# 第三章需求建模

本章主要的内容是对业务和需求进行建模。首先介绍了系统的整体情况，指出了利益相关者，并解释了关键的业务概念。根据实际需求给出了系统的用例图，并指出分析了系统的关键用例。最后，给出了系统的领域模型。



## 业务建模

通过业务建模使用系统的需求更加清晰，确保客户、最终用户和开发人员就目标组织达成共识，它是软件工程中重要的一环。同时，通过业务建模可以确定系统的目标和范围，指出利益相关者。

### 利益相关者

本文所介绍的服务器监控系统的主要功能是针对服务器的各种性能参数进行实时监控，在出现异常情况时系统可自动发送邮件通知用户。主要目的是帮助维护人员对需要监控的服务器实现实时监控，并且可以使维护人员在服务器出现异常情况时及时采取措施处理。该模块的主要功能如下：

维护人员可以在给定的监控点中选择监控点（部分或全部监控点）对服务器（所有或部分服务器）实施监控。

在页面中选择需要查看的监控内容，如所有服务器的运行情况、所有服务器的某个监控点（如CPU、Net等）的详细信息、某个服务器的所有监控点或单个监控点的监控信息变换等持续实时监控信息。

维护人员还可以为每个监控点设置相应的阈值，在监控所得到的监控值超出阈值时，由系统发送报警邮件通知维护人员。

该监控系统主要的利益相关者有：

* 运维人员：运维人员可以利用该服务器监控系统对目标监控的服务器进行实时监控，运维人员登录该系统注册服务器添加服务器IP等配置就能查看该服务器的监控数据，同时能自己设置阈值，当服务器监控项数据超过设置的阈值，运维人员会收到报警邮件。
* 系统管理员：系统管理员可通过该监控系统对运维人员注册的服务器进行监控，阈值超过时系统管理员能编辑自动发给运维人员的警报邮件。

### 业务概念

本小节对系统所涉及的相关业务概念进行介绍，如表3-1所示：

表3‑1 业务概念释义

|  |  |
| --- | --- |
| **业务概念** | **释义** |
| 用户 | 系统的使用者（需要对服务器进行监控的人员） |
| 监控 | 系统对服务器群的性能信息进行实时采集并分析，在出现异常情况时触发一定操作以保证各服务器正常运行 |
| 监控点 | 监控功能所需要实施监控的内容 |
| 被监控  服务器 | 监控功能所适用的，需要被监控的服务器 |
| 阈值 | 为每个监控点所包含的监控项所设置的限制值 |
| 警报信息 | 在监控过程中，监控项超出阈值时产生的提示信息 |
| 警报邮箱 | 系统在产生警报信息之后，会自动将警报信息发送到被指定的邮箱 |

### 核心业务流程分析

**实时监控**：实时监控是本系统最核心的业务，主要包括几个过程：用户即维护人员首先登陆运维系统，注册好服务器，然后对服务器的监控点进行设置，同时设置需要监控的监控项的阈值，并设置好警报邮箱。接下来该模块会自动对设置的服务器进行实时监控。

**定义监控点：**更改在服务器中的开机自动运行的agent代码；更改监控程序中的监控信息解析代码，使监控程序可以解析新的由服务器发送到数据库中的监控信息；使用更改过的agent代码，更新已运行在被监控的服务器中的agent代码；重启被监控的服务器，更改后的agent代码自动运行，定期发送监控数据。

