Novell Sentinel

6.0

www.novell.com

VOLUME I - GUIA DE INSTALAÇÃO

Apr. 30, 2007

Novell®

Informações Legais

A Novell, Inc., não faz nenhuma representação ou garantia com relação ao conteúdo ou uso desta documentação e especificamente se isenta de qualquer garantia expressa ou implícita de comercialização ou adequação a um propósito específico. Além disso, a Novel, Inc., se reserva o direito de revisar esta publicação e fazer mudanças no conteúdo, a qualquer momento, sem obrigação de notificar nenhum pessoa ou entidade sobre essas revisões ou mudanças.

A Novell, Inc., não faz nenhuma representação ou garantia com relação a nenhum software e especificamente se isenta de qualquer garantia expressa ou implícita de comercialização ou adequação a um propósito específico. Além disso, a Novell, Inc., se reserva o direito de fazer mudanças em qualquer ou todas as partes do software Novell, a qualquer momento, sem nenhuma obrigação de notificar nenhuma pessoa ou entidade sobre essas mudanças.

Qualquer produto ou informação técnica fornecida sob este Contrato pode estar sujeita aos controles de exportação dos Estados Unidos e leis de comércio de outros países. Você concorda em atender a todos os regulamentos de controle de exportação e para obter qualquer licença necessária ou classificação para exportar, reexportar ou importar produtos. Você concorda em não exportar ou reexportar para entidades nas listas de exclusão de exportação dos Estados Unidos atuais ou para países terroristas ou com embargo conforme especificado nas leis de exportação dos Estados Unidos. Você concorda em não usar produtos para fins proibidos relacionados a armas nucleares, biológicas e químicas ou mísseis. Veja a página da Web Novell International Trade Services (http://www.novell.com/info/exports/) para obter mais informações sobre exportação do software Novell. A Novell não assume nenhuma responsabilidade por sua falha em obter quaisquer aprovações de exportação necessárias.

A Novell, Inc., tem direitos de propriedade intelectual relacionados à tecnologia incorporada no produto descrito neste documento. Em particular, e sem limitação, esses direitos de propriedade intelectual podem incluir uma ou mais das patentes dos Estados Unidos listadas na página da Web Novell Legal Patents (http://www.novell.com/company/legal/patents/) e uma ou mais patentes adicionais ou solicitações de patente pendentes nos Estados Unidos e em outros países.

Novell, Inc.
404 Wyman Street, Suite 500
Waltham, MA 02451
EUA
www.novell.com

Documentação Online: Para acessar a mais recente documentação online referente a este e a outros produtos da Novell, consulte a página da Web de Documentação da Novell (http://www.novell.com/documentation).

Marcas Registradas da Novell

Para ver marcas registradas da Novell, consulte a lista de Marcas registradas e Marcas de Serviço da Novell (http://www.novell.com/company/legal/trademarks/tmlist.html).

Materiais de Terceiros

Todas as marcas registradas de terceiros são de propriedade de seus respectivos donos.

Índice

Prefácio 9

1 Introdução 11

1.1 Visão geral do Sentinel . . . 11
1.1.1 Sentinel Server . . . 13
1.1.2 Servidor de Comunicação do Sentinel . . . 13
1.1.3 Mecanismo de Correlação . . . 13
1.1.4 Workflow de iTRAC . . . 13
1.1.5 Banco de Dados do Sentinel . . . 13
1.1.6 Gerenciador do Coletor do Sentinel . . . 14
1.1.7 Coletores do Sentinel . . . 14
1.1.8 Sentinel Control Center . . . 14
1.1.9 Construtor de Coletor do Sentinel . . . 15
1.1.10 Gerenciador de Dados do Sentinel . . . 15
1.1.11 Crystal Reporting Server . . . 15
1.1.12 Sentinel Advisor . . . 15
1.1.13 Integração com Terceiros . . . 15
1.2 Suporte de idiomas . . . 15
1.3 Outras referências da Novell . . . 16
1.4 Entrar em Contato com a Novell . . . 16

2 Melhores práticas 17

2.1 Plataformas Suportadas . . . 17
2.1.1 Sistemas operacionais . . . 17
2.1.2 Bancos de Dados . . . 17
2.1.3 Servidor de Relatório . . . 18
2.1.4 Pilhas suportadas . . . 18
2.2 Recomendações de hardware . . . 18
2.2.1 Arquitetura . . . 19
2.3 Benchmarks de Desempenho . . . 22
2.3.1 Prova de conceito ou Configuração de demonstração . . . 23
2.3.2 Configuração do Sistema de Produção - Opção 1 . . . 24
2.3.3 Configuração do Sistema de Produção - Opção 2 . . . 25
2.4 Configuração de matriz de disco . . . 26
2.4.1 Requisito mínimo para instalação empresarial (1000 EPS ou mais) . . . 26
2.4.2 Configuração otimizada . . . 26
2.4.3 Exemplo de configuração de armazenamento para uma instalação do Microsoft SQL . . . 27
2.4.4 Exemplo de configuração de armazenamento para uma instalação do Oracle . . . 28
2.5 Configuração de rede . . . 28
2.6 Melhor Prática-Instalação/Configuração de Banco de Dados . . . 29
2.6.1 Patches do Banco de Dados do Sentinel . . . 29
2.6.2 Configurações do Kernel do UNIX recomendadas para Oracle . . . 30
2.6.3 Configura Parâmetros ao criar sua própria instância do banco de dados. . . . 30
2.7 Instalação e configuração do Sentinel . . . 32
2.8 Definindo senhas - melhores práticas . . . 33
2.9 Configuração de Relatórios . . . 34
2.9.1 Relatórios fornecidos com o Sentinel . . . 35
2.9.2 Dicas ao desenvolver Crystal Reports personalizados . . . 36

2.10 Manutenção do Banco de Dados . . . 36
2.10.1 Informações de eventos no banco de dados . . . 36
2.10.2 Outras informações no banco de dados . . . 36
2.10.3 Manutenção de banco de dados adicional . . . 37
2.10.4 Verificação de saúde de banco de dados para Oracle . . . 38
2.10.5 Manutenção do Banco de Dados . . . 40
2.11 Mecanismo de Correlação . . . 40
2.11.1 Sincronização de horário . . . 40
2.11.2 Uso da memória . . . 40
2.11.3 Análise de curto-circuito . . . 40
2.11.4 Regras de formato livre . . . 41
2.12 Arquivos de registro do Sentinel . . . 41

3 Instalando o Sentinel 6 43

3.1 Instalar o Sentinel no Linux, Solaris e Windows . . . 43
3.1.1 Configuração do Sentinel . . . 43
3.1.2 Pré-requisitos para instalar Sentinel 6.0 . . . 45
3.2 Instale o Oracle no Linux, SUSE Linux, Redhat Linux e Solaris . . . 48
3.2.1 Definir valores do Kernel . . . 48
3.2.2 Criar Grupo e Conta de Usuário do Oracle no Solaris . . . 50
3.2.3 Definindo variáveis de ambiente para Oracle no Solaris . . . 50
3.2.4 Verificar o layout do Solaris . . . 50
3.2.5 Instalação do Oracle . . . 51
3.3 Instalando o Sentinel . . . 57
3.3.1 Instalação Simples . . . 58
3.3.2 Instalação Personalizada . . . 60
3.4 Configuração de pós-instalação . . . 70
3.4.1 Atualizando o e-mail do Sentinel para autenticação SMTP . . . 70
3.4.2 Banco de Dados do Sentinel . . . 71
3.4.3 Serviço do Coletor . . . 72
3.4.4 Atualizando a chave de licença (da chave de avaliação) . . . 72

4 Configuração do Advisor 73

4.1 Visão geral do Consultor . . . 73
4.2 Instalação do Advisor . . . 74
4.2.1 Configuração Independente . . . 74
4.2.2 Configuração Download Direto da Internet . . . 74
4.3 Relatórios do Consultor . . . 75
4.3.1 Configuração de relatório do Consultor . . . 75
4.4 Atualizando dados nas tabelas do Advisor . . . 76
4.5 Redefinindo a senha do Advisor (somente Download Direto) . . . 76

5 Testando a instalação 79

5.1 Testando a instalação . . . 79
5.2 Limpar do teste . . . 89
5.3 Introdução . . . 89

6 Upgrade para Sentinel 6 91

6.1 Upgrade de Sentinel 5.x para Sentinel 6.0 . . . 91
6.2 Upgrade do Sentinel 4.x para o Sentinel 6.0 . . . 92

7 Instalando componentes do Sentinel 95

7.1 Instalando um novo componente em uma máquina do Sentinel 95
7.1.1 Instalando o Banco de Dados do Sentinel 97

8 Camada de Comunicação (iSCALE) 101

8.1 Proxy SSL e Comunicação Direta 102
8.1.1 Sentinel Control Center 102
8.1.2 Gerenciador de Coletor 103
8.2 Mudanças da Chave Criptográfica 105
8.2.1 Mudanças na senha do Consultor 106

9 Crystal Reports para Windows 107

9.1 Visão geral 108
9.2 Requisitos do sistema 109
9.3 Requisitos de configuração 109
9.3.1 Instalando o Microsoft Internet Information Server (IIS) e o ASP.NET 110
9.4 Problemas conhecidos 111
9.5 Usando Crystal Reports 111
9.6 Visão geral da instalação 111
9.6.1 Visão geral da instalação para Microsoft SQL 2005 Server com Autenticação do Windows 111
9.6.2 Visão geral da instalação para Microsoft SQL 2005 Server com autenticação do servidor SQL 112
9.6.3 Visão geral da instalação para Oracle 112
9.7 Instalação 113
9.7.1 Instalando o Crystal Server Para Microsoft SQL 2005 Server com Autenticação do Windows 113
9.7.2 Instalando o Crystal Server para Microsoft SQL 2005 Server com autenticação de SQL 118
9.7.3 Instalando o Crystal Server para Oracle 122
9.8 Configuração para todas as autenticações e configurações 124
9.8.1 Mapeando o Crystal Reports para uso com o Sentinel 125
9.8.2 Definindo uma Conta de Usuário Nomeado 128
9.8.3 Configurando Permissões de Relatórios 129
9.8.4 Desabilitando os 10 Principais Relatórios do Sentinel 130
9.8.5 Aumentando o limite de atualização de registro do relatório do Crystal Enterprise Server 131
9.8.6 Configurando o Sentinel Control Center para integração com o Crystal Enterprise Server 132

10 Crystal Reports para Linux 133

10.1 Usando Crystal Reports 134
10.2 Configuração 134
10.3 Instalação 134
10.3.1 Pré-instalação do Crystal BusinessObjects Enterprise™ XI 135
10.3.2 Instalando o Crystal BusinessObjects Enterprise™ XI 136
10.3.3 Aplicando patch do Crystal Reports para uso com o Sentinel 137
10.4 Publicando gabaritos de Crystal Reports 138
10.4.1 Publicando gabaritos de relatórios – Assistente de Publicação de Crystal Reports 139
10.4.2 Publicando gabaritos de relatório – Console de Gerenciamento Central 141
10.5 Usando o servidor Web Crystal XI 142
10.5.1 Testando a conectividade com o servidor Web 142

10.6 Definindo uma conta de ‘Usuário Nomeado’ 142
10.7 Configurando Permissões de Relatórios 143
10.8 Habilitando os relatórios 10 Primeiros do Sentinel 143
10.9 Aumentando o limite de atualização de registro do relatório do Crystal Enterprise Server . . 144
10.10 Configurando o Sentinel Control Center para integração com o Crystal Enterprise Server. . 145
10.11 Utilitários e solução de problemas 146
10.11.1 Iniciando o MySQL 146
10.11.2 Iniciando o Tomcat 146
10.11.3 Iniciando o Crystal Servers 146
10.11.4 Erro de nome de host Crystal 147
10.11.5 Não é possível conectar-se ao CMS 147

11 Desinstalando o Sentinel 149

11.1 Desinstalando o Sentinel 149
11.1.1 Desinstalação no Solaris e Linux 149
11.1.2 Desinstalação no Windows 150
11.1.3 Desinstalando com o Painel de Controle 150
11.2 Pós-desinstalação 151
11.2.1 Arquivos de dados do Sentinel 151
11.2.2 Configurações do Sentinel 153

A Questionário de pré-instalação 157

B Registro de instalação para Sentinel no Linux com Oracle 159

C Registro de instalação para Sentinel no Solaris com Oracle 163

D Registro de instalação para o Sentinel no Windows com Microsoft SQL Server 169

Prefácio

A documentação Técnica do Sentinel é um guia de operação e referência para fins gerais. Esta documentação se destina a Profissionais de Segurança de Informações. O texto desta documentação se destina a servir como fonte de referência sobre o Sistema de Gerenciamento de Segurança Corporativa do Sentinel. Há documentação adicional disponível no portal da Web do Sentinel.

A documentação Técnica do Sentinel está dividida em cinco volumes diferentes. São eles:

- Volume I – Guia de Instalação do Sentinel™
- Volume II – Guia do Usuário do Sentinel™
- Volume III – Guia do Usuário do Coletor do Sentinel™
- Volume IV – Guia de Referência do Usuário do Sentinel™
- Volume V – Integração de Terceiros do Sentinel™

Volume I – Guia de Instalação do Sentinel

Este guia explica como instalar:

- Sentinel Server
- Console do Sentinel
- Mecanismo de Correlação do Sentinel
- Crystal Reports do Sentinel
- Construtor de Coletor
- Gerenciador de Coletor
- Consultor

Volume II – Guia do Usuário do Sentinel

Este guia aborda o seguinte:

- Operação do Console do Sentinel
- Recursos do Sentinel
- Arquitetura do Sentinel
- Comunicação do Sentinel
- Encerramento/Inicialização do Sentinel
- Avaliação de vulnerabilidade
- Monitoramento de eventos
- Filtragem de eventos
- Correlação de eventos
- Gerenciador de Dados do Sentinel
- Configuração de Eventos para Relevância Comercial
- Serviço de Mapeamento
- Geração de relatórios de histórico
- Gerenciamento de Host do Coletor
- Incidentes
- Casos
- Gerenciamento de usuários
- Workflow

Volume III – Guia do Usuário do Coletor

Este guia aborda o seguinte:

- Operação do Construtor do Coletor
- Gerenciador de Coletor
- Coletores
- Gerenciamento de Host do Coletor
- Construção e manutenção de coletores

Volume IV – Guia de Referência do Usuário do Sentinel

Este guia aborda o seguinte:

- Linguagem de criação de scripts do coletor
- Comandos de análise do coletor
- Funções de administrador do coletor
- Metatags do coletor e do Sentinel
- Permissões de usuário
- Mecanismo de correlação do Sentinel
- Opções da linha de comando de correlação
- Esquema do banco de dados do Sentinel

Volume V – Guia de Integração de Terceiros do Sentinel

- Remedy
- HP OpenView Operations
- HP Service Desk

Introdução 1

Tópicos contidos neste capítulo:

- Seção 1.1, “Visão geral do Sentinel” na página 11
- Seção 1.1.2, “Servidor de Comunicação do Sentinel” na página 13
- Seção 1.1.3, “Mecanismo de Correlação” na página 13
- Seção 1.1.4, “Workflow de iTRAC” na página 13
- Seção 1.1.6, “Gerenciador do Coletor do Sentinel” na página 14
- Seção 1.1.7, “Coletores do Sentinel” na página 14
- Seção 1.1.8, “Sentinel Control Center” na página 14
- Seção 1.1.9, “Construtor de Coletor do Sentinel” na página 15
- Seção 1.1.10, “Gerenciador de Dados do Sentinel” na página 15
- Seção 1.1.11, “Crystal Reporting Server” na página 15
- Seção 1.1.12, “Sentinel Advisor” na página 15
- Seção 1.1.13, “Integração com Terceiros” na página 15
- Seção 1.2, “Suporte de idiomas” na página 15

Esse guia orientará uma instalação básica. O Guia do Usuário do Sentinel possui procedimentos administrativos, arquitetura e operação mais detalhados.

Este guia supõe que você está familiarizado com segurança de rede, administração de bancos de dados e dos sistemas operacionais Windows e UNIX.

1.1 Visão geral do Sentinel

Sentinel™ é uma solução de Gerenciamento de Eventos e Informações de Segurança que recebe informações de muitas fontes em toda a empresa, as padroniza, as prioriza e apresenta para que você tome medidas relacionadas a ameaças, riscos e política.

O Sentinel automatiza os processos de relatórios, análise e coleta de registro para garantir que os controles de TI sejam eficazes no suporte à detecção de ameaças e aos requisitos de auditoria. O Sentinel substitui esses processos manuais de trabalho intensivo por monitoração contínua e automatizada de eventos de conformidade e segurança e controles de TI.

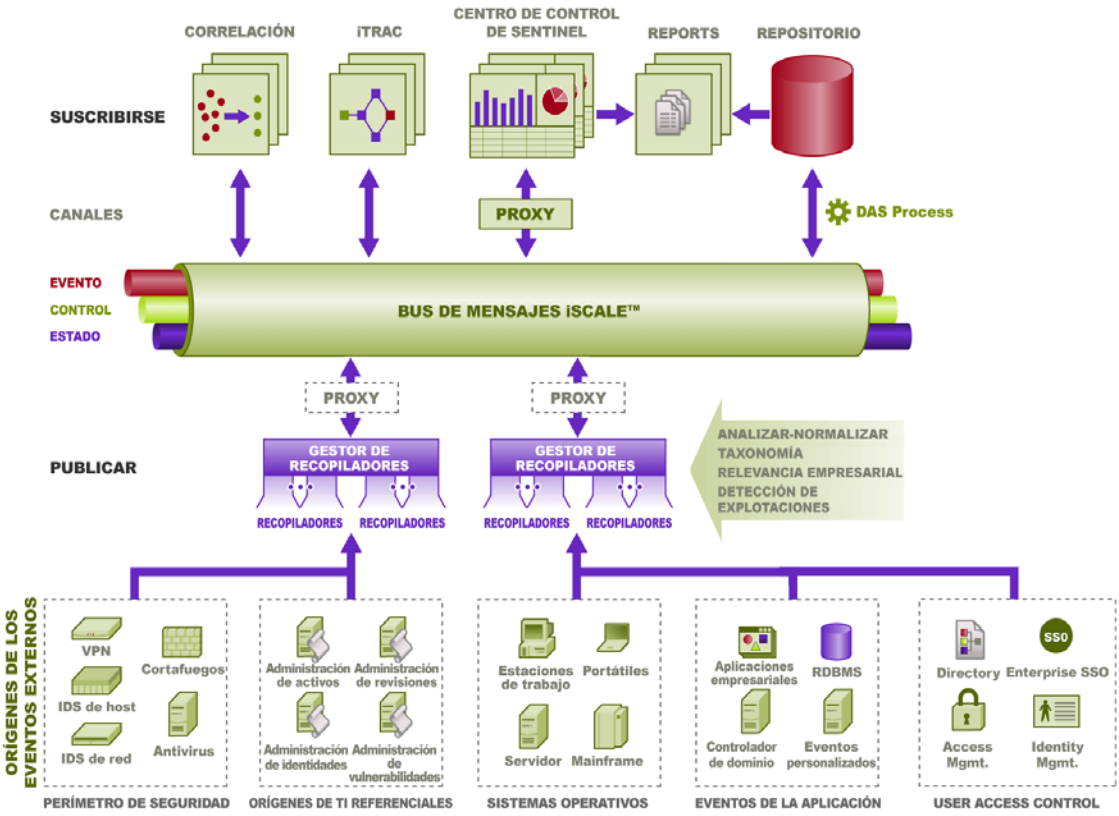
O Sentinel coleta e correlaciona informações de segurança e outros tipos de informações de toda a infra-estrutura de rede da organização, bem como sistemas, dispositivos e aplicativos de terceiros. A Sentinel apresenta os dados coletados em uma GUI mais sensível, identifica problemas de conformidade ou segurança e controla atividades de remédios, facilitando processos sujeitos a erros e construindo um programa de gerenciamento rigoroso e seguro.

O gerenciamento de resposta de incidentes automatizado permite que você documente e formalize o processo de monitoramento, escala e resposta aos incidentes e violações de política, e fornece a integração bidirecional com sistemas de comunicação de problemas. O Sentinel permite que você reaja prontamente e resolva incidentes de forma eficiente.

Com o Sentinel, você obtém:

- Gerenciamento de segurança em tempo real automatizado e integrado e monitoramento de conformidade entre todos os sistemas e redes
- Uma estrutura que habilita políticas de negócios para orientar ações e políticas de TI.
- Documentação e relatórios automáticos de segurança, sistemas e eventos de acesso em toda a empresa
- Gerenciamento de incidentes e reparação incorporados
- A possibiliade de demonstrar e monitorar a conformidade com políticas internas e regulamentos governamentais como Sarbanes-Oxley, HIPAA, GLBA, FISMA e outros

Veja a seguir uma arquitetura conceitual do Sentinel, que ilustra os componentes envolvidos na execução do Gerenciamento de Segurança.



O Sentinel é composto por vários componentes:

- Sentinel Server
- Servidor de Comunicação do Sentinel
- Mecanismo de Correlação
- iTRAC
- Banco de Dados do Sentinel
- Gerenciador do Coletor do Sentinel
- Coletores do Sentinel

- Sentinel Control Center
- Construtor de Coletor do Sentinel
- Gerenciador de Dados do Sentinel
- Crystal Report Server
- Sentinel Advisor
- Integração com Terceiros
  - HP OpenView Operations
  - HP Service Desk
  - Remedy

1.1.1 Sentinel Server

O Sentinel Server é formado por vários componentes que executam os serviços essenciais de processamento de eventos. Isso inclui receber eventos dos Gerenciadores do Coletor, armazená-los no banco de dados, filtrar, processar exibições de Tela Ativa, executar consultas em bancos de dados e processar resultados, e gerenciar tarefas administrativas como autenticação e autorização de usuários.

1.1.2 Servidor de Comunicação do Sentinel

O Barramento de Mensagem iSCALE pode mover milhares de pacotes de mensagens em um segundo entre os componentes do Sentinel. Isso permite o dimensionamento independente dos componentes e a integração baseada em padrões com aplicativos externos.

1.1.3 Mecanismo de Correlação

A correlação agrega inteligência ao gerenciamento de eventos de segurança, automatizando a análise do fluxo de eventos de entrada para encontrar padrões relevantes. A correlação permite definir regras que identificam as ameaças importantes e padrões complexos de ataque, para que você consiga priorizar os eventos e iniciar o gerenciamento e a resposta eficazes aos incidentes.

1.1.4 Workflow de iTRAC

O Sentinel fornece um sistema de gerenciamento de workflow de iTRAC para definir e automatizar processos para resposta a incidentes. Incidentes identificados no Sentinel, seja por uma regra de correlação ou manualmente, podem ser associados a um workflow de iTRAC.

1.1.5 Banco de Dados do Sentinel

O Sentinel tem como base um banco de dados de backend que armazena eventos de segurança e todos os metadados do Sentinel. Os eventos são armazenados em um formato regularizado juntamente com dados de vulnerabilidade e de ativos, informações de identidade, status de incidente e de workflow e muitos outros tipos de dados.

1.1.6 Gerenciador do Coletor do Sentinel

O Gerenciador de Coletor gerencia os Coletores, monitora as mensagens de status do sistema e executa a filtragem de eventos conforme necessário. As principais funções do Gerenciador de Coletor incluem transformar eventos, adicionar relevância comercial aos eventos por meio de taxonomia, executar filtragem global dos eventos, rotear eventos e enviar mensagens sobre a saúde do sistema ao Sentinel Server.

O Gerenciador do Coletor do Sentinel pode se conectar diretamente ao barramento de mensagem ou usar um proxy SSL.

1.1.7 Coletores do Sentinel

O Sentinel coleta dados dos dispositivos de origem e distribui um fluxo de eventos enriquecido ao aplicar a taxonomia, detecção de exploração e relevância comercial no fluxo de dados antes de correlacionar, analisar e enviar os eventos para o banco de dados. Um fluxo de eventos enriquecido significa que os dados estão correlacionados ao contexto comercial necessário para identificar e resolver ameaças internas ou externas e violações às políticas.

Os Coletores do Sentinel podem analisar dados dos tipos de dispositivos listados abaixo:

Sistemas de detecção de intrusão (host)	Antivírus
Sistemas de detecção de intrusão (rede)	Servidores da web
Firewalls.	Bancos de Dados
Sistemas operacionais	Mainframe
Monitoramento de políticas	Avaliação de vulnerabilidade
Autenticação	NDS
Roteadores e Switches	Gerenciador de Redes
VPN	Sistemas proprietários

Você pode fazer download de coletores existentes específicos para dispositivos, no site de Produtos da Novell (http://support.novell.com/products/sentinel/collectors.html). Os coletores podem ser construídos ou modificados no Construtor de Coletor, um aplicativo independente incluído no sistema do Sentinel.

1.1.8 Sentinel Control Center

O Sentinel Control Center fornece um painel de gerenciamento de segurança integrado que permite que analistas identifiquem rapidamente novas tendências ou ataques, manipulem e interajam com informações gráficas em tempo real e respondam a incidentes. Os recursos principais do Sentinel Control Center incluem:

- Telas Ativas: estatísticas e visualização em tempo real
- Incidentes: criação e gerenciamento de incidentes
- Admin: definição e gerenciamento de regras de correlação
- iTRAC: gerenciamento de processos para documentação, aplicação e rastreamento dos processos de resolução de incidentes.

- Relatórios: histórico de métricas e relatórios
- Gerenciamento de Fonte de Eventos: distribuição e monitoramento de Coletores

1.1.9 Construtor de Coletor do Sentinel

O Construtor de Coletor do Sentinel permite que você construa Coletores. Você pode criar e personalizar os gabaritos para que o coletor possa analisar os dados.

1.1.10 Gerenciador de Dados do Sentinel

O SDM (Gerenciador de Dados do Sentinel) permite que você gerencie o Banco de Dados do Sentinel. Você pode executar as seguintes operações no SDM:

- Monitorar a utilização de espaço do banco de dados
- Ver e gerenciar as partições de banco de dados
- Gerenciar arquivos de bancos de dados
- Importar dados para o banco de dados
- Configurar o mapeamento de dados
- Configurar os nomes de tags de eventos
- Definir configurações de relatório de resumo

1.1.11 Crystal Reporting Server

Serviços de relatórios abrangentes dentro do Sentinel Control Center são fornecidos por Crystal Enterprise Server by Business Objects™. O Sentinel vem com relatórios predefinidos direcionados às solicitações de relatórios mais comuns de organizações que monitoram suas posturas de segurança e conformidade. Usando o Crystal Report Developer, novos relatórios personalizados também podem ser desenvolvidos no esquema de tela de relatório publicado do Sentinel.

1.1.12 Sentinel Advisor

O Sentinel Advisor é um módulo opcional que efetua a referência cruzada entre os dados de alerta em tempo real do Sentinel com vulnerabilidades conhecidas e informações de resolução.

1.1.13 Integração com Terceiros

O Sentinel usa plugins API de terceiros para integração com os seguintes sistemas:

- HP OpenView Operations
- HP Service Desk
- Remedy AR

1.2 Suporte de idiomas

Os componentes do Sentinel foram localizados para os seguintes idiomas:

- Inglês

- Português (Brasil)
- Francês
- Italiano
- Alemão
- Espanhol
- Japonês
- Chinês (Tradicional)
- Chinês (Simplificado)

Há várias exceções:

- A interface do Construtor de Coletor e a criação de scripts estão somente em inglês, embora possam ser executados nos sistemas operacionais nos outros idiomas listados acima.
- No momento, os Gerenciadores de Coletor só processam dados ASCII e ASCII estendido (isto é, não processam dados double-byte ou Unicode).
- Coletores criados no Novell são projetados para analisar eventos em inglês.
- Eventos internos (para auditar operações do Sentinel) são apenas em inglês.

1.3 Outras referências da Novell

Os manuais a seguir estão disponíveis no site de Documentação da Novell (http://www.novell.com/documentation/):

- Guia de Instalação do Sentinel
- Guia do usuário do Sentinel
- Guia do Usuário do Construtor de Coletor do Sentinel
- Guia de Referência do Usuário do Sentinel
- Guia de Integração de Terceiros do Sentinel
- Notas de versão

1.4 Entrar em Contato com a Novell

- Website: http://www.novell.com (http://www.novell.com)
- Suporte Técnico da Novell: http://support.novell.com/phone.html?sourceidint=suplnav4_phonesup (http://support.novell.com/phone.html?sourceidint=suplnav4_phonesup)
- Auto-suporte: http://support.novell.com/support_options.html?sourceidint=suplnav_supportprog (http://support.novell.com/support_options.html?sourceidint=suplnav_supportprog)
- Site de download de patches: http://download.novell.com/index.jsp (http://download.novell.com/index.jsp)
- Suporte 24 horas, 7 dias por semana: http://www.novell.com/offices (http://www.novell.com/offices)

Melhores práticas

2

Tópicos incluídos neste capítulo:

- Seção 2.1, “Plataformas Suportadas” na página 17
- Seção 2.1.4, “Pilhas suportadas” na página 18
- Seção 2.2, “Recomendações de hardware” na página 18
- Seção 2.3, “Benchmarks de Desempenho” na página 22
- Seção 2.6, “Melhor Prática-Instalação/Configuração de Banco de Dados” na página 29
- Seção 2.8, “Definindo senhas - melhores práticas” na página 33
- Seção 2.10, “Manutenção do Banco de Dados” na página 36
- Seção 2.11.2, “Uso da memória” na página 40

Este capítulo aborda as melhores práticas e recomendações para o uso do Sentinel.

2.1 Plataformas Suportadas

Os componentes do Sentinel devem ser sempre instalados em uma plataforma aceita pela Novell. O Sentinel era suportado nas plataformas a seguir, quando da impressão deste documento. Para obter informações atualizadas, se houver, verifique a documentação online em http://www.novell.com/documentation (http://www.novell.com/documentation) e veja se há atualizações.

2.1.1 Sistemas operacionais

Componentes do Sentinel (incluindo o banco de dados) são certificados para serem executados nos seguintes sistemas operacionais:

- SuSE Linux Enterprise Server 9 SP2 e SP3
- SuSE Linux Enterprise Server 10 (patch de 1/7/2006)
- Atualização 5 ES do Red Hat Enterprise Linux 3 (x86)
- Sun Solaris 9 (DATA recomendada do cluster de patch de 03/05/05)
- Sun Solaris 10
- Windows 2003 Standard ou Enterprise Edition SP1
- Windows XP SP1 (para Sentinel Control Center, Construtor de Coletor e Gerenciador de Dados do Sentinel somente)
- Windows 2000 SP4, Standard ou Enterprise Edition (para Sentinel Control Center, Construtor de Coletor e Gerenciador de Dados do Sentinel somente)

2.1.2 Bancos de Dados

O funcionamento do Sentinel é garantido com os seguintes bancos de dados:

- Oracle 10g Enterprise Edition (v 10.2.0.3 com o patch essencial da Oracle #5881721)
- Oracle 9i Enterprise Edition (v 9.2.0.7 p. 5490841)

- Microsoft SQL Server 2005 SP1 32-bit (v.9.00.2047), Standard ou Enterprise Edition
- Microsoft SQL Server 2005 64-bit (v.9.00.2047), Standard ou Enterprise Edition

---

Observação: Todos os bancos de dados devem estar instalados em um sistema operacional certificado pelo fornecedor do banco de dados e também pela Novell para uso com componentes do Sentinel. O Oracle deve ser executado no Linux ou Solaris (não no Windows).

2.1.3 Servidor de Relatório

O servidor de relatórios aceito é o Crystal Enterprise Server XI R2, que pode ser executado em qualquer das plataformas a seguir no ambiente do Sentinel:

- Windows 2003 SP1 Server, Standard ou Enterprise Edition
  - Banco de dados do Crystal no Microsoft SQL 2005
- Atualização 5 ES do Red Hat Enterprise Linux 3 (x86)
  - Banco de dados do Crystal no MySQL
- SuSE Linux Enterprise Server 9 SP2 (x86)
  - Banco de dados do Crystal no MySQL

2.1.4 Pilhas suportadas

A Novell oferece suporte aos componentes do Sentinel instalados em qualquer dos sistemas operacionais aceitos, e o ambiente pode ser misto (Linux, Solaris e Windows) com algumas exceções e advertências:

- Construtor de Coletor - executa somente em plataformas Windows.
- Crystal Enterprise Server
  - Não pode ser executado no Solaris
  - Não pode ser executado no Windows 2000 em um ambiente do Sentinel
  - Não pode ser executado com MSDE como o banco de dados em um ambiente do Sentinel
- Banco de Dados
  - Deve ser SQL Server se o Sentinel Server estiver no Windows
  - Deve ser Oracle se o Sentinel Server estiver no Linux ou Solaris (não Windows)
  - O Oracle no Windows não é suportado no ambiente do Sentinel
- DAS (Data Access Service - Serviço de Acesso a Dados)
  - A Autenticação do Windows não pode ser usada se o DAS estiver instalado em um ambiente misto com o DAS no Windows e o banco de dados é Oracle ou com o DAS no UNIX ou Linux e o banco de dados é SQL Server.

2.2 Recomendações de hardware

Ao ser instalado no Linux ou Windows, o Sentinel Server e os componentes de banco de dados podem ser executados em hardware x86 (32 bits) ou x86-64 (64 bits), incluindo AMD Opteron e Intel Xeon. Servidores Itanium não são suportados.

Para Solaris, a arquitetura SPARC é suportada.

2.2.1 Arquitetura

O Sentinel tem uma arquitetura altamente escalável e, se altas taxas de eventos forem esperadas, os componentes poderão ser distribuídos por várias máquinas para atingir o melhor desempenho para o sistema.

Há muitos fatores que devem ser considerados ao criar um sistema do Sentinel. Eis uma lista parcial dos fatores a serem considerados ao desenvolver um design:

- Taxa de eventos (eventos por segundo, ou EPS)
- Localização geográfica/de rede de fontes de eventos e largura de banda entre redes.
- Hardware disponível
- Sistemas operacionais preferidos
- Planos para escalabilidade futura
- Quantidade de filtragem de eventos esperada
- Políticas de retenção de dados locais
- Número desejado e complexidade de regras de correlação
- Número esperado de incidentes por dia
- Número esperado de workflows gerenciados por dia
- Número de usuários conectados ao sistema
- Vulnerabilidade e infra-estrutura de bens

O fator mais significativo no design de sistema do Sentinel é a taxa de eventos - quase todos os componentes da arquitetura do Sentinel serão afetados por aumento nas taxas de evento. Em um ambiente de alta taxa de eventos, a maior demanda estará no banco de dados, que é muito dependente da E/S e pode estar tratando simultaneamente inserções de centenas ou milhares de eventos por segundo, criação de objetos por vários usuários, atualizações de processo de workflow, consultas históricas simples do Sentinel Control Center e relatórios de longo prazo do Crystal Enterprise Server. Portanto, a Novell faz as seguintes recomendações:

- O banco de dados deve ser instalado sem nenhum outro componente do Sentinel.
- O servidor do banco de dados deve ser dedicado às operações do Sentinel. Aplicativos adicionais (ou processos de ETL) podem afetar o desempenho do banco de dados.
- O servidor do banco de dados deve ter uma matriz de armazenamento de alta velocidade que atenderá os requisitos de E/S com base nas taxas de inserção de eventos.
- Um DBA dedicado deve avaliar regularmente os seguintes aspectos do banco de dados:
  - Tamanho
  - Operações de E/S
  - Espaço em disco
  - Memória
  - Indexação

Em ambientes de baixa taxa de eventos (ex.: eps <25), as recomendações acima podem ser relaxadas, porque o banco de dados e outros componentes usarão menos recursos.

Esta seção inclui algumas recomendações de hardware gerais como orientação para o design do sistema do Sentinel. Em geral, as recomendações de design são baseadas em faixas de taxas de eventos. No entanto, as recomendações são baseadas nas seguintes presunções:

- A taxa de eventos está na extremidade alta da faixa de EPS.
- A média de tamanho dos eventos é 600 bytes.
- Todos eventos são armazenados no banco de dados (isto é, não há filtros para descartar eventos).
- Um volume de dados de trinta dias será armazenado online no banco de dados.
- O espaço de armazenamento para os dados do Consultor não está incluído nas especificações abaixo.
- O Sentinel Server tem um padrão de 5 GB de espaço em disco para armazenar em cache temporariamente os dados de eventos que deixam de ser inseridos no banco de dados devido a falhas.
- O Sentinel Server também tem um padrão de 5 GB de espaço em disco para eventos deixam de ser gravados nos arquivos de eventos de agregação devido a falhas.

As recomendações de hardware para uma implementação do Sentinel podem variar dependendo de cada implementação, por isso recomenda-se que o Novell Consulting Services seja consultado antes de finalizar a arquitetura do Sentinel. As recomendações abaixo podem ser usadas como diretrizes.

Observação: Devido a altas cargas de eventos e ao armazenamento em cache local, a máquina do Sentinel Server com DAS é necessária para ter uma matriz de disco distribuída local ou compartilhada (RAID) com um mínimo de 4 eixos de disco.

Os hosts distribuídos devem ser conectados aos outros hosts Sentinel Server via um switch único de alta velocidade (GIGE) para impedir gargalos de tráfego de rede.

A Novell recomenda que o Crystal Enterprise Server seja instalado em uma máquina dedicada, especialmente se o banco de dados for grande ou o uso de relatórios for intenso. O Crystal pode ser instalado na mesma máquina que o banco de dados se o banco de dados for pequeno, o uso de relatórios for leve e o banco de dados estiver instalado no Windows ou Linux.

Observação: O Sentinel 6.0 ainda estava em desenvolvimento quando este documento foi escrito, portanto os números a seguir são baseados em testes para o Sentinel 5.1.3. Para obter informações atualizadas, consulte o site de Documentação da Novell no endereço http://www.novell.com/documentation (http://www.novell.com/documentation).

1-500 EPS: Configuração em 2 Máquinas (Sentinel 5.1.3)			
Componentes	**RAM**	**Espaço em disco**	**CPU**
Máquina 1: Sentinel Server / Gerenciador de Coletor ◆ Mecanismo de Correlação ◆ DAS ◆ Servidor de Comunicação ◆ Consultor ◆ Gerenciador de Coletor / Coletores ◆ Banco de Dados ◆ Crystal Server (opcional para Windows/Linux)	6 GB	250 GB	Windows ou Linux - 2 x Dual Core Intel® Xeon® 5150 (2,66 GHz) ou Sun Solaris - 4 x UltraSPARC IIIi (1,5 GHz)
Máquina 2: Servidor de Relatório ◆ Crystal Server	2 GB	20 GB	Windows ou Linux - 1 x Dual Core Intel® Xeon® 5150 (2,66 GHz)

500 – 1500 EPS: Configuração em 3 Máquinas (Sentinel 5.1.3)			
Componentes	**RAM**	**Espaço em disco**	**CPU**
Máquina 1: Sentinel Server / Gerenciador de Coletor ◆ Mecanismo de Correlação ◆ DAS ◆ Servidor de Comunicação ◆ Consultor ◆ Gerenciador de Coletor / Coletores	4 GB	40 GB	Windows ou Linux - 2 x Dual Core Intel® Xeon® 5160 (3,0 GHz) ou Sun Solaris - 2 x 1,8 GHz UltraSPARC IV+
Máquina 2: Banco de dados ◆ Banco de Dados ◆ Crystal Server (opcional para Windows/Linux)	4 GB+	1 TB+	Windows ou Linux - 2 x Dual Core Intel® Xeon® 5160 (3,0 GHz) ou Sun Solaris - 2 x 1,8 GHz UltraSPARC IV+
Máquina 3: Servidor de Relatório (necessário somente se o Sentinel/BD estiverem em Solaris) ◆ Crystal Server	2 GB	20 GB	Wiindows ou Linux - 1 x Dual Core Intel® Xeon® 5150 (2,66 GHz)

1500 - 3000 EPS: Configuração em 4-5 Máquinas (Sentinel 5.1.3)			
Componentes	**RAM**	**Espaço em disco**	**CPU**
Máquina 1: Sentinel Server ◆ Mecanismo de Correlação ◆ DAS ◆ Servidor de Comunicação ◆ Consultor	4 GB	40 GB	Windows ou Linux - 2 x Dual Core Intel® Xeon® 5160 (3,0 GHz) ou Sun Solaris 2 x 1,8 GHz UltraSPARC IV+
Máquina 2: Banco de dados ◆ Banco de Dados ◆ Crystal Server (opcional para Windows/Linux)	8 GB+	3 TB+	Windows ou Linux - 2 x Dual Core Intel® Xeon® 5160 (3,0 GHz) ou Sun Solaris - 2 x 1,8 GHz UltraSPARC IV+
Máquina 3: Gerenciador de Coletor ◆ Gerenciador de Coletor/ Coletores	2 GB	20 GB	Windows ou Linux - 2 x Dual Core Intel® Xeon® 5160 (3,0 GHz) ou Sun Solaris - 2 x 1,8 GHz UltraSPARC IV+
Máquina 4: Servidor de Relatório ◆ Crystal Server	4 GB	20 GB	Wiindows ou Linux - 1 x Dual Core Intel® Xeon® 5150 (2,66 GHz)
Máquina 5: Componente DAS (necessário se EPS > 2000)	2 GB	40 GB	Windows ou Linux - 2 x Dual Core Intel® Xeon® 5160 (3,0 GHz) Sun Solaris - 2 x 1,8 GHz UltraSPARC IV+

2.3 Benchmarks de Desempenho

As tabelas a seguir descrevem várias configurações representativas e resultados de testes.

O objetivo dessas classificações é ser um ponto de referência para determinar o design da arquitetura; elas não representam limites fixos. Nestes testes, as cargas de sistema não excederam 75% da utilização, e as taxas de eventos representam desempenho de estado constante.

Observação: Os testes de benchmark se concentram nas inserções de eventos, na correlação e no serviço de mapeamento do Sentinel. Atividades adicionais, como geração de relatórios ou consulta de dados históricos, não foram incluídas no teste.

Todos os testes abaixo foram executados em um sistema com RAID 5 com distribuição com uma configuração 4+1.

2.3.1 Prova de conceito ou Configuração de demonstração

Essa configuração de máquina única é adequada para demonstrações ou provas limitadas de conceito e pode ser instalada com a opção "simples" no instalador do Sentinel. Essa configuração é altamente desaconselhável para uso em um sistema de produção.

Observação: O Sentinel 6.0 ainda estava em desenvolvimento quando este documento foi escrito, portanto os números a seguir são baseados em testes no Sentinel 5.1.3. Para obter informações atualizadas, consulte o site da Documentação da Novell no endereço http://www.novell.com/documentation/index.html (http://www.novell.com/documentation/index.html).

Função	RAM	MODEL
Sentinel Server + BD + Gerenciador de Coletor	5 GB, 5x36GB RAID	SLES9 - 2 x Dual Core Intel® Xeon® 5150 2,66 GHz

As seguintes métricas de desempenho foram observadas neste sistema.

Atributo	Classificação	Comentários
Eventos Processados e Armazenados por Dia (no BD)	86 milhões	
Eventos por Segundo (Gerenciador de Coletor)	1000	Uma única CPU (dual core) Xeon foi usada para o Gerenciador de Coletor
Eventos Por Segundo (Collector Engine)	300	PIX, Snort e outros dispositivos foram usados com este teste
Eventos por Segundo (SYSLOG)	300	1 servidor Syslog foi executado no host do Gerenciador de Coletor com 1 Mecanismo
Coletores distribuídos por Gerenciador de Coletor	3	1 coletor utilizou syslog; outros utilizaram um conector de arquivo
Número de Gerenciadores de Coletor	1	20 é o número máximo de CMs suportados por Sentinel Server
Número de Mecanismos de Correlação Distribuídos	1	É executado na máquina do Sentinel Server
Regras distribuídas por Mecanismo de correlação	10	
Active Views™ em execução	10	
Número de usuários simultâneos	3	
Número de telas por Instância de Tela Ativa	2	
Número de mapas distribuídos	2	
Tamanho do maior mapa no serviço de mapeamento	1.5 MB	
Número de linhas no maior mapa	1.5 milhões	

2.3.2 Configuração do Sistema de Produção - Opção 1

Essa configuração inclui três máquinas e trata aproximadamente 2000 eventos por segundo.

Observação: O Sentinel 6.0 ainda estava em desenvolvimento quando este documento foi escrito, portanto os números a seguir são baseados em testes no Sentinel 5.1.3. Para obter informações atualizadas, consulte o site da Documentação da Novell no endereço http://www.novell.com/documentation/index.html (http://www.novell.com/documentation/index.html).

