Sentinel Log Manager 1.2.2

Guia de Instalação

Julho de 2014

NetIQ

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 guia

Este guia fornece uma visão geral do Novell Sentinel Log Manager e sua instalação.

Público

Este guia se destina a administradores e usuários finais do Novell Sentinel Log Manager.

Comentários

Gostaríamos de receber seus comentários e suas sugestões sobre este manual e sobre as outras documentações incluídas no produto. Use o recurso Comentários do Usuário, localizado na parte inferior de cada página da documentação online ou acesse o site Novell Documentation Feedback (http://www.novell.com/documentation/feedback.html) para enviar seus comentários.

Documentação adicional

Para obter mais informações sobre a criação de seus próprios plug-ins (por exemplo, JasperReports), vá para a página da Web do Sentinel SDK (http://developer.novell.com/wiki/index.php/Develop_to_Sentinel). O ambiente de criação para plug-ins de relatório do Sentinel Log Manager é idêntico ao que é documentado para o Novell Sentinel.

Para obter mais informações sobre a documentação do Sentinel, consulte o site de Documentação do Sentinel (http://www.novell.com/documentation/sentinel61/index.html).

Para obter documentação adicional sobre a configuração do Sentinel Log Manager, consulte o *Sentinel Log Manager 1.2.2 Administration Guide (Guia de Administração do Sentinel Log Manager 1.2)*.

Contatando a Novell

- Site da Novell (http://www.novell.com)
- Suporte Técnico da Novell (http://support.novell.com/phone.html?sourceidint=suplnav4_phonesup)

- Suporte por autoatendimento da Novell (http://support.novell.com/support_options.html?sourceidint=suplnav_supportprog)
- Site para download de patches (http://download.novell.com/index.jsp)
- Suporte 24 horas da Novell (http://www.novell.com/company/contact.html)
- TIDS do Sentinel (http://support.novell.com/products/sentinel)
- Fórum de suporte da comunidade do Sentinel (http://forums.novell.com/novell-product-support-forums/sentinel/)

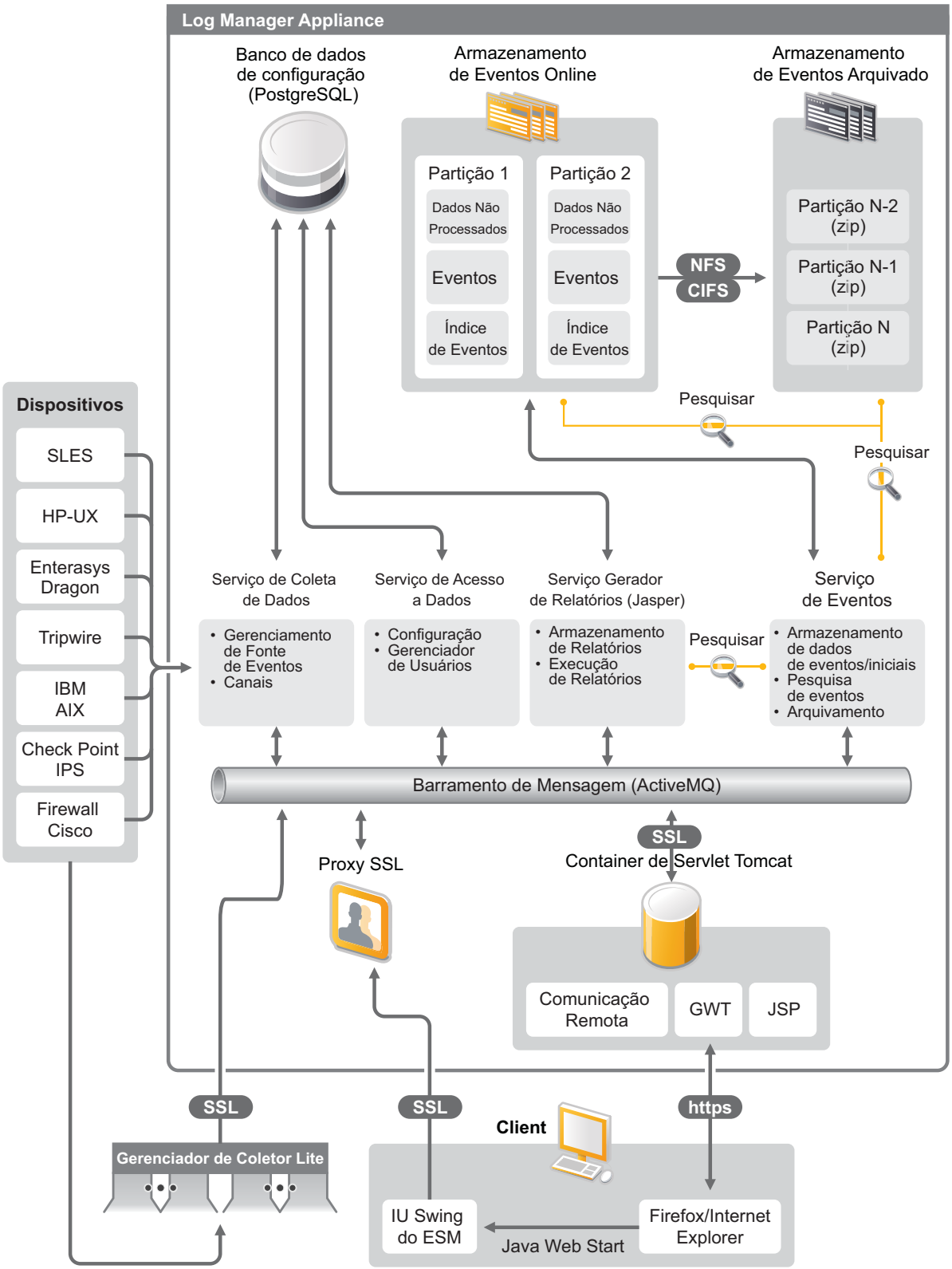
1 Introdução

O Novell Sentinel Log Manager coleta e gerencia dados em uma grande variedade de dispositivos e aplicativos, inclusive sistemas de detecção de intrusão, firewalls, sistemas operacionais, roteadores, servidores web, bancos de dados, switches, mainframes e fontes de eventos antivírus. O Novell Sentinel Log Manager fornece elevado processamento de taxa de eventos, retenção de dados em longo prazo, retenção de dados baseada em políticas, agregação de dados regionais e pesquisa e gerador de relatórios simples para uma ampla gama de aplicativos e dispositivos.

1.1 Visão geral do produto

O Novell Sentinel Log Manager 1.2 oferece uma solução flexível e escalável para gerenciamento de registros em organizações. O Novell Sentinel Log Manager é uma solução para gerenciamento de registros que resolve desafios básicos de coleta e gerenciamento de registros e também fornece uma solução completa focada na redução de custos e na complexidade de gerenciar o risco e simplificar requisitos de conformidade.

Figura 1-1 *Arquitetura do Novell Sentinel Log Manager*



O Novell Sentinel Log Manager possui os seguintes recursos:

- A pesquisa distribuída permite pesquisar eventos coletados não apenas no servidor local do Sentinel Log Manager, mas também em um ou mais servidores do Sentinel Log Manager a partir de um console centralizado.
- Os relatórios de conformidade pré-instalados simplificam a tarefa de gerar relatórios de conformidade para auditoria ou para análise forense.
- Utilizando uma tecnologia de armazenamento não patenteada, os clientes podem aproveitar sua infraestrutura atual e gerenciar mais os custos.
- A interface aprimorada baseada em browser suporta a coleta, o armazenamento, a geração de relatórios e a pesquisa de dados de registro para simplificar bastante as tarefas de monitoramento e gerenciamento.
- Controles granulados e eficientes e personalização para administradores de TI através dos novos recursos de grupos e usuários para fornecer mais transparência nas atividades da infraestrutura de TI.

Esta seção contém as seguintes informações:

1.1.1 Fontes de eventos

O Novell Sentinel Log Manager coleta dados de fontes de eventos que geram registros para o syslog, do registro de atividades do Windows, de arquivos, bancos de dados, SNMP, Novell Audit, Security Device Event Exchange (SDEE), Check Point Open Platforms for Security (OPSEC) e outros mecanismos e protocolos de armazenamento.

O Sentinel Log Manager suporta todas as fontes de eventos se houver Conectores adequados para analisar os dados das fontes de eventos. O Novell Sentinel Log Manager fornece Coletores para diversas fontes de eventos. O Coletor de Eventos Genérico coleta e processa dados de fontes de eventos não reconhecidas que possuam conectores adequados.

Para configurar a coleta de dados nas fontes de eventos, use a interface de Gerenciamento de Fonte de Eventos.

Para obter uma lista completa das fontes de eventos suportadas, consulte a Seção 2.6, “Fontes de eventos suportadas” na página 24

1.1.2 Gerenciamento de Fonte de Eventos

A interface de Gerenciamento de Fonte de Eventos permite importar e configurar os Conectores e Coletores do Sentinel 6.0 e 6.1.

As seguintes tarefas podem ser efetuadas através da Tela Ativa da janela Gerenciamento de Fonte de Eventos:

- Adicionar ou editar conexões a fontes de eventos usando assistentes de Configuração.
- Ver o status em tempo real das conexões com fontes de eventos.
- Importar ou exportar as configurações das fontes de eventos para ou da Tela Ativa.
- Ver e configurar Conectores e Coletores instalados com o Sentinel.
- Importar ou exportar Conectores e Coletores de ou para um repositório centralizado.
- Monitorar o fluxo de dados dos Coletores e Conectores configurados.
- Ver as informações de dados iniciais.
- Projetar, configurar e criar os componentes da hierarquia da Fonte de Eventos, além de executar as ações necessárias usando esses componentes.

Para obter mais informações, consulte a seção Gerenciamento de Fonte de Eventos do *Guia do Usuário do Sentinel* (http://www.novell.com/documentation/sentinel61/#admin).

1.1.3 Coleta de dados

O Novell Sentinel Log Manager coleta dados de fontes de eventos configuradas com a ajuda de Conectores e Coletores.

Os Coletores são scripts que analisam os dados de várias fontes de eventos na estrutura normalizada do Sentinel, ou em alguns casos coletam outras formas de dados em fontes de dados externas. Cada Coletor deve ser implantado com um Conector compatível. Os Conectores facilitam a conectividade entre os Coletores do Sentinel Log Manager e as fontes de eventos ou dados.

O Novell Sentinel Log Manager oferece uma interface do usuário com base na Web aprimorada para o syslog e o Novell Audit para coletar com facilidade registros de fontes de eventos diferentes.

O Novell Sentinel Log Manager usa diversos métodos de conexão para coletar dados:

- O Conector Syslog automaticamente aceita e configura fontes de dados syslog que enviam dados usando UDP, TCP ou TLS seguro.
- O Conector de Auditoria automaticamente aceita e configura fontes de dados da Novell habilitadas para auditoria.
- O Conector de Arquivos lê arquivos de registro.
- O Conector SNMP recebe detecções de SNMP.
- O Conector JDBC lê tabelas em bancos de dados.
- O Conector WMS acessa os registros de eventos do Windows em computadores e servidores.
- O Conector SDEE conecta-se a dispositivos que suportam o protocolo SDEE, tais como os dispositivos Cisco.
- O Conector de Exportação de Registros de Pontos de Verificação (LEA) facilita a integração entre os Coletores do Sentinel e servidores de Pontos de Verificação com firewall.

- O Conector de Link do Sentinel aceita dados de outros servidores do Novell Sentinel Log Manager.
- O Conector de Processos aceita dados de processos personalizados que geram registros de eventos.

Você também pode adquirir uma licença adicional para fazer download dos conectores em sistemas operacionais mainframe e SAP.

Para obter a licença, ligue para 1-800-529-3400 ou contate o Suporte Técnico da Novell (http://support.novell.com).

Para obter mais informações sobre configuração de Conectores, consulte os documentos sobre Conectores no site de plug-ins do Sentinel (http://support.novell.com/products/sentinel/secure/sentinelplugins.html).

Para obter mais informações sobre a configuração da coleta de dados, consulte a seção "Configurando a coleta de dados" no *Sentinel Log Manager 1.2.2 Administration Guide (Guia de Administração do Sentinel Log Manager 1.2)*.

Observação: Você sempre deve fazer o download e importar a versão mais recente dos Coletores e Conectores. Os Coletores e Conectores atualizados são disponibilizados regularmente no site de plug-ins do Sentinel 6.1 (http://support.novell.com/products/sentinel/secure/sentinelplugins.html). As atualizações dos Conectores e Coletores incluem correções, suporte a eventos adicionais e melhorias de desempenho.

1.1.4 Gerenciador de Coletor

O Gerenciador de Coletor oferece um ponto flexível para coleta de dados no Sentinel Log Manager. O Novell Sentinel Log Manager instala um Gerenciador de Coletor por padrão durante a instalação. Porém, você pode instalar Gerenciadores de Coletor remotamente em lugares adequados na rede. Esses Gerenciadores de Coletor remotos executam Conectores e Coletores, encaminhando os dados coletados ao Novell Sentinel Log Manager para armazenamento e processamento.

Para obter informações sobre a instalação de Gerenciadores de Coletor adicionais, consulte "Instalação de Gerenciadores de Coletor adicionais" na página 60.

1.1.5 Armazenamento de Dados

Os dados fluem dos componentes de coleta de dados para os componentes de armazenamento de dados. Esses componentes usam um armazenamento de dados baseado em arquivos e um sistema de indexação para manter os dados de registros coletados, e um banco de dados PostgreSQL para manter os dados de configuração do Novell Sentinel Log Manager.

Os dados são armazenados em formato comprimido no sistema de arquivos do servidor e depois armazenados em um local configurado para armazenamento de longo prazo. Os dados podem ser armazenados localmente ou em um compartilhamento NFS ou SMB (CIFS) montado remotamente. Os arquivos de dados são apagados dos locais de armazenamento local e em rede com base na programação configurada na política de retenção de dados.

Você pode configurar políticas de retenção de dados para apagar dados no local de armazenamento se o limite de tempo para a retenção de dados específicos for excedido ou se o espaço disponível estiver abaixo de um valor especificado.

Para obter mais informações sobre a configuração do armazenamento de dados, consulte a seção "Configurando o armazenamento de dados" no *Sentinel Log Manager 1.2.2 Administration Guide (Guia de Administração do Sentinel Log Manager 1.2)*.

