**1018项目三权分立架构文档**

北京京联云软件有限公司

2019年2月

目录

[第1章 需求分析 - 3 -](#_Toc1467865)

[1.1 概述 - 3 -](#_Toc1467866)

[1.2 场景描述 - 3 -](#_Toc1467867)

[第2章 架构设计 - 8 -](#_Toc1467868)

[2.1 系统架构 - 8 -](#_Toc1467869)

[第3章 系统设计 - 10 -](#_Toc1467870)

[3.1 核心业务流程 - 10 -](#_Toc1467871)

[第4章 持续集成 - 11 -](#_Toc1467872)

[4.1 配置管理 - 11 -](#_Toc1467873)

[4.2 部署架构 - 11 -](#_Toc1467874)

1. 需求分析
   1. 概述

从系统安全角度考虑，客户提出对于敏感的，涉及设备命令相关的操作，采用三权分立的操作模式。系统中设置操作员，安全管理员和安全审核员的角色。操作员和MDM的管理员角色类似，能够对系统进行管理操作。对于普通的操作，操作员可以直接完成。对于安全敏感操作，操作员完成操作后，需要安全管理员进行审批，确认后，该操作才能生效。审核员能够看到操作员的敏感操作和安全管理员对其相关的审批动作。

* 1. 场景描述
     1. 操作员登录

操作员，即mdm管理员能够通过mdm登录界面，登录到mdm系统中。

* + 1. 操作员进行敏感操作

敏感操作的范围目前定义为：下发命令，下发策略。

当操作员进行敏感操作后，系统应提示“提交操作成功，等待安全管理员审核”。其他操作流程和原有mdm管理员操作流程一致。

* + 1. 操作员查看安全操作记录列表

操作员提交操作后，应能在”安全操作记录”列表中看到敏感操作记录。

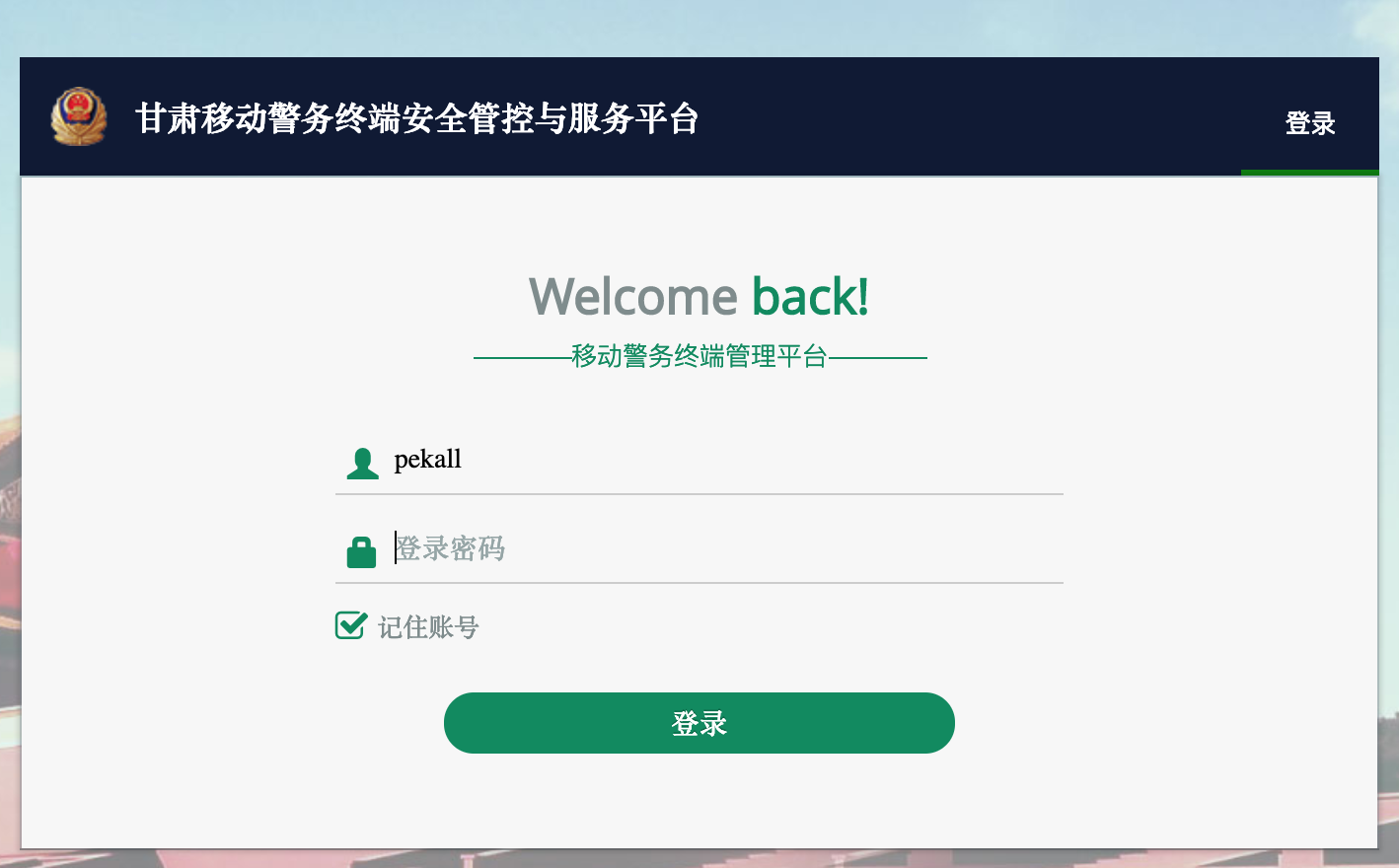


安全操作记录可以在日志管理的“管理员操作日志”上面添加一个子菜单。内容和“管理员操作记录”一样。可将“说明”字段修改成“状态”字段。状态有“待审核”， “审核成功“， “审核拒绝”。操作员可以对状态进行过滤。“安全操作记录”仅仅包括了敏感操作，即下发策略和命令。

* + 1. 操作员查看安全记录审核详情

对于 “审核成功“， “审核拒绝”两类状态的记录，可以在记录项后添加“审核详情”的按钮。点击该按钮，操作员可以看到审核详情。

* + 1. 安管管理员登录



安全管理员能通过单独的web入口登录安全管理界面。登录界面和mdm界面风格和保持一致。文案内容可为“安全管理员入口”。登录后可以看到“安全操作记录”列表。该列表和操作员看到的基本一致。

* + 1. 安全管理员查看安全操作记录列表

安全管理员看到的“安全操作记录”列表和操作员看到的基本一致。可以通过状态过滤操作记录。状态包括（但不限于）“待审核”， “审核通过“， “审核拒绝”。对于待审核的记录项，后面可提供“审核”的按钮。对于已经审核的按钮，后面可提供“审核详情”的按钮。

