence 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 desvios (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 NetIQ Sentinel 7.1*.

2.7 Correção de incidente

O Sentinel fornece um sistema de gerenciamento automatizado de respostas a incidentes que permite que você documente e formalize o processo de monitoramento, encaminhamento e resposta a incidentes e violações de política, além de fornecer uma 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 NetIQ Sentinel 7.1*.

2.8 Fluxos de trabalho do iTrac

Os fluxos de dados iTRAC foram projetados para fornecer 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 solução.

Os workflows podem ser criados usando etapas manuais ou automáticas. Recursos avançados, como ramificação, escalonamento em tempo real e variáveis locais, são suportados 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 NetIQ Sentinel 7.1*.

2.9 Ações e integradores

No Sentinel, as ações executam manual ou automaticamente algum tipo de ação, como enviar um e-mail. As ações podem ser acionadas 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 NetIQ Sentinel 7.1*.

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 NetIQ Sentinel 7.1*.

2.10 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 apresentam flexibilidade para permitir que você especifique as colunas que devem ser exibidas nos resultados.

É possível executar, programar e enviar relatórios PDF por e-mail. 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 NetIQ Sentinel 7.1*.

2.11 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 sistema é ajustado e otimizado para obter a máxima eficiência em qualquer tipo de análise específica, e os métodos para executar facilmente transições de um tipo de análise para outro são fornecidos a fim de obter transições contínuas.

A investigação de eventos do Sentinel geralmente começa com as Telas Ativas em tempo real. Embora ferramentas mais avançadas estejam disponíveis, as Telas ativas exibem fluxos de evento filtrados juntamente com gráficos resumidos que podem ser usados para análises simples e gerais de tendências de evento, dados de evento e identificação de eventos específicos. Ao longo do tempo, você cria filtros ajustados para classes de dados específicas, como os resultados da correlação. Você pode usar as Telas ativas como um painel mostrando um comportamento geral operacional e de segurança.

Em seguida, você pode usar a pesquisa interativa para executar análises mais 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 transferir as pesquisas interativas criadas na Interface de pesquisa para um modelo de relatório, o qual cria instantaneamente um relatório que exibe os mesmos dados em um formato que se adequa melhor a uma quantidade maior de eventos.

O Sentinel inclui vários modelos para esse fim. Alguns modelos são ajustados para exibir tipos específicos de informações, como dados de autenticação ou criação de usuários, e outros modelos são para fins gerais que permitem personalizar grupos e colunas de forma interativa no relatório.

Ao longo do tempo, você desenvolverá filtros e relatórios usados com frequência que facilitarão seus fluxos de trabalho. O Sentinel suporta totalmente o armazenamento e a distribuição dessas informações para as pessoas da sua empresa. Para obter mais informações, consulte o *Guia do usuário do NetIQ Sentinel 7.1*.

2.12 Armazenamento e roteamento de dados no Sentinel

O Sentinel fornece diversas opções para rotear, armazenar e extrair os dados coletados. Por padrão, o Sentinel recebe dois fluxos de dados diferentes, porém relacionados, dos Gerenciadores de coletor: os dados de eventos e os dados não processados. Os dados não processados são imediatamente armazenados em partições protegidas para providenciar uma cadeia de evidência segura. Os dados de eventos analisados são roteados de acordo com regras que você define e podem ser filtrados, enviados para armazenamento, enviados para análises em tempo real e roteados para sistemas externos. Todos os dados de eventos enviados para o armazenamento são então vinculados a políticas de retenção definidas pelo usuário, que determinam as partições em que os dados são colocados e também definem a política de remoção segundo a qual os dados do evento são retidos e eventualmente excluídos.

O armazenamento de dados do Sentinel baseia-se em uma estrutura em três níveis:

- **Armazenamento online**
  - **Armazenamento local ou primário:** Otimizado para gravação e recuperação rápida. Os dados de evento coletados mais recentemente (e os mais frequentemente pesquisados) são armazenados aqui.

- **Armazenamento em rede ou secundário:** Otimizado para reduzir o uso do espaço ainda assim permitindo recuperação rápida. O Sentinel automaticamente migra as partições de dados para o armazenamento secundário.

Nota: O uso de um armazenamento secundário é opcional. Políticas de retenção de dados, pesquisas e relatórios funcionam em partições de dados de evento independentemente se residem de fato em armazenamentos primários, secundários ou em ambos.

- **Armazenamento para arquivamento ou offline:**

  Quando as partições são fechadas, você pode fazer o backup delas para um armazenamento offline tão barato quanto armazenamento em massa, Amazon Glacier, etc. Caso necessário, você pode reimportar temporariamente partições offline para análises forense de longo termo.

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 o armazenamento de dados" no *Guia de Administração do NetIQ Sentinel 7.1*.

Planejando a instalação do Sentinel

Esta seção oferece orientação sobre considerações de planejamento antes de instalar o Sentinel. Se você desejar instalar uma configuração que não está identificada nas seções que seguem ou se tiver quaisquer perguntas, entre em contato com o Suporte técnico da NetIQ.

3 Lista de verificação da implementação

Use a lista de verificação a seguir para concluir o planejamento, instalação e configuração do Sentinel:

❒	Tarefas	Consulte
❒	Revise as informações da arquitetura do produto para aprender sobre os componentes do Sentinel.	Parte I, “Compreendendo o Sentinel”, en la página 13.
❒	Revise a licença do Sentinel para determinar se é necessário instalar a versão de avaliação ou a versão corporativa do Sentinel.	Capítulo 4, “Compreendendo as informações da licença”, en la 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”, en la página 35.
❒	Por padrão, o Sentinel vem com um Gerenciador de Coletor e um Mecanismo de Correlação. Revisar os Gerenciadores de coletor e os eventos por segundo (EPS) do Mecanismo de correlação e determinar se você precisa instalar Gerenciadores de coletor e Mecanismos de correlação adicionais para melhorar o desempenho e o equilíbrio de carga.	Sección 9.1, “Vantagens de Gerenciadores de Coletor adicionais”, en la página 68 e Sección 9.2, “Vantagens dos mecanismos de correlação adicional”, en la página 68.
❒	Instale o Sentinel.	Parte III, “Instalando o Sentinel”, en la página 65.
❒	Certifique-se de configurar o horário no servidor Sentinel.	Capítulo 16, “Configurando o horário”, en la página 101.
❒	Ao instalar o Sentinel, os plug-ins do Sentinel disponíveis no momento da liberação do Sentinel são instalados como padrão. Configure os plug-in prontos para o uso para coleta de dados e criação de relatórios.	Capítulo 17, “Configurando plug-ins prontos para o uso”, en la página 105.
❒	Instalando coletores e conectores adicionais no seu ambiente conforme necessário.	Capítulo 13, “Instalando coletores e conectores adicionais”, en la página 93.
❒	Instalando Gerenciadores de coletor e Mecanismos de correlação adicionais no seu ambiente conforme necessário.	Sección 11.6, “Instalando Gerenciadores de Coletor e Mecanismos de Correlação adicionais”, en la página 78.

4 Compreendendo as informações da licença

O Sentinel tem várias licenças que podem ser usadas. Por padrão, o Sentinel vem com a licença de avaliação.

4.1 Licença de avaliação

O licenciamento padrão do Sentinel permite usar todos os recursos corporativos do Sentinel pelo período de avaliação de 90 dias. Um sistema em execução com a licença de avaliação exibe um indicador na interface da web indicando que a chave de licença temporária está sendo usada. Ele também exibe o número de dias restante antes que a funcionalidade expire e indica como atualizar para uma licença completa.

Nota: A data de expiração do sistema é baseada nos dados mais antigos do sistema. Se você restaurar eventos antigos no sistema, a data de expiração será ajustada de acordo com eles.

Após o período de 90 dias de avaliação, a maioria das funcionalidades fica desabilitada, mas você ainda pode efetuar login e atualizar o sistema para usar uma chave de licença empresarial.

Depois de atualizar para uma licença empresarial, todas as funcionalidades são restauradas. Para evitar qualquer interrupçã9o na funcionalidade, é preciso atualizar o sistema com uma licença corporativa antes da data de expiração.

4.2 Licenças corporativas

Ao adquirir o Sentinel, você receberá uma chave de licença por meio do portal do cliente. Dependendo do que foi adquirido, sua chave de licença ativará certos 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. Para adicionar a chave de licença ao sistema, veja no *Guia de Administração do NetIQ Sentinel 7.1*.

5 Atendendo aos requisitos do sistema

Este capítulo fornece informações sobre os requisitos de hardware, sistema operacional e navegador do Sentinel.

5.1 Sistemas operacionais e plataformas suportados

O NetIQ é compatível com o Sentinel nos sistemas operacionais descritos nesta seção. O NetIQ também é compatível com o Sentinel em sistemas com atualizações secundárias a esses sistemas operacionais, como patches de segurança ou hotfixes. No entanto, o NetIQ não suporta a execução do Sentinel em sistemas com atualizações importantes nesses sistemas operacionais até que o NetIQ teste e certifique tais atualizações.

A NetIQ suporta o servidor do Sentinel, o Gerenciador de Coletor e o Mecanismo de Correlação nos seguintes sistemas operacionais e plataformas:

Categoria	Requisito
Sistema Operacional	O Sentinel é suportado nos seguintes sistemas operacionais: ◆ SUSE Linux Enterprise Server (SLES) 11 SP2 de 64 bits * ◆ Red Hat Enterprise Linux for Servers (RHEL) 6 de 64 bits * O Sentinel não é suportado nas instalações do Open Enterprise Server no SLES. **Importante:** Para instalações tradicionais, certifique-se de que o protocolo de Internet versão 6 (IPv6) está ativado no seu sistema operacional. Se o IPv6 não estiver ativado, componentes importantes não funcionarão corretamente. Para instalações de aplicação, o IPv6 é ativado por padrão.
Plataforma virtual	O NetIQ fornece aplicações que instalam um servidor SLES 11 SP2 de 64 bits e o Sentinel nas seguintes plataformas virtuais: ◆ VMWare ESX 4.0 e 5.0 ◆ Xen 4.0

Categoria	Requisito
DVD ISO	O NetIQ fornece um arquivo ISO de DVD que instala o SLES 11 SP2 de 64 bits e o Sentinel em: ◆ Hyper-V Server 2008 R2 ◆ Hardware sem um sistema operacional instalado
Sistema de Arquivos	**Instalações tradicionais:** ◆ **Nos sistemas SLES:** O Sentinel suporta sistemas de arquivos ext3 e XFS. ◆ **Em sistemas RHEL:** O Sentinel suporta sistemas de arquivos ext4 e XFS. **Instalações da aplicação:** O Sentinel usa o sistema de arquivos ext3. Para obter mais informações sobre sistemas de arquivos, consulte Visão geral de sistemas de arquivos no Linux (http://www.novell.com/documentation/sles11/stor_admin/data/filesystems.html) no *Guia de administração de armazenamento do SLES 11 SP2*.

5.2 Plataformas de banco de dados suportadas

O Sentinel inclui um sistema de armazenamento baseado em arquivo embutido e o banco de dados PostgreSQL, tudo o que é necessário para sua execução. No entanto, se você usar o recurso opcional de sincronização de dados para copiar dados para um data warehouse, o Sentinel suportará o uso do PostgreSQL, Oracle versão 11g R2 ou Microsoft SQL Server 2008 R2 como o data warehouse.

5.3 Browsers suportados

A interface da Web do Sentinel é otimizada para uma resolução de 1280 x 1024 ou mais alta nos seguintes browsers suportados:

Nota: Para carregar os aplicativos do cliente Sentinel adequadamente, você deve instalar o Java Webstart no sistema.

Plataforma	Browser
Windows 7	◆ Firefox versão 5 a 18 ◆ Internet Explorer 8, 9 e 10.* Para obter mais informações sobre o Internet Explorer 8, consulte “Pré-requisitos para o Internet Explorer” en la página 37.
SLES 11 SP2 e RHEL 6	◆ Firefox versão 5 a 18

5.3.1 Pré-requisitos para o Internet Explorer

Se o Nível de Segurança da Internet for definido como Alto, uma página em branco será exibida após o login no Sentinel e a janela pop-up de download do arquivo poderá ser bloqueada pelo browser. Para resolver esse problema, é necessário primeiro definir o nível de segurança para Médio-alto e, em seguida, alterar para Nível personalizado da seguinte forma:

1. Navegue até *Ferramentas* > *Opções da Internet* > *guia Segurança* e defina o nível de segurança como *Médio-alto*.
2. Certifique-se de que a opção *Ferramentas* > *Modo de Exibição de Compatibilidade* não está selecionada.
3. Navegue até *Ferramentas* > *Opções da Internet* > *guia Segurança* > *Nível personalizado* e, em seguida mova a barra de rolagem para baixo até a seção *Downloads* e selecione *Habilitar* na opção *Aviso automático para downloads de arquivo*.

5.4 Informações de dimensionamento 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 NetIQ ou qualquer um dos parceiros do NetIQ Sentinel antes de finalizar a arquitetura do Sentinel.

Esta seção fornece informações de dimensionamento baseadas no teste realizado na NetIQ com o hardware disponível quando o teste foi realizado. É provável que existam configurações de hardware maiores e mais fortes, capazes de lidar com cargas maiores.

Configurações "tudo em um" colocam toda a carga de processamento no servidor do Sentinel em vez de distribuí-la para Mecanismos de correlação e Gerenciadores de coletor remotos. Enquanto uma configuração "tudo em um" pode funcionar bem para cenários simples, nos quais somente um pequeno conjunto de recursos é usado de forma limitada, ela não funciona bem com grandes números de recursos ou usos de forma estendida. Por exemplo, se você usar mais do que as regras de correlação prontas para o uso, isso colocará uma carga maior no sistema, o que pode afetar negativamente outros recursos do mesmo servidor devido à maior utilização de recursos do Mecanismo de correlação.

- Distribuir a carga para Gerenciadores de coletor remotos é necessário quando mais que um pequeno número de coletores é usado.
- Distribuir a carga para Mecanismos de correlação remotos é necessário quando você usa mais do que as regras de correlação prontas para o uso.
- Distribuir a carga é uma boa ideia quando você planeja aumentar o número de recursos usados ou a extensão em que você usa esses recursos.

A capacidade da CPU de utilizar a tecnologia Hyperthreading demonstrou ter um impacto significativamente positivo na carga que o sistema conseguir manipular. Logo, ao decidir qual CPU comprar, verifique se a tecnologia Hyperthreading estava ativa no teste de referência abaixo e certifique-se de que a CPU escolhida possui capacidades de Hyperthreading tão boas ou melhores.

Configurações	Descrição	"Tudo em um" demo não visa produção	"Tudo em um" médio	Coleta de dados baseada em agente média	"Tudo em um" grande	Coleta de dados sem agente distribuída grande	Extra grande
Capacidade EPS retida	A taxa de eventos por segundo processada por componente em tempo real e retida em armazenamento pelo sistema.	100 EPS	2500 EPS	2500 EPS	9000 EPS	11000 EPS	11000+ EPS
Capacidade EPS operacional	A taxa total de eventos por segundo recebida pelo sistema das fontes de eventos. Isso inclui dados descartados pela filtragem inteligente do sistema antes de serem armazenados e é o número usado para propósitos de conformidade com a licença baseada em EPS.	100 EPS	2500+ EPS	2500+ EPS	9000 EPS	16000 EPS	16000+ EPS
Hardware do servidor Sentinel							

Configurações	Descrição	"Tudo em um" demo não visa produção	"Tudo em um" médio	Coleta de dados baseada em agente média	"Tudo em um" grande	Coleta de dados sem agente distribuída grande	Extra grande
CPU		Intel Xeon CPU E5420 @ 2,50 GHz (CPU de 4 núcleos), sem Hyperthreading	Dois Intel Xeon CPU E5450 @ 3,00GHz (4 núcleos por CPU; 8 núcleos no total), sem Hyperthreading	Dois AMD Opteron 2431 @ 2,40 GHz (6 núcleos por CPU; 12 núcleos no total)	Dois Intel(R) Xeon(R) CPU E5-2680 0 @ 2,70GHz (8 núcleos) CPUs (16 núcleos no total), com Hyperthreading		Entre em contato com os Serviços da NetIQ
Armazenamento local	Dados armazenados localmente em cache para melhor desempenho de pesquisa.	Unidade de 500 GB e 7,2k RPM	5 x 300 GB SAS 15k RPM (Hardware RAID 0)	3 x 146 GB SAS 10K RPM (RAID 0, tamanho de faixa 128k)	5 TB, 8 x 600 GB SAS 15k RPM (Hardware RAID 0, tamanho de faixa 128k)		
Armazenamento em rede	Inclui uma cópia dos dados em armazenamento local.	Não usado	Não usado	Não usado	Não usado		
Memória		4 GB	24 GB	16 GB	64 GB		
Gerenciador de coletor remoto # 1 Hardware							
CPU		Não aplicável (somente CM embutido local)				Dois Intel(R) Xeon(R) CPU E5-2680 0 @ 2,70GHz (8 núcleos) CPUs (16 núcleos no total), com Hyperthreading	Entre em contato com os Serviços da NetIQ

Configurações	Descrição	"Tudo em um" demo não visa produção	"Tudo em um" médio	Coleta de dados baseada em agente média	"Tudo em um" grande	Coleta de dados sem agente distribuída grande	Extra grande
Armazenamento						20 GB de espaço livre	Entre em contato com os Serviços da NetIQ
Memória						24 GB	
Gerenciador de coletor remoto # 2 Hardware							
CPU		Não aplicável (somente CM embutido local)				CPU de 8 núcleos Intel(R) Xeon(R) X5570 @ 2,93 GHz (máquina virtual)	Entre em contato com os Serviços da NetIQ
Armazenamento						50 GB	
Memória						8 GB	
Hardware de gerenciador de agente							
CPU		Não aplicável (somente coleta sem agente)		Dois Intel Xeon 5140 @ 2,33 GHz (2 núcleos por CPU; 4 núcleos no total)	Não aplicável (somente coleta sem agente)		Entre em contato com os Serviços da NetIQ
Armazenamento				2 x 300 GB SAS 10K RPM (RAID 0, tamanho de faixa 128k)			
Memória				16 GB			
Hardware de mecanismo de correlação remoto							

Configurações	Descrição	“Tudo em um” demo não visa produção	“Tudo em um” médio	Coleta de dados baseada em agente média	“Tudo em um” grande	Coleta de dados sem agente distribuída grande	Extra grande
CPU		Não aplicável (somente CE embutido local)					Entre em contato com os Serviços da NetIQ
Armazenamento							
Memória							

Configurações	Descrição	“Tudo em um” demo não visa produção	“Tudo em um” médio	Coleta de dados baseada em agente média	“Tudo em um” grande	Coleta de dados sem agente distribuída grande	Extra grande
Coleta de dados							
Distribuição do gerenciador de coletor (CM)	O número de fontes de eventos e carga de eventos por segundo colocada em cada gerenciador de coletor. O porcentagem filtrada indica quantos eventos padronizados foram filtrados imediatamente depois da coleta, sem serem armazenados ou passados para mecanismo de análise. Observe que os dados não processados de registro não padronizados nos quais os eventos padronizados se baseiam não são afetados pela filtragem e são sempre armazenados. O CM embutido local fica localizado na máquina do servidor Sentinel.	**CM embutido local** Fontes de eventos: 101 EPS: 100 Filtrado: 0%	**CM embutido local** Fontes de eventos: 2500 EPS: 2500 Filtrado: 0%	**CM embutido local** Fontes de eventos: 5000 EPS: 2500 Filtrado: 0%	**CM embutido local** Fontes de eventos: 500 EPS: 9000 Filtrado: 0%	**CM embutido local** Não usado **CM remoto #1** Fontes de eventos: 110 EPS: 9500 Filtrado: 21% Dados não processados desativados **CM remoto #2** Fontes de eventos: 20 EPS: 6500 Filtrado: 54% Dados não processados desativados	Entre em contato com os Serviços da NetIQ

