5.1 SP4 Web相关架构方案

# 新增概念

## 机房

机房主要包含媒体资源集合，为平台提供媒体能力；

平台域必须要有一个主机房；

平台域可以没有副机房，也可以有一个或多个副机房；

### 主机房

主机房必须部署相应的业务服务，同时部署媒体资源；

管理业务部署在主机房，主机房不可用时管理业务也就不可用，整个平台域就不可用，所有副机房也就不可用；

### 副机房

副机房只能部署资源，用于做资源的水平扩展；

## 服务发现

动态查询（通过RMQ）所需服务（MQ/MYSQL等）的状态与对外暴露的配置信息；

可以查询同一服务域下其他平台域的服务状态与配置信息；

## RMS（资源管理服务）

提供查询机房、媒体资源能力的接口；

## PMS（平台监控服务）

用于监控机房、平台域的状态；

### PMS中平台域状态的业务含义

平台域不可用时，其下管理业务及机房都不可用；

主机房不可用时，整个平台域都不可用，副机房也不可用；

### 监控

监控平台域的状态；

### 查询

查询当前平台域的状态，以及托管到当前平台域的平台域列表（由当前平台域为这些平台域提供备份服务），接口提供方式为RMQ；

PMS还是需要提供查询平台域状态的接口：根据平台域Moid，查询该平台域及其备份平台域的状态；

### 广播

PMS监控到平台域状态发生变化后，会通过RMQ广播给相关平台域中各业务；

# 关联关系

## 机房备份

1. 机房可以配置另外一个机房为它的备份机房；后续版本一个机房可以配置多个备份机房，存在优先级；
2. 同一个平台域中，可以设置副机房作为主机房的备份机房，也可以设置主机房作为副机房的备份机房，副机房与副机房之间也能设置备份关系；
3. 不同平台域间，只能设置其中的主机房作为另一个平台域中主机房的备份；
4. 同一个平台域中所有机房的所有备份机房，只能归属于本平台域及另外一个平台域，不可以归属于第三个平台域；
5. 允许一个机房同时成为多个机房的备份机房；
6. 备份机房与原机房必须在同一个服务域中；

## 平台域备份

1. 平台域间存在备份关系，其备份关系由机房的备份关系映射而来，界面上不提供平台域间备份关系的配置功能；
2. 平台域间只允许存在一主一备；
3. 平台域的会管数据会同步到备份平台域中；

## 用户域绑定机房

1. 用户域可以绑定到所属平台域中的某个机房，绑定后该用户域将使用指定机房的媒体资源；
2. 用户域绑定的机房不可用，则使用这个机房的备份机房资源；
3. 若用户域未绑定机房，则系统默认该用户域使用其所属平台域中主机房的资源；

# 灾备

## 灾备关系

1. 机房的备份关系在BMC中设置；
2. 当前版本机房只支持一主一备；
3. 底层设计中机房的备份关系为一主多备结构，多个备份机房间有优先级设置；
4. 平台域的备份关系由机房的备份关系计算出来，BMC中不提供设置平台域的备份平台域功能；
5. 平台域只能有一个备份平台域（底层设计亦是如此）；
6. 在设置机房的备份机房时，需要限制平台域只能有一个备份平台域；

## 灾备模式

灾备模式只影响机房资源的使用，不影响CMC的使用；

### 模式设置

1. 可以对机房进行灾备模式（自动、手动-使用备机房、手动-不使用备机房、关闭）的设置；
2. 无需提供同时选择多个机房，同时设置他们的备份模式的快捷操作；

### 自动模式

1. 自动模式下，当机房为不可用状态时，用户会自动切换使用备份机房的资源；
2. 自动模式下，原机房恢复，会自动切换使用原机房的资源；
3. 自动模式下，机房切换时，正在召开的会议不结会；

### 手动模式-使用备机房

1. 设置后，正在该机房召开的会议自动结会，在备机房恢复会议；终端迁移到备机房；同时主机房的资源不可使用；
2. 如果该机房为平台域的主机房，PMS会将该平台域设置为不可用状态，同时通知各业务；

### 手动模式-不使用备机房

1. 设置后，正在备机房召开的会议不结会，等会议结束后迁回；终端迁回到主机房；
2. 如果该机房为平台域的主机房，PMS会将该平台域设置为可用状态，同时通知各业务；