* + 1. 操作员查看安全记录审核详情

对于 “审核成功“， “审核拒绝”两类状态的记录，可以在记录项后添加“审核详情”的按钮。点击该按钮，操作员可以看到审核详情。

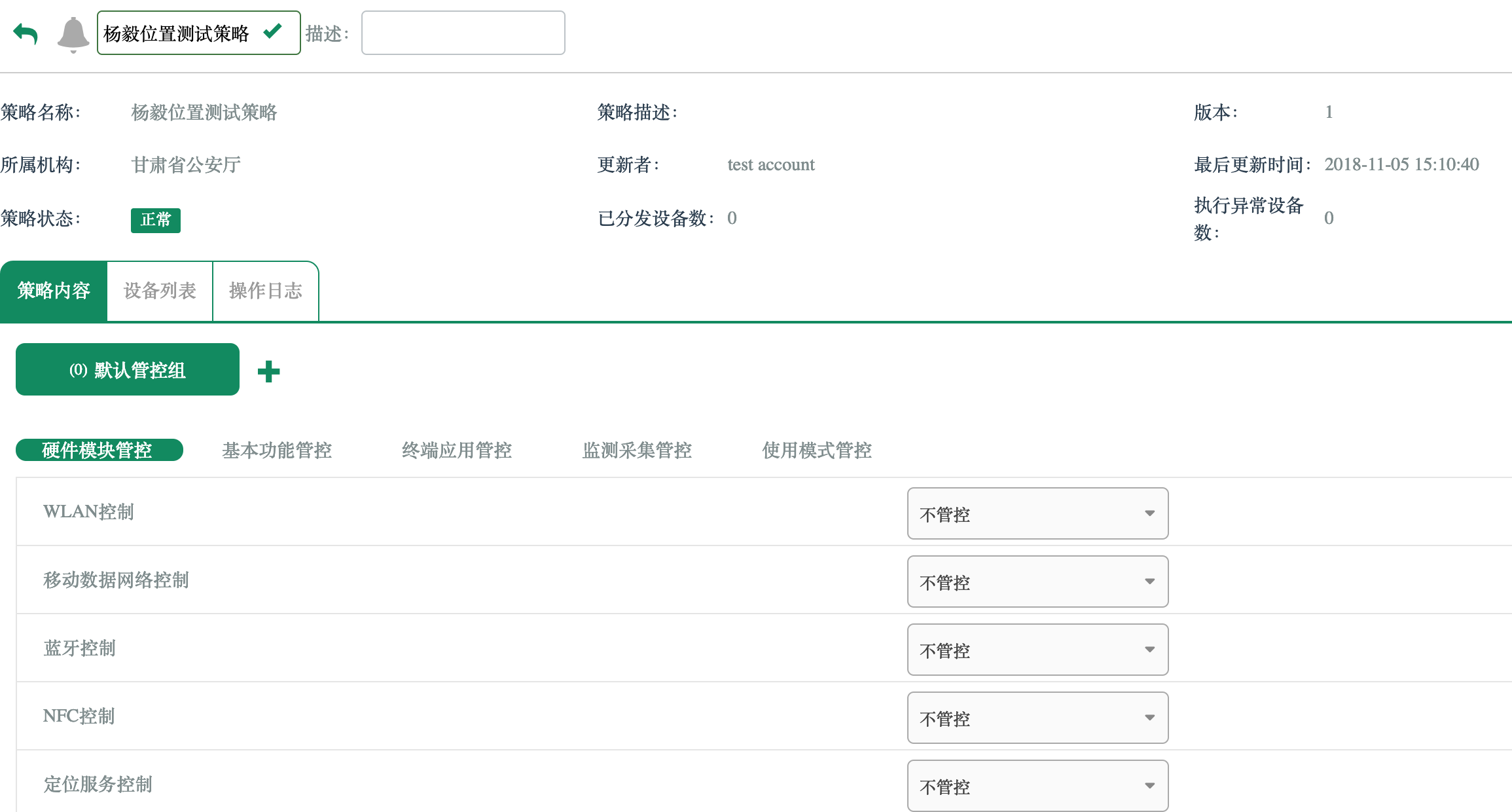
* + 1. 安全管理员审核操作

安全管理员点击“安全操作记录”列表项后的审核按钮后开启审核流程。