Função	RAM	MODEL
Sentinel Server	4 GB, 5x36GB RAID	SLES9 - 2 x Dual Core Intel® Xeon® 5150 2,66 GHz
Banco de Dados	4 GB, 5x250GB RAID	SLES9 - 2 x Dual Core Intel® Xeon® 5150 2,66 GHz
Gerenciador de Coletor	2 GIG, 72 GIG	SLES9 - 1 x Dual Core Intel® Xeon® 5150 2,66 GHz

As seguintes métricas de desempenho foram observadas neste sistema:

Atributo	Classificação	Comentários
Eventos Processados e Armazenados por Dia (em BD)	173 milhões	
Eventos por Segundo (Gerenciador de Coletor)	2000	Uma única CPU (dual core) Xeon foi usada para o Gerenciador de Coletor
Eventos Por Segundo (Mecanismo do Coletor)	1200	PIX, Snort e outros dispositivos foram usados com este teste
Eventos por Segundo (SYSLOG)	1200	1 servidor Syslog foi executado no host do Gerenciador de Coletor com 1 Mecanismo
Coletores distribuídos por Gerenciador de Coletor	10	1 coletor utilizou syslog; outros utilizaram um conector de arquivo
Número de Gerenciadores de Coletor	1	20 é o número máximo de CMs suportados por Sentinel Server
Mecanismos de Correlação Distribuídos	1	Executado na máquina do Sentinel Server
Regras distribuídas por Mecanismo de correlação	20	
Active Views™ em execução	20	
Número de usuários simultâneos	5	
Número de telas por Instância de Tela Ativa	4	
Número de mapas distribuídos	4	
Tamanho do maior Mapa	1.5 MB	
Número de linhas no maior mapa	1.5 milhões	

2.3.3 Configuração do Sistema de Produção - Opção 2

Essa configuração exige quatro máquinas e trata aproximadamente 3000 eventos por segundo.

Observação: O Sentinel 6.0 ainda estava em desenvolvimento quando este documento foi escrito, portanto os números a seguir são baseados em testes no Sentinel 5.1.3. Para obter informações atualizadas, consulte o site da Documentação da Novell no endereço http://www.novell.com/documentation/index.html (http://www.novell.com/documentation/index.html).

Função	RAM	MODEL
Sentinel Server	4 GB, 5x36GB RAID	SLES9 - 2 x Dual Core Intel® Xeon® 5160 3,0 GHz
Banco de Dados	8 GB, 5x250GB RAID	SLES9 - 2 x Dual Core Intel® Xeon® 5160 3,0 GHz
Gerenciador de Coletor	2 GB, 72 GB	SLES9 - 2 x Dual Core Intel® Xeon® 5160 3,0 GHz
Sentinel Server (DAS - nó 2)	2 GB, 5x36GB RAID	SLES9 - 2 x Dual Core Intel® Xeon® 5160 3,0 GHz

As seguintes métricas de desempenho foram observadas neste sistema:

Atributo	Classificação	Comentários
Eventos Processados e Armazenados por Dia (no BD)	260 milhões	
Eventos por Segundo (Gerenciador de Coletor)	3000	Uma CPU dupla (dual core) Xeon foi usada para o Gerenciador do Coletor
Eventos Por Segundo (Collector Engine)	1200	PIX, Snort e outros dispositivos foram usados com este teste
Eventos por Segundo (SYSLOG)	2500	1 servidor syslog foi executado no host do Gerenciador de Coletor
Coletores distribuídos por Gerenciador de Coletor	10	3 coletores utilizaram syslog; outros utilizaram um conector de arquivo
Número de Gerenciadores de Coletor	1	
Mecanismos de Correlação Distribuídos	1	Executado na máquina do Sentinel Server
Regras distribuídas por Mecanismo de correlação	20	
Active Views™ em execução	20	
Número de usuários simultâneos	5	
Número de telas por Instância de Tela Ativa	4	
Número de mapas distribuídos	4	
Tamanho do maior Mapa	1.5 MB	

Atributo	Classificação	Comentários
Número de linhas no maior mapa	1.5 milhões	

2.4 Configuração de matriz de disco

Em uma configuração de produção, o servidor do Novell Sentinel exige uma matriz de disco de alta velocidade para o banco de dados e os hosts do sentinel. Esta seção aborda recomendações de configuração de disco típicas (RAID). Os seguintes recursos são afetados pelo desempenho do hardware de disco:

- Componente do banco de dados (Microsoft SQL/Oracle): a taxa de eventos (eventos por segundo) e recursos de consulta são afetados (incluindo Consulta de Histórico de Eventos, Consulta Offline e relatórios Crystal).
- DAS-RT (componente do serviço de acesso de dados em tempo real): o recurso de Telas Ativas é afetado.
- DAS-Aggregation: o número de resumos que podem ser ativados é afetado.

2.4.1 Requisito mínimo para instalação empresarial (1000 EPS ou mais)

É recomendável usar no mínimo uma configuração RAID 5. A RAID 5 pode proporcionar a melhor relação custo/benefício. Essa configuração sacrifica parcialmente o desempenho e a redundância para reduzir o custo. Observe que estas são apenas recomendações, que devem ser usadas como guia. A maioria das instalações empresariais de produção em grande-escala exigirá uma análise mais detalhada dos requisitos de velocidade, throughput e redundância.

- Grupo RAID 1 – BD (Dados, Índices, registros de transação etc.)
- Grupo RAID 2 – DAS do Sentinel Server (diretório de Dados, DIR* Temporário)
- Discos mínimos: 13 por Grupo de RAID
- Tipo de Disco: 12 k+ RPM, Fiber Channel ou SCSI
- LUN 1 (Grupo de RAID 1): 5 GB – 144 GB+ por disco
- LUN 2 (Grupo de RAID 2): 5 GB – 144 GB+ por disco

2.4.2 Configuração otimizada

Para a obtenção de uma configuração com desempenho e redundância ideais, uma RAID 1+0 pode ser utilizada com as mesmas configurações. No entanto, Grupos de RAID adicionais e LUNs que sigam as mesmas diretrizes acima podem ser necessárias para obter mais paralelismo e E/S para certos bancos de dados.

Observação: Para obter mais informações sobre como apontar o DAS TEMP DIR para um local diferente, consulte Seção 2.7, “Instalação e configuração do Sentinel” na página 32

2.4.3 Exemplo de configuração de armazenamento para uma instalação do Microsoft SQL

Este exemplo usa o subsistema de armazenamento EMC2 CLARiiON com:

- 1 TB de armazenamento
- 60 unidades, 36 GB, 15 K RPM

Grupos de RAID

Matriz	LUN	Tipo de RAID	Grupo RAID	Tamanho (GB)
1	0	8	0-0-13, 0-0-14, 1-0-13, 1-0-14, 2-0-13, 2-0-14, 3-0-13, 3-0-13	Grupo RAID 0
1	1	8	0-0-11, 0-0-12, 1-0-11, 1-0-12, 2-0-11, 2-0-12, 3-0-11, 3-0-12	Grupo RAID 1
1	2	8	0-0-9, 0-0-10, 1-0-9, 1-0-10, 2-0-9, 2-0-10, 3-0-9, 3-0-10	Grupo RAID 2
1	3	8	0-0-7, 0-0-8, 1-0-7, 1-0-8, 2-0-7, 2-0-8, 3-0-7, 3-0-8	Grupo RAID 3
1	4	8	0-0-5, 0-0-6, 1-0-5, 1-0-6, 2-0-5, 2-0-6, 3-0-5, 3-0-6	Grupo RAID 4
1	5	8	0-0-3, 0-0-4, 1-0-3, 1-0-4, 2-0-3, 2-0-4, 3-0-3, 3-0-4	Grupo RAID 5
1	6	12	0-0-0, 0-0-1, 0-0-2, 1-0-0, 1-0-1, 1-0-2, 2-0-0, 2-0-1, 2-0-2, 3-0-0, 3-0-1, 3-0-2	Grupo RAID 6

Atribuições da LUN

Matriz	LUN	Tipo de RAID	Grupo RAID	Tamanho (GB)	Processador de armazenamento	Nome
1	0	0	0	263	A	LUN 0
1	1	0	1	263	B	LUN 1
1	2	0	2	263	A	LUN 2
1	3	0	3	263	B	LUN 3
1	4	0	4	263	A	LUN 4
1	5	0	5	214	B	LUN 5
1	6	0	6	160	A	LUN 6
1	7	0	6	160	B	LUN 7

Grupos de armazenamento

Matriz	Grupo de armazenamento	LUN	Host	Letra da unidade	Nome
1	Sentinel	0	E2P0 (E3P0)	E:	SQLData1
1	Sentinel	1	E2P0 (E3P0)	F:	SQLData2
1	Sentinel	2	E2P0 (E3P0)	C:	SQLData3
1	Sentinel	3	E2P0 (E3P0)	C:	SQLData4
1	Sentinel	4	E2P0 (E3P0)	I:	SQLIndex1
1	Sentinel	5	E2P0 (E3P0)	J:	SQLIndex2
1	Sentinel	6	E2P0 (E3P0)	L:	SQLLog
1	Sentinel	7	E2P0 (E3P0)	T:	TempDB

2.4.4 Exemplo de configuração de armazenamento para uma instalação do Oracle

volume 1	RAID 1	Home page da Oracle
volume 2	RAID 1	membro de redo log a
volume 3	RAID 1	membro de redo log b
volume 4	RAID 0+1 ou RAID 5	tablespaces undo e temp
volume 5	RAID 0+1 ou RAID 5	Tablespaces de dados do Sentinel
volume 6	RAID 0+1 ou RAID 5	Tablespaces de índice do Sentinel
volume 7	RAID 0+1 ou RAID 5	Tablespaces de dados de resumo do Sentinel
volume 8	RAID 0+1 ou RAID 5	Tablespaces de índice de resumo do Sentinel
volume 9	RAID 1	arquivos de registro de arquivos

2.5 Configuração de rede

Componentes adicionais do Sentinel Server: devem ser conectados uns aos outros por um único switch de 1 GB. Isso inclui Banco De Dados, Servidor de Comunicação, Consultor, Serviços de base do Sentinel, Mecanismo de Correlação e DAS.

Sentinel Control Center, Construtor de Coletor e Collector Service (Gerenciador de Coletor): devem estar conectados ao Sentinel Server por meio de switches DUPLEX de 100Mbit-FULL, pelo menos.

2.6 Melhor Prática-Instalação/Configuração de Banco de Dados

Observação: A maioria dos parâmetros de instalação de banco de dados pode ser mudada depois da instalação do banco de dados por meio das ferramentas de gerenciamento do banco de dados ou da linha de comando.

1. O Sentinel usa uma estratégia de arquivo predefinida para gerenciar as tabelas que crescem rapidamente (a tabela EVENTOS, por exemplo). Essas tabelas são particionadas, e porções mais antigas podem ser arquivadas e descartadas sem afetar dados mais recentes. No entanto, há outras tabelas não são cobertas por esse esquema de particionamento e arquivamento e precisarão ser gerenciadas separadamente.
2. Por motivos de desempenho, dependendo de se tratar da instalação em RAID, e se o ambiente RAID permitir, os registros a seguir devem ser instalados no disco de gravação mais rápido disponível.
   - Registro Redo (Oracle)
   - Registro de Transação (Microsoft SQL)
3. Para determinar com mais com precisão o tamanho do banco de dados, você pode começar com um banco de dados pequeno e aumentar o tamanho depois de utilizar o sistema por um breve período. Isso lhe permitirá observar o crescimento do banco de dados com base na taxa de inserção de eventos para determinar os requisitos de espaço do banco de dados do sistema.
4. Para fins de recuperação, um DBA deve executar backups agendados regularmente das tabelas não particionadas do banco de dados.
5. Em instalações do Oracle, o instalador do Sentinel desativa o Registro de Arquivos por padrão. Para fins de recuperação de bancos de dados, é altamente recomendável que, após a instalação e antes de começar a receber dados de eventos de produção, você habilite o Registro de Arquivos. Você também deve programar um backup dos seus registros de arquivo para liberar espaço no destino do registro de arquivos, do contrário o banco de dados irá parar de aceitar eventos quando o destino de registro de arquivos atingir a capacidade completa.
6. Por motivos de desempenho em ambientes de alta taxa de eventos, os locais de armazenamento deve apontar para locais diferentes (ex.: controladores de disco diferentes) para evitar contenções de E/S.
   - Diretório de dados
   - Diretório de índices
   - Diretório de Dados de Resumo
   - Diretório de Índices de Resumo
   - Diretório de Registro (apenas Microsoft SQL)
   - Diretório Temporário e Undo Tablespace: (Apenas Oracle)
   - Diretório A do Membro de Redo Log (Apenas Oracle)
   - Diretório B do Membro de Redo Log (Apenas Oracle)

2.6.1 Patches do Banco de Dados do Sentinel

Para Microsoft SQL apenas, quando os patches do Banco de Dados do Sentinel são aplicados, o instalador só adicionará novos índices a *_P_MAX. As partições já existentes não serão atualizadas.

Você precisará adicionar índices manualmente às partições já existentes se desejar que os novos índices aprimorem o desempenho para consultas executadas em relação às partições existentes.

2.6.2 Configurações do Kernel do UNIX recomendadas para Oracle

A seguir estão sugestões de valores mínimos. Para obter mais informações, consulte a documentação do sistema e do Oracle.

Valores de parâmetros de Kernel mínimos para Linux

Para obter mais informações sobre como ver e definir parâmetros do kernel no Linux, consulte Capítulo 3, “Instalando o Sentinel 6” na página 43 no Guia de Instalação.

```
shmmax=2147483648 (minimum value)
shmmni=4096
semmns=32000
semmni=1024
semmsl=1024
semopm=100
```

Valores de parâmetros de Kernel mínimos para Solaris

Verifique os parâmetros de kernel UNIX para Oracle em /etc/system e defina o seguinte:

```
shmmax=4294967295
shmmin=1
shmseg=50
shmmni=400
semmns=14000
semmni=1024
semmsl=1024
shmopm=100
shmvmx=32767
```

2.6.3 Configura Parâmetros ao criar sua própria instância do banco de dados

Você pode criar a estrutura de banco de dados (no nível do tablespace) manualmente em vez de usar o instalador do Sentinel, se desejar. Em seguida, durante a instalação, você pode selecionar a opção "adicionar objetos de banco de dados a um banco de dados existente". As configurações a seguir são recomendadas para criar sua própria instância do banco de dados. Suas configurações podem variar dependendo da configuração e dos requisitos do sistema.

Na instância Oracle, será necessário criar:

- Parâmetros de inicialização Oracle (esses valores dependem do tamanho e da configuração do sistema)
- Parâmetros de Configuração de tablespaces do Sentinel necessários para Solaris e Linux

Parâmetros Mínimos Recomendados para Configuração

Parâmetros	Tamanho (bytes ou outra especificação)
db_cache_size	1 GB
java_pool_size	33,554,432
large_pool_size	8,388,608
shared_pool_size	100 MB
pga_aggregate_target	150,994,944
sort_area_size	109,051,904
open_cursors	500
cursor_sharing	SIMILAR
hash_join_enabled	TRUE
optimizer_index_caching	50
optimizer_index_cost_adj	55

Tamanho Mínimo Recomendado para Tablespace

Tabela	Tamanho de Exemplo	Observações
REDO	3 x 100M	Este é o valor mínimo. Você deve criar redo logs maiores se tiver um EPS elevado.
SYSTEM	500M	Valor mínimo
TEMP	1G	Valor mínimo
UNDO	1G	Valor mínimo
ESENTD	5G	Valor mínimo
		Este é para dados de eventos
ESENTD2	500M	Valor mínimo
		Dados de configuração, bens, vulnerabilidade e associações (autoextend habilitado)
ESENTWFD	250M	Para dados do iTRAC (autoextend habilitado)
ESENTWFX	250M	Para índice do iTRAC (autoextend habilitado)
ESENTX	3G	Valor mínimo
		Para índice de eventos
ESENTX2	500M	Valor mínimo
		Índice de configuração, bens, vulnerabilidade e associações (autoextend habilitado)

Tamanho Mínimo Recomendado para Tablespace		
Tabela	**Tamanho de Exemplo**	**Observações**
SENT_ADVISORD	200M	Valor mínimo
		Para dados do Advisor (autoextend habilitado)
SENT_ADVISORX	100M	Valor mínimo
		Para índice do Advisor (autoextend habilitado)
SENT_LOBS	100M	Valor mínimo
		Para objetos grandes de bancos de dados (autoextend habilitado)
SENT_SMRYD	3G	Valor mínimo
		Para dados de resumo de Agregação
SENT_SMRYX	2G	Valor mínimo
		Para índice de resumo de Agregação

2.7 Instalação e configuração do Sentinel

Quando o Sentinel é instalado, por motivos de desempenho e backup, os itens a seguir devem ser considerados.

1. Ao executar uma instalação limpa do Sentinel depois de ter uma versão anterior do Sentinel instalada, é ALTAMENTE recomendável que você remova certos arquivos e configurações de sistema da instalação anterior. Se esses arquivos não forem removidos, uma nova instalação limpa poderá falhar. Esse procedimento deve ser realizado em cada máquina onde esteja sendo feita uma instalação limpa. Para obter mais informações sobre quais arquivos remover, consulte Capítulo 11, “Desinstalando o Sentinel” na página 149 no Guia de Instalação.
2. O desempenho de Telas Ativas e Mapeamento poderá ser bastante aprimorado se o diretório temp dos processos de DAS_RT e Das_Query apontar para um disco rápido (por exemplo, uma matriz de disco). Para apontar o diretório temp dos processos para um disco rápido, faça o seguinte no computador em que o DAS está instalado:
   - **2a** Crie um diretório no disco rápido para colocar nele os arquivos temporários. No UNIX, esse diretório deve pertencer e ser gravável pelo Usuário Administrador do Sentinel e pelo grupo esec.
   - **2b** Faça uma cópia de backup do arquivo %ESEC_HOME%\config\configuration.xml.
   - **2c** Abra o arquivo %ESEC_HOME%\config\configuration.xml em um editor de texto.
   - **2d** Para os processos DAS_RT e DAS_Query, adicione o argumento JVM java.io.tmpdir, definindo-o para o diretório que você acabou de criar.
   - **2e** Para fazer essa mudança para o processo DAS_RT, procure a linha que contém o texto

     ```
     -Dsrv_name=DAS_RT
     ```

     e adicione o argumento mencionado abaixo ao lado dela.

     ```
     -Djava.io.tmpdir=<tmp_directory>
     ```

Um exemplo de como a linha deve ser (seus argumentos –Xmx, -Xms e –XX podem ter aparência diferente) é:

```
<process component="DAS" image="&amp;quot;$(ESEC_JAVA_HOME)/
java&amp;quot; -server -Dsrv_name=DAS_RT -Djava.io.tmpdir=D:\Temp2
-Xmx310m -Xms103m -XX:+UseParallelGC -Xss128k -Xrs -
Desecurity.dataobjects.config.file=/xml/BaseMetaData.xml -
Djava.util.logging.config.file=../config/das_rt_log.prop -
Dcom.esecurity.configurationfile=../../configuration.xml -
Djava.security.auth.login.config=../config/auth.login -
Djava.security.krb5.conf=../../lib/krb5.conf -jar ../../lib/
ccsbase.jar ..//config//das_rt.xml" min_instances="1"
post_startup_delay="5" shutdown_command="cmd //C
&amp;quot;$(ESEC_HOME)/bin/stop_container.bat&amp;quot; localhost
DAS_RT" working_directory="$(ESEC_HOME)/bin"/>
```

2f Para fazer essa mudança para o processo DAS_Query, procure a linha que contém o texto

```
-Dsrv_name=DAS_Query
```

e adicione o argumento mencionado abaixo ao lado dela.

```
-Djava.io.tmpdir=<tmp_directory>
```

Um exemplo de como a linha deve ser (seus argumentos –Xmx, -Xms e –XX podem ter aparência diferente) é:

```
<process component="DAS" image="&amp;quot;$(ESEC_JAVA_HOME)/
java&amp;quot; -server -Dsrv_name=DAS_Query -
Djava.io.tmpdir=D:\Temp2 -Xmx256m -Xms85m -XX:+UseParallelGC -
Xss128k -Xrs -Desecurity.dataobjects.config.file=/xml/
BaseMetaData.xml,/xml/WorkflowMetaData.xml -
Djava.util.logging.config.file=../config/das_query_log.prop -
Djava.security.auth.login.config=../config/auth.login -
Djava.security.krb5.conf=../../lib/krb5.conf -
Desecurity.execution.config.file=../config/execution.properties
-Dcom.esecurity.configurationfile=../../configuration.xml -jar
../../lib/ccsbase.jar ..//config//das_query.xml"
min_instances="1" post_startup_delay="5" shutdown_command="cmd
//C &amp;quot;$(ESEC_HOME)/bin/stop_container.bat&amp;quot; localhost
DAS_Query" working_directory="$(ESEC_HOME)/bin"/>
```

2.8 Definindo senhas - melhores práticas

Para atender a configurações de segurança rígidas exigidas pela Certificação de Critérios Comuns:

1. Escolha senhas com no mínimo 8 caracteres, que incluam pelo menos um caractere em MAIÚSCULA, um em minúscula, um símbolo especial (!@#$%^&*()_+) e um numérico (0-9).
2. A senha não deve conter o nome usado no e-mail nem partes do seu nome completo.
3. A senha não deve ser uma palavra “comum” (por exemplo, não deve ser uma palavra registrada em dicionário nem gíria de uso comum).
4. A senha não deve conter palavras de idioma algum, pois existem vários programas de invasão de senha capazes de verificar milhões de possibilidades de combinações de palavras em segundos.

5 Escolha uma senha de que possa se lembrar, mas que seja complexa. Por exemplo, Mft5#AIdade (meu filho tem 5 anos de idade) OU EmnCh5#a (eu moro na Califórnia há 5 anos).

2.9 Configuração de Relatórios

Dependendo do número de eventos que o Crystal estiver consultando, você poderá receber um erro sobre o tempo máximo de processamento ou o limite máximo de registros. Para definir o servidor para processar um número maior ou ilimitado de registros, será necessário reconfigurar o Crystal Page Server. Isso pode ser feito usando ou o Central Configuration Manager ou a página da Web do Crystal.

Para reconfigurar o Crystal Page Server por meio do Central Configuration Manager:

1. Clique em Iniciar > Todos os programas > Businessobjects 11 > Crystal Reports Server > Central Configuration manager.
2. Clique o botão direito em Crystal Reports Page Server e selecione Parar.
3. Clique o botão direito em Crystal Reports Page Server e selecione Propriedades.
4. No campo Comando, sob a guia Propriedades, ao final da linha de comando, adicione:
   ```
   maxDBResultRecords <value greater than 20000 or 0 to disable the default limit>
   ```
5. Reinicie o Crystal Page Server.

Para reconfigurar o Crystal Page Server por meio da página da Web do Crystal:

1. Clique em Iniciar > Todos os programas > Businessobjects 11 > Crystal Reports Server > .Net administration Launchpad.
2. Clique em Central Management Console.
3. O nome do sistema deve ser o nome do computador do host. O tipo de autenticação deve ser Enterprise. Caso contrário, escolha Enterprise.
4. Digite o nome do usuário e a senha e clique em Log On.
5. Clique em Servidores.
6. Clique em <nome do servidor>.pageserver.
7. Em Database Records to Read When previewing or Refreshing a report (Registros do Banco de Dados para Ler quando Visualizar ou Atualizar um Relatório), selecione Unlimited records (Registros ilimitados).
8. Clique em Aplicar.
9. Será exibido um prompt para reiniciar o servidor de página; clique em OK.

Talvez seja preciso fornecer um nome de logon e uma senha para acessar o gerenciador do serviço do sistema operacional.

Para reconfigurar o Crystal Page Server (Servidores Linux ou Windows Crystal):

1. Abra um browser e digite este url:

   Para Servidores Linux Crystal:

```
http://<DNS or IP of Crystal Server>:8080/businessobjects/
enterprise11/adminlaunch
```

Para Servidores Windows Crystal:

```
http://<DNS name or IP address of your web server>/businessobjects/
enterprise11/WebTools/adminlaunch/default.aspx
```

2. Clique em Central Management Console.
3. O nome do sistema deve ser o nome do computador do host. O tipo de autenticação deve ser Enterprise. Caso contrário, escolha Enterprise.
4. Digite o nome do usuário e a senha e clique em Log On.
5. Clique em Servidores.
6. Clique em <nome do servidor>.pageserver.
7. Em Database Records to Read When Previewing Or Refreshing a report (Registros do Banco de Dados para Ler quando Visualizar ou Atualizar um Relatório), selecione Unlimited records (Registros ilimitados).
8. Clique em Aplicar.
9. Será exibido um prompt para reiniciar o servidor de página; clique em OK.
10. Talvez seja preciso fornecer um nome de logon e uma senha para acessar o gerenciador do serviço do sistema operacional.

2.9.1 Relatórios fornecidos com o Sentinel

Para melhorar o desempenho, os dez principais relatórios consultam tabelas de resumo em vez da tabela de eventos. As tabelas de resumo contêm contagens por tempo para combinações de campos nos dados de eventos. Isso fornece um conjunto de dados muito menor para certos tipos de consultas e resulta em consultas e tempos de execução de relatórios muito mais rápidos.

O serviço Agregação é responsável pelo preenchimento das tabelas de resumo com resumos de todos os eventos na tabela de eventos. O serviço Agregação só gerará dados resumidos para resumos que estão ativos. Os resumos a seguir são exigidos pelos 10 principais relatórios e são habilitados por padrão:

- EventDestSummary
- EventSevSummary
- EventSrcSummary

Os resumos podem ser ativados ou desativados com a janela de configuração de Dados de relatórios na guia Admin do Sentinel Control Center.

O serviço Agregação também depende do componente EventFileRedirectService em DAS binária para alimentá-lo com os dados de eventos que ele resumirá. Portanto, esse componente deve ser habilitado para que o serviço Agregação seja executado adequadamente. Esse componente é habilitado ou desabilitado modificando o atributo "status" do componente EventFileRedirectService no arquivo das_binary.xml para "on" (ativado) ou "off" (desativado). Por padrão, este componente é ativado ("on").

Observação: Para obter informações sobre EventFileRedirectService e os três resumos de agregação, consulte o "Gerenciador de Dados do Sentinel" no Guia do Usuário do Sentinel Control

Central ou Crystal Reports para Windows e Capítulo 10, “Crystal Reports para Linux” na página 133 no Guia de Instalação do Sentinel.

Observação: Os relatórios que consultam uma grande faixa de dados podem demorar para ser executados. Eles podem ser programados em vez de ser executados interativamente. Para obter informações sobre a programação do Crystal Reports, consulte a documentação do Crystal BusinessObjects Enterprise™ 11.

2.9.2 Dicas ao desenvolver Crystal Reports personalizados

Para relatórios desenvolvidos com personalização, é recomendável o seguinte:

1. Se os relatórios puderem utilizar tabelas agregadas predefinidas, escolha a tabela agregada que resultar no processamento da menor quantidade de dados.
2. Tente to distribuir a maioria do processamento de dados para o mecanismo de banco de dados.
3. Para reduzir o overhead de processamento no Crystal Server, minimize a quantidade de dados para recuperar para o Crystal Server.
4. Sempre grave relatórios nas telas do banco de dados fornecidas pela Novell em vez de gravar relatórios nas tabelas básicas.

2.10 Manutenção do Banco de Dados

O Sentinel usa seu banco de dados back end para armazenar todos os eventos, bem como os dados de configuração. Este banco de dados precisará ser gerenciado cuidadosamente para garantir que continue a ser executado de forma eficiente.

2.10.1 Informações de eventos no banco de dados

Grande parte do banco de dados consiste em dados de eventos resumidos e regularizados. Para facilitar o gerenciamento desse conjunto de dados de crescimento constante, a Novell particiona essas tabelas e fornece uma ferramenta de gerenciamento, o Gerenciador de Dados do Sentinel, para arquivar e apagar partições mais antigas. Você pode desenvolver um plano de arquivamento, que pode ser automatizado para minimizar a interação do usuário.

Observação: Para obter mais informações sobre o Gerenciador de Dados do Sentinel, consulte “Gerenciador de Dados do Sentinel” no Guia de Usuário do Sentinel Control Center.

2.10.2 Outras informações no banco de dados

O banco de dados do Sentinel inclui muitas outras informações como contas de usuário, informações de configuração, incidentes, workflows, dados de bens, dados de vulnerabilidade, etc. Deve ser feito backup de todos esses dados usando ferramentas comuns de banco de dados para recuperação em caso de falha. A Novell recomenda que uma estratégia de backup abrangente seja desenvolvida para o banco de dados do Sentinel inteiro (bem como para os servidores), exceto as tabelas particionadas acima.

Para o SQL Server, por padrão, os bancos de dados do Sentinel são criados de acordo com o modelo de recuperação completa. Segundo esse modelo, o espaço usado do Registro de Transações só é

liberado depois que um backup do Registro de Transações é executado. Para impedir que o Registro de Transações fique cheio, os backups do registro devem ser programados no SQL Server ao longo do dia (3 a 4 vezes por dia, dependendo da taxa de eventos). Se a sua organização não necessitar da capacidade de executar a recuperação de ponto de falha, você poderá comutar o modelo de recuperação de banco de dados para simples. Segundo o modelo simples de recuperação de banco de dados, o espaço do Registro de Transações será liberado automaticamente pelo SQL Server, sem quaisquer backups do registro.

2.10.3 Manutenção de banco de dados adicional

Além do backup, é necessário verificar regularmente se há consistência interna no banco de dados. A Novell fornece algumas ferramentas automatizadas para ajudar com essa tarefa. Para obter mais informações, consulte o Guia de Usuário do Sentinel.

Esses utilitários incluem:

- Analisar Partições - Reúne estatísticas de partições que foram recentemente preenchidas.
- Verificação da Saúde do Banco de Dados: reúne informações sobre o banco de dados. Ele relata:
  - Verifica se a instância do banco de dados está ativada
  - Verifica se a escuta do Oracle está ativada
  - Exibe o uso do espaço
  - Verifica se há índices não utilizáveis
  - Verifica se há objetos inválidos do banco de dados
  - Verifica se há análises do banco de dados

Observação: Esses utilitários não substituem a manutenção regular de banco de dados por um DBA qualificado.

Análise de banco de dados para Oracle

À medida que eventos são inseridos continuamente no banco de dados do Sentinel, as estatísticas do banco de dados devem ser atualizadas regularmente para garantir um bom desempenho de consulta. O Utilitário de Análise de banco de dados atualiza as estatísticas do banco de dados para dados de eventos no Oracle. Para a obtenção de um desempenho otimizado, esse utilitário deve ser programado para ser executado regularmente.

Observação: Esse utilitário inclui um script SQL necessário que pode ser atualizado periodicamente. É recomendável verificar periodicamente o site de Suporte Técnico da Novell (http://support.novell.com/techselect/index.html) para determinar se há atualizações.

Analisar partições

O script AnalyzePartitions.sh analisa partições que foram preenchidas recentemente. Este script deve ser programado diariamente por meio de cron ou outro programador para atualizar estatísticas de banco de dados nas partições preenchidas no dia anterior. É recomendável executar esse script em um horário do dia em que o uso de banco de dados seja baixo.

Esse script está localizado em $ESEC_HOME/bin. Ele deve ser executado localmente no servidor em que o banco de dados do Sentinel está instalado. A conta de usuário UNIX que executa o script deve poder se conectar ao banco de dados como sysdba (ex.: oracle).

Observação: Se tiver feito download de uma versão desse utilitário mais recente do que a versão instalada no momento no computador, você precisará instalar sp_esec_dba_utl.sql.

Para instalar sp_esec_dba_utl.sql:

1. Efetue login como proprietário do software Oracle.
2. Usando SQL*Plus, conecte-se ao banco de dados como Usuário do Banco de Dados do Sentinel.
3. Instale o pacote ESEC_DBA_UTL. No prompt do SQL (SQL>), digite:
   `@sp_esec_dba_utl.sql`
4. Saia doSQL*Plus.

Para executar AnalyzePartitions.sh:

1. Em seu servidor de banco de dados Oracle, vá para:
   `$ESEC_HOME/bin/`

   ou vá para o local onde você fez o download do arquivo mais recente.
2. No prompt de comando, digite o seguinte:

   Para Solaris:

   `./AnalyzePartitions.sh <ORACLE_SID> >> <LogFileName>`

   Para Linux:

   `ksh ./AnalyzePartitions.sh <ORACLE_SID> >> <LogFileName>`

   - ORACLE_SID - o nome da instância do Oracle para o banco de dados.
   - LogFileName - o nome do caminho completo para o arquivo em que você deseja que as mensagens de registro sejam gravadas.

   Se o script for bem-sucedido, sairá com o código de retorno 0. Se falhar, sairá com p código de retorno 1. Programe seus trabalhos de maneira adequada para verificar o código de retorno. Se o trabalho de análise falhar, consulte o arquivo de registro para obter mensagens de erro detalhadas.

2.10.4 Verificação de saúde de banco de dados para Oracle

dbHealthCheck.sh é um script que reúne informações sobre o banco de dados do Sentinel Oracle. O script dbHealthCheck.sh está localizado na pasta %esec_home%\bin. O script faz o seguinte:

- Verifica se a instância do banco de dados está ativada
- Verifica se a escuta do Oracle está ativada
- Exibe o uso do espaço
- Verifica se há índices não utilizáveis
- Verifica se há objetos inválidos do banco de dados
- Verifica se há análises do banco de dados

O script deve ser executado regularmente por meio de cron ou outro programador.

Observação: Essa ferramenta de utilitário, incluindo um script SQL necessário, pode ser atualizada periodicamente. É recomendável verificar periodicamente o site de Suporte Técnico da Novell (http://support.novell.com/techselect/index.html) para determinar se há atualizações.

Observação: Se tiver feito download de uma versão desse utilitário mais recente do que a versão instalada no momento no computador, você precisará instalar sp_esec_dba_utl.sql.

Para instalar 'sp_esec_dba_utl.sql':

1. Efetue login como proprietário do software Oracle.
2. No servidor de banco de dados, verifique se $ORACLE_HOME e $ORACLE_SID estão definidos no ambiente.
3. Usando SQL*Plus, conecte-se ao banco de dados como Usuário do Banco de Dados do Sentinel.
4. Instale o pacote ESEC_DBA_UTL. No prompt do SQL (SQL>), digite:

   ```
   @sp_esec_dba_utl.sql
   ```
5. Saia doSQL*Plus.

Para executar 'dbHealthCheck.sh':

Observação: O script deve ser executado com uma conta de proprietário do software Oracle ou qualquer outra conta que possa se conectar "COMO SYSDBA"

Observação: dbHealthCheck.sh deve ser executado localmente no servidor de banco de dados.

---

1. No servidor de banco de dados, verifique se $ORACLE_HOME e $ORACLE_SID estão definidos no ambiente.
2. Em seu Servidor de banco de dados Oracle, vá para:

   ```
   $ESEC_HOME/utilities/db/
   ```

   ou vá para o local onde você fez o download do arquivo mais recente.
3. No prompt de comando, digite o seguinte:

   Para Solaris:

   ```
   ./dbHealthCheck.sh
   ```

   Informações sobre o banco de dados do Sentinel serão exibidas na tela, ou você poderá gravar os resultados em um arquivo.

   ```
   ./dbHealthCheck.sh >> <filename>
   ```

   Para Linux:

   ```
   ksh ./dbHealthCheck.sh
   ```

   Informações sobre o banco de dados do Sentinel serão exibidas na tela, ou você poderá gravar os resultados em um arquivo.

   ```
   ksh ./dbHealthCheck.sh >> <filename>
   ```

2.10.5 Manutenção do Banco de Dados

O particionamento do banco de dados é configurado automaticamente quando o Sentinel é instalado. É recomendável que o administrador revise as configurações no Gerenciador de Dados do Sentinel e faça ajustes conforme necessário. Para obter mais informações sobre o Gerenciador de Dados do Sentinel, consulte "Gerenciador de Dados do Sentinel" no Guia de Usuário do Sentinel.

2.11 Mecanismo de Correlação

2.11.1 Sincronização de horário

O Mecanismo de Correlação do Sentinel é muito sensível ao horário, por isso a Novell recomenda enfaticamente que todas as máquinas do Mecanismo de Correlação e Gerenciador de Coletor sejam conectadas a um Servidor NTP (Network Time Protocol) ou outro tipo de Servidor de Horário. Para que o Mecanismo de Correlação do Sentinel funcione corretamente, o horário da máquina do sistema precisa estar sincronizado com diferença máxima de de ± 30 segundos em relação a todas as máquinas do Gerenciador de Coletor.

2.11.2 Uso da memória

Na linguagem da regra de correlação, os operadores "Window" e "Trigger" têm ambos uma janela de tempo associada a eles. Quanto maior for a janela de tempo, mais informações de eventos poderão ser armazenadas na memória para essa janela de tempo. Isso afeta a quantidade de memória necessária para fazer a correlação do Sentinel na memória. Se o Mecanismo de Correlação estiver usando memória demais, considere as seguintes opções:

- Instale o Mecanismo de Correlação em uma máquina dedicada e redistribua todas as regras atuais para o novo Mecanismo de Correlação.
- Instale um novo Mecanismo de Correlação e redistribua as regras atuais selecionadas para o novo Mecanismo de Correlação.
- Ajuste a cláusula Janela de suas Regras de Correlação.
  - Torne o filtro para eventos passados mais específico
  - Diminua o tamanho da janela de tempo.
- Ajuste a cláusula Acionador de suas Regras de Correlação.
  - Diminua o tamanho da janela de tempo.
  - Diminua o limite do número de eventos necessários para acionar a regra.
  - Escolha discriminadores com menor importância (ex.: Tipo de Dispositivo).
  - Se seu discriminador tiver pequena importância (por exemplo, Endereço IP de Origem), diminua o limite do número de eventos necessário para acionar a regra e, ao mesmo tempo, diminua o tamanho da janela de tempo para obter um resultado equivalente.

2.11.3 Análise de curto-circuito

As comparações numéricas são mais rápidas do que comparações de string e as comparações de string são mais rápidas do que as comparações de expressões regulares. A operação dfe Filtro

executa uma análise de curto-circuito nas expressões Booleanas. Ordenando cuidadosamente sua expressão, você pode tornar a avaliação mais rápida.

2.11.4 Regras de formato livre

Se você não puder expressar uma regra de correlação usando o Assistente de Regra de Correlação, construa uma regra de formato livre usando a linguagem de regra de correlação. Para obter mais informações sobre como criar uma regra de formato livre, consulte “Mecanismo de Correlação” no Guia de Referência.

2.12 Arquivos de registro do Sentinel

É uma boa prática revisar periodicamente os arquivos de registro gerados pelo Sentinel em busca de erros. Para obter mais informações sobre esses arquivos e seus locais, consulte “Locais de registro do Sentinel” no Guia de Referência.

Instalando o Sentinel 6

3

Tópicos incluídos neste capítulo:

- Seção 3.1, “Instalar o Sentinel no Linux, Solaris e Windows” na página 43
- Seção 3.1.2, “Pré-requisitos para instalar Sentinel 6.0” na página 45
- Seção 3.2, “Instale o Oracle no Linux, SUSE Linux, Redhat Linux e Solaris” na página 48
- Seção 3.2.5, “Instalação do Oracle” na página 51
- Seção 3.3, “Instalando o Sentinel” na página 57
- Seção 3.3.1, “Instalação Simples” na página 58
- Seção 3.3.2, “Instalação Personalizada” na página 60
- Seção 3.4, “Configuração de pós-instalação” na página 70

3.1 Instalar o Sentinel no Linux, Solaris e Windows

Este capítulo ajuda você a instalar o Sentinel para Oracle no SUSE Linux Enterprise Server, Red Hat Enterprise Linux e Solaris e Microsoft SQL Server no Windows.

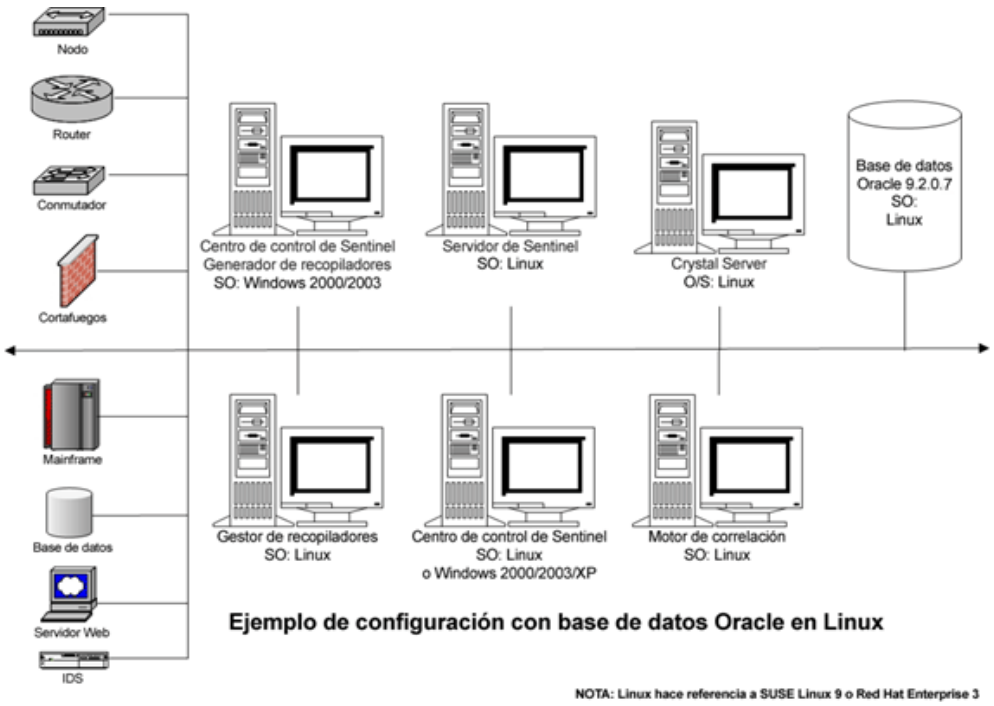
Ao realizar uma instalação limpa do Sentinel depois de ter desinstalado uma versão anterior do Sentinel, você deve remover manualmente certos arquivos e configurações de sistema que possam ter restado. Para obter mais informações sobre como desinstalar o Sentinel 6.0, consulte Capítulo 11, “Desinstalando o Sentinel” na página 149. Para obter informações sobre como desinstalar versões anteriores de Sentinel, consulte as versões de documento relacionadas disponíveis no site da Documentação da Novell no endereço http://www.novell.com/documentation/ (http://www.novell.com/documentation/).

Observação: Para instalar o Sentinel Server no SLES, a Novell recomenda usar qualquer sistema de arquivos que não seja ReiserFS, pois a Novell observou problemas intermitentes ao executar Sentinel no SLES com ReiserFS. Embora haja várias opções, os testes internos do Sentinel da Novell foram realizados usando o sistema de arquivos ext3.

3.1.1 Configuração do Sentinel

A seguir estão configurações típicas do Linux para Sentinel. A configuração pode ser diferente, dependendo do ambiente. Independentemente da configuração escolhida, é necessário instalar o banco de dados primeiro.

