Azure

Azure 연결 개요

멀티 클라우드 방어 컨트롤러에서 사용할 Azure 환경을 준비하려면 이미 구독이 있고 구독이 Azure Active Directory에 연결되어 있다고 가정합니다.

Azure 구독을 멀티 클라우드 방어 컨트롤러에 스크립트로 연결

Azure 구독을 멀티 클라우드 방어 컨트롤러에 연결하는 가장 좋은 방법은 다음 멀티 클라우드 방어 대시보드에서 멀티 클라우드 방어 컨트롤러에 Azure 구독 연결, on page 4을(를) 수행하는 것입니다. 이 온보딩 마법사는 스크립트를 사용하여 연결 프로세스를 간소화합니다. 스크립트는 마법사를 사용하여 Azure 구독을 멀티 클라우드 방어에 연결하는 데 필요한 모든 정보를 제공합니다.

자동화된 스크립트를 사용할 수 없는 경우 Azure용 수동 온보딩 옵션 에 있는 고급 절차를 참조하십시오.

Azure용 수동 온보딩 옵션

멀티 클라우드 방어 컨트롤러 대시보드에서 제공되는 스크립트를 사용하여 Azure 구독을 직접 연결할 수 없는 경우 아래 워크플로우를 사용하여 구독을 수동으로 연결합니다.

1. Azure Active Directory에 애플리케이션 등록.
2. 애플리케이션에 할당할 사용자 지정 역할 생성, 2 페이지.
3. 애플리케이션에 역할을 수동으로 할당합니다.
4. (선택 사항) 키 저장소 및 Blob 저장소 액세스를 위해 사용자가 할당하는 관리 ID, 2 페이지.
5. 마켓플레이스 약관 동의, 4 페이지.

(선택 사항) 키 저장소 및 Blob 저장소 액세스를 위해 사용자가 할당하는 관리 ID

멀티 클라우드 방어 게이트웨이은(는) 선택적으로 Azure 키 저장소와 통합하여 TLS 인증서를 검색하고, PCAP(패킷 캡처) 파일을 저장하기 위해 Blob 저장소와 통합할 수 있습니다. 사용자가 할당하는 관리형 ID는 이러한 서비스에 대한 액세스 권한을 부여하는 데 사용됩니다.

Azure Portal에서 **Managed Identities(**관리되는 **ID)**로 이동하여 ID를 생성합니다.

또는 Azure Cloud Shell에서 다음 명령을 실행합니다.

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

Azure 키 저장소에서 TLS 인증서 암호를 생성하는 방법에 대한 자세한 내용은 Azure 키 저장소의 내용을 참조하십시오.

Azure Active Directory에 애플리케이션 등록

단계 **1** **Azure Active Directory**로 이동합니다.

단계 **2** **App registrations(**앱 등록**)**를 선택합니다.

단계 **3** **New registration(**새 등록**)**을 클릭합니다.

단계 **4** 새 앱 등록을 참조할 이름을 제공합니다. 예를 들어 멀티 클라우드 방어 컨트롤러. *Supported account types(*지원되는 계정 유형*)*에서 두 번째 옵션인 *Accounts in any organizational directory(*조직 디렉터리의 계정*)*를 선택합니다.

단계 **5** 조직에 적절한 옵션을 선택합니다. **Redirect URI(**리디렉션 **URI)**는 앱 등록을 생성하는 데 필요하지 않습니다.

단계 **6** **Register(**등록**)**를 클릭합니다.

단계 **7** 새로 생성된 애플리케이션 아래의 왼쪽 탐색 모음에서 **Certificates and secrets(**인증서 및 암호**)**를 클릭합니다.

단계 **8** **+ New client secret(+** 새 클라이언트 비밀번호**)**를 클릭한 다음 *Add client secret(*클라이언트 비밀번호 추가*)* 대화 상자에 필요한 정보를 입력합니다.

- **Description(**설명**)**- 설명을 추가합니다(예: 멀티 클라우드 방어-controller-secret1).
- **Expires(**만료**) - Never(**안 함**)**를 선택합니다. 또한 편의에 따라 선택할 수 있습니다. 현재 암호가 만료되면 새 암호를 생성해야 함)를 선택합니다.

단계 **9** **Add(**추가**)**를 클릭합니다. 클라이언트 비밀이 **Value(**값**)** 열에 채워집니다.

단계 **10** 클라이언트 비밀은 한 번만 표시되고 다시 표시되지 않으므로 메모장에 복사합니다.

단계 **11** 왼쪽 내비게이션 바에서 **Overview(**개요**)**를 클릭합니다.

