Building the Foundation for a Private Cloud

KOBAYASHI Kenichi[*1] KUME Masahiro[*1]

Abstract:

As part of DX strategy, JFE Steel has been promoting a project to open, including the core systems of its headquarters, to carry out IT structural reforms. To complete these projects, a company-wide system infrastructure to replace the conventional host computer is essential. We built an open platform (private cloud) for the JFE Group as a foundation with high availability, continuity, and cost optimality to support core systems. In this paper, we discuss the outline and aim of the key technologies adopted for the private cloud and the future prospects based on the actual operation.*

**Private cloud: A form of service in which a company builds its own cloud environment and provides it to internal organizations and group companies*

1. Introduction

The core systems of JFE Steel have operated on highly reliable host computers. Because the host computers were constructed based on the proprietary standards of each manufacturer, there were various problems in terms of data asset utilization. For example, the options for system configuration and extensibility of functions were limited, and it was difficult to utilize state-of-the-art digital technologies. Thus, in order to realize a "flexible IT structure with resilience against change" through digital transformation (DX), it was essential to integrate the company's aging legacy systems and build a foundation for transitioning to an open platform. Considering the direction of technology, the characteristics of the systems and other relevant factors, a private cloud (hereinafter, J-OSCloud) which satisfies the following requirements was selected as the foundation to be built.

i) Cost rationalization by standardization and avoiding vendor lock-in.
ii) Shortening of the lead time for providing new services by automation.
iii) Guaranteeing availability and business continuity.

This article describes the following two main technologies that were adopted for implementation of J-OSCloud.

i) OpenStack technology
To avoid vendor lock-in and to automate server construction by adopting OpenStack technology, which is an OSS (open source software)
ii) Network virtualization (NV) technology
To guarantee availability and business continuity by logically integrating utilization and having redundant configuration at the data centers of JFE Steel's East Japan and West Japan areas (hereinafter, East DC and West DC)

2. Overview of Private Cloud

An overview of the J-OSCloud system is shown in **Figure 1**. Various types of hardware have been installed in the East DC and West DC. Using the OpenStack technology, virtual servers were configured and private clouds were constructed in the East DC and West DC, and all devices (servers, storage, network (NW) switches, etc.) were made redundant in each DC in preparation for possible emergencies. In addition, the

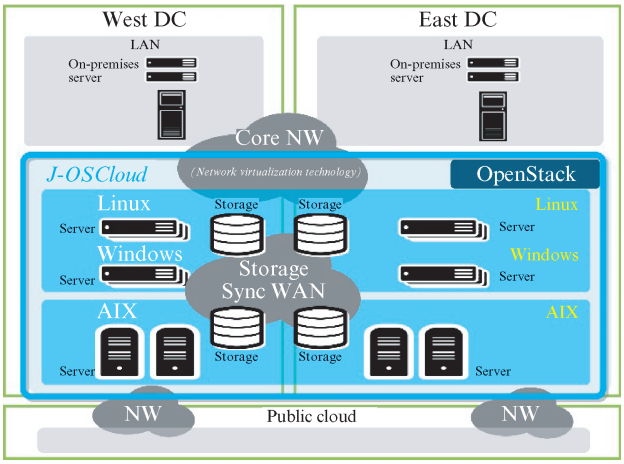

Fig. 1 J-OSCloud system overview

[†] Originally published in *JFE GIHO* No. 51 (Feb. 2023), p. 6−10

[*1] Staff Manager, IT Innovation Leading Dept., JFE Steel

same NW segments between the East DC and West DC are managed by virtual NW technology, while the DCs themselves are implementing improvements that support 24/365 core system operations, aiming at Tier 4 equivalent requirements.

Although the individual on-premises servers in the company are linked on J-OSCloud, use as a hybrid cloud linked with public clouds is also possible.

3. Overview and Aims of Adopted Technologies

3.1 Overview and Aims of OpenStack Technology

3.1.1 What is OpenStack?

OpenStack is an open source software IaaS (Infrastructure as a Service) cloud computing platform management stack that was begun by Rackspace and NASA in 2010. It provides management functions for supplying IaaS and storage service in combination with a hypervisor (software for virtual server implementation) such as KVM or Xen, VMware ESX, Hyper-V, etc. All development and license management function were transferred to the NPO (nonprofit organization) OpenStack Foundation in 2012, and open development that is not biased to the technology of any particular vendor is now possible. **Figure 2** shows the history of OpenStack, which began from a small scale and has evolved through more advanced and subdivided functions year by year. Kilo was adopted for J-OSCloud.

Table 1 lists the components that make up OpenStack. J-OSCloud was constructed using Nova, Glance, Cinder, Keystone and Horizon. The only general function used is the virtual NW management plugin Neutron.

