基于 Docker 技术的静态安全分析云计算应用

刘　洋，赵瑞锋，李　波，王海柱，邓大为

（广东电网有限责任公司电力调度控制中心，广东 广州 510600）

摘　要：为适应电力调度系统中响应多用户静态安全分析计算的并发性和扩展性需求的不断发展，通过分析静态安全分析计算的特点，并将其与 Docker 技术结合，提出一种基于 Docker 技术的静态安全分析云计算应用方法。首先，设计该应用方法的运行架构，对不同的潮流计算算法制作对应的 Docker 容器镜像；随后通过 Protobuf 按照给定格式实现用户和容器之间数据交互，根据计算请求动态创建新的容器或分配空闲容器，并在计算结束后释放容器资源；所提方法利用 Docker 技术提高云平台计算资源的利用率，满足静态安全分析计算功能的并发要求。最后，对实际算例进行分析，结果表明，该方法可以提高云平台下静态安全分析计算功能的并发性和扩展性。

关　键　词：Docker；静态安全分析；云计算；Protobuf

DOI：10.19781/j.issn.1673-9140.2021.04.023　　**中图分类号**：TM734　　**文章编号**：1673-9140(2021)04-0181-07

Application research of static security analysis cloud computing based on Docker technology

LIU Yang, ZHAO Ruifeng, LI Bo, WANG Haizhu, DENG Dawei

(Power Dispatch and Control Center, Guangdong Power Grid Co., Ltd., Guangzhou 510600, China)

Abstract: To match to the development of the concurrency and expansibility requirements of multi-user static security analysisin power dispatching systems, this paper analyzes the characteristics of static security analysis and calculation, and combines it with docker technology. Based on Docker technology, astatic security analysis cloud computing application method is proposed for designing the operation architecture of the application. In this method, Docker container images are generated corresponding to different power flow algorithms, and the data exchangebetween users and containers are realized by using Protobuf. New containers are dynamically created and idle containers is allocated according to the calculation request. Containerswill be released once the calculation is finished. This method uses Docker technology to improve the utilization of cloud platform computing resources, and meet the concurrent requirements of static security analysis calculation function. The case studiesshow that the proposed method can effectively utilize the computing resources and extend the concurrency and extensibility of static security analysis.

Key words: Docker; static security analysis; cloud computing; Protobuf

收稿日期：2019-07-30；**修回日期**：2020-03-18

基金项目：中国南方电网有限责任公司科技项目(GD-KJXM-20180250)

通信作者：刘　洋(1982-)，女，高级工程师，主要从事调度自动化运行及研究；E-mail：judy_liuy@126.com

现代电网系统构成复杂,安全运行压力大,对电力分析业务的性能和效率的要求越来越高,传统电力调度系统已无法满足当前智能电网的数据量和分析量的要求;随着基于网络和虚拟化资源的云计算的不断发展,电力调度自动化系统的云化趋势明显[1-4]。软件即服务(software as a service,SaaS)的发展带来了应用虚拟化技术的极大拓展,应用虚拟化技术的目标在于实现应用软件运行环境与操作系统轻耦合,用户通过网络在服务器上申请并建立独立的内存空间和界面,用户需求的应用程序在建立的"另一个系统"中运行,同时用户终端通过协议接受应用程序返回结果,从而依靠互联网通讯及云技术完成对服务器上的各种应用软件的访问及调用,在云服务器资源的充分利用的同时极大丰富了用户的应用能力[5-7]。云计算技术在电力系统监控领域的应用仍是研究和探索阶段,尚没有成熟的应用软件投入到电力系统工业生产中。

