Azure

Azure 连接概述

准备 Azure 环境以供 多云防御控制器 使用时，假定您已拥有订用，并且该订用已关联到 Azure Active Directory。

Azure 订用的脚本化连接 多云防御控制器

将 Azure 订用连接到 多云防御控制器 的最佳方式是关注 从 多云防御 控制面板将 Azure 订用连接到 多云防御控制器], on page 4。此激活向导使用脚本来简化连接过程。该脚本提供使用向导将 Azure 订用连接到 多云防御 所需的所有信息。

如果您发现无法使用自动化脚本，请参阅 Azure 的手动激活选项 的高级程序。

Azure 的手动激活选项

如果您无法使用 多云防御控制器 控制面板中提供的脚本直接连接 Azure 订用，请使用下面的工作流程手动连接您的订用：

1. 在 Active Directory 中注册应用。
2. 创建要分配给应用的自定义角色， 第 2 页。
3. 手动将角色分配给应用。
4. （可选）用户分配的用于 Key Vault 和 Blob 存储访问的托管身份， 第 2 页。
5. 接受市场条款， 第 4 页。

（可选）用户分配的用于 Key Vault 和 Blob 存储访问的托管身份

多云防御网关可以选择性地与 Azure Key Vault 集成以检索 TLS 证书，并与 Blob 存储集成以保存 PCAP（数据包捕获）文件。用户分配的托管身份用于授予对这些服务的访问权限。

在 Azure 门户中，导航到 **托管身份** 以创建身份。

或者，在 Azure Cloud Shell 中运行以下命令：

```
az identity create -g <RESOURCE GROUP> -n <USER ASSIGNED IDENTITY NAME>
```

有关在 Azure Key Vault 中创建 TLS 证书密钥的信息，请参阅 Azure Key Vault。

在 Active Directory 中注册应用

步骤 1 导航至 **Azure Active Directory**。

步骤 2 选择 **应用注册**。

步骤 3 点击 **新注册**。

步骤 4 提供一个名称以引用新应用注册，例如 多云防御控制器 在 支持的账户类型 中，选择第二个选项 任意组织目录中的账户。

步骤 5 选择适合您的组织的选项。请注意，创建应用注册不需要 **重定向 URI** 。

步骤 6 点击**注册 (Register)**。

步骤 7 在新创建的应用下的左侧导航栏中，点击 **证书和密钥**。

步骤 8 点击 **+ 新客户端密钥**，然后在 添加客户端密钥 对话框中输入所需信息

- **说明** - 添加说明（例如 多云防御-controller-secret1）
- **到期** - 选择 **从不**。您也可以在方便时进行此选择。当当前密钥到期时，您需要创建新密钥）

步骤 9 点击**添加 (Add)**。客户端密钥填充在 **值** 列下。

步骤 10 将 **客户端密钥** 复制到记事本中，因为它只显示一次，永远不会再次显示。

步骤 11 在左侧导航栏中，点击 **概述**。

步骤 12 将 **应用（客户端）ID** 和 **目录（租户）ID** 复制到记事本中。

创建要分配给应用的自定义角色

创建将分配给为 多云防御控制器创建的应用的 **自定义角色** 。自定义角色为应用提供读取资产信息和创建资源（例如，VM、负载均衡器等）的权限。可以通过多种方式创建自定义角色。