审核界面应包括操作员，下发内容，下发目标三个Tab。在操作员tab中，能看到操作员的详细信息。类似用户详情中的所有内容。



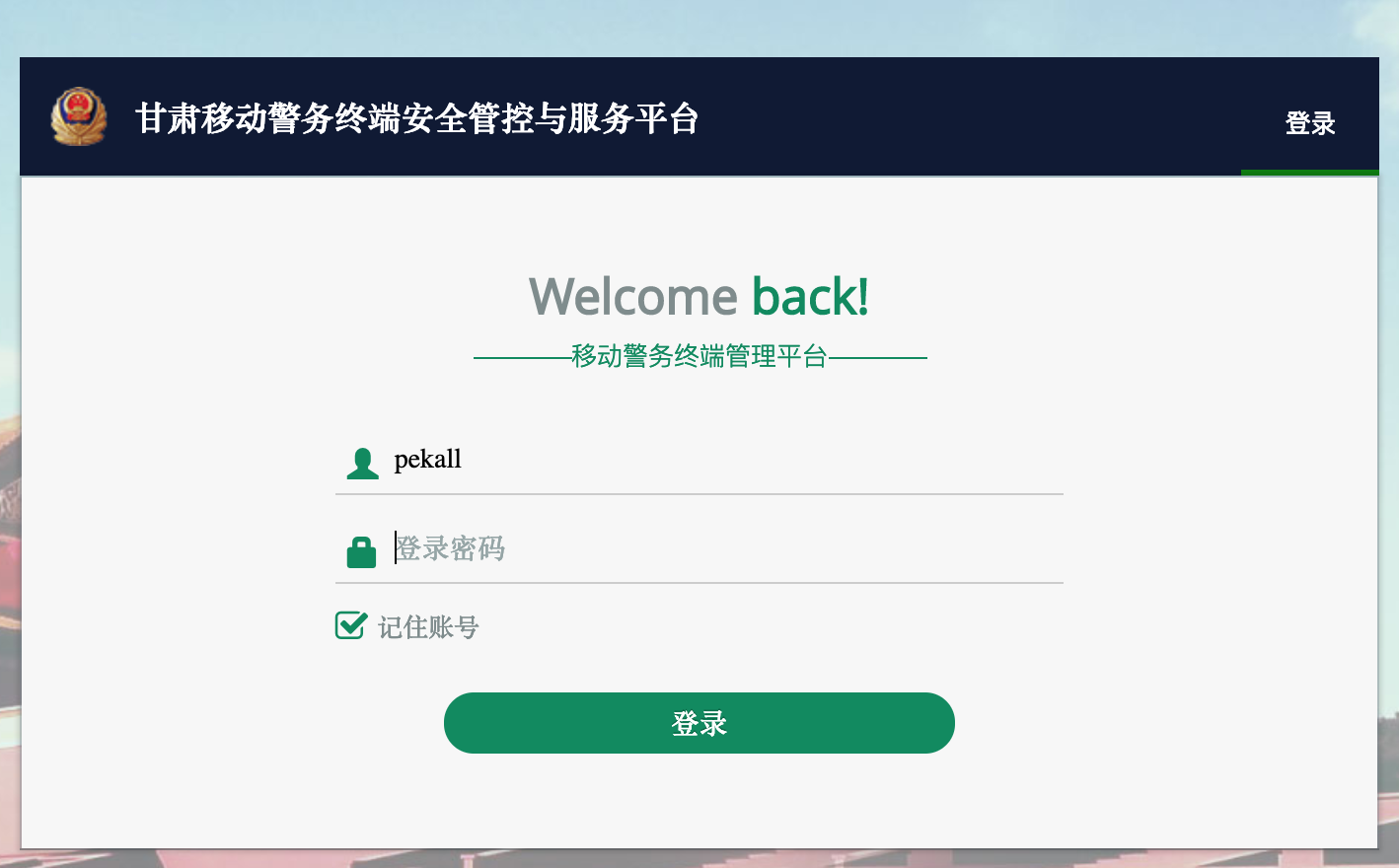
下发内容可以为策略或是命令。策略界面和mdm中策略详情界面内容一致，所有编辑项都变成只读。安全管理员能查看各个策略项的细节。



