

5G 核心网容灾方案及部署策略研究

Research on 5G Core Network Disaster Recovery Solution and Deployment Strategy

李延斌(中国联通研究院,北京 100176)

Li Yanbin(China Unicom Research Institute, Beijing 100176, China)

摘要:

网络安全及可靠性对运营商来说至关重要。5G 网络更多地采用虚拟化、服务化架构,对网络安全部署带来挑战。不同网元对容灾的要求和流程各有不同,可根据网元自身特点及需求采用不同的容灾部署方式。在 5G 大规模商用之际,更需要平衡网络投资与业务可靠性的关系,找到更为合适的容灾部署策略。

关键词:

5G 核心网;容灾;部署策略

doi:10.12045/j.issn.1007-3043.2020.09.016

文章编号:1007-3043(2020)09-0079-04

中图分类号:TN915

文献标识码:A

开放科学(资源服务)标识码(OSID):



Abstract:

Network security and reliability are very important to operators. 5G network adopts more virtualization and service architecture, which brings challenges to network security deployment. Different network elements have different requirements and processes for disaster recovery, and different disaster recovery deployment methods can be adopted according to the characteristics and requirements of network elements. It is more necessary to balance the relationship between network investment and business reliability, and find a more appropriate disaster recovery deployment strategy.

Keywords:

5G core network; Disaster recovery; Deployment strategy

引用格式:李延斌. 5G 核心网容灾方案及部署策略研究[J]. 邮电设计技术, 2020(9): 79-82.

1 概述

随着 5G 商用步伐加快,5G 网络进入实际部署及商用阶段,网络面临的各种安全问题和隐患也越来越被重视。一方面,用户及产业对网络的要求越来越高,对网络的依赖性越来越强,使得网络承担了更多的使命和责任;另一方面,运营商自身的建设投资及运维压力较之前显著增大。如何既能保证业务体验,又能降低成本,既能保证网络的安全可靠性,又可以灵活部署,是当前运营商面临的重大课题之一。

5G 核心网容灾技术的研究本质上是对网络运营成本和网络服务质量的平衡把控,也是在核心网网络

虚拟化之后,对新型网络安全可靠性的探索。与此同时,对运营商网络安全和健壮性的考量也不仅仅要求核心网应用层网元具备相应功能流程,而是一种基于网络整体的综合能力评估,其中可能包括对网络整体短板的判断、对网络冲击的防御机制、对虚拟化网络硬件层和虚拟层的容灾能力评估、对其他异常场景的模拟和预判等。

2 容灾总体原则

2.1 特性及优势

由于 5G 网络架构相对于 EPC、IMS 网络,引入了服务化架构、计算与存储分离、控制面和用户面分离。基于这些新特性,5G 容灾方案具有如下特性和优势。

a) 服务化架构。服务化架构下,NF 网元容灾可

收稿日期:2020-08-01

以利用NRF的注册和发现机制实现,具体如下。

- (a) 服务注册时包含容灾节点信息。
- (b) NRF在服务发现时向消费者提供生产者列表的同时包含容灾节点。
- (c) 消费者向NRF订阅生产者状态变更通知。
- (d) NRF辅助通知生产者退出服务。

b) 计算与存储分离。5GC核心网NF无状态设计采用计算与存储分离的技术,NF的状态数据保存在外部UDSF中。UDSF实现数据层容灾,将NF保存的数据在UDSF容灾节点间同步。发生容灾切换后,NF备用节点从UDSF获取数据,进行业务恢复。

c) 控制与转发分离。5G是基于控制面和用户面分离架构(CUPS),SMF的用户上下文等状态数据存储在UDSF中,由UDSF对数据进行备份处理。在某SMF故障后,由其备份SMF从UDSF获取上下文状态数据并继续处理业务。

2.2 网元类型与容灾关系

同种类型网元的容灾方式也有一定相似性,如:

