Guia de instalação e configuração

NetIQ Sentinel 7.0.1

March 2012

Informações legais

Para obter mais informações, entre em contato com a NetIQ em:

1233 West Loop South, Houston, Texas 77027

E.U.A.

www.netiq.com

Índice

Sobre este guia

Este guia fornece uma introdução ao NetIQ Sentinel e explica como instalar, migrar e configurar o Sentinel.

Público

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

Comentários

Gostaríamos de receber seus comentários e suas sugestões sobre este manual e sobre as outras documentações incluídas no produto. Use o recurso User Comments (Comentários do Usuário) na parte inferior de cada página da documentação online.

Atualizações da documentação

Para obter a versão mais recente do *Guia de instalação e configuração do NetIQ Sentinel 7.0.1*, acesse o site de documentação do Sentinel (http://www.novell.com/documentation/sentinel70).

Documentação adicional

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

- Guia de visão geral do Sentinel (http://www.novell.com/documentation/sentinel70/s70_overview/data/bookinfo.html)
- Guia de Inicialização Rápida do Sentinel (http://www.novell.com/documentation/sentinel70/s70_quickstart/data/s70_quickstart.html)
- Guia de Administração do Sentinel (http://www.novell.com/documentation/sentinel70/s70_admin/data/bookinfo.html)
- Guia do Usuário do Sentinel (http://www.novell.com/documentation/sentinel70/s70_user/data/bookinfo.html)
- Guia de Visão Geral de Vínculo do Sentinel (http://www.novell.com/documentation/sentinel70/sentinel_link_overview/data/bookinfo.html)
- Eventos de Auditoria Interna do Sentinel (http://www.novell.com/documentation/sentinel70/s70_auditevents/data/bookinfo.html)
- Sentinel SDK (http://www.novell.com/developer/develop_to_sentinel.html)

  O site do Sentinel SDK fornece informações sobre como você pode criar seus próprios plug-ins.

Entrando em contato com a Novell e a NetIQ

Agora o Sentinel é um produto NetIQ, mas a Novell continua administrando muitas funções de suporte.

- Site da Novell (http://www.novell.com)

- Site da NetIQ (http://www.netiq.com)
- Suporte técnico (http://support.novell.com/contact/getsupport.html?sourceidint=suplnav4_phonesup)
- Suporte Pessoal (http://support.novell.com/support_options.html?sourceidint=suplnav_supportprog)
- Site para download de patches (http://download.novell.com/index.jsp)
- Fóruns de suporte da comunidade do Sentinel (http://forums.novell.com/novell-product-support-forums/sentinel/)
- TIDS do Sentinel (http://support.novell.com/products/sentinel)
- Site de plug-ins do Sentinel (http://support.novell.com/products/sentinel/secure/sentinel61.html)
- **Lista de e-mails de notificação:** Inscreva-se no site de plug-ins do Sentinel

Entrando em contato com o Suporte a Vendas

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

Mundial: Escritórios da NetIQ (http://www.netiq.com/about_netiq/officelocations.asp)

Estados Unidos e Canadá: 888-323-6768

E-mail: info@netiq.com

Site: www.netiq.com

Instalando

Use as seguintes informações para instalar o Sentinel:

1 Atendendo aos requisitos do sistema

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

1.1 Requisitos do sistema e plataformas suportadas

O NetIQ é compatível com o Sentinel nos sistemas operacionais descritos nesta seção. O NetIQ também é compatível com o Sentinel em sistemas com atualizações secundárias a esses sistemas operacionais, como patches de segurança ou hotfixes. No entanto, a execução do Sentinel em sistemas com atualizações importantes para esses sistemas operacionais não é suportada enquanto o NetIQ não tiver testado e certificado essas atualizações.

1.1.1 Sistemas operacionais e plataformas suportados

O servidor do Sentinel, o Gerenciador de Coletor e o Mecanismo de Correlação são suportados nos seguintes sistemas operacionais e plataformas:

Categoria	Requisito
Sistema Operacional	O Sentinel é suportado nos seguintes sistemas operacionais: ◆ SUSE Linux Enterprise Server (SLES) 11 SP1 de 64 bits * ◆ Red Hat Enterprise Linux for Servers (RHEL) 6 de 64 bits * O Sentinel 7 não é suportado nas instalações do Open Enterprise Server no SLES.
Plataforma virtual	O NetIQ fornece aplicações que instalam um servidor SLES 11 SP1 de 64 bits e o Sentinel nas seguintes plataformas virtuais: ◆ VMWare ESX 4.0 ◆ Xen 4.0
DVD ISO	O NetIQ fornece um arquivo ISO de DVD que instala o SLES 11 SP1 de 64 bits e o Sentinel em: ◆ Hyper-V Server 2008 R2 ◆ Hardware sem um sistema operacional instalado

1.1.2 Requisitos de hardware

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

- "Servidor do Sentinel" na página 12
- "Gerenciador de Coletor" na página 13
- "Mecanismo de Correlação" na página 14

Servidor do Sentinel

Esta seção lista as recomendações de hardware para um sistema de produção que armazena 90 dias de dados online. As recomendações pressupõem um tamanho de evento médio de 600 bytes. As recomendações de armazenamento local e de rede incluem um buffer de 20% acima das estimativas reais de armazenamento. A NetIQ recomenda ter um buffer caso as estimativas sejam imprecisas ou alguns dos servidores fiquem ocupados demais ao longo do tempo.

Use as seguintes recomendações de hardware para executar o servidor Sentinel com todos os seus componentes instalados em um único servidor:

Categoria	100 EPS	2500 EPS	5000 EPS
CPU	Um Intel Xeon X5570 2,93 GHz (4 núcleos de CPU)	Duas CPUs Intel Xeon X5470 de 3.33 GHz (4 núcleos - 8 núcleos no total)	Duas CPUs Intel Xeon X5470 de 3.33 GHz (4 núcleos - 8 núcleos no total)
Armazenamento local (30 dias)	2 unidades de 256 GB e 7.200 RPM (Hardware RAID 1 com 256 MB de cache)	8 unidades de 1.2 TB e 7.200 RPM (Hardware RAID 10 com cache de 256 MB)	16 unidades de 1.2 TB e 15.000 RPM, (Hardware RAID 10 com cache de 512 MB) ou uma SAN (storage area network) equivalente
Armazenamento em rede (90 dias)	2 de 128 GB	4 de 1 TB	8 de 1 TB
Memória	**Outras instalações:** 4 GB **Instalação ISO de DVD:** 4.5 GB	16 GB	24 GB

NOTE: O Sentinel é suportado em processadores x86-de 64 bits Intel Xeon e AMD Opteron, mas não é suportado em processadores de 64 bits puros, como Itanium.

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 1.1.5, “Estimativa dos requisitos para armazenamento de dados” na página 16.
- 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 por motivos de desempenho da pesquisa e da geração de relatórios. O tamanho do armazenamento local pode ser reduzido se o custo de armazenamento for levado em consideração. 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).
- O volume de estado estável recomendado é 80% do máximo de EPS licenciados. O NetIQ recomenda que você adicione instâncias adicionais do Sentinel se o limite for atingido.

Gerenciador de Coletor

Use os seguintes requisitos de hardware para executar o Gerenciador de Coletor em um sistema separado do Sentinel Server em um ambiente de produção:

Categoria	Mínimo	Recomendação
CPU	Intel Xeon L5240 3-Ghz (2 núcleos)	Um Intel Xeon X5570 2,93 GHz (4 núcleos de CPU)
Espaço em disco	10 GB (RAID 1)	20 GB (RAID 1)
Memória	1.5 GB	4 GB
Taxa estimada (EPS)	500	2000

Mecanismo de Correlação

Use os seguintes requisitos de sistema para executar o Mecanismo de Correlação em um sistema separado do Sentinel Server em um ambiente de produção:

Categoria	Mínimo	Recomendação
CPU	Intel Xeon L5240 3-Ghz (2 núcleos)	Um Intel Xeon X5570 2,93 GHz (4 núcleos de CPU)
Espaço em disco	10 GB (não é necessário RAID)	10 GB (não é necessário RAID)
Memória	1.5 GB	4 GB
Taxa estimada (EPS)	500	2500

1.1.3 Plataformas de banco de dados suportadas

O Sentinel inclui um sistema de armazenamento baseado em arquivos incorporado e um banco de dados que são necessários para executar o Sentinel. No entanto, se você usar o recurso opcional de sincronização de dados para copiar dados para um data warehouse, o Sentinel suportará o Oracle versão 11g R2 ou o Microsoft SQL Server 2008 R2 como o data warehouse.

1.1.4 Browsers suportados

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

NOTE: Para carregar os aplicativos do cliente Sentinel corretamente, é necessário ter o plug-in Sun Java instalado no seu sistema.

Plataforma	Browser
Windows 7	◆ Firefox 5, 6, 7, 8, 9 e 10 ◆ Internet Explorer 8 e 9* Para obter mais informações sobre o Internet Explorer 8, consulte "Pré-requisitos para o Internet Explorer" na página 15.
SLES 11 SP1 e RHEL 6	◆ Firefox 5, 6, 7, 8, 9 e 10 Para obter mais informações, consulte "Atualização manual da versão do Firefox" na página 15.

Pré-requisitos para o Internet Explorer

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

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

Atualização manual da versão do Firefox

O Sentinel é compatível com o Firefox versões 5 a 10; no entanto, o sistema SLES 11 SP1 é fornecido com o Firefox versão 3.6*x*. Execute as seguintes etapas para atualizar manualmente uma instalação do SLES 11 SP1 para incluir uma versão compatível do Firefox:

1. Abra o YaST.
2. Selecione *Software* > *Repositórios de Software* para exibir a janela Repositórios de Software Configurados.
3. Clique em *Adicionar* para abrir a janela Tipo de Mídia.
4. Selecione a opção *Especificar URL* e, em seguida, clique em *Avançar*.

   Isso exibe a janela URL do Repositório.
5. Digite o link do Repositório de Software (http://download.opensuse.org/repositories/mozilla/SLE_11/) na caixa de texto do URL e, em seguida, clique em *Avançar*.

   É feito o download do repositório de software.
6. Clique em *OK* para atualizar o repositório de software.
7. Clique em *Gerenciamento de Software* para abrir a janela YaST2.
8. Insira `Firefox` na caixa de texto *Pesquisa*.

   A lista de pacotes do Firefox é exibida.
9. Selecione os pacotes necessários para a versão compatível do Firefox que deseja instalar.

Se você selecionar um pacote que entre em conflito com a versão existente, uma caixa de diálogo de Aviso será exibida. Selecione a opção apropriada e, em seguida, clique no botão *OK, tentar novamente*.

10 Clique em *Aceitar.*

1.1.5 Estimativa dos requisitos para armazenamento de dados

O Sentinel é usado para reter dados iniciais por um longo período de tempo e atender a conformidades legais e outros requisitos. O Sentinel 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 em longo prazo" no *Guia de administração do NetIQ Sentinel 7.0.1*.

