Google Cloud Platform에 ASA 가상 구축

GCP(Google Cloud Platform)에서 ASA 가상을 구축할 수 있습니다.

GCP의 ASA 가상 구축 정보

GCP를 사용하면 Google과 동일한 인프라에서 애플리케이션, 웹사이트 및 서비스를 빌드, 구축 및 확장할 수 있습니다.

ASA 가상은 물리적 ASA 와 동일한 소프트웨어를 실행하여 가상 폼 팩터에서 검증된 보안 기능을 제공합니다. ASA 가상은 퍼블릭 GCP에서 구축될 수 있습니다. 그러면 시간이 경과함에 따라 해당 위치를 확장, 축소 또는 이동하는 가상 및 물리적 데이터 센터 워크로드를 보호하기 위한 구성이 가능하게 됩니다.

GCP 시스템 유형 지원

ASA 가상 필요에 따라 Google 가상 머신 유형 및 크기를 선택합니다.

ASA 가상에서는 다음 범용 *N1, N2* 및 컴퓨팅 최적화 *C2* GCP 머신 유형을 지원합니다.

표 *1:* 지원되는 컴퓨팅 최적화 시스템 유형

컴퓨팅 최적화 시스템 유형	속성	
	vCPUs	메모리**(GB)**
c2-standard-4	4	16
c2-standard-8	8	32

컴퓨팅 최적화 시스템 유형	속성	
	vCPUs	메모리**(GB)**
c2-standard-16	16	64

표 *2:* 지원되는 범용 시스템 유형

머신 유형	속성	
	vCPUs	메모리**(GB)**
n1-standard-4	4	15
n1-standard-8	8	30
n1-standard-16	16	60
n2-standard-4	4	16
n2-standard-8	8	32
n2-standard-16	16	64
n1-highcpu-8	8	7.2
n1-highcpu-16	16	14.4
n2-highcpu-8	8	8
n2-highcpu-16	16	16
n2-highmem-4	4	32
n2-highmem-8	8	64
n2-highmem-16	16	128

- ASA 가상에는 최소 3 개의 인터페이스가 필요합니다.
- 지원되는 최대 vCPU는 16개입니다.
- 메모리 최적화 머신 유형은 지원되지 않습니다.

GCP에서 계정을 생성하고, GCP Marketplace의 ASA 가상 방화벽(ASA 가상) 제품을 사용해서 ASA 가상 인스턴스를 실행한 다음 GCP 머신 유형을 선택합니다.

C2 컴퓨팅 최적화 머신 유형 제한

컴퓨팅 최적화 C2 머신 유형에는 다음과 같은 제한 사항이 있습니다.

- 컴퓨팅 최적화 머신 유형에는 지역 영구 디스크를 사용할 수 없습니다. 자세한 내용은 Google 문서 지역 영구 디스크 추가 또는 크기 조정을 참조하십시오.

- 범용 및 메모리 최적화 시스템 유형과는 다른 디스크 제한이 적용됩니다. 자세한 내용은 Google 문서 블록 스토리지 성능을 참고하십시오.
- 일부 영역 및 지역에서만 사용할 수 있습니다. 자세한 내용은 Google 문서 사용 가능한 지역 및 영역을 참조하십시오.
- 일부 CPU 플랫폼에서만 사용 가능합니다. 자세한 내용은 Google 문서 CPU 플랫폼을 참조하십시오.

ASA 가상 및 GCP의 사전 요건

- https://cloud.google.com에서 GCP 계정을 만듭니다.
- GCP 프로젝트를 생성합니다. Google 문서, 프로젝트 생성을 참조하십시오.
- ASA 가상에 라이선스를 부여합니다. ASA 가상 라이선스를 등록하기 전에는 저성능 모드에서 실행됩니다. 이 모드에서는 100개의 연결 및 100Kbps의 처리량만 허용됩니다. 라이선스: 스마트 소프트웨어 라이선싱을 참조하십시오.
- 인터페이스 요구 사항:
  - 관리 인터페이스 - ASA 가상을 ASDM에 연결할 때 사용합니다. 통과 트래픽에는 사용할 수 없습니다.
  - 내부 인터페이스 - ASA 가상을 내부 호스트에 연결하는 데 사용합니다.
  - 외부 인터페이스 - ASA 가상을 공용 네트워크에 연결하는 데 사용합니다.
- 통신 경로:
  - ASA 가상에 액세스하기 위한 공용 IP.
- ASA 가상 시스템 요구 사항은 Cisco Secure Firewall ASA호환성을 참조하십시오.

