一种 VNFM 分域方案的研究、测试与应用

沈 强[1] 刘 绚[1] 李碧涵[1] 曹星凯[1] 杨东锋[1]
SHEN Qiang LIU Xuan LI Bihan CAO Xingkai YANG Dongfeng

摘 要 当前虚拟化和云化技术已在 5G 移动通信核心网领域得到了广泛应用，VNFM 是虚拟化技术必不可少的组件，随着 VNFM 上管理的 VNF 越来越多，管理难度和安全性问题日渐凸显。提出了一种分域方案，描述了其设计实现过程和测试场景，并在现网中得到了实践应用，能帮助运营商解决 VNFM 上 VNF 运维问题。

关键词 5GC；VNFM；RBAC；分域；测试

doi：10.3969/j.issn.1672-9528.2024.01.028

0 引言

网络功能虚拟化（network function virtualization，NFV）是一种实现软硬件解耦的技术[1]，新建的 5G 核心网（5G core network，5GC）网元几乎全部是通过 VNF 管理器（virtual network function Management，VNFM）部署的虚拟化网元（virtual network function，VNF）。

国内运营商已经过若干期 5GC 网络建设，5GC VNF 数量越来越多，单个 VNFM 上管理的 VNF 可能达到数百个，虚拟机（virtual machine，VM）数量更是数以万计。且 5GC VNF 在通信组网中属于核心枢纽位置，一旦操作不当或者误操作导致了异常将会影响数百万用户甚至会使整个网络瘫痪，后果很严重。因此，运营商对 VNFM 的登录访问、权限管理、资源管控等操作的安全性方面提出了更高的诉求。

1 VNFM 简介

在 ETSI 标准制定的 NFV 架构体系中，NFV 编排器（network function virtualization orchestration，NFVO）、VNF 管理器（virtual network function management，VNFM）和虚拟化基础设施管理器（virtual infrastructure management，VIM）共同构成了 MANO（management and orchestration，MANO）系统，如图 1 所示[2]。

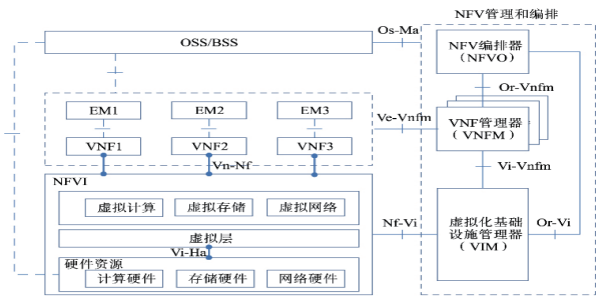

图 1 ETSI MANO 架构图

其中 VNFM 负责 VNF 描述符（virtual network function descriptor，VNFD）管理、云服务管理以及 VNF 的实例化、弹性、自愈、卸载等生命周期管理[3]，是部署和运维 5GC VNF 的核心组件。

2 VNFM 面临的问题

当前 VNFM 上一般用 admin 用户登录对 VNF 实例化、弹性、自愈、卸载等生命周期管理操作，VNFM 上所有 VNF 资源都对 admin 用户可见且能操作，可能会导致以下安全隐患和问题。

（1）VNFM 上管理的 VNF 规模越来越大，对 VNF 查找和操作变得更不方便。

（2）对于不同省份的同一类 VNF，名称很接近，容易混淆，误操作风险大。

（3）不同运维人员同时登录 admin 用户操作 VNF，容易引起冲突。

（4）所有 VNF 操作都用 admin 用户，出现问题无法追踪溯源。

（5）admin 是最高等级用户，经常暴露给不同人员，密码容易泄露，存在安全风险。

以下章节提出基于 RBAC 基本模型的 VNF 分域管理解决方案，并且描述了该方案的设计实现和测试，来满足运营商的诉求。

3 基于 RBAC 模型的分域管理解决方案

3.1 RBAC 模型简介

基于角色的访问控制（role-based access control，RBAC）模型于 1992 年由美国国家标准与技术研究院（national institute of standards and technology，NIST）组织开发，它是一种基于角色的信息访问控制方法[4]。RBAC 模型的核