1.1.6 Pesquisa e geração de relatórios

Os componentes de pesquisa e geração de relatórios ajudam a pesquisar e gerar relatórios nos dados de registro de eventos nos armazenamentos de dados locais ou em rede e nos sistemas de indexação. Os dados de eventos armazenados podem ser pesquisados genericamente ou usando campos de eventos específicos, como o nome de usuário de origem. Os resultados da pesquisa podem ser refinados ou filtrados e gravados como um gabarito de relatório para utilização futura.

O Sentinel Log Manager vem com relatórios pré-instalados. Você também pode fazer upload de relatórios adicionais. Você pode executar relatórios programados ou sempre que for necessário.

Para obter uma lista de relatórios padrão, consulte a seção "Geração de relatórios" no *Sentinel Log Manager 1.2.2 Administration Guide (Guia de Administração do Sentinel Log Manager 1.2)*.

Para obter mais informações sobre a pesquisa de eventos e a geração de relatórios, consulte as seções "Pesquisa de eventos" e "Gerador de relatórios" no *Guia de Administração do Sentinel Log Manager 1.2.2*.

1.1.7 Link do Sentinel

O Sentinel Link pode ser usado para encaminhar dados de eventos de um Sentinel Log Manager para outro. Com a organização hierárquica dos Sentinel Log Managers, é possível reter registros completos em várias regiões e encaminhar eventos mais importantes para um único Sentinel Log Manager, de modo a centralizar a realização de pesquisas e a geração de relatórios.

Além disso, o Link do Sentinel pode encaminhar eventos importantes para o Novell Sentinel, um sistema completo de Gerenciamento de Segurança, Informações e Eventos (SIEM), para correlação avançada, correção de incidentes e injeção de informações contextuais de alto valor, como informações de identidade ou importância do servidor fornecidas por um sistema de gerenciamento de identidade.

1.1.8 Interface do usuário com base na Web

O Novell Sentinel Log Manager vem com uma interface do usuário com base na web para configurar e usar o Log Manager. A funcionalidade da interface do usuário é fornecida por um servidor Web e uma interface gráfica do usuário com base no Java Web Start. Todas as interfaces de usuário comunicam-se com o servidor através de uma conexão criptografada.

Você pode usar a interface da Web do Novell Sentinel Log Manager para executar as seguintes tarefas:

- Pesquisar eventos
- Gravar os critérios de pesquisa como um gabarito de relatório
- Exibir e gerenciar relatórios
- Iniciar a interface de Gerenciamento de Fonte de Eventos para configurar a coleta de dados em fontes de eventos diferentes do syslog e aplicativos Novell. (somente administradores)
- Configurar o encaminhamento de dados (somente administradores)
- Fazer download do instalador do Gerenciador de Coletor do Sentinel para instalação remota (somente administradores)
- Ver a saúde de fontes de eventos (somente administradores)
- Configurar a coleta de dados em fontes de eventos syslog e Novell (somente administradores)

- Configurar o armazenamento de dados e ver a saúde do banco de dados (somente administradores)
- Configurar o arquivamento de dados (somente administradores)
- Configurar ações associadas para enviar dados de eventos correspondentes aos canais de saída (somente administradores)
- Gerenciar contas e permissões de usuários (somente administradores)

1.2 Visão geral da instalação

O Novell Sentinel Log Manager pode ser instalado como uma aplicação ou em um sistema operacional SUSE Linux Enterprise Server (SLES) 11 SP1. Quando o Sentinel Log Manager é instalado como uma aplicação, o servidor do Log Manager é instalado em um sistema operacional SLES 11 SP1.

O Novell Sentinel Log Manager instala os seguintes componentes por padrão:

- Servidor do Sentinel Log Manager
- Servidor de comunicações
- Servidor Web e interface do usuário com base na web
- Servidor do gerador de relatórios
- Gerenciador de Coletor

Alguns desses componentes exigem configuração adicional.

O Novell Sentinel Log Manager instala um Gerenciador de Coletor por padrão. Se desejar Gerenciadores de Coletor adicionais, instale-os separadamente em máquinas remotas. Para obter mais informações, consulte a Capítulo 7, “Instalação de Gerenciadores de Coletor adicionais” na página 59.

2 Requisitos do sistema

As seções a seguir descrevem os requisitos de hardware, sistema operacional, browser, Conectores suportados e requisitos de compatibilidade com fontes de eventos para o Novell Sentinel Log Manager.

2.1 Requisitos de hardware

2.1.1 Servidor do Sentinel Log Manager

O Novell Sentinel Log Manager é suportado em processadores Intel Xeon e AMD Opteron de 64 bits, mas não é suportado em processadores Itanium.

Os requisitos de hardware relacionados na tabela a seguir são recomendados para um sistema de produção que armazena 90 dias de dados online. Esses requisitos são para um tamanho médio de eventos de 300 bytes.

Tabela 2-1 *Requisitos de hardware do Sentinel Log Manager*

Requisitos	Sentinel Log Manager (500 EPS)	Sentinel Log Manager (2500 EPS)	Sentinel Log Manager (7500 EPS)
Compactação	Até 10:1	Até 10:1	Até 10:1

Requisitos	Sentinel Log Manager (500 EPS)	Sentinel Log Manager (2500 EPS)	Sentinel Log Manager (7500 EPS)
Máximo de fontes de eventos	Até 1000	Até 1000	Até 2000
Taxa máxima de eventos	500	2500	7500
CPU	Uma CPU Intel Xeon E5430 de 3 GHz (4 núcleos) ou Duas CPUs Intel Xeon L5240 3-(2 núcleos - 4 núcleos no total)	Uma CPU Intel Xeon E5430 de 3 GHz (4 núcleos) ou Duas CPUs Intel Xeon L5240 3-(2 núcleos - 4 núcleos no total)	Duas CPUs Intel Xeon X5470 de 3.33 GHz (4 núcleos - 8 núcleos no total)
Memória RAM	4 GB	4 GB	8 GB
Armazenamento local (30 dias)	2 unidades de 500 GB e 7.200 RPM (Hardware RAID com 256 MB de cache, RAID 1)	4 unidades de 10 TB e 7.200 RPM (Hardware RAID com 256 MB de cache, RAID 1)	16 unidades RPM de 600 GB, 15k (RAID de hardware com cache de 512 MB, RAID 10) ou uma SAN (storage area network) equivalente
Armazenamento em rede (90 dias)	600 GB	2 TB	5.8 TB

Siga estas diretrizes para ter um desempenho ideal do sistema:

- O armazenamento local deve ter espaço suficiente para reter, pelo menos, 5 dias válidos de dados, que inclui dados de eventos e dados não processados. Para obter mais detalhes sobre como calcular os requisitos de armazenamento de dados, consulte Seção 2.1.3, “Estimativa dos requisitos para armazenamento de dados” na página 19.
- O armazenamento em rede contém todos os 90 dias válidos de dados, incluindo uma cópia totalmente compactada dos dados de evento no armazenamento local. Uma cópia dos dados de evento é mantida no armazenamento local para pesquisa e relatório de motivos de desempenho. O tamanho do armazenamento local pode ser diminuído se o tamanho de armazenamento for uma preocupação. No entanto, devido ao overhead de descompactação, haverá uma diminuição estimada de 70% na pesquisa e no relatório de desempenho em dados que estariam no armazenamento local.
- Você deve definir o local de armazenamento em rede em uma área externa de armazenamento em rede com diversas unidades SAN ou em um armazenamento anexado à rede (NAS).
- Uma máquina pode incluir mais de uma fonte de eventos. Por exemplo, um servidor Windows pode incluir duas fontes de eventos do Sentinel para coletar dados do sistema operacional Windows e também do banco de dados do Servidor SQL hospedado na mesma máquina.
- O volume de estado estável recomendado é 80% do máximo de EPS licenciados. A Novell recomenda que você adicione instâncias adicionais do Sentinel Log Manager se o limite for atingido.
- Os limites máximos de fontes de eventos não são limites rígidos, mas sim recomendações baseadas em testes de desempenho feitos pela Novell e assumem uma média baixa para a taxa de eventos por segundo por fonte de eventos (menos de 3 EPS). Taxas de EPS mais altas resultam em mais baixa sustentação máxima de fontes de eventos. Você pode usar a equação

(máximo de fontes de eventos) x (média de EPS por fonte de eventos) = taxa máxima de eventos para encontrar os limites aproximados para a sua taxa de EPS específica ou o número de fontes de eventos, desde que o máximo de fontes de eventos não exceda o limite indicado acima.

2.1.2 Sistema do Gerenciador de Coletor

- ❒ Um Intel Xeon X5570 2,93 GHz (4 núcleos de CPU)
- ❒ 4 GB de RAM
- ❒ 10 GB de espaço livre em disco

2.1.3 Estimativa dos requisitos para armazenamento de dados

O Sentinel Log Manager é usado para reter dados iniciais por um longo período de tempo e atender a conformidades legais e outros requisitos. O Sentinel Log Manager usa compactação para auxiliar na utilização eficiente do espaço de armazenamento local e em rede. Porém, os requisitos de armazenamento podem se tornar significativos ao longo de um extenso período de tempo.

Para superar problemas de limitação de custos em grandes sistemas de armazenamento, você pode usar sistemas econômicos que armazenam dados por longos períodos. Sistemas de armazenamento baseados em fitas são a solução mais comum e econômica. Entretanto, a fita não permite acesso aleatório aos dados armazenados, o que é necessário para efetuar pesquisas rápidas. Por causa disso, uma abordagem híbrida para armazenamento de dados é desejável, onde os dados que precisam ser pesquisados estão disponíveis em um sistema de acesso aleatório e os dados que precisam ser retidos, mas não pesquisados, são mantidos em uma alternativa econômica, como a fita. Para obter instruções sobre a utilização dessa abordagem híbrida, consulte a seção "Usando armazenamento de acesso sequencial para armazenar dados a longo prazo" no *Sentinel Log Manager 1.2.2 Administration Guide (Guia de Administração do Sentinel Log Manager 1.2)*.

Para determinar o espaço de armazenamento de acesso sequencial necessário para o Sentinel Log Manager, primeiro estime quantos dias de dados você precisa para efetuar pesquisas regularmente ou executar relatórios. Você deve ter espaço suficiente no disco rígido local da máquina do Sentinel Log Manager, ou remotamente nos protocolos SMB ou CIFS, o sistema de arquivos da rede (NFS) ou um SAN para ser usado no arquivamento de dados pelo Sentinel Log Manager.

Além dos requisitos mínimos, você também deve ter o espaço adicional a seguir no disco rígido:

- Para lidar com taxas de eventos acima do esperado.
- Para copiar dados de fitas e de volta ao Sentinel Log Manager para realizar pesquisas e gerar relatórios sobre dados históricos.

Use as seguintes fórmulas para estimar o espaço necessário para armazenar dados:

- **Armazenamento de evento local (parcialmente compactado):** {tamanho médio de byte por evento} x {número de dias} x {eventos por segundo} x 0,00007 = total de armazenamento em GB necessário

  O tamanho dos eventos geralmente varia entre 300 e 1.000 bytes.
- **Armazenamento de eventos em rede (totalmente compactado):** {tamanho médio de byte por evento} x {número de dias} x {eventos por segundo} x 0,00002 = total de armazenamento em GB necessário
- **Armazenamento de dados não processados (totalmente compactados em armazenamento local e em rede):** {tamanho médio de byte por registro de dados não processados} x {número de dias} x {eventos por segundo} x 0,000012 = total de armazenamento em GB necessário

O tamanho médio típico dos dados iniciais de mensagens syslog é 200 bytes.

- **Tamanho de armazenamento local total (com armazenamento em rede habilitado):** {Tamanho de armazenamento de eventos local para número desejado de dias} + {Tamanho de armazenamento de dados não processados por um dia) = Total de armazenamento em GB necessário

  Se o armazenamento em rede estiver habilitado, os dados de eventos serão movidos para armazenamento em rede quando o armazenamento local for preenchido. No entanto, os dados não processados estão localizados no armazenamento local somente temporariamente antes de serem movidos para armazenamento em rede. Geralmente, leva menos de um dia para mover os dados não processados do armazenamento local para o armazenamento em rede.

- **Tamanho de armazenamento local total (com armazenamento em rede desabilitado):**

  {Tamanho de armazenamento de eventos local para tempo de retenção} + {Tamanho de armazenamento de dados não processados para tempo de retenção) = Total de armazenamento em GB necessário

- **Tamanho total de armazenamento em rede:** {Tamanho de armazenamento de eventos em rede para tempo de retenção} + {Tamanho de armazenamento de dados não processados para tempo de retenção) = Total de armazenamento em GB necessário

---

Observação:

- Os coeficientes em cada fórmula representam (segundos por dia) x (GB por byte) x taxa de compactação).
- Esses números são apenas estimativas e dependem do tamanho dos dados de eventos e do tamanho dos dados compactados.
- Parcialmente compactados significa que os dados estão compactados, mas o índice dos dados não está compactado. Totalmente compactados significa que os dados de eventos e de índice estão compactados. As proporções de compactação de dados de eventos são geralmente 10:1. As taxas de compactação de índice são geralmente 5:1. O índice é usado para otimizar a pesquisa nos dados.

Você também pode usar as fórmulas acima para determinar o espaço de armazenamento necessário para um sistema de armazenamento de longo prazo, como as fitas.

2.1.4 Estimativa de utilização de E/S de disco

Use as fórmulas a seguir para estimar a quantidade de utilização de disco no servidor em várias taxas de EPS.