静态安全分析是电力系统监控领域所广泛使用的电网故障风险评估手段,需要响应电力监控系统中不同层级用户并发的静态安全分析计算请求,当前电力系统采用本地服务器组作为计算的主体,对云的应用很少,而实际中大部分服务器上只运行单一应用,CPU 利用率很低,并且由于电力系统运行的高可靠性要求,电力系统数据中心的分析计算任务在不同的物理服务器上都有备用冗余,对备用冗余资源的无序分配也会加剧服务器资源利用率低的现象。静态安全分析计算通常会独立占用大量计算资源,且因数据准备、整理、结果输出复杂性等原因很难做到资源利用的最大化;同时传统的调度员潮流大多是基于 C/S 方式,支持并发用户数有限;潮流计算功能与其他业务共享困难[8-10]。为解决以上静态安全分析计算的问题,利用云平台的存储资源、计算资源以及资源分配能力的优势,选择云计算技术作为解决方案,该文提出一种基于 Docker 技术的静态安全分析云计算应用方法,采用容器技术集成潮流计算所需的最小系统,通过合理创建及释放云计算平台的计算、通信、存储资源,实现电力监控系统中响应多用户静态安全分析计算请求的强并发性和强动态扩展能力。

1 Docker 容器技术

传统的应用虚拟化技术可以满足企业对云计算处理性能的要求,但对底层系统功能依赖较强,与服务器操作系统强耦合。例如:ThinApp 是 VMware-View 的组件,且依赖宿主机操作系统完成应用的虚拟化,并不能很好地实现运算结果在云平台中的共享。近年来,Docker 技术的出现实现了虚拟技术的"轻量化",Docker 技术是基于容器技术的一种实现,容器技术可以实现对单个操作系统所管理的计算和存储能力进行有效重组,解决了单操作系统多余资源无法响应灵活计算和存储需求的问题。Docker 基于 Linux 内核对进程进行封装隔离,可理解为将所需操作系统内容进行虚拟化。封装后各进程独立于宿主以及其他隔离进程的系统即被称为容器。Docker 在容器的基础上,通过对文件系统等进一步的封装,极大简化了容器的创建、释放和维护,使得 Docker 技术比虚拟机技术更为轻便、快捷。针对实现容器的虚拟化,Linux 的内核引入具有强大特性的命名空间(Namespace)功能,实现了对内存、CPU、网络 IO、存储空间、文件系统、网络、PID(process identification)、UID(user identification)、IPC(inter-process communication)等等的相互隔离,容器技术通过独立的命名空间,保证了其运行的独立性。因此,应用 Docker 容器技术运行实际应用,使得应用软件的运行几乎完全不依赖本地操作系统,可以在不同组织方式的不同云之间便捷的迁移,实现了面向应用的系统级层面的虚拟化技术[11-13]。

Docker 的镜像包括环境变量的设置、计算所需程序的安装和信息传输的服务端口,通过 Docker-file 描述镜像的构建过程;通过 push 指令将镜像上传到 Docker Registry(容器注册中心)[14-16]。其他宿主机上采用部署的 Docker Engine 去查询并搜索 Docker Registry 中服务所需要的镜像并完成所需镜像的加载。完整的镜像包含了应用运行的所需的系统文件功能及相关联的软件功能,完成这一系列的操作后,新的宿主系统上应用可以直接对外提供

服务，利用新的宿主系统的硬件资源进行程序运行，而不需要配置环境变量、安装关联软件等操作，其宿主机通过注册中心加载统一镜像的工作方式极大提高了新功能、新应用的发布、修改、测试的便捷性。

2　基于 Docker 技术的静态安全分析云计算架构

静态安全分析是在指定电力系统预想事故下的潮流计算，完成静态安全分析需要的数据包括待计算电力网络的节点信息、连接线信息、潮流初值、重要元件（包括发电机、母线、变压器等）运行限值和预想事故方案等。潮流计算的方法也包括有 PQ 分解法、功率式牛顿法、电流式牛顿法、最佳乘子法、PQ 分解转牛顿法等多种，计算结果用来判断越限的设备。充分利用静态安全分析的计算特点可以更好地发挥 Docker 技术的优势，以往使用虚拟机的方式进行电力系统云平台计算需要在虚拟机中安装全部的计算功能，包括数据接收、潮流计算、结果分析及输出等；应用 Docker 技术后可将整个计算流程分散，针对各个功能部分分别进行设计[17-19]，从而实现根据静态安全分析任务需求的变化动态组合各个功能部分，不仅实现对系统资源的有效利用，也方便了应用功能的调试和发布。