3.1.2 Automation of server construction by OpenStack

By using OpenStack to automate server construction, construction work that had conventionally required a few weeks to one month was shortened to about 3 days. Server construction was standardized as preliminary preparation for construction automation. Specifically, the OS were limited to three types (Windows, Linux, AIX), the OS disk size, file configuration, etc. were unified, and security setting templating was adopted.

Figure 3 shows the flow of server construction automation. Server construction responding to the content of construction requests (specification requirements for CPUs, memory, etc., option setting) is realized by using the OpenStack components in Table 1 and the scripts prepared for each template.

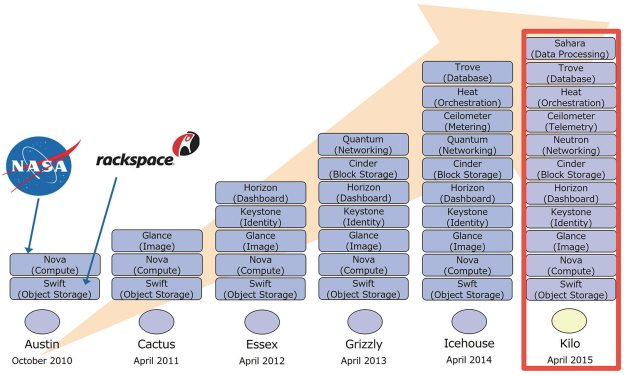

Fig. 2 History of OpenStack

Table 1 Components that make up OpenStack

Project	Service	Overview
Nova	Compute	Determining virtual machine placement, starting and stopping
Swift	Object storage	Object storage
Glance	Image	Managing virtual machine images
Neutron	Networking	Virtual network management
Cinder	Block storage	Providing block volumes
Keystone	Identity	Integrated authentication
Horizon	Dashboard	Web user interface
Heat	Orchestration	Orchestration (AWS cloud formation compatible)
Ceilometer	Telemetry	Collecting information on which to charge
Trove	Database	Database as a service
Sahara	Data processing	Hadoop duster provisioning

3.2 Overview and Aims of Network Virtualization Technology

3.2.1 Overview and aims of network virtualization technology

If the East DC and West DC are to be utilized logically as one DC, it is necessary to realize a redundant system configuration spanning the two sites (i.e., inter-site live migration). Although several methods for realizing this are possible, ones with flexibility and a relatively low operation load were studied. Concretely, this problem was solved by applying network virtualization technology, which eliminates the need for IP address change work and DNS server registration change operation during live migration between the DCs. At the time, there were no examples of the application of this technology in Japan and few examples even at the global level, and the degree of difficulty of introduction was high. However, JFE Steel succeeded in introducing this technology through repeated verifications of numerous technologies for realizing the future IT infra-

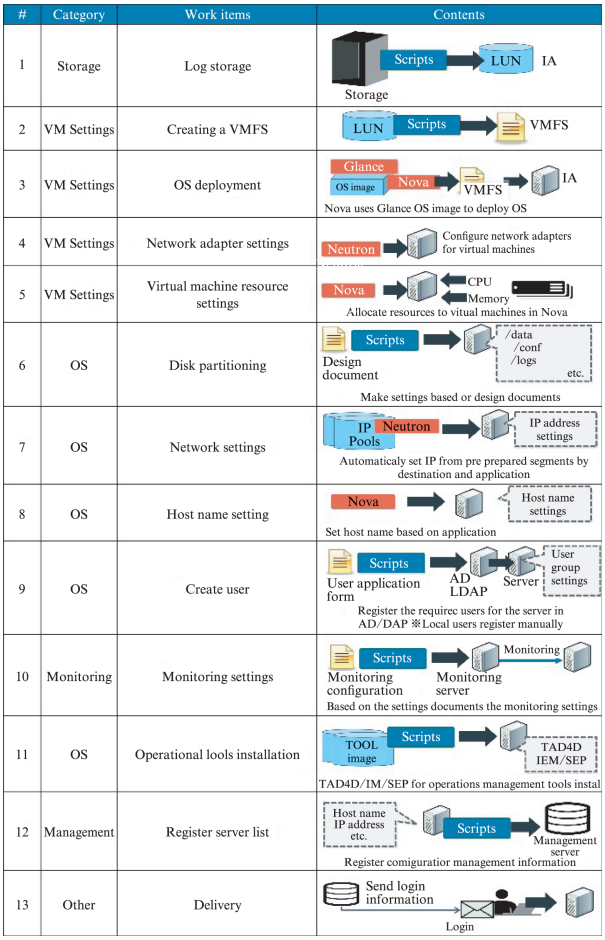

Fig. 3 Flow of server construction automation

structure concept. The actual element technologies are introduced in the following.