Configurações	Descrição	“Tudo em um” demo não visa produção	“Tudo em um” médio	Coleta de dados baseada em agente média	“Tudo em um” grande	Coleta de dados sem agente distribuída grande	Extra grande
Coletores usados		**IBM AIX 6.1r3** Fontes: 100 EPS: 99 **NetIQ Universal Event 2011.1r1** Fontes: 1 EPS: 1	Cada coletor tem seu próprio servidor syslog. **Oracle Solaris 6.1r3** Fontes: 1000 EPS: 1000 **IBM AIX 6.1r3** Fontes: 1000 EPS: 1000 **Sourcefire Snort 2011.1r1** Fontes: 500 EPS:500	Coletor de teste personalizado (sem análise) **Servidor 1 do conector do gerenciador de agente** Fontes: 5000 EPS: 2500	Cada um dos seguintes coletores tem seu próprio servidor syslog, analisando nas seguintes taxas de EPS: **Oracle Solaris 6.1r3** EPS: 2000 **Sourcefire Snort 2011.1r1** EPS: 1500 **NetIQ Universal Event 2011.1r1** EPS: 2000 **Juniper Netscreen Series 2011.1r1** EPS: 1500 **IBM AIX 6.1r3: 2000** EPS: 2000	Cada um dos seguintes coletores tem seu próprio servidor syslog, analisando nas seguintes taxas de EPS: **Oracle Solaris 6.1r3** RCM #1: 2000 RCM #2: 2000 **Sourcefire Snort 2011.1r1** RCM #1: 2000 RCM #2: 1000 **NetIQ Universal Event 2011.1r1** RCM #1: 2000 RCM #2: 0 **Juniper Netscreen Series 2011.1r1** RCM #1: 2000 RCM #2: 1500	Entre em contato com os Serviços da NetIQ

Configurações	Descrição	“Tudo em um” demo não visa produção	“Tudo em um” médio	Coleta de dados baseada em agente média	“Tudo em um” grande	Coleta de dados sem agente distribuída grande	Extra grande
						IBM AIX 6.1r3 RCM #1: 1500 RCM #2: 0 **IBM iSeries 2011.1r3** RCM #1: 0 RCM #2: 2000	Entre em contato com os Serviços da NetIQ
Total		Fonte de evento: 101 EPS: 100 Filtrado: 0%	Fonte de evento: 2500 EPS: 2500 Filtrado: 0%	Fonte de evento: 5000 EPS: 2500 Filtrado: 0%	Fonte de evento: 500 EPS: 9000 Filtrado: 0%	Fontes de eventos: 130 EPS operacional: 16000 EPS retido: 11000 Filtrado: 25%	
Armazenamento de Dados							

Configurações	Descrição	"Tudo em um" demo não visa produção	"Tudo em um" médio	Coleta de dados baseada em agente média	"Tudo em um" grande	Coleta de dados sem agente distribuída grande	Extra grande
Até quanto no passado os usuário pesquisarão dados regularmente?	Quantidade de dados armazenados localmente em cache para melhor desempenho de pesquisa.	7 dias					Entre em contato com os Serviços da NetIQ
Que porcentagem das pesquisas estarão acima de dados mais antigos que os dados acima?	Influencia a quantidade de operações de entrada/saída por segundo (IOPS) para armazenamento de rede local	10%					
Com que retroatividade os dados precisam ser retidos?	Influencia quanto espaço em disco é necessário para reter todos os dados. Caso o armazenamento em rede esteja ativado, isso influencia o tamanho do armazenamento em rede necessário. Caso contrário, influencia o tamanho do armazenamento local necessário.	14 dias					

Configurações	Descrição	"Tudo em um" demo não visa produção	"Tudo em um" médio	Coleta de dados baseada em agente média	"Tudo em um" grande	Coleta de dados sem agente distribuída grande	Extra grande
Um dispositivo de armazenamento em rede estará disponível e conectado?	Influencia se todos os dados serão armazenados localmente ou se armazenamento em rede está disponível para armazenamento online de longo prazo e baixo custo. Dados em armazenamento em rede permanecem online.	Não					Entre em contato com os Serviços da NetIQ
Quantos relatórios serão otimizados usando resumos e outras políticas de sincronização de dados?	Influencia o número de políticas de sincronização de dados, o que por sua vez influencia o tamanho e o IOPS do armazenamento local.	5 (pronto para uso)			4 (pronto para uso, exceto o RDD de resumo de fonte, que fica para trás)		
Atividades do usuário							

Configurações	Descrição	"Tudo em um" demo não visa produção	"Tudo em um" médio	Coleta de dados baseada em agente média	"Tudo em um" grande	Coleta de dados sem agente distribuída grande	Extra grande
Quantos usuários estarão ativos ao mesmo tempo em média?	Influencia a quantidade de IOPS para armazenamento loca e em rede, assim como outros itens.	1					Entre em contato com os Serviços da NetIQ
Quantas pesquisas um usuário ativo fará ao mesmo tempo em média?	Influencia a quantidade de IOPS para armazenamento local e em rede.	1 pesquisa ou relatório (mas não ambas ao mesmo tempo) 20k eventos por mês 100M eventos por pesquisa		Não testado com carga de relatórios ou pesquisa	1 80M eventos por pesquisa	1 20M eventos por pesquisa	
Quantos relatórios um usuário ativo executará ao mesmo tempo em média?	Influencia a quantidade de IOPS para armazenamento local e em rede.	1 pesquisa ou relatório (mas não ambas ao mesmo tempo) 20k eventos por mês 100M eventos por pesquisa		Não testado com carga de relatórios ou pesquisa	1 1k eventos por relatório	1 60k eventos, 5k páginas, por relatório	
Análises							
Que porcentagem dos dados de evento é relevante para as regras de correlação?	Quantidade de dados que o mecanismo de correlação irá processar.	100% (prontos para uso) (3 correlações por segundo)		100% (prontos para uso) (0 correlações por segundo)	0%	0% (alguns dados chegam muito tarde para a correlação em tempo real)	Entre em contato com os Serviços da NetIQ

Configurações	Descrição	"Tudo em um" demo não visa produção	"Tudo em um" médio	Coleta de dados baseada em agente média	"Tudo em um" grande	Coleta de dados sem agente distribuída grande	Extra grande
Quantas regras de correlação simples (somente acionamento/filtragem) serão usadas?	Influencia o uso da CPU do mecanismo de correlação.	84 (pronto para uso)			0		Entre em contato com os Serviços da NetIQ
Quantas regras de correlação complexas serão usadas?	Influencia o uso do CPU e da memória do mecanismo de correlação.	0 (pronto para uso)					
Distribuição do mecanismo de correlação (CE)		CE embutido local (todas as regras)					
Em quantos conjuntos de dados a detecção de anomalia será realizada?	O número de painéis de Inteligência de segurança, que influencia a CPU, o tamanho do armazenamento local e o uso da memória.	1 (1% do fluxo do evento cada)		0			

Configurações	Descrição	“Tudo em um” demo não visa produção	“Tudo em um” médio	Coleta de dados baseada em agente média	“Tudo em um” grande	Coleta de dados sem agente distribuída grande	Extra grande
Alta disponibilidade							
Notas	Desativação de funcionalidades notáveis ou alertas sobre o que acontece ao exceder a carga do sistema descrita acima.				Dados não processados desativados Correlação e Inteligência de segurança não usados Relatórios em 30k+ eventos causam instabilidade	Dados não processados desativados Correlação e Inteligência de segurança não usados Relatórios de quantidades de eventos acima dos valores determinados causarão instabilidade Aumentar o EPS retido com o tempo causará instabilidade na configuração do sistema	Entre em contato com os Serviços da NetIQ

5.5 Planejamento de partições para armazenamento de dados

Ao instalar o Sentinel, é necessário montar a partição de disco para o armazenamento local no mesmo local em que o Sentinel foi 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 excluir dados de eventos prematuramente. Para obter mais informações sobre o diretório do Sentinel, consulte Capítulo 15, “Estrutura de diretórios do Sentinel”, en la página 97.

Como prática recomendada, certifique-se de que o diretório de dados esteja localizado em uma partição de disco diferente de onde 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 "Partição de disco".

5.5.1 Use partições nas instalações tradicionais

Nas instalações tradicionais, você pode modificar o layout da partição de disco do 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 Sección 15, “Estrutura de diretórios do Sentinel”, en la página 97. Ao executar o instalador, o Sentinel é instalado nos diretórios pré-criados, resultando em uma instalação que abrange várias partições.

Nota:

- 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`.

5.5.2 Use partições em uma instalação da aplicação

Usando o formato de aplicação DVD ISO, é possível configurar o particionamento do sistema de arquivos da aplicação durante a instalação. 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 Sección 12.4.2, “Criando partições”, en la página 90.

5.6 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 na página da web de plug-ins do Sentinel (http://support.novell.com/products/sentinel/secure/sentinelplugins.html).

5.7 Ambiente virtual

O Sentinel é extensivamente testado e completamente suportado em servidores VMware ESX. Ao configurar um ambiente virtual, as máquinas virtuais devem ter duas ou mais CPUs. Para atingir resultados de desempenho comparáveis aos resultados de teste de máquina física no ESX ou em qualquer outro ambiente virtual, o ambiente virtual deve ter as mesmas recomendações de memória, CPU, espaço em disco e E/S que a máquina física.

Para obter informações sobre recomendações para máquina física, consulte Capítulo 5, “Atendendo aos requisitos do sistema”, en la página 35.

6 Considerações sobre a implementação do Sentinel Operacional no modo FIPS140-2

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

Ativar o modo Sentinel FIPS 140-2 causa a comunicação entre o servidor do Sentinel, os Gerenciadores de Coletor remotos do Sentinel, os Mecanismos de Correlação remotos do Sentinel, a UI da web do Sentinel, o Sentinel Control Center e o serviço Sentinel Advisor para usar a criptografia validada pelo FIPS 140-2.

6.1 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 6.2 é validado pelo FIPS 140-2. O módulo de criptografia NSS fornecido pelo SLES 11 SP2 ainda não foi oficialmente validado pelo FIPS 140-2, mas o trabalho está em progresso para obter a validação do FIPS 140-2 para o módulo SUSE. 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 informações sobre a certificação RHEL 6.2 FIPS 140-2, veja *Módulos criptográficos validados para FIPS 140-1 e FIPS 140-2*.

6.1.1 Pacotes RHEL NSS

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

- nspr-4.9-1.el6.x86_64;
- nss-sysinit-3.13.3-6.el6.x86_64;
- nss-util-3.13.3-2.el6.x86_64;
- nss-softokn-freebl-3.12.9-11.el6.x86_64;

- nss-softokn-3.12.9-11.el6.x86_64;
- nss-3.13.3-6.el6.x86_64;
- nss-tools-3.13.3-6.el6.x86_64.

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

6.1.2 Pacotes SLES NSS

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

- libfreebl3-3.13.1-0.2.1;
- mozilla-nspr-4.8.9-1.2.2.1;
- mozilla-nss-3.13.1-0.2.1;
- mozilla-nss-tools-3.13.1-0.2.1.

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

6.2 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.

  Para obter informações sobre como configurar esses plug-ins do Sentinel para executar no modo FIPS 140-2, veja "Configurando os plug-ins do Sentinel para execução em modo FIPS 140-2" en la página 112.

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" en la página 117.

- Check Point (LEA) Connector 2011.1r2
- Cisco SDEE Connector 2011.1r1

- File Connector 2011.1r1: as funcionalidades CIFS e SCP envolvem criptografia e não funcionarão no modo FIPS 140-2.
- NetIQ 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, veja o site na web 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.

6.3 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.	Sección 6.4, “Cenários de implantação”, en la página 54.
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.	Sección 11.2.2, “Instalação Personalizada”, en la página 73. Sección 11.3, “Realizando uma instalação silenciosa”, en la página 75 Capítulo 18, “Ativando o modo FIPS 140-2 em uma instalação existente do Sentinel”, en la página 107
Configure os plug-ins do Sentinel para executar no Modo FIPS 140-2.	Sección 19.5, “Configurando os plug-ins do Sentinel para execução em modo FIPS 140-2”, en la página 112.
Importe certificados para o Sentinel FIPS Keystore.	Sección 19.6, “Importando certificados para o banco de dados de keystore do FIPS”, en la página 118

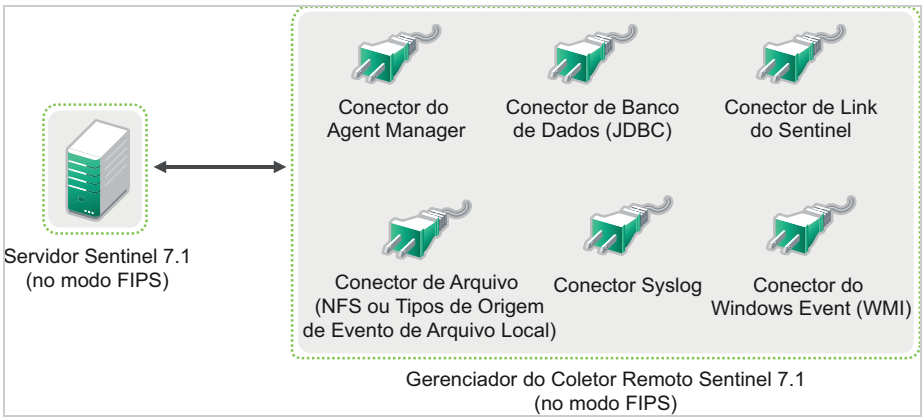
Nota: O NetIQ recomenda fortemente fazer backup dos sistemas Sentinel antes de iniciar a conversão para o modo FIPS. Se, por algum motivo, o servidor precisar ser revertido para o modo não FIPS, o único método suportado para fazer isso envolve a restauração de um backup. Para obter mais informações sobre a reversão para o modo não FIPS, veja “Revertendo o Sentinel para o modo não FIPS” en la página 118.

6.4 Cenários de implantação

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

6.4.1 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 Gerenciador de Coletor remoto. Você pode ter um ou mais Gerenciadores de Coletor remotos.



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 7.1 no modo FIPS 140-2.

   Nota: 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" en la página 107.

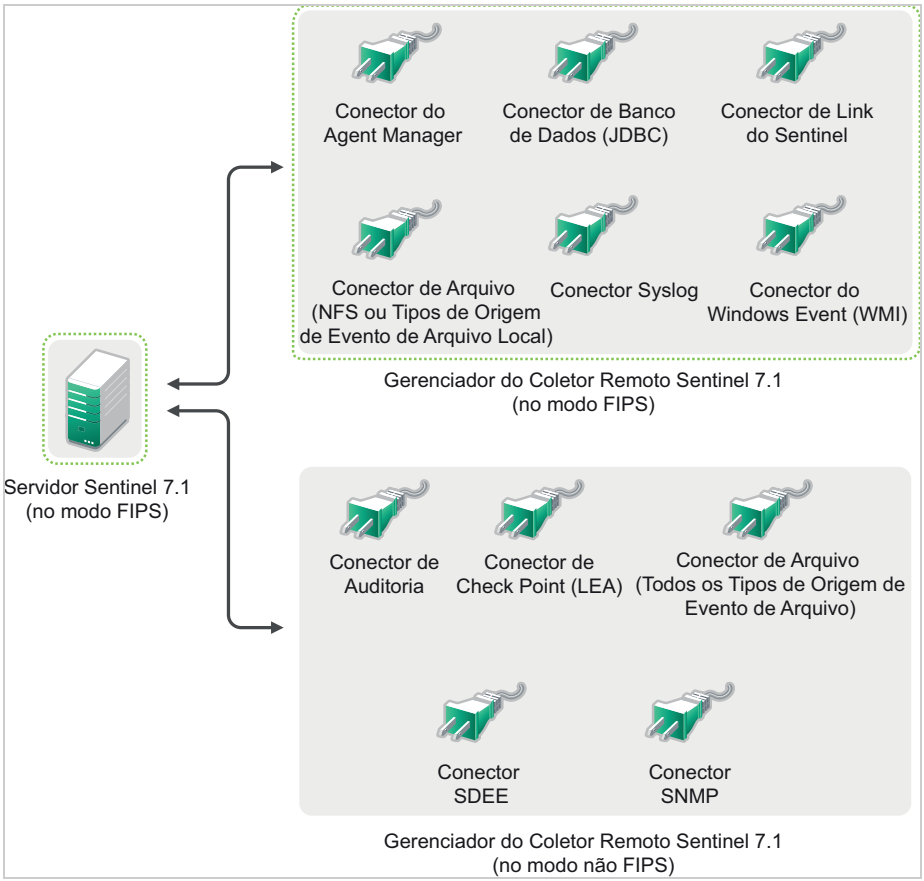
2. Um Gerenciador de Coletor remoto do Sentinel 7.1 deve estar executando no modo FIPS 140-2.

   Nota: Se o seu Gerenciador de Coletor remoto (instalado ou atualizado recentemente) estiver executando no modo não FIPS, você deverá habilitar o FIPS no Gerenciador de Coletor remoto. Para obter mais informações, consulte "Ativando o modo FIPS 140-2 nos Gerenciadores de Coletor e Mecanismos de Correlação remotos" en la página 107.

3. Certifique-se de que o servidor FIPS e os Gerenciadores de Coletor remotos comuniquem-se entre si.
4. Converta os Mecanismos de Correlação Remotos se algum deles estiver executando no modo FIPS. Para obter mais informações, consulte "Ativando o modo FIPS 140-2 nos Gerenciadores de Coletor e Mecanismos de Correlação remotos" en la página 107.
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" en la página 112.

6.4.2 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. Presumiremos que esse ambiente envolve um servidor do Sentinel e os dados são coletados por meio de um Gerenciador de Coletor remoto. Você pode ter um ou mais Gerenciadores de Coletor remotos.



Para manipular a coleta de dados usando Conectores que suportam e que não suportam o modo FIPS 140-2, é recomendado que você tenha dois Gerenciadores de Coletor remotos: um executando no modo FIPS 140-2 para Conectores com suporte para FIPS, e outro executando 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 ainda.

1 É necessário ter um servidor do Sentinel 7.1 no modo FIPS 140-2.

Nota: 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" en la página 107.

2 Certifique-se de que um Gerenciador de coletor remoto esteja sendo executando em modo FIPS 140-2 e outro Gerenciador de coletor remoto continue a ser executado no modo não FIPS.

   2a Se não tiver nenhum Gerenciador de coletor remoto ativado para o modo FIPS 140-2, você precisará habilitar o modo FIPS em um Gerenciador de coletor remoto. Para obter mais informações, consulte "Ativando o modo FIPS 140-2 nos Gerenciadores de Coletor e Mecanismos de Correlação remotos" en la página 107.