基于 Docker 技术的静态安全分析云计算架构如图 1 所示。为提高云平台计算分析系统的开放性及标准化程度，通过 Protobuf 规范服务接口参数格式，通过服务管理规范服务注册流程，用户在 Web 前端请求静态安全分析计算，请求信息即包括待计算的网络模型编号及预想事故信息，网络模型编号用于在数据库中调用电力网络的元件模型、节点和连接线数据；在 Docker 代理接收到请求信息后，从已经制作好的静态安全分析 Docker 容器镜像动态中创建一个容器实例，Docker 容器主要为潮流计算功能，针对每一种潮流方程计算方法建立一种潮流计算容器镜像，根据请求的不同要求加以调用。容器目录挂载 Volume 读取实时电网分析模型更新容器内部的电网分析模型组件，支持多用户多容器实例并行运行；通过 Docker 代理，利用 Protobuf 作为数据载体在用户和静态安全分析容器间进行通信，实现用户的预想事故设置操作和计算结果的返回，并定时释放该用户占用的容器资源。

针对多并发的计算过程，设计并发计算管理功能，按照任务触发序列依次进行计算任务的执行；并建立静态安全分析并发计算任务信息库，并发任务信息库处于实时更新的状态，包含预想事故设置信息、任务信息、资源状态信息等。其中预想事故设置信息包括已完成计算的预想事故及将要完成计算的预想事故；任务信息包括任务编号、启动者标识、任务超时时间、任务启动时间、任务完成时间、任务失败等信息；计算任务的排序根据预想事故的时标次序确定；资源状态信息包括容器数目、容器地址列信息、容器计算状态，采用相应的队列存放各个状态容器的标识。若计算任务返回超时、失败或者当前容器创建失败，则取消当前任务并即时重新加入任务序列，继续等待执行，直至所有计算任务序列完成。

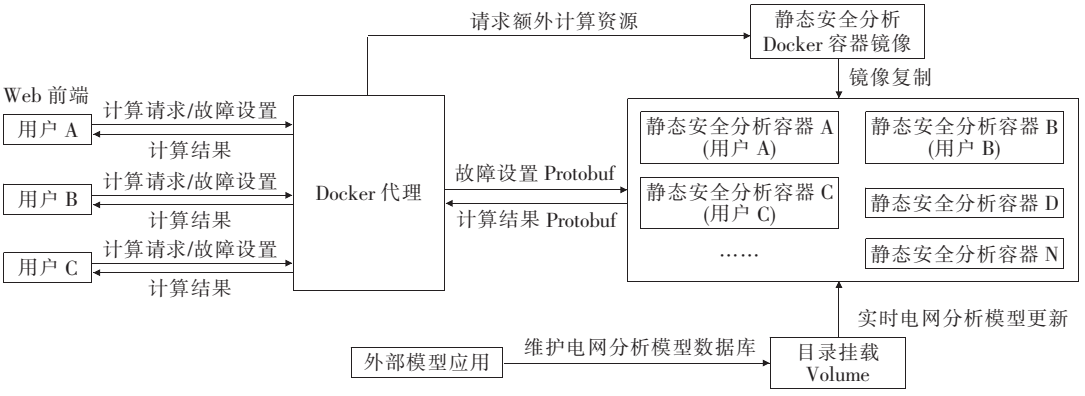

图 1　基于 Docker 技术的静态安全分析云计算架构

Figure 1　Static security analysis cloud computing architecture based on Docker technology

3 新架构的关键技术

3.1 静态安全分析 Docker 容器镜像

静态安全分析是一定条件下电网运行情况的评估，通过计算确定母线电压在安全范围、发电机负荷在机组运行安全值以内、线路没有过载以及变压器在运行安全值以内，其依据的计算条件包括当前的电网结构、线路参数、发电机运行状态、线路及节点的电压电流及切除元件。因此，静态安全分析的本质是一组各种特定预想事故设置的潮流计算的集合。制作的静态安全分析 Docker 容器镜像中包括 5 个组件。

1)电网分析模型数据库。数据库用来描述和记录静态安全分析计算所需的电网设备、结构相关模型和参数；设备包括电动机负荷、阻容型负荷、变压器、电力线路、电容滤波/补偿器、发电机等；电网结构包括各个设备与线路的连接信息。