同时界面上也能看到分发对象(用户，机构，设备)的详细信息。

全审核员可点击批准和拒绝按钮。对于拒绝操作，需要提供说明文字。

* + 1. 安管审核员登录



安全审核员能通过单独的web入口登录安全审核界面。登录界面和mdm界面风格和保持一致。文案内容可为“安全审核员入口”。登录后可以看到“安全操作记录”列表。该列表和安全管理员看到的基本一致。

* + 1. 安全审核员查看安全操作记录列表

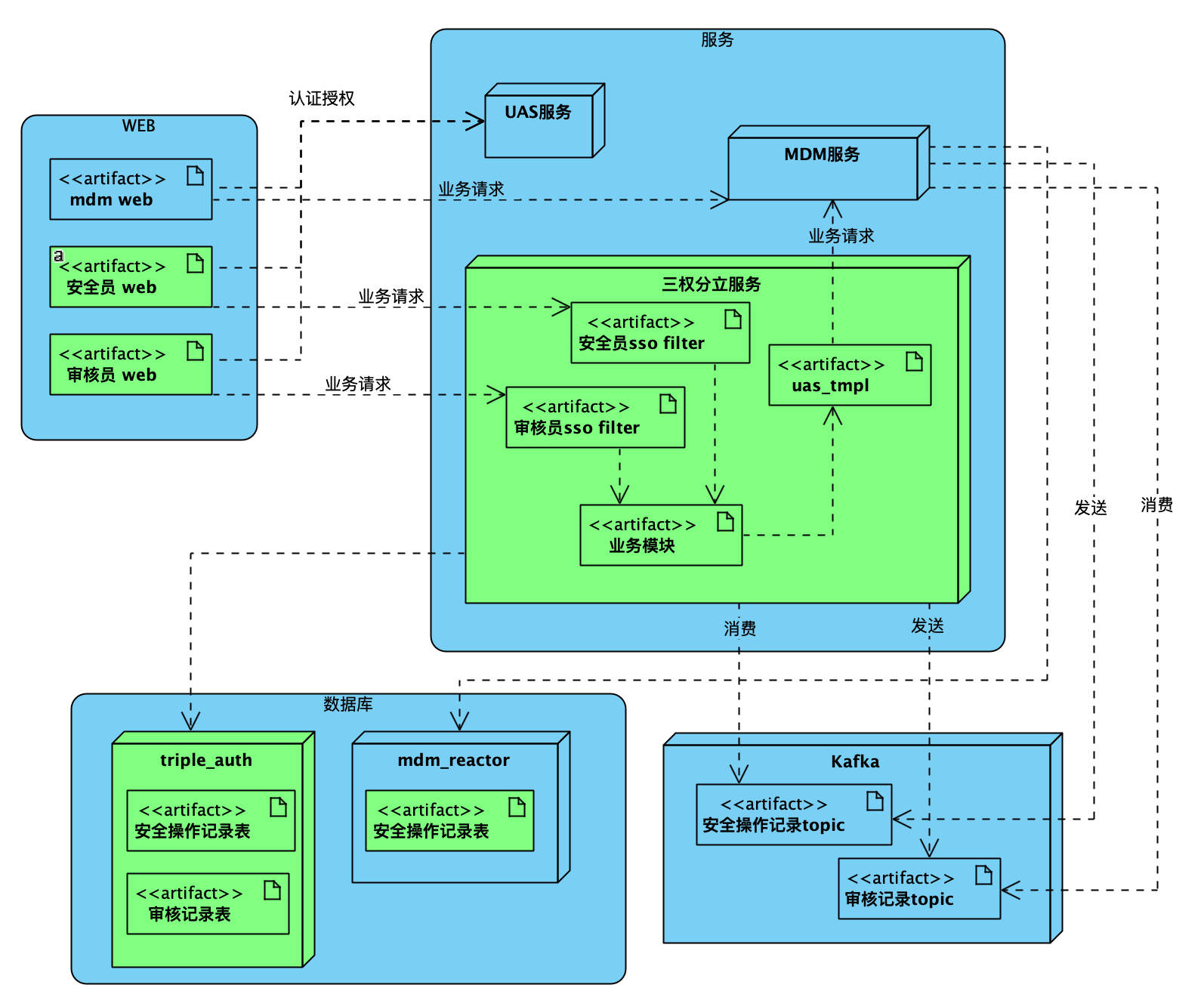
安全管理员看到的“安全操作记录”列表和安全管理员员看到的基本一致。可以通过状态过滤操作记录。状态包括（但不限于）“待审核”， “审核通过“， “审核拒绝”。对于已经审核的按钮，后面可提供“审核详情”的按钮。

