

# Novell Sentinel

6.0

Apr. 30, 2007

第 1 卷 - 安装指南

[www.novell.com](http://www.novell.com)



Novell®

## 法律声明

Novell, Inc. 对本文档的内容或使用不作任何声明或保证，特别是对适销性或用于任何特定目的的适用性不作任何明示或暗示保证。另外，Novell, Inc. 保留随时修改本出版物及其内容的权利，并且没有义务将这些修改通知任何个人或实体。

Novell, Inc. 对任何软件不作任何声明或保证，特别是对适销性或用于任何特定目的的适用性不作任何明示或暗示保证。另外，Novell, Inc. 保留随时修改 Novell 软件全部或部分内容的权利，并且没有义务将这些修改通知任何个人或实体。

依据本协议提供的任何产品或技术信息都将受到美国出口控制和其他国家 / 地区的贸易法律的约束。您同意遵守所有出口控制法规，并同意在出口、再出口或进口可交付产品之前取得所有必要的许可证或分类证书。您同意不出口或再出口至当前美国出口排除列表上所列的实体，或者美国出口法律中规定的任何被禁运的国家 / 地区或支持恐怖主义的国家 / 地区。您同意不将可交付产品用于禁止的核武器、导弹或生物化学武器等终端用途。有关出口 Novell 软件的详细信息，请访问 [Novell International Trade Services 万维网页面 \(http://www.novell.com/info/exports/\)](http://www.novell.com/info/exports/)。如果您未能获得任何必要的出口许可，Novell 对此不承担任何责任。

版权所有 © 2007 Novell, Inc. 保留所有权利。未经出版商的明确书面许可，不得复制、影印、传送此出版物的任何部分或将其储存在检索系统上。

Novell, Inc. 对本文档中介绍的产品中所包含的相关技术拥有知识产权。特别是，这些知识产权包括但不限于 [Novell Legal Patents 万维网页面 \(http://www.novell.com/company/legal/patents/\)](http://www.novell.com/company/legal/patents/) 中列出的一项或多项美国专利，以及美国和其他国家 / 地区的一项或多项其他专利或正在申请的专利。

Novell, Inc.  
404 Wyman Street, Suite 500  
Waltham, MA 02451  
U.S.A.  
[www.novell.com](http://www.novell.com)

*联机文档:* 要访问该 Novell 产品及其他 Novell 产品的最新联机文档，请参见 [Novell 文档万维网网页 \(http://www.novell.com/documentation/\)](http://www.novell.com/documentation/)。

## **Novell 商标**

有关 Novell 商标，请参见 [Novell 商标和服务标记列表 \(http://www.novell.com/company/legal/trademarks/tmlist.html\)](http://www.novell.com/company/legal/trademarks/tmlist.html)。

## **第三方资料**

所有第三方商标均属其各自所有者的财产。



# 目录

前言	9
<b>1 介绍</b>	<b>11</b>
1.1 Sentinel 概述	11
1.1.1 Sentinel 服务器	13
1.1.2 Sentinel 通讯服务器	13
1.1.3 Correlation Engine	13
1.1.4 iTRAC 工作流程	13
1.1.5 Sentinel 数据库	13
1.1.6 Sentinel 收集器管理器	13
1.1.7 Sentinel 收集器	13
1.1.8 Sentinel 控制中心	14
1.1.9 Sentinel 收集器构建器	14
1.1.10 Sentinel 数据管理器	14
1.1.11 Crystal Reporting Server	15
1.1.12 Sentinel 顾问	15
1.1.13 第三方集成	15
1.2 语言支持	15
1.3 其它 Novell 参考	16
1.4 联系 Novell	16
<b>2 最佳实践</b>	<b>17</b>
2.1 支持的平台	17
2.1.1 操作系统	17
2.1.2 数据库	17
2.1.3 报告服务器	18
2.1.4 受支持的堆栈	18
2.2 硬件建议	18
2.2.1 体系结构	19
2.3 性能基准测试	22
2.3.1 论证或演示配置	22
2.3.2 生产系统配置 - 选项 1	23
2.3.3 生产系统配置 - 选项 2	24
2.4 磁盘阵列配置	25
2.4.1 企业安装 (1000 EPS 或以上) 的最低要求	25
2.4.2 最佳配置	25
2.4.3 Microsoft SQL 安装的存储配置示例	26
2.4.4 Oracle 安装的存储配置示例	27
2.5 网络配置	27
2.6 最佳实践 - 数据库安装 / 配置	28
2.6.1 Sentinel 数据库增补程序	28
2.6.2 为 Oracle 推荐的 UNIX 内核设置	28
2.6.3 创建您自己的数据库实例时配置参数	29
2.7 Sentinel 安装和配置	31
2.8 设置口令 - 最佳实践	32
2.9 “Reporting Configuration”	32
2.9.1 Sentinel 提供的报告	33
2.9.2 开发自定义 Crystal Reports 时的提示	34
2.10 数据库维护	34

2.10.1	数据库中的事件信息	34
2.10.2	数据库中的其他信息	34
2.10.3	其他数据库维护	35
2.10.4	Oracle 数据库运行状况检查	36
2.10.5	数据库维护	37
2.11	Correlation Engine	37
2.11.1	时间同步	37
2.11.2	内存使用	38
2.11.3	短路分析	38
2.11.4	自由格式的规则	38
2.12	Sentinel 日志文件	38
<b>3</b>	<b>安装 Sentinel 6</b>	<b>39</b>
3.1	在 Linux、Solaris 和 Windows 上安装 Sentinel	39
3.1.1	Sentinel 配置	39
3.1.2	安装 Sentinel 6.0 的先决条件	41
3.2	在 Linux、SUSE Linux、Redhat Linux 和 Solaris 上安装 Oracle	43
3.2.1	设置内核值	44
3.2.2	为 Solaris 上的 Oracle 创建组和用户帐户	45
3.2.3	为 Solaris 上的 Oracle 设置环境变量	45
3.2.4	验证 Solaris 布局	46
3.2.5	安装 Oracle	46
3.3	安装 Sentinel	52
3.3.1	简单安装	52
3.3.2	自定义安装	54
3.4	安装后配置	63
3.4.1	更新用于 SMTP 鉴定的 Sentinel 电子邮件	64
3.4.2	Sentinel 数据库	64
3.4.3	收集器服务	65
3.4.4	更新许可证密钥（通过评估密钥）	65
<b>4</b>	<b>顾问配置</b>	<b>67</b>
4.1	Advisor 概述	67
4.2	安装顾问	67
4.2.1	独立配置	68
4.2.2	直接从因特网下载配置	68
4.3	Advisor 报告	69
4.3.1	Advisor 报告配置	69
4.4	更新顾问表中的数据	70
4.5	重设置顾问口令（仅限直接下载）	70
<b>5</b>	<b>测试安装</b>	<b>71</b>
5.1	测试安装	71
5.2	通过测试进行清理	80
5.3	入门	80
<b>6</b>	<b>升级到 Sentinel 6</b>	<b>81</b>
6.1	从 Sentinel 5.x 升级到 Sentinel 6.0	81
6.2	从 Sentinel 4.x 升级到 Sentinel 6.0	82

<b>7</b>	<b>安装 Sentinel 部件</b>	<b>85</b>
7.1	在 Sentinel 计算机上安装新部件	85
7.1.1	安装 Sentinel 数据库	87
<b>8</b>	<b>通讯层 (iSCALE)</b>	<b>91</b>
8.1	SSL 代理和直接通讯	92
8.1.1	Sentinel 控制中心	92
8.1.2	收集器管理器	93
8.2	加密密钥更改	95
8.2.1	Advisor 口令更改	95
<b>9</b>	<b>用于 Windows 的 Crystal Reports</b>	<b>97</b>
9.1	概述	98
9.2	系统要求	98
9.3	配置要求	99
9.3.1	安装 Microsoft Internet 信息服务 (IIS) 和 ASP.NET	100
9.4	已知问题	100
9.5	使用 Crystal Reports	100
9.6	安装概述	101
9.6.1	使用 Windows 鉴定执行 Microsoft SQL 2005 Server 安装概述	101
9.6.2	使用 SQL Server 鉴定执行 Microsoft SQL 2005 Server 安装概述	101
9.6.3	Oracle 安装概述	102
9.7	安装	102
9.7.1	使用 Windows 鉴定安装 Crystal Server for Microsoft SQL 2005 Server	102
9.7.2	使用 SQL 鉴定安装 Crystal Server for Microsoft SQL 2005 Server	107
9.7.3	安装 Crystal Server for Oracle	111
9.8	所有鉴定和配置的配置	113
9.8.1	映射 Crystal Reports, 使之可以与 Sentinel 一起使用	113
9.8.2	设置“命名用户”帐户	117
9.8.3	配置报告权限	118
9.8.4	禁用 Sentinel 的前 10 个报告	119
9.8.5	提高 Crystal Enterprise Server 报告刷新记录限制	120
9.8.6	将 Sentinel 控制中心配置为与 Crystal Enterprise Server 集成	120
<b>10</b>	<b>用于 Linux 的 Crystal Reports</b>	<b>123</b>
10.1	使用 Crystal Reports	124
10.2	配置	124
10.3	安装	124
10.3.1	Crystal BusinessObjects Enterprise™ XI 的预安装	124
10.3.2	安装 Crystal BusinessObjects Enterprise™ XI	126
10.3.3	为 Crystal Reports 安装增补程序, 使之可以与 Sentinel 一起使用	127
10.4	发布 Crystal Report 模板	128
10.4.1	发布报告模板 – Crystal 发布向导	128
10.4.2	发布报告模板 – 中央管理控制台	130
10.5	使用 Crystal XI 万维网服务器	131
10.5.1	测试万维网服务器的连接性	131
10.6	设置“命名用户”帐户	131
10.7	配置报告权限	132
10.8	启用 Sentinel 的前 10 个报告	132
10.9	提高 Crystal Enterprise Server 报告刷新记录限制	133
10.10	将 Sentinel 控制中心配置为与 Crystal Enterprise Server 集成	134

10.11 实用程序和查错 . . . . .	135
10.11.1 启动 MySQL . . . . .	135
10.11.2 启动 Tomcat . . . . .	135
10.11.3 启动 Crystal Server . . . . .	135
10.11.4 Crystal 主机名错误 . . . . .	135
10.11.5 无法连接到 CMS . . . . .	136
<b>11 卸载 Sentinel . . . . .</b>	<b>137</b>
11.1 卸载 Sentinel . . . . .	137
11.1.1 在 Solaris 和 Linux 上进行卸载 . . . . .	137
11.1.2 在 Windows 上卸载 . . . . .	138
11.1.3 使用“控制面板”卸载 . . . . .	138
11.2 后卸载 . . . . .	139
11.2.1 Sentinel 数据文件 . . . . .	139
11.2.2 Sentinel 设置 . . . . .	140
<b>A 安装前调查问卷 . . . . .</b>	<b>145</b>
<b>B 在包含 Oracle 的 Linux 上安装 Sentinel 的记录 . . . . .</b>	<b>147</b>
<b>C 在包含 Oracle 的 Solaris 上安装 Sentinel 的记录 . . . . .</b>	<b>151</b>
<b>D 在包含 Microsoft SQL Server 的 Windows 上安装 Sentinel 的记录 . . . . .</b>	<b>155</b>



# 前言

Sentinel 技术文档是通用操作和参考指南。本文档供信息安全专业人员使用。本文档旨在为 Sentinel 企业安全管理系统提供参考资料。在 Sentinel 的入口网站上还提供了其它文档。

Sentinel 技术文档共分五卷，每卷内容各不相同。它们是：

- ◆ 第一卷 - 《Sentinel™ 安装指南》
- ◆ 第二卷 - 《Sentinel™ 用户指南》
- ◆ 第三卷 - 《Sentinel™ 收集器用户指南》
- ◆ 第四卷 - 《Sentinel™ 用户参考指南》
- ◆ 第五卷 - 《Sentinel™ 第三方集成》

## 第一卷 - 《Sentinel 安装指南》

本指南说明如何安装：

- 
- |                            |           |
|----------------------------|-----------|
| ◆ Sentinel 服务器             | ◆ 收集器构建程序 |
| ◆ Sentinel 控制台             | ◆ 收集器管理器  |
| ◆ Sentinel 关联引擎            | ◆ Advisor |
| ◆ Sentinel Crystal Reports |           |
- 

## 第二卷 - 《Sentinel 用户指南》

本指南探讨：

- 
- |                    |             |
|--------------------|-------------|
| ◆ Sentinel 控制台操作   | ◆ 事件的业务相关配置 |
| ◆ Sentinel 功能      | ◆ 映射服务      |
| ◆ Sentinel 体系结构    | ◆ 历史报告      |
| ◆ Sentinel 通讯      | ◆ 收集器主机管理   |
| ◆ 关闭 / 启动 Sentinel | ◆ 事件        |
| ◆ 漏洞评估             | ◆ 案例        |
| ◆ 事件监视             | ◆ 用户管理      |
| ◆ 事件过滤             | ◆ 工作流程      |
| ◆ 事件关联性            |             |
| ◆ Sentinel 数据管理器   |             |
- 

## 第三卷 - 《收集器用户指南》

本指南探讨：

- 
- ◆ 收集器构建程序操作
  - ◆ 收集器管理器
  - ◆ 收集器
  - ◆ 收集器主机管理
  - ◆ 构建和维护收集器
- 

## 第四卷 - 《Sentinel 用户参考指南》

本指南探讨：

- 
- ◆ 收集器脚本编写语言
  - ◆ 收集器分析命令
  - ◆ 收集器管理员功能
  - ◆ 收集器和 Sentinel 元标签
  - ◆ 用户许可权限
  - ◆ Sentinel 关联引擎
  - ◆ 关联命令行选项
  - ◆ Sentinel 数据库纲要
- 

## 第五卷 - 《Sentinel 第三方集成指南》

- 
- ◆ Remedy
  - ◆ HP OpenView 操作
  - ◆ HP Service Desk
-

本章包含下列主题：

- ◆ [Sentinel 概述](#)（第 11 页）
- ◆ [Sentinel 通讯服务器](#)（第 13 页）
- ◆ [Correlation Engine](#)（第 13 页）
- ◆ [iTRAC 工作流程](#)（第 13 页）
- ◆ [Sentinel 收集器管理器](#)（第 13 页）
- ◆ [Sentinel 收集器](#)（第 13 页）
- ◆ [Sentinel 控制中心](#)（第 14 页）
- ◆ [Sentinel 收集器构建器](#)（第 14 页）
- ◆ [Sentinel 数据管理器](#)（第 14 页）
- ◆ [Crystal Reporting Server](#)（第 15 页）
- ◆ [Sentinel 顾问](#)（第 15 页）
- ◆ [第三方集成](#)（第 15 页）
- ◆ [语言支持](#)（第 15 页）

本指南为您介绍基本安装的全过程。《Sentinel 用户指南》更详细地介绍了体系结构、操作以及管理过程。

本指南假定您熟悉网络安全、数据管理以及 Windows 和 UNIX 操作系统。

## 1.1 Sentinel 概述

Sentinel™ 是一个安全性信息和事件管理解决方案，从企业中的许多信息源接收信息，将信息标准化，确定信息的优先级，然后将信息提供给您，以便作出与威胁、风险和策略有关的决定。

Sentinel 自动执行日志收集、分析和报告流程，以确保 IT 控件是有效的，满足威胁检测和审计的要求。Sentinel 将这些劳动密集型的手动流程转化为对安全性事件和遵从性事件的自动、连续的监视和 IT 控制。

Sentinel 从组织的整个网络基础设施以及第三方系统、设备和应用程序中收集安全性信息和非安全性信息，并对其进行关联。Sentinel 以可读性更好的 GUI 的形式来呈现所收集的数据，确定安全性或遵从性问题，跟踪修正措施，从而优化以前容易出错的流程并构建一个更加强化和安全的管理程序。

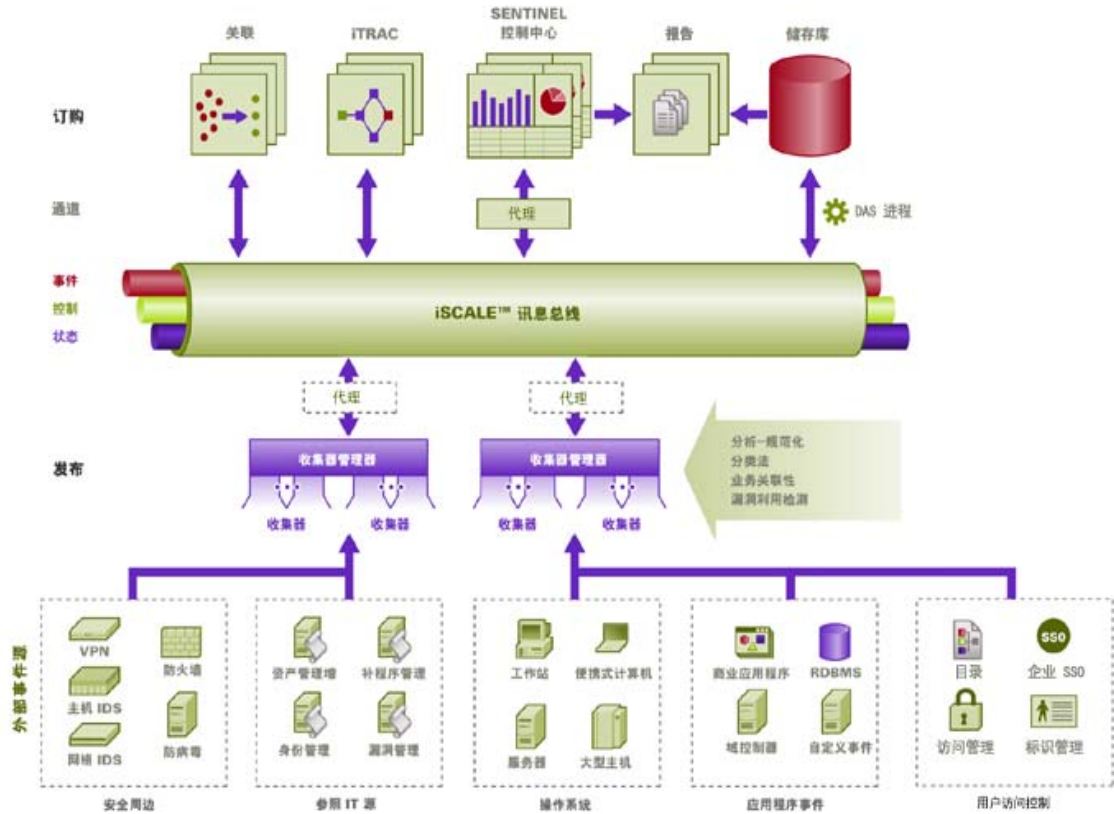
通过自动的事件响应管理，Sentinel 可以记录并规范化对事件和策略违规进行跟踪、升级和响应的整个流程，并提供与故障标记系统的双向集成。Sentinel 使您可以迅速作出反应，有效地处理事件。

使用 Sentinel，您可以获得：

- ◆ 集成的自动化实时安全性管理和遵从性监视功能（覆盖所有系统和网络）
- ◆ 使业务策略可以推动 IT 策略和行动的框架

- ◆ 对企业中的安全性事件、系统事件和访问事件进行自动存档和报告的功能
- ◆ 内置的事件管理和补救功能
- ◆ 证明和监视对内部策略和政府法规（Sarbanes-Oxley、HIPAA、GLBA、FISMA 以及其他法规）的遵从性的功能

以下是 Sentinel 的总体体系结构，其中说明了执行安全管理所涉及的部件。



Sentinel 由多个部件组成：

- ◆ Sentinel 服务器
- ◆ Sentinel 通讯服务器
- ◆ Correlation Engine
- ◆ iTRAC
- ◆ Sentinel 数据库
- ◆ Sentinel 收集器管理器
- ◆ Sentinel 收集器
- ◆ Sentinel 控制中心
- ◆ Sentinel 收集器构建器
- ◆ Sentinel 数据管理器
- ◆ Crystal Report Server
- ◆ Sentinel 顾问

- ◆ 第三方集成
  - ◆ HP OpenView 操作
  - ◆ HP Service Desk
  - ◆ Remedy

### 1.1.1 Sentinel 服务器

Sentinel 服务器由多个部件组成，这些部件执行核心事件处理服务。其中包括：从收集器管理器接收事件，将事件存储在数据库中，过滤、处理活动视图显示，执行数据库查询并处理结果，管理管理性任务（例如用户鉴定和授权）

### 1.1.2 Sentinel 通讯服务器

iSCALE 讯息总线可以在一秒钟内在 Sentinel 部件之间移动数千个讯息数据包。这样可以独立地扩展或缩减部件，并与外部应用程序进行基于标准的集成。

### 1.1.3 Correlation Engine

关联通过自动分析传入事件流来查找所需的模式，从而提高安全性事件管理的智能水平。关联功能允许您定义用于确定严重威胁以及复杂攻击模式的规则，以便确定事件的优先级并进行有效的事件管理和响应。

### 1.1.4 iTRAC 工作流程

Sentinel 提供了 iTRAC 工作流程管理系统，用于定义并自动化事件响应流程。可以将 Sentinel 中通过关联规则标识的事件或手动标识的事件与 iTRAC 工作流程关联。

### 1.1.5 Sentinel 数据库

Sentinel 产品基于存储安全性事件以及所有 Sentinel 元数据的后端数据库构建。事件以规范化的形式与资产和漏洞数据、身份信息、事件和工作流程状态以及许多其他类型的数据存储在一起。

### 1.1.6 Sentinel 收集器管理器

收集器管理器可以管理收集器、监视系统状态讯息以及根据需要执行事件过滤。收集器管理器的主要功能包括：转换事件，通过分类为事件添加业务相关性，对事件执行全局过滤，路由事件，将运行状况讯息发送到 Sentinel 服务器。

Sentinel 收集器管理器可以直接连接到讯息总线，也可以使用 SSL 代理。

### 1.1.7 Sentinel 收集器

Sentinel 从源设备收集数据，在对事件进行关联和分析并发往数据库之前，通过将分类、不正当利用检测和业务相关性注入数据流，从而提供更丰富的事件流。更丰富的事件流意味着数据已与所需业务环境相关联，从而可确定并清除内部或外部的威胁以及违反策略的情况。

Sentinel 收集器可以分析来自下列设备类型的数据：

入侵检测系统 ( 主机 )	反病毒软件
入侵检测系统 ( 网络 )	万维网服务器
防火墙	数据库
操作系统	大型主机
策略监视	漏洞评估
鉴定	目录服务
路由器和交换机	网络管理
VPN	专有系统

可以从 [Novell 产品站点 \(http://support.novell.com/products/sentinel/collectors.html\)](http://support.novell.com/products/sentinel/collectors.html) 下载现有的设备特定的收集器。可以在 **Collector Builder** 中构建或修改收集器，Collector Builder 是 Sentinel 系统附带的一个独立应用程序。

### 1.1.8 Sentinel 控制中心

Sentinel 控制中心提供了一个集成的安全管理仪表盘，分析人员利用此仪表盘提供的信息，可以快速确定新的趋势或攻击、处理实时图形信息并与之交互，以及对事件做出响应。

Sentinel 控制中心的主要功能包括：

- ◆ 活动视图：实时分析和显示
- ◆ 事件：事件的创建和管理
- ◆ 管理：关联规则的定义和管理
- ◆ iTRAC：用于记录、执行和跟踪事件解决流程的流程管理
- ◆ 报告：历史报告和度量标准
- ◆ 事件源管理：收集器的部署和监视

### 1.1.9 Sentinel 收集器构建器

使用 Sentinel Collector Builder 可以构建收集器。可以创建和自定义模板，以便收集器可以分析数据。

### 1.1.10 Sentinel 数据管理器

使用 Sentinel 数据管理器 (SDM) 可以管理 Sentinel 数据库。可以在 SDM 中执行下列操作：

- ◆ 监视数据库空间的利用率
- ◆ 查看和管理数据库分区
- ◆ 管理数据库存档
- ◆ 将数据导入数据库
- ◆ 配置数据映射
- ◆ 配置事件标记名
- ◆ 配置摘要报告设置

## 1.1.11 Crystal Reporting Server

Sentinel 控制中心中全面的报告服务通过利用 Business Objects™ 的 Crystal Enterprise Server 而得到增强。Sentinel 附带了预定义的报告，可以满足组织在监视其安全性和遵从性状态时的常见报告需求。还可以使用 Crystal Report Developer，根据 Sentinel 发布的报告视图纲要开发新的自定义报告。

## 1.1.12 Sentinel 顾问

Sentinel 顾问是一个可选装的扩充模块，该模块在 Sentinel 实时警报数据和已知的漏洞与补救信息之间进行交叉参照。

## 1.1.13 第三方集成

Sentinel 使用第三方 API 插件与下列系统集成：

- ◆ HP OpenView 操作
- ◆ HP Service Desk
- ◆ Remedy AR

## 1.2 语言支持

Sentinel 部件已本地化为下列语言：

- ◆ 英语
- ◆ 葡萄牙语（巴西）
- ◆ 法语
- ◆ 意大利语
- ◆ 德语
- ◆ 西班牙语
- ◆ 日语
- ◆ 繁体中文
- ◆ 简体中文

存在下列几种例外情况：

- ◆ 尽管可以在上述非英文版操作系统上运行 Collector Builder 界面和脚本，但是它们均只有英文版。
- ◆ 目前，收集器管理器只能处理 ASCII 数据和扩展 ASCII 数据（即不能处理双字节数据或 Unicode 数据）。
- ◆ Novell 构建的收集器用于分析英文事件。
- ◆ 内部事件（用于审计 Sentinel 操作）只有英文版。

## 1.3 其它 Novell 参考

Novell 文档站点 (<http://www.novell.com/documentation/>) 上提供下列手册:

- ◆ Sentinel 安装指南
- ◆ 《Sentinel 用户指南》
- ◆ Sentinel Collector Builder 用户指南
- ◆ Sentinel 用户参考指南
- ◆ Sentinel 第三方集成指南
- ◆ 版本发行说明

## 1.4 联系 Novell

- ◆ 万维网站点: <http://www.novell.com> (<http://www.novell.com>)
- ◆ Novell 技术支持: [http://support.novell.com/phone.html?sourceidint=suplnav4\\_phonesup](http://support.novell.com/phone.html?sourceidint=suplnav4_phonesup) ([http://support.novell.com/phone.html?sourceidint=suplnav4\\_phonesup](http://support.novell.com/phone.html?sourceidint=suplnav4_phonesup))
- ◆ 自助支持: [http://support.novell.com/support\\_options.html?sourceidint=suplnav\\_supportprog](http://support.novell.com/support_options.html?sourceidint=suplnav_supportprog) ([http://support.novell.com/support\\_options.html?sourceidint=suplnav\\_supportprog](http://support.novell.com/support_options.html?sourceidint=suplnav_supportprog))
- ◆ 增补程序下载站点: <http://download.novell.com/index.jsp> (<http://download.novell.com/index.jsp>)
- ◆ 24x7 全天候支持: <http://www.novell.com/offices> (<http://www.novell.com/offices>)



本章包含下列主题：

- ◆ 支持的平台（第 17 页）
- ◆ 受支持的堆栈（第 18 页）
- ◆ 硬件建议（第 18 页）
- ◆ 性能基准测试（第 22 页）
- ◆ 最佳实践 - 数据库安装 / 配置（第 28 页）
- ◆ 设置口令 - 最佳实践（第 32 页）
- ◆ 数据库维护（第 34 页）
- ◆ 内存使用（第 38 页）

本章讨论最佳做法和建议，以充分利用 Sentinel，其中包括下列主题：

## 2.1 支持的平台

Sentinel 部件应始终安装在 Novell 支持的平台上。在出版本指南时，下列平台支持 Sentinel。有关更新的信息（如果有），请查阅 <http://www.novell.com/documentation> (<http://www.novell.com/documentation>) 上的联机文档，以获取更新。

### 2.1.1 操作系统

已证明 Sentinel 部件（包括数据库）可以在下列操作系统上运行：

- ◆ SuSE Linux Enterprise Server 9 SP2 和 SP3
- ◆ SuSE Linux Enterprise Server 10（2006 年 7 月 1 日的增补程序）
- ◆ Red Hat Enterprise Linux 3 Update 5 ES (x86)
- ◆ Sun Solaris 9（推荐的增补程序集日期：2005 年 5 月 3 日）
- ◆ Sun Solaris 10
- ◆ Windows 2003 标准版或企业版 SP1
- ◆ Windows XP SP1（仅对于 Sentinel 控制中心、Collector Builder 和 Sentinel 数据管理器）
- ◆ Windows 2000 SP4 标准版或企业版（仅对于 Sentinel 控制中心、Collector Builder 和 Sentinel 数据管理器）

### 2.1.2 数据库

已证明 Sentinel 可以与下列数据库一起运行：

- ◆ Oracle 10g 企业版（版本 10.2.0.3，包含 Oracle 关键增补程序 #5881721）
- ◆ Oracle 9i 企业版（版本 9.2.0.7，包含增补程序 5490841）
- ◆ Microsoft SQL Server 2005 SP1 32 位（版本 9.00.2047）标准版或企业版
- ◆ Microsoft SQL Server 2005 64 位（版本 9.00.2047）标准版或企业版

---

**注释：**所有数据库都应安装在数据库供应商和 Novell 均认可的操作系统上，以便与 Sentinel 部件一起使用。Oracle 必须在 Linux 或 Solaris（而不是 Windows）上运行。

---

### 2.1.3 报告服务器

受支持的报告服务器软件是 Crystal Enterprise Server XI R2，该软件可以在 Sentinel 环境中的下列任意平台上运行：

- ◆ Windows 2003 SP1 Server 标准版或企业版
  - ◆ Microsoft SQL 2005 上的 Crystal 数据库
- ◆ Red Hat Enterprise Linux 3 Update 5 ES (x86)
  - ◆ MySQL 上的 Crystal 数据库
- ◆ SuSE Linux Enterprise Server 9 SP2 (x86)
  - ◆ MySQL 上的 Crystal 数据库

### 2.1.4 受支持的堆栈

Novell 支持将 Sentinel 部件安装在任何受支持的操作系统上，该环境可以混用多种操作系统（Linux、Solaris 和 Windows），例外情况和警告如下：

- ◆ Collector Builder - 只能在 Windows 平台上运行。
- ◆ Crystal Enterprise Server
  - ◆ 不能在 Solaris 上运行
  - ◆ 在 Sentinel 环境中，不能在 Windows 2000 上运行
  - ◆ 在 Sentinel 环境中，不能与 MSDE 数据库一起运行
- ◆ 数据库
  - ◆ 如果 Sentinel 服务器在 Windows 上运行，则必须是 SQL Server
  - ◆ 如果 Sentinel 服务器在 Linux 或 Solaris（而不是 Windows）上运行，则必须是 Oracle
  - ◆ Sentinel 环境中不支持在 Windows 上运行 Oracle
- ◆ 数据访问服务 (DAS)
  - ◆ 如果 DAS 安装在混合环境中，其中 DAS 在 Windows 上运行，而数据库是 Oracle，或 DAS 在 UNIX 或 Linux 上运行，而数据库是 SQL Server，则不能使用 Windows 鉴定。

## 2.2 硬件建议

如果安装在 Linux 或 Windows 上，Sentinel 服务器和数据库部件可以在 x86（32 位）或 x86-64（64 位）硬件（包括 AMD Opteron 和 Intel Xeon 硬件）上运行。不支持 Itanium 服务器。

对于 Solaris，支持 SPARC 体系结构。

## 2.2.1 体系结构

Sentinel 的体系结构具有良好的可伸缩性，如果预计事件发生率较高，可以将部件分布到多台计算机上，以获得最佳的系统性能。

在设计 Sentinel 系统时应考虑许多因素。以下是在开发设计时要考虑的部分因素的列表：

- ◆ 事件发生率（每秒发生的事件数，即 EPS）
- ◆ 事件源的地理位置 / 网络位置以及网络之间的带宽
- ◆ 可用硬件
- ◆ 首选的操作系统
- ◆ 规划未来的可伸缩性
- ◆ 预计的事件过滤量
- ◆ 本地数据保留策略
- ◆ 所需的关联规则数和复杂程度
- ◆ 预计每天发生的事件数
- ◆ 预计每天管理的工作流程数
- ◆ 登录到系统的用户数
- ◆ 漏洞和资产基础结构

Sentinel 系统设计中最重要因素是事件发生率 – 如果事件发生率升高，Sentinel 体系结构中几乎所有部件都将受到影响。在事件发生率较高的环境中，最大的需求产生于数据库，数据库非常依赖于 IO，可能会每秒同时处理数百个或数千个事件的插入、多个用户的对象创建、工作流程更新、通过 Sentinel 控制中心进行的简单历史查询以及来自 Crystal Enterprise Server 的长期报告。因此，Novell 提出以下建议：

- ◆ 数据库不应与其他任何 Sentinel 部件安装在一起。
- ◆ 数据库服务器应专门用于 Sentinel 操作。其他应用程序（或 ETL 流程）可能会影响数据库性能。
- ◆ 数据库服务器应配备高速存储阵列，以便根据事件插入率来满足 I/O 需求。
- ◆ 专职的 DBA 应定期评估数据库的下列方面：
  - ◆ 大小
  - ◆ I/O 操作
  - ◆ 磁盘空间
  - ◆ 内存
  - ◆ 索引

在事件发生率较低的环境中（例如  $EPS < 25$ ），因为数据库和其他部件占用的资源较少，可以不必严格遵守上述建议。

本节包含的一些常见硬件建议可以作为 Sentinel 系统设计的指南。通常，设计建议是根据事件发生率范围而得出的。但是，这些建议基于下列假设：

- ◆ 事件发生率处于 EPS 范围的上限。
- ◆ 平均事件大小是 600 个字节。
- ◆ 所有事件均存储在数据库中（即没有任何删除事件的过滤器）。

- ◆ 30 天内的数据将联机存储在数据库中。
- ◆ 下列规格不包括用于 Advisor 数据的存储空间。
- ◆ 默认情况下， Sentinel 服务器将 5 GB 的磁盘空间用于临时超速缓存无法插入数据库的事件数据。
- ◆ 默认情况下， Sentinel 服务器还将 5 GB 的磁盘空间用于存储无法写入聚合事件文件的事件。

根据不同的实现方式， Sentinel 实现的硬件建议也会有所不同，所以，建议在确定 Sentinel 体系结构之前，先向 Novell 咨询服务部门进行咨询。下列建议可以作为指南使用。

**注释：**由于高事件负载以及需要本地超速缓存，所以，要求安装 DAS 的 Sentinel 服务器计算机拥有本地或共享的条带型磁盘阵列 (RAID)，并且该阵列至少包含 4 个磁盘主轴。

必须通过单台高速交换机 (GIGE) 将分布式主机连接到其它 Sentinel 服务器主机，以防止出现网络交通量瓶颈。

Novell 建议将 Crystal Enterprise Server 安装在专用的计算机上，数据库较大或报告利用率较高的情况下尤其如此。如果数据库较小，报告利用率较低，并且数据库安装在 Windows 或 Linux 上，则 Crystal 可以与数据库安装在同一台计算机上。

**注释：**在编写本文档时， Sentinel 6.0 仍在开发过程中，所以，下列数字基于对 Sentinel 5.1.3 的测试。有关更新的信息，请参阅 Novell 文档站点 <http://www.novell.com/documentation> (<http://www.novell.com/documentation>)。

1-500 EPS : 2 台计算机的配置 (Sentinel 5.1.3)			
部件	RAM	空格	CPU
计算机 1 : Sentinel 服务器 / 收集器管理器	6 GB	250 GB	Windows 或 Linux - 2 个双核 Intel® Xeon® 5150 (2.66 GHz)
<ul style="list-style-type: none"> <li>◆ Correlation Engine</li> <li>◆ DAS</li> <li>◆ 通讯服务器</li> <li>◆ Advisor</li> <li>◆ 收集器管理器 / 收集器</li> <li>◆ 数据库</li> <li>◆ Crystal Server (对 Windows/Linux 可选)</li> </ul>			或 Sun Solaris - 4 个 UltraSPARC IIIi (1.5 GHz)
计算机 2 : 报告服务器	2 GB	20 GB	Windows 或 Linux - 1 个双核 Intel® Xeon® 5150 (2.66 GHz)
<ul style="list-style-type: none"> <li>◆ Crystal Server</li> </ul>			

500 – 1500 EPS : 3 台计算机的配置 (Sentinel 5.1.3)			
部件	RAM	空格	CPU
计算机 1 : Sentinel 服务器 / 收集器管理器 <ul style="list-style-type: none"> <li>◆ Correlation Engine</li> <li>◆ DAS</li> <li>◆ 通讯服务器</li> <li>◆ Advisor</li> <li>◆ 收集器管理器 / 收集器</li> </ul>	4 GB	40 GB	Windows 或 Linux - 2 个双核 Intel® Xeon® 5160 (3.0 GHz) 或 Sun Solaris - 2 个 1.8 GHz UltraSPARC IV+
计算机 2 : 数据库 <ul style="list-style-type: none"> <li>◆ 数据库</li> <li>◆ Crystal Server (对 Windows/ Linux 可选)</li> </ul>	4 GB+	1 TB+	Windows 或 Linux - 2 个双核 Intel® Xeon® 5160 (3.0 GHz) 或 Sun Solaris - 2 个 1.8 GHz UltraSPARC IV+
计算机 3 : 报告服务器 (只有 Sentinel/ 数据库在 Solaris 上运行时才需要) <ul style="list-style-type: none"> <li>◆ Crystal Server</li> </ul>	2 GB	20 GB	Windows 或 Linux - 1 个双核 Intel® Xeon® 5150 (2.66 GHz)

