New Solution for Isolation of Multi-tenant in cloud computing

Manzhi Yang[1, a], Huixiang Zhou[2,b*]

[1,2]State Key Laboratory of Networking and Switching Technology, BUPT

Beijing, China

[1]yangmanzhi@eversec.cn, [2*]zhouhuixiang168@163.com

Keywords: Cloud computing; multi-tenant; data isolation; virtualization.

Abstract. Data of multi-tenant is stored together in cloud computing, in order to ensure the data security of tenants that we must to isolate the application and data of each tenant, the security of all tenants may be affected and even cause the whole system to be broken down if the scheme of data isolate is failure, therefore it is worthy to research and analysis the solution of data isolation of multi-tenant in cloud computing environment, in this paper, we research and analyze the solution for application and data isolation of multi-tenant in cloud computing thoroughly, finally we given a related application scenario.

Introduction

Each tenant is not aware of the existence of other tenants in the environment of cloud computing [1], which means that each tenant thought they have own the all service resource and data in system, however, multi-tenant data is stored together in order to be sure the security of application data [2], so the application and data of tenants must to be isolated completely, it is critical that each tenant cannot be allowed to access the data of others, the security solution for all tenants of the data is likely to be affected seriously if isolation is fail or not completed, it is very critical to research on multi-tenant data isolation to ensure the security of each tenants.

New solution for isolation of Multi-tenant

Data isolation

Multi-tenant data isolation is a critical technology in multi-tenant scheme, the failure to isolate the data will be the safe hidden trouble in multi-tenant environment to each tenant [3]. In Multi-tenant environment, the data does not allow to be shared, so the associated protective measures should be taken to support multi-tenant data cannot be accessed by other tenants.

Multi-tenant data isolation is usually divided into three levels, including:

a) An independent database

b) A shared database, isolated data structure

c) Shared database, shared data architecture.

Independent Ddatabase

This scheme is that each tenant has a separate database, so tenant data isolation is the highest level and security is best, but the cost is too high.

Advantages: for each tenant has the independent database, which simplifies the expansion of the data model and meets the unique needs of different tenants; if something would fail, it is relatively simple to restore the data.

Disadvantages: with the increasing number of installation database, the maintenance costs and purchase costs are higher. This scheme is like the traditional one that a customer, a set of data, a set of

deployment, the only difference is that the software are unified arranged by operators. This scheme is suitable for the bank and hospital that data require a very high level of the data isolation. You can choose this scheme to improve the rental pricing. If the price is low, the product takes the low road. Then this scheme is not fit.

shared database and data structure isolation

Show as in Fig1, more or all tenants share the database, but a tenant corresponds to a separate Schema (Schema is the set of database objects, in order to distinguish the various sets needing to give each set a name, such as a table corresponds to a schema's object, the schema name is generally equal to the tenant's account name). The scheme supply logical data isolation for the higher safety of tenants' requirement is not completely isolated.

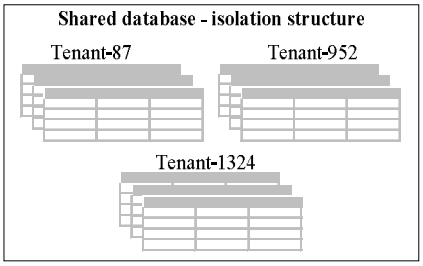

Fig. 1 Sructure of shared database isolatetion

TenantID	Shipment	ShipName
1	TenantID	CustName Address
8	1	TenantID ProductID Date
9	8	1342 12784 2010-18-17
1	9	87 45341 2010-18-23
	1	952 22147 2010-18-19
		1342 98125 2010-18-17

Fig. 2 Sructure of shared data isolatetion

Advantages: each database can support more number of tenants.

Disadvantages: if a failure occurs, data recovery more difficult, because the database will involve other tenants of the data; Therefor, you must need cross-tenants statistics, there are certain difficulties.

shared database and shared data structure

Show as in Fig2, the tenants share with a same Database Schema, but in the data table by Tenant ID (tenant identification) distinguish between the tenants of data. This is the highest level of sharing, the lowest level of data isolation.

Advantages: the cost of maintenance and purchase of the third scheme is the lowest, and it allows each database to support the largest number of tenants.

Disadvantages: the lowest isolation level, minimum security, designing and development is required to increase the amount of the security development; It is the most difficult to data backup and restore, need to one by one by the table. If you want the least amount of servers to provide services for up to tenants, and tenants accept the expense of lower isolation level to exchange for the cost, then this scheme is the most suitable.

Application isolation

Multi-tenant application isolation, mainly considering the different levels of the application deployment technology system, is usually divided into sharing middleware methods and virtualization method. The two applications schemes are summarized below:

a) Sharing middleware approach can be achieved separately: single application instance/shared middleware, multi-application instance/shared middleware, multi-application instance/isolation middleware, etc.

b) The virtual approach, mainly downs the tenant's application into the operating system level isolation. Respectively, based on operating system images for different users achieve application-level isolation.

Sharing Middleware Scheme

Middleware solution can also be divided into three types.

