Challenges and Analysis of Business Supporting System Deployment Based on Cloud Computing

Zhonglin Han
Coal Hall of Shanxi Province, Taiyuan, Shanxi, 030012, China
*Corresponding author’s e-mail: 13703512943@139.com

Abstract. Cloud computing is a computing system consisting of large-scale and low-cost computing units over IP network to provide computing and storage services. It presents a new technical method and service mode for IT development taking full advantages of its high performance, low cost, and flexible scalability. However, numerous challenges might emerge from IT infrastructure design and deployment based on cloud computing system. Currently, the potential difficulties lie in cloud architecture design, resource pool division, realization of unified management, security mechanism, and service layer design. This paper analyses the challenges and suggests possible solutions accordingly in cloud computing scenarios.

1. Introduction

Nowadays, the business support system (BSS) involves the IT-domain system, CT-domain system, and public-domain system. The BSS is constructed based on service requirements at different stages. Multiple isolated nodes in the BSS make service interconnection and data sharing impossible because there is no unified planning and a requirement-based reconstruction mode is adopted for the IT system. With extensive IT construction, there is an urgent need for high system functionality, integration, and centralization. In addition, as the BSS scale grows, the IT system construction and maintenance bear considerable pressure. Long BSS construction cycle cannot meet unexpected requirements in a timely manner, which weakens competitiveness of the company. The following problems exist in the IT support system[1][2]:

1.1 High Construction and operation cost

Construction costs for DCs (Data Centers) are high. The application-based OS is constructed vertically. If new services need to be provisioned or services are to be expanded, existing DCs must be expanded correspondingly. Construction and maintenance costs for a large number of small-sized DCs are higher than those for a large-capacity DCs.

1.2 Low resource utilization

Currently, DC resources are isolated between applications, and resource capacity is designed based on the estimated maximum load of applications. In addition, resources are statically allocated to applications. In most cases, usage of computing, storage, and network resources of DCs is low.

1.3 Unguaranteed SLA

As multiple layers exist in a DC, a long latency occurs when a user accesses applications, especially when the user accesses applications on the top. Long latency increases the connection failure rate or traffic congestion possibility. Capacity of the DC infrastructure is planned based on the peak traffic of
applications, and the infrastructure is unaware of user roaming and service hotspots. Therefore, it is difficult to optimize user experience of end users.

1.4 Complex management
A DC carries various services, which have different requirements on software and hardware systems and DR (Disaster Recovery) policies. Therefore, application-based vertical infrastructure makes synergy management difficult.

Therefore, cloud DC is widely applied to solve the existing problems for BSS. In Chapter 2, the difficulties of constructing an operation platform with distributive cloud DC at the background will be discussed in details[3][4][5].

2. Design and deployment challenge
The design of cloud DC should follow several principles which are critical to service realization and further maintenance:

2.1 Availability and reliability
The system reliability covers entire system reliability, data reliability, and single device reliability. The distributed architecture of the cloud platform improves the overall system reliability and reduces the system reliance on the reliability of single devices. Features, such as redundancy, HA cluster, and loose coupling between applications and underlying layer devices, ensure the overall system reliability in terms of hardware devices, links, and applications.

2.2 Security
A security protection system that complies with the industry security specifications is designed to ensure the security of DCs. It focuses on security of networks, hosts, virtualization, and data.

2.3 Maturity
The DC solution uses the architecture, hardware, and software that have been put into large-scale commercial use, and the IT management solution that complies with the Information Technology Infrastructure Library (ITIL) specifications to ensure solution maturity.

2.4 Advancement
The advanced technology and idea of the cloud computing highlight customer benefits. Advanced technologies and modes, such as virtualization and dynamic resource deployment, are used with the services, ensuring the efficiency of advanced technologies and modes.

2.5 Scalability
With the loose coupling between IT infrastructure and service systems, the solution allows DC resources to be elastically expanded or reduced depending on service application workloads. Users can expand the capacity of service systems by simply adding IT hardware devices.

2.6 Openness
Mainstream OpenStack integrates with the industry ecosystem, prevents hardware and software vendor lock-in, and ensures ROI on resource pool.

3. Solution to Design and Deployment Difficulties
In order to ensure unified management of multiple DCs, accomplish converged infrastructure, achieve fast application management and reliable services, the solution is presented in Chapter 3 in various aspects: cloud architecture design, resource pool division, realization of unified management, security mechanism, and service layer design.
3.1 Cloud architecture design

The cloud DC design can be divided into two main parts: physical architecture design and logical architecture design. Figure 1 explains the physical design of a distributive cloud DC.

