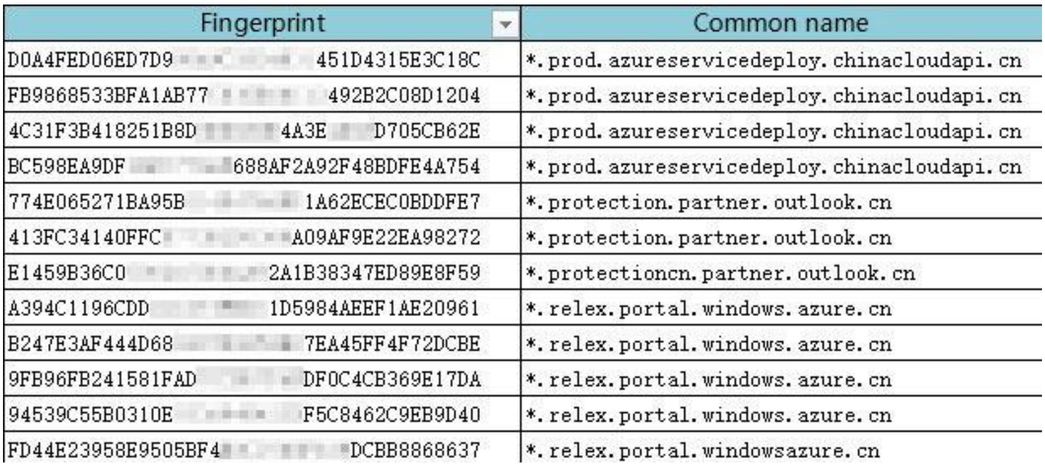
SSL certificate deployment must be "One machine, One certificate"

"One machine, One certificate" is a term created by the author, which means that each physical server must deploy an independent SSL certificate with an independent private key. It is easy to ignore or not thought of at times, but it is very important, so I think it is necessary to write a blog post about it.

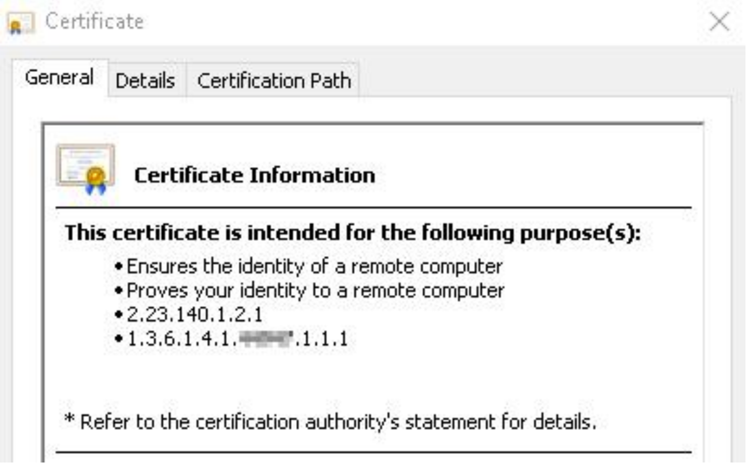
Users who have used SSL certificates know that SSL certificates have wildcard certificates and bind the domain name *.yourdomain.com, this certificate can be used for all subdomain websites, which is convenient for users to add new subdomain websites for https encryption. You can use this certificate to deploy immediately without having to apply for a new SSL certificate for a new subdomain from the CA.

Please look at the screenshot below. This is the SSL certificate application record of Microsoft cloud service Azure China. Why they apply for multiple certificates for the same wildcard domain name? Logically, only one wildcard certificate is needed! But why does Microsoft apply for SSL certificate like this? The author asked the person in charge of cloud security at Microsoft about this question. The answer gave me a lot of insight, so I would like to share it with you here.



Fingerprint	Common name
D0A4FED06ED7D9[redacted]451D4315E3C18C	*.prod.azureservicedeploy.chinacloudapi.cn
FB9868533BFA1AB77[redacted]492B2C08D1204	*.prod.azureservicedeploy.chinacloudapi.cn
4C31F3B418251B8D[redacted]4A3E[redacted]D705CB62E	*.prod.azureservicedeploy.chinacloudapi.cn
BC598EA9DF[redacted]688AF2A92F48BDFE4A754	*.prod.azureservicedeploy.chinacloudapi.cn
774E065271BA95B[redacted]1A62ECEC0BDDFE7	*.protection.partner.outlook.cn
413FC34140FFC[redacted]A09AF9E22EA98272	*.protection.partner.outlook.cn
E1459B36C0[redacted]2A1B38347ED89E8F59	*.protectioncn.partner.outlook.cn
A394C1196CDD[redacted]1D5984AEEF1AE20961	*.relex.portal.windows.azure.cn
B247E3AF444D68[redacted]7EA45FF4F72DCBE	*.relex.portal.windows.azure.cn
9FB96FB241581FAD[redacted]DF0C4CB369E17DA	*.relex.portal.windows.azure.cn
94539C55B0310E[redacted]F5C8462C9EB9D40	*.relex.portal.windows.azure.cn
FD44E23958E9505BF4[redacted]DCBB8868637	*.relex.portal.windowsazure.cn