### 关闭灾备

1. 关闭灾备模式，只能在本机房及平台域提供服务；
2. 关闭灾备模式时，若之前该机房已设置备份机房，需要删除；
3. 由此产生的平台域间备份关系一并删除，同时删除备份平台域中相应的备份CMC数据库；

# 会管数据同步

## 数据同步方案

### 数据同步机制

1. 基础组件基于数据库间的binlog同步方案来进行数据同步，会管数据需要为不同平台域进行分库；
2. 因为分库，会管业务在处理多个平台域的数据时，需要连接不同的数据源，并进行相应的事务管理；
3. 数据同步采用半同步机制：强一致性写加30秒超时。

### 数据库读写

1. 业务读写数据库，直接连接Mysql；若平台域状态为不可用（或处于数据同步状态时），由底层组件确保Mysql数据库不能进行读写操作；
2. 业务读写数据时，永远连接当前平台域的Mysql数据库；

### 数据恢复

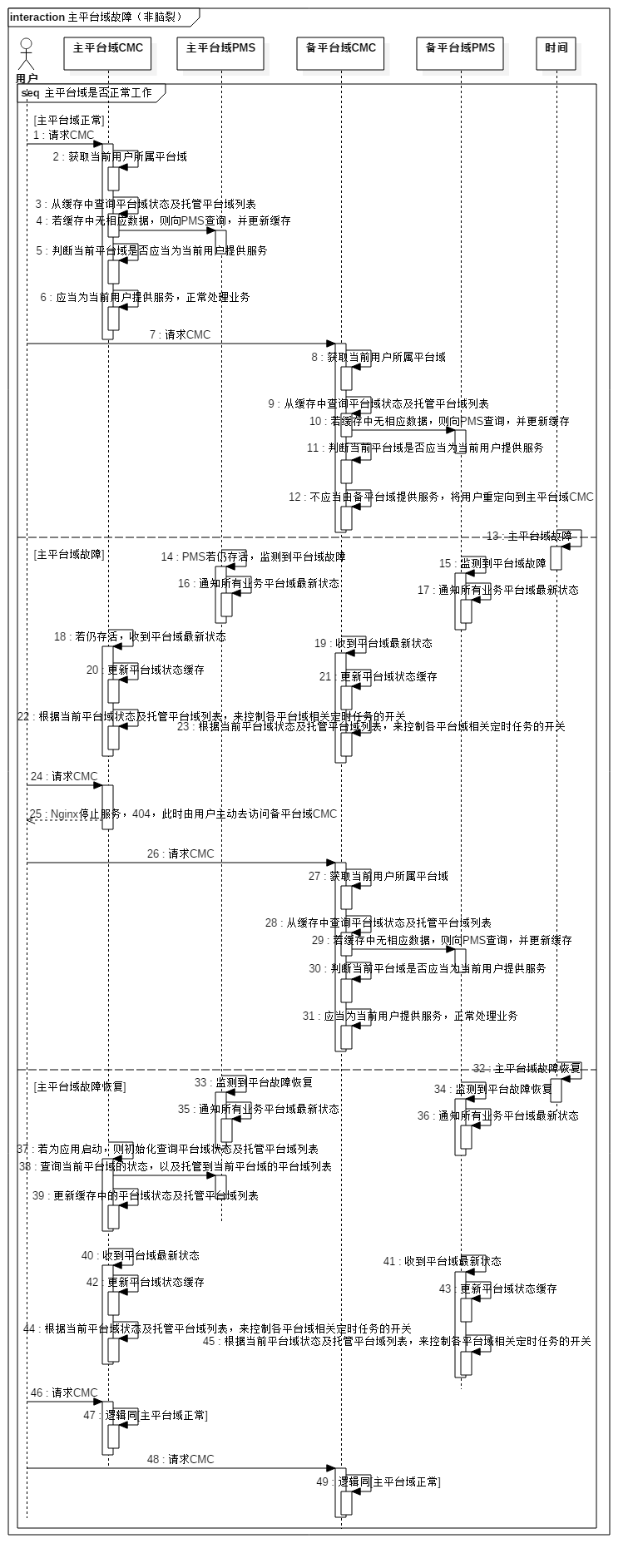
1. 主平台域故障恢复后，必须要先将备平台域的数据同步回主平台域，然后Mysql才能正常读写数据；
2. 若主备平台域间的数据不一致，无法同步，则使用其中一个平台域的数据为主进行覆盖；具体选择哪个平台域的数据为主由基础组件组决定，Web业务不关心；
3. 数据恢复完成后，PMS通知各业务最新的平台域状态；