1500 - 3000 EPS : 4-5 台计算机的配置 (Sentinel 5.1.3)			
部件	RAM	空格	CPU
计算机 1 : Sentinel 服务器 <ul style="list-style-type: none"> <li>◆ Correlation Engine</li> <li>◆ DAS</li> <li>◆ 通讯服务器</li> <li>◆ Advisor</li> </ul>	4 GB	40 GB	Windows 或 Linux - 2 个双核 Intel® Xeon® 5160 (3.0 GHz) 或 Sun Solaris - 2 个 1.8 GHz UltraSPARC IV+
计算机 2 : 数据库 <ul style="list-style-type: none"> <li>◆ 数据库</li> <li>◆ Crystal Server (对 Windows/ Linux 可选)</li> </ul>	8 GB+	3 TB+	Windows 或 Linux - 2 个双核 Intel® Xeon® 5160 (3.0 GHz) 或 Sun Solaris - 2 个 1.8 GHz UltraSPARC IV+
计算机 3 : 收集器管理器 <ul style="list-style-type: none"> <li>◆ 收集器管理器 / 收集器</li> </ul>	2 GB	20 GB	Windows 或 Linux - 2 个双核 Intel® Xeon® 5160 (3.0 GHz) 或 Sun Solaris - 2 个 1.8 GHz UltraSPARC IV+
计算机 4 : 报告服务器 <ul style="list-style-type: none"> <li>◆ Crystal Server</li> </ul>	4 GB	20 GB	Windows 或 Linux - 1 个双核 Intel® Xeon® 5150 (2.66 GHz)

1500 - 3000 EPS : 4-5 台计算机的配置 (Sentinel 5.1.3)			
部件	RAM	空格	CPU
计算机 5 : DAS 部件 ( EPS > 2000 时 需要 )	2 GB	40 GB	Windows 或 Linux - 2 个双核 Intel® Xeon® 5160 (3.0 GHz)  Sun Solaris - 2 个 1.8 GHz UltraSPARC IV+

## 2.3 性能基准测试

下表介绍几种有代表性的配置和测试结果。

这些指标可以作为参照点来确定体系结构设计，并不是硬性限制。在这些测试中，系统负载未超过 75% 的利用率，事件发生率表明性能处于稳定状态。

**注释：**基准测试主要针对 Sentinel 事件插入、关联和映射服务。测试中未涉及其他活动（例如报告或历史数据查询）。

下列所有测试均在采用 4+1 配置的条带型 RAID 5 系统上执行。

### 2.3.1 论证或演示配置

此单计算机配置适合进行演示或有限的论证，可以使用 Sentinel 安装程序中的“简单”选项进行安装。强烈建议您不要在生产系统中使用此配置。

**注释：**在编写本文档时，Sentinel 6.0 仍在开发过程中，所以，下列数字基于对 Sentinel 5.1.3 的测试。有关更新的信息，请参阅 Novell 文档站点 <http://www.novell.com/documentation/index.html> (<http://www.novell.com/documentation/index.html>)。

功能	RAM	MODEL
Sentinel 服务器 + 数据库 + 收集器管理器	5 GB , 5x36GB RAID	SLES9 - 2 个双核 Intel® Xeon® 5150 2.66 GHz

在此系统上观察下列性能指标。

特性	额度数值	注释
每天处理和存储的事件数 ( 在数据库中 )	8600 万	
每秒的事件数 ( 收集器管理器 )	1000	一个 ( 双核 ) Xeon CPU 用于收集器管理器
每秒的事件数 ( 收集器引擎 )	300	此测试使用了 PIX、Snort 以及其它设备
每秒的事件数 (SYSLOG)	300	1 个 Syslog 服务器在配备 1 个引擎的收集器管理器主机上运行
每个收集器管理器部署的收集器数	3	1 个收集器使用 syslog，其他收集器使用文件连接器

特性	额度数值	注释
收集器管理器数	1	20 是每个 Sentinel 服务器支持的最大 CM 数
已部署的关联引擎数	1	在 Sentinel 服务器计算机上运行
每个关联引擎部署的规则数	10	
正在运行的 Active Views™	10	
允许同时使用的用户数	3	
每个 Active View 实例的视图数	2	
已部署的映射数	2	
映射服务中最大映射的大小	1.5 MB	
最大映射中的行数	150 万	

## 2.3.2 生产系统配置 – 选项 1

此配置包括三台计算机，每秒处理大约 2000 个事件。

**注释：**在编写本文档时，Sentinel 6.0 仍在开发过程中，所以，下列数字基于对 Sentinel 5.1.3 的测试。有关更新的信息，请参阅 Novell 文档站点 <http://www.novell.com/documentation/index.html> (<http://www.novell.com/documentation/index.html>)。

功能	RAM	MODEL
Sentinel 服务器	4 GB , 5x36GB RAID	SLES9 - 2 个双核 Intel® Xeon® 5150 2.66 GHz
数据库	4 GB , 5x250GB RAID	SLES9 - 2 个双核 Intel® Xeon® 5150 2.66 GHz
收集器管理器	2 GIG , 72 GIG	SLES9 - 1 个双核 Intel® Xeon® 5150 2.66 GHz

在此系统上观察下列性能指标：

特性	额度数值	注释
每天处理和存储的事件数（在数据库中）	1 亿 7300 万	
每秒的事件数（收集器管理器）	2000	一个（双核）Xeon CPU 用于收集器管理器
每秒的事件数（收集器引擎）	1200	此测试使用了 PIX、Snort 以及其它设备
每秒的事件数 (SYSLOG)	1200	1 个 Syslog 服务器在配备 1 个引擎的收集器管理器主机上运行
每个收集器管理器部署的收集器数	10	1 个利用 syslog 的收集器；其他的收集器使用文件连接器

特性	额度数值	注释
收集器管理器数	1	20 是每个 Sentinel 服务器支持的最大 CM 数
已部署的关联引擎数	1	在 Sentinel 服务器计算机上运行
每个关联引擎部署的规则数	20	
正在运行的 Active Views™	20	
允许同时使用的用户数	5	
每个 Active View 实例的视图数	4	
已部署的映射数	4	
最大映射大小	1.5 MB	
最大映射中的行数	150 万	

### 2.3.3 生产系统配置 – 选项 2

此配置要求有四台计算机，每秒处理大约 3000 个事件。

**注释：**在编写本文档时，Sentinel 6.0 仍在开发过程中，所以，下列数字基于对 Sentinel 5.1.3 的测试。有关更新的信息，请参阅 Novell 文档站点 <http://www.novell.com/documentation/index.html> (<http://www.novell.com/documentation/index.html>)。

功能	RAM	MODEL
Sentinel 服务器	4 GB , 5x36GB RAID	SLES9 - 2 个双核 Intel® Xeon® 5160 3.0 GHz
数据库	8 GB , 5x250GB RAID	SLES9 - 2 个双核 Intel® Xeon® 5160 3.0 GHz
收集器管理器	2 GB, 72 GB	SLES9 - 2 个双核 Intel® Xeon® 5160 3.0 GHz
Sentinel 服务器 ( DAS - 节点 2 )	2 GB , 5x36GB RAID	SLES9 - 2 个双核 Intel® Xeon® 5160 3.0 GHz

在此系统上观察下列性能指标：

特性	额度数值	注释
每天处理和存储的事件数 ( 在数据库中 )	2 亿 6000 万	
每秒的事件数 ( 收集器管理器 )	3000	双 ( 双核 ) Xeon CPU 用于收集器管理器
每秒的事件数 ( 收集器引擎 )	1200	此测试使用了 PIX、Snort 以及其它设备
每秒的事件数 (SYSLOG)	2500	1 个 Syslog 服务器在收集器管理器主机上运行
每个收集器管理器部署的收集器数	10	3 个收集器使用 syslog ; 其他收集器使用文件连接器



特性	额度数值	注释
收集器管理器数	1	
已部署的关联引擎数	1	在 Sentinel 服务器计算机上运行
每个关联引擎部署的规则数	20	
正在运行的 Active Views™	20	
允许同时使用的用户数	5	
每个 Active View 实例的视图数	4	
已部署的映射数	4	
最大映射大小	1.5 MB	
最大映射中的行数	150 万	

## 2.4 磁盘阵列配置

在生产设置中，Novell Sentinel 服务器要求为数据库和 Sentinel 主机配备高速磁盘阵列。本节介绍典型的磁盘 (RAID) 配置建议。下列功能受磁盘硬件性能的影响：

- ◆ 数据库部件 (Microsoft SQL/Oracle)：事件发生率（每秒处理的事件数）和查询功能受到影响（包括“历史事件查询”、“脱机查询”和“Crystal 报告”）。
- ◆ DAS-RT（数据访问服务实时部件）：活动视图功能受到影响。
- ◆ DAS-Aggregation：可激活的摘要数会受到影响。

### 2.4.1 企业安装（1000 EPS 或以上）的最低要求

最低建议使用 RAID 5 配置。RAID 5 可能是最合算的配置。此配置出于成本考虑，其性能和冗余性会稍有不足。请注意，以上建议仅供参考。多数生产性大规模企业系统要求对速度、吞吐量和冗余性需求进行更详细的分析。

- ◆ RAID 组 1 – 数据库（数据、索引、事务日志等）
- ◆ RAID 组 2 – Sentinel 服务器 DAS（数据目录，临时目录\*）
- ◆ 最少磁盘数：每个 RAID 组 13 个磁盘
- ◆ 磁盘类型：12000 以上的 RPM，光纤通道或 SCSI
- ◆ LUN 1（RAID 组 1）：每个磁盘 5GB – 144GB 以上
- ◆ LUN 2（RAID 组 2）：每个磁盘 5GB – 144GB 以上

### 2.4.2 最佳配置

可以利用上述设置的 RAID 1+0 来实现最佳性能和冗余配置。但是，对于某些数据库，遵照上述指南的其他 RAID 组和 LUN 可能需要实现更高的并行度和 I/O。

---

**注释：**有关如何使 DAS TEMP DIR 指向其他位置的更多信息，请参阅 [Sentinel 安装和配置（第 31 页）](#)。

---

### 2.4.3 Microsoft SQL 安装的存储配置示例

本示例使用 EMC2 CLARiiON 储存子系统，配备有：

- ◆ 1 TB 储存空间
- ◆ 60 台驱动器，36 GB，15K RPM

#### RAID 组

阵列	LUN	RAID 类型	RAID 组	大小 (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	RAID 组 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	RAID 组 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	RAID 组 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	RAID 组 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	RAID 组 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	RAID 组 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	RAID 组 6

#### LUN 指派

阵列	LUN	RAID 类型	RAID 组	大小 (GB)	储存处理器	名称
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

## 储存组

阵列	储存组	LUN	主机	驱动器字母	名称
1	Sentinel	0	E2P0 (E3P0)	E:	SQLData1
1	Sentinel	1	E2P0 (E3P0)	F:	SQLData2
1	Sentinel	2	E2P0 (E3P0)	G:	SQLData3
1	Sentinel	3	E2P0 (E3P0)	H:	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 Oracle 安装的存储配置示例

卷 1	RAID 1	Oracle 主目录
卷 2	RAID 1	重做日志成员 a
卷 3	RAID 1	重做日志成员 b
卷 4	RAID 0+1 或 RAID 5	复原和临时表空间
卷 5	RAID 0+1 或 RAID 5	Sentinel 数据表空间
卷 6	RAID 0+1 或 RAID 5	Sentinel 索引表空间
卷 7	RAID 0+1 或 RAID 5	Sentinel 摘要数据表空间
卷 8	RAID 0+1 或 RAID 5	Sentinel 摘要索引表空间
卷 9	RAID 1	存档日志文件

## 2.5 网络配置

Sentinel 服务器端部件：应该用一个 1 GB 的交换机将这些部件相互连接起来。其中包括数据库、通讯服务器、Advisor、基本 Sentinel 服务、关联引擎和 DAS。

Sentinel 控制中心、Collector Builder 和收集器服务（收集器管理器）：要求这些部件通过至少 100Mbit 的全双工交换机连接到 Sentinel 服务器。

## 2.6 最佳实践 - 数据库安装 / 配置

**注释：**在数据库安装完成后，大多数数据库安装参数都可以通过数据库管理工具或命令行更改。

- 1 Sentinel 使用预定义的存档策略来管理迅速增长的表（例如 EVENTS 表）。这些表已分区，可以存档和删除较旧的部分，而不会影响较新的数据。但是，此分区和存档方案不涉及其他表，需要单独进行管理。
- 2 出于性能考虑，如果您是在 RAID 中进行安装并且您的 RAID 环境允许，应该在您可用的写入速度最快的磁盘上安装下列日志。
  - ◆ 重做日志 (Oracle)
  - ◆ 事务日志 (Microsoft SQL)
- 3 为了更精确地确定您的数据库大小，您可能需要先运行一个小型数据库，然后在系统启动并运行一会儿之后再扩展数据库大小。这样您就可以根据事件插入率观察数据库的增长情况，从而确定您的系统数据库的空间需求。
- 4 为了进行恢复，DBA 应定期对数据库中未分区的表执行计划备份。
- 5 对于 Oracle 安装，Sentinel 安装程序默认情况下禁用“存档日志记录”。出于恢复数据库的目的，强烈建议您在安装结束之后先启用存档日志记录功能，然后再开始接收生产事件数据。您还应该定期备份您的存档日志，以释放存档日志目标的空间，否则当存档日志目标上的容量已满时，您的数据库将停止接受事件。
- 6 出于性能考虑，在事件发生率较高的环境中，存储位置应指向不同的位置（例如，不同的磁盘控制器），以避免发送 I/O 争用。
  - ◆ 数据目录
  - ◆ 索引目录
  - ◆ 摘要数据目录
  - ◆ 摘要索引目录
  - ◆ 日志目录（仅限 Microsoft SQL）
  - ◆ 临时和复原表空间目录（仅限 Oracle）
  - ◆ 重做日志成员 A 目录（仅限 Oracle）
  - ◆ 重做日志成员 B 目录（仅限 Oracle）

### 2.6.1 Sentinel 数据库增补程序

下面这种情况仅限于 Microsoft SQL：应用 Sentinel 数据库增补程序时，安装程序将只添加新索引，并且只将其添加到 \*\_P\_MAX。已经存在的分区将不进行更新。如果希望新索引能够提高对现有分区查询的性能，必须手工向已经存在的分区添加索引。

### 2.6.2 为 Oracle 推荐的 UNIX 内核设置

以下是建议的最小值。有关更多信息，请参阅您的系统文档和 Oracle 文档。

## Linux 内核参数下限值

有关如何在 Linux 上查看和设置内核参数的更多信息，请参阅《安装指南》中的第 3 章“安装 Sentinel 6”（第 39 页）。

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

## Solaris 内核参数下限值

在 /etc/system 中检查用于 Oracle 的 UNIX 内核参数并进行以下设置：

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

### 2.6.3 创建您自己的数据库实例时配置参数

如果需要，可以手动（而不是通过 Sentinel 安装程序）创建数据库结构（在表空间级别）。然后，在安装期间，可以选择“向现有数据库中添加数据库对象”选项。以下是创建您自己的数据库实例时的建议设置。您的设置可能会因系统配置和要求的不同而不同。

在 Oracle 实例中需要创建：

- ◆ Oracle 初始化参数（这些值取决于系统大小和配置）
- ◆ Sentinel 所需的表空间配置参数（对于 Solaris 和 Linux）

---

#### 配置参数最小值建议

---

参数	大小（以字节为单位或另行指定）
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	同上
hash_join_enabled	TRUE

---

**配置参数最小值建议**

---

参数	大小（以字节为单位或另行指定）
optimizer_index_caching	50
optimizer_index_cost_adj	55

---

---

**建议的表空间大小下限值**

---

表空间	示例大小	注释
REDO	3 x 100M	此值为最小值。如果 EPS 较高，则应该创建更大的重做日志。
SYSTEM	500M	最小值
TEMP	1G	最小值
UNDO	1G	最小值
ESENTD	5G	最小值 用于事件数据
ESENTD2	500M	最小值 用于配置、资产、漏洞和关联的数据（自动扩展功能启用）
ESENTWFD	250M	用于 iTRAC 数据（自动扩展功能启用）
ESENTWFX	250M	用于 iTRAC 索引（自动扩展功能启用）
ESENTX	3G	最小值 用于事件索引
ESENTX2	500M	最小值 用于配置、资产、漏洞和关联的索引（自动扩展功能启用）
SENT_ADVISORD	200M	最小值 用于顾问数据（自动扩展功能启用）
SENT_ADVISORX	100M	最小值 用于顾问索引（自动扩展功能启用）
SENT_LOBS	100M	最小值 用于大型数据库对象（自动扩展功能启用）
SENT_SMRYD	3G	最小值 用于汇总、摘要数据
SENT_SMRYX	2G	最小值 用于汇总、摘要索引

---

## 2.7 Sentinel 安装和配置

安装 Sentinel 时，出于性能和备份的原因，应考虑到以下情况。

- 1 如果在进行 Sentinel 全新安装时已安装有早期版本的 Sentinel，强烈建议您去除以前安装的某些文件和系统设置。如不去除这些文件，可能会导致全新安装失败。在进行全新安装的每一台计算机上都应执行此操作。有关要去除的文件的更多信息，请参阅《安装指南》中的第 11 章“卸装 Sentinel”（第 137 页）。
- 2 将 DAS\_RT 和 DAS\_Query 流程的临时目录指向速度较快的磁盘（例如磁盘阵列），可以显著提高活动视图和映射的性能。要将这些进程的临时目录指向某个快速磁盘，请在安装 DAS 的计算机上执行以下操作：

**2a** 在快速磁盘上创建放置临时文件的目录。如果是在 UNIX 上，Sentinel 管理员用户以及组 esec 必须拥有此目录，并且可对其执行写操作。

**2b** 备份 %ESEC\_HOME%\config\configuration.xml 文件。

**2c** 在文本编辑器中打开文件 %ESEC\_HOME%\config\configuration.xml。

**2d** 对于 DAS\_RT 和 DAS\_Query 进程，添加 JVM 自变量 java.io.tmpdir，并将其设置为刚才创建的目录。

**2e** 要对 DAS\_RT 进程进行此项更改，请查找包含文本

```
-Dsrv_name=DAS_RT
```

的行，并在其后添加参数（如下所述）。

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

下面是该行的一个示例（您的 -Xmx、-Xms 和 -XX 自变量可能有所不同）：

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

**2f** 要对 DAS\_RT 进程进行此项更改，请查找包含文本

```
-Dsrv_name=DAS_Query
```

的行，并在其后添加参数（如下所述）。

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

下面是该行的一个示例（您的 -Xmx、-Xms 和 -XX 自变量可能有所不同）：

```
<process component="DAS" image="&quot;$(ESEC_JAVA_HOME)/
java&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 &quot;$(ESEC_HOME)/bin/stop_container.bat&quot; localhost
DAS_Query" working_directory="$(ESEC_HOME)/bin"/>
```

## 2.8 设置口令 – 最佳实践

### 满足常用条件认证所要求的严格的安全性配置:

- 1 选择的口令长度至少为 8 个字符，其中至少包括一个大写字母、一个小写字母、一个特殊符号 (!@#\$%^&\*()\_+) 以及一个数字 (0-9)。
- 2 请不要在口令中包含您的电子邮件名称或您的全名的一部分。
- 3 不应使用“常用”单词作为口令（例如，不应采用字典中的单词或常用的俚语）。
- 4 口令不应包含任何语言的单词，因为有许多口令破解程序可以在很短的时间内处理成百上千万个可能的单词组合。
- 5 应该选择可以记住但又复杂的口令。例如，Msi5!YOld（My son is 5 years Old，我儿子 5 岁了）或 ihlicf 5#Yn（I have lived in California for 5 years now，目前我在加利福尼亚已经住了 5 年了）。

## 2.9 “Reporting Configuration”

根据 Crystal 正在查询的事件数，可能会出现关于最长处理时间或最大记录限制的错误。要将服务器设置为可以处理更多数量或数量不限的记录，需要重配置 Crystal Page Server。使用中央配置管理器或 Crystal 网页可以执行此操作。

### 通过中央配置管理器重配置 Crystal Page Server:

- 1 单击“开始” > “所有程序” > “Businessobjects 11” > “Crystal Reports Server” > “中央配置管理器”。
- 2 右击“Crystal Reports Page 服务器”并选择“停止”。
- 3 再次右击“Crystal Reports Page 服务器”并选择“属性”。
- 4 在“属性”选项卡下的“命令”字段中，在命令行的末尾添加：  
maxDBResultRecords <value greater than 20000 or 0 to disable the default limit>
- 5 重新启动 Crystal Page Server。

### 通过 Crystal 万维网网页重配置 Crystal Page Server:

- 1 单击“开始” > “所有程序” > “Businessobjects 11” > “Crystal Reports Server” > “.NET 管理启动板”。
- 2 单击“中央管理控制台”。
- 3 “System Name”应该是您的主机名。“Authentication Type”应该是“Enterprise”。如果不是，请选择“企业”。
- 4 输入您的用户名、口令，然后单击“登录”。
- 5 单击“服务器”。



- 6 单击 < 服务器名称 >.pageserver。
- 7 在 “预览或刷新报告时要读取的数据库记录” 下，单击 “无限记录”。
- 8 单击 “应用”。
- 9 将会出现要求重新启动 Page 服务器的提示，单击 “确定”。

可能会提示您输入登录名和口令，以访问操作系统服务管理器。

### 重配置 Crystal Page Server (Linux 或 Windows Crystal Server) :

- 1 打开万维网浏览器并输入以下 URL:

对于 Linux Crystal 服务器:

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

对于 Window Crystal 服务器:

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

- 2 单击 “中央管理控制台”。
- 3 “System Name” 应该是您的主机名。“Authentication Type” 应该是 “Enterprise”。如果不是，请选择 “企业”。
- 4 输入您的用户名、口令，然后单击 “登录”。
- 5 单击 “服务器”。
- 6 单击 < 服务器名称 >.pageserver。
- 7 在 “Database Records to Read When Previewing Or Refreshing a report” (预览或刷新报告时要读取的数据库记录) 下，选择 “Unlimited records” (无限记录)。
- 8 单击 “应用”。
- 9 将会出现要求重新启动 Page 服务器的提示，单击 “确定”。
- 10 可能会提示您输入登录名和口令，以访问操作系统服务管理器。

## 2.9.1 Sentinel 提供的报告

为了提高性能，前 10 个报告查询摘要表而不是事件表。摘要表包含事件数据中的字段组合的计数（按时间）。对于某些类型的查询，此方式提供的数据集要小得多，因此，查询速度会明显加快，报告运行时间也会明显缩短。

聚合服务负责使用事件表中所有事件的摘要填充摘要表。聚合服务只为处于活动状态的摘要生成摘要数据。前 10 个报告需要下列摘要，默认情况下启用这些摘要：

- ◆ EventDestSummary
- ◆ EventSevSummary
- ◆ EventSrcSummary

可以在 Sentinel 控制中心的 “管理” 选项卡下使用报告数据配置窗口激活或禁用摘要。

聚合服务还依靠 DAS 二进制文件中的 EventFileRedirectService 部件获取将汇总的事件数据。因此，必须启用此部件，聚合服务才能正常运行。通过在 das\_binary.xml 文件中将

EventFileRedirectService 部件的 “status” 特性修改为 “on” 或 “off”，可以启用或禁用此部件。默认情况下，此部件设置为 “on”。

---

**注释：**有关 EventFileRedirectService 以及三个聚合摘要的信息，请参阅《Sentinel 控制中心用户指南》中的“Sentinel 数据管理器”或《Sentinel 安装指南》中的“用于 Windows 的 Crystal Reports”和 [第 10 章 “用于 Linux 的 Crystal Reports”](#)（第 123 页）。

---

**注释：**查询较长日期范围的报告可能需要运行一段时间。这些报告可以按日程安排运行，而不采用交互方式运行。有关为 Crystal Reports 制订日程安排的信息，请参阅 Crystal BusinessObjects Enterprise™ 11 文档。

---

## 2.9.2 开发自定义 Crystal Reports 时的提示

对于自定义开发的报告，建议如下：

- 1 如果报告可以利用预定义的汇总表，请选择产生的数据处理量最少的汇总表。
- 2 尽量将大部分数据处理任务推给数据库引擎。
- 3 为减少 Crystal 服务器的处理开销，应尽量减少检索到 Crystal 服务器的数据量。
- 4 始终根据 Novell 提供的数据库视图编写报告，而不要根据基础表编写报告。

## 2.10 数据库维护

Sentinel 使用其后端数据库存储所有事件以及配置数据。需要认真地管理此数据库，以确保可以继续有效地运行。

### 2.10.1 数据库中的事件信息

数据库的数据块由规范化的摘要事件数据组成。为了便于管理这个不断增长的数据集，Novell 对这些表进行分区，并提供管理工具（Sentinel 数据管理器）来存档和删除较旧的分区。可以制订存档计划，通过自动存档来最大程度地减少用户交互。

---

**注释：**有关 Sentinel 数据管理器的更多信息，请参阅《Sentinel 控制中心用户指南》中的“Sentinel 数据管理器”。

---

### 2.10.2 数据库中的其他信息

Sentinel 数据库包括许多其他信息，例如用户帐户、配置信息、事件、工作流程、资产数据、漏洞数据等。必须使用正常的数据库工具备份所有这些数据，以便在出现故障时进行恢复。Novell 建议为整个 Sentinel 数据库（以及服务器）制订一个全面的备份策略（上面所述的分区表除外）。

对于 SQL Server 而言，默认情况下 Sentinel 数据库是在完全恢复模型下创建的。在完全恢复模型下，在事物日志备份运行前不会释放使用过的事物日志空间。为防止事物日志变满，全天都应对 SQL Server 安排日志备份（每天备份 3 至 4 次，具体取决于您的事件率）。如果您的组织不要求具备执行故障点恢复的能力，可以将数据库恢复模型切换为简单。在简单数据库恢复模型下，无需任何日志备份，SQL Server 将自动释事物日志空间。

## 2.10.3 其他数据库维护

除了备份之外，应定期检查数据库的内部一致性。Novell 提供了一些自动工具来帮助完成此任务。有关更多信息，请参阅《Sentinel 用户指南》。

这些实用程序包括：

- ◆ 分析分区：收集最近填充过的分区的分区统计数字。
- ◆ 数据库运行状况检查：收集数据库信息。它将报告：
  - ◆ 检查数据库实例是否已启动
  - ◆ 检查 Oracle 监听器是否已启动
  - ◆ 显示空间使用情况
  - ◆ 检查不可用的索引
  - ◆ 检查无效的数据库对象
  - ◆ 检查数据库分析

---

**注释：**这些实用程序不能取代合格 DBA 的定期数据库维护。

---

### Oracle 数据库分析

随着事件不断地插入到 Sentinel 数据库中，应定期更新数据库统计数字，以确保查询性能良好。数据库分析实用程序可以更新 Oracle 中事件数据的数据库统计数字。为了获得最佳性能，应安排此实用程序定期运行。

---

**注释：**该实用程序包括一个可能会定期更新的、必需的 SQL 底稿。建议定期检查 [Novell 技术支持站点 \(http://support.novell.com/techselect/index.html\)](http://support.novell.com/techselect/index.html) 以获取更新。

---

### 分析分区

AnalyzePartitions.sh 底稿分析最近被填充过的分区。应通过 cron 或其他日程安排器每天安排运行此底稿，以便更新前一天填充的分区上的数据库统计数字。在数据库利用率较低时，建议在每天的某个时间运行此底稿。

该底稿位于 \$ESEC\_HOME/bin。它应该在安装 Sentinel 数据库的服务器本地运行。运行该底稿的 UNIX 用户帐户必须能够以 sysdba 的身份连接到数据库（例如 oracle）。

---

**注释：**如果该实用程序的下载版本高于计算机上当前安装的版本，则需要安装 sp\_esec\_dba\_utl.sql。

---

### 安装 sp\_esec\_dba\_utl.sql:

- 1 以 Oracle 软件拥有者的身份登录。
- 2 使用 SQL\*Plus 以 Sentinel 数据库用户的身份连接到数据库。
- 3 安装 ESEC\_DBA\_UTL 程序包。在 SQL 提示符 (SQL>) 处输入：  
@sp\_esec\_dba\_utl.sql

4 退出 SQL\*Plus。

### 运行 AnalyzePartitions.sh:

1 在您的 Oracle 数据库服务器计算机上，转到：

```
$ESEC_HOME/bin/
```

或转到将最新的文件下载到的位置。

2 在命令提示符处输入：

对于 Solaris:

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

对于 Linux:

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

- ◆ ORACLE\_SID - 数据库的 Oracle 实例名称。
- ◆ LogFileName - 希望写入日志讯息的文件的完整路径名。

如果该底稿运行成功，它退出时将返回代码 0。如果失败，它退出时将返回代码 1。请根据返回代码的检查结果安排作业。如果分析作业失败，请查看日志文件中的详细错误讯息。

## 2.10.4 Oracle 数据库运行状况检查

dbHealthCheck.sh 底稿收集有关您的 Sentinel Oracle 数据库的信息。dbHealthCheck.sh 底稿位于 %esec\_home%\bin 文件夹中。该底稿用于：

- ◆ 检查数据库实例是否已启动
- ◆ 检查 Oracle 监听器是否已启动
- ◆ 显示空间使用情况
- ◆ 检查不可用的索引
- ◆ 检查无效的数据库对象
- ◆ 检查数据库分析

应通过 cron 或其它日程安排器安排该底稿定期运行。

---

**注释：**该实用程序工具包括一个必需的、可能会定期更新的 SQL 底稿。建议定期检查 [Novell 技术支持站点 \(http://support.novell.com/techselect/index.html\)](http://support.novell.com/techselect/index.html) 以获取更新。

---

**注释：**如果该实用程序的下载版本高于计算机上当前安装的版本，则需要安装 sp\_esec\_dba\_utl.sql。

---

### 安装 “sp\_esec\_dba\_utl.sql”：

- 1 以 Oracle 软件拥有者的身份登录。
- 2 在数据库服务器中，请确保您的环境中已设置了 \$ORACLE\_HOME 和 \$ORACLE\_SID。
- 3 使用 SQL\*Plus 以 Sentinel 数据库用户的身份连接到数据库。
- 4 安装 ESEC\_DBA\_UTL 程序包。在 SQL 提示符 (SQL>) 处输入：  
@sp\_esec\_dba\_utl.sql

## 5 退出 SQL\*Plus。

### 运行 “dbHealthCheck.sh”：

---

**注释：**运行此底稿时，必须使用 Oracle 软件所有者帐户，或任何其它能够 “以 SYSDBA 身份” 连接的帐户

---

**注释：**必须在数据库服务器本地运行 dbHealthCheck.sh。

---

**1** 在数据库服务器中，请确保您的环境中已设置了 \$ORACLE\_HOME 和 \$ORACLE\_SID。

**2** 在 Oracle 数据库服务器计算机上，转到：

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

或转到将最新的文件下载到的位置。

**3** 在命令提示符处输入：

对于 Solaris：

```
./dbHealthCheck.sh
```

有关您的 Sentinel 数据库的信息将显示在屏幕上，您也可以将结果写入文件中。

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

对于 Linux：

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

有关您的 Sentinel 数据库的信息将显示在屏幕上，您也可以将结果写入文件中。

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

## 2.10.5 数据库维护

在安装 Sentinel 时自动配置数据库分区。建议管理员审阅 Sentinel 数据管理器中的设置并根据需要进行调整。有关 Sentinel 数据管理器的更多信息，请参阅《Sentinel 用户指南》中的“Sentinel 数据管理器”。

# 2.11 Correlation Engine

## 2.11.1 时间同步

Sentinel 关联引擎对时间要求很高，所以，Novell 强烈建议将所有关联引擎和收集器管理器计算机连接到 NTP（网络时间协议）服务器或其他类型的时间服务器。为了使 Sentinel 关联引擎正常运行，需要同步计算机的系统时间，确保所有收集器管理器计算机之间的时间误差在  $\pm 30$  秒内。

## 2.11.2 内存使用

在关联规则语言中，“Window”和“Trigger”操作符均有关联的时间窗口。时间窗口越大，在内存中为该时间窗口存储的事件信息可能就越多。这会影响到 Sentinel 内存中关联所需的内存量。如果关联引擎占用的内存过多，请考虑采用下列方式：

- ◆ 将关联引擎安装在专用的计算机上，并将所有当前的规则重新部署到新的关联引擎。
- ◆ 安装新的关联引擎，并将所选的当前规则重新部署到新的关联引擎。
- ◆ 调整关联规则的 Window 子句。
  - ◆ 使过去事件的过滤器更加具体。
  - ◆ 减小时间窗口的大小。
- ◆ 调整关联规则的 Trigger 子句。
  - ◆ 减小时间窗口的大小。
  - ◆ 减小触发规则所需的事件数的阈值。
  - ◆ 选择基数低的鉴别器（例如设备类型）。
  - ◆ 如果鉴别器的基数低（例如源 IP 地址），则减小触发规则所需的事件数的阈值，同时减小时间窗口的大小，以获得等效的结果。

## 2.11.3 短路分析

数字比较快于字符串比较，而字符串比较快于正则表达式比较。过滤器运算对布尔表达式执行短路分析。通过仔细对表达式进行排序，可以提高计算速度。

## 2.11.4 自由格式的规则

如果无法使用关联规则向导表达关联规则，可以使用关联规则语言构建自由格式的规则。有关创建自由格式的规则的更多信息，请参阅《参考指南》中的“关联引擎”。

## 2.12 Sentinel 日志文件

最好定期审阅 Sentinel 生成的日志文件，以查看是否出现错误。有关这些文件及其位置的更多信息，请参阅《参考指南》中的“Sentinel 日志位置”。

本章包含下列主题：

- ◆ 在 Linux、Solaris 和 Windows 上安装 Sentinel（第 39 页）
- ◆ 安装 Sentinel 6.0 的先决条件（第 41 页）
- ◆ 在 Linux、SUSE Linux、Redhat Linux 和 Solaris 上安装 Oracle（第 43 页）
- ◆ 安装 Oracle（第 46 页）
- ◆ 安装 Sentinel（第 52 页）
- ◆ 简单安装（第 52 页）
- ◆ 自定义安装（第 54 页）
- ◆ 安装后配置（第 63 页）

## 3.1 在 Linux、Solaris 和 Windows 上安装 Sentinel

本章帮助您为 SUSE Linux Enterprise Server、Red Hat Enterprise Linux 和 Solaris 上的 Oracle 以及 Windows 上的 Microsoft SQL Server 安装 Sentinel。

如果在卸装 Sentinel 的早期版本后进行全新的 Sentinel 安装，您必须手动去除可能遗留的某些文件和系统设置。有关卸装 Sentinel 6.0 的更多信息，请参阅第 11 章“卸装 Sentinel”（第 137 页）。有关卸装 Sentinel 的早期版本的信息，请参阅相关文档版本，这些文档可以从 Novell 文档万维网站点 <http://www.novell.com/documentation/> (<http://www.novell.com/documentation/>) 获得。

---

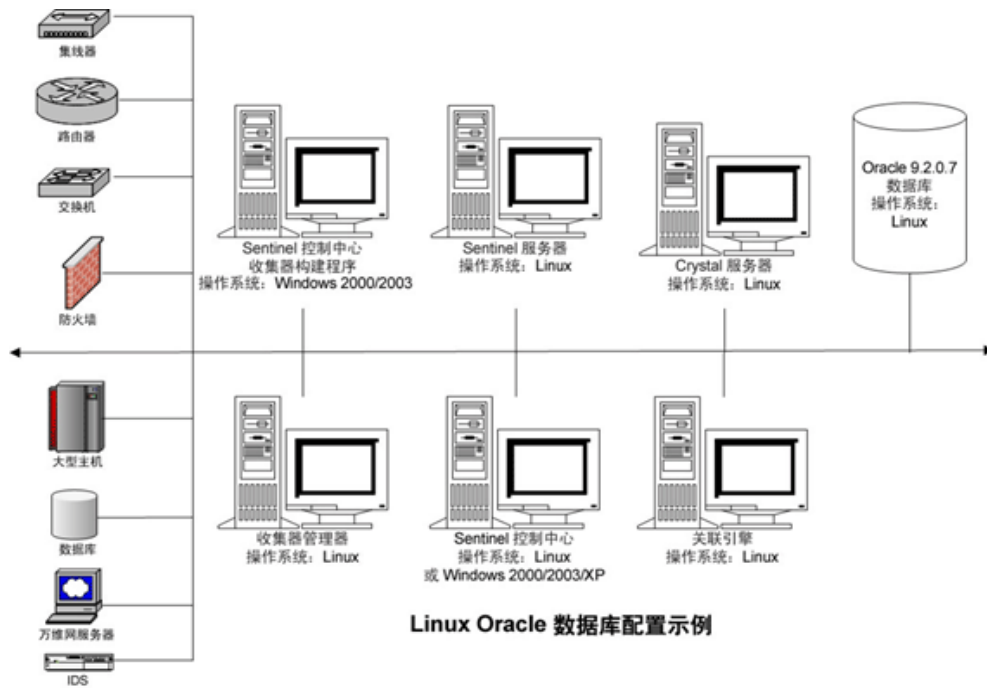
**注释：**要在 SLES 上安装 Sentinel 服务器，Novell 建议使用 ReiserFS 以外的其他文件系统，因为 Novell 发现在使用 ReiserFS 的 SLES 上运行 Sentinel 时存在间歇性的问题。Novell 的内部 Sentinel 测试是使用 ext3 文件系统执行的（尽管有多种选择）。