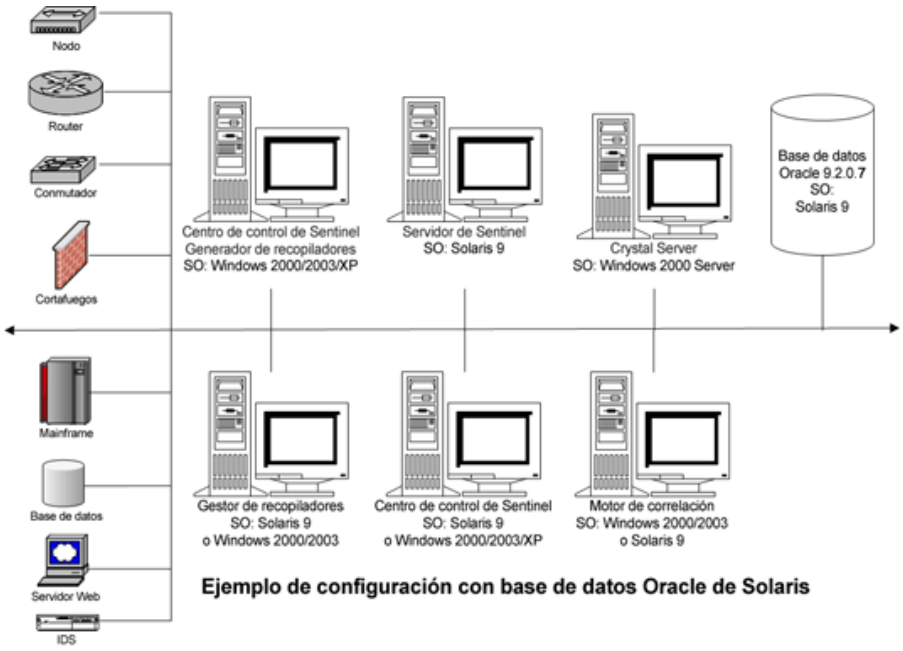
No Linux



Ejemplo de configuración con base de datos Oracle en Linux

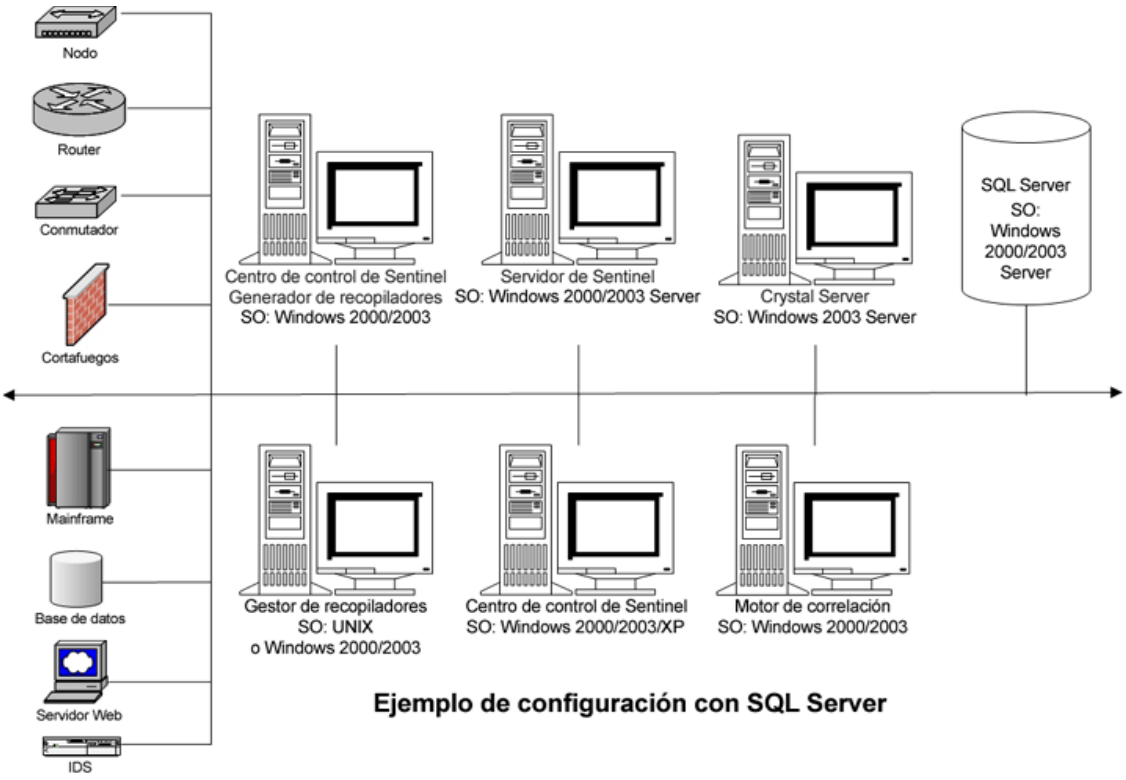
NOTA: Linux hace referencia a SUSE Linux 9 o Red Hat Enterprise 3

No Solaris



Ejemplo de configuración con base de datos Oracle de Solaris

No Windows



Ejemplo de configuración con SQL Server

3.1.2 Pré-requisitos para instalar Sentinel 6.0

Antes de instalar Sentinel, verifique se:

- Suas máquinas atendem aos requisitos mínimos e se o sistema operacional foi "reforçado" com as melhores práticas de segurança atuais. Para obter maiores informações, consulte Capítulo 2, “Melhores práticas” na página 17
- Para instalar o Sentinel no Solaris e Linux, instale o Oracle Enterprise com particionamento. O Gerenciador de Dados do Sentinel precisa desse recurso para gerenciar o Banco de dados do Sentinel.
- Você atendeu as condições necessárias para instalar o seguinte:
  - Banco de Dados do Sentinel
  - Sentinel Server
  - Sentinel Control Center e Construtor de Coletor do Sentinel
  - Sentinel Advisor
- Você instalou o Oracle no Linux, SUSE Linux, Red Hat Linux e Solaris.

Banco de Dados do Sentinel

Antes de instalar o Banco de Dados do Sentinel, é necessário:

No Linux/Solaris:

- No Linux, ter as credenciais de login do usuário do sistema operacional Oracle (padrão: oracle).
- No Solaris:
  - Ter uma cópia de Oracle 148673.1 SOLARIS: Guia de Início Rápido
  - Ter um usuário do sistema operacional Oracle (padrão: oracle).
- No Linux/Solaris, verifique se as seguintes variáveis do ambiente estão definidas para o usuário do sistema operacional Oracle:
  - ORACLE_HOME (por ex.: echo $ORACLE_HOME resulta em /opt/oracle/product/10gR2/db)
  - ORACLE_BASE (Por ex.: eco $ORACLE_BASE resulta em /opt/oracle)
  - PATH (é preciso ter $ORACLE_HOME/bin)
- Embora NÃO seja recomendável, se você pretende criar manualmente a instância do banco de dados do Oracle na qual o banco de dados do Sentinel será instalado, consulte "Criação de banco de dados e configuração para altas taxas de eventos", para obter instruções sobre como criar sua instância do Oracle para que ela seja compatível com o Sentinel. Se você escolher essa opção, ainda deverá usar o instalador do Sentinel para adicionar os objetos do banco de dados à instância do banco de dados do Oracle manualmente criada. Para obter maiores informações, consulte Seção 3.3.2, "Instalação Personalizada" na página 60

Observação: Caso esteja usando uma instância de banco de dados Oracle existente ou criada manualmente, ela precisa estar vazia, exceto pela presença do Usuário do Banco de Dados do Sentinel.

No Windows:

- No Windows, tenha o SQL Server 2005 SP1 instalado e em execução.

Observação: Por motivos de desempenho, é ALTAMENTE recomendável que, se estiver instalando em RAID ou se seu ambiente RAID permitir, você configure o sistema para que o Registro de Transação aponte para o disco de gravação mais rápido disponível, um disco físico separado em que os arquivos do banco de dados são armazenados.

- No Windows, você precisa instalar o SQL Server com autenticação de modo misto para fazer login usando a autenticação do Windows ou do SQL Server. Se você instalar o SQL Server no modo não misto, poderá fazer login usando a Autenticação do Windows apenas.
- Para modificar suas configurações de modo de autenticação:
  - No Microsoft SQL Server Management Studio, clique com o botão direito do mouse no servidor cujas configurações você gostaria de modificar.
  - Selecione propriedades e clique em Segurança.
  - Das duas opções, selecione Modo de Autenticação do SQL Server e do Windows ou Modo de Autenticação do Windows para Autenticação.
  - Assegure-se também de que o serviço MSSQLSERVER faz login usando a Conta de Sistema Local.
- Determine o Nome de Instância do SQL Server (padrão recomendado).

Observação: Se você tiver especificado o nome da instância durante a instalação do servidor SQL, use esse nome ao ser solicitado a fornecer o nome da instância do Servidor SQL ao instalar os componentes do Banco de Dados do Sentinel e/ou do DAS. Se não tiver especificado o nome da instância durante a instalação do Servidor SQL, deixe o nome da instância em branco durante a instalação (ou seja, se digitar o nome de host, não adicione "\<nome_da_instância>" ao nome do host do banco de dados).

- Determine o número da porta da instância do servidor SQL (o padrão é 1433).
- Se você usar a Autenticação do Windows para um ou mais dos usuários do Sentinel usados durante a instalação do Sentinel, o usuário de Domínio do Windows correspondente deve existir antes de instalar o Banco de Dados do Sentinel. Os usuários do Sentinel a seguir podem ser atribuídos a um usuário do domínio Windows:
  - Administrador do Banco de Dados do Sentinel (esecdba, o proprietário do esquema do Banco de Dados)
  - Usuário do Aplicativo do Sentinel (esecapp, usado por aplicativos do Sentinel para se conectar ao banco de dados)
  - Administrador do Sentinel (esecadm, Administrador para fazer login no Sentinel Control Center)
  - Usuário do Sentinel Report (esecrpt, usado para criar relatórios)

Observação: O banco de dados conterá o usuário Administrador do Banco de Dados do Sentinel, o Usuário do Aplicativo do Sentinel e o Usuário Administrador do Sentinel por padrão.

Observação: O Sentinel não suporta cluster da Microsoft ou Alta Disponibilidade para Windows.

Sentinel Server

Observação: Se o Banco de Dados do Sentinel não for instalado na mesma máquina que o Sentinel Server, você deve instalar o Banco de Dados do Sentinel primeiro.

- Se for instalar o componente DAS, tenha o Número de Série e chave de Licença (para o DAS).
- Escolha um Servidor SMTP (Nome do DNS). Isso é obrigatório para enviar e-mails do Sentinel.
- No Windows, conceda a um usuário o privilégio "Fazer login como um Serviço", se estiver instalando DAS e usando uma conta de usuário de Domínio do Windows para o Aplicativo Sentinel. Para oferecer esse privilégio:
  - Adicione o usuário em 'Política de Segurança Local" na máquina em que você instalará o DAS (Iniciar > Configurações > Painel de Controle > Ferramentas Administrativas > Política de Segurança Local).
  - Na janela Política de Segurança Local, vá até Políticas Locais > Atribuição de Direitos do Usuário.
  - Clique duas vezes em Efetuar logon como política de serviço e adicione o usuário.

Consultor

Para instalar o Consultor, será necessário um ID e senha do Consultor do Sentinel. Você recebe o ID e a senha do Consultor ao comprar o software. Se você escolher Download Direto da Internet, use a porta de saída 443. Você deve ter software Crystal Enterprise instalado em seu sistema para executar relatórios.

Observação: Caso pretenda usar o Advisor para o Exploit Detection somente, não é necessário instalar o software Crystal Enterprise. Para obter maiores informações, consulte Capítulo 4, "Configuração do Advisor" na página 73.

3.2 Instale o Oracle no Linux, SUSE Linux, Redhat Linux e Solaris

Para instalar o Oracle no Linux/Solaris, certifique-se de:

- Definir valores do Kernel
- Configurar arquivo init.ora no Linux
- No Solaris:
  - Criar uma conta de Grupo e de Usuário do Oracle
  - Definir as variáveis de ambiente
  - Verificar o layout do Solaris
- Instalação do Oracle 9.2.0.4
- Aplicar patches no Oracle 9.2.0.7

3.2.1 Definir valores do Kernel

Importante: Os valores de Kernel sugeridos nesta seção são apenas valores mínimos. Essas configurações devem ser mudadas somente se as configurações de seu sistema forem menores que os valores mínimos recomendados, e somente após consultar seu administrador de sistema e a documentação do Oracle

---

Para definir os valores do Kernel no Solaris:

No Solaris, os valores de kernel a seguir devem estar definidos em /etc/system.

shmmax=4294967295	semmni=1024
shmmin=1	semmsl=1024
shmseg=50	shmopm=100
shmmni=400	shmvmx=32767
semmns=14000	

1. Efetue login como Usuário Root.
2. Faça uma cópia de backup de /etc/system.

3 Usando um editor de texto, mude as configurações do parâmetro de kernel no arquivo /etc/system conforme a tabela acima.

4 Reinicializar.

Para definir os valores do Kernel no Linux:

No Solaris, os valores de kernel a seguir devem estar definidos em /etc/system.

shmmax=2147483648 (valor mínimo)	semmni=1024
shmmni=4096	semmsl=1024
semmns=32000	semopm=100

1 Efetue login como Usuário Root.

2 Para definir os parâmetros de kernel, adicione o texto a seguir ao final do arquivo "/etc/sysctl.conf":

Observação: Para determinar a configuração atual de um determinado parâmetro de kernel, execute o comando:

sysctl <parâmetro_do_kernel>

Por exemplo, para verificar o valor atual do parâmetro de kernel "kernel.sem", execute o comando: sysctl kernel.sem

No SUSE LINUX

```
kernel.sem = 1024        32000   100      1024
kernel.shmmax = 2147483648
kernel.shmmni = 4096
vm.disable_cap_mlock=1
```

No REDHAT LINUX

```
# Kernel settings for Oracle
# kernel.sem = <SEMMSL> <SEMMNS> <SEMOPM> <SEMMNI>
kernel.sem = 1024        32000   100      1024
kernel.shmmax = 2147483648
kernel.shmmni = 4096
fs.file-max = 65536
net.ipv4.ip_local_port_range = 1024 65000
```

3 Execute o comando a seguir para carregar as modificações no arquivo "/etc/sysctl.conf":

```
sysctl -p
```

4 Para definir os manipuladores de arquivo e limites de processo, adicione o texto a seguir ao final do arquivo "/etc/security/limits.conf". "nproc" é o limite máximo do número de processos, e "nofile" é o limite máximo do número de arquivos abertos. Trata-se de valores recomendados, mas que podem ser modificados se necessário.

```
# Settings added for Oracle
oracle          soft    nproc   16384
oracle          hard    nproc   16384
oracle          soft    nofile  65536
oracle          hard    nofile  65536
```

3.2.2 Criar Grupo e Conta de Usuário do Oracle no Solaris

Para criar um grupo e conta de usuário e definir variáveis de ambiente:

1. Efetue login como Usuário Root.
2. Crie um grupo UNIX e uma conta de usuário UNIX para o proprietário do banco de dados Oracle.
   - Adicione um grupo dba (como root):
     `groupadd –g 400 dba`
   - Adicione o usuário do Oracle (como root):
     `useradd –g dba –d /export/home/oracle –m –s /bin/csh oracle`

3.2.3 Definindo variáveis de ambiente para Oracle no Solaris

Para definir variáveis de ambiente:

1. Efetue login como Usuário Root.
2. Para definir as variáveis de ambiente necessárias para o Oracle, sugerimos adicionar as seguintes informações ao arquivo local.cshrc:

```
umask 022
setenv ORACLE_HOME /opt/oracle
setenv ORACLE_SID ESEC
setenv LD_LIBRARY_PATH ${ORACLE_HOME}/lib
setenv DISPLAY :0.0
set path=(/bin /bin/java /usr/bin /usr/sbin ${ORACLE_HOME}/bin /
usr/ucb/etc.)
if ( $?prompt ) then
set history=32
endif
```

3.2.4 Verificar o layout do Solaris

Para definir variáveis de ambiente:

1. Vá até o site da Sun na internet e faça o download do conjunto de patches recomendado para o Solaris 9:
   - DATA de Cluster de Patch: 03/05/05

   Observação: Consulte o arquivo README e a documentação adicional incluída. É ALTAMENTE recomendável que um backup completo do sistema seja feito antes da aplicação de patches.

   ---

2. Efetue login como Usuário Root e instale o cluster de patches aplicável e os patches de kernel.
3. Após a conclusão dos patches, apague o arquivo *_Recommended.zip e os arquivos estendidos contidos nos diretórios criados pelo patch e reinicialize o servidor.

3.2.5 Instalação do Oracle

Esta seção explica como instalar o Oracle no:

- SUSE Linux
- Red Hat Linux
- Solaris

Importante: As instruções a seguir não têm por objetivo substituir a documentação do Oracle. Trata-se apenas de um exemplo de cenário de configuração. Recomenda-se enfaticamente que essas instruções sejam seguidas. Esta documentação supõe que o diretório pessoal dos usuários do Oracle é /home/oracle e que o Oracle será instalado em /Opt/oracle. Sua configuração específica pode ser diferente. Consulte a documentação do sistema operacional e do Oracle para obter mais informações.

No SUSE Linux (SLES 9 SP3)

Para instalar o Oracle no SUSE Linux:

1. Siga as instruções de instalação fornecidas no manual de instalação do SLES 9. Instale o SLES 2 com os pacotes padrão junto com Ferramentas e Compilador C/c++ e SP2.

   Observação: Se você já tiver instalado o SUSE Linux, pode usar o YaST (Yet Another Setup Tool - Mais uma Ferramenta de Configuração) na GUI do SUSE Linux para instalar Ferramentas e Compilador C/C++.

   ---

2. Efetue login como Usuário Root.
3. Instale gcc_old usando YaST.
4. Verifique se está executando o SP3 digitando:

   ```
   SPident
   ```

   ou

   ```
   cat /etc/SuSE-release
   ```

   Deve aparecer:

   ```
   CONCLUSION: System is up-to-date!
         Found     SLES-9-i386-SP3
   ```

   ou

   ```
   SUSE LINUX Enterprise Server (i586)
   VERSION = 9
   PATCHLEVEL = 3
   ```

5. Para automatizar a maioria das tarefas de pré-instalação do Oracle e criar o usuário oracle, instale orarun.rpm, incluído no SLES 9.

   Observação: Consulte o documento de instalação do Oracle para obter uma lista completa dos pré-requisitos.

   ```
   rpm -i <path>/orarun-1.8-109.15.i586.rpm
   ```

   Observação: orarun também está disponível em http://www.novell.com (http://www.novell.com).

   ---

6. A conta do usuário oracle está desativada. Ative-a alterando o shell para o usuário oracle de /bin/false para /bin/bash usando a administração de usuário do YaST ou editando o /etc/passwd.
7. Defina uma nova senha para o usuário oracle usando o YaST ou digitando:
   ```
   /usr/bin/passwd oracle
   ```
8. Para definir os parâmetros de kernel, execute
   ```
   /usr/sbin/rcoracle start
   ```
   Ignore qualquer erro.
   ```
   /sbin/chkconfig oracle on
   ```
9. Mude o usuário do Oracle:
   ```
   su - oracle
   ```
10. Para instalar o Oracle 9.2.0.4, de dentro do Disk1, execute o script:
    ```
    ./runinstaller
    ```
11. Ao avançar no instalador, deixe todos os prompts em seus valores padrão, salvo se houver especificação em contrário abaixo.
    - Ao ser solicitado a fornecer o Nome do Grupo UNIX, digite: dba
    - Ao ser solicitado a fornecer o Tipo de Instalação, escolha Personalizada.

    Selecione os componentes a seguir para serem instalados:
    - Oracle 9i 9.2.0.4.0
    - Opções do Enterprise Edition 9.2.0.1.0
      - Particionamento do Oracle 9i 9.2.0.4.0
    - Serviços de rede do Oracle 9.2.0.1.0
      - Escuta de rede do Oracle 9.2.0.4.0
    - Produtos do Oracle Enterprise Manager 9.2.0.1.0 (Todos)
    - Oracle 9i Development Kit 9.2.0.1.0 (Todos)
    - Oracle 9i para Documentação do UNIX 9.2.0.1.0
    - Servidor HTTP do Oracle 9.2.0.1.0 (Todos)
    - iSQL*Plus 9.2.0.4.0 (Todos)
    - Interfaces do Oracle JDBC/OCI 9.2.0.1.0
12. Na solicitação para criar banco de dados, escolha NÃO.
13. Opcional, cancele todos os assistentes de configuração que o instalador iniciar.
14. Modifique o arquivo '/opt/oracle/network/admin/sqlnet.ora' (ou crie o arquivo se ele não existir) para que contenha o seguinte (remova qualquer informação sem comentário existente no arquivo):
    ```
    NAMES.DIRECTORY_PATH = (TNSNAMES, HOSTNAME)
    ```
15. Para aplicar o patch do Oracle 9.2.0.7 ao Oracle, de dentro do Disk1 da distribuição de patch do Oracle 9.2.0.7, execute o script:
    ```
    ./runInstaller
    ```
16. Ao avançar no instalador, deixe todos os prompts em seus valores padrão, salvo se houver especificação em contrário abaixo.
    - Na tela de boas-vindas, clique em Avançar.

- Na tela Especificar Locais de Arquivos, escolha “OUIHome” como Nome de Destino na lista suspensa (ou o que você usar como Nome de Destino durante a instalação do Oracle 9.2.0.4). Clique em Avançar.
- Dependendo da versão, na tela Selecionar Produto para Instalar, escolha Oracle 9iR2 Patchset 9.2.0.7.0. Depois, clique em Avançar.
- Na tela Resumo, revise o resumo de instalação e clique em Instalar.
- Na tela Fim da Instalação, clique em Sair.

17 Edite o arquivo init.ora para especificar o caminho de diretório no qual os dados de Sentinel arquivados devem ser gravados. Essa informação é especificada no parâmetro UTL_FILE_DIR. Você deve ter um dos seguintes:

- UTL_FILE_DIR = *

  ou

- UTL_FILE_DIR = <caminho de diretório específico>

No SUSE Linux (SLES 10)

Para instalar o Oracle no SUSE Linux:

1 Siga as instruções de instalação fornecidas no manual de instalação do SLES 10. Instale o SLES 10 com os pacotes padrão junto com Oracle Server Base, Compilador C/C++ e Ferramentas.

2 Efetue login como Usuário Root.

3 Instale o Service pack do SLES 10. Verifique as informações do service pack digitando:

```
SPident
```

ou

```
cat /etc/SuSE-release
```

Na data desta documentação, o service pack do SLES 10 não havia sido lançado. Use SPident ou o lançamento cat/etc/SUSE para verificar.

Deve aparecer:

```
CONCLUSION: System is up-to-date!
      Found     SLES-10-x86_64-current
```

4 Para automatizar a maioria das tarefas de pré-instalação do Oracle e criar o usuário oracle, instale orarun.rpm, incluído no SLES 9.

Observação: Consulte o documento de instalação do Oracle para obter uma lista completa dos pré-requisitos.

```
rpm -ivh/orarun-1.9-21.2.x86_64.rpm
```

Observação: orarun também está disponível no endereço http://www.novell.com (http://www.novell.com).

---

5 A conta do usuário oracle está desativada. Ative-a, alterando o shell do usuário oracle de /bin/false para /bin/bash usando a administração de usuário do YaST ou editando o arquivo /etc/passwd.

6 Defina uma nova senha para o usuário oracle usando o YaST ou digitando:

```
/usr/bin/passwd oracle
```

7. Altere o ambiente do Oracle padrão definido pelo orarun, caso necessário:
   - Altere o diretório pessoal do Oracle editando a variável ORACLE_HOME no arquivo '/etc/profile.d/oracle.sh'.
   - O ORACLE_SID padrão definido pela instalação do orarun é 'orcl'. Mude-o para ESEC no arquivo '/etc/profile.d/oracle.sh'.
8. Para definir os parâmetros de kernel, execute
   ```
   /usr/sbin/rcoracle start
   ```
9. Mude o usuário do Oracle:
   ```
   su - oracle
   ```
10. Mude para diretório do banco de dados e execute./runinstaller (Oracle Universal Installer) Um erro ocorrerá conforme mostrado abaixo:
11. Corrija o erro, executando um destes procedimentos:
    - Modifique o arquivo "database/install/oraparam.ni" para adicionar suporte ao SUSE Linux 10. Depois de modificar o arquivo oraparam.ini, a linha "[Versões Certificadas]" estará assim:
      ```
      [Certified Versions]
      Linux=redhat=3,SuSE-9,SuSE-10,redhat-4,UnitedLinux-1.0.asianux-1,asianux-2
      ```
    - Instale com a opção -ignoreSysPrereqs
      ```
      i.e. ./runInstaller –ignoreSysPrereqs
      ```
12. Aceite o diretório de inventário padrão ou Procure e selecione um novo diretório. Clique em Avançar.
13. Nos Tipos de instalação, selecione Enterprise Edition. Clique em Avançar.
14. Para verificar os requisitos de configuração de Rede, selecione Verificado pelo Usuário. Clique em Avançar.
15. Nas opções de Configuração, selecione Instalar Software de Banco de Dados apenas. Clique em Avançar.
16. O resumo da Instalação será exibido. Revise e clique em Instalar.
17. Execute os scripts especificados como raiz e clique em OK ao concluir.
18. Quando a instalação for concluída com sucesso, clique em Sair.

No Red Hat Linux

Para instalar o Oracle no Red Hat Linux:

1. Efetue login como Usuário Root.
2. Crie um grupo UNIX e uma conta de usuário UNIX para o proprietário do banco de dados Oracle.

   Adicione um grupo dba (como root):
   ```
   groupadd dba
   ```
3. Adicione o usuário do Oracle (como root):
   ```
   useradd –g dba –s /bin/bash –d /home/oracle –m oracle
   ```
4. Crie um diretório para ORACLE_HOME e ORACLE_BASE:
   ```
   mkdir –p /opt/oracle/
   ```

5 Mude a propriedade do diretório ORACLE_BASE e complete para o oracle/dba:

```
chown -R oracle:dba /opt/oracle
```

6 Mude o usuário do Oracle:

```
su - oracle
```

7 Abra o arquivo '.bash_profile' (no diretório pessoal do usuário do Oracle) para editá-lo e adicione o seguinte ao final do arquivo:

Observação: Esse conjunto de variáveis de ambiente somente devem ser usadas para o usuário do Oracle. Especificamente, elas não devem ser definidas no ambiente de sistema nem no ambiente de Usuário do Administrador do Sentinel.

```
# Set the LD_ASSUME_KERNEL environment variable only for Red Hat 9,
# RHEL AS 3, and RHEL AS 4 !!
# Use the "Linuxthreads with floating stacks" implementation
instead of NPTL:
# for RH 9 and RHEL AS 3
export LD_ASSUME_KERNEL=2.4.1
# for RHEL AS 4
# export LD_ASSUME_KERNEL=2.4.19
# Oracle Environment
export ORACLE_BASE=/opt/oracle
export ORACLE_HOME=$ORACLE_BASE/
export ORACLE_SID=test
export ORACLE_TERM=xterm
# export TNS_ADMIN= Set if sqlnet.ora, tnsnames.ora, etc. are not
in $ORACLE_HOME/network/admin
export NLS_LANG=AMERICAN;
export ORA_NLS33=$ORACLE_HOME/ocommon/nls/admin/data
LD_LIBRARY_PATH=$ORACLE_HOME/lib:/lib:/usr/lib
LD_LIBRARY_PATH=$LD_LIBRARY_PATH:/usr/local/lib
export LD_LIBRARY_PATH
# Set shell search paths
export PATH=$PATH:$ORACLE_HOME/bin
```

8 Repita o login como usuário do Oracle para carregar mudanças de variáveis de ambiente a partir da última etapa:

```
exit
su - oracle
```

9 Vincule o gcc com a versão 2.9.6

Observação: Se /usr/bin/gcc296 ou /usr/bin/g++296 não existir, gcc ou g++ não foi instalado. Nesse caso, instale esses componentes e retorne para essa etapa.

```
su - root
ln -s /usr/bin/gcc296 /usr/bin/gcc
ln -s /usr/bin/g++296 /usr/bin/g++
```

10 Saia para retornar ao prompt de usuário do Oracle.

```
exit
```

11 Execute o patch p3006854_9204_LINUX.zip do Oracle, que aplica o patch do sistema operacional Linux para a instalação do Oracle. Esse patch pode ser obtido com a Oracle.

```
su - root
unzip p3006854_9204_LINUX.zip
```

```
cd 3006854
sh rhel3_pre_install.sh
```

12 Saia para retornar ao prompt de usuário do Oracle.

```
exit
```

13 Para instalar o Oracle 9.2.0.4, de dentro do Disk1, execute o script:

```
./runInstaller
```

14 Ao avançar no instalador, deixe todos os prompts em seus valores padrão, salvo se houver especificação em contrário abaixo.

- No prompt Nome do Grupo UNIX, digite: dba
- Ao ser solicitado a fornecer o Tipo de Instalação, escolha Personalizada.

Selecione os componentes a seguir para serem instalados:

- Oracle 9i 9.2.0.4.0
- Opções do Enterprise Edition 9.2.0.1.0
  - Particionamento do Oracle 9i 9.2.0.4.0
- Serviços de rede do Oracle 9.2.0.1.0
  - Escuta de rede do Oracle 9.2.0.4.0
- Produtos do Oracle Enterprise Manager 9.2.0.1.0 (Todos)
- Oracle 9i Development Kit 9.2.0.1.0 (Todos)
- Oracle 9i para Documentação do UNIX 9.2.0.1.0
- Servidor HTTP do Oracle 9.2.0.1.0 (Todos)
- iSQL*Plus 9.2.0.4.0 (Todos)
- Interfaces do Oracle JDBC/OCI 9.2.0.1.0

15 Ao ser solicitado a criar banco de dados, escolha NÃO.

16 Opcional, cancele todos os assistentes de configuração que o instalador iniciar

17 Modifique o arquivo '/opt/oracle/network/admin/sqlnet.ora' (ou crie o arquivo se ele não existir) para que contenha o seguinte (remova qualquer informação sem comentário existente no arquivo):

```
NAMES.DIRECTORY_PATH = (TNSNAMES, HOSTNAME)
```

18 Para aplicar o patch do Oracle 9.2.0.7 ao Oracle, de dentro do Disk1 da distribuição de patch do Oracle 9.2.0.7, execute o script:

```
./runInstaller
```

19 Ao avançar no instalador, deixe todos os prompts em seus valores padrão, salvo se houver especificação em contrário abaixo.

- Na tela de boas-vindas, clique em Avançar.
- Na tela Especificar Locais de Arquivos, escolha "OUIHome" como Nome de Destino na lista suspensa (ou o que você usar como Nome de Destino durante a instalação do Oracle 9.2.0.4). Clique em Avançar.
- Dependendo da versão, na tela Selecionar Produto para Instalar, escolha Oracle 9iR2 Patchset 9.2.0.7.0. Depois, clique em Avançar.
- Na tela Resumo, revise o resumo de instalação e clique em Instalar.
- Na tela Fim da Instalação, clique em Sair.

20 Desvincule o gcc:

```
su – root
rm /usr/bin/gcc
rm /usr/bin/g++
```

21 Saia para retornar ao prompt de usuário do Oracle.

```
Exit
```

22 Edite o arquivo init.ora para especificar o caminho do diretório no qual os dados do Sentinel arquivados devem ser gravados. Essas informações são especificadas no parâmetro UTL_FILE_DIR. Você deve ter um dos seguintes:

- UTL_FILE_DIR = *

ou

- UTL_FILE_DIR = [caminho de diretório específico

No Solaris

Para instalar Oracle no Solaris:

1 Efetue login como Usuário Root.

2 Siga as etapas descritas em Oracle Note: 148673.1 SOLARIS: Guia de Início Rápido.

3 Instale o Oracle 9i Release 2 (9.2.0.1) com o usuário oracle. Serão solicitados dois CD-ROMs adicionais. Você precisará navegar até diferentes diretórios para cada um dos CD-ROMs adicionais.

4 Aplique patches no seu sistema para Oracle 9.2.0.7. Consulte a documentação do Oracle para saber sobre os procedimentos de aplicação de patches.

5 Para verificar o nível de patch, como o usuário do Oracle UNIX, digite:

```
sqlplus '/as sysdba'
```

Os resultados devem indicar a versão 9.2.0.7. Para sair, digite quit.

6 Remova o diretório criado para o patch.

7 Depois de instalar os patches, remova os diretórios e arquivos dos patches.

8 Edite o arquivo init.ora para especificar o caminho de diretório no qual os dados de Sentinel arquivados devem ser gravados. Essas informações são especificadas no parâmetro UTL_FILE_DIR. Você deve ter um dos seguintes:

- UTL_FILE_DIR = *

ou

- UTL_FILE_DIR = [caminho de diretório específico]

9 Reinicializar.

3.3 Instalando o Sentinel

O Sentinel dá suporte a dois tipos de instalação. São eles:

- **Simples:** A opção de instalação completa. Serviços do Sentinel, Serviço do Coletor e Aplicativos do Oracle na mesma máquina. O tipo de instalação se destina a fins demonstrativos apenas.
- **Personalizada:** Permite uma instalação totalmente distribuída.

3.3.1 Instalação Simples

Depois de atender aos pré-requisitos mencionados na seção anterior, você pode continuar a instalação do Sentinel.

Para instalar o Sentinel:

1. Efetue login como usuário root no Solaris/Linux ou usuário administrador no Windows.
2. Insira e monte o CD de instalação do Sentinel.
3. No Linux/Solaris, verifique se o sistema umask está definido como 0027 executando o comando a seguir no mesmo prompt de comando de onde você executará o instalador:

   ```
   umask 0027
   ```
4. Para iniciar o programa de instalação, vá para o diretório de instalação no CD-ROM e
   - No Windows, execute setup.bat
   - No Solaris/Linux:

   Para o modo de interface gráfica:

   ```
   ./setup.sh
   ```

   ou

   Para o modo baseado em texto ("console serial"):

   ```
   ./setup.sh –console
   ```
5. Clique na seta para baixo e selecione uma das seguintes opções de idioma:

Inglês	Italiano
francês	Português (Brasil)
Alemão	Espanhol
Chinês Simplificado	Japonês
Chinês Tradicional	

6. Depois de ler a tela de boas-vindas, clique em Avançar.
7. Leia e aceite o Contrato de Licença de Usuário Final e clique em Próximo.
8. Aceite o diretório de instalação padrão ou clique em Procurar para especificar o local da instalação. Clique em Avançar.
9. Selecione Simples. Clique em Avançar.
10. Nessa tela, digite as informações de configuração e clique em Próximo.
    - Número de Série
    - Chave de Licença
    - SMTP Server
    - E-mail

      O IP do Servidor SMTP ou nome DNS digitado aqui ajudará você a configurar o envio de e-mails do Sentinel por meio do ID de e-mail digitado.
    - Senha do Sistema Global

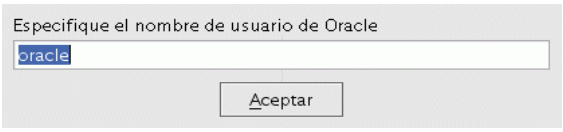
A senha que você digitou aqui será válida para todos os usuários padrão. Isso inclui o usuário do Administrador do Sentinel e os usuários do banco de dados. Para obter mais informações sobre a lista de usuários de banco de dados padrão criados com a instalação, consulte Seção 3.4.2, “Banco de Dados do Sentinel” na página 71.

- Nome de usuário e Senha do Consultor

  Para instalar o Consultor, digite o Nome de Usuário e Senha fornecidos quando você adquiriu o software. Se o nome de usuário ou senha não puder ser verificado, após clicar em Avançar você será perguntado se deseja continuar (não recomendado). Se optar por continuar, digite a senha do Advisor novamente na janela de confirmação de senha.

Observação: Se estiver instalando o Consultor, a opção de instalação Simples configurará o Consultor para que use o Download Direto da Internet com um intervalo de atualização de 12 horas e todas as notificações de e-mail habilitadas.

No Solaris/Linux, você será solicitado a especificar o nome de usuário do Oracle. Digite o nome de usuário e clique em OK.

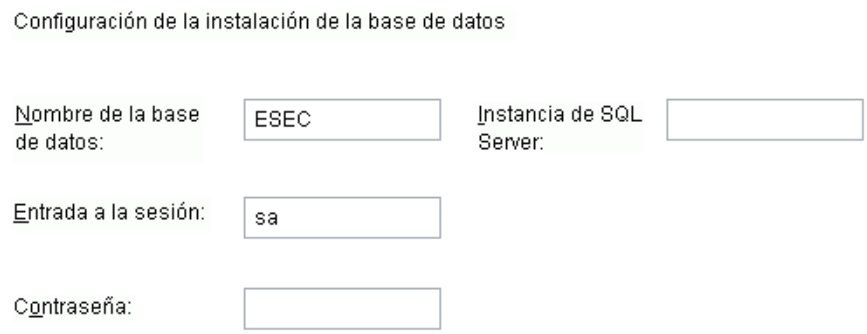


11 Para configuração do banco de dados:

- Selecione a plataforma de Banco de dados de destino.
- Digite nome de banco de dados
  - No Linux/Solaris, especifique o Arquivo de Driver JDBC do Oracle.
  - No Windows, digite credenciais do usuário do Banco de Dados e nome de instância do SQL Server.

Clique em Avançar.

O tamanho do BD para a Instalação Simples é 10 GB.



12 O resumo dos parâmetros do banco de dados selecionados será exibido. Clique em Avançar.:

13 O resumo da instalação será exibido. Clique em Instalar.

14 Quando a instalação for concluída com sucesso, clique em Concluir.

3.3.2 Instalação Personalizada

Depois de atender aos pré-requisitos mencionados na seção anterior, você pode continuar a instalação do Sentinel.

Para instalar o Sentinel:

1. Efetue login como usuário root no Solaris/Linux ou usuário administrador no Windows.
2. Insira e monte o CD de instalação do Sentinel.
3. No Linux/Solaris, verifique se o sistema umask está definido como 0027, executando o comando a seguir no mesmo prompt de comando de onde você executará o instalador:

   ```
   umask 0027
   ```
4. Para iniciar o programa de instalação, vá para o diretório de instalação no CD-ROM e
   - No Windows, execute setup.bat
   - No Solaris/Linux:

   Para o modo de interface gráfica:

   ```
   ./setup.sh
   ```

   ou

   Para modo textual:

   ```
   ./setup.sh -console
   ```
5. Clique na seta para baixo e selecione uma das seguintes opções de idioma:

Inglês	Italiano
francês	Português (Brasil)
Alemão	Espanhol
Chinês Simplificado	Japonês
Chinês Tradicional	

6. Depois de ler a tela de boas-vindas, clique em Avançar.
7. Leia e aceite o Contrato de Licença de Usuário Final e clique em Avançar.
8. Aceite o diretório de instalação padrão ou clique em Procurar para especificar o local da instalação. Clique em Avançar.
9. Selecione Personalizado. Clique em Avançar.
10. Selecione os componentes do Sentinel a serem instalados.

Observação: Para obter mais informações sobre a Instalação de cada componente para as diversas configurações, consulte Capítulo 2, “Melhores práticas” na página 17 no Guia de Instalação.

As seguintes opções estão disponíveis:

Banco de Dados – instala o Banco de Dados do Sentinel	Serviço do Coletor do Sentinel
Servidor de Comunicação - instala o barramento de mensagem (iSCALE) e Proxy DAS	Construtor de Coletor
Consultor	Sentinel Control Center
Mecanismo de Correlação	Gerenciador de Dados do Sentinel
DAS (para comunicação de banco de dados)	HP OpenView Service Desk
	Integração do Remedy

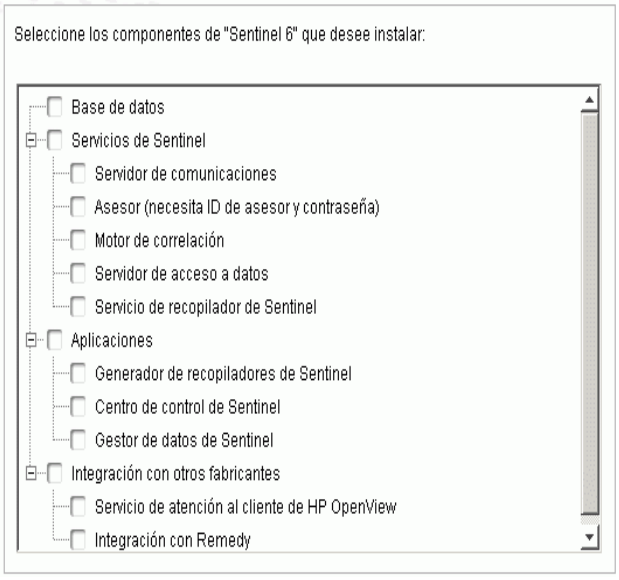
Observação: Para obter informações sobre como instalar o HP OPenView Service Desk ou Remedy Integration, consulte o Guia de Integração de Terceiros.

Observação: Há um tempo de atraso na interface quando você seleciona ou anula a seleção de um componente.

Observação: Se nenhum dos recursos filhos de Serviços do Sentinel for selecionado, anule a seleção do recurso Serviços do Sentinel também. Ele ficará esmaecido com uma marca de seleção se ainda estiver selecionado, mas todos os recursos filho serão desmarcados.

Observação: Como parte da instalação do componente Banco de Dados do Sentinel, o instalador colocará arquivos na pasta %ESEC_home%\db.

Observação: Na Instalação Simples o tamanho da Instalação do Banco de Dados para MSSQL e Oracle é 10 GB.



11 Se você selecionar a instalação do DAS, será solicitado a fornecer:

- Número de Série
- Chave de Licença

12 Se você selecionar a instalação de qualquer componente de integração de terceiros, será solicitado a fornecer uma senha para desbloquear o(s) componente(s) de integração de terceiros selecionado(s). Para obter mais informações, consulte o Guia de Integração de Terceiros.

13 No Linux/Solaris, especifique o nome de usuário do Administrador do Sentinel no sistema operacional e o local do diretório pessoal. Esse é o nome de usuário que terá a propriedade do produto Sentinel instalado. Se o usuário não existir ainda, um usuário será criado com um diretório pessoal no diretório especificado.

- Nome de usuário do Administrador do sistema operacional – O padrão é esecadm
- Diretório pessoal do Administrador do sistema operacional – O padrão é "/export/home". Se o nome de usuário for esecadm, o diretório pessoal do usuário será /export/home/esecadm.

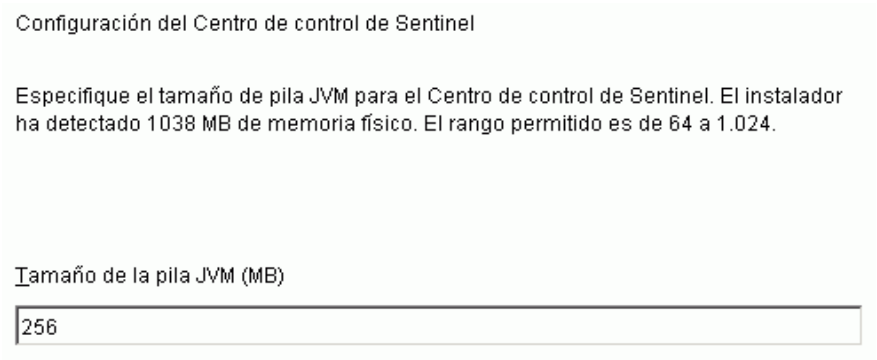
Observação: Para atender às configurações de segurança rígidas exigidas pela Certificação de Critérios Comuns, consulte a seção Definindo senha - melhores práticas em Capítulo 2, "Melhores práticas" na página 17.

Observação: O usuário do esecadm será criado sem uma senha definida. Para efetuar login como esse usuário, você precisará definir primeiro a senha.

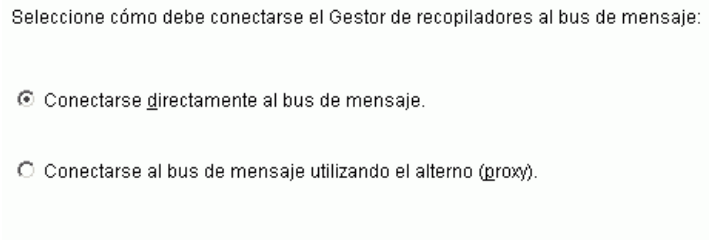
---

14 Se você optou por instalar o Sentinel Control Center, o instalador solicitará que você digite o espaço em memória máximo a ser alocado para o Sentinel Control Center. Digite o tamanho de heap JVM máximo (MB) que você deseja que seja usado somente pelo Sentinel Control Center.

- Tamanho de heap JVM (Mb) - por padrão, é definido como metade do tamanho da memória física detectada na máquina, com um máximo de 1024 MB.



15 Você tem duas opções para estabelecer a comunicação entre os clientes do Sentinel e o Servidor. Você pode selecionar a comunicação do tipo Barramento de Mensagem Direta ou comunicação do tipo Proxy. Para obter mais informações sobre essas duas opções, consulte Capítulo 8, "Camada de Comunicação (iSCALE)" na página 101 no Guia de Instalação.



16 Você é solicitado a digitar informações de nome do servidor host/porta. Digite as informações necessárias e clique em Próximo. Se você selecionar a comunicação do tipo Proxy, será solicitado a digitar a Porta do Proxy do Sentinel Communication Center também.

- Porta do barramento de mensagem: a porta que o barramento de mensagem está escutando. Os componentes que se conectam diretamente ao barramento de mensagem usarão essa porta.
- Porta Proxy do Sentinel Control Center: a porta que o servidor proxy SSL (DAS Proxy) está escutando para aceitar conexões autenticadas com nome de usuário e senha. Como o Sentinel Control Center solicita um nome de usuário e senha, ele usa essa porta para se conectar ao Sentinel Server.
- Porta Proxy de Autenticação Básica de Certificado: a porta que o servidor proxy SSL (DAS Proxy) está escutando para aceitar conexões autenticadas com certificados. Como o Gerenciador de Coletor não pode solicitar um nome de usuário e senha, ele usa essa porta para se conectar ao Sentinel Server se estiver configurado para se conectar através do proxy.