互联互通:NRF、NEF、NSSF,考虑1+1主备或者负荷分担容灾方式。

接入管理:AMF、PCF、SMF、AUSF,建议组POOL且多DC部署。

存储类:UDM、UDR、CDB(UDSF),建议采用组POOL或者负荷分担等方式,并要求数据实时同步。

3 主要网元容灾方式

3.1 AMF

AMF提供POOL/SET(NF SET)容灾方式。同一个Region内,同一个Set的AMF对应一个POOL(见图1)。

正常情况下,所有话务由POOL/SET内的所有AMF共同承担。用户注册时,RAN按一定规则(如容

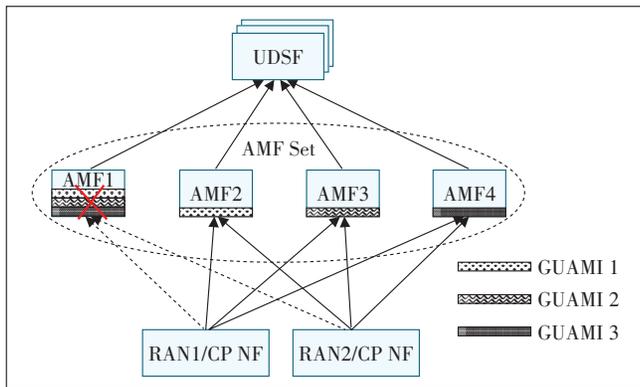


图1 AMF容灾

量/权重)选择AMF完成用户注册及执行后续业务流程。

AMF进入工作状态后,主动向NRF进行注册(通过Nrf_NFManagement_NFRegister携带GUAMI List以及各GUAMI对应的备份AMF),并根据配置周期定时发送与NRF之间的心跳消息(通过Nrf_NFManagement_NFUpdate)。NRF通过此心跳消息检测以及维护AMF的工作状态。当一定时间未接收心跳消息后,NRF将此AMF状态设置为不可用,并向订阅了此AMF状态的CP NF发送AMF状态通知消息,其他CP NF由此获知AMF故障,并触发后续故障处理相关流程。

当任何AMF故障宕机时,其新话务由POOL/SET内其他AMF共同分担。

当任何AMF故障宕机时,其原承担话务由NG-RAN或CP NF选择其备份AMF接管继续处理;备份关系以GUAMI为粒度体现,根据配置,其原承担话务可以由多个备份AMF(按GUAMI区分)共同接管并分担处理。

AMF的用户上下文等状态数据存储在UDSF中,由UDSF对数据进行备份处理。在某AMF故障后,由其备份AMF从UDSF获取上下文状态数据并继续处理业务。

3.2 SMF

SMF提供POOL/SET(NF SET)容灾方式。一组SMF组成一个POOL/SET,为一个业务区域或一组业务区域的用户提供服务(见图2)。

正常情况下,所有话务由POOL/SET内的所有SMF共同承担。AMF按一定规则(如SMF的容量权重,运行负荷)分担选择SMF执行业务流程。

SMF进入工作状态后,主动向NRF进行注册(通过Nrf_NFManagement_NFRegister),并根据配置周期

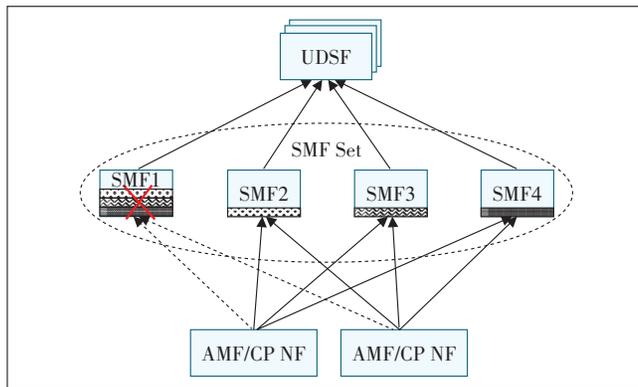


图2 SMF容灾

定时发送与 NRF 之间的心跳消息(通过 Nnrf_NFManagement_NFUpdate)。NRF 通过此心跳消息检测以及维护 SMF 的工作状态。当一定时间未接收心跳消息后,NRF 将此 SMF 状态置为不可用,并向订阅了此 SMF 状态的 CP NF 发送 SMF 状态通知消息,其他 CP NF 由此获知 SMF 故障,并触发后续故障处理相关流程。

当任何 SMF 故障宕机时,其新话务由 POOL/SET 内其他 SMF 共同分担。

当任何 SMF 故障宕机时,其原承担的会话,可通过会话迁移的方式由其备份 SMF 继续处理。其他 NF 如 AMF、PCF 等选择其备份 SMF 继续处理会话。

SMF 的用户上下文等状态数据存储在 UDSF 中,由 UDSF 对数据进行备份处理。在某 SMF 故障后,由其备份 SMF 从 UDSF 获取上下文状态数据并继续处理业务。