1. 航空工业西安航空计算技术研究所 陕西西安 710065

心思想是引入角色的概念，用户和权限之间以角色为桥梁进行连接[5]，RABC 基本关系如图 2 所示。

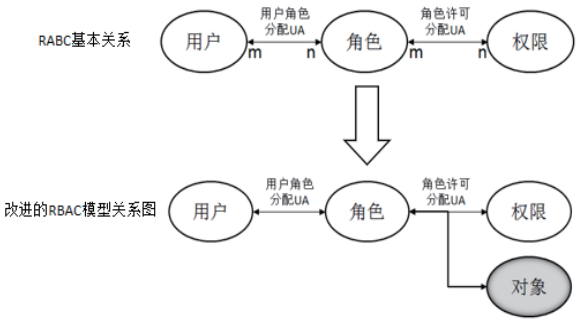

图 2 改进的 RBAC 模型关系图

模型中，用户是访问的主体；角色是权限的载体。用户和角色之间为多对多关系，即每一个用户都能绑定一个或多个角色，同时每个角色也都能指定给一个或多个用户；同样地，角色和操作权限之间也存在多对多的关系，即每一个角色都能分配到一个或多个操作权限，同时每个操作权限也都能分配给一个或多个角色[6]。改变一个用户的权限可以通过改变角色与权限的关系来实现。

基于 RBAC 模型原理，本文提出了如图 2 中所示的改进的 RBAC 模型，即角色增加了与对象的绑定关系，使用户能管理不同对象。角色和对象之间存在多对多的关系，即每一个角色可以分配到一个或多个对象，同时每个对象也可以分配给一个或多个角色。改变一个用户的对象可以通过改变角色与对象的关系来实现。本文中的对象主要是 VNFM 上的 VNF 资源。

3.2 分域管理概念

分域管理是针对访问对象的控制，通过域能限定管理和使用的对象资源的范围。在本文中，主要是特定用户对 5GC VNF 资源的管理和使用，使某些用户登录后只能管理所属范围内的 VNF 资源，对其他范围内的 VNF 资源不可见，不能跨区域增、删、改、查或未经授权资源[7]。根据图 2 改进的 RBAC 模型，设计某类角色与 5GC VNF 的绑定关系来实现 VNF 的分域管理。

3.3 分域管理方案

根据网上公开资料显示，国内某运营商出于运维、管理、成本以及安全的考虑，将整个中国区 5GC 网络资源划分为若干个大区，每个大区下辖一些省份，如表 1 所示。一般一个大区规划部署 1 套 VNFM，统一负责该大区下所有省份的 VNF 等资源管理。各省运维人员只负责本省的运维，跨省份的操作由大区运维人员来协调配合。

表 1 运营商大区划分示例

大区名称	大区中心省份	下辖省份
华北大区	河北	北京、天津、河北、山西、内蒙古
东北大区	黑龙江	辽宁、吉林、黑龙江
华东北大区	江苏	江苏、山东、安徽
华东南大区	浙江	上海、浙江、江西、福建
华南大区	广东	广东、广西、海南
华中大区	河南	湖北、湖南、河南
西南大区	四川	四川、重庆、贵州、云南、西藏
西北大区	陕西	陕西、甘肃、青海、宁夏、新疆

根据表 1 某运营商 5GC 的大区划分模型，本文提出了三层分域管理解决方案，自上而下分别是大区级、区域级和 VNF 级。每一层规划创建角色和用户，角色与该层级的 VNF 资源绑定，角色再与用户绑定，实现用户只管理该层级的 VNF 资源。三层分域管理方案模型如图 3 所示。VNF 根据其功能定位可以分为接入类网元、数据类网元、转发类网元等，可以根据 VNF 分类来设计不同的角色。