- **Dados gravados no disco (kilobytes por segundo):** (tamanho de eventos médio em bytes + tamanho médio de dados não processados em bytes) x (eventos por segundo) x coeficiente de compactação de dados 0,004 = dados gravados por segundo em disco

  Por exemplo, a 500 EPS, para um tamanho de evento médio de 464 bytes e um tamanho médio de dados não processados de 300 bytes no arquivo de registro, os dados gravados no disco são determinados da seguinte forma:

  (464 bytes + 300 bytes) x 500 EPS x 0,004 = 1.558 KB

- **Número de solicitação de E/S para o disco (transferências por segundo):** (tamanho de eventos médio em bytes + tamanho médio de dados não processados em bytes) x (eventos por segundo) x coeficiente de compactação de dados 0,00007 = solicitações de E/S por segundo para disco

Por exemplo, a 500 EPS, para um tamanho de evento médio de 464 bytes e um tamanho médio de dados não processados de 300 bytes no arquivo de registro, o número de solicitações de E/S por segundo para o disco é determinado da seguinte forma:

(464 bytes + 300 bytes) x 500 EPS x 0,00007 = 26 tps

- **Número de blocos gravados por segundo no disco:** (tamanho de eventos médio em bytes + tamanho médio de dados não processados em bytes) x (eventos por segundo) x coeficiente de compactação de dados 0,008 = dados gravados por segundo em disco

  Por exemplo, a 500 EPS, para um tamanho de evento médio de 464 bytes e um tamanho médio de dados não processados de 300 bytes no arquivo de registro, o número de blocos gravados por segundo no disco é determinado da seguinte forma:

  (464 bytes + 300 bytes) x 500 EPS x 0,008 = 3.056

- **Dados lidos por segundo do disco ao realizar uma pesquisa:** (tamanho médio de eventos em bytes + tamanho médio de dados não processados em bytes) x (número de eventos correspondendo à consulta em milhões) x coeficiente de compactação 0,013 = kilobytes lidos por segundo do disco

  Por exemplo, em 3 milhões de eventos correspondentes à consulta de pesquisa, para um tamanho médio de eventos de 464 bytes e um tamanho médio de dados não processados de 300 bytes no arquivo de registro, os dados lidos por segundo no disco é determinado da seguinte forma:

  (464 bytes + 300 bytes) x 3 x 0,013 = 300 KB

2.1.5 Estimativa de utilização de largura de banda de rede

Use as fórmulas a seguir para estimar a utilização de largura de banda em rede no servidor em várias taxas de EPS:

{tamanho médio de eventos em bytes + tamanho médio de dados não processados em bytes} x {eventos por segundo} x coeficiente de compactação 0,0003 = largura de banda de rede em Kbps (kilobits por segundo)

Por exemplo, a 500 EPS, para um tamanho de evento médio de 464 bytes e um tamanho médio de dados não processados de 300 bytes no arquivo de registro, a utilização de largura de banda de rede é determinada da seguinte forma:

(464 bytes + 300 bytes} x 500 EPS x 0,0003 = 115 Kbps

2.1.6 Ambiente virtual

O Sentinel Log Manager é extensivamente testado e completamente suportado em servidores VMware ESX. 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 Seção 2.1, “Requisitos de hardware” na página 17.

2.2 Sistemas operacionais suportados

A Novell é compatível com o Sentinel Log Manager nos sistemas operacionais descritos nesta seção. A Novell também é compatível com o Sentinel Log Manager em sistemas com atualizações secundárias a esses sistemas operacionais, como patches de segurança ou hotfixes. No entanto, a

execução do Sentinel Log Manager em sistemas com importantes atualizações para esses sistemas operacionais não é suportada enquanto a Novell não tiver testado e certificado essas atualizações.

2.2.1 Sentinel Log Manager

- ❒ SUSE Linux Enterprise Server 11 SP3 de 64 bits.
- ❒ Um sistema de arquivos de alto desempenho.

Observação: Todos os testes da Novell são feitos com o sistema de arquivos ext3.

2.2.2 Gerenciador de Coletor

Você pode instalar Gerenciadores de Coletor adicionais nos seguintes sistemas operacionais:

Linux

- ❒ SUSE Linux Enterprise Server 11 SP3 (64 bits)

Windows

- ❒ Windows Server 2003 (32 bits e 64 bits)
- ❒ Windows Server 2003 SP2 (32 bits e 64 bits)
- ❒ Windows Server 2003 R2 (32 bits e 64 bits)
- ❒ Windows Server 2008 (64 bits)
- ❒ Windows Server 2008 R2 (64 bits)

2.3 Browsers suportados

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

2.3.1 Linux

- ❒ Mozilla Firefox 5 e versões posteriores

2.3.2 Windows

- ❒ Mozilla Firefox 5 e versões posteriores
- ❒ Microsoft Internet Explorer 8 e 11*

* Consulte a "Pré-requisitos para o Internet Explorer" na página 23.

Pré-requisitos para o Internet Explorer

- Se o Nível de Segurança da Internet estiver definido como Alto, aparecerá uma página vazia após efetuar login no Sentinel Log Manager. Para resolver esse problema, vá em *Ferramentas* > *Opções da Internet* > *guia Segurança* > *Sites Confiáveis*. Clique no botão *Site* e adicione o site do Sentinel Log Manager à lista de sites confiáveis.
- Certifique-se de que a opção *Ferramentas* > *Modo de Exibição de Compatibilidade* não está selecionada.
- Se a opção *Aviso automático para downloads de arquivo* não estiver habilitada, o pop-up de download de arquivo pode ser bloqueado pelo browser. Para resolver esse problema, vá em *Ferramentas* > *Opções da Internet* > *guia Segurança* > *Nível personalizado*, então mova a barra de rolagem para baixo até a seção de download e selecione *Habilitar* para habilitar a opção *Aviso automático para downloads de arquivo*.

2.4 Ambientes virtuais suportados

- ❒ VMware ESX/ESXi 3.5/4.0 ou superior
- ❒ VMPlayer 3 (apenas para demonstração)
- ❒ Xen 3.1.1

2.5 Conectores suportados

O Sentinel Log Manager suporta todos os Conectores suportados pelo Sentinel e pelo Sentinel RD.

- ❒ Conector de Auditoria
- ❒ Conector do Processo do Ponto de Verificação LEA
- ❒ Conector de Banco de Dados
- ❒ Conector de Gerador de Dados
- ❒ Conector de Arquivos
- ❒ Conector de Processo
- ❒ Conector Syslog
- ❒ Conector SNMP
- ❒ Conector SDEE
- ❒ Conector do Link do Sentinel
- ❒ Conector WMS

- ❒ Conector de Mainframe
- ❒ Conector SAP

Observação: Os Conectores de Mainframe e SAP exigem uma licença separada.

2.6 Fontes de eventos suportadas

O Sentinel Log Manager suporta uma variedade de dispositivos e aplicativos, inclusive sistemas de detecção de intrusão, firewalls, sistemas operacionais, roteadores, servidores web, bancos de dados, switches, mainframes e fontes de eventos antivírus. Os dados dessas fontes de eventos são analisados e normalizados em diferentes graus, dependendo se os dados são processados usando o Coletor de eventos genérico que coloca todo o payload do evento em um campo comum, ou usando um Coletor específico de um dispositivo que analisa os dados em campos individuais.

As seguintes fontes de eventos são suportadas pelo Sentinel Log Manager:

- ❒ Cisco Firewall (6 e 7)
- ❒ Cisco Switch Catalyst 6500 Series (CatOS 8.7)
- ❒ Cisco Switch Catalyst 6500 Series (IOS 12.2SX)
- ❒ Cisco Switch Catalyst 5000 Series (CatOS 4.x)
- ❒ Cisco Switch Catalyst 4900 Series (IOS 12.2SG)
- ❒ Cisco Switch Catalyst 4500 Series (IOS 12.2SG)
- ❒ Cisco Switch Catalyst 4000 Series (CatOS 4.x)
- ❒ Cisco Switch Catalyst 3750 Series (IOS 12.2SE)
- ❒ Cisco Switch Catalyst 3650 Series (IOS 12.2SE)
- ❒ Cisco Switch Catalyst 3550 Series (IOS 12.2SE)
- ❒ Cisco Switch Catalyst 2970 Series (IOS 12.2SE)
- ❒ Cisco Switch Catalyst 2960 Series (IOS 12.2SE)
- ❒ Cisco VPN 3000 (4.1.5, 4.1.7 e 4.7.2)
- ❒ Extreme Networks Summit X650 (com ExtremeXOS 12.2.2 e anteriores)
- ❒ Extreme Networks Summit X450a (com ExtremeXOS 12.2.2 e anteriores)
- ❒ Extreme Networks Summit X450e (com ExtremeXOS 12.2.2 e anteriores)
- ❒ Extreme Networks Summit X350 (com ExtremeXOS 12.2.2 e anteriores)
- ❒ Extreme Networks Summit X250e (com ExtremeXOS 12.2.2 e anteriores)
- ❒ Extreme Networks Summit X150 (com ExtremeXOS 12.2.2 e anteriores)
- ❒ Enterasys Dragon (7.1 e 7.2)
- ❒ Coletor de Eventos genérico
- ❒ HP HP-UX (11iv1 e 11iv2)
- ❒ IBM AIX (5.2, 5.3 e 6.1)
- ❒ Juniper Netscreen Series 5

- McAfee Firewall Enterprise
- Plataforma McAfee Network Security (2.1, 3.x e 4.1)
- McAfee VirusScan Enterprise (8.0i, 8.5i e 8.7i)
- McAfee ePolicy Orchestrator (3.6 e 4.0)
- McAfee AV Via ePolicy Orchestrator 8.5
- Microsoft Active Directory (2000, 2003 e 2008)
- Microsoft SQL Server (2005 e 2008)
- Nortel VPN (1750, 2700, 2750 e 5000)
- Novell Access Manager 3.1
- Novell Identity Manager 3.6.1
- Novell Netware 6.5
- Novell Modular Authentication Services 3.3
- Novell Open Enterprise Server 2.0.2
- Novell Privileged User Manager 2.2.1
- Novell Sentinel Link 1
- Novell SUSE Linux Enterprise Server
- Novell eDirectory 8.8.3 com o patch de instrumentação do eDirectory encontrado no site de Suporte da Novell (http://download.novell.com/Download?buildid=RH_B5b3M6EQ~)
- Novell iManager 2.7
- Red Hat Enterprise Linux
- Sourcefire Snort (2.4.5, 2.6.1, 2.8.3.2 e 2.8.4)
- Snare for Windows Intersect Alliance (3.1.4 e 1.1.1)
- Sun Microsystems Solaris 10
- Symantec AntiVirus Corporate Edition (9 e 10)
- TippingPoint Security Management System (2.1 e 3.0)
- Websense Web Security 7.0
- Websense Web Filter 7.0

Observação: Para habilitar a coleta de dados em fontes de eventos Novell iManager e Novell Netware 6.5, adicione uma instância de um coletor e de um conector filho (conector de Auditoria) na interface de Gerenciamento de Fonte de Eventos para cada uma das fontes de eventos. Quando isso for feito, essas fontes de eventos serão exibidas na interface da Web do Sentinel Log Manager > *collection* > *Event Sources*.

Coletores que suportam fontes de eventos adicionais podem ser obtidos no site de plug-ins do Sentinel (http://support.novell.com/products/sentinel/secure/sentinelplugins.html) ou construídos usando os plug-ins do SDK que estão disponíveis no site do SDK de Plug-ins do Sentinel (http://developer.novell.com/wiki/index.php?title=Develop_to_Sentinel).

2.7 Limites recomendados

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

2.7.1 Limites do Gerenciador de Coletor

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

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

Atributo	Limites	Comentários
Número máximo de Gerenciadores de Coletor	20	Este limite considera que cada Gerenciador de Coletor esteja sendo executado a um EPS baixo (ex. menos de 100 EPS). O limite cai à medida que os eventos por segundo aumentam.
Número máximo de Conectores (totalmente utilizados) em um único Gerenciador de Coletor	1 por núcleo de CPU, com pelo menos 1 núcleo da CPU reservado para o sistema operacional e outro processamento	Um Conector totalmente utilizado é aquele que é executado com o maior EPS possível para seu tipo de Conector.
Número máximo de Coletores (totalmente utilizados) em um único Gerenciador de Coletor	1 por núcleo de CPU, com pelo menos 1 núcleo da CPU reservado para o sistema operacional e outro processamento	Um Coletor totalmente utilizado é aquele que é executado com o maior EPS possível para seu tipo de Coletor.
Número máximo de fontes de eventos em um único Gerenciador de Coletor	2000	O limite do servidor Sentinel Log Manager é 1.000 ou 2.000, dependendo do hardware. Se o limite de servidor for atingido em um único Gerenciador de Coletor, então o limite de fontes de eventos para o sistema Sentinel geral terá sido atingido com esse único Gerenciador de Coletor.
Número máximo de fontes de eventos por instância de servidor Sentinel Log Manager	2.000	

2.7.2 Limites de relatórios

Tabela 2-3 *Números de Desempenho de Relatórios*

Atributo	Limites	Comentários
Número máximo de relatórios salvos	200	
Número máximo de relatórios sendo executados simultaneamente	3	O limite pressupõe que o servidor ainda não está altamente utilizado executando coleta de dados ou outras tarefas.

2.7.3 Limites de EPS de ações

Salvo especificação contrária, os limites de EPS de ações pressupõem que uma ação seja configurada por regra.

Tabela 2-4 *Números de desempenho de ações*

Ação	EPS por ação
Link do Sentinel	300
Registrar-se no arquivo	30 a 50
Enviar um e-mail	40
Registrar-se no Syslog	5 a 10
Executar Script	5 a 10

2.7.4 Limites de arquivos abertos SLES

Em sistemas onde há um número maior de fontes de eventos (por exemplo, mais de 75) com a maioria usando o Conector de Arquivo e o deslocamento definido para o início do arquivo, o limite de arquivos abertos SLES pode não ser o mesmo que o número de arquivos atualmente abertos no sistema; isso pode levar a problemas de desempenho no Sentinel Log Manager.

Para evitar esse problema, você pode definir os limites de software e hardware para o número máximo de arquivos abertos com base no número de arquivos que estão abertos.

Realize as etapas a seguir para definir os limites de arquivos abertos:

1. Efetue login no sistema como usuário Novell.
2. Veja o número de arquivos que estão abertos para o usuário Sentinel (Novell).

   ```
   lsof | wc -l
   ```

3. Veja os limites de hardware e software:

   ```
   ulimit -Hn
   ulimit -Sn
   ```

Com base no número de arquivos abertos, é possível definir os limites de descritor de arquivo no arquivo `/etc/security/limits.conf`. Por exemplo, se o número de arquivos abertos for 1.000, os limites poderão ser definidos como 2.000.

Observação: Somente o usuário raiz pode editar o arquivo `/etc/security/limits.conf`.

4 Certifique-se de que o usuário raiz defina os limites do descritor de arquivo da seguinte forma:

```
novell soft nofile 2000
novell hard nofile 2000
```

Observação: É opcional definir os limites de software; no entanto, definir os limites de hardware é obrigatório.

