# 系统架构要求



图3-1智能网NFV化网络架构图

SCP-开通计费层作为图中的虚拟化网元（VNF），部署在虚拟化平台（Hypervisor）之上，不依赖于硬件类型，由一个或者若干个虚机（VM）组成，共同提供网元功能。

# 功能和接口总体要求

## SCP-开通计费层功能要求

### SCP-开通模块功能

SCP-开通模块功能支持MML指令和SOAP指令，实现BOSS系统与业务系统之间开销户指令的翻译和分发，开通模块需提供数据一致性保证方案。开通模块在业务办理的时候，如果存在多个站点，需要保证各个站点的数据一致性。开通模块需要提供数据一致性稽查和改正的手段或工具，支持手工或定时自动比对各个站点的数据一致性。

### SCP-计费模块功能

SCP-计费模块是SCP-应用逻辑层以及其他业务系统和计费中心之间传输话单文件的通道。在传输的过程中，SCP-计费模块能对文件进行拆分、过滤、压缩等操作。

具体功能如下：

(1) 进程检测：检测计费模块网元是否已处于运行状态，若是则不会再次启动；

(2) 检测空间：检查磁盘剩余空间，若磁盘剩余空间小于下限（ 如150MB）则

告警并中断采集过程，待正常后系统自动恢复运行；

(3) 话单采集：每天定时从 SCP-应用逻辑层以及其他业务系统获取话单文件到计费模块网元的本地目录；

(4) 话单验证：在采集、发送话单过程中将进行话单文件的校验，保证文件传输的完整性；

(5) 话单的合并：将某个目录下的多个话单进行合并处理，减小话单的个数；

(6) 话单备份：可设置各种备份文件的存放目录和保留权限，包括对采集文件的备份、对话单拆分后的文件的备份、对被外部实体取走文件的备份、对发送文件的备份；

(7) 话单清除：每天凌晨 5：00 检查计费模块网元上的备份目录，将指定的保留期限之前生成的备份文件删除；

(8) 文件传输：从外部实体采集文件到本地，从本地发送文件到外部实体；

(9) 文件编号：在发送文件中，系统可以对发送的文件进行编号；

(10) 日志记录：系统运行中的信息、话单采集和话单传输信息需记录在日志文件中；

(11) 日志备份：当日志文件很大时备份到另一目录。

(12) 告警上报：计费中心的连接状态，如发生断连，上报告警到网管并发起自动重连。

## 接口要求



图4-1 开通计费层接口

表4-1 涉及接口

|  |  |  |  |
| --- | --- | --- | --- |
| **接口名** | **连接网元** | **承载协议** | **接口功能** |
| 开通接口 | 虚拟网业务服务器/家庭亲情网业务服务器-开通计费层网元（开通） | SOAP/MML | 实现家庭亲情网用户数据写入/虚拟网业务的开通 |
| 计费接口 | 虚拟网业务服务器-开通计费层网元(离线计费) | FTP | 实现虚拟网业务用户业务的离线计费功能 |
| 网管接口 | 家庭亲情网业务服务器/虚拟网业务服务器-网管系统 | SNMP | 实现家庭亲情网服务器/虚拟网业务服务器设备的管理和监控 |

所有IP协议接口可以支持IPv4/IPv6双栈。

（1）SOAP/MML协议处理功能要求

应用逻辑层业务服务器应支持SOAP/MML协议处理功能。

（2）FTP协议处理功能要求

应用逻辑层业务服务器应支持FTP/SFTP协议处理功能。

（3）SNMP协议处理功能要求

应用逻辑层业务服务器应支持SNMP协议处理功能。

# 网管要求

需提供EMS网管系统，实现对应用逻辑层业务服务器的管理，网管需具备如下功能：

（1）集中的故障管理

提供告警的接收、同步、过滤、恢复、清除、定位、重复告警抑制等功能，帮助管理员从多个维度了解整个网络中告警的分布情况，并根据告警的详细信息进行故障处理。

（2）综合的性能管理

管理员通过性能监视能及时全面了解网元的各项性能指标和趋势走向，为整个运营网络的优化和维护提供依据。

（3）完善的安全管理

提供认证、鉴权、用户管理、角色管理等功能，保证用户帐号的安全性和系统运行的安全性。

网管需满足集团EMS相关系列规范，同时考虑到现网上级NMS网管系统能力，新建网管系统需适配上级网管系统接口（SNMP/FTP/SFTP）要求、相关指标要求。

## 告警管理部分

* 提供丰富的告警管理能力，支持多种网元和设备的告警实时接收和展示，以及历史告警查看。
* 提供丰富的告警提示能力，通过界面上的提示和远程通知的方式提醒管理员告警信息。
* 提供屏蔽指定告警的能力
* 提供告警内容的搜索过滤能力，能够快速定位查询到具体的告警。
* 提供告警的信息维护管理能力，能够在日常维护中及时总结告警维护经验，为后续的维护提供更丰富和精确的维护方案。
* 对告警震泛滥的基本抑制能力，减少无效告警数量，支持告警相关性的配置与展示，能够进一步的分析与配置实现告警更加有效的分析与上报
* 提供告警的远程通知能力，可以对重要的告警发送短信或者email通知
* 提供告警基本信息统计能力，支持管理员在对所有的告警信息进行汇总分析，找出整体中可能存在的问题，提高管理效率。