---

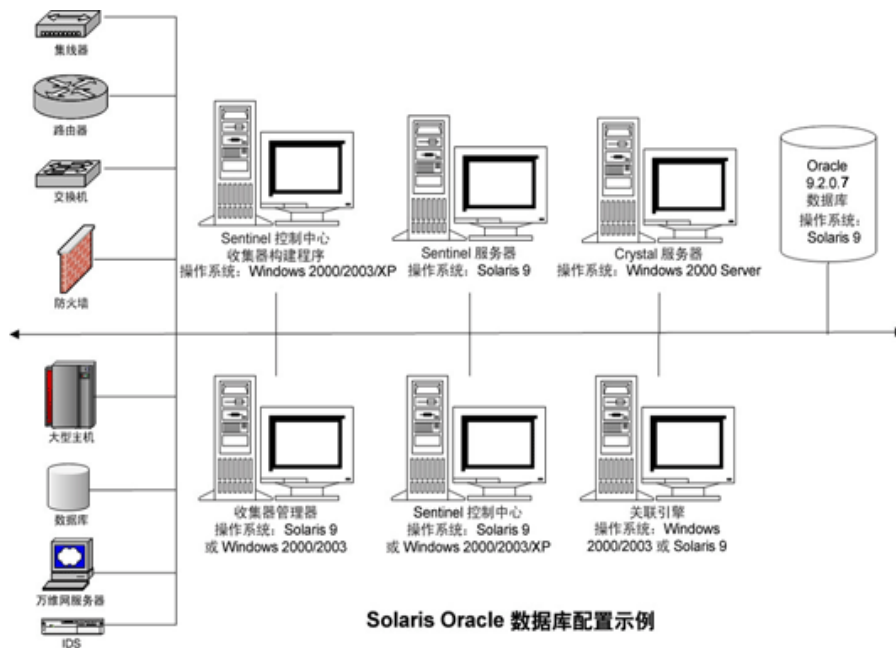
### 3.1.1 Sentinel 配置

以下为 Linux 上用于 Sentinel 的典型配置。您的配置可能会因环境的不同而有所不同。无论选择何种配置，都需要先安装数据库。

## 在 Linux 上

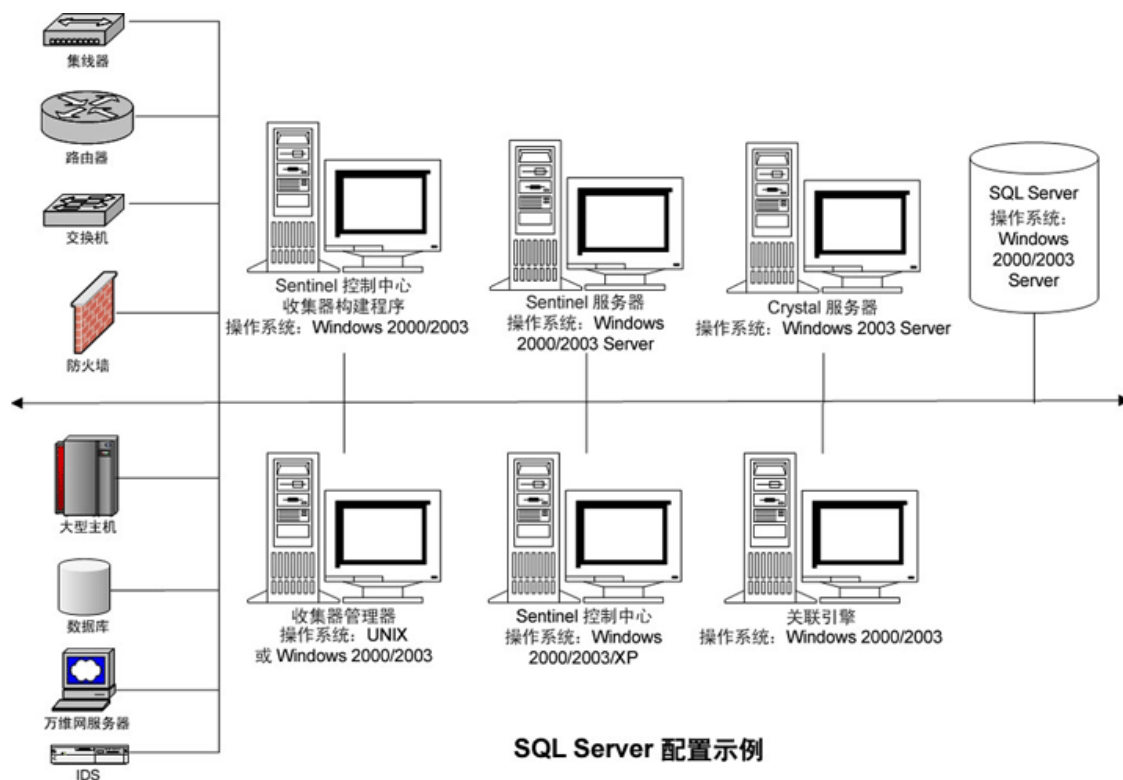


## 在 Solaris 上





## 在 Windows 上:



### 3.1.2 安装 Sentinel 6.0 的先决条件

在安装 Sentinel 之前，请确保：

- ◆ 您的计算机满足最低系统要求，且操作系统已使用当前的最佳安全措施得到了“强化”。有关详细信息，请参见第 2 章“最佳实践”（第 17 页）
- ◆ 要在 Solaris 和 Linux 上安装 Sentinel，请安装带分区的 Oracle Enterprise。Sentinel 数据管理器需要具备此功能才能管理 Sentinel 数据库。
- ◆ 您已满足了安装下列部件所需的条件：
  - ◆ Sentinel 数据库
  - ◆ Sentinel 服务器
  - ◆ Sentinel 控制中心和 Sentinel Collector Builder
  - ◆ Sentinel 顾问
- ◆ 您已在 Linux、SUSE Linux、Red Hat Linux 和 Solaris 上安装了 Oracle。

#### Sentinel 数据库

在安装 Sentinel 数据库之前，您需要：

#### 在 Linux/Solaris 上:

- ◆ 在 Linux 上，拥有 Oracle 操作系统用户（默认用户：oracle）的登录凭证。

- ◆ 在 Solaris 上：
  - ◆ 拥有《Oracle 148673.1 Solaris: 快速入门指南》的副本
  - ◆ 拥有 Oracle 操作系统用户（默认用户：oracle）
- ◆ 在 Linux/Solaris 上，确保为 Oracle 操作系统用户设置了下列环境变量：
  - ◆ ORACLE\_HOME（例如，echo \$ORACLE\_HOME 生成 /opt/oracle/product/10gR2/db）
  - ◆ ORACLE\_BASE（例如，echo \$ORACLE\_BASE 生成 /opt/oracle）
  - ◆ PATH（必须包含 \$ORACLE\_HOME/bin）
- ◆ 如果计划手动创建 Sentinel 数据库将安装到的 Oracle 数据库实例（尽管不建议这样做），请参阅“高事件发生率的数据库创建和配置”，以获得创建与 Sentinel 兼容的 Oracle 实例的说明。如果选择此选项，仍必须使用 Sentinel 安装程序将数据库对象添加到手动创建的 Oracle 数据库实例中。有关详细信息，请参见 [自定义安装（第 54 页）](#)

---

**注释：**如果使用现有的或手动创建的 Oracle 数据库实例，除了存在 Sentinel 数据库用户外，该实例必须为空。

---

### 在 Windows 上：

- ◆ 在 Windows 上，已安装并正在运行 SQL Server 2005 SP1。

---

**注释：**出于性能考虑，如果您是在 RAID 中进行安装并且您的 RAID 环境允许，强烈建议您配置系统，使事务日志指向可用的写入速度最快的磁盘，该磁盘是存储数据库文件的独立物理磁盘。

---

- ◆ 在 Windows 上，需要安装采用混合模式鉴定的 SQL Server，以使用 Windows 或 SQL Server 鉴定进行登录。如果安装非混合模式的 SQL 服务器，则只能使用 Window 鉴定进行登录。
- ◆ 修改鉴定模式设置：
  - ◆ 在 Microsoft SQL Server Management Studio 中，右击要修改其设置的服务器。
  - ◆ 选择属性并单击“安全性”。
  - ◆ 从两个选项中选择“SQL Server 和 Windows 鉴定模式”或“Windows 鉴定模式”进行鉴定。
  - ◆ 还要确保 MSSQLSERVER 服务应使用本地系统帐户进行登录。
- ◆ 确定 SQL Server 实例名（建议使用默认值）。

---

**注释：**如果在安装 SQL Server 期间已命名了实例，则在安装 Sentinel 数据库和 / 或 DAS 部件过程中，当提示输入 SQL Server 实例名称时，请使用此名称。如果在安装 SQL Server 期间未命名实例，则在安装过程中实例名称应保留为空（即，在主机名中键入时，不要在数据库主机名中添加“\<实例名称>”）。

---

- ◆ 确定 SQL Server 实例端口号（默认值为 1433）。
- ◆ 如果要对安装 Sentinel 期间使用的一个或多个 Sentinel 用户使用 Windows 鉴定，则在安装 Sentinel 数据库之前必须存在相应的 Windows 域用户。可以将以下 Sentinel 用户指派给 Windows 域用户：
  - ◆ Sentinel 数据库管理员（esecdba，数据库纲要拥有者）
  - ◆ Sentinel 应用程序用户（esecapp，Sentinel 应用程序使用该用户连接到数据库）

- ◆ Sentinel 管理员（esecadm，用于登录到 Sentinel 控制中心的管理员）
- ◆ Sentinel 报告用户（esecrpt，用于创建报告）

---

**注释：**默认情况下，数据库将包含 Sentinel 数据库管理员用户、 Sentinel 应用程序用户和 Sentinel 管理员用户。

---

---

**注释：**Sentinel 不支持 Microsoft 群集或 Windows 高可用性。

---

## Sentinel 服务器

---

**注释：**如果不打算在安装 Sentinel 服务器的计算机上安装 Sentinel 数据库，则必须首先安装 Sentinel 数据库。

---

- ◆ 如果要安装 DAS 部件，应拥有 Sentinel 序列号和许可证密钥（对于 DAS）。
- ◆ 决定 SMTP 服务器（DNS 名称）。通过 Sentinel 发送电子邮件时需要这样做。
- ◆ 在 Windows 上，如果安装 DAS 并且对 Sentinel 应用程序使用 Windows 域用户帐户，则为用户提供“作为服务登录”特权。提供此特权：
  - ◆ 在要安装 DAS 的计算机上的“本地安全策略”中添加该用户（“开始” > “设置” > “控制面板” > “管理工具” > “本地安全策略”）。
  - ◆ 在“本地安全策略”窗口中，转到“本地策略” > “用户权利指派”。
  - ◆ 双击“作为服务登录”策略并添加该用户。

## Advisor

要安装 Advisor，需要从 Sentinel 获取 Advisor ID 和口令。您在购买该软件时会收到 Advisor ID 和口令。如果选择“直接因特网下载”，请使用传出端口 443。应在系统上安装 Crystal Enterprise 软件以运行报告。

---

**注释：**如果您使用顾问只是为了进行漏洞利用检测，则无需安装 Crystal Enterprise 软件。有关更多信息，请参考第 4 章“顾问配置”（第 67 页）。

---

## 3.2 在 Linux、SUSE Linux、Redhat Linux 和 Solaris 上安装 Oracle

要在 Linux/Solaris 上安装 Oracle，请确保：

- ◆ 设置内核值
- ◆ 在 Linux 上配置 init.ora 文件
- ◆ 在 Solaris 上：
  - ◆ 为 Oracle 创建组 and 用户帐户
  - ◆ 设置环境变量
  - ◆ 验证 Solaris 布局
- ◆ 安装 Oracle 9.2.0.4
- ◆ 增补至 Oracle 9.2.0.7

### 3.2.1 设置内核值

**重要：**本节中建议的内核值只是最小值。只有系统设置低于建议的最小值时，并且向系统管理员咨询并参阅了 Oracle 文档之后，才应更改这些设置。

#### 在 Solaris 上设置内核值：

在 Solaris 上，必须在 /etc/system 中设置下列内核值。

---

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

---

- 1 以根用户身份登录。
- 2 备份 /etc/system。
- 3 使用文本编辑器，按照上表内容，更改 /etc/system 文件中的内核参数设置。
- 4 重引导。

#### 在 Linux 上设置内核值：

在 Linux 上，必须在 /etc/sysctl.conf 中设置下列内核值。

---

shmmmax=2147483648 ( 下限值 )	semmni=1024
shmmni=4096	semmsl=1024
semmns=32000	semopm=100

---

- 1 以根用户身份登录。
- 2 将以下内容添加到 “/etc/sysctl.conf” 文件的末尾，以设置内核参数：

**注释：**要想确定某个特殊内核参数的当前设置，请执行下面的命令：

```
sysctl <kernel_parameter>
```

例如，要检查内核参数 “kernel.sem” 的当前值，请执行命令：sysctl kernel.sem

---

在 SUSE LINUX 上

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

在 REDHAT LINUX 上

```
# Kernel settings for Oracle
# kernel.sem = <SEMMSL> <SEMMNS> <SEMOPM> <SEMMNI>
kernel.sem = 1024          32000    100      1024
kernel.shmmmax = 2147483648
```

```
kernel.shmmni = 4096
fs.file-max = 65536
net.ipv4.ip_local_port_range = 1024 65000
```

- 3 执行以下命令，将修改的内容加载到 “/etc/sysctl.conf” 文件中：

```
sysctl -p
```

- 4 将以下内容添加到 “/etc/security/limits.conf” 文件的末尾，以设置文件句柄和进程限制。“nproc” 是进程数的上限，而 “nofile” 是打开文件数的上限。这些值是推荐值，如有需要可以修改它们。

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

## 3.2.2 为 Solaris 上的 Oracle 创建组 and 用户帐户

### 创建组 and 用户帐户并设置环境变量：

- 1 以根用户身份登录。
- 2 为 Oracle 数据库所有者创建 UNIX 组和 UNIX 用户帐户。
  - ♦ 添加一个 dba 组（以 root 用户身份）：

```
groupadd -g 400 dba
```
  - ♦ 添加 Oracle 用户（以 root 用户身份）：

```
useradd -g dba -d /export/home/oracle -m -s /bin/csh oracle
```

## 3.2.3 为 Solaris 上的 Oracle 设置环境变量

### 设置环境变量：

- 1 以根用户身份登录。
- 2 要设置 Oracle 所需的环境变量，建议向 local.cshrc 文件添加以下信息：

```
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 验证 Solaris 布局

### 设置环境变量:

- 1 转到 Sun 因特网站点并下载为 Solaris 9 推荐的增补程序集:
  - ◆ 增补程序集 日期: 2005 年 5 月 3 日

---

**注释:** 请参阅 README 文件及其它包含的文档。强烈建议您在应用任何增补程序之前, 对系统进行完整系统备份。

---

- 2 以根用户身份登录, 然后安装适用的增补程序群集和内核增补程序。
- 3 增补程序安装完成后, 应删除增补程序所创建的目录中的 \*\_Recommended.zip 文件以及展开的文件, 然后重引导服务器。

## 3.2.5 安装 Oracle

本节说明如何在下列平台上安装 Oracle:

- ◆ SUSE Linux
- ◆ Red Hat Linux
- ◆ Solaris

---

**重要:** 下列说明并非为了取代 Oracle 的文档。这只是一个示例安装方案。强烈建议您按照这些说明操作。本文档假定 Oracle 用户的主目录为 /home/oracle, Oracle 将安装到 /opt/oracle 中。您的实际配置可能会有所不同。有关更多信息, 请参见您的操作系统文档和 Oracle 文档。

---

### 在 SUSE Linux (SLES 9 SP3) 上

#### 在 SUSE Linux 上安装 Oracle:

- 1 按照 SLES 9 安装手册中提供的安装说明操作。安装包包含默认程序包的 SLES 9 以及 C/C++ 编译程序和工具及 SP2。

---

**注释:** 如果已安装 SUSE Linux, 则可以在 SUSE Linux GUI 中使用 YaST (另一个安装工具) 安装 C/C++ 编译程序和工具。

---

- 2 以根用户身份登录。
- 3 使用 YaST 安装 gcc\_old。
- 4 通过输入以下命令验证您是否正在运行 SP3:

```
SPident
```

或

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

您应获得:

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

或

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

- 5** 要自动完成预装 Oracle 的大多数任务并创建 oracle 用户，请安装随 SLES 9 附带的 orarun.rpm。

---

**注释：**有关先决条件的完整列表，请参考 Oracle 安装文档。

---

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

---

**注释：**orarun 也可以从 <http://www.novell.com> (<http://www.novell.com>) 获得。

---

- 6** oracle 用户的帐户已禁用。通过使用 YaST 用户管理或编辑 /etc/passwd 将 oracle 用户的壳层从 /bin/false 更改为 /bin/bash，从而启用该帐户。

- 7** 通过使用 YaST 或输入以下命令为 oracle 用户设置新口令：

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

- 8** 要设置内核参数，请运行

```
/usr/sbin/rcoracle start
```

忽略出现的任何错误。

```
/sbin/chkconfig oracle on
```

- 9** 更改为 Oracle 用户：

```
su - oracle
```

- 10** 要安装 Oracle 9.2.0.4，请从 Disk1 运行底稿：

```
./runinstaller
```

- 11** 安装程序执行过程中，如果下面未作指定，应按默认值处理所有提示。

- ◆ 提示输入“UNIX 组名”时，请输入：dba
- ◆ 提示选择“Installation Type”时，请选择“Custom”。

选择安装下列部件：

- ◆ Oracle 9i 9.2.0.4.0
- ◆ 企业版选项 9.2.0.1.0
  - ◆ Oracle Partitioning 9i 9.2.0.4.0
- ◆ Oracle Net Services 9.2.0.1.0
  - ◆ Oracle Net Listener 9.2.0.4.0
- ◆ Oracle Enterprise Manager 产品 9.2.0.1.0（全部）
- ◆ Oracle 9i 开发工具包 9.2.0.1.0（全部）
- ◆ 用于 UNIX 的 Oracle 9i 文档 9.2.0.1.0
- ◆ Oracle HTTP Server 9.2.0.1.0（全部）
- ◆ iSQL\*Plus 9.2.0.4.0（全部）
- ◆ Oracle JDBC/OCI 接口 9.2.0.1.0

- 12** 提示是否创建数据库时，选择“否”。

- 13** 也可选择取消安装程序启动的所有配置助手。

- 14** 修改文件“/opt/oracle/network/admin/sqlnet.ora”（如果此文件不存在，请创建它），使其包含以下内容（去除文件中现有的所有未注释的信息）：

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

- 15** 要将 Oracle 增补程序应用于 Oracle，请在 Oracle 9.2.0.7 增补程序分发包的 Disk1 中，运行以下底稿：

```
./runInstaller
```

- 16** 安装程序执行过程中，如果下面未作指定，应按默认值处理所有提示。
- ◆ 在 “Welcome” 屏幕上单击 “Next”。
  - ◆ 在 “Specify File Locations” 屏幕上，从下拉列表中，选择 “OUIHome”（或在安装 Oracle 9.2.0.4 期间所设置的任何目标名称）作为 “Destination Name”。然后单击 “Next”。
  - ◆ 根据您的版本，请在 “选择要安装的产品” 屏幕上，选择 “Oracle 9iR2 Patchset 9.2.0.7.0”。然后单击 “下一步”。
  - ◆ 在 “Summary” 屏幕上，审阅安装摘要，然后单击 “Install”。
  - ◆ 在 “End of Installation” 屏幕上，单击 “Exit”。
- 17** 编辑 init.ora 文件，以指定应将存档的 Sentinel 数据写入的目录路径。此信息在 UTL\_FILE\_DIR 参数中指定。应包含下列项目之一：
- ◆ UTL\_FILE\_DIR = \*
  - 或
  - ◆ UTL\_FILE\_DIR = <特定的目录路径 >

## 在 SUSE Linux (SLES 10) 上

### 在 SUSE Linux 上安装 Oracle:

- 1** 按照 SLES 10 安装手册中提供的安装说明操作。将包含默认程序包的 SLES 10 与 Oracle Server Base、C/C++ 编译程序和工具一起安装。
- 2** 以根用户身份登录。
- 3** 安装 SLES 10 Service Pack。通过输入以下命令验证 Service Pack 信息：

```
SPident
```

或

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

在编写本文档时，尚未发布 SLES 10 Service Pack。使用 SPident 或 cat/etc/SUSE-release 进行验证。

您应获得：

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

- 4** 要自动完成预装 Oracle 的大多数任务并创建 oracle 用户，请安装随 SLES 9 附带的 orarun.rpm。

---

**注释：**有关先决条件的完整列表，请参考 Oracle 安装文档。

---

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

---

**注释：**orarun 也可以从 <http://www.novell.com> (<http://www.novell.com>) 获得。

---

- 5** oracle 用户的帐户已禁用。通过使用 YaST 用户管理或编辑 /etc/passwd 文件将 oracle 用户的外壳从 /bin/false 更改为 /bin/bash，从而启用该帐户。



- 6 通过使用 YaST 或输入以下命令为 oracle 用户设置新口令：  
`/usr/bin/passwd oracle`
- 7 如果需要，应更改 orarun 设置的默认 Oracle 环境：
  - ◆ 通过在 “/etc/profile.d/oracle.sh” 文件中编辑 ORACLE\_HOME 变量，更改 Oracle 主目录。
  - ◆ orarun 安装所设置的默认 ORACLE\_SID 为 “orcl”。在 “/etc/profile.d/oracle.sh” 文件中将其更改为 ESEC。
- 8 要设置内核参数，请运行  
`/usr/sbin/rcoracle start`
- 9 更改为 Oracle 用户：  
`su - oracle`
- 10 切换到数据库目录并运行 ./runinstaller（Oracle 通用安装程序）。此时将出现如下所示的错误：
- 11 通过执行下列操作之一纠正错误：
  - ◆ 修改 “database/install/oraparam.ini” 文件，以增加对 SUSE Linux 10 的支持。修改了 oraparam.ini 文件后，“[Certified Versions]” 行将类似如下所示：  

```
[Certified Versions]
Linux=redhat=3,SuSE-9,SuSE-10,redhat-4,UnitedLinux-1.0.asianux-1,asianux-2
```
  - ◆ 使用 -ignoreSysPrereqs 选项安装  
 i.e. `./runInstaller -ignoreSysPrereqs`
- 12 接受默认库存目录或浏览并选择新目录。单击“下一步”。
- 13 从“安装类型”中选择“企业版”。单击“下一步”。
- 14 为了检查网络配置要求，请选择“用户已验证”。单击“下一步”。
- 15 从配置选项中选择“仅安装数据库软件”。单击“下一步”。
- 16 此时将显示安装摘要。审阅并单击“安装”。
- 17 以根用户的身份执行指定的底稿，并在完成后单击“确定”。
- 18 在成功安装后，单击“退出”。

## 在 Red Hat Linux 上

### 在 Red Hat Linux 上安装 Oracle:

- 1 以根用户身份登录。
- 2 为 Oracle 数据库所有者创建 UNIX 组和 UNIX 用户帐户。  
 添加一个 dba 组（以 root 用户身份）：  
`groupadd dba`
- 3 添加 Oracle 用户（作为根用户）：  
`useradd -g dba -s /bin/bash -d /home/oracle -m oracle`
- 4 为 ORACLE\_HOME 和 ORACLE\_BASE 创建目录：  
`mkdir -p /opt/oracle/`
- 5 更改 ORACLE\_BASE 目录的所有权，一直更改到下级目录 oracle/dba：  
`chown -R oracle:dba /opt/oracle`

**6** 更改为 Oracle 用户:

```
su - oracle
```

**7** 打开 “.bash\_profile” 文件（位于 oracle 用户的主目录中）以进行编辑，将以下内容添加到该文件末尾:

---

**注释:** 这一组环境变量只能用于 oracle 用户。特别是不应在系统环境或 Sentinel 管理员用户的环境中设置这些变量。

---

```
# 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** 以 Oracle 用户身份重登录，然后加载上一步中更改的环境变量:

```
exit  
su - oracle
```

**9** 将 gcc 链接到 2.9.6 版

---

**注释:** 如果 /usr/bin/gcc296 或 /usr/bin/g++296 不存在，则说明未安装 gcc 或 g++。如果出现这种情况，请安装这些部件，然后返回至此步骤。

---

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

**10** 退出以返回 Oracle 用户提示符。

```
exit
```

**11** 运行 Oracle 增补程序 p3006854\_9204\_LINUX.zip，它将为 Linux 操作系统安装增补程序以安装 Oracle。此增补程序可从 Oracle 获得。

```
su - root  
unzip p3006854_9204_LINUX.zip  
cd 3006854  
sh rhel3_pre_install.sh
```

**12** 退出以返回 Oracle 用户提示符。

```
exit
```

**13** 要安装 Oracle 9.2.0.4, 请从 Disk1 运行底稿:

```
./runInstaller
```

**14** 安装程序执行过程中, 如果下面未作指定, 应按默认值处理所有提示。

- ◆ 提示输入 “UNIX 组名” 时, 请输入: dba
- ◆ 提示选择 “Installation Type” 时, 请选择 “Custom”。

选择安装下列部件:

- ◆ Oracle 9i 9.2.0.4.0
- ◆ 企业版选项 9.2.0.1.0
  - ◆ Oracle Partitioning 9i 9.2.0.4.0
- ◆ Oracle Net Services 9.2.0.1.0
  - ◆ Oracle Net Listener 9.2.0.4.0
- ◆ Oracle Enterprise Manager 产品 9.2.0.1.0 (全部)
- ◆ Oracle 9i 开发工具包 9.2.0.1.0 (全部)
- ◆ 用于 UNIX 的 Oracle 9i 文档 9.2.0.1.0
- ◆ Oracle HTTP Server 9.2.0.1.0 (全部)
- ◆ iSQL\*Plus 9.2.0.4.0 (全部)
- ◆ Oracle JDBC/OCI 接口 9.2.0.1.0

**15** 提示创建数据库时, 选择 “否”。

**16** 也可选择取消安装程序启动的所有配置助手

**17** 修改文件 “/opt/oracle/network/admin/sqlnet.ora” (如果此文件不存在, 请创建它), 使其包含以下内容 (去除文件中现有的所有未注释的信息):

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

**18** 要将 Oracle 增补程序应用于 Oracle, 请在 Oracle 9.2.0.7 增补程序分发包的 Disk1 中, 运行以下底稿:

```
./runInstaller
```

**19** 安装程序执行过程中, 如果下面未作指定, 应按默认值处理所有提示。

- ◆ 在 “Welcome” 屏幕上单击 “Next”。
- ◆ 在 “Specify File Locations” 屏幕上, 从下拉列表中, 选择 “OUIHome” (或在安装 Oracle 9.2.0.4 期间所设置的任何目标名称) 作为 “Destination Name”。然后单击 “Next”。
- ◆ 根据您的版本, 请在 “选择要安装的产品” 屏幕上, 选择 “Oracle 9iR2 Patchset 9.2.0.7.0”。然后单击 “下一步”。
- ◆ 在 “Summary” 屏幕上, 审阅安装摘要, 然后单击 “Install”。
- ◆ 在 “End of Installation” 屏幕上, 单击 “Exit”。

**20** 取消链接 gcc:

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

**21** 退出以返回 Oracle 用户提示符。

```
Exit
```

**22** 编辑 `init.ora` 文件，以指定应将存档的 Sentinel 数据写入的目录路径。此信息在 `UTL_FILE_DIR` 参数中指定。应包含下列项目之一：

- ◆ `UTL_FILE_DIR = *`

或

- ◆ `UTL_FILE_DIR = [ 特定的目录路径 ]`

## 在 Solaris 上

### 在 Solaris 上安装 Oracle:

- 1 以根用户身份登录。
- 2 按照《Oracle 注释：148673.1 SOLARIS：快速入门指南》中所述的步骤操作。
- 3 以 `oracle` 用户身份安装 Oracle 9i Release 2 (9.2.0.1)。将提示您提供两个额外的 CD-ROM。您需要导航至每个额外 CD-ROM 的不同目录中。
- 4 将您的系统增补至 Oracle 9.2.0.7。有关增补步骤，请参考 Oracle 文档。
- 5 要验证增补程序级别，请以 Oracle UNIX 用户身份输入：  
`sqlplus '/as sysdba'`  
结果应指示为发行版本 9.2.0.7。输入“quit”退出。
- 6 去除为增补程序创建的目录。
- 7 增补程序安装结束后，应去除增补程序目录和文件。
- 8 编辑 `init.ora` 文件，以指定应将存档的 Sentinel 数据写入的目录路径。此信息在 `UTL_FILE_DIR` 参数中指定。应包含下列项目之一：
  - ◆ `UTL_FILE_DIR = *`或
  - ◆ `UTL_FILE_DIR = [ 特定的目录路径 ]`
- 9 重引导。

## 3.3 安装 Sentinel

Sentinel 支持两种安装类型。它们是：

- ◆ **简单：**一步式安装选项。在 Oracle 所在的同一台计算机上安装 Sentinel 服务、收集器服务和应用程序。此安装类型仅供演示使用。
- ◆ **自定义：**允许完全分布式安装。

### 3.3.1 简单安装

满足了上一节中提到的先决条件之后，可以继续安装 Sentinel。

#### 安装 Sentinel:

- 1 以根用户的身份（在 Solaris/Linux 上）或管理员用户的身份（在 Windows 上）登录。
- 2 插入并装入 Sentinel 安装光盘。

- 3 在 Linux/Solaris 上，通过在运行安装程序时所处的命令提示符下执行以下命令，确保系统 umask 设置为 0027：

```
umask 0027
```

- 4 通过转到 CD-ROM 上的安装目录并输入以下命令来启动安装程序：

- ◆ 在 Windows 上，运行 setup.bat
- ◆ 在 Solaris/Linux 上：

进入 GUI 方式：

```
./setup.sh
```

或

对于基于文本（“串行控制台”）模式：

```
./setup.sh -console
```

- 5 单击向下箭头，并选择以下语言之一：

---

英语	意大利语
法语	葡萄牙语 (巴西)
德语	西班牙语
简体中文	日语
繁体中文	

---

- 6 阅读 “Welcome”（欢迎）屏幕后单击 “下一步”。

- 7 阅读并接受 《最终用户许可协议》并单击 “下一步”。

- 8 接受默认的安装目录，或单击 “浏览” 指定安装位置。单击 “下一步”。

- 9 选择 “简单”。单击 “下一步”。

- 10 在此屏幕中，输入配置信息并单击 “下一步”。

- ◆ 序列号
- ◆ 许可证密钥
- ◆ SMTP 服务器
- ◆ 电子邮件

在此处输入的 SMTP 服务器 IP 或 DNS 名称将帮助您配置为使用在此处输入的电子邮件 ID，通过 Sentinel 发送电子邮件。

- ◆ 全局系统口令

在此处输入的口令对于所有默认用户都有效。其中包括 Sentinel 管理员用户和数据库用户。有关使用安装创建的默认数据库用户的列表的更多信息，请参阅 [Sentinel 数据库（第 64 页）](#)。

- ◆ Advisor 用户名和口令

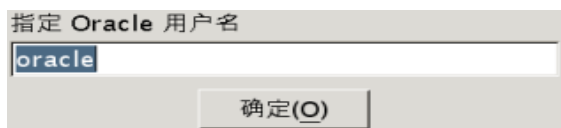
要安装 Advisor，请输入在购买软件时为您提供的用户名和口令。如果无法验证您的用户名或口令，在单击 “下一步” 后将询问您是否继续（不推荐）。如果选择继续，在口令确认窗口中再次输入您的顾问口令。

---

**注释：**如果要安装 Advisor，采用 “简单” 安装方式时会对 Advisor 进行以下配置：使用 “直接因特网下载”，更新间隔为 12 小时，并且启用所有电子邮件通知。

---

在 Solaris/Linux 上，系统将提示您指定 Oracle 用户名。输入用户名并单击“确定”。



**11** 对于数据库配置：

- ◆ 选择目标数据库平台。
- ◆ 输入数据库名称
  - ◆ 在 Linux/Solaris 上，指定 Oracle JDBC 驱动程序文件。
  - ◆ 在 Windows 上，输入数据库用户凭证和 SQL Server 实例名。

单击“下一步”。

“简单”安装的数据库大小为 10 GB。

Microsoft SQL Server 配置

数据库(D) :	<input type="text" value="ESEC"/>	SQL Server 实例	<input type="text"/>
登录(L) :	<input type="text" value="sa"/>		
密码(P) :	<input type="text"/>		

**12** 此时将显示所选数据库参数的摘要。单击“下一步”。

**13** 此时将显示安装摘要。单击“安装”。

**14** 成功安装后，单击“完成”。

### 3.3.2 自定义安装

满足了上一节中提到的先决条件之后，可以继续安装 Sentinel。

#### 安装 Sentinel:

- 1** 以根用户的身份（在 Solaris/Linux 上）或管理员用户的身份（在 Windows 上）登录。
- 2** 插入并装入 Sentinel 安装光盘。
- 3** 在 Linux/Solaris 上，通过在运行安装程序时所处的命令提示符下执行以下命令，确保系统 umask 设置为 0027：  
`umask 0027`
- 4** 通过转到 CD-ROM 上的安装目录并输入以下命令来启动安装程序：
  - ◆ 在 Windows 上，运行 `setup.bat`
  - ◆ 在 Solaris/Linux 上：

进入 GUI 方式：

`./setup.sh`

或

进入文本（“无头”）方式：

```
./setup.sh -console
```

- 5 单击向下箭头，并选择以下语言之一：

---

英语	意大利语
法语	葡萄牙语 (巴西)
德语	西班牙语
简体中文	日语
繁体中文	

---

- 6 阅读 “Welcome”（欢迎）屏幕后单击 “下一步”。
- 7 阅读并接受 《最终用户许可协议》并单击 “下一步”。
- 8 接受默认的安装目录，或单击 “浏览” 指定安装位置。单击 “下一步”。
- 9 选择 “自定义”。单击 “下一步”。
- 10 选择要安装的 Sentinel 部件。

---

**注释：**有关对不同配置安装每个部件的更多信息，请参阅 《安装指南》中的 [第 2 章 “最佳实践”（第 17 页）](#)。

---

下列选项可用：

---

数据库 – 安装 Sentinel 数据库	Sentinel 收集器服务
通讯服务器 – 安装讯息总线 (iSCALE) 和 DAS 代理	收集器构建程序
Advisor	Sentinel 控制中心
Correlation Engine	Sentinel 数据管理器
DAS (用于数据库通讯)	HP OpenView Service Desk
	Remedy Integration

---

---

**注释：**有关安装 HP OpenView Service Desk 或 Remedy Integration 的信息，请参阅 《第三方集成指南》。

---

---

**注释：**选择或取消选择部件时，界面中会出现时间延迟。

---

---

**注释：**如果未选择 Sentinel 服务的任何子功能，请确保也取消选择 Sentinel 服务功能。如果仍选中 Sentinel 服务，而取消选择它的所有子功能，则 Sentinel 服务将变灰，同时带有白色选中标记。

---

---

**注释：**作为安装 Sentinel 数据库部件的一部分，安装程序会将文件放置到 %ESEC\_HOME%\db 文件夹中。

---

---

**注释：**在 “简单” 安装中，MSSQL 和 ORACLE 的数据库安装大小为 10GB。

---

选择要安装的“Sentinel 6”功能部件：



- 11 如果选择安装 DAS，将提示您提供：
  - ◆ 序列号
  - ◆ 许可证密钥
- 12 如果选择安装任何第三方集成部件，将提示您提供解除锁定所选第三方集成部件的口令。有关更多信息，请参阅《第三方集成指南》。
- 13 在 Linux/Solaris 上，指定操作系统的 Sentinel 管理员用户名及其用户主目录的位置。这是所安装 Sentinel 产品所有者的用户名。如果此用户尚不存在，将创建此用户，并在指定的目录中创建其用户主目录。
  - ◆ 操作系统管理员用户名 - 默认为 `esecadm`
  - ◆ 操作系统管理员用户主目录 - 默认为 `“/export/home”`。如果用户名为 `esecadm`，则用户主目录将是 `/export/home/esecadm`。

---

**注释：**要满足通用条件认证所需的严格的安全性配置，请参阅第 2 章“最佳实践”（第 17 页）中的“设置口令 - 最佳实践”一节。

---

**注释：**不必设置口令即可创建 `esecadm` 用户。要以此用户的身份登录，将需要先设置其口令。

---



- 14 如果选择安装 Sentinel 控制中心，安装程序将提示输入要为 Sentinel 控制中心分配的最大内存空间。输入希望只供 Sentinel 控制中心使用的最大 JVM 内存堆大小 (MB)。
- ◆ JVM 内存堆大小 (MB) - 默认情况下，设置为在该计算机上检测到的物理内存的一半大小，最大为 1024 MB。

Sentinel 控制中心配置

指定 Sentinel 控制中心的 JVM 堆大小。安装程序检测到 2087 MB 的物理内存。允许的范围是 64-1024。

JVM 内存堆大小 (M)(MB)

256

- 15 为 Sentinel 客户端与服务器之间的通讯提供了两个选项。可以选择“直接讯息总线型”通讯或“代理型”通讯。有关这两个选项的更多信息，请参阅《安装指南》中的第 8 章“通讯层 (iSCALE)”（第 91 页）。

