G-Cloud 사용자 Guide

V1.3 (2022.10)

KT

문서 생성일: 2022-10 ver1.3

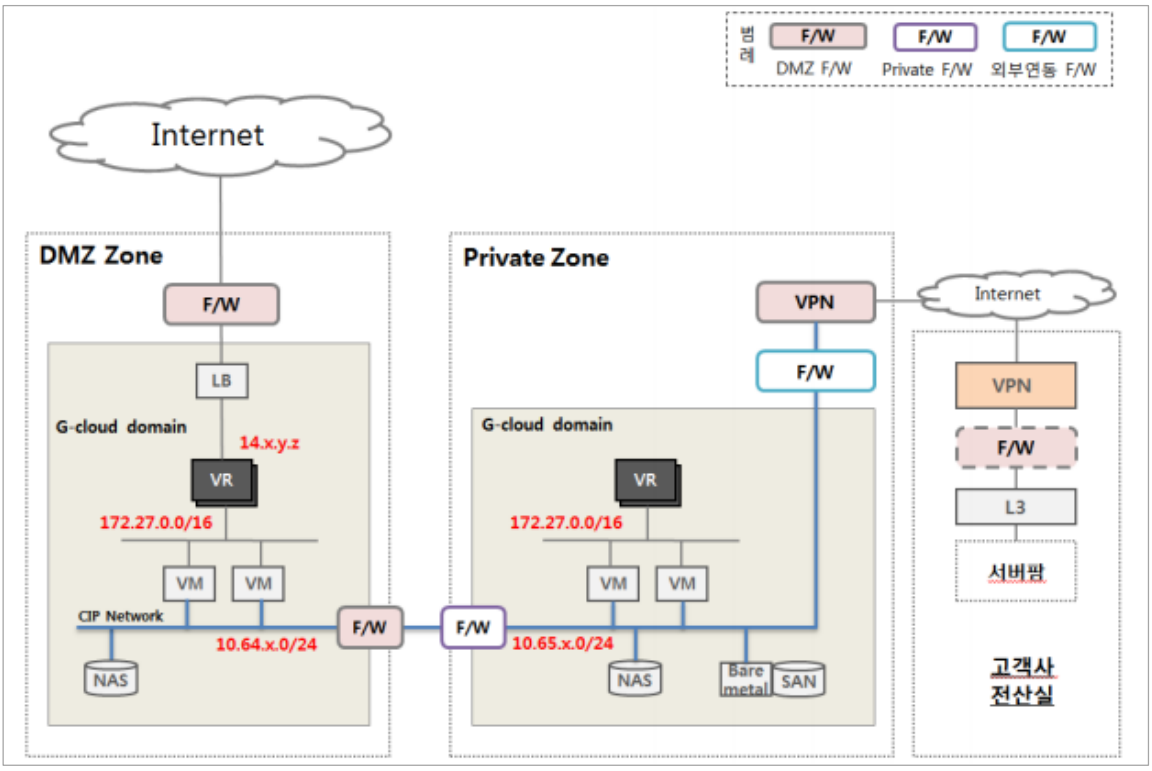
Revision History

version	변경사항	작성일
1.0	공식 배포 버전	2015.07
1.1	일부 내용 수정 / 방화벽 정책 신청방법 추가 / Repository 서버 이용방법 추가	2015.10
1.2	Userdata 를 이용한 if-up 및 routing table 추가 자동적용 방법 추가	2016.02
1.3	G-Cloud 도메인 정보 수정 - gov.ucloudbiz.kt.com → gcloud.kt.com	2022.10

목 차

1. G-Cloud 의 구조

G-Cloud 의 구조는 아래와 같습니다.