Para determinar o espaço de armazenamento de acesso aleatório necessário para o Sentinel, 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, 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.

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 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 0.00008 = 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 0.00001 = 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 0.000003 = 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 evento serão copiados para ele geralmente após 2 dias. Para obter mais informações, consulte "Configurando o armazenamento de dados" no *Guia de Administração do NetIQ Sentinel 7.0.1*.

- **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

---

NOTE:

- 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.

1.1.6 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 0,002 = dados gravados por segundo em disco

  Por exemplo, a 500 EPS, para um tamanho de evento médio de 758 bytes e um tamanho médio de dados não processados de 490 bytes no arquivo de registro, os dados gravados no disco são determinados da seguinte forma:

  (758 bytes + 490 bytes) x 500 EPS x .002 = ~1100 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 0,0002 = solicitações de E/S por segundo para disco

  Por exemplo, a 500 EPS, para um tamanho de evento médio de 758 bytes e um tamanho médio de dados não processados de 490 bytes no arquivo de registro, o número de solicitações de E/S por segundo para o disco é determinado da seguinte forma:

  (758 bytes + 490 bytes) x 500 EPS x .00002 = ~10 transferências por segundo

- **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 0,003 = blocos gravados por segundo em disco

Por exemplo, a 500 EPS, para um tamanho de evento médio de 758 bytes e um tamanho médio de dados não processados de 490 bytes no arquivo de registro, o número de blocos gravados por segundo no disco é determinado da seguinte forma:

(758 bytes + 490 bytes) x 500 EPS x .003 = ~1800 blocos por segundo

- **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 correspondentes à consulta em milhões) x coeficiente de compactação 0,40 = kilobytes lidos por segundo do disco

  Por exemplo, em 5 milhões de eventos correspondentes à consulta de pesquisa, para um tamanho médio de eventos de 758 bytes e um tamanho médio de dados não processados de 490 bytes no arquivo de registro, os dados lidos por segundo no disco é determinado da seguinte forma:

  (758 bytes + 490 bytes) x 5 x 0.40 = ~500 KB

1.1.7 Estimativa de utilização de largura de banda de rede

Use as seguintes fórmulas para estimar a utilização de largura de banda da rede entre o servidor Sentinel e o Gerenciador de Coletor remoto em várias taxas 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 758 bytes e um tamanho médio de dados não processados de 490 bytes no arquivo de registro, a utilização de largura de banda de rede é determinada da seguinte forma:

(758 bytes + 490 bytes} x 500 EPS x 0,0003 = ~175 Kbps

1.1.8 Ambiente virtual

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

Para obter informações sobre recomendações para máquina física, consulte Seção 1.1, “Requisitos do sistema e plataformas suportadas” na página 11.

1.2 Requisitos do sistema do Conector e do Coletor

Cada Conector e Coletor tem seu próprio conjunto de requisitos de sistema e plataformas suportadas. Consulte a documentação do Conector e do Coletor na página da web de plug-ins do Sentinel (http://support.novell.com/products/sentinel/secure/sentinelplugins.html).

1.3 Portas usadas

1.3.1 Servidor do Sentinel

Portas locais

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

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).
TCP 27017	Usado para o banco de dados de configuração de Inteligência de Segurança.
TCP 28017	Usado para a interface da web do banco de dados de Inteligência de Segurança.
TCP 32000	Usado para comunicação interna entre o processo do agrupador e o processo do servidor.

Portas de rede

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

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

Portas	Descrição
TCP 1099 e 2000	Usadas com ferramentas de monitoramento para conectarem-se com o processo do servidor do Sentinel usando o JMX (Java Management Extensions).
TCP 1289	Usada para conexões de auditoria.
UDP 1514	Usada para mensagens syslog.
TCP 8443	Usada para comunicação HTTPS.
TCP 1443	Usada para mensagens syslog criptografas por SSL.
TCP 61616	Usada para comunicação entre os Gerenciadores de Coletor e o servidor.
TCP 10013	Usadas pelo Sentinel Control Center e pelo Designer de Soluções.
TCP 1468	Usada para mensagens syslog.
TCP 10014	Usadas pelos Gerenciadores de Coletor remotos para conectar ao servidor por meio do proxy SSL. No entanto, isso é incomum. Por padrão, os Gerenciadores de Coletor remotos usam a porta SSL 61616 para conectar ao servidor.

Portas específicas da aplicação do Sentinel Server

Além das portas acima, as seguintes portas ficam abertas na aplicação do servidor Sentinel:

Portas	Descrição
TCP 22	Usada para fornecer acesso seguro ao shell para a aplicação do Sentinel.
TCP 54984	Usadas pelo Console de Gerenciamento da Aplicação do Sentinel (WebYaST). Também usada pelo serviço de atualização da aplicação do Sentinel.
TCP 289	Encaminhada para 1289 para conexões de auditoria.
UDP 443	Encaminhada para 8443 para comunicação HTTPS.
UDP 514	Encaminhada para 1514 para mensagens syslog.
TCP 1290	Esta é a porta de vinculação do Sentinel que tem permissão para se conectar por meio do Firewall do SuSE.
UDP e TCP 40000 - 41000	As portas podem ser usadas ao configurar servidores de coleta de dados, como o syslog. O Sentinel não se comunica nessas portas por padrão.

1.3.2 Gerenciador de Coletor

Portas de rede

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

Portas	Descrição
TCP 1289	Usada para conexões de auditoria.
UDP 1514	Usada para mensagens syslog.
TCP 1443	Usada para mensagens syslog criptografas por SSL.
TCP 1468	Usada para mensagens syslog.
TCP 1099 e 2000	Usadas com ferramentas de monitoramento para conectarem-se com o processo do servidor do Sentinel usando o JMX (Java Management Extensions).

Portas específicas da aplicação do Gerenciador de Coletor

Além das portas acima, as seguintes portas ficam abertas na aplicação do Gerenciador de Coletor do Sentinel:

Portas	Descrição
TCP 22	Usada para fornecer acesso seguro ao shell para a aplicação do Sentinel.
TCP 54984	Usadas pelo Console de Gerenciamento da Aplicação do Sentinel (WebYaST). Também usada pelo serviço de atualização da aplicação do Sentinel.
TCP 289	Encaminhada para 1289 para conexões de auditoria.
UDP 514	Encaminhada para 1514 para mensagens syslog.
TCP 1290	Esta é a porta de vinculação do Sentinel que tem permissão para se conectar por meio do Firewall do SuSE.
UDP e TCP 40000 - 41000	As portas podem ser usadas ao configurar servidores de coleta de dados, como o syslog. O Sentinel não se comunica nessas portas por padrão.

1.3.3 Mecanismo de Correlação

Portas de rede

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

Portas	Descrição
TCP 1099 e 2000	Usadas com ferramentas de monitoramento para conectarem-se com o processo do servidor do Sentinel usando o JMX (Java Management Extensions).

Portas específicas da aplicação do Mecanismo de Correlação

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

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

2 Instalando o Sentinel

O Sentinel pode ser instalado como uma instalação independente ou como uma instalação de aplicação. O instalador independente instala o Sentinel em um sistema operacional SUSE Linux Enterprise Server (SLES) 11 SP1 ou Red Hat Enterprise Linux (RHEL) 6 existente. O instalador da aplicação instala o sistema operacional SLES 11 SP1 de 64 bits e o Sentinel.

Esta seção descreve o procedimento para uma instalação independente do servidor do Sentinel em um sistema SLES 11 SP1 ou RHEL 6 existente. Para ver o procedimento para a instalação da aplicação, consulte Capítulo 5, "Instalando a aplicação" na página 41.

2.1 Métodos de instalação

Os métodos a seguir estão disponíveis para a instalação independente:

- **Interativo:** A instalação prossegue com entradas do usuário. Durante a instalação, é possível gravar as opções de instalação (entradas do usuário ou valores padrão) em um arquivo, que poderá ser posteriormente usado para instalação silenciosa.
- **Silencioso:** É possível usar essa opção se as opções de instalação estiverem pré-gravadas. A instalação Silenciosa consulta o arquivo que tem a entrada de instalação gravada e executa a instalação com os valores capturados no arquivo. A instalação silenciosa é eficaz quando você instala várias réplicas da mesma configuração no seu ambiente. Para obter mais informações, consulte a Seção 2.5, "Instalação silenciosa" na página 29.

Tanto a instalação interativa quanto a silenciosa do Sentinel podem ser feitas com um usuário `root` ou um usuário não root.

2.1.1 Instalação normal e personalizada

Ao instalar o Sentinel, as seguintes configurações estão disponíveis:

- **Normal:** Nesta configuração, a instalação usa valores padrões para a definição da configuração. A entrada do usuário só é obrigatória para a senha. Para obter mais informações sobre a instalação do Sentinel com a configuração padrão, consulte Seção 2.4.1, "Configuração padrão" na página 26.
- **Personalizado:** Nesta configuração, a instalação solicita que você especifique os valores para a definição da configuração. É possível selecionar os valores padrão ou especificar os valores necessários. Para obter mais informações sobre a instalação do Sentinel com uma configuração personalizada, consulte Seção 2.4.2, "Personalizar Configuração" na página 27.

Configuração padrão	Personalizar Configuração
Instala com uma chave de avaliação padrão de 90 dias.	Permite instalar com a chave de licença de 90 dias ou com uma chave de licença válida.
Permite que você especifique a senha do administrador e use-a como senha padrão tanto para dbuser quanto para appuser.	Permite que você especifique a senha do administrador. Para dbauser e appuser, é possível especificar uma nova senha ou usar a senha do administrador.
Instala as portas padrão para todos os componentes.	Permite especificar portas para diferentes componentes.
Autentica os usuários com o banco de dados interno.	Dá a opção de autenticar usuários com o banco de dados interno ou com a autenticação LDAP.

2.1.2 Componentes instalados

Há vários componentes no Sentinel. Todos os componentes a seguir são instalados por padrão:

- Servidor do Sentinel
- Mecanismo de Correlação
- Gerenciador de Coletor

Mecanismos de Correlação ou Gerenciadores de Coletor adicionais podem ser instalados em diferentes sistemas.

2.2 Antes de começar

Verifique se você concluiu as seguintes tarefas antes de iniciar a instalação:

- Verifique se o hardware e o software atendem aos requisitos de sistema listados em Seção 1.1, "Requisitos do sistema e plataformas suportadas" na página 11.
- Se houver uma instalação anterior do Sentinel, certifique-se de que não haja arquivos ou configurações de sistema restantes dessa instalação anterior. Para obter mais informações, consulte Parte V, "Desinstalação" na página 97.