步骤 1 导航至 **订用** ，然后点击 **访问控制 (IAM)**。

步骤 2 点击 **角色** ，然后导航至顶部菜单栏，点击 **+添加** > **添加自定义角色**。

步骤 3 为自定义角色命名（例如， `多云防御-controller-role`）。

步骤 4 继续点击 **下一步** ，直到进入 JSON 编辑屏幕。

步骤 5 点击屏幕上的 **编辑**，在 JSON 文本的 **权限 > 操作** 部分下，将以下内容复制并粘贴到方括号之间（无需保持缩进）：

```
"Microsoft.ApiManagement/service/*",
"Microsoft.Compute/disks/*",
"Microsoft.Compute/diskEncryptionSets/read",
"Microsoft.Compute/images/read",
"Microsoft.Compute/sshPublicKeys/read",
"Microsoft.Compute/virtualMachines/*",
"Microsoft.ManagedIdentity/userAssignedIdentities/read",
"Microsoft.ManagedIdentity/userAssignedIdentities/assign/action",
"Microsoft.Network/loadBalancers/*",
"Microsoft.Network/locations/serviceTags/read",
"Microsoft.Network/networkinterfaces/*",
"Microsoft.Network/networkSecurityGroups/*",
"Microsoft.Network/publicIPAddresses/*",
"Microsoft.Network/routeTables/*",
"Microsoft.Network/virtualNetworks/*",
"Microsoft.Resources/subscriptions/resourcegroups/*",
"Microsoft.Storage/storageAccounts/blobServices/*",
"Microsoft.Storage/storageAccounts/listkeys/action",
"Microsoft.Network/networkWatchers/*",
"Microsoft.Network/applicationSecurityGroups/*",
"Microsoft.Compute/diskEncryptionSets/read",
"Microsoft.Insights/Metrics/Read"
```

步骤 6 **可选** - 如果您计划通过 多云防御使用多个订用，则必须在 `assignableScopes` 处编辑 JSON 以添加另一个订用行或将其更改为 ***** （星号），以便所有订用均可使用自定义角色。

步骤 7 点击文本框顶部的 **保存**。

步骤 8 点击 **查看 + 创建** 并创建角色。

步骤 9 创建自定义角色后，请返回 **访问控制 (IAM)**。

步骤 10 点击 **添加** > **添加角色分配**。

步骤 11 在 **角色** 下拉列表中，选择上面创建的自定义角色。

步骤 12 在 **将访问权限分配给** 下拉列表中，将其保留为默认值（Azure AD 用户、组、服务主体）。

步骤 13 在 **选择** 文本框中，输入之前创建的应用的名称（例如 `多云防御controllerapp`），然后点击 **保存**。

步骤 14 在 **订用** 页面中，点击左侧菜单栏中的 **概述**，然后将订用 ID 复制到记事本。

多云防御控制器 激活所需的值

在继续之前，请确保您拥有以下信息：

- 订用 ID（来自订用概述页面）
- 目录（租户）ID（来自 *Azure AD* 应用概述页面）
- 应用（客户端）ID（来自 *Azure AD* 应用概述页面）
- 客户端密钥（创建客户端密钥时复制）

接受市场条款

多云防御控制器 使用来自 Azure 市场的 多云防御 虚拟机 (VM) 映像创建网关实例。必须接受每个订用的条款和条件。从 Azure 门户网站（位于顶部菜单栏右侧）打开 Azure 云外壳。选择或切换到 bash shell 并执行以下命令（将 subscription-id 替换为上一部分中复制的订用 ID）：

```
az vm image terms accept --publisher valtix --offer datapath --plan valtix_dp_image
--subscription subscription-id
```

从多云防御控制面板将 Azure 订用连接到多云防御控制器]

按照前面部分所述准备好 Azure 账户和订用后，即可将其链接到 多云防御控制器。

步骤 1 在 CDO 菜单栏上，点击 多云防御。

步骤 2 点击 多云防御控制器 按钮。

步骤 3 在云账户窗格中，点击 **添加账户**。

步骤 4 在常规信息页面上，从 **账户类型** 列表框中选择 Azure。

步骤 5 在步骤 1 中，点击链接以 bash 模式打开 Azure 云外壳。

步骤 6 在步骤 2，点击 **复制** 按钮。

步骤 7 在 bash shell 中运行自行激活脚本。

Note

- 如果有另一个 Azure 订用已连接到 多云防御，则在创建具有相同现有名称的 IAM 角色时，此脚本可能会失败。不能有多个 IAM 角色。解决方法是运行带有 `-p` 前缀的 Bash 脚本。
- 要支持跨订用的分支 VNet 保护，请使用 Active Directory 应用注册自行激活订用。

