一般情况下，如果我们没有为Azure Service Fabric开启群集安全证书功能，我们只需要将域名的DNS解析绑定到Service Fabric群集使用的负载均衡器对应的公网IP上即可。但对于开启了安全证书功能的群集，我们需要将证书和域名进行绑定，相对要麻烦一些。

**生成证书**

我们可以在CA申请自定义域名的可信证书，也可以使用自签名证书，无论哪种证书，我们都需要将证书使用者的名称和自定义域名保持一致。以下是使用Github上提供的[PowerShell模块](https://github.com/ChackDan/Service-Fabric/tree/master/Scripts/ServiceFabricRPHelpers)，可以借此快速生成证书，并上传至Key Vault。下载Github 代码后，将其解压，并执行以下命令导入PowerShell模块

Import-Module "C:\..\ServiceFabricRPHelpers\ServiceFabricRPHelpers.psm1"

此模块中提供Invoke-AddCertTokeyVault命令自动将证书的私钥格式设置为JSON字符串，并将它上传到密钥保管库，参考以下脚本。

$ResouceGroup = "kevin-group"

$VName = "kevinsfvault"

$SubID = "e0fbea86-6cf2-4b2d-81e2-9c59f4f96bcb"

$locationRegion = "chinanorth"

$newCertName = "aruicert"

$dnsName = "test.arui.me"

$localCertPath = "C:\"

Invoke-AddCertToKeyVault -SubscriptionId $SubID -ResourceGroupName $ResouceGroup -Location $locationRegion -VaultName $VName -CertificateName $newCertName -CreateSelfSignedCertificate -DnsName $dnsName -OutputPath $localCertPath

其中dnsName 必须和我们的自定义域名一致。

**设置域名解析**

我们需要创建一个静态公网IP，并将我们的自定义域名DNS解析到该IP之上，如下图，绑定DNS域名并解析至之前创建静态公网IP地址，以下是Aliyun示例，每个域名提供商的设置可能不一样，请参考各域名提供商的设置进行配置。

计算机生成了可选文字:
kevin-group 
中 王 北 部 
订 阅 《 
CIETest03 
订 豆 旧 
IP 址 
40 125 2 爵 97 
DNS 称 
kevln-ip chinanorth ℃ loudapp.chinacloudapi.cn 
已 关 到 

设置DNS域名解析

主 机 记 录 厶 
解 祈 线 路 〔 运 莒 商 〕 厶 
记 录 
40 ． 125 ． 207 ． 97 
温 生 示 
众 记 录 值 适 垣 写 您 服 器 IP 她 址 〔 鬯 须 力 IPv4 地 址 ， 0 ： 202 ． 105 ℃ ． 20 } 茜 不 适 P ， 适 您 咨 词 您 矿 河 服 商 。 
如 判 P 址 的 中 带 有 蓊 囗 ， 如 ． 202 彐 05n20 ： 8080 ， 则 只 添 加 202 ． 105n20 可 ． 

**使用用ARM 资源模板创建Service Fabric**

使用Azure Service Fabric 资源模板创建Service Fabric，在创建时，我们需要修改模板的一些地方，以确保整个群集都能够正常的使用自定义域名进行访问。

设置负载均衡器的前端IP

"frontendIPConfigurations": [

{

"name": "LoadBalancerIPConfig",

"properties": {

"publicIPAddress": {

"id": "[concat('/subscriptions/', subscription().subscriptionId, '/resourceGroups/', parameters('staticIpResourceGroups'), '/providers/Microsoft.Network/publicIPAddresses/', parameters('staticIpName'))]"

}

}

}

]

为群集配置安全证书，可参考[此文档](https://docs.microsoft.com/zh-cn/azure/service-fabric/service-fabric-cluster-creation-via-arm)进行设置，之后修改群集的Manager Endpoint设置，使其使用自定义域名访问群集。，此示例中的staticIpDnsFQDN指的是test.arui.me

"managementEndpoint": "[concat('https://',parameters('staticIpDnsFQDN'),':',parameters('nt0fabricHttpGatewayPort'))]"

配置好之后，就可以使用该模板创建Service Fabric。当创建完成时，就可以使用https://test.arui.me:19080，如下图：

C A Not secure 
Apps Bookmarks 
Microsoft Azure 
Tech 
Personlly 
Freelancer 
Stock 
Software 
21 via net 
0K 
A Waming 
Service Fabric Explorer 
@ Error 
Cluster https://test.arui.me 
Search Custer 
v Cluster 
> Applications 
> Nodes 
> System 
ESSENTIALS 
Custer Health State 
DETAILS 
CLU 
System Application Health State 
Healthy Seed Nodes 

**注意事项：**

如果创建时，虚拟机规模集创建完成，但Service Fabric群集还是处于等待节点状态。很有可能是因为Service Fabric客户端无法与虚拟机规模集中的群集系统服务进行通信。造成这样情况的原因大部分是因为证书的使用者名称和设置managementEndpoint地址不匹配。

**相关文档**

示例模板代码

<https://gist.github.com/chenrui1988/97ceed4d88cba3d74f3fc348f52348ba>

如何使用ARM模板创建安全Service Fabric

<https://docs.microsoft.com/zh-cn/azure/service-fabric/service-fabric-cluster-creation-via-arm>