The existing DC is located at place A. The DC is deployed with VMware virtual resources. Existing devices are reused to build one physical resource pool. Based on this, Huawei FusionSphere OpenStack is deployed to achieve unified management of VMware virtual resources. The new DC is located at place B. The DC is deployed with FusionSphere OpenStack, which is compatible with computing and storage devices provided by different vendors. The DC provides multi-level resource pool services, such as physical resource pools, high-performance resource pools, and common resource pools. The DC that is built as planned in Phase 2 is located at place C. The DC adopts the mode of modular replication to build a DC that has the same architecture as place B, rapidly achieving delivery. The new DC that is located at place B is deployed with a unified cloud management platform to connect and manage these 3 DCs in a unified manner, achieving the unified management and resource sharing among DCs. Based on such a platform, resources are allocated among VDCs.

Apart from the physical design, the logical architecture is described in figure 2, which is specified into 4 layers.
3.1.1 Infrastructure. This layer provides computing, storage, and network resources for physical DCs. It supports mainstream vendors’ server, storage, and network devices, which can be divided into different AZs to meet different service requirements for performance, reliability, and networking structures.

3.1.2 Resource pool. This layer converges computing, storage, and network resources into resource pools. Infrastructures and virtualization platforms (FusionCompute and VMware vSphere) of different vendors can be managed under the OpenStack architecture as unified resource pools.

3.1.3 Service domain. This layer converges unified resource pools of each physical DC into a global resource pool across DCs. Then the global resource pool provisions resource services on demand.

  **VDC service:** A virtual DC (VDC) enables resources in the global resource pool to be allocated to different tenants, departments, or service domains. Computing, storage, and network resources are allocated as a whole, equivalent to an independent DC.

  **Cloud services in a VDC:** Managers can allocate the resources of a VDC in the form of services to VDC users as required. Services supported include cloud hosts, cloud disks, PMs, elastic IP addresses, and applications.

3.1.4 Management domain. This layer consists of ServiceCenter and OperationCenter. It manages the operation and maintenance of services as a whole.

3.2 Resource pool design
In a converged resource pool, physically dispersed DC resources are centrally managed. Unified O&M capabilities are provided for multiple DCs. With distributed management capabilities, computing, network, and storage resources in multiple DCs are pooled and centrally managed. Based on flexible resource scheduling policies, such as stagger reuse, dynamic scaling, and cross-DC resource sharing and migration, applications can be deployed across resource pools and DCs to implement resource scaling. In addition, the converged resource pool solution provides powerful unified O&M capabilities for heterogeneous virtual resources. The centralized O&M portal flexibly provides user views based on user roles so that users can focus on their concerned services. In specific scenarios, the converged resource pool solution integrates NAS, SAN, and FusionStorage.

![Figure 3 Resource pool design of distributive DC.](image-url)
3.3 Unified Management Solution Design

The unified management solution design is achieved by introducing the management software named ManageOne. The design of ManageOne is classified into two layers:

3.3.1 Resource layer. Software at this layer is used to manage resource information (for example, collecting device information) and send resource information to the service layer for service assembling, provisioning, and comprehensive O&M analysis.

3.3.2 Service layer. Operation software and O&M software are used at this layer. Operation software provides operational services for tenants after resource orchestration, and provides a unified operation platform for managers. O&M software implements comprehensive analysis of collected O&M information, such as alarms and performance, displays analysis results, and provides a unified O&M platform for managers.

3.4 Security Guarantees

Security issues are triggered from multiple sources with various scenarios. Besides, security problems concerns contingencies from different dimensions. For example, DC security challenges include physical contingencies such as unauthorized access, theft and natural disaster, network contingencies such as information collection, network sniffing, and network spoofing, system contingencies such as virus, Trojans, worms and password cracking, application layer such as input verification, identity authorization, sensitive data protection, and exception handling.

Management problems, such as unclear rules, lack of security awareness and lack of security guidance. Thus, the security isolation design principles are proposed to reduce the security risks. Accordingly, figure 5 and table 1 illustrates the implementation of isolated design principles.