- Para obter desempenho, estabilidade e confiabilidade ideais do servidor Sentinel, use o sistema de arquivos ext3 no SLES e o sistema de arquivos ext4 no RHEL. Para obter mais informações sobre sistemas de arquivos, consulte Visão geral de sistemas de arquivos no Linux (http://www.novell.com/documentation/sles11/stor_admin/data/filesystems.html) no *Guia de administração de armazenamento*.
- Defina as configurações de rede para que o sistema tenha um endereço IP e 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) se planeja instalar a versão licenciada.
- Sincronize o horário usando o protocolo NTP (Network Time Protocol).
- Confirme se as portas listadas em Seção 1.3, “Portas usadas” na página 19 estão abertas no firewall.
- Para obter o desempenho ideal, as definições da memória devem ser adequadas para o banco de dados PostgreSQL:

  O parâmetro SHMMAX deve ser maior ou igual a 1073741824. Para definir o valor adequado, anexe as seguintes informações ao arquivo `/etc/sysctl.conf`:

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

- Para uma instalação mínima ou sem periféricos, o sistema operacional do servidor Sentinel deve incluir pelo menos os componentes Servidor Base do servidor SLES ou do servidor RHEL 6. O Sentinel exige as versões de 64 bits dos seguintes RPMs:
  - bash
  - bc
  - coreutils
  - glibc
  - grep
  - libgcc
  - libstdc
  - lsof
  - net-tools
  - openssl
  - python-libs
  - sed
  - zlib

2.3 Opções de instalação

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

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

2.4 Instalação interativa

2.4.1 Configuração padrão

1. Faça download do arquivo de instalação do Sentinel na página Downloads da Novell (http://download.novell.com/index.jsp):
   - **1a** No campo *Produto ou tecnologia*, navegue para selecionar *SIEM-Sentinel*.
   - **1b** Clique em *Pesquisar*.
   - **1c** Clique no botão na coluna *Download* para *Avaliação do Sentinel 7.0*.
   - **1d** Clique em *continuar com o download* e especifique seu nome e senha de cliente.
   - **1e** Clique em *download* para obter a versão de instalação para sua plataforma.
2. Especifique na linha de comando o seguinte comando para extrair o arquivo de instalação.

   ```
   tar zxvf <install_filename>
   ```

   Substitua <*nome_arquivo_instalação*> pelo nome real do arquivo de instalação.
3. Mude para o diretório no qual extraiu o instalador:

   ```
   cd sentinel_server-7.0.0.0.x86_64
   ```
4. Especifique o seguinte comando para instalar o Sentinel:

```
./install-sentinel
```

ou

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

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

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

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

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

7. Digite `yes` ou `y` para aceitar a licença e continuar a instalação.

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

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

   A instalação prossegue com a chave de licença de avaliação de 90 dias incluída com o instalador. Essa chave de licença ativa o conjunto completo de recursos do produto por um período de teste de 90 dias. A qualquer momento durante ou após o período de teste, você pode substituir a licença de avaliação por uma chave de licença comprada.

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

10. Confirme a senha novamente.

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

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

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

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

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

2.4.2 Personalizar Configuração

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

1. Faça download do arquivo de instalação do Sentinel na página Downloads da Novell (http://download.novell.com/index.jsp):

   1a No campo *Produto ou tecnologia*, navegue para selecionar *SIEM-Sentinel*.

   1b Clique em *Pesquisar*.

   1c Clique no botão na coluna *Download* para *Avaliação do Sentinel 7.0*.

   1d Clique em *continuar com o download* e especifique seu nome e senha de cliente.

   1e Clique em *download* para obter a versão de instalação para sua plataforma.

2. Especifique na linha de comando o seguinte comando para extrair o arquivo de instalação.

```
tar zxvf <install_filename>
```

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

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

```
./install-sentinel
```

ou

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

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

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

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

5. Pressione a barra de espaço para ler o contrato de licença.
6. Digite `yes` ou `y` para aceitar o contrato de licença e prosseguir com a instalação.

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

7. Especifique `2` para executar uma instalação personalizada do Sentinel.
8. Insira `1` para usar a chave de licença padrão de avaliação de 90 dias.

ou

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

9. Especifique a senha do usuário administrador `admin` e confirme a senha novamente.
10. Especifique a senha do usuário do banco de dados `dbauser` e confirme a senha novamente.

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

11. Especifique a senha do usuário do aplicativo `appuser` e confirme a senha novamente.
12. Altere as atribuições de porta para os serviços do Sentinel inseerindo o número desejado e, em seguida, especificando o novo número da porta.
13. Depois de alterar as portas, especifique 7 para concluir.
14. Insira `1` para autenticar os usuários usando somente o banco de dados interno.

ou

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

O valor padrão é `1`.

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

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

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

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

2.5 Instalação silenciosa

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

Para realizar a instalação silenciosa, você deve ter gravado os parâmetros de instalação em um arquivo. Para obter informações sobre a criação do arquivo de resposta, consulte Seção 2.4.1, "Configuração padrão" na página 26 ou Seção 2.4.2, "Personalizar Configuração" na página 27.

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

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

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

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

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

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

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

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

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

2.6 Instalando o Sentinel como um usuário não raiz

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

1. Faça download dos arquivos de instalação na página Downloads da Novell (http://download.novell.com/index.jsp).
2. Especifique o seguinte comando na linha de comando para extrair os arquivos de instalação do arquivo tar:

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

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

3 Efetue login como `root` no servidor em que você deseja instalar o Sentinel como `root`.

4 Especifique o seguinte comando:

```
./bin/root_install_prepare
```

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

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

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

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

5 Aceite a lista de comandos.

Os comandos exibidos serão executados.

6 Especifique o seguinte comando para mudar o usuário não root `novell` recém-criado: `novell`:

```
su novell
```

7 (Condicional) Para realizar uma instalação interativa:

7a Especifique o seguinte comando:

```
./install-sentinel
```

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

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

7b Continue na Etapa 9.

8 (Condicional) Para realizar uma instalação silenciosa:

8a Especifique o seguinte comando:

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

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

8b Continue na Etapa 12.

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

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

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

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

11 Será solicitado que você especifique o modo de instalação.

- Se você escolher prosseguir com a instalação padrão, continue com Etapa 8a Etapa 10 em Seção 2.4.1, “Configuração padrão” na página 26.
- Se você escolher prosseguir com a instalação personalizada, continue com Etapa 7a Etapa 14 em Seção 2.4.2, “Personalizar Configuração” na página 27.

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

```
./bin/root_install_finish
```

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

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

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

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

2.7 Modificando a configuração depois da instalação

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

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

   ```
   ./configure.sh
   ```

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

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

   ou

   Insira `2` para informar uma chave de licença adquirida do Sentinel.
6. Decida se deseja manter a senha existente para o usuário administrador `admin`.
   - Se desejar manter a senha existente, insira `1` e, em seguida, continue com Etapa 7.
   - Se desejar alterar a senha existente, insira `2`, especifique a nova senha, confirme-a e, em seguida, continue com Etapa 7.
7. Decida se deseja manter a senha existente para o usuário do banco de dados `dbauser`.
   - Se desejar manter a senha existente, insira `1` e, em seguida, continue com Etapa 8.
   - Se desejar alterar a senha existente, insira `2`, especifique a nova senha, confirme-a e, em seguida, continue com Etapa 8.

   A conta `dbauser` é a identidade usada pelo Sentinel para interagir com o banco de dados. A senha inserida aqui pode ser usada para realizar tarefas de manutenção de banco de dados, incluindo a redefinição da senha do administrador, caso ela seja esquecida ou perdida.
8. Decida se deseja manter a senha existente para o usuário do aplicativo `appuser`.
   - Se desejar manter a senha existente, insira `1` e, em seguida, continue com Etapa 9.
   - Se desejar alterar a senha existente, insira `2`, especifique a nova senha, confirme-a e, em seguida, continue com Etapa 9.

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

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

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

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

ou

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

O valor padrão é `1`.

3 Instalação de Gerenciadores de Coletor adicionais

Por padrão, o Sentinel instala um Gerenciador de Coletor. Dependendo de seu ambiente, poderá ser necessário mais de um Gerenciador de Coletor. Use as seguintes informações para instalar Gerenciadores de Coletor remotos.

IMPORTANT: Não é possível instalar outro Gerenciador de Coletor ou Mecanismo de Correlação no mesmo servidor em que o Sentinel está sendo executado.

3.1 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 adicionais podem analisar e processar dados de eventos em um ambiente distribuído, o que aumenta o desempenho do sistema.
- **Segurança de dados adicional e menores requisitos de largura de banda de rede:** Se os Gerenciadores de Coletor estiverem co-localizados com fontes de eventos, então a filtragem, criptografia e compactação de dados pode ser realizada na origem.
- **Cache de arquivos:** 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.

3.2 Antes de começar

Verifique se você concluiu as seguintes tarefas antes de iniciar a instalação.

- ❒ Certifique-se de que o hardware e o software atendem aos requisitos mínimos. Para obter mais informações, consulte a Seção 1.1, “Requisitos do sistema e plataformas suportadas” na página 11.

- ❒ Sincronize o horário usando o protocolo NTP (Network Time Protocol).
- ❒ Os Gerenciadores de Coletor exigem conectividade de rede na porta de barramento de mensagens (61616) no servidor do Sentinel. Antes de iniciar a instalação do Gerenciador de Coletor, certifique-se de que todas as configurações do firewall e de rede podem se comunicar através dessa porta.

3.3 Instalando um Gerenciador de Coletor adicional

É preciso instalar o Gerenciador de Coletor remoto em um sistema diferente daquele em que o Sentinel ou o Mecanismo de Correlação está instalado.

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

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

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

   Efetue login com o nome de usuário e senha especificados durante a instalação do servidor do Sentinel.
2. Na barra de ferramentas, clique em *Downloads*.
3. No cabeçalho do Gerenciador de Coletor, clique em *Download dp Instalador*.
4. Clique em *Salvar Arquivo* para salvar o instalador no local desejado.
5. Especifique o seguinte comando para extrair o arquivo de instalação.

   `tar zxvf <install_filename>`

   Substitua <*nomearquivo_instalação*> pelo nome real do arquivo de instalação.
6. Mude para o diretório no qual extraiu o instalador. Por exemplo:

   `cd sentinel_collector_mgr-7.0.0.0.x86_64`
7. Especifique o seguinte comando para instalar o Gerenciador de Coletor do Sentinel:

   `./install-cm`

   O script de instalação primeiro verifica a memória disponível e o espaço em disco. Se a memória disponível for menor do que 1.5 GB, o script terminará a instalação automaticamente.
8. Especifique o número do idioma que deseja usar na instalação.

   O contrato de licença de usuário final será exibido no idioma selecionado.
9. Pressione a barra de espaço para ler o contrato de licença.
10. Digite `yes` ou `y` para aceitar o contrato de licença e prosseguir com a instalação.

    A instalação poderá levar alguns segundos antes de solicitar o tipo de configuração.
11. Quando solicitado, especifique 1 para prosseguir com a configuração padrão.
12. Insira o nome de host ou o endereço IP do servidor de comunicação da máquina na qual o Sentinel está instalado.
13. Especifique o nome de usuário e a senha para o Gerenciador de Coletor.