选择此收集器管理器应如何连接到讯息总线：

直接连接到讯息总线 (D)。

使用代理连接到讯息总线 (P)。

- 16 系统提示您输入端口 / 主机服务器名称的信息。输入所需的信息并单击“下一步”。如果选择“代理型”通讯，系统将要求您同时输入 Sentinel 通讯中心的代理端口。
- ◆ 讯息总线端口：讯息总线正在侦听的端口。直接连接到讯息总线的部件将使用此端口。
  - ◆ Sentinel 控制中心的代理端口：SSL 代理服务器（DAS 代理）正在侦听的端口，以接受基于用户名和口令的鉴定连接。因为 Sentinel 控制中心提示输入用户名和口令，所以，将使用此端口连接到 Sentinel 服务器。
  - ◆ 证书库鉴定的代理端口：SSL 代理服务器（DAS 代理）正在侦听的端口，以接受基于证书的鉴定连接。因为收集器管理器无法提示输入用户名和口令，所以，将使用此端口连接到 Sentinel 服务器（如果配置为通过代理连接）。

---

**注释：** Sentinel 系统中每台计算机上的端口号必须相同，才能进行通讯。请记录此信息，以便以后在其他计算机上安装。

---

- 17 如果要安装将直接连接到讯息总线的部件或要安装通讯服务器，系统将提示您如何获取共享讯息总线的加密密钥：
- ◆ 生成随机加密密钥（在安装通讯服务器时建议这样做）
  - ◆ 从密钥存储区文件导入加密密钥（在安装其他部件时建议这样做）系统将提示您选择导入加密密钥的源文件。

- ◆ .keystore 文件将放置在 \$ESEC\_HOME/config 中（在 Linux 和 Solaris OS 上）或 %ESEC\_HOME%\config 中（在 Windows OS 上）。

**18** 指定要生成随机密钥存储区文件还是从 Sentinel 系统中的其他计算机上导入现有的密钥存储区文件。

选择如何获取讯息总线加密密钥：

生成随机讯息总线加密密钥(G)。

为讯息总线通信生成随机加密密钥，并将其存储在密钥存储区文件中。通常，只有在安装通信服务器时才使用此选项。

从现有密钥存储区文件导入讯息总线加密密钥(I)。

从现有密钥存储区文件导入讯息总线加密密钥。在安装直接连接到讯息总线的组件并且在其他位置已生成密钥时使用此选项。导入的密钥必须与通信服务器所使用的密钥匹配。

---

**注释：**所有直接连接到讯息总线的部件必须共享相同的加密密钥。Novell 建议在安装通讯服务器时生成随机加密密钥，然后在其他计算机上安装部件时导入此密钥。通过代理连接的部件不需要共享讯息总线的加密密钥。

---

- 19** 如果选择导入现有的密钥存储区文件，则必须导航至相应的位置并选择密钥存储区文件。单击“下一步”。
- 20** 如果选择安装 DAS，请选择希望分配给数据访问服务的系统 RAM 大小。对于分布式环境，建议选择最大内存，因为数据库将需要占用部分内存。
- 21** 如果选择安装 DAS，但未选择安装 Sentinel 数据库，将提示您提供以下 Sentinel 数据库信息。此信息将用于配置 DAS，使其指向 Sentinel 数据库。
- ◆ 数据库主机名或 IP 地址 - 如果您希望配置 DAS 部件使其连接到现有的 Sentinel 数据库，可在此处提供该数据库的名称或 IP 地址。
  - ◆ 数据库名称 - 如果您希望配置 DAS 部件使其连接到 Sentinel 数据库实例，可在此处提供该实例的名称（默认为 ESEC）。
  - ◆ 数据库端口（默认值 - Microsoft SQL: 1433, Oracle: 1521）
  - ◆ Sentinel 应用程序数据库用户：指定“esecapp”作为登录名，并输入在安装 Sentinel 数据库期间为此用户指定的口令。

**22** 配置要安装的数据库：

**在 Windows 上：**

- ◆ 选择 Microsoft SQL server 2005 作为目标数据库服务器平台。
  - ◆ 创建包含数据库对象的新数据库 – 新建 Microsoft SQL 数据库并使用数据库对象填充新数据库
  - ◆ 将数据库对象添加到现有的空数据库：仅将数据库对象添加到现有的 Microsoft SQL 2005 数据库。现有数据库必须为空。

- ◆ 指定数据库安装日志目录。

单击“下一步”。

- ◆ 指定下列目录的存储位置：
  - ◆ 数据目录
  - ◆ 索引目录
  - ◆ 摘要数据目录
  - ◆ 摘要索引目录
  - ◆ 日志目录

单击“下一步”。

- ◆ 选择数据库字符集支持选项（Unicode 数据库或仅 ASCII 数据库）。如果选择非亚洲语言（列表中除了简体中文 / 繁体中文和日文以外的其他语言），系统将提示您在 Unicode 数据库和非 Unicode 数据库之间做出选择。选择数据库格式并单击“确定”。

---

**注释：**要完成 Unicode 数据库的安装，将需要更多的硬盘空间。

---

---

**注释：**如果选择亚洲语言，默认情况下将安装 Unicode 数据库。单击“下一步”。

---

- ◆ 指定数据库大小。单击“下一步”。
- ◆ 配置数据库分区。
  - ◆ 您可以选择“启用自动数据库分区”。
  - ◆ 对于数据分区，指定存档目录；输入添加和存档数据的指定时间。

单击“下一步”。

### 在 Linux/Solaris 上：

- ◆ 选择目标数据库服务器平台。
  - ◆ 从下拉列表中选择“Oracle 10g”。
  - ◆ 选择“创建包含数据库对象的新数据库”。

单击“下一步”。

- ◆ 指定 Oracle 用户名或接受默认用户名。单击“确定”。
- ◆ 如果选择新建数据库，请输入下列内容：
  - ◆ **Oracle JDBC 驱动程序文件的路径：**（jar 文件典型的名称为 ojdbc14.jar）。这是该 jar 文件的完全限定路径，通常为 \$ORACLE\_HOME/jdbc/lib/ojdbc14.jar（在此字段中不能使用环境变量）。
  - ◆ **主机名：**安装数据库的计算机的主机名。安装程序只支持在本地主机上创建新的数据库实例。
  - ◆ **数据库名称：**要安装的数据库实例的名称。
- ◆ 如果选择将数据库对象添加到现有的空 Oracle 数据库中，将提示您提供以下信息。

**Oracle JDBC 驱动程序文件的路径：**（jar 文件典型的名称为 ojdbc14.jar）。这是该 jar 文件的完全限定路径，通常为 \$ORACLE\_HOME/jdbc/lib/ojdbc14.jar（在此字段中不能使用环境变量）。

**数据库主机名或 IP 地址：** 您希望将数据库对象添加到的 Oracle 数据库所在主机的名称或 IP 地址。可以是本地主机名，也可以是远程主机名。

**数据库名称：** 您希望将数据库对象添加到的现有空 Oracle 数据库实例的名称（默认为 ESEC）。该数据库名称必须作为一个服务名称，出现在您正在运行安装程序的计算机的 tnsnames.ora 文件（位于 \$ORACLE\_HOME/network/admin 目录下）中。

**数据库端口：** 默认端口为 1521。

**口令：** 对于 Sentinel 数据库管理员用户 (DBA)，请为 “esecdba” 用户指定口令。该提示中的用户名字段不可编辑。

---

**注释：** 如果 tnsnames.ora 中不存在该数据库名称，安装程序此时不会向您发出错误提示（因为安装程序使用直接 JDBC 连接验证该连接），但是当数据库安装程序尝试通过 sqlplus 连接该数据库时，数据库安装将失败。如果这个时候数据库安装失败，则您应该不退出该安装程序，修改该计算机上 tnsnames.ora 文件中此数据库的服务名称，然后在安装程序中后退一个屏幕，再继续操作。这样，就会使用 tnsnames.ora 文件中的新值重试数据库安装。

---

**注释：** 安装程序将 tnsnames.ora 和 listener.ora 备份到 \$ORACLE\_HOME/network/admin 目录中。安装程序将使用 Sentinel 数据库的连接信息覆盖 listener.ora 文件，并将 Sentinel 数据库的连接信息追加到 tnsnames.ora 文件中。如果 Sentinel 数据库所在的服务器上还有其他数据库，管理员必须手动将备份 listener.ora 文件中的信息合并到新文件中，并重启动 Oracle 侦听程序，以便其他应用程序可以继续连接到该数据库。

---

- ◆ 在创建新数据库时，接受默认内存空间和侦听程序端口或指定新值。
- ◆ 输入 SYS 和 SYS 凭证，然后单击“下一步”。
- ◆ 指定数据库大小。可以选择“标准”、“大”或“自定义”。如果选择“自定义”，系统将提示您输入：
  - ◆ 每个数据库文件的初始大小 (100 – 10,000)，单位 MB
  - ◆ 每个数据库文件的最大大小 (2,000 – 100,000)，单位 MB
  - ◆ 所有数据库文件的大小 (7,000 – 2,000,000)，单位 MB
  - ◆ 每个日志文件的大小 (100 – 100,000)，单位 MB
- ◆ 指定为事件和事件摘要表空间分配的数据库的总大小。
- ◆ 指定下列目录的存储位置：
  - ◆ 数据目录
  - ◆ 索引目录
  - ◆ 摘要数据目录
  - ◆ 摘要索引目录
  - ◆ 日志目录

单击“下一步”。

---

**注释：** 为了便于恢复以及提升性能，建议将这些位置安排在不同的输入输出设备上。

由于安装程序不会创建这些目录，因此在继续执行后续步骤之前，必须使用外部应用程序创建这些目录。

出于性能考虑，重做日志应指向可用的写入速度最快的磁盘。

Oracle 用户必须可对这些目录执行写操作。要使 Oracle 用户可对这些目录执行写操作，以 root 用户身份对每个目录执行以下命令：

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

- 
- ◆ 假定 “oracle” 是您的 oracle 用户名，“dba” 是您的 oracle 组名。
  - ◆ 配置数据库分区。
    - ◆ 选择 “启用自动数据库分区” 并
    - ◆ 指定数据分区存档目录。
    - ◆ 输入添加和存档数据的指定时间。

单击 “下一步”。

**23** 输入下列用户的鉴定信息：

- ◆ Sentinel 数据库管理员用户
- ◆ Sentinel 应用程序数据库用户
- ◆ Sentinel 管理员用户
- ◆ Sentinel 报告用户（仅在 Windows 上）

单击 “下一步”。

**24** 此时将显示指定的数据库参数的摘要。单击 “下一步”。

**25** 如果选择安装 DAS，请配置 Sentinel 电子邮件支持。指定执行服务在发送邮件时应使用的 SMTP 服务器以及发件人电子邮件地址（可选 – 在 Linux/Solaris 上安装 \$ESEC\_HOME/sentinel/config/execution.properties 之后以及在 Windows 上安装 %ESEC\_HOME%/sentinel/config/execution.properties 之后，可以手动编辑此设置。）

**26** 如果选择安装顾问，将出现以下提示，要求提供安装类型：

- ◆ **直接因特网下载：** Advisor 计算机直接连接到因特网。在这种配置下，将通过因特网定期从 Novell 万维网站点自动下载更新。
- ◆ **独立：** Advisor 配置为独立系统，要求人工介入才能从 Sentinel 接收更新。

**27** 如果选择安装顾问，并选择使用 “Direct Internet Download”，请输入您的顾问用户名、口令以及更新顾问数据的频率。单击 “下一步”。如果未验证用户名和口令，系统将询问您是否要继续（不建议）。如果选择继续，在口令确认窗口中再次输入您的顾问口令。否则，请改正您的顾问口令。

**28** 如果选择安装顾问，请输入：

- ◆ 发件人地址，它将显示在电子邮件通知中
- ◆ 电子邮件通知的收件人地址

---

**注释：**安装完成后，通过编辑 attackcontainer.xml 和 alertcontainer.xml 可更改顾问电子邮件地址。有关更多信息，请参阅《Sentinel 用户指南》中的“‘Advisor’选项卡”。

---

- ◆ 选择 “Yes” 或 “No” 确认是否希望接收通知顾问更新成功的电子邮件。

---

**注释：**错误通知则始终都会发送。

---

**29** 单击 “下一步”。此时将出现包含已选装的功能的摘要屏幕。单击 “安装”。

---

**注释：**如果选择安装 HP Service Desk 或 Remedy Integration，将提示您提供更详细的信息。有关更多信息，请参阅《Sentinel 第三方集成指南》。

---

**30** 在成功安装之后，系统将提示您重引导。单击“完成”重引导系统。

---

**注释：**Sentinel 安装程序在默认情况下会关闭存档日志记录功能。出于恢复数据库的目的，强烈建议您在安装结束之后先打开存档日志功能，然后再开始接收生产事件数据。您还应该定期备份您的存档日志，以释放存档日志目标的空间，否则您的数据库将停止接受事件。

---

---

**注释：**如果预计事件发生率较高（每秒的事件数大于 500），则必须按照“在数据库创建期间设置 Oracle 调用接口 (OCI) 事件插入策略”一节中的其他配置说明操作。

---

## Linux/Solaris 上的控制台安装

```
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]
```

## 客户程序安装

Sentinel 控制中心、Collector Builder 和 Sentinel 数据管理器可以使用完整安装程序进行安装，也可以使用仅客户端安装程序进行安装。通过主安装程序可以选择三个应用程序中的任何一个，仅客户端安装程序自动安装全部三个应用程序。

---

**注释：**由于仅客户端安装程序自动安装 Collector Builder，所以，只能在 Windows 操作系统上使用此安装程序。所有这些基于 Windows 的应用程序都可以与基于 Linux 的 Sentinel 服务器一起使用。

---

### 使用仅客户端安装程序安装 Sentinel 控制中心和 Collector Builder:

- 1 浏览到 CD 并运行 setup.sh（在 Linux 和 Solaris 上）或 setup.bat（在 Windows 上）。安装向导将初始化。
- 2 选择向导要使用的语言，然后单击“确定”。
- 3 此时将显示“Sentinel 欢迎”屏幕。阅读“Welcome”（欢迎）屏幕后单击“下一步”。
- 4 此时将显示“Sentinel 最终用户许可协议”屏幕。阅读并接受《最终用户许可协议》并单击“下一步”。
- 5 接受默认的安装目录，或单击“浏览”指定安装位置。单击“下一步”。
- 6 输入安装通讯服务器的主机地址。
- 7 选择“生成随机密钥存储区文件”，然后单击“下一步”。
- 8 单击“下一步”。
- 9 此时将显示安装摘要。单击“安装”。
- 10 成功安装后，单击“完成”。

## 3.4 安装后配置

### 3.4.1 更新用于 SMTP 鉴定的 Sentinel 电子邮件

如果系统要求进行 SMTP 鉴定，则需要更新 `execution.properties` 文件。该文件位于安装了 DAS 的计算机上。该文件位于 `$ESEC_HOME/sentinel/config`。要配置该文件，运行 `mailconfig.sh` 更改该文件，然后运行 `mailconfigtest.sh` 测试更改。

#### 配置 `execution.properties` 文件：

---

**注释：**此示例是在 Linux/Solaris 操作系统上。必须对 Windows 操作系统进行类似的配置。

---

- 1 在安装了 DAS 的计算机上，以 Sentinel 管理员用户的身份登录，并转到：

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

- 2 按如下方式执行 `mailconfig`:

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

示例：

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

输入该命令后，将提示您提供新口令。

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

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

---

**注释：**使用口令选项时，它必须是最后一个自变量。

---

#### 测试 `execution.properties` 配置：

- 1 在安装了 DAS 的计算机上，以 Sentinel 管理员用户的身份登录，并转到：

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

- 2 按如下方式执行 `mailconfigtest`:

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

如果邮件发送成功，屏幕输出上将显示以下信息，同时目标地址将收到电子邮件。

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

检查目标电子邮件邮箱，确认收到电子邮件。主题行和正文应如下所示：

```
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 Sentinel 数据库

---

**注释：**默认情况下，安装程序将所有表空间设置为自动增长。默认情况下，文件增长大小为 200 MB，但是，最大文件大小取决于安装期间提供的值（例如 2000MB 等）。

应启用 Sentinel 数据库自动分区管理（存档、删除和添加分区），以使事件数据保持在受控制的大小之内。可以使用 Sentinel 数据管理器 (SDM) 配置自动分区管理。

---

应安排进行 SDM 分区管理（存档、删除和添加分区）以控制事件数据的大小。



Sentinel 数据库安装完成后，该数据库将包含以下默认用户：

- ◆ **esecdba:** 数据库纲要所有者。出于安全考虑，未向 Sentinel 数据库用户授予 DBA 特权。要使用 Enterprise Manager，应创建具有 DBA 特权的用户。
- ◆ **esecapp:** 数据库应用程序用户。这是用于连接到数据库的应用程序用户。
- ◆ **esecadm:** 作为 Sentinel 管理员的数据库用户。此帐户不是 Sentinel 管理员操作系统用户的用户帐户。
- ◆ **esecrpt:** 数据库报告用户
- ◆ **SYS:** SYS 数据库用户
- ◆ **SYSTEM:** SYSTEM 数据库用户

### 3.4.3 收集器服务

在安装收集器服务期间，将配置名为“常规收集器”的收集器。可以使用此收集器测试安装。

---

**注释：**有关详细信息，请参见第 5 章“测试安装”（第 71 页）

---

**注释：**有关收集器的更多信息，请参阅 <http://support.novell.com/products/sentinel/collectors.html> (<http://support.novell.com/products/sentinel/collectors.html>)。

---

### 3.4.4 更新许可证密钥（通过评估密钥）

如果在评估之后购买了产品，请按照如下所述的过程更新系统中的许可证密钥，以避免重装。

#### 更新许可证密钥：

- 1 以 esecadm 身份登录到安装了 DAS 的计算机上。
- 2 在命令提示符下，转到目录 \$ESEC\_HOME/bin。
- 3 运行可执行程序：/softwarekey。系统将通过如下所示的菜单提示您。
  - ◆ 输入主密钥
  - ◆ 输入次密钥
  - ◆ 查看主密钥
  - ◆ 查看次密钥
  - ◆ 退出
- 4 键入 1 输入新的主密钥。



# 顾问配置

本章包含下列主题：

- ◆ [安装顾问](#)（第 67 页）
- ◆ [重设置顾问口令](#)（仅限直接下载）（第 70 页）

本章讨论如何配置 Sentinel，以便直接通过 Sentinel 控制中心运行 Advisor 报告。Advisor 报告由 Novell 创建，用于报告和分析。正确配置了 Sentinel 控制中心集成后，将出现在“Advisor”选项卡中。

## 4.1 Advisor 概述

Sentinel Advisor 针对企业漏洞提供实时智能，提供专家建议并推荐补救措施。Advisor 还提供漏洞利用检测，这是实时 IDS 攻击签名与 Advisor 漏洞知识库之间的交叉参照。

---

**注释：**顾问的安装是可选的。但是，如果您希望使用 Sentinel 漏洞利用检测或 Advisor 报告功能，则 Advisor 为必需部件。Advisor 是一项基于订阅的数据服务。

---

受支持的系统为：

入侵检测系统	漏洞扫描程序
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	防火墙
Symantec Network Security 4.0 (ManHunt)	Cisco IOS Firewall
Symantec Intruder Alert	
McAfee IntruShield	

## 4.2 安装顾问

---

**注释：**Advisor 必须安装在数据库访问服务 (DAS) 所在的计算机上。

---

有两个不同的安装选项可供选用。它们是：

- ◆ 独立
- ◆ 直接从因特网下载

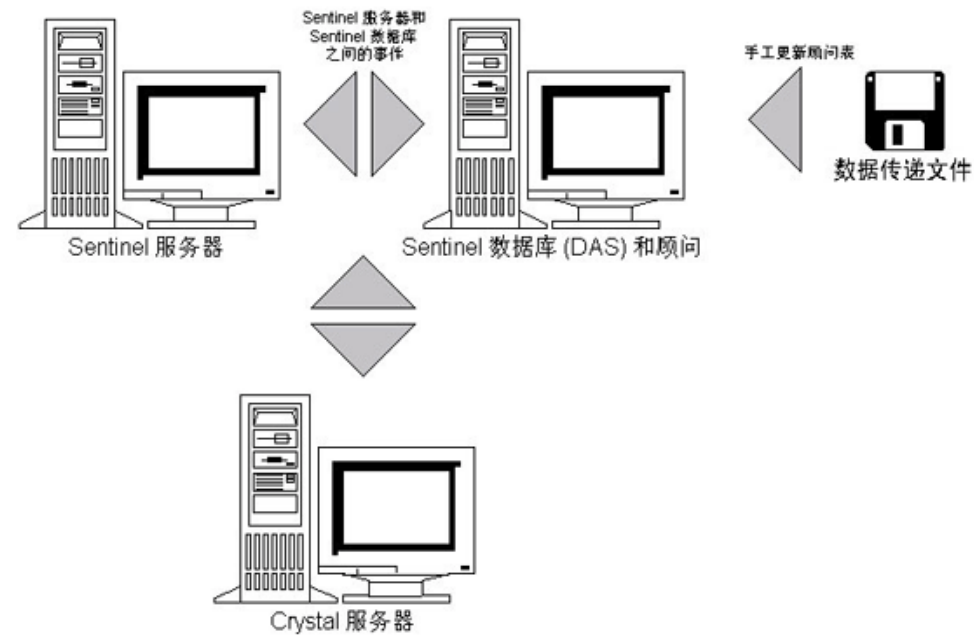
---

**注释：**安装顾问之前，请确保您具有由 Novell 提供的顾问用户名和口令。安装过程中，将提示您提供用户名和口令。

---

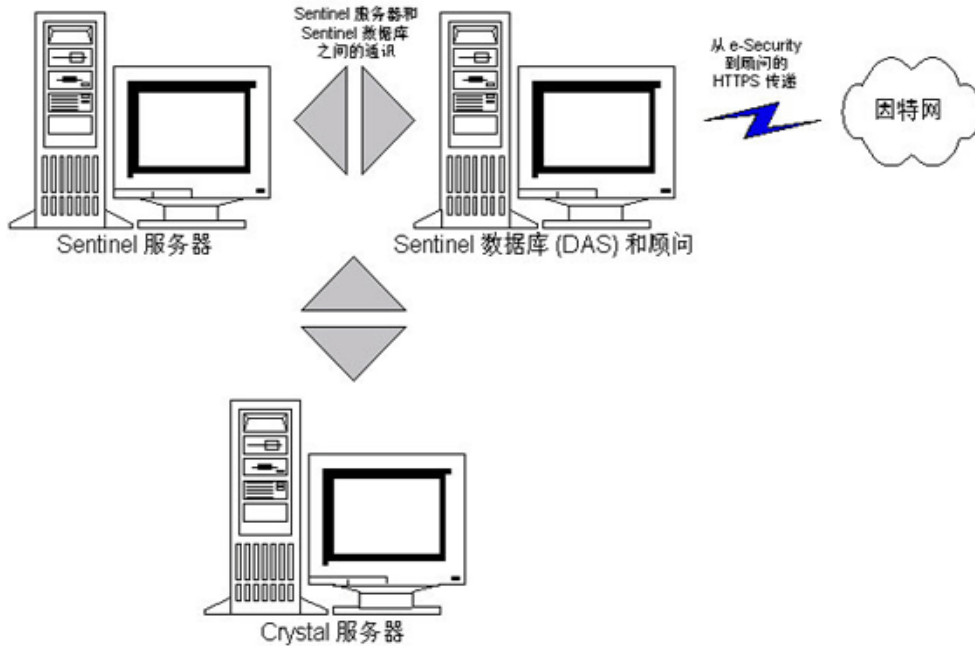
### 4.2.1 独立配置

若采用独立安装，顾问将是一个孤立的系统，需要进行手工操作才能从 Novell 接收更新。



### 4.2.2 直接从因特网下载配置

若采用直接从因特网下载，顾问计算机将直接连接到因特网上。在这种配置下，将通过因特网定期从 Novell 万维网站点自动下载更新。



## 4.3 Advisor 报告

Crystal BusinessObjects Enterprise™ XI 是与 Sentinel 集成的报告工具。有关 Crystal BusinessObjects Enterprise™ XI 安装的更多信息，请参阅《安装指南》中的第 9 章“用于 Windows 的 Crystal Reports”（第 97 页）和第 10 章“用于 Linux 的 Crystal Reports”（第 123 页）。

---

**注释：**只有要运行报告时才需要 Crystal Server。如果打算仅将顾问用于漏洞利用检测，则无需安装 Crystal 服务器。

---

在 Advisor 上运行 Crystal 报告：

- ◆ 安装并配置 Crystal Server。有关更多信息，请参阅《安装指南》中的第 9 章“用于 Windows 的 Crystal Reports”（第 97 页）。
- ◆ 将 Advisor Crystal Reports 发布到 Crystal Server。有关更多信息，请参阅“导入报告模板”。

### 4.3.1 Advisor 报告配置

如果您打算运行 Advisor 报告（Crystal Reports），请按照所示的顺序执行下列步骤。如果您打算仅将顾问用于漏洞利用检测，则无需执行以下步骤。

- ◆ 如果尚未完成，请执行下列操作（有关更多信息，请参阅《安装指南》中的第 9 章“用于 Windows 的 Crystal Reports”（第 97 页））：
  - ◆ 安装 Microsoft Internet 信息服务 (IIS)
  - ◆ 安装 Crystal BusinessObjects Enterprise™ 11
  - ◆ 对于 Oracle 上的 Sentinel 数据库 (Solaris/Linux)：配置 Oracle 本机驱动程序（对于 Oracle 安装）

- ◆ 对于 Microsoft SQL 2005 上的 Sentinel 数据库 (Windows): 配置开放数据库连接 (ODBC)
- ◆ 为 Crystal Reports 安装增补程序。有关更多信息, 请参阅《安装指南》中的第 9 章“用于 Windows 的 Crystal Reports” (第 97 页)。
- ◆ 安装 Advisor – 有关安装 Advisor 的更多信息, 请参阅《安装指南》中的第 7 章“安装 Sentinel 部件” (第 85 页)。
- ◆ 导入 Crystal Report 模板
- ◆ 创建 Crystal 万维网主页
- ◆ 将 Sentinel 控制中心配置为与 Crystal Enterprise 服务器集成

---

**注释:** 有关导入报告模板和配置 Sentinel 控制中心以显示 Advisor 报告的更多信息, 请参阅《安装指南》中的第 9 章“用于 Windows 的 Crystal Reports” (第 97 页) 和第 10 章“用于 Linux 的 Crystal Reports” (第 123 页)。

---

## 4.4 更新顾问表中的数据

除非您具有独立配置, 否则在安排的下一次顾问传递下载过程中将自动更新顾问表中的数据。但是, 也可以手工更新这些数据。有关手动更新的更多信息, 请参阅《Sentinel 用户指南》中的“Advisor 的使用和维护”。

## 4.5 重设置顾问口令 (仅限直接下载)

如果您以直接下载方式运行顾问并且已获得新的顾问口令, 或安装时设置的顾问口令不正确, 则需要重设置存储在顾问配置文件中的加密顾问口令。

如果是在独立配置中运行顾问, 则无法更新加密顾问口令, 因为在此方式中, 口令并未存储在顾问配置文件中。

要重设置存储在顾问配置文件中的加密顾问口令, 请执行以下步骤:

- 1 在 UNIX 上, 以 `esecadm` 身份登录; 在 Windows 上, 以具有管理权限的用户身份登录。登录到已安装顾问的计算机上。
- 2 转至:
  - 对于 UNIX:  
`$ESEC_HOME/bin`
  - 对于 Windows 系统:  
`%ESEC_HOME%\bin`
- 3 执行以下命令:
  - 对于 UNIX:  
`./adv_change_passwd.sh <newpassword>`
  - 对于 Windows 系统:  
`adv_change_passwd.bat <newpassword>`其中 `<newpassword>` 是要设置的 Advisor 口令。

# 测试安装

本章包含下列主题：

- ◆ 测试安装（第 71 页）
- ◆ 通过测试进行清理（第 80 页）
- ◆ 入门（第 80 页）

## 5.1 测试安装

Sentinel 随演示版收集器一起安装，演示版收集器可以用于测试系统的许多基本功能。使用此收集器可以测试活动视图、事件创建、关联规则和报告。以下过程介绍测试系统的步骤以及预计的结果。您看到的结果可能不完全相同，但是结果应与以下结果类似。

通过这些测试，基本上可以确认下列事项：

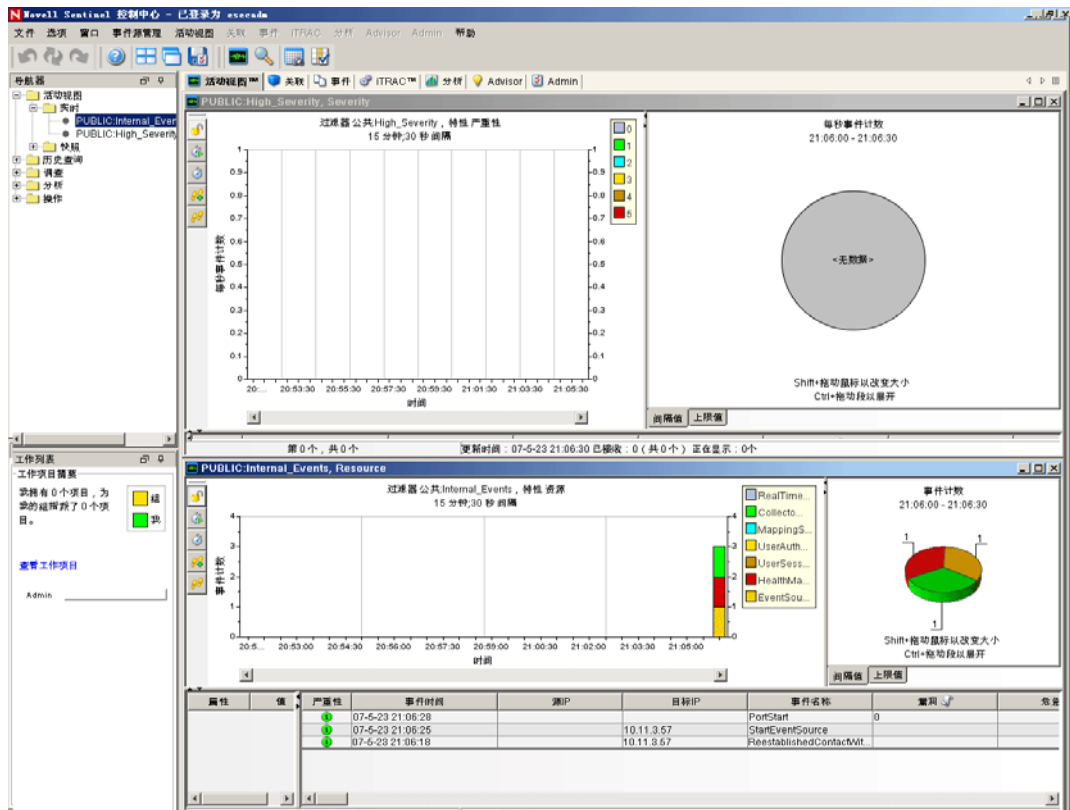
- ◆ Sentinel 服务已启动并且正在运行
- ◆ 可以通过讯息总线进行通讯
- ◆ 正在发送内部审计事件
- ◆ 可以通过收集器管理器发送事件
- ◆ 正在将事件插入数据库，可以使用历史事件查询或报告服务器进行检索
- ◆ 可以创建和查看事件
- ◆ 关联引擎正在评估规则并触发关联的事件
- ◆ Sentinel 数据管理器可以连接到数据库并读取分区信息

如果其中的任何测试失败，请审阅安装日志和其他日志文件，如果需要，请与 Novell 技术支持部门联系。

### 测试安装：

- 1 双击桌面上的“Sentinel 控制中心”图标。

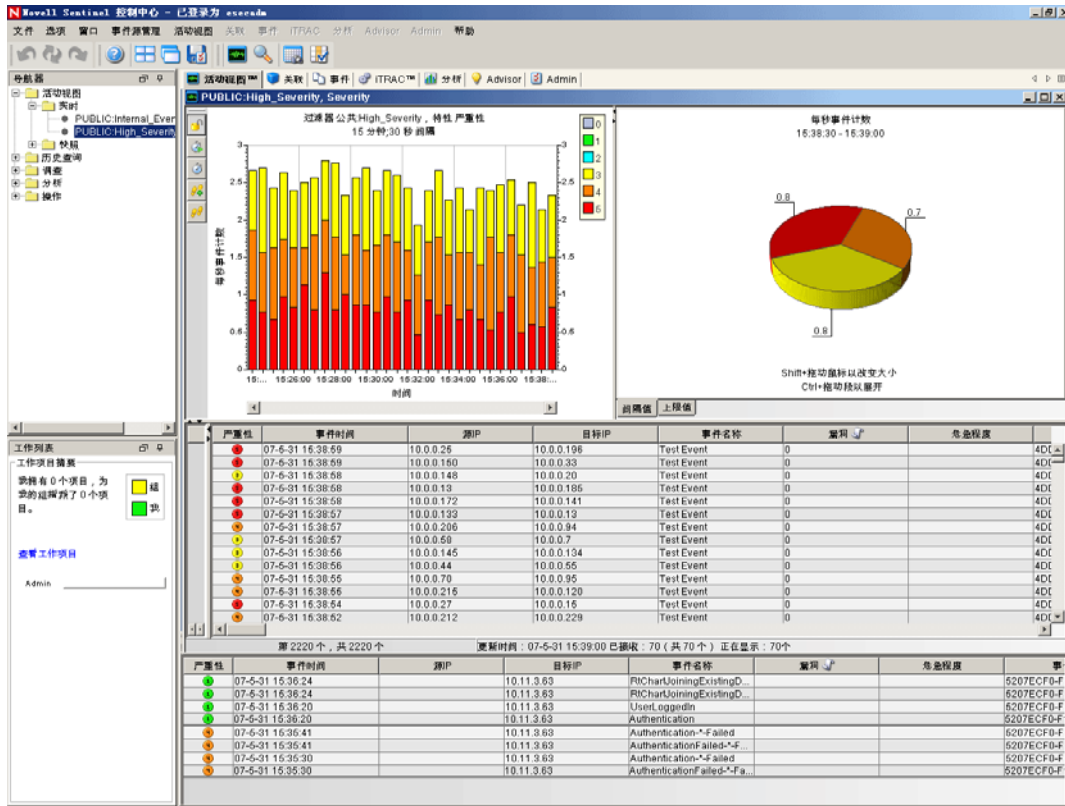
- 2 使用安装期间指定的 Sentinel 管理用户（默认用户为 esecadm）登录到系统上。Sentinel 控制中心将打开，您可能会看到“活动视图”选项卡，并打开一个名为“公共：所有，严重性”的窗口。



- 3 转到“事件源管理”菜单并选择“实时视图”。
- 4 在图形视图中，右击 5 eps 事件源，然后选择“启动”。
- 5 关闭“事件源管理实时视图”窗口。



6 转到“活动视图”选项卡。此时将出现一个名为“公共：高严重性，严重性”的实时窗口。启动收集器并在此窗口中显示数据可能需要一段时间。



7 单击工具栏中的“事件查询”按钮。此时将显示“历史事件查询”窗口。

8 在“历史事件查询”窗口中，单击“过滤器”下拉箭头选择过滤器。高亮显示“公共：所有”过滤器，然后单击“选择”。

9 选择收集器处于活动状态的时段。通过“从”和“到”下拉箭头选择日期范围。

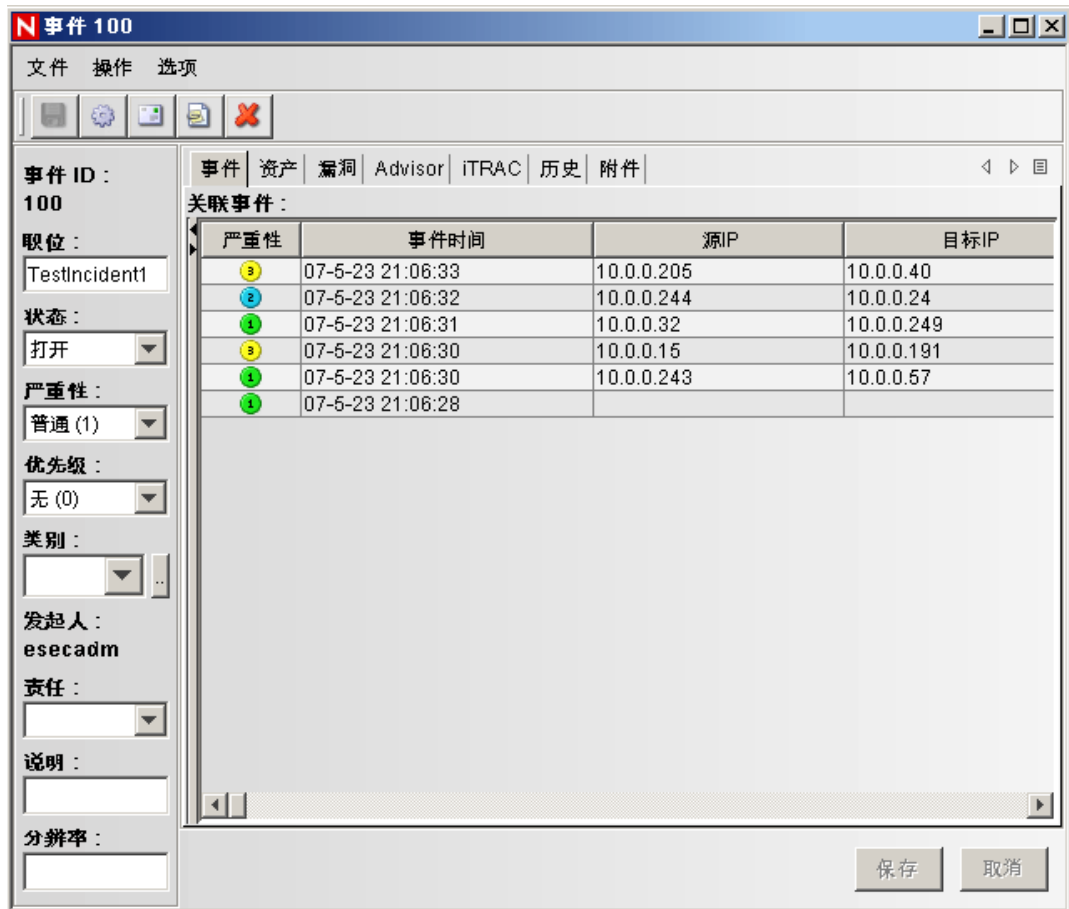
10 通过“批大小”下拉箭头选择批大小。

11 单击放大镜图标运行查询。



12 按住 Ctrl 或 Shift 键，从历史事件查询窗口中选择多个事件。

13 单击右键并选择“创建事件”。



- 14 将事件命名为 TestIncident1，然后单击“创建”。此时将显示成功通知。单击“确定”。
- 15 转到“事件”选项卡。此时将显示“事件视图管理器”。在“事件视图管理器”中，将可以看到刚创建的事件。

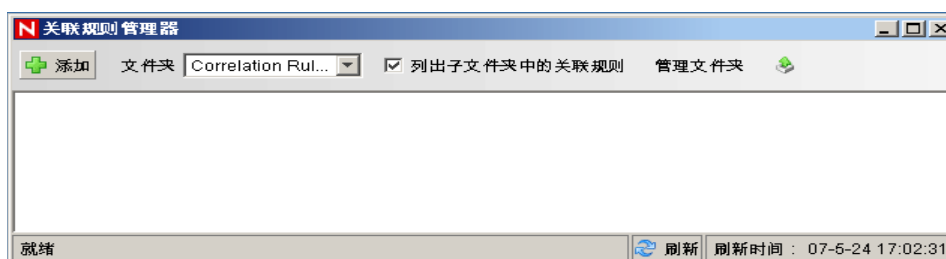


- 16 双击要打开的事件。



- 17 关闭事件窗口，转到“文件” > “退出”关闭，或通过单击窗口右上角的“X”关闭。
- 18 单击“分析”选项卡。在“分析导航器”中，打开“历史报告”文件夹。
- 19 单击“事件查询”。

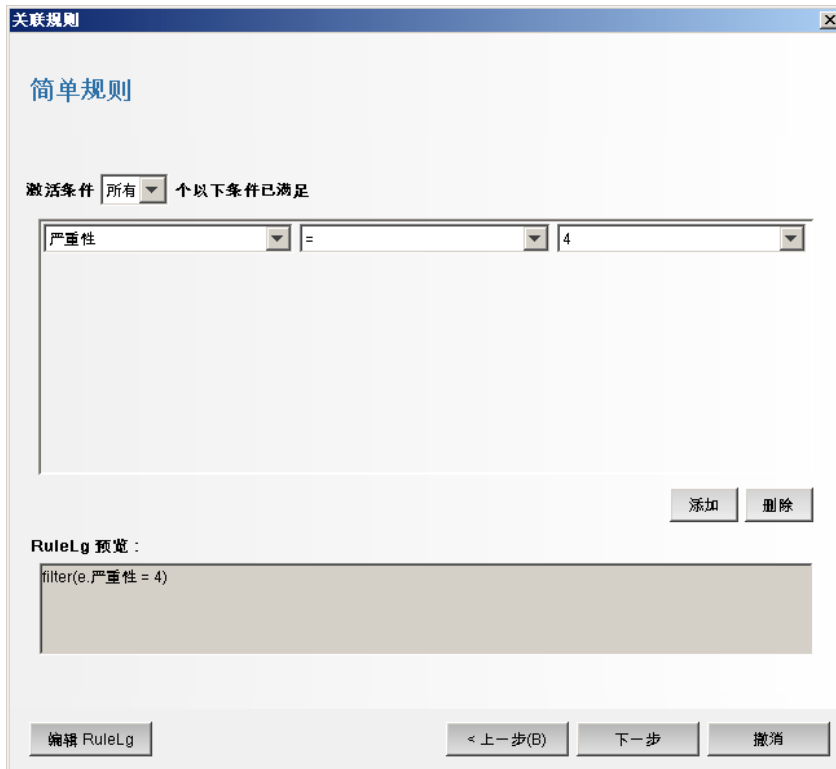
- 20 单击“分析” > “创建报告”，或单击“创建报告”图标。此时将打开一个“事件查询”窗口。设置下列选项：
  - ◆ 时间框
  - ◆ 过滤器
  - ◆ 严重性级别
  - ◆ 批大小（此值是要查看的事件数 – 事件从最早的事件显示到较新的事件）
- 21 单击“刷新查询”。
- 22 要查看下一批事件，单击“更多”。
- 23 通过拖放重排各列，并通过单击列标题设置排列顺序。
- 24 查询完成后，将加入导航器中的快速查询列表。
- 25 转到“关联”选项卡。此时将显示“关联规则管理器”。



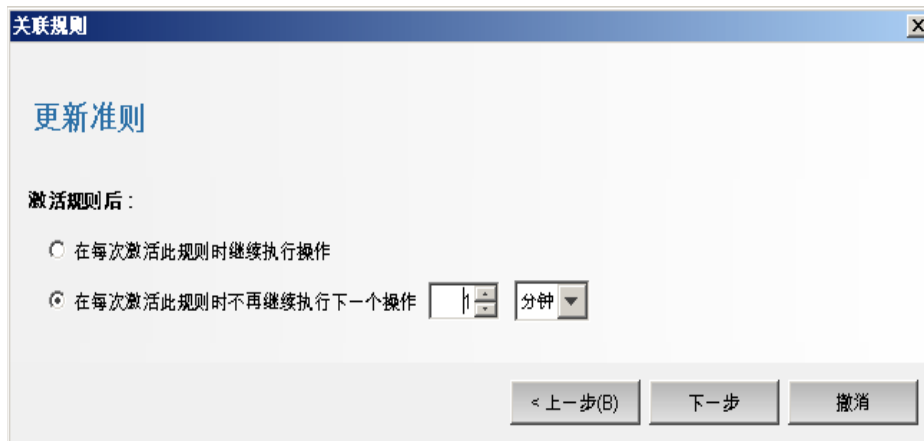
- 26 单击“添加”。“关联规则向导”将打开。



27 单击“简单”。此时将显示“简单规则”窗口。



28 使用下拉菜单将条件设置为“严重性=4”。单击“下一步”。此时将显示“更新条件”窗口。



- 29 选择“每次激活此规则时不执行操作的时间”，并使用下拉菜单将时段设置为“1分钟”。单击“下一步”。此时将显示“常规说明”窗口。



- 30 将该规则命名为“TestRule1”，输入说明，然后单击“下一步”。
- 31 选择“否，不创建其他规则”并单击“下一步”。
- 32 打开“关联规则管理器”窗口。
- 33 高亮显示规则，然后单击“部署规则”链接。此时将显示“部署规则”窗口。



- 34 在“部署规则”窗口中，从下拉列表中选择要部署规则的引擎。
- 35 选择“发送电子邮件”操作与该规则关联，然后单击“确定”。

36 选择“关联引擎管理器”。在关联引擎下，可以看到该规则已部署 / 启用。



37 转到“活动视图”选项卡，并验证“关联的事件”是否已生成。

严重性	事件时间	源 IP	目标 IP	事件名称	漏洞	危急程度
●	2007/6/7 下午 11:20	10.0.0.42	10.0.0.88		0	B3622
●	2007/6/7 下午 11:20	10.0.0.148	10.0.0.188		0	B3622
●	2007/6/7 下午 11:20	10.0.0.4	10.0.0.57		0	B3622
●	2007/6/7 下午 11:20	10.0.0.234	10.0.0.236		0	B3622
●	2007/6/7 下午 11:20	10.0.0.48	10.0.0.147		0	B3622
●	2007/6/7 下午 11:20	10.0.0.174	10.0.0.99		0	B3622
●	2007/6/7 下午 11:20	10.0.0.61	10.0.0.130		0	B3622
●	2007/6/7 下午 11:20	10.0.0.228	10.0.0.180		0	B3622
●	2007/6/7 下午 11:20			CorrelatedEvent		AD50A
●	2007/6/7 下午 11:20	10.0.0.48	10.0.0.85		0	B3622
●	2007/6/7 下午 11:20	10.0.0.254	10.0.0.112		0	B3622
●	2007/6/7 下午 11:20	10.0.0.69	10.0.0.91		0	B3622
●	2007/6/7 下午 11:20	10.0.0.70	10.0.0.183		0	B3622

38 关闭“Sentinel 控制中心”。

39 双击桌面上的“Sentinel 数据管理器 (SDM)”图标。

40 使用安装期间指定的数据库管理用户登录到 SDM（默认用户为 esecdba）。



41 单击每个选项卡，以验证是否可以访问。

42 关闭“Sentinel 数据管理器”。

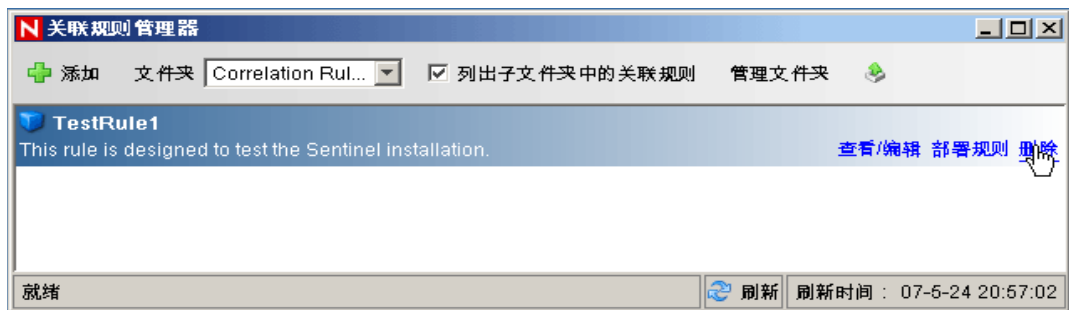
如果可以完成上述所有步骤而未出现任何错误，则已完成对 Sentinel 系统安装的基本验证。

## 5.2 通过测试进行清理

完成了系统验证之后，应去除为测试创建的对象。

**在系统测试后进行清理：**

- 1 使用安装期间指定的 Sentinel 管理用户登录到系统（默认用户为 esecadm）。
- 2 转到“关联”选项卡。
- 3 打开“关联引擎管理器”。
- 4 在“关联引擎管理器”中右击 TestRule1，然后选择“取消部署”。
- 5 打开“关联规则管理器”。
- 6 选择 TestRule1 并单击“删除”。



- 7 转到“事件源管理”菜单并选择“实时视图”。
- 8 在图形事件源层次结构中，右击“常规收集器”并选择“停止”。
- 9 关闭“事件源管理”窗口。
- 10 转到“事件”选项卡。
- 11 打开“事件视图管理器”。
- 12 选择 TestIncident1，单击右键并选择“删除”。

## 5.3 入门

现在可以使用您的系统启动。有关更多信息，请参阅《SCC 用户指南》中的“快速入门”。



# 升级到 Sentinel 6

# 6

本章包含下列主题：

- ◆ 从 Sentinel 5.x 升级到 Sentinel 6.0（第 81 页）
- ◆ 从 Sentinel 4.x 升级到 Sentinel 6.0（第 82 页）

本章提供从早期版本的 Sentinel 升级到 Sentinel 6.0 的高级概述。基本步骤是备份早期版本的 Sentinel，安装 / 卸载软件，更改配置，以及迁移数据。

---

**注释：**本文档未提供执行升级的详细步骤。详细信息在 [Novell 文档万维网站点 \(http://www.novell.com/documentation/\)](http://www.novell.com/documentation/) 上提供的增补程序安装文档中提供。

---

可以用于增补到 Sentinel 6.0 的增补程序安装程序是：

- ◆ Sentinel 4.x 增补到 Sentinel 6.0
- ◆ Sentinel 5.x 增补到 Sentinel 6.0

Sentinel 6.0 与早期版本之间的几个重要改动可能会影响您的升级。增补程序安装文档中提供详细信息。

- ◆ Sentinel 5.x 与 6.0 之间进行了一些小的数据库纲要更改，Sentinel 4.x 与 6.0 之间进行了一些大的数据库纲要更改。由于纲要的更改，Sentinel 6.0 提供了新的报告库，自定义报告可能需要进行修改。
- ◆ 新的事件源管理框架可能要求对收集器进行一些小的更改，以便使用新连接器。
- ◆ Sentinel 控制中心用户拥有一些新的用户权限。
- ◆ 系统要求已更改，包括支持几种新平台。
- ◆ 目录结构已更改，所以，引用目录路径的底稿可能要求进行更新。

## 6.1 从 Sentinel 5.x 升级到 Sentinel 6.0

**注意事项：**

- ◆ 使用 Sentinel 增补程序安装程序从 Sentinel 5.x 就地升级到 Sentinel 6.0。
- ◆ 支持将数据从 Microsoft SQL Server 2000 for Sentinel 5.x 迁移到 Microsoft SQL Server 2005 for Sentinel 6.0。（Sentinel 6 中不再支持 SQL Server 2000。）
- ◆ 支持将数据从 Oracle 9i for Sentinel 5.x 迁移到 Oracle 10g for Sentinel 6.0。
- ◆ 不支持将数据从非 Unicode 数据库迁移到 Unicode 数据库。
- ◆ 成功迁移数据后，不迁移关联规则和 iTRAC 工作流程模板。关联规则可以从 5.x 导出并导入到 6.0。iTRAC 工作流程模板必须在 Sentinel 6.0 中重创建。

## 从 Sentinel 5.x 升级到 Sentinel 6.0:

- ◆ 验证系统要求
  - ◆ 验证系统的硬件规格是否满足第 2 章 “最佳实践”（第 17 页）中提到的硬件要求。
  - ◆ 验证操作系统和数据库的版本是否满足第 2 章 “最佳实践”（第 17 页）中提到的系统要求。
- ◆ 执行所需部件的备份
  - ◆ Sentinel 服务器
  - ◆ Sentinel 收集器管理器
  - ◆ Crystal Reporting Server
  - ◆ 数据库服务器
  - ◆ 收集器底稿
  - ◆ 导出关联规则
  - ◆ 备份 iTRAC 工作流程
- ◆ 运行 Novell 提供的增补程序安装程序
- ◆ 安装 Sentinel 6.0 数据库
- ◆ 执行数据迁移
- ◆ 安装 Sentinel 6.0（数据库除外）
- ◆ 配置对象
  - ◆ 更新用户权限
  - ◆ 更新菜单配置
  - ◆ 重配置电子邮件设置
  - ◆ 重部署收集器（某些收集器可能需要进行修改）
  - ◆ 重部署报告

## 6.2 从 Sentinel 4.x 升级到 Sentinel 6.0

### 注意事项:

- ◆ 支持将数据从 Microsoft SQL Server 2000 for Sentinel 4.x 迁移到 Microsoft SQL Server 2005 for Sentinel 6.0。（Sentinel 6 中不再支持 SQL Server 2000。）
- ◆ 支持将数据从 Oracle 9i for Sentinel 4.x 迁移到 Oracle 10g for Sentinel 6.0。
- ◆ 成功迁移数据后，下列对象从 Sentinel 4.x 迁移到 Sentinel 6.0:
  - ◆ 用户和指派的权限
  - ◆ 过滤器
  - ◆ 右击菜单配置选项
  - ◆ 重命名的 CV 标签
  - ◆ 分区配置
  - ◆ 4.x 中的案例作为事件迁移到 6.0
  - ◆ 事件和与事件相关的事件

- ◆ 成功迁移数据后，不迁移关联规则以及所有事件。关联规则可以从 5.x 导出并导入到 6.0。将迁移作为事件 (incident) 一部分的事件 (event)；不会迁移其他事件。

## 从 Sentinel 4.x 升级到 Sentinel 6.0:

- ◆ 系统要求
  - ◆ 验证系统的硬件规格是否满足第 2 章 “最佳实践” (第 17 页) 中提到的硬件要求。可能需要更新您的硬件，因为 Sentinel 4.x 和 Sentinel 6.0 的硬件规格有所不同。
  - ◆ 验证操作系统和数据库的版本是否满足第 2 章 “最佳实践” (第 17 页) 中提到的系统要求。
  - ◆ 执行所需部件的备份
  - ◆ Sentinel 服务器
  - ◆ Sentinel 收集器管理器
  - ◆ Crystal Reporting Server
  - ◆ 数据库服务器
  - ◆ 收集器底稿
  - ◆ 导出关联规则
  - ◆ 备份 iTRAC 工作流程
- ◆ 运行 Novell 提供的增补程序安装程序
- ◆ 安装 Sentinel 6.0 数据库
  - ◆ 您可能必须安装新数据库或新数据库实例。Sentinel 4.x 的数据库纲要与 Sentinel 6.0 有所不同。Sentinel 6.0 中添加 / 删除了一些表。安装新数据库或新数据库实例将在 Sentinel 6.0 中创建 / 删除这些表。
- ◆ 执行数据迁移
- ◆ 安装 Sentinel 6.0 (数据库除外)
- ◆ 配置对象
  - ◆ 更新用户权限
  - ◆ 更新菜单配置
  - ◆ 重配置电子邮件设置
  - ◆ 重部署收集器 (某些收集器可能需要进行修改)
  - ◆ 修改并重部署报告



# 安装 Sentinel 部件

本章包含下列主题：

- ◆ 在 Sentinel 计算机上安装新部件（第 85 页）
- ◆ 安装 Sentinel 数据库：（第 87 页）

下列几种情况可能需要向现有安装中添加部件：

- ◆ 计算机上有 Sentinel 部件，但是需要其他部件（例如，计算机上有收集器管理器，但是，添加 Sentinel 控制中心会很有帮助）
- ◆ 出于性能考虑，在事件发生率较高的环境中，可能会添加一个新的收集器管理器或关联引擎。

使用 Sentinel 安装程序很容易处理这两种情况。

## 7.1 在 Sentinel 计算机上安装新部件

有时，可能需要在 Sentinel 环境中再添加一台计算机。如果关联引擎上的内存利用率较高，可能会决定再添加一个关联引擎。可能会在远程站点添加一个收集器管理器，用于在本地收集数据，或者新员工可能需要在其台式机上安装 Sentinel 控制中心。

在新计算机上安装 Sentinel 部件有多个先决条件：

- ◆ 托管通讯服务器的计算机的 IP 地址或主机名
- ◆ 通过现有 Sentinel 安装中的任意计算机访问 .keystore 文件的副本
- ◆ 此文件可以在 %ESEC\_HOME%\config（在 Windows 上）或 \$ESEC\_HOME/config（在 Linux 和 Solaris 上）中找到。
- ◆ 必须可以通过要安装到的计算机浏览到 .keystore 文件。
- ◆ 初次安装 Sentinel 时使用的端口号

---

**注释：** Sentinel 系统中每台计算机上的 .keystore 文件和端口号必须相同，才能进行通讯。存在两个例外：如果要安装 Sentinel 控制中心或要使用 SSL 代理通讯安装收集器管理器，则不需要 .keystore 文件。

---

### 添加部件：

- 1 以拥有管理权限的用户的身分登录（在 Windows 上）；或以根用户的身分登录（在 Solaris 上）。
- 2 将 Sentinel 安装光盘插入 CD-ROM 驱动器。
- 3 浏览至该光盘并双击：
  - ◆ 在 Solaris 上，  
进入 GUI 方式：  
`./setup.sh`  
或

进入文本（“无头”）方式：