2)计算参数文件。参数文件 capara.ini 描述静态安全分析计算所需参数，包括有功功率收敛判据、无功功率收敛判据、最大迭代次数、平衡节点及其对应的发电机、设备 $N-1$ 设置、自定义预想事故设置。

3)Protobuf 通讯程序。为可执行程序 caprotobuf，实现按照预先定义的 Protobuf 结构化数据格式编码和解码。

4)静态安全分析计算程序。通过可执行程序 caproccal 从电网分析模型数据库中读取静态安全分析计算所需的基础数据，从计算参数文件读取静态安全分析计算的设置，进而依据数据进行电力系统预想事故后的电网潮流值计算，完成支路、断面越限分析计算。

5)依赖动态库。应对电网拓扑和结构的变化，采用动态库连接结构变化与静态安全分析计算，动态库主要包含拓扑分析、电网断面以及潮流计算动态库。

静态安全分析 Docker 容器镜像内部组件如图 2 所示。

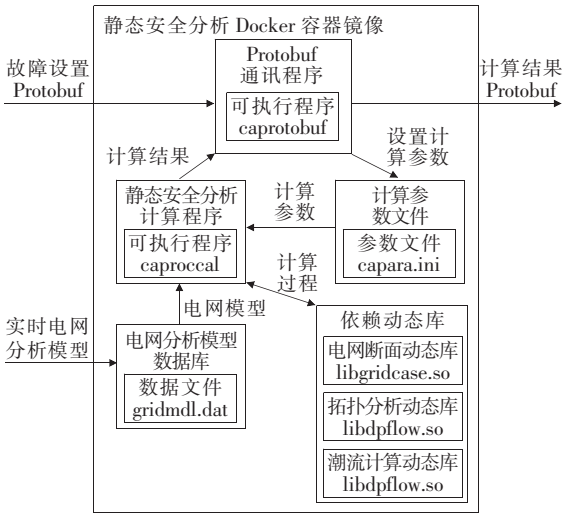

图 2 静态安全分析 Docker 容器镜像内部组件

Figure 2 Internal component diagram of Docker container image for static security analysis

3.2 动态创建 Docker 容器

动态创建静态安全分析容器流程如图 3 所示。基本步骤如下：

1)统计正在运行的未被用户使用的空闲静态安全分析容器数目，Docker 代理逐个检查运行中静态安全分析容器是否已分配给用户；

2)若存在空闲容器则将该容器分配给该用户，记录该容器关联用户信息，否则由静态安全分析 Docker 容器镜像启动一个新的容器实例分配给该用户；

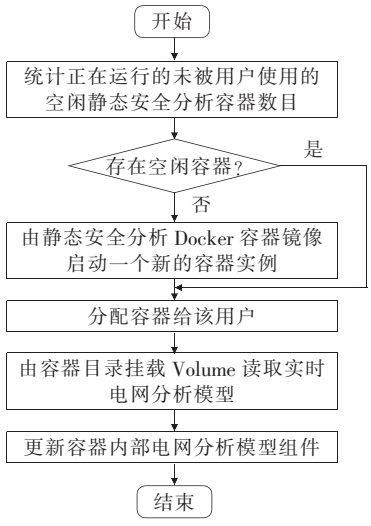

图 3 动态创建静态安全分析容器流程

Figure 3 Flow chart of dynamically creating static security analysis container

3）电网的拓扑模型采用相应的外部应用进行更新，以响应电网实际的拓扑变化以及发电机、电动机负荷、阻抗负荷、变压器、电力线路、容抗器等的模型及参数变化；更新的电网拓扑模型即时对模型数据库的数据进行更新，同时在容器目录中挂载 Volume，感知数据刷新并读取当前的实时电网分析模型。

3.3　预想事故设置和计算结果返回

采用 Protobuf 作为数据载体实现用户对电网预想事故设置并对返回的计算结果进行分析，其步骤如下。

1）对 Protobuf 结构化数据格式进行定义，然后在此基础上将用户对电网的预想事故设置进行编码。用户对电网预想事故设置内容的 Protobuf 数据结构设置为

```
package screquest;
message sc_re {
    required string usr_name = 1;//用户名
    required string usrid = 2;//用户 id
    optional string cal_method = 3;//计算方法
    optional float epsp = 4;//有功收敛判据
    optional float epsq = 5;//无功收敛判据
    optional int32 maxn = 6; //最大迭代次数
    optional string bgid = 7; //平衡发电机 id
    optional int64 fid = 8;//预想事故设备 id
    optional string fobject=9;//预想事故设备名
    optional string station=10;//厂站名
}
```