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

    Por exemplo:

```
collectormanager=1c51ae55
```

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

14 Quando solicitado, aceite o certificado permanentemente.

A instalação do Gerenciador de Coletor do Sentinel está concluída.

3.4 Adicionando um usuário personalizado para um Gerenciador de Coletor

O Sentinel recomenda que você use o nome de usuário padrão do Gerenciador de Coletor, `collectormanager`. No entanto, se você tiver vários Gerenciadores de Coletor remotos instalados e desejar identificá-los sepradamente, poderá criar novos usuários:

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

2 Abra o arquivo `activemqgroups.properties`.

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

3 Adicione o novo usuário do Gerenciador de Coletor na seção `cm`, separado por vírgulas. Por exemplo:

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

4 Grave e feche o arquivo.

5 Abra o arquivo `activemqusers.properties`.

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

6 Adicione a senha para o usuário que você criou em Etapa 3.

A senha pode ser qualquer string aleatório. Por exemplo:

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

7 Grave e feche o arquivo.

8 Reinicie o servidor do Sentinel.

4 Instalando Mecanismos de Correlação adicionais

Por padrão, o Sentinel instala um Mecanismo de Correlação. Para ambientes com grandes números de regras de correlação ou taxas de eventos extremamente altas, poderá ser vantajoso instalar mais de um Mecanismo de Correlação. Para obter informações sobre taxas de evento recomendadas por Mecanismo de Correlação, consulte Mecanismo de Correlação em Capítulo 1, "Atendendo aos requisitos do sistema" na página 11.

IMPORTANT: Não é possível instalar outro Gerenciador de Coletor ou Mecanismo de Correlação no servidor em que o Sentinel está sendo executado.

4.1 Antes de começar

Verifique se você concluiu as seguintes tarefas antes de iniciar a instalação.

- ❒ Certifique-se de que o hardware e o software atendem aos requisitos mínimos. Para obter mais informações, consulte a Seção 1.1, "Requisitos do sistema e plataformas suportadas" na página 11.
- ❒ Sincronize o horário usando o protocolo NTP (Network Time Protocol).
- ❒ Um Mecanismo de Correlação exige conectividade de rede na porta de barramento de mensagens (61616) no servidor do Sentinel. Antes de iniciar a instalação do Mecanismo de Correlação, certifique-se de que todas as configurações do firewall e de rede podem se comunicar através dessa porta.

4.2 Adicionando um Mecanismo de Correlação adicional

É preciso instalar o Mecanismo de Correlação remoto em um sistema diferente daquele em que o Sentinel ou um Gerenciador de Coletor remoto está instalado.

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

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

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

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

2 Na barra de ferramentas, clique em *Downloads*.

3 No cabeçalho do Mecanismo de Correlação, clique em *Download do Instalador*.

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

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

```
tar zxvf <install_filename>
```

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

6 Mude para o diretório no qual extraiu o instalador. Por exemplo:

```
cd sentinel_correlation_engine-7.0.0.0.x86_64
```

7 Especifique o seguinte comando para instalar o Mecanismo de Correlação do Sentinel:

```
./install-ce
```

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

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

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

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

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

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

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

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

13 Especifique o nome de usuário e a senha para o Mecanismo de Correlação.

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

Por exemplo:

```
correlationengine=68790d7a
```

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

14 Quando solicitado, aceite o certificado permanentemente.

A instalação do Mecanismo de Correlação do Sentinel está concluída.

4.3 Adicionando um usuário personalizado para o Mecanismo de Correlação

O Sentinel recomenda que você use o nome de usuário padrão do Mecanismo de Correlação, `correlationengine`. No entanto, se você tiver vários Mecanismos de Correlação remotos instalados e desejar identificá-los sepradamente, poderá criar novos usuários:

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

2 Abra o arquivo `activemqgroups.properties`.

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

3 Adicione o novo usuário do Mecanismo de Correlação na seção `admin`, sperado por uma vírgula. Por exemplo:

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

4 Grave e feche o arquivo.

5 Abra o arquivo `activemqusers.properties`.

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

6 Adicione a senha para o usuário que você criou em Etapa 3.

A senha pode ser qualquer string aleatório. Por exemplo:

```
system=c7f34372ecd20d831cceb29e754e5ac9
correlationengine=68790d7a
ceuser1=69700c6d
ceuser2=70701b5c
```

7 Grave e feche o arquivo.

8 Reinicie o servidor do Sentinel.

5 Instalando a aplicação

A aplicação Sentinel é uma aplicação de software pronta para execução integrada no SUSE Studio. A aplicação combina um sistema operacional SUSE Linux Enterprise Server (SLES) 11 SP 1 robusto e o serviço de atualização integrado do software Sentinel para fornecer uma experiência de usuário fácil e eficiente que permite que os clientes paroveitem investimentos existentes. A aplicação de software pode ser instalada tanto em hardware quanto em um ambiente virtual.

5.1 Antes de começar

Assegure-se de ter concluído as seguintes tarefas antes de iniciar a instalação da aplicação.

- ❒ Verifique se os requisitos de hardware são atendidos. Para obter mais informações, consulte a Seção 1.1, “Requisitos do sistema e plataformas suportadas” na página 11.
- ❒ 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) se planeja instalar a versão licenciada.
- ❒ Obtenha seu código de registro 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 se registrar e receber atualizações de software.

5.2 Instalando a aplicação VMware

5.2.1 Instalando o Sentinel

Para importar e instalar a imagem da aplicação Sentinel em um servidor VMware ESX:

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

   O arquivo correto da aplicação VMware possui `vmx` em seu nome. Por exemplo, `sentinel_server_7.0.0.0.x86_64.vmx.tar.gz`

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

   ```
   tar zxvf <install_file>
   ```

   Substitua *<arquivo_instalação>* pelo nome real do arquivo.
5. Para importar a imagem VMware no servidor ESX, use o VMware Converter e siga as instruções na tela do assistente de instalação.
6. Efetue login na máquina do servidor ESX.
7. Selecione a imagem VMware importada da aplicação e clique no ícone *Ligar*.
8. Selecione o idioma desejado e clique em *Avançar*.
9. Selecione o layout do teclado e clique em *Avançar*.
10. Leia e aceite o Contrato de Licença do Software SUSE Linux Enterprise Server (SLES) 11 SP1.
11. Leia e aceite o Contrato de Licença do Usuário Final do NetIQ Sentinel.
12. Na tela Nome de Host e Nome de Domínio, especifique o nome de host e o nome de domínio. Certifique-se de que a opção *Atribuir nome do host ao IP de loopback* esteja selecionada.
13. Clique em *Avançar*. As configurações do nome de host são gravadas.
14. Siga um destes procedimentos:
    - Para usar as configuraçõs atuais da conexão de rede, selecione *Usar configuração a seguir* na página Configuração de Rede II e, em seguida, clique em *Avançar*.
    - Para mudar as configurações de conexão de rede, selecione *Alterar*, faça as mudanças desejadas e, em seguida, clique em *Avançar*.

    As configurações de conexão da rede serão gravadas.
15. Defina a data e o horário e clique em *Avançar*.

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

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

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

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

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

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

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

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

19 Avance para a Seção 5.5, "Configuração pós-instalação para a aplicação" na página 51.

5.2.2 Instalando o Gerenciador de Coletor

Para importar e instalar a imagem da aplicação Sentinel no servidor VMware ESX:

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

O arquivo correto da aplicação VMware possui `vmx` em seu nome. Por exemplo, `sentinel_colletor_manager_7.0.0.0.x86_64.vmx.tar.gz`

2 Estabeleça um armazenamento de dados do ESX onde a imagem da aplicação possa ser instalada.

3 Efetue login como Administrador no servidor em que deseja instalar a aplicação.

4 Especifique o seguinte comando para extrair a imagem compactada da aplicação a partir da máquina onde o VM Converter está instalado:

```
tar zxvf <install_file>
```

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

5 Para importar a imagem VMware no servidor ESX, use o VMware Converter e siga as instruções na tela do assistente de instalação.

6 Efetue login na máquina do servidor ESX.

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

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

9 Especifique o número da porta do Servidor de Comunicação. A porta padrão de barramento de mensagem é `61616`.

10 Especifique o nome de usuário do JMS, que é o nome de usuário do Gerenciador de Coletor. O nome de usuário padrão é `collectormanager`.

11 Especifique a senha do usuário do JMS.

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

12 (Opcional) Para verificar a senha, veja a seguinte linha em `activemqusers.properties`

```
collectormanager=<password>
```

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

13 Clique em *Avançar*.

14 Quando solicitado, aceite o certificado.

15 Clique em *Avançar* para concluir a instalação.

Quando a instalação estiver concluída, ela exibirá uma mensagem indicando que essa aplicação é o Gerenciador de Coletor do Sentinel, juntamente com o endereço IP. Ela também exibe o endereço IP da interface do usuário do servidor do Sentinel.

5.2.3 Instalando o Mecanismo de Correlação

Instalar a aplicação do Mecanismo de Correlação é similar a instalar a aplicação do Gerenciador de Coletor.

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

O arquivo correto da aplicação do Mecanismo de Correlação do VMware possui `vmx` em seu nome. Por exemplo, `sentinel_correlation_engine_7.0.0.0.x86_64.vmx.tar.gz`

2 Estabeleça um armazenamento de dados do ESX onde a imagem da aplicação possa ser instalada.

3 Efetue login como Administrador no servidor em que deseja instalar a aplicação.

4 Especifique o seguinte comando para extrair a imagem compactada da aplicação a partir da máquina onde o VM Converter está instalado:

```
tar zxvf <install_file>
```

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

5 Para importar a imagem VMware no servidor ESX, use o VMware Converter e siga as instruções na tela do assistente de instalação.

6 Efetue login na máquina do servidor ESX.

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

8 Especifique o nome de host/endereço IP do servidor do Sentinel ao qual o Mecanismo de Correlação deverá se conectar.

9 Especifique o número da porta do Servidor de Comunicação. A porta padrão de barramento de mensagem é `61616`.

10 Especifique o nome de usuário do JMS, que é o nome de usuário do Mecanismo de Correlação. O nome de usuário padrão é `correlationengine`.

11 Especifique a senha do usuário do JMS.

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

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

```
correlationengine=<password>
```

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

13 Clique em *Avançar*.

14 Quando solicitado, aceite o certificado.

15 Clique em *Avançar* para concluir a instalação.

Quando a instalação estiver concluída, ela exibirá uma mensagem indicando que essa aplicação é o Mecanismo de Correlação do Sentinel, juntamente com o endereço IP. Ela também exibe o endereço IP da interface do usuário do servidor do Sentinel.