5 Grave as mudanças.

2.8 Desempenho de pesquisa e relatórios

O desempenho do Sentinel Log Manager pode variar dependendo do ambiente, configuração e hardware. A Novell realizou testes avançados de desempenho no sistema Sentinel Log Manager para validar e verificar os atributos de qualidade do sistema, como escalabilidade, confiabilidade e uso de recursos.

- Seção 2.8.1, "Velocidade de conclusão e resposta de pesquisa" na página 28
- Seção 2.8.2, "Velocidade de geração de relatório" na página 29

2.8.1 Velocidade de conclusão e resposta de pesquisa

Foram realizados vários testes com a seguinte configuração para determinar a duração de uma pesquisa para retornar dados iniciais:

- **Hardware:** 4 núcleos de CPU em 2,93 GHz cada, 4 GB de RAM, executando em SLES 11
- **Taxa de EPS:** A taxa de EPS de entrada ao realizar a pesquisa é de 2.000
- **Armazenamento de dados:** Todos os dados de eventos no intervalo de tempo estão no armazenamento local

Os seguintes itens são observações:

Tabela 2-5 *Resultados de desempenho de pesquisa*

Total de eventos	Número de eventos correspondendo à consulta de pesquisa	Horário para resultados de pesquisa inicial
10.000.000	1.000 - 10.000.000	5 a 10 segundos
100.000.000	20.000.000 - 100.000.000	10 a 30 segundos
200.000.000	110.000.000 - 200.000.000	1 a 5 minutos

2.8.2 Velocidade de geração de relatório

Foram realizados vários testes com a seguinte configuração para determinar a duração utilizada para a geração de relatório.

- **Hardware:** 4 núcleos de CPU em 2,93 GHz cada, 4 GB de RAM, executando em SLES 11
- **Taxa de EPS:** A taxa de EPS de entrada ao realizar a pesquisa é de 2.000
- **Localização dos dados:** Todos os dados de eventos no intervalo de tempo estão no armazenamento local

Os seguintes são observações:

Tabela 2-6 *Resultados de desempenho de relatórios*

Total de eventos	Número de eventos correspondendo à consulta de pesquisa	Tempo para geração do relatório
10.000.000	1.000 - 10.000.000	1 a 2 minutos
100.000.000	20.000.000 - 100.000.000	10 a 50 minutos
200.000.000	110.000.000 - 200.000.000	1 a 3 horas

Observação: Para relatórios com um grande número de eventos e uma grande quantidade de campos, como o relatório Detalhes do evento, a geração de relatórios pode ser bastante demorada e o sistema pode ficar sem memória. A fim de melhorar os resultados de desempenho da geração de relatórios, você pode aumentar a memória RAM do sistema.

3 Instalação em um sistema SLES 11 SP1 existente

Esta seção descreve o procedimento de instalação do Sentinel Log Manager em um sistema SUSE Linux Enterprise Server (SLES) 11 SP1 usando o instalador do aplicativo. Você pode instalar o servidor do Sentinel Log Manager de diversas maneiras: o procedimento de instalação padrão, o procedimento de instalação personalizado ou o procedimento de instalação silencioso, onde a instalação prossegue sem a interferência do usuário e usa os valores padrão. Você também pode instalar o Sentinel Log Manager como um usuário não raiz.

Se escolher o método de instalação personalizada, você tem a opção de instalar o produto com uma chave de licença e também selecionar uma opção de autenticação. Você pode configurar a autenticação LDAP para o Sentinel Log Manager além da autenticação do banco de dados. Quando o Sentinel Log Manager é configurado para autenticação LDAP, os usuários podem efetuar login no servidor usando suas credenciais do Novell eDirectory ou do Microsoft Active Directory.

Se você deseja instalar diversos servidores do Sentinel Log Manager na sua implantação, você pode registrar as opções de instalação em um arquivo de configuração e usá-lo para executar uma instalação autônoma. Consulte a Seção 3.4, “Instalação silenciosa” na página 36 para obter mais informações.

3.1 Antes de começar

- Certifique-se de que o hardware e o software atendem aos requisitos mínimos mencionados no Capítulo 2, “Requisitos do sistema” na página 17.
- Certifique-se de que o rpm libstdc++33 de 32 bits esteja instalado. Instale este rpm usando YaST ou o comando zypper:

  ```
  zypper in libstdc++33-32bit
  ```

- Para que o Sentinel Log Manager 1.2 e versão posterior funcione com êxito no SLES 11 SP1, a versão seguinte ou posterior de RPMs deve ser instalada:
  - **Patches kernel:**
    - `kernel-default-2.6.32.29-0.3.1.x86_64.rpm`
    - `kernel-default-base-2.6.32.29-0.3.1.x86_64.rpm`
  - **RPMs util Linux:**
    - `libblkid1-2.16-6.11.1.x86_64.rpm`

- `libuuid1-2.16-6.11.1.x86_64.rpm`
- `util-linux-2.16-6.11.1.x86_64.rpm`
- `util-linux-lang-2.16-6.11.1.x86_64.rpm`
- `uuid-runtime-2.16-6.11.1.x86_64.rpm`

O Sentinel Log Manager 1.1.0.x usa o squashfs versão 3.4-35.1; no entanto, o SLES 11 SP.1 é compatível com o squashfs 4.0 e versão posterior, que não é compatível com versões anteriores e não pode abrir um sistema de arquivos do squashfs criado com versões anteriores do squashfs. Instalar esses RPMs resolve o problema de incompatibilidade entre as versões squashfs do Sentinel Log Manager 1.1.0.x e SLES 11 SP1.

Esses RPMs estão disponíveis através do canal de atualização on-line do SLES 11. Para obter mais informações sobre como atualizar o sistema SLES, consulte "Atualização on-line do YaST" (http://www.novell.com/documentation/sles11/book_sle_admin/?page=/documentation/sles11/book_sle_admin/data/cha_onlineupdate_you.html) no *Guia de administração do SLES 11 SP1 (http://www.novell.com/documentation/sles11/book_sle_admin/data/book_sle_admin_pre.html)*.

Observação: A instalação não prosseguirá a menos que os patches kernel e os RPMs util Linux mencionados acima estejam instalados.

- Configure o sistema operacional de maneira que o comando `hostname -f` retorne um nome de host válido.
- Obtenha sua chave de licença com o Atendimento ao Cliente Novell (https://secure-www.novell.com/center/ICSLogin/?%22https://secure-www.novell.com/center/regadmin/jsps/home_app.jsp%22) para instalar a versão licenciada.
- Sincronize o horário usando o protocolo NTP (Network Time Protocol).
- Instale os seguintes comandos do sistema operacional:
  - `mount`
  - `umount`
  - `id`
  - `df`
  - `du`
  - `sudo`
- Certifique-se de que as seguintes portas estão abertas no firewall:

  TCP 8080, TCP 8443, TCP 61616, TCP 10013, TCP 1289, TCP 1468, TCP 1443 e UDP 1514

  Para obter mais informações sobre a utilização dessas portas, consulte Seção 4.2, "Portas usadas" na página 39.

3.2 Instalação padrão

O procedimento de instalação padrão instala o Sentinel Log Manager com uma licença de avaliação de 60 dias e instala todos os recursos, exceto o recurso de restauração de dados.

1. Faça o download e copie os arquivos de instalação no site de Download da Novell.
2. Efetue login como `root` no servidor em que você deseja instalar o Sentinel Log Manager.
3. Especifique o comando a seguir para extrair os arquivos de instalação do arquivo tar:

   `tar xfz <install_filename>`

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

4 Altere para o diretório de onde o arquivo install foi extraído.

5 Especifique o comando a seguir para executar o script `install-slm` e instalar o Sentinel Log Manager:

```
./install-slm
```

Se desejar instalar o Sentinel Log Manager em mais de um sistema, você pode registrar as opções de instalação em um arquivo. Esse arquivo pode ser usado para instalar o Sentinel Log Manager de maneira autônoma em outros sistemas. Para registrar as opções de instalação, especifique o seguinte comando:

```
./install-slm -r responseFile
```

6 Para prosseguir com o idioma de sua escolha, selecione o número especificado ao lado de cada idioma.

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

7 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.

A instalação cria um grupo `novell` e um usuário `novell`, caso ainda não existam.

8 Quando solicitado, especifique a opção para continuar com a instalação padrão.

A instalação prossegue com a chave de licença de avaliação de 60 dias incluída com o instalador. A chave de licença ativa o conjunto completo de recursos de produto por um período de avaliação de 60 dias, exceto o recurso de restauração de dados. A qualquer momento durante ou após o período de teste, você pode adicionar a licença de avaliação a uma chave de licença comprada.

9 Especifique a senha do usuário administrador.

10 Confirme a senha do usuário administrador.

O instalador seleciona o método *Autenticar apenas para o banco de dados* e continua com a instalação.

A instalação do Sentinel Log Manager é finalizada e o servidor é iniciado. Pode levar cerca de 5 a 10 minutos para que todos os serviços sejam iniciados após a instalação, enquanto o sistema efetua uma inicialização única. Aguarde por esse período antes de efetuar login no servidor.

11 Para efetuar login no servidor do Sentinel Log Manager, use o URL especificado na saída da instalação. O URL é similar a `https://10.0.0.1:8443/novelllogmanager`.

Para obter mais informações sobre login no servidor, consulte o Capítulo 6, “Efetuando login na interface na Web” na página 57.

12 Para configurar fontes de eventos para que enviem dados ao Sentinel Log Manager, consulte a seção “Configurando a coleta de dados” no *Sentinel Log Manager 1.2.2 Administration Guide (Guia de Administração do Sentinel Log Manager 1.2)*.

Observação: Quando o sistema é reiniciado pela primeira vez após a instalação, esse processo pode demorar aproximadamente cinco minutos até que você possa começar a usá-lo. Esse atraso ocorre somente quando você inicia o sistema pela primeira vez após a instalação ou uma atualização.

3.3 Instalação personalizada

Se escolher o método de instalação personalizada, você tem a opção de instalar o produto com uma chave de licença e também selecionar uma opção de autenticação. Você pode configurar a autenticação LDAP para o Sentinel Log Manager além da autenticação do banco de dados. Quando o Sentinel Log Manager é configurado para autenticação LDAP, os usuários podem efetuar login no servidor usando as credenciais do diretório LDAP.

Se o Sentinel Log Manager não for configurado para a autenticação LDAP durante o processo de instalação, isso poderá ser configurado após a instalação, se necessário. Para configurar a autenticação LDAP após a instalação, consulte a seção "Autenticação LDAP" no *Sentinel Log Manager 1.2.2 Administration Guide (Guia de Administração do Sentinel Log Manager 1.2)*.

1. Faça o download e copie os arquivos de instalação no site de Download da Novell.
2. Efetue login como `root` no servidor em que você deseja instalar o Sentinel Log Manager.
3. Especifique o comando a seguir para extrair os arquivos de instalação do arquivo tar:

   ```
   tar xfz <install_filename>
   ```

   Substitua <*nome_arquivo_instalação*> pelo nome real do arquivo de instalação.
4. Altere para o diretório de onde o arquivo install foi extraído.
5. Especifique o comando a seguir para executar o script `install-slm` e instalar o Sentinel Log Manager:

   ```
   ./install-slm
   ```
6. Para prosseguir com o idioma de sua escolha, selecione o número especificado ao lado de cada idioma.

   O contrato de licença de usuário final será exibido no idioma selecionado.
7. 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.

   A instalação cria um grupo `novell` e um usuário `novell`, caso ainda não existam.
8. Quando solicitado, especifique a opção para continuar com a instalação personalizada.
9. Quando for solicitado que você especifique a opção da chave de licença, digite `2` para especificar a chave de licença do produto adquirido.
10. Especifique a chave de licença e pressione Enter.

    Para obter mais informações sobre chaves de licença, consulte a seção "Informações de licença" no *Guia de Administração do Sentinel Log Manager 1.2.2*.
11. Especifique a senha do usuário administrador.
12. Confirme a senha do usuário administrador.
13. Especifique a senha do administrador do banco de dados (dbauser).
14. Confirme a senha do administrador do banco de dados (dbauser).
15. Você pode configurar qualquer número de porta válido dentro da faixa especificada para os seguintes serviços:
    - Servidor Web
    - Serviço de Mensagens Java
    - Serviço Proxy do Cliente

- Serviço de Banco de Dados
- Gateway Interno do Agente

Se você deseja prosseguir com as portas padrão, digite a opção 6 e continue com a instalação personalizada.

16 Especifique a opção para autenticar usuários através de um diretório LDAP externo.

17 Especifique o endereço IP ou o nome de host do servidor LDAP.

O valor padrão é localhost. Porém, você não deve instalar o servidor LDAP na mesma máquina que o servidor do Sentinel Log Manager.

18 Selecione um dos seguintes tipos de conexão LDAP:

- **Conexão LDAP SSL/TSL:** Estabelece uma conexão segura entre o browser e o servidor para autenticação. Digite 1 para especificar esta opção.
- **Conexão LDAP não criptografada:** Estabelece uma conexão não criptografada. Digite 2 para especificar esta opção.

19 Especifique o número da porta do servidor LDAP. A porta SSL padrão é 636 e a porta não SSL padrão é 389.

20 (Condicional) Se você selecionou a conexão LDAP SSL/TSL, especifique se o certificado do servidor LDAP é assinado por um CA conhecido.

21 (Condicional) Se você especificou `n`, especifique o nome do arquivo do certificado do servidor LDAP.

22 Selecione se você deseja efetuar pesquisas anônimas no diretório LDAP:

- **Efetuar pesquisas anônimas no diretório LDAP:** O servidor do Sentinel Log Manager efetua uma *pesquisa anônima* no diretório LDAP com base no nome de usuário especificado para buscar o nome de usuário LDAP exclusivo (DN) correspondente. Digite 1 para especificar este método.
- **Não efetuar pesquisas anônimas no diretório LDAP:** Digite 2 para especificar esta opção.

23 (Condicional) Se você selecionou a pesquisa anônima, especifique o atributo de pesquisa e avance para a Etapa 26.

24 (Condicional) Se você não selecionou a pesquisa anônima na Etapa 22, especifique se o Microsoft Active Directory está sendo usado.

Para o Active Directory, o atributo `userPrincipalName`, cujo valor segue o formato `nomeUsuário@nomeDomínio`, pode ser usado opcionalmente para autenticar o usuário antes de pesquisar o objeto usuário LDAP, sem a necessidade de digitar o DN do usuário.