   2b Atualize o certificado do servidor no Gerenciador de Coletor remoto não FIPS. Para obter mais informações, consulte "Atualizando certificados do servidor nos Gerenciadores de Coletor e Mecanismos de Correlação remotos" en la página 111.

3 Certifique-se de que dois Gerenciadores de Coletor remotos se comuniquem com o servidor Sentinel ativado para o modo FIPS 140-2.

4 Converta os Mecanismos de Correlação remotos se algum deles estiver executando no modo FIPS. Para obter mais informações, consulte "Ativando o modo FIPS 140-2 nos Gerenciadores de Coletor e Mecanismos de Correlação remotos" en la página 107.

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" en la página 112.

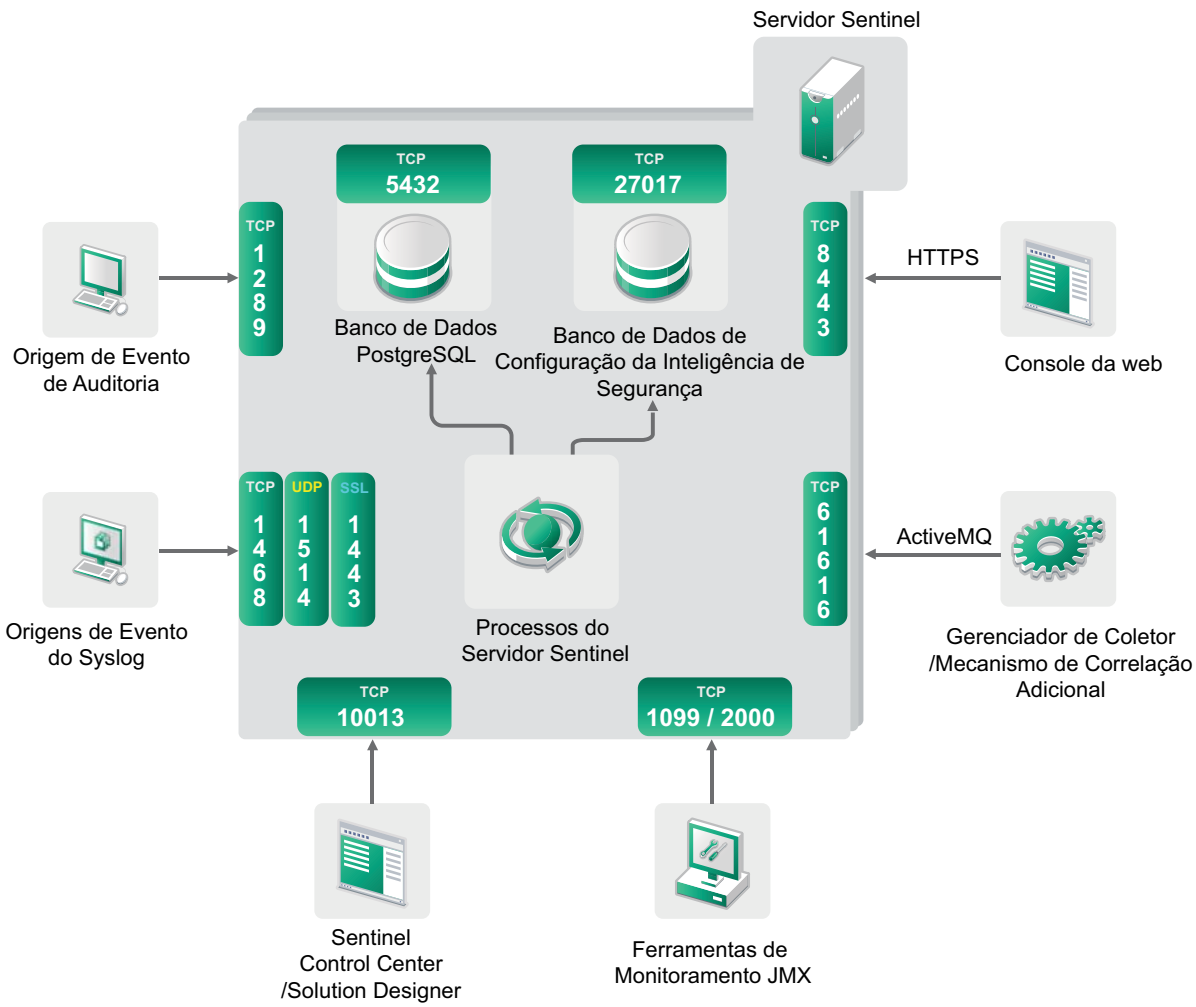
   5a Implante Conectores que suportam o modo FIPS 140-2 no Gerenciador de Coletor remoto executando no modo FIPS.

   5b Distribua os Conectores que não suportam o modo FIPS 140-2 no Gerenciador de Coletor remoto não FIPS.

7 Portas usadas

O Sentinel usa diferentes 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. A figura a seguir ilustra as portas usadas no Sentinel:

Figura 7-1 *Portas usadas no Sentinel*



7.1 Portas do servidor do Sentinel

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

7.1.1 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 a interface 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.

7.1.2 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	Entrada	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	Opcional	Usadas com ferramentas de monitoramento para conectarem-se 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	Obrigatória	Usada para comunicação HTTPS.
TCP 1443	Interno	Opcional	Usada para mensagens syslog criptografas por SSL.
TCP 61616	Interno	Opcional	Usada para conexões de entrada dos Gerenciadores de Coletor e os Mecanismos de Correlação.
TCP 10013	Interno	Obrigatório	Usadas pelo Sentinel Control Center e pelo Designer de Soluções.
TCP 1468	Interno	Opcional	Usada para mensagens syslog.
TCP 10014	Interno	Opcional	Usadas pelos Gerenciadores de Coletor remotos para conectar ao servidor por meio do proxy SSL. No entanto, isso é incomum. Por padrão, os Gerenciadores de Coletor remotos usam a porta SSL 61616 para conectar ao servidor.

Portas	Direção	Necessária/ opcional	Descrição
TCP 443	Saída	Opcional	Se o Consultor for usado, a porta iniciará uma conexão ao serviço do Consultor pela Internet para o URL de atualizações do Consultor (https://secure-www.novell.com/sentinel/download/advisor/).
TCP 8443	Externo	Opcional	Se a pesquisa distribuída 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 de rede estiver configurado para usar o NFS.
TCP 137, 138, 139, 445	Externo	Opcional	Se o armazenamento de rede estiver configurado para usar o CIFS.
TCP JDBC (dependente do banco de dados)	Externo	Opcional	Se a sincronização de dados for usada, a porta iniciará uma conexão para o banco de dados de destino usando JDBC. A porta usada depende do banco de dados de destino.
TCP 25	Externo	Opcional	Inicia uma conexão ao servidor de e-mail.
TCP 1290	Externo	Opcional	Quando o Sentinel encaminha eventos para outro sistema Sentinel, essa porta inicia uma conexão do Sentinel Link para esse sistema.
UDP 162	Externo	Opcional	Quando o Sentinel encaminha eventos para o sistema que está recebendo a detecção de SNMP, a porta envia um pacote para o receptor.
UDP 514 ou TCP 1468	Externo	Opcional	Essa porta é usada quando o Sentinel encaminha eventos para o sistema que está recebendo mensagens Syslog. Se a porta é UDP, ela envia um pacote para o receptor. Se a porta é TCP, ela inicia uma conexão ao receptor.

7.1.3 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 54984	Interno	Obrigatório	Usadas pelo Console de Gerenciamento da Aplicação do Sentinel (WebYaST). Também usada pelo serviço de atualização da aplicação do Sentinel.
TCP 289	Interno	Opcional	Encaminhada para 1289 para conexões de auditoria.
UDP 443	Interno	Opcional	Encaminhada para 8443 para comunicação HTTPS.
UDP 514	Interno	Opcional	Encaminhada para 1514 para mensagens syslog.

Portas	Direção	Necessária/ opcional	Descrição
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 NetIQ na Internet ou um serviço SMT (Subscription Management Tool) na rede.
TCP 80	Externo	Opcional	Inicia uma conexão à SMT.

7.2 Portas do Gerenciador de Coletor

O Gerenciador de Coletor usa as seguintes portas para se comunicar com outros componentes.

7.2.1 Portas de rede

Para que o Gerenciador de Coletor 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	Opcional	Usadas com ferramentas de monitoramento para conectarem-se 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.

7.2.2 Portas específicas da aplicação do Gerenciador de Coletor

Além das portas acima, as seguintes portas ficam abertas para a aplicação do Gerenciador de Coletor do Sentinel.

Portas	Direção	Necessária/ opcional	Descrição
TCP 22	Interno	Obrigatório	Usada para fornecer acesso seguro ao shell para a aplicação do Sentinel.
TCP 54984	Interno	Obrigatório	Usadas pelo Console de Gerenciamento da Aplicação do Sentinel (WebYaST). Também usada pelo serviço de atualização da aplicação do Sentinel.

Portas	Direção	Necessária/ opcional	Descrição
TCP 289	Interno	Opcional	Encaminhada para 1289 para conexões de auditoria.
UDP 514	Interno	Opcional	Encaminhada para 1514 para mensagens syslog.
TCP 1290	Interno	Opcional	Esta é a porta de vinculação do Sentinel que tem permissão para se conectar por meio do Firewall do SuSE.
UDP e TCP 40000 - 41000	Interno	Opcional	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	Externo	Obrigatório	Inicia uma conexão ao repositório de atualização do software da aplicação NetIQ na Internet ou um serviço SMT (Subscription Management Tool) na rede.
TCP 80	Externo	Opcional	Inicia uma conexão à SMT.

7.3 Portas do mecanismo de correlação

O Mecanismo de Correlação usa as seguintes portas para se comunicar com outros componentes.

7.3.1 Portas de rede

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

Portas	Direção	Necessária/ opcional	Descrição
TCP 1099 e 2000	Interno	Opcional	Usadas com ferramentas de monitoramento para conectarem-se 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.

7.3.2 Portas específicas da aplicação do Mecanismo de Correlação

Além das portas acima, as seguintes portas ficam abertas na aplicação do Mecanismo de Correlação do Sentinel.

Portas	Direção	Necessária/ opcional	Descrição
TCP 22	Interno	Obrigatório	Usada para fornecer acesso seguro ao shell para a aplicação do Sentinel.
TCP 54984	Interno	Obrigatório	Usadas pelo Console de Gerenciamento da Aplicação do Sentinel (WebYaST). Também usada pelo serviço de atualização da aplicação do Sentinel.

Portas	Direção	Necessária/ opcional	Descrição
TCP 443	Externo	Obrigatório	Inicia uma conexão ao repositório de atualização do software da aplicação NetIQ na Internet ou um serviço SMT (Subscription Management Tool) na rede.
TCP 80	Externo	Opcional	Inicia uma conexão à SMT.

8 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.

8.1 Instalação tradicional

A instalação tradicional instala o Sentinel em um sistema operacional SUSE Linux Enterprise Server (SLES) 11 ou Red Hat Enterprise Linux (RHEL) 6 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 de 90 dias.	Permite instalar com a chave de licença de 90 dias 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, veja Sección 11.2, “Executando instalações interativas”, en la página 72.

- **Silencioso:** Se você desejar instalar diversos servidores Sentinel na sua implantação, poderá registrar as opções de instalação durante a instalação padrão ou personalizada em um arquivo de configuração e usá-lo para executar uma instalação autônoma. Para obter mais informações sobre a instalação silenciosa, veja Sección 11.3, “Realizando uma instalação silenciosa”, en la página 75.

8.2 Instalação da aplicação

A instalação da aplicação instala o sistema operacional SLES 11 SP2 de 64 bits e o Sentinel.

A aplicação do Sentinel está disponível nos seguintes formatos:

- Uma imagem da aplicação VMWare
- Uma imagem do appliance Xen
- Uma imagem do DVD Live de appliance diretamente implantada em um servidor de hardware

Para obter mais informações sobre a instalação da aplicação, veja Capítulo 12, “Instalação da aplicação”, en la página 81.

III Instalando o Sentinel

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

9 Visão geral da instalação

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

- **Processo do servidor do Sentinel:** Este é o componente principal do Sentinel. O processo do servidor do Sentinel processa solicitações de outros componentes do Sentinel e viabiliza a funcionalidade perfeita do sistema. O processo do servidor do Sentinel manipula solicitações como filtragem de dados, processamento de consultas e gerenciamento de tarefas administrativas que incluem a autenticação e autorização do usuário.
- **Servidor Web:** O Sentinel usa o Jetty como seu servidor Web para conectar-se com segurança à interface da Web do Sentinel.
- **Banco de dados PostgreSQL:** O Sentinel tem um banco de dados integrado que armazena informações de configuração do Sentinel, dados de ativos e vulnerabilidade, informações de identidade, status de incidente e workflow e assim por diante.
- **Banco de dados do MongoDB:** Armazena os dados da Inteligência de Segurança.
- **Gerenciador de Coletor:** O Gerenciador de Coletor oferece um ponto flexível para coleta de dados no Sentinel. O instalador do Sentinel instala um Gerenciador de Coletor por padrão durante a instalação.
- **Mecanismo de Correlação:** O Mecanismo de Correlação processa eventos do fluxo de eventos em tempo real para determinar se eles devem acionar qualquer uma das regras de correlação.
- **Advisor:** O Advisor, desenvolvido por Security Nexus, é um serviço de inscrição de dados opcional que fornece correlação no nível do dispositivo entre eventos em tempo real de detecções de intrusão e sistemas de prevenção e resultados de exploração de vulnerabilidades da empresa. Para obter mais informações sobre o Consultor, consulte "Configurando o Consultor" no *Guia de administração do NetIQ Sentinel 7.1*.
- **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 o download dos plug-ins e atualizações adicionais do Site na Web 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;
  - Pacotes de soluções

O Sentinel tem uma arquitetura altamente escalável e, se altas taxas de eventos forem esperadas, você poderá distribuir componentes por várias máquinas para obter o melhor desempenho do sistema. A expansão independente de componentes proporciona escalabilidade e desempenho com excelente relação custo-benefício.

9.1 Vantagens de Gerenciadores de Coletor adicionais

Você pode instalar os Gerenciadores de Coletor adicionais nos locais adequados na rede. Esses Gerenciadores de Coletor remotos executam Conectores e Coletores e encaminham os dados coletados ao servidor do Sentinel para armazenamento e processamento. Para obter informações sobre a instalação de Gerenciadores de Coletor adicionais, consulte Sección 11.6, “Instalando Gerenciadores de Coletor e Mecanismos de Correlação adicionais”, en la página 78.

A instalação de mais de um Gerenciador de Coletor em uma rede distribuída oferece diversas vantagens:

- **Melhor desempenho do sistema:** Os Gerenciadores de Coletor 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 os Gerenciadores de Coletor estiverem co-localizados com fontes de eventos, então a filtragem, criptografia e compactação de dados pode ser realizada na origem.
- **Cache de arquivos:** Os Gerenciadores de Coletor 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.

Nota: Não é possível instalar mais do que um Gerenciador de Coletor em um único sistema. Você pode instalar Gerenciadores de Coletor adicionais nos sistemas remotos, e conectá-los ao servidor do Sentinel.

9.2 Vantagens dos mecanismos de correlação adicional

Você pode implementar vários Mecanismos de Correlação, 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 Mecanismo de correlação e reimplementar algumas regras no novo Mecanismo de correlação. Vários Mecanismos de Correlação fornecem a capacidade de escalar à medida que o sistema Sentinel incorpora origens de dados adicionais ou à medida que as taxas de evento aumentam. Para obter informações sobre como instalar Mecanismos de Correlação adicionais, veja Sección 11.6, “Instalando Gerenciadores de Coletor e Mecanismos de Correlação adicionais”, en la página 78.

Nota: Não é possível instalar mais do que um Mecanismo de Correlação em um único sistema. Você pode instalar Mecanismos de Correlação adicionais nos sistemas remotos, e conectá-los ao servidor do Sentinel.

10 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”, en la página 35.
- ❒ 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 Apéndice C, “Desinstalando”, en la página 153.
- ❒ Se você pretende instalar a versão licenciada, obtenha a chave de licença do Centro de Atendimento ao Cliente da Novell.
- ❒ Confirme se as portas listadas em Capítulo 7, “Portas usadas”, en la 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:**
  - ❒ Certifique-se de que o protocolo IPv6 está ativado no seu sistema operacional. Se o IPv6 não estiver ativado, componentes importantes não funcionarão corretamente.
  - ❒ O sistema operacional do servidor do Sentinel deve incluir, pelo menos, os componentes do Servidor Base do servidor SLES ou do servidor RHEL 6. O Sentinel exige as versões de 64 bits dos seguintes RPMs:
    - bash
    - bc
    - coreutils
    - gettext
    - glibc
    - grep
    - libgcc
    - libstdc

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

11 Instalação tradicional

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

11.1 Compreendendo as opções de instalação

`./install-sentinel --help` exibe as seguintes opções:

Opções	Valor	Descrição
--location	Diretório	Especifica um diretório diferente do root (/) para instalar o Sentinel.
-m, --manifest	Nome do arquivo	Especifica um arquivo de manifesto do produto a usar em vez do arquivo de manifesto padrão.
--no-configure		Especifica para não configurar o produto após a instalação.
-n, --no-start		Especifica para não iniciar ou reiniciar o Sentinel depois da instalação ou configuração.
-r, --recordunattended	Nome do arquivo	Especifica um arquivo para registrar os parâmetros que podem ser usados para instalação independente.
-u, --unattended	Nome do arquivo	Usa os parâmetros do arquivo especificado para instalar o Sentinel em sistemas independentes.
-h, --help		Exibe as opções que podem ser usadas durante a instalação do Sentinel.
-l, --log-file	Nome do arquivo	Registra mensagens de log em um arquivo.
--no-banner		Suprime a exibição da mensagem de faixa.
-q, --quiet		Exibe nenos mensagens.
-v, --verbose		Exibe todas as mensagens durante a instalação.

11.2 Executando instalações interativas

Esta seção fornece informações sobre instalação padrão e personalizada.

11.2.1 Instalação padrão

Use as seguintes etapas para executar uma instalação padrão:

1. Faça download do arquivo de instalação do Sentinel na página Downloads da Novell (http://download.novell.com/index.jsp):
   - **1a** No campo *Produto ou tecnologia*, navegue para selecionar *SIEM-Sentinel*.
   - **1b** Clique em *Pesquisar*.
   - **1c** Clique no botão na coluna *Download* para *Avaliação do Sentinel 7.1*.
   - **1d** Clique em *continuar com o download* e especifique seu nome e senha de cliente.
   - **1e** Clique em *download* para obter a versão de instalação para sua plataforma.
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 `yes` ou `y` 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 de 90 dias incluída com o instalador. Essa chave de licença ativa o conjunto completo de recursos do produto por um período de teste de 90 dias. A qualquer momento durante ou após o período de teste, 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 da web do Sentinel, especifique o seguinte URL no seu navegador:

`https://<IP_Address_Sentinel_server>:8443.`

O <*endereço_IP_servidor_Sentinel*> é o endereço IP ou o nome DNS do servidor do Sentinel, e 8443 é a porta padrão para o servidor do Sentinel.