2）由 Docker 代理将序列化编码数据传入用户关联容器，由容器内部 Protobuf 通讯程序进行解码并更新计算参数文件组件：更新有功和无功收敛判据、最大迭代次数、平衡电厂、平衡发电机、设备 $N-1$ 设置。

3）容器的静态安全分析计算程序组件按照电网分析模型数据库、计算参数文件中的电网架构、设备模型和参数、静态安全分析条件、预想事故等，完成静态安全分析计算，计算结果包括：①越限对象类型（线路、变压器、母线、稳定断面）；②越限对象名（越限设备或稳定断面具体名称）；③预想事故设备（引起越限的预想事故设备名称）；④预想事故类型（引起越限的预想事故类型，分为线路、变压器、母线、发动机 $N-1$ 以及自定义预想事故）；⑤限值（设备或断面越限的限值）；⑥当前值（设备或断面当前的潮流值）。

将计算结果由 Protobuf 通讯程序序列化编码后由 Docker 代理返回给 Web 前端用户，并释放该用户占用的容器资源。计算结果的 Protobuf 数据结构设置为

```
package careturn;
message sc_return {
    required string otype = 1; //越限类型
    required string objid = 2;//越限对象名
    required float lmt = 5; //限值
    required float val = 6; //当前值
    optional string fequ = 3;//预想事故设备
    optional string ftype = 4; //预想事故类型
}
```

4　应用效果

为验证基于 Docker 技术的静态安全分析云计算应用效果，该文自行搭建模拟云环境。硬件设施：一台 Linux 操作系统、4 核 Intel 中央处理器、8 G 内存的计算机；采用的虚拟机配置：Linux 操作系统、600 MB 内存、2 G 硬盘。

以 IEEE 30 节点为算例，节点系统如图 4 所示。系统的基准容量 $S_b=100$ MV·A；1、2、5、8、11、13 为发电机节点，1 为平衡节点，2、5、8、11、13 为 PV 节点，其余为 PQ 节点；负荷节点电压允许波动范围为 0.95～1.10 p.u.，发电机无功出力允许波动范围为－40～50 MVar，发电机节点电压允许范围为 0.97～1.10 p.u.；潮流初值采用标准 IEEE-14.30.57.118 中的数据。

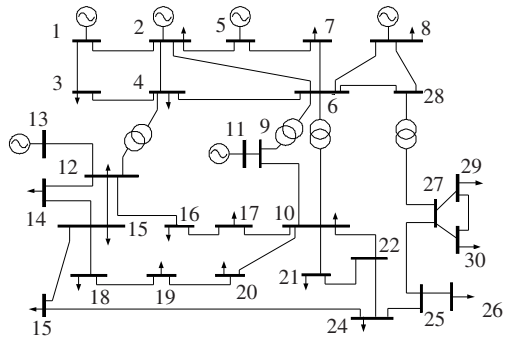

图 4　IEEE 30 节点模型

Figure 4　IEEE 30 node model

模拟中采用的潮流计算均相同，针对 IEEE 30 节点模型进行发电机节点 2 切除的静态安全分析，模拟支持 5 人同时在线使用功能，即在任一时刻能够满足随机产生的 1～5 个静态安全分析请求。采用原有的在云平台中设置虚拟机的运行方式，每个虚拟机独立完成一个静态安全分析任务，则必须启动 5 个具有离线调度员潮流计算功能的虚拟机，以等待可能的调用；应用该文方法不需要提前设置容器数量，通过静态安全分析请求动态创建新静态安全分析容器，当静态安全分析结束后将容器释放。对不同请求数目进行潮流计算，观察记录运行期间的 CPU 使用率和内存使用率。该文与原方法在不同静态安全分析请求情况下的 CPU 使用率和内存使用率情况如表 1 所示。

表 1 不同静态安全分析请求下资源使用情况对比

Table 1 Comparison of resource usage under different static security analysis requests %

