SSL 证书部署必须是“一机一证”？

“一机一证”是我自创的一个名词，意思是每一台物理服务器必须部署一张独立私钥的 SSL 证书，简称为“一机一证”，这个是目前所有网站在部署 SSL 证书时容易忽视或根本没有想到的安全问题，但是非常重要，所以，笔者认为有必要专门写一篇博文来讲这事。

用过 SSL 证书的用户都知道，SSL 证书有通配证书，绑定域名*.yourdomain.com，也就是说，这张证书可以用于所有子域名网站，方便用户需要增加新的子域名网站时可以使用此证书马上部署，而无需向 CA 申请新子域名的 SSL 证书。

请大家看一下下面的截图，这是微软云服务 Azure 中国的服务器 SSL 证书申请记录，同一个通配域名为何要同时申请多张？按道理，只需一张通配证书就可以了！那为何微软要这样申请证书？笔者就这个疑问询问了微软云安全负责人，他给出的解释让我大长见识，特在此分享给大家。

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

大家都知道，为了合规，微软中国云服务的服务器都是托管在世纪互联的机房，由世纪互联负责相关管理，那么如何保证接入微软云服务系统的服务器的身份真实可信呢？如何保证不会有非法服务器接入微软云服务系统？答案是给每台接入云服务系统的服务器都配置 SSL 证书来证明服务器的合法身份和用于服务器中间的加密通信。因为 SSL 证书不仅仅是用于加密，其中一个重要作用是证明其身份，这就是为何点击查看 SSL 证书时显示如下的证书目的：向远程计算机证明你的身份和保证远程计算机的身份，如下图所示。

“向远程计算机证明你的身份”意思是证明此服务器的身份，远程计算机是指用户使用的电脑，用户使用浏览器访问此网站时浏览器会在完成验证服务器的身份后正常显示“安全锁”标识。

“保证远程计算机的身份” 这里的远程计算机则是指服务器，是针对用户电脑讲的，用户在使用浏览器同服务器通信时，服务器使用 SSL 证书来保证其可信身份。

“远程计算机”指双方互为远程计算机，不仅仅适合于浏览器同服务器通信，也适合于服务器之间的通信，服务器之间也都需要用 SSL 证书来证明各自的可信身份。

微软云服务系统中每台服务器都部署一张私钥唯一的独立服务器证书，即使是同一域名，这样不仅能保证服务器身份的唯一性(证书唯一指纹、唯一私钥)，更重要的是在需要吊销证书时非常方便管理，一台服务器出现问题不会影响其他服务器。

这里我再详细解释一下“一机一证”对于安全运维有多重要。对于大访问量的网站和业务系统一定有多台服务器，这些服务器都需要部署 SSL 证书，一般的做法是把绑定同一个域名的 SSL 证书部署在所有这些服务器上使用，这不仅节省了 SSL 证书费用(只需买一张证书)，而且简单复制服务器拷贝即可增加服务器数量。但是，这里面存在一个巨大的证书使用风险，假如有 100 台服务器部署使用了同一张 SSL 证书，如果其中有一台服务器被黑或由于其他原因导致这张 SSL 证书私钥泄露，则必须吊销这张证书，这时候问题就来了，必须重新申请证书并把新证书重新部署到这 100 台服务器上，不仅工作量巨大，而且可能影响业务的正常运行。

而如果每台服务器都是使用一张独立的 SSL 证书的话，则只需吊销可能泄露的那台服务器部署的那张 SSL 证书即可，其他使用同一域名的服务器都不用动！这大大降低了运维成本和提升了系统安全，因为运维成本远比多购买一张 SSL 证书高。所以，最明智的选择是为**每一台服务器都单独购买一张 SSL 证书，而不是使用同一张证书！**现在，相信读者就能明白为何微软云要申请多张同一域名的证书的原因了吧。

读者也许还会问：那我申请通配证书有什么用？通配证书是为了在一台服务器上有多个子域名的网站系统能使用同一张 SSL 证书，而不是为了把这张证书用在不同的服务器上，虽然可以用在不同的服务器上。

最后总结一下：部署 SSL 证书必须是“一机一证”，每台服务器使用独立一张 SSL 证书，而

不是共用一张证书，这样的部署方式虽然增加了 SSL 证书的购买成本，但是相对于服务器的可信身份管理和因证书泄露而吊销证书重新部署证书的管理成本来讲，总的运维成本还是要低许多的，因为运维的人工成本和安全成本比一张 SSL 证书要贵很多！笔者在此强烈推荐所有网站都要做到“一机一证”，而不要“丢西瓜而捡芝麻”和“因小失大”！

王高华

2022 年 9 月 23 日于深圳

请关注公司公众号，实时推送公司 CEO 精彩博文。