25 (Condicional) Se você deseja usar a abordagem acima no Active Directory, especifique o nome do domínio.

26 Especifique o DN Base.

27 Pressione s para especificar que as opções selecionadas estão corretas, caso contrário pressione n e mude a configuração.

28 Para efetuar login no servidor do Sentinel Log Manager, use o URL especificado na saída da instalação. O URL é similar a `https://10.0.0.1:8443/novelllogmanager`.

Para obter mais informações sobre login no servidor, consulte o Capítulo 6, “Efetuando login na interface na Web” na página 57.

29 Para configurar fontes de eventos para que enviem dados ao Sentinel Log Manager, consulte a seção “Configurando a coleta de dados” no *Sentinel Log Manager 1.2.2 Administration Guide (Guia de Administração do Sentinel Log Manager 1.2)*.

Observação: Quando o sistema é reiniciado pela primeira vez após a instalação, esse processo pode demorar aproximadamente cinco minutos até que você possa começar a usá-lo. Esse atraso ocorre somente quando você inicia o sistema pela primeira vez após a instalação ou uma atualização.

3.4 Instalação silenciosa

A instalação silenciosa ou autônoma do Sentinel Log Manager é útil se for necessário instalar mais de um servidor do Sentinel Log Manager na sua implantação. Em cenários como esse, você pode registrar os parâmetros durante a primeira instalação e depois executar o arquivo registrado nos outros servidores.

1. Faça o download e copie os arquivos de instalação no site de Download da Novell.
2. Efetue login como `root` no servidor em que você deseja instalar o Sentinel Log Manager.
3. Especifique o comando a seguir para extrair os arquivos de instalação do arquivo tar:

   ```
   tar xfz <install_filename>
   ```

   Substitua *<nome_arquivo_instalação>* pelo nome real do arquivo de instalação.
4. Altere para o diretório de onde o arquivo install foi extraído.
5. Especifique o comando a seguir para executar o script `install-slm` e instalar o Sentinel Log Manager no modo silencioso:

   ```
   ./install-slm -u responseFile
   ```

   Para obter informações sobre a criação do arquivo de resposta, consulte a Seção 3.2, “Instalação padrão” na página 32. A instalação prossegue com os valores armazenados no arquivo de resposta.
6. Para efetuar login no servidor do Sentinel Log Manager, use o URL especificado na saída da instalação. O URL é similar a `https://10.0.0.1:8443/novelllogmanager`.

   Para obter mais informações sobre login no servidor, consulte o Capítulo 6, “Efetuando login na interface na Web” na página 57.
7. Para configurar fontes de eventos para que enviem dados ao Sentinel Log Manager, consulte a seção “Configurando a coleta de dados” no “Sentinel Log Manager 1.2.2 Administration Guide (Guia de Administração do Sentinel Log Manager 1.2)”.

Observação: Quando o sistema é reiniciado pela primeira vez após a instalação, esse processo pode demorar aproximadamente cinco minutos até que você possa começar a usá-lo. Esse atraso ocorre somente quando você inicia o sistema pela primeira vez após a instalação ou uma atualização.

3.5 Instalação não root

Se a sua política organizacional não permitir que você execute a instalação completa do Sentinel Log Manager como `root`, a maioria das etapas da instalação pode ser executada como usuário não root (`novell`).

1. Faça o download e copie os arquivos de instalação no site de Download da Novell.
2. Especifique o comando a seguir para extrair os arquivos de instalação do arquivo tar:

   ```
   tar xfz <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 Log Manager como `root`.

4 Altere para o diretório de onde o arquivo install foi extraído.

5 Especifique o seguinte comando:

```
./bin/root_install_prepare
```

Uma lista de comandos a serem executados com privilégios de root será exibida.

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

6 Aceite a lista de comandos.

Os comandos exibidos serão executados.

7 Especifique o comando a seguir para mudar o usuário não root (`novell`) recém-criado:

```
su novell
```

8 Especifique o seguinte comando:

```
./install-slm
```

9 Para prosseguir com o idioma de sua escolha, selecione o número especificado ao lado de cada idioma.

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 continuar com a instalação padrão, continue com a Etapa 8 em Seção 3.2, "Instalação padrão" na página 32.
- Se você escolher continuar com a instalação atual, continue com a Etapa 8 em Seção 3.3, "Instalação personalizada" na página 34.

A instalação do Sentinel Log Manager é concluída e o servidor é iniciado.

12 Especifique o comando a seguir para mudar para o usuário `root`:

```
su root
```

13 Especifique o comando a seguir para finalizar a instalação:

```
./bin/root_install_finish
```

14 Para efetuar login no servidor do Sentinel Log Manager, use o URL especificado na saída da instalação. O URL é similar a `https://10.0.0.1:8443/novelllogmanager`.

Para obter mais informações sobre login no servidor, consulte o Capítulo 6, "Efetuando login na interface na Web" na página 57.

Observação: Quando você iniciar o sistema pela primeira vez após a instalação, pode demorar aproximadamente cinco minutos para que o sistema seja inicializado para que você possa começar a usá-lo. Esse atraso ocorre somente quando você inicia o sistema pela primeira vez após a instalação ou uma atualização.

---

4 Instalando a aplicação

O Sentinel Log Manager Appliance é uma aplicação de software pronta para ser executada e construída no SUSE Studio que combina um sistema operacional SUSE Linux Enterprise Server (SLES) 11 SP1 fortificado e o serviço de atualização integrado do Novell Sentinel Log Manager para oferecer uma experiência simples e uniforme ao usuário e também permitir que os clientes aproveitem seus investimentos existentes. A aplicação de software pode ser instalada tanto em hardware quanto num ambiente virtual.

4.1 Antes de começar

- Certifique-se de que os requisitos de hardware são atendidos. Para obter mais informações, consulte a Seção 2.1, “Requisitos de hardware” na página 17.
- Obtenha sua chave de licença com o Atendimento ao Cliente Novell (http://www.novell.com/center) para instalar a versão licenciada.
- Obtenha seu código de registro com o Atendimento ao Cliente Novell (http://www.novell.com/center) para se registrar e receber atualizações de software.
- Sincronize o horário usando o protocolo NTP (Network Time Protocol).
- (Condicional) Se você planeja usar o VMware, certifique-se de que você tem o VMware Converter para fazer upload da imagem para o servidor VMware ESX e simultaneamente convertê-la para um formato que pode ser executado no servidor ESX.

4.2 Portas usadas

Observe que a aplicação do Novell Sentinel Log Manager usa as seguintes portas para comunicação, e algumas delas são abertas no firewall:

4.2.1 Portas abertas no firewall

Tabela 4-1 *Portas de rede usadas pelo Sentinel Log Manager*

Portas	Descrição
TCP 1289	Usada para conexões do Novell Audit.
TCP 289	Encaminhada para 1289 para conexões do Novell Audit.
TCP 22	Usada para fornecer acesso seguro ao shell para a aplicação do Sentinel Log Manager.
UDP 1514	Usada para mensagens syslog.
UDP 514	Encaminhada para 1514 para mensagens syslog.
TCP 8080	Usada para comunicação HTTP.
TCP 80	Encaminhada para 8080 para comunicação HTTP do Servidor Web do Sentinel Log Manager.
TCP 8443	Usada para comunicação HTTPS.
TCP 1443	Usada para mensagens syslog criptografas por SSL.
TCP 443	Encaminhada para 8443 para comunicação HTTPS do Servidor Web do Sentinel Log Manager. Também usada pelo serviço de atualização do Sentinel Log Manager Appliance.
TCP 61616	Usada para comunicação entre os Gerenciadores de Coletor e o servidor.
TCP 10013	Usada pelo Proxy SSL da interface de Gerenciamento de Fonte de Eventos.
TCP 54984	Usada pelo Console de Gerenciamento da aplicação do Sentinel Log Manager (WebYaST).
TCP 1468	Usada para mensagens syslog.

4.2.2 Portas usadas localmente

Tabela 4-2 *Portas usadas para comunicação local*

Portas	Descrição
TCP 61617	Usada para comunicação interna entre o Servidor Web e o servidor.
TCP 5556	Usada para comunicação interna na interface de loopback, com o servidor_gateway_interno e o gateway_interno. É usada para comunicação entre o mecanismo do agente e o Gerenciador de Coletor.

Portas	Descrição
TCP 5432	Usada pelo banco de dados PostgreSQL. Esta porta não precisa ser aberta por padrão. Porém, se você estiver desenvolvendo relatórios usando o SDK do Sentinel, então a porta deve ser aberta. Para obter mais informações, consulte o site do SDK de Plug-ins do Sentinel (http://developer.novell.com/wiki/index.php?title=Develop_to_Sentinel).
Duas portas TCP adicionais selecionadas aleatoriamente	Usadas para comunicação interna entre o mecanismo do agente e o Gerenciador de Coletor.
TCP 8005	Usada para comunicação interna com os processos Tomcat.
TCP 32000	Usadas para comunicação interna entre o mecanismo do agente e o Gerenciador de Coletor.

4.3 Instalando a aplicação VMware

Para executar a imagem da aplicação a partir do servidor VMware ESX, importe e instale a imagem da aplicação no servidor.

1. Faça o download do arquivo de instalação da aplicação VMware.

   O arquivo correto da aplicação VMware possui `vmx` em seu nome. Por exemplo,`<sentinel_log_manager_vmx.tar.gz>`

2. Especifique o comando a seguir 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.

3. Para importar a imagem VMware no servidor ESX, use o VMware Converter e siga as instruções na tela do assistente de instalação.
4. Efetue login na máquina do servidor ESX.
5. Selecione a imagem VMware importada da aplicação e clique no ícone *Ligar*.
6. Selecione o idioma desejado e clique em *Avançar*.
7. Selecione o layout do teclado e clique em *Avançar*.
8. Leia e aceite o Contrato de Licença do Software Novell SUSE Enterprise Server.
9. Leia e aceite o Contrato de Licença do Usuário Final do Novell Sentinel Log Manager.
10. 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 *Assign Hostname to Loopback IP* (Atribuir nome de host a IP de loopback) esteja selecionada.
11. Selecione *Avançar*. As configurações do nome de host são gravadas.

12 Siga um destes procedimentos:

- Para usar as configurações de conexão da rede atuais, selecione *Usar a seguinte configuração* na tela Configuração de Rede .
- Para mudar as configurações de conexão da rede, clique em *Mudar*.

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

Observação: 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` do Novell SUSE Enterprise Server e clique em *Avançar*.

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

16 Defina a senha admin e a senha dbauser do Sentinel Log Manager e clique em *Avançar*.

17 Selecione *Avançar*.

A instalação prossegue e termina. Anote o endereço IP da aplicação, exibido no console.

18 Avance para a Seção 4.6, "Configuração pós-instalação para a aplicação" na página 45.

Observação: Quando você iniciar o sistema pela primeira vez após a instalação, pode demorar aproximadamente cinco minutos para que o sistema seja inicializado para que você possa começar a usá-lo. Esse atraso ocorre somente quando você inicia o sistema pela primeira vez após a instalação ou uma atualização.

4.4 Instalando a aplicação Xen

1 Faça o download e copie o arquivo de instalação da aplicação virtual Xen em `/var/lib/xen/images`.

O nome correto do arquivo da aplicação virtual Xen contém `xen`. Por exemplo, *<sentinel_log_manager_xen.tar.gz>*

2 Especifique o comando a seguir para descompactar o arquivo:

```
tar -xvzf <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` arquivo de imagem
- *<nome_arquivo>*`.xenconfig` arquivo

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 `nome` e `memória`.

Por exemplo:

```
# -*- mode: python; -*-
name="Sentinel_Log_Manager_1.2.0.0_64"
memory=4096
disk=[ "tap:aio:/var/lib/xen/images/Sentinel_Log_Manager_1.2.0.0_64_Xen-
0.777.0/Sentinel_Log_Manager_1.2.0.0_64_Xen.x86_64-0.777.0.raw,xvda,w" ]
vif=[ "bridge=br0" ]
```

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

```
xm create <nome_arquivo>.xenconfig
```

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

xm list

A MV aparece na lista.

Por exemplo, se você configurou `name="Sentinel_Log_Manager_1.2.0.0_64"` no arquivo `.xenconfig`, a VM aparecerá com este nome.

8 Para iniciar a instalação, especifique este comando:

```
xm console <nome_mv>
```

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_Log_Manager_1.2.0.0_64
```

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 Novell SUSE Enterprise Server.

12 Leia e aceite o Contrato de Licença do Usuário Final do Novell Sentinel Log Manager.

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 *Assign Hostname to Loopback IP* (Atribuir nome de host a 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 .
- Para mudar as configurações de conexão da rede, clique em *Mudar*.

16 Defina a data e o horário, clique em *Avançar* e depois em *Concluir*.

Observação: 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
```

---

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

18 Defina a senha admin e a senha dbauser do Sentinel Log Manager e clique em *Avançar*.

A instalação prossegue e termina. Anote o endereço IP da aplicação, exibido no console.

19 Avance para a Seção 4.6, “Configuração pós-instalação para a aplicação” na página 45.

Observação: Quando você iniciar o sistema pela primeira vez após a instalação, pode demorar aproximadamente cinco minutos para que o sistema seja inicializado para que você possa começar a usá-lo. Esse atraso ocorre somente quando você inicia o sistema pela primeira vez após a instalação ou uma atualização.

4.5 Instalando a aplicação em hardware

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.

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.
4. Leia e aceite o Contrato de Licença do Software Novell SUSE Enterprise Server.
5. Leia e aceite o Contrato de Licença do Usuário Final do Novell Sentinel Log Manager.
6. Selecione *Avançar*.
7. 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 *Assign Hostname to Loopback IP* (Atribuir nome de host a IP de loopback) esteja selecionada.
8. Selecione *Avançar*. As configurações de nome de host são gravadas.
9. Siga um destes procedimentos:
   - Para usar as configurações de conexão da rede atuais, selecione *Usar a seguinte configuração* na tela Configuração de Rede
   - Para mudar as configurações de conexão da rede, clique em *Mudar*.
10. Selecione *Avançar*. As configurações de conexão da rede serão gravadas.
11. Defina a data e o horário e clique em *Avançar*.