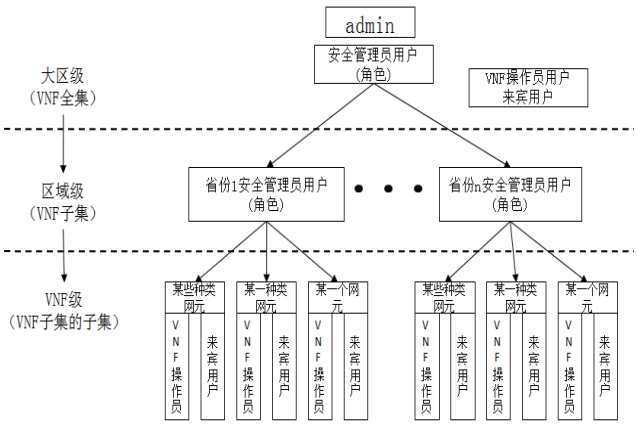

图 3 三层分域管理方案模型

大区级是最高层级，对应的是 VFNM 全系统，该层上的 admin 是系统自带的最高等级用户，具有所有管理资源权限。大区的安全管理员用户（角色）、VNF 操作员用户（角色）和来宾用户（角色）由 admin 创建，并且由 admin 来给各个角色绑定 VNF 资源，大区级的角色一般会绑定所有 VNF 资源。区域级对应的是大区下的省份，一个大区下有几个省份就对应创建几个区域，每个区域一般会规划一个区域级的安全管理员用户（角色），区域级的角色和用户由大区级的安全管理员用户来创建和分配 VNF 资源，区域级的安全管理员角色绑定的权限和 VNF 资源是大区级的安全管理员角色绑定的子集。VNF 级对应的是区域内某类或者某个 VNF 创建的角色和用户，通常每个区域下由区域级的安全管理员用户创建某类或者某个 VNF 的 VNF 操作员用户（角色）和来宾用户（角色）。

安全管理员用户只有用户配置权限和资源分域能力，不能具有 VNF 操作权限。VNF 操作员用户权限可以自定义，一般情况下会配置对 VNF、云服务资源、VNFD 等做配置权限。来宾用户只能查看 VNF 等资源，不能做增、删、改等变更操作。VNF 操作员用户和来宾用户都不能具有用户配置和分域的权限。

以上方案实现了某个区域（省份）的用户只能管理该区域下的 VNF 资源，某类网元的用户只能管理某类 VNF 资源，某个网元的用户只能管理某个 VNF 资源，这样能起到资源分域隔离的效果，保证了 VNF 操作的安全性和可追溯性。每个层级的用户用途都已定义清楚，只需把该层级的用户暴露给该层级的相关人员即可满足运维诉求，保证了用户使用的安全性。

4 设计实现

本文中 VNFM 已经具备了分权管理和安全管理功能，分域管理功能是在安全管理功能的基础进行设计开发。本文只对主要的界面框架和联动性机制、新增数据库表和接口函数进行描述，还有一些界面布局、易用性或增强设计等非关键功能不再详细说明。

4.1 前台界面设计

（1）区域以及区域内用户 / 角色 / 操作集配置界面

区域以及区域内用户 / 角色 / 操作集配置界面设计以及配置流程如下。

① 在已有的“安全管理”界面增加“区域”手风琴菜单，点击区域后，会出现如图 4 中第 1 个方框所示的内容。

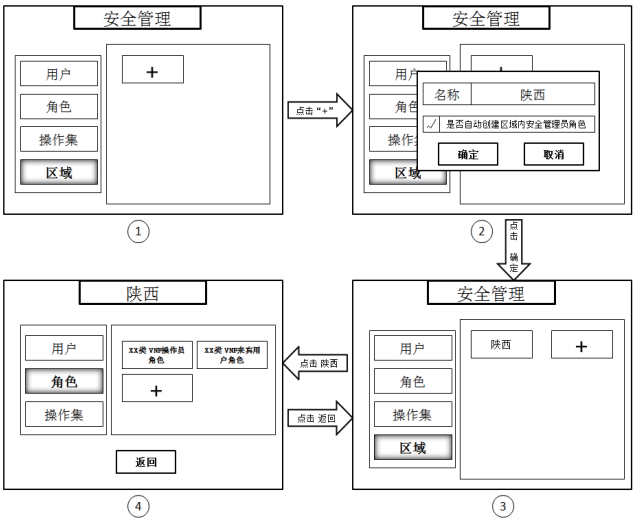

图 4 区域以及区域内用户 / 角色 / 操作集配置界面示意图

② 点击“+”后进行区域添加，弹出的框中如图 4 中第 2 个方框所示，必要的参数填写后点击“确定”，配置成功后如图 4 中第 3 个方框所示，如果配置失败则需界面给出报错信息提示。