**报警设置**：用户对需要监控异常的监控点设置阈值，或者更改已有的阈值；用户设置接收报警邮件的邮箱，或更改、添加、删除已设置的邮箱；开始监控后，系统监控过程中监测到出现异常时会自动发送邮件到指定邮箱。

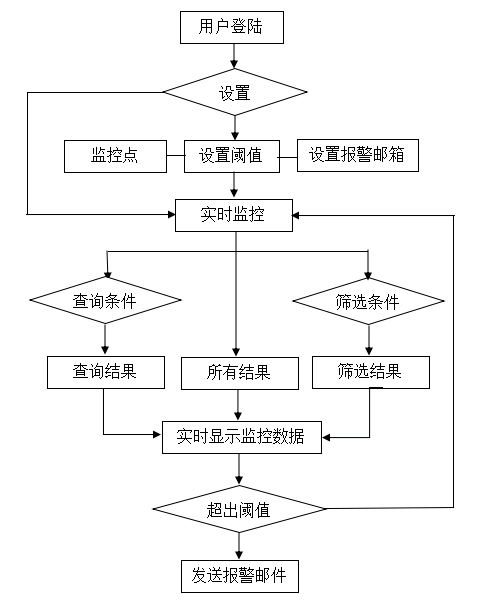
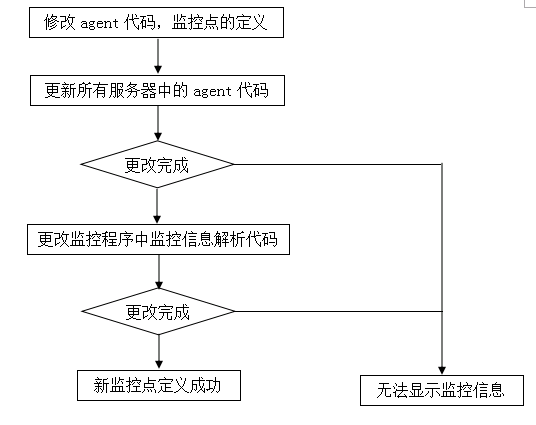
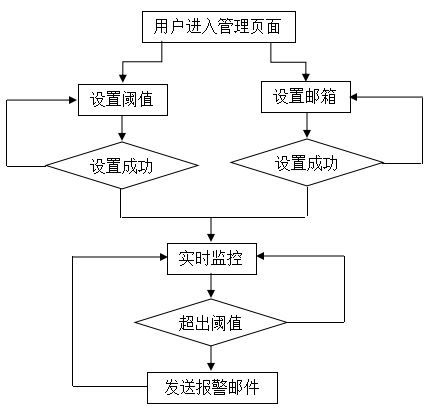


