Security Design and Implementation of the Cloud-based Online System

Wei Chen  
Guangdong Vocational Institute of Science and Technology  

Yuting Shang  
Zhuhai Gree Electric Appliance Co., Ltd., Zhuhai, Guangdong 519090

ABSTRACT: This paper discusses safety analysis and design based on the online system of the cloud computing, to enhance system security from the deployment of HTTP endpoint security, database key and certificate, server security strategy. According to the performance of the system, the results were satisfactory, the evaluation from the user is high, also served as an example of the similar online system designed to promote safety.

KEYWORDS: Cloud computing; Security; Online system

1 FOREWORD

The online system based on cloud-computing, making advantage of the Internet to provide paid information search, analysis and other services of account card table at all times and places, providing a convenient, professional, collaborative and efficient management. But the latest study found that the customers do not renew the product, over 68% of them complain the quality of products can not be guaranteed after the free trial, including security, stability, data migration, personalization and so on. The online system in the current applications should be focused more on its security. The online system save all user and their financial information on "cloud", the customers require high level of security and privacy, all information should not be reached by the unrelated employees or others accidentally.

2 SAFE DEPLOYMENT OF HTTP ENDPOINT

The online system is a service-oriented applications typically rely on Web services. The system use the format not applied in the platform that accepts the request and sends the response, which is called SOAP. SOAP uses XML as the encoding scheme of request and response, while using HTTP for transportation. This article describes how to deploy an HTTP endpoint and how to ensure safety when the Web server is directly linked to the database.

2.1 Create HTTP endpoint

Create endpoints include two regular parts, the first part specifies the transport protocol TCP or HTTP, designated HTTP can create HTTP endpoints, you can set the endpoint of the listening port number, authentication methods, and other HTTP protocol configuration of endpoint. The second part will define the load supported by the endpoint. Creating HTTP endpoints is as the following:

```
Create endpoint endpointname [AUTHORIZATION Login] STATE= { STARTED\STOPPED\DISABLED } AS {HTTP\TCP}(<PROTOCAL_specific_arguments>) FOR {SOAP\TSQL\SERVICE_BROKER\DATABASE_MIRRORING}
```

The most important settings to create a secure HTTP endpoint included in language_specific_arguments of SOAP load.

2.2 Specify Web Method

In order to make effective HTTP endpoint, SOAP load must specify at least one Web method. Web method simply stored procedures and functions as a public callable Web service. In a language-specific parameter of SOAP load, the endpoints want to expose specific stored procedures and functions mapping as Web methods. A part of general formats of SOAP load are as follows: {{WEBMETHOD [namespace.] method_alias ( NAME = database.owner.name [SCHEMA = {NONE\STANDARD\DEFAULT}] ) | | , FORMAT = {ALL_RESULTS\ROWSETS_ONLY \}}}
The endpoint disclosed the names of method_alias should be different with the actual stored procedure or function name, use different names could prevent hackers from accessing HTTP endpoint to obtain the disclosed method, or the hackers will access the underlying stored procedures and functions directly and the data is not secure any more.

2.3 Specify the WSDL support, mode and namespace

Each HTTP SOAP endpoint contains a clause in the load to specify WSDL support. If you specify NONE, the endpoint does not provide WSDL support, if you specify DEFAULT, the endpoint was return to the default WSDL. If you specify NONE for SCHEMA, then will not return inline XSD with SOAP request. If you specify STANDARD, then inline XSD and the result set returned together. SOAP payload can specify an explicit namespace for HTTP endpoint. If WEBMETHOD select DEFAULT value (typical value), the default namespace is http://tempuri.org. It must be rewritten in WEBMETHOD option definitions for reasons of security.

2.4 Other SOAP load parameters

You should always disable option of BATCHES for reasons of security. If allowed to connect to ad hoc SQL queries of the endpoint, it equals an invitation for hackers to track the database. For disclosed data of HTTP endpoint, we have to use words of WEBMETHOD to define a specific set of procedures or functions.

3 DEPLOYMENT OF KEY AND CERTIFICATE IN THE DATABASE LAYER

Symmetric encryption of part confidential information stored in the database, while the stored access procedure of confidential information will not been tampered through checking the user certificates. Meanwhile, the enterprise databases must be copied through the network, therefore it needs encrypted copy protection across multiple servers. Create key and certificate for sensitive data can realise the identity verification based on the certification. Using the key or password of the database owner can guarantee the security of the private key for the database.

The Database Engine of SQL Server supports using encryption keys and digital certificates to achieve code signing and encryption. X.509 certificate can be created, export and import in SQL Server and the certificate realise the security solutions based on Public Key Infrastructure. Using a key and certificate architecture of encryption, the architecture of each layer is used to ensure the safety of the items in the next layer.

Create an asymmetric key, the code is as follows: create symmetric key symkey with algorithm_aes_256 encryption by password='j7%ga5c ¥ b+$hdbo$5'

The code above uses a password to encrypt the private key of an asymmetric key.

Create a new certificate, the code is as follows: create certificate awcustrelationscert Encryption by password='pgfd4bb925dgvbd2439587y' with subject='adventure works customers relations' Expiry_date='10/31/2013'

Export certificates, the code is as follows: Backup certificate awcustrelationscert To file='C:\certs\awcustrelationscert'

You can achieve authentication by installing the database mirroring server instance on the server with the certificate. Thus, the server instances could authenticate each other in order to facilitate secure communications.