11.2.2 Instalação Personalizada

Se você estiver instalando o Sentinel com uma configuração personalizada, será possível especificar a chave de licença, alterar a senha dos diversos usuários e especificar os valores para diferentes portas usadas para interagir com os componentes internos.

1 Faça download do arquivo de instalação do Sentinel na página Downloads da Novell:

- **1a** No campo *Produto ou tecnologia*, navegue para selecionar *SIEM-Sentinel*.
- **1b** Clique em *Pesquisar*.
- **1c** Clique no botão na coluna *Download* para *Avaliação do Sentinel 7.1*.
- **1d** Clique em *continuar com o download* e especifique seu nome e senha de cliente.
- **1e** Clique em *download* para obter a versão de instalação para sua plataforma.

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 na raiz do diretório extraído para instalar o Sentinel.

`./install-sentinel`

ou

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

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

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 `yes` ou `y` 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 padrão de avaliação de 90 dias.

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 você deseja habilitar o Sentinel no modo FIPS 140-2***, pressione `s`.

15a Especifique uma senha forte para o banco de dados de keystore e confirme a senha novamente.

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

15c Conclua a configuração do modo FIPS 140-2 seguindo as tarefas mencionadas no Capítulo 19, “Operando o Sentinel no modo FIPS 140-2”, en la página 109

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 da web do Sentinel, especifique o seguinte URL no seu navegador:

`https://<IP_Address_Sentinel_server>:8443.`

O <*endereço_IP_servidor_Sentinel*> é o endereço IP ou o nome DNS do servidor do Sentinel, e 8443 é a porta padrão para o servidor do Sentinel.

11.3 Realizando uma instalação silenciosa

A instalação silenciosa ou autônoma será útil se for necessário instalar mais de um servidor do Sentinel em sua implantação. Em cenários como esse, você pode registrar os parâmetros de instalação durante a instalação interativa e depois executar o arquivo registrado nos outros servidores. É possível gravar os parâmetros de instalação durante a instalação do Sentinel com a configuração padrão ou uma configuração personalizada.

Para realizar a instalação silenciosa, você deve ter gravado os parâmetros de instalação em um arquivo. Para obter informações sobre a criação do arquivo de resposta, consulte Sección 11.2.1, “Instalação padrão”, en la página 72 ou Sección 11.2.2, “Instalação Personalizada”, en la página 73.

Para habilitar o Sentinel no modo FIPS 140-2, certifique-se de que o arquivo de resposta inclua os seguintes parâmetros:

- ENABLE_FIPS_MODE
- NSS_DB_PASSWORD

Para executar uma instalação silenciosa, use as seguintes etapas:

1. Faça download dos arquivos de instalação na página Downloads da Novell.
2. Efetue login como `root` no servidor em que deseja instalar o Sentinel.
3. Especifique o seguinte comando para extrair os arquivos de instalação do arquivo tar:

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

   Substitua <*nome_arquivo_instalação*> pelo nome real do arquivo de instalação.
4. Especifique o seguinte comando para instalar o Sentinel em modo silencioso:

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

   A instalação prossegue com os valores armazenados no arquivo de resposta.
5. **Se você optou por ativar o modo FIPS 140-2,** conclua a configuração do modo FIPS 140-2 seguindo as tarefas mencionadas no Capítulo 19, “Operando o Sentinel no modo FIPS 140-2”, en la página 109.

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.

11.4 Instalando o Sentinel como um usuário não raiz

Se a política organizacional não permitir que você execute a instalação completa do Sentinel como `root`, será possível instalá-lo como outro usuário. Nessa instalação, algumas etapas são executadas como um usuário `root` e, em seguida, você prossegue para a instalação do Sentinel como outro usuário criado pelo usuário `root`. Finalmente, o usuário `root` completa a instalação.

1. Faça download dos arquivos de instalação na página Downloads da Novell.
2. Especifique o seguinte comando na linha de comando para extrair os arquivos de instalação do arquivo tar:

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

   Substitua <*nome_arquivo_instalação*> pelo nome real do arquivo de instalação.
3. Efetue login como `root` no servidor em que você deseja instalar o Sentinel como `root`.

4 Especifique o seguinte comando:

```
./bin/root_install_prepare
```

Uma lista de comandos a serem executados com privilégios de root será exibida. Se você desejar que o usuário não raiz 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 Especifique o seguinte comando para mudar o usuário não root `novell` recém-criado: `novell`:

```
su novell
```

7 (Condicional) Para realizar uma instalação interativa:

7a Especifique o seguinte comando:

```
./install-sentinel
```

Para instalar o Sentinel em um local que não seja o padrão, especifique a opção --location juntamente com o comando. Por exemplo:.

```
./install-sentinel --location=/foo
```

7b Continue na Paso 9.

8 (Condicional) Para realizar uma instalação silenciosa:

8a Especifique o seguinte comando:

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

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

8b Continue na Paso 12.

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

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

10 Leia a licença do usuário final e digite `yes` ou `y` para aceitar a licença e continuar com a instalação.

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

11 Será solicitado que você especifique o modo de instalação.

- Se você escolher prosseguir com a instalação padrão, continue com Paso 8a Paso 10 em Sección 11.2.1, “Instalação padrão”, en la página 72.
- Se você escolher prosseguir com a instalação personalizada, continue com Paso 7a Paso 14 em Sección 11.2.2, “Instalação Personalizada”, en la página 73.

12 Efetue login como um usuário `root` e especifique o seguinte comando para concluir a instalação:

```
./bin/root_install_finish
```

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

Para acessar a interface da web do Sentinel, especifique o seguinte URL no seu navegador:

`https://<IP_Address_Sentinel_server>:8443.`

O <*endereço_IP_servidor_Sentinel*> é o endereço IP ou o nome DNS do servidor do Sentinel, e 8443 é a porta padrão para o servidor do Sentinel.

11.5 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 modificá-las. O script encontra-se na pasta `/opt/novell/sentinel/setup`.

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

   `./configure.sh`

2. Especifique `1` para realizar uma configuração padrão ou `2` para realizar uma configuração personalizada do Sentinel.
3. Pressione a barra de espaço para ler o contrato de licença.
4. Digite `yes` ou `y` para aceitar o contrato de licença e prosseguir com a instalação.

   A instalação poderá levar alguns segundos para carregar os pacotes de instalação.
5. Insira `1` para usar a chave de licença padrão de avaliação de 90 dias.

   ou

   Insira `2` para informar uma chave de licença adquirida do Sentinel.
6. 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 Paso 7.
   - Se desejar alterar a senha existente, insira `2`, especifique a nova senha, confirme-a e, em seguida, continue com Paso 7.
7. 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 Paso 8.
   - Se desejar alterar a senha existente, insira `2`, especifique a nova senha, confirme-a e, em seguida, continue com Paso 8.

   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.
8. 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 Paso 9.
   - Se desejar alterar a senha existente, insira `2`, especifique a nova senha, confirme-a e, em seguida, continue com Paso 9.
9. Altere as atribuições de porta para os serviços do Sentinel inseerindo o número desejado e, em seguida, especificando o novo número da porta.
10. Depois de alterar as portas, especifique 7 para concluir.
11. 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`.

11.6 Instalando Gerenciadores de Coletor e Mecanismos de Correlação adicionais

Por padrão, o Sentinel instala um Gerenciador de Coletor e um Mecanismo de Correlação. Dependendo do seu ambiente, talvez você precise de Gerenciadores de Coletor e Mecanismos de Correlação adicionais. Para obter informações sobe as vantagens dos Gerenciadores de Coletor e Mecanismos de Correlação adicionais, veja Sección 9.1, “Vantagens de Gerenciadores de Coletor adicionais”, en la página 68 e Sección 9.2, “Vantagens dos mecanismos de correlação adicional”, en la página 68.

Importante: Você deve instalar o Gerenciador de Coletor ou o Mecanismo de Correlação adicional em sistemas separados: O Gerenciador de Coletor remoto ou o Mecanismo de Correlação remoto não deve estar no mesmo sistema no qual o servidor Sentinel está instalado.

11.6.1 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 a Capítulo 5, “Atendendo aos requisitos do sistema”, en la página 35.
- ❒ Sincronize o horário usando o protocolo NTP (Network Time Protocol).
- ❒ Os Gerenciadores de Coletor exigem conectividade de rede na porta de barramento de mensagens (61616) no servidor do Sentinel. Antes de iniciar a instalação do Gerenciador de Coletor, certifique-se de que todas as configurações do firewall e de rede podem se comunicar através dessa porta.

11.6.2 Instalando Gerenciadores de Coletor e Mecanismos de Correlação adicionais

1. Inicie a interface da web do Sentinel especificando o seguinte URL em seu navegador:

   `https://<IP_Address_Sentinel_server>:8443.`

   O *<endereço_IP_servidor_Sentinel>* é o endereço IP ou o nome DNS do servidor do Sentinel, e 8443 é a porta padrão para o 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. No cabeçalho do Gerenciador de Coletor, clique em *Download dp Instalador*.

4 Clique em *Salvar Arquivo* para salvar o instalador no local desejado.

5 Especifique o seguinte comando para extrair o arquivo de instalação.

```
tar zxvf <install_filename>
```

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

6 Mude para o diretório no qual extraiu o instalador.

7 Especifique o comando a seguir para instalar o Gerenciador de Coletor ou os Mecanismos de Correlação:

Para o Gerenciador do Coletor:

```
./install-cm
```

Para o Mecanismo de Correlação:

```
./install-ce
```

O script de instalação primeiro verifica a memória disponível e o espaço em disco. Se a memória disponível for menor do que 1.5 GB, o script terminará a instalação automaticamente.

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

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

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

10 Digite `yes` ou `y` para aceitar o contrato de licença e prosseguir com a instalação.

A instalação poderá levar alguns segundos antes de solicitar o tipo de configuração.

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

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

13 Especifique o nome de usuário e senha do Gerenciador de Coletor ou do Mecanismo de Correlação.

O nome de usuário e a senha estão armazenados no arquivo `/<install_dir>/etc/opt/novell/sentinel/config/activemqusers.properties` localizado no servidor do Sentinel.

14 Quando solicitado, aceite o certificado permanentemente.

15 Insira `yes`(sim) ou `y` (s) para habilitar o modo FIPS 140-2 no Sentinel e continue com a configuração do FIPS.

16 Continue com a instalação, como solicitado, até que ela esteja concluída.

11.6.3 Adicionando um usuário personalizado ao Gerenciador de Coletor ou Mecanismo de Correlação.

O Sentinel recomenda que você use os nomes de usuário padrão para o Gerenciador de Coletor e Mecanismo de Correlação remotos. No entanto, se você tiver vários Gerenciadores de Coletor remotos instalados e desejar identificá-los sepradamente, poderá criar novos usuários:

1 Efetue login no servidor como o usuário que tem acesso aos arquivos de instalação do Sentinel.

2 Abra o arquivo `activemqgroups.properties`.

Esse arquivo está localizado no diretório `/<install_dir>/etc/opt/novell/sentinel/config/`.

3 Adicione os novos nomes de usuário separados por vírgula, como segue:

Para o Gerenciador de Coletor, adicione os novos usuários na seção cm. Por exemplo:

```
cm=collectormanager,cmuser1,cmuser2,...
```

Para o Mecanismo de Correlação, adicione os novos usuários na seção admins. Por exemplo:

```
admins=system,correlationengine,ceuser1,ceuser2,...
```

4. Grave e feche o arquivo.
5. Abra o arquivo `activemqusers.properties`.

   Esse arquivo está localizado no diretório `/<install_dir>/etc/opt/novell/sentinel/config/`.
6. Adicione a senha para o usuário que você criou em Paso 3.

   A senha pode ser qualquer string aleatório. Por exemplo:

   Para os usuários do Gerenciador de Coletor:

   ```
   system=c7f34372ecd20d831cceb29e754e5ac9
   collectormanager=1c51ae56
   cmuser1=1b51de55
   cmuser2=1a51ce57
   ```

   Para os usuários do Mecanismo de Correlação:

   ```
   system=c7f34372ecd20d831cceb29e754e5ac9
   correlationengine=68790d7a
   ceuser1=69700c6d
   ceuser2=70701b5c
   ```
7. Grave e feche o arquivo.
8. Reinicie o servidor do Sentinel.

12 Instalação da aplicação

A aplicação Sentinel é uma aplicação de software pronta para execução integrada no SUSE Studio. A aplicação combina um sistema operacional SUSE Linux Enterprise Server (SLES) 11 SP 2 robusto e o serviço de atualização integrado do software Sentinel para fornecer uma experiência de usuário fácil e eficiente que permite que os clientes aproveitem os investimentos existentes. A aplicação de software pode ser instalada tanto no hardware quanto em um ambiente virtual.

12.1 Instalando a aplicação VMware

Esta seção fornece informações sobre a instalação do Sentinel, Gerenciador de Coletor e Mecanismo de Correlação em um servidor VMware ESX.

12.1.1 Instalando o Sentinel

Use as etapas a seguir para instalar o Sentinel em um servidor VMware ESX:

1. Faça download do arquivo de instalação da aplicação VMware no site de Download da Novell.

   O arquivo correto da aplicação VMware possui `vmx` em seu nome. Por exemplo, `sentinel_server_7.1.0.0.x86_64.vmx.tar.gz`
2. Estabeleça um armazenamento de dados do ESX onde a imagem da aplicação possa ser instalada.
3. Efetue login como Administrador no servidor em que deseja instalar a aplicação.
4. Especifique o seguinte comando para extrair a imagem compactada da aplicação a partir da máquina onde o VM Converter está instalado:

   ```
   tar zxvf <install_file>
   ```

   Substitua *<arquivo_instalação>* pelo nome real do arquivo.
5. Para importar a imagem VMware no servidor ESX, use o VMware Converter e siga as instruções na tela do assistente de instalação.

6 Efetue login na máquina do servidor ESX.

7 Selecione a imagem VMware importada da aplicação e clique no ícone *Ligar*.

8 Selecione o idioma desejado e clique em *Avançar*.

9 Selecione o layout do teclado e clique em *Avançar*.

10 Leia e aceite o Contrato de Licença do Software SUSE Linux Enterprise Server (SLES) 11 SP2.

11 Leia e aceite o Contrato de Licença do Usuário Final do NetIQ Sentinel.

12 Na tela Nome de Host e Nome de Domínio, especifique o nome de host e o nome de domínio. Certifique-se de que a opção *Atribuir nome do host ao IP de loopback* esteja selecionada.

13 Clique em *Avançar*. As configurações do nome de host são gravadas.

14 Siga um destes procedimentos:

- Para usar as configuraçõs atuais da conexão de rede, selecione *Usar configuração a seguir* na página Configuração de Rede II e, em seguida, clique em *Avançar*.
- Para mudar as configurações de conexão de rede, selecione *Alterar*, faça as mudanças desejadas e, em seguida, clique em *Avançar*.

As configurações de conexão da rede serão gravadas.

15 Defina a data e o horário e clique em *Avançar*.

Para mudar a configuração NTP após a instalação, use YaST na linha de comando da aplicação. O WebYast pode ser usado para mudar a data e o horário, mas não a configuração NTP.

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

```
rcntp restart
```

16 Defina a senha `root` e clique em *Avançar*.

A instalação verifica a memória e o espaço em disco disponíveis. Se a memória disponível for menor do que 2.5 GB, a instalação não permitirá que você prossiga e o botão *Avançar* estará em cinza.

Se a memória disponível for maior do que 2,5 GB, mas menor do que 6,7 GB, a instalação exibirá uma mensagem informando que você tem menos memória do que o recomendado. Quando essa mensagem for exibida, clique em *Avançar* para prosseguir com a instalação.

17 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 de uma única vez. Aguarde até que a instalação termine antes de efetuar login no servidor.

18 Anote o endereço IP da aplicação, exibido no console.

19 Avance para a Sección 12.4, “Configuração pós-instalação para a aplicação”, en la página 89.

12.1.2 Instalando Gerenciadores de Coletor e Mecanismos de Correlação adicionais

O procedimento para instalar um Gerenciador de coletor ou um Mecanismo de correlação é o mesmo, exceto que você precisa fazer download do arquivo apropriado no site de download da Novell.

1 Faça download do arquivo de instalação da aplicação VMware no site de Download da Novell (http://download.novell.com/index.jsp).

O arquivo correto da aplicação VMware possui `vmx` em seu nome. Por exemplo, `sentinel_collector_manager_7.1.0.0.x86_64.vmx.tar.gz`

2. Estabeleça um armazenamento de dados do ESX onde a imagem da aplicação possa ser instalada.
3. Efetue login como Administrador no servidor em que deseja instalar a aplicação.
4. Especifique o seguinte comando para extrair a imagem compactada da aplicação a partir da máquina onde o VM Converter está instalado:

   `tar zxvf <install_file>`

   Substitua *<arquivo_instalação>* pelo nome real do arquivo.
5. Para importar a imagem VMware no servidor ESX, use o VMware Converter e siga as instruções na tela do assistente de instalação.
6. Efetue login na máquina do servidor ESX.
7. Selecione a imagem VMware importada da aplicação e clique no ícone *Ligar*.
8. Especifique o nome de host/endereço IP do servidor do Sentinel ao qual o Gerenciador de Coletor deverá se conectar.
9. Especifique o número da porta do Servidor de Comunicação. A porta padrão de barramento de mensagem é `61616`.
10. Especifique o nome de usuário do JMS, que é o nome de usuário do Gerenciador de Coletor e Mecanismo de Correlação. O nome de usuário padrão é collectormanager para o Gerenciador de Coletor e correlationengine para o Mecanismo de Correlação.
11. Especifique a senha do usuário do JMS.

    O nome do usuário e senha estão armazenados no arquivo `/<dir_instalação>/etc/opt/novell/sentinel/config/activemqusers.properties`, que está localizado no servidor do Sentinel.
12. (Opcional) Para verificar a senha, veja a seguinte linha em `activemqusers.properties`

    Para o Gerenciador do Coletor:

    `collectormanager=<password>`

    Nesse exemplo, `collectormanager` é o nome de usuário, e o valor correspondente é a senha.

    Para o Mecanismo de Correlação:

    `correlationengine=<password>`

    Nesse exemplo, `correlationengine` é o nome de usuário, e o valor correspondente é a senha.
13. Clique em *Avançar*.
14. Aceite o certificado.
15. Clique em *Avançar* para concluir a instalação.

    Quando a instalação está concluída, o instalador exibe uma mensagem indicando que essa aplicação é o Gerenciador de Coletor do Sentinel ou Mecanismo de Correlação 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.

12.1.3 Instalando o VMware Tools

Para que o Sentinel funcione efetivamente no servidor VMware, é preciso instalar o VMware Tools. O VMware Tools é um conjunto de utilitários que aprimora o desempenho do sistema operacional da máquina virtual. Ele também aprimora o gerenciamento da máquina virtual. Para obter mais informações sobre a instalação do VMware Tools, consulte VMware Tools para convidados do Linux (https://www.vmware.com/support/ws55/doc/ws_newguest_tools_linux.html#wp1127177).

Para obter mais informações sobre a documentação do VMware, consulte o Manual do Usuário da estação de trabalho (http://www.vmware.com/pdf/ws71_manual.pdf).

12.2 Instalando a aplicação Xen

Esta seção fornece informações sobre a instalação do Sentinel, Gerenciador de coletor e Mecanismo de correlação em uma imagem da aplicação Xen.