1). sharing middleware of containing

2). multi-instance and multi-space sharing middleware

3). multi-instance and single space sharing middleware

They share middleware and application components among multiple tenants, only difference is the degree. The following is a detailed description of each scheme; all tenants share the operating system, middleware and a single application instance. The method is to parameterize the single application instance with the logo parameters of tenants. For example, if the application has web services interfaces and implementation, then you can add tenants ID parameter to the interface of operations and data objects. If the application uses a database table, then each database table adds a new column that is the tenant ID. In this model, there are some configuration elements that are unique for each tenant. For example, the virtual portal provides a different look and feel and the unique database schema elements for each tenant, the topology of a sample using this method, the example has three tenants: A, B and C, they share the same code in Application1. Application1 uses Tomcat and DB2 running on Windows in the Blade server, and Apache HTTP Server running on Linux on another physical server. All tenants share the middleware, operating systems and servers. When a new tenant appears, and you can create the relevant configuration (such as CSS files, etc.), but only one application instance is shared by all tenants.

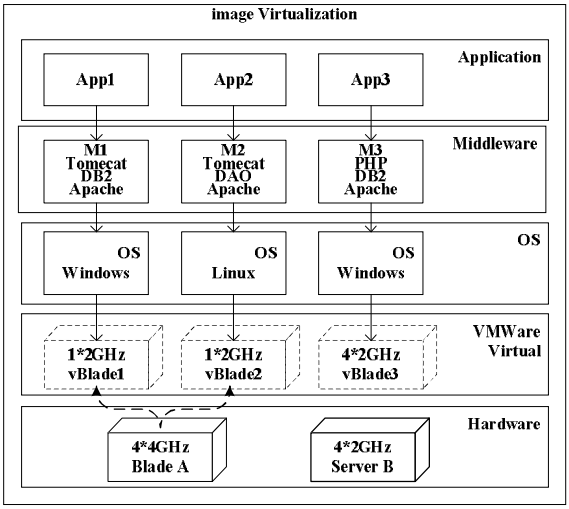

Fig. 4 Application scenario of data isolation.

Using technology of virtualization to run multi- partition of operating system on shared server, assign specific applications and middleware instance for each tenant, in this scenario, tenants use different virtual image different applications, middleware and operating system instances, only share the physical server. In recent years, virtualization technology of server have been widely used on x86-based server, it is becoming a low-cost mature technology rapidly.

Compared with the approach of middleware, virtualization of server does not require a great deal of code for developing to enable multi-tenancy. After installing the virtualization of server for each tenant on the physical server (host), the service provider will instantiate a virtual server which contains the tenant-related software that including middleware and applications, in order to support the new tenants, service providers may need to perform long and complex steps for installing and configuration, than use virtual appliances (for example, VMware Virtual Appliance [4]), which contains pre-configurator operating systems and middleware for tenants, This help to solve the supply problem quickly.

Show as in Fig4, the procedure of local system management be installed on the physical server (such as VMware ESX [5] or Xen [6]). In this scenario, blade physical server has two CPU, it is divided into

two virtual blade servers (vBlade1 and vBlade2 [7]), and each virtual server has a 4 GHz CPU. vBlade3 (Virtual blade server) contains the server B, there are four 2 GHz CPU, virtual servers also share other resources of physical servers, such as memory, space of disk and connectivity of network. The App1 and App2 are respectively deployed on vBlade1 and vBlade2 for services of two tenants, App3 is deployed on the vBlade3, and it is means that all tenants can also use different operating systems.

Conclusion

We repeatedly analyze various solutions for application and data isolation of multi-tenant in cloud computing environment, and finally we given a related application scenario, each tenant can run independently and cannot interfere with each other in this application scenario, so that it well guarantee each tenant running in cloud computing environment safely, and also enhance the data security of cloud system.

Acknowledgment

This work is supported by NSFC (Grant Nos. 61300181, 61202434), the Fundamental Research Funds for the Central Universities (Grant No. 2015RC23)

References

[1] J.Girard and J.Pescatore,"Teleworking in Cloud:SecurityRisks and Services"–A Gartner Report,May 15 2009.
[2] Aulbach S, Grust T, Jacobs D, et al. Multi-tenant databases for software as a service: schema-mapping techniques[C]//Proceedings of the 2008 ACM SIGMOD international conference on Management of data. ACM, 2008: 1195-1206.
[3] Bezemer C P, Zaidman A. Multi-tenant SaaS applications: maintenance dream or nightmare?[C]//Proceedings of the Joint ERCIM Workshop on Software Evolution (EVOL) and International Workshop on Principles of Software Evolution (IWPSE). ACM, 2010: 88-92.
[4] Rosenblum M. VMware's virtual platform™[C]//Proceedings of hot chips. 1999: 185-196.
[5] Chang C H, Scott G K, Kuo W L, et al. ESX: a structurally unique Ets overexpressed early during human breast tumorigenesis[J]. Oncogene, 1997, 14(13).
[6] Barham P, Dragovic B, Fraser K, et al. Xen and the art of virtualization[J]. ACM SIGOPS Operating Systems Review, 2003, 37(5): 164-177.
[7] Yang S, Shih C, Yen C, et al. Blade server management system: U.S. Patent 20,040,024,831[P]. 2004-2-5.