    Observação: 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
    ```
12. Defina a senha `root` e clique em *Avançar*.
13. Defina a senha admin e a senha dbauser do Sentinel Log Manager e clique em *Avançar*.
14. 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 `senha`.
15. Redefina as configurações do terminal:

    ```
    reset
    ```
16. Para instalar a aplicação no servidor físico, execute este comando:

    ```
    /sbin/yast2 live-installer
    ```

A instalação prossegue e termina. Anote o endereço IP da aplicação, exibido no console.

17 Avance para a Seção 4.6, “Configuração pós-instalação para a aplicação” na página 45.

Observação: Quando você iniciar o sistema pela primeira vez após a instalação, pode demorar aproximadamente cinco minutos para que o sistema seja inicializado para que você possa começar a usá-lo. Esse atraso ocorre somente quando você inicia o sistema pela primeira vez após a instalação ou uma atualização.

4.6 Configuração pós-instalação para a aplicação

4.6.1 Instalando o VMware Tools

Para que o Sentinel Log Manager 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).

4.6.2 Efetuando login na interface da Web da aplicação

Para efetuar login no console da Web da aplicação e inicializar o software:

1 Abra um browser da Web e acesse https://*<endereço IP>*:*8443*. A página do Sentinel Log Manager é exibida.

   O endereço IP da aplicação é exibido no console da aplicação após o término da instalação e o reinício do servidor.

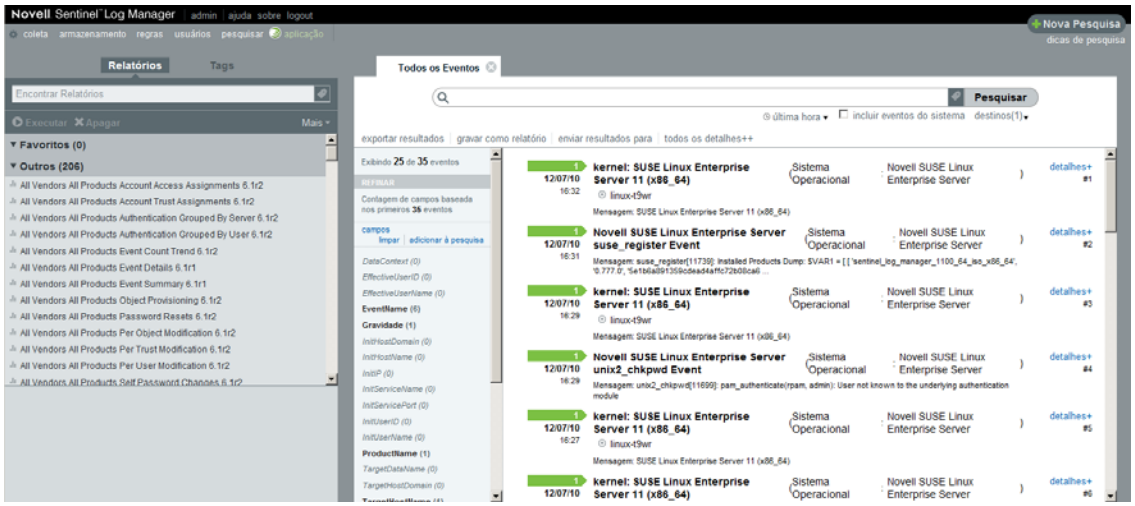
2 A aplicação do Sentinel Log Manager pode ser configurada para armazenar e coletar dados. Para obter mais informações, consulte o *Guia de Administração do Sentinel Log Manager 1.2.2*.

3 Para se registrar e receber atualizações, consulte a Seção 4.10, “Registrando para receber atualizações” na página 49.

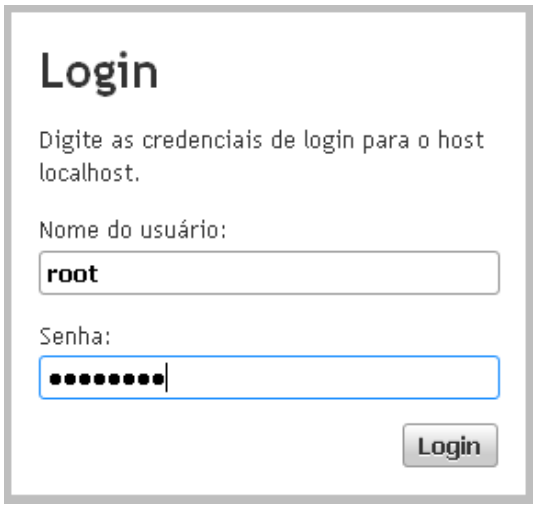
4.7 Configuração do WebYaST

A interface da aplicação do Novell Sentinel Log Manager é equipada com WebYaST. WebYaST é um console remoto baseado na Web para controlar aplicações baseadas em SUSE Linux Enterprise. Você pode acessar, configurar e monitorar as aplicações do Sentinel Log Manager 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 Log Manager.



2 Clique em *Aplicação*.



3 Configure o Servidor do Sentinel Log Manager para receber atualizações, conforme descrito na Seção 4.10, “Registrando para receber atualizações” na página 49.

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

4.8 Configurando a aplicação com SMT

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

4.8.1 Pré-requisitos

- Obtenha as credenciais do Novell Customer Center para Sentinel Log Manager para obter atualizações da Novell. Para obter informações sobre como obter as credenciais, contate Suporte da Novell (http://support.novell.com/phone.html?sourceidint=suplnav4_phonesup).
- Certifique-se de que o SLES 11 SP1 esteja instalado com os seguintes pacotes na máquina onde você deseja instalar a SMT:
  - htmldoc
  - smt
  - perl-DBIx-Transaction
  - perl-File-Basename-Object
  - pertl-DBIx-Migration-Director
  - perl-MIME-Lite
  - perl-Text-ASCIITable
  - smt-support
  - yast2-smt
  - yum-metadata-parser
  - createrepo
  - sle-smt-release-cd
  - sle-smt_en
  - 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 (http://www.novell.com/documentation/smt11/):
  - Instalação da SMT
  - Configuração do servidor da SMT
  - Espelhamento de instalação e atualização de repositórios com a SMT
- Instale o utilitário `wget` na máquina de aplicação.

4.8.2 Configurando a aplicação

Para obter mais informações sobre a aplicação com a SMT, consulte "Configurando clientes para usar a SMT" (http://www.novell.com/documentation/smt11/smt_sle_11_guide/?page=/documentation/smt11/smt_sle_11_guide/data/smt_client.html) na documentação da *Subscription Management Tool*.

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

- **Imagem de aplicação VMWare:**

  ```
  smt-repos -p sentinel_log_manager_1100_64_vmx_x86_64
  ```

- **Imagem de aplicação Xen:**

  ```
  smt-repos -p sentinel_log_manager_1100_64_xen_x86_64
  ```

- **ISO:**

  ```
  smt-repos -p sentinel_log_manager_1100_64_xen_x86_64
  ```

4.8.3 Atualizando a aplicação

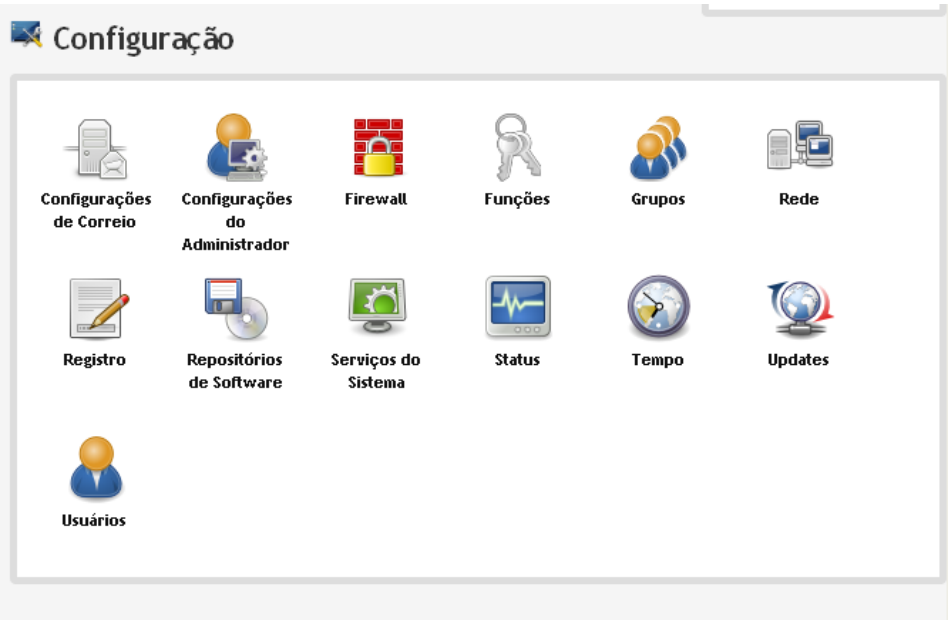
Para obter informações sobre como atualizar o aplicativo, consulte Seção 5.4.3, "Atualizando o aplicativo usando SMT" na página 56.

4.9 Parando e iniciando a aplicação com a IU da Web

É possível iniciar e parar o servidor Sentinel Log Manager usando a IU da Web da seguinte forma:

1. Efetue login na aplicação do Sentinel Log Manager.

   A interface do Sentinel Log Manager na Web é exibida.
2. Clique em *Aplicação* para iniciar o WebYaST.



3. Clique em *System Services* (Serviços de sistema).

4 Para parar o servidor Sentinel Log Manager, clique em *parar*.

5 Para iniciar o servidor Sentinel Log Manager, clique em *iniciar*.

4.10 Registrando para receber atualizações

1 Efetue login na aplicação do Sentinel Log Manager.

A IU da Web do Sentinel Log Manager é exibida.

2 Clique em *Aplicação* para iniciar o WebYaST.

3 Clique em *Registro*.

4. Especifique a ID de email no qual deseja receber atualizações, o nome do sistema e o código de registro do appliance.
5. Clique em *Gravar*.

Para obter informações sobre como atualizar o aplicativo, consulte Seção 5.4, “Atualizando a aplicação” na página 54.

5 Fazendo upgrade do Sentinel Log Manager

Você pode instalar o Sentinel Log Manager 1.2.0.2 nas versões Sentinel Log Manager 1.2 e posterior. Se você desejar fazer upgrade do Sentinel Log Manager versões 1.1*x*, primeiro faça upgrade para o Sentinel Log Manager 1.2.0.1 e, em seguida, instale o Sentinel Log Manager 1.2.0.2.

Observação: Após a atualização, quaisquer personalizações do Coletor realizadas usando o Modo de Execução Personalizada e método de arquivo auxiliar recomendados na documentação do SDK serão preservadas.

5.1 Pré-requisitos

- O Sentinel Log Manager 1.2 e versão posterior requer a plataforma SUSE Linux Enterprise Server (SLES) 11 SP1. Se você estiver atualizando para o Sentinel Log Manager 1.2 ou para uma versão posterior, você deverá garantir que o sistema opreacional seja atualizado para SLES 11 SP1.
- Para que o Sentinel Log Manager 1.2 e versão posterior funcione com êxito no SLES 11 SP1, a versão seguinte ou posterior de RPMs deve ser instalada:
  - **Patches kernel:**
    - `kernel-default-2.6.32.29-0.3.1.x86_64.rpm`
    - `kernel-default-base-2.6.32.29-0.3.1.x86_64.rpm`
  - **RPMs util Linux:**
    - `libblkid1-2.16-6.11.1.x86_64.rpm`
    - `libuuid1-2.16-6.11.1.x86_64.rpm`
    - `util-linux-2.16-6.11.1.x86_64.rpm`
    - `util-linux-lang-2.16-6.11.1.x86_64.rpm`
    - `uuid-runtime-2.16-6.11.1.x86_64.rpm`

  O Sentinel Log Manager 1.1.0.*x* usa o squashfs versão 3.4-35.1; no entanto, o SLES 11 SP.1 é compatível com o squashfs 4.0 e versão posterior, que não é compatível com versões anteriores e não pode abrir um sistema de arquivos do squashfs criado com versões anteriores do squashfs. Instalar esses RPMs resolve o problema de incompatibilidade entre as versões squashfs do Sentinel Log Manager 1.1.0.*x* e SLES 11 SP1.

Esses RPMs estão disponíveis através do canal de atualização on-line do SLES 11. Para obter mais informações sobre como atualizar o sistema SLES, consulte "Atualização on-line do YaST" (http://www.novell.com/documentation/sles11/book_sle_admin/?page=/documentation/sles11/book_sle_admin/data/cha_onlineupdate_you.html) no *Guia de administração do SLES 11 SP1 (http://www.novell.com/documentation/sles11/book_sle_admin/data/book_sle_admin_pre.html)*.

Observação: A instalação não prosseguirá a menos que os patches kernel e os RPMs util Linux mencionados acima estejam instalados.

- Se você desejar fazer upgrade do Sentinel Log Manager versões 1.1*x*, primeiro faça upgrade para o Sentinel Log Manager 1.2.0.1 e, em seguida, instale o Sentinel Log Manager 1.2.0.2.
- Certifique-se de que os links simbólicos não tenham sido usados para as seguintes pastas e subpastas:
  - `opt/novell` (Pasta base)
  - `etc/opt/novell` (Pasta de configuração)
  - `var/opt/novell` (Pasta de dados)

  Se links simbólicos tiverem sido usados, remova-os; ou seja, mova esses diretórios de volta para os diretórios de instalação padrão.

5.2 Atualizando o Sentinel Log Manager Server

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

   Para obter mais informações sobre o backup de dados, consulte a seção "Backup e restauração de dados."
2. Faça download do patch mais recente no site de download da Novell (http://download.novell.com).
3. (Condicional) Se você desejar fazer upgrade para o Sentinel Log Manager Hotfix 1, faça download do patch no site localizador de patches da Novell (http://download.novell.com/patch/finder/).
4. Efetue login como `root` no servidor em que você deseja instalar o Sentinel Log Manager.
5. Especifique o comando a seguir para interromper o servidor do Sentinel do Log Manager:

   `<install_directory>/bin/server.sh stop`

   Por exemplo, `/opt/novell/sentinel_log_mgr/bin # ./server.sh stop`.
6. 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.
7. Altere para o diretório de onde o arquivo install foi extraído.
8. Especifique o comando a seguir para executar o script `install-slm` e fazer upgrade do Sentinel Log Manager:

   `./install-slm`
9. 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.
10. Leia a licença do usuário final e digite `sim` ou `s` para aceitar a licença e continuar com a instalação.

11 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. Se você pressionar n, a instalação será encerrada. 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.