- Sección 12.2.1, “Instalando o Sentinel”, en la página 84
- Sección 12.2.2, “Instalando Gerenciadores de Coletor e Mecanismos de Correlação adicionais”, en la página 86

12.2.1 Instalando o Sentinel

Use as etapas a seguir para instalar o Sentinel em uma imagem da aplicação Xen:

1. Faça download do arquivo de instalação da aplicação virtual Xen no site de Download da Novell (http://download.novell.com/index.jsp) para `/var/lib/xen/images`.

   O nome do arquivo correto da aplicação virtual Xen tem `xen` no nome do arquivo. Por exemplo, `Sentinel_7.1.0.0.x86_64.xen.tar.gz`.

2. Especifique o comando a seguir para descompactar o arquivo:

   ```
   tar -zxvf <install_file>
   ```

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

3. Vá para o novo diretório de instalação. O diretório contém os seguintes arquivos:
   - *<nome_arquivo>*`.raw`
   - *<nome_arquivo>*`.xenconfig`

4. Abra o arquivo *<nome_arquivo>*`.xenconfig` usando um editor de texto.

5. Modifique o arquivo da seguinte maneira:
   - Especifique o caminho completo do arquivo `.raw` na configuração de `disk`.
   - Especifique a configuração de ponte para a configuração da rede. Por exemplo, `"bridge=br0"` ou `"bridge=xenbr0"`.
   - Especifique os valores para as configurações de `name` e `memory`.

     Por exemplo:

     ```
     # -*- mode: python; -*-
     name="Sentinel_7.1.0.0.x86_64"
     memory=4096
     ```

   - Comente a seguinte linha:

     ```
     vfb=["type=vnc,vncunused=1,vnclisten=0.0.0.0"]
     ```

- Adicione a linha a seguir:

  ```
  extra = "console=hvc0 xencons=tty"
  ```

O arquivo `xenconfig` atualizado deve ser como segue:

```
# -*- mode: python; -*-
name=install_file_name
memory=4096
disk=["tap:aio:/var/lib/xen/images/install_directory/install_filename]
vif=[ "bridge=br0" ]
#vfb=["type=vnc,vncunused=1,vnclisten=0.0.0.0"]
extra = "console=hvc0 xencons=tty"
```

6 Após modificar o arquivo *<nome_arquivo>*`.xenconfig`, especifique o seguinte comando para criar a MV:

```
xm create <file_name>.xenconfig
```

7 (Opcional) Para verificar se a MV foi criada, especifique o seguinte comando:

```
xm list
```

O VM é exibido na lista que é gerada.

Por exemplo, se você configurou `name="Sentinel_7.1.0.0.x86_64"` no arquivo `.xenconfig`, então a VM aparecerá com este nome.

8 Para iniciar a instalação, especifique este comando:

```
xm console <vm name>
```

Substitua *<nome_mv>* pelo nome especificado na configuração de nome do arquivo `.xenconfig`, que também é o valor retornado na Etapa 7. Por exemplo:

```
xm console Sentinel_7.1.0.0.x86_64
```

A instalação primeiro verifica a memória e o espaço em disco disponíveis. Se a memória disponível for menor do que 2.5 GB, a instalação será automaticamente encerrada. Se a memória disponível for maior do que 2,5 GB, mas menor do que 6,7 GB, a instalação exibirá uma mensagem informando que você tem menos memória do que o recomendado. Digite `y` se quiser continuar com a instalação ou digite `n` se não quiser prosseguir.

9 Selecione o idioma desejado e clique em *Avançar*.

10 Selecione o layout do teclado e clique em *Avançar*.

11 Leia e aceite o Contrato de Licença do Software SUSE Linux Enterprise Server (SLES) 11 SP2.

12 Leia e aceite o Contrato de Licença do Usuário Final do NetIQ Sentinel.

13 Na tela Nome de Host e Nome de Domínio, especifique o nome de host e o nome de domínio. Certifique-se de que a opção *Atribuir nome do host ao IP de loopback* esteja selecionada.

14 Selecione *Avançar*. As configurações do nome de host são gravadas.

15 Siga um destes procedimentos:

- Para usar as configurações de conexão da rede atuais, selecione *Usar a seguinte configuração* na tela *Configuração de Rede II*.
- Para mudar as configurações de conexão de rede, selecione *Mudar* e faça as mudanças desejadas.

16 Selecione *Avançar*. As configurações de conexão da rede serão gravadas.

17 Defina a data e o horário, clique em *Avançar* e em *Concluir*

Para mudar a configuração NTP após a instalação, use YaST na linha de comando da aplicação. O WebYast pode ser usado para mudar a data e o horário, mas não a configuração NTP.

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

```
rcntp restart
```

18 Defina a senha `root` do SUSE Enterprise Server e clique em *Avançar*.

19 Configure a senha do administrador do Sentinel e, em seguida, clique em *Avançar*.

A instalação do Sentinel prossegue e conclui. 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.

Anote o endereço IP da aplicação, exibido no console.

20 Avance para a Sección 12.4, “Configuração pós-instalação para a aplicação”, en la página 89.

12.2.2 Instalando Gerenciadores de Coletor e Mecanismos de Correlação adicionais

O procedimento para instalar um Gerenciador de coletor ou um Mecanismo de correlação é o mesmo, exceto que você precisa fazer download do arquivo apropriado no site de download da Novell.

1 Conclua Paso 1 aPaso 14 em Sección 12.2.1, “Instalando o Sentinel”, en la página 84.

2 Na tela Network Configuration II (Configuração de Rede II), selecione *Change* (Alterar) e especifique o endereço IP da máquina virtual em que você deseja instalar o Gerenciador de Coletor ou Mecanismo de Correlação adicional.

3 Especifique a máscara de sub-rede do IP especificado.

4 Selecione *Avançar*. As configurações de conexão da rede serão gravadas.

5 Defina a data e o horário e selecione *Avançar*.

Para mudar a configuração NTP após a instalação, use YaST na linha de comando da aplicação. O WebYast pode ser usado para mudar a data e o horário, mas não a configuração NTP.

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

```
rcntp restart
```

6 Defina a senha `root` do SUSE Enterprise Server e, em seguida, selecione *Avançar*.

7 Especifique o nome de host/endereço IP do servidor do Sentinel ao qual o Gerenciador de Coletor ou Mecanismo de Correlação deve se conectar.

8 Especifique o número da porta do servidor de comunicação. A porta padrão de barramento de mensagem é `61616`.

9 Especifique o nome de usuário do JMS, que é o nome de usuário do Gerenciador de Coletor e Mecanismo de Correlação.

10 Especifique a senha do usuário do JMS.

O nome de usuário e a senha estão armazenados no arquivo `/<install_dir>/etc/opt/novell/sentinel/config/activemqusers.properties` localizado no servidor do Sentinel.

11 (Opcional) Para verificar a senha, veja a seguinte linha no arquivo `activemqusers.properties`

Para o Gerenciador do Coletor:

```
collectormanager=<password>
```

Nesse exemplo, `collectormanager` é o nome de usuário, e o valor correspondente é a senha.

Para o Mecanismo de Correlação:

```
correlationengine=<password>
```

Nesse exemplo, `correlationengine` é o nome de usuário, e o valor correspondente é a senha.

12 Selecione *Avançar* para concluir a instalação.

Quando a instalação está concluída, o instalador exibe uma mensagem indicando que essa aplicação é o Gerenciador de Coletor do Sentinel ou o Mecanismo de Correlação do Sentinel dependendo do que você escolheu instalar, junto com o endereço IP.

12.3 Instalação do aplicação ISO

Antes de instalar a aplicação no hardware, certifique-se de que a imagem ISO do disco da aplicação foi obtida no site de suporte, foi descompactada e está disponível em um DVD.

Importante: A instalação no hardware usando a imagem de disco ISO (bare metal e Hyper-V) exige memória de, no mínimo, 4,5 GB para a conclusão da instalação.

- Sección 12.3.1, “Instalando o Sentinel”, en la página 87
- Sección 12.3.2, “Instalando Gerenciadores de Coletor e Mecanismos de Correlação adicionais”, en la página 88

12.3.1 Instalando o Sentinel

Use as etapas a seguir para instalar a aplicação Sentinel no hardware:

1 Inicialize a máquina física a partir da unidade de DVD contendo o disco.

2 Use as instruções na tela do assistente de instalação.

3 Execute a imagem da aplicação no DVD Ativo selecionando a primeira entrada no menu de inicialização.

A instalação primeiro verifica a memória e o espaço em disco disponíveis. Se a memória disponível for menor do que 2.5 GB, a instalação será automaticamente encerrada. Se a memória disponível for maior do que 2,5 GB, mas menor do que 6,7 GB, a instalação exibirá uma mensagem informando que você tem menos memória do que o recomendado. Digite `y` se quiser continuar com a instalação ou digite `n` se não quiser prosseguir.

4 Selecione o idioma desejado e clique em *Avançar*.

5 Selecione o layout do teclado e clique em *Avançar*.

6 Leia e aceite o Contrato de Licença do Software SUSE Enterprise Server.

7 Leia e aceite o Contrato de Licença do Usuário Final do NetIQ Sentinel.

8 Selecione *Avançar*.

9 Na tela Nome de Host e Nome de Domínio, especifique o nome de host e o nome de domínio. Certifique-se de que a opção *Atribuir nome do host ao IP de loopback* esteja selecionada.

10 Selecione *Avançar*. As configurações de nome de host são gravadas.

11 Siga um destes procedimentos:

- Para usar as configurações atuais de conexão da rede, selecione *Usar a seguinte configuração* na tela Configuração de Rede II.
- Para mudar as configurações de conexão de rede, selecione *Mudar* e faça as mudanças desejadas.

12 Selecione *Avançar*. As configurações de conexão da rede serão gravadas.

13 Defina a data e o horário e clique em *Avançar*.

Para mudar a configuração NTP após a instalação, use YaST na linha de comando da aplicação. O WebYast pode ser usado para mudar a data e o horário, mas não a configuração NTP.

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

```
rcntp restart
```

14 Defina a senha `root` e clique em *Avançar*.

15 Configure a senha do administrador do Sentinel e, em seguida, clique em *Avançar*.

16 Digite o nome de usuário e a senha no console para efetuar login na aplicação.

O valor padrão para o nome de usuário é `root` e a senha é a senha definida em Paso 14.

17 Pare o servidor do Sentinel:

```
service sentinel stop
```

18 Insira o seguinte comando para redefinir a IU para uma exibição clara no YaST:

```
reset
```

19 Para instalar a aplicação no servidor físico, assegure-se de que a caixa de seleção *Install Sentinel appliance to hard drive (for Live DVD image only)* [Instalar aplicação do Sentinel no disco rígido (apenas para imagem do Live DVD)] esteja selecionada.

Essa caixa de seleção fica marcada por padrão. Se você anular a seleção dessa caixa de seleção, a aplicação não será instalada no servidor físico e será executada somente no modo LIVE DVD.

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.

20 Anote o endereço IP da aplicação, exibido no console.

21 Avance para a Sección 12.4, “Configuração pós-instalação para a aplicação”, en la página 89.

12.3.2 Instalando Gerenciadores de Coletor e Mecanismos de Correlação adicionais

O procedimento para instalar um Gerenciador de Coletor ou um Mecanismo de Correlação é o mesmo, exceto que você precisa fazer download do arquivo apropriado no site na Web de download da Novell.

1 Conclua Paso 1 aPaso 14 em Sección 12.3.1, “Instalando o Sentinel”, en la página 87.

2 Especifique o nome de host/endereço IP do servidor do Sentinel ao qual o Gerenciador de Coletor deverá se conectar.

3 Especifique o número da porta do servidor de comunicação. A porta padrão de barramento de mensagem é `61616`.

4 Especifique o Nome do usuário do JMS, que é o nome de usuário do Gerenciador de Coletor ou Mecanismo de Correlação.

5 Especifique a senha do usuário do JMS.

6 Clique em *Avançar*.

O nome de usuário e a senha estão armazenados no arquivo `/<install_dir>/etc/opt/novell/sentinel/config/activemqusers.properties` localizado no servidor do Sentinel.

7 Para verificar a senha, veja a seguinte linha no arquivo `activemqusers.properties`

Para o Gerenciador do Coletor:

```
collectormanager=<password>
```

Nesse exemplo, `collectormanager` é o nome de usuário, e o valor correspondente é a senha.

Para o Mecanismo de Correlação:

```
correlationengine=<password>
```

Nesse exemplo, `correlationengine` é o nome de usuário, e o valor correspondente é a senha.

8 Para instalar a aplicação no servidor físico, assegure-se de que a caixa de seleção *Instalar aplicação do Sentinel no disco rígido (apenas para imagem do Live DVD)* esteja selecionada.

Essa caixa de seleção fica marcada por padrão. Se você anular a seleção dessa caixa de seleção, a aplicação não será instalada no servidor físico e executará apenas no modo LIVE DVD.

9 Quando solicitado, aceite o certificado.

10 Insira `yes`(sim) ou `y` (s) para ativar o modo FIPS 140-2 no Sentinel e continue com a configuração do FIPS.

11 Continue com a instalação, como avisado, até que a instalação esteja concluída.

Quando a instalação está concluída, o instalador exibe uma mensagem indicando que essa aplicação é o Gerenciador de Coletor do Sentinel ou Mecanismo de Correlação 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.

12.4 Configuração pós-instalação para a aplicação

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

- Sección 12.4.1, “Configuração do WebYaST”, en la página 89
- Sección 12.4.2, “Criando partições”, en la página 90
- Sección 12.4.3, “Registrando para receber atualizações”, en la página 90
- Sección 12.4.4, “Configurando a aplicação com SMT”, en la página 91

12.4.1 Configuração do WebYaST

A interface do usuário da aplicação Sentinel é equipada com WebYaST, que é um console remoto com base na Web para controlar aplicações baseadas no SUSE Linux Enterprise. Você pode acessar, configurar e monitorar as aplicações do Sentinel com o WebYaST. O procedimento a seguir descreve brevemente as etapas para configurar o WebYaST. Para obter mais informações sobre a configuração detalhada, consulte o *Guia do Usuário do WebYaST* (http://www.novell.com/documentation/webyast/).

1 Efetue login na aplicação do Sentinel.

2 Clique em *Aplicação*.

3 Configure o Servidor do Sentinel para receber atualizações, conforme descrito na Sección 12.4.3, “Registrando para receber atualizações”, en la página 90.

4 Clique em *Avançar* para concluir a configuração inicial.

12.4.2 Criando partições

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.
9. Monte a nova partição em `/var/opt/novell/sentinel`.
10. Especifique o seguinte comando para mudar para o usuário `novell`:

    ```
    su -novell
    ```
11. Mova o conteúdo do diretório de dados do local temporário (onde foi salvo em Paso 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
    ```

12.4.3 Registrando para receber atualizações

Você deve registrar a aplicação do Sentinel com o canal de atualização da aplicação para receber atualizações de correção. Para registrar a aplicação, você deve obter o código de registro ou a chave de ativação da aplicação no Centro de Atendimento ao Cliente da Novell.

Use as etapas a seguir para registrar a aplicação para atualizações:

1. Efetue login na aplicação do Sentinel.
2. Clique em *Aplicação* para iniciar o WebYaST.
3. Clique em *Registro*.
4. Especifique o ID de e-mail no qual deseja receber atualizações e, em seguida, especifique o nome do sistema e o código de registro da aplicação.
5. Clique em *Gravar*.

12.4.4 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 Novell Customer Center e fornece os principais recursos do Novell Customer Center.

Pré-requisitos

- Obtenha as credenciais do Novell Customer Center para Sentinel para obter atualizações da Novell. Para obter informações sobre como obter as credenciais, contate Suporte da Novell.
- Certifique-se de que o SLES 11 SP2 esteja instalado com os seguintes pacotes na máquina onde você 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 seguintes seções na Documentação da 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

Para obter informações sobre a configuração da aplicação com a SMT, veja a documentação SMT (Subscription Management Tool) para SUSE Linux Enterprise 11.

Para habilitar os repositórios de aplicação, execute o seguinte comando:

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

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

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

Atualizando a aplicação

Para obter informações sobre a atualização da aplicação, veja Sección 21.3, “Atualizando o aplicativo usando SMT”, en la página 126

12.5 Parando e iniciando o servidor com o WebYaST

É possível iniciar e parar o servidor Sentinel usando a interface da Web da seguinte forma:

1. Efetue login na aplicação do Sentinel.
2. Clique em *Aplicação* para iniciar o WebYaST.
3. Clique em *System Services* (Serviços de sistema).
4. Para parar o servidor do Sentinel, clique em *parar*.
5. Para iniciar o servidor do Sentinel, clique em *iniciar*.

13 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.

13.1 Instalando um Coletor

Siga as etapas abaixo para instalar um Coletor:

1. Faça o download do Coletor desejado do site na web de plug-ins do Sentinel.
2. Efetue login na interface da web do Sentinel em https://<*endereço IP*>:8443, onde 8443 pe a porta padrão do servidor do Sentinel.
3. Clique em *aplicações* na barra de ferramentas e, em seguida, em *Aplicações*.
4. Clique em *Iniciar o Control Center* para iniciar o Sentinel Control Center.
5. Na barra de ferramentas, clique em *Gerenciamento de Fonte de Eventos* > *Tela Ativa* e, a segiur, clique em *Ferramentas* > *Importar plugin*.
6. Procure e selecione o arquivo do Coletor cujo download foi feito em Paso 1 e, em seguida, clique em *Avançar*.
7. Siga as instruções remanescentes e, em seguida, clique em *Concluir*.

Para configurar o Coletor, consulte a documentação do Coletor específico no site na web de plug-ins do Sentinel.

13.2 Instalando um Conector

Use as etapas abaixo para instalar um Conector:

1. Faça o download do Conector desejado do site na web de plug-ins do Sentinel.
2. Efetue login na interface da web do Sentinel em https://<*endereço IP*>:8443, onde 8443 pe a porta padrão do servidor do Sentinel.
3. Clique em *aplicativos* na barra de ferramentas e, em seguida, em *Aplicativos*.
4. Clique em *Iniciar o Control Center* para iniciar o Sentinel Control Center.
5. Na barra de ferramentas, selecione *Gerenciamento de Fonte de Eventos* > *Tela Ativa* e, em seguida, clique em *Ferramentas* > *Importar plugin*.

6 Procure e selecione o arquivo do Conector cujo download foi feito em Paso 1 e, em seguida, clique em *Avançar*.

7 Siga as instruções remanescentes e, em seguida, clique em *Concluir*.

Para configurar o Conector, consulte a documentação do Conector específico no site na web de plug-ins do Sentinel.

14 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:

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

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

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

  O número de porta padrão é 8443.

- Acesse a interface da web do Sentinel:

  1. Ative um browser da Web suportado.
  2. Especifique o URL da interface da web do Sentinel:

     ```
     https://<IP_Address/DNS_Sentinel_server:8443>
     ```

     O <endereço_IP/servidor_DNS_do_Sentinel> é o endereço IP ou o nome DNS do servidor do Sentinel, e 8443 é a porta padrão para o servidor do Sentinel.
  3. Efetue login com o nome do administrador e senha especificados durante a instalação. O nome de usuário padrão é admin.