ASA 가상 및 GCP에 대한 지침 및 제한 사항

지원 기능

GCP의 ASA 가상은 다음 기능을 지원합니다.

- GCP VPC(Virtual Private Cloud)에 구축
- 인스턴스당 최대 16개의 vCPU
- 라우팅 모드(기본값)
- 라이선싱 – BYOL만 지원됩니다.

지원되지 않는 기능

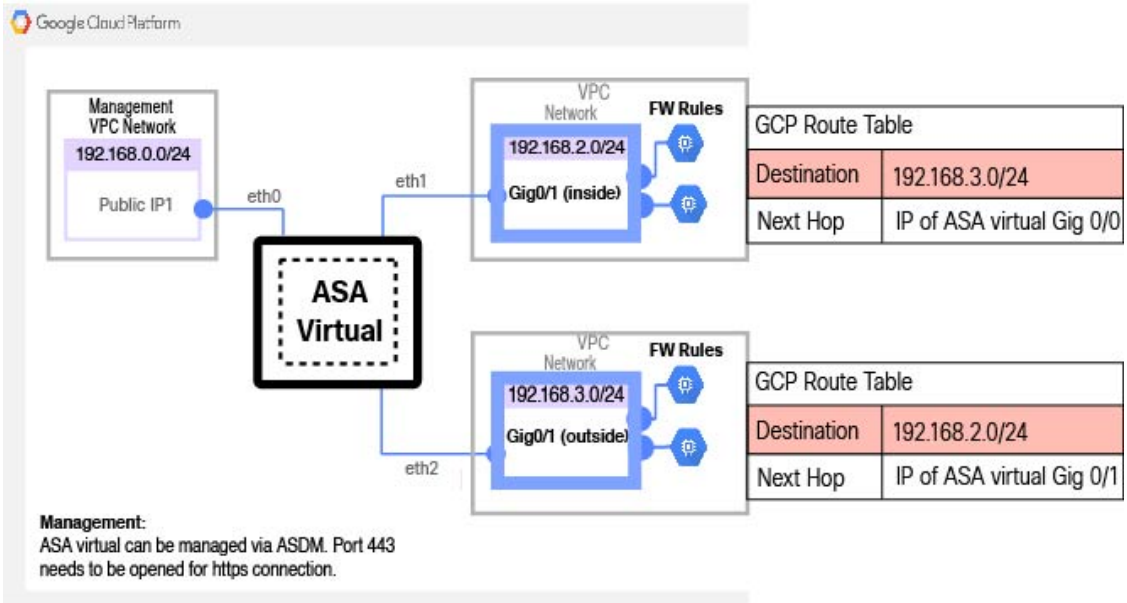
GCP의 ASA 가상은 다음을 지원하지 않습니다.

- IPv6
  - 인스턴스 수준 IPv6 설정은 GCP에서 지원되지 않습니다.
  - 로드 밸런서만이 IPv6 연결을 수락하고, IPv4를 통해 GCP 인스턴스로 프록시할 수 있습니다.
- 점보 프레임
- ASA 가상 기본 HA
- 자동 확장
- 투명/인라인/패시브 모드

GCP의 ASA 가상을 위한 네트워크 토폴로지 샘플

다음 그림은 Routed Firewall Mode의 ASA 가상에 대한 권장 네트워크 토폴로지와 ASA 가상에 대해 GCP에 구성된 3개의 서브넷(관리, 내부 및 외부)을 보여줍니다.

그림 *1: GCP* 구축에 대한 *ASA* 가상 샘플



Google Cloud Platform에 ASA 가상 구축

Google Cloud Platform에 ASA 가상 구축

GCP(Google Cloud Platform)에서 ASA 가상을 구축할 수 있습니다.

VPC 네트워크 생성

시작하기 전에

ASA 가상을 구축하려면 ASA 가상을 구축하기 전에 3개의 네트워크를 생성해야 합니다. 네트워크는 다음과 같습니다.

- 관리 서브넷의 관리 VPC
- 내부 서브넷의 내부 VPC
- 외부 서브넷의 외부 VPC

또한 ASA 가상로 트래픽 흐름을 허용하도록 경로 테이블 및 GCP 방화벽 규칙을 설정합니다. 경로 테이블 및 방화벽 규칙은 ASA 가상 자체에 구성된 규칙과 다릅니다. 연결된 네트워크 및 기능에 따라 GCP 경로 테이블 및 방화벽 규칙의 이름을 지정합니다. GCP의 ASA 가상을 위한 네트워크 토폴로지 샘플, 4 페이지의 내용을 참조하십시오.