③ 双击配置完成的区域“陕西”，进入区域内部界面，执行该区域内的用户、角色和操作集的配置，如图 4 中第 4 个方框所示。

④ 配置角色，点击“角色”菜单后点击右侧“+”进行添加，已配置完成的角色如图 4 中第 4 个方框所示。用户和操作集的配置同理。

⑤ 区域内配置完成后点击“返回”则重新进入图 4 第 3 个方框的“安全管理”的“区域”界面。

（2）资源分域管理界面

区域内用户、角色、操作集配置完成后，通过“资源分域管理”界面对角色和 VNF 资源进行关联。“资源分域管理”是新增菜单，界面示意图如图 5 所示，区域和角色可以被选中，云服务、VPC 和 VNF 前有勾选框。一般由大区级安全管理员登录 VNFM 给区域级安全管理员角色分配 VNF 资源，然后再由区域级安全管理员登录 VNFM 给区域内角色分配 VNF 资源。

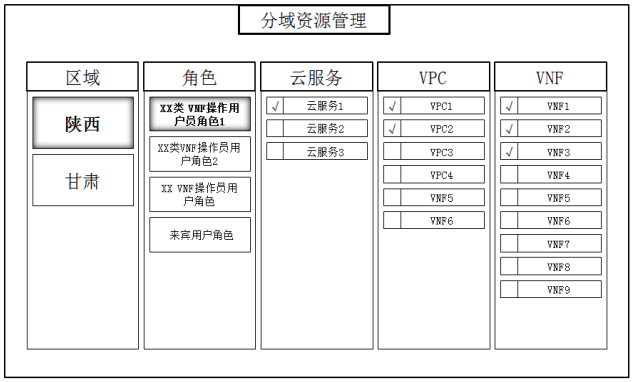

图 5 资源分域管理示意图

“区域”框中是已配置的各个区域，对应的是各个省份。选中区域名称，在“角色”框中就只会显示这个区域内已配置的角色名称，更换选中的区域名称，则在“角色”框中也同样只显示该区域内已配置的角色名称，区域和角色有联动关系。在“区域”框中同时只能选中一个区域名称，在“角色”框中同时只能选中一个角色。

“云服务”框中会显示的是区域级安全管理员角色绑定云服务，“VPC”框中会显示这些云服务下的 VPC，“VNF”框中会显示这些 VPC 下的 VNF。以区域级安全管理员登录，这些云服务、VPC 和 VNF 是大区级资源的子集；以大区级安全管理员登录，这些云服务、VPC 和 VNF 是全集。

一个 VNF 只能归属于一个 VPC，一个 VPC 只能归属于一个云服务，相反一个云服务下可以有多个 VPC，一个 VPC 下也可以有多个 VNF。

选中角色后，如果 √ 云服务，则会联动 √ 该云服务下所有的 VPC 和 VNF；如果 √ 了 VPC，则会联动 √ 该 VPC 下所

有的 VNF；如果 √ 了 VNF，则会联动将该 VNF 对应的 VPC 和对应的云服务前面的框置为选择状态，注意框中不能置为 √，只有把 VPC 下所有的 VNF 都 √ 了，VPC 名称前的框中才会置为 √，只有把云服务下所有的 VPC 或者 VNF 全部 √，云服务名称前的框中才会置为 √。

选中角色后，如果角色之前已与 VNF 有绑定，则会显示出来云服务、VPC 和 VNF 的勾选关系，运维人员可以按需进行勾选和去除勾选操作。云服务、VPC 和 VNF 的去除勾选也是同样的联动机制，不再赘述。

4.2 数据库设计

（1）新增角色和 VNF 关联表 regionResMgrList，存储配置的区域、角色、VNF 关联关系，如表 2 所示。

表 2 角色和 VNF 关联表

字段名	字段说明	备注
Id	区域 Id	主键
zoneId	对应区域 Id，与 zoneResList 表中的 Id 对应	
roleId	区域内的角色 Id，与角色表中的 Id 对应	
VNFId	VNF 的 Id，与 VNF 表中的 Id 对应	