## 会管业务平台域切换逻辑

### 平台域故障

平台域状态不可用时，Nginx停止web业务相关的请求转发，Mysql不能进行读写操作，业务不会写RabbitMQ数据；

### 平台域故障恢复



### 脑裂

1. 平台域PMS不能有效监测到发生脑裂，只能感知连不上其他平台域；
2. 脑裂后，平台域管理业务要求能正常服务；
3. 脑裂恢复后，要求以其中一个平台域的数据为准进行覆盖；
4. CMC业务不去管是否发生脑裂，正常处理业务逻辑即可，发生数据问题不予理会，必要时进行报错；

## 会管业务处理方案

### 业务http请求（含api请求）

1. 当平台域不可用时，nginx会拒绝掉所有的http请求；
2. 平台域可用时，会校验用户所属平台域是否与当前平台域匹配（此时用户访问的是主平台域CMC），或者用户所属平台域是否在当前平台域的托管平台域列表中（此时用户访问的是正确的备份平台域CMC），校验通过正常提供服务，校验不通过则向PMS查询用户主备平台域状态，根据状态将用户重定向到正确的平台域CMC首页；
3. 终端在主平台域不可用时，会被踢，然后重新登录备APS，得到备平台域CMC地址，接下来访问的是请求备平台域的CMC API；
4. 主平台域恢复后，如果终端还在会议中（在备平台域上），终端不会被踢出，此时终端调用的还是备平台域的CMC API，可能会报错；
   1. 波及：终端访问CMC API报错，是否有可能会导致终端崩溃，需要告知各终端负责人，进行波及分析；

### 定时任务

1. CMC业务启动时就去PMS获取当前平台域状态及托管平台域列表；
2. 若当前平台域为不可用状态，全局定时任务开关为关闭状态，此时定时任务照常触发，只是在执行时其执行范围（平台域）为空，不进行任何实际操作（空转）；
3. 若当前平台域为可用状态，全局定时任务开关为开启状态，CMC定时任务需要执行任务的范围，是当前平台域以及托管平台域列表；
4. 定时任务执行时，全局定时任务开关为开启时则运行实际业务；每次执行任务时，为执行范围内的每个平台域启动一个线程来完成相应的定时任务业务；
5. 定时任务相关的数据库表（quartz表）不进行同步，也就是说这一块要单独一个库；

### 与其他业务（如CSS）间交互逻辑

1. 平台域不可用时，与其他业务的交互被屏蔽
   1. nginx会拒绝掉所有的http请求，包括api请求，此时不会通过http向任何其他业务提供服务；
   2. 基于rabbitmq的业务交互，在平台域不可用时，不再进行rabbitmq写操作，故CSS不会再有rabbitmq的交互产生；
2. 平台域不可用时，java应用内交互不会触发
   1. tomcat内各业务间的cxf请求能被继续调用，但由于没有人为触发，也没有定时任务触发，此类cxf请求也没有任何来源，故不会有实际调用；
   2. 即使有个别遗漏请求被触发，由于数据库不能读写，底层不会执行任何有效的业务逻辑，可能后台会有数据库读写报错；
3. 平台域可用时，与CSS的交互消息中，消息体都需要带上用户域信息，这样CMC在处理这类交互消息时，就能知道要操作哪个平台域的数据库；