As we all know, in order to comply with the China regulations, the servers of Microsoft China Cloud Service are hosted in the facility of 21Vianet, 21Vianet is responsible for the relevant management, so how to ensure that the identity of the server accessing the Microsoft cloud service system is authentic and trust? How to ensure that no illegal server connects to the Microsoft cloud service system? The answer is to configure an independent SSL certificate for each server connected to the cloud service system to prove the identity of the server and for encrypted communication between servers. Because the SSL certificate is not only used for encryption, one of the important functions is to prove its identity, which is why the following certificate purpose is displayed when you click to view the SSL certificate: Proves your identity to a remote computer, Ensures the identity of a remote computer, as shown in the figure below Show.



Certificate Information

This certificate is intended for the following purpose(s):

- Ensures the identity of a remote computer
- Proves your identity to a remote computer
- 2.23.140.1.2.1
- 1.3.6.1.4.1.[redacted].1.1.1

* Refer to the certification authority's statement for details.

"Proves your identity to a remote computer" means to prove the identity of the server. A remote computer refers to the computer used by the client. When the user (client) uses a browser to access this website, the browser will normally display the padlock after verifying the identity of the server to prove the validated identity of the website.

"Ensures the identity of a remote computer", a remote computer here refers to the server, which is reviewed at the user's computer. When the user communicates with the server using the browser, the server uses an SSL certificate to ensure its trusted identity.

"Remote computer" means that both parties are remote computers, which is not only suitable for the communication between the browser and the server, but also for the communication between the servers. The servers also need to use SSL certificates to prove their trusted identities.

Each server in the Microsoft cloud service system deploys an independent server certificate with a unique private key, even if it is the same domain name. This not only ensures the uniqueness of the server's identity (the unique fingerprint of the certificate, the unique private key), but more importantly, it is very convenient to manage when the certificate needs to be revoked, and a problem with one server will not affect other servers.

The important of "One machine, One certificate" is for secure operation and maintenance. For websites and business systems with big traffic, there must be multiple servers, and these servers need to deploy SSL certificates. The general practice is to deploy SSL certificates bound to the same domain name on all these servers, which not only saves SSL certificates cost (just buy one SSL certificate), and you can increase the number of servers simply by duplicating a server copy. However, there is a huge risk of certificate usage. If 100 servers deploy the same SSL certificate, if one of the servers is hacked or the private key of this SSL certificate is leaked, this SSL certificate must be revoked. This time the problem comes, you must re-apply for the certificate and redeploy the new certificate to these 100 servers, which is not only a huge workload, but also may affect the normal operation of the business.

If each server uses an independent SSL certificate, you only need to revoke the SSL certificate deployed by the server that may be leaked, and other servers using the same domain name do not need to do anything! This greatly reduces the operation and maintenance cost and improves the system security, because the operation and maintenance cost are much higher than purchasing an additional SSL certificate. So, the wisest choice is to buy a separate SSL certificate for each server instead of using the same certificate! Now, I believe readers can understand why Microsoft Cloud wants to apply for multiple certificates for the same domain name.

Readers may also ask: what is the use of applying for a wildcard certificate? The wildcard certificate is to use the same SSL certificate for website with multiple subdomains on one server, not to use this certificate on different servers, although it can be used on different servers.

Finally, for summary, the deployment of SSL certificates must be "One machine, One certificate". Each server uses an independent SSL certificate instead of a shared certificate. Although this deployment method increases the purchase cost of SSL certificates, but it is more expensive for the maintenance cost and business interruption. For business continues and system security, it is still cheaper for “One machine, One certificate” than the management cost of certificate revocation due to certificate leak and redeployment of certificate. The author strongly recommends that all websites must achieve "one machine, one certificate", instead of "losing watermelon and picking up sesame".

Richard Wang

Sept. 23, 2022
In Shenzhen, China