* + 1. 安全审核员查看安全记录审核详情

对于 “审核成功“， “审核拒绝”两类状态的记录，可以在记录项后添加“审核详情”的按钮。点击该按钮，安全审核员可以看到审核详情。

1. 架构设计

* 1. 系统架构



* + 1. WEB

Web端分别为操作员，安全员和审核员提供三个独立的入口。操作员即为原有mdm web。

* + 1. 认证授权

安全员和审核员web及服务都需要集成UAS。

* + 1. 三权分立服务

三权分立服务为安全员和审核员web提供restful服务。服务需要和uas集成单点登录。需要确认是否能够集成两个sso filter。服务可通过uas\_template组件调用mdm接口，获取如策略详情等等信息。

* + 1. 数据设计

MDM中创建“安全操作记录表”，记录操作员的安全操作。三权分立服务创建“安全操作记录表”和“审核记录表”。

* + 1. 消息设计

MDM服务发送“安全操作记录消息”， 接收“审核记录消息”。

三权分立服务接收“安全操作记录消息”，发送“审核记录消息”。

1. 系统设计
   1. 核心业务流程
      1. 分发策略

操作员在web端分发策略后，服务端记录安全操作记录到数据库，并发送安全操作kafka消息，即可返回。操作记录的初始状态为待审核。

三权分立服务接收到安全操作kafka消息，将其保存到数据库。操作记录的初始状态为待审核。

安全员在其web审核通过了这条操作记录后，记录审核记录到数据库，并发送审核记录kafka消息。同时更新操作记录状态为已通过。

Mdm收到审核记录kafka消息后，更新安全操作记录为已通过。然后根据安全操作记录发送策略到目标机构。

* + 1. 下发命令

和分发策略流程相同

* + 1. 修改策略

操作员修改策略后，服务端会保存策略到数据库。但是不会自动触发策略的下发。

服务端将下发策略的动作保存成安全操作记录。

后续流程和分发策略流程一致

* + 1. 设备注册

当设备注册时，会自动分发策略。如果这时策略处于待审核状态，就会存在问题。

这里考虑两种设计思路：

不用做任何修改。考虑到这种场景出现不多？

如果设备的策略正好是待审核，设备集成一个默认的只读策略。当策略通过审核后，设备会自动获取到审核后的策略。

1. 持续集成
   1. 配置管理

三权分立功能，在MDM中应能够通过配置项在系统部署时打开或关闭。该配置项为静态配置，部署完毕后，**不能修改**。

* 1. 部署架构

三权分立服务及web应能独立达成一个发布包，能通过脚本一键部署。生产环境上默认和mdm服务部署到一起。