## 技术方案：动态切换数据源

1. 动态生成数据源配置
   1. tomcat数据源配置中，只配置当前平台域的数据源；
   2. tomcat数据源配置由部署工具写入配置文件；
   3. 在BMC中配置机房间的备份关系时，会关联产生平台域的备份关系；在基础组件创建完备份数据库，并同步完数据后，需要通知CMC，CMC需要依此动态创建托管平台域对应数据库的数据源（Spring Bean）；这个通知由哪个模块发出，目前还没有明确。
   4. 在BMC中删除机房间的备份关系，关联删除了平台域间备份关系时，会同步删除原备份平台域中托管平台域的数据库；删除数据库前通知CMC，CMC需要动态删除对应数据库的数据源；
   5. 应用启动时，读取平台域间的备份关系，动态创建数据源；
      1. Service需要提供平台域查询接口：根据平台域moid获取设置该平台域为备份的所有平台域列表；
2. 动态切换数据源
   1. 在每个用户请求线程中，或定时任务实际执行线程中，根据当前用户信息（所属平台域）来动态切换数据源；
   2. 事务管理中配置成动态数据源方式；

# 单点登录

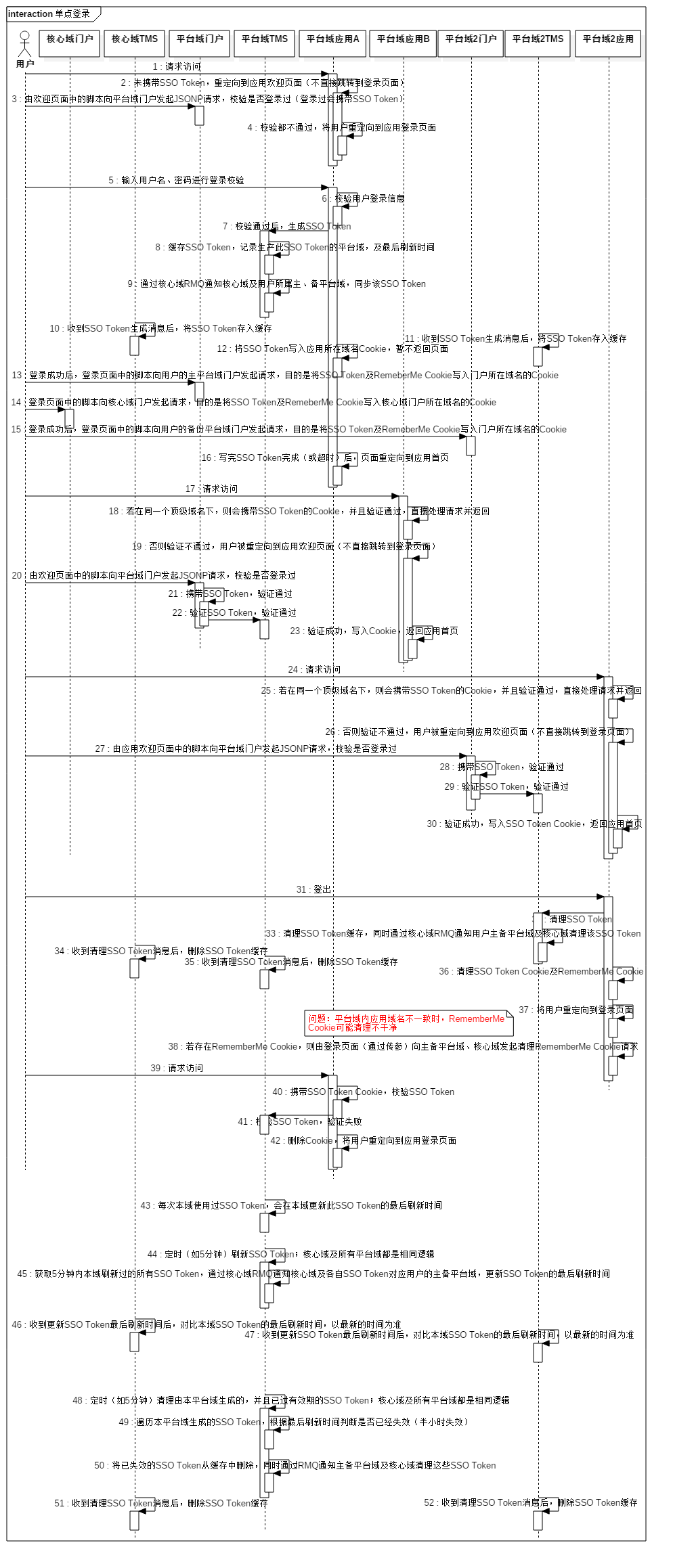
已确定：5.1 sp4版本无需实现跨域的单点登录功能，保持现状（跨域时需要再次登录）