请求数目	CPU 使用率		内存使用率	
	该文方法	原方法	该文方法	原方法
1	20.1	32.2	33.8	45.2
2	20.8	33.1	35.7	45.3
3	21.9	33.8	37.2	45.4
4	22.8	33.5	38.4	45.5
5	24.2	34.3	39.0	45.5

通过表 1 的对比情况可以看出，原虚拟机方式相比容器方式就需要更多系统资源的支持，为维持多人同时在线的最大请求响应能力，原有的云平台运行方式需要保持运行足够多的虚拟机，从而使得系统资源消耗增加；而 Docker 技术在做好镜像文件后，根据请求数目的不同建立对应的容器，实现动态响应，从而极大降低了对资源的消耗；虚拟机对资源的需求限制了一台服务器上设置的虚拟机数，Docker 技术的计算资源需求随节点规模自动扩大，不需要预置固定的内存量。因此，同一服务器上虚拟机的设置数肯定远小于可设置的 Docker 容器数，在此次试验的环境中，可用容器最大值约为可用虚拟机最大值的 2.4 倍，从而采用 Docker 技术在云平台中可以极大增加静态安全分析计算的并行响应计算的数量，相较于基于本地服务器的工作模式，避免了大量空转应用的被迫等待，实现了计算资源利用的最大化；同时，容器采用基于请求的灵活建立和释放、最大化资源的利用率实现静态安全分析计算能力的拓展。

5 结语

针对日益复杂的电网分析计算要求和云计算中进行静态安全分析的技术需求，该文提出了一种基于 Docker 技术的静态安全分析云计算应用方法，预先制作包含电网分析模型、计算参数、Protobuf 通讯程序、静态安全分析计算程序、依赖动态库的 Docker 容器镜像；收到潮流计算请求时由云计算平台动态创建新的容器或分配空闲容器；通过 Protobuf 按照给定格式实现用户和容器之间数据交互，包括服务请求参数的反序列化和计算结果的序列化；计算结束后释放容器资源。实际应用结果表明，该方法实现了静态安全分析服务的动态扩展，实现了计算资源的按需配给，降低了计算资源的无效等待时间，从而达到在保证静态安全分析计算可靠的前提下优化整体云计算资源配置的目的。

参考文献：

[1] 沐连顺，崔立忠，安宁. 电力系统云计算中心的研究与实践[J]. 电网技术，2011，35(6)：171-175.
MU Lianshun，CUI Lizhong，AN Ning. Research and practice of cloud computing center for power system [J]. Power System Technology，2011，35(6)：171-175.

[2] 赵俊华，文福拴，薛禹胜，等. 云计算：构建未来电力系统的核心计算平台[J]. 电力系统自动化，2010，34(15)：1-8.
ZHAO Junhua，WEN Fushuan，XUE Yusheng. Cloud computing：Implementing an essential computing platform for future power systems[J]. Automation of Electric Power Systems，2010，34(15)：1-8.

[3] 杨利，张哲，张秋实，等. 基于云计算的配网不停电作业仿真培训平台设计[J]. 电力科学与技术学报，2019，34(1)：142-148.
YANG Li，ZHANG Zhe，ZHANG Qiushi，et al. Research on simulation training platform of live working in distribution networks based on the cloud computing[J]. Journal of Electric Power Science and Technology，2019，34(1)：142-148.

[4] 马越，黄刚. 基于 Docker 的应用软件虚拟化研究[J]. 软件，2015，36(3)：10-14.

MA Yue, HUANG Gang. Research on application virtualization based on Docker[J]. Computer Engineering & Software, 2015, 36(3): 10-14.

[5] 张建，谢天钧. 基于 Docker 的平台即服务架构研究[J]. 信息计算与信息化，2014(10)：131-134.
ZHANG Jian, XIE Tianjun. Research of platform as a service architecture based on the Docker[J]. Information Technology & Informatization, 2014(10): 131-134.

[6] 王申华，何湘威，方小方，等. 基于泛在电力物联网多源信息的电网动态风险评估系统[J]. 中国电力，2019，52(12)：10-19.
WANG Shenhua, HE Xiangwei, FANG Xiaofang, et al. Dynamic risk assessment system for power system based on multi-source information of the ubiquitous power internet of things[J]. Electric Power, 2019, 52(12): 10-19.