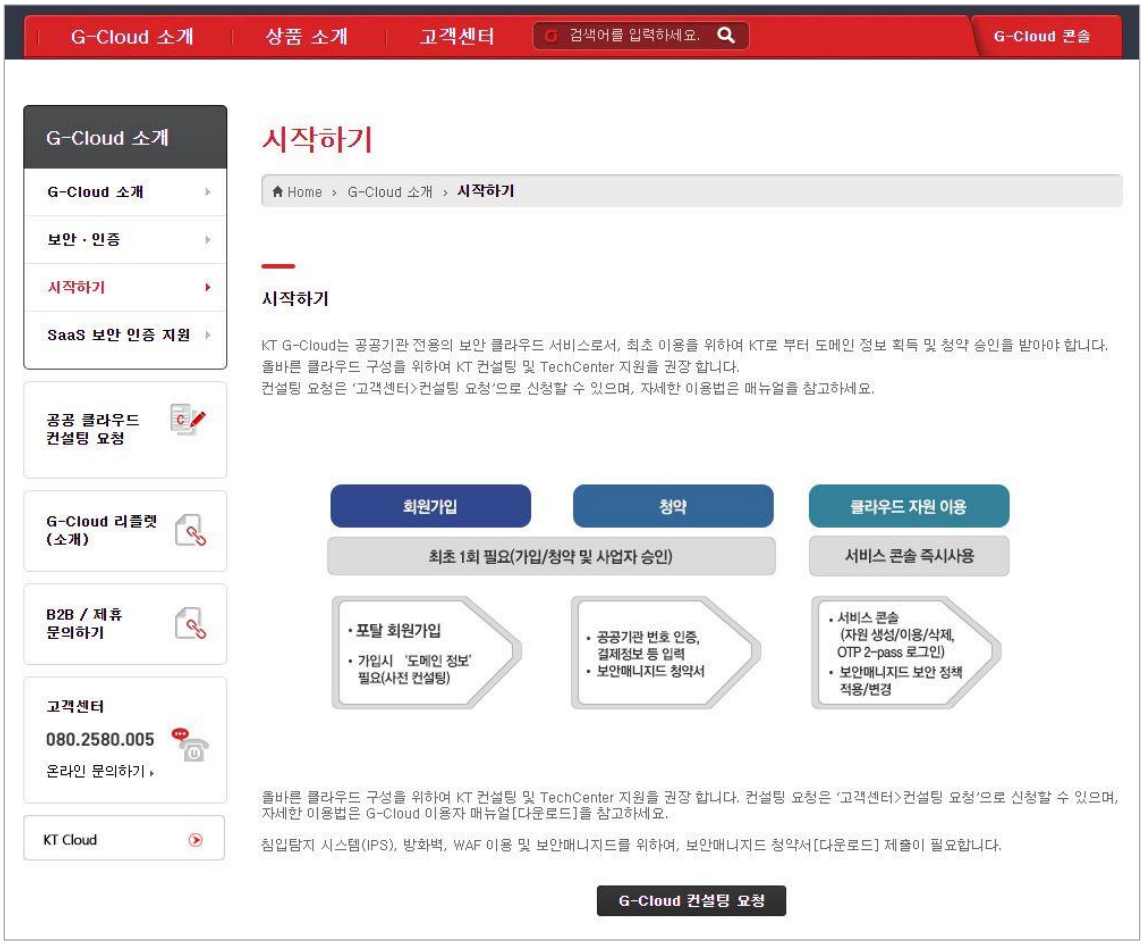
- DMZ Zone 과 Private Zone 으로 구분
- DMZ Zone VM 과 Private Zone VM (또는 BareMetal(물리머신))간에는 DMZ F/W 과 Private F/W 에 의해 차단되며 CIP 네트워크 이용하여 연동
- DMZ Zone 에는 웹서버등 Public 으로 노출되는 VM 배치(표준)
- Private Zone 에는 WAS 및 DB 등 배치(표준)
- Private Zone 에 배치되는 시스템은 VM 또는 BareMetal(물리머신)
- 웹서비스를 이용하는 최종 사용자는 DMZ F/W → IPS → DMZ LB (옵션) → VR → VM 의 경로로 접근
- 고객사 전산실 또는 Collocation 시스템은 VPN 또는 전용회선과 연동하여 Private Zone 으로 연동(고객사 서버팜 → VPN/전용회선 → 외부연동 F/W → Private VM 또는 BareMetal)
- DMZ F/W, Private F/W, 외부연동 F/W 의 세 가지 방화벽을 제공하고 방화벽 및 IPS 의 관리 및 관제는 보안 매니지드 서비스 담당자가 수행
- NAS, Backup Service, Baremetal(물리머신) 연결은 각 존의 CIP 를 통해 연결

2. 단계별 처리 방법

이번 장은 서비스 이용을 위해 고객사에서 수행할 단계별 처리 방법을 설명합니다.