15 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 ficam armazenadas nos seguintes diretórios?
  - `/opt/novell/sentinel/bin`
  - `/opt/novell/sentinel/setup`
  - `/opt/novell/sentinel/3rdparty`
- Arquivos de registro estão no diretório `/var/opt/novell/sentinel/log`
- Os arquivos de configuração estão no seguinte diretório `/etc/opt/novell/sentinel`
- O arquivo de ID do processo (PID) está no diretório `/var/run/sentinel/server.pid`.

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

IV Configurando o Sentinel

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

16 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.

16.1 Entendendo o horário no Sentinel

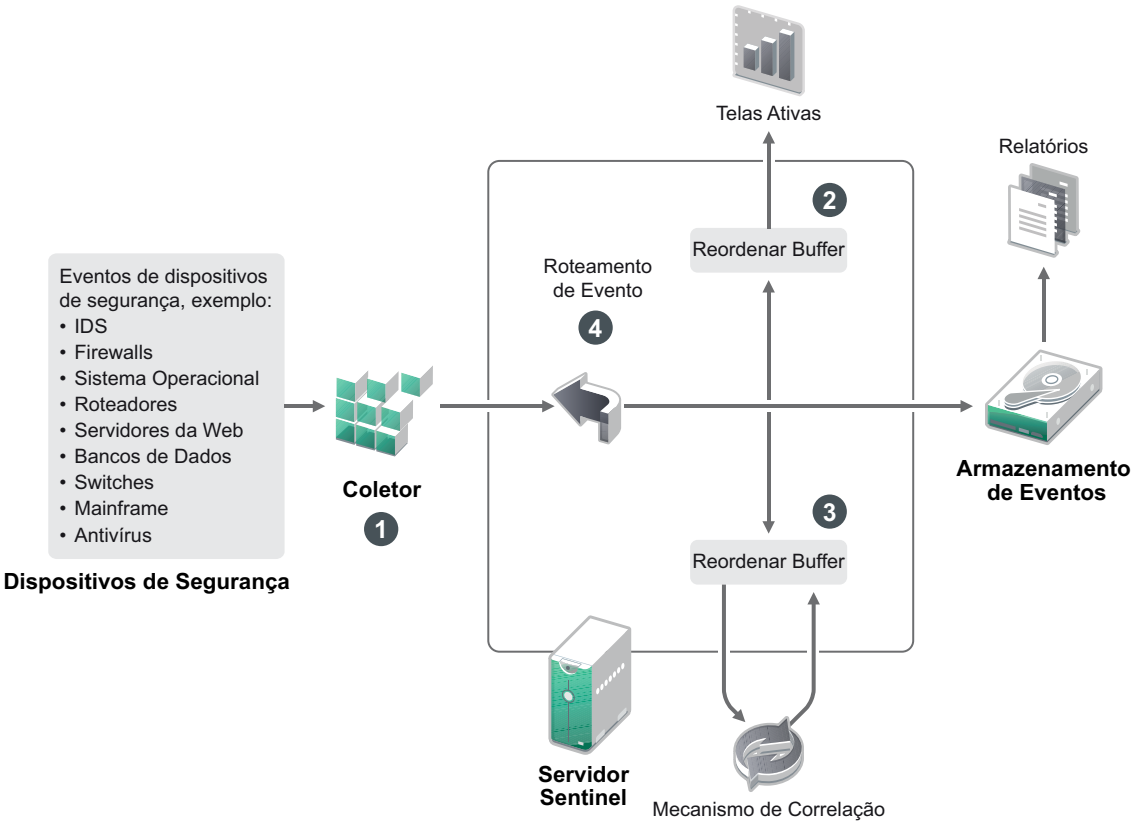
O Sentinel é um sistema distribuído, composto por vários processos distribuídos por toda a sua rede. Além disso, podem ocorrer certos atrasos introduzidos pela fonte de eventos. Para lidar com essa situação, os processos do Sentinel reordenam os eventos em um fluxo ordenado por horários antes de realizar 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 Gerenciador de coletor.
- **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 a seguir explica como o Sentinel faz isso:

Figura 16-1 *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. Eventos com Horários de evento com variações de 5 minutos em relação ao horário do servidor (para passado ou futuro) são processados normalmente pelas Telas ativas. Os eventos com Horários de evento mais de 5 minutos no futuro não são exibidos nas Telas ativas, 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 Mecanismo de correlação 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 Mecanismo de correlação não processará os eventos.
4. Se o Horário do evento é mais antigo do que 5 minutos em relação ao horário do sistema do Gerenciador de coletor, o Sentinel faz o roteamento direto dos eventos para o armazenamento de eventos, ignorando sistemas em tempo real como Correlação, Telas ativas e Inteligência de segurança.

16.2 Configurando o horário no Sentinel

O Mecanismo de Correlação 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 Gerenciador de Coletor e desmarque *Horário da Fonte de Eventos Confiável* na fonte de eventos, no Gerenciador de Fonte de Eventos. O Sentinel usa o Gerenciador de Coletor 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 NetIQ Sentinel 7.1*.
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.

16.3 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 Gerenciador de Coletor 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 Gerenciador de Coletor. DeviceEventTime e EventTime são armazenados como UTC e os campos ObserverTZ são armazenados como strings definidos para o horário local da fonte de evento. Essas informações são enviadas do Gerenciador de Coletor para o servidor Sentinel e ficam armazenadas no armazenamento de eventos. O fuso horário em que o Gerenciador de Coletor 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 navegador, o EventTime UTC é convertido para o horário local de acordo com o navegador, 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.

17 Configurando plug-ins prontos para o uso

Por padrão, o Sentinel vem com vários plug-ins. Este capítulo fornece informações sobre como configurar os plug-ins prontos para o uso.

17.1 Configurando os Solution Packs

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 NetIQ Sentinel 7.1*

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 Pacotes de soluções são pré-instalados para fornecer o conteúdo pronto para o uso, porém os controles devem ser implementados ou testados formalmente com o console da Web do Sentinel.

Se for necessário mostrar que a implementação do Sentinel está funcionando como desejado, use o processo de atestação formal incorporado aos Pacotes de Solução. 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 NetIQ Sentinel 7.1*.

17.2 Configurando os coletores, conectores, integradores e ações

Para obter informações sobre como configurar os plug-ins prontos para o uso, veja a documentação de plug-in específica disponível no site na web de plug-ins do Sentinel.

18 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.

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

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

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

1. Efetue login no servidor do Sentinel.
2. Alterne para o usuário `novell` (`su novell`).
3. Navegue para o diretório bin do Sentinel.
4. Execute o script `convert_to_fips.sh` e siga as instruções na tela.
5. Conclua a configuração do modo FIPS 140-2 seguindo as tarefas mencionadas no Capítulo 19, “Operando o Sentinel no modo FIPS 140-2”, en la página 109

18.2 Ativando o modo FIPS 140-2 nos Gerenciadores de Coletor e Mecanismos de Correlação remotos

Você deve ativar o modo FIPS 140-2 no Gerenciador de Coletor e Mecanismo de Correlação remotos se desejar usar as comunicações aprovadas do FIPS com o servidor do Sentinel executando no modo FIPS 140-2.

Para ativar um Gerenciador de Coletor e Mecanismo de Correlação remotos para executar no modo FIPS 140-2:

1. Efetue login no sistema do Gerenciador de Coletor ou Mecanismo de Correlação remotos.
2. Alterne para o usuário `novell` (`su novell`).
3. Navegue para o diretório bin. O local padrão é `/opt/novell/sentinel/bin`.

4 Execute o script `convert_to_fips.sh` e siga as instruções na tela.

5 Conclua a configuração do modo FIPS 140-2 seguindo as tarefas mencionadas no Capítulo 19, “Operando o Sentinel no modo FIPS 140-2”, en la página 109

19 Operando o Sentinel no modo FIPS 140-2

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

19.1 Configurando o servido do Consultor em modo FIPS 140-2

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

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

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

   Para obter mais informações sobre como importar o certificado, veja “Importando certificados para o banco de dados de keystore do FIPS” en la página 118.

19.2 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" en la página 118.
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>/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" en la página 118.
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>/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" en la página 118.
5. Reinicie os serviços do Sentinel no computador de origem.

19.3 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" en la página 118.
3. Efetue login no console da Web do Sentinel como um usuário na função de administrador e prossiga com a configuração da autenticação do LDAP.

   Para obter mais informações, consulte *Configurando a autenticação do LDAP* no *Guia de Administração do NetIQ Sentinel 7.1.*

Nota: 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`.

19.4 Atualizando certificados do servidor nos Gerenciadores de Coletor e Mecanismos de Correlação remotos

Para configurar Gerenciadores de coletor e Mecanismos de correlação remotos para se comunicar com um servidor do Sentinel executado em modo FIPS 140-2, coloque o sistema remoto no modo FIPS 140-2 ou atualize o certificado do servidor do Sentinel para o sistema remoto e deixe o Gerenciador de coletor ou Mecanismo de correlação em modo não FIPS. Os Gerenciadores de Coletor 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 Gerenciador de coletor ou Mecanismo de correlação remotos, você precisa copiar o último certificado do servidor do Sentinel para o sistema remoto, de modo que o Gerenciador de coletor ou Mecanismo de correlação possa se comunicar com o servidor do Sentinel.

Para atualizar o certificado do servidor do Sentinel no Gerenciador de Coletor ou Mecanismo de Correlação remoto:

1. Efetue login no computador do Gerenciador de coletor ou Mecanismo de correlação 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.

19.5 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.

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

19.5.1 Conector do Gerenciador de Agente

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

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

1. Adicione ou edite o Servidor de Origem de Evento do Gerenciador de Agente. Avance pelas telas de configuração até que a janela Segurança seja exibida. Para obter mais informações, veja o *Guia do Conector do Gerenciador de Agente*.
2. Selecione uma das opções no campo *Client Authentication Type* (Tipo de autenticação do cliente). O tipo de autenticação do cliente determina estritamente como o Servidor de Origem de Evento do Gerenciador de Agente SSL verifica a identidade das Fontes de Evento do Gerenciador de Agente que estão tentando enviar dados.
   - **Abrir:** Permite todas as conexões SSL provenientes dos agentes do Gerenciador de Agente. Não executa nenhuma validação ou autenticação de certificado de cliente.
   - **Rígida:** Valida o certificado como um certificado X.509 válido e também verifica se o certificado do cliente é de confiança para o Servidor de Origem de Evento. Novas fontes precisarão ser explicitamente adicionadas ao Sentinel (isso evita que fontes fraudulentas enviem dados não autorizados).

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

     Para obter mais informações sobre como importar o certificado, veja “Importando certificados para o banco de dados de keystore do FIPS” en la página 118.

Nota: 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 Gerenciador de coletor 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 Gerenciador de coletor remoto: `/etc/opt/novell/sentinel/config/rcm.cer`

Nota: 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.

19.5.2 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" en la página 118.

3 Prossiga com a configuração do Conector.

19.5.3 Conector do Link do Sentinel

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

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

1 Adicione ou edite o Servidor de Origem de Evento do Sentinel Link. Avance pelas telas de configuração até que a janela Segurança seja exibida. Para obter mais informações, consulte *Guia do Sentinel Link Connector*.

2 Selecione uma das opções no campo *Client Authentication Type* (Tipo de autenticação do cliente). O tipo de autenticação do cliente determina com que rigidez o Servidor de Origem de Evento SSL Sentinel Link verifica a identidade das Fontes de Evento do Sentinel Link (Integradores de Sentinel Link) que estão tentando enviar dados.

- **Abrir:** Permite todas as conexões SSL provenientes dos clientes (Sentinel Link Integrators). Não executa nenhuma validação ou autenticação de certificado do Integrator.
- **Rígida:** Valida o certificado do Integrator como um certificado X.509 válido e também verifica se o certificado do Integrator é de confiança para o Servidor de Origem de Evento. Para obter mais informações, consulte a respectiva documentação do banco de dados.

Para a opção *Strict* (Rígida):

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

  Nota: 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.

  Nota: 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" en la página 118.

Nota: 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.

19.5.4 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" en la página 118.

Nota: 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 Gerenciador de coletor 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`.

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

19.5.5 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 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" en la página 118.

Nota: 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 Gerenciador de coletor 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`.

Nota: 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" en la página 118.

19.5.6 Sentinel Link Integrator

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

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

1 Quando o Sentinel Link Integrator está no modo FIPS 140-2, a autenticação do servidor é obrigatória. Antes de configurar a instância do Integrador, importe o certificado do servidor de Link do Sentinel para a keystore FIPS do Sentinel:

- **Se o Conector do link do Sentinel estiver em modo FIPS 140-2**:

  Se o Conector estiver implantado no servidor do Sentinel, você precisa copiar o arquivo `/etc/opt/novell/sentinel/config/sentinel.cer` da máquina Sentinel receptora para a máquina Sentinel emissora.

  Se o Conector estiver implantado em um Gerenciador de coletor remoto, você precisa copiar o arquivo `/etc/opt/novell/sentinel/config/rcm.cer` da máquina receptora do Gerenciador de coletor remoto para a máquina receptora do Sentinel.

  Importe esse certificado para o keystore do Sentinel FIPS emissor.

  Nota: 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.

  Nota: 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" en la página 118.

2 Prossiga com a configuração da instância do Integrator.

Nota: 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.

19.5.7 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" en la página 118.
3. Prossiga com a configuração da instância do Integrator.

19.5.8 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.

19.5.9 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 Gerenciador de Coletor remoto no modo não FIPS para conectar ao servidor do Sentinel no modo FIPS 140-2.

   Para obter mais informações, consulte Sección 11.6, "Instalando Gerenciadores de Coletor e Mecanismos de Correlação adicionais", en la página 78.
2. Implemente os Conectores não FIPS especificamente para o Gerenciador de Coletor remoto não FIPS.

Nota: Há alguns problemas conhecidos quando Conectores não FIPS, como o Conector de Auditoria e o Conector de Arquivo, são implementados em um Gerenciador de Coletor remoto não FIPS conectado a um servidor do Sentinel 7.1 no modo FIPS 140-2. Para obter mais informações sobre esses problemas conhecidos, consulte o arquivo"Readme do NetIQ Sentinel 7.0.1".

19.6 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 como normal quando o modo FIPS 140-2 estiver ativado no Sentinel. 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 Gerenciador de Coletor remoto, você deve importar os certificados para o banco de dados de keystore do FIPS do Gerenciador de Coletor 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 Gerenciador de Coletor 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 `yes` (sim) ou `y` (s) quando solicitado a reiniciar o servidor do Sentinel ou o Gerenciador de Coletor remoto.

19.7 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.

- Sección 19.7.1, “Revertendo o servidor do Sentinel para o modo não FIPS”, en la página 118
- Sección 19.7.2, “Revertendo Gerenciadores de Coletor ou Mecanismos de Correlação remotos para o modo não FIPS”, en la página 119

19.7.1 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.

Nota: 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-fips201301241911359034887.tar.gz` for o arquivo de backup, execute o seguinte comando:

```
./backup_util.sh -f non-fips201301241911359034887.tar.gz -m 'restore'
```

5 Reinicie o servidor do Sentinel.

19.7.2 Revertendo Gerenciadores de Coletor ou Mecanismos de Correlação remotos para o modo não FIPS

É possível reverter Gerenciadores de Coletor ou Mecanismos de Correlação remotos para o modo não FIPS

Para reverter um Gerenciador de Coletor ou um Mecanismo de Correlação remoto para o modo não FIPS:

1 Efetue login no sistema do Gerenciador de Coletor ou Mecanismo de Correlação 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 Gerenciador de Coletor ou o Mecanismo de Correlação remoto.

V Fazendo upgrade do Sentinel

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

20 Fazendo upgrade do servidor Sentinel

Importante: O Sentinel 7.1 ou mais recente exige que o sistema operacional esteja com o protocolo IPv6 ativado. Certifique-se de que o IPv6 esteja ativado no sistema operacional antes de fazer atualização para o Sentinel 7.1 ou mais recente. Se o IPv6 não estiver ativado, componentes importantes não funcionarão corretamente.

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

1. Faça um backup de sua configuração e crie uma exportação de ESM.

   Para obter mais informações sobre o backup de dados, consulte "Fazendo backup e restaurando dados" no *Guia de administração do NetIQ Sentinel 7.1*.
2. Faça download do instalador mais recente no site de download da Novell.
3. Efetue login como `root` no servidor em que você deseja fazer upgrade do Sentinel.
4. 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.
5. Altere para o diretório de onde o arquivo install foi extraído.
6. Especifique o seguinte comando para fazer upgrade do Sentinel:

   ```
   ./install-sentinel
   ```
7. 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.
8. Leia a licença do usuário final e digite `sim` ou `s` para aceitar a licença e continuar com a instalação.
9. O script de instalação detecta que uma versão mais antiga do produto já existe e solicita que você especifique se deseja fazer upgrade do produto. Para continuar com o upgrade, pressione s.

   A instalação de todos os pacotes RPM será iniciada. A instalação pode levar alguns segundos para ser concluída.
10. Limpe o cache do navegador web para visualizar a última versão do Sentinel.
11. (Condicional) Para atualizar sistemas de Gerenciador de coletor e Mecanismo de correlação, consulte Capítulo 22, "Fazendo upgrade do Gerenciador de Coletor ou o Mecanismo de correlação", en la página 127.

21 Fazendo upgrade da aplicação Sentinel

Os procedimentos neste capítulo fornecem orientações sobre como fazer a atualização da aplicação Sentinel e das aplicações Gerenciador de Coletor e Mecanismo de Correlação.

21.1 Fazendo upgrade do Sentinel 7.0.2 e aplicações posteriores

1. Efetue login na aplicação Sentinel como usuário na função de administrador.
2. **Se você quiser fazer upgrade da Aplicação Sentinel**, clique em *Aplicação* para iniciar a WebYaST.
3. **Se você quiser fazer upgrade de uma Aplicação Gerenciador de Coletor ou Mecanismo de Correlação**, especifique o URL do computador Gerenciador de Coletor ou Mecanismo de Correlação usando a porta 54984 para iniciar a WebYaST.
4. Faça um backup de sua configuração e crie uma exportação de ESM.

   Para obter mais informações sobre o backup de dados, consulte “Fazendo backup e restaurando dados” no *Guia de administração do NetIQ Sentinel 7.1*.
5. (Condicional) Se você ainda não tiver registrado o aplicativo para atualizações automáticas, registre-o.

   Para obter mais informações, consulte Sección 12.4.3, “Registrando para receber atualizações”, en la página 90.

   Se a aplicação não estiver registrada, o Sentinel exibirá uma alerta amarelo, indicando que a aplicação não está registrada.
6. Para verificar se existem atualizações disponíveis, clique em *Atualizações*.

   As atualizações disponíveis serão exibidas.
7. Selecione e aplique as atualizações.

   A conclusão das atualizações pode demorar alguns minutos. Depois que a atualização for bem-sucedida, a página de login do WebYaST será exibida.

   Antes de atualizar o aplicativo, o WebYaST interromperá automaticamente o serviço Sentinel. Você deve reiniciar manualmente esse serviço depois que a atualização for concluída.
8. Reinicie o serviço Sentinel usando a interface da Web.

   Para obter mais informações, consulte Sección 12.5, “Parando e iniciando o servidor com o WebYaST”, en la página 92.
9. Limpe o cache do navegador web para visualizar a última versão do Sentinel.