提供告警合并能力，支持管理员指定网元类型之间的相关告警进行合并处理，较少界面上直接展示的告警数量，进一步提高告警有效性。

当前告警页面中的一条故障告警被确认而且被清除后，系统会自动将这条告警移入历史告警表中，历史告警管理主要提供了对这些历史告警的查询、导出和过滤功能。

通过设置告警远程通知规则，管理员不在机房也能够实时了解当前有哪些紧急告警需要处理。

管理员在创建远程通知规则后，系统会自动启动该规则匹配新产生的告警，系统将匹配成功的告警中指定内容将以短信、Email方式通知对的通知组用户(短信中心或者邮件服务器由管理员提供) ，从而提高告警处理的响应速度。

管理员可以按告警级别或具体告警、告警风暴远程通知三种方式创建告警远程通知规则，同时支持远程通知风暴抑制：

* 按告警级别转发

管理员如果按照告警级别创建远程通知规则，那么一旦选中了转发某个级别的告警，那么被EMS管理的所有网元的该级别告警都会被转发，无须再选择具体的告警源。

* 按具体告警/事件转发

管理员如果按具体告警创建远程通知规则，需要指定该规则匹配的告警源及具体告警，因此该规则仅对指定告警源的具体告警生效。

* 告警风暴远程通知

管理员如果需要远程了解整个系统或者某个网元上告警过多的异常时，可以设置告警风暴远程通知

告警风暴远程通知是对单个网元或者整个系统单位时间内的告警数量进行统计，单位时间内产生的告警数量超过了配置值的情况下，EMS会汇总发送一条远程通知，提醒管理员系统可能出现了不正常的情况，需要尽快处理。

* 远程通知风暴抑制

系统支持针对每个周期内每个用户的发送远程通知数量进行配置，当系统发现超出配置值时对远程通知进行抑制。并在每个周期之后发送一条抑制情况的汇总的通知给用户。

这样在系统中由于告警产生的通知过多的情况下，不会过多的向管理员的手机、邮箱发送通知，减少管理员手机、邮箱的压力，同时会对抑制的通知数量进行统计，统计信息也会通过远程通知发送给管理员，减少了系统抑制通知造成的风险。

告警同步：当网元新接入、或因为网络异常，网管未运行等情况，为保证网管侧的活动告警与网元侧的活动告警内容一致，EMS需自动从网元侧重新获取告警数据。

日常运维中，对于网元产生的告警数量进行统计，以分析网络质量瓶颈以及事故多发点。EMS需支持用户选择多个条件：如告警源、告警名称、告警级别、告警类型、确认状态、清除状态、清除时间、告警首次发生时间；同时支持按日或按小时统计，比如按照每天，来统计网元的告警数量。统计结果可以表格的方式显示。

* 告警汇聚

告警上报时有些告警之间是有关联的，这时候需要支持用户根据告警之间的关系进行告警相关性的配置。

OMC将多个告警汇聚在一起生成新告警，或者经由一个根源告警产生其它衍生告警的场景。这样多个告警在逻辑上是一个整体，界面上直接显示的只有最终汇聚的新告警或者根源告警，从而在界面上减少了告警数量，同时支持整个相关告警一次性的确认、清除操作，降低的用户的工作量。

* 告警振荡抑制

告警短时间内反复上报和清除的场景称作告警振荡，对于这样的场景一般情况下是不需要反复提示用户产生了告警，需要对振荡中的告警进行抑制。

EMS支持用户对系统整体或者某个告警配置告警振荡的阈值条件，在阈值条件达到之后的告警将不再继续上报，只到振荡抑制的阈值条件不再满足后才继续上报。

阈值条件包括两个参数：告警数量（告警上报与清除告警各算一次）和振荡周期。

* 告警级别提升

当前系统对一段时间内反复上报的个告警进行了抑制，但是同时需要考虑反复上报可能说明故障更加紧急的场景。

EMS支持在界面上指定具体的告警设置级别提升规则，支持系统在一段时间内连续上报的数量超过一个阈值后将当前告警级别提升一级。

* 告警屏蔽

日常操作维护人员希望屏蔽不关心或者不重要的告警，或者当被管理业务系统升级、割接时希望屏蔽一些已知的告警，基于这样的使用场景EMS提供了告警屏蔽功能。

OMC需支持通过界面设置告警屏蔽规则。当网元上报符合屏蔽规则的告警时，网管将这些告警转移到屏蔽告警表中，不显示到当前/历史告警浏览界面，也不会上报上级网管。EMS提供屏蔽告警查看页面。