2.1 컨설팅 신청

고객은 포탈을 통하여 서비스 컨설팅 요청을 합니다.
G-Cloud 는 컨설팅을 통해서만 서비스가 활성화됩니다.



위 화면에서 G-Cloud 컨설팅 요청 버튼을 눌러서 컨설팅을 신청합니다.

위 화면에서 각각의 항목을 입력하고 "신청" 버튼을 누르시면 기재된 연락번호로 컨설팅 담당자가 고객께 연락하여 컨설팅을 진행합니다.

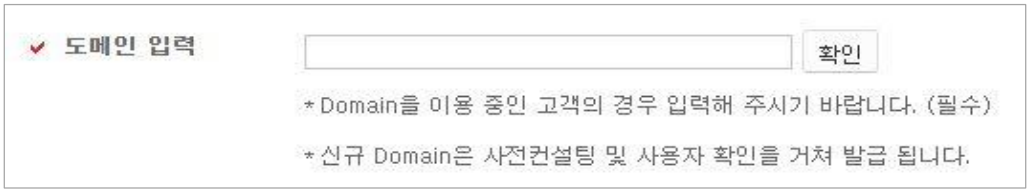
2.2 고객 컨설팅

컨설팅 담당자가 오프라인으로 시스템 수요 파악 및 서비스 이용 프로세스에 대한 가이드를 제공합니다.

고객사에서 서비스 이용을 희망하실 경우 고객사 전용의 도메인 생성 및 계정생성 단계로 넘어갑니다.

2.3 고객 도메인 생성(KT 운영센터) 및 고객 계정 생성(고객사)

컨설팅 담당자의 요청으로 KT 운영센터에서 해당 고객사에 해당하는 도메인을 생성합니다.
도메인을 생성하면 고유의 도메인 네임이 만들어지며 이를 고객사에 전달합니다. 고객사는 전달받은 도메인 명을 이용하여 회원가입을 수행합니다.
G-Cloud Portal(https://gcloud.kt.com)에서 회원가입 시 도메인 입력란에 전달받은 도메인 명을 입력합니다.

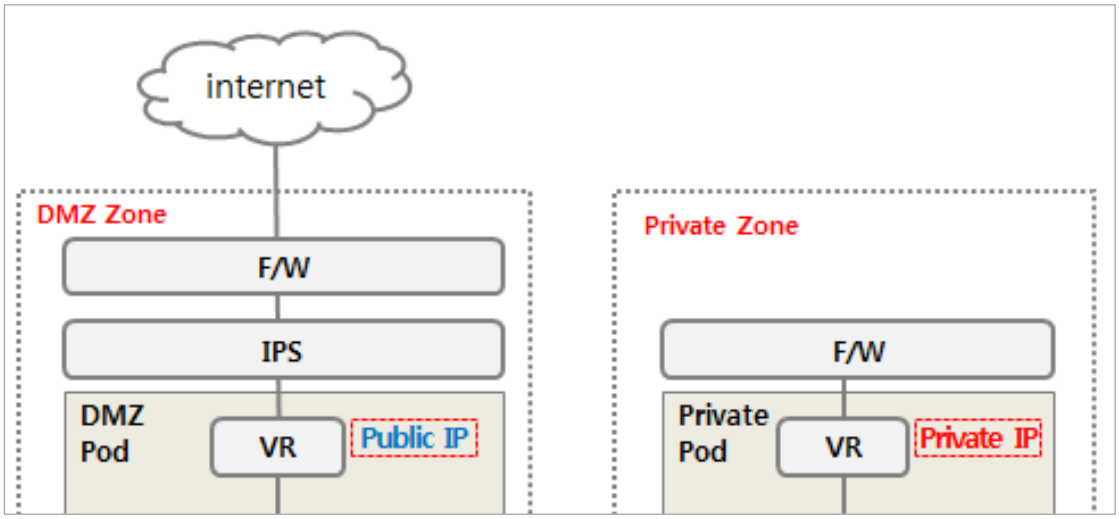


회원가입신청이 완료되면 등록하신 이메일 계정으로 인증메일이 발송됩니다.
접속하시어 "회원가입 완료하러 가기"를 클릭합니다.