5.3 Instalando a aplicação Xen

5.3.1 Instalando o Sentinel

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

   O nome correto do arquivo da aplicação virtual Xen contém `xen`. Por exemplo, `Sentinel_7.0.0.0.x86_64.xen.tar.gz`

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

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

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

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

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

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

   Por exemplo:

   ```
   # -*- mode: python; -*-
   name="Sentinel_7.0.0.0.x86_64"
   memory=4096
   disk=[ "tap:aio:/var/lib/xen/images/sentinel_7.0.0.0.x86_64/
   sentinel_7.0.0.0.x86_64.raw,xvda,w" ]
   vif=[ "bridge=br0" ]
   ```

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

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

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

   ```
   xm list
   ```

   O VM é exibido na lista que é gerada.

   Por exemplo, se você configurou `name="Sentinel_7.0.0.0.x86_64"` no arquivo `.xenconfig`, então a VM aparecerá com este nome.

8. Para iniciar a instalação, especifique este comando:

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

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

```
xm console Sentinel_7.0.0.0.x86_64
```

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

9. Selecione o idioma desejado e clique em *Avançar*.
10. Selecione o layout do teclado e clique em *Avançar*.
11. Leia e aceite o Contrato de Licença do Software SUSE Linux Enterprise Server (SLES) 11 SP1.
12. Leia e aceite o Contrato de Licença do Usuário Final do NetIQ Sentinel.
13. Na tela Nome de Host e Nome de Domínio, especifique o nome de host e o nome de domínio. Certifique-se de que a opção *Atribuir nome do host ao IP de loopback* esteja selecionada.
14. Selecione *Avançar*. As configurações do nome de host são gravadas.
15. Siga um destes procedimentos:
    - Para usar as configurações de conexão da rede atuais, selecione *Usar a seguinte configuração* na tela *Configuração de Rede II*.
    - Para mudar as configurações de conexão de rede, selecione *Mudar* e faça as mudanças desejadas.
16. Selecione *Avançar*. As configurações de conexão da rede serão gravadas.
17. Defina a data e o horário, clique em *Avançar* e em *Concluir*

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

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

    ```
    rcntp restart
    ```
18. Defina a senha `root` do SUSE Enterprise Server e clique em *Avançar*.
19. Configure a senha do administrador do Sentinel e, em seguida, clique em *Avançar*.

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

    Anote o endereço IP da aplicação, exibido no console.
20. Avance para a Seção 5.5, “Configuração pós-instalação para a aplicação” na página 51.

5.3.2 Instalando o Gerenciador de Coletor

É possível instalar o Gerenciador de Coletor como uma aplicação em um sistema Linux compatível com Xen que atenda aos requisitos mínimos de hardware do Gerenciador de Coletor. Para obter mais informações, consulte a Seção 1.1.2, “Requisitos de hardware” na página 12.

1. Conclua Etapa 1 aEtapa 14 em Seção 5.3.1, “Instalando o Sentinel” na página 45.

   O nome correto do arquivo de instalação da aplicação virtual do Gerenciador de Coletor do Xen é `sentinel_collector_manager_7.0.0.0.x86_64.xen.tar.gz`
2. Na tela Configuração de Rede II, selecione *Alterar* e especifique o endereço IP da máquina virtual em que você deseja instalar a aplicação do Gerenciador de Coletor adicional.

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

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

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

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

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

```
rcntp restart
```

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

7 Especifique o nome de host/endereço IP do servidor do Sentinel ao qual o Mecanismo de Correlação deverá se conectar.

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

9 Especifique o nome de usuário do JMS, que é o nome de usuário do Gerenciador de Coletor. O nome de usuário padrão é `collectormanager`.

10 Especifique a senha do usuário do JMS.

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

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

```
collectormanager=<password>
```

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

12 Selecione *Avançar* para concluir a instalação.

Quando a instalação estiver concluída, ela exibirá uma mensagem indicando que essa aplicação é o Gerenciador de Coletor do Sentinel, juntamente com o endereço IP.

5.3.3 Instalando o Mecanismo de Correlação

É possível instalar o Mecanismo de Correlação como uma aplicação em um sistema Linux compatível com Xen que atenda aos requisitos mínimos de hardware do Mecanismo de Correlação. Para obter mais informações, consulte a Seção 1.1.2, “Requisitos de hardware” na página 12.

1 Conclua Etapa 1 aEtapa 14 em Seção 5.3.1, “Instalando o Sentinel” na página 45.

O nome correto do arquivo de instalação da aplicação virtual do Mecanismo de Correlação do Xen é `sentinel_correlation_engine_7.0.0.0.x86_64.xen.tar.gz`

2 Na tela Configuração de Rede II, selecione *Alterar* e especifique o endereço IP da máquina virtual onde deseja instalar a aplicação do Mecanismo de Correlação adicional.

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

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

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

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

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

```
rcntp restart
```

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

7 Especifique o nome de host/endereço IP do servidor do Sentinel ao qual o Mecanismo de Correlação deverá se conectar.

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

9 Especifique o nome de usuário do JMS, que é o nome de usuário do Mecanismo de Correlação. O nome de usuário padrão é `correlationengine`.

10 Especifique a senha do usuário do JMS.

11 Clique em *Avançar*.

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

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

```
correlationengine=<password>
```

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

13 Quando solicitado, aceite o certificado.

14 Clique em *Avançar* para concluir a instalação.

Quando a instalação estiver concluída, ela exibirá uma mensagem indicando que essa aplicação é o Mecanismo de Correlação do Sentinel, juntamente com o endereço IP. Ela também exibe o endereço IP da interface do usuário do servidor do Sentinel.

5.4 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.

IMPORTANT: A instalação no hardware usando a imagem de disco ISO (bare metal e Hyper-V) exige memória de no mínimo 4,5 GB para a sua conclusão. Para obter mais informações sobre os requisitos de hardware, consulte o Seção 1.1.2, “Requisitos de hardware” na página 12.

5.4.1 Instalando o Sentinel

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

2 Use as instruções na tela do assistente de instalação.

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

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

4. Selecione o idioma desejado e clique em *Avançar*.
5. Selecione o layout do teclado e clique em *Avançar*.
6. Leia e aceite o Contrato de Licença do Software SUSE Enterprise Server.
7. Leia e aceite o Contrato de Licença do Usuário Final do NetIQ Sentinel.
8. Selecione *Avançar*.
9. Na tela Nome de Host e Nome de Domínio, especifique o nome de host e o nome de domínio. Certifique-se de que a opção *Atribuir nome do host ao IP de loopback* esteja selecionada.
10. Selecione *Avançar*. As configurações de nome de host são gravadas.
11. Siga um destes procedimentos:
    - Para usar as configurações atuais de conexão da rede, selecione *Usar a seguinte configuração* na tela Configuração de Rede II.
    - Para mudar as configurações de conexão de rede, selecione *Mudar* e faça as mudanças desejadas.
12. Selecione *Avançar*. As configurações de conexão da rede serão gravadas.
13. Defina a data e o horário e clique em *Avançar*.

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

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

    ```
    rcntp restart
    ```
14. Defina a senha `root` e clique em *Avançar*.
15. Configure a senha do administrador do Sentinel e, em seguida, clique em *Avançar*.
16. Digite o nome de usuário e a senha no console para efetuar login na aplicação.

    O valor padrão para o nome de usuário é `root` e a senha é a senha definida em Etapa 14.
17. Parar o servidor do Sentinel:

    ```
    service sentinel stop
    ```
18. Insira o seguinte comando para redefinir a IU para uma exibição clara no YaST:

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

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

    Poderá levar alguns minutos até que todos os serviços sejam iniciados depois da instalação, pois o sistema executa uma inicialização de uma única vez. Aguarde até que a instalação termine antes de efetuar login no servidor.
20. Anote o endereço IP da aplicação, exibido no console.
21. Avance para a Seção 5.5, “Configuração pós-instalação para a aplicação” na página 51.

5.4.2 Instalando o Gerenciador de Coletor

É possível instalar o Gerenciador de Coletor como uma aplicação em um sistema que atenda aos requisitos mínimos de hardware do Gerenciador de Coletor. Para obter mais informações, consulte a Seção 1.1.2, "Requisitos de hardware" na página 12.

1. Conclua Etapa 1 aEtapa 14 em Seção 5.4.1, "Instalando o Sentinel" na página 48.
2. Especifique o nome de host/endereço IP do servidor do Sentinel ao qual o Gerenciador de Coletor deverá se conectar.
3. Especifique o número da porta do Servidor de Comunicação. A porta padrão de barramento de mensagem é `61616`.

   A instalação tenta conectar ao servidor com as credenciais especificadas. Se qualquer um desses valores tiver sido inserido incorretamente, a instalação exibirá um erro.
4. Especifique o nome de usuário do JMS, que é o nome de usuário do Gerenciador de Coletor. O nome de usuário padrão é `collectormanager`.
5. Especifique a senha do usuário do JMS.
6. Clique em *Avançar*.

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

   ```
   collectormanager=<password>
   ```

   Nesse exemplo, `collectormanager` é o nome de usuário, e o valor correspondente é a senha.
8. Quando solicitado, aceite o certificado.
9. Clique em *Avançar* para concluir a instalação.

   Quando a instalação estiver concluída, ela exibirá uma mensagem indicando que essa aplicação é o Gerenciador de Coletor do Sentinel, juntamente com o endereço IP. Ela também exibe o endereço IP da interface do usuário do servidor do Sentinel.

5.4.3 Instalando o Mecanismo de Correlação

É possível instalar o Mecanismo de Correlação como uma aplicação em um sistema que atenda aos requisitos mínimos de hardware do Mecanismo de Correlação. Para obter mais informações, consulte a Seção 1.1.2, "Requisitos de hardware" na página 12.

1. Conclua Etapa 1 aEtapa 14 em Seção 5.4.1, "Instalando o Sentinel" na página 48.
2. Especifique o nome de host/endereço IP do servidor do Sentinel ao qual o Mecanismo de Correlação deverá se conectar.
3. Especifique o número da porta do Servidor de Comunicação. A porta padrão de barramento de mensagem é `61616`.
4. Especifique o nome de usuário do JMS, que é o nome de usuário do Mecanismo de Correlação. O nome de usuário padrão é `correlationengine`.
5. Especifique a senha do usuário do JMS.
6. Clique em *Avançar*.

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

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

   `correlationengine=<password>`

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

8 Quando solicitado, aceite o certificado.

9 Clique em *Avançar* para concluir a instalação.

   Quando a instalação estiver concluída, ela exibirá uma mensagem indicando que essa aplicação é o Mecanismo de Correlação do Sentinel, juntamente com o endereço IP. Ela também exibe o endereço IP da interface do usuário do servidor do Sentinel.

10 Avance para a Seção 5.5, "Configuração pós-instalação para a aplicação" na página 51.

5.5 Configuração pós-instalação para a aplicação

5.5.1 Instalando o VMware Tools

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

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

5.5.2 Efetuando login na interface da Web da aplicação

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

1 Abra um navegador e efetue login em https://<*endereço_IP*>:8443, onde 8443 é a porta padrão para o servidor do Sentinel. A página do Sentinel é exibida.