用户可以设置告警屏蔽规则。告警屏蔽规则是如下字段的灵活组合：告警源、告警名称、生效开始时间、生效结束时间。

* 告警级别提升

日常运行期间有的网元可能在短时间内反复上报同一个告警，这种场景下对于有的服务可能属于一种异常的状态，需要将告警的级别进行提升，达到让用户尽快处理的目的。

这时候用户可以针对这个告警设置具体的级别提升规则，规则包含两个主要参数，检测周期和发生次数。指的是在一个检测周期内发生次数达到设定的发生次数阈值则当前告警中该告警的级别会提升一级，如果下个检测周期仍然超过阈值则告警级别继续提升，直到达到最高级别。

## 性能管理部分

性能管理为网络管理、维护人员提供一种监视手段，检查和监视过去一段时间内网络或者业务的运行情况，帮助用户了解网络运行的性能趋势、对网络进行性能优化，保证网络的正常运行。

* 性能准实时监控

日常运维过程中，用户经常需要对一些重要的网元的重要性能指标进行准实时监控，比如业务请求成功率，消息延迟等。而通过图形化的展示方式，用户可以直观地观察到性能指标的动态变化，进行相关的网络质量和容量的评估。

OMC将性能指标的变化趋势以图形显示出来。支持曲线图展示性能数据曲线。在图中，不同的指标用不同颜色的折线显示。

OMC支持数据按表格方式呈现，用户可以设置按曲线还是表格展示方式。

用户可以在OMC中添加性能监视视图，用户在登陆OMC后就可以立即看到用户关心的关键性能指标的趋势图。

* 历史性能数据展示

通过图形化的展示方式，用户可以直观地观察到一段时间范围内性能指标的动态变化。

另外用户还可以在界面上对时间段进行微调，系统会实时展现用户选定时间内的性能数据，默认情况下，在查询界面显示的点超过720点情况下，性能数据查询结果按原始数据(最大值)结果展示，同时也支持查询结果以最小值，平均值，求和展示。

用户可以选择展示方式为曲线或者表格方式。

OMC支持将查询到的性能数据导出到本地文件中。

* 性能阈值告警

当业务负荷较大并导致性能指标的值超过设定的阈值时，OMC产生相应的性能阈值告警，用户可以及时发现关键性能指标的异常情况，从而及时采取措施，避免异常情况恶化。

用户可以对关键的性能指标设置性能阈值告警产生条件。

用户设置的指标阈值告警产生条件，会作用到每个网元上，当某个网元的指标达到阈值条件后，进行针对某个网元的具体告警。

* 性能数据采集

用户在创建或修改任务时，要指定被采集的资源对象与采集周期(1，5、15、30、60分钟)，将周期性发送请求给网元，网元收到请求后将上报请求的性能采集任务的性能指标结果给OMC。

用户可以增加、删除、暂停或者启动定时性能采集任务。

用户可以手工创建汇聚任务，并自定义指标，这类指标支持对多个设备上的相同指标进行汇聚计算出新的指标，汇聚计算支持算法包括：加减乘除，求和，平均。

* 性能数据齐全性保障

如果某一时刻的性能数据，因为网络异常、网管未运行等情况，而没有采集到。系统会自动从网元侧重新获取原始的性能数据，以补齐之前空缺的数据。

要支持性能数据补齐能力，网元侧需要支持缓存性能历史数据。

## 系统管理维护

* 支持扩缩容

支持在线对计算节点和存储服务器的规模进行扩缩容，而不影响现有节点服务。

* 升级和安全回退

业务层需支持在当前版本的基础上进行版本（补丁）在线升级，保证业务无损。版本升级过程需支持分批进行，且在混合使用新、旧版本的暂存状态下，业务层需支持正常上线运营。

升级失败时支持回退。

* 系统管理可靠性要求

节点需要具备冗余能力，同时保证系统不能出现脑裂问题。

## 安全合规要求

依据工信部《省级基础电信企业网络与信息安全工作考核要点与评分标准》，要求本期网络建设及运维需落实网络与信息安全“三同步”工作，即在本工程项目中对安全配套或安全合规进行同步规划、同步建设、同步维护。

* 设备安全配置要求

随着各类通信和IT设备采用通用操作系统、数据库，及各类设备间越来越多的使用IP协议进行通信，其网络安全问题日渐凸出，为了维持通信网、业务系统和支撑系统设备安全，工程中要贯彻中国移动网络部颁布的《中国移动设备通用安全功能和配置规范》等系列规范要求，在设备选型、入网测试、工程验收和运行维护等环节，设备全生命周期各个阶段均需落实安全功能和配置要求。本工程需满足规范中安全功能要求以及必须采用的配置要求。

* 安全防护要求

本期工程要贯彻中国移动网络部下发的“安全防护手段集中配置以及安全服务要求”，根据需要配置或接入防火墙、流量清洗、入侵检测和防御、防病毒、系统漏洞扫描、Web漏洞扫描、网站防攻击、僵木蠕监测、安全管控平台等防护设备和系统，同时，安全服务能力需根据最新要求进行提升。