```
./setup.sh -console
```

- ◆ 在 Windows 上，运行 setup.bat。

---

**注释：**Windows 不支持以控制台方式进行安装。

---

- 4 阅读 “Welcome”（欢迎）屏幕后单击 “下一步”。
- 5 阅读并接受 《最终用户许可协议》并单击 “下一步”。
- 6 如果要安装其他部件，将显示一个屏幕，指示上一个安装的位置以及已安装的部件。如果要安装全新的 Sentinel，将显示一个屏幕，指示默认安装目录。单击 “浏览” 更改安装位置。单击 “下一步”。
- 7 选择要添加的部件。

方案 1：如果只安装应用程序：

- 7a 选择安装类型 “自定义” 安装并单击 “下一步”。
- 7b 选择 “应用程序”（Sentinel Collector Builder、Sentinel 控制中心和 Sentinel 数据管理器），然后单击 “下一步”。
- 7c 此时将出现 JVM（Java 虚拟机）内存堆大小提示。单击 “下一步”。  
JVM 内存堆大小 (MB) - 默认情况下，设置为在该计算机上检测到的物理内存的一半大小，最大为 1024 MB。这将是只能由 Sentinel 控制中心使用的最大 JVM 内存堆大小。
- 7d 系统提示您输入端口 / 主机服务器名称的信息。输入所需的信息并单击 “下一步”。

**方案 2：如果在安装应用程序之后安装关联引擎（其他部件）：**

- 7e 选择 “关联引擎”，然后单击 “下一步”。
- 7f 选择获取消息总线密钥的方法。指定要生成随机密钥存储区文件还是从 Sentinel 系统中的其他计算机导入现有的密钥存储区文件。如果选择导入现有的密钥存储区文件，则必须导航至相应的位置并选择密钥存储区文件。单击 “下一步”。

**方案 3：如果安装关联引擎和应用程序：**

- 7g 选择安装类型 “自定义” 安装并单击 “下一步”。
- 7h 选择 “应用程序”（Sentinel Collector Builder、Sentinel 控制中心和 Sentinel 数据管理器），然后单击 “下一步”。
- 7i 此时将出现 JVM（Java 虚拟机）内存堆大小提示。单击 “下一步”。
- 7j 系统提示您输入 Sentinel 控制中心代理端口和通讯服务器主机名信息。输入所需的信息并单击 “下一步”。
- 7k 选择获取消息总线加密密钥的方法。指定要生成随机密钥存储区文件还是从 Sentinel 系统中的其他计算机导入现有的密钥存储区文件。如果选择导入现有的密钥存储区文件，则必须导航至相应的位置并选择密钥存储区文件。单击 “下一步”。

**方案 4：如果安装 Sentinel 收集器服务和应用程序：**

- 7l 选择安装类型 “自定义” 安装并单击 “下一步”。

- 7m 选择“应用程序”（Sentinel Collector Builder、Sentinel 控制中心和 Sentinel 数据管理器），然后单击“下一步”。
- 7n 此时将出现 JVM（Java 虚拟机）内存堆大小提示。单击“下一步”。
- 7o 为 Sentinel 客户端与服务器之间的通讯提供了两个选项。可以选择“直接连接到消息总线”通讯或“使用代理连接到消息总线”通讯。单击“下一步”。
- 7p 系统提示您输入“消息总线端口”、“Sentinel 控制中心代理端口”和“通讯服务器主机名”信息。输入所需的信息并单击“下一步”。

---

**注释：**如果选择“使用代理连接到消息总线”，将增加一个“收集器管理器证书鉴定端口”选项。

---

- 7q 选择获取消息总线密钥的方法。指定要生成随机密钥存储区文件还是从 Sentinel 系统中的其他计算机导入现有的密钥存储区文件。如果选择导入现有的密钥存储区文件，则必须导航至相应的位置并选择密钥存储区文件。单击“下一步”。
- 8 此时将显示摘要屏幕。审阅安装摘要，然后单击“安装”。
- 9 安装完成后，将提示您进行重引导。选择“是，重新启动我的计算机”，并单击“完成”重引导系统。

## 7.1.1 安装 Sentinel 数据库：

### 安装 Sentinel 6 数据库：

- 1 在开始安装之前，如果以前已安装 Sentinel，请在 Windows 上删除下列环境变量。
  - ◆ ESEC\_HOME
  - ◆ ESEC\_VERSION
  - ◆ ESEC\_JAVA\_HOME
  - ◆ ESEC\_CONF\_FILE
  - ◆ WORKBENCH\_HOME
- 2 以拥有管理权限的用户的身分登录（在 Windows 上）。或以根用户的身分登录（在 Solaris 或 Linux 上）。
- 3 将 Sentinel 安装光盘插入 CD-ROM 驱动器。
- 4 浏览至该光盘并双击：
  - ◆ 在 Linux/Solaris 上，  
进入 GUI 方式：  
`./setup.sh`  
或  
进入文本（“无头”）方式：  
`./setup.sh -console`
  - ◆ 在 Windows 上，运行 `setup.bat`。

---

**注释：**Windows 不支持以控制台方式进行安装。

---

- 5 阅读“Welcome”（欢迎）屏幕后单击“下一步”。
- 6 阅读并接受《最终用户许可协议》并单击“下一步”。

7 接受默认的安装目录，或单击“Browse”指定其它位置。单击“下一步”。

目录(D):

- 8 对于安装类型，请选择“Custom”（默认）。单击“下一步”。
- 9 在功能选择窗口中，取消选择所有选项并选择“数据库”。单击“下一步”。

---

**注释：**请确保您取消选中了父“Sentinel Services”功能。如果仍选中 Sentinel 服务，而取消选择它的所有子功能，则 Sentinel 服务将变灰，同时带有白色选中标记。

---

10 配置要安装的数据库：

- ◆ 在 Windows 上：

**10a** 选择目标数据库服务器平台。

- ◆ 选择 Microsoft SQL Server 2005。
- ◆ 指定数据库安装日志目录。

单击“下一步”。

**10b** 指定下列目录的存储位置：

- ◆ 数据目录
- ◆ 索引目录
- ◆ 摘要数据目录
- ◆ 摘要索引目录
- ◆ 日志目录

单击“下一步”。

**10c** 选择数据库字符集支持选项（Unicode 数据库或仅 ASCII 数据库）。单击“下一步”。

**10d** 指定数据库大小。单击“下一步”。

**10e** 配置数据库分区。

- ◆ 您可以选择“启用自动数据库分区”。
- ◆ 对于数据分区，指定存档目录；输入添加和存档数据的指定时间。

单击“下一步”。

**在 Linux/Solaris 上：**

**10f** 选择目标数据库服务器平台。

- ◆ 从下拉列表中选择 Oracle 10g。
- ◆ 选择“创建包含数据库对象的新数据库”。

单击“下一步”。

**10g** 指定 Oracle 用户名或接受默认用户名。单击“确定”。

**10h** 选择 Oracle JDBC 驱动程序并指定数据库名称。单击“下一步”。

**10i** 接受默认内存空间和侦听程序端口或指定新值。



**10j** 输入 SYS 和 SYS 凭证，然后单击“下一步”。

**10k** 指定数据库大小。单击“下一步”。

**10l** 指定下列目录的存储位置：

- ◆ 数据目录
- ◆ 索引目录
- ◆ 摘要数据目录
- ◆ 摘要索引目录
- ◆ 日志目录

单击“下一步”。

**10m**配置数据库分区。

- ◆ 选择“启用自动数据库分区”并
- ◆ 指定数据分区存档目录。
- ◆ 输入添加和存档数据的指定时间。

单击“下一步”。

**11** 输入下列用户的鉴定信息：

- ◆ Sentinel 数据库管理员用户
- ◆ Sentinel 应用程序数据库用户
- ◆ Sentinel 管理员用户
- ◆ Sentinel 报告用户（仅在 Windows 上）

单击“下一步”。

**12** 此时将显示指定的数据库参数的摘要。单击“下一步”。

**13** 此时将显示安装摘要。单击“安装”。

**14** 成功安装后，选择重新启动系统并单击“完成”。



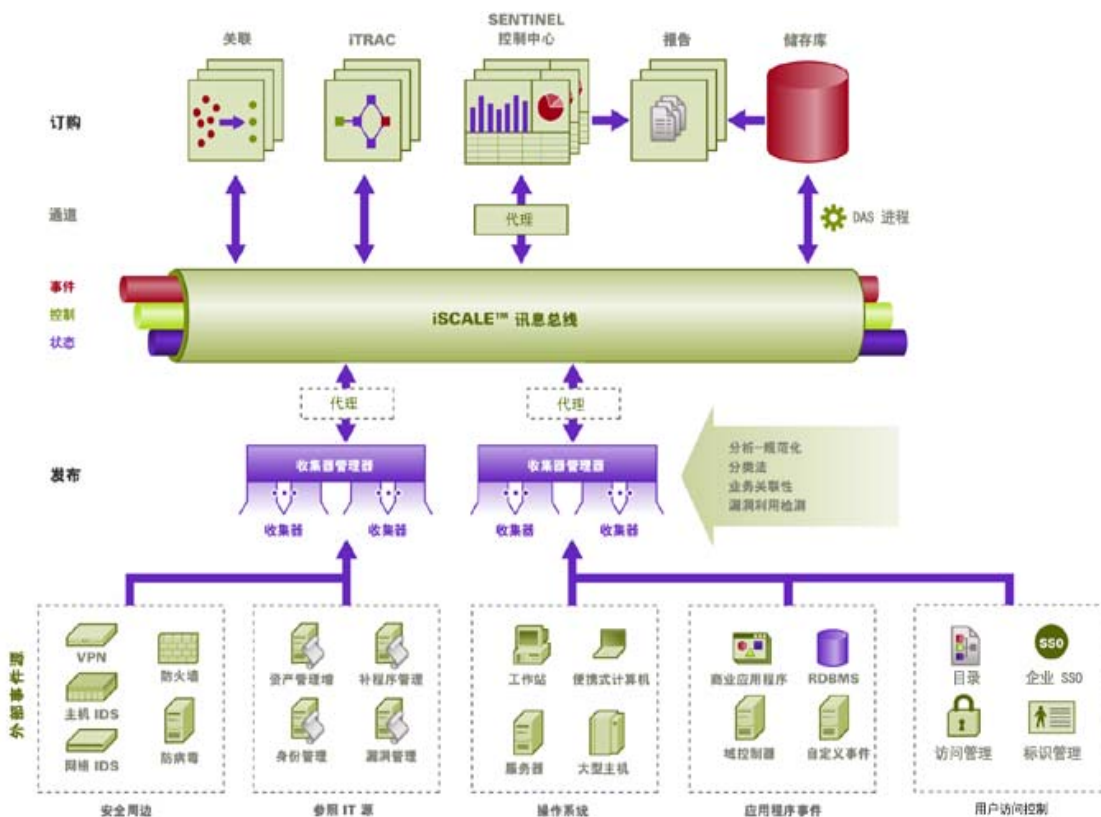
# 通讯层 (iSCALE)

# 8

本章中包含的主题：

- ◆ [SSL 代理和直接通讯 \(第 92 页\)](#)
- ◆ [加密密钥更改 \(第 95 页\)](#)

连接体系结构的所有部件的通讯层 (iSCALE) 是在 JMS (Java 讯息交换服务) 主干上建立的基于 TCP/IP 的加密连接。Sentinel 6 已增加了可选的 SSL 代理，用于保护安装在防火墙之外的收集器管理器和 Sentinel 控制中心部件。



安装收集器管理器时有两个可用的通讯选项：

- ◆ **直接连接到讯息总线 (默认)：** 这是最简单并且最快速的选项。但是，此选项要求收集器管理器了解共享讯息总线加密密钥，如果收集器管理器在受到安全威胁的计算机（例如 DMZ 中的计算机）上运行时，这样做可能会存在安全风险。此选项将基于称为 .keystore 的文件中的值，使用 AES 128 位加密对通讯进行加密。
- ◆ **通过代理连接到讯息总线：** 此选项将收集器管理器配置为通过 SSL 代理服务器进行连接，从而增加了一个安全保护层。在这种情况下，将使用基于证书的鉴定和加密，所以，.keystore 不必存储在收集器管理器计算机上。收集器管理器安装在不太安全的环境中时，适合使用此选项。

在安装收集器管理器时可以选择任何一个选项。默认情况下，Sentinel 控制中心使用代理。

## 8.1 SSL 代理和直接通讯

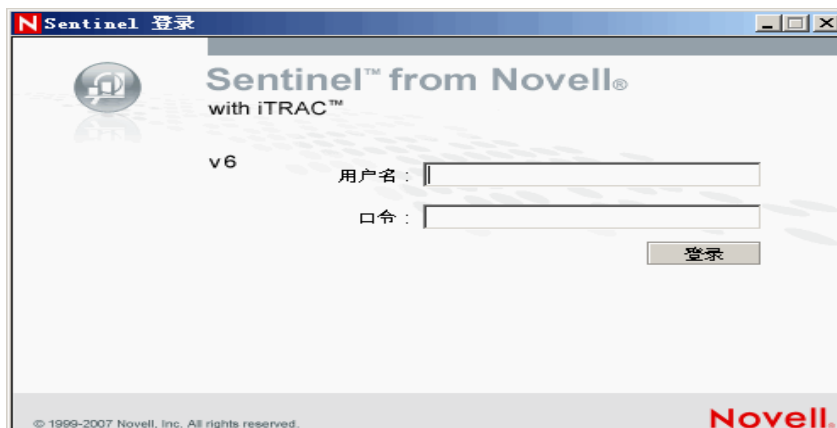
可能会使用 SSL 代理的 Sentinel 部件是 Sentinel 控制中心和收集器管理器。

### 8.1.1 Sentinel 控制中心

默认情况下，Sentinel 控制中心使用 SSL 代理。Sentinel 控制中心通过 proxied\_client 端口连接到 SSL。此端口设置为只使用服务器端的 SSL 证书鉴定。客户端鉴定使用 Sentinel 控制中心用户的用户名和口令。

**初次登录到 Sentinel 控制中心：**

- 1 转到“开始” > “程序” > “Sentinel”，然后选择“Sentinel 控制中心”。此时将显示 Sentinel 登录窗口。



- 2 输入为您提供的用户凭证，以登录到 Sentinel 控制中心。
  - ◆ 用户名和口令（如果使用 SQL Server 鉴定），或者
  - ◆ 域\用户名和口令（如果使用 Windows 鉴定）
- 3 单击“登录”。

4 初次尝试登录时，将显示下图中所示的警告讯息。



5 如果选择“接受”，将在每次尝试在系统上打开 Sentinel 时显示此讯息。为了避免出现这种情况，可以选择“永久接受”。

### 在 Linux 和 Solaris 上启动 Sentinel 控制中心：

- 1 以 Sentinel 管理员用户 (esecadm) 的身份将目录切换到：  
`$ESEC_HOME/bin`
- 2 运行以下命令：  
`control_center.sh`
- 3 输入用户名和口令，然后单击“确定”。
- 4 此时将显示证书窗口，单击“接受”。

在下面的情况下， Sentinel 控制中心用户将需要重复上述步骤，以接受新证书：

- ◆ 重安装 Sentinel 通讯服务器
- ◆ 将 Sentinel 通讯服务器移至新服务器

## 8.1.2 收集器管理器

收集器管理器可以在代理模式下安装（使用 SSL 代理），也可以在直接模式下安装（直接连接到讯息总线）。

- ◆ 对于可能更容易受到威胁的收集器管理器（例如 DMZ 中的计算机）， SSL 代理是更安全的通讯方法。
- ◆ 如果收集器管理器处于比较安全的环境中或高事件吞吐量非常重要的环境中，或者与数据访问服务 (DAS) 安装在同一台计算机上，则建议直接与讯息总线进行通讯。

收集器管理器通过 `proxied_trusted_client` 连接到 SSL。为了在重引导后，无须人工干预即可重新启动收集器管理器，请将此端口设置为同时使用服务器 SSL 证书鉴定和客户端 SSL 证书鉴定。在代理与收集器连接器之间建立信任关系（证书交换），以后的连接使用证书进行鉴定。此信任关系在安装期间自动建立。

在下列情况下，需要为每个使用 SSL 代理的收集器管理器重设置信任关系。

- ◆ 重安装 Sentinel 通讯服务器
- ◆ 将 Sentinel 通讯服务器移至新服务器

### 为收集器管理器重设置信任关系：

- 1 以 Sentinel 管理员的身份登录到收集器管理器服务器（默认用户为 esecadm）。
- 2 在文本编辑器中打开 \$ESEC\_HOME/config 或 %ESEC\_HOME%\config 中的 configuration.xml 文件。
- 3 将 configuration.xml 中的 “Collector\_Manager”、“agentmanager\_events” 和 “Sentinel” 服务修改为使用 “proxied\_trusted\_client” 策略 ID。以下是示例文件中的摘要：

```
<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 保存文件并退出。
- 5 在文本编辑器中打开 \$ESEC\_HOME/config 或 %ESEC\_HOME%\config 中的 sentinel.xml 文件。
- 6 将以下部件从 sentinel.xml 文件中去除：

```
<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 保存文件并退出。
- 8 运行 %ESEC\_HOME%\bin\register\_trusted\_client.bat（如果在 UNIX 上，则运行 .sh 文件）。您将看到类似如下所示的输出：

```
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 在托管通讯服务器的服务器上重新启动 Sentinel 服务。等待 DAS 代理完成初始化。
- 10 在托管收集器管理器的服务器上重新启动 Sentinel 服务。
- 11 对所有使用代理通讯的收集器管理器重复这些步骤。

## 8.2 加密密钥更改

Sentinel 安装允许管理员生成随机的新加密密钥（存储在 .keystore 文件中）或导入现有的 .keystore 文件。无论哪一种方法，Sentinel 环境中的每台计算机上的 .keystore 文件必须相同，才能正常进行通讯。