3.2.2 Inter-site network segment extension technology

Inter-site live migration means that a virtual server in operation is migrated to a physical server at a different site as-is, without stopping the OS or applications. Although an instantaneous network interruption occurs, the user (client) of the virtual server can continue use with no awareness of the migration of the virtual server.

In order to carry out inter-site live migration without performing a DNS server registration change operation, migration is premised on connection of the physical server at the migration destination to the same Layer 2 network as the physical server before migration. "Layer 2 network" refers to the "data link layer" in the second layer of the OSI (Open Systems Interconnection) reference model. Communications in the data link layer are done by learning the MAC address information of the connected devices. If a virtual server is migrated to a physical server which is connected to a different Layer 2 network, the network address will

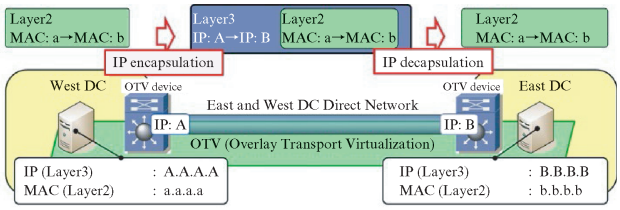

Fig. 4 Inter-site network segment extension technology

	IP address (ID)			
	Network address (Locator)			Host
· IP address	1 .	1 .	1 .	1
· Subnet mask	255 .	255 .	255 .	0

Fig. 5 IP address format

also be different, so this operation takes a form in which the IP address is changed on the virtual server side and the server is started up. However, as result, it becomes impossible to continue communications from the user (client) side.

Therefore, Overlay Transport Virtualization (OTV) was adopted as inter-site network segment extension technology. Use of OTV enables communication with the system of a different site, which has the same network address. Layer 2 communication is performed in communications between systems that have the same network address. On the other hand, in communications with a partner at a different site, Layer 3 routing control becomes necessary. In OTV, communication is realized by hiding the Layer 2 frame by encapsulation by the Layer 3 IP, as shown in **Figure 4**.

3.2.3 In-network communication routing control technology

Before explaining the routing control technology, **Figure 5** shows the IP address format. "IP address" means identification information (ID) comprising a total of 32 bits = host address information, and the "network address" part means the locational information (Locator). The Locator is important as part of the ID.

While inter-site network segments can be extended by OTV, communication is not possible if an appropriate communication partner destination (communication recipient) is not designated on a wide extended network. As one constraint on the ordinary communication network infrastructure, it is not possible to configure a condition in which the same network address exists at multiple sites.

As shown in **Figure 6**, each router maintains table information that indicates the router to which communications should be delivered for the network addresses of addressees. As routing information, each router

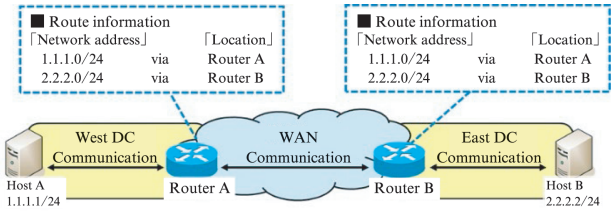

Fig. 6 Conventional network routing technology

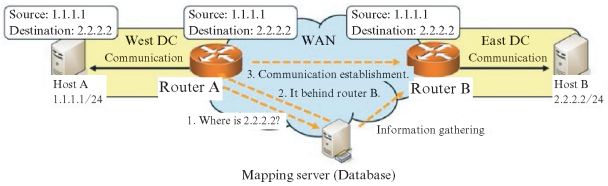

Fig. 7 Virtual network (LISP) routing technology

manages the locational information (Locator) in network address units (part of the ID), and as a result, inter-site migration is not possible with the same network address in its existing form.

LISP[1] (Locator/ID Separation Protocol) was applied to solve this problem. LISP is a routing architecture that separates the Locator (locational information) and the ID (identifying information) in an IP address. LISP maintains the Locators corresponding to IP addresses in a database called a mapping server.

In routing control using LISP, control tied to routers corresponding to network addresses is not performed. Rather, as shown in **Figure 7**, routing control is realized by the database by responding to inquiries using the communication destination information (IP address) as a key and returning information showing the appropriate router.

The applied element technologies are summarized as follows. OTV, which is a Layer 2 extension technology, is applied between the East DC and West DC, and migration of the virtual servers between the two DCs is detected by the LISP VM Mobility function. In communications from the user (client) side to various systems, routing control in host address units is realized by applying LISP.

