**无法使用Azure AD连接到Service Fabric安全群集**

安全的群集是防止未经授权访问管理操作的群集，这些操作包括部署、升级和删除应用程序、服务及其包含的数据。

我们可以使用 Azure Resource Manager 在 Azure 中设置安全的 Azure Service Fabric 群集，在众多安全集群实现机制中，AAD (Azure Active Directory) 通过让组织(称为租户)管理和控制用户对应用程序的访问从而实现安全的身份验证。

我们今天主要讨论使用Azure AD去连接安全群集过程中遇到的问题。

**问题描述：**

当我们根据参考[文档](https://www.azure.cn/documentation/articles/service-fabric-cluster-creation-via-arm/) 成功创建完使用AAD的安全集群后， 通过PowerShell或者service fabric explore去连接集群时会遇到以下问题：

1. PowerShell连接失败，提示指定的凭证无效。

*Connect-ServiceFabricCluster -ConnectionEndpoint $ClusterConnectionEndpoint -serverCertThumbprint $PrimaryClusterKVThumbprint -AzureActiveDirectory -SecurityToken $accessToken*

*Connect-ServiceFabricCluster :* ***The specified credentials are invalid.***

*At line:1 char:1*

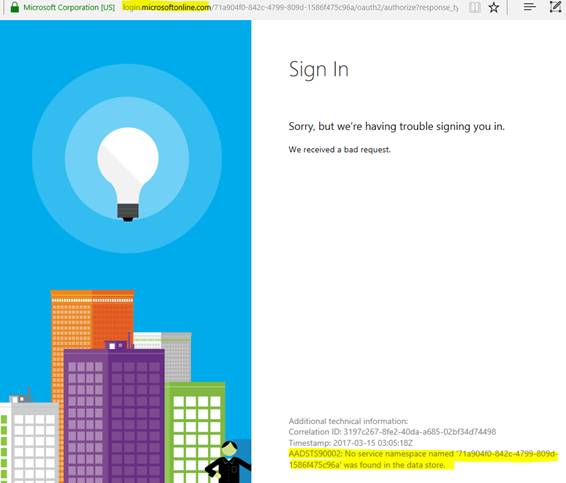
*+ Connect-ServiceFabricCluster -ConnectionEndpoint $ClusterConnectionEndpoint -ser ...*

*+ ~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~*

*+ CategoryInfo          : InvalidOperation: (:) [Connect-ServiceFabricCluster], FabricException*

*+ FullyQualifiedErrorId :*

1. 通过管理门户使用Service Fabric Explore访问时提示AADSTS90002错误，并且注意到跳转的url指向了login.microsoftonline.com。



**问题原因：**

正如前面提到的，由于AAD认证将中国的用户重定向到global的服务，而不是中国的服务（https://login.partner.microsoftonline.cn/），所以出现以上问题。

**解决方案：**

目前中国用户可以通过在ARM的部署模板中加入以下内容来指定中国AAD服务，从而解决该问题（在添加以下内容的过程中请注意JSON格式的验证）。

*"fabricSettings": [  
{  
"parameters": [  
{  
"name": "ClusterProtectionLevel",  
"value": "EncryptAndSign"  
},  
{  
"name": "AADLoginEndpoint",  
"value": "*[*https://login.partner.microsoftonline.cn*](https://na01.safelinks.protection.outlook.com/?url=https%3A%2F%2Flogin.partner.microsoftonline.cn&data=02%7C01%7Cwenche%40064d.mgd.microsoft.com%7Cd61727906af942388aa708d46d1b1e64%7C72f988bf86f141af91ab2d7cd011db47%7C1%7C0%7C636253410764913723&sdata=X86SBpCZVa%2FtlxtF1cgdMcyGom8DMzwaFIrez%2FOP1p0%3D&reserved=0)*"  
},  
{  
"name": "AADTokenEndpointFormat",  
"value": "*[*https://login.partner.microsoftonline.cn/{0}*](https://na01.safelinks.protection.outlook.com/?url=https%3A%2F%2Flogin.partner.microsoftonline.cn%2F%257b0%257d&data=02%7C01%7Cwenche%40064d.mgd.microsoft.com%7Cd61727906af942388aa708d46d1b1e64%7C72f988bf86f141af91ab2d7cd011db47%7C1%7C0%7C636253410764913723&sdata=UOwg3VAXz36%2Bof14ao67HbTPs1%2FW9lV5QeSecsirQis%3D&reserved=0)*"  
},  
{  
"name": "AADCertEndpointFormat",  
"value": "*[*https://login.partner.microsoftonline.cn/{0}/federationmetadata/2007-06/federationmetadata.xml*](https://na01.safelinks.protection.outlook.com/?url=https%3A%2F%2Flogin.partner.microsoftonline.cn%2F%257b0%257d%2Ffederationmetadata%2F2007-06%2Ffederationmetadata.xml&data=02%7C01%7Cwenche%40064d.mgd.microsoft.com%7Cd61727906af942388aa708d46d1b1e64%7C72f988bf86f141af91ab2d7cd011db47%7C1%7C0%7C636253410764913723&sdata=g3shZXYzGx0DXgx%2BjPlQRBulpjqqRjCsAfn%2BNQaQTyI%3D&reserved=0)*"  
}  
],  
"name": "Security"  
}*

另外该问题已经在global版本的5.4 CU3及以上版本修复，中国也将会在后续上线修复后的版本 ，届时问题将会得到根本解决。