단계 **1** GCP 콘솔에서 **Networking(**네트워킹**)** > **VPC network(VPC** 네트워크**)** > **VPC networks(VPC** 네트워크**)**를 선택하고 **Create VPC Network(VPC** 네트워크 생성**)**를 클릭합니다.

단계 **2** **Name(**이름**)** 필드에 VPC 네트워크를 설명하는 이름(예: *vpc-asiasouth-mgmt*)을 입력합니다.

단계 **3** **Subnet creation mode(**서브넷 생성 모드**)**에서 **Custom(**맞춤형**)**을 클릭합니다.

단계 **4** **New subnet(**새로운 서브넷**)** 아래의 **Name(**이름**)** 필드에 원하는 이름(예: *vpc-asiasouth-mgmt*)을 입력합니다.

단계 **5** **Region(**지역**)** 드롭 다운 목록에서 자신의 구축에 적합한 지역을 선택합니다. 세 개의 네트워크는 모두 같은 지역에 있어야 합니다.

단계 **6** **IP** 어드레스 레인지 필드에 CIDR 포맷, 예를 들면 10.10.0.0/24의 형식으로 첫 번째 네트워크의 서브넷을 입력합니다.

단계 **7** 기타 모든 설정은 기본값으로 하고 **Create(**생성**)**를 클릭합니다.

단계 **8** 1~7 단계를 반복하여 VPC에 나머지 2개의 네트워크를 생성합니다.

방화벽 규칙 생성

ASA 가상인스턴스를 구축하는 동안 (SSH 및 HTTPS 연결을 허용하도록) 관리 인터페이스에 대한 방화벽 규칙을 적용합니다. GCP에서 ASA 가상 인스턴스 생성, 6 페이지를 참조하십시오. 요구 사항에 따라 내부 및 외부 인터페이스에 대한 방화벽 규칙을 생성할 수도 있습니다.

단계 1 GCP 콘솔에서 **Networking(**네트워킹**)** > **VPC network(VPC** 네트워크**)** > **Firewall(**방화벽**)**을 선택하고 **Create Firewall Rule(**방화벽 규칙 생성**)**을 클릭합니다.

단계 2 **Name(**이름**)** 필드에 방화벽 규칙을 설명하는 이름(예: *vpc-asiasouth-inside-fwrule*)을 입력합니다.

단계 3 **Network(**네트워크**)** 드롭 다운 목록에서 방화벽 규칙을 생성할 VPC 네트워크의 이름(예: *asav-south-inside*)을 선택합니다.

단계 4 **Targets(**대상**)** 드롭 다운 목록에서 방화벽 규칙을 위해서 적용할 옵션(예: **All instances in the network**)을 선택합니다.

단계 5 **Source IP ranges(**소스 **IP** 범위**)** 필드에 소스 IP 주소 범위를 CIDR 형식으로 입력합니다(예: 0.0.0.0/0).

트래픽은 이들 IP 주소 범위 내의 소스로부터만 허용됩니다.

단계 6 **Protocols and ports(**프로토콜 및 포트**)** 아래에서 **Specified protocols and ports(**명시된 프로토콜 및 포트**)**를 선택합니다.

단계 7 보안 규칙을 추가합니다.

단계 8 **Create(**생성**)**를 클릭합니다.

GCP에서 ASA 가상 인스턴스 생성

아래 단계를 완료하면 GCP Marketplace에서 제공하는 Cisco ASA 가상 방화벽(ASA 가상) 제품을 사용하여 ASA 가상 인스턴스를 구축할 수 있습니다.

단계 1 GCP 콘솔로 로그인합니다.

단계 2 **Navigation(**탐색**)** 메뉴**(** > **Marketplace(**마켓플레이스**)**를 클릭합니다 .

단계 3 Marketplace에서 “Cisco ASA virtual firewall(ASAv)”을 검색하고 제품을 선택합니다.

단계 4 **Launch(**실행**)**를 클릭합니다.

단계 5 인스턴스의 고유한 **Deployment name(**구축 이름**)**을 추가합니다.

단계 6 ASA 가상를 구축할 **Zone(**영역**)**을 선택합니다.

단계 7 적절한 **Machine type(**머신 유형**)**을 선택합니다. 지원되는 머신 유형 목록은 GCP의 ASA 가상 구축 정보, 1 페이지를 참조하십시오.