## 单点登录目标

1. 需要支持平台域与核心域间的单点登录，跨平台域的单点登录；
2. 即使在同一个平台域间的应用，都可能不在同一个顶级域名下，甚至是使用IP地址；需要支持这种场景下的单点登录；
3. 单点登出；

## 实现方案

1. 在生成SSO Token后，通过核心域rabbitmq同步到核心域与用户所属的平台域及其备份平台域；
2. 登出时，通过核心域rabbitmq同步删除核心域与用户所属的平台域及其备份平台域的SSO Token；
3. 用户登录成功后，浏览器主动向核心域及主、备平台域门户写SSO Token的Cookie，若勾选了“记住我”，则同时也将RemeberMe的Cookie写到核心域、主、备平台域域名中；
4. SSO Token有效期不能太长，30分钟；
5. 若SSO Token失效，且Cookie中有RemeberMe信息，则通过RemeberMeCookie信息再换取一个新的SSO Token，新SSO Token也需要通过rabbitmq进行同步；
6. SSO Token最后刷新时间，定时将最后刷新时间（如果有变化）进行同步；



## 兼容历史版本

1. Web应用不存在版本兼容问题；
2. 其他系统（服务器）对于Web应用API的调用，需要同步修改为调用新版本的API，其登录流程（换Account Token、SSO Token）与老的流程出入不大，有变化会更新文档要求改变调用方式；
3. 终端对于的API的调用，需要保持以前的登录流程（换Account Token、SSO Token）不变；

# RMS

输入用户域Moid；

输出当前平台域的机房列表，机房内CMU列表，机房灾备策略，机房状态；

# 其他问题与方案

## CMC跨平台域会议邀请

由于CMC中存在邀请其他平台域用户入会（预约会议）的需求，故存在往其他平台域写入会议信息的需求。

### 需求

1. 是否存在跨服务域（或上下级服务域）的会议邀请需求场景？
   1. 暂时没有；
   2. 如果存在，可以按照第三方帐号进行处理（记录终端号码，不在对方CMC中写入会议数据）；
2. 跨平台域的会议邀请，对方只能看到会议列表，不能进行会议操作（会控操作），是否可行？
   1. 可以；

### 方案

1. 跨平台域API调用时的身份认证

方案一：通过密钥的方式进行签名，在服务器端解密签名，校验是否合法；

方案二：通过JWT验证，每个JWT中带有效期

跨平台域的API调用，为了防止重播攻击，Token有效期必须很短（3~5秒）；因此，方案依赖于各个域间的时间是完全同步的；——已确认平台域是与核心域NTP进行时间同步；

1. 如何获取各平台域的CMC地址

方案：由服务发现将各平台域CMC地址写入Redis；会管调用时通过平台域Moid去Redis获取该平台域的CMC地址；（服务发现中有全网的服务信息）

1. 平台域不正常时，如何去备份平台域请求
   1. 根据平台域Moid去PMS获取主备平台域列表，及其状态；
   2. 调用API时去请求状态可用的平台域CMC API；都不可用时，报错；

## JD2000 JMS（SP3开始）

JMS是兼具BMC、AMC、门户以及简单部署功能（通过嵌入部署工具极简界面，或调用部署工具API实现）的一个Web应用；

实现方案是JMS依赖BMC、AMC、门户的jar包，底层设计保持不变，根据需求来新增接口与界面；

## 虚拟会议室

1. 所有的会议请求都会从CMC走；
2. CMC会对会议资源权限进行逻辑控制，但不控制具体的媒体资源；
3. 由CMC统一分配E164号；

## 数据迁移

详细设计时对数据迁移工作进行细化；

## 通过临时方案绕开身份认证的API请求

问题：网管、VRS等应用调用API时，没有走任何身份认证流程，调用的是CXF用户登录接口；

这个属于同平台域应用间的接口调用，理论上使用CXF接口调用是合理的，问题在于CXF接口是针对Java应用内部的接口，底层结构稍有变化，会波及到调用方；

结论：暂时保持现状；