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

2 Configure a aplicação do Sentinel para armazenar e coletar dados.

   Para obter mais informações sobre a configuração da aplicação, consulte o *Guia de administração do NetIQ Sentinel 7.0.1*.

3 Registre-se para obter atualizações.

   Para obter mais informações, consulte a Seção 5.9, "Registrando para receber atualizações" na página 53.

5.6 Configuração do WebYaST

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

1. Efetue login na aplicação do Sentinel.
2. Clique em *Aplicação*.
3. Configure o Servidor do Sentinel para receber atualizações, conforme descrito na Seção 5.9, "Registrando para receber atualizações" na página 53.
4. Clique em *Avançar* para concluir a configuração inicial.

5.7 Configurando a aplicação com SMT

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

5.7.1 Pré-requisitos

- Obtenha as credenciais do Novell Customer Center para Sentinel para obter atualizações da Novell. Para obter informações sobre como obter as credenciais, contate Suporte da Novell (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.

5.7.2 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.

5.8 Parando e iniciando o servidor com a interface da Web

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

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

5.9 Registrando para receber atualizações

1. Efetue login na aplicação do Sentinel.
2. Clique em *Aplicação* para iniciar o WebYaST.
3. Clique em *Registro*.

4 Especifique o ID de e-mail no qual deseja receber atualizações e, em seguida, especifique o nome do sistema e o código de registro da aplicação.

5 Clique em *Gravar*.

6 Solucionando problemas da instalação

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

6.1 Falha na instalação devido a configuração de rede incorreta

Durante a primeira inicialização, uma mensagem de erro é exibida se o instalador determinar que as configurações de rede estão incorretas. Se a rede estiver indisponível, a instalação do Sentinel na aplicação falhará.

Para resolver esse problema, defina corretamente as configurações de rede. Para verificar a configuração, use o comando `ipconfig` para retornar o endereço IP válido e o comando `hostname -f` para retornar o nome do host válido.

6.2 O UUID não é criado para Gerenciadores de Coletor em imagens nem para Mecanismos de Correlação

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

É preciso gerar um novo UUID executando as seguintes etapas nos sistemas em que acabou de instalar o Gerenciador de Coletor:

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

   O Gerenciador de Coletor gera automaticamente o UUID.

7 O que acontece em seguida

Depois que o Sentinel estiver instalado, há dois guias para ajudar a configurá-lo: o *Guia de administração do NetIQ Sentinel 7.0.1* e o *Guia do usuário do NetIQ Sentinel 7.0.1*.

O Guia de Administração contém informações sobre tarefas de configuração que apenas um usuário com direitos de administração podem executar. Por exemplo:

- "Configurando usuários e funções"
- "Configurando o armazenamento de dados "
- "Configurando a coleta de dados"
- "Eventos de pesquisa e relatório em um ambiente distribuído"

Para obter mais informações sobre essas e outras tarefas de administração, consulte o *Guia de administração do NetIQ Sentinel 7.0.1*.

O Guia do Usuário contém instruções para ajudar os usuários a executar tarefas no Sentinel. Por exemplo:

- "Pesquisando eventos"
- "Analisando tendências em dados"
- "Gerando relatórios"
- "Configurando incidentes"

Para obter mais informações sobre essas e outras tarefas, consulte o *Guia do Usuário do NetIQ Sentinel 7.0.1*.

Você também pode configurar o Sentinel para analisar seus eventos, adicionar dados usando regras de correlação, definir linhas de base, configurar fluxos de trabalho para atuar nas informações e muito mais. Use as informações no *Guia de administração do NetIQ Sentinel 7.0.1* para ajudar você a configurar esses recursos do Sentinel.

II Configurando

Depois que o Sentinel estiver instalado, será possível configurá-lo para executar em seu ambiente.

8 Acessando a interface da web do Sentinel

Depois que o Sentinel estiver instalado, será possível efetuar login na interface da web do Sentinel para executar tarefas de administração e configurar o Sentinel para coletar dados.

1. Abra um navegador e efetue login em https://<*endereço IP*>:8443, onde 8443 é a porta padrão para o servidor do Sentinel.
2. (Condicional) Na primeira vez que efetuar login no Sentinel, aceite o certificado quando solicitado.

   A página de login do Sentinel é exibida quando você aceita o certificado.
3. Especifique o nome de usuário e a senha do administrador do Sentinel.
4. Clique em *Efetuar Login*.

   A interface da Web do NetIQ Sentinel é exibida.

9 Adicionando novos componentes do Sentinel

Por padrão, o Sentinel tem um Conector e Coletor de Syslog instalados e configurados, bem como diferentes Conectores de Auditoria e diversos coletores de produtos da Novell. A seção a seguir explica como instalar e configurar Conectores e Coletores adicionais.

9.1 Instalando Coletores e Conectores

Por padrão, todos os Coletores e Conectores lançados são instalados quando você instala o Sentinel 7. Se um novo Coletor ou Conector for lançado depois do Sentinel 7, é preciso instalar os arquivos do Coletor ou Conector antes que seja possível configurá-los.

9.1.1 Instalando um Coletor

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

Para configurar o Coletor, consulte a documentação do Coletor específico na página da web de plug-ins do Sentinel (http://support.novell.com/products/sentinel/secure/sentinelplugins.html).

9.1.2 Instalando um Conector

1. Faça o download do Conector correto da página da web de plug-ins do Sentinel (http://support.novell.com/products/sentinel/secure/sentinelplugins.html).
2. Efetue login na interface da web do Sentinel em https://<*endereço IP*>:8443, onde 8443 pe a porta padrão do servidor do Sentinel.
3. Clique em *aplicativos* na barra de ferramentas e, em seguida, em *Aplicativos*.
4. Clique em *Iniciar o Control Center* para iniciar o Sentinel Control Center.
5. Na barra de ferramentas, selecione *Gerenciamento de Fonte de Eventos* > *Tela Ativa* e, em seguida, clique em *Ferramentas* > *Importar plugin*.
6. Procure e selecione o arquivo do Conector cujo download foi feito em Etapa 1 e, em seguida, clique em *Avançar*.
7. Siga as instruções remanescentes e, em seguida, clique em *Concluir*.

Para configurar o Conector, consulte a documentação do Conector específico na página da web de plug-ins do Sentinel (http://support.novell.com/products/sentinel/secure/sentinelplugins.html).

9.2 Adicionando novos Coletores e Conectores

9.2.1 Adicionando novos Coletores

É possível adicionar novos Coletores para normalizar dados de outras origens.

1. Efetue login na interface da web do Sentinel em https://<*endereço IP*>:8443, onde 8443 pe a porta padrão do servidor do Sentinel.
2. Clique em *aplicativos* na barra de ferramentas e, em seguida, em *Aplicativos*.
3. Clique em *Iniciar o Connector Center* para iniciar o Sentinel Control Center.
4. Na barra de ferramentas, selecione *Gerenciamento de Fonte de Eventos* > *Tela Ativa*.
5. Clique com o botão direito do mouse em Gerenciador de Coletor e clique em *Adicionar Coletor*.
6. Selecione seu Coletor na coluna *Fornecedor* e, em seguida, clique em *Avançar*.
7. Os campos são diferentes para cada Coletor, portanto é preciso seguir a documentação do Coletor específico para configurá-lo nesse ponto.

   A documentação do Coletor está localizada na página da web de plug-in do Sentinel (http://support.novell.com/products/sentinel/secure/sentinelplugins.html).

9.2.2 Adicionando novos Conectores

É possível adicionar novos Conectores para obter informações de outras fontes.

1. Efetue login na interface da web do Sentinel em https://<*endereço IP*>:8443, onde 8443 pe a porta padrão do servidor do Sentinel.
2. Clique em *aplicativos* na barra de ferramentas e, em seguida, em *Aplicativos*.
3. Clique em *Iniciar o Control Center* para iniciar o Sentinel Control Center.

4 Na barra de ferramentas, selecione *Gerenciamento de Fonte de Eventos* > *Tela Ativa*.

5 Clique com o botão direito do mouse no Coletor ao qual deseja adicionar o novo Conector e, em seguida, clique em *Adicionar Conector*.

6 Selecione o Conector desejado na coluna *Nome* e, em seguida, clique em *Avançar*.

7 Os campos são diferentes para cada Conector, portanto é preciso seguir a documentação do Conector específico para configurá-lo nesse ponto.

A documentação do Conector está localizada na página da web de plug-in do Sentinel (http://support.novell.com/products/sentinel/secure/sentinelplugins.html).

10 Gerenciando dados

10.1 Estrutura de diretórios

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

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

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

10.2 Consideração sobre armazenamento

Ao armazenar os arquivos de dados do Sentinel, assegure-se de que eles sejam armazenados em uma partição separada dos arquivos de executáveis, configuração e sistema operacional. Os benefícios de armazenar os dados separadamente permite a criação de imagem mais fácil de um conjunto de arquivos e a recuperação em caso de corrompimento. Ele também melhora o desempenho geral de sistemas em que sistemas de arquivos menores são mais eficientes. Para obter mais informações, consulte “Particionamento de disco” (http://en.wikipedia.org/wiki/Disk_partitioning#Benefits_of_multiple_partitions).

Você pode decidir instalar o Sentinel em diversas partições ou em uma única partição, dependendo dos seguintes tipos de instalação:

- Instalação independente
- Instalação da aplicação.

10.2.1 Usando partição em uma instalação independente

Se você estiver instalando o Sentinel como uma instalação independente, poderá modificar o layout da partição do sistema operacional antes de instalar o Sentinel. O administrador deverá criar e montar as partições desejadas para os diretórios adequados com base na estrutura de diretório detalhada em Seção 10.1, "Estrutura de diretórios" na página 67. Ao executar o instalador, o Sentinel é instalado nos diretórios pré-criados, resultando em uma instalação que abrange várias partições.

NOTE:

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

10.2.2 Usando partição em uma instalação da aplicação

Se você estiver instalando o Sentinel usando a instalação da aplicação, não será possível reconfigurar o sistema operacional antes da instalação do Sentinel porque o sistema operacional é instalado juntamente com ele. No entanto, é possível adicionar a partição na aplicação e mover um diretório para a nova partição usando a ferramenta YaST.