Se você estiver atualizando um sistema Sentinel Log Manager 1.1 que foi atualizado do Sentinel Log Manager 1.0, a atual instalação do Sentinel Log Manager 1.0 será mantida intacta, com as seguintes exceções:

- Se o diretório de dados da versão 1.0 (por exemplo, `/opt/novell/sentinel_log_manager_1.0_x86-64/data`) e o diretório de dados da versão 1.1 (por exemplo, `/var/opt/novell/sentinel_log_mgr/data`) estiverem no mesmo sistema de arquivos, então os subdiretórios `<1.0>/data/eventdata` e `<1.0>/data/rawdata` serão movidos para o local da versão 1.1 porque os diretórios de dados de eventos e de dados iniciais geralmente são grandes. Se os diretórios de dados das versões 1.0 e 1.1 estiverem em sistemas de arquivos diferentes, então os subdiretórios de dados de eventos e de dados iniciais serão copiados para o local da versão 1.1 e os arquivos da versão 1.0 serão deixados intactos.
- Se o diretório de dados existente da versão 1.0 (por exemplo, `/opt/novell/sentinel_log_mgr_1.0_x86-64`) estiver em um sistema de arquivos montado separadamente e não houver espaço suficiente no sistema de arquivos que contém o diretório de dados da versão 1.1 (`/var/opt/novell/sentinel_log_mgr/data`), então você pode permitir que o instalador remonte o sistema de arquivos, do local da versão 1.0 para o local da versão 1.1. Todas as entradas em `/etc/fstab` também serão atualizadas. Se você não permitir que o instalador remonte o sistema de arquivos existente, o upgrade será encerrado. Você pode, então, criar espaço suficiente no sistema de arquivos para o diretório de dados da versão 1.1.

Depois que a instalação do Sentinel Log Manager 1.2.0.2 tiver sido realizada com êxito e o servidor estiver funcional, você deverá especificar o comando a seguir para remover manualmente o diretório do Sentinel Log Manager 1.0:

```
rm -rf /opt/novell/slm_1.0_install_directory
```

Por exemplo:

```
rm -rf /opt/novell/sentinel_log_mgr_x86-64
```

A remoção do diretório de instalação apaga permanentemente a instalação do Sentinel Log Manager 1.0.

12 Especifique o comando a seguir para iniciar o servidor do Sentinel do Log Manager:

```
<install_directory>/bin/server.sh start
```

13 Certifique-se de que todos os Gerenciadores de Coletor sejam atualizados para uma versão compatível com o servidor Sentinel Log Manager atualizado.

Para obter mais informações sobre a atualização de Gerenciadores de Coletor, consulte Seção 5.3, “Fazendo upgrade do Gerenciador de Coletor” na página 54.

Observação: Quando o sistema for iniciado pela primeira vez após o upgrade, um tempo de aproximadamente cinco minutos poderá ser necessário para que o sistema inicialize e fique pronto para ser usado. Esse atraso ocorre somente quando você inicia o sistema pela primeira vez após a instalação ou uma atualização.

5.3 Fazendo upgrade do Gerenciador de Coletor

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

   Para obter mais informações, consulte a seção "Backup e restauração de dados" no *Sentinel Log Manager 1.2.2 Administration Guide (Guia de Administração do Sentinel Log Manager 1.2)*.
2. Efetue login no Sentinel Log Manager como administrador.
3. Selecione *coleta* > *Avançado*.

   Nesta página, você pode fazer download do instalador de atualização mais recente para o Gerenciador de Coletor que seja compátivel com o Sentinel Log Manager.
4. Clique no link *Download do Instalador* na seção Instalador de Atualização do Gerenciador do Coletor.

   Uma janela é exibida com opções para abrir ou gravar o arquivo `scm_upgrade_installer.zip` na máquina local.
5. Grave o arquivo.
6. Copie o arquivo para um local temporário.
7. Extraia o conteúdo do arquivo `.zip`.
8. Execute um dos seguintes scripts:
   - Para fazer upgrade do Gerenciador de Coletor para Windows, execute `service_pack.bat`.
   - Para fazer upgrade do Gerenciador de Coletor para Linux, execute `service_pack.sh`.
9. Siga as instruções na tela para completar a instalação.

5.4 Atualizando a aplicação

Você pode atualizar o aplicativo Sentinel Log Manager usando o WebYaST ou o using SMT.

- Seção 5.4.1, "Fazendo upgrade da aplicação pelo WebYast" na página 54
- Seção 5.4.2, "Fazendo upgrade da aplicação usando zypper" na página 55
- Seção 5.4.3, "Atualizando o aplicativo usando SMT" na página 56

5.4.1 Fazendo upgrade da aplicação pelo WebYast

Observação: Se você estiver fazendo upgrade de uma aplicação Sentinel Log Manager instalada em um sistema operacional anterior ao SLES 11 SP3, será necessário fazer upgrade da aplicação usando o utilitário de linha de comando zypper, uma vez que a interação com o usuário é necessária para concluir o upgrade. O WebYast não pode promover a interação necessária com o usuário. Para obter mais informações sobre como usar o zypper para fazer upgrade da aplicação, consulte Seção 5.4.2, "Fazendo upgrade da aplicação usando zypper" na página 55

1. Especifique o URL do Sentinel Log Manager usando a porta 4984 para iniciar o WebYaST.
2. Faça login no WebYast usando as credenciais da aplicação.
3. Faça um backup de sua configuração e crie uma exportação de ESM.

   Para obter mais informações sobre o backup de dados, consulte a seção "Backup e restauração de dados."
4. (Condicional) Se você ainda não tiver registrado o aplicativo para atualizações automáticas, registre-o.

Para obter mais informações, consulte a Seção 4.10, “Registrando para receber atualizações” na página 49.

Se a aplicação não estiver registrada, um aviso amarelo será exibido no WebYast, indicando que a aplicação não está registrada.

5 Para verificar se existem atualizações disponíveis, clique em *Atualizações*.

As atualizações disponíveis serão exibidas.

6 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 Log Manager. Você deve reiniciar manualmente esse serviço depois que a atualização for concluída.

7 Reinicie o servidor Sentinel Log Manager usando a IU da Web.

Para obter mais informações, consulte a Seção 4.9, “Parando e iniciando a aplicação com a IU da Web” na página 48.

5.4.2 Fazendo upgrade da aplicação usando zypper

Para fazer upgrade da aplicação usando o patch zypper:

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

Para obter mais informações sobre o backup de dados, consulte a seção “Backup e restauração de dados.”

2 (Condicional) Se você ainda não tiver registrado o aplicativo para atualizações automáticas, registre-o.

Para obter mais informações, consulte a Seção 4.10, “Registrando para receber atualizações” na página 49.

Se a aplicação não estiver registrada, um aviso amarelo será exibido no WebYast, indicando que a aplicação não está registrada.

3 Faça login no console de aplicativo como o usuário `root`.

4 Execute o seguinte comando:

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

5 (Condicional) Se você estiver fazendo upgrade de um Sentinel Log Manager anterior à versão 1.2, será exibida uma mensagem, indicando um conflito de versões do squashfs. Insira `1` para atualizar a versão 4.0-1.2.10 do squashfs e para aceitar a alteração do fornecedor.

As versões 1.1. do Sentinel Log Manager usam a versão 3.4 do squashfs, mas o Sentinel Log Manager 1.2 e versão posterior usam a versão 4.0 do squashfs. Além disso, o fornecedor para instalador yast2-live-installer do squashfs foi alterado de OpenSUSE para SLES. Para continuar com a atualização, primeiro atualize o squashfs e aceite a alteração de fornecedor.

6 Digite `Y` (S) para continuar.

7 (Condicional) Se você estiver fazendo upgrade do Sentinel Log Manager anterior à versão 1.2, será exibido o contrato de licença por usuário final do Sentinel Log Manager. Insira `sim` para aceitar a licença.

O contrato de licença do Sentinel Log Manager 1.2 e versão posterior é diferente do contrato de licença do Sentinel Log Manager 1.1. Você deve aceitar o novo contrato de licença para fazer upgrade do Sentinel Log Manager 1.1 e versão posterior para 1.2 e versão posterior.

8 (Condicional) Se você estiver fazendo upgrade de uma aplicação Sentinel Log Manager instalada em um sistema operacional anterior ao SLES 11 SP3, será exibido o contrato de licença por usuário final. Insira `sim` para aceitar a licença.

   O aplicativo Sentinel Log Manager foi atualizado com êxito.

9 (Condicional) Se você estiver fazendo upgrade de um Sentinel Log Manager anterior à versão 1.2, será exibido um aviso de descontinuação após a conclusão do upgrade.

   Isso é porque o Sentinel Log Manager 1.2.0.1 usa WebYaST 1.1, mas as versões 1.1 do Sentinel Log Manager usam o WebYaST 1.0. Durante a atualização, o módulo de idiomas do WebYaST 1.0 é depreciado no WebYaST 1.1. No entanto, esse aviso não afeta a atualização.

10 Reinicie o aplicativo Sentinel Log Manager.

5.4.3 Atualizando o aplicativo usando SMT

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

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

   Para obter mais informações, consulte Seção 4.8, “Configurando a aplicação com SMT” na página 46.

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_ipaddress>:SLM-1.1.0.0-ISO
```

7 Atualize o aplicativo:

```
zypper up -t patch -r SMT-http_<smt_server_ipaddress>:SLM-1.1.0.0-ISO
```

8 Reinicie o aplicativo.

```
rcsentinel_log_mgr restart
```

5.5 Fazendo upgrade de plug-ins do Sentinel

Os plug-ins do Sentinel novos e atualizados são frequentemente carregados no site de plug-ins do Sentinel (http://support.novell.com/products/sentinel/secure/sentinelplugins.html). Para obter as correções de bug, atualizações de documentação e melhorias mais recentes para um plug-in, faça download da versão mais recente do plug-in. Para obter informações sobre como instalar ou atualizar um plug-in, consulte a documentação específica do plug-in.

6 Efetuando login na interface na Web

O usuário administrador criado durante a instalação pode efetuar login na interface na Web para configurar e usar o Sentinel Log Manager:

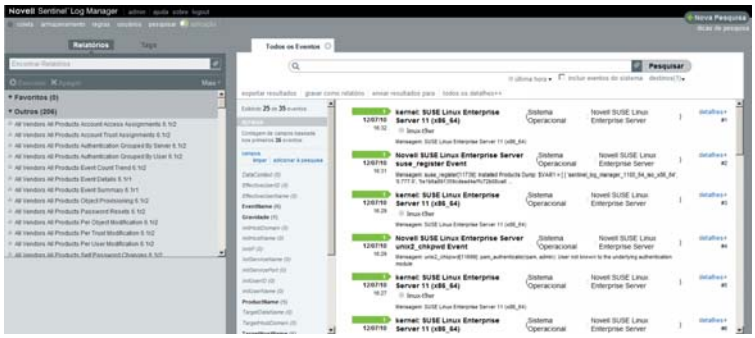
1. Abra um browser da Web suportado. Para obter mais informações, consulte a Seção 2.3, “Browsers suportados” na página 22.
2. Especifique o URL da página do Novell Sentinel Log Manager (por exemplo, `https://10.0.0.1:8443/novelllogmanager`) e pressione Enter.
3. (Condicional) Na primeira vez que você efetuar login no Sentinel Log Manager, será solicitado que você aceite um certificado. A página de login do Sentinel Log Manager é exibida quando você aceita o certificado.

4. Especifique o nome de usuário e a senha do administrador do Sentinel Log Manager.
5. Selecione o idioma para a interface do Sentinel Log Manager.

A interface do usuário do Sentinel Log Manager está disponível em inglês, português, francês, italiano, alemão, espanhol, japonês, chinês tradicional ou chinês simplificado.

6 Clique em *Entrar*.

A interface do Novell Sentinel Log Manager na Web é exibida.



7 Instalação de Gerenciadores de Coletor adicionais

Os Gerenciadores de Coletor gerenciam toda a coleta e análise de dados no Novell Sentinel Log Manager. O processo de instalação do Sentinel Log Manager instala um Gerenciador de Coletor por padrão no servidor do Sentinel Log Manager. Porém, é possível instalar diversos Gerenciadores de Coletor em configurações distribuídas.

7.1 Antes de começar

- Certifique-se de que o hardware e o software atendem aos requisitos mínimos mencionados no Capítulo 2, “Requisitos do sistema” na página 17.
- 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 Log Manager. Antes de iniciar a instalação do Gerenciador de Coletor, certifique-se de que todas as configurações do firewall e outras configurações de rede podem se comunicar através dessa porta.
- Para instalar o Collector Manager no RHEL 6, o script e pacotes a seguir devem ser instalados:
  - Instale o script ksh:

    ```
    install ksh-20100621-2.el6.x86_64
    ```

  - Para executar o instalador no modo de console, os seguintes pacotes devem ser instalados:
    - glibc-2.12-1.7.el6.i686
    - nss-softokn-freebl-3.12.7-1.1.el6.i686
  - Para executar o instalador no modo GUI, os seguintes pacotes devem ser instalados:
    - glibc-2.12-1.7.el6.i686
    - libX11-1.3-2.el6.i686
    - libXau-1.0.5-1.el6.i686
    - libxcb-1.5-1.el6.i686
    - libXext-1.1-3.el6.i686
    - libXi-1.3-3.el6.i686
    - libXtst-1.0.99.2-3.el6.i686
    - nss-softokn-freebl-3.12.7-1.1.el6.i686

7.2 Vantagens de Gerenciadores de Coletor adicionais

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

- **Melhor desempenho do sistema:** Os Gerenciadores de Coletor podem analisar e processar dados de eventos em um ambiente distribuído, o que melhora 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.
- **Coleta de dados em sistemas operacionais adicionais:** Por exemplo, você pode instalar um Gerenciador de Coletor no Microsoft Windows para habilitar a coleta de dados através do protocolo WMI.
- **Cache de arquivos:** O Gerenciador de Coletor remoto pode 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.

7.3 Instalação de Gerenciadores de Coletor adicionais

1. Efetue login no Sentinel Log Manager como administrador.
2. Selecione *coleta* > *Avançado*.
3. Clique no link *Download do Instalador* na seção do instalador do Gerenciador de Coletor.

   Uma janela é exibida com opções para abrir ou gravar o arquivo `scm_installer.zip` na máquina local. Grave o arquivo.
4. Copie e extraia o arquivo no local onde você deseja instalar o Gerenciador de Coletor.
5. Execute um dos arquivos de instalação a seguir, dependendo do seu software operacional:
   - Para instalar o Gerenciador de Coletor em um sistema Windows, execute `setup.bat`.
   - Para instalar o Gerenciador de Coletor em um sistema Linux, execute `setup.sh`.
6. Selecione um idioma e clique em *OK*.

   O assistente de instalação é exibido.
7. Clique em OK.
8. Leia e aceite o contrato de licença e clique em *Avançar*.
9. Você pode prosseguir com o diretório de instalação padrão ou procurar e selecionar o diretório; depois clique em *Avançar*.
10. Mantenha a porta de barramento de mensagens padrão (61616) inalterada e especifique o endereço IP/nome do host do servidor Sentinel Log Manager.
11. Clique em *Avançar* para prosseguir com Configuração Automática de Memória padrão (256 Megabytes).

    É exibido um resumo da instalação.
12. Clique em *Instalar*.
13. Especifique o nome do usuário e a senha para o Gerenciador de Coletor.

    O nome de usuário e a senha são armazenados no arquivo `/etc/opt/novell/sentinel_log_mgr/config/activemqusers.properties`, localizado no servidor do Sentinel Log Manager.

Consulte a linha a seguir no arquivo `activemqusers.properties`:

```
collectormanager=<password>
```

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

14 Quando solicitado, aceite o certificado permanentemente.

15 Clique em *Concluir* para concluir a instalação.

16 Reinicie a máquina.

Se seu Gerenciador de Coletor estiver sendo executado no Windows 2008 e se forem registradas exceções no arquivo `collector_manager0.0.log` após reiniciar, consulte Seção A.4, “O Gerenciador de Coletor gera uma exceção no Windows 2008 quando o UAC está habilitado” na página 69 para resolver o problema.

8 Desinstalação

Esta seção discute os procedimentos para desinstalar o servidor do Novell Sentinel Log Manager e o Gerenciador de Coletor.

8.1 Desinstalando a aplicação

Se você deseja reter quaisquer dados do Log Manager, então você deve fazer backup dos dados antes de desinstalar a aplicação, para que você possa restaurar os dados posteriormente. Para obter mais informações, consulte a seção “Backup e restauração de dados” no *Sentinel Log Manager 1.2.2 Administration Guide (Guia de Administração do Sentinel Log Manager 1.2)*.

Se você não precisa reter nenhum dado, use os procedimentos a seguir para desinstalar a aplicação:

- **Aplicação VMware ESX:** Se a máquina virtual for dedicada ao Novell Sentinel Log Manager e você não precisar reter nenhum dado, apague a máquina virtual para desinstalar a aplicação virtual do Log Manager.
- **Aplicação Xen:** Se a máquina virtual Xen for dedicada ao Novell Sentinel Log Manager e você não precisar reter nenhum dado, apague-a para desinstalar a aplicação virtual do Log Manager.
- **Aplicação em hardware:** Se o sistema for dedicado ao Novell Sentinel Log Manager e você não precisar reter nenhum dado, reformate a unidade de disco rígido para desinstalar o Log Manager em uma máquina física.

8.2 Desinstalando o Sentinel Log Manager

1. Efetue login no servidor do Sentinel Log Manager como `root`.
2. Para executar o script de desinstalação, execute o seguinte comando:

   ```
   /opt/novell/sentinel_log_mgr/setup/uninstall-slm
   ```

3. Quando for solicitado que você confirme novamente que deseja prosseguir com a desinstalação, pressione s.

   O servidor do Sentinel Log Manager será interrompido e desinstalado.

8.3 Desinstalando o Gerenciador de Coletor

Esta seção discute os procedimentos para desinstalar o Gerenciador de Coletor instalado em máquinas Windows ou Linux.

8.3.1 Desinstalando o Gerenciador de Coletor no Linux

1. Efetue login como `root`.
2. Na máquina onde o Gerenciador de Coletor está instalado, navegue até o seguinte local:

   `$ESEC_HOME/_uninst`
3. Execute o seguinte comando:

   `./uninstall.bin`
4. Selecione um idioma e clique em *OK*.
5. Clique em *Avançar* no assistente de instalação.
6. Selecione os recursos que deseja desinstalar e clique em *Avançar*.
7. Pare todos aplicativos do Sentinel Log Manager em execução e clique em *Avançar*.
8. Clique em *Desinstalar*.
9. Clique em *Concluir*.
10. Selecione *Reinicializar o sistema* e clique em *Concluir*.

8.3.2 Desinstalando o Gerenciador de Coletor no Windows

1. Efetue login como administrador.
2. Pare o servidor do Sentinel Log Manager.
3. Selecione Iniciar > Executar.
4. Especifique o seguinte:

   `%Esec_home%\_uninst`
5. Clique duas vezes sobre o arquivo `uninstall.exe` para executá-lo.
6. Selecione um idioma e clique em *OK*.

   O assistente de instalação é exibido.
7. Clique em Avançar.
8. Selecione os recursos que deseja desinstalar e clique em *Avançar*.
9. Pare todos aplicativos do Sentinel Log Manager em execução e clique em *Avançar*.
10. Clique em *Desinstalar*.
11. Clique em *Concluir*.
12. Selecione *Reinicializar o sistema* e clique em *Concluir*.

8.3.3 Limpeza manual dos diretórios

Linux

1. Efetue login como `root` na máquina onde o Gerenciador de Coletor foi desinstalado.
2. Pare todos os processos do Sentinel Log Manager.
3. Remova o conteúdo do diretório `/opt/novell/sentinel6`

Windows

1. Efetue login como administrador na máquina onde o Gerenciador de Coletor foi desinstalado.
2. Apague a pasta `%CommonProgramFiles%\InstallShield\Universal` e todo o seu conteúdo.
3. Apague a pasta `%ESEC_HOME%` . Por padrão, esta é a pasta `C:\Program Files\Novell\Sentinel6`.

A Solucionando problemas de instalação

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

A.1 Se a senha dbauser não corresponder à senha dbauser armazenada no arquivo .pgpass, o upgrade do Sentinel Log Manager falhará.

Problema:

Durante o upgrade do Sentinel Log Manager, o upgrade do banco de dados falhará se a senha dbauser não corresponder à senha armazenada no arquivo `.pgpass`.

O comportamento varia de acordo com o modo de instalação:

Instalador padrão: O upgrade não prossegue e é exibida uma mensagem relacionada, indicando a causa do erro e a solução.

Console da aplicação: A seguinte mensagem de erro é exibida:

```
Installing: novell-SLMdb-1.2.0.2-954 [error]
Installation of novell-SLMdb-1.2.0.2-954 failed:
(with --nodeps --force) Error: Subprocess failed. Error: RPM failed: Unable to
login to the database, cannot continue with the upgrade. Check if the dbauser
password specified in /home/novell/.pgpass is correct and try again.
error: %pre(novell-SLMdb-1.2.0.2-954.x86_64) scriptlet failed, exit status 2
error:   install: %pre scriptlet failed (2), skipping novell-SLMdb-1.2.0.2-954

Abort, retry, ignore? [a/r/i] (a):
```

WebYaST: O WebYaST continua indicando que uma atualização ainda está disponível. Você pode verificar o arquivo `/var/opt/novell/sentinel_log_mgr/log/install.log` para conhecer a causa real desse erro.

Solução temporária:

Atualize a senha no arquivo `.pgpass` com a senha dbauser atual e prossiga com o upgrade. Para obter mais informações sobre o arquivo `.pgpass`, consulte a documentação do PostgreSQL.

Se você estiver fazendo upgrade pelo console da aplicação, realize uma destas ações:

- Digite `a` para interromper a instalação, atualize a senha no arquivo `/home/novell/.pgpass` e, em seguida, execute o `patch zypper` para prosseguir com o upgrade.
- Abra outro console e atualize a senha no arquivo `/home/novell/.pgpass`. No console de upgrade, digite `r` para prosseguir com o upgrade.
- Digite `i` para ignorar a mensagem de erro e prosseguir com a instalação. Quando o upgrade for concluído, atualize a senha no arquivo `/home/novell/.pgpass` e, em seguida, execute o `patch zypper` no console para concluir o procedimento de upgrade com êxito.

Se você estiver fazendo upgrade usando o WebYaST:

1. Faça login no console da aplicação.
2. Atualize a senha dbauser no arquivo `/home/novell/.pgpass`.
3. No WebYaST, clique em *Atualizar Tudo* para continuar o processo de upgrade.

   Quando o upgrade for concluído, a mensagem `O sistema está atualizado` será exibida no WebYaST.

A.2 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 Log Manager na aplicação falhará.

Para resolver esse problema, defina corretamente as configurações de rede para que o sistema tenha um endereço IP e um nome de host válidos.

A.3 Problemas ao configurar a rede com o VMware Player 3 no SLES 11

Você pode encontrar o erro a seguir ao tentar configurar a rede com o VMware Player 3 no SLES 11:

```
Jan 12 14:57:34.761: vmx| VNET: MACVNetPortOpenDevice: Ethernet0: can't open vmnet
device (No such device or address)
Jan 12 14:57:34.761: vmx| VNET: MACVNetPort_Connect: Ethernet0: can't open data fd
Jan 12 14:57:34.761: vmx| Msg_Post: Error
Jan 12 14:57:34.761: vmx| [msg.vnet.connectvnet] Could not connect Ethernet0 to
virtual network "/dev/vmnet0". More information can be found in the vmware.log
file.
Jan 12 14:57:34.761: vmx|[msg.device.badconnect] Failed to connect virtual device
Ethernet0.
Jan 12 14:57:34.761: vmx| --
```

Este erro indica que o arquivo VMX pode ter sido aberto por outra MV. Para resolver esse problema, você deve atualizar o endereço MAC no arquivo VMX da seguinte maneira:

1. Abra o arquivo VMX em um editor de texto.
2. Copie o endereço MAC no campo `ethernet0.generatedAddress`.

3 Abra o arquivo `/etc/udev/rules.d/70-persistent-net.rules` a partir do sistema operacional convidado.

4 Comente a linha original, então digite uma linha `SUBSYSTEM` da seguinte maneira:

```
SUBSYSTEM=="net", DRIVERS=="?*", ATTRS{address}==<MAC address>, NAME="eth0"
```

5 Substitua *<endereço_MAC>* pelo endereço MAC copiado em Etapa 2.

6 Grave e feche o arquivo.

7 Abra a MV no VMware Player.

A.4 O Gerenciador de Coletor gera uma exceção no Windows 2008 quando o UAC está habilitado

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

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

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

Solução temporária: Mude o proprietário de Logon dos serviços de Implantação Rápida do Sentinel 6.1 para o usuário atual. Por padrão, o proprietário de Logon está definido como Conta Sistema Local. Para mudar a opção padrão:

1 Execute `services.msc` para abrir a janela Serviços.

2 Clique o botão direito do mouse em Sentinel e selecione *Propriedades*.

3 Na janela Propriedade do Sentinel, selecione a guia *Login*.

4 Selecione *Esta Conta* e forneça as credenciais do usuário atual que foram usadas para instalar o Gerenciador de Coletor.

Observação: O usuário deverá estar no grupo de administradores.

A.5 Fazendo upgrade do Log Manager como um usuário não root diferente do usuário Novell

O procedimento de upgrade falhará se você tentar fazer o upgrade do servidor instalado do Sentinel Log Manager como um usuário não root diferente do usuário `novell`. Este problema ocorre devido à natureza das permissões de arquivo definidas durante a instalação do Sentinel Log Manager 1.0.

Para fazer upgrade do servidor instalado do Sentinel Log Manager 1.0 como um usuário não root diferente do usuário `novell`, faça o seguinte:

1 Crie o usuário `novell`.

2 Mude a propriedade da instalação do Sentinel Log Manager 1.0 para `novell:novell`.

```
chown -R novell:novell /opt/novell/<install_directory>
```

Substitua *<diretório_instalação>* pelo nome do diretório de instalação. Por exemplo,

```
chown -R novell:novell /opt/novell/sentinel_log_mgr_1.0_x86-64
```

3. Altere a entrada ESEC_USER em `/etc/opt/novell/sentinel_log_mgr/config/esecuser.properties` para `novell`.

A.6 A UUID não é criada para Gerenciadores de Coletor com Imagens

Se você tiver obtido uma imagem do servidor do Gerenciador de Coletor (por exemplo, usando ZenWorks Imaging) e restaurar as imagens em diferentes máquinas, o Sentinel Log Manager não identificará exclusivamente as novas instâncias do Gerenciador de Coletor. Isso ocorre devido a UUIDs duplicadas.

Você deve gerar a UUID nos sistemas de Gerenciador de Coletor recentemente instalados realizando as seguintes etapas:

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

   O Gerenciador de Coletor gera automaticamente a UUID.

Terminologia do Sentinel

Esta seção descreve a terminologia usada neste documento.

Coletores. Um utilitário que analisa os dados e distribui um fluxo de eventos enriquecido aplicando taxonomia, detecção de exploração e relevância comercial ao fluxo de dados antes que os eventos sejam correlacionados, analisados e enviados para o banco de dados.

Conectores. Um utilitário que usa métodos padrão de mercado para conectar-se à fonte de dados e obter dados iniciais.

Retenção de dados. Uma política que define a duração pela qual os eventos serão mantidos antes de serem apagados do servidor do Sentinel Log Manager.

Fonte de eventos. O aplicador ou sistema que registra o evento.

Gerenciamento de Fonte de Eventos. ESM. A interface que permite gerenciar e monitorar conexões entre o Sentinel e suas fontes de eventos usando Conectores e Coletores do Sentinel.

Eventos por Segundo. EPS. Um valor que mede a velocidade com que a rede gera dados a partir de seus dispositivos e aplicativos de segurança. Também é uma taxa em que o Sentinel Log Manager pode coletar e armazenar dados de dispositivos de segurança.

Integrador. Plug-ins que permitem que sistemas Sentinel conectem-se a outros sistemas externos. As ações em JavaScript podem usar Integradores para interagir com outros sistemas.

Dados iniciais . Os eventos não processados que são recebidos pelo conector e enviados diretamente para o barramento de mensagens do Sentinel Log Manager e então gravados no disco do servidor do Sentinel Log Manager. Os dados iniciais variam de Conector para Conector por causa do formato dos dados armazenados no dispositivo.