단계 **12** 애플리케이션**(**클라이언트**) ID** 및 디렉터리**(**테넌트**) ID**를 메모장에 복사합니다.

애플리케이션에 할당할 사용자 지정 역할 생성

멀티 클라우드 방어 컨트롤러을(를) 위해 생성된 애플리케이션에 할당할 맞춤형 역할을 생성합니다. 사용자 지정 역할은 재고 목록 정보를 읽고 리소스(예: VM, 로드 밸런서 등)를 생성할 수 있는 애플리케이션 권한을 제공합니다. 사용자 지정 역할은 여러 방법으로 생성할 수 있습니다.

단계 **1** **Subscription(**구독**)**으로 이동하여 **Access Control (IAM)(**액세스 제어**(IAM))**을 클릭합니다.

단계 **2** **Roles(**역할**)**를 클릭하고 상단 메뉴 모음에서 **+Add(+**추가 **)** > **Add Custom Role(**맞춤형 역할 추가**)**로 이동하여 클릭합니다.

단계 **3** 맞춤형 역할에 이름을 지정합니다(예: `멀티 클라우드 방어-controller-role`).

단계 **4** JSON 편집 화면이 표시될 때까지 **Next(**다음**)**를 계속 클릭합니다.

단계 **5** 화면에서 **Edit(**편집**)**를 클릭하고 JSON 텍스트에서 **permissions(**권한**) > Action(**작업**)** 섹션 아래의 다음 내용을 복사하여 대괄호 사이에 붙여넣습니다(들여쓰기는 유지할 필요 없음).

```
"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"
```

단계 **6** 선택 사항 - 여러 구독을 멀티 클라우드 방어과(와) 함께 사용하려는 경우 `assignableScopes`에서 JSON을 편집하여 다른 구독 라인을 추가하거나 모든 구독에 사용자 지정 역할을 사용할 수 있도록 *****(별표)로 변경해야 합니다.

단계 **7** 텍스트 상자 맨 위에서 **Save(**저장**)**를 클릭합니다.

단계 **8** **Review + Create(**검토 **+** 생성**)**를 클릭하고 역할을 생성합니다.

단계 **9** Custom Role(사용자 지정 역할)이 생성되면 **Access Control(IAM)(**액세스 제어**(IAM))**으로 돌아갑니다.

단계 **10** 상단 메뉴 모음에서 **Add(**추가**)** > **Add role assignment(**역할 할당 추가**)**를 클릭합니다.

단계 **11** **Role(**역할**)** 드롭다운에서 위에서 생성한 Custom Role(사용자 지정 역할)을 선택합니다.

단계 **12** **Assign access to(**액세스 권한 할당 대상**)** 드롭다운에서 이를 기본값(Azure AD 사용자, 그룹, 서비스 주체)으로 유지합니다.

단계 **13** **Select(**선택**)** 텍스트 상자에 이전에 생성한 애플리케이션 이름(예: `멀티 클라우드 방어controllerapp`)을 입력하고 **Save(**저장**)**를 클릭합니다.

단계 **14** **Subscription(**구독**)** 페이지의 왼쪽 메뉴 모음에서 **Overview(**개요**)**를 클릭하고 구독 ID를 메모장에 복사합니다.

멀티 클라우드 방어 컨트롤러 온보딩에 필요한 값

계속 진행하기 전에 다음 정보가 있는지 확인하십시오.

- 구독 ID(*subscription overview(*구독 개요*)* 페이지)
- 디렉터리(테넌트) ID(*Azure AD app overview(Azure AD* 앱 개요*)* 페이지)
- 애플리케이션(클라이언트) ID(*Azure AD app overview(Azure AD* 앱 개요*)* 페이지)
- 클라이언트 암호(클라이언트 암호 생성 시 복사됨)

마켓플레이스 약관 동의

멀티 클라우드 방어 컨트롤러은(는) Azure Marketplace에서 멀티 클라우드 방어 VM(가상 머신) 이미지를 사용하여 게이트웨이 인스턴스를 생성합니다. 각 구독에 대해 약관에 동의해야 합니다. Azure 포털 웹사이트(오른쪽 상단 메뉴 모음)에서 Azure Cloud 쉘을 엽니다. Bash 쉘을 선택하거나 전환하고 다음 명령을 실행합니다(subscription-id를 이전 섹션에서 복사한 구독 ID로 대체).

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

멀티 클라우드 방어 대시보드에서 멀티 클라우드 방어 컨트롤러에 **Azure** 구독 연결

이전 섹션에서 설명한 대로 Azure 계정 및 구독을 준비했으면 멀티 클라우드 방어 컨트롤러에 연결할 수 있습니다.