---

**注释：**如果数据库是数据库计算机上安装的唯一一个 Sentinel 部件，则该计算机上不需要 .keystore 文件。

---

可以使用称为 keymgr 的实用程序更改加密密钥。该程序会在 Sentinel 的安装目录 lib（\$ESEC\_HOME/lib 或 %ESEC\_HOME%\lib）中生成一个名为 .keystore 的文件。必须将该文件复制到安装了 Sentinel 部件的每台计算机上的相同目录中。

### 更改直接通讯的加密密钥：

**1** 对于 UNIX，以 Sentinel 管理员用户的身份登录（默认用户为 esecadm）。对于 Windows，请以具有管理权限的用户身份登录。

**2** 转至：

对于 Windows 系统：

```
%ESEC_HOME%\bin
```

对于 UNIX：

```
$ESEC_HOME/bin
```

**3** 运行以下命令：

在 Windows 上：

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

在 UNIX 上：

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

**4** 将 .keystore 复制到安装了 Sentinel 部件的每台计算机上（除非使用的是代理通讯）。此文件应复制到：

对于 Windows 系统：

```
%ESEC_HOME%\config
```

对于 UNIX：

```
$ESEC_HOME/config
```

### 8.2.1 Advisor 口令更改

如果要在直接下载模式下使用 Advisor，必须更新 Advisor 配置文件中存储的口令。此口令使用 .keystore 中的信息进行加密，必须使用新的 .keystore 值重创建。

#### 加密密钥更改后，为 Advisor 口令加密：

**1** 对于 UNIX，以 Sentinel 管理员用户的身份登录到安装了 Advisor 的计算机（默认用户为 esecadm）。对于 Windows，请以具有管理权限的用户身份登录。

**2** 将目录更改为：

对于 UNIX:

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

对于 Windows 系统:

```
%ESEC_HOME%\sentinel\bin
```

**3** 输入以下命令:

对于 UNIX:

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

对于 Windows 系统:

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



# 用于 Windows 的 Crystal Reports

# 9

本章包含下列主题：

- ◆ 配置要求（第 99 页）
- ◆ 安装 Microsoft Internet 信息服务 (IIS) 和 ASP.NET（第 100 页）
- ◆ 使用 Windows 鉴定执行 Microsoft SQL 2005 Server 安装概述（第 101 页）
- ◆ Oracle 安装概述（第 102 页）
- ◆ 使用 Windows 鉴定安装 Crystal Server for Microsoft SQL 2005 Server（第 102 页）
- ◆ 为 SQL 鉴定配置开放数据库连接 (ODBC)（第 110 页）
- ◆ 安装 Crystal Server for Oracle（第 111 页）
- ◆ 使用 Crystal 发布向导发布 Report 模板（第 115 页）
- ◆ 将 Sentinel 控制中心配置为与 Crystal Enterprise Server 集成（第 120 页）

Crystal BusinessObjects Enterprise™ XI 是一种报告工具。

本章讨论 Crystal Reports Server for Sentinel 的安装和配置。

Sentinel 支持在以下平台上运行 Crystal Reports Server：

- ◆ Windows – 在 Windows 或 Linux 上运行 Sentinel 数据库时支持。
- ◆ Linux - 在 Linux 上运行 Sentinel 数据库时支持。

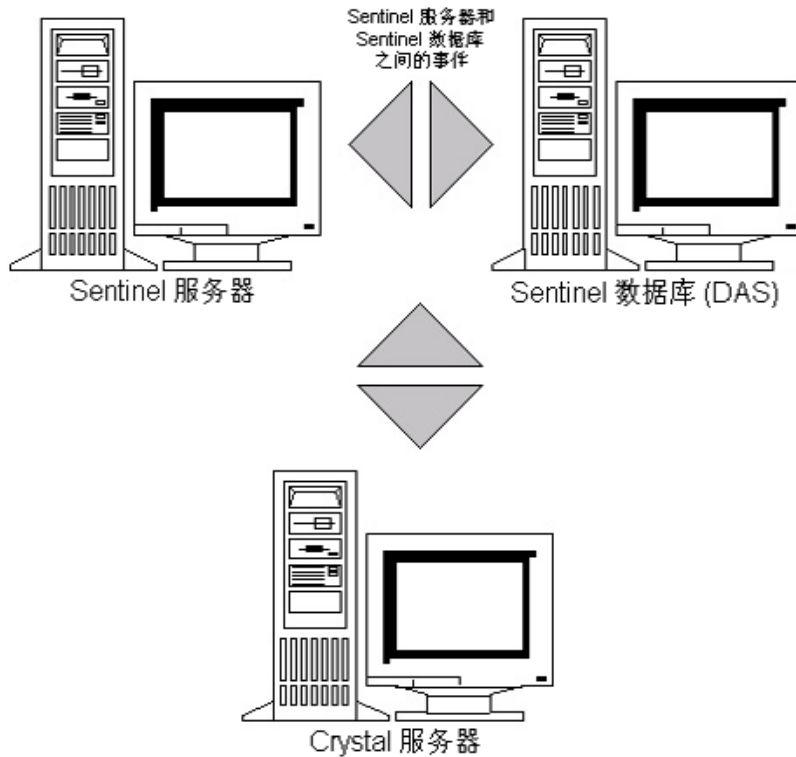
本章讨论在 Windows 上运行 Crystal Reports Server。有关在 Linux 上运行 Crystal Reports Server 的更多信息，请参阅第 10 章“用于 Linux 的 Crystal Reports”（第 123 页）。

## 安装 Crystal Reports Server:

- 1 安装 Microsoft IIS 和 ASP.NET
- 2 安装 Microsoft SQL（取决于配置是 Windows 鉴定还是 SQL Server 鉴定）
- 3 安装 Crystal 服务器
  - ◆ 为 SQL 身份验证配置开放式数据库连接 (ODBC)
  - 或
  - ◆ 安装并配置 Oracle 9i 客户端软件
- 4 配置 inetmgr
- 5 为 Crystal Reports 安装增补程序
- 6 发布（导入）Crystal Reports
- 7 设置“命名用户”帐户
- 8 测试万维网服务器的连接性
- 9 提高 Crystal Enterprise Server 报告刷新记录限制（推荐）
- 10 将 Sentinel 控制中心配置为与 Crystal Enterprise Server 集成。

应按以下顺序进行安装。

**注释：**必须按照上面所述的顺序安装 Crystal Reports Server。



## 9.1 概述

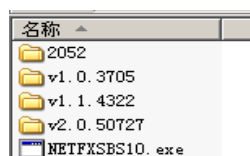
Crystal Reports Server 需要一个存储系统信息及其用户信息的数据库。该数据库称为中央管理服务器 (CMS) 数据库。CMS 是一种存储 Crystal Reports Server 系统信息的服务器。Crystal Reports Server 的其它部件可以根据需要访问这些信息。

这需要在本地 Microsoft SQL Server 数据库的顶部设置 CMS 数据库。如果尚未在本地安装 Microsoft SQL 2005 Server，则可以使用 Crystal Reports Server 安装程序在 MSDE 数据库的顶部设置 CMS 数据库。但 Sentinel 不支持 MSDE 配置。

## 9.2 系统要求

安装了 SP1 的 Windows<sup>®</sup> 2003 Server 系统，使用 NTFS 格式分区，且安装了 IIS（Microsoft Internet 信息服务）和 NET.ASP。在 Windows<sup>®</sup> 2000 Server 上，Sentinel 不支持 Crystal XI。

.NET Framework 1.1（默认情况下安装在 Windows 2003 上。BusinessObjects Enterprise™ XI 不支持 .NET Framework 2.0）。要确定计算机上 .NET Framework 的版本，可以转到 %SystemRoot%\Microsoft.NETFramework。文件夹的最大数字不应大于 v.1.1.xxxx。例如：

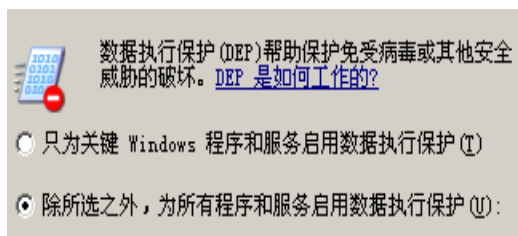


## 9.3 配置要求

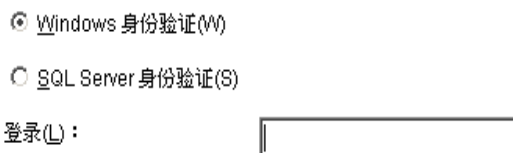
- 1 确保用于安装 Crystal Reports Server 的帐户拥有本地管理员权限。
- 2 设置仅对必要的 Windows 程序和服务启用数据执行保护 (Data Execution Prevention, DEP)。这对于避免出现“错误 1920。Windows 2003 上的服务 Crystal Report Cache Server”尤其有用。

通过“控制面板”>“系统”>“高级”选项卡>“性能设置”>“数据执行保护”，可以访问 DEP。

选择仅对必要的 Windows 程序和服务启用 DEP。



如果打算使用 Windows NT 身份鉴定运行 Sentinel 报告，应确保 Sentinel 数据库中已存在 Sentinel 报告用户的 Windows 域帐户。完成此操作的方法是：在 Sentinel 安装过程中设置 Sentinel 报告用户的身份鉴定方法时，按如下所示选择“Windows Authentication”（Windows 身份鉴定）。



- 3 如果打算使用 SQL Server 鉴定（Sentinel Oracle 安装也同样需要）运行 Sentinel 报告，应确保 Sentinel 数据库中已存在 SQL Server 登录 (esecrpt)。
  - ◆ 对于 Sentinel Microsoft SQL 数据库 - 完成此操作的方法是：在用于 Microsoft SQL 的 Sentinel 安装过程中设置 Sentinel 报告用户的身份验证方法时，按如下所示选择“SQL Server 身份验证”。



- ◆ 对于 Sentinel Oracle 数据库 - 此操作在将 Sentinel 安装到 Oracle 时完成。esecrpt 将采用与 esecadm 相同的口令。
- 4 对于 Oracle - 在安装 Crystal BusinessObjects Enterprise™ XI 前安装 Oracle 9i Client Release 2 (9.2.0.1.0)。

- 5 对于 Microsoft SQL Server - 在安装 Crystal Reports Server XI 前安装 Microsoft SQL 2005。
- 6 视频分辨率 1024 x 768 或更高
- 7 安装 Microsoft Internet 信息服务 (IIS) 和 NET.ASP

---

**注释：** Sentinel 不支持 MSDE。在安装 Crystal Reports Server XI 前安装 Microsoft SQL 2005。

---

### 9.3.1 安装 Microsoft Internet 信息服务 (IIS) 和 ASP.NET

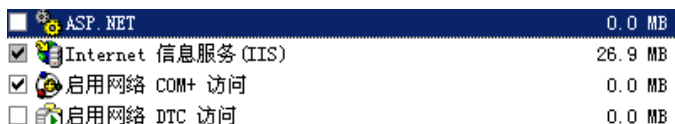
安装这些 Windows 部件可能需要有 Windows 2003 Server 安装光盘。

#### 安装 IIS 和 ASP.NET：

- 1 转到 Windows “控制面板” > “添加 / 删除程序”。
- 2 在左侧纵向窗格中，单击 “添加 / 删除 Windows 组件”。
- 3 选择 “Application Server”（应用程序服务器）。



- 4 单击 “细节”。
- 5 选择 “ASP.NET” 和 “Internet 信息服务 (IIS)”。



- 6 单击 “确定”。
- 7 单击 “下一步”。可能会出现提示，要求插入 Windows 安装光盘。
- 8 单击 “完成”。

## 9.4 已知问题

- 1 安装 Crystal Reports - 向您颁发有两个密钥，一个用于 Crystal Reports Server，另一个用于 Crystal Reports Developer。确保在安装 Crystal Reports Server 时使用 Crystal Reports Server 密钥。
- 2 卸装 Crystal Reports – 如果必须卸装 Crystal Reports Server，可以使用手工卸装过程清除注册表密钥。如果您的安装已被破坏，这会非常有用。转到 BusinessObjects 万维网站点 <http://support.businessobjects.com/library/kbase/articles/c2017905.asp> (<http://support.businessobjects.com/library/kbase/articles/c2017905.asp>)，以了解手动卸装 BusinessObjects Enterprise XI 的过程。

---

**注释：** 到本文档发布之日为止，以上 URL 有效。

---

## 9.5 使用 Crystal Reports

有关为 Sentinel 报告使用 Crystal Reports 的更多信息，请参阅 Crystal Reports 文档和《Sentinel 用户指南》。

## 9.6 安装概述

### 9.6.1 使用 Windows 鉴定执行 Microsoft SQL 2005 Server 安装概述

安装采用 Windows 鉴定的 Microsoft SQL Server:

- 1 安装 Crystal Reports Server XI – 在安装 Sentinel 应用程序时, 如果已为 Sentinel 报告用户选择了 Windows 鉴定, 请转到[使用 Windows 鉴定安装 Crystal Server for Microsoft SQL 2005 Server \(第 102 页\)](#) 的链接, 按其说明进行操作。
- 2 配置开放数据库连接 (ODBC)
- 3 映射 Crystal Reports, 使之可以与 Sentinel 一起使用
- 4 为 Crystal Reports 安装增补程序
- 5 发布报告
- 6 将用户设置为命名用户帐户
- 7 导入 Crystal Report 模板
- 8 创建一个 Crystal 网页 (配置 .NET Administration Launchpad)
- 9 配置 Sentinel 以集成 Crystal Enterprise 服务器

---

注释: 必须按照上面所述的顺序安装采用 Windows 鉴定的 Microsoft SQL Server。

---

### 9.6.2 使用 SQL Server 鉴定执行 Microsoft SQL 2005 Server 安装概述

安装采用 SQL Server 鉴定的 Microsoft SQL Server:

- 1 安装 Crystal Reports Server XI。

---

注释: 在安装 Sentinel 应用程序时, 如果已为 Sentinel 报告用户选择了 SQL Server 鉴定, 请转到[使用 SQL 鉴定安装 Crystal Server for Microsoft SQL 2005 Server \(第 107 页\)](#) 的链接, 按其说明进行操作。

---

- 2 配置开放数据库连接 (ODBC)
- 3 映射 Crystal Reports, 使之可以与 Sentinel 一起使用
- 4 导入 Crystal Report 模板
- 5 创建一个 Crystal 网页 (配置 .NET Administration Launchpad)
- 6 配置 Sentinel 以集成 Crystal Enterprise 服务器

---

注释: 必须按照上面所述的顺序安装采用 SQL Server 鉴定的 Microsoft SQL Server。

---

## 9.6.3 Oracle 安装概述

### 安装 Oracle:

为正确安装 Crystal Reports，请按如下所示的步骤执行安装。

- 1 安装 Oracle 9i 客户程序
- 2 安装 Crystal Reports Server XI。有关更多信息，请参考[使用 SQL 鉴定安装 Crystal Server for Microsoft SQL 2005 Server](#)（第 107 页）。
- 3 配置 Oracle 本机驱动程序
- 4 映射 Crystal Reports，使之可以与 Sentinel 一起使用
- 5 导入 Crystal Report 模板
- 6 创建一个 Crystal 网页（配置 .NET Administration Launchpad）
- 7 配置 Sentinel 以集成 Crystal Enterprise 服务器

---

**注释：**必须按照上面所述的顺序安装 Oracle。

---

## 9.7 安装

本节说明如何为以下数据库安装 Crystal 服务器：

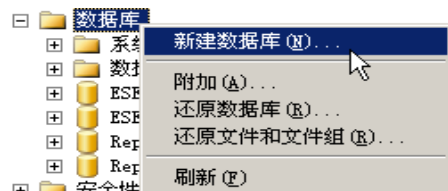
- ◆ 使用 Windows 鉴定的 Microsoft SQL 2005 Server Sentinel 数据库
- ◆ 使用 SQL Server 鉴定的 Microsoft SQL 2005 Server Sentinel 数据库
- ◆ Oracle Sentinel 数据库

### 9.7.1 使用 Windows 鉴定安装 Crystal Server for Microsoft SQL 2005 Server

安装采用 Windows 鉴定的 BOE XI Crystal Server:

- 1 在混合模式下安装 Microsoft SQL 2005。
- 2 启动 Microsoft SQL Management Studio。
- 3 在导航窗格中展开“数据库”。

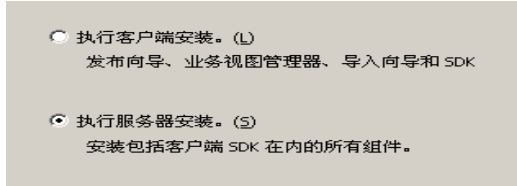
高亮显示并右击“数据库”，然后选择“新建数据库...”。



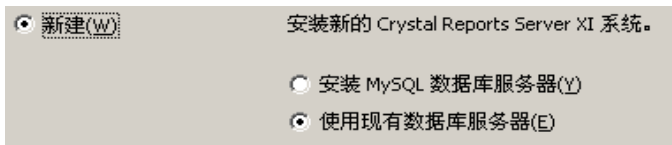
- 4 在“数据库名称”字段下，输入 BOE11 并单击“确定”。

数据库名称(N):

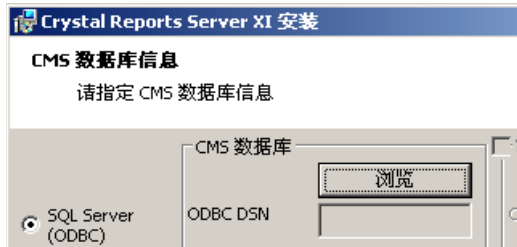
- 5 退出 Microsoft SQL Management Studio。
- 6 将 Crystal Reports XI Server CD 插入 CD-ROM。
- 7 如果计算机已禁用自动播放，运行 setup.exe。
- 8 在“选择客户端安装还是服务器安装”窗口中，选择“执行服务器安装”。



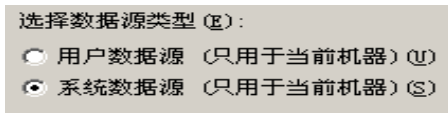
- 9 选择安装类型时，选择“新建”，不要选择“Install MSDE or use existing local SQL Server”（安装 MSDE 或使用现有的本地 SQL Sever）。



- 10 在“CMS 数据库”窗格中，单击“浏览”。



- 11 单击“Machine Data Source”（计算机数据源）选项卡。
- 12 单击“新建”。
- 13 选择“System Data Source”（系统数据源）。



单击“下一步”。

14 向下滚动并选择 “SQL Server”，然后单击 “下一步”。

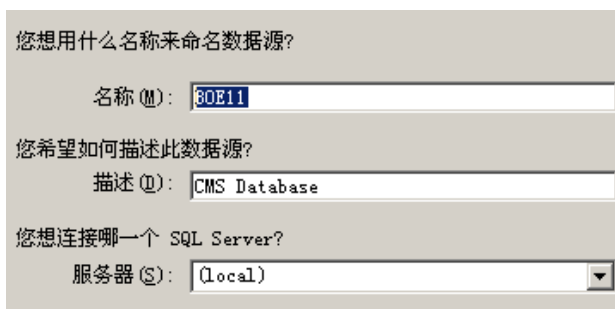


15 出现新的源后，单击 “完成”。



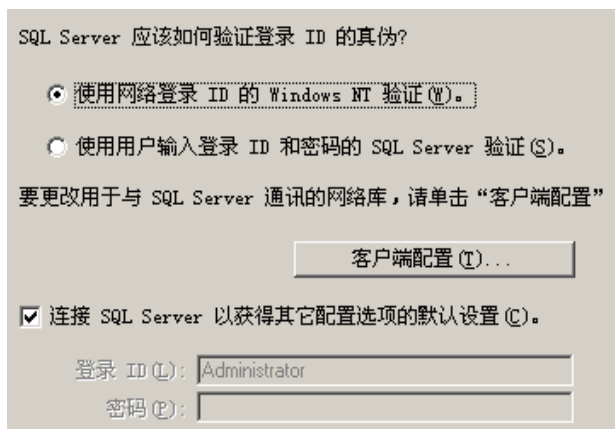
16 在 “新建到 SQL Server 的数据源” 窗口中，输入：

- ◆ 数据源的名称（ex: 即 BOE\_XI）
- ◆ 描述（选填）
- ◆ 对于 “服务器”，请单击向下箭头，选择 “（本地）”



单击 “下一步”。

如果尚未完成验证步骤，请选择 “使用网络登录 ID 的 Windows NT 验证”，然后选择 “下一步”。



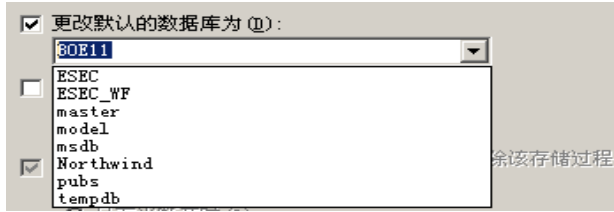


---

**注释：**登录 ID（已变灰）是您的 Windows 登录名。

---

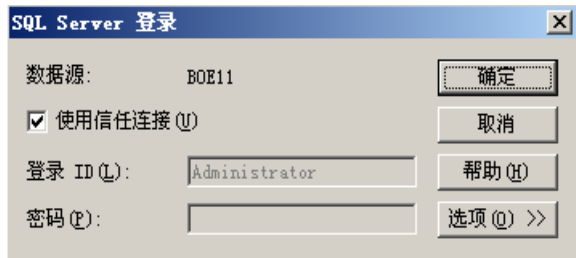
选中“将默认数据库更改为”复选框。将默认数据库更改为“BOE11”。单击“下一步”。



17 在“新建到 SQL Server 的数据源”窗口中，单击“完成”。

18 单击“测试数据源”并测试数据源。成功测试数据源后，单击“确定”。

在“选择数据源”窗口中，高亮显示 BOE11 并继续单击“确定”，直到进入“SQL Server 登录”。请确保选定了“Use Trusted Connection”。单击“确定”。



---

**注释：**登录 ID（已变灰）是您的 Windows 登录名。

---

19 在“Web Component Adapter Type”（Web 组件适配器类型）窗口中，选择“IIS ASP.NET”。

**注释：**如果尚未通过“控制面板”>“添加/删除程序”>“添加/删除 Windows 组件”安装 IIS 和 ASP.NET，IIS ASP.NET 将为灰色。

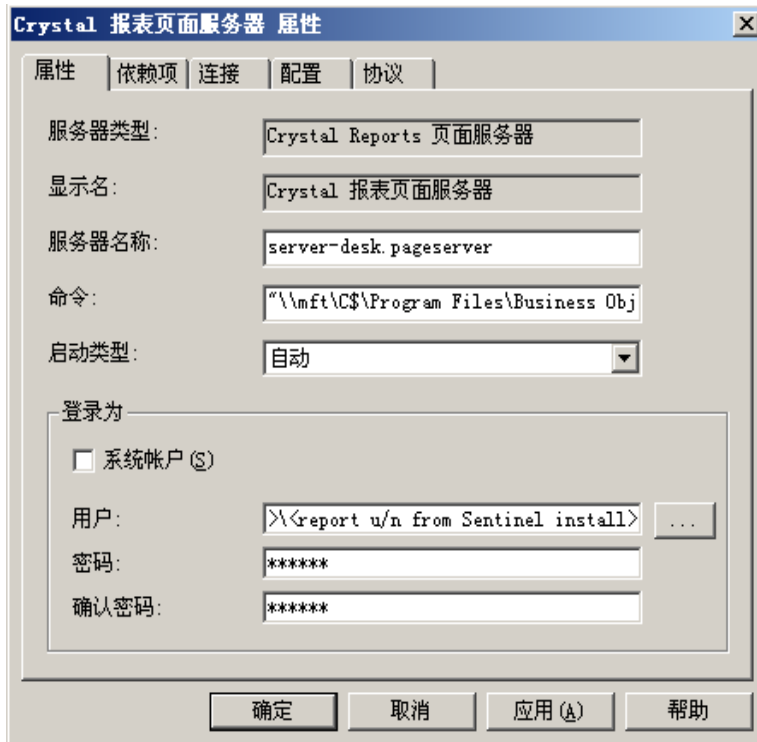
---



1 安装后，需要将 Crystal Reports Page 服务器和 Crystal Reports Job 服务器的登录帐户更改为 Sentinel 报告用户域帐户。

- 单击“开始”>“所有程序”>“BusinessObjects”>“Crystal Reports Server”>“中央配置管理器”。

- ◆ 右击 “Crystal Reports Page Server”（Crystal Reports Page 服务器）并选择 “停止”。
- ◆ 再次右击 “Crystal Reports Page 服务器” 并选择 “属性”。
- ◆ 取消选中 “Log On As System Account”（以系统帐户登录），然后输入在安装 Sentinel 期间用于 Sentinel 报告用户的 Sentinel 报告用户域帐户用户名和口令。单击 “确定”。



2 高亮显示 Crystal Reports Page 服务器，右击启动 Crystal Reports Page 服务器。

### 为 Windows 身份鉴定配置开放数据库连接 (ODBC)

本步骤在位于 Windows 和 SQL Server 上的 Crystal Reports 之间设置 ODBC 数据源。只能在 Crystal 服务器计算机上执行此步骤。

### 为 Windows 鉴定设置 ODBC 数据源：

- 1 转到 Windows “控制面板” > “管理工具” > “数据源 (ODBC)”。
- 2 单击 “系统 DSN” 选项卡并单击 “添加”。
- 3 选择 “SQL Server”。单击 “完成”。
- 4 将出现一个屏幕，提示输入驱动程序配置信息。
  - ◆ 数据源名称，输入 “esecuritydb”
  - ◆ 对于 “描述” 字段（选填），输入描述
  - ◆ 对于 “服务器” 字段，输入 Sentinel 服务器的主机名或 IP 地址

名称 (N):

您希望如何描述此数据源?  
描述 (D):

您想连接哪一个 SQL Server?  
服务器 (S):

单击“下一步”。

在下一个屏幕中，选择 Windows 身份验证。

SQL Server 应该如何验证登录 ID 的真伪?

使用网络登录 ID 的 Windows NT 验证 (W)。

使用用户输入登录 ID 和密码的 SQL Server 验证 (S)。

要更改用于与 SQL Server 通讯的网络库，请单击“客户端配置”

连接 SQL Server 以获得其它配置选项的默认设置 (C)。

登录 ID (L):

密码 (P):

---

**注释：**登录 ID（已变灰）是您的 Windows 登录名。

---

5 在下一个屏幕中选择：

- ◆ 更改 Sentinel 数据库（默认名称为 ESEC）
- ◆ 保留所有默认设置

单击“下一步”。

6 单击“完成”。

7 单击“测试数据源...”。应该能够成功连接。单击“确定”直至退出。

## 9.7.2 使用 SQL 鉴定安装 Crystal Server for Microsoft SQL 2005 Server

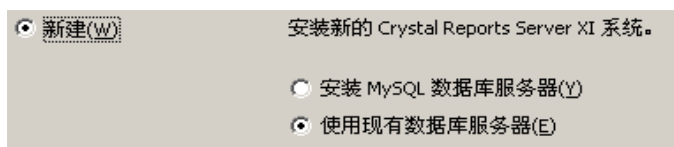
### 鉴定 BOE XI Crystal Server SQL:

在“选择客户端安装还是服务器安装”窗口中，选择“执行服务器安装”。

执行客户端安装。(C)  
发布向导、业务视图管理器、导入向导和 SDK

执行服务器安装。(S)  
安装包括客户端 SDK 在内的所有组件。

- 1 通过“安装 MSDE”安装新的 BusinessObjects Enterprise System，或使用现有的本地 SQL Server。

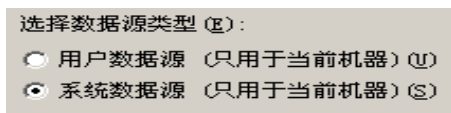


**注释：**Crystal 服务器和 Microsoft SQL Server 必须位于同一台计算机上。

- 2 在“CMS 数据库”窗格中，单击“浏览”。



- 3 单击“Machine Data Source”（计算机数据源）选项卡。
  - 4 单击“新建”。
- 选择“System Data Source”（系统数据源）。

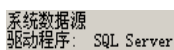


单击“下一步”。

向下滚动并选择“SQL Server”，然后单击“下一步”。



出现新的源后，单击“完成”。



- 5 在“新建到 SQL Server 的数据源”窗口中，输入：
  - ◆ 数据源的名称（ex: 即 BOE\_XI）

- ◆ 描述（选填）
- ◆ 对于“服务器”，请单击向下箭头，选择“（本地）”

单击“下一步”。

- 6 如果尚未完成验证步骤，请选择“使用用户输入的登录 ID 和口令的 SQL Server 鉴定”，并输入 sa 作为用户名，输入 sa 作为口令。单击“下一步”。

选中“将默认数据库更改为：”复选框。将默认数据库更改为“BOE11”。单击“下一步”。

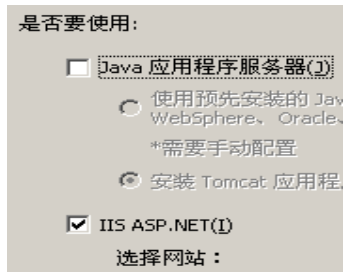
- 7 在“新建到 SQL Server 的数据源”窗口中，单击“完成”。
- 8 单击“测试数据源”并测试数据源。成功测试数据源后，单击“确定”。

在“选择数据源”窗口中，高亮显示 BOE11 并继续单击“确定”，直到进入“SQL Server 登录”。确保未选中“使用可信连接”。单击“确定”。单击“下一步”。



- 9 在“Web Component Adapter Type”（Web 组件适配器类型）窗口中，选择“IIS ASP.NET”。

**注释：**如果尚未通过“控制面板”>“添加/删除程序”>“添加/删除 Windows 组件”安装 IIS 和 ASP.NET，IIS ASP.NET 将为灰色。

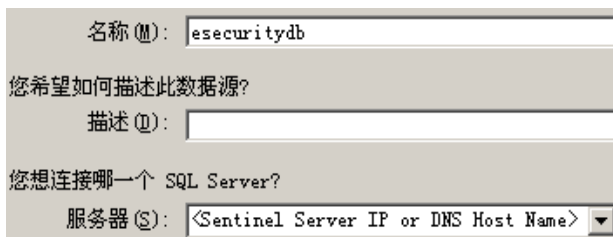


### 为 SQL 鉴定配置开放数据库连接 (ODBC)

本步骤在位于 Windows 和 SQL Server 上的 Crystal Reports 之间设置 ODBC 数据源。只能在 Crystal 服务器计算机上执行此步骤。

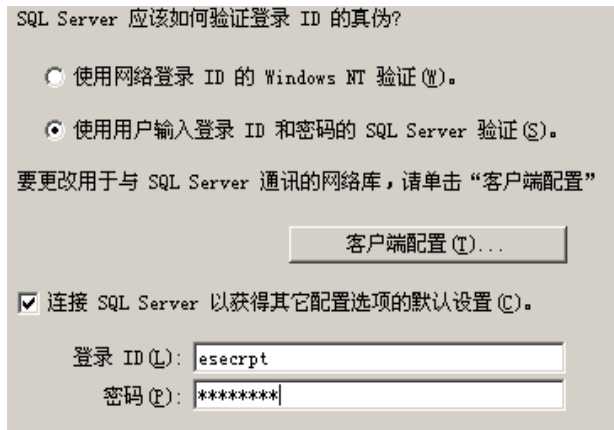
#### 为 Windows 设置 ODBC 数据源：

- 1 转到 Windows “控制面板”>“管理工具”>“数据源 (ODBC)”。
- 2 单击“系统 DSN”选项卡并单击“添加”。
- 3 选择“SQL Server”。单击“完成”。
- 4 将出现一个屏幕，提示输入驱动程序配置信息。
  - ◆ 数据源名称，输入“esecuritydb”
  - ◆ 对于“描述”字段（选填），输入描述
  - ◆ 对于“服务器”字段，输入 Sentinel 服务器的主机名或 IP 地址



单击“下一步”。

- 5 在下一个屏幕中，选择“SQL Authentication”（SQL 鉴定）。输入“esecrpt”和口令作为登录 ID。单击“下一步”。



- 6 在下一个屏幕中选择：
  - ◆ 更改 Sentinel 数据库（默认名称为 ESEC）
  - ◆ 保留所有默认设置

单击“下一步”。

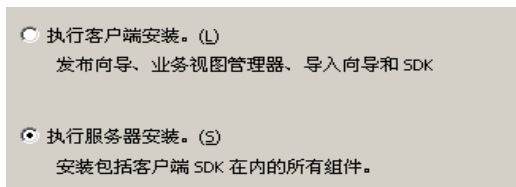
- 7 单击“完成”。

- 8 单击“测试数据源”并测试数据源。成功测试数据源后，单击“确定”。单击“确定”直至退出。

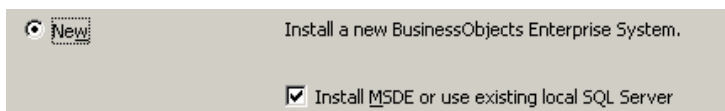
### 9.7.3 安装 Crystal Server for Oracle

#### 安装 Crystal Reports Server XI for Oracle:

- ◆ 执行服务器安装



- ◆ 选中“Install MSDE or use existing local SQL Server”，安装新的 BusinessObjects Enterprise 系统。



---

**注释：**Crystal 服务器和 Microsoft SQL Server 2005 必须位于同一台计算机上。

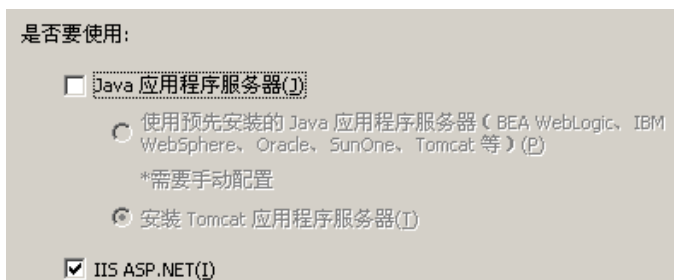
---

- ◆ IIS ASP.NET。

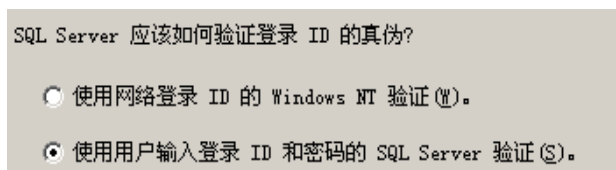
---

**注释：**如果尚未通过“控制面板”>“添加/删除程序”>“添加/删除 Windows 组件”安装 IIS 和 ASP.NET，IIS ASP.NET 将为灰色。

---



- ◆ 将提示您指定身份验证方式。选择 SQL Server 身份验证。



Crystal Reports 支持直接访问 Oracle 9 数据库。此访问能力由 crdb\_oracle.dll 转换文件提供。该文件与 Oracle 9 数据库驱动程序之间进行通讯，该驱动程序直接与 Oracle 数据库和客户程序一同工作，以检索报告所需的数据。

---

**注释：**为使 Crystal Reports 可以使用 Oracle 9 数据库，必须在您的系统上安装 Oracle 客户端软件，并在 PATH 环境变量中包括该客户程序。

---

## 安装并配置 Oracle 9i 客户端软件

在安装 Oracle 9i 客户程序时：

- ◆ 接受默认安装位置
- ◆ 对“Perform Typical Configuration”选择“No”
- ◆ 对“Directory Service”选择“No”
- ◆ 选择“Local”
- ◆ TNS 服务名称：ESEC
- ◆ 用户（可选）：esecrpt

安装结束后，创建本地 Net Service 名称配置。

### 创建网络服务名称配置（配置 Oracle 本机驱动程序）：

- 1 选择“Oracle-Orahome92”>“Configuration and Migration Tools”（配置和迁移工具）>“Net Manager”（网络管理器）。
- 2 在导航窗格中，展开“本地”并高亮显示“Service Naming”（服务命名）。
- 3 单击左侧的加号，添加服务名称。



- 4 在 “Service Name”（服务名称）窗口中，输入 “Net Service Name”（网络服务名称）。
  - ◆ 输入 ESECURITYDB单击 “下一步”。
- 5 在 “Select Protocols” 窗口中，选择默认协议：
  - ◆ TCP/IP（因特网协议）单击 “下一步”。
- 6 对于主机名和端口号：
  - ◆ 输入数据库所在的计算机主机名或 IP 地址
  - ◆ 选择 Oracle 端口（默认安装端口为 1521）单击 “下一步”。
- 7 确定数据库或服务：
  - ◆ 选择（Oracle8i 或更新版本），输入您的服务名称（该名称为 Oracle 的实例名称）。
  - ◆ 对于连接类型，选择 “Database Default”。单击 “下一步”。
- 8 在 “Test” 窗口中，单击 “Test...”。单击 “下一步”。测试可能会失败，因为此测试使用的可能是数据库的 ID 和口令。
- 9 如果测试失败，请执行以下操作：
  - ◆ 在 “Connecting” 窗口中，单击 “Change Login”。
  - ◆ 输入 Sentinel Oracle 的 ID “esecrpt” 及其口令。单击 “确定”。如果测试仍然失败，请执行以下操作：
  - ◆ 对 Sentinel 服务器执行 Ping 命令
  - ◆ 校验 Sentinel 服务器的主机名是否位于 Crystal Reports Server 的 hosts 文件中。hosts 文件位于 %SystemRoot%\system32\drivers\etc\。
- 10 单击 “完成”。

## 9.8 所有鉴定和配置的配置

### 9.8.1 映射 Crystal Reports，使之可以与 Sentinel 一起使用

Crystal 服务器若要与 Sentinel 控制中心一起使用，需遵循以下步骤。

#### 配置 inetmgr

#### 配置 inetmgr:

- 1 从以下位置复制 web.config 文件：  
C:\Program Files\Business Objects\BusinessObjects Enterprise  
11.5\Web Content

复制到 c:\Inetpub\wwwroot。

- 2 单击“开始”>“运行”，启动因特网服务管理器。输入“inetmgr”并单击“确定”。
- 3 展开“(local Computer)”（本地计算机）>“Web Sites”（万维网站点）>“Default Web Site”（默认万维网站点）>“businessobjects”。
- 4 右击“businessobjects”>属性。
- 5 在“虚拟目录”选项卡下，单击“配置...”
- 6 应找到以下映射。如果没有，则添加它们。要添加映射，请勿单击“businessobjects”或“crystalreportsviewer11”节点。

扩展	可执行文件
.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:\Program Files\Business Objects\BusinessObjects Enterprise 11\win32_x86\cdzISAPI.dll

单击“OK”关闭窗口。

- 7 重新启动 IIS，方法是：展开“(local Computer)”（本地计算机）>“Web Sites”（万维网站点）>“Default Web Site”（默认万维网站点），然后右击>“Start”（启动）。

### 为 Crystal Reports 安装增补程序，使之可以与 Sentinel 一起使用

为了从 Sentinel 控制中心的“Analysis”选项卡查看 Crystal 报告，需要更新几个 Crystal Enterprise 文件，使它们与嵌入在 Sentinel 中的浏览器兼容。

下表列出了这些文件，并说明了每个文件的用途。这些文件可以在 Sentinel Reports 分发包中找到，Sentinel Reports 分发包可以从 Novell 技术支持站点下载。

文件名	说明
calendar.js	选择日期作为报告参数时，显示弹出日历。
calendar.html	
grouptree.html	加载报告时，显示“Loading...”讯息。
exportframe.html	显示窗口，可在该窗口中导出报告以进行保存或打印。
exportlce.html	Sentinel 导出报告以进行保存或打印时所使用的文件。
GetInfoStore.asp	查询 Crystal 服务器所使用的文件
GetReports.asp	Sentinel 控制中心建立与 Crystal 服务器的连接和显示报告列表时所使用的文件。
GetReportURL.asp	支持报告间超级链接所使用的文件。
helper_js.asp	GetInfoStore.asp 使用的调用文件。

### 为 Crystal Reports 安装增补程序:

- 1 从 Novell 技术支持站点获取 Sentinel Reports 分发包。

---

**注释:** 强烈建议您在执行此任务之前查看 Sentinel Reports 发行说明。可能存在更新的文件、底稿以及其它步骤。

---

- 2 在 Sentinel Reports 分发包中，转到“patch”目录并将所有 \*.html 和 \*.js 文件复制到查看器文件位置，默认为:

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

- 3 在 Sentinel Reports 分发包中，转到“patch”目录并将所有 \*.asp 和 \*.js 文件复制到:

C:\inetpub\wwwroot

---

**注释:** 您的万维网文件夹所在的驱动器或位置可能与上面指定的不同。

---

### Crystal Report 模板

Crystal 报告模板使用 Crystal 发布向导发布到 Crystal Reports Server。可以从 Novell 技术支持站点下载最新的报告模板集。

### 使用 Crystal 发布向导发布 Report 模板

---

**注释:** 强烈建议您在执行此任务之前查看 Sentinel Reports 发行说明。可能存在更新的文件、底稿以及其它步骤。

---

### 发布 Crystal Report 模板


---

**注释:** 如果重新发布报告模板，请删除先前导入的报告模板。

---

- 1 单击“开始” > “所有程序” > “BusinessObjects” > “Crystal Reports Server” > “发布向导”。
- 2 单击“下一步”。
- 3 登录。“System”必须是您的主机名，并且“Authentication”应该是“Enterprise”。“用户名”可以是 Administrator。为了安全起见，强烈推荐新建一个用户，而不要使用 Administrator。输入您的口令，然后单击“下一步”。

**注释：**以用户 Administrator 身份发布报告后，所有用户都可以访问这些报告。



- 4 单击“添加文件夹”。
- 5 选择“Include Subfolder”。在 Sentinel Reports 分发中导航至：

对于在 Microsoft SQL 上运行的 Sentinel 数据库：

Crystal\_v11\SQL-Server

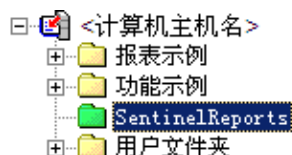
对于在 Oracle 上运行的 Sentinel 数据库：

Crystal\_v11\Oracle

单击“确定”。

- 6 单击“下一步”。

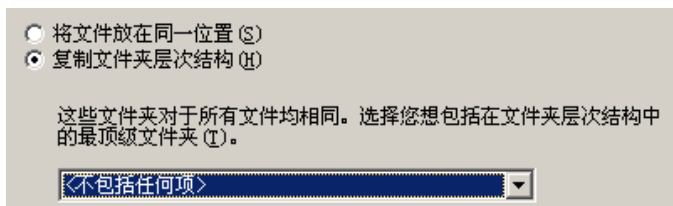
在“指定位置”窗口中，单击“新建文件夹”（右上角），并创建一个称为 SentinelReports 的文件夹。单击“下一步”。



- 7 选择：

- ◆ Duplicate the folder hierarchy.