[7] 刘少辉，李新，孟泽文，等. 基于调度自动化系统的断路器动作特性研究及其状态评估[J]. 高压电器，2019，55(6)：31-37.
LIU Shaohui, LI Xin, MENG Zewen, et al. Analysis and status assessment of circuit breaker's operation characteristics based on power dispatching automation system [J]. High Voltage Apparatus, 2019, 55(6): 31-37.

[8] 杨延昊. 基于云计算的智能电网调度系统设计研究[J]. 电网与清洁能源，2019，35(9)：7-11.
YANG Yanhao. Design of intelligent grid scheduling system based on cloud computing[J]. Power System and Clean Energy, 2019, 35(9): 7-11.

[9] 李俊楠，李伟，李会君，等. 基于大数据云平台的电力能源大数据采集与应用研究[J]. 电测与仪表，2019，56(12)：104-109.
LI Junnan, LI Wei, LI Huijun, et al. Research on big data acquisition and application of power energy based on big data cloud platform[J]. Electrical Measurement & Instrumentation, 2019, 56(12): 104-109.

[10] Gupta V, Chaunhan S, Sharma D. Platform virtualization: Understanding virtual machines, LXC, Docker, Kubernetes and Ubernetes[J]. International Journal of Innovations in Engineering and Technology, 2016, 7(6): 442-447.

[11] 曾鸣，刘英新，赵静，等. "云大物移智"与泛在电力物联网融合的安全风险分析及安全架构体系设计[J]. 智慧电力，2019，47(8)：25-31.
ZENG Ming, LIU Yingxin, ZHAO Jing, et al. Security risk analysis and security architecture design of widespread power internet of things with the use of cloud computing big data internet of things mobile internet and smart city technology[J]. Smart Power, 2019, 47(8): 25-31.

[12] 李静，罗雅迪，郭健，等. 调控云环境下在线计算软件服务研究与应用分析[J]. 电力系统保护与控制，2019，47(8)：159-164.
LI Jing, LUO Yadi, GUO Jian, et al. On-line calculation software service and its application analysis under dispatching cloud[J]. Power System Protection and Control, 2019, 47(8): 159-164.

[13] Machen A, Wang S Q, Leung K K, et al. Live service migration in mobile edge clouds[J]. IEEE Wireless Communications, 2018, 25(2): 140-147.

[14] 浙江大学 SEL 实验室. Docker 容器与容器云[M]. 北京：人民邮电出版社，2016：201-308.

[15] 化振谦，卢世祥，阙华坤，等. 基于弹性分布数据集和有向无环图的潮流优化云计算系统设计研究[J]. 电力系统保护与控制，2019，47(23)：160-165.
HUA Zhenqian, LU Shixiang, QUE Huakun, et al. Design and research of power flow optimization cloud computing system based on elastic distribution data set and directed acyclic graph[J]. Power System Protection and Control, 2019, 47(23): 160-165.

[16] 杨志. 基于 Docker 的 PaaS 云平台的设计与实现[D]. 北京：北京邮电大学，2016.

[17] 张忠琳，黄炳良. 基于 openstack 云平台的 Docker 应用[J]. 软件，2014，35(11)：73-76.
ZHANG Zhongling, HUANG Bingliang. The Docker application based on openstack cloud platform[J]. Computer Engineering & Software, 2014, 35(11): 73-76.

[18] 丁海斌，崔隽，陆凯. 基于 Docker 的 DevOps 系统设计与实现[J]. 指挥信息系统与技术，2017，8(3)：87-92.
DING Haibing, CUI Juan, LU Kai. Design and implementation of DevOps system based on Docker[J]. Command Information System and Technology, 2017, 8(3): 87-92.

[19] 李振华，陶渊，赵爽，等. 智能配电网状态估计方法研究现状分析[J]. 电力科学与技术学报，2019，34(1)：115-122.
LI Zhenhua, TAO Yuan, ZHAO Shuang, et al. Research situation analysis of state estimation in smart distribution networks[J]. Journal of Electric Power Science and Technology, 2019, 34(1): 115-122.