（2）新增区域配置表 zoneResList，存储配置的区域信息，如表 3 所示。

表 3 区域信息表

字段名	字段说明	备注
Id	区域 Id	主键
zoneName	区域名称	必填
isAutoAddZoneSecRole	是否自动添加区域安全管理员角色	True 或 False

（3）还需在已有的用户、角色、权限以及它们之前关系表中增加 zoneId 字段，用来区分是否是区域内配置的，如果是则填充 zoneId 值，否则填写 NULL。

4.3 接口函数设计

（1）新增了区域创建、删除、修改、查询的接口函数。

① creatZoneRes

说明：创建区域信息。

输入：zoneName, isAutoAddZoneSecRole。

输出：成功返回 True，否则返回 False 并携带失败原因。

② deleteZoneRes

说明：删除区域信息。

输入：zoneName。

输出：成功返回 True，否则返回 False 并携带失败原因。

③ modifyZoneRes

说明：修改区域信息。

输入：zoneName, newZoneName。

输出：成功返回 True，否则返回 False 并携带失败原因。

④ queryZoneRes

说明：查询区域信息。

输入：zoneName。

输出：成功返回区域信息，否则返回 False 并携带失败原因。

（2）新增了区域 - 角色 -VNF 关联关系的创建、删除、修改、查询的接口函数。

① creatRegionResMgr

说明：创建区域 - 角色 -VNF 关联关系。

输入：zoneName, roleName, VNFName。

输出：成功返回 True，否则返回 False 并携带失败原因。

② deleteRegionResMgr

说明：删除区域 - 角色 -VNF 关联关系。

输入： zoneName, roleName, VNFName。

输出：成功返回 True，否则返回 False 并携带失败原因。

③ modifyRegionResMgr

说明：修改区域 - 角色 -VNF 关联关系。

输入： zoneName, roleName, VNFName。

输出：成功返回 True，否则返回 False 并携带失败原因。

④ queryRegionResMgr

说明：查询区域 - 角色 -VNF 关联关系。

输入： zoneName, roleName, VNFName。

输出：成功返回关联信息，否则返回 False 并携带失败原因。

（3）在区域内创建用户、角色、权限以及它们之间关联关系复用已有的接口函数，但函数的输入扩充 zoneId 以及其处理逻辑，这里不再赘述。

5 测试与应用

5.1 测试场景

本文主要从功能、性能、可靠性、易用性方面对测试场景进行简单描述，不再说明具体的测试用例、测试过程和测试结果。

（1）功能场景主要包括 VNFM 新建场景和升级场景，新建场景进行区域增删改查、区域内用户 / 角色等增删改查、VNF 分域配置、VNF 用户登录进行生命周期管理操作等；升级场景主要是升级前资源的继承性和升级后对已有资源的分域配置管理。