单击下箭头并选择 <不包含任何内容>



单击“下一步”。

- 8 在“确认位置”窗口中，单击“下一步”。

在“指定类别”窗口中，输入所选的类别名（例如 sentinel），高亮显示该名称并单击 + 按钮。



**注释：**单击“Next”以后，该类别下面将仅出现第一个报告。

单击“Next”。

- 9 在“Specify Repository Refresh”窗口中，单击“Enable All”以启用储存库刷新。单击“下一步”。
- 10 在“Specify Keep Saved Data”（指定保留已保存的数据）窗口中，单击“全部启用”以在发布报告时保留已保存的数据。单击“下一步”。
- 11 在“Change Defaults Values”（更改默认值）窗口中，单击“Publish reports without modifying properties”（发布报告而不修改属性）（此选项应为默认选项）。单击“下一步”。
- 12 单击“下一步”添加对象。
- 13 单击“下一步”。
- 14 出现已发布的列表后，单击“完成”。

将用于 Crystal Reports 的 Sentinel 模板发布到 Crystal Enterprise 服务器后，这些模板必须位于 SentinelReports 目录中。

## 9.8.2 设置“命名用户”帐户

随 Crystal Server 提供的许可证密钥是“命名用户”帐户的密钥。Guest 帐户已由“并发用户”更改为“命名用户”。

**将 Guest 帐户设置为“命名用户”：**

- 1 单击“开始” > “所有程序” > “Businessobjects” > “Crystal Reports Server” > “.NET 管理启动板”。
- 2 单击“中央管理控制台”。
- 3 “System Name”应该是您的主机名。“Authentication Type”应该是“Enterprise”。如果不是，请选择“企业”。
- 4 单击“登录”。
- 5 在“组织”窗格中，单击“用户”。
- 6 单击 GUEST。
- 7 将连接类型从“并行用户”更改为“命名用户”。
- 8 单击“更新”。
- 9 注销并关闭窗口，或转至“配置 .NET 管理启动板”一节。

### 9.8.3 配置报告权限

此步骤讨论如何使用 .NET Administration Launchpad 配置对报告的权限，以便根据需要查看和修改报告。

#### 配置报告权限：

- 1 如果尚未开始配置过程，请启动 .Net 管理启动板（单击“开始”>“所有程序”>“BusinessObjects”>“Crystal Reports Server”>“.NET 管理启动板”）。
- 2 单击“中央管理控制台”。  
“System Name”应该是您的主机名。“Authentication Type”应该是“Enterprise”。如果不是，请选择“企业”。
- 3 输入您的用户名、口令，然后单击“登录”。
- 4 在“组织”窗格中，单击“文件夹”。
- 5 单击 SentinelReports。
- 6 选择“全部”。
- 7 单击“权限”选项卡。
- 8 对于所有用户，在“Access Level”右下方的下拉菜单中，选择“View on Demand”。
- 9 单击“更新”。
- 10 注销并关闭该窗口。

#### 测试万维网服务器与数据库间的连接

##### 测试万维网服务器与数据库的连接：

- 1 如果尚未开始测试过程，启动 .Net 管理启动板（“开始”>“所有程序”>“BusinessObjects”>“Crystal Reports Server”>“.NET 管理启动板”）。
- 2 单击“中央管理控制台”。
- 3 输入 Administrator 作为用户名。输入口令（默认情况下，此处为空）。单击“登录”。
- 4 导航到“文件夹”>“SentinelReports”>“内部事件”。
- 5 选择“Column Display Details”。
- 6 单击“预览”。
- 7 根据您的系统，以 escript 身份或 Sentinel 报告用户身份登录。
- 8 在排序字段下拉菜单中，选择“标签”。
- 9 单击“确定”。应出现一个报告。

#### 测试万维网服务器的连接性

##### 测试与万维网服务器的连接：

- 1 转到与您的万维网服务器位于同一网络中的另一台计算机。
- 2 Enter  
`http://<DNS name or IP address of your web server>/businessobjects/enterprise11/WebTools/adminlaunch/default.aspx`

应该会出现 Crystal BusinessObjects 万维网主页。

## 9.8.4 禁用 Sentinel 的前 10 个报告

默认情况下启用 Sentinel 的前 10 个报告。要禁用 Sentinel 的前 10 个报告，必须：

- ◆ 禁用聚合
- ◆ 禁用 EventFileRedirectService

### 禁用聚合：

- 1 启动 Sentinel 数据管理器。
- 2 登录。
- 3 单击 “Reporting Data”（报告数据）选项卡。
- 4 禁用下列摘要
  - ◆ EventDestSummary
  - ◆ EventSevSummary
  - ◆ EventSrcSummary

单击 “状态” 列中的 “活动”，直到其更改为 “不活动”。

摘要名称	时间	特性	源	状态
EventDestSummary	1 小时	CUST_ID.RSRC_ID ...	TransformedEvent	活动
EventSevDestTxnmyS...	1 小时	CUST_ID.DEST_EV ...	TransformedEvent	非活动
EventSevDestEvtSum...	1 小时	CUST_ID.DEST_EV ...	TransformedEvent	非活动
EventSevDestPortSu...	1 小时	SEV.DEST_PORT.C ...	TransformedEvent	非活动
EventSevSummary	1 小时	CUST_ID.SEV.EVT ...	TransformedEvent	活动
EventSrcSummary	1 小时	CUST_ID.RSRC_ID ...	TransformedEvent	活动

### 禁用 EventFileRedirectService:

- 1 在您的 DAS 计算机上，使用文本编辑器打开：

对于 UNIX:

```
$ESEC_HOME/config/das_binary.xml
```

对于 Windows 系统:

```
%ESEC_HOME%\config\das_binary.xml
```

- 2 对于 EventFileRedirectService，将状态更改为关闭。

```
<property name="status">off</property>
```

- 3 执行以下操作，重新启动 DAS 组件：

在 Windows 上:

Use Service Manager to stop then start the “sentinel” service.

## 9.8.5 提高 Crystal Enterprise Server 报告刷新记录限制

根据 Crystal 正在查询的事件数，可能会出现关于最长处理时间或最大记录限制的错误。要将服务器设置为可以处理更多数量或数量不限的记录，需要重配置 Crystal Page Server。使用中央配置管理器或 Crystal 网页可以执行此操作。

### 通过中央配置管理器重配置 Crystal Page Server:

- 1 单击“开始” > “所有程序” > “BusinessObjects” > “Crystal Reports Server” > “中央配置管理器”。
- 2 右击“Crystal Reports Page 服务器”并选择“停止”。
- 3 再次右击“Crystal Reports Page 服务器”并选择“属性”。
- 4 在“属性”选项卡下的“命令”字段中，在命令行的末尾添加：  
`maxDBResultRecords <value greater than 20000 or 0 to disable the default limit>`
- 5 重新启动 Crystal Page Server。

### 通过 Crystal 万维网网页重配置 Crystal Page Server:

- 1 单击“开始” > “所有程序” > “Businessobjects” > “Crystal Reports Server” > “.NET 管理启动板”。
- 2 单击“中央管理控制台”。
- 3 “System Name”应该是您的主机名。“Authentication Type”应该是“Enterprise”。如果不是，请选择“企业”。
- 4 输入您的用户名、口令，然后单击“登录”。
- 5 单击“服务器”。
- 6 单击 <服务器名称>.pageserver。
- 7 在“预览或刷新报告时要读取的数据库记录”下，单击“无限记录”。
- 8 单击“应用”。
- 9 将会出现要求重新启动 Page 服务器的提示，单击“确定”。
- 10 可能会提示您输入登录名和口令，以访问操作系统服务管理器。

## 9.8.6 将 Sentinel 控制中心配置为与 Crystal Enterprise Server 集成

Sentinel 控制中心可以配置为与 Crystal Enterprise Server 集成，这样可以在 Sentinel 控制中心中查看 Crystal Reports。

要启用 Sentinel 控制中心与 Crystal Enterprise Server 的集成，请按照以下说明操作。

---

**注释：**必须在安装了 Crystal Enterprise Server 并向其发布了 Crystal Reports 后再执行此配置。

---

### 将 Sentinel 配置为与 Crystal Enterprise Server 集成：

- 1 以具有访问“管理”选项卡特权的用户身份登录到 Sentinel 控制中心。



2 在“管理”选项卡中，选择“报告配置”。

3 在“Analysis URL”（分析 URL）字段中，输入以下内容：

```
http://<hostname_or_IP_of_web_server>/  
GetReports.asp?APS=<hostname>&user=Guest&password=&tab=Analysis
```

---

**注释：**必须将 < 万维网服务器的主机名或 IP 地址 > 替换为 Crystal Enterprise Server 的 IP 地址或主机名。

---

**注释：**如果将 APS 设置为 IP 地址，则上述 URL 将无法正常工作。它必须为 Crystal 服务器的主机名。

---

4 单击“Analysis URL”字段旁边的“刷新”。

5 如果您已经安装顾问，请在“Advisor URL”（顾问 URL）字段中输入以下内容：

```
http://<hostname_or_IP_of_web_server>/  
GetReports.asp?APS=<hostname>&user=Guest&password=&tab=Advisor
```

---

**注释：**必须将 < 万维网服务器的主机名或 IP 地址 > 替换为 Crystal Enterprise Server 的 IP 地址或主机名。

---

**注释：**如果将 APS 设置为 IP 地址，则上述 URL 将无法正常工作。它必须为 Crystal 服务器的主机名。

---

6 单击“顾问 URL”字段旁边的“刷新”。

7 单击“保存”。

8 注销，然后重新登录至 Sentinel 控制中心。现在，“Analysis”和“Advisor”（如果已安装顾问）选项卡中的 Crystal Report 树应出现在“Navigator”窗口中。



本章包含下列主题：

- ◆ 使用 Crystal Reports （第 124 页）
- ◆ 安装 Crystal BusinessObjects Enterprise™ XI （第 126 页）
- ◆ 发布 Crystal Report 模板 （第 128 页）
- ◆ 使用 Crystal XI 万维网服务器 （第 131 页）
- ◆ 设置 ‘命名用户’ 帐户 （第 131 页）
- ◆ 启用 Sentinel 的前 10 个报告 （第 132 页）
- ◆ 将 Sentinel 控制中心配置为与 Crystal Enterprise Server 集成 （第 134 页）
- ◆ 实用程序和查错 （第 135 页）

Crystal Business Objects Enterprise™ XI 是随 Sentinel 提供的报告工具之一。

本章讨论 Crystal Reports Server for Sentinel 的安装和配置。

Sentinel 支持在以下平台上运行 Crystal Reports Server：

- ◆ Windows – 在 Windows、Linux 或 Solaris 上运行 Sentinel 数据库时支持。
- ◆ Linux - 在 Linux 或 Solaris 上运行 Sentinel 数据库时支持。

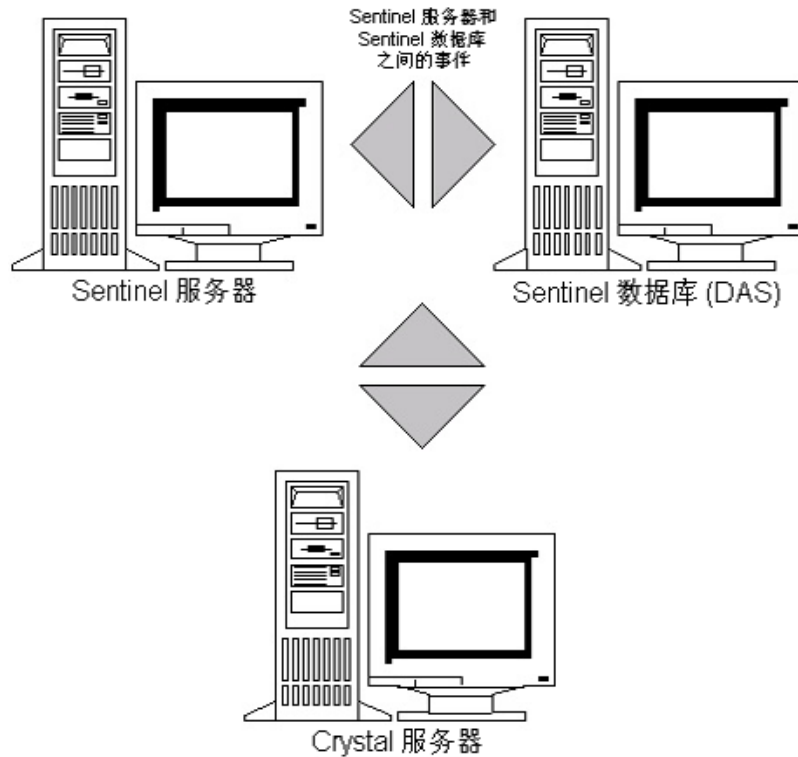
本章讨论在 Linux 上运行 Crystal Reports Server。有关在 Windows 上运行 Crystal Reports Server 的更多信息，请参阅《安装指南》中的第 9 章 “用于 Windows 的 Crystal Reports”（第 97 页）。

---

**注释：**应按如下所述的顺序进行安装。

---

- ◆ Crystal BusinessObjects Enterprise™ XI 的预安装和安装
- ◆ 为 Crystal Reports 安装增补程序
- ◆ 发布（导入）Crystal Reports
- ◆ 设置 ‘命名用户’ 帐户
- ◆ 测试万维网服务器的连接性
- ◆ 启用前 10 个报告（可选）
- ◆ 提高 Crystal Enterprise Server 报告刷新记录限制（推荐）
- ◆ 将 Sentinel 控制中心配置为与 Crystal Enterprise Server 集成



## 10.1 使用 Crystal Reports

有关使用 Crystal Reports 进行 Sentinel 报告的信息，请参阅《安装指南》中的第 9 章“用于 Windows 的 Crystal Reports”（第 97 页）。

## 10.2 配置

- ◆ Linux 版本：
  - ◆ SUSE Linux Enterprise Server 9 (SLES 9) SP2
  - ◆ Red Hat Enterprise Linux 3 Update 5 ES (x86)
- ◆ 已安装 BusinessObjects Enterprise XI 服务器
- ◆ 对于 Oracle - Oracle 9i Client Release 2 (9.2.0.1.0)

## 10.3 安装

### 10.3.1 Crystal BusinessObjects Enterprise™ XI 的预安装

**预安装 Crystal BusinessObjects Enterprise:**

- 1 如果 Sentinel 数据库和 Crystal Server 没有安装在同一台计算机上，则必须在 Crystal Server 计算机上安装 Oracle 客户软件。如果 Sentinel 数据库和 Crystal Server 安装在同一

台计算机上，则无需进行此附加步骤，因为在此情况下已安装有所需的 Oracle 软件，且带有 Sentinel 数据库所需的 Oracle 数据库软件。

**2** 以 root 用户身份登录至 Crystal 服务器计算机

**3** 创建 bobje 组

```
groupadd bobje
```

**4** 创建 Crystal 用户（本示例中的主目录为 “/export/home/crystal”，可根据需要进行更改；路径的 “/export/home” 部分必须已存在）。

```
useradd -g bobje -s /bin/bash -d /export/home/crystal -m crystal
```

**5** 为 Crystal 软件创建目录：

```
mkdir -p /opt/crystal_xi
```

**6** 将 Crystal 软件目录的所有权（递归地）更改为 crystal/bobje：

```
chown -R crystal:bobje /opt/crystal_xi
```

**7** 更改为 Crystal 用户身份：

```
su - crystal
```

**8** 必须在 Crystal 用户环境中设置 ORACLE\_HOME 环境变量。为此，应修改 Crystal 用户的登录底稿，将 ORACLE\_HOME 环境变量设置为 Oracle 软件的基址。例如，如果 Crystal 用户的壳层是 bash，并且 Oracle 软件安装在 /opt/oracle/product/9.2 目录下，请打开文件 ~crystal/.bash\_profile，将下面这一行添加至该文件末尾：

```
export ORACLE_HOME=/opt/oracle/product/9.2
```

**9** Crystal 用户环境中的 LD\_LIBRARY\_PATH 环境变量必须包含 Oracle 软件库的路径。为此，应修改 Crystal 用户的登录底稿，将 LD\_LIBRARY\_PATH 环境变量设置为包含 Oracle 软件库。例如，如果 Crystal 用户的壳层是 bash，请打开文件 ~crystal/.bash\_profile，将下面这一行添加至该文件末尾（即添加到用于设置 ORACLE\_HOME 环境变量的行后）：

```
export LD_LIBRARY_PATH=$ORACLE_HOME/lib:$LD_LIBRARY_PATH
```

**10** 必须在 Oracle tnsnames.ora 文件中添加一个服务名称为 “esecuritydb” 并指向 Sentinel 数据库的项。为此，请在 Crystal Server 计算机上执行以下操作：

**10a** 以 Oracle 用户身份登录。

**10b** 将目录更改为 \$ORACLE\_HOME/network/admin

**10c** 制作文件 tnsnames.ora 的备份。

**10d** 打开文件 tnsnames.ora 以进行编辑。

**10e** 如果 Sentinel 数据库位于 Crystal Server 计算机上，则 tnsnames.ora 文件中应该已经存在指向 Sentinel 数据库的项。例如，如果 Sentinel 数据库名为 ESEC，则应存在类似于以下内容的项：

```
ESEC =
  (DESCRIPTION =
    (ADDRESS_LIST =
      (ADDRESS = (PROTOCOL = TCP) (HOST = dev-linux02) (PORT = 1521))
    )
    (CONNECT_DATA =
      (SID = ESEC)
    )
  )
)
```

**10f** 如果 Crystal Server 计算机上没有 Sentinel 数据库，请在 Sentinel 数据库计算机中打开 tnsnames.ora 文件，找到上述项。

- 10g** 复制整个项，然后将其粘贴到 Crystal Server 计算机的 tnsnames.ora 文件的底部。必须将该项的“Service Name”部分重命名为“esecuritydb”。例如，复制上述项并正确重命名后，它的内容将类似于：

```
esecuritydb =
(DESCRIPTION =
  (ADDRESS_LIST =
    (ADDRESS = (PROTOCOL = TCP)(HOST = dev-linux02)(PORT = 1521))
  )
  (CONNECT_DATA =
    (SID = ESEC)
  )
)
```

- 10h** 确保该项的 HOST 部分正确（例如，如果 Crystal 服务器和 Sentinel 数据库位于不同的计算机上，请确保未将其设置为 localhost）。
- 10i** 保存对 tnsnames.ora 文件所做的更改。
- 10j** 执行下面的命令，检查 esecuritydb 服务名称是否配置正确：  
tnsping esecuritydb
- 10k** 如果命令执行成功，您应获得一个讯息，指示连接正常。

## 10.3.2 安装 Crystal BusinessObjects Enterprise™ XI

### 安装 Crystal Businessobjects Enterprise:

- 1 以 Crystal 用户身份登录。
- 2 将目录更改为 Crystal 安装程序的 DISK\_1。
- 3 执行：  
./install
- 4 选择语言：英语
- 5 选择“全新安装”
- 6 接受许可协议
- 7 输入产品密钥代码
- 8 输入安装目录：  
/opt/crystal\_xi
- 9 选择：“用户安装”
- 10 选择：“全新安装”
- 11 选择：“安装 MySQL”
- 12 输入 MySQL 的配置信息：
  - 12a 使用默认端口 3306
  - 12b 管理员口令
- 13 输入 MySQL 的更多配置信息：
  - 13a 默认数据库名称：BOE11
  - 13b 用户 ID：mysqladm
  - 13c 口令

- 14 输入 MySQL 的更多配置信息：
  - 14a 本地名称服务器：<本地计算机的主机名>
  - 14b 默认 CMS 端口号：6400
- 15 选择：“安装 Tomcat”
- 16 输入 Tomcat 配置信息：
  - 16a 接收 HTTP 请求的默认端口：8080
  - 16b 默认重定向 jsp 请求端口：8443
  - 16c 关闭挂接程序的默认端口：8005
- 17 按 Enter 开始安装

### 10.3.3 为 Crystal Reports 安装增补程序，使之可以与 Sentinel 一起使用

为了从 Sentinel 控制中心的“Analysis”选项卡查看 Crystal 报告，需要更新几个 Crystal Enterprise 文件，使它们与嵌入在 Sentinel 中的浏览器兼容。

下表列出了这些文件，并说明了每个文件的用途。这些文件可以在 Sentinel Reports 分发包中找到，Sentinel Reports 分发包可以从 Novell 技术支持站点下载。

文件名	说明
calendar.js	选择日期作为报告参数时，显示弹出日历。
calendar.html	
grouptree.html	加载报告时，显示“Loading...”讯息。
exportframe.html	显示窗口，可在该窗口中导出报告以进行保存或打印。
exportlce.html	Sentinel 导出报告以进行保存或打印时所使用的文件。
GetReports.jsp	Sentinel 控制中心建立与 Crystal 服务器的连接和显示报告列表时所使用的文件。
GetReportURL.jsp	支持报告间超级链接所使用的文件。

#### 为 Crystal Reports 安装增补程序：

- 1 从 Novell 技术支持站点获取 Sentinel Reports 分发包。

---

**注释：**强烈建议您在执行此任务之前查看 Sentinel Reports 发行说明。可能存在更新的文件、底稿以及其它步骤。

---

- 2 在 Sentinel 报告分发包中，转到“patch”目录并将所有 \*.html 和 \*.js 文件复制到查看器文件位置，默认为：

```
/opt/crystal_xi/bobje/webcontent/enterprisell/viewer/en/
```

- 3 在 Sentinel 报告分发包中，转到“patch”目录并将所有 \*.jsp 文件复制到：

```
/opt/crystal_xi/bobje/tomcat/webapps/esec-script/
```

---

**注释：**创建一个名为 esec-script 的文件夹

---

#### 4 将所有 \*.jar 文件:

```
From:
/opt/crystal_xi/bobje/tomcat/webapps/jsfadmin/WEB-INF/lib/
To:
/opt/crystal_xi/bobje/tomcat/webapps/esec-script/WEB-INF/lib
```

---

**注释:** 创建文件夹结构 WEB-INF/lib

---

## 10.4 发布 Crystal Report 模板

---

**注释:** 强烈建议您在执行此任务之前查看 Sentinel Reports 发行说明。可能存在更新的文件、底稿以及其它步骤。

---

这些报告模板由 Novell 创建，在 Sentinel 控制中心的 “Analysis” 和 “Advisor” 选项卡中使用。

有两种发布报告的方法。

- ◆ Crystal 发布向导
- ◆ Crystal Reports 中央管理控制台

---

**注释:** 要运行前 10 个报告中的任意一个，必须启用集合功能，DAS\_Binary.xml 中的 **EventFileRedirectService** 也必须处于打开状态。有关如何启用聚合的信息，请参阅《Sentinel 用户指南》中 “Sentinel 数据管理器” 的 “‘报告数据’ 选项卡” 一节，或参阅 [启用 Sentinel 的前 10 个报告（第 132 页）](#) 一节。

---

### 10.4.1 发布报告模板 – Crystal 发布向导

---

**注释:** 需要 Windows 平台才能运行 Crystal 发布向导。

---

#### 导入 Crystal 报告模板:

---

**注释:** 若要重新导入（发布）报告模板，请删除以前导入的报告模板。

---

- 1 单击 “开始” > “所有程序” > “Businessobjects 11” > “Crystal Reports Server” > “发布向导”。
- 2 单击 “下一步”。
- 3 登录。“System” 必须是您的主机名，并且 “Authentication” 应该是 “Enterprise”。“用户名” 可以是 Administrator。为安全起见，您使用的用户不应该是 Administrator。输入您的口令，然后单击 “下一步”。

---

**注释:** 以用户 Administrator 身份发布报告后，所有用户都可以访问这些报告。

---

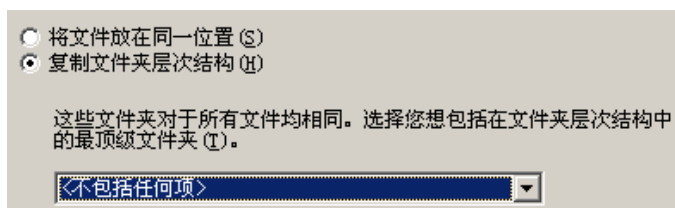




- 4 单击“添加文件夹”。
- 5 单击“包含子文件夹”。在 Sentinel Reports 分发中导航至：  
Crystal\_v11\Oracle  
单击“确定”。
- 6 单击“下一步”。
- 7 在“指定位置”窗口中，单击“新建文件夹”（右上角），创建一个名为 eSecurity\_Reports 的文件夹。单击“下一步”。

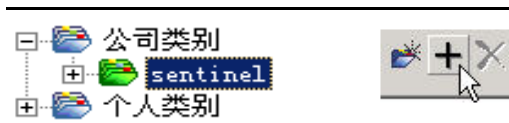


- 8 选择：
  - ◆ Duplicate the folder hierarchy.
  - ◆ 单击下箭头并选择 < 不包含任何内容 >



单击“下一步”。

- 9 在“确认位置”窗口中，单击“下一步”。
- 10 在“Specify Categories”窗口中：
  - ◆ 选择类别名称（例如，“sentinel”）
  - ◆ 高亮显示该名称，并单击“+”按钮



---

**注释：**单击“Next”以后，该类别下面将仅出现第一个报告。

---

- ◆ 单击“下一步”。

- 11 在 “Specify Schedule” 窗口中，单击 “Let users update the object”（此选项应为默认选项）。单击 “下一步”。
- 12 在 “Specify Repository Refresh” 窗口中，单击 “Enable All” 以启用储存库刷新。单击 “下一步”。
- 13 在 “Specify Keep Saved Data”（指定保留已保存的数据）窗口中，单击 “全部启用” 以在发布报告时保留已保存的数据。单击 “下一步”。
- 14 在 “Change Defaults Values”（更改默认值）窗口中，单击 “Publish reports without modifying properties”（发布报告而不修改属性）（此选项应为默认选项）。单击 “下一步”。
- 15 单击 “下一步” 添加对象。
- 16 单击 “下一步”。
- 17 单击 “完成”。

将用于 Crystal Reports 的 Sentinel 模板发布到 Crystal Enterprise Server 后，这些模板必须位于 eSecurity\_Reports 目录中。

## 10.4.2 发布报告模板 – 中央管理控制台

使用 “Central Management Console” 发布报告时，无法像使用 Windows 驱动的开发向导时一样成批发布报告。

### 导入 Crystal 报告模板：

- 1 打开 Web 浏览器并输入以下 URL：  
`http://  
<hostname_or_IP_of_web_server>:<web_server_port_default_8080>/  
businessobjects/enterprise11/adminlaunch`
- 2 单击 “中央管理控制台”。
- 3 登录至 Crystal Server。
- 4 在 “组织” 窗格中，单击 “文件夹”。
- 5 在右上角，单击 “新建文件夹...”。
- 6 创建一个名为 eSecurity\_Reports 的文件夹。单击 “确定”。
- 7 单击 eSecurity\_Reports。
- 8 单击 “Subfolders”（子文件夹）选项卡，然后创建下列子文件夹。
  - ◆ Advisor\_Vulnerability
  - ◆ Incident Management
  - ◆ Internal Events
  - ◆ Security Events
  - ◆ Top 10
- 9 单击 “Home”。
- 10 单击 “对象”。
- 11 单击 “New Object”（新建对象）。
- 12 在页面左侧，高亮显示 “报告”。

**13** 单击“浏览”并浏览到包含 Sentinel Reports 分发包的以下文件夹：

```
Crystal_v11\Oracle
```

选择文件夹，然后选择报告。

**14** 高亮显示 eSecurity\_Reports，单击“显示子文件夹”。

**15** 选择该报告的相应文件夹，单击“显示子文件夹”。

**16** 单击“确定”。

**17** 单击“更新”。

**18** 要添加其余报告，请重复步骤 9 到 17，直到添加完所有报告。

## 10.5 使用 Crystal XI 万维网服务器

Linux 上的 Crystal 服务器 XI 会安装万维网服务器，通过该服务器可以执行管理任务，发布和查看报告。

在浏览器中输入以下 URL 即可访问管理入口站点：

```
http://<hostname_or_IP_of_web_server>:<web_server_port_default_8080>/  
businessobjects/enterprise11/adminlaunch
```

非管理（常用）入口站点则通过在浏览器中输入以下 URL 进行访问：

```
http://<hostname_or_IP_of_web_server>:<web_server_port_default_8080>/  
businessobjects/enterprise11
```

### 10.5.1 测试万维网服务器的连接性

**测试与万维网服务器的连接：**

**1** 转到与您的万维网服务器位于同一网络中的另一台计算机。

**2** Enter

```
http://  
<hostname_or_IP_of_web_server>:<web_server_port_default_8080>/  
businessobjects/enterprise11/adminlaunch
```

**3** 应该会出现 Crystal BusinessObjects 万维网首页。

## 10.6 设置‘命名用户’帐户

随 Crystal Server 提供的许可证密钥是“命名用户”帐户的密钥。Guest 帐户已由“并发用户”更改为“命名用户”。

**将 Guest 帐户设置为“命名用户”：**

**1** 打开 Web 浏览器并输入以下 URL：

```
http://  
<hostname_or_IP_of_web_server>:<web_server_port_default_8080>/  
businessobjects/enterprise11/adminlaunch
```

**2** 单击“中央管理控制台”。

**3** “System Name”应该是您的主机名。“Authentication Type”应该是“Enterprise”。如果不是，请选择“企业”。

- 4 在“组织”窗格中，单击“用户”。
- 5 单击 GUEST。
- 6 将连接类型从“并行用户”更改为“命名用户”。
- 7 单击“更新”。
- 8 注销并关闭窗口。

## 10.7 配置报告权限

此步骤讨论如何使用 Administration Launchpad 配置对报告的权限，以便根据需要查看和修改报告。

### 配置报告权限：

- 1 打开万维网浏览器并输入以下 URL：  
`http://  
<hostname_or_IP_of_web_server>:<web_server_port_default_8080>/  
businessobjects/enterprise11/adminlaunch`
- 2 单击“中央管理控制台”。
- 3 “System Name”应该是您的主机名。“Authentication Type”应该是“Enterprise”。如果不是，请选择“企业”。
- 4 输入您的用户名、口令，然后单击“登录”。
- 5 在“组织”窗格中，单击“文件夹”。
- 6 单击 eSecurity\_Reports。
- 7 选择“全部”。
- 8 单击“权限”选项卡。
- 9 对于所有用户，在右侧的下拉菜单中选择“按需要查看”。
- 10 单击“更新”。
- 11 注销并关闭该窗口。

## 10.8 启用 Sentinel 的前 10 个报告

要启用 Sentinel 的前 10 个报告，必须：

- ◆ 打开汇总
- ◆ 启用 EventFileRedirectService

### 启用聚合

- 1 在 Sentinel 控制中心 GUI 中，单击“管理”选项卡。
- 2 在导航窗格中单击“报告数据”或单击“报告数据”按钮。
- 3 启用下列摘要
  - ◆ EventDestSummary
  - ◆ EventSevSummary
  - ◆ EventSrcSummary

在“Status”列中单击“InActive”，直到其更改为“Active”。

摘要名称	时间	特性	源	状态
EventDestSummary	1 小时	CUST_ID.RSRC_ID ...	TransformedEvent	活动
EventSevDestTxnmyS...	1 小时	CUST_ID.DEST_EV ...	TransformedEvent	非活动
EventSevDestEvtSum...	1 小时	CUST_ID.DEST_EV ...	TransformedEvent	非活动
EventSevDestPortSu...	1 小时	SEV_DEST_PORT_C ...	TransformedEvent	非活动
EventSevSummary	1 小时	CUST_ID.SEV_EVT ...	TransformedEvent	活动
EventSrcSummary	1 小时	CUST_ID.RSRC_ID ...	TransformedEvent	活动

## 启用 EventFileRedirectService

- 1 在您的 DAS 计算机上，使用文本编辑器打开：  
\$ESEC\_HOME/sentinel/config/das\_binary.xml
- 2 对于 EventFileRedirectService，将状态更改为“on”（打开）。  
<property name="status">on</property>
- 3 重新启动 DAS\_Binary 进程。可以通过使用 Sentinel 控制中心或重引导计算机完成此操作。

使用 Sentinel 控制中心：

- ◆ 以具有管理员权限的用户身份登录到 Sentinel 控制中心。此用户必须具有下列“服务器视图”权限：
  - ◆ 查看服务器
  - ◆ 控制服务器
- ◆ 从“Admin”选项卡打开一个服务器视图以查看所有 Sentinel 服务器进程。
- ◆ 右击 DAS\_Binary 进程，然后选择“重新启动”。
- ◆ 如果成功重新启动该流程，则该流程的“启动”计数将增加一。

