Guia de Inicialização Rápida do NetIQ Sentinel 7.0.1

Março de 2012

Novell®

Introdução

Use as seguintes informações para instalar e executar o Sentinel rapidamente.

Atendendo aos requisitos do sistema

Verifique se você possui os requisitos mínimos para instalar o Sentinel.

Requisitos de hardware para 500 EPS:

- **Memória:** 6.7 GB
- **Disco rígido:** Drivers com 4 x 500 GB e 7,2K RPM em execução no RAID 1 com cache de 256 MB ou uma área de armazenamento equivalente (SAN)
- **Processadores:** CPU Intel Xeon X5470 de 3,33 GHz (4 núcleos)

Sistemas operacionais:

- SUSE Linux Enterprise Server (SLES) 11 SP1
- Red Hat Enterprise Linux (RHEL) 6

Máquinas virtuais:

- VMWare ESX 4.0
- Xen 4.0
- Hyper-V Server 2008 R2 - somente arquivo DVD ISO

DVD ISO:

- Hyper-V Server 2008 R2
- Hardware sem um sistema operacional instalado

Para os requisitos de hardware, se o EPS estiver acima ou abaixo de 500, consulte “Atendendo aos requisitos do sistema” no *Guia de Instalação e Configuração do NetIQ Sentinel 7.0.1*.

Instalando o Sentinel

Você pode instalar o Sentinel como uma instalação autônoma ou como uma instalação de aplicação.

Instalando no Hardware

A instalação padrão do Sentinel instala todos os componentes do Sentinel na máquina. Para executar uma instalação personalizada ou instalar o Sentinel como um usuário que não seja `raiz`, consulte “Instalando o Sentinel” no *Guia de Instalação e Configuração do NetIQ Sentinel 7.0.1*.

Para instalar o Sentinel:

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. Use o seguinte comando para extrair o arquivo de instalação:

```
tar xfz <install_filename>
```

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

3. Use o seguinte comando para executar o script `install-sentinel`:

```
./install-sentinel
```

4. Especifique o número do idioma desejado para executar a instalação e pressione Enter.

   O valor padrão é 3 para Inglês.

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

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

6. Digite `sim` ou `s` para aceitar a licença e continuar a instalação.

   A instalação pode levar alguns minutos para ser concluída.

7. Quando solicitado, digite 1 para continuar a instalação padrão do Sentinel 7.0.

8. Especifique uma senha duas vezes para a conta admin padrão criada durante a configuração.

Para obter informações detalhadas, consulte "Instalando o Sentinel" no *Guia de Instalação e Configuração do NetIQ Sentinel 7.0.1*.

Instalando a Aplicação

A aplicação está disponível para as plataformas virtuais VMware ESX, Xen e Hyper-V. Você também pode instalar a aplicação no hardware. As seguintes instruções se referem ao servidor VMware ESX. Para obter instruções sobre outras plataformas, consulte "Instalando a aplicação" no *Guia de Instalação e Configuração do NetIQ Sentinel 7.0.1*.

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

   O arquivo correto da aplicação VMware possui `vmx` em seu nome.

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. Use o seguinte comando para extrair a imagem compactada da aplicação na máquina em que 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 Novell SUSE Linux Enterprise Server.

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.

13. Certifique-se de que a opção *Assign Hostname to Loopback IP* (Atribuir nome de host a IP de loopback) esteja selecionada.

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

15. Siga um destes procedimentos:

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

16. Clique em *Avançar* para salvar as configurações de conexão de rede.

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 `raiz` do Novell SUSE Linux Enterprise Server e clique em *Avançar*.

19. Defina a senha `raiz` e clique em *Avançar*.

20. Defina a senha admin e a senha dbauser do Sentinel e clique em *Avançar*.

21. Clique em *Avançar*. As configurações de conexão da rede serão gravadas.

    Quando a instalação for concluída, anote o endereço IP da aplicação exibido no console.

Para obter informações de configuração pós-instalação, consulte "Configuração Pós-instalação da Aplicação" no *Guia de Instalação e Configuração do NetIQ Sentinel 7.0.1*.