2.4 상품 신청

회원가입이 완료되면 포탈 로그인 진행 후 아래 페이지에서 Server 상품을 신청합니다.

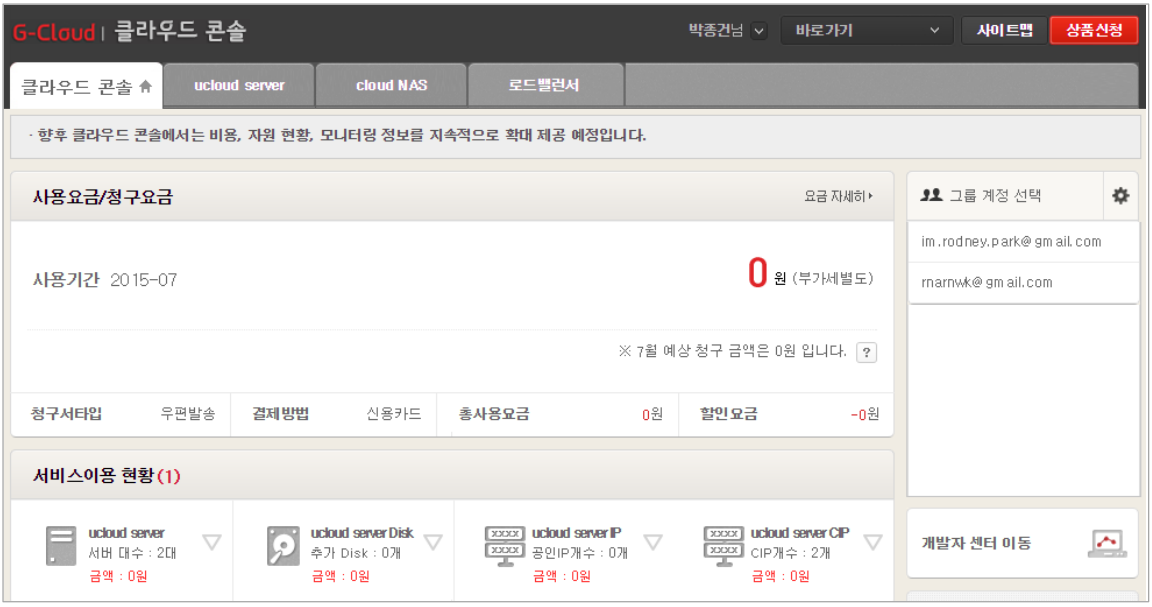
상품 신청 후에 컨설팅 담당자에게 상품신청 결과를 통보해주시면 KT 운영센터의 승인을 거쳐 회원가입이 완료됩니다. 이 때 해당 계정이 사용할 DMZ IP Address Pool 과 Private IP Address Pool(즉 몇 개의 IP 를 사용할 것인지)에 대해 컨설팅 담당자와의 협의를 통해 할당하게 됩니다. IP 는 추후에도 추가로 신청이 가능합니다.



위 그림에서 DMZ IP 는 공인 IP 인 14.63.180.0/22 IP 중 일부가 할당되고 Private IP 는 사설 IP 인 10.221.4.0/22 중 일부가 할당됩니다. 할당 받은 네트워크 자원에 대해 운용센터에서의 별도의 작업이 필요하여 처리되는데 Business Day 기준 약 3 일의 시간이 소요됩니다.

2.5 VM 생성

상품 신청이 완료되면 다음과 같은 G-Cloud 서비스 포탈의 클라우드 콘솔 화면을 보실 수 있습니다.