## 10.9 提高 Crystal Enterprise Server 报告刷新记录限制

根据 Crystal 正在查询的事件数，可能会出现关于最长处理时间或最大记录限制的错误。要将服务器设置为可以处理更多数量或数量不限的记录，需要重配置 Crystal Page Server。

### 重配置 Crystal Page Server:

- 1 打开 Web 浏览器并输入以下 URL：  
http://  
<hostname\_or\_IP\_of\_web\_server>:<web\_server\_port\_default\_8080>/  
businessobjects/enterprisell/adminlaunch
- 2 单击“中央管理控制台”。
- 3 “System Name”应该是您的主机名。“Authentication Type”应该是“Enterprise”。如果不是，请选择“企业”。
- 4 输入您的用户名、口令，然后单击“登录”。
- 5 单击“服务器”。
- 6 单击<服务器名称>.pageserver。
- 7 在“预览或刷新报告时要读取的数据库记录”下，单击“无限记录”。

- 8 单击“应用”。
- 9 将会出现要求重新启动 Page 服务器的提示，单击“确定”。
- 10 可能会提示您输入登录名和口令，以访问操作系统服务管理器。

## 10.10 将 Sentinel 控制中心配置为与 Crystal Enterprise Server 集成

Sentinel 控制中心可以配置为与 Crystal Enterprise Server 集成，这样可以在 Sentinel 控制中心中查看 Crystal Reports。

要启用 Sentinel 控制中心与 Crystal Enterprise Server 的集成，请按照以下说明操作。

---

**注释：**必须在安装了 Crystal Enterprise Server 并向其发布了 Crystal Reports 后再执行此配置。

---

### 将 Sentinel 配置为与 Crystal Enterprise Server 集成：

- 1 以具有访问“管理”选项卡特权的用户身份登录到 Sentinel 控制中心。
- 2 在“管理”选项卡中，选择“报告配置”。
- 3 在“Analysis URL”（分析 URL）字段中，输入以下内容：

```
http://  
<hostname_or_IP_of_web_server>:<web_server_port_default_8080>/  
esec-script/  
GetReports.jsp?APS=<hostname>&user=Guest&password=&tab=Analysis
```

---

**注释：**必须将 <万维网服务器的主机名或 IP 地址> 替换为 Crystal Enterprise Server 的 IP 地址或主机名。

---

**注释：**如果将 APS 设置为 IP 地址，则上述 URL 将无法正常工作。它必须为主机名。

---

**注释：**必须将 <万维网服务器的默认端口 8080> 替换为 Crystal 万维网服务器正在监听的端口。

---

- 4 单击“分析 URL”字段旁边的“刷新”。
- 5 如果您已经安装顾问，请在“Advisor URL”（顾问 URL）字段中输入以下内容：

```
http://  
<hostname_or_IP_of_web_server>:<web_server_port_default_8080>/  
esec-script/  
GetReports.jsp?APS=<hostname>&user=Guest&password=&tab=Advisor
```

---

**注释：**必须将 <万维网服务器的主机名或 IP 地址> 替换为 Crystal Enterprise Server 的 IP 地址或主机名。

---

**注释：**如果将 APS 设置为 IP 地址，则上述 URL 将无法正常工作。它必须为主机名。

---

**注释：**必须将 <万维网服务器的默认端口 8080> 替换为 Crystal 万维网服务器正在监听的端口。

---

- 6 单击“顾问 URL”字段旁边的“刷新”。

- 7 单击“保存”。
- 8 注销，然后重新登录至 Sentinel 控制中心。现在，“Analysis”和“Advisor”（如果已安装顾问）选项卡中的 Crystal Report 树应出现在“Navigator”窗口中。

## 10.11 实用程序和查错

### 10.11.1 启动 MySQL

确保 MySQL 正在运行：

- 1 以 Crystal 用户身份登录。
- 2 转至 `/opt/crystal_xi/bobje`
- 3 `./mysqlstartup.sh`

### 10.11.2 启动 Tomcat

确保 Tomcat 正在运行：

- 1 以 Crystal 用户身份登录
- 2 转至 `/opt/crystal_xi/bobje`
- 3 `./tomcatstartup.sh`

### 10.11.3 启动 Crystal Server

确保 Crystal Server 正在运行：

- 1 以 Crystal 用户身份登录
- 2 转至 `/opt/crystal_xi/bobje`
- 3 `./startservers`

### 10.11.4 Crystal 主机名错误

纠正主机名错误：

- 1 如果收到以下错误提示：

```
Warning: ORB::BOA_init: hostname lookup returned `localhost'
(127.0.0.1)
Use the -OAhost option to select some other hostname
```

请确保您的 IP 地址和主机名在 `/etc/hosts` 文件中。例如，`192.0.2.46linuxCE02`

## 10.11.5 无法连接到 CMS

如果系统报告无法连接到 CMS，请尝试执行以下命令。

### 解决 CMS 连接故障：

- 1 如果命令 `netstat -an | grep 6400` 未返回任何结果，请尝试执行以下操作：
  - ◆ 重新输入 MySQL 连接信息：
    - a. 以 Crystal 用户身份登录
    - b. 转至 `/opt/crystal_xi/bobje`
    - c. `./cmsdbsetup.sh`
    - d. [`<hostname>.cms`] 出现时按 Enter 键
    - e. 选择“选择并重输入在安装时输入的所有 MySQL DB 信息”。有关更多信息，请参阅安装说明。
    - f. 完成后，退出 `cmsdbsetup.sh`
    - g. `./stopservers`
    - h. `./startservers`
  - ◆ 重初始化 MySQL 数据库：
    - a. 以 Crystal 用户身份登录
    - b. 转至 `/opt/crystal_xi/bobje`
    - c. `./cmsdbsetup.sh`
    - d. [`<hostname>.cms`] 出现时按 Enter 键。
    - e. 选择“重初始化”，然后按照说明操作。
    - f. 完成后，退出 `cmsdbsetup.sh`
    - g. `./stopservers`
    - h. `./startservers`
- 2 确保已启用所有 CCM 服务器：
  - 2a 以 Crystal 用户身份登录
  - 2b 转至 `/opt/crystal_xi/bobje`
  - 2c `./ccm.sh` - 全部启用



本章包含下列主题：

- ◆ 卸载 Sentinel（第 137 页）
- ◆ 在 Solaris 和 Linux 上进行卸载（第 137 页）
- ◆ 在 Windows 上卸载（第 138 页）
- ◆ 使用“控制面板”卸载（第 138 页）
- ◆ 后卸载（第 139 页）

为了去除 Sentinel 安装，提供了用于 Linux、Solaris 和 Windows 的卸载程序。保留几个文件（包括日志文件），如果需要，可以手动去除这些文件。此外，强烈建议您执行下列所有步骤，以确保不会发生以前的安装所留下的文件或系统设置影响新安装的情况。

---

**警告：**以下说明包括修改操作系统设置和文件。如果您对修改这些系统设置和 / 或文件不熟悉，请与系统管理员联系。

---

## 11.1 卸载 Sentinel

### 11.1.1 在 Solaris 和 Linux 上进行卸载

启动用于 Solaris 的 Sentinel 卸载程序。

- 1 以根用户身份登录。
- 2 关闭 Sentinel 服务器。
- 3 转至：  
\$ESEC\_HOME/\_uninst
- 4 Enter:  
./uninstall.bin
- 5 选择语言并单击“确定”。
- 6 此时将显示 Sentinel InstallShield 向导。单击“下一步”。
- 7 选择必须卸载的部件，然后单击“下一步”。

---

**注释：** Sentinel 将显示警告讯息，指示关闭所有打开的 Sentinel 应用程序。

---

- 8 系统提示您从下列两个选项中选择：
  - ◆ 删除整个数据库实例。
  - ◆ 只删除数据库对象。选中您的选项并单击“下一步”。
- 9 单击“卸载”。

## 11.1.2 在 Windows 上卸载

### 使用 Sentinel Windows 卸载程序:

- 1 以管理员身份登录。
- 2 关闭 Sentinel 服务器。
- 3 选择“开始” > “程序文件” > “Sentinel” > “卸载 Sentinel”。
- 4 选择语言并单击“确定”。
- 5 此时将显示 Sentinel InstallShield 向导。单击“下一步”。
- 6 选择要卸载的部件，然后单击“下一步”。

---

**注释：** Sentinel 将显示警告讯息，指示关闭所有打开的 Sentinel 应用程序。

---

- 7 系统提示您从下列两个选项中选择：
  - ◆ 删除整个数据库实例。
  - ◆ 只删除数据库对象。选中您的选项并单击“下一步”。
- 8 指定鉴定信息，选择 Windows 鉴定或 SQL 鉴定，并在系统提示时输入登录凭证。单击“下一步”。
- 9 此时将显示选择卸载的功能的摘要。单击“卸载”。
- 10 选择“重引导系统”并单击“完成”。

## 11.1.3 使用“控制面板”卸载

### 卸载 Sentinel Windows 应用程序:

- 1 单击“开始” > “控制面板” > “添加 / 删除程序” > “Sentinel” > “删除 / 更改”。
- 2 选择语言并单击“确定”。
- 3 此时将显示 Sentinel InstallShield 向导。单击“下一步”。
- 4 选择要卸载的部件，然后单击“下一步”。

---

**注释：** Sentinel 将显示警告讯息，指示关闭所有打开的 Sentinel 应用程序。

---

- 5 系统提示您从下列两个选项中选择：
  - ◆ 删除整个数据库实例。
  - ◆ 只删除数据库对象。选中您的选项并单击“下一步”。
- 6 指定鉴定信息，选择 Windows 鉴定或 SQL 鉴定，并在系统提示时输入登录凭证。单击“下一步”。
- 7 此时将显示选择卸载的功能的摘要。单击“卸载”。
- 8 选择“重引导系统”并单击“完成”。

## 11.2 后卸装

### 11.2.1 Sentinel 数据文件

要在卸装 Sentinel 后保留可能有价值的信息，应保留几个文件。如果不再需要此信息，可以手动去除下列文件和文件夹。

- ◆ 3rd Party
  - ◆ SonicMQ
    - ◆ Docs7.0
    - ◆ InstallLogs7.0
    - ◆ MQ7.0
    - ◆ 安装程序
    - ◆ mq\_documentation\_7.0.htm
    - ◆ sonicsw.properties
    - ◆ uninstall.sh
    - ◆ wizard.jar
- ◆ Bin
  - ◆ control\_center.jar
  - ◆ sdm\_gui.jar
- ◆ 配置
  - ◆ .proxyServerKeystore
  - ◆ .primary\_key
  - ◆ .keystore
- ◆ 数据
  - ◆ .超速缓存
  - ◆ .sessionState
  - ◆ .uuid
  - ◆ .uuidlock
  - ◆ DatabaseManager.log
  - ◆ agent-84EBED40-9AB1-1029-9C3F-0003BAC9707D.lock
  - ◆ 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
- ◆ 所有这些文件可以在 \$ESEC\_HOME 或 %ESEC\_HOME% 目录及其子目录中找到。
- ◆ 对于 Advisor，用于 Advisor 数据文件的 attack 和 alert 文件夹将保留。

### 11.2.2 Sentinel 设置

卸装了 Sentinel 后，某些系统设置仍将保留，可以手动删除。在执行 Sentinel 的全新安装之前，应去除这些设置， Sentinel 卸装遇到错误时尤其应当如此。

---

**注释：**在 Solaris 和 Linux 上，卸载 Sentinel 服务器不会将 Sentinel 管理员用户从操作系统中去除。如果需要，您将需要手动去除该用户。

---

## 在包含 Oracle 的 Linux 上去除 Sentinel 系统设置

### 在 Linux 上手动清理 Sentinel:

- 1 以根用户身份登录。
- 2 确保所有 Sentinel 流程均已停止。
- 3 去除 /opt/sentinelXX（或 Sentinel 软件的任何安装和命名位置）下的内容
- 4 将 S98sentinel 文件从 /etc/rc.d/rc5.d 目录中去除。
- 5 将 S98sentinel 文件从 /etc/rc.d/rc3.d 目录中去除。
- 6 将 K02sentinel 文件从 /etc/rc.d/rc0.d 目录中去除。
- 7 将 sentinel 文件从 /etc/init.d 目录中去除。
- 8 去除 /root/Install Shield 目录。
- 9 去除 /root/vpd.properties 文件
- 10 确保任何用户都无法以 Sentinel 管理员用户的身份登录（默认用户为 esecadm），然后去除 Sentinel 管理员用户（和主目录）和 esec 组。
  - ◆ 运行：userdel -r esecadm
  - ◆ 运行：groupdel esec
- 11 如果存在 .login 文件，则去除 /etc/profile、/etc/.login 的 Install Shield 部分。
- 12 去除 Sentinel Oracle 数据库。有关更多信息，请参考在 [Linux 上手动清理 Sentinel Oracle 数据库：（第 141 页）](#)。
- 13 重新启动操作系统。

### 在 Linux 上手动清理 Sentinel Oracle 数据库:

---

**注释：**在去除之前，确保没有任何其他应用程序正在使用此数据库。

---

- 1 以 oracle 身份登录。
- 2 停止 Oracle 侦听程序：
  - ◆ 运行：lsnrctl stop
- 3 停止 Sentinel 数据库。
  - ◆ 将 ORACLE\_SID 环境变量设置为 Sentinel 数据库实例的名称（通常为 ESEC）。
  - ◆ 运行：sqlplus '/ as sysdba'
  - ◆ 在 sqlplus 提示符下运行：shutdown immediate
- 4 去除 /etc/oratab 文件中 Sentinel 数据库的项
- 5 去除目录 \$ORACLE\_HOME/dbs 中的 init<您的实例名称>.ora（通常为 initESEC.ora）文件。
- 6 从 \$ORACLE\_HOME/network/admin 目录中的以下文件中去除 Sentinel 数据库的项：
  - ◆ tnsnames.ora

- ◆ listener.ora

7 将数据库数据文件从您所选的安装位置删除。

## 在包含 Oracle 的 Solaris 上去除 Sentinel 系统设置

### 在 Solaris 上手动清理 Sentinel:

---

**注释:** 卸装 Sentinel 遇到错误时, 通常使用手动清理。

---

- 1 以根用户身份登录。
- 2 确保未在运行任何 Sentinel 流程。
- 3 去除 /opt/sentinelxx (或任何安装了 Sentinel 软件的位置) 下的内容。
- 4 将 S98sentinel 文件从 /etc/rc3.d 目录中去除。
- 5 将 K02sentinel 文件从 /etc/rc0.d 目录中去除。
- 6 将 sentinel 文件从 /etc/init.d 目录中去除。
- 7 清理 /var/sadm/pkg 中的 Installshield 参照。去除 /var/sadm/pkg 目录中的以下文件:
  - ◆ 所有以 IS 开头的文件 (在命令行中为 IS\*)
  - ◆ 所有以 ES 开头的文件 (在命令行中为 ES\*)
  - ◆ 所有以 MISCwp 开头的文件 (在命令行中为 MISCwp\*)
- 8 确保任何用户都无法以 Sentinel 管理员用户的身份登录, 然后去除 Sentinel 管理员用户 (和主目录) 和 esec 组。
  - ◆ 运行: userdel -r esecadm
  - ◆ 运行: groupdel esec
- 9 如果存在 .login 文件, 则去除 /etc/profile、/etc/.login 的 Install Shield 部分。
- 10 去除 /Install Shield 目录 (如果存在)。
- 11 重新启动操作系统。

### 在 Solaris 上手动清理 Sentinel Oracle 数据库:

---

**注释:** 在去除之前, 确保没有任何其他应用程序正在使用此数据库。

---

- 1 以 oracle 身份登录。
- 2 停止 Oracle 侦听程序:
  - ◆ 运行: lsnrctl stop
- 3 停止 Sentinel 数据库:
  - ◆ 将 ORACLE\_SID 环境变量设置为 Sentinel 数据库实例的名称 (通常为 ESEC)。
  - ◆ 运行: sqlplus '/ as sysdba'
  - ◆ 在 sqlplus 提示符下运行: shutdown immediate
- 4 去除 /var/opt/oracle/oratab 文件中 Sentinel 数据库的项
- 5 去除目录 \$ORACLE\_HOME/dbs 中的 init<您的实例名称>.ora (通常为 initESEC.ora) 文件。

6 从 \$ORACLE\_HOME/network/admin 目录中的以下文件中去除 Sentinel 数据库的项:

- ◆ tnsnames.ora
- ◆ listener.ora

7 将数据库数据文件从您所选的安装位置删除。

## 在包含 SQL Server 的 Windows 上去除 Sentinel 系统设置

### 在 Windows 上手动清理 Sentinel:

- 1 删除文件夹 %CommonProgramFiles%\InstallShield\Universal 及其所有内容。
- 2 删除 %ESEC\_HOME% 文件夹 (默认文件夹: C:\Program Files\novell\sentinel6)。
- 3 右击“我的电脑” > “属性” > “高级”选项卡。
- 4 单击“环境变量”按钮。
- 5 删除下列变量 (如果存在):
  - ◆ ESEC\_HOME
  - ◆ ESEC\_VERSION
  - ◆ ESEC\_JAVA\_HOME
  - ◆ ESEC\_CONF\_FILE
  - ◆ WORKBENCH\_HOME
- 6 去除 PATH 环境变量中所有指向 Sentinel 安装的项。

---

**警告:** 不要去除旧 Sentinel 安装以外的任何其他路径。这样可能会导致系统无法正常运行。

---

- 7 删除桌面上的所有 Sentinel 快捷方式。
- 8 从“开始”菜单中删除快捷方式文件夹“开始” > “程序” > “Sentinel”。
- 9 重新启动操作系统。

### 在 Windows 上手动清理 Sentinel Microsoft SQL Server 数据库:

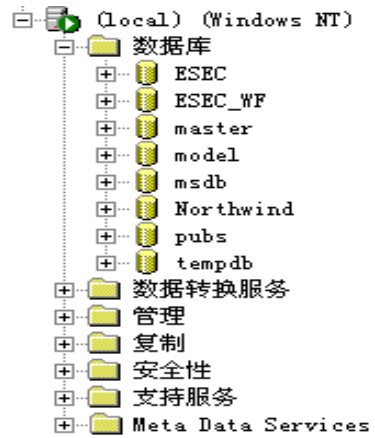
---

**注释:** 在去除之前, 确保没有任何其他应用程序正在使用此数据库。

---

- 1 打开 Microsoft SQL Server Management Studio, 并连接到已安装 Sentinel 数据库的 SQL Server 实例。

2 展开“数据库”树，找到 Sentinel 数据库。



3 应有 Sentinel 数据数据库（通常称为 ESEC）和 workflow 数据库（通常称为 ESEC\_WF）。右击每个数据库并选择“删除”。

4 出现提示后，选择“Yes”删除该数据库。



# 安装前调查问卷



## 安装前问题

- 1 您使用 Novell Sentinel 是要达到什么目标或目的？
  - 1a 与业界标准保持一致
  - 1b SEM
  - 1c 其他 \_\_\_\_\_
- 2 为安装 Sentinel 分配了什么硬件？是否符合《Sentinel 安装指南》中提供的硬件规格？
- 3 是否已根据您的配置验证《Sentinel 安装指南》中所述的 Sentinel 硬件和操作系统要求？
  - ◆ 操作系统增补程序级别
  - ◆ 服务增补程序
  - ◆ 热修复等
- 4 您的 DAS 计算机是否满足所需的操作系统和硬件要求？
- 5 源设备相对于 Sentinel 和收集器硬件所在的安全性段，使用的是什么网络结构？

---

**注释：**了解收集器数据集合的层次，以及确定为启用 Sentinel 通讯的收集器、数据库通讯的 Sentinel 或数据库通讯的 Crystal 服务器而必须穿透的全部防火墙非常重要。

---

在下面输入信息（文本和 / 或图形），或信息的链接。

- 6 您希望系统生成哪些报告？这对于确保收集器能收集到要传递给 Sentinel 数据库的正确数据非常重要。
  - 6a \_\_\_\_\_
  - 6b \_\_\_\_\_
  - 6c \_\_\_\_\_
  - 6d \_\_\_\_\_

6e \_\_\_\_\_

6f \_\_\_\_\_

- 7 您希望从哪些源设备中收集数据（IDS、HIDS、路由器、防火墙等）？事件发生率（EPS – 每秒发生的事件数）、版本、连接方法、平台和增补程序各是什么？

---

设备 ( 制造商 / 型号 )	事件率 (EPS)	版本	连接方法	平台	增补程序
-----------------	-----------	----	------	----	------

---

---

您能够举例说明您希望 Sentinel 收集器收集哪些数据并对其进行语法分析吗？可以将 Sentinel 配置为根据此处提供的信息提供所需的输出。

- 8 您的站点上有哪些安全模型 / 标准？
- ◆ 您对本地帐户和域鉴定怎么看？
    - ◆ 如果使用 Windows 域鉴定，则必须创建正确的域帐户设置，确保可以安装 Sentinel。
    - ◆ 对于 Solaris 安装，此问题不适用。因为 Sentinel 不支持 NIS。
- 9 必需的数据保留时间为多少天？
- 10 根据数据保留时间信息和 EPS，您需使用的磁盘大小是多少？估算大小时，请按每个事件要占用 500 到 800 字节来计算。

# 在包含 Oracle 的 Linux 上安装 Sentinel 的记录

此核对清单适用于分布式安装（最多包含三个收集器管理器和关联引擎实例）。

请参阅《安装指南》中的硬件和操作系统要求以及安装步骤。

## 配置变量

- |   |   |  |
|---|---|--|
| 1. Sentinel 版本：   | 当前日期：   |  |
| 2. 用于 Oracle 的 UNIX 内核值。以下是<br>最小值：在 SLES 和 RHEL 中，可以在“etc/sysctl.conf”中设置参数。 |   |  |
| ◆ shmmax  | <input type="checkbox"/> ：是   <input type="checkbox"/> ：否 | 如果大于该值，请采用该值：  |
| ◆ shmmmin   | <input type="checkbox"/> ：是   <input type="checkbox"/> ：否 | 如果大于该值，请采用该值：  |
| ◆ shmseg  | <input type="checkbox"/> ：是   <input type="checkbox"/> ：否 | 如果大于该值，请采用该值：  |
| ◆ shmmni  | <input type="checkbox"/> ：是   <input type="checkbox"/> ：否 | 如果大于该值，请采用该值：  |
| ◆ semmns  | <input type="checkbox"/> ：是   <input type="checkbox"/> ：否 | 如果大于该值，请采用该值：  |
| ◆ semmni  | <input type="checkbox"/> ：是   <input type="checkbox"/> ：否 | 如果大于该值，请采用该值：  |
| ◆ semmsl  | <input type="checkbox"/> ：是   <input type="checkbox"/> ：否 | 如果大于该值，请采用该值：  |
| ◆ shmopm  | <input type="checkbox"/> ：是   <input type="checkbox"/> ：否 | 如果大于该值，请采用该值：  |
| ◆ shmvmx  | <input type="checkbox"/> ：是   <input type="checkbox"/> ：否 | 如果大于该值，请采用该值：  |
| 3. 数据库系统  |   |  |
| ◆ Sentinel 部件的操作系统是否正确  | <input type="checkbox"/> ：是   <input type="checkbox"/> ：否 | ◆ 增补程序是否正确 <input type="checkbox"/> ：是   <input type="checkbox"/> ：否 |
| ◆ 数据库的操作系统是否正确  | <input type="checkbox"/> ：是   <input type="checkbox"/> ：否 | ◆ 增补程序是否正确 <input type="checkbox"/> ：是   <input type="checkbox"/> ：否 |
| ◆ 版本  |   | ◆ 增补程序级别   |
| ◆ 带有分区功能的 Oracle 数据库是否正确  | <input type="checkbox"/> ：是   <input type="checkbox"/> ：否 | ◆ 增补程序是否正确 <input type="checkbox"/> ：是   <input type="checkbox"/> ：否 |
| ◆ 版本  |   | ◆ 增补程序级别   |

---

**配置变量**

---

- ◆ 为 Oracle 操作系统用户设置的环境变量是否正确。  : 是 |  : 否
- ◆ Init.ora 文件是否已配置  : 是 |  : 否
- 4. DAS 计算机
  - ◆ Sentinel 部件的操作系统是否正确 : 是 | : 否
  - ◆ 序列号
  - ◆ 许可证密钥
  - ◆ 增补程序是否正确 : 是 | : 否
- 5. DAS 安装
  - ◆ 数据库主机名或 IP
  - ◆ 数据库名称 默认 : ESEC
  - ◆ 数据库端口 默认 : 1521
  - ◆ JDBC 文件位置
- 6. 数据库实例 (SID)
- 7. 数据库名称
- 8. Sentinel 部件 :
  - ◆ Sentinel 数据库 ( IP 或 DNS ) OS:  
增补程序 :
  - ◆ 数据库安装日志
  - ◆ Oracle 内存 (RAM)
  - ◆ 实例名称
  - ◆ 监听器端口 默认 : 1521
  - ◆ SYS 口令
  - ◆ SYSTEM 口令
  - ◆ .keystore 文件是否已在安装时导入 :
  - ◆ 关联  : 是 |  : 否
  - ◆ DAS  : 是 |  : 否
  - ◆ 收集器管理器  : 是 |  : 否
  - ◆ 通讯服务器  : 是 |  : 否
  - ◆ 通讯服务器 (iSCALE) ( IP 或 DNS ) ◆ IP/DNS : OS:  
增补程序 :
  - ◆ DAS/Advisor ( IP 或 DNS ) ( Advisor 为可选 ) ◆ OS:  
增补程序 :

---

**配置变量**

---

- ◆ DAS RAM ◆
- ◆ 关联引擎 ( IP 或操作系统 )
  - ◆ IP : OS:
  - ◆ IP : OS:
  - ◆ IP : OS:
- ◆ 收集器构建程序 ( IP 或 DNS )  
( 推荐安装一个 )
- ◆ 收集器管理器 输入要部署的每个收集器管理器的细节。
- ◆ 收集器管理器 : 是 | : 否
  - ◆ IP : ◆ 讯息总线端口 :
  - ◆ OS: ◆ Sentinel 控制中心代理端口 :
  - ◆ ◆ 通讯服务器的主机名 :
  - ◆ ◆ 收集器管理器证书鉴定端口 :
- 9. 顾问 ( 可选 )
  - ◆ 是否与 DAS 安装在同一台计算机上? : 是 | : 否
  - ◆ Advisor 下载 : : 单独 | : 直接因特网下载
  - ◆ 数据传递文件位置
  - ◆ 顾问源地址
  - ◆ 顾问目标地址
  - ◆ 用户名 u/n:
- 10. 数据库文件位置 :
  - ◆ 数据文件
  - ◆ 索引文件
  - ◆ 摘要数据文件
  - ◆ 摘要索引文件
  - ◆ 临时和复原表空间文件
  - ◆ 重做日志成员 A 目录
  - ◆ 重做日志成员 A 目录
- 11. 数据库大小 :
  - ◆ 标准 (20 GB)
  - ◆ 大型 (400 GB)
  - ◆ 自定义 ( 大小 )



# 在包含 Oracle 的 Solaris 上安装 Sentinel 的记录



此核对清单适用于分布式安装（最多包含三个收集器管理器和关联引擎实例）。

有关更多信息，请参阅《安装指南》中的硬件和操作系统要求以及安装步骤。

---

## 配置变量

---

- |   |   |  |
|---|---|--|
| 1. Sentinel 版本 :  | 当前日期 :  |  |
| 2. 用于 Oracle 的 UNIX 内核值。以下是最小值：在 SLES 和 RHEL 中，可以在“etc/sysctl.conf”中设置参数。 |   |  |
| shmmax  | <input type="checkbox"/> : 是   <input type="checkbox"/> : 否 | 如果大于该值，请采用该值：  |
| shmmin  | <input type="checkbox"/> : 是   <input type="checkbox"/> : 否 | 如果大于该值，请采用该值：  |
| shmseg  | <input type="checkbox"/> : 是   <input type="checkbox"/> : 否 | 如果大于该值，请采用该值：  |
| shmmni  | <input type="checkbox"/> : 是   <input type="checkbox"/> : 否 | 如果大于该值，请采用该值：  |
| semms   | <input type="checkbox"/> : 是   <input type="checkbox"/> : 否 | 如果大于该值，请采用该值：  |
| semni   | <input type="checkbox"/> : 是   <input type="checkbox"/> : 否 | 如果大于该值，请采用该值：  |
| semmsl  | <input type="checkbox"/> : 是   <input type="checkbox"/> : 否 | 如果大于该值，请采用该值：  |
| shmopm  | <input type="checkbox"/> : 是   <input type="checkbox"/> : 否 | 如果大于该值，请采用该值：  |
| shvmx   | <input type="checkbox"/> : 是   <input type="checkbox"/> : 否 | 如果大于该值，请采用该值：  |
| 3. 数据库系统  |   |  |
| Sentinel 部件的操作系统是否正确  | <input type="checkbox"/> : 是   <input type="checkbox"/> : 否 | 增补程序是否正确 <input type="checkbox"/> : 是   <input type="checkbox"/> : 否   |
| ◆ 数据库的操作系统是否正确  | <input type="checkbox"/> : 是   <input type="checkbox"/> : 否 | ◆ 增补程序是否正确 <input type="checkbox"/> : 是   <input type="checkbox"/> : 否 |
| ◆ 带有分区功能的 Oracle 数据库是否正确  | <input type="checkbox"/> : 是   <input type="checkbox"/> : 否 | ◆ 增补程序是否正确 <input type="checkbox"/> : 是   <input type="checkbox"/> : 否 |
| ◆ 版本  |   | ◆ 增补程序级别   |
| ◆ 是否已复制 Oracle 注释：148673.1  | <input type="checkbox"/> : 是   <input type="checkbox"/> : 否 |  |

---

## 配置变量

---

- ◆ 为 Oracle 操作系统用户设置的环境变量是否正确。  : 是 |  : 否
  - ◆ Init.ora 文件是否已配置  : 是 |  : 否
  - ◆ Sentinel 部件的操作系统是否正确  : 是 |  : 否
  - ◆ 增补程序是否正确  : 是 |  : 否
4. DAS 计算机
- ◆ 序列号
  - ◆ 许可证密钥
5. DAS 安装
- ◆ 数据库主机名或 IP
  - ◆ 数据库名称 默认 : ESEC
  - ◆ 数据库端口 默认 : 1521
  - ◆ JDBC 文件位置
6. 数据库实例 (SID)
7. 数据库名称
8. Sentinel 部件 :
- ◆ Sentinel 数据库 ( IP 或 DNS ) OS:
  - ◆ 数据库安装日志 增补程序 :
  - ◆ Oracle 内存 (RAM)
  - ◆ 实例名称
  - ◆ 监听器端口 默认 : 1521
  - ◆ SYS 口令
  - ◆ SYSTEM 口令
  - ◆ .keystore 文件是否已在安装时导入 :
  - ◆ 关联  : 是 |  : 否
  - ◆ DAS  : 是 |  : 否
  - ◆ 收集器管理器  : 是 |  : 否
  - ◆ 收集器管理器
  - ◆ 安装收集器管理器 :  : 是 |  : 否 代理 | 直接讯息总线



---

**配置变量**

---

- ◆ IP :
- ◆ OS:
- ◆ 消息总线端口 :
- ◆ Sentinel 控制中心代理端口 :
- ◆ 通讯服务器的主机名 :
- ◆ 收集器管理器证书鉴定端口 :
  
- ◆ 通讯服务器 : 是 | : 否
- ◆ 通讯服务器 (iSCALE) ( IP 或 DNS ) : 是 | : 否 OS:  
增补程序 :
- ◆ DAS/Advisor ( IP 或 DNS ) OS:  
( Advisor 为可选 ) 增补程序 :
- ◆ DAS RAM
- ◆ 关联引擎 ( IP 或操作系统 )
  
- IP : OS:
- IP : OS:
- IP : OS:
  
- ◆ Crystal 服务器 ( IP 或 DNS )
- ◆ 用于 Crystal Server 的 MySQL MySQL 版本 :  
MySQL 增补程序 :  
sa 命令或口令的占位符 :
- ◆ IP : u/n: 命令 : OS:
- ◆ 收集器构建程序 ( IP 或 DNS )  
( 推荐安装一个 )
- ◆ 收集器管理器
- ◆ 安装收集器管理器时使用 : : 是 | : 否 : 代理 | : 直接消息总线
- ◆ IP : 命令 : OS:
- ◆ IP : 命令 : OS:
- ◆ IP : 命令 : OS:

**9. 顾问 ( 可选 )**

- 是否与 DAS 安装在同一台计算机上? : 是 | : 否
- ◆ Advisor 下载 : : 单独 : 直接因特网下载
  - ◆ 数据传递文件位置
  - ◆ 顾问源地址
  - ◆ 顾问目标地址
  - ◆ 用户名和口令 u/n:



# 在包含 Microsoft SQL Server 的 Windows 上安装 Sentinel 的记录

此核对清单适用于分布式安装（最多包含三个收集器管理器和关联引擎实例）。

有关更多信息，请参阅《安装指南》中的硬件和操作系统要求以及安装步骤。

---

**配置变量**

---

1. Sentinel 版本 : 当前日期 :  
 数据库系统

- ◆ 数据库的操作系统是否正确  : 是 |  : 否
- ◆ SQL 数据库是否正确  : 是 |  : 否
- ◆ 版本
- ◆ 增补程序是否正确  : 是 |  : 否
- ◆ 增补程序是否  : 是 |  : 否
- ◆ 增补程序级别

2. 对于 Windows 域帐户下的 DAS 安装，指派 ‘作为服务登录’  : 是 |  : 否

3. DAS 计算机

- ◆ 序列号
- ◆ 许可证密钥

4. 数据库主机名或 IP : < 主机名 >[\< 实例名称 >]

5. 数据库名称 : 默认 : ESEC

6. 端口 : 默认 : 1433

7. 鉴定方式  : 混合  
 : 非混合

8. SQL Server sa 口令或口令的占位符。  口令 :

9. Sentinel 部件 :

- ◆ Sentinel 数据库 ( IP 或 DNS ) OS:
- ◆ .keystore 文件是否已在安装时导入 : 增补程序 :
- ◆ 关联  : 是 |  : 否
- ◆ DAS  : 是 |  : 否

---

**配置变量**

---

- ◆ 收集器管理器服务  : 是 |  : 否
  - ◆ 通讯服务器  : 是 |  : 否
  - ◆ 通讯服务器 (iSCALE) ( IP 或 DNS ) OS:  
增补程序 :
  - ◆ DAS/Advisor ( IP 或 DNS ) OS:  
( Advisor 为可选 ) 增补程序 :
  - ◆ 关联引擎 ( IP 或操作系统 )  
IP : OS:  
IP : OS:  
IP : OS:
  - ◆ Crystal 服务器 ( IP 或 DNS ) OS:  
增补程序 :
  - ◆ 用于 Crystal Server 的 Microsoft SQL Server MS SQL 版本 :  
MS SQL 增补程序 :  
sa 口令或口令的占位符 :
  - ◆ 收集器构建程序 ( IP 或 DNS ) ( 推荐安装一个 )
  - ◆ 收集器管理器 ( 收集器服务 口令以及 IP 或 DNS 和操作系统 )
  - ◆ 收集器管理器  : 是 |  : 否  代理 |  直接讯息总线
  - ◆ IP :
    - ◆ 讯息总线端口 :
  - ◆ OS:
    - ◆ Sentinel 控制中心代理端口 :
    - ◆ 通讯服务器的主机名 :
    - ◆ 收集器管理器证书鉴定端口 :
10. 顾问 ( 可选 )
- 是否与 DAS 安装在同一台计算机上?  : 是 |  : 否
- ◆ Advisor 下载 :  : 单独 |  : 直接因特网下载
  - ◆ 数据传递文件位置
  - ◆ 顾问源地址
  - ◆ 顾问目标地址
  - ◆ 用户名和口令 u/n:
11. 数据库文件位置 :
- ◆ 数据文件

---

**配置变量**

---

- ◆ 索引文件
  - ◆ 摘要数据文件
  - ◆ 摘要索引文件
  - ◆ 日志文件
12. 数据库大小：
- ◆ 标准 (20 GB)
  - ◆ 大型 (400 GB)
  - ◆ 自定义 (大小)
13. SMTP 服务器  
(DNS 或 IP)
14. 用于 SQL 身份验证 (口令)
- ◆ esecadm                      口令：
  - ◆ esecapp                      口令：
  - ◆ esecdba                      口令：
  - ◆ esecrpt                      口令：
15. 用于 Windows 身份验证 (口令)
- ◆ 数据库管理员 (登录名)    u/n:
  - ◆ 应用程序用户 (登录名和口 u/n:                      口令：  
令)
  - ◆ Sentinel 管理员 (登录名) u/n:
  - ◆ Sentinel 报告用户 (登录 u/n:  
名)

**Crystal 安装**

1. Crystal 版本：  
OS  
数据库  
Crystal 服务器 (IP 或 DNS)  
Microsoft SQL (推荐；可选)    Microsoft SQL 版本：  
Microsoft SQL 增补程序：  
sa 口令或口令的占位符：  
IP :                      u/n:                      口令 :                      OS:
2. Crystal Reports  
报告类型                       : SQL                       : Oracle

---

**配置变量**

---

- ◆ 是否已发布所有报告      : 是 | : 否
  - ◆ 是否已在 SCC 上配置报告      : 是 | : 否
-