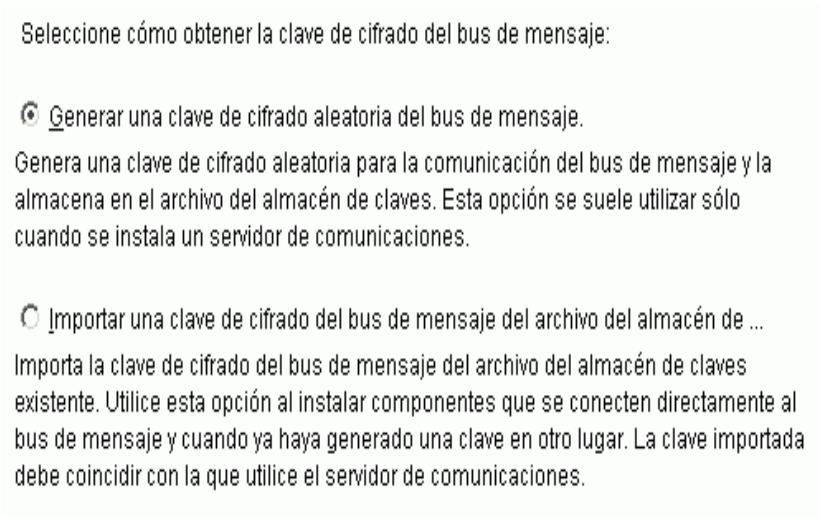
Observação: Os números de porta devem ser idênticos em todas as máquina do sistema do Sentinel para habilitar a comunicação. Anote essas informações para instalações futuras em outras máquinas.

---

17 Se estiver instalando um componente que fará uma conexão direta com o barramento de mensagem ou se estiver instalando o Servidor de Comunicação, você deverá indicar como obter a chave criptográfica compartilhada de barramento de mensagem:

- Gerar chave criptográfica aleatória (recomendada ao instalar o Servidor de Comunicação)
- Importar chave criptográfica do arquivo keystore (recomendado ao instalar outros componentes). Você deverá selecionar o arquivo do qual importar a chave criptográfica.
- O arquivo .keystore será colocado em $ESEC_HOME/config no OS do Linux e Solaris ou %ESEC_HOME%\config no Windows OS.

18 Especifique se você deseja gerar um arquivo keystore aleatório ou importar o arquivo de armazenamento de chave existente de outra máquina do sistema do Sentinel.



Observação: Todos os componentes que se conectam diretamente ao barramento de mensagem devem compartilhar a mesma chave criptográfica. A Novell recomenda gerar uma chave criptográfica aleatória ao instalar o Servidor de Comunicação e importar essa chave ao instalar os componentes em outras máquinas. Os componentes que se conectam através do proxy não precisam da chave criptográfica do barramento de mensagem.

19 Se optar por importar um arquivo keystore existente, você terá que navegar até o local e selecioná-lo. Clique em Avançar.

20 Se optar por instalar o DAS, selecione a quantidade de RAM do sistema que deseja alocar para o Serviço de Acesso a Dados. Para ambientes distribuídos, é recomendável selecionar o máximo de memória, pois o banco de dados exigirá alguma memória.

21 Se você optou por instalar o DAS, mas não optou por instalar o Banco de Dados do Sentinel, será solicitado a fornecer as informações do Banco de dados do Sentinel para a seguir. Essas informações serão usadas para configurar o DAS para que aponte para o Banco de Dados do Sentinel.

- Nome de host do banco de dados ou endereço IP: o nome ou IP do Banco de Dados do Sentinel existente a ser configurado para se conectar ao componente DAS.
- Nome do banco de dados: o nome da instância do Banco de Dados do Sentinel a ser configurada para se conectar ao componente DAS (o padrão é ESEC).
- Porta do banco de dados (padrão - Microsoft SQL:1433 e Oracle 1521)
- Usuário do Banco de Dados do Aplicativo Sentinel: Especifique o login esecapp e digite a senha fornecida a esse usuário durante a instalação do Banco de Dados do Sentinel.

22 Configure o banco de dados para instalação:

No Windows:

- Selecione o Microsoft SQL server 2005 como a plataforma de servidor de banco de dados de destino.
  - Criar um novo banco de dados com objetos de banco de dados: cria um novo banco de dados do Microsoft SQL e preenche o novo banco com objetos de banco de dados
  - Adicionar objetos de banco de dados a um banco de dados vazio existente: somente adiciona objetos de banco de dados a um banco de dados do Microsoft SQL 2005 existente. O banco de dados existente precisa estar vazio.
  - Especifique o diretório de registro de Instalação do Banco de Dados.

Clique em Avançar.

- Especifique o local de armazenamento para:
  - Diretório de dados
  - Diretório de Índices
  - Diretório de Dados de Resumo
  - Diretório de Índices de Resumo
  - Diretório de Registro

Clique em Avançar.

- Selecione a opção de suporte do conjunto de caracteres do banco de dados, banco de dados Unicode ou ASCII somente. Se você selecionar idiomas não asiáticos (idiomas diferentes do chinês simplificado/tradicional e japonês nesta lista), o sistema solicitará que você

selecione entre os bancos de dados Unicode e Não unicode. Selecione um formato de banco de dados e clique em OK.

Observação: Você precisaria de mais espaço em disco para realizar a instalação do banco de dados Unicode.

Observação: Se você selecionar um idioma asiático, o banco de dados Unicode será instalado por padrão. Clique em Avançar.

- Especifique o tamanho do banco de dados. Clique em Avançar.
- Configure partições de banco de dados.
  - Você pode selecionar Habilitar partições de banco de dados automaticamente.
  - Para partições de dados, especifique o diretório de arquivo; digite especificações de Horário para adicionar e arquivar dados.

Clique em Avançar.

No Linux/Solaris:

- Selecione a plataforma de servidor do banco de dados de destino.
  - Selecione Oracle 10g na lista suspensa.
  - Selecione Criar Novo banco de dados com objetos de banco de dados.

Clique em Avançar.

- Especifique o Nome de Usuário do Oracle ou Aceite o nome de usuário padrão. Clique em OK
- Se você optar por criar um novo banco de dados, digite o seguinte:
  - **O caminho para o arquivo de driver do Oracle JDBC:** (o nome típico do arquivo jar é ojdbc14.jar). Esse é o caminho completo para o arquivo .jar, normalmente $ORACLE_HOME/jdbc/lib/ojdbc14.jar (não é possível usar variáveis de ambiente nesse campo).
  - **Nome do host:** O nome de host da máquina onde o banco de dados será instalado. O instalador só suporta a criação de uma nova instância do banco de dados no host local.
  - **Nome do banco de dados:** O nome da instância do banco de dados a ser instalada.
- Se você optou por adicionar objetos de bancos de dados a um banco Oracle vazio existente, será solicitado a fornecer as informações a seguir.

  O caminho para o arquivo de driver do Oracle JDBC: (o nome típico do arquivo jar é ojdbc14.jar). Esse é o caminho completo para o arquivo .jar, normalmente $ORACLE_HOME/jdbc/lib/ojdbc14.jar (não é possível usar variáveis de ambiente nesse campo).

  Nome de host do banco de dados ou endereço IP: o nome ou endereço IP do host em que está o banco de dados Oracle ao qual você deseja adicionar objetos de banco de dados. Pode ser o nome de host local ou um nome de host remoto.

  Nome do banco de dados: O nome da instância do banco de dados Oracle vazio existente à qual você deseja adicionar objetos de banco de dados (o padrão é ESEC). Esse nome de banco de dados precisa aparecer como nome de um serviço no arquivo

tnsnames.ora (no diretório $ORACLE_HOME/network/admin/) da máquina onde o instalador está sendo executado.

Porta do banco de dados: O padrão é 1521

Senha: Para o usuário Administrador do Banco de Dados do Sentinel (DBA), especifique a senha do usuário "esecdba". O campo de nome de usuário desse prompt não é editável.

Observação: Se o nome do banco de dados não estiver no arquivo tnsnames.ora, o instalador não exibirá um erro nesse momento da instalação (porque ele verifica a conexão usando uma conexão JDBC direta), mas a instalação do Banco de dados irá falhar quando o instalador tentar se conectar ao banco de dados por meio de sqlplus. Se a instalação do banco de dados falhar nesse ponto, modifique o nome do serviço desse banco de dados no arquivo tnsnames.ora nessa máquina, sem sair do instalador, retroceda uma tela no instalador e avance novamente. Será feita uma nova tentativa de instalação do banco de dados com os novos valores no arquivo tnsnames.ora.

Observação: O instalador fará backup de tnsnames.ora e listener.ora no diretório $ORACLE_HOME/network/admin. Ele sobregravará o arquivo listener.ora com as informações de conexão de banco de dados do Sentinel e anexará as informações de conexão do banco de dados ao arquivo tnsnames.ora. Se você tiver outros bancos de dados no mesmo servidor do banco de dados do Sentinel, o administrador deve mesclar manualmente informações dos arquivos listener.ora do backup com o novo arquivo e reiniciar a escuta do Oracle, para que outros aplicativos possam continuar a se conectar ao banco de dados.

- Ao criar um banco de dados, aceite o espaço na memória e a porta de escuta padrão ou especifique novos valores.
- Digite as credenciais SYS e SYS e clique em Avançar.
- Especifique o tamanho do banco de dados. Você pode selecionar Padrão, Grande ou Personalizado. Se você escolheu Personalizado, deverá especificar:
  - o tamanho inicial de cada arquivo de banco de dados em MB (100 a 10.000)
  - o tamanho máximo de cada arquivo de banco de dados em MB (2.000 a 100.000)
  - o tamanho de todos os arquivos de banco de dados em MB (7.000 a 2.000.000)
  - o tamanho de cada arquivo de registro em MB (100 a 100.000)
- Especifique o tamanho total do banco de dados alocado para os espaços Evento e Tabela de Resumo de Eventos.
- Especifique o local de armazenamento para:
  - Diretório de dados
  - Diretório de índices
  - Diretório de Dados de Resumo
  - Diretório de Índices de Resumo
  - Diretório de Registro

  Clique em Avançar.

Observação: Para fins de recuperação e desempenho, recomenda-se que esses locais estejam em dispositivos de E/S diferentes.

Como o instalador não irá criar esses diretórios, eles precisam ser criados externamente antes de avançar.

Por motivos de desempenho, o Registro Redo deve apontar para o disco de gravação mais rápido disponível.

Esses diretórios precisam permitir gravação pelo usuário do Oracle. Para tornar esses diretórios graváveis pelo usuário do Oracle, execute os comandos a seguir para cada diretório como Usuário Root:

```
chown –R oracle:dba <directory_path>
chmod –R 770 <directory_path>
```

- Supondo que “oracle” seja seu nome de usuário no oracle e “dba” seu nome de grupo no oracle.
- Configure partições de banco de dados.
  - Selecione Habilitar partições de banco de dados automáticas e
  - Especifique o diretório de arquivo de partição de dados.
  - Digite as especificações de Horário para adicionar e arquivar dados.

  Clique em Avançar.

23 Digite Informações de Autenticação para:

- Usuário Administrador do Banco de Dados do Sentinel
- Usuário de Banco de Dados do Aplicativo Sentinel
- Usuário Administrador do Sentinel
- Usuário de Relatório do Sentinel (somente no Windows)

Clique em Avançar.

24 O resumo de parâmetros de Banco de Dados especificados será exibido. Clique em Avançar.

25 Se você optou por instalar o DAS, configure o suporte de e-mail do Sentinel. Especifique o servidor SMTP e o endereço de e-mail que o Serviço de Execução deve usar para enviar mensagens (opcional – isso pode ser editado manualmente depois da instalação [$ESEC_HOME\sentinel\config\execution.properties no Linux/Solaris e %ESEC_HOME%\sentinel\config\execution.properties no Windows]).

26 Se você optou por instalar o Advisor, aparecerá o prompt a seguir solicitando o tipo de instalação:

- **Download Direto da Internet:** A máquina do Consultor está conectada diretamente à Internet. Nessa configuração, é feito o download automático das atualizações da Novell da Internet com regularidade.
- **Independente:** O Consultor é configurado como um sistema isolado que requer intervenção manual para receber uma atualização do Sentinel.

27 Se você optou por instalar o Advisor e selecionou o uso do Download Direto da Internet, digite seu nome de usuário, senha e freqüência de atualização dos dados do Advisor. Clique em Próximo. Você deverá responder se deseja continuar (não recomendável), se seu nome de usuário e senha não forem verificados. Se optar por continuar, digite a senha do Advisor novamente na janela de confirmação de senha. Caso contrário, corrija a senha do Advisor.

28 Se você optou por instalar o Advisor, digite:

- Endereço do remetente, que será exibido nas notificações de e-mail
- Endereço do destinatário para o envio de notificações por e-mail

Observação: Após a instalação, para mudar os endereços de e-mail do Advisor, edite os arquivos attackcontainer.xml e alertcontainer.xml. Para obter mais informações, consulte "Guia Consultor" no Guia de Usuário do Sentinel.

- Selecione Sim ou Não para o recebimento de e-mails sobre atualizações bem sucedidas do Advisor.

Observação: As notificações de erro serão sempre enviadas.

29 Clique em Próximo. Será exibida a tela de Resumo com os recursos selecionados para instalação. Clique em Instalar.

Observação: Se você optou por instalar o HP Service Desk ou a Integração do Remedy, será solicitado a fornecer informações adicionais. Para obter mais informações, consulte o Guia de Integração de Terceiros do Sentinel.

30 Quando a instalação for concluída com sucesso, você deverá reiniciar. Clique em Concluir para reinicializar o sistema.

Observação: O instalador do Sentinel desliga o Registro de Arquivos por padrão. Para fins de recuperação de bancos de dados, é altamente recomendável que, após a instalação e antes de começar a receber dados de eventos de produção, você habilite o Registro de Arquivos. Você também deve programar um backup dos seus registros de arquivo para liberar espaço no destino do registro de arquivos, do contrário o banco de dados irá parar de aceitar eventos.

Observação: Se você espera uma taxa de eventos elevada (superior a 500 eventos por segundo) é necessário seguir as instruções de configuração adicionais da seção "Configurando a estratégia de inserção de eventos da Interface de Chamada Oracle (OCI) na criação de banco de dados".

Instalação de console no Linux/Solaris

```
Select the features for "Sentinel 6" you would like to install:
   Sentinel 6
   To select/deselect a feature or to view its children, type its
number:
     1.  [ ] Database
     2. +[x] Sentinel Services
     3. +[x] Applications
     4. +[ ] 3rd Party Integration
   Other options:
     0. Continue installing
   Enter command [0] 2
    1. Deselect 'Sentinel Services'
    2. View 'Sentinel Services' subfeatures
   Enter command [1] 2

Select the features for "Sentinel 6" you would like to install:
   Sentinel 6
    - Sentinel Services
      To select/deselect a feature or to view its children, type its
number:
        1. [ ] Communication Server
```

```
        2. [ ] Advisor (Install requires Advisor ID and Password)
        3. [x] Correlation
        4. [x] DAS
        5. [x] Sentinel Collector Service
      Other options:
       -1. View this feature's parent
        0. Continue installing
      Enter command [0] 1

Select the features for "Sentinel 6" you would like to install:
   Sentinel 6
    - Sentinel Services
      To select/deselect a feature or to view its children, type its
number:
        1. [x] Communication Server
        2. [ ] Advisor (Install requires Advisor ID and Password)
        3. [x] Correlation
        4. [x] DAS
        5. [x] Sentinel Collector Service
      Other options:
       -1. View this feature's parent
        0. Continue installing
      Enter command [0] -1

Select the features for "Sentinel 6" you would like to install:
   Sentinel 6
   To select/deselect a feature or to view its children, type its
number:
     1. [ ] Database
     2. +[x] Sentinel Services
     3. +[x] Applications
     4. +[ ] 3rd Party Integration
   Other options:
     0. Continue installing
   Enter command [0]
```

Instalação do Cliente

O Sentinel Control Center, Construtor de Coletor e o Gerenciador de Dados do Sentinel podem ser instalados com o instalador completo ou o instalador somente cliente. O instalador principal permite que você escolha qualquer um dos três aplicativos, e o instalador somente cliente automaticamente instalará todos os três.

Observação: Como o instalador somente cliente inclui automaticamente o Construtor de Coletor, ele só pode ser usado nos sistemas operacionais Windows. Todos esses aplicativos baseados em Windows funcionam com um Sentinel Server baseado em Linux.

Para Instalar o Sentinel Control Center e o Construtor do Coletor usando o Instalador Somente Cliente:

1. Pesquise no CD e execute setup.sh (no Linux e Solaris) ou setup.bat (no Windows). O assistente de instalação será inicializado.

2 Selecione o idioma a ser usado no assistente e clique em OK.

3 A tela de Boas-vindas do Sentinel será exibida. Depois de ler a tela de boas-vindas, clique em Avançar.

4 A tela do Contrato de Licença de Usuário Final do Sentinel será exibida. Leia e Aceite o Contrato de Licença de Usuário Final e clique em Avançar.

5 Aceite o diretório de instalação padrão ou clique em Procurar para especificar o local da instalação. Clique em Avançar.

6 Digite o endereço do host em que o Servidor de Comunicação está instalado.

7 Selecione Gerar um arquivo keystore aleatório, clique em Avançar.

8 Clique em Avançar.

9 O resumo da instalação será exibido. Clique em Instalar.

10 Quando a instalação for concluída com sucesso, clique em Concluir.

3.4 Configuração de pós-instalação

3.4.1 Atualizando o e-mail do Sentinel para autenticação SMTP

Se o sistema exigir autenticação SMTP, você precisará atualizar o arquivo execution.properties. Esse arquivo está na máquina em que o DAS foi instalado. Ele está localizado em $ESEC_HOME/sentinel/config. Para configurar esse arquivo, execute mailconfig.sh para mudar o arquivo e mailconfigtest.sh para testar as mudanças.

Para configurar o arquivo execution.properties:

Observação: Esse exemplo está no OS Linux/Solaris. É necessário uma configuração similar no Windows OS.

---

1 Na máquina em que o DAS foi instalado, faça login como Usuário Administrador do Sentinel e mude para o diretório:

```
$ESEC_HOME/sentinel/config
```

2 Execute mailconfig desta maneira:

```
./mailconfig.sh -host <SMTP Server> -from <source email address> -user <mail authentication user> –password
```

Exemplo:

```
./mailconfig.sh -host 10.0.1.14 -from my_name@domain.com -user my_user_name –password
```

Depois de digitar esse comando, você será solicitado a fornecer uma nova senha.

```
Enter your password:*********
Confirm your password:*********
```

Observação: Ao usar a opção password, ela deve ser o último argumento.

Para testar a configuração de execution.properties:

1. Na máquina em que o DAS foi instalado, faça login como Usuário Administrador do Sentinel e mude para o diretório:

   ```
   $ESEC_HOME/sentinel/config
   ```

2. Execute mailconfigtest desta maneira:

   ```
   ./mailconfigtest.sh -to <destination email address>
   ```

   Se o e-mail for enviado com êxito, será exibida a seguinte saída na tela e o e-mail será recebido no endereço de destino.

   ```
   Email has been sent successfully!
   ```

   Verifique a caixa de correio do e-mail de destino para confirmar o recebimento da mensagem. A linha de assunto e o conteúdo devem ser:

   ```
   Subject: Testing Sentinel mail property
   This is a test for Sentinel mail property set up. If you see this
   message, your Sentinel mail property has been configured correctly
   to send emails
   ```

3.4.2 Banco de Dados do Sentinel

Observação: Por padrão, o instalador define todos os tablespaces como autogrow (crescimento automático). Por padrão, o tamanho de crescimento de arquivo é 200 MB, mas o tamanho de arquivo máximo depende do valor fornecido durante a instalação, por exemplo: 2000 MB, etc.

O gerenciamento de partição automática do banco de dados do Sentinel (arquivamento, descarte e adição de partições) deve ser habilitado, para controlar o tamanho dos dados do evento. O gerenciamento de partição automático pode ser configurado com o SDM (Gerenciador de Dados do Sentinel).

O gerenciamento de partições SDM (arquivamento, descarte e adição de partições) deve ser programado de modo a manter os dados do evento dentro de um tamanho controlado.

Após instalar o Banco de Dados do Sentinel, o banco irá conter os usuários padrão a seguir:

- **esecdba:** Proprietário do esquema de banco de dados. O privilégio de DBA não é concedido ao Usuário do Banco de Dados do Sentinel por questões de segurança. Para usar o Enterprise Manager, crie um usuário com privilégios de DBA.
- **esecapp:** Usuário do aplicativo de banco de dados. Este é o usuário do aplicativo utilizado para a conexão com o banco de dados.
- **esecadm:** Usuário do banco de dados que é o Administrador do Sentinel. Não é a mesma conta do usuário do sistema operacional do Administrador do Sentinel.
- **esecrpt:** Usuário de relatório de banco de dados
- SYS: Usuário do banco de dados SYS
- SYSTEM - Usuário do banco de dados SYSTEM

3.4.3 Serviço do Coletor

Durante a instalação do Serviço de Coletor, será configurado um coletor chamado Coletor Geral. Esse coletor pode ser usado para testar a instalação.

Observação: Para obter maiores informações, consulte Capítulo 5, “Testando a instalação” na página 79

Observação: Para obter mais informações sobre Coletores, consulte http://suport.novell.com/products/sentinel/collectors.html (http://support.novell.com/products/sentinel/collectors.html).

3.4.4 Atualizando a chave de licença (da chave de avaliação)

Se você adquiriu o produto depois da avaliação, siga o procedimento abaixo para atualizar sua chave de licença no sistema e evitar a reinstalação.

Para atualizar a chave de Licença:

1. Faça login na máquina em que o componente DAS está instalado como esecadm.
2. No prompt de comando, vá para o diretório $ESEC_HOME/bin.
3. Execute o executável: /softwarekey. Um menu como o mostrado abaixo será exibido.
   - Digite a Chave Principal
   - Digite a Chave Secundária
   - Ver a Chave Principal
   - Ver a Chave Secundária
   - Sair
4. Digite 1 para inserir uma nova Chave Principal.

Configuração do Advisor

4

Tópicos incluídos neste capítulo:

- Seção 4.2, “Instalação do Advisor” na página 74
- Seção 4.5, “Redefinindo a senha do Advisor (somente Download Direto)” na página 76

Este capítulo discute como configurar o Sentinel para executar Relatórios do Consultor diretamente do Sentinel Control Center. Os Relatórios do Consultor são criados pela Novell para geração de relatórios e análise. Uma vez que a integração do Sentinel Control Center esteja configurada adequadamente, eles serão exibidos na guia Consultor.

4.1 Visão geral do Consultor

O Consultor do Sentinel fornece informações em tempo real quanto a vulnerabilidades da empresa, orientações técnicas e passos recomendados para a resolução. O Consultor fornece detecção de exploração, uma referência cruzada entre assinaturas de ataque de IDS em tempo real e a base de conhecimentos de vulnerabilidades do Consultor.

Observação: A instalação do Advisor é opcional. Porém, ele será um componente necessário se você quiser usar os recursos Sentinel Exploit Detection ou Advisor Reporting. O Consultor é um serviço de dados baseado em assinatura.

Os sistemas suportados são:

Sistemas de detecção de intrusão	Verificadores de vulnerabilidades
Cisco Secure IDS	eEYE Retina
Enterasys Dragon Host Sensor	Foundstone Foundscan
Enterasys Dragon Network Sensor	ISS Database Scanner
Intrusion.com (SecureNet_Provider)	ISS Internet Scanner
ISS BlackICE	ISS System Scanner
ISS RealSecure Desktop	ISS Wireless Scanner
ISS RealSecure Network	Nessus
ISS RealSecure Server	nCircle IP360
ISS RealSecure Guard	Qualys QualysGuard
Snort	**Firewalls.**
Symantec Network Security 4.0 (ManHunt)	Cisco IOS Firewall
Symantec Intruder Alert	
McAfee IntruShield	

4.2 Instalação do Advisor

Observação: O Consultor só pode ser instalado na mesma máquina em que reside o DAS (Database Access Service).

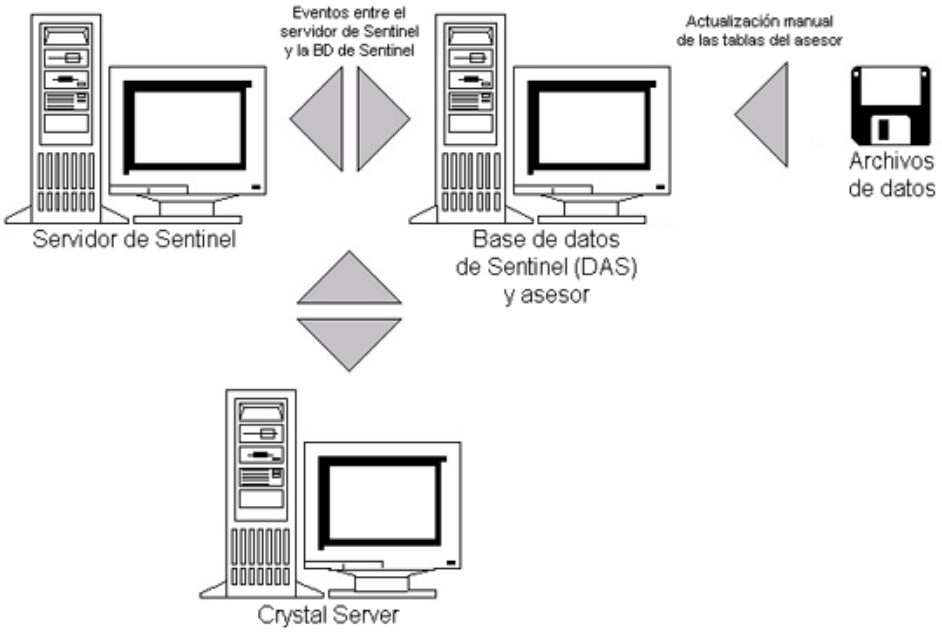
Há duas opções de instalação diferentes disponíveis. São eles:

- Independente
- Download Direto da Internet

Observação: Antes de instalar o Advisor, verifique se tem o nome do usuário e a senha do Advisor fornecidos pela Novell. Durante a instalação, você será solicitado a fornecer o nome do usuário e a senha.

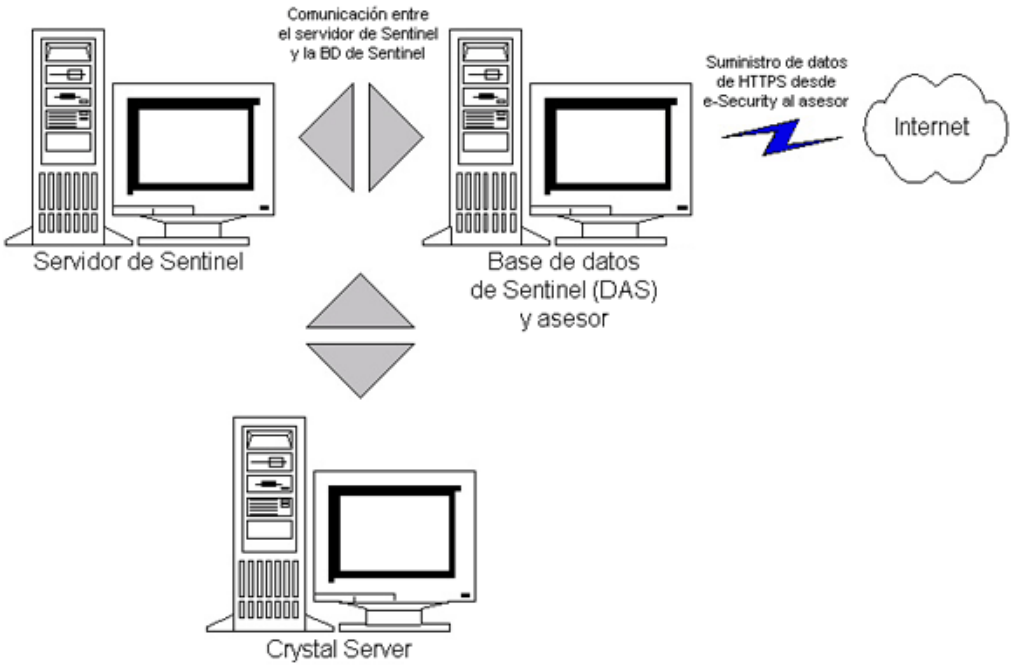
4.2.1 Configuração Independente

Na instalação Independente, o Advisor é um sistema isolado que requer intervenção manual para receber uma atualização da Novell.



4.2.2 Configuração Download Direto da Internet

Na instalação Download Direto da Internet, a máquina do Advisor está diretamente conectada à Internet. Nessa configuração, é feito o download automático das atualizações da Novell da Internet com regularidade.



4.3 Relatórios do Consultor

Crystal BusinessObjects Enterprise™ XI é a ferramenta de relatório que se integra com o Sentinel. Para obter mais informações sobre a instalação do Crystal BusinessObjects Enterprise™ XI, consulte Capítulo 9, “Crystal Reports para Windows” na página 107 e Capítulo 10, “Crystal Reports para Linux” na página 133 no Guia de Instalação.

Observação: O Crystal Server é obrigatório somente se você pretende executar relatórios. Caso use o Advisor somente para a Detecção de Exploração, não é necessário instalar o Crystal Server.

Para executar os relatórios do Crystal no Consultor:

- Instale e configure o Crystal Server. Para obter mais informações, consulte Capítulo 9, “Crystal Reports para Windows” na página 107 no Guia de Instalação.
- Publique Crystal Reports do Consultor no Crystal Server. Para obter mais informações, consulte Importando gabaritos de relatório.

4.3.1 Configuração de relatório do Consultor

Se você pretende executar relatórios do Consultor (Crystal Reports), execute o procedimento a seguir na ordem apresentada. Não é necessário realizar este procedimento se apenas quiser usar o Advisor para Detecção de Exploração.

- Execute as ações a seguir, caso ainda não tenha feito (para obter mais informações, consulte Capítulo 9, “Crystal Reports para Windows” na página 107, no Guia de Instalação:
  - Instale o Microsoft Internet Information Server (IIS)
  - Instale o Crystal BusinessObjects Enterprise™ 11

- No Banco de Dados do Sentinel no Oracle (Solaris/Linux): configure o driver nativo do Oracle (para instalações do Oracle)
- No Banco de Dados do Sentinel no Microsoft SQL 2005 (Windows): configure ODBC (Open Database Connectivity)
- Aplique os patches do Crystal Reports. Para obter mais informações, consulte Capítulo 9, "Crystal Reports para Windows" na página 107 no Guia de Instalação.

- Instale o Consultor – para obter mais informações sobre como instalar o Consultor, consulte Capítulo 7, "Instalando componentes do Sentinel" na página 95 no Guia de Instalação.
- Importe gabaritos do Crystal Reports
- Cria uma página da Web Crystal
- Configure o Sentinel Control Center para integração com o Crystal Enterprise Server

---

Observação: Para obter mais informações sobre como importar gabaritos de relatórios e configurar o Sentinel Control Center para mostrar os relatórios do Consultor, consulte Capítulo 9, "Crystal Reports para Windows" na página 107 e Capítulo 10, "Crystal Reports para Linux" na página 133 no Guia de Instalação.

4.4 Atualizando dados nas tabelas do Advisor

Se você não tiver uma configuração independente, os dados das tabelas do consultor serão atualizados automaticamente durante o próximo download de alimentação programado do consultor. No entanto, os dados também podem ser atualizados manualmente. Para obter mais informações sobre a atualização manual, consulte "Uso e manutenção do Consultor" no Guia de Usuário do Sentinel.

4.5 Redefinindo a senha do Advisor (somente Download Direto)

Se você estiver executando o Advisor no modo Download Direto e tiver obtido uma nova senha do Advisor ou se a senha definida durante a instalação estiver incorreta, será necessário redefinir a senha criptografada armazenada no arquivo de configuração do Advisor.

A atualização da senha criptografada do Advisor não se aplicará se você estiver executando o Advisor em uma configuração Independente porque, nesse modo, não é armazenada uma senha no arquivo de configuração do Advisor.

Para redefinir a senha criptografada armazenada no arquivo de configuração do Advisor, execute estas etapas:

1. Para Unix, efetue login como esecadm ou, para Windows, efetue login com direitos administrativos. Faça login na máquina em que está instalado o Advisor.
2. Consulte:

   Para UNIX:

   `$ESEC_HOME/bin`

   Para Windows:

   `%ESEC_HOME%\bin`
3. Execute o seguinte comando:

Para UNIX:

```
./adv_change_passwd.sh <newpassword>
```

Para Windows:

```
adv_change_passwd.bat <newpassword>
```

onde <newpassword> é a senha que você deseja definir para o Consultor.

Testando a instalação

5

Tópicos incluídos neste capítulo:

- Seção 5.1, “Testando a instalação” na página 79
- Seção 5.2, “Limpar do teste” na página 89
- Seção 5.3, “Introdução” na página 89

5.1 Testando a instalação

O Sentinel é instalado com um Coletor de demonstração que pode ser usado para testar muitas das funções básicas do sistema. Usando esse coletor, você pode testar Telas Ativas, a criação de Incidentes, regras de Correlação e Relatórios. O procedimento a seguir descreve as etapas para testar o sistema e os resultados esperados. Você pode não ver os mesmos eventos exatamente, mas seus resultados devem ser similares aos resultados abaixo.

Em um nível básico, esses testes permitirão que você confirme o seguinte:

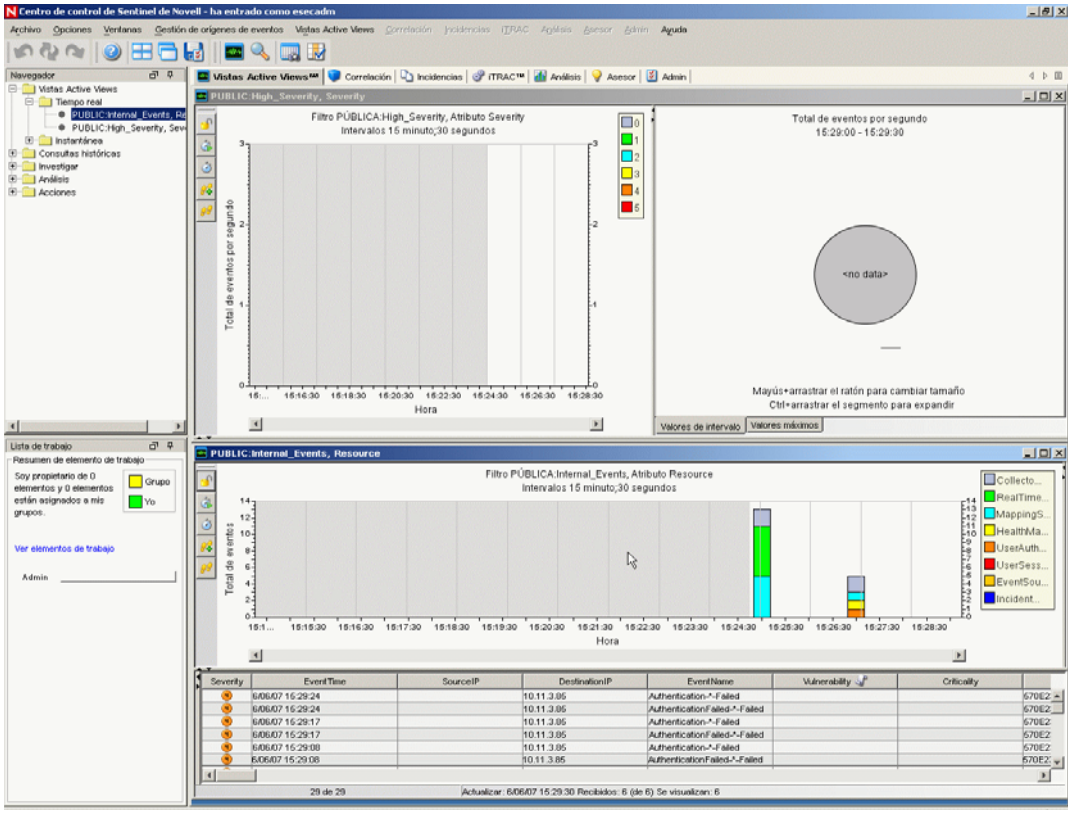
- Se os Serviços do Sentinel estão ativos
- Se a comunicação pelo barramento de mensagem é funcional
- Se os eventos internos de auditoria estão sendo enviados
- So os eventos podem ser enviados de um Gerenciador de Coletor
- Se os eventos estão sendo inseridos no banco de dados e podem ser recuperados usando a Consulta de Eventos do Histórico ou o servidor de Relatórios
- Se os Incidentes podem ser criados e vistos
- Se o Mecanismo de Correlação está avaliando regras e acionando os eventos correlacionados
- Se o Gerenciador de Dados do Sentinel pode se conectar ao banco de dados e ler as informações de partição

Se qualquer um desses testes falhar, revise o registro de instalação e outros arquivos de registro e entre em contato com o Suporte Técnico da Novell, caso necessário.

Para testar a instalação:

1. Clique duas vezes no ícone do Sentinel Control Center na área de trabalho.

2 Faça login no sistema usando o Usuário Administrativo do Sentinel especificado durante a instalação (esecadm por padrão). O Sentinel Control Center será aberto e você poderá ver a guia Telas Ativas com uma janela aberta com o título "PUBLIC:All, Severity"

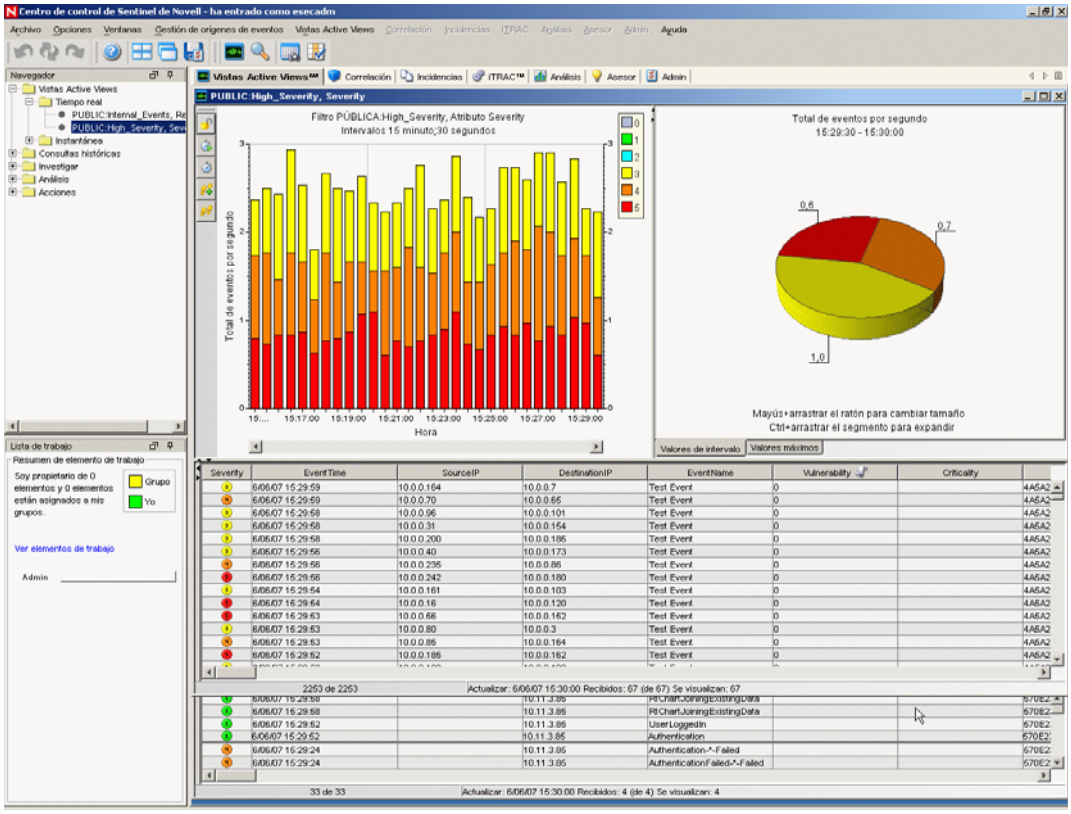


3 Vá para o menu Gerenciamento de Fonte de Eventos e escolha Live View.

4 Em Formato de Gráfico, clique o botão direito do mouse na fonte de evento 5 eps e selecione Iniciar.

5 Feche a janela Live View do Gerenciamento de Fonte de Eventos.

6 Vá para a guia Telas Ativas. Haverá uma janela ativa chamada "PUBLIC:High_Severity, Severity". Pode levar algum tempo para que o coletor inicie e os dados sejam exibidos nessa janela.



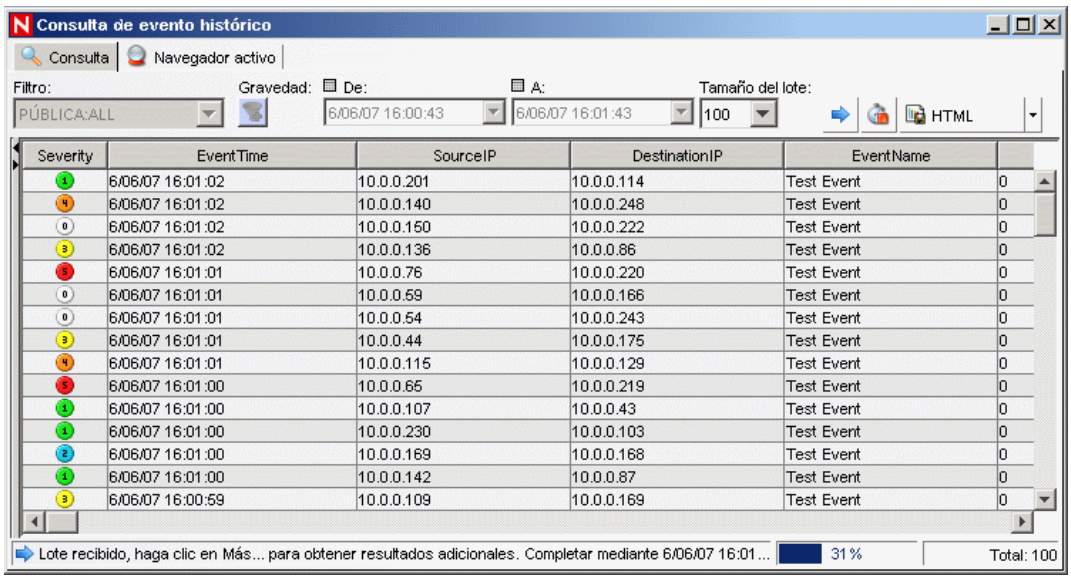
7 Clique no botão Consulta de Eventos na barra de ferramentas. A janela Consulta de Eventos do Histórico será exibida.

8 Na janela Consulta de Eventos do Histórico, clique na seta para baixo do Filtro para selecionar o filtro. Realce Público: Todos os filtros e clique em Selecionar.

9 Escolha um horário que abranja o horário em que o coletor ficou ativo. Selecione o intervalo de datas na seta dos menus suspensos De e Até.

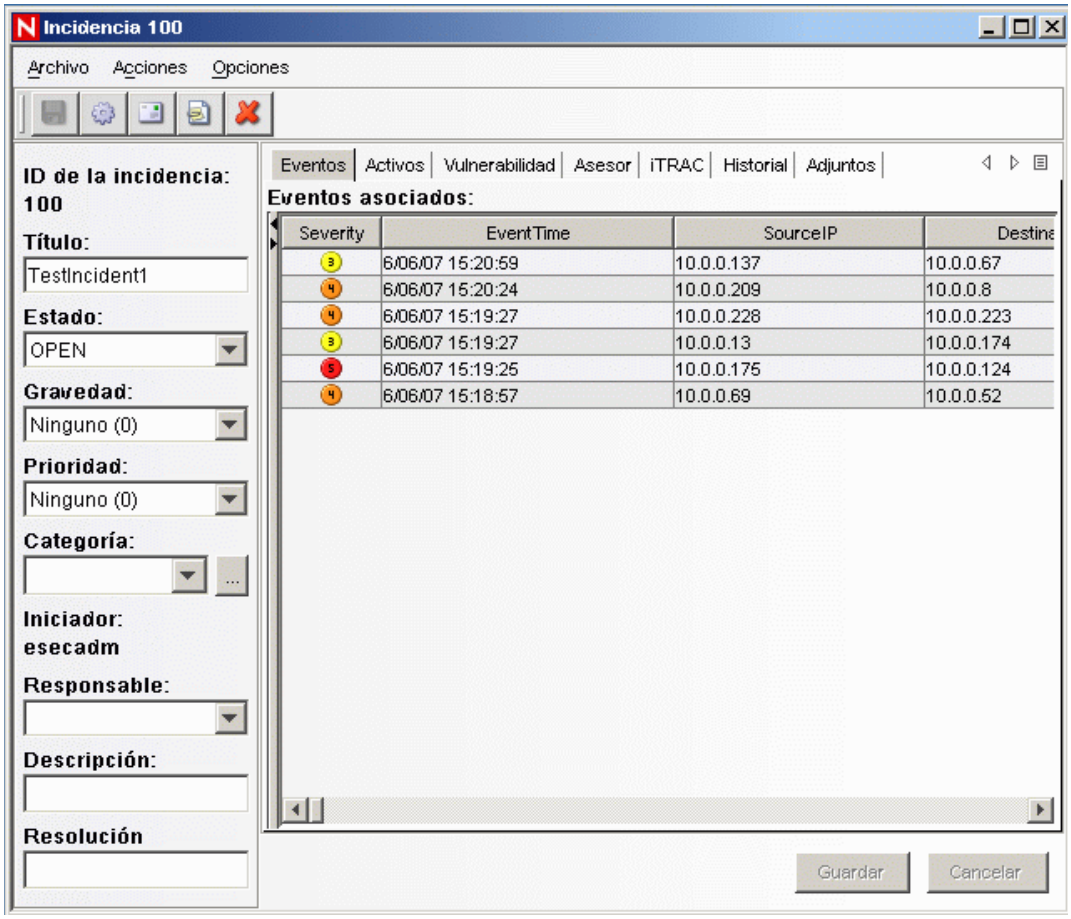
10 Selecione um tamanho de lote no menu suspenso.