21.2 Fazendo upgrade das aplicações Sentinel 7.0 e 7.0.1

O upgrade das aplicações Sentinel 7.0 e 7.0.1 falha no WebYaST porque o nome do fornecedor do patch mudou de Novell para NetIQ. Você precisa fazer upgrade da aplicação usando o patch zypper.

Para fazer upgrade da aplicação usando o patch zypper:

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 NetIQ Sentinel 7.1*.
2. Faça login no console de aplicativo como o usuário `root`.
3. Execute o seguinte comando:

   ```
   /usr/bin/zypper patch
   ```

4. Digite `1` para aceitar a mudança de fornecedor de Novell para NetIQ.
5. Digite `Y` (S) para continuar.
6. Digite `yes` (sim) para aceitar o contrato de licença.
7. Reinicie a aplicação Sentinel.
8. Limpe o cache do navegador web para visualizar a última versão do Sentinel.

21.3 Atualizando o aplicativo usando SMT

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

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

   Para obter mais informações, consulte a Sección 12.4.4, "Configurando a aplicação com SMT", en la página 91.
2. Faça login no console do aplicativo como o usuário `root`.
3. Atualize o repositório para atualização:

   ```
   zypper ref -s
   ```

4. Verifique se o aplicativo está habilitado para atualização:

   ```
   zypper lr
   ```

5. (Opcional) Verifique se há atualizações disponíveis para o aplicativo:

   ```
   zypper lu
   ```

6. (Opcional) Verifique se há pacotes que incluem as atualizações disponíveis para o dispositivo:

   ```
   zypper lp -r SMT-http_<smt_server_fqdn>:<package_name>
   ```

7. Atualize o aplicativo:

   ```
   zypper up -t patch -r SMT-http_<smt_server_fqdn>:<package_name>
   ```

8. Reinicie o aplicativo.

   ```
   rcsentinel restart
   ```

22 Fazendo upgrade do Gerenciador de Coletor ou o Mecanismo de correlação

Use as etapas a seguir para fazer a atualização do Gerenciador de coletor ou do Mecanismo de correlação:

1. Faça um backup de sua configuração e crie uma exportação de ESM.

   Para obter mais informações, consulte "Fazendo backup e restaurando dados" no *Guia de administração do NetIQ Sentinel 7.1*.
2. Efetue login na interface da Web do Sentinel como usuário na função de administrador.
3. Selecione *Downloads*.
4. Clique no *Download do Instalador* na seção Instalador do Gerenciador do Coletor.

   Uma janela é exibida com opções para abrir ou salvar o arquivo do instalador na máquina local.
5. Grave o arquivo.
6. Copie o arquivo para um local temporário.
7. Extraia o conteúdo do arquivo.
8. Execute o script a seguir:

   Para o Gerenciador do Coletor:

   ```
   ./install-cm
   ```

   Para o Mecanismo de Correlação:

   ```
   ./install-ce
   ```
9. Siga as instruções na tela para completar a instalação.
10. Limpe o cache do navegador web para visualizar a última versão do Sentinel.

23 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 são frequentemente carregados no site na web 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 Apêndices

A Configurando o Sentinel para alta disponibilidade

Muitos clientes procuram instalar o Sentinel em ambientes altamente disponíveis com o objetivo de assegurar que os dados críticos de evento corporativo sejam coletados da forma mais consistente possível. Muitos requisitos de segurança e conformidade dependem da coleta abrangente de dados para demonstrar aderência aos requisitos - alguns poucos eventos perdidos podem prevenir a detecção de uma ameaça ou violação e causar risco inaceitável à organização. O NetIQ foi testado e certificado para trabalhar em um ambiente de alta disponibilidade, e suporta arquiteturas de recuperação de desastres.

Este apêndice descreve como instalar o produto em um modo de alta disponibilidade ativo-passivo, permitindo que o Sentinel alterne para um nó do cluster redundante no caso de falha de hardware ou software. Ele não abrange configurações ativa-ativa, e não garante nenhum objetivo de tempo de atividade específico. O NetIQ Consulting e os parceiros do NetIQ podem ajudar você a implementar a alta disponibilidade e a recuperação de desastres do Sentinel.

Nota: O NetIQ suporta a configuração de alta disponibilidade apenas nas instalações completas do Sentinel. Ele não suporta diretamente instalações distribuídas dos Gerenciadores de Coletor e Mecanismos de Correlação.

A.1 Conceitos

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.

A.1.1 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 incidente. A maioria das soluções de alta disponibilidade permite que os implementadores declarem as dependências entre os serviços que devem estar altamente disponíveis e os serviços dependentes, 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/receber dados entre o sistema de terceiro e o Sentinel, então, o sistema de terceiro deverá ser configurado para aceitar sessões de origem ou iniciar sessões para qualquer nó de cluster (o Sentinel deve ser configurado com um IP virtual para esse fim). O NetIQ não pode garantir nenhum nível específico de alta disponibilidade entre o nosso produto e os sistemas de terceiros fora de nosso controle.

A.1.2 Armazenamento compartilhado

Todos os clusters de alta disponibilidade 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.

Nota: 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/ou largura de banda para o armazenamento for mais lenta do que o recomendado.

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 o 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.

A.1.3 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.

A.1.4 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.

A.2 Suportabilidade

O NetIQ suporta essa solução com base nas características do cluster definidas e no comportamento esperado como definido nesse documento e testado em nossos laboratórios. Outras configurações de cluster somente serão suportadas se os problemas observados no seu ambiente puderem ser replicados em nossos ambientes de teste internos, eliminando, dessa forma, diferenças locais na implementação como a causa do problema.

A.3 Requisitos do Sistema

Ao alocar recursos do cluster para suportar uma instalação altamente disponível, considere os seguintes requisitos:

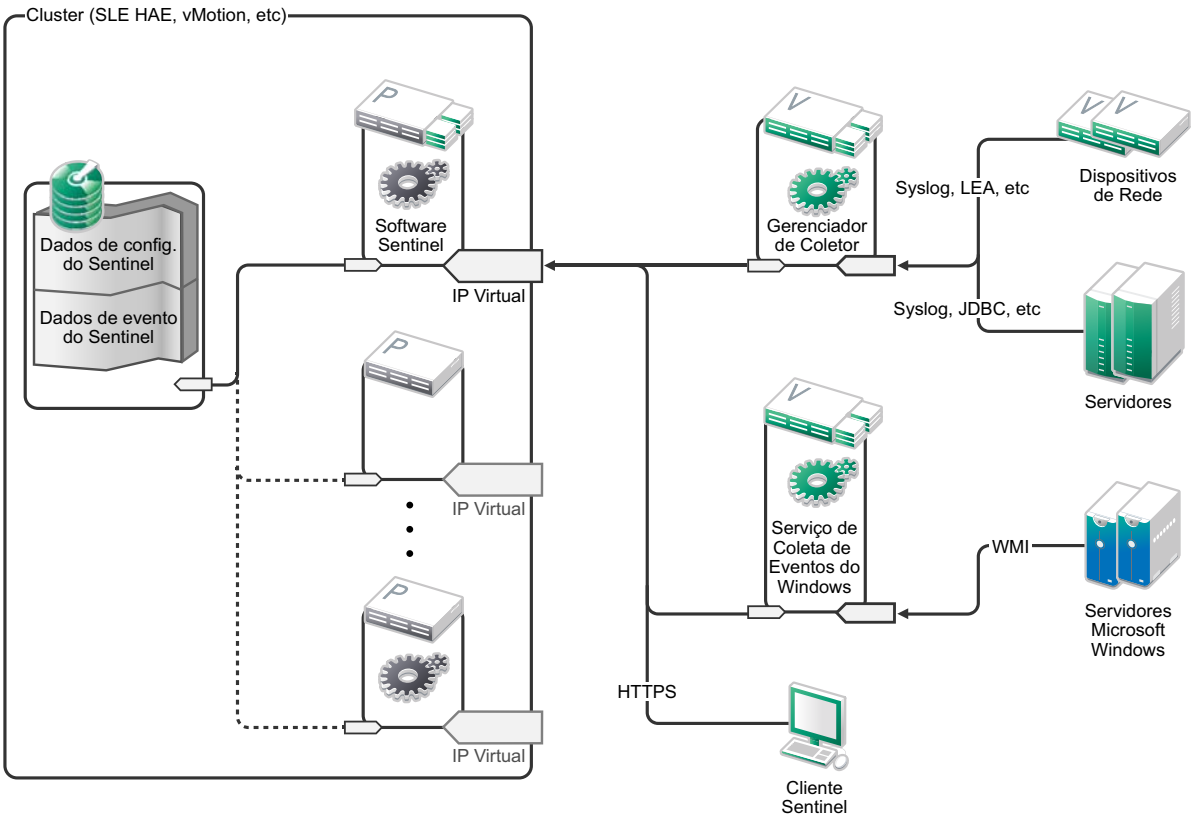
- Cada nó de cluster que hospeda os serviços do Sentinel deve corresponder aos requisitos especificados em Capítulo 5, “Atendendo aos requisitos do sistema”, en la página 35

- Verifique se está disponível armazenamento compartilhado suficiente para os dados e aplicativo do Sentinel.
- Um endereço IP virtual dos serviços que podem ser migrados de nó a nó no failover.
- O instalador do Sentinel (arquivo TAR) com uma licença válida.
- A Extensão de Alta Disponibilidade do SUSE Linux (imagem ISO) com uma licença válida.
- Um dispositivo de armazenamento compartilhado que satisfaça às características de desempenho e tamanho como documentado no Capítulo 5, “Atendendo aos requisitos do sistema”, en la página 35 A solução de exemplo usará uma VM SUSE Linux padrão configurada com destinos iSCSI como armazenamento compartilhado.
- Dois nós de cluster mínimos que satisfaçam aos requisitos do recurso para executar o Sentinel no ambiente do cliente. A solução de exemplo usará duas VMs SUSE Linux.
- Um método para que os nós do cluster se comuniquem com o armazenamento compartilhado, como o Fibre Channel para uma SAN. A solução de exemplo usará um endereço IP dedicado para se conectar ao destino iSCSI.
- Um IP virtual que possa ser migrado do nó do cluster para o nó do cluster para servir como o endereço IP externo do Sentinel.
- Pelo menos um endereço IP por nó do cluster para comunicações internas do cluster. A solução de exemplo usará um endereço IP unicast simples, mas o multicast é preferido para ambientes de produção.

A.4 Instalação e configuração

Esta seção fornece as etapas para instalação e configuração do Sentinel em um ambiente de alta disponibilidade. Cada etapa descreve a abordagem geral, em seguida, faz referência a uma configuração de demonstração que documenta os detalhes de uma solução de cluster de exemplo. Você pode usar outras opções ou tecnologias diferentes das listadas neste documento, sujeitas às restrições descritas no Sección A.2, “Suportabilidade”, en la página 135.

O diagrama a seguir representa uma arquitetura de alta disponibilidade ativa-passiva:



A.4.1 Configuração inicial

Configure o hardware da máquina, 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 adequada e estabilidade.

- Como uma prática recomendada, todos os nós do cluster devem estar sincronizados ao mesmo tempo - use NTP ou uma tecnologia similar para esse fim.
- O cluster exigirá uma resolução de nome de host confiável. Como uma prática recomendada, talvez você deseje inserir todos os nomes de host de cluster internos no arquivo `/etc/hosts` para assegurar a continuidade do cluster no caso de falha do DNS. Se qualquer nó do cluster não puder resolver todos os outros nós ***por nome***, a configuração do cluster descrita nesta seção falhará.
- 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”, en la página 35 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”, en la página 35 com base na taxa de eventos esperada e nas políticas de retenção de dados para armazenamento local e/ou de rede.
- Para configurar os firewalls do sistema operacional de modo a restringir o acesso ao Sentinel e ao cluster, consulte o Capítulo 7, “Portas usadas”, en la página 57 para obter detalhes de quais portas devem estar disponíveis dependendo da configuração local e das origens que enviarão dados de evento.

A solução de exemplo usará a seguinte configuração:

- Duas VMs do nó do cluster SUSE Linux 11 SP2
  - A instalação do sistema operacional não precisa instalar X Windows, mas pode fazê-lo, caso a configuração da GUI seja desejada. Os scripts de inicialização podem ser configurados para iniciar sem X (nível de execução 3), o que pode ser iniciado apenas quando necessário.
  - Os nós terão dois NICS: um 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 do sistema SUSE Linux e SLE HAE, e os requisitos da aplicação Sentinel.
- Uma VM do SUSE Linux 11 SP2 configurada com os destinos iSCSI do armazenamento compartilhado
  - A instalação do sistema operacional não precisa instalar X Windows, mas pode fazê-lo, caso a configuração da GUI seja desejada. Os scripts de inicialização podem ser configurados para iniciar sem X (nível de execução 3), o que pode ser iniciado apenas 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. Para este exemplo, utilizaremos 172.16.0.3 (storage03 [armazenamento 03])
  - 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. Veja os requisitos do sistema SUSE Linux e os requisitos do armazenamento de dados do evento do Sentinel. Para a solução de exemplo, colocaremos todos os dados (local, rede, SBD) em um único disco, mas para implementações de produção, isso pode ser alocado para nós diferentes.

Nota: Em um cluster de produção, você pode usar IPs internos, não roteáveis, em NICs separados (possivelmente um par, para redundância) para comunicações internas do cluster.

A.4.2 Configuração de armazenamento compartilhado

Configure o armazenamento compartilhado e verifique se você pode montá-lo em cada nó do cluster. Se estiver usando o Fibre Channel e uma SAN, isso pode envolver conexões físicas e outra configuração. O armazenamento compartilhado será usado para manter os bancos de dados do Sentinel e os dados de evento, assim deve ser dimensionado concordemente para o ambiente do cliente com base na taxa de evento e políticas de retenção de dados esperadas.

Uma implementação típica pode usar uma SAN 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 de rede mais lento. Contanto que o nó do cluster possa montar o armazenamento local como um dispositivo de blocos normal, ele pode ser usado pela solução. O armazenamento de rede também pode ser montado como um dispositivo de bloco ou pode ser um volume NFS ou CIFS.

Nota: Você deve configurar seu armazenamento compartilhado e testar sua montagem em cada nó de cluster, mas a montagem real do armazenamento será manipulada pela configuração do cluster.

Para a solução de exemplo, usaremos os Destinos iSCSI hospedados por uma VM SUSE Linux:

A solução de exemplo usará Destinos iSCSI configurados em uma VM SUSE Linux. A VM é `storage03` (armazenamento 03) como listada na Configuração inicial Os dispositivos iSCSI podem ser criados usando qualquer arquivo ou dispositivo de blocos, mas, por questão de simplicidade, utilizaremos aqui um arquivo que criamos para esse fim.

Conecte-se ao `storage03` (armazenamento 03) e inicie uma sessão de console. Use o comando `dd` para criar um arquivo vazio de qualquer tamanho desejado para o armazenamento local desejado do Sentinel:

```
dd if=/dev/zero of=/localdata count=10240000 bs=1024
```

Neste caso, criamos um arquivo de 10 GB preenchido com zeros (copiado de `/dev/zero pseudo-device`). Veja a página de informações ou do manual referente à `dd` para obter detalhes sobre as opções da linha de comandos. Por exemplo, para criar "discos" com tamanhos diferentes. O Destino iSCSI trata esse arquivo como se fosse um disco; você pode, evidentemente, usar um disco real se preferir.

Repita este procedimento para criar um arquivo para o armazenamento de rede:

```
dd if=/dev/zero of=/networkdata count=10240000 bs=1024
```

Para este exemplo, usamos dois arquivos ("discos") do mesmo tamanho e características de desempenho. Para uma implementação de produção, você pode colocar o armazenamento local em uma SAN rápida e o armazenamento de rede em um volume iSCSI, NFS ou CIFS mais lento.

Configure esses arquivos como Destinos iSCSI:

1. Execute o YaST da linha de comandos (ou use a GUI, 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 **Address** (Endereço), designe o endereço IP estático 10.0.0.3. Esse será o IP interno das comunicações iSCSI.
6. Clique em **Next** (Próximo) e, em seguida, clique em **OK**.

7 Na tela principal, selecione **Network Services** (Serviços de Rede) > **iSCSI Target** (Destino iSCSI).

8 Quando solicitado, instale o software (`iscsitarget RPM`) necessário da mídia SUSE Linux 11 SP2.

9 Clique·em·**Service**·(Serviço), selecione a opção **When Booting** (Ao Inicializar) para assegurar que o serviço inicie na inicialização do sistema operacional.

10 Clique em **Global** e selecione **No Authentication** (Sem Autenticação), porque o Agente de Recurso OCF para iSCSI atual não suporta autenticação.

11 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.

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

13 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`.

14 Repita as etapas 12 e 13, e adicione LUN 1 e `/networkdata` desta vez.

15 Deixe as outras opções como seus padrões. Clique em **OK** e, em seguida, em **Next** (Próximo).

16 Clique em **Next** (Próximo) novamente para selecionar as opções de autenticação padrão, e em **Finish** (Terminar) para sair da configuração. Se solicitado, aceite para reiniciar o iSCSI.

17 Saia do YaST.

O procedimento acima expõe dois Destinos iSCSI no servidor no endereço IP 10.0.0.3. Em cada nó do cluster, certifique-se de que seja possível montar o dispositivo de armazenamento dos dados locais compartilhados. Você também deve formatar os dispositivos (uma vez):

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 no **Address** (Endereço), atribua o endereço IP estático 10.0.0.1. Esse será o IP interno das comunicações iSCSI.

6 Selecione **Next** (Próximo) e, em seguida, clique em **OK**.

7 Clique em **Network Services** (Serviços de Rede) > **iSCSI Initiator** (Iniciador iSCSI).

8 Quando solicitado, instale o software (open-iscsi RPM) necessário da mídia SUSE Linux 11 SP2.

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 iSCSI (10.0.0.3), selecione **No Authentication** (Sem Autenticação) e clique em **Next** (Próximo).

12 Selecione o Destino iSCSI descoberto com o endereço IP 10.0.0.3 e selecione **Log In** (Efetuar Login).

13 Alterne para automático na lista suspensa **Startup** (Inicialização), selecione **No Authentication** (Sem Autenticação) e clique em **Next** (Próximo).

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 System View (Tela do Sistema), você deve ver novos discos rígidos (por exemplo, `/dev/sdb` e `/dev/sdc` na lista - eles terão o tipo IET-VIRTUAL-DISK. Pressione Tab para o primeiro item na lista (que deve ser o armazenamento local), 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 ext3 primária, mas não a monte. Certifique-se que a opção Do not mount partition (Não montar partição) esteja selecionada.

19 Selecione **Next** (Próximo) e **Finish** (Terminar) após examinar as mudanças que serão feitas. Presumindo que você crie uma única partição grande nesse LUN iSCSI compartilhado, você deve encerrar com um `/dev/sdb1` ou disco formatado similar (chamado como `/dev/<COMPARTILHADO1>` abaixo).

20 Volte para o particionador e repita o processo de particionamento/formatação (etapas 16-19) para `/dev/sdc` ou para qualquer dispositivo de blocos que corresponda ao armazenamento de rede. Isso resultará em uma partição `/dev/sdc1` ou disco formatado similar (chamado como `/dev/<REDE1>` abaixo).