3.3 UPF

UPF 提供 POOL 容灾方式。一组 UPF 组成一个 POOL,由 SMF 进行管理,负责一个或一组业务区域(见图3)。

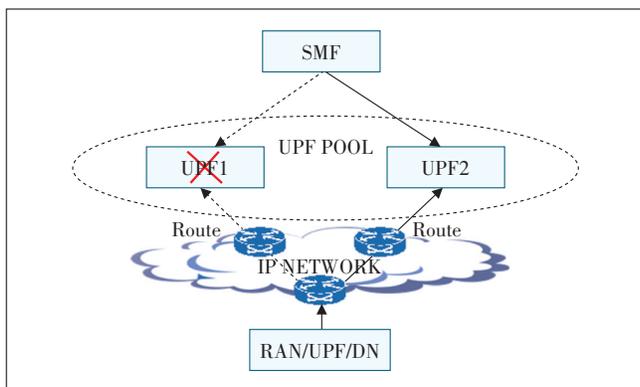


图3 UPF 容灾

正常情况下,所有话务由 POOL 内所有 UPF 共同承担。SMF 按一定规则分担选择 UPF 执行业务流程。

正常工作状态,SMF 通过 PFCP 接口的状态检测消息 Heartbeat Request/Heartbeat Response 进行 UPF 状态的检测与维护,当一定时间未正常接收到心跳响应后,SMF 将此 UPF 状态置为故障,同时根据配置启动 UPF 的故障处理流程。

当任何 UPF 故障宕机时,由 SMF 选择 UPF POOL 内其他的 UPF 执行会话流程。

3.4 NRF

NRF 提供 1+1 互备容灾方式(见图4)。

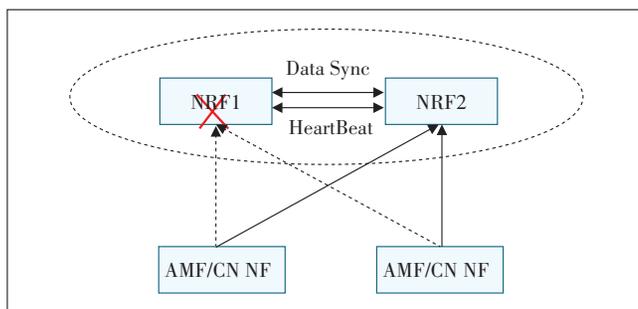


图4 NRF 容灾

在正常情况下,所有话务由 2 个 NRF 共同承担。对端 NF(例如 AMF、SMF)优选本地 NRF 执行相关业务流程;只有当此 NRF 故障宕机时,对端 NF 会将业务发送给另一个 NRF 进行处理。

2 台互为备份的 NRF 设备之间支持数据实时自动同步,接收到 NF 数据的 NRF 在完成本设备数据更新后,主动将更新数据同步到另一台 NRF,确保 2 台设备的数据完全一致。

3.5 UDM

UDM 容灾采用组 POOL 的方式,此时业务查询可采用负荷分担方式。UDM 用户数据保存在 UDR 中,要求 UDR 节点间数据同步可靠性高(见图5)。

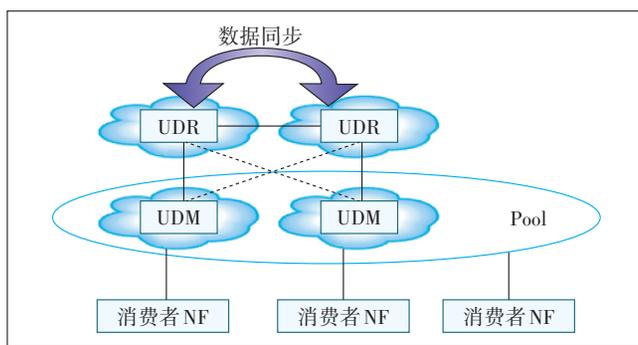


图5 UDM 容灾

正常情况下,所有话务由 POOL 内的所有 UDM 共同承担。用户请求时,消费者 NF 按一定规则分担选择 UDM 完成用户鉴权及执行后续业务流程。

UDM 进入工作状态后,主动向 NRF 进行注册(通过 Nnrf_NFManagement_NFRegister 携带 UDM Group ID。UDM Group ID 用于索引可支持相同 SUPI 集合的一组 UDM),并根据配置周期定时发送与 NRF 之间的心跳消息(通过 Nnrf_NFManagement_NFUpdate)。NRF 通过此心跳消息检测以及维护 UDM 的工作状态。当一定时间未接收心跳后,NRF 将此 UDM 状态置为不可用,并向订阅了此 UDM 状态的 CP NF 发送 UDM 状