O procedimento a seguir cria uma nova partição e move os arquivos de dados de seu diretório para a partição recém-criada:

1. Efetue login no Sentinel como `root`.
2. Execute o seguinte comando para parar o Sentinel na aplicação:

   ```
   /etc/init.d/sentinel stop
   ```
3. Especifique o seguinte comando para mudar para o usuário `novell`:

   ```
   su -novell
   ```
4. Mova o conteúdo do diretório em `/var/opt/novell/sentinel/` para um local temporário.
5. Mude para o usuário `root`.
6. Insira o seguinte comando para acessar o YaST2 Control Center:

   ```
   yast
   ```
7. Selecione *Sistema* > *Particionador*.
8. Leia o aviso e selecione *Sim* para adicionar a nova partição não utilizada.
9. Monte a nova partição em `/var/opt/novell/sentinel`.
10. Especifique o seguinte comando para mudar para o usuário `novell`:

    ```
    su -novell
    ```
11. Mova o conteúdo do diretório de dados do local temporário (onde foi salvo em Etapa 4) de volta para `/var/opt/novell/sentinel/` na nova partição.
12. Mude para o usuário `root`.
13. Execute o seguinte comando para reiniciar a aplicação do Sentinel:

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

11 Configurando conteúdos prontos para instalação

O Sentinel acompanha uma ampla variedade de conteúdos úteis prontos para instalar que você pode usar imediatamente para atender suas necessidades de análise. A maioria desses conteúdos vêm de um Sentinel Core Solution Pack pré-instalado. Para obter mais informações, consulte "Usando pacotes de solução" no *Guia de administração do NetIQ Sentinel 7.0.1*.

O Pacote de Solução permite realizar a categorização e o agrupamento de conteúdos em "controles" ou conjuntos de políticas tratados como uma unidade. Os controles presentes no Sentinel Core Solution Pack são pré-instalados para fornecer a você esse conteúdo pronto para instalação, mas esses controles devem ser implementados ou testados formalmente com a IU da Web do Sentinel.

Se for necessário mostrar que a implementação do Sentinel está funcionando como desejado, use o processo de atestação formal incorporado aos Pacotes de Solução. Esse processo de atestação implementa e testa os controles principais do Sentinel da mesma forma que você faria com qualquer outro Pacote de Solução. Como parte desse processo, o implementador e testador atestarão que eles concluíram o trabalho; em seguida, essas atestações farão parte de uma trilha de auditoria que poderá ser examinada para demonstrar que qualquer controle específico foi corretamente implantado.

Você pode executar o processo de atestação usando o Solution Manager. Para obter mais informações sobre como implementar e testar os controles, consulte "Instalando e gerenciando pacotes de solução" no *Guia de administração do NetIQ Sentinel 7.0.1*.

12 Configurando o horário

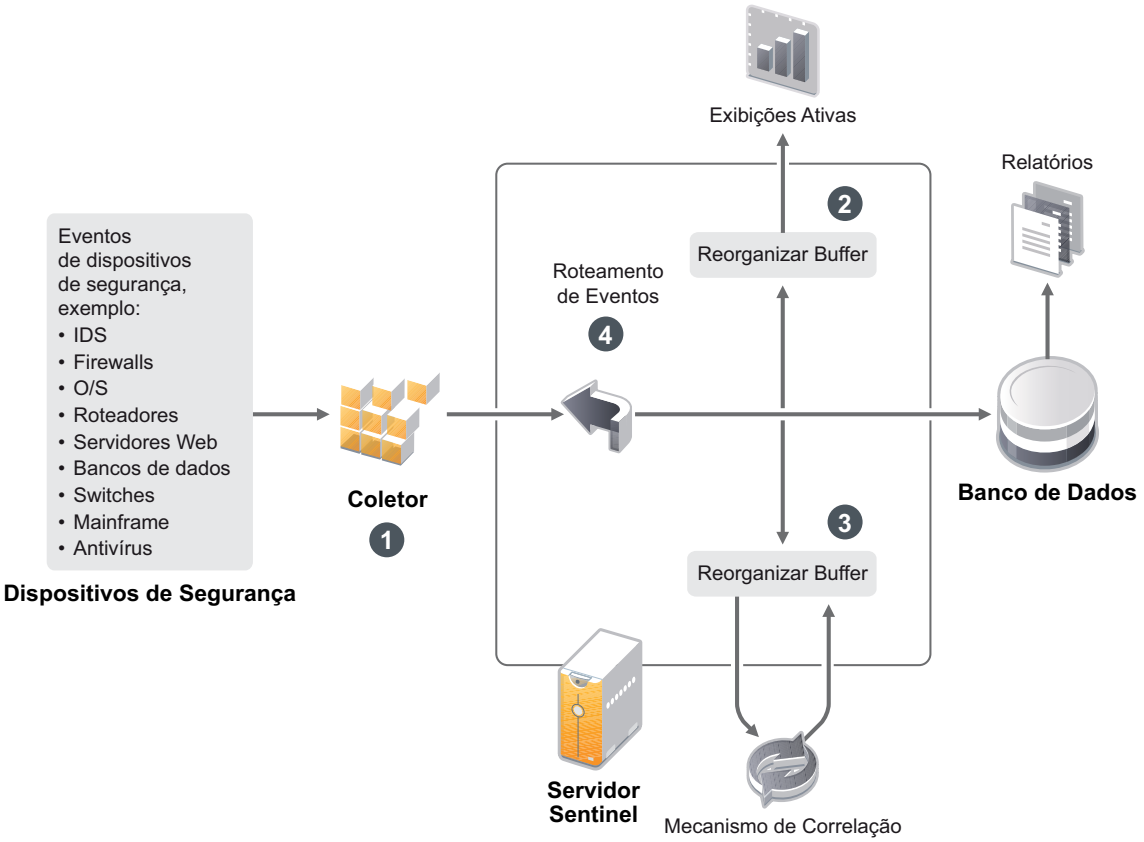
O horário de um evento é vital para seu processamento no Sentinel. É importante para fins de auditoria e geração de relatórios, bem como para o processamento em tempo real.

12.1 Entendendo o horário no Sentinel

O Sentinel é um sistema distribuído que consiste em vários processos que podem ocorrer em partes diferentes da rede. Além disso, pode haver algum atraso introduzido pelo dispositivo. Para lidar com essa situação, os processos do Sentinel reordenam os eventos em um fluxo classificado por horário antes de realizar o processamento.

A ilustração a seguir explica como o Sentinel faz isso:

Figura 12-1 *Horário do Sentinel*



1. Por padrão, o horário do evento é definido para o horário do Gerenciador de Coletor. O horário ideal é o horário da aplicação. Portanto, convém definir o horário do evento como o horário da aplicação se ele estiver disponível, for exato e tiver sido adequadamente analisado pelo Coletor.
2. Eventos são classificados em intervalos de 30 segundos para que possam ser visualizados em Active Views. Por padrão, os eventos que têm uma marcação de horário dentro de um intervalo de 5 minutos do horário do servidor (no passado ou no futuro) são processados normalmente. Os eventos que têm marcações de horário mais de 5 minutos no futuro não são exibidos nas Telas Ativas, mas são inseridos no armazenamento de eventos. Eventos que têm marcações de horário de mais de 5 minutos e menos de 24 horas no passado ainda são exibidos nos gráficos, mas não são exibidos nos dados de evento para aquele gráfico. Uma operação de detalhamento é necessária para recuperar esses eventos do armazenamento de eventos.
3. Se o horário do evento for maior que 30 segundos anterior ao horário do servidor, o Mecanismo de Correlação não processará os eventos.
4. Se o horário do evento for anterior a 5 minutos do horário do Gerenciador de Coletor (horário correto), os eventos serão diretamente encaminhados para o armazenamento de eventos.

12.2 Configurando o horário no Sentinel

O Mecanismo de Correlação processa fluxos de eventos ordenados por horário e detecta padrões nos eventos, bem como padrões temporais no fluxo. No entanto, às vezes o dispositivo que gera o evento poderá não incluir o horário em suas mensagens do registro. Para configurar o horário para que funcione corretamente com o Sentinel, há duas opções:

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

Para alterar essa configuração na fonte de eventos:

1. Efetue login no Gerenciamento de Fonte de Eventos.

   Para obter mais informações, consulte "Acessando o gerenciamento de fonte de eventos" no *Guia de administração do NetIQ Sentinel 7.0.1*.
2. Clique com o botão direito do mouse na fonte de eventos para a qual alterar a configuração de horário e, em seguida, selecione *Editar*.
3. Marque ou desmarque a opção *Confiar na Fonte de Eventos* na parte inferior da guia *Geral*.
4. Clique em *OK* para gravar a mudança.

12.3 Tratando fusos horários

Tratar fusos horários pode se tornar muito completo em um ambiente ditribuido. Por exemplo, você pode ter uma fonte de eventos em um fuso horário, o Gerenciador de Coletor em outro, o servidor back end do Sentinel em outro e o cliente que visualiza os dados em outro. Ao adicionar preocupações como horário de verão e as várias fontes de evento que não relatam para que fuso horário estão configuradas (como todas as fontes de syslog), há muitos problemas possíveis que precisam ser tratados. O Sentinel é flexível, de forma que você possa representar adequadamente o horário quando os eventos ocorrem de fato, e comparar esses eventos a outros eventos de outras fontes em fusos horários iguais ou diferentes.

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

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

No primeiro cenário, é possível calcular o horário UTC absoluto em que um evento ocorreu (presumindo que um protocolo de sincronização de horário esteja em uso), para que você possa facilmente comparar o horário daquele evento a qualquer outra fonte de eventos no mundo. No entanto, não é possível determinar automaticamente qual era o horário local quando o evento ocorreu. Por esse motivo, o Sentinel permite que os clientes definam manualmente o fuso horário de

uma fonte de evento adicionando o nó Fonte de Eventos no Gerenciador de Fontes de evento e especificando o fuso horário apropriado. Essa informação não afeta o cálculo de DeviceEventTime ou EventTime, mas é colocada no campo ObserverTZ e é usada para calcular os vários campos ObserverTZ, como ObserverTZHour. Esses campos são sempre expressos em horário local.

O secundo cenário é o mais simples, em várias formas. Se os IDs em formato longo do horário ou os deslocamentos forem usados, será possível converter facilmente para UTC e obter o horário canônico UTC absoluto (armazenado em DeviceEventTime), mas também é possível calcular facilmente os campos ObserverTZ de horário local. Se um ID em formato curto do fuso horário for usado, há algum potencial para conflitos.

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

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

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

13 Informações sobre licença

Essa seção descreve as várias licenças do Sentinel e fornece informações sobre como gerenciar as licenças.

13.1 Entendendo as licenças do Sentinel

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

13.1.1 Licença de avaliação

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

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

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

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

13.1.2 Licenças corporativas

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

Para fazer alterações no seu licenciamento, contate o gerente da sua conta. Para adicionar a chave de licença ao sistema, consulte Seção 13.2.1, “Adicionando uma Chave de Licença usando a interface da Web” na página 76.

13.2 Adicionando uma Chave de Licença

NOTE: Para adicionar, visualizar ou excluir uma licença, é preciso ter direitos de administrador.

É possível adicionar uma chave de licença usando a interface da web ou por meio da linha de comando.

- Seção 13.2.1, "Adicionando uma Chave de Licença usando a interface da Web" na página 76
- Seção 13.2.2, "Adicionando uma Chave de Licença por meio da Linha de Comando" na página 76

13.2.1 Adicionando uma Chave de Licença usando a interface da Web

1. Efetue login na interface da web do Sentinel como administrador.
2. Clique no link *Sobre* no canto superior esquerdo da página.
3. Clique na guia *Licença*.
4. Na seção Licenças, clique em *Adicionar Licença*.
5. Especifique a chave de licença no campo *Chave*. Depois de especificar a licença, as seguintes informações são exibidas na seção Visualização:

   Recursos: Os recursos que estão disponíveis com a licença.