21 Saia do YaST.

22 Finalmente, crie um ponto de montagem e teste a montagem da partição local como segue (o nome do dispositivo exato pode depender da implementação específica):

```
# mkdir /var/opt/novell
# mount /dev/<SHARED1> /var/opt/novell
```

23 Você deve ser capaz de criar arquivos na nova partição e vê-los onde quer que estejam montados.

Para desmontar:

```
# umount /var/opt/novell
```

Repita as etapas 1-15 no procedimento acima para assegurar que cada nó do cluster possa montar o armazenamento compartilhado local. Substitua o IP do nó na etapa 5, por um IP diferente (por exemplo, node02 > 10.0.0.2).

A.4.3 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 onde quer que você tenha montado o armazenamento compartilhado) ou apenas colocar os dados variáveis do aplicativo no armazenamento compartilhado.

Nesta solução de exemplo, seguiremos esta última abordagem e instalaremos o Sentinel para cada nó do cluster que possa hospedá-lo. A primeira vez que o Sentinel for instalado, faremos uma instalação completa incluindo os binários do aplicativo, configuração e todos os armazenamentos de dados. As instalações subsequentes nos outros nós do cluster apenas instalarão o aplicativo e presumiremos que os dados reais do Sentinel estarão disponíveis algum tempo mais tarde (por exemplo, assim que o armazenamento compartilhado for montado).

Solução de exemplo:

Nesta solução de exemplo, instalaremos o Sentinel em cada nó do cluster, armazenando apenas os dados variáveis do aplicativo no estágio compartilhado. Isso mantém os binários do aplicativo e configuração nos locais padrão, permitindo-nos verificar os RPMs, além de nos permitir dar suporte a patches a quente em determinados cenários.

Instalação no primeiro nó

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 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
   ```

1. Execute a instalação padrão, configurando o produto, conforme apropriado. O instalador instalará os binários, configuração, bancos de dados e configurará nomes de usuário/senhas e portas de rede.
2. Inicie o Sentinel e teste as funções básicas. Você pode usar o IP do nó do cluster externo padrão para acessar o produto.
3. Encerre o Sentinel e desmonte o armazenamento compartilhado:

   ```
   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 do nó subsequente

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.

1. Conecte-se a cada nó de cluster adicional (node02) e abra uma janela do console.
2. Execute o que segue:

   ```
   cd /tmp
   ```

   ```
   scp root@node01:/tmp/sentinel_server*.tar.gz
   ```

   ```
   scp root@node01:/tmp/install.props
   ```

   ```
   tar -xvzf sentinel_server*.tar.gz
   ```

```
./install-sentinel --no-start --cluster-node --unattended=/tmp/install.props
cd /
insserv -r 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.

A.4.4 Instalação do cluster

Instale o software do cluster em cada nó e registre cada nó do cluster com o gerenciador de cluster. Os procedimentos a serem executados variarão dependendo da implementação do cluster, mas, no final do processo, cada nó do cluster deverá aparecer no console de gerenciamento do cluster.

Para nossa solução de exemplo, configuraremos a Extensão de Alta Disponibilidade do SUSE Linux e a sobreporemos com os Agentes de Recurso específico do Sentinel:

Se você não usar o Agente de Recurso OCF para monitorar o Sentinel, provavelmente teremos que desenvolver uma solução de monitoramento similar para o ambiente do cluster local. 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 você deseja desenvolver por conta própria, deve examinar o Agente de Recurso existente para obter exemplos (o Agente de Recurso está armazenado no `sentinel-ha.rpm` no pacote de download do Sentinel).

Há muitos modos diferentes em que um cluster SLE HAE pode ser configurado, mas nós selecionaremos as opções que mantêm isso razoavelmente simples. A primeira etapa é instalar o software principal do SLE HAE, o processo está completamente detalhado na Documentação do SLE HAE. Para obter informações sobre a instalação dos complementos do SLES, veja o Guia de Implementação.

Você deve instalar o SLE HAE em todos os nós do cluster, node01 e node02 em nosso exemplo. 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.

Após a instalação do software do cluster, um RPM adicional deverá ser instalado para fornecer Agentes de Recurso do cluster adicionais específicos do Sentinel. O RPM pode ser encontrado no `novell-Sentinel-ha-7.1*.rpm` armazenado no download normal do Sentinel, que você descompacta para instalar o produto.

Em cada nó do cluster, copie o `novell-Sentinel-ha-7.1*.rpm` para o diretório `/tmp`, em seguida:

```
cd /tmp
rpm -i novell-Sentinel-ha-7.1*.rpm
```

A.4.5 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, também é possível configurar o fencing e recursos STONITH para assegurar a consistência do cluster.

Na nossa solução de exemplo, basicamente usamos a configuração mais simples sem redundância adicional ou outros recursos avançados. Também usamos um endereço unicast (em vez do endereço multicast preferido) porque ele requer menos interação com os administradores de rede, e é suficiente para fins de teste. Configuramos também um recurso fencing simples baseado em SBD.

Solução de exemplo:

A solução de exemplo usará endereços IP privados para comunicações internas do cluster, e usará unicast para minimizar a necessidade de solicitar um endereço multicast de um administrador de rede. A solução também usará um Destino iSCSI configurado na mesma VM SUSE Linux que hospeda o armazenamento compartilhado para servir como um dispositivo SBD para os fins de fencing. Como antes, os dispositivos iSCSI podem ser criados usando qualquer arquivo ou dispositivo de blocos, mas, por questão de simplicidade, utilizaremos aqui um arquivo que criamos para esse fim.

As etapas de configuração a seguir são muito similares às contidas em Configuração do armazenamento compartilhado:

Configuração do SBD

Conecte-se ao `storage03` e inicie uma sessão de console. Use o comando **dd** para criar um arquivo vazio de qualquer tamanho:

```
dd if=/dev/zero of=/sbd count=1024 bs=1024
```

Neste caso, criamos um arquivo de 1 MB preenchido com zeros (copiado de `/dev/zero` pseudo-device).

Configure esse arquivo como um Alvo iSCSI:

1. Execute o YaST da linha de comandos (ou use a GUI, se preferir): `/sbin/yast`
2. Selecione **Network Services** (Serviços de Rede) > **iSCSI Target** (Destino iSCSI).
3. Clique em **Targets** (Destinos) e selecione o destino existente.
4. Selecione **Edit** (Editar). A IU apresentará uma lista de LUNs (unidades) que estão disponíveis.
5. Selecione **Add** (Adicionar) para incluir uma nova LUN.
6. Deixe o número da LUN como 2. Navegue na caixa de diálogo **Path** (Caminho) e selecione o arquivo `/sbd` que você criou.
7. 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.
8. Clique em **Finish** (Terminar) para sair da configuração. Reinicie os serviços, se necessário. Saia do YaST.

Nota: 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 DNS não estiver configurado ou disponível, adicione entradas para cada host ao arquivo `/etc/hosts` que lista cada IP e seu nome de host (como informado pelo comando hostname).

Este procedimento deve expor um Destino iSCSI para o dispositivo SBD no servidor no endereço IP 10.0.0.3 (storage03).

Node Configuration (Configuração do nó)

Conecte a um nó do cluster (node01) e abra um console:

1. Execute o YaST.
2. Abra **Network Services** (Serviços de Rede) > **iSCSI Initiator** (Iniciador iSCSI).
3. Selecione **Connected Targets**(Destinos Conectados) e, em seguida, o iSCSI Target (Destino iSCSI) que você configurou acima.
4. Selecione a opção **Log Out** (Efetuar logout) e efetue logout do Destino.

5. Alterne para a guia **Discovered Targets** (Destinos Descobertos), selecione o **Target** (Destino) e efetue login novamente para atualizar a lista de dispositivos (deixe a opção automatic startup [inicialização automática] e No Authentication [Sem 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. Execute o comando `sleha-init`.
11. Quando solicitado sobre a qual endereço de rede vincular, especifique o 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 "y" (s) para ativar o SBD, em seguida, especifique `/dev/disk/by-id/<id do dispositivo>`, onde `<id do dispositivo>` é o ID que você localizou acima (é possível usar Tab para preencher automaticamente o caminho).
14. Conclua o assistente e certifique-se de que nenhum erro seja informado.
15. Inicie o YaST.
16. Selecione **High Availability** (Alta Disponibilidade) > **Cluster** (ou apenas Cluster em alguns sistemas).
17. Na caixa à esquerda, certifique-se de que **Communication Channels** (Canais de Comunicação) esteja selecionado.
18. Pressione Tab até a linha superior da configuração e mude a seleção udp para udpu (isso desativa o multicast e seleciona o unicast).
19. Selecione **Add a Member Address** (Adicionar um Endereço de Membro) e especifique esse nó (172.16.0.1), em seguida, repita e adicione o(s) outro(s) nó(s) do cluster: 172.16.0.2.
20. Selecione **Finish** (Terminar) para completar a configuração.
21. Saia do YaST.
22. 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 seguinte comando:`sleha-join`
2. Insira o endereço IP do primeiro nó do cluster.

Em algumas circunstâncias, as comunicações do cluster não inicializam corretamente. Se o cluster não iniciar (o serviço `openais` falhará ao iniciar):

- Copie manualmente `corosync.conf` de node1 para node02, ou execute `csync2 -x -v` no nó 1, ou configure manualmente o cluster para node02 via YaST.
- Execute `/etc/rc.d/openais start` no node02

Em alguns casos, o script pode falhar porque o serviço `xinetd` não adiciona adequadamente o novo serviço `csync2`. Esse serviço é necessário para que o outro nó possa sincronizar os arquivos de configuração do cluster em relação a esse nó. Se você vir erros como`csync2 run failed` (execução de csync2 com falha), talvez haja um problema. Para corrigir isso, execute: `kill -HUP `cat /var/run/xinetd.init.pid` e execute novamente o script `sleha-join`.

A esta altura, você deve ser capaz de executar crm_mon em cada nó e ver se o cluster está executando adequadamente. Como alternativa, você pode usar "hawk", o console da web - as credenciais de login padrão são "hacluster / linux".

Há dois parâmetros adicionais que precisamos ajustar para este exemplo. Se eles se aplicarão a um cluster de produção do cliente, isso dependerá da sua configuração:

1. Configure a opção global do cluster `no-quorum-policy` como `ignore` (ignorar). Fazemos isso porque temos apenas um cluster com dois nós, assim qualquer falha no nó único quebrará o quorum e encerrará o cluster inteiro: `crm configure property no-quorum-policy=ignore`

   Nota: Se o seu cluster tiver mais de dois nós, não configure essa opção.

2. Configure a opção do cluster global `default-resource-stickiness como 1.` Isso encorajará o gerenciador de recurso a deixar os recursos executando no local em vez de movê-los ao redor: `crm configure property default-resource-stickiness=1`.

A.4.6 Configuração do recurso

Como mencionado na Instalação do Cluster, esta solução fornece um Agente de Recurso OCF para monitorar os principais serviços em SLE HAE, e você pode criar alternativas, se desejado. O software também depende de diversos outros recursos, para os quais os Agentes de Recurso são fornecidos por padrão com SLE HAE. Se você não deseja usar o SLE HAE, terá que monitorar estes recursos adicionais usando alguma outra tecnologia:

- Um recurso Filesystem (sistema de arquivos) correspondente para o armazenamento compartilhado que o software usa;
- Um recurso de endereço IP correspondente ao IP virtual pelo qual os serviços serão acessados;
- O software do banco de dados Postgres que o software usa para armazenar a configuração e os metadados do evento.

Há recursos adicionais, como o MongoDB usado pela Inteligência de Segurança e o barramento de mensagem ActiveMQ; por ora, pelo menos esses são monitorados como parte dos serviços principais.

Solução de exemplo

A solução de exemplo usa versões simples dos recursos necessários, por exemplo, o Agente de Recurso Filesystem (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.

A solução de exemplo fornece um script `crm` para auxiliar na configuração do cluster. O script extrai variáveis de configuração relevantes do arquivo de configuração autônomo gerado como parte da instalação do Sentinel. Se você não gerar o arquivo de configuração ou quiser mudar a configuração dos recursos, poderá editar o script concordemente.

Conecte-se ao nó original em que o Sentinel foi instalado (esse deve ser o nó em que você executou a instalação completa do Sentinel) e execute o procedimento a seguir (<COMPARTILHADO1> é o volume compartilhado criado acima):

```
mount /dev/<SHARED1> /var/opt/novell

cd /usr/lib/ocf/resource.d/novell

./install-resources.sh
```

Pode haver problemas com os novos recursos aparecendo no cluster; execute `/etc/rc.d/openais restart` no node02 (nó 2) se tiver esse problema.

O script `install-resources.sh` solicitará alguns valores, ou seja, o IP virtual que você deseja que as pessoas usem para acessar o Sentinel e o nome do dispositivo do armazenamento compartilhado, e, em seguida, 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.

Se o ambiente do cliente variar em relação a esta solução de exemplo, você pode editar o arquivo `resources.cli` (no mesmo diretório) e modificar as definições primitivas em tal arquivo. Por exemplo, a solução de exemplo usa um recurso Filesystem (sistema de arquivos) simples; talvez você deseje usar outro recurso cLVM com reconhecimento de cluster.

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
```

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.

A.4.7 Configuração do armazenamento de rede

Como a etapa final deste processo, configure o armazenamento de rede de modo que o Sentinel possa migrar as partições de evento para um armazenamento menos oneroso. Isso é opcional e, na verdade, o armazenamento de rede não precisa ser feito altamente disponível do mesmo modo que o resto do sistema - você pode usar qualquer diretório (montado de uma SAN ou não) ou volume NFS ou CIFS.

Clique em **Storage** (Armazenamento) na barra de menu superior, e selecione **Configuration** (Configuração), em seguida, selecione um dos botões de opção debaixo do armazenamento de rede não configurado para configurá-lo.

Solução de exemplo

A solução de exemplo usará um Destino iSCSI simples como um local de armazenamento compartilhado de rede, em muito a mesma configuração que o armazenamento local. Nas implementações de produção, isso será provavelmente tecnologias de armazenamento diferentes.

Use o procedimento a seguir para configurar o armazenamento de rede a ser usado pelo Sentinel:

Nota: Como usaremos um Destino iSCSI para esta solução de exemplo, o destino será montado como um diretório a ser usado como armazenamento de rede. Assim, precisamos configurar a montagem como um recurso Filesystem (sistema de arquivos) considerando o modo como o sistema de arquivo

do armazenamento local está configurado. Esse não foi automaticamente configurado como parte do script de instalação de recurso, visto que há outras variações possíveis; faremos a configuração manualmente aqui.

---

1. Examine as etapas acima para determinar que partição foi criada para ser usada como armazenamento de rede (`/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 GUI da web 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 de rede esteja devidamente montado (usar o comando mount).
5. Efetue login na interface da web do Sentinel.
6. Selecione **Storage** (Armazenamento) e **Configuration** (Configuração), e selecione **SAN (locally mounted)** (SAN [localmente montada]) debaixo do Armazenamento de rede não configurado.
7. Digite o caminho no qual o armazenamento de rede está montado, por exemplo, `/var/opt/netdata`.

A solução de exemplo usa versões simples dos recursos necessários, por exemplo, Agente de Recurso Filesystem (Sistema de arquivos) - os clientes podem optar por usar recursos de cluster mais sofisticados como cLVM (uma versão de volume lógico do sistema de arquivos), se desejarem.

A.5 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.

- Sección A.5.1, “Backup”, en la página 148
- Sección A.5.2, “da PlateSpin”, en la página 149

A.5.1 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 NetIQ Sentinel 7.1* 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.

A.5.2 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 NetIQ Sentinel 7.1* 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.

B Solucionando problemas da instalação

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

B.1 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.

B.2 O UUID não é criado para Gerenciadores de Coletor em imagens nem para Mecanismos de Correlação

Se você cria uma imagem de um servidor Gerenciador de Coletor (por exemplo, usando o ZENworks Imaging) e restaura as imagens em diferentes máquinas, o Sentinel não identifica exclusivamente as novas instâncias do Gerenciador de Coletor. 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 Gerenciador de Coletor:

1. Exclua o arquivo `host.id` ou `sentinel.id` que está localizado na pasta `/var/opt/novell/sentinel/data`.
2. Reinicie o Gerenciador de Coletor.

   O Gerenciador de Coletor gera automaticamente o UUID.

C Desinstalando

Este apêndice fornece informações sobre como desinstalar o Sentinel e as tarefas pós-desinstalação.

C.1 Lista de verificação da desinstalação

Use a lista de verificação a seguir para desinstalar o Sentinel:

- ❒ Desinstale o servidor do Sentinel.
- ❒ Desinstale o Gerenciador de Coletor e o Mecanismo de Correlação, se houver.
- ❒ Execute as tarefas de pós-desinstalação para concluir a desinstalação do Sentinel.

C.2 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.

Advertencia: 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.

C.2.1 Desinstalando o Sentinel Server

Use as etapas a seguir para desinstalar o servidor Sentinel:

1. Efetue login no servidor do Sentinel como `root`.

   Nota: 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:

   ```
   /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.

C.2.2 Desinstalando o Gerenciador de Coletor ou Mecanismo de Correlação

Use as etapas a seguir para desinstalar o Gerenciador de Coletor e o Mecanismo de Correlação:

1 Efetue login como `root`.

   Nota: Você não pode desinstalar o Gerenciador de Coletor Remoto nem o Mecanismo de correlação remota como usuário não root quando a instalação é executada como usuário `root`. No entanto, o usuário não root pode desinstalar quando a instalação é executada pelo 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 Gerenciador de Coletor ou o Mecanismo de correlação e todos os dados associados serão completamente removidos.

4 Insira s para remover o Gerenciador de Coletor ou o Mecanismo de Correlação.

   O script primeiro para o serviço e, em seguida, remove-o completamente. No entanto, os ícones do Gerenciador de coletor e Mecanismo de correlação ainda são exibidos em estado inativo na interface da Web.

5 Realize as seguintes etapas adicionais para excluir manualmente o Gerenciador de coletor e o Mecanismo de correlação na interface da Web:

   Gerenciador de Coletor:

   1. Clique em *Gerenciamento de Fonte de Eventos* > *Tela Ativa*.
   2. Clique com o botão direito do mouse no Gerenciador de Coletor que deseja apagar e clique em *Apagar*.

   Mecanismo de Correlação:

   1. Efetue login na interface da web do Sentinel como administrador.
   2. Expanda *Correlação* e, em seguida, selecione o Mecanismo de Correlação que deseja apagar.
   3. Clique no botão *Apagar* (ícone da lixeira).

C.3 Tarefas pós-desinstalação

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

Depois de desinstalar o Sentinel, certas configurações dos sistemas permanecerão. Essas configurações deverão ser removidas antes de realizar uma instalação "limpa" do Sentinel, particularmente se a desinstalação do Sentinel encontrou erros.

Para limpar manualmente as configurações do sistema Sentinel:

1. Efetue login como `root`.
2. Verifique se todos os processos do Sentinel foram parados.
3. Remova o conteúdo de `/opt/novell/sentinel` ou do local onde o software Sentinel foi instalado.
4. Assegure-se de que ninguém está conectado ao sistema operacional como Administrador do Sentinel (o padrão é novell). Em seguida, remova o usuário, o diretório pessoal e o grupo.

   ```
   userdel -r novell
   ```

   ```
   groupdel novell
   ```
5. Reinicie o sistema operacional.