Table 1 Security device deployment in DC.

| DC Zone                  | Security Device Deployment                                                                 |
|--------------------------|-------------------------------------------------------------------------------------------|
| Internet external zone   | • Anti-DDoS/Next-Generation Firewalls (NGFWs)                                             |
|                          | • SSL VPN gateways, intrusion detection systems (IDSs)/intrusion prevention systems (IPSs) |
| Extranet                 | • Firewalls                                                                               |
| Core network zone        | • Firewalls, SSL VPN gateways, IDSs/IPSs                                                  |
| High security service zone | • Firewalls and intrusion prevention systems (IPSs) are deployed among Web servers, application servers, and databases. |

Figure 4 Unified management solution design layout.
3.5 Service Stage Solution realization
FusionStage, a micro service cloud application platform, enables end-to-end application orchestration, deployment, scheduling, flexible scaling, and O&M. It can integrate ISV and customer services in the general service catalog for quick service publishing. ServiceStage applies to scenarios that feature high concurrency, low latency, and rapid service provisioning and capacity expansion, which has the key technologies and specifications such as:

- Mixed orchestration of containers and VM applications
- Resource expansion in seconds easily addresses public service surges.
- Gracefully quitting interworks with load balancing to timely release resources, exerting no impact on services.
- Large-scale cluster management: A single cluster supports a maximum of 2000 nodes and 50,000 containers.
- GUI-based designer: enables fast publishing of complex applications with drag and drop operations.
- Automatic O&M for application faults: Collects application KPI data in a non-intrusive manner and aggregates application KPI data.

4. Conclusion and Outlook
Nowadays the DC design and deployment is facing multidimensional challenges and difficulties. With analysis of the existing problems and selection of newly emerged technologies, a comprehension solution of distributive DC deployment is proposed in this paper. In general, several key points should be strictly controlled to ensure the performance of cloud DC.
4.1 Efficiency
Resource consolidation and efficient O&M is of great significance. Physical and mainstream virtual resources and multiple DCs are managed in a unified manner, achieving the consolidation of global resource pools, unified O&M, scheduling, and on-demand allocation.

Self-O&M of services and organizations
Data can be divided among VDCs. Flexible rights- and domain-based management and automatic O&M should meet the management requirements of organizations and services.

4.2 Agile
The IT platform is supposed to be Service-driven. Resources are deployed in a differential manner, ensuring service SLA. Resources are scaled up and down and scheduled based on the load and running condition of services. VMs and PMs are orchestrated in a mixed manner and perform one-click deployment, achieving minute-level service rollout.

Physical networks and virtual networks are converged to form an SDN, achieving flexible deployment of services among DCs.

4.3 Reliability
Service continuity should be guaranteed, where zero data loss and data consistency among multiple hosts is the goal. Besides, data safety is of great value, where second-level backup and restoration could increase the service efficiency effectively.

4.4 Open
Based on the OpenStack architecture, the virtualization of devices from multiple vendors is compatible with heterogeneous IT devices, and could be applied to the scenarios such as private clouds, public clouds, and hybrid clouds.

5. Appendices
List of Abbreviation:
BSS: Business Supporting System
OS: Operating System
SLA: Service Level Agreement
ITIL: Information Technology Infrastructure Library
IaaS: Infrastructure as a Service
NaaS: Network as a Service
SECaas: Security as a Service
Maas: Migration as a Service
Paas: Platform as a Service
DC: Data Center
VDC: Virtual Data Center
VM: Virtual Machine
PM: Power Module
HDFS: Hadoop Distributed File System
VPC: Virtual Private Cloud
SDC: Service Data Center
SDS: Scalable Data Store
DR: Data Route
DCI: Data Center Interconnect

References
[1] Wuhib, F., Stadler, R., & Lindgren, H. (2012). Dynamic resource allocation with management objectives: implementation for an openstack cloud. Communication Networks, 610: 309-315.
[2] Dykstra, J., & Sherman, A. T. (2013). Design and implementation of FROST: Digital forensic tools for the OpenStack cloud computing platform. Elsevier Science Publishers B. V.
[3] Dykstra, J., & Sherman, A. T. (2013). Design and implementation of FROST: digital forensic tools for the openstack cloud computing platform. Digital Investigation, 10(8): S87–S95.
[4] Abhat, A., Aboul-Enein, S., & Malatidis, N. A. (1981). Heat-of-Fusion Storage Systems for Solar Heating Applications. Thermal storage of solar energy: proceedings of an
international TNO-symposium held in Amsterdam, The Netherlands, 5-6 November 1980/C. den Ouden, Editor.

[5] Laing, N. (1973). REFRIGERATION MACHINE CIRCUIT WITH FUSIONSTORAGE. US, US 3766752 A.