11 Clique no ícone da lupa para executar a consulta.



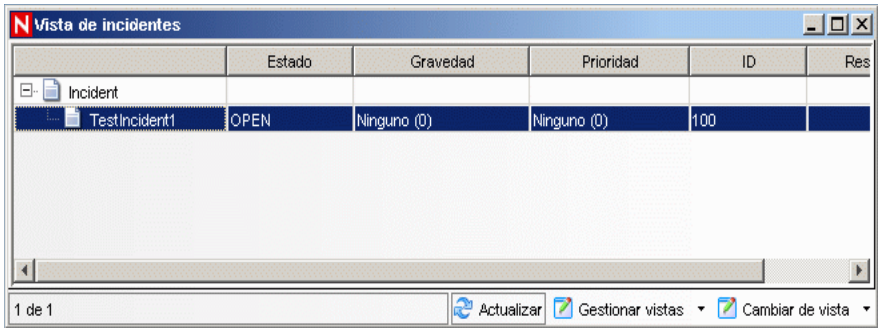
12 Mantenha pressionada a tecla Crtl ou Shift e selecione vários eventos na janela de consulta de eventos de histórico.

13 Clique o botão direito do mouse e escolha Criar Incidente.

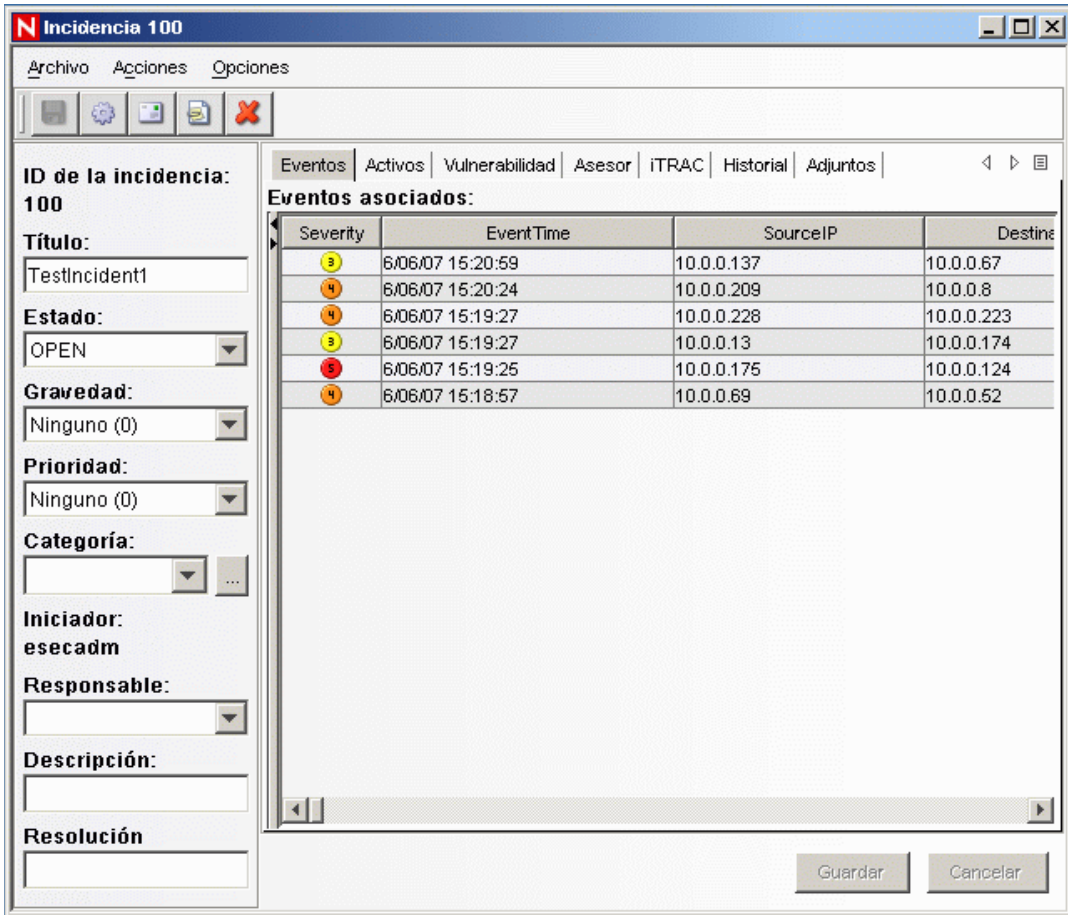


14 Nomeie o incidente como TestIncident1 e clique em Criar. Uma notificação de êxito será exibida. Clique em OK.

15 Vá até a Guia Incidente. O Gerenciador de Tela de Incidentes será exibido. No Gerenciador de Tela de Incidentes você poderá ver o incidente que acaba de criar.



16 Clique duas vezes no incidente para abri-lo.



17 Feche a janela do incidente, vá para Arquivo > Sair para fechar ou clique em "X" no canto superior direito da janela.

18 Clique na guia Análise. No Navegador de Análise, abra a pasta Relatórios de Histórico.

19 Clique em Consulta de Evento.

20 Clique em Análise > Criar relatório ou clique no ícone Criar Relatório. Uma janela Consulta de Evento será aberta. Defina o seguinte:

- espaço de tempo
- filtro
- nível de severidade
- tamanho do lote (este é o número de eventos a ver – eventos exibidos dos mais antigos para os mais recentes)

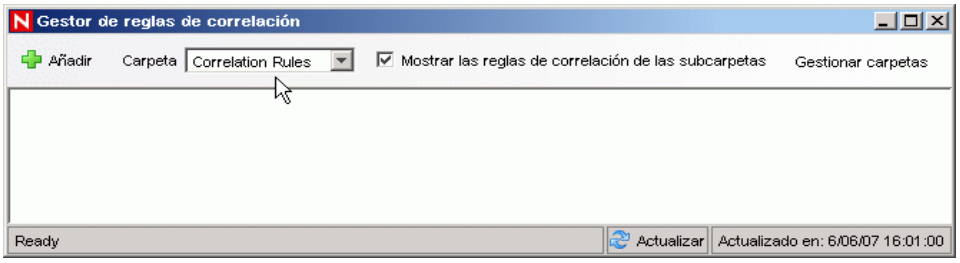
21 Clique em Atualizar Consulta.

22 Para ver o próximo lote de eventos, clique em Mais.

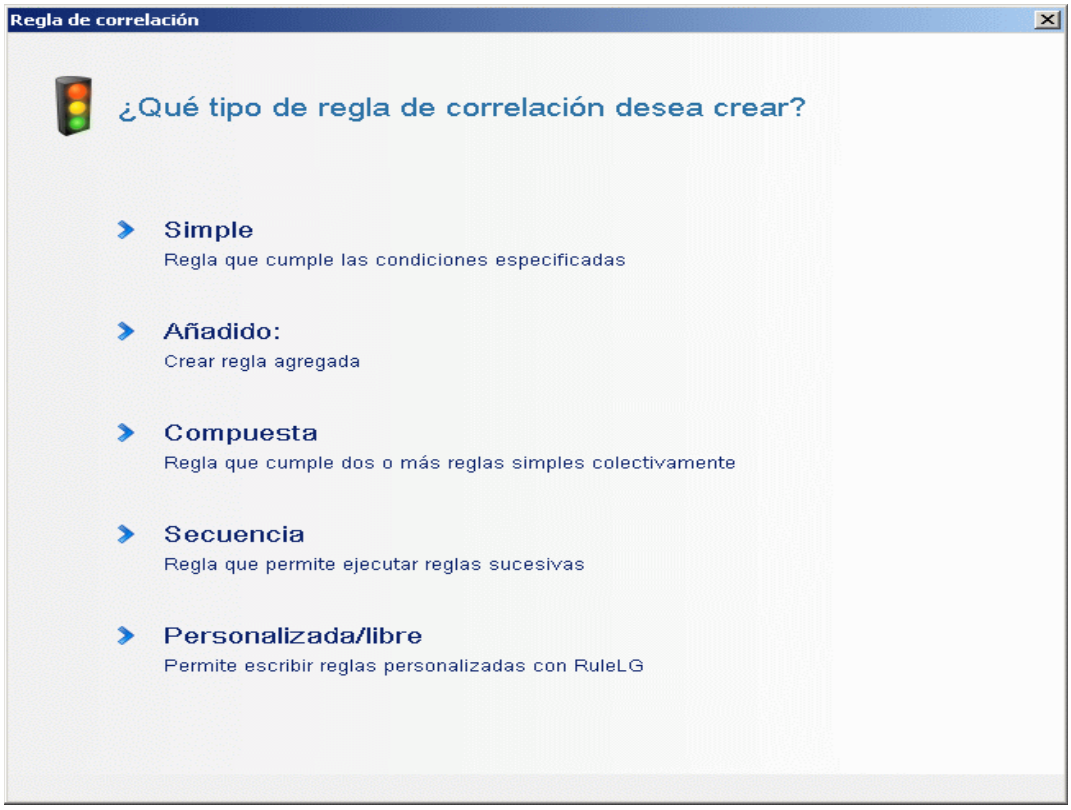
23 Reorganize as colunas arrastando-as e soltando-as, e organize a ordem de classificação clicando no cabeçalho da coluna.

24 Quando sua consulta estiver completa, ela será adicionada à lista de consultas rápidas do navegador.

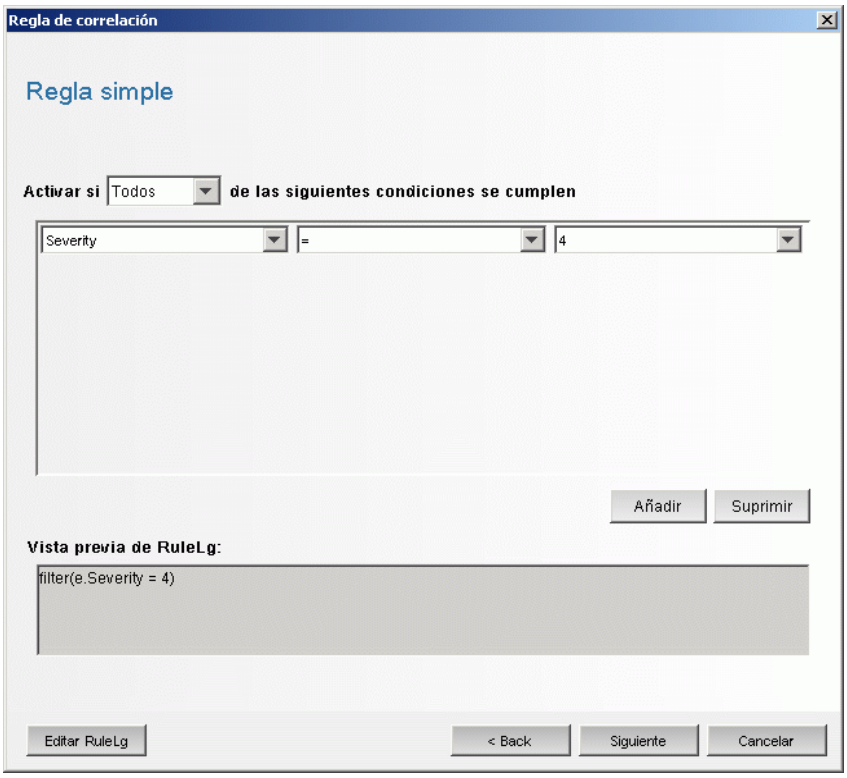
25 Vá para a guia Correlação. O Gerenciador de Regra de Correlação será exibido.



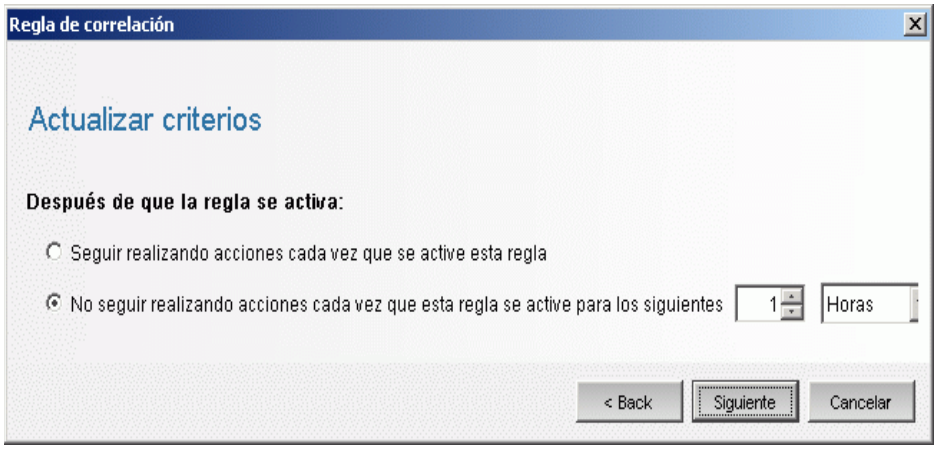
26 Clique em Adicionar. O Assistente de Regra de Correlação é aberto.



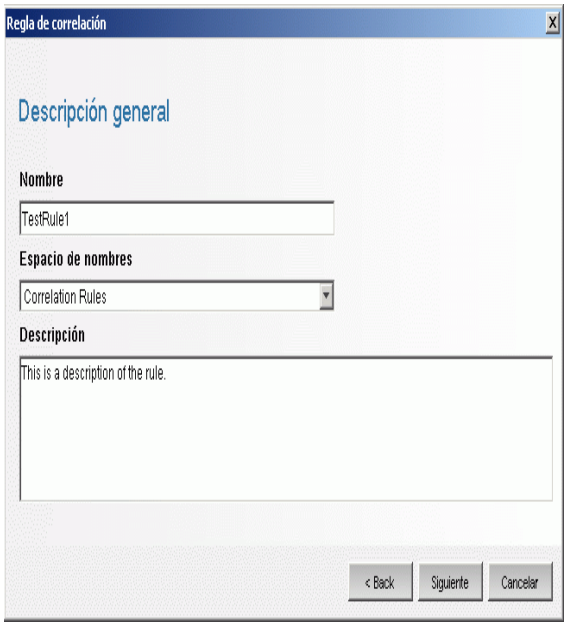
27 Clique em Simples. A janela Regra Simples será exibida.



28 Use os menus suspensos para definir os critérios como Severity=4. Clique em Próximo. A janela Critérios de Atualização será exibida.



29 Selecione "Do not perform actions every time this rule fires for next" (Não executar ações toda vez que esta regra acionar a próxima) e use o menu suspenso para definir o período como 1 minuto. Clique em Próximo. A janela Descrição Geral será exibida.

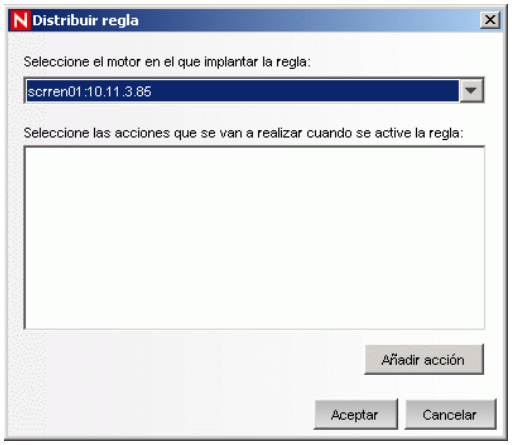


30 Nomeie a regra como 'TestRule1", digite a descrição e clique em Avançar.

31 Selecione "Não, não criar outra regra" e clique em Avançar.

32 Abra a janela do Gerenciador da Regra de Correlação.

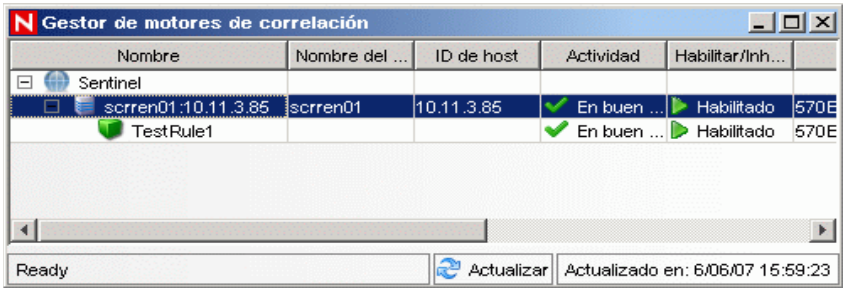
33 Realce uma regra e clique no link Distribuir regras. A janela Distribuir Regra será exibida.



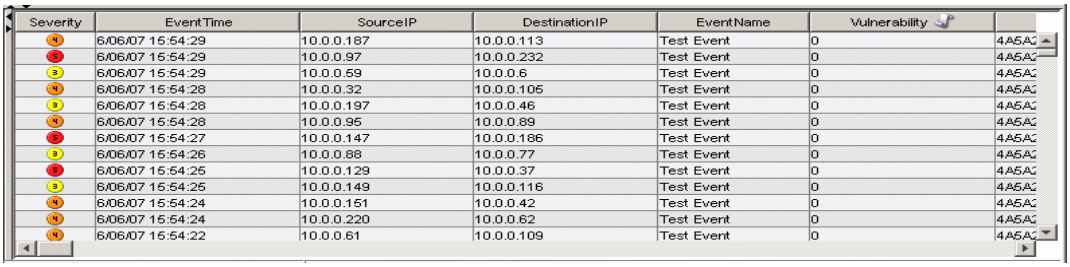
34 Na janela Distribuir regra, selecione o Mecanismo para distribuir a regra na lista suspensa.

35 Selecione uma ação 'Enviar e-mail" para associá-la à regra e clique em OK.

36 Selecione o Gerenciador de Mecanismo de Correlação. No mecanismo de Correlação, você pode ver que a regra está distribuída/habilitada.



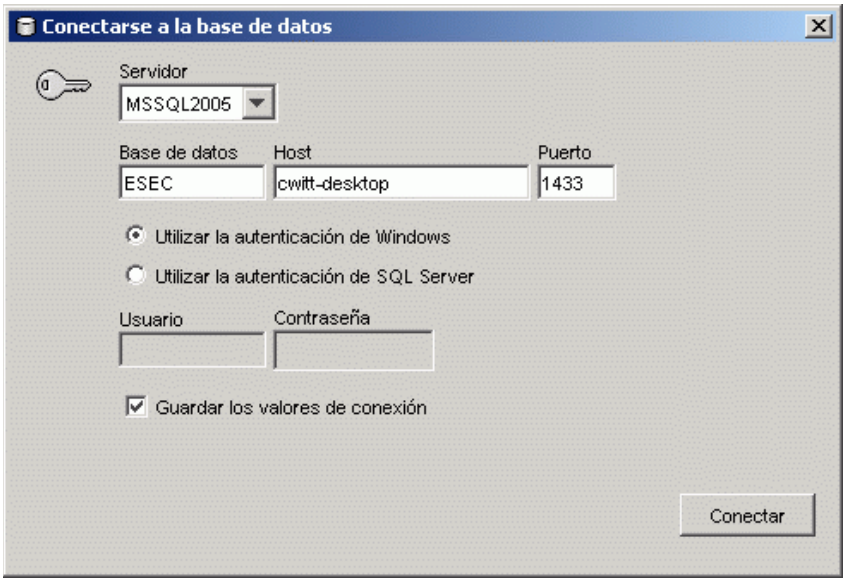
37 Vá para a guia Telas Ativas e verifique se o Evento Correlacionado foi gerado.



38 Feche o Sentinel Control Center.

39 Clique duas vezes no ícone do SDM (Gerenciador de Dados do Sentinel) na área de trabalho.

40 Faça login no SDM usando o Usuário Administrativo do Banco de Dados especificado durante a instalação (esecdba por padrão).



41 Clique em cada guia para verificar se você pode acessá-las.

42 Feche o Gerenciador de Dados do Sentinel.

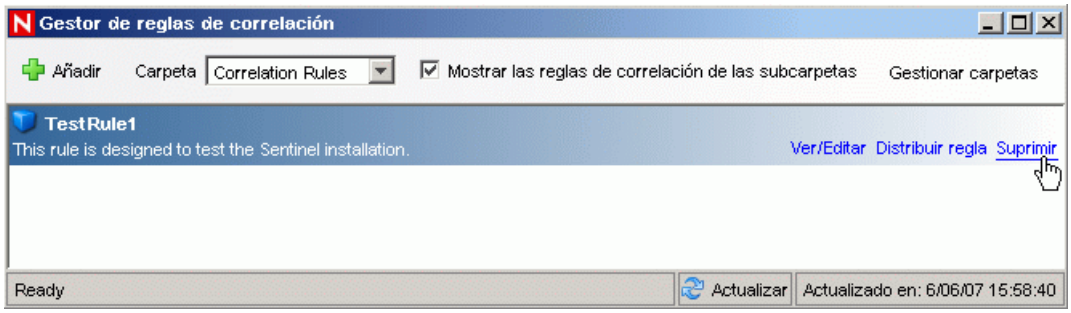
Se puder executar todas essas etapas sem erros, você concluiu uma verificação básica da instalação do sistema do Sentinel.

5.2 Limpar do teste

Depois de concluir a verificação do sistema, você deve remover os objetos criados para os testes.

Para a limpeza após o teste do sistema:

1. Faça login no sistema usando o Usuário Administrativo do Sentinel especificado durante a instalação (esecadm por padrão).
2. Vá para a guia Correlação.
3. Abra o Gerenciador do Mecanismo de Correlação.
4. Clique o botão direito do mouse em TestRule1 no Gerenciador de Mecanismo de Correlação e selecione Desfazer Distribuição.
5. Abra o Gerenciador do Mecanismo de Correlação.
6. Selecione TestRule1 e clique em Apagar.



7. Vá para o menu Gerenciamento de Fonte de Eventos e escolha Live View.
8. Na hierarquia de origem de evento Gráfica, clique o botão direito do mouse em Coletor Geral e escolha Parar.
9. Feche a Janela Gerenciamento de Origem de Evento.
10. Vá até a guia Incidentes.
11. Abra o Gerenciador da Tela Incidente.
12. Selecione TestIncident1, clique o botão direito do mouse e escolha Apagar.

5.3 Introdução

Você pode agora começar a usar seu sistema. Para obter mais informações, consulte “Início Rápido” no Guia de Usuário do SCC.

Upgrade para Sentinel 6

6

Tópicos incluídos neste capítulo:

- Seção 6.1, “Upgrade de Sentinel 5.x para Sentinel 6.0” na página 91
- Seção 6.2, “Upgrade do Sentinel 4.x para o Sentinel 6.0” na página 92

Este capítulo fornece uma visão geral de alto nível sobre como atualizar das versões anteriores do Sentinel para Sentinel 6.0. As etapas básicas são backup de versões anteriores do Sentinel, instalação/desinstalação de software, mudanças de configuração e migração de dados.

Observação: Este documento não fornece procedimentos detalhados para executar o upgrade. Informações detalhadas são fornecidas na documentação de Instalação de Patch disponível no Site de Documentação da Novell (http://www.novell.com/documentation/).

Os instaladores de patch disponíveis para aplicar patches no Sentinel 6.0 são:

- Sentinel 4.x para Sentinel 6.0
- Sentinel 5.x para Sentinel 6.0

Há várias mudanças importantes entre o Sentinel 6.0 e as versões anteriores que podem afetar seu upgrade. Mais detalhes são fornecidos na documentação de Instalação do Patch.

- Há pequenas mudanças no esquema de banco de dados entre o Sentinel 5.x e 6.0 e mudanças grandes no esquema de banco de dados entre o Sentinel 4.x e 6.0. Por causa das mudanças do esquema, há uma nova biblioteca de relatório disponível com o Sentinel 6.0, e os relatórios personalizados podem exigir modificação
- A nova estrutura de Gerenciamento de Fonte de Evento pode exigir algumas mudanças nos coletores para usar novos conectores.
- Há novas permissões de usuário disponíveis para usuários do Sentinel Control Center.
- Os requisitos do sistema mudaram, incluindo o suporte para várias novas plataformas.
- A estrutura do diretório mudou, assim scripts que se referem a caminhos de diretório podem exigir atualização.

6.1 Upgrade de Sentinel 5.x para Sentinel 6.0

Questões a considerar:

- Sentinel 5.x para Sentinel 6.0 é um upgrade "in-place" com o Instalador de Patch do Sentinel.
- A Migração de Dados do Microsoft SQL Server 2000 para Sentinel 5.x para Microsoft SQL Server 2005 para Sentinel 6.0 é suportada. (O SQL Server 2000 não é mais suportado no Sentinel 6.)
- A Migração de dados do Oracle 9i para Sentinel 5.x para o Oracle 10g para Sentinel 6.0 é suportada.
- A Migração de dados de banco de dados não Unicode para banco de dados Unicode não é suportada.

- Quando a Migração de Dados é concluída com sucesso, as regras de correlação e os gabaritos de Workflow do iTRAC não são migrados. As regras de correlação podem ser exportadas do 5.x e importadas para o 6.0. Os gabaritos de workflow do iTRAC devem ser recriados no Sentinel 6.0.

Para fazer upgrade do Sentinel 5.x para 6.0:

- Verifique os Requisitos do Sistema
  - Verifique se as especificações de hardware do sistema atendem aos requisitos de hardware mencionados em Capítulo 2, “Melhores práticas” na página 17.
  - Verifique se o sistema operacional e as versões de banco de dados atendem aos requisitos de sistema mencionados em Capítulo 2, “Melhores práticas” na página 17.
- Execute backup dos componentes necessários
  - Sentinel Server
  - Gerenciador do Coletor do Sentinel
  - Crystal Reporting Server
  - Servidor do banco de dados
  - Scripts do Coletor
  - Exporte Regras de Correlação
  - Faça backup de workflows do iTRAC
- Execute o Instalador de Patch fornecido pela Novell
- Instale o Banco de Dados do Sentinel 6.0
- Execute a Migração de Dados
- Instale o Sentinel 6.0 (exceto o Banco de Dados)
- Configure objetos
  - Atualize as permissões de usuário
  - Atualize as configurações de menu
  - Redefina as configurações de e-mail
  - Redistribua coletores (podem ser necessárias modificações em coletores selecionados)
  - Redistribua relatórios

6.2 Upgrade do Sentinel 4.x para o Sentinel 6.0

Questões a considerar:

- A Migração de dados do Microsoft SQL Server 2000 para Sentinel 4.x para Microsoft SQL Server 2005 para Sentinel 6.0 é suportada. (O SQL Server 2000 não é mais suportado no Sentinel 6.)
- A Migração de dados do Oracle 9i para Sentinel 4.x para Oracle 10g para Sentinel 6.0 é suportada.
- Quando a Migração de dados for bem-sucedida, os objetos a seguir são migrados do Sentinel 4.x para Sentinel 6.0:
  - Usuários e permissões designadas

- Filtros
- Opções de configuração do menu popup
- Tags CV renomeadas
- Configuração de partição
- Casos de 4.X são migrados para 6.0 como incidentes
- Incidentes e eventos relacionados a incidentes

- Quando a Migração de Dados é concluída, as regras de correlação e os eventos não são migrados. As regras de correlação podem ser exportadas do 5.x e importadas para o 6.0. Os eventos que são parte de um incidente serão migrados; outros eventos, não.

Para atualizar do Sentinel 4.x para Sentinel 6.0:

- Requisitos do sistema
  - Verifique se as especificações de Hardware do sistema atendem aos requisitos mencionados em Capítulo 2, “Melhores práticas” na página 17. Você pode precisar atualizar seu Hardware, pois as especificações de hardware do Sentinel 4.x e do Sentinel 6.0 são diferentes.
  - Verifique se o sistema operacional e as versões de banco de dados atendem aos requisitos de sistema mencionados em Capítulo 2, “Melhores práticas” na página 17.
  - Execute backup dos componentes necessários
  - Sentinel Server
  - Gerenciador do Coletor do Sentinel
  - Crystal Reporting Server
  - Servidor do banco de dados
  - Scripts do Coletor
  - Exporte Regras de Correlação
  - Faça backup de workflows do iTRAC
- Execute o Instalador do Patch fornecido pela Novell
- Instale o Banco de Dados do Sentinel 6.0
  - Você pode precisar instalar um novo Banco de Dados ou uma nova instância do Banco de Dados. O esquema de banco de dados do Sentinel 4.x é diferente do Sentinel 6.0. Há algumas tabelas que são incluídas/apagadas no Sentinel 6.0. A instalação de um novo Banco de Dados ou nova instância de banco de dados criaria/apagaria essas tabelas no Sentinel 6.0.
- Execute a Migração de Dados
- Instale o Sentinel 6.0 (excluindo Banco de dados)
- Configure objetos
  - Atualize as permissões de usuário
  - Atualize as configurações de menu
  - Redefina as configurações de e-mail
  - Redistribua coletores (podem ser necessárias modificações em coletores selecionados)
  - Modifique e redistribua relatórios

Instalando componentes do Sentinel

7

Tópicos incluídos neste capítulo:

- Seção 7.1, “Instalando um novo componente em uma máquina do Sentinel” na página 95
- Seção 7.1.1, “Instalando o Banco de Dados do Sentinel” na página 97

Há várias situações nas quais você pode precisar adicionar componentes a uma instalação existente:

- Os componentes do Sentinel estão em uma máquina e componentes adicionais são necessários (por ex., o Gerenciador de Coletor está em uma máquina e seria útil adicionar o Sentinel Control Center)
- Por motivos de desempenho em um ambiente de elevada taxa de eventos, um novo Gerenciador de Coletor ou Mecanismo de Correlação pode ser adicionado.

Qualquer das situações é simplificada com o instalador do Sentinel.

7.1 Instalando um novo componente em uma máquina do Sentinel

Às vezes, pode ser necessária uma máquina adicional para o ambiente do Sentinel. Se o uso de memória for alto no Mecanismo de Correlação, você pode adicionar outra. Você pode adicionar um Gerenciador de Coletor em um site remoto para coletar dados localmente, ou um novo funcionário pode precisar que o Sentinel Control Center seja instalado em seu computador.

Há vários pré-requisitos para instalação dos componentes do Sentinel em uma nova máquina:

- Endereço IP ou nome de host da máquina que hospeda o Servidor de Comunicação
- Acesso a uma cópia do arquivo .keystore de qualquer das máquinas na instalação do Sentinel existente
- Esse arquivo pode ser localizado em %ESEC_HOME%\config (no Windows) ou $ESEC_HOME/config (no Linux e Solaris).
- Você deve poder pesquisar o arquivo .keystore da máquina em que estiver instalando.
- Os números de porta usados na instalação inicial do Sentinel

---

Observação: O arquivo .keystore e os números de porta devem ser idênticos em todas as máquinas do sistema do Sentinel para permitir comunicação. Há duas exceções: o arquivo .keystore não é necessário na instalação do Sentinel Control Center ou na instalação do Gerenciador do Coletor usando comunicação proxy SSL.

Para adicionar Componentes:

1. Efetue login como usuário com direitos administrativos (no Windows); ou usuário root (no Solaris).
2. Insira o CD de instalação do Sentinel na unidade de CD-ROM.

3 Procure o CD e clique duas vezes em:

- No Solaris,

  Para o modo de interface gráfica:

  `./setup.sh`

  ou

  Para modo textual:

  `./setup.sh –console`

- No Windows, setup.bat.

  Observação: Não há suporte para a instalação no modo de console no Windows.

4 Depois de ler a tela de boas-vindas, clique em Avançar.

5 Leia e aceite o Contrato de Licença de Usuário Final e clique em Avançar.

6 Se você estiver instalando componente adicional, uma tela será exibida indicando o local da instalação anterior e quais componentes já estão instalados. Se você estiver instalando uma cópia nova do Sentinel, então uma tela indicando o diretório de instalação padrão será exibida. Clique em Pesquisar para alterar o local de instalação. Clique em Avançar.

7 Selecione os componentes que deseja adicionar.

Situação 1: se você instalar apenas Aplicativos:

7a Selecione o tipo de instalação "Personalizada" e clique em Avançar.

7b Selecione os Aplicativos (Construtor de Coletor do Sentinel, Sentinel Control Center e Gerenciador de Dados do Sentinel) e clique em Avançar.

7c Um prompt de tamanho de heap JVM (Máquina Virtual Java) será exibido. Clique em Avançar.

Tamanho de heap JVM (Mb) - por padrão, é definido como metade do tamanho da memória física detectada na máquina, com um máximo de 1024 MB. Esse será o tamanho de heap JVM máximo usado somente pelo Sentinel Control Center.

7d Você é solicitado a digitar informações de nome do servidor host/porta. Digite as informações necessárias e clique em Próximo.

Situação 2: se você instalar o Mecanismo de Correlação (componentes adicionais) depois de instalar o Aplicativo:

7e Selecione o Mecanismo de Correlação, clique em Avançar.

7f Selecione o método de obtenção da chave de barramento de mensagem. Especifique se deseja gerar um arquivo keystore aleatório ou importar o arquivo de armazenamento de chave existente de outra máquina no sistema do Sentinel. Se você selecionar importar um arquivo keystore existente, terá que navegar até o local e selecioná-lo. Clique em Avançar.

Situação 3: se você instalar o Mecanismo de Correlação e Aplicativos:

7g Selecione o tipo de instalação "Personalizada" e clique em Avançar.

7h Selecione os Aplicativos (Construtor de Coletor do Sentinel, Sentinel Control Center e Gerenciador de Dados do Sentinel) e Mecanismo de Correlação, clique em Avançar.

7i Um prompt de tamanho de heap JVM (Máquina Virtual Java) será exibido. Clique em Avançar.

7j Você será solicitado a digitar as informações da porta proxy do Sentinel Control Center e do nome de host do Servidor de Comunicação. Digite as informações necessárias e clique em Próximo.

7k Selecione o método de obtenção da chave criptográfica do barramento de mensagem. Especifique se deseja gerar um arquivo keystore aleatório ou importar o arquivo de armazenamento de chave existente de outra máquina no sistema do Sentinel. Se você selecionar importar um arquivo keystore existente, deverá navegar até o local e selecioná-lo. Clique em Avançar.

Situação 4: se você instalar o Sentinel Collector Service e Aplicativos:

7l Selecione o tipo de instalação "Personalizada" e clique em Avançar.

7m Selecione os Aplicativos (Construtor de Coletor do Sentinel, Sentinel Control Center e Gerenciador de Dados do Sentinel) e Sentinel Collector Service, e clique em Avançar.

7n Um prompt de tamanho de heap JVM (Máquina Virtual Java) será exibido. Clique em Avançar.

7o Você tem duas opções de comunicação entre os clientes do Sentinel e o Servidor. Você pode selecionar a comunicação "Conectar ao barramento de mensagem diretamente" ou "Conectar o barramento de mensagem com proxy". Clique em Avançar.

7p Você deverá digitar as informações de "Porta de barramento de mensagem" e "Nome de host do Servidor de Comunicação". Digite as informações necessárias e clique em Próximo.

Observação: Se você selecionar "Conectar ao barramento de mensagem usando proxy", a opção adicional "Porta de autenticação de Certificado do Gerenciador do Coletor" ficará disponível.

7q Selecione o método de obtenção da chave de barramento de mensagem. Especifique se deseja gerar um arquivo keystore aleatório ou importar o arquivo de armazenamento de chave existente de outra máquina no sistema do Sentinel. Se você selecionar importar um arquivo keystore existente, deverá navegar até o local e selecioná-lo. Clique em Avançar.

8 A tela Resumo é exibida. Revise o resumo de instalação, clique em Instalar.

9 Depois de concluída a instalação, será necessário reinicializar. Selecione "Sim, reinicie meu computador" e clique em Concluir para reiniciar seu sistema.

7.1.1 Instalando o Banco de Dados do Sentinel

Para instalar o Banco de Dados do Sentinel 6:

1 Antes de começar a instalação, apague as seguintes variáveis ambientais no Windows, se você tiver instalado o Sentinel anteriormente.

- ESEC_HOME
- ESEC_VERSION
- ESEC_JAVA_HOME
- ESEC_CONF_FILE
- WORKBENCH_HOME

2. Efetue login como usuário com direitos administrativos (no Windows); ou como usuário root (no Solaris ou Linux).
3. Insira o CD de instalação do Sentinel na unidade de CD-ROM.
4. Procure o CD e clique duas vezes em:
   - No Linux/Solaris,

     Para o modo de interface gráfica:

     ```
     ./setup.sh
     ```

     ou

     Para modo textual:

     ```
     ./setup.sh –console
     ```
   - No Windows, setup.bat.

   Observação: Não há suporte para a instalação no modo de console no Windows.
5. Depois de ler a tela de boas-vindas, clique em Avançar.
6. Leia e aceite o Contrato de Licença de Usuário Final e clique em Avançar.
7. Aceite o diretório de instalação padrão ou clique em Procurar para especificar um local diferente. Clique em Avançar.

8. No tipo de instalação, selecione Personalizado (padrão). Clique em Avançar.
9. Na janela de seleção de recursos, anule a seleção de todas as opções e selecione Banco de Dados. Clique em Avançar.

   Observação: Verifique se desmarcou o recurso pai “Serviços do Sentinel”. Ele ficará esmaecido com uma marca de seleção se ainda estiver selecionado, mas todos os recursos filho serão desmarcados.
10. Configure o banco de dados para instalação:
    - No Windows:

    10a Selecione a plataforma de servidor do banco de dados de destino.
    - Selecione Microsoft SQL server 2005.
    - Especifique o diretório de registro de Instalação do Banco de Dados.

    Clique em Avançar.

    10b Especifique o local de armazenamento para:
    - Diretório de dados
    - Diretório de Índices
    - Diretório de Dados de Resumo
    - Diretório de Índices de Resumo
    - Diretório de Registro

Clique em Avançar.

10c Selecione a opção de suporte do conjunto de caracteres do banco de dados, banco de dados Unicode ou ASCII somente. Clique em Avançar.

10d Especifique o tamanho do banco de dados. Clique em Avançar.

10e Configure partições de banco de dados.

- Você pode selecionar Habilitar partições de banco de dados automáticas.
- Para partições de dados, especifique o diretório de arquivo; digite especificações de Horário para adicionar e arquivar dados.

Clique em Avançar.

No Linux/Solaris:

10f Selecione a plataforma de servidor do banco de dados de destino.

- Selecione Oracle 10g na lista suspensa.
- Selecione Criar Novo banco de dados com objetos de banco de dados.

Clique em Avançar.

10g Especifique o Nome de Usuário do Oracle ou Aceite o nome de usuário padrão. Clique em OK

10h Selecione o driver JDBC do Oracle e especifique o nome do Banco de dados. Clique em Avançar.

10i Aceite o espaço de memória e porta de escuta padrão ou especifique novos valores.

10j Digite as credenciais SYS e SYS e clique em Avançar.

10k Especifique o tamanho do banco de dados. Clique em Avançar.

10l Especifique o local de armazenamento para:

- Diretório de dados
- Diretório de Índices
- Diretório de Dados de Resumo
- Diretório de Índices de Resumo
- Diretório de Registro

Clique em Avançar.

10m Configure partições de banco de dados.

- Selecione Habilitar partições de banco de dados automáticas e
- Especifique o diretório de arquivo de partição de dados.
- Digite as especificações de Horário para adicionar e arquivar dados.

Clique em Avançar.

11 Digite Informações de Autenticação para:

- Usuário Administrador do Banco de Dados do Sentinel
- Usuário de Banco de Dados do Aplicativo Sentinel
- Usuário Administrador do Sentinel
- Usuário de Relatório do Sentinel (somente no Windows)

Clique em Avançar.

12 O resumo de parâmetros de Banco de Dados especificados será exibido. Clique em Avançar.

13 O Resumo da instalação será exibido. Clique em Instalar.

14 Quando a instalação for concluída, selecione reiniciar o sistema e clique em Concluir.

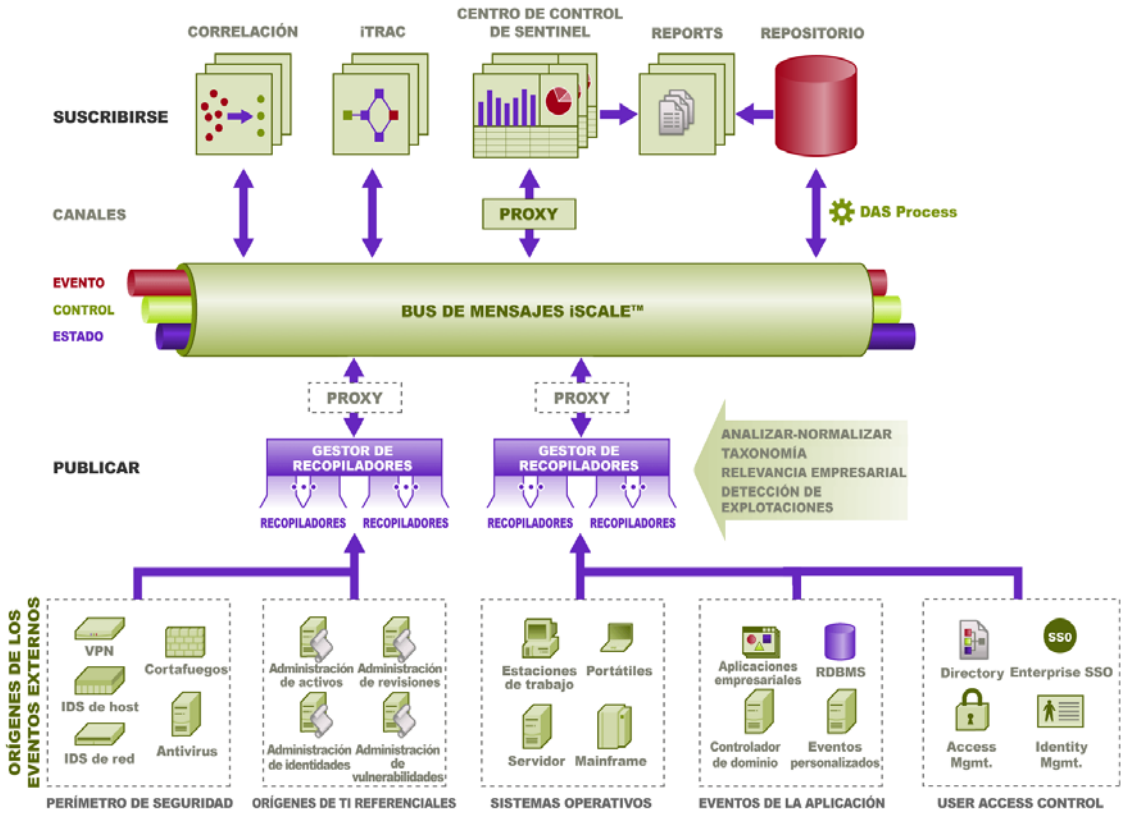
Camada de Comunicação (iSCALE)

8

1 Tópicos incluídos neste capítulo:

- Seção 8.1, “Proxy SSL e Comunicação Direta” na página 102
- Seção 8.2, “Mudanças da Chave Criptográfica” na página 105

A camada de comunicação (iSCALE) que conecta todos os componentes da arquitetura é uma conexão baseada em TCP/IP criptografada criada em um backbone JMS (Java Messaging Service). No Sentinel 6, um proxy SSL opcional foi adicionado para proteger o Gerenciador de Coletor e os componentes do Sentinel Control Center, se eles estiverem instalados fora do firewall.