步骤 8 提供此 Azure 账户的名称。您可以选择将其命名为与您的 Azure 订用相同的名称。此名称仅在 多云防御控制器 账户页面上可见。

步骤 9 （可选）提供订用说明。

步骤 10 输入 **目录 ID**，也称为租户 ID。

步骤 11 输入要激活的订用的订用 **ID** 。

步骤 12 输入由自行激活脚本创建的 **应用 ID**（也称为客户端 ID）。

步骤 13 输入 **客户端密钥**，也称为密钥 ID。

步骤 14 点击**保存并继续**。

Azure 订用已激活，您将返回到控制面板，以查看新设备是否已添加。

What to do next

- 激活后程序, on page 5。

- 启用流量可视性。

由 多云防御创建的角色

当您使用提供的脚本将云服务账户载入多云防御控制器时，系统会在云服务提供商的参数中创建用户角色，以确保服务之间的通信受到保护。根据云服务提供商，创建不同的角色和权限。

当您载入账户时，系统会创建以下角色。

Azure IAM 角色

本文档介绍上一部分中使用的 CloudFormation 模板创建的 IAM 角色的详细信息。

CloudFormation 模板创建以下角色：

- **自定义角色** - 自定义角色为应用提供读取资产信息和创建资源（例如，VM、负载均衡器等）的权限。可以通过多种方式创建自定义角色。

激活后程序

-

子网

配置网关部署时， 多云防御控制器 将提示您输入 **管理** 和 **数据路径** 子网信息。

管理 子网是必须与具有互联网默认路由的路由表关联的公共子网。 多云防御网关 实例具有连接到此子网的接口，用于与 多云防御控制器通信。此接口用于 多云防御控制器 和 多云防御网关 实例之间的策略推送以及其他管理和遥测活动。客户应用流量 **不** 流经此接口和子网。该接口与**管理** 安全组相关联，如下面的“安全组”部分所述。

数据路径 子网是必须与具有互联网默认路由的路由表关联的公共子网。 多云防御控制器 在此子网中创建网络负载均衡器 (NLB)。此外， 多云防御网关 实例具有连接到此子网的接口。客户应用流量 **流经** 此接口。安全策略应用于通过此接口的流量入口。接口与 **数据路径** 安全组相关联，如安全组部分所述。

Azure VNet 设置

本文档介绍要在 VNet 中创建的要求和资源（子网、安全组），以便在 VNet 中创建 多云防御网关。

安全组

管理和数据路径安全组与 多云防御网关 实例上的相应接口关联，如上面的子网部分所述。

管理 安全组必须允许允许网关实例与控制器通信的出站流量。或者，对于入站规则，启用端口 22 (SSH) 以允许对网关实例进行 SSH 访问。要使 多云防御网关 正常运行，并非必须使用 SSH。

数据路径 安全组连接到数据路径接口，并允许从互联网到 多云防御网关的流量。目前， 多云防御控制器 不管理此安全组。必须存在出站规则，允许流量传出此接口。必须为 多云防御控制器 安全策略中配置并由 多云防御网关使用的每个端口打开入站端口。

例如，如果应用在端口 3000 上运行，并由端口 443 上的 多云防御网关 代理，则必须在数据路径安全组上打开端口 443。此示例还意味着连接到应用的安全组上的端口 3000 已打开。

ARM 模板

使用 ARM 模板 https://valtix-public.s3.amazonaws.com/azure-rm/datapath.json 创建此页面上所述的所有资源。

此模板创建新的 VNet。这对于在不涉及现有生产环境的情况下开始使用 多云防御 非常有用。

该模板将创建以下资源：

- vNET
- 管理子网
- 数据路径子网
- 使用出站规则管理安全组
- 具有端口 443 的出站规则和入站规则的数据路径安全组

您可以根据需要创建其他子网来运行应用并创建应用特定的安全组。

启动 ARM 模板

使用以下步骤启动 ARM 模板：

步骤 1 搜索在 Azure 门户中 **部署自定义模板** 或 点击此处。
步骤 2 点击 **在编辑器中生成自己的模板**。
步骤 3 从 ARM 模板复制内容并粘贴到编辑器中。
步骤 4 点击**保存**。
步骤 5 选择 订用、 资源组和 区域。
步骤 6 点击 **查看+创建**。
步骤 7 等待几分钟，以便创建所有资源。

当地语言翻译版本说明

思科可能会在某些地方提供本内容的当地语言翻译版本。请注意，翻译版本仅供参考，如有任何不一致之处，以本内容的英文版本为准。