단계 **1** CDO 메뉴 바에서 멀티 클라우드 방어을(를) 클릭합니다.

단계 **2** 멀티 클라우드 방어 컨트롤러 버튼을 클릭합니다.

단계 **3** Cloud Accounts(클라우드 계정) 창에서 **Add Account(**계정 추가**)**를 클릭합니다.

단계 **4** General Information(일반 정보) 페이지에 있는 **Account Type(**계정 유형**)** 목록 상자에서 Azure를 선택합니다.

단계 **5** 1단계에서 링크를 클릭하여 Bash 모드에서 Azure Cloud Shell을 엽니다.

단계 **6** 2단계에서 **Copy(**복사**)** 버튼을 클릭합니다.

단계 **7** Bash 셸에서 온보딩 스크립트를 실행합니다.

Note

- 멀티 클라우드 방어에 이미 연결된 다른 Azure 구독이 있는 경우 동일한 기존 이름으로 IAM 역할을 생성하면 이 스크립트가 실패할 수 있습니다. IAM 역할은 둘 이상 있을 수 없습니다. 이 문제를 해결하려면 `-p` 접두사를 사용하여 Bash 스크립트를 실행합니다.
- 구독 전반에서 스포크 VNet 보호를 지원하려면 Active Directory 앱 등록을 사용하여 구독을 온보딩해야 합니다.

단계 **8** 이 Azure 계정의 이름을 제공합니다. 이 이름은 Azure 구독 이름과 동일하게 지정할 수 있습니다. 이 이름은 멀티 클라우드 방어 컨트롤러 계정 페이지에만 표시됩니다.

단계 **9** (선택 사항) 구독에 대한 설명을 제공합니다.

단계 **10** 테넌트 ID라고도 하는 디렉터리 **ID**를 입력합니다.

단계 **11** 온보딩 중인 구독의 구독 **ID**를 입력합니다.
단계 **12** 온보딩 스크립트에서 생성한 애플리케이션 **ID**(클라이언트 ID라고도 함)를 입력합니다.
단계 **13** **Client Secret(**클라이언트 암호**)**(암호 ID라고도 함)을 입력합니다.
단계 **14** **Save & Continue(**저장 후 계속**)**를 클릭합니다.

Azure 구독이 온보딩되고 새 디바이스가 추가된 것을 확인하기 위해 대시보드로 다시 연결되었습니다.

What to do next

- 사후 온보딩 절차, on page 5.
- 트래픽 가시성을 활성화합니다.

역할 생성자: 멀티 클라우드 방어

제공된 스크립트를 사용하여 클라우드 서비스 계정을 멀티 클라우드 방어 컨트롤러에 온보딩할 경우 서비스 간 통신이 보호되도록 클라우드 서비스 제공자의 매개변수 내에서 사용자 역할이 생성됩니다. 클라우드 서비스 제공자에 따라 서로 다른 역할 및 권한이 생성됩니다.

계정을 온보딩할 때 다음 역할이 생성됩니다.

Azure IAM 역할

이 문서에서는 이전 섹션에서 사용된 CloudFormation 템플릿으로 생성된 IAM 역할에 대해 자세히 설명합니다.

CloudFormation 템플릿은 다음 역할을 생성합니다.

- **Custom Role(**사용자 지정 역할**)** - 사용자 지정 역할은 재고 목록 정보를 읽고 리소스(예: VM, 로드 밸런서 등)를 생성할 수 있는 애플리케이션 권한을 제공합니다. 사용자 지정 역할은 여러 방법으로 생성할 수 있습니다.

사후 온보딩 절차

-

서브넷

게이트웨이 구축을 구성할 때 멀티 클라우드 방어 컨트롤러에서 관리 및 데이터 경로서브넷 정보를 입력하라는 메시지가 표시됩니다.

관리 서브넷은 인터넷에 대한 기본 경로가 있는 라우트 테이블과 연결해야 하는 퍼블릭 서브넷입니다. 멀티 클라우드 방어 게이트웨이 인스턴스에 멀티 클라우드 방어 컨트롤러과(와)의 통신에 사용하는 이 서브넷에 연결된 인터페이스가 있습니다. 이 인터페이스는 멀티 클라우드 방어 컨트롤러 및 멀

티 클라우드 방어 게이트웨이 인스턴스 간의 정책 푸시와 기타 관리, 텔레메트리 활동에 사용됩니다. 고객 애플리케이션 트래픽은 이 인터페이스 및 서브넷을 통과하지 않습니다. 아래의 보안 그룹 섹션에서 설명하는 관리 보안 그룹과 인터페이스가 연결됩니다.