Acessando a interface da web do Sentinel

Após a instalação do Sentinel, o próximo passo é acessar a interface da web do Sentinel para executar tarefas de administração e configurar o Sentinel para coletar dados.

Para acessar a interface da web, especifique o seguinte URL no seu browser da web:

`https://<Endereço_IP_do_servidor_Sentinel>:8443`

A porta 8443 é o valor padrão.

Coletando dados

A coleta de dados é executada por Conectores e Coletores. Por padrão, o Sentinel possui alguns Conectores e Coletores instalados e configurados.

Por padrão, há servidores syslog SSL, UDP e TCP instalados no servidor Sentinel. Se você estiver usando a aplicação, os servidores syslog serão automaticamente configurados quando começarem a receber eventos do arquivo syslog local.

É possível configurar dispositivos syslog, como um servidor Linux, para enviar informações para esses servidores syslog. Além disso, você pode configurar Conectores adicionais para permitir que o Sentinel colete dados.

- "Configurando um servidor Linux para enviar informações de syslog para o Sentinel" na página 3
- "Configurando a coleta de dados para Windows" na página 3
- "Configurando Conectores e Coletores adicionais" na página 5

Configurando um servidor Linux para enviar informações de syslog para o Sentinel

O servidor Sentinel contém um servidor de eventos de syslog pré-configurado que está escutando conexões de entrada em uma destas portas:

- **TCP:** 1468
- **UDP:** 1514
- **SSL:** 1443

Use as seguintes informações para configurar um servidor Linux para enviar eventos para o servidor de origem dos eventos de syslog TCP.

Para configurar o arquivo syslog no Linux:

1. Abra o arquivo `/etc/syslog-ng/syslog-ng.conf`.
2. Adicione as seguintes linhas de código ao final do arquivo `syslog-ng.conf`.

```
# Forward all messages to Sentinel:
#
destination d_slm { tcp("127.0.0.1"
port(1468)); };
log { source(src); destination(d_slm); };
```

3. Mude o valor de TCP no endereço IP do servidor Linux.
4. Salve o arquivo e feche-o.
5. Reinicie o serviço syslog:

```
/etc/init.d/syslog restart
```

Para obter detalhes sobre como configurar os dispositivos para enviar informações para o Conector de Syslog, consulte a documentação do Conector de Syslog na página da web Sentinel Plug-ins (http://support.novell.com/products/sentinel/secure/sentinelplugins.html).

Configurando a coleta de dados para Windows

Se você tiver um sistema Windows do qual deseja coletar dados, será necessário configurar um Conector de Eventos do Windows (WMI). O Conector de Eventos do Windows (WMI) é instalado no Gerenciador de Coletor e recebe eventos do Serviço de Coleta de Eventos do Windows instalado no servidor Windows.

- "Configurando o Conector de Eventos do Windows" na página 3
- "Instalando o Serviço de Coleta de Eventos do Windows no servidor Windows" na página 4
- "Configurando o Serviço de Coleta de Eventos do Windows" na página 5

Configurando o Conector de Eventos do Windows

1. Efetue login na interface da web do Sentinel.

   `https://<Endereço_IP_do_servidor_Sentinel>:8443`

   A porta 8443 é a porta padrão.
2. Clique em *Aplicativos* na barra de ferramentas e clique em *Iniciar Control Center*.
3. Efetue login no Sentinel Control Center usando seu nome de usuário e senha administrativos e clique em *Efetuar Login*.
4. Na barra de ferramentas, clique em *Gerenciamento de Origem de Evento* > *Tela Ativa*.
5. Adicione um Coletor específico para Windows ao Gerenciador de Coletor.

É necessário ter um Coletor específico para Windows configurado antes de adicionar o Conector de Eventos do Windows.

5a Clique com o botão direito do mouse em Gerenciador de Coletor e clique em *Adicionar Coletor*.

5b Selecione *Mircosoft* na coluna *Fornecedor* e, em seguida, selecione sua versão do Windows ou do Active Directory na coluna *Versão*.

5c Clique em *Avançar*.

5d Selecione os scripts que deseja visualizar e clique em *Avançar*.