단계 8 (선택 사항) **SSH** 키**(**선택 사항**)**에 있는 SSH 키 쌍의 공개 키를 붙여넣습니다.

키 쌍은 GCP가 저장하는 공용 키와 사용자가 저장하는 개인 키 파일로 구성됩니다. 이 두 키를 함께 사용하면 인스턴스에 안전하게 연결할 수 있습니다. 인스턴스에 연결할 때 필요한 만큼 키 쌍을 알고 있는 위치에 확실히 저장해야 합니다.

단계 9 이 인스턴스에 액세스하기 위해 프로젝트 전체 SSH 키를 허용할지 아니면 차단할지를 선택합니다. Google 문서 Allowing or blocking project-wide public SSH keys from a Linux instance를 참조하십시오.

단계 10 (선택 사항) **Startup script(**시작 스크립트**)**에 ASA 가상에 대한 day0 컨피그레이션을 입력합니다. day0 컨피그레이션은 ASA 가상의 첫 번째 부팅 중에 적용됩니다.

다음 예는 시작 스크립트 필드에 복사하여 붙여 넣은 Day0 컨피그레이션의 샘플을 보여줍니다.

ASA 명령에 대한 자세한 내용은 ASA 구성 가이드 및 ASA 명령 참조를 참조하십시오.

중요 이 예의 텍스트를 복사할 때는 서드파티 텍스트 편집기 또는 검증 엔진에서 스크립트를 검증하여 형식 오류를 방지하고 유효하지 않은 유니코드 문자를 제거해야 합니다.

```
!ASA Version 9.15.1

interface management0/0

management-only
nameif management
security-level 100
ip address dhcp setroute
no shut
!
same-security-traffic permit inter-interface
same-security-traffic permit intra-interface
!
crypto key generate rsa modulus 2048
ssh 0 0 management
ssh timeout 60
ssh version 2
username admin password cisco123 privilege 15
username admin attributes
service-type admin
! required config end
dns domain-lookup management
dns server-group DefaultDNS
name-server 8.8.8.8
```

단계 **11** 프로비저닝된 디스크 공간에는 기본 **Boot disk type(**부팅 디스크 유형**)**과 **Boot disk size in GB(**부팅 디스크 크기 **(GB)**를 그대로 유지합니다.

단계 **12** **Network interfaces(**네트워크 인터페이스**)**에서 인터페이스를 구성합니다.

- 관리
- 내부
- 외부

참고 인터페이스를 생성한 후엔 거기에 인터페이스를 추가할 수 없습니다. 부적절한 인터페이스 컨피그레이션으로 인스턴스를 생성했을 경우 해당 인스턴스를 삭제하고 적절한 인터페이스 컨피그레이션으로 다시 생성해야 합니다.

a) **Network(**네트워크**)** 드롭 다운 목록에서 VPC 네트워크(예 : *vpc-asiasouth-mgmt*)를 선택합니다.

b) **External IP(**외부 **IP)** 드롭 다운 목록에서 적절한 옵션을 선택합니다.

관리 인터페이스를 위해선 **External IP(**외부 **IP) - Ephemeral(**일회성**)**을 선택합니다. 이는 내부 및 외부 인터페이스의 경우 선택 사항입니다.

c) **Done(**완료**)**을 클릭합니다.

단계 **13** **Firewall(**방화벽**)**에서 방화벽 규칙을 적용합니다.

- 인터넷의 **TCP** 포트 **22** 트래픽**(SSH** 액세스**)** 허용 확인란을 선택하여 SSH를 허용합니다.

- HTTPS 연결을 허용하려면 **Allow HTTPS traffic from the Internet(ASDM** 액세스**)(**인터넷에서 **HTTPS** 트래픽 허용**(ASDM** 액세스**))** 확인란을 선택합니다.

단계 **14** **More(**더 보기**)**를 클릭하여 보기를 확장하고 **IP Forwarding(IP** 전달**)**이 **On(**켜짐**)**으로 설정되어 있는지 확인합니다.

단계 **15** **Deploy(**구축**)**를 클릭합니다.

GCP 콘솔의 VM 인스턴스 페이지에서 인스턴스 상세 정보를 확인합니다. 내부 IP 주소, 외부 IP 주소 그리고 인스턴스를 시작하고 중지할 수 있는 제어 기능을 확인할 수 있습니다. 인스턴스를 수정해야 하는 경우 인스턴스를 중지해야 합니다.