   Nome do host: Esse campo é somente para uso interno do NetIQ.

   Serial: Esse campo é somente para uso interno do NetIQ.

   EPS: Taxa de evento incorporada à chave de licença. Além dessa taxa, o Sentinel gerará avisos, mas continuará a coletar dados.

   Expira: Data de expiração da licença. É preciso especificar uma chave de licença válida antes da data de expiração para evitar uma interrupção na funcionalidade.
6. Clique em *Gravar*.

13.2.2 Adicionando uma Chave de Licença por meio da Linha de Comando

É possível adicionar a licença por meio da linha de comando usando o script `softwarekey.sh`.

1. Efetue login no servidor do Sentinel como `root`.
2. Acesse o diretório `/opt/novell/sentinel/bin`.
3. Especifique o seguinte comando para mudar para o usuário novell:

   ```
   su novell
   ```
4. Especifique o seguinte comando para executar o script `softwarekey.sh`.

   ```
   ./softwarekey.sh
   ```
5. Digite 1 para inserir a chave de licença.
6. Especifique a chave de licença e pressione Enter.

14 Configurando o Sentinel para alta disponibilidade

O Sentinel foi testado e certificado para trabalhar em um ambiente de alta disponivbilidade, e suporta arquiteturas de recuperação de desastres. O NetIQ Consulting e os parceiros do NetIQ podem ajudar você a implementar a alta disponibilidade e a recuperação de desastres do Sentinel.

Para ativar os servidores do Sentinel para alta disponibilidade, é preciso do seguinte:

- Nós do Sentinel redundantes em cluster.
- Acesso ao armazenamento de dados compartilhado.
- Endereços IP virtuais que possam ser usados para mudar transparentemente de um nó com falha para outro nó.
- Scrips para iniciar, parar e monitorar o aplicativo com base em políticas definidas em suas soluções de cluster. É possível usar soluções de cluster, como Cluster Resource Agents ou scripts LSB init em sistemas Linux Enterprise High Availability.

Há muitos pacotes no mercado que possibilitam a alta disponibilidade. O teste para o Sentinel foi realizado com o *SUSE Linux Enterprise High Availability (HA) Extension* (http://www.novell.com/products/highavailability/), unidades RAID de armazenamento compartilhado e scripts personalizados. Essa arquitetura pode ser replicada em centros de dados para garantir a disponibilidade de tudo, desde o servidor do Sentinel aos Gerenciadores de Coletor e os Coletores.

A alta disponibilidade para fontes de evento devem ser consideradas caso a caso, por causa da ampla variedade de dispositivos que podem ser usados.

III Fazendo upgrade do Sentinel

15 Fazendo upgrade do servidor Sentinel

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

   Para obter mais informações sobre o backup de dados, consulte "Fazendo backup e restaurando dados" no *Guia de administração do NetIQ Sentinel 7.0.1*.

2. Faça download do instalador mais recente no site de download da Novell (http://download.novell.com).

3. Efetue login como `root` no servidor em que você deseja fazer upgrade do Sentinel.

4. Especifique o seguinte comando para extrair os arquivos de instalação do arquivo tar:

   ```
   tar xfz <install_filename>
   ```

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

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

6. Especifique o seguinte comando para fazer upgrade do Sentinel:

   ```
   ./install-sentinel
   ```

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

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

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

9. O script de instalação detecta que uma versão mais antiga do produto já existe e solicita que você especifique se deseja fazer upgrade do produto. 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.

10. (Condicional) Para fazer upgrade dos sistemas do Gerenciador de Coletor, consulte Capítulo 17, "Fazendo upgrade do Gerenciador de Coletor" na página 85.

11. (Condicional) Para fazer upgrade do sistema do Mecanismo de Correlação, consulte Capítulo 18, "Fazendo upgrade do Mecanismo de Correlação" na página 87.

16 Fazendo upgrade da aplicação Sentinel

Esse procedimento orienta você a fazer upgrade da Aplicação Sentinel como Aplicações Gerenciador de Coletor e Mecanismo de Correlação.

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

   Para obter mais informações sobre o backup de dados, consulte "Fazendo backup e restaurando dados" no *Guia de administração do NetIQ Sentinel 7.0.1*.
5. (Condicional) Se você ainda não tiver registrado o aplicativo para atualizações automáticas, registre-o.

   Para obter mais informações, consulte a Seção 5.9, "Registrando para receber atualizações" na página 53.

   Se o aplicativo não estiver registrado, um aviso amarelo será exibido, indicando que o aplicativo não está registrado.
6. Para verificar se existem atualizações disponíveis, clique em *Atualizações*.

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

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

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

   Para obter mais informações, consulte Seção 5.8, "Parando e iniciando o servidor com a interface da Web" na página 53.

17 Fazendo upgrade do Gerenciador de Coletor

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

   Para obter mais informações, consulte "Fazendo backup e restaurando dados" no *Guia de administração do NetIQ Sentinel 7.0.1*.
2. Efetue login na interface da Web do Sentinel como usuário na função de administrador.
3. Selecione *Downloads*.
4. Clique no *Download do Instalador* na seção Instalador do Gerenciador do Coletor.

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

   ./install-cm
9. Siga as instruções na tela para completar a instalação.

18 Fazendo upgrade do Mecanismo de Correlação

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

   Para obter mais informações, consulte "Fazendo backup e restaurando dados" no *Guia de administração do NetIQ Sentinel 7.0.1*.
2. Efetue login na interface da Web do Sentinel como usuário na função de administrador.
3. Selecione *Downloads*.
4. Clique em *Download do Instalador* na seção Instalador do Mecanismo de Correlação.

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

   ./install-ce
9. Siga as instruções na tela para completar a instalação.

19 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.

IV Migrando

20 Cenários de migração suportados

Para essa versão do Sentinel, não há cenários de migração suportados. É preciso fazer uma nova instalação do Sentinel, em vez de uma migração ou uma atualização. No entanto, uma ferramenta para migrar dados será lançada em breve.

Para obter instruções, consulte Capítulo 2, “Instalando o Sentinel” na página 23.

21 O que acontece em seguida

Depois que o Sentinel estiver instalado, há dois guias para ajudar a configurá-lo: o *Guia de administração do NetIQ Sentinel 7.0.1* e o *Guia do usuário do NetIQ Sentinel 7.0.1*.

O Guia de Administração contém informações sobre tarefas de configuração que apenas um usuário com direitos de administração podem executar. Por exemplo:

- "Configurando usuários e funções"
- "Configurando o armazenamento de dados "
- "Configurando a coleta de dados"
- "Eventos de pesquisa e relatório em um ambiente distribuído"

Para obter mais informações sobre essas e outras tarefas de administração, consulte o *Guia de Administração do NetIQ Sentinel 7.0.1*.

O Guia do Usuário contém instruções para ajudar os usuários a executar tarefas no Sentinel. Por exemplo:

- "Pesquisando eventos"
- "Analisando tendências em dados"
- "Gerando relatórios"
- "Configurando incidentes"

Para obter mais informações sobre essas e outras tarefas, consulte o *Guia do Usuário do NetIQ Sentinel 7.0.1*.

Você também pode configurar o Sentinel para analisar seus eventos, adicionar dados usando regras de correlação, definir linhas de base, configurar fluxos de trabalho para atuar nas informações e muito mais. Use as informações no *Guia de administração do NetIQ Sentinel 7.0.1* para ajudar você a configurar esses recursos do Sentinel.

V Desinstalação

O Sentinel é desinstalado realizando as seguintes tarefas:

- Capítulo 22, “Desinstalando o Sentinel” na página 99
- Capítulo 23, “Tarefas pós-desinstalação” na página 101

22 Desinstalando o Sentinel

Um script de desinstalação está disponível para ajudá-lo a remover uma instalação do Sentinel. Vários arquivos, incluindo arquivos de registro, são preservados e podem ser removidos manualmente, caso desejado. Antes de realizar uma nova instalação, você deverá executar todas as etapas a seguir para verificar se não restaram arquivos ou configurações do sistema de uma instalação anterior.

WARNING: Essas instruções envolvem a modificação de configurações e arquivos do sistema operacional. Se você não estiver familiarizado com a modificação dessas configurações e arquivos do sistema, contate o administrador do sistema.

22.1 Desinstalando o Sentinel Server

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

   NOTE: Você não pode desinstalar o servidor Sentinel como usuário não root quando a instalação é realizada como usuário `root`. No entanto, o usuário não root pode desinstalar o servidor Sentinel quando a instalação é executada pelo usuário não root.

2. Acesse o seguinte diretório:

   ```
   /opt/novell/sentinel/setup/
   ```

3. Execute o seguinte comando:

   ```
   ./uninstall-sentinel
   ```

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

   O script primeiro para o serviço e, em seguida, remove-o completamente.

22.2 Desinstalando o Gerenciador de Coletor remoto ou o Mecanismo de Correlação

1. Efetue login como `root`.

NOTE: Você não pode desinstalar o Gerenciador de Coletor Remoto nem o Mecanismo de correlação remota como usuário não root quando a instalação é executada como usuário `root`. No entanto, o usuário não root pode desinstalar quando a instalação é executada pelo usuário não root.

2. Vá para o seguinte local:

   ```
   /opt/novell/sentinel/setup
   ```

3. Execute o seguinte comando:

   ```
   ./uninstall-sentinel
   ```

   O script exibe um aviso informando que o Gerenciador de Coletor ou o Mecanismo de correlação e todos os dados associados serão completamente removidos.

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

   O script primeiro para o serviço e, em seguida, remove-o completamente.

23 Tarefas pós-desinstalação

NOTE: A desinstalação do Sentinel Server não remove do sistema operacional o Usuário Administrador do Sentinel. Se desejar remover esse usuário, você deverá fazê-lo manualmente.

23.1 Removendo as configurações do Sentinel

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

Para limpar manualmente as configurações do sistema Sentinel:

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

   ```
   userdel -r novell
   ```

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

23.1.1 Concluindo a desinstalação do Mecanismo de Correlação

Depois de executar o script de desinstalação para desinstalar o Mecanismo de Correlação, o ícone do Mecanismo de Correlação ainda será exibido em estado inativo na interface da Web. É preciso executar as seguintes etapas adicionais para apagar manualmente o Mecanismo de Correlação na interface da Web:

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

23.1.2 Concluindo a instalação do Gerenciador de Coletor

Depois de executar o script de desinstalação para desinstalar o Gerenciador de Coletor, o ícone do Gerenciador de Coletor ainda será exibido em estado inativo na interface da Web. É preciso executar as seguintes etapas adicionais para apagar manualmente o Gerenciador de Coletor na interface da Web:

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