Há duas opções de comunicação disponíveis ao instalar o Gerenciador de Coletor:

- **Conectar diretamente com o barramento de mensagem (padrão):** Essa é a opção mais simples e rápida. Ela exige que o Gerenciador do Coletor conheça a chave criptográfica compartilhada do barramento de mensagem; no entanto, isso pode ser um risco de segurança se o Gerenciador de Coletor estiver sendo executado em uma máquina que é exposta a ameaças de segurança (ex.: uma máquina no DMZ). Essa opção critografará a comunicação usando criptografia AES de 128 bits com base no valor de um arquivo chamado .keystore.
- **Conectar ao barramento de mensagem por meio de proxy:** Essa opção adiciona uma camada de segurança extra, configurando o Gerenciador de Coletor para se conectar por meio

de um servidor proxy SSL. Nesse caso, a autenticação e a criptografia baseadas em certificado serão usadas para que .keystore não precise ser armazenado na máquina do Gerenciador do Coletor. Essa é uma boa opção quando o Gerenciador do Coletor está instalado em um ambiente menos seguro.

Qualquer uma dessas opções pode ser escolhida ao instalar o Gerenciador do Coletor. O Sentinel Control Center usa o proxy por padrão.

8.1 Proxy SSL e Comunicação Direta

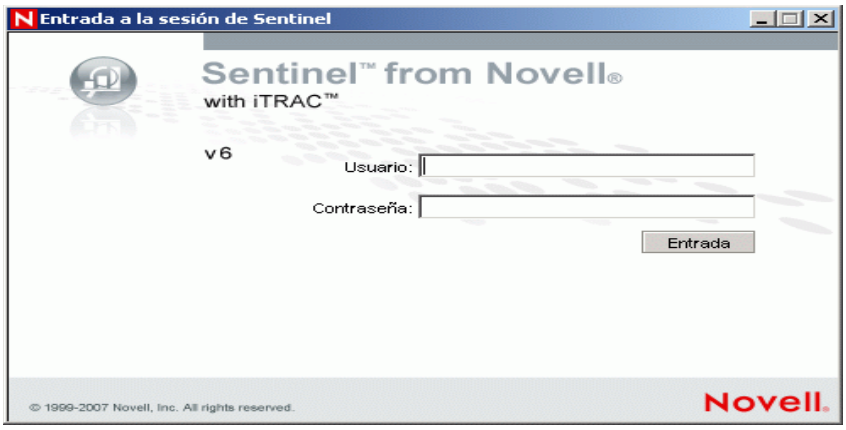
Os componentes do Sentinel que podem usar o proxy SSL são o Sentinel Control Center e o Gerenciador de Coletor.

8.1.1 Sentinel Control Center

O Sentinel Control Center usa o proxy SSL por padrão. O Sentinel Control Center se conecta ao SSL por meio da porta proxied_client. Essa porta é configurada para usar apenas a autenticação de certificado SSL do lado do servidor. A autenticação de cliente usa o nome de usuário e senha do usuário do Sentinel Control Center.

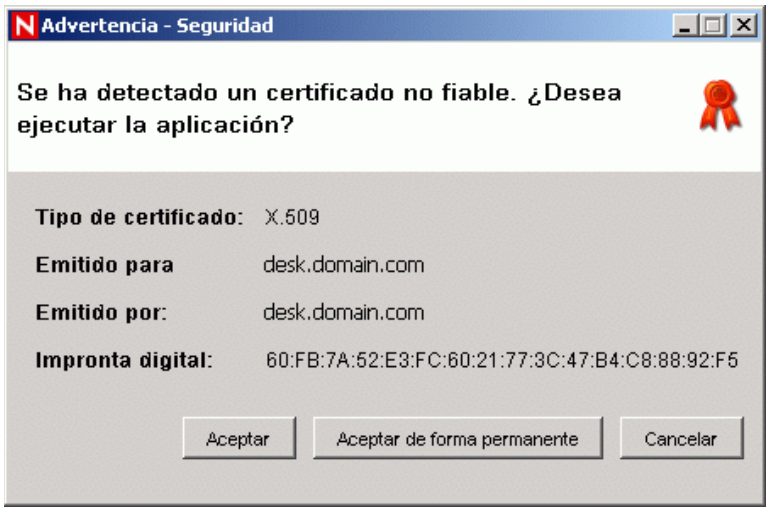
Para fazer login no Sentinel Control Center pela primeira vez:

1. Ir para Iniciar > Programas > Sentinel e selecionar Sentinel Control Center. A janela de Login do Sentinel será exibida.



2. Digite as credenciais do usuário que você possui para fazer login no Sentinel Control Center.
   - Nome de usuário e senha, se estiver usando autenticação do SQL Server, OU
   - Domínio\nome de usuário e senha, se estiver usando a autenticação do Windows
3. Clique em Login.

4 Será exibida uma mensagem de aviso conforme mostrado na figura abaixo, para a primeira tentativa de logon.



5 Se você selecionar Aceitar, essa mensagem será exibida toda vez que você tentar abrir o Sentinel em seu sistema. Para evitar isso, você pode selecionar Aceitar permanentemente.

Para Iniciar o Sentinel Control Center no Linux e Solaris:

1 Como Usuário do Administrador do Sentinel (esecadm), mude o diretório para:
`$ESEC_HOME/bin`

2 Execute o seguinte comando:
`control_center.sh`

3 Digite seu nome de usuário e senha e clique em OK.

4 Uma janela Certificado será exibida, clique em Aceitar.

Os usuários do Sentinel Control Center precisarão repetir o procedimento acima para aceitar um novo certificado nas circunstâncias a seguir:

- O servidor de comunicação do Sentinel é reinstalado
- O servidor de comunicação do Sentinel é movido para um novo servidor

8.1.2 Gerenciador de Coletor

O Gerenciador de Coletor pode ser instalado no modo proxy (usando o proxy SSL) ou modo direto (conectando diretamente ao barramento de mensagem.

- Para Gerenciadores de Coletor que possam ser comprometidos mais facilmente (por exemplo, uma máquina no DMZ), o proxy SSL é o método de comunicação mais seguro.
- Para Gerenciadores do Coletor em um ambiente mais seguro ou em que uma alta circulação de eventos é importante ou instalado na mesma máquina que o DAS (Data Access Service), a comunicação direta para o barramento de mensagem é recomendada.

O Gerenciador de Coletor se conecta ao SSL por meio do proxied_trusted_client. Para habilitar o Gerenciador de Coletor para ser reiniciado sem intervenção humana depois de uma reinicialização,

essa porta é configurada para usar a autenticação de certificado SSL de servidor e cliente. Um relacionamento de confiança é estabelecido entre o proxy e o Gerenciador de Coletor (troca de certificados), com conexões futuras usando os certificados para autenticação. Esse relacionamento de confiança é configurado automaticamente durante a instalação.

O relacionamento de confiança precisará ser redefinido para cada Gerenciador de Coletor usando o proxy SSL nestas circunstâncias:

- O servidor de comunicação do Sentinel é reinstalado
- O servidor de comunicação do Sentinel é movido para um novo servidor

Para redefinir o relacionamento de confiança de um Gerenciador de Coletor:

1. Faça login no servidor de Gerenciador de Coletor como o Administrador do Sentinel (esecadm por padrão).
2. Abra o arquivo configuration.xml em $ESEC_HOME/config ou %ESEC_HOME%\config em um editor de texto.
3. Modifique os serviços "Collector_Manager", "agentmanager_events" e "Sentinel" em configuration.xml para que usem o ID de estratégia "proxied_trusted_client". A seguir, uma amostra do arquivo de exemplo:

```
<service name="Collector_Manager" plugins=""
strategyid="proxied_trusted_client"/>
<service name="agentmanager_events" plugins=""
strategyid="proxied_trusted_client"/>
<service name="Sentinel" plugins=""
strategyid="proxied_trusted_client"/>
```

4. Grave o arquivo e saia.
5. Abra o arquivo sentinel.xml em $ESEC_HOME/config ou %ESEC_HOME%\config em um editor de texto.
6. Remova os componentes a seguir do arquivo sentinel.xml:

```
<obj-component id="SentinelRemoteLoggingService">
<!-- Must be after the service manager -->
<class>esecurity.ccs.comp.audit.LogHandlerService</class>
<property name="Level">SEVERE</property>
</obj-component>
```

7. Grave o arquivo e saia.
8. Execute %ESEC_HOME%\bin\register_trusted_client.bat (ou arquivo .sh no UNIX). Você verá uma saída similar esta:

```
E:\Program Files\novell\sentinel6>bin\register_trusted_client.bat
Please review the following server certificate:
Type:X.509
Issued To:foo.bar.net
Issued By:foo.bar.net
Would you like to accept this certificate? [Y/N] (defaults to N): Y
Please enter a Sentinel username and password that has permissions
to register a trusted client.
Username: esecadm
Password:*********
*Writing to keystore file: E:\Program
Files\novell\sentinel6\config\.proxyClientKeystore
```

9 Reinicie o Serviço do Sentinel no servidor que hospeda o Servidor de Comunicação. Aguarde até que o Proxy do DAS conclua a inicialização.

10 Reinicie o Serviço do Sentinel no servidor que hospeda o Gerenciador de Coletor.

11 Repita essas etapas em todos os Gerenciadores de Coletor usando a comunicação proxy.

8.2 Mudanças da Chave Criptográfica

A instalação do Sentinel permite que o administrador gere uma nova chave criptográfica aleatória (armazenada no arquivo .keystore) ou importe um arquivo .keystore existente. Com qualquer um dos métodos, o arquivo .keystore deve ser o mesmo em todas as máquinas do ambiente do Sentinel para que as comunicações funcionem adequadamente.

Observação: O arquivo .keystore não é necessário na máquina do banco de dados se o banco de dados for o único componente do Sentinel instalado nessa máquina.

A chave criptográfica pode ser mudada com um utilitário chamado keymgr. O programa gera um arquivo no diretório lib de uma instalação do Sentinel ($ESEC_HOME/lib ou %ESEC_HOME%\lib) chamado .keystore. Esse arquivo deve ser copiado para o mesmo diretório em todas as máquinas que tenha um componente do Sentinel instalado.

Para alterar a chave criptográfica para Comunicação Direta:

1 Em UNIX, faça login como o Usuário Administrador do Sentinel (esecadm por padrão). No Windows, efetue login como um usuário com direitos administrativos.

2 Consulte:

Para Windows:

```
%ESEC_HOME%\bin
```

Para UNIX:

```
$ESEC_HOME/bin
```

3 Execute o seguinte comando:

No Windows:

```
"%ESEC_JAVA_HOME%\java" -jar keymgr.jar --keyalgo AES --keysize 256
--keystore <filename, usually .keystore>
```

No UNIX:

```
$ESEC_JAVA_HOME/java -jar keymgr.jar --keyalgo AES --keysize 256 --
keystore <filename, usually .keystore>
```

4 Copie .keystore em todas as máquinas com um componente Sentinel instalado (a menos que esteja usando a comunicação proxy). O arquivo deve ser copiado em:

Para Windows:

```
%ESEC_HOME%\config
```

Para UNIX:

```
$ESEC_HOME/config
```

8.2.1 Mudanças na senha do Consultor

Se estiver usando o Consultor no modo Download Direto, você deve atualizar as senhas armazenadas nos arquivos de configuração do Consultor. Essa senha é criptografada com as informações em .keystore e deve ser recriada com o novo valor de .keystore.

Para criptografar a senha do Consultor depois de uma mudança da chave criptográfica:

1. Em UNIX, faça login na máquina em que o Consultor está instalado como o Usuário Administrador do Sentinel (esecadm por padrão). No Windows, efetue login como um usuário com direitos administrativos.
2. Mude de diretório:

   Para UNIX:

   ```
   $ESEC_HOME/sentinel/bin
   ```

   Para Windows:

   ```
   %ESEC_HOME%\sentinel\bin
   ```
3. Digite os seguintes comandos:

   Para UNIX:

   ```
   ./adv_change_passwd.sh <newpassword>
   ```

   Para Windows:

   ```
   adv_change_passwd.bat <newpassword>
   ```

Crystal Reports para Windows

9

Tópicos incluídos neste capítulo:

- Seção 9.3, “Requisitos de configuração” na página 109
- Seção 9.3.1, “Instalando o Microsoft Internet Information Server (IIS) e o ASP.NET” na página 110
- Seção 9.6.1, “Visão geral da instalação para Microsoft SQL 2005 Server com Autenticação do Windows” na página 111
- Seção 9.6.3, “Visão geral da instalação para Oracle” na página 112
- Seção 9.7.1, “Instalando o Crystal Server Para Microsoft SQL 2005 Server com Autenticação do Windows” na página 113
- “Configurando o Open Database Connectivity (ODBC) para Autenticação SQL” na página 121
- Seção 9.7.3, “Instalando o Crystal Server para Oracle” na página 122
- “Publicando gabaritos de relatório usando o Crystal Publishing Wizard” na página 127
- Seção 9.8.6, “Configurando o Sentinel Control Center para integração com o Crystal Enterprise Server” na página 132

O Crystal Businessobjects Enterprise™ é uma ferramenta de geração de relatórios.

Este capítulo aborda a instalação e configuração do Crystal Reports Server para Sentinel.

O Sentinel suporta a execução do Crystal Reports Server nas seguintes plataformas:

- Windows - suportado para execução do Banco de Dados do Sentinel no Windows ou Linux.
- Linux - suportado para execuão do Banco de Dados do Sentinel no Linux.

Este capítulo aborda a execução do Crystal Reports Server no Windows. Para obter mais informações sobre a execução do Crystal Reports Server no Linux, consulte Capítulo 10, “Crystal Reports para Linux” na página 133.

Para Instalar o Crystal Reports Server:

1. Instale o Microsoft IIS e o ASP.NET
2. Instale o Microsoft SQL (dependendo da configuração como autenticação do Windows ou autenticação do SQL Server)
3. Instale o Crystal Server
   - Configurando o Open Database Connectivity (ODBC) para Autenticação SQL

     ou
   - Instalando e configurando o software cliente do Oracle 9i
4. Configure inetmgr
5. Aplicação do patch do Crystal Reports;
6. Publicação (importação) de Crystal Reports;
7. Definindo uma conta de Usuário Nomeado

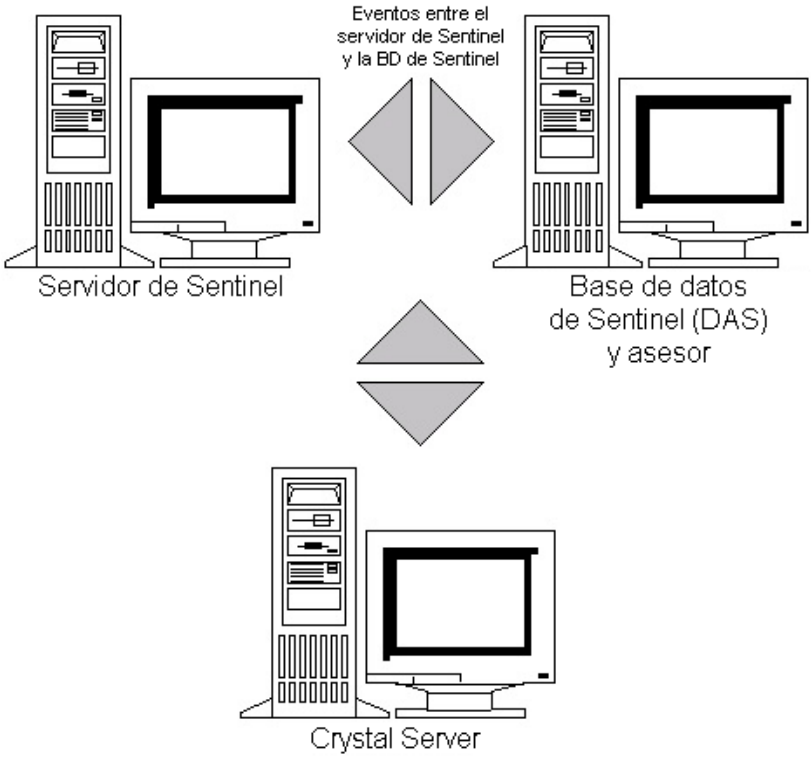
8 Testando a conectividade com o servidor Web

9 Aumentando o limite de atualização de registro do relatório do Crystal Enterprise Server (recomendado)

10 Configurando o Sentinel Control Center para integração com o Crystal Enterprise Server.

A instalação deve ser feita na ordem apresentada.

Observação: Você deve instalar o Crystal Reports Server na ordem fornecida acima.



9.1 Visão geral

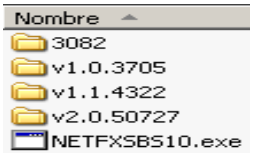
O Crystal Reports Server requer um banco de dados para armazenar informações sobre o sistema e seus usuários. Esse banco de dados é conhecido como o banco de dados do Central Management Server (CMS). O CMS é um servidor que armazena informações sobre o sistema do Crystal Reports Server. Outros componentes do Crystal Reports Server podem acessar essas informações de acordo com a necessidade.

É preciso configurar um banco de dados CMS sobre um banco de dados Microsoft SQL Server Local. O instalador do Crystal Reports Server permite configurar o banco de dados CMS sobre o banco de dados MSDE se um Microsoft SQL 2005 Server local não estiver instalado. O Sentinel não tem suporte para uma configuração MSDE.

9.2 Requisitos do sistema

Windows® 2003 Server com SP1 com uma partição formatada em NTFS com o IIS (Microsoft Internet Information Server) e o NET.ASP instalados. O Sentinel não tem suporte para o Crystal XI no Windows® 2000 Server.

.NET Framework 1.1 (Instalado por padrão no Windows 2003. O BusinessObjects Enterprise™ XI não suporta o .NET Framework 2.0). Para determinar qual versão do .NET Framework está na máquina, vá para %SystemRoot%\Microsoft.NET\Framework. A pasta com o maior valor numérico não deve ser maior do que v.1.1.xxxx. Por exemplo:

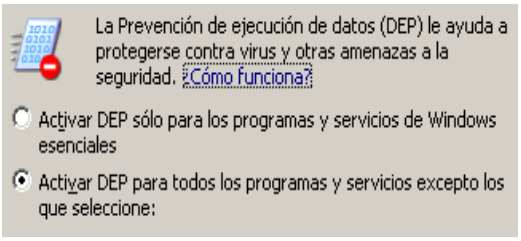


9.3 Requisitos de configuração

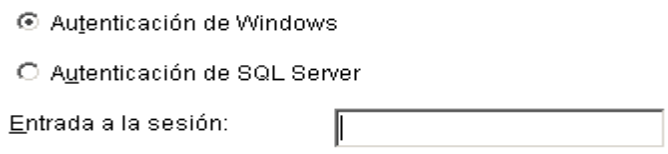
1. Verifique se a conta usada para instalar o Crystal Reports Server tem direito de administrador local.
2. Configure a DEP (Prevenção de Execução de Dados) para que seja executada apenas em programas e serviços essenciais do Windows. Isso é particularmente útil para evitar o "Erro 1920. Servidor de Cache do Serviço Crystal Report no Windows 2003".

   DEP é acessado em Painel De Controle > Sistema > guia Avançado > Configurações de Desempenho > Prevenção de Execução de Dados.

   Selecione Ativar DEP apenas para programas e serviços essenciais do Windows.



Se você planeja executar relatórios do Sentinel usando a autenticação do Windows NT, verifique se a conta do domínio Windows para o usuário do Sentinel Report já existe no banco de dados do Sentinel. Isso é feito durante a instalação do Sentinel, selecionando a Autenticação do Windows ao definir Método de Autenticação para Usuário do Sentinel Report, como mostra a ilustração a seguir.



3 Se você planeja executar relatórios do Sentinel usando a autenticação do SQL Server (também necessária para instalações do Sentinel Oracle), verifique se o login do SQL Server (esecrpt) já existe no banco de dados do Sentinel.

- No banco de dados do Microsoft SQL do sentinel - isso é feito durante a instalação do Sentinel para Microsoft SQL, selecionando Autenticação do Servidor SQL ao definir o Método de Autenticação para usuário do Sentinel Report, como na ilustração a seguir.

- No banco de dados Oracle do Sentinel – isso é feito durante a instalação do Sentinel para Oracle. O esecrpt recebe a mesma senha que esecadm.

4 No Oracle - Oracle 9i Client Release 2 (9.2.0.1.0), instale-o antes de instalar o Crystal Business Enterprise™ XI.

5 No Microsoft SQL Server - instale o Microsoft SQL 2005 antes de instalar o Crystal Reports Server XI.

6 Resolução de vídeo de 1024 x 768 ou superior

7 Instale o Microsoft Internet Information Server (IIS) e o NET.ASP

Observação: O Sentinel não tem suporte para o MSDE. Instale o Microsoft SQL 2005 antes de instalar o Crystal Reports Server XI.

9.3.1 Instalando o Microsoft Internet Information Server (IIS) e o ASP.NET

Para adicionar esses componentes do Windows, talvez seja necessário usar o CD de instalação do Windows 2003 Server.

Para instalar IIS e ASP.NET:

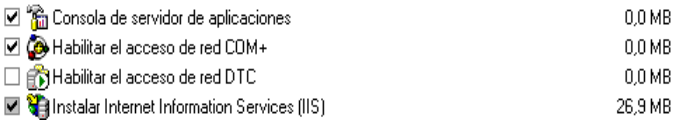
1 Vá para o Painel de Controle do Windows>Adicionar ou remover programas.

2 No painel vertical esquerdo, clique em Adicionar ou remover componentes do Windows.

3 Selecione Servidor de aplicativo.

4 Clique em Detalhes.

5 Selecione ASP.NET e Internet Information Services (IIS).



6 Clique em OK.

7 Clique em Próximo. Você pode ser solicitado a usar o CD de instalação do Windows.

8 Clique em Concluir.

9.4 Problemas conhecidos

1 Instalando o Crystal Reports – você recebe duas chaves, uma para o Crystal Reports Server e outra para o Crystal Reports Developer. Use a chave do Crystal Reports Server ao instalar o Crystal Reports Server.

2 Desinstalando o Crystal Reports – caso seja necessário desinstalar o Crystal Reports Server, há um procedimento manual de desinstalação disponível que limpa as chaves do registro. Isso é útil quando a instalação é corrompida. Visite este site da Businessobjects para obter os procedimentos para desinstalar manualmente o BusinessObjects Enterprise XI, http://support.businessobjects.com/library/kbase/articles/c2017905.asp (http://support.businessobjects.com/library/kbase/articles/c2017905.asp).

Observação: Esse URL estava correto no momento da publicação deste documento.

9.5 Usando Crystal Reports

Para obter mais informações sobre o uso do Crystal Reports para Relatórios do Sentinel, consulte a Documentação do Crystal Reports e o Guia do Usuário do Sentinel.

9.6 Visão geral da instalação

9.6.1 Visão geral da instalação para Microsoft SQL 2005 Server com Autenticação do Windows

Para instalar o Microsoft SQL Server com Autenticação do Windows:

1 Instale o Crystal Reports Server XI - ao instalar o aplicativo Sentinel, se você selecionar a Autenticação do Windows para o usuário do Sentinel Report, siga o link para Seção 9.7.1, “Instalando o Crystal Server Para Microsoft SQL 2005 Server com Autenticação do Windows” na página 113.

2 Configure ODBC (Open Database Connectivity)

3 Mapeie Crystal Reports para uso com o Sentinel

4 Aplique patches do Crystal Reports

5 Publique relatórios

6 Defina o usuário conforme Conta de usuário nomeado

7 Importe gabaritos do Crystal Reports

8 Crie uma página na Web do Crystal (Configurando o Launchpad de Administração do .NET)

9 Configure o Sentinel para o Crystal Enterprise Server

Observação: Você deve instalar o Microsoft SQL Server com Autenticação do Windows na ordem fornecida abaixo.

9.6.2 Visão geral da instalação para Microsoft SQL 2005 Server com autenticação do servidor SQL

Para instalar o Microsoft SQL Server com Autenticação do SQL Server:

1 Instalar Crystal Reports Server XI.

Observação: Ao instalar o aplicativo Sentinel, se você selecionou a Autenticação do SQL Server para o usuário do Sentinel Report, siga o link para Seção 9.7.2, “Instalando o Crystal Server para Microsoft SQL 2005 Server com autenticação de SQL” na página 118.

---

2 Configure ODBC (Open Database Connectivity)

3 Mapeando o Crystal Reports para uso com o Sentinel

4 Importe gabaritos do Crystal Reports

5 Crie uma página na Web do Crystal (Configurando o Launchpad da Administração do .NET)

6 Configure o Sentinel para o Crystal Enterprise Server

Observação: Você deve instalar o Microsoft SQL Server com Autenticação do SQL Server na ordem fornecida abaixo.

9.6.3 Visão geral da instalação para Oracle

Para instalar o Oracle:

Para instalar adequadamente o Crystal Reports, execute o seguinte procedimento na ordem apresentada.

1 Instale o cliente do Oracle 9i

2 Instale Crystal Reports Server XI. Para obter maiores informações, consulte Seção 9.7.2, “Instalando o Crystal Server para Microsoft SQL 2005 Server com autenticação de SQL” na página 118.

3 Configure o driver nativo do Oracle

4 Mapeando o Crystal Reports para uso com o Sentinel

5 Importe gabaritos do Crystal Reports

6 Crie uma página da Web do Crystal (Configurando o Launchpad da Administração do .NET)

7 Configure o Sentinel para o Crystal Enterprise Server

Observação: Você deve instalar o Oracle na ordem fornecida acima.

9.7 Instalação

Esta seção descreve como instalar o Crystal Server para:

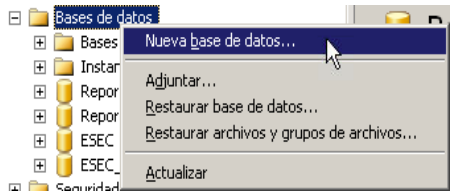
- Banco de dados do Sentinel do Microsoft SQL 2005 Server com autenticação de Windows
- Banco de dados do Sentinel do Microsoft SQL 2005 Server com autenticação do Servidor SQL
- Banco de dados Oracle do Sentinel

9.7.1 Instalando o Crystal Server Para Microsoft SQL 2005 Server com Autenticação do Windows

Para instalar BOE XI Crystal Server com autenticação do Windows:

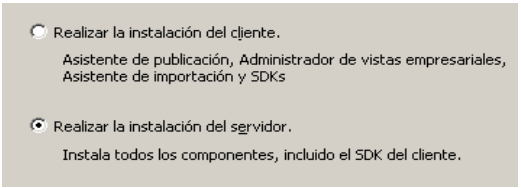
1. Instale Microsoft SQL 2005 no modo misto.
2. Inicie o Microsoft SQL Management Studio.
3. No painel de navegação, expanda Bancos de Dados.

   Realce e clique o botão direito em Banco de Dados e selecione Novo Banco de Dados…

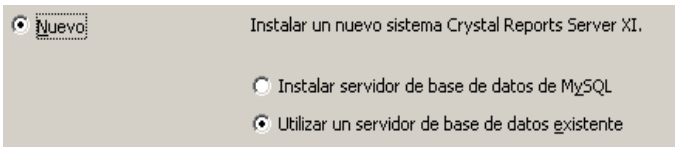


4. No campo de nome do Banco de Dados, BOE11 e clique em OK.

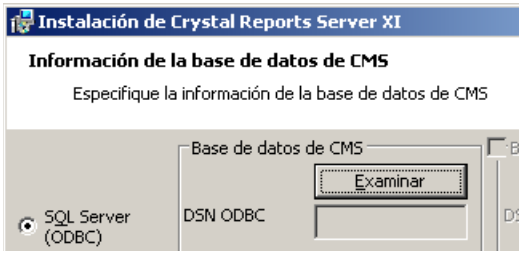
5. Saia do Microsoft SQL Management Studio.
6. Insira o CD do Crystal Reports XI Server na unidade de CD-ROM.
7. Se a Reprodução Automática estiver desativada na máquina, execute setup.exe.
8. Na janela Select Client or Server Installation (Selecionar Instalação de Cliente ou Servidor), selecione Perform Server Installation (Executar Instalação de Servidor).



9 Como o tipo de instalação, selecione o botão New (Nova) e não marque ‘Install MSDE or use existing local SQL Server’ (Instalar MSDE ou usar Servidor SQL local existente).



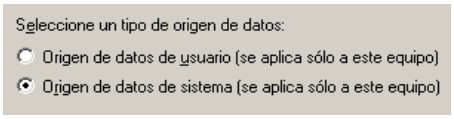
10 No Painel de Banco de Dados CMS, clique em Pesquisar.



11 Clique na guia Machine Data Source (Fonte de Dados da Máquina).

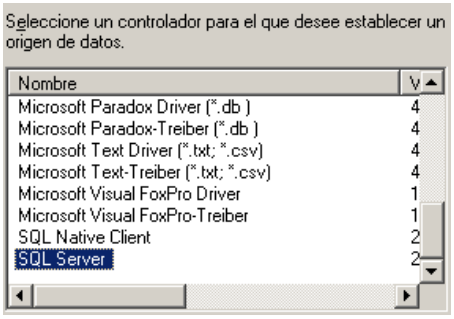
12 Clique em Novo.

13 Selecione Origem de Dados do Sistema.

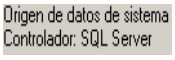


Clique em Avançar.

14 Role para baixo, selecione Servidor SQL e clique em Avançar.

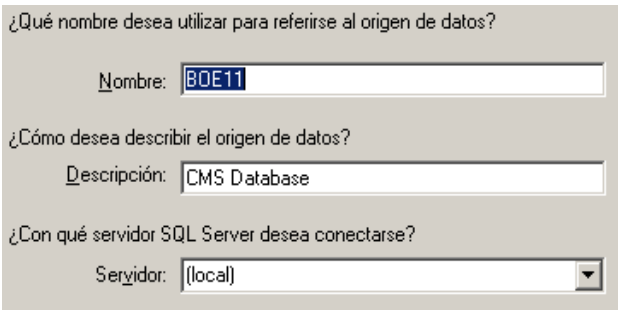


15 Será exibida uma nova fonte. Clique em Concluir.



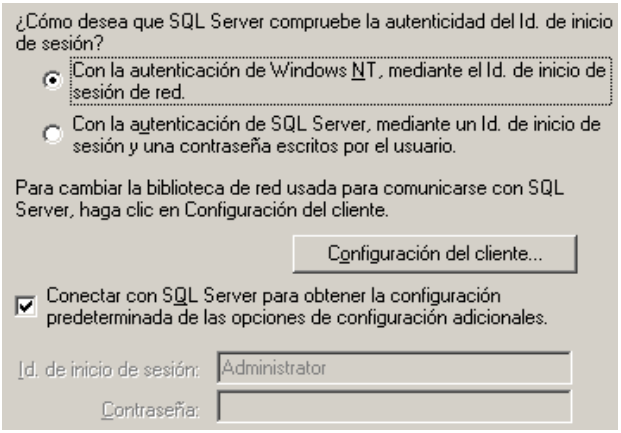
16 Na janela Nova Fonte de Dados para Servidor SQL, digite:

- Nome de sua fonte de dados (por ex.: i.e. BOE_XI)
- A descrição (opcional)
- Para o servidor, clique na seta para baixo e selecione (local)



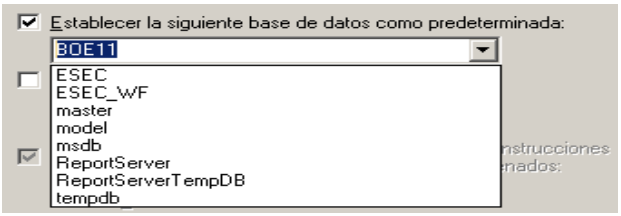
Clique em Avançar.

Se ainda não tiver feito isso, selecione Com Windows NT, clique em Avançar.



Observação: A ID de login (esmaecida) é o seu nome de login no Windows.

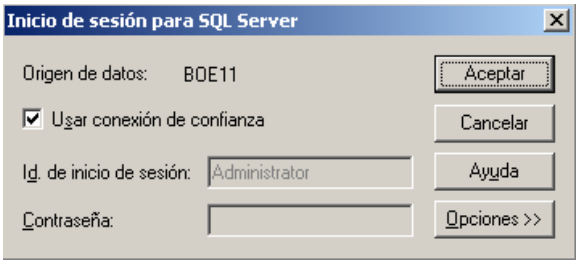
Marque a caixa ‘change default database to:’ (mudar o banco de dados padrão para). Altere o banco de dados padrão para BOE11. Clique em Avançar.



17 Na janela ‘Create a New Data Source to SQL Server’ (criar nova fonte de dados para servidor SQL), clique em Concluir.

18 Clique em Testar Fonte de Dados e teste a fonte de dados. Quando o teste da fonte de dados for concluído, clique em OK.

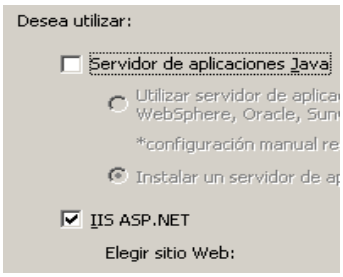
Na janela Select Data Source (selecionar fonte de dados), realce BOE11 e continue a clicar em OK até que seja exibido ‘SQL Server Login’ (login do servidor SQL). Verifique se Use Trusted Connection (Usar Conexão Confiável) está selecionado. Clique em OK.



Observação: A ID de login (esmaecida) é o seu nome de login no Windows.

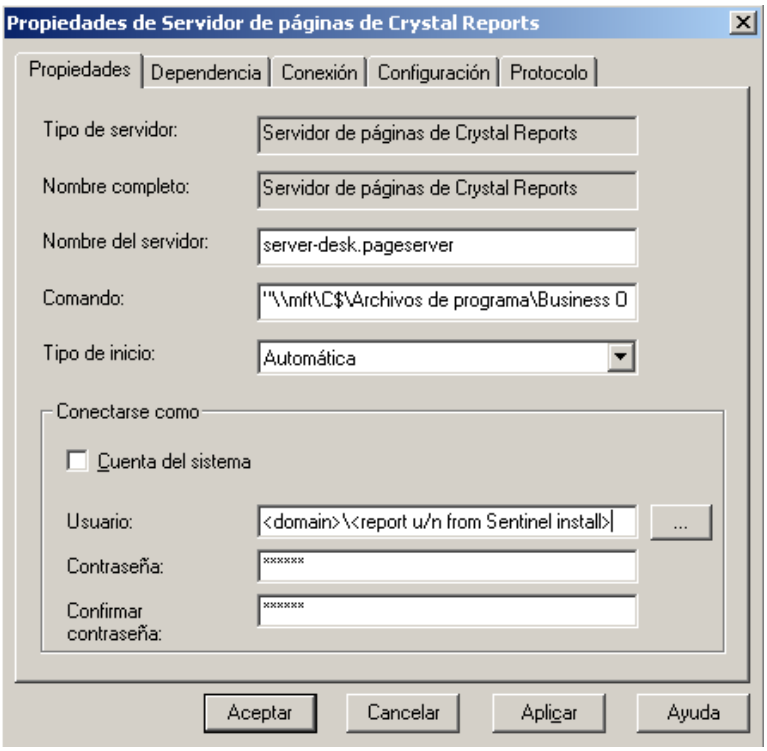
19 Na janela Web Component Adapter Type (Tipo de Adaptador de Componente Web), selecione IIS ASP.NET.

Observação: Se você não tiver instalado o IIS e o ASP.NET usando o Painel de Controle > Adicionar Remover Programas > Adicionar ou remover componentes do Windows, o IIS ASP.NET ficará esmaecido.



1 Após a instalação, será preciso mudar a conta de login para o Crystal Reports Page Server e o Crystal Reports Job Server para a conta de domínio do Usuário do Relatório do Sentinel.

- Clique Em Iniciar>Todos Os Programas>Businessobjects>Crystal Reports Server>Central Configuration Manager.
- Clique o botão direito em Crystal Reports Page Server e selecione Parar.
- Clique novamente o botão direito em Crystal Reports Page Server e selecione Propriedades.
- Desmarque Log On As System Account (Fazer Logon como Conta do Sistema) e digite o nome de usuário e a senha do domínio do Usuário do Relatório do Sentinel usados durante a instalação do Sentinel Clique em OK.



2 Realce Crystal Reports Page Server, clique o botão direito do mouse para iniciar o Crystal Reports Page Server.

Configurando o Open Database Connectivity (ODBC) para Autenticação do Windows

Este procedimento configura uma fonte de dados ODBC entre o Crystal Reports no Windows e o Servidor SQL. Isso precisa ser realizado na máquina do Crystal Server.

Para configurar uma fonte de dados ODBC para autenticação do Windows:

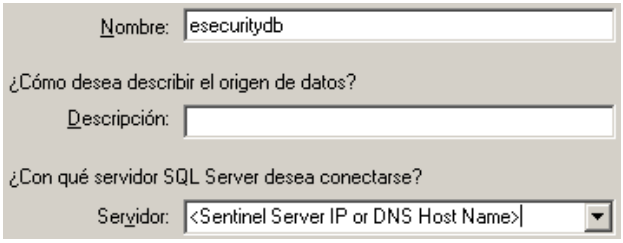
1 Vá para o Painel de Controle do Windows>Ferramentas Administrativas>Fontes de Dados (ODBC).

2 Clique na guia DSN de Sistema e clique no botão Adicionar.

3 Selecione Servidor SQL. Clique em Concluir.

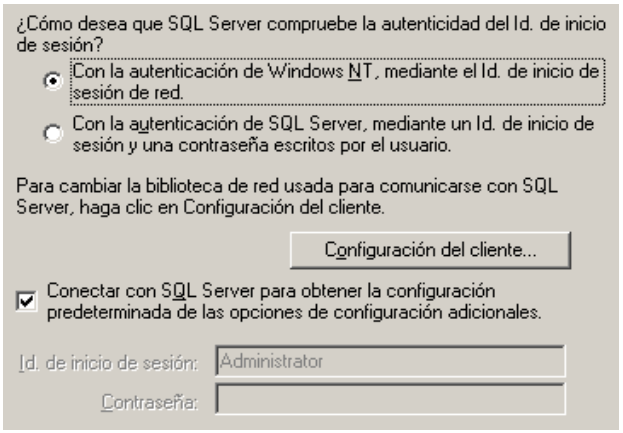
4 Será exibida uma tela solicitando as informações de configuração do driver:

- Em Nome da Fonte de Dados, digite esecuritydb
- No campo Descrição (opcional), digite uma descrição
- No campo Servidor, digite o nome do host ou o endereço IP do Sentinel Server



Clique em Avançar.

Na tela seguinte, selecione Autenticação do Windows.



Observação: A ID de login (esmaecida) é o seu nome de login no Windows.

5 Na próxima tela, selecione:

- Mude o banco de dados do Sentinel (o nome padrão é ESEC)
- Deixe todas as configurações padrão

Clique em Avançar.

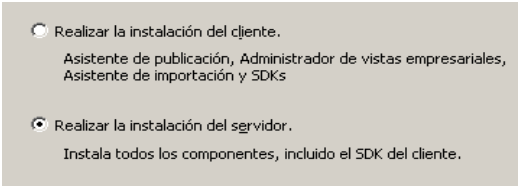
6 Clique em Concluir.

7 Clique em Test Data Source… (Testar Fonte de Dados). Você deve conseguir estabelecer uma conexão. Clique em OK até sair.

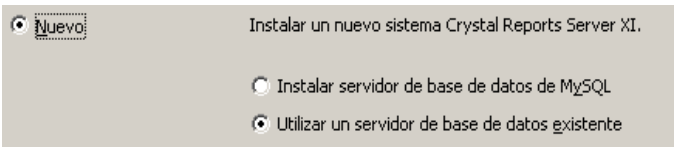
9.7.2 Instalando o Crystal Server para Microsoft SQL 2005 Server com autenticação de SQL

Para autenticar BOE XI Crystal Server SQL:

Na janela Select Client or Server Installation (Selecionar Instalação de Cliente ou Servidor), selecione Perform Server Installation (Executar Instalação de Servidor).

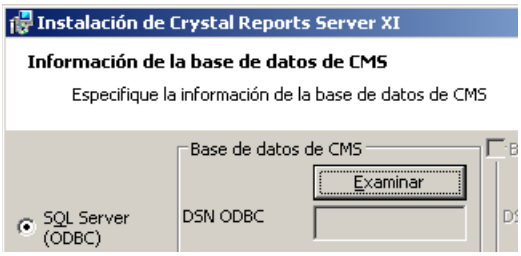


1 Instale novo BusinessObjects Enterprise System com o MSDE de instalação ou use o Servidor SQL local existente.



Observação: O Crystal server e o Microsoft SQL Server devem residir na mesma máquina.

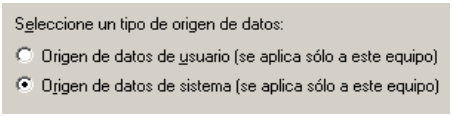
2 No Painel de Banco de Dados CMS, clique em Pesquisar.



3 Clique na guia Machine Data Source (Fonte de Dados da Máquina).

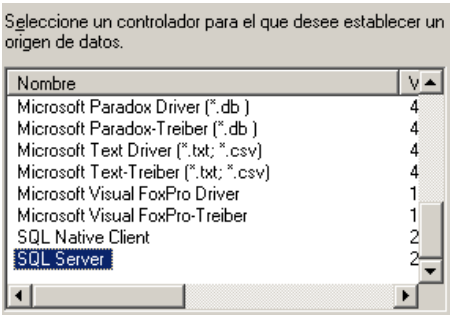
4 Clique em Novo.

Selecione Origem de Dados do Sistema.

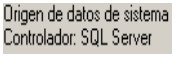


Clique em Avançar.

Role para baixo, selecione Servidor SQL e clique em Avançar.



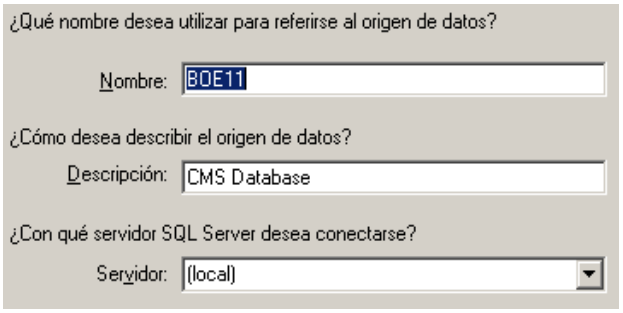
Será exibida uma nova fonte. Clique em Concluir.



5 Na janela Nova Fonte de Dados para Servidor SQL, digite:

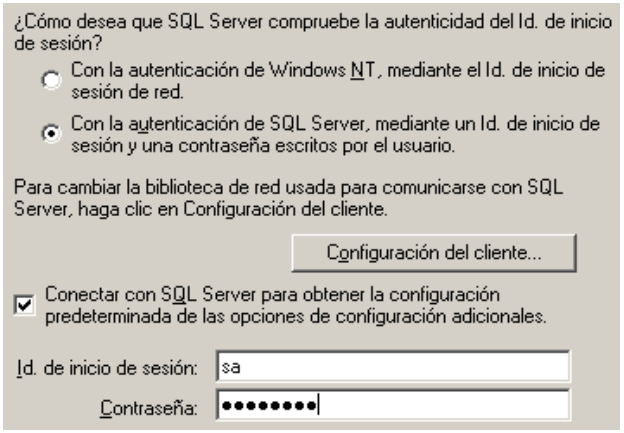
- Nome de sua fonte de dados (por ex.: i.e. BOE_XI)

- A descrição (opcional)
- Para o servidor, clique na seta para baixo e selecione (local)

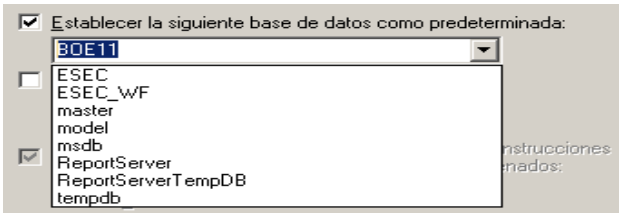


Clique em Avançar.

6 Se não tiver feito isso ainda, selecione Com SQL Server, digite sa como o nome de usuário e digite a senha de sa. Clique em Avançar.



Marque a caixa ‘Change the default database to:’ (mudar o banco de dados padrão para). Altere o banco de dados padrão para BOE11. Clique em Avançar.



7 Na janela ‘Create a New Data Source to SQL Server’ (criar nova Fonte de Dados para Servidor SQL), clique em Concluir.

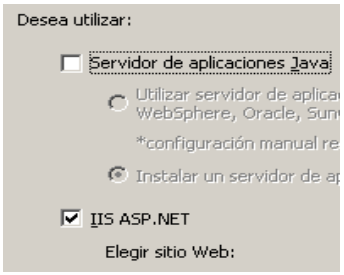
8 Clique em Testar Fonte de Dados e teste a fonte de dados. Quando o teste da fonte de dados for concluído, clique em OK.