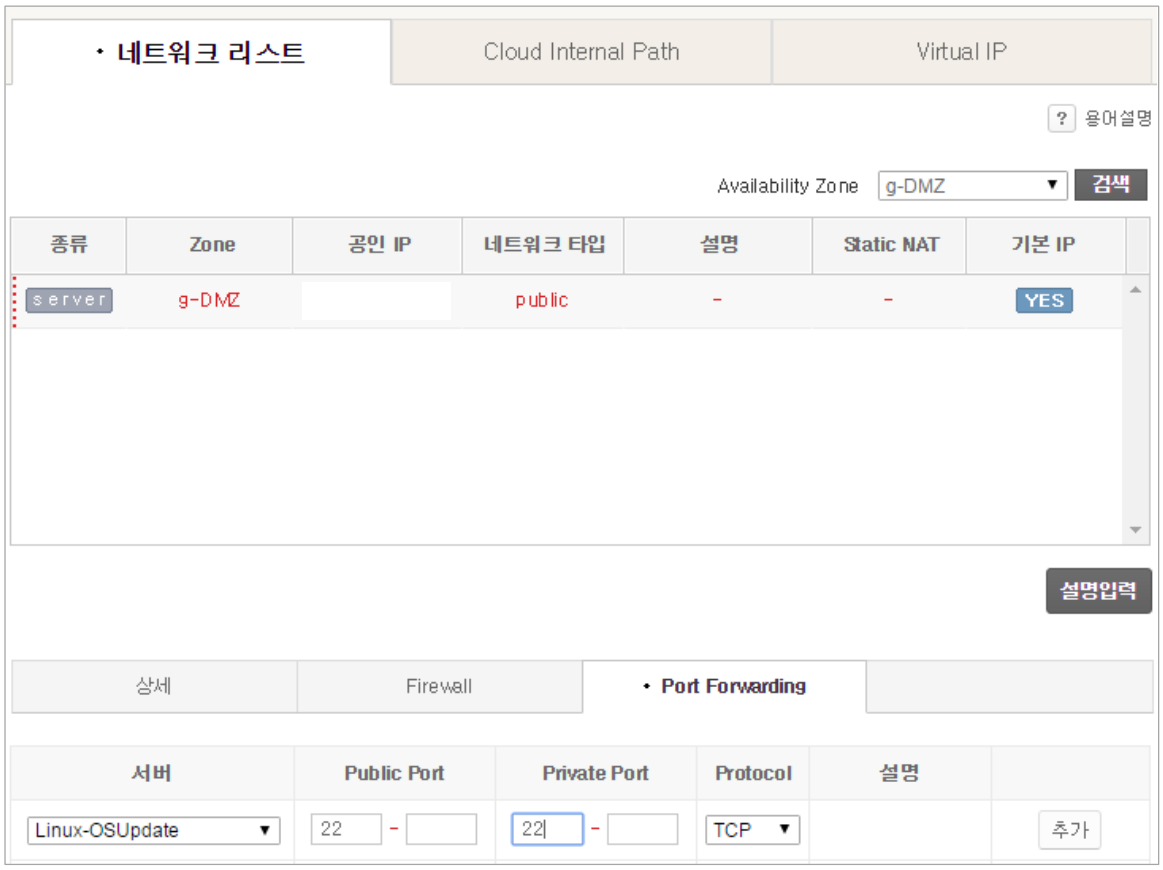


G-Cloud server 메뉴에서 '서버 신청'을 이용하여 zone 별로 필요한 VM 을 생성합니다. DMZ Zone 은 g-DMZ, Private Zone g-priv 로 표시됩니다.

- VM 을 생성할 Zone(DMZ/Private)과 서버 사양, 사용할 이미지를 선택하여 VM 을 생성합니다.