4 DEPLOYMENT SERVER SECURITY POLICY

The most important thing of SQL Server protection is to protect the security of the server, the user can usually connect to the SQL Server server locally or via a computer network, how to ensure that only authorized users can access the SQL Server instance. So security policy of the server layer is very important for the online system

4.1 Password complexity and expiration policy

The password policy ensure that all passwords are complex and changing passwords regularly for maximum security, prevent access without Identity verification, password policy shown in Figure 1. The password complexity policy prevent attacks by cracking the password after repeated trial. The new password must meet the policy requirements of Windows through enhancing the complexity of the password. The following are examples of password policy:

- The password does not contain all or part of the user's account name. Part of the account name is defined at both ends with a blank (space, Tab, Enter, etc.) three consecutive delimited or more letters, numbers, or a lower character, "-- ".
- The password should have at least seven characters.
- The password contains characters can be divided into the following four categories: English uppercase letters (A ~ Z), English lowercase letters (a ~ z), numbers 0 to 9, the non-character symbols (eg, ! 、 ¥ 、 #、 %)

Password expiration policy is used for the
management of the password validity period. When using a password expiration policy, the user will be reminded to change the old password and disable the use of an account with expired password.

4.2 User with complex password

When the WEB system deployed, it requires the user with appropriate privileges to access the system. These users log on the server with a Windows account, so a Windows logon name must be created specifically for these users. For example, members of the corporate sales department, first create specific local user groups SALES in the server’s "Computer Management", then add these users to join the group, and then create a new login name for the group and specify the user group has authority to access the system.

—Create a Windows login name SERVERX for SalesDBUsers, local Windows group

—Specify the default database my school create login [SERVERX$SalesDBUsers]FROM WINDOWS With default_database=myschool

—Create a SQL login name called the administrator

—password of Identity verification pa ¥¥ word, default database is my school

Create login administrator WITH PASSWORD='pa ¥¥ word’With default_database=myschool

Because Windows Server2003 may reach lockout Threshold due to several failed login attempts to prevent incorrect password attempts, which may lead to the immediate lock of the account. By simply setting check_expiration = off, then setting check_policy = on to reset the count of incorrect password. The following code is perform the unlock operation to a locked account.

Alter login administrator with password='newpa$wWord’ UNLOCK

4.3 Assign roles for those users

The enterprises create several new login name for employees as companies need to make employees responsible for different parts of the administration and they will not interfere with each other, therefore they need to assign roles for these logins, so that employees have different operating authority.

The easiest way to assign permissions is to assign roles to users' built-in database, because different built-in database roles are used to perform different operations, under normal circumstances, these roles match with enterprise employees to complete the tasks in association. For special employees, you can create a custom database roles with the appropriate permissions to complete his work.

For example: db_backupoperator could backup of the database role, db_datareader read data from any table, db_datawriter add, change, or delete data in any table. When the built-in database roles can not meet the demand, we can create our own defined database roles.

—Auditors Create a user-defined database role auditors

—Change the name of the role of auditors as purchasing

Use adventure works
Create role auditors
alter rol buyers with name = purchasing, go;

if the user does not have the appropriate permissions, users can not perform the require operation of the system, or the user can perform operations over allowed authority which would endanger the database safety, in short, you must assign the appropriate permissions to every user.

4.4 Add application roles and privileges

The companies have developed an online system, it performs data operations in a particular company database for the purpose of maintaining the database security, companies want employees could not manipulate data directly, their permission are limited in the application and then access the database through the application. In order to keep the system functioning properly, you need to create an application role for the online system.

When you create an application role, you must specify a password, and then use the password to activate the application role. After creating a character, you can also use sp_addrolemember, the stored procedure of system, to add a user as a member of the roles. The application roles enhance security in specific applications. The application role provide users safe access to the database with an alternate security context (means a group of user name and password).

——Create an application role called the weekly_receipts

——Use complex password protection

CREATE APPLICATION ROLE weekly_receipts
WITH PASSWORD = ’987Gbv876spyy5m23’

Create a character named weekly_receipts in the application and use complex password protection. The stored procedure of Sp_setapprole is used to activate an application role. Sp_setapprole only be performed by direct T_SQL statement and can not executed in another stored procedure or user-defined transaction. The following code is used to activate Sp_setapprole, the role of application weekly_receipts created before. Execsp_setapprole 'weekly_receipts', '987Gbv876spyy5m23' go

In the enterprise, operating authority for the database can not rely on the default permissions of the database itself, such as work features of supervisor and cashier in accounting does not match any of the characters in the built-in database. Then you need to assign permissions for each one.
The following code shows how to grant permissions for the supervisors.

Use adventure works GRANT ALTER ANY USER TO HR Manager GO

5 CONCLUSION

This article discusses safety analysis and design of the online system based on cloud computing to realize system security from three aspects: deploying HTTP endpoint security, key and certificate in the database layer, server security policy. The security level of the online system is high and the operation results were satisfactory, this design could serve as an example of similar online system to promote safety.

REFERENCES

[1] Lin Jing, Cai Lixin. SWOT analysis of online accounting services based on cloud computing. Friends of Accounting [J]. 2010 (2)