5e Mude os parâmetros da configuração e clique em *Avançar*.

5f Defina parâmetros de configuração adicionais para o Coletor e clique em *Concluir*.

6 Adicione o Conector de Eventos do Windows ao Coletor que você criou em Etapa 5:

6a Clique com o botão direito do mouse no Coletor e clique em *Adicionar Conector*.

6b Selecione o Conector de Eventos do Windows e clique em *Avançar*.

6c Defina as configurações de rede para o servidor do Conector de Eventos do Windows e clique em *Avançar*.

6d Defina as configurações SSL e clique em *Avançar*.

6e Selecionar como o Conector de Eventos do Windows é gerenciado:

- **Manualmente:** Selecione esta opção para gerenciar manualmente a origem do evento.
- **Automaticamente:** Selecione esta opção para sincronizar automaticamente com o Active Directory.

6f Clique em *Avançar*.

6g Especifique as credenciais de usuário utilizadas para conectar ao Serviço de Coleta de Eventos do Windows e à origem do evento.

6h Especifique os parâmetros de configuração e clique em *Concluir*.

7 Adicione uma origem de evento para os sistemas Windows de onde você deseja coletar dados.

7a Clique com o botão direito do mouse em Conector de Eventos do Windows e clique em *Adicionar Origem do Evento*.

7b Especifique o endereço IP ou o nome do host do sistema Windows

ou

Selecione um sistema Windows do Active Directory e clique em *Avançar*.

7c Selecione um modo de conexão para a origem do evento e clique em *Avançar*.

7d Especifique os parâmetros de configuração para a origem do evento e clique em *Concluir*.

Instalando o Serviço de Coleta de Eventos do Windows no servidor Windows

1 Verifique se você criou uma conta de usuário no servidor Windows com os direitos apropriados para executar o Serviço de Coleta de Eventos do Windows e para coletar eventos nos registros de Eventos do Windows dos sistemas remotos Windows. Os direitos são:

- Permissão para acessar os registros de Eventos do Windows
- Permissões WMI
- Permissões DOCM
- Direitos de leitura, gravação e exclusão da ACL devem ser atribuídos ao grupo Usuários COM Distribuídos para todos os tipos de registros de eventos.
- Permissão de leitura para o registro de evento de segurança
- O usuário deve ter privilégios administrativos para instalar o Agente do Windows
- O usuário deve ter o direito *Efetuar login como serviço*.

Para obter mais informações, consulte a documentação do Conector de Eventos do Windows na página da web Sentinel Plug-ins (http://support.novell.com/products/sentinel/secure/sentinelplugins.html). As informações sobre permissões estão nos capítulos 4 e 5.

2 Copie o arquivo `WindowsEvent-CollectionService.msi` do arquivo `.zip` do Conector de Eventos do Windows para o servidor Windows no qual deseja instalar o Serviço de Coleta de Eventos do Windows.

3 Clique duas vezes no arquivo `WindowsEvent-CollectionService.msi` para iniciar o Assistente de Configuração do Serviço de Coleta de Eventos do Windows.

4 Na tela Boas-vindas, clique em *Avançar*.

5 (Condicional) Leia o aviso de limitação de suporte e clique em *Avançar*.

6 Aceite a licença de usuário final e clique em *Avançar*.

7 Use as seguintes informações para personalizar a configuração do Serviço de Coleta de Eventos do Windows:

Recursos adicionais: Selecione os recursos que você deseja instalar. Nem todos os recursos são instalados por padrão. Os recursos são:

- **Serviço de coleta:** Instala o Serviço de Coleta de Eventos do Windows que se comunica com o Sentinel.
- **Documentação:** Instala a documentação fornecida com o Conector.

Localização: (Opcional) Mude o local de instalação padrão clicando em *Procurar* e selecionando um novo local. O local de instalação padrão é `Program Files\Novell\SentinelWECS`.

Utilização do Disco: (Opcional) Clique em *Utilização do Disco* para saber se há espaço suficiente em disco para instalar o Serviço de Coleta de Eventos do Windows.