GCP에서 ASA 가상 인스턴스에 액세스

구축 중에 SSH(포트 22를 통한 TCP 연결)를 허용하는 방화벽 규칙을 이미 활성화했는지 확인합니다. 자세한 내용은 GCP에서 ASA 가상 인스턴스 생성, 6 페이지를 참조하십시오.

이 방화벽 규칙은 ASA 가상 인스턴스에 대한 액세스를 활성화하고 다음 방법을 사용하여 해당 인스턴스에 연결할 수 있도록 합니다.

- 외부 IP
  - 기타 SSH 클라이언트 또는 서드파티 도구
- 시리얼 콘솔
- Gcloud 명령줄

더 자세한 내용은 Google 문서 Connecting to instances를 참조하십시오.

참고 day0 컨피그레이션에 지정된 자격 증명을 사용하거나 인스턴스 시작 과정에서 생성된 SSH 키 쌍을 사용하여 ASA 가상 인스턴스에 로그인할 수 있습니다.

외부 IP를 사용하여 ASA 가상 인스턴스에 연결

ASA 가상 인스턴스는 내부 IP와 외부 IP로 할당됩니다. 외부 IP를 사용해서 ASA 가상 인스턴스에 액세스할 수 있습니다.

단계 **1** GCP 콘솔에서 **Compute Engine(**컴퓨팅 엔진**)** > **VM instances(VM** 인스턴스**)**를 선택합니다.

단계 **2** ASA 가상 인스턴스 이름을 클릭해서 **VM** 인스턴스 상세정보 페이지를 엽니다.

단계 **3** **Details(**상세정보**)** 탭 아래에서 **SSH** 필드를 위한 드롭 다운 메뉴를 엽니다.

단계 **4** **SSH** 드롭 다운 메뉴에서 원하는 옵션을 선택합니다.

다음 방법을 사용해서 ASA 가상 인스턴스에 연결할 수 있습니다.

- 기타 SSH 클라이언트 또는 서드파티 도구 - 더 자세한 내용은 Google 문서 Connecting using third-party tools을 참조하십시오.

참고 day0 컨피그레이션에 지정된 자격 증명을 사용하거나 인스턴스 시작 과정에서 생성된 SSH 키 쌍을 사용하여 ASA 가상 인스턴스에 로그인할 수 있습니다.

SSH를 사용하여 ASA 가상 인스턴스에 연결

Unix식 시스템에서 ASA 가상 인스턴스에 연결하려면 SSH를 사용해서 인스턴스에 연결합니다.

단계 1 다음 명령을 사용해서 파일 권한을 설정해서 본인만 파일을 읽을 수 있도록 합니다.

```
$ chmod 400 <private_key>
```

여기서 각 항목은 다음을 나타냅니다.

<private_key>는 액세스하고자 하는 인스턴스에 연결된 개인 키를 포함하고 있는 파일의 전체 경로와 이름입니다.

단계 2 다음 SSH 명령을 사용해서 인스턴스에 액세스합니다.

```
$ ssh -i <private_key> <username>@<public-ip-address>
```

여기서 각 항목은 다음을 나타냅니다.

<private_key>는 액세스하고자 하는 인스턴스에 연결된 개인 키를 포함하고 있는 파일의 전체 경로와 이름입니다.

<username>은 ASA 가상 인스턴스를 위한 사용자 이름입니다.

<public-ip-address>는 콘솔에서 가져온 인스턴스 IP 주소입니다.

직렬 콘솔을 사용해서 ASA 가상 인스턴스 연결

단계 1 GCP 콘솔에서 **Compute Engine(**컴퓨팅 엔진**)** > **VM instances(VM** 인스턴스**)**를 선택합니다.

단계 2 ASA 가상 인스턴스 이름을 클릭해서 **VM** 인스턴스 상세정보 페이지를 엽니다.

단계 3 **Details(**상세정보**)** 탭 아래에서 **Connect to serial console(**직렬 콘솔 연결**)**을 클릭합니다.

더 자세한 내용은 Google 문서 Interacting with the serial console을 참조하십시오.

Gcloud를 사용하여 ASA 가상 인스턴스에 연결

단계 1 GCP 콘솔에서 **Compute Engine(**컴퓨팅 엔진**)** > **VM instances(VM** 인스턴스**)**를 선택합니다.

단계 2 ASA 가상 인스턴스 이름을 클릭해서 **VM** 인스턴스 상세정보 페이지를 엽니다.

단계 3 **Details(**상세정보**)** 탭 아래에서 **SSH** 필드를 위한 드롭 다운 메뉴를 엽니다.