4. Continuous Enhancement of Functions

J-OSCloud was built in 2016, and a total of several hundred servers were started up in the East and West areas, including the Head Office core system server, which is a critical system. Since startup, J-OSCloud has been improved continuously, as shown in the following representative examples.

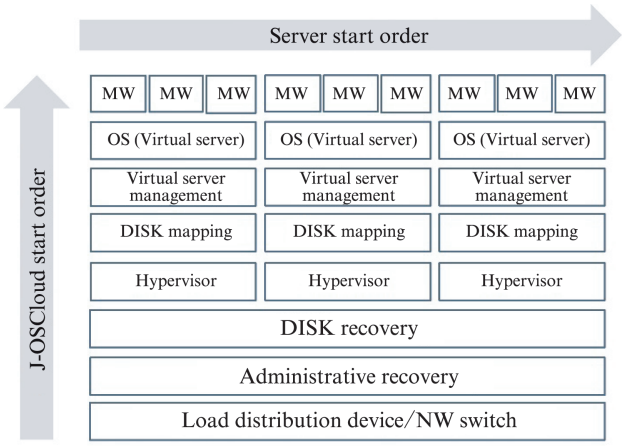

Fig. 8 Scope of automation building

4.1 Automation of Startup of Disaster Countermeasures Sites

Since several hundred servers operate on the J-OSCloud platform, it is assumed that considerable time will be required for system startup at sites where disaster countermeasures are required when an emergency occurs, and it is also necessary to consider the priority order of each server in case of sequential startup. Therefore, automation was attempted in order to shorten the startup time of storage, OS and middleware (MW). **Figure 8** shows the range of automation. Here as well, the open source software Ansible was adopted in awareness of standardization. Ansible has been widely adopted as a programless, agentless automation tool that does not require installation, and was also actively adopted in J-OSCloud in multiple cases, for example, in automation of operation management, etc. Automatic startup was realized by designing the system considering the starting order of each function of J-OSCloud, i.e., the NW and management functions, and the starting order of each server, and describing the startup of each constituent element by scripts.

4.2 Enabling High Availability of Storage

Because trouble accompanying hardware malfunction has occurred in recent years, JFE Steel has also reinspected all devices and implemented measures to heighten fault tolerance against physical failure. One example is full redundancy of storages and automation of redundancy switching.

Figure 9 shows the content studied to enable high availability of storage. A function that enables high availability corresponding to the recovery time and data freshness (recovery point) when a failure occurs in each system was constructed.

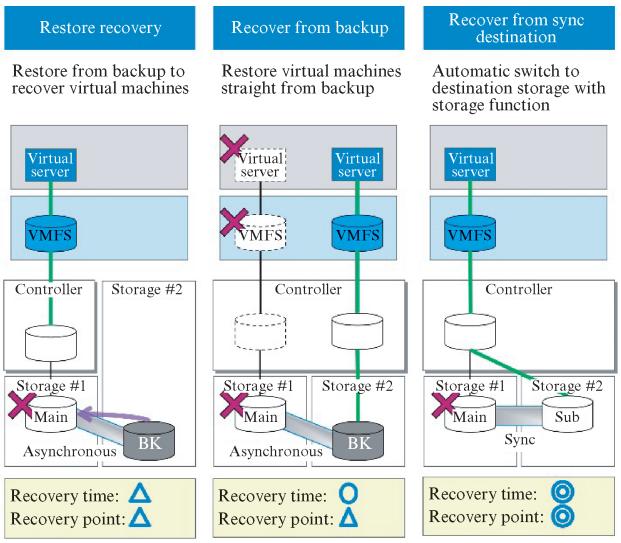

Fig. 9 Enabled storage high availability

5. Conclusion

As described above, a private cloud was built using OpenStack technology and network virtualization technology in order to improve the foundation for operation of critical systems in JFE Steel. Repeated work to enhance functions was also carried out continuously after this project, and efforts were made to further improve the service level in terms of availability and business continuity.

On the other hand, in comparison with 2016, when this foundation was built, the evolution of the technology of public clouds*, beginning with AWS (Amazon Web Service) has been remarkable, and examples of the startup of critical systems are continuing to increase, particularly in the financial industry and manufacturing industries. The authors plan to study strengthening of linkage, including linkage with public clouds, and application to private clouds, based on a full consideration of the distinctive features of the systems at JFE Steel.

* Public cloud: A form of service in which a cloud computing environment is supplied widely to general users and corporate customers via the internet.

Reference

1) Farinacci, D.; Fuller, V.; Meyer, D.; Lewis D. 2013. The Locator/ID Separation Protocol (LISP) . RFC 6830. http://www.rfc-editor.org/rfc/rfc6830.txt