8 Clique em *Avançar*.

9 Defina a conta de serviço que o Serviço de Coleta de Eventos do Windows usa para conectar-se a origens de eventos externas do Windows.

Conta de Sistema Local: Selecione esta opção para executar o Serviço de Coleta de Eventos do Windows como um usuário de Conta do Sistema Local. Se selecionar essa opção, será necessário especificar as credenciais de usuário ao implantar o Conector de Eventos do Windows no Gerenciador de Coletor.

Nome desta conta: Selecione esta opção para executar o Serviço de Coleta de Eventos do Windows como um usuário ou um usuário de domínio específico. Use as credenciais do usuário que possui direitos para executar o Serviço de Coleta de Eventos do Windows.

O sistema do Serviço de Coleta de Eventos do Windows deve ter acesso de leitura para o registro de eventos do Windows em cada sistema de origem de evento a ser monitorado. Assim, os usuários criados devem ter permissões apropriadas atribuídas em cada sistema de origem de evento.

Iniciar o serviço instalado: Selecione esta opção se desejar que o Serviço de Coleta de Eventos do Windows seja iniciado assim que a instalação for concluída.

10 Clique em *Avançar*.

11 Clique em *Instalar* para instalar o Serviço de Coleta de Eventos do Windows.

12 Clique em *Concluir* para sair do assistente de configuração.

Após a instalação do Serviço de Coleta de Eventos do Windows, será necessário configurá-lo.

Configurando o Serviço de Coleta de Eventos do Windows

1 Abra o arquivo `eventManagement.config` usando um editor de arquivos.

O local padrão do arquivo é `Program Files\Novell\SentinelWECS`.

2 Na seção <`cliente`>, copie a linha `endereço de endPoint` e cole-a abaixo da linha existente. Substitua o endereço IP existente pelo endereço IP do servidor (Gerenciador de Coletor) ao qual o Serviço de Coleta de Eventos do Windows se conecta e o número da porta pela qual ele se comunica com o Conector.

Por exemplo:

```
<client>
    <!-- Additional collectors/plugins can be
added with different host/
port configurations -->
     <!-- <endPoint address="tcp://
127.0.0.1:1024"
behaviorConfiguration="localhost" />-->
     <endPoint address="tcp://
<IP_address_Sentinel_server:<port_number>"
behaviorConfiguration="localhost" />-->
  </client>
```

3 Você pode configurar quantos Conectores desejar repetindo Etapa 2. Você pode configurar um agente para vários conectores ou um agente para um Conector.

4 Salve e feche o arquivo `eventManagement.config`.

5 Abra a janela Serviço para iniciar o Serviço de Coleta de Eventos do Windows.

5a Clique em *Iniciar* > *Executar* para abrir a caixa de diálogo Executar.

5b Digite `services.msc` e clique em *OK*.

6 Selecione *Serviço de Conexão de Eventos do Windows ao Sentinel*, clique com o botão direito do mouse e selecione *Iniciar* para iniciar o Serviço de Coleta de Eventos do Windows.

7 Feche a janela Serviço.

Para obter mais informações sobre o Microsoft Active Directory, o Coletor do Windows Collector e o Conector de Eventos do Windows (WMI), consulte a página da web Sentinel Plug-ins (http://support.novell.com/products/sentinel/secure/sentinelplugins.html).

Configurando Conectores e Coletores adicionais

Os Conectores e Coletores disponíveis são instalados no servidor Sentinel durante a instalação do Sentinel. Contudo, Conectores e Coletores novos e atualizados estão disponíveis com frequência.

Visite a página da web Sentinel Plug-ins (http://support.novell.com/products/sentinel/secure/sentinelplugins.html) para obter as versões atualizadas de Conectores e Coletores.

Se precisar configurar um Conector ou Coletor que não seja configurado por padrão, consulte “Incluindo Componentes Adicionais do Sentinel” no *Guia de Instalação e Configuração do NetIQ Sentinel 7.0.1*.

O que acontece em seguida

Neste ponto, o Sentinel já está instalado. Há dois guias para ajudar a configurar o Sentinel: 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 usuários executarem 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 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 ajudá-lo a configurar esses recursos do Sentinel.