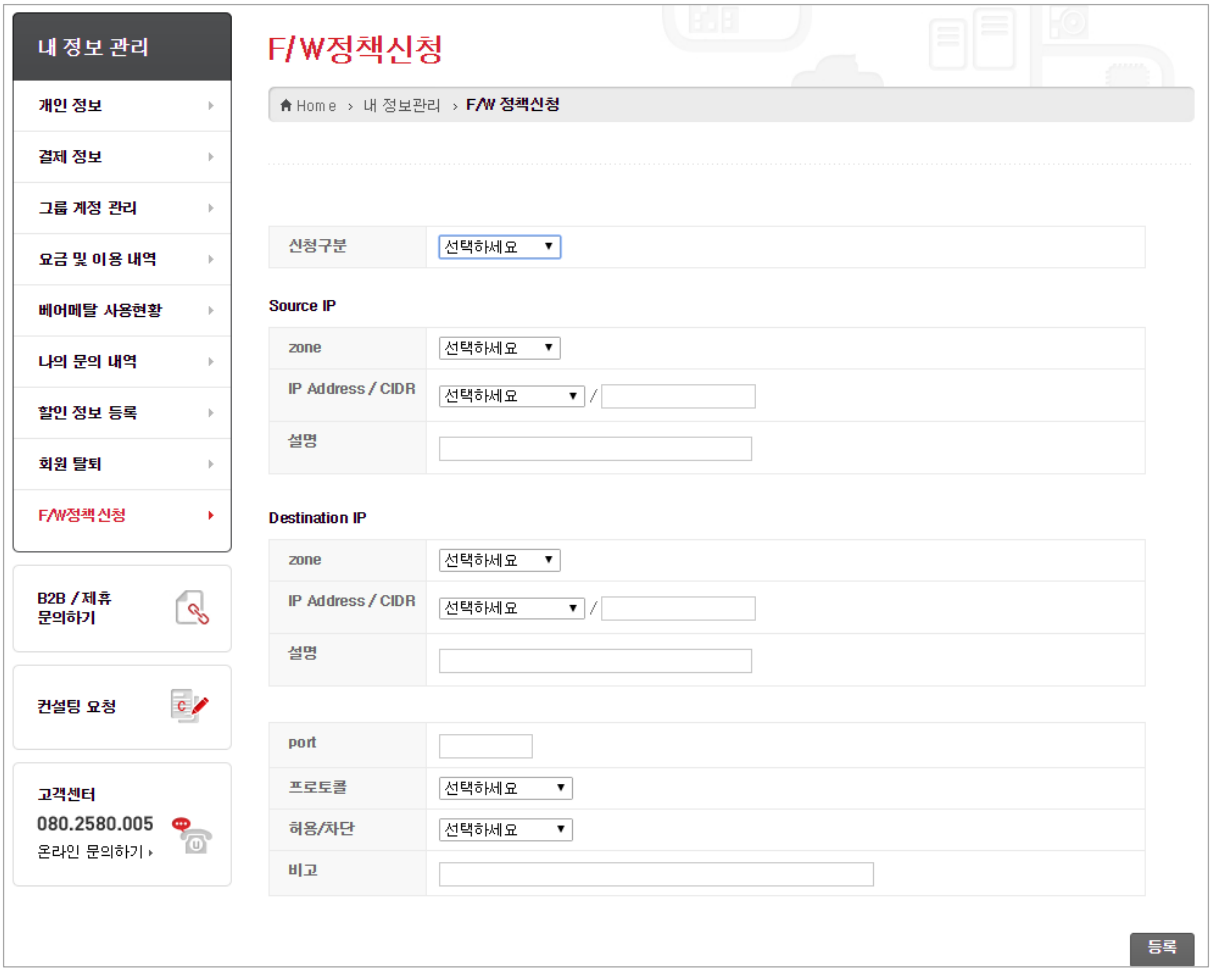
2.6 DMZ VR 에서 VM 으로 Port Forwarding 설정

VR 은 DMZ Zone 이나 Private Zone 이나 모두 NAT 방식으로 동작합니다. 때문에 DMZ IP 또는 Private IP 에서 내부 guest network 으로 접근하기 위해 Port Forwarding 이 설정되어 있어야 합니다. 아래는 DMZ IP(14.63.180.XX)/22 번 포트에서 Public VM(gov-pub1)/22 번 포트로 Port Forwarding 을 설정하는 화면입니다.



2.7 VM 방화벽 정책 설정 요청

방화벽(DMZ F/W, Private F/W, 외부연동 F/W)의 정책설정은 보안 매니지드 서비스를 통해 이용가능하며 서비스 이용을 위해서는 포탈에서 '방화벽 정책설정 신청'을 하셔야 합니다. 신청은 서비스 포탈 > 우측 상단의 '내정보관리' > F/W 정책신청에서 요청합니다.



신청 방법은 다음과 같습니다.