图3‑1 整体业务流程

图3‑2 定义监控点业务流程 图3‑3 报警设置业务流程

## 需求分析

### 系统用例图

本小节根据系统的业务模型，分析出系统利益相关者的用例图。

维护人员主要的权限有：定义点监控、报警设置、监控数据等功能。用例图如图3-4所示。

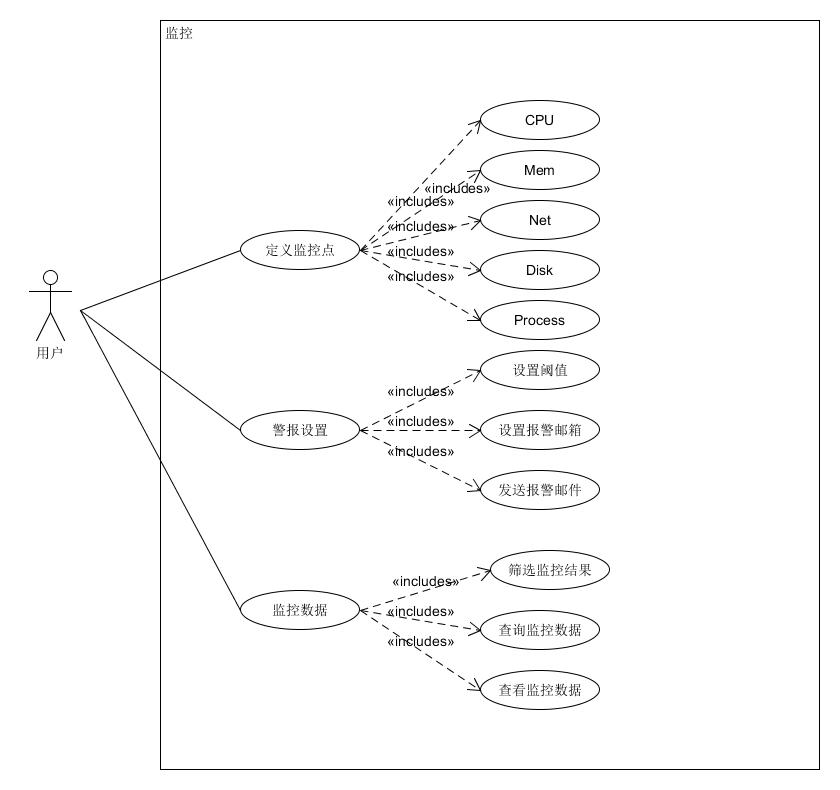


图3‑4 维护人员用例

### 关键用例分析

根据上一小节的用例图，简单介绍系统的一些关键用例。

* 监控点定义

定义监控点是启动实时监控前的首要工作，监控点关系到监控的对象，监控点定义会直接影响到监控结果。

表3‑2 定义监控点用例

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| 用例基本  属性 | 用例编号 | 1 | 用例名称 | | 定义监控点 |
| 业务说明 | 定义需被监控的监控点 | | 优先级 | 高 |
| 使用级别 | 低（配置服务器时将代码放入服务器中，之后不再改变） | | | |
| 前置条件 | | 用户可更改代码 | | | |
| 后置条件 | | 系统中的每个服务器中的agent程序将会定期获取各监控点所监控的内容，发送监控信息到数据库中 | | | |
| 用例事件流说明 | 基本事件流 | 1. 更改在服务器中的开机自动运行的agent代码，更改监控点的定义（如：需要对哪些监控点，哪些监控点的监控项进行监控） 2. 更改监控程序中的监控信息解析代码，使监控程序可以解析新的由服务器发送到数据库中的监控信息 3. 使用更改过的agent代码，更新已运行在被监控的服务器中的agent代码 4. 重启被监控的服务器，更改后的agent代码自动运行，定期发送监控数据 | | | |
| 异常事件流 | 1. 用户只更改agent代码，没有更改监控程序中的监控信息解析代码，则监控程序无法继续监控，所有监控信息都不显示 2. 用户未修改agent代码，而修改了监控程序中的监控信息解析代码，则监控程序无法继续监控，所有监控信息都不显示 | | | |
| 辅助功能（可选） | 在监控信息解析出错时，监控程序发出警报 | | | |
| 提示信息（可选） | 提示：“可能监控信息解析过程出错” | | | |
| 业务表单 | | 数据库中维护表单：<Key（服务器ID）,Value（监控信息）> | | | |

* 监控数据

监控数据主要是对监控显示的数据进行一系列操作，如筛选监控结果、查找监控结果、或选择性查看监控结果。

表3‑3 监控数据用例

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| 用例基本  属性 | 用例编号 | 2 | 用例名称 | | 监控数据 | |
| 业务说明 | 实时监控，并对查询结果进行操作 | | 优先级 | | 中 |
| 使用级别 | 高 | | | | |
| 前置条件 | | 用户已登录，进入监控页面对服务器进行实时监控 | | | | |
| 后置条件 | | 根据用户设置的筛选条件或查询条件，监控页面中显示出相应的监控数据结果。或用户未设置筛选/查询条件时，则监控页面显示所有的监控信息。 | | | | |
| 用例事件流说明 | 基本事件流 | 筛选：用户在监控点列表中选择需要筛选的监控点，在页面中显示出对应服务器以及对应监控点的监控数据。  查询：用户输入查询条件，系统在监控结果中对监控数据进行查询，并将查询结果返回，在页面中显示出查询结果  查看：查看查询条件后或未设置查询条件的监控信息 | | | | |
| 异常事件流 | 筛选：若用户只选择监控点未选择宿主机或容器，则显示所有宿主机和容器对应监控点的信息。若只选择宿主机或容器未选择监控点，则显示该宿主机或容器的所有监控信息。若全部筛选条件都未选择，则显示所有服务器的所有监控信息。  查询：若用户输入不合法的查询条件（如不合法的限制值），或查询条件不完整时，无返回结果，提示错误信息。若用户所有查询条件都为输入时，显示所有服务器的所有监控信息。  筛选、查询：如查询结果为空，则在监控页面显示“无结果” | | | | |
| 辅助功能（可选） | 显示监控结果时，若监控结果出现有异常（可与阈值限制结合），则在该条监控信息被标记为其他形式（如在信息前标记报警小图标、字体颜色显示为红色等）  查询条件、筛选条件清除按钮  查询条件、筛选条件记录,且可下拉选择最近几次的查询记录 | | | | |
| 提示信息（可选） | 查询：如果输入不合法的查询信息或查询条件输入不完全，则弹出窗口通知错误。  筛选、查询：如查询筛选结果为空，则在监控页面显示“无结果” | | | | |
| 业务表单 | | 数据库中维护表单：<Key（服务器ID）,Value（监控信息）> | | | | |