단계 4 **View gcloud command(gcloud** 명령 보기**)** > **Run in Cloud Shell(**클라우드 셸에서 구동**)**을 클릭합니다.

클라우드 셸 터미널 창이 열립니다. 더 자세한 내용은 Google 문서 gcloud command-line tool overview 그리고 gcloud compute ssh를 참조하십시오.

CPU 사용량 및 보고

CPU Utilization(CPU 사용률) 보고서에는 지정된 시간 내에 사용된 CPU의 백분율이 요약되어 있습니다. 일반적으로 코어는 사용량이 적은 시간에는 총 CPU 용량의 약 30~40%, 사용량이 많은 시간에는 약 60~70%로 작동합니다.

ASA Virtual의 vCPU 사용량

ASA virtual vCPU 사용량에서는 데이터 경로, 제어 지점, 외부 프로세스에 사용된 vCPU 양을 확인할 수 있습니다.

GCP에서 보고하는 vCPU 사용량에는 앞서 설명한 ASA virtual 사용량이 포함됩니다.

- ASA Virtual 유휴 시간
- ASA 가상 머신에 사용된 %SYS 오버헤드
- vSwitch, vNIC, pNIC 간 패킷 이동의 오버헤드. 이 오버헤드가 상당히 클 수 있습니다.

CPU 사용량의 예

show cpu usage 명령을 사용하여 CPU 사용률 통계를 표시할 수 있습니다.

예

```
Ciscoasa#show cpu usage

CPU utilization for 5 seconds = 1%; 1 minute: 2%; 5 minutes: 1%
```

다음은 보고된 vCPU 사용량이 상당한 차이를 보이는 예입니다.

- ASA Virtual 보고서: 40%
- DP: 35%

- 외부 프로세스: 5%
- ASA(ASA Virtual 보고서): 40%
- ASA 유휴 폴링: 10%
- 오버헤드: 45%

이 오버헤드는 하이퍼바이저 기능을 수행하고 vSwitch를 사용하여 NIC와 vNIC 간에 패킷을 이동하는 데 사용됩니다.

GCP CPU 사용량 보고

GCP 콘솔에서 인스턴스 이름을 클릭한 다음 **Monitoring(**모니터링**)** 탭을 클릭합니다. CPU 사용률을 확인할 수 있습니다.

Compute Engine에서는 사용량 내보내기 기능을 사용하여 Compute Engine 사용량에 관한 자세한 보고서를 Google Cloud Storage 버킷으로 내보낼 수 있습니다. 사용량 보고서는 리소스의 수명에 관한 정보를 제공합니다. 예를 들어 프로젝트에서 `n2-standard-4` 머신 유형을 실행 중인 VM 인스턴스의 수와 각 인스턴스가 실행된 기간을 확인할 수 있습니다. 또한 영구 디스크의 스토리지 공간과 다른 Compute Engine 기능에 대한 정보도 검토할 수 있습니다.

ASA Virtual 및 GCP 그래프

ASA Virtual과 GCP의 CPU % 수치가 다릅니다.

- GCP 그래프 수치가 항상 ASA Virtual 수치보다 높습니다.
- GCP에서는 이를 %CPU 사용량, ASA Virtual에서는 %CPU 활용이라고 부릅니다.

용어 “%CPU utilization”과 “%CPU usage”의 의미는 서로 다릅니다.

- CPU utilization은 물리적 CPU의 통계를 제공합니다.
- CPU usage는 논리적 CPU의 통계로서 CPU 하이퍼스레딩을 기반으로 합니다. 그러나 단 하나의 vCPU가 사용되므로 하이퍼스레딩은 켜져 있지 않습니다.

GCP는 CPU % 사용량을 다음과 같이 계산합니다.

활발하게 사용 중인 가상 CPU의 양 - 총 가용 CPU 기준 백분율로 표시

이 계산은 게스트 운영 체제가 아닌 호스트의 관점에서 본 CPU 사용량입니다. 그리고 가상 머신에 있는 사용 가능한 모든 가상 CPU의 평균 CPU 사용률입니다.

예를 들어, 가상 CPU 1개를 사용하는 가상 시스템이 4개의 물리적 CPU를 가진 호스트에서 실행되는 중이고 CPU usage가 100%라면 가상 머신에서 하나의 물리적 CPU를 온전히 사용하는 것입니다. 가상 CPU 사용량 계산: 사용량(MHz) / 가상 CPU 수 x 코어 주파수