데이터 경로 서브넷은 인터넷에 대한 기본 경로가 있는 라우트 테이블과 연결해야 하는 퍼블릭 서브넷입니다. 멀티 클라우드 방어 컨트롤러은(는) 이 서브넷에 네트워크 로드 밸런서(NLB)를 생성합니다. 또한, 멀티 클라우드 방어 게이트웨이 인스턴스에 이 서브넷에 연결된 인터페이스가 있습니다. 고객 애플리케이션 트래픽은 이 인터페이스를 통해 흐릅니다. 보안 정책은 이 인터페이스를 통해 트래픽 인그레스에 적용됩니다. 인터페이스는 보안 그룹 섹션에서 설명하는 데이터 경로 보안 그룹과 연결됩니다.

Azure VNet 설정

이 문서에서는 VNet에서 멀티 클라우드 방어 게이트웨이을(를) 생성할 수 있도록 VNet에서 생성해야 하는 요구 사항 및 리소스(서브넷, 보안 그룹)에 대해 설명합니다.

보안 그룹

관리 및 데이터 경로 보안 그룹은 위의 서브넷 섹션에서 설명한 대로 멀티 클라우드 방어 게이트웨이 인스턴스의 각 인터페이스와 연결됩니다.

관리 보안 그룹은 게이트웨이 인스턴스가 컨트롤러와 통신하도록 허용하는 아웃바운드 트래픽을 허용해야 합니다. 선택적으로, 인바운드 규칙의 경우 포트 22(SSH)를 활성화하여 게이트웨이 인스턴스에 대한 SSH 액세스를 허용합니다. 멀티 클라우드 방어 게이트웨이이(가) 제대로 작동하기 위해 SSH가 반드시 필요한 것은 아닙니다.

데이터 경로 보안 그룹은 데이터 경로 인터페이스에 연결되며 인터넷에서 멀티 클라우드 방어 게이트웨이(으)로의 트래픽을 허용합니다. 현재 멀티 클라우드 방어 컨트롤러은(는) 보안 그룹을 관리하지 않습니다. 이 인터페이스의 트래픽 이그레스를 허용하는 아웃바운드 규칙이 있어야 합니다. 인바운드 포트는 멀티 클라우드 방어 컨트롤러 보안 정책에 구성되어 있고 멀티 클라우드 방어 게이트웨이에서 사용하는 각 포트에 대해 열려 있어야 합니다.

예를 들어 애플리케이션이 포트 3000에서 실행 중이고 포트 443의 멀티 클라우드 방어 게이트웨이에서 프록시되는 경우, 데이터 경로 보안 그룹에서 포트 443을 열어야 합니다. 또한 이 예시는 애플리케이션에 연결된 보안 그룹에서 포트 3000이 열려 있음을 의미합니다.

ARM 템플릿

ARM 템플릿 https://valtix-public.s3.amazonaws.com/azure-rm/datapath.json을(를) 사용하여 이 페이지에서 설명하는 모든 리소스를 생성합니다.

이 템플릿은 새 VNet을 생성합니다. 기존 프로덕션 환경을 터치하지 않고 멀티 클라우드 방어을(를) 시작할 때 매우 유용합니다.

템플릿은 다음 리소스를 생성합니다.

- Vnet

- 관리 서브넷
- 데이터 경로 서브넷
- 아웃바운드 규칙이 있는 관리 보안 그룹
- 포트 443에 대한 아웃바운드 규칙 및 인바운드 규칙이 있는 데이터 경로 보안 그룹

필요에 따라 추가 서브넷을 생성하여 앱을 실행하고 앱별 보안 그룹을 생성할 수 있습니다.

ARM 템플릿 실행

ARM 템플릿을 실행하려면 다음 단계를 수행합니다.

단계 **1** Azure 포털에서 사용자 지정 템플릿 구축을 검색하거나 여기를 클릭합니다.
단계 **2** **Build your own template in the editor(**편집기에서 자체 템플릿 구축**)**를 클릭합니다.
단계 **3** ARM 템플릿의 내용을 복사하여 편집기에 붙여넣습니다.
단계 **4** **Save(**저장**)**를 클릭합니다.
단계 **5** *Subscription(*구독*)*, *Resource group(*리소스 그룹*)* 및 *Region(*지역*)*을 선택합니다.
단계 **6** **Review+ Create(**검토+ 생성**)**를 클릭합니다.
단계 **7** 모든 리소스가 생성될 때까지 몇 분 정도 기다립니다.