Na janela Select Data Source (selecionar fonte de dados), realce BOE11 e continue a clicar em OK até que seja exibido ‘SQL Server Login’ (login do servidor SQL). Verifique se Use Trusted

Connection (usar conexão confiável) NÃO está selecionado. Clique em OK. Clique em Avançar.

9 Na janela Web Component Adapter Type (Tipo de Adaptador de Componente Web), selecione IIS ASP.NET.

Observação: Se você não tiver instalado o IIS e o ASP.NET usando o Painel de Controle > Adicionar Remover Programas > Adicionar ou remover Componentes do Windows, o IIS ASP.NET ficará esmaecido.



Configurando o Open Database Connectivity (ODBC) para Autenticação SQL

Este procedimento configura uma fonte de dados ODBC entre o Crystal Reports no Windows e o Servidor SQL. Isso precisa ser realizado na máquina do Crystal Server.

Para Configurar uma fonte de dados ODBC para Windows:

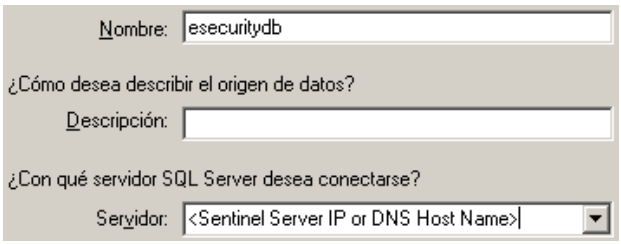
1 Vá para o Painel de Controle do Windows > Ferramentas Administrativas > Fontes de Dados (ODBC).

2 Clique na guia DSN de Sistema e clique no botão Adicionar.

3 Selecione Servidor SQL. Clique em Concluir.

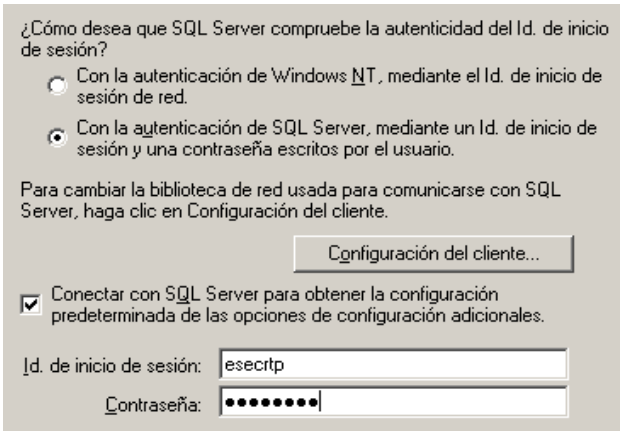
4 Será exibida uma tela solicitando as informações de configuração do driver:

- Em Nome da Fonte de Dados, digite esecuritydb
- No campo Descrição (opcional), digite uma descrição
- No campo Servidor, digite o nome do host ou o endereço IP do Sentinel Server



Clique em Avançar.

5 Na tela seguinte, selecione Autenticação SQL. Digite esecrpt como a ID de login e a senha. Clique em Avançar.



6 Na próxima tela, selecione:

- Mude o banco de dados do Sentinel (o nome padrão é ESEC)
- Deixe todas as configurações padrão

Clique em Avançar.

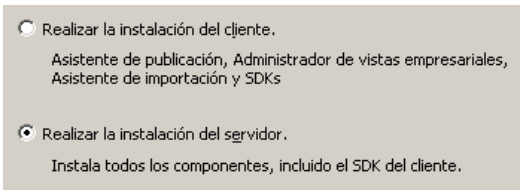
7 Clique em Concluir.

8 Clique em Testar Fonte de Dados e teste a fonte de dados. Quando o teste da fonte de dados for concluído, clique em OK. Clique em OK até sair.

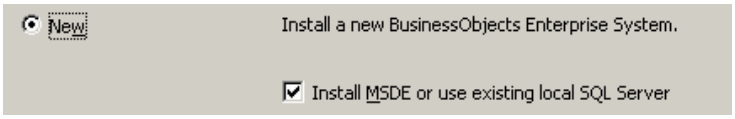
9.7.3 Instalando o Crystal Server para Oracle

Para Instalar o Crystal Reports Server XI para Oracle:

- Execute a instalação do servidor



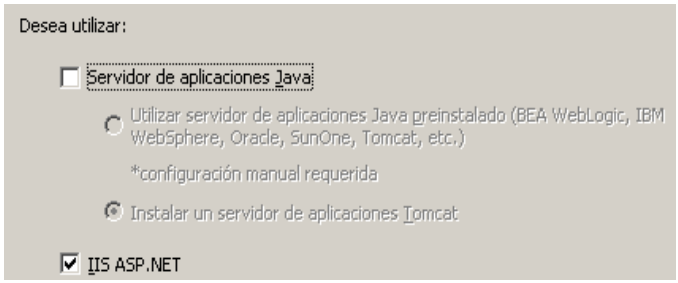
- Instalar um novo BusinessObjects Enterprise System com Install MSDE or use existing local SQL Server (Instalar MSDE ou usar Servidor SQL local existente).



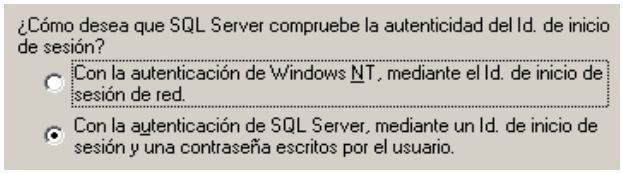
Observação: O Crystal Server e o Microsoft SQL Server 2005 devem residir na mesma máquina.

- IIS ASP.NET.

Observação: Se você não tiver instalado o IIS e o ASP.NET usando o Painel de Controle > Adicionar Remover Programas > Adicionar ou remover componentes do Windows, o IIS ASP.NET ficará esmaecido.



- Você será solicitado a especificar o Modo de Autenticação. Selecione Autenticação do Servidor SQL.



O Crystal Reports tem suporte para acesso direito a bancos de dados do Oracle 9. Esse tipo de acesso é fornecido pelo arquivo de tradução crdb_oracle.dll. Esse arquivo se comunica com o driver do banco de dados do Oracle 9, que funciona diretamente com bancos de dados do Oracle e clientes, recuperando os dados de que você precisa no relatório.

Observação: Para que o Crystal Reports use bancos de dados do Oracle 9, o software do cliente do Oracle deve ser instalado no sistema, e o local do cliente do Oracle deve estar na variável de ambiente PATH.

Instalando e configurando o software cliente do Oracle 9i

Ao instalar o cliente do Oracle 9i:

- Aceite o local de instalação padrão
- Não – para Perform Typical Configuration (Realizar Configuração Típica)
- Não – para Serviço de Diretório
- Selecione Local
- Nome do Serviço TNS: ESEC

- Usuário (opcional): esecrpt

Após a instalação, crie uma configuração de nome de serviço de rede local.

Para criar a configuração do Nome do Serviço da Net (Configurando driver nativo do Oracle):

1. Selecione Oracle-Orahome92>Configuration and Migration Tools (Ferramentas de Configuração e Migração)>Net Manager.
2. No painel de navegação, expanda Local e realce Service Naming (Nome de Serviço).
3. Clique no sinal de mais à esquerda para adicionar um nome de serviço.
4. Na janela Service Name (Nome de Serviço), digite um nome de serviço de rede.
   - Digite ESECURITYDB

   Clique em Avançar.
5. Na janela Select Protocols (Selecionar Protocolos), selecione o padrão:
   - TCP/IP (Protocolo da Internet)

   Clique em Avançar.
6. Para o nome do host e o número da porta:
   - Digite o nome do host ou o endereço IP da máquina em que reside o banco de dados
   - Selecione a Porta Oracle (padrão 1521 durante a instalação)

   Clique em Avançar.
7. Para identificar o banco de dados ou o serviço:
   - Selecione (Oracle8i ou posterior), digite o nome do serviço (este é o nome da instância do Oracle).
   - Para o tipo de conexão, selecione Database Default (Banco de Dados Padrão).

   Clique em Avançar.
8. Na janela de teste, clique em Testar... Clique em Avançar. O teste pode falhar porque ele usa um ID de banco de dados e uma senha.
9. Se o teste falhar, execute este procedimento:
   - Na janela Connecting (Conectando), clique em Change Login (Mudar Login).
   - Digite o ID do Oracle do Sentinel (use esecrpt) e a senha. Clique em OK.

   Se o teste falhar:
   - Use o comando ping no Sentinel Server
   - Verifique se o nome do host do Sentinel Server está no arquivo de hosts no Crystal Reports Server. Esse arquivo se encontra em %SystemRoot%\system32\drivers\etc\.
10. Clique em Concluir.

9.8 Configuração para todas as autenticações e configurações

9.8.1 Mapeando o Crystal Reports para uso com o Sentinel

Os procedimentos a seguir são necessários para que o Crystal Server funcione com o Sentinel Control Center.

Configurando inetmgr

Para configurar inetmgr:

1. Copie o arquivo web.config de:

   `C:\Program Files\Business Objects\BusinessObjects Enterprise 11.5\Web Content`

   para c:\Inetpub\wwwroot.
2. Inicie o Internet Service manager clicando em Iniciar>Executar. Digite inetmgr e clique em OK.
3. Expanda (computador local)>Web Sites>Default Web Site>businessobjects.
4. Em businessobjects, clique o botão direito do mouse>propriedades.
5. Na guia Virtual Directory (Diretório Virtual), clique em Configuration... (Configuração).
6. Você deve ter os mapeamentos a seguir. Caso não os tenha, adicione-os. Se você for adicionar um mapeamento, não clique nos nós businessobjects ou crystalreportsviewer11.

Extensão	Executável
.csp	C:\Windows\Microsoft.NET\Framework\v1.1.4322\aspnet_isapi.dll
.cwr	C:\Windows\Microsoft.NET\Framework\v1.1.4322\aspnet_isapi.dll
.cri	C:\Windows\Microsoft.NET\Framework\v1.1.4322\aspnet_isapi.dll
.wis	C:\Arquivos de Programas\Business Objects\BusinessObjects Enterprise 11\win32_x86\cdzISAPI.dll

   Clique em OK para fechar a janela.
7. Reinicie o IIS, expanda (computador local)>Web Sites>Default Web Site, realce default Web Site (Web site padrão), clique o botão direito >Iniciar.

Aplicando patch do Crystal Reports para uso com o Sentinel

Para que os Crystal Reports sejam vistos na guia Análise do Sentinel Control Center, vários arquivos do Crystal Enterprise precisam ser atualizados para ficarem compatíveis com o browser embutido no Sentinel.

A tabela a seguir mostra esses arquivos e descreve para que cada um deles é usado. Esses arquivos podem ser encontrados na Distribuição do Sentinel Reports cujo download pode ser feito do Suporte Técnico da Novell.

Nome do arquivo	Descrição
calendar.js calendar.html	Exibe um calendário popup quando você seleciona uma data como parâmetro para um relatório.
grouptree.html	Exibe a mensagem Carregando... enquanto os relatórios são carregados.
exportframe.html	Exibe a janela em que você pode exportar um relatório para gravação ou impressão.
exportIce.html	Arquivo usado pelo Sentinel na exportação de um relatório para gravação ou impressão.
GetInfoStore.asp	Arquivo usado para consultar o Crystal Server
GetReports.asp	Arquivo usado pelo Sentinel Control Center para estabelecer uma conexão com o Crystal Server e exibir a lista de relatórios.
GetReportURL.asp	Arquivo usado para dar suporte a hiperlinks entre relatórios.
helper_js.asp	Um arquivo de chamadas usado por GetInfoStore.asp.

Para aplicar patches do Crystal Reports:

1. Obtenha o Distribuição do Sentinel Reports do Suporte Técnico da Novell.

   Observação: É altamente aconselhável que as Notas de Versão do Sentinel Reports sejam lidas antes de realizar essa tarefa. Pode haver arquivos atualizados, scripts e etapas adicionais.

2. Da Distribuição do Sentinel Reports, vá para o diretório do "patch" e copie todos os arquivos *.html e *.js para o local do arquivo do viewer, o padrão é:

   ```
   C:\Program Files\Business Objects\BusinessObjects Enterprise 11.5\Web Content\Enterprise115\viewer\en
   ```

3. Da Distribuição do Sentinel Reports, vá para o diretório do "patch" e copie todos os arquivos *.asp e *.js para:

   ```
   C:\inetpub\wwwroot
   ```

   Observação: A pasta da Web pode estar em uma unidade ou um local diferente da especificação acima.

Gabaritos do Crystal Report

Gabaritos do Crystal Report são publicados no Crystal Reports Server com o Crystal Publishing Wizard. É possível fazer o download do conjunto de gabaritos de relatórios mais recentes no site de Suporte Técnico da Novell.

Publicando gabaritos de relatório usando o Crystal Publishing Wizard

Observação: É altamente aconselhável que as Notas de Versão do Sentinel Reports sejam lidas antes de realizar essa tarefa. Pode haver arquivos atualizados, scripts e etapas adicionais.

Publicando gabaritos de Crystal Reports

Observação: Se você quiser publicar os gabaritos de relatórios novamente, exclua os gabaritos importados anteriormente.

1. Clique em Iniciar>Todos Os Programas>Businessobjects>Crystal Reports Server>Publishing Wizard.
2. Clique em Avançar.
3. Login. Sistema deve ser o nome do seu computador host e Autenticação deve ser Enterprise. O nome do usuário pode ser Administrador. Por questão de segurança, recomenda-se enfaticamente criar um novo usuário diferente de Administrador. Digite sua senha e clique em Avançar.

   Observação: Relatórios publicados no usuário Administrador podem ser acessados por todos os usuários.

4. Clique em Adicionar Pasta.
5. Selecione Incluir Subpasta. Da Distribuição do Sentinel Reports, navegue para:

   No Banco de dados do Sentinel executados no Microsoft SQL:
   `Crystal_v11\SQL-Server`

   No Banco de dados do Sentinel executados no Oracle:
   `Crystal_v11\Oracle`

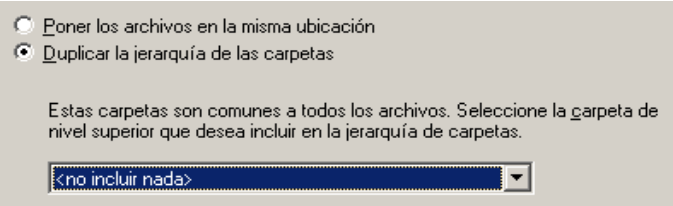
   Clique em OK.
6. Clique em Avançar.

   Na janela Especificar Localização, clique em Nova Pasta (canto superior direito) e crie uma pasta chamada SentinelReports. Clique em Avançar.

7 Selecionar:

- Duplicar hierarquia de pasta;

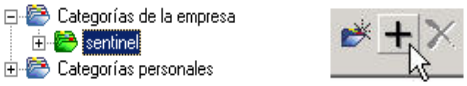
Clique na seta para baixo e selecione <incluir nenhum>



Clique em Avançar.

8 Na janela Confirm Location (Confirmar Local), clique em Avançar.

Na janela Especificar Categorias, digite o nome de categoria escolhido (como sentinel), realce o nome e clique no botão +



Observação: Somente o primeiro relatório será exibido na categoria depois que você clicar em Avançar.

clique em Próximo.

9 Na janela Especificar Atualização do Repositório, clique em Habilitar Tudo para habilitar a atualização do repositório. Clique em Avançar.

10 Na janela Specify Keep Saved Data (Especificar Manutenção dos Dados Gravados), clique em Ativar Tudo para manter os dados gravados quando publicar relatórios. Clique em Avançar.

11 Na janela Mudar Valores Padrão, clique em Publicar relatórios sem modificar propriedades (essa deve ser a opção padrão). Clique em Avançar.

12 Clique em Avançar para adicionar seus objetos.

13 Clique em Avançar.

14 Uma lista publicada será exibida; clique em Concluir.

Quando os gabaritos do Sentinel para Crystal Reports são publicados no Crystal Enterprise server, os gabaritos devem residir no diretório SentinelReports.

9.8.2 Definindo uma Conta de Usuário Nomeado

A chave de licença fornecida com o Crystal Server É uma chave de conta do Usuário Nomeado. A conta Guest foi mudada de Usuário Simultâneo para Usuário Nomeado.

Para definir a Conta Guest como Usuário Nomeado:

1 Clique em Iniciar>Todos Os Programas>Businessobjects>Crystal Reports Server>.Net Administration Launchpad.

2 Clique em Central Management Console.

3. O nome do sistema deve ser o nome do computador do host. O tipo de autenticação deve ser Enterprise. Caso contrário, escolha Enterprise.
4. Clique em Log On (Fazer conexão).
5. No painel Organizar, clique em Usuários.
6. Clique em Guest.
7. Mude o tipo de conexão de Usuário Simultâneo para Usuário Nomeado.
8. Clique em Atualizar.
9. Faça logoff e feche a janela ou vá para a seção Configurando o .NET Administration Launchpad.

9.8.3 Configurando Permissões de Relatórios

Esse procedimento discute como usar o Launchpad de Administração do .NET para configurar as permissões sobre relatórios que permitam ver e modificar relatórios sobre demanda.

Para configurar permissões de relatórios:

1. Se ainda não tiver feito isso, inicie o .Net Administration Launchpad (Clique em Iniciar>Todos os Programas>Businessobjects>Crystal Reports Server>.NET Administration Launchpad).
2. Clique em Central Management Console.

   O nome do sistema deve ser o nome do computador do host. O tipo de autenticação deve ser Enterprise. Caso contrário, escolha Enterprise.
3. Digite o nome do usuário e a senha e clique em Log On.
4. No painel Organizar, clique em Pastas.
5. Clique em SentinelReports.
6. Selecionar Tudo.
7. Clique na guia Direitos.
8. Para Everyone (Todos), no menu suspenso à direita de Access Level (Nível de Acesso), selecione View on Demand (Ver por Demanda).
9. Clique em Atualizar.
10. Efetue logoff e feche a janela.

Testando a conexão do servidor Web com o banco de dados

Para testar a conexão do servidor Web para o banco de dados:

1. Se ainda não tiver feito isso, inicie o .net Administration Launchpad (Iniciar>Todos os Programas>Businessobjects>Crystal Reports Server>.NET Administration Launchpad).
2. Clique em Central Management Console.
3. Digite Administrator como o nome do usuário. Digite a senha (por padrão, este campo estará vazio). Clique em Log On (Fazer conexão).
4. Navegue para Folder>SentinelReports>Internal Events.
5. Selecione Column Display Details (Detalhes de Exibição de Coluna).
6. Clique em Visualizar.

7 Dependendo do sistema, faça login como esecrpt ou como o usuário do Relatório do Sentinel.

8 No menu suspenso do campo de classificação, selecione Tag.

9 Clique em OK. Um relatório deve ser exibido.

Testando a conectividade com o servidor Web

Para testar a conectividade com o servidor Web:

1 Vá para outra máquina na mesma rede que o servidor Web.

2 Digite

```
http://<DNS name or IP address of your web server>/businessobjects/
enterprise11/WebTools/adminlaunch/default.aspx
```

Você deve obter uma página Web do Crystal BusinessObjects.

9.8.4 Desabilitando os 10 Principais Relatórios do Sentinel

Por padrão, os 10 Principais Relatórios do Sentinel são habilitados. Para desabilitar os 10 Principais Relatórios do Sentinel, é necessário:

- Desativar Agregação
- Desabilitar EventFileRedirectService

Para Desativar Agregação:

1 Inicie o Gerenciador de Dados do Sentinel.

2 Login.

3 Clique na guia Relatando Dados.

4 Desabilite os seguintes resumos

- EventDestSummary
- EventSevSummary
- EventSrcSummary

Clique em Ativo na coluna status até que mude para Inativo.

Nombre del res...	Hora	Atributos	Origen	Estado
EventDestSum...	1 hora	CUST_ID.RS ...	TransformedEv...	Activo
EventSevDestT...	1 hora	CUST_ID.DE ...	TransformedEv...	Inactivo
EventSevDestE...	1 hora	CUST_ID.DE ...	TransformedEv...	Inactivo
EventSevDestP...	1 hora	SEV.DEST_F ...	TransformedEv...	Inactivo
EventSevSumm...	1 hora	CUST_ID.SE ...	TransformedEv...	Activo
EventSrcSumm...	1 hora	CUST_ID.RS ...	TransformedEv...	Activo

Para desabilitar EventFileRedirectService:

1 Na máquina DAS, usando o editor de texto, abra:

Para UNIX:

```
$ESEC_HOME/config/das_binary.xml
```

Para Windows:

```
%ESEC_HOME%\config\das_binary.xml
```

2. Para o EventFileRedirectService, mude o status para off (desativado).
```
<property name="status">off</property>
```
3. Reinicie o componente DAS, executando este procedimento:

   No Windows:
```
Use Service Manager to stop then start the "sentinel" service.
```

9.8.5 Aumentando o limite de atualização de registro do relatório do Crystal Enterprise Server

Dependendo do número de eventos que o Crystal estiver consultando, você poderá receber um erro sobre o tempo máximo de processamento ou o limite máximo de registros. Para definir o servidor para processar um número maior ou ilimitado de registros, será necessário reconfigurar o Crystal Page Server. Isso pode ser feito usando ou o Gerenciador de Configuração Central ou a página da Web do Crystal.

Para reconfigurar o Crystal Page Server por meio do Central Configuration Manager:

1. Clique em Iniciar>Todos Os Programas>Businessobjects>Crystal Reports Server>Central Configuration Manager (Gerenciador de Configuração Central).
2. Clique o botão direito em Crystal Reports Page Server e selecione Parar.
3. Clique o botão direito em Crystal Reports Page Server e selecione Propriedades.
4. No campo Comando, sob a guia Propriedades, ao final da linha de comando, adicione:
```
maxDBResultRecords <value greater than 20000 or 0 to disable the
default limit>
```
5. Reinicie o Crystal Page Server.

Para reconfigurar o Crystal Page Server por meio da página da Web do Crystal:

1. Clique em Iniciar>Todos Os Programas>Businessobjects>Crystal Reports Server>.Net Administration Launchpad.
2. Clique em Central Management Console.
3. O nome do sistema deve ser o nome do computador do host. O tipo de autenticação deve ser Enterprise. Caso contrário, escolha Enterprise.
4. Digite o nome do usuário e a senha e clique em Log On.
5. Clique em Servidores.
6. Clique em <nome do servidor>.pageserver.
7. Em Database Records to Read When Previewing or Refreshing a report, (Registros do Banco de Dados para Ler ao Visualizar ou Atualizar um Relatório), selecione Unlimited records (Registros ilimitados).
8. Clique em Aplicar.
9. Será exibido um prompt para reiniciar o servidor de página; clique em OK.
10. Talvez seja preciso fornecer um nome de logon e uma senha para acessar o gerenciador do serviço do sistema operacional.

9.8.6 Configurando o Sentinel Control Center para integração com o Crystal Enterprise Server

O Sentinel Control Center pode ser configurado para se integrar ao Crystal Enterprise Server, permitindo que você veja Relatórios do Crystal a partir do Sentinel Control Center.

Para habilitar a integração do Sentinel Control Center com Crystal Enterprise Server, siga as instruções abaixo.

Observação: Essa configuração deve ser executada somente depois que o Crystal Enterprise Server tiver sido instalado e Relatórios Crystal tiverem sido publicados nele.

Para configurar o Sentinel para se integrar ao Crystal Enterprise Server:

1. Efetue login no Centro de Controle do Sentinel como um usuário com privilégios para a guia Admin;
2. Na guia Admin, selecione Configuração de Relatórios.
3. No campo URL de Análise, digite o seguinte:

   ```
   http://<hostname_or_IP_of_web_server>/
   GetReports.asp?APS=<hostname>&user=Guest&password=&tab=Analysis
   ```

   Observação: <nome_do_host_ou_IP_do_servidor_da_Web> deve ser substituído pelo endereço IP ou nome de host do Crystal Enterprise Server.

   Observação: O URL acima não funcionará corretamente se o APS estiver definido como o endereço IP. Ele deve ser o nome do host do Crystal Server.
4. Clique em Atualizar ao lado do campo URL de Análise.
5. Se o Advisor estiver instalado, digite o seguinte no campo URL de Análise:

   ```
   http://<hostname_or_IP_of_web_server>/
   GetReports.asp?APS=<hostname>&user=Guest&password=&tab=Advisor
   ```

   Observação: <nome_do_host_ou_IP_do_servidor_da_Web> deve ser substituído pelo endereço IP ou nome de host do Crystal Enterprise Server.

   Observação: O URL acima não funcionará corretamente se o APS estiver definido como o endereço IP. Ele deve ser o nome do host do Crystal Server.
6. Clique em Atualizar ao lado do campo URL de Consultor.
7. Clique em Gravar.
8. Efetue logout e login novamente no Sentinel Control Center. As árvores do Crystal Report nas guias Análise e Consultor (se o Advisor estiver instalado) devem agora aparecer na janela Navegador.

Crystal Reports para Linux

10

Tópicos incluídos neste capítulo:

- Seção 10.1, “Usando Crystal Reports” na página 134
- Seção 10.3.2, “Instalando o Crystal BusinessObjects EnterpriseTM XI” na página 136
- Seção 10.4, “Publicando gabaritos de Crystal Reports” na página 138
- Seção 10.5, “Usando o servidor Web Crystal XI” na página 142
- Seção 10.6, “Definindo uma conta de ‘Usuário Nomeado’” na página 142
- Seção 10.8, “Habilitando os relatórios 10 Primeiros do Sentinel” na página 143
- Seção 10.10, “Configurando o Sentinel Control Center para integração com o Crystal Enterprise Server.” na página 145
- Seção 10.11, “Utilitários e solução de problemas” na página 146

O Crystal Business Objects Enterprise™ XI é uma das ferramentas de relatórios com o Sentinel.

Este capítulo aborda a instalação e configuração do Crystal Reports Server para Sentinel.

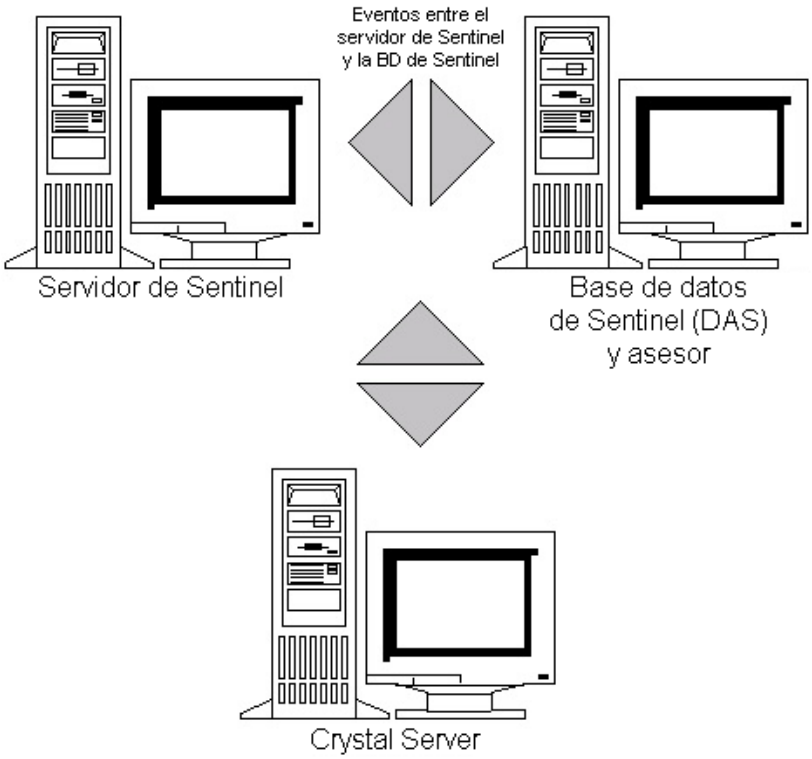
O Sentinel suporta a execução do Crystal Reports Server nas plataformas a seguir:

- Windows - suportado para execução do Banco de Dados do Sentinel no Windows, Linux ou Solaris.
- Linux - suportado para execução do Banco de Dados do Sentinel no Linux ou Solaris.

Este capítulo aborda a execução do Crystal Reports Server no Linux. Para obter mais informações sobre a execução do Crystal Reports Server no Windows, consulte Capítulo 9, “Crystal Reports para Windows” na página 107 no Guia de Instalação.

Observação: A instalação deve ser feita na ordem apresentada abaixo.

- Pré-instalação e instalação do Crystal BusinessObjects Enterprise™ XI
- Aplicação do patch do Crystal Reports;
- Publicação (importação) de Crystal Reports;
- Configurando uma conta ‘Usuário Nomeado’
- Testando a conectividade com o servidor Web
- Habilitando os relatórios dos Dez Melhores (opcional)
- Aumentando o limite de atualização de registro do relatório do Crystal Enterprise Server (recomendado)
- Configurando o Sentinel Control Center para integração com o Crystal Enterprise Server



10.1 Usando Crystal Reports

Para obter informações sobre como usar Crystal Reports para Relatórios do Sentinel, consulte Capítulo 9, “Crystal Reports para Windows” na página 107 no Guia de Instalação.

10.2 Configuração

- As versões do Linux:
  - SUSE Linux Enterprise Server 9 (SLES 9) com SP2
  - Atualização 5 ES do Red Hat Enterprise Linux 3 (x86)
- BusinessObjects Enterprise XI Server instalado;
- Para Oracle - Oracle 9i Client Release 2 (9.2.0.1.0).

10.3 Instalação

10.3.1 Pré-instalação do Crystal BusinessObjects Enterprise™ XI

Para pré-instalar o Crystal BusinessObjects Enterprise:

1. Se o banco de dados do Sentinel não estiver na mesma máquina que o Crystal Server, você deverá instalar o software Oracle Client na máquina do Crystal Server. Esta etapa adicional não será necessária se o banco de dados do Sentinel estiver na mesma máquina do Crystal Server, pois nesse caso o software Oracle necessário já está instalado com o software do banco de dados Oracle exigido pelo banco de dados do Sentinel.
2. Efetue login na máquina do Crystal Server como usuário Root.
3. Crie o grupo bobje:
   ```
   groupadd bobje
   ```
4. Crie um usuário do Crystal (o diretório pessoal deste exemplo é o /export/home/crystal, você pode mudá-lo se necessário; a parte /export/home do caminho já deve existir).
   ```
   useradd –g bobje –s /bin/bash –d /export/home/crystal –m crystal
   ```
5. Crie um diretório para o software de relatórios Crystal:
   ```
   mkdir –p /opt/crystal_xi
   ```
6. Mude a propriedade do diretório do software de Crystal (recursivamente) para crystal/bobje:
   ```
   chown -R crystal:bobje /opt/crystal_xi
   ```
7. Mude para o usuário do Crystal:
   ```
   su - crystal
   ```
8. A variável de ambiente ORACLE_HOME deve ser definida no ambiente do usuário do Crystal. Para fazer isso, modifique o script de login do usuário do Crystal para definir a variável de ambiente ORACLE_HOME para a base do software Oracle. Por exemplo, se o shell do usuário do Crystal for um bash e o software Oracle estiver instalado no diretório /opt/oracle/product/9.2, abra o arquivo ~crystal/.bash_profile e adicione a seguinte linha ao final do arquivo:
   ```
   export ORACLE_HOME=/opt/oracle/product/9.2
   ```
9. A variável de ambiente LD_LIBRARY_PATH no ambiente do usuário do Crystal deve conter o caminho para as bibliotecas do software Oracle. A variável de ambiente LD_LIBRARY_PATH no ambiente do usuário do Crystal deve conter o caminho para as bibliotecas do software Oracle. Por exemplo, se o shell do usuário do Crystal for um bash, abra o arquivo ~crystal/.bash_profile e adicione a seguinte linha ao final do arquivo (abaixo da variável de ambiente ORACLE_HOME definida):
   ```
   export LD_LIBRARY_PATH=$ORACLE_HOME/lib:$LD_LIBRARY_PATH
   ```
10. Deve ser adicionada uma entrada ao arquivo tnsnames.ora do Oracle com o Nome do serviço esecuritydb, que aponta para o Banco de dados do Sentinel. Para fazer isso na máquina do Crystal Server:
    - **10a** Efetue login como usuário do Oracle;
    - **10b** Mude os diretórios para $ORACLE_HOME/network/admin;
    - **10c** Faça backup do arquivo tnsnames.ora;
    - **10d** Abra o arquivo tnsnames.ora para edição;
    - **10e** Se o banco de dados do Sentinel estiver na máquina do Crystal Server, já deve haver uma entrada no arquivo tnsnames.ora para o banco de dados do Sentinel. Por exemplo, se o banco de dados do Sentinel se chamar ESEC, existirá uma entrada semelhante a esta:

```
ESEC =
(DESCRIPTION =
 (ADDRESS_LIST =
  (ADDRESS = (PROTOCOL = TCP)(HOST = dev-linux02)(PORT = 1521))
  )
  (CONNECT_DATA =
  (SID = ESEC)
  )
)
```

10f Se o banco de dados do Sentinel não estiver na máquina do Crystal Server, abra o arquivo arquivo tnsnames.ora na máquina do banco de dados do Sentinel para localizar a entrada descrita anteriormente.

10g Faça uma cópia de toda a entrada e cole-a no final do arquivo tnsnames.ora da máquina do Crystal Server. A parte da entrada do Nome do Serviço deve ser renomeada como esecuritydb. Por exemplo, quando a entrada anterior é copiada e renomeada corretamente, fica da seguinte forma:

```
esecuritydb =
(DESCRIPTION =
 (ADDRESS_LIST =
  (ADDRESS = (PROTOCOL = TCP)(HOST = dev-linux02)(PORT = 1521))
  )
  (CONNECT_DATA =
  (SID = ESEC)
  )
)
```

10h Verifique se a parte da entrada HOST está correta (por exemplo, verifique se não está definida como localhost (host local) se o Crystal Server e o banco de dados do Sentinel estiverem em máquinas diferentes).

10i Grave as mudanças feitas no arquivo tnsnames.ora.

10j Execute o seguinte comando para verificar se o Nome do Serviço esecuritydb está configurado corretamente:

```
tnsping esecuritydb
```

10k Se o comando for executado corretamente, você receberá uma mensagem que informa que a conexão está OK.

10.3.2 Instalando o Crystal BusinessObjects Enterprise™ XI

Para instalar o Crystal BusinessObjects Enterprise:

1. Efetue login como usuário do Crystal.
2. Mude os diretórios no DISK_1 do instalador do Crystal.
3. Executar:
   ```
   ./install
   ```
4. Selecione o idioma: Inglês
5. Selecione Nova Instalação.
6. Aceite o Contrato de Licença.
7. Digite o Código do Produto.

8 Digite o diretório de instalação:
`/opt/crystal_xi`

9 Selecione: Instalação do usuário

10 Selecione: Nova Instalação

11 Selecione: Instalar MySQL

12 Digite informações de configuração do MySQL:

12a Use a porta padrão 3306

12b Senha do administrador

13 Digite mais informações de configuração do MySQL:

13a Nome de BD padrão: BOE11

13b Id do usuário: mysqladm

13c Senha

14 Digite mais informações de configuração do MySQL:

14a Servidor de Nome Local: <nome de host da máquina local>

14b Número da Porta CMS padrão: 6400

15 Selecione: Instalar Tomcat

16 Digite informações de configuração do Tomcat:

16a Porta padrão de solicitações http de recebimento: 8080

16b Porta padrão de solicitações jsp de redirecionamento: 8443

16c Porta padrão Hook de encerramento: 8005

17 Pressione Enter para iniciar a instalação.

10.3.3 Aplicando patch do Crystal Reports para uso com o Sentinel

Para que os Crystal Reports sejam vistos na guia Análise do Sentinel Control Center, vários arquivos do Crystal Enterprise precisam ser atualizados para ficarem compatíveis com o browser embutido no Sentinel.

A tabela a seguir mostra esses arquivos e descreve para que cada um deles é usado. Esses arquivos podem ser encontrados na Distribuição do Sentinel Reports cujo download pode ser feito do Suporte Técnico da Novell.

Nome do arquivo	Descrição
calendar.js calendar.html	Exibe um calendário popup quando você seleciona uma data como parâmetro para um relatório.
grouptree.html	Exibe a mensagem Carregando... enquanto os relatórios são carregados.
exportframe.html	Exibe a janela em que você pode exportar um relatório para gravação ou impressão.
exportIce.html	Arquivo usado pelo Sentinel na exportação de um relatório para gravação ou impressão.
GetReports.jsp	Arquivo usado pelo Sentinel Control Center para estabelecer uma conexão com o Crystal Server e exibir a lista de relatórios.
GetReportURL.jsp	Arquivo usado para dar suporte a hiperlinks entre relatórios.

Para aplicar patches do Crystal Reports:

1. Obtenha a Distribuição do Sentinel Reports do Suporte Técnico da Novell.

   Observação: É altamente aconselhável que as Notas de Versão do Sentinel Reports sejam lidas antes de realizar essa tarefa. Pode haver arquivos atualizados, scripts e etapas adicionais.

2. Da distribuição do Sentinel Reports, vá para o diretório do patch e copie todos os arquivos *.html e *.js para o local do arquivo do viewer, o padrão é:
   `/opt/crystal_xi/bobje/webcontent/enterprise11/viewer/en/`
3. Da distribuição do Sentinel Reports, vá para o diretório do "patch" e copie todos os arquivos *.jsp para:
   `/opt/crystal_xi/bobje/tomcat/webapps/esec-script/`

   Observação: Crie uma pasta chamada esec-script

4. Copie todos os arquivos *.jar:
   ```
   From:
   /opt/crystal_xi/bobje/tomcat/webapps/jsfadmin/WEB-INF/lib/
   To:
   /opt/crystal_xi/bobje/tomcat/webapps/esec-script/WEB-INF/lib
   ```

   Observação: Crie a estrutura de pastas WEB-INF/lib

10.4 Publicando gabaritos de Crystal Reports

Observação: É altamente aconselhável que as Notas de Versão do Sentinel Reports sejam lidas antes de realizar essa tarefa. Pode haver arquivos atualizados, scripts e etapas adicionais.

Estes gabaritos de relatório são criados pela Novell para uso nas guias Análise e Consultor do Sentinel Control Center.

Existem dois métodos de publicação de relatórios:

- Assistente de Publicação de Crystal Reports;
- Console de Gerenciamento Central do Crystal Reports.

Observação: Para a execução dos 10 relatórios principais, a agregação deve estar habilitada e EventFileRedirectService no das_binary.xml deve estar ativado. Para obter informações sobre como habilitar a agregação, consulte a seção Guia de Dados de Relatórios do Gerenciador de Dados do Sentinel no Guia do Usuário do Sentinel ou consulte a seção Seção 10.8, "Habilitando os relatórios 10 Primeiros do Sentinel" na página 143.

10.4.1 Publicando gabaritos de relatórios – Assistente de Publicação de Crystal Reports

Observação: Uma plataforma Windows é obrigatória para a execução do Assistente de Publicação de Relatórios Crystal.

Para importar gabaritos do Crystal Reports:

Observação: Se você importar (publicar) seus Gabaritos de Relatórios outra vez, apague a importação anterior dos Gabaritos de Relatórios.

1. Clique em Iniciar>Todos os Programas>BusinessObjects 11> Crystal Reports Server>Assistente de Publicação.
2. Clique em Avançar.
3. Login. Sistema deve ser o nome do seu computador host e Autenticação deve ser Enterprise. O nome do usuário pode ser Administrador. Por segurança, você deve usar um usuário que não seja o Administrador. Digite sua senha e clique em Avançar.

   Observação: Relatórios publicados no usuário Administrador podem ser acessados por todos os usuários.

4. Clique em Adicionar Pasta.
5. Clique em Incluir Subpasta. Da Distribuição do Sentinel Reports, navegue para:

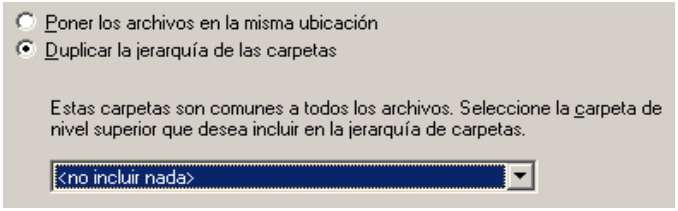
   `Crystal_v11\Oracle`

   Clique em OK.
6. Clique em Avançar.

7 Na janela Especificar Localização, clique em Nova Pasta (canto superior direito) e crie uma pasta chamada eSecurity_Reports. Clique em Avançar.

8 Selecionar:

- Duplicar hierarquia de pasta;
- Clique na seta para baixo e selecione <incluir nenhum>

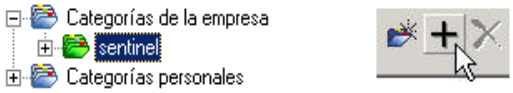


Clique em Avançar.

9 Na janela Confirm Location (Confirmar Local), clique em Avançar.

10 Na janela Especificar Categorias:

- selecione um nome de categoria (como sentinel);
- realce o nome e clique no botão +;



Observação: Somente o primeiro relatório será exibido na categoria depois que você clicar em Avançar.

- Clique em Avançar.

11 Na janela Especificar Programação, clique em Permitir que usuários atualizem o objeto (essa deve ser a opção padrão). Clique em Avançar.

12 Na janela Especificar Atualização do Repositório, clique em Habilitar Tudo para habilitar a atualização do repositório. Clique em Avançar.

13 Na janela Specify Keep Saved Data (Especificar Manutenção dos Dados Gravados), clique em Ativar Tudo para manter os dados gravados quando publicar relatórios. Clique em Avançar.

14 Na janela Mudar Valores Padrão, clique em Publicar relatórios sem modificar propriedades (essa deve ser a opção padrão). Clique em Avançar.

15 Clique em Avançar para adicionar seus objetos.

16 Clique em Avançar.

17 Clique em Concluir.

Quando os gabaritos do Sentinel para Crystal Reports são publicados no Crystal Enterprise Server, eles devem ficar no diretório eSecurity_Reports.

10.4.2 Publicando gabaritos de relatório – Console de Gerenciamento Central

Quando são publicados com o Console de Gerenciamento Central, os relatórios não podem ser publicados em lote, como quando se usa o Assistente para Publicação do Windows.

Para importar gabaritos do Crystal Report:

1. Abra um browser e digite este url:
   `http://<hostname_or_IP_of_web_server>:<web_server_port_default_8080>/businessobjects/enterprise11/adminlaunch`
2. Clique em Central Management Console
3. Efetue login no Crystal Server.
4. No painel Organizar, clique em Pastas.
5. No canto superior direito, clique em Nova Pasta...
6. Crie uma pasta denominada eSecurity_Reports. Clique em OK.
7. Clique em eSecurity_Reports.
8. Clique na guia Subpastas e crie estas subpastas:
   - Vulnerabilidade do Consultor
   - Gerenciamento de Incidentes
   - Eventos Internos
   - Eventos de Segurança
   - 10 Principais
9. Clique em Home.
10. Clique em Objetos.
11. Clique em Novo Objeto.
12. À esquerda da página, realce o Relatório.
13. Clique em Pesquisar e navegue até a pasta a seguir com a Distribuição do Sentinel Reports:
    `Crystal_v11\Oracle`

    Escolha uma pasta e selecione um relatório.
14. Realce eSecurity_Reports e clique em Mostrar Subpastas.
15. Selecione a pasta apropriada para o relatório e clique em Mostrar Subpastas.
16. Clique em OK.
17. Clique em Atualizar.
18. Para adicionar os relatórios restantes, repita as etapas 9 até 17 até que todos os relatórios tenham sido adicionados.

10.5 Usando o servidor Web Crystal XI

O Crystal Server XI no Linux instala um servidor Web com o qual você pode executar tarefas administrativas além de publicar e ver relatórios.

O portal administrativo é acessado via browser no seguinte URL:

```
http://<hostname_or_IP_of_web_server>:<web_server_port_default_8080>/
businessobjects/enterprise11/adminlaunch
```

O portal não-administrativo, ou de uso geral, é acessado via browser no seguinte URL:

```
http://<hostname_or_IP_of_web_server>:<web_server_port_default_8080>/
businessobjects/enterprise11
```

10.5.1 Testando a conectividade com o servidor Web

Para testar a conectividade para o servidor Web:

1. Vá para outra máquina na mesma rede que o servidor Web.
2. Digite

   ```
   http://
   <hostname_or_IP_of_web_server>:<web_server_port_default_8080>/
   businessobjects/enterprise11/adminlaunch
   ```
3. Você deve obter uma página Web do Crystal BusinessObjects.