态通知消息,其他CP NF由此获知UDM故障,并触发后续故障处理相关流程。

当任何UDM故障宕机时,其新话务由POOL内其他UDM共同分担。

当任何UDM故障宕机时,其原承担话务由CP NF选择其备份UDM接管继续处理。其原承担话务可以由多个备份UDM共同接管并分担处理。

4 容灾部署方案

4.1 容灾目标架构

如图6所示,5G网络采用分层部署的架构,划分区域DC、本地DC和边缘DC,基于5G网元特性及业务需求将5GC、RAN部署在各个DC中。

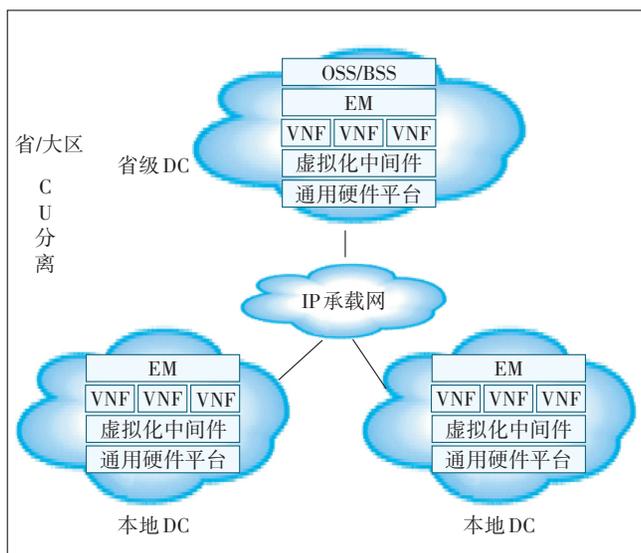


图6 容灾架构

区域DC出于容灾考虑,DC站点间根据不同网元的特性,利用POOL组网、1+1负荷分担、1+1主备等NF级容灾机制保证业务组网可靠性,当一个数据中心发生故障后,通过VNF内软件模块的迁移来实现在异地的业务恢复;边缘DC主要用于uRLLC业务的U面接入,以做到流量本地转发,达到时延最短。由于边缘DC承载的是uRLLC业务,对时延要求高,统一考虑站内容灾方式;本地DC用于接入各地(市)的业务流,利用现有网络资源(如地(市)Internet出口、CDN等),将媒体面接入网元UPF部署在本地DC,减少控制面的业务时延;DC内则考虑通用硬件/虚拟化层池组化,利用VNF池化/N+M备份实现类似板卡级备份。

4.2 部署策略及建议

a) 部署方案。大区DC采用双DC节点建设,保证

容灾和可靠性;5GC商用建设时采用融合版本,兼容2G/3G/4G/5G接入,业务开通大区集中;平滑迁移用户数据至大区DC融合UDM/UDR,保证数据安全可靠。

b) 部署时间点。核心网容灾产品成熟时间点同SA架构,容灾主要在部署层面实施,部分容灾流程需进一步验证。

c) 引入建议。运营商在5G部署阶段应紧密结合部署策略,按省部署及大区部署等方式分别给出容灾策略。部署应考虑NFV架构及通信云建设方式以及容灾方案,减少对核心网的影响和投资。

5 总结及思考

SA架构容灾与网络部署架构密切相关,不同组网不同网元有不同容灾方案。国际标准对网元容灾方案及实现流程不做详细规定,各个厂家实现方式、机制及流程有较大不同,这就给运营商部署带来很大影响及风险。如何既能够满足5G核心网商用部署要求及策略,又能满足各种异厂家组合场景下的现网环境容灾备份,是网络部署中极难解决的问题之一。

另一方面,5G网络架构引入了服务化架构、计算与存储分离、控制面和用户面分离,需要综合考虑并利用新技术实施容灾,而不仅仅依靠某一层网络或者某一种技术,充分利用技术的发展带来的安全性和可靠性,而不是被更加复杂的网络所束缚。

总之,5G核心网容灾技术面临的问题和困难比想象的要大的多,在后续网络部署及运营阶段还会遇到各种问题,需要持续关注。

参考文献:

- [1] 朱常波. 电信云的发展和对新业务的支撑思考[J]. 邮电设计技术, 2018(1):33-37.
- [2] 韦国锐,陈立栋,于秋思,等. 跨DC的虚拟化核心网容灾体系研究[J]. 邮电设计技术, 2019(9):78-81.
- [3] 陆广海. 爱立信核心网CSFB快速容灾方法研究[J]. 电信快报:网络与通信, 2018(2).

作者简介:

李延斌,高级工程师,硕士,长期从事移动核心网相关标准制定、技术研究等工作。