（2）性能场景主要考虑的是容量规格和时间规格，包括性能背景下区域配置规格、分域管理性能测试、多客户端同时操作等场景。

（3）可靠性场景主要考虑的是分域配置过程中微服务启停、设备上下电、主备倒换、数据库备份恢复等 [8]。

（4）易用性场景主要考虑的是 UI 界面布局、方便性、指导资料等。

（下转第 140 页）

[8] 杨洋 , 褚志刚 . 高性能波束形成声源识别方法研究综述 [J]. 机械工程学报 ,2021,57(24):166-183.
[9] 杨洋 , 褚志刚 . 四种典型波束形成声源识别清晰化方法 [J]. 数据采集与处理 ,2014,29(2):316-326.
[10] SCHWARZ U J.Mathematical-statistical description of the iterative beam removing technique (method CLEAN)[J].Astronomy and Astrophysics,1978, 65:345-356.
[11] 褚志刚 , 段云炀 , 沈林邦 , 等 . 函数波束形成声源识别性能分析及应用 [J]. 机械工程学报 , 2017, 53(4):71-73.
[12] 段云炀 . 基于谱矩阵分解重构的波束形成声源识别方法 [D]. 重庆 : 重庆大学 ,2016.
[13] SARRADJ E.A fast signal subspace approach for the determination of absolute levels from phased microphone array measurements[J].Journal of sound and vibration, 2010,329:1553-1569.
[14] DOUGHERTY R E. Functional beamfomfing[C]// 2014 5th Berlin Beamforming Conference. Berlin:Bellevue, 2014 :1-28.
[15] 余立志 . 实时阵列声成像定位技术研究 [D]. 湘潭 : 湘潭大学 , 2013.
[16] 周昌国 . 基于传声器阵列的声源定位技术研究 [D]. 济南 : 山东科技大学 , 2012.
[17] 崔丽娟 . 输气管道泄漏监测及定位技术研究 [D]. 太原 : 太原科技大学 , 2013.
[18] DOUGHERTY R P.Functional beamforming for aeroacoustic source distributions[C]//20th AIAA/CEAS Aeroacoustics Conference. Reston:American Institute of Aeronautics and Astronautics, 2014: 2738-2755.

【作者简介】

刘姿琪（2003—），女，湖南郴州人，本科，研究方向：阵列信号处理。

李吉祥（2002—），男，湖南涟源人，本科，研究方向：阵列信号处理。

李伟（1999—），男，湖南岳阳人，硕士研究生，研究方向：阵列信号处理。

赵慎（1983—），男，河北肃宁人，通信作者（email: zhaoshen_nudt@163.com），讲师，研究方向：阵列信号处理、卫星导航时空信息处理。

（收稿日期：2023-06-16）

（上接第 134 页）

对于功能、性能主要是自动化测试为主，可靠性和易用性主要是人工测试为主。

5.2 实际应用

该方案在多轮迭代开发和测试完成后，经过充分系统评估可以商用。目前已在某运营商选取某省份局点升级试用，该功能经受住了现网应用场景考验，运行稳定。一线运维人员反馈该方案配置简单易操作，能切实解决实际问题，对该方案给予肯定和认可，后续计划在全网范围内推广使用。

6 结语

本文立足于 5GC 规模化建设和组网演进过程中 VNFM 遇到的运维安全隐患问题，结合某运营商 5GC 组网形态，引入 RBAC 模型基本原理，提出了基于 RBAC 模型的分域管理解决方案，并对该方案进行了详细介绍、设计实现和测试验证。目前该方案已经在某运营商现网 VNFM 上得到了实际应用，效果反馈良好。且该方案基于已有的理论模型，设计思路清晰，易于实现，无特殊硬件要求，具有一定的通用性，可为其他类型组件的分域管理设计提供参考借鉴。

参考文献

[1] 郝慧杰 , 肖建 , 张粮 , 等 .VNF 生命周期管理系统设计与实现 [J]. 计算机技术与发展 , 2020,30(7):12-16.
[2] 金镝 , 赵鹏 . 王成利 .NFV 网络编排器发展现状与关键技术研究 [J]. 信息通信技术与政策 , 2020(3):86-91.
[3] 阳志明 , 毛斌 .NFV MANO 的关键问题研究与实践 [J]. 广东通信技术 , 2016(12):21-27.
[4] 郭冬升 , 徐建良 . 基于角色理论的 RBAC96 模型改进 [J]. 微型机与应用 , 2016,35(16):9-12.
[5] 许斌斌 , 黄均才 . 面向广域测量系统的 RBAC 扩展模型研究 [J]. 电工技术 , 2023(9):57-60.
[6] 方正宁 . 基于 CloudStack 的权限管理模块的设计与实现 [D]. 北京 : 北京邮电大学 ,2015.
[7] 戴念东 , 刘育文 .IMS 网管分权分域功能与应用前瞻 [J]. 电信技术 , 2014(1):217-220.
[8] 王贞凯 , 叶昊灵 , 戴新星 , 等 . 基于微服务架构的 5G 网管云化应用研究 [J]. 长江信息通信 , 2023(3):201-204.

【作者简介】

沈强（1986—），男，河南信阳人，硕士，助理工程师，研究方向：航空电子设备和系统验证技术。

（收稿日期：2023-09-20）