* 警报设置

警报设置主要是对用户设置的监控点进行阈值设置后，当监控数据超过阈值，系统会自动给维护人员发送警报信息的过程。

表3-4 警报设置用例

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| 用例基本  属性 | | 用例编号 | 3 | 用例名称 | 警报设置 | |
| 业务说明 | 定义阈值实现报警功能 | | 优先级 | 高 |
| 使用级别 | 中 | | | |
| 前置条件 | | | 用户已登录，进入监控管理页面对警报功能进行设置 | | | |
| 后置条件 | | | 当超过设定阈值，系统可在发现异常时自动发送报警邮件 | | | |
| 用例事件流说明 | 基本事件流 | | 1. 用户对需要监控的监控点设置阈值，或者更改已有阈值 2. 用户设置接收报警信息的方式，短信、微信或者邮箱 3. 用户设置接收报警邮件的邮箱（先暂定为此方式），或更改、添加、删除已设置邮箱 4. 开始监控后，系统监控过程中监测到异常时会自动发送邮件（或其他方式）到指定邮箱。 | | | |
| 异常事件流 | | 1. 若用户设置的阈值不合法，则提示错误信息 ，设置失败 2. 若用户设置的邮箱不合法，则提示错误信息，设置失败 | | | |
| 辅助功能（可选） | | 显示监控结果时，若监控结果出现有异常，则在该条监控信息被标记为其他形式用以提醒维护人员（如在信息前标记报警小图标、字体颜色显示为红色等） | | | |
| 提示信息（可选） | | 1. 若用户设置的阈值不合法，则提示“阈值不合法，请重新输入” 2. 若用户设置的邮箱不合法，则提示“请输入合法邮箱” | | | |
| 业务表单 | | | 数据库中维护报警邮箱表单，包含信息:<key（邮箱）,value（用户信息等）>  数据库中维护阈值表单，包含信息:<key（监控点）,value（阈值）> | | | |

### 领域模型

根据上述的业务需求和用例分析，可以得出系统的领域模型，如图3-5。首先，多个运维人员可以在运维系统上注册多个服务器，服务器列表展现多个服务器，每个服务器可以定义多个监控点，多个监控点对应多个监控阈值。对于警报设置，一个运维人员可以有多个警报邮箱，一个邮箱可以发送多个警报邮件。最后各个领域对象之间的关系构成领域模型。

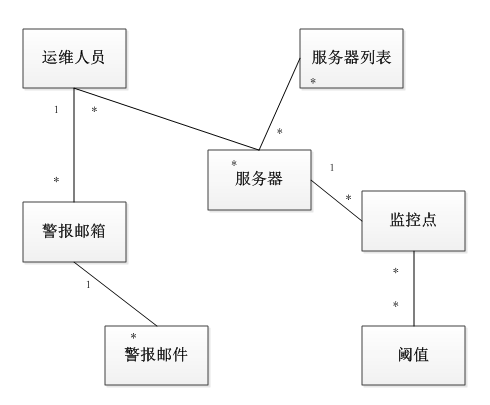


图3‑5 领域模型

## 本章小结