10.6 Definindo uma conta de ‘Usuário Nomeado’

A chave de licença fornecida com o Crystal Server É uma chave de conta do Usuário Nomeado. A conta Guest foi mudada de Usuário Simultâneo para Usuário Nomeado.

Para definir a Conta Guest como Usuário Nomeado:

1. Abra um browser e digite este url:

   ```
   http://
   <hostname_or_IP_of_web_server>:<web_server_port_default_8080>/
   businessobjects/enterprise11/adminlaunch
   ```
2. Clique em Central Management Console.
3. O nome do sistema deve ser o nome do computador do host. O tipo de autenticação deve ser Enterprise. Caso contrário, escolha Enterprise.
4. No painel Organizar, clique em Usuários.
5. Clique em Guest.
6. Mude o tipo de conexão de Usuário Simultâneo para Usuário Nomeado.
7. Clique em Atualizar.
8. Efetue logoff e feche a janela.

10.7 Configurando Permissões de Relatórios

Esse procedimento discute como usar o Launchpad de Administração para configurar as permissões para relatórios, para permitir que você veja e modifique relatórios sob demanda.

Para configurar permissões de relatórios:

1. Abra um browser e digite este URL:
   `http://<hostname_or_IP_of_web_server>:<web_server_port_default_8080>/businessobjects/enterprise11/adminlaunch`
2. Clique em Central Management Console.
3. O nome do sistema deve ser o nome do computador do host. O tipo de autenticação deve ser Enterprise. Caso contrário, escolha Enterprise.
4. Digite o nome do usuário e a senha e clique em Log On.
5. No painel Organizar, clique em Pastas.
6. Clique em eSecurity_Reports.
7. Selecionar Tudo.
8. Clique na guia Direitos.
9. Em Todos, no menu suspenso à direita, selecione Ver por Demanda.
10. Clique em Atualizar.
11. Efetue logoff e feche a janela.

10.8 Habilitando os relatórios 10 Primeiros do Sentinel

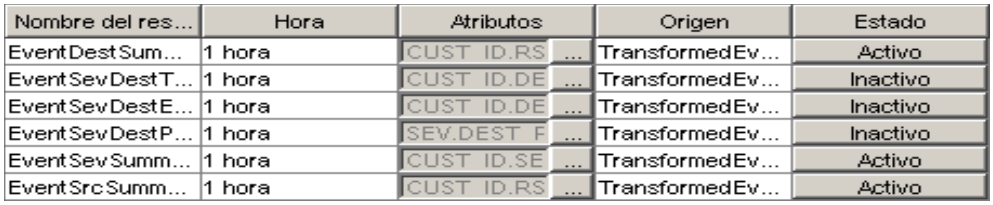
Para habilitar os relatórios 10 Primeiros do Sentinel, é necessário:

- Ativar a agregação;
- Habilitar o EventFileRedirectService;

Para ativar a Agregação

1. Na GUI do Sentinel Control Center, clique na guia Admin.
2. No painel de navegação, clique em Dados de Relatórios ou clique no botão de Dados de Relatórios.
3. Habilite estes resumos:
   - EventDestSummary
   - EventSevSummary
   - EventSrcSummary

Clique nos botões ‘Inativo’ na coluna Status até que mudem para ‘Ativo’.



Nombre del res...	Hora	Atributos	Origen	Estado
EventDestSum...	1 hora	CUST_ID.RS ...	TransformedEv...	Activo
EventSevDestT...	1 hora	CUST_ID.DE ...	TransformedEv...	Inactivo
EventSevDestE...	1 hora	CUST_ID.DE ...	TransformedEv...	Inactivo
EventSevDestP...	1 hora	SEV.DEST_F ...	TransformedEv...	Inactivo
EventSevSumm...	1 hora	CUST_ID.SE ...	TransformedEv...	Activo
EventSrcSumm...	1 hora	CUST_ID.RS ...	TransformedEv...	Activo

Para Habilitar EventFileRedirectService

1. Na máquina DAS, usando o editor de texto, abra:
   `$ESEC_HOME/sentinel/config/das_binary.xml`
2. Para o EventFileRedirectService, mude o status para “on” (ativado):
   `<property name="status">on</property>`
3. Reinicie o processo DAS_Binary. Para fazer isso, use o Sentinel Control Center ou reinicialize a máquina.

   Usando o Sentinel Control Center:

   - Efetue login no Sentinel Control Center como um usuário com direitos de administrador. Esse usuário deve ter as seguintes permissões de Telas de Servidor:
     - Ver Servidores
     - Controlar Servidores
   - Na guia Admin, abra uma tela de servidor para ver todos os processos do Sentinel Server.
   - Clique o botão direito do mouse no processo DAS_Binary e selecione Reiniciar.
   - A conta Início desse processo aumentará em uma unidade se o processo for reiniciado com êxito.

10.9 Aumentando o limite de atualização de registro do relatório do Crystal Enterprise Server

Dependendo do número de eventos que o Crystal estiver consultando, você poderá receber um erro sobre o tempo máximo de processamento ou o limite máximo de registros. Para definir o servidor para processar um número maior ou ilimitado de relatórios, será necessário reconfigurar o Crystal Page Server.

Para reconfigurar o Crystal Page Server:

1. Abra um browser e digite este url:
   `http://`
   `<hostname_or_IP_of_web_server>:<web_server_port_default_8080>/`
   `businessobjects/enterprise11/adminlaunch`
2. Clique em Central Management Console.
3. O nome do sistema deve ser o nome do computador do host. O tipo de autenticação deve ser Enterprise. Caso contrário, escolha Enterprise.
4. Digite o nome do usuário e a senha e clique em Log On.
5. Clique em Servidores.

6 Clique em <nome do servidor>.pageserver.

7 Em Registros do Banco de Dados para Ler ao Visualizar ou Atualizar um Relatório, selecione Registros ilimitados.

8 Clique em Aplicar.

9 Será exibido um prompt para reiniciar o servidor de página; clique em OK.

10 Talvez seja preciso fornecer um nome de logon e uma senha para acessar o gerenciador do serviço do sistema operacional.

10.10 Configurando o Sentinel Control Center para integração com o Crystal Enterprise Server.

O Sentinel Control Center pode ser configurado para se integrar ao Crystal Enterprise Server, permitindo que você veja Relatórios do Crystal a partir do Sentinel Control Center.

Para habilitar a integração do Sentinel Control Center com Crystal Enterprise Server, siga as instruções abaixo.

Observação: Essa configuração deve ser executada somente depois que o Crystal Enterprise Server tiver sido instalado e Relatórios Crystal tiverem sido publicados nele.

Para configurar o Sentinel para integração com o Crystal Enterprise Server:

1 Efetue login no Centro de Controle do Sentinel como um usuário com privilégios para a guia Admin;

2 Na guia Admin, selecione Configuração de Relatórios.

3 No campo URL de Análise, digite o seguinte:

```
http://
<hostname_or_IP_of_web_server>:<web_server_port_default_8080>/
esec-script/
GetReports.jsp?APS=<hostname>&user=Guest&password=&tab=Analysis
```

Observação: <nome_do_host_ou_IP_do_servidor_da_Web> deve ser substituído pelo endereço IP ou nome de host do Crystal Enterprise Server.

Observação: O URL acima não funcionará corretamente se o APS estiver definido como o endereço IP. Ele precisa ser o nome do host.

Observação: <porta_padrão_do_servidor_Web_8080> deve ser substituída pela porta que o servidor Web do Crystal estiver escutando.

---

4 Clique em Atualizar ao lado do campo URL de Análise.

5 Se o Advisor estiver instalado, digite o seguinte no campo URL de Análise:

```
http://
<hostname_or_IP_of_web_server>:<web_server_port_default_8080>/
esec-script/
GetReports.jsp?APS=<hostname>&user=Guest&password=&tab=Advisor
```

Observação: <nome_do_host_ou_IP_do_servidor_da_Web> deve ser substituído pelo endereço IP ou nome de host do Crystal Enterprise Server.

Observação: O URL acima não funcionará corretamente se o APS estiver definido como o endereço IP. Ele precisa ser o nome do host.

Observação: <porta_padrão_do_servidor_Web_8080> deve ser substituída pela porta que o servidor Web do Crystal estiver escutando.

6 Clique em Atualizar ao lado do campo URL de Consultor.

7 Clique em Gravar.

8 Efetue logout e login novamente no Sentinel Control Center. As árvores do Crystal Report nas guias Análise e Consultor (se o Advisor estiver instalado) devem agora aparecer na janela Navegador.

10.11 Utilitários e solução de problemas

10.11.1 Iniciando o MySQL

Para verificar se o MySQL está em execução:

1 Efetue login como o usuário crystal.

2 cd /opt/crystal_xi/bobje

3 ./mysqlstartup.sh

10.11.2 Iniciando o Tomcat

Para verificar se o Tomcat está em execução:

1 Efetue login como o usuário crystal

2 cd /opt/crystal_xi/bobje

3 ./tomcatstartup.sh

10.11.3 Iniciando o Crystal Servers

Para verificar se o Crystal Servers está em execução:

1 Efetue login como o usuário crystal

2 cd /opt/crystal_xi/bobje

3 ./startservers

10.11.4 Erro de nome de host Crystal

Para resolver erro de Nome de Host:

1. Se receber este erro:

   ```
   Warning: ORB::BOA_init: hostname lookup returned `localhost'
   (127.0.0.1)
   Use the -OAhost option to select some other hostname
   ```

   Verifique se o IP e o nome do host estão no arquivo /etc/hosts. ex.:

   ```
   192.0.2.46linuxCE02
   ```

10.11.5 Não é possível conectar-se ao CMS

Se o sistema relatar que não é possível conectar com o CMS, tente executar os comandos a seguir.

Para solucionar problemas da falha de conexão CMS:

1. Se o comando netstat –an | grep 6400 não retornar um resultado, tente o seguinte:
   - Digite novamente as informações da conexão MySQL:
     a. Efetue login como o usuário crystal
     b. cd /opt/crystal_xi/bobje
     c. ./cmsdbsetup.sh
     d. Pressione Enter quando for exibido [<nome de host>.cms].
     e. Escolha selecionar e digite novamente todas as informações do banco de dados MySQL fornecidas durante a instalação. Para obter mais informações, consulte as instruções de instalação.
     f. Quando tiver concluído, saia de cmsdbsetup.sh.
     g. ./stopservers
     h. ./startservers
   - Reinicialize o banco de dados MySQL:
     a. Efetue login como o usuário crystal
     b. cd /opt/crystal_xi/bobje
     c. ./cmsdbsetup.sh
     d. Pressione Enter quando for exibido [<nome de host>.cms].
     e. Selecione reiniciar e siga as instruções.
     f. Quando tiver concluído, saia de cmsdbsetup.sh.
     g. ./stopservers
     h. ./startservers
2. Verifique se todos os servidores CCM estão habilitados:
   2a Efetue login como o usuário crystal
   2b cd /opt/crystal_xi/bobje
   2c ./ccm.sh -enable all

Desinstalando o Sentinel 11

Tópicos incluídos neste capítulo:

- Seção 11.1, “Desinstalando o Sentinel” na página 149
- Seção 11.1.1, “Desinstalação no Solaris e Linux” na página 149
- Seção 11.1.2, “Desinstalação no Windows” na página 150
- Seção 11.1.3, “Desinstalando com o Painel de Controle” na página 150
- Seção 11.2, “Pós-desinstalação” na página 151

Para remover uma instalação do Sentinel, são fornecidos desinstaladores para Linux, Solaris e Windows. Vários arquivos, incluindo arquivos de registro, são preservados e podem ser removidos manualmente, caso desejado. Além disso, é altamente recomendável que você execute todas as etapas a seguir para garantir que não haja arquivos ou configurações de sistema restantes de uma instalação anterior que possam interferir com uma nova instalação.

Aviso: Essas instruções envolvem a modificação de configurações e arquivos do sistema operacional. Se você não estiver familiarizado com a modificação dessas configurações e/ou arquivos do sistema, contate o Administrador do Sistema.

11.1 Desinstalando o Sentinel

11.1.1 Desinstalação no Solaris e Linux

Para iniciar o Desinstalador do Sentinel para Solaris:

1. Faça login como usuário Root.
2. Pare o Sentinel Server.
3. Consulte:
   `$ESEC_HOME/_uninst`
4. Digite:
   `./uninstall.bin`
5. Selecione um idioma e clique em OK.
6. O Assistente do Install Shield do Sentinel será exibido. Clique em Avançar.
7. Selecione os componentes que você precisa desinstalar e clique em Próximo.

   Observação: O sentinel exibirá uma mensagem de aviso para fechar qualquer aplicativo aberto do Sentinel.

   ---

8. Selecione uma dentre as duas opções exibidas:
   - Apagar a instância do banco de dados inteira.
   - Apagar somente os objetos do banco de dados

Marque sua opção e clique em Avançar.

9 Clique em Desinstalar.

11.1.2 Desinstalação no Windows

Para usar o Desinstalador do Sentinel no Windows:

1 Efetue login como Administrador.

2 Pare o Sentinel Server.

3 Selecione Iniciar > Arquivos De Programas > Sentinel > Desinstalar Sentinel.

4 Selecione um idioma e clique em OK.

5 O Assistente do Install Shield do Sentinel será exibido. Clique em Avançar.

6 Selecione os componentes que você deseja desinstalar e clique em Próximo.

Observação: O Sentinel exibirá mensagem de aviso para fechar qualquer Aplicativo aberto do Sentinel.

---

7 Selecione uma das duas opções do prompt:

- Apagar a instância do banco de dados inteira.
- Apagar somente os objetos do banco de dados

Marque sua opção e clique em Avançar.

8 Especifique as informações de autenticação, selecione a Autenticação SQL ou Windows e digite as credenciais de login se solicitado. Clique em Avançar.

9 O resumo dos recursos selecionados para desinstalação será exibido. Clique em Desinstalar.

10 Selecione Reinicializar o sistema e clique em Concluir.

11.1.3 Desinstalando com o Painel de Controle

Para desinstalar os aplicativos do Sentinel no Windows:

1 Clique em Iniciar>Painel de Controle>Adicionar ou Remover Programas>Sentinel>Remover/Alterar.

2 Selecione um idioma e clique em OK.

3 O Assistente do Install Shield do Sentinel será exibido. Clique em Avançar.

4 Selecione os componentes que você deseja desinstalar e clique em Próximo.

Observação: O Sentinel exibirá mensagem de aviso para fechar qualquer Aplicativo aberto do Sentinel.

---

5 Selecione uma das duas opções do prompt:

- Apagar a instância do banco de dados inteira.
- Apagar somente os objetos do banco de dados

Marque sua opção e clique em Avançar.

6 Especifique as informações de autenticação, selecione a Autenticação SQL ou Windows e digite credenciais de login se solicitado. Clique em Próximo

7 O resumo dos recursos selecionados para desinstalação será exibido. Clique em Desinstalar.

8 Selecione Reinicializar o sistema e clique em Concluir.

11.2 Pós-desinstalação

11.2.1 Arquivos de dados do Sentinel

Para preservar informações potencialmente valiosas depois de desinstalar o Sentinel, vários arquivos são preservados. Se essas informações não forem mais necessárias, os arquivos e as pastas a seguir podem ser removidos manualmente.

- Terceiros
  - SonicMQ
    - Docs7.0
    - InstallLogs7.0
    - MQ7.0
    - Instalador
    - mq_documentation_7.0.htm
    - sonicsw.properties
    - uninstall.sh
    - wizard.jar
- Bin
  - control_center.ja
  - sdm_gui.jac
- Opção de
  - .proxyServerKeystore
  - .primary_key
  - .keystore
- Dados
  - .cache
  - .sessionState
  - .uuid
  - .uuidlock
  - DatabaseManager.log
  - agent-84EBED40-9AB1-1029-9C3F-0003BAC9707D.lck
  - collector_mgr.cache
  - eventfiles
  - map_data
  - portcfg_84EBED40-9AB1-1029-9C3F-0003BAC9707D.dat

- uuid.dat
- Install_log
  - CreateAdminUserSimpleErr.txt
  - CreateAdminUserSimpleOut.txt
  - PostInstallSetup2Err.log
  - PostInstallSetup2Out.log
  - PostInstallSetupErr.log
  - PostInstallSetupOut.log
  - advcronjoberr.txt
  - advcronjobout.txt
  - configupdateerr.txt
  - configupdateout.txt
  - containerFileUpdate.log
  - cronjoberr.txt
  - cronjobout.txt
  - db
  - dbupdateerr.txt
  - dbupdateout.txt
  - extractJre64_err.log
  - extractJre64_out.log
  - key_generation.log
  - sentinelInstall.log
  - sentinelUninstall.log
  - shutdown_database_err.log
  - shutdown_database_out.log
  - sonic_silent_install_err.log
  - sonic_silent_install_out.log
  - sonic_silent_uninstall_err.log
  - sonic_silent_uninstall_out.log
  - stopAM_err.txt
  - stopAM_out.txt
  - stopSentinel_err.txt
  - stopSentinel_out.txt
  - uninstallDB_err.log
  - uninstallDB_out.log
  - Todos esses arquivos podem ser localizados no diretório $ESEC_HOME ou %ESEC_HOME% e seus subdiretórios.
  - Para Consultor, as pastas de ataque e alerta usadas para seus arquivos de dados do Consultor permanecerão.

11.2.2 Configurações do Sentinel

Após desinstalar o Sentinel, certas configurações de sistemas permanecem, e podem ser removidas manualmente. Essas configurações devem ser removidas antes de executar uma nova instalação do Sentinel, particularmente se a desinstalação do Sentinel tiver erros.

Observação: No Solaris e Linux, a desinstalação do Sentinel Server não removerá do sistema operacional o Usuário Administrador do Sentinel. Você precisará remover manualmente esse usuário, caso desejado.

Remover configurações do sistema do Sentinel no Linux com Oracle

Para limpar manualmente o Sentinel no Linux:

1. Efetue login como Usuário Root.
2. Verifique se todos os processos do Sentinel foram parados.
3. Remova os conteúdos de /opt/sentinelXX (ou onde o software do Sentinel foi instalado ou nomeado)
4. Remova o arquivo S98sentinel do diretório /etc/rc.d/rc5.d.
5. Remova o arquivo S98sentinel do diretório /etc/rc.d/rc3.d.
6. Remova o arquivo K02sentinel do diretório /etc/rc.d/rc0.d.
7. Remova o arquivo do sentinel do diretório /etc/init.d.
8. Remova o diretório /root/Install Shield
9. Remova o arquivo /root/vpd.properties
10. Verifique se alguém está conectado como Usuário Administrador do Sentinel (esecadm por padrão), depois remova o Usuário Administrador do Sentinel (e dir. home) e grupo esec.
    - Execute: userdel-r esecadm
    - Execute: groupdel esec
11. Se o arquivo .login existir, remova a seção Install Shield de /etc/profile, /etc/.login
12. Remova o banco de dados do Oracle do Sentinel. Para obter maiores informações, consulte “Para limpar manualmente o banco de dados do Oracle do Sentinel no Linux:” na página 153.
13. Reinicie o sistema operacional.

Para limpar manualmente o banco de dados do Oracle do Sentinel no Linux:

Observação: Verifique se nenhum outro aplicativo está usando esse banco de dados antes de removê-lo.

---

1. Efetue login como oracle.
2. Pare a Escuta do Oracle:
    - Execute: lsnrctl stop
3. Pare o banco de dados do Sentinel.
    - Defina a variável de ambiente ORACLE_SID como o nome da instância do banco de dados do Sentinel (geralmente ESEC).

- Execute: sqlplus '/ como sysdba'
- No prompt do sqlplus, execute: shutdown immediate

4. Remova a entrada para o banco de dados do Sentinel no arquivo /etc/oratab
5. Remova init<nome_de_sua_ instância>.ora (usualmente initESEC.ora) do diretório $ORACLE_HOME/dbs.
6. Remova as entradas para o banco de dados do Sentinel dos seguintes arquivos no diretório $ORACLE_HOME/network/admin.
   - tnsnames.ora
   - listener.ora
7. Apague os arquivos do banco de dados do local onde escolheu para instalá-los.

Remover configurações do sistema do Sentinel no Solaris com Oracle

Para limpar manualmente o Sentinel no Solaris:

Observação: A limpeza manual é geralmente usada quando a desinstalação do Sentinel encontra um erro.

---

1. Efetue login como Usuário Root.
2. Verifique se não há processos do Sentinel em execução.
3. Remova o conteúdo de /opt/sentinelxx (ou do local onde o software do Sentinel foi instalado).
4. Remova o arquivo S98sentinel do diretório /etc/rc3.d.
5. Remova o arquivo K02sentinel do diretório /etc/rc0.d.
6. Remova o arquivo do sentinel do diretório /etc/init.d.
7. Limpe referências do installshield em /var/sadm/pkg. Remova os seguintes arquivos do diretório var/sadm/pkg:
   - Todos os arquivos que começam com IS (IS* na linha de comando)
   - Todos os arquivos que começam com ES (ES* na linha de comando)
   - Todos os arquivos que começam com MISCwp (MISCwp* na linha de comando)
8. Certifique-se de que ninguém está conectado como Usuário Administrador do Sentinel, remova o Usuário Administrador do Sentinel (e home dir) e o grupo esec.
   - Execute: userdel-r esecadm
   - Execute: groupdel esec
9. Se o arquivo .login existir, remova a seção Install shield de /etc/profile, /etc/.login
10. Remova o diretório /Install Shield, se houver um.
11. Reinicie o sistema operacional.

Para limpar manualmente o banco de dados do Oracle do Sentinel no Solaris:

Observação: Verifique se nenhum outro aplicativo está usando esse banco de dados antes de removê-lo.

---

1. Efetue login como oracle.

2 Pare a Escuta do Oracle:
   - Execute: lsnrctl stop
3 Pare o banco de dados do Sentinel:
   - Defina a variável de ambiente ORACLE_SID como o nome da instância do banco de dados do Sentinel (geralmente ESEC).
   - Execute: sqlplus '/ como sysdba'
   - No prompt do sqlplus, execute: shutdown immediate
4 Remova a entrada para o banco de dados do Sentinel no arquivo /var/opt/oracle/oratab
5 Remova init<nome_de_sua_ instância>.ora (usualmente initESEC.ora) do diretório $ORACLE_HOME/dbs.
6 Remova as entradas para o banco de dados do Sentinel dos seguintes arquivos no diretório $ORACLE_HOME/network/admin.
   - tnsnames.ora
   - listener.ora
7 Apague os arquivos do banco de dados do local onde escolheu para instalá-los.

Remova as configurações do sistema do Sentinel no Windows com o SQL Server

Para limpar manualmente o Sentinel no Windows:

1 Apague a pasta %CommonProgramFiles%\InstallShield\Universal e todo o seu conteúdo.
2 Apague a pasta %ESEC_HOME% (por padrão: C:\Arquivos de Programas\novell\sentinel6).
3 Clique o botão direito do mouse em Meu Computador > Propriedades > guia Avançado.
4 Clique no botão Variáveis do Ambiente.
5 Exclua as seguintes variáveis, se elas existirem:
   - ESEC_HOME
   - ESEC_VERSION
   - ESEC_JAVA_HOME
   - ESEC_CONF_FILE
   - WORKBENCH_HOME
6 Remova quaisquer entradas na variável de ambiente CAMINHO que apontam para a instalação do Sentinel.

   Aviso: Não remova caminhos para nada diferente da instalação do Sentinel antiga. Isso poderia resultar no funcionamento não adequado do seu sistema.

7 Apague todos os atalhos do Sentinel da sua área de trabalho.
8 Apague a pasta de Atalhos Iniciar>Programas>Sentinel do menu Iniciar.

9 Reinicie o sistema operacional.

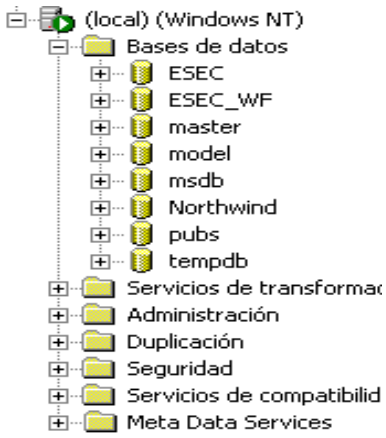
Para limpar manualmente o banco de dados do Microsoft SQL Server do Sentinel no Windows:

Observação: Verifique se nenhum outro aplicativo está usando esse banco de dados antes de removê-lo.

---

1 Abra o Microsoft SQL Server Management Studio e conecte a instância do SQL Server onde você instalou o banco de dados do Sentinel.

2 Expanda a árvore do Banco de Dados e localize o seu banco de dados do Sentinel.



3 Deveria haver um banco de dados do Sentinel (geralmente chamado ESEC) e um banco de dados de workflow (geralmente chamado ESEC_WF). Clique o botão direito do mouse em cada um e selecione Apagar.

4 Ao ser solicitado, selecione Sim para apagar o banco de dados.

Questionário de pré-instalação

A

Questões pré-instalação

1 Qual o seu objetivo ou propósito ao usar o Novell Sentinel?

1a Conformidade

1b SEM

1c Outros_____

2 Qual hardware foi alocado para a instalação do Sentinel? Ele está de acordo com as especificações de hardware fornecidas no Guia de Instalação do Sentinel?

3 Você já validou o hardware do Sentinel e os requisitos do sistema operacional descritos no Guia de Instalação do Sentinel em sua configuração?

- Níveis de patch do OS
- Patches de serviços
- Hot Fixes, etc.

4 Sua máquina DAS atende o requisitos de hardware e OS necessários?

5 Qual é a arquitetura de rede para os dispositivos de origem com relação ao segmento de segurança no qual o hardware do Sentinel e Coletor será localizado?

Observação: Isto é importante para compreender a hierarquia da coleta de dados do coletor e para identificar todos os firewalls que devem ser atravessados para habilitar a comunicação do Coletor com o Sentinel ou comunicação do Sentinel com BD ou Crystal Server com BD.

Digite as informações abaixo (texto e/ou desenho) ou link para a informação.

6 Que relatórios você quer retirar do sistema? Isto é importante para garantir que os coletores reúnam os dados corretos para serem passados para o banco de dados do Sentinel.

6a _____

6b _____

6c _____

6d _____

6e _____

6f _____

7 De quais dispositivos de origem você deseja coletar dados (IDS, HIDS, Roteadores, Firewalls, etc.), taxas de eventos (EPS - eventos por segundo), versões, métodos de conexão, plataformas e patches?

Dispositivo (mfr/ modelo)	Taxa de eventos (EPS)	Versão	Método de conexão	Plataforma	Patches

Você pode oferecer exemplos dos dados que você deseja que os coletores do Sentinel coletem e analisem? O Sentinel pode ser configurado para fornecer a saída desejada com base nas informações fornecidas aqui.

8 Quais padrões/modelos de segurança existem no seu site?

- Qual a sua postura em relação a contas locais versus autenticação de domínio?
  - Para Windows com autenticação de domínio, configurações de conta de domínio apropriado devem ser criadas para garantir que o Sentinel possa ser instalado.
  - Para a instalação do Solaris, isso não se aplica. Contudo, o Sentinel não tem suporte para NIS.

9 Qual a retenção de dados necessária por dia?

10 Com base nas informações de retenção de dados e EPS, qual tamanho de disco será usado? Use 500 a 800 bytes/evento para estimativas de tamanho.

Registro de instalação para Sentinel no Linux com Oracle

B

Essa lista de verificação funciona para instalações distribuídas com até três instâncias do Gerenciador do Coletor e Mecanismo de Correlação.

Consulte os requisitos de Hardware e OS e procedimento de instalação no Guia de Instalação.

	Variável de configuração			
1.	Versão do Sentinel:		Data de hoje:	
2.	Valores de Kernel UNIX para o Oracle. Abaixo, os valores mínimos. No SLES e RHEL, você pode definir parâmetros no "etc/sysctl.conf".			
	◆ shmmax		☐ : Sim | ☐ : Não	Valor se maior:
	◆ shmmin		☐ : Sim | ☐ : Não	Valor se maior:
	◆ shmseg		☐ : Sim | ☐ : Não	Valor se maior:
	◆ shmmni		☐ : Sim | ☐ : Não	Valor se maior:
	◆ semmns		☐ : Sim | ☐ : Não	Valor se maior:
	◆ semmni		☐ : Sim | ☐ : Não	Valor se maior:
	◆ semmsl		☐ : Sim | ☐ : Não	Valor se maior:
	◆ shmopm		☐ : Sim | ☐ : Não	Valor se maior:
	◆ shmvmx		☐ : Sim | ☐ : Não	Valor se maior:
3.	Sistema de Banco de Dados			
	◆ Sistema operacional correto para Componentes do Sentinel	☐ : Sim | ☐ : Não	◆ Patch adequado	☐ : Sim | ☐ : Não
	◆ SO correto para DB	☐ : Sim | ☐ : Não	◆ Patch adequado	☐ : Sim | ☐ : Não
	◆ Versão		◆ Nível de patch	
	◆ BD Oracle correto c/ Particionamento	☐ : Sim | ☐ : Não	◆ Patch adequado	☐ : Sim | ☐ : Não
	◆ Versão		◆ Nível de patch	
	◆ Variáveis de ambiente corretas definidas para o usuário do sistema operacional Oracle.	☐ : Sim | ☐ : Não		
	◆ arquivo init.ora configurado	☐ : Sim | ☐ : Não		
4.	Máquina DAS			

Variável de configuração				
	◆ Sistema operacional correto para Componentes do Sentinel	: Sim | : Não	◆ Patch adequado	: Sim | : Não
	◆ número de série			
	◆ chave de licença			
5.	Install DAS (Instalar DAS)			
	◆ Nome de host ou IP do Banco de Dados			
	◆ Nome do banco de dados			Padrão: ESEC
	◆ Porta do banco de dados			Padrão: 1521
	◆ Local do arquivo JDBC			
6.	Instância do Banco de Dados (SID)			
7.	Nome do banco de dados			
8.	Componentes do Sentinel:			
	◆ Banco de Dados do Sentinel (IP ou DNS)			Sistema Operacional: Patch:
	◆ Registro de instalação do banco de dados			
	◆ Memória Oracle (RAM)			
	◆ Nome da instância			
	◆ Porta de escuta		Padrão: 1521	
	◆ Senha do SISTEMA			
	◆ Senha do SISTEMA			
	◆ arquivo .keystore importado ao instalar:			
	◆ Correlação	☐ : Sim | ☐ : Não		
	◆ DAS	☐ : Sim | ☐ : Não		
	◆ Gerenciador de Coletor	☐ : Sim | ☐ : Não		
	◆ Servidor de Comunicação	☐ : Sim | ☐ : Não		
	◆ Servidor de Comunicação (iSCALE) (IP ou DNS)	◆ IP/DNS:		Sistema Operacional: Patch:
	◆ DAS/Consultor (IP ou DNS) (O consultor é opcional)	◆		Sistema Operacional: Patch:

Variável de configuração		
◆ DAS RAM	◆	
◆ Mecanismo de Correlação (IP e OS)		
	◆ IP:	Sistema Operacional:
	◆ IP:	Sistema Operacional:
	◆ IP:	Sistema Operacional:
◆ Construtor de Coletores (IP ou DNS) (recomenda-se uma instalação)		
◆ Gerenciador de Coletor	Digite os detalhes de cada Gerenciador de Coletor que você distribuir.	
◆ Gerenciador de Coletor	☐ : Sim | ☐ : Não	
◆ IP: ◆ Sistema Operacional:	◆ Porta de barramento de mensagem: ◆ Porta proxy do Sentinel Control Center: ◆ Nome de host do Servidor de Comunicação: ◆ Porta de autenticação do Certificado do Gerenciador de Coletor:	

9. Consultor (opcional)

◆ Instalado em algumas máquinas como DAS?	☐ : Sim | ☐ : Não
◆ Download do Consultor:	☐ : Independente | ☐ : Download Direto da Internet
◆ Local do arquivo de alimentação de dados	
◆ Endereço de do Consultor	
◆ Endereço para do Consultor	
◆ Nome de usuário	u/n:

10. Locais de arquivo do banco de dados:

- ◆ Arquivos de dados
- ◆ Arquivos de índice
- ◆ Arquivos de dados de resumo
- ◆ Arquivos de índice de resumo
- ◆ Arquivos Temporário e Desfazer Tabela

Variável de configuração		
◆ Diretório A do Membro de Redo Log		
◆ Diretório A do Membro de Redo Log		
11. Tamanho do banco de dados:		
◆ Padrão (20 GB)		
◆ Grande (400 GB)		
◆ Personalizado (tamanho)		
12. SMTP Server		
(DNS ou IP)		
13. Senhas de usuário		
◆ esecadm	PW:	
◆ Diretório pessoal		Padrão: /export/home
◆ esecapp	PW:	
◆ esecdba	PW:	
◆ esecrpt	PW:	
Instalação do Crystal		
1. Versão do Crystal:		
◆ Sistema Operacional		
◆ BD do Crystal		
◆ Crystal Server (IP ou DNS)		
◆ Servidor Web (IP ou DNS)		
2. Crystal Reports		
◆ Todos os relatórios publicados	☐ : Sim | ☐ : Não	
◆ Relatórios configurados no SCC	☐ : Sim | ☐ : Não	

Registro de instalação para Sentinel no Solaris com Oracle

C

Essa lista de verificação funciona para instalações distribuídas com até três instâncias do Gerenciador do Coletor e Mecanismo de Correlação.

Para mais informações, consulte o Hardware e os requisitos de OS e o Procedimento de Instalação no Guia de Instalação.

	Variável de configuração			
1.	Versão do Sentinel:			Data de hoje:
2.	Valores de Kernel UNIX para o Oracle. Abaixo, os valores mínimos. No SLES e RHEL, você pode definir parâmetros no "etc/sysctl.conf".			
	shmmax		☐ : Sim | ☐ : Não	Valor se maior:
	shmmin		☐ : Sim | ☐ : Não	Valor se maior:
	shmseg		☐ : Sim | ☐ : Não	Valor se maior:
	shmmni		☐ : Sim | ☐ : Não	Valor se maior:
	semmns		☐ : Sim | ☐ : Não	Valor se maior:
	semmni		☐ : Sim | ☐ : Não	Valor se maior:
	semmsl		☐ : Sim | ☐ : Não	Valor se maior:
	shmopm		☐ : Sim | ☐ : Não	Valor se maior:
	shmvmx		☐ : Sim | ☐ : Não	Valor se maior:
3.	Sistema de Banco de Dados			
	Sistema operacional correto para Componentes do Sentinel	☐ : Sim | ☐ : Não	Patch adequado	☐ : Sim | ☐ : Não
	◆ SO correto para DB	☐ : Sim | ☐ : Não	◆ Patch adequado	☐ : Sim | ☐ : Não
	◆ BD Oracle correto c/ Particionamento	☐ : Sim | ☐ : Não	◆ Patch adequado	☐ : Sim | ☐ : Não
	◆ Versão		◆ Nível de patch	
	◆ Cópia do Oracle Note: 148673.1	☐ : Sim | ☐ : Não		
	◆ Variáveis de ambiente corretas definidas para o usuário do sistema operacional Oracle.	☐ : Sim | ☐ : Não		

	Variável de configuração			
	◆ arquivo init.ora configurado	☐ : Sim | ☐ : Não		
	◆ Sistema operacional correto para Componentes do Sentinel	☐ : Sim | ☐ : Não	◆ Patch adequado	☐ : Sim | ☐ : Não
4.	Máquina DAS			
	◆ número de série			
	◆ chave de licença			
5.	Install DAS (Instalar DAS)			
	◆ Nome de host ou IP do Banco de Dados			
	◆ Nome do banco de dados			Padrão: ESEC
	◆ Porta do banco de dados			Padrão: 1521
	◆ Local do arquivo JDBC			
6.	Instância do Banco de Dados (SID)			
7.	Nome do banco de dados			
8.	Componentes do Sentinel:			
	◆ Banco de Dados do Sentinel (IP ou DNS)			Sistema Operacional: Patch:
	◆ Registro de instalação do banco de dados			
	◆ Memória Oracle (RAM)			
	◆ Nome da instância			
	◆ Porta de escuta		Padrão: 1521	
	◆ Senha do SISTEMA			
	◆ Senha do SISTEMA			
	◆ arquivo .keystore importado ao instalar:			
	◆ Correlação	☐ : Sim | ☐ : Não		
	◆ DAS	☐ : Sim | ☐ : Não		
	◆ Gerenciador de Coletor	☐ : Sim | ☐ : Não		
	◆ Gerenciador de Coletor			
	◆ Instalar Gerenciador do Coletor	☐ : Sim | ☐ : Não	Proxy | Barramento de Mensagem Direta	

Variável de configuração			
◆ IP: ◆ Sistema Operacional:	◆ Porta de barramento de mensagem: ◆ Porta proxy do Sentinel Control Center: ◆ Nome de host do Servidor de Comunicação: ◆ Porta de autenticação do Certificado do Gerenciador de Coletor:		
◆ Servidor de Comunicação	☐ : Sim | ☐ : Não		
◆ Servidor de Comunicação (iSCALE) (IP ou DNS)	☐ : Sim | ☐ : Não		Sistema Operacional: Patch:
◆ DAS/Consultor (IP ou DNS) (O consultor é opcional)			Sistema Operacional: Patch:
◆ DAS RAM			
◆ Mecanismo de Correlação (IP e OS)			
	IP:		Sistema Operacional:
	IP:		Sistema Operacional:
	IP:		Sistema Operacional:
◆ Crystal Server (IP ou DNS)			
◆ MySQL para Crystal Server	Versão do MySQL: Patch do MySQL: senha sa ou portador de senha:		
◆ IP:	u/n:	PW:	Sistema Operacional:
◆ Construtor de Coletores (IP ou DNS) (recomenda-se uma instalação)			
◆ Gerenciador de Coletor			
◆ Instalar Gerenciador de Coletor usando:	☐ : Sim | ☐ : Não	☐ : Proxy | ☐ : Barramento de Mensagem Direto	
◆ IP:	PW:		Sistema Operacional:
◆ IP:	PW:		Sistema Operacional:
◆ IP:	PW:		Sistema Operacional:

	Variável de configuração		
9.	Consultor (opcional)		
	Instalado em algumas máquinas como DAS?	☐ : Sim | ☐ : Não	
	◆ Download do Consultor:	☐ : Independente ☐ : Download Direto da Internet	
	◆ Local do arquivo de alimentação de dados		
	◆ Endereço de do Consultor		
	◆ Endereço para do Consultor		
	◆ Nome de usuário e senha	u/n:	
10.	Locais de arquivo do banco de dados:		
	◆ Arquivos de dados		
	◆ Arquivos de índice		
	◆ Arquivos de dados de resumo		
	◆ Arquivos de índice de resumo		
	◆ Arquivos Temporário e Desfazer Tabela		
	◆ Diretório A do Membro de Redo Log		
	◆ Diretório A do Membro de Redo Log		
11.	Tamanho do banco de dados:		
	◆ Padrão (20 GB)		
	◆ Grande (400 GB)		
	◆ Personalizado (tamanho)		
12.	SMTP Server		
	(DNS ou IP)		
13.	Senhas de usuário		
	◆ esecadm	PW:	
	◆ Diretório pessoal		Padrão: /export/home
	◆ esecapp	PW:	
	◆ esecdba	PW:	
	◆ esecrpt	PW:	
	Instalação do Crystal		

	Variável de configuração	
1.	◆ Versão do Crystal:	
	◆ Sistema Operacional	
	◆ BD do Crystal	
	◆ Crystal Server (IP ou DNS)	
	◆ Servidor Web (IP ou DNS)	
2.	Crystal Reports	
	◆ Todos os relatórios publicados	☐ : Sim | ☐ : Não
	◆ Relatórios configurados no SCC	☐ : Sim | ☐ : Não

Registro de instalação para o Sentinel no Windows com Microsoft SQL Server

D

Essa lista de verificação funciona para instalações distribuídas com até três instâncias do Gerenciador do Coletor e Mecanismo de Correlação.

Para obter mais informações, consulte os requisitos de Hardware e OS e os Procedimento de Instalação no Guia de Instalação.

	Variável de configuração			
1.	Versão do Sentinel:			Data de hoje:
	Sistema de Banco de Dados			
	◆ SO correto para DB	☐ : Sim | ☐ : Não	◆ Patch adequado	☐ : Sim | ☐ : Não
	◆ BD SQL correto	☐ : Sim | ☐ : Não	◆ Patch adequado	☐ : Sim | ☐ : Não
	◆ Versão		◆ Nível de patch	
	◆			◆
2.	Para instalação DAS em Conta de Domínio Windows, atribua 'Fazer login como serviço'	☐ : Sim | ☐ : Não		
3.	Máquina DAS			
	◆ número de série			
	◆ chave de licença			
4.	Nome de host do banco de dados ou IP:	<nome de host>[\<Nome de Instância>]		
5.	Nome do banco de dados:			Padrão: ESEC
6.	Porta:			Padrão: 1433
7.	Modo de Autenticação	☐ : mista		
		☐ : não mista		
8.	Senha sa de servidor SQL ou portador de senha.	PW:		
9.	Componentes do Sentinel:			
	◆ Banco de Dados do Sentinel (IP ou DNS)			Sistema Operacional:
				Patch:

Variável de configuração			
◆ arquivo .keystore importado ao instalar:			
◆ Correlação	☐ : Sim | ☐ : Não		
◆ DAS	☐ : Sim | ☐ : Não		
◆ Serviço do Gerenciador do Coletor	☐ : Sim | ☐ : Não		
◆ Servidor de Comunicação	☐ : Sim | ☐ : Não		
◆ Servidor de Comunicação (iSCALE) (IP ou DNS)			Sistema Operacional: Patch:
◆ DAS/Consultor (IP ou DNS) (O consultor é opcional)			Sistema Operacional: Patch:
◆ Mecanismo de Correlação (IP e OS)			
	IP:		Sistema Operacional:
	IP:		Sistema Operacional:
	IP:		Sistema Operacional:
◆ Crystal Server (IP ou DNS)			Sistema Operacional: Patch:
◆ Microsoft SQL Server para Crystal Server	Versão do MS SQL: Patch do MS SQL: senha sa ou portador de senha:		
◆ Construtor de Coletores (IP ou DNS) (recomenda-se uma instalação)			
◆ Gerenciador de Coletores (senhas de Serviços de Coletor w/ IP ou DNS e OS)			
◆ Gerenciador de Coletor	☐ : Sim | ☐ : Não	☐ : Proxy | ☐ : Barramento De Mensagem Direto	

	Variável de configuração	
	◆ IP: ◆ Sistema Operacional:	◆ Porta de barramento de mensagem: ◆ Porta proxy do Sentinel Control Center: ◆ Nome de host do Servidor de Comunicação: ◆ Porta de autenticação do Certificado do Gerenciador de Coletor:
10.	Consultor (opcional)	
	Instalado em algumas máquinas como DAS?	☐ : Sim | ☐ : Não
	◆ Download do Consultor:	☐ : Independente | ☐ : Download Direto da Internet
	◆ Local do arquivo de alimentação de dados	
	◆ Endereço de do Consultor	
	◆ Endereço para do Consultor	
	◆ Nome de usuário e senha	u/n:
11.	Locais de arquivo do banco de dados:	
	◆ Arquivos de dados	
	◆ Arquivos de índice	
	◆ Arquivos de dados de resumo	
	◆ Arquivos de índice de resumo	
	◆ Arquivos de registro	
12.	Tamanho do banco de dados:	
	◆ Padrão (20 GB)	
	◆ Grande (400 GB)	
	◆ Personalizado (tamanho)	
13.	SMTP Server	
	(DNS ou IP)	
14.	Para autenticação SQL (senhas)	
	◆ esecadm	PW:
	◆ esecapp	PW:
	◆ esecdba	PW:
	◆ esecrpt	PW:

	Variável de configuração			
15.	Para autenticação do Windows (senhas)			
	◆ DBA (login)	u/n:		
	◆ Usuário do aplicativo (login e senha)	u/n:		PW:
	◆ Administrador do Sentinel (login)	u/n:		
	◆ Usuário de Geração de Relatórios do Sentinel (login)	u/n:		
	Instalação do Crystal			
1.	Versão do Crystal:			
	Sistema Operacional			
	DB			
	Crystal Server (IP ou DNS)			
	Microsoft SQL (Opcional, mas recomendado)	Versão do Microsoft SQL:		
		Patch do Microsoft SQL:		
		senha sa ou portador de senha		
	IP:	u/n:	PW:	Sistema Operacional:
2.	Crystal Reports			
	Tipo de Relatório	☐ : SQL	☐ : Oracle	
	◆ Todos os relatórios publicados	☐ : Sim | ☐ : Não		
	◆ Relatórios configurados no SCC	☐ : Sim | ☐ : Não		