1. '신청구분'에서 '신규/변경/삭제' 중 필요한 요청을 선택합니다.
2. Source IP 와 Destination IP 항목의 Zone 과 IP Address/CIDR 을 입력합니다.
   Zone 선택 방법 ('1. G-Cloud 의 구조'의 구조도 참고)
   A. Source=Internet 이면, Destination=LB, DMZ 선택이 가능
   B. Source=DMZ 이면, Destination=Internet, Private 선택이 가능
   C. Source=Private 이면, Destination=Private, Legacy(외부연동) 선택이 가능
   D. Source= Legacy(외부연동) 이면, Destination=Private 선택이 가능
   E. Source=LB 이면, Destination=Internet 선택이 가능
3. 허용/차단할 Port 와 프로토콜(TCP/UDP/ICMP) 정보를 입력합니다.
4. '등록'을 클릭하면 자동으로 보안매니지드 업체로 접수처리 됩니다.

기타 방화벽 정책 설정 관련 문의는 다음의 이메일 또는 전화로 연락을 하셔야 합니다. (E-mail: mss1@wins21.co.kr, 전화: 031-622-8592~4)

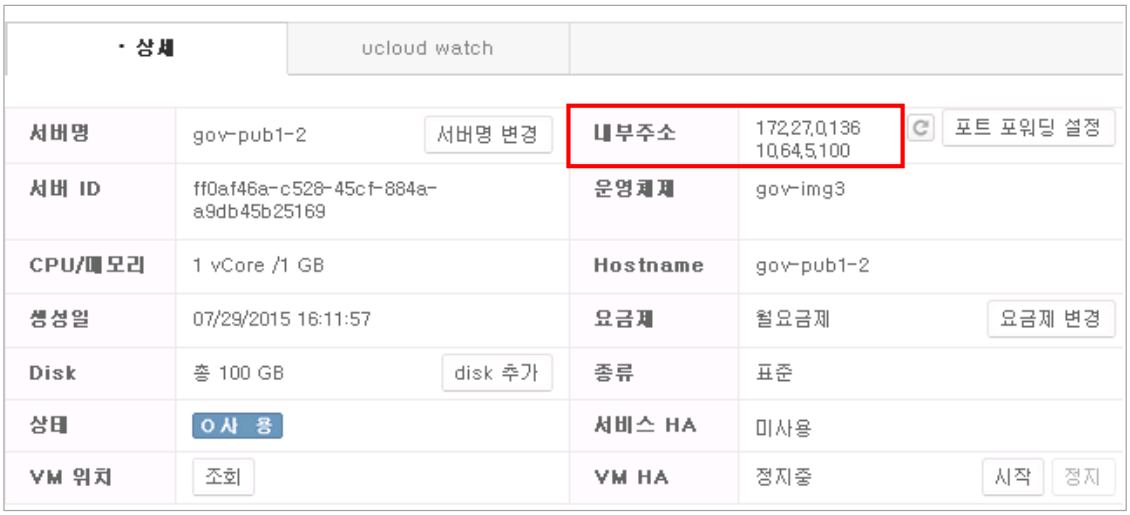
고객의 시스템으로부터 Public VM 에 접속하는 경로는 다음과 같습니다.

- 고객 시스템 → IPS → DMZ F/W → VR → Public VM

따라서 고객사가 Public VM 에 접근하기 위해서는 DMZ F/W 이 오픈되어 있어야 합니다. 이 때 Source IP 는 고객이 접속을 시도하려는 Client IP 이고 Destination IP 는 2.4 절에서 명시한 DMZ IP 입니다. 예를 들어, 사용자 VM 에 원격접속을 하고자 할 때 포탈에서 SSH(22 번 포트) 또는 RDP(3389 포트)를 Open 해야 하며 추가로 Public F/W 에 **Source IP: Client IP/32 → Destination IP: 14.63.180.XX/32, TCP 22 Port 허용**과 같은 형태로 Open 정책을 요청해야 합니다.

2.8 DMZ/Private VM CIP interface 설정

(DMZ Zone 의 CIP 는 10.64.0.0/16 내에서 Private Zone 의 CIP 는 10.65.0.0/16 내에서 할당됨)
CIP 를 연결하고자 하는 서버를 서버리스트에서 선택한 후 'CIP 연결'을 해줍니다. 서버에 CIP 연결 시 하단 상세정보의 내부주소에서 CIP 주소를 확인하실 수 있습니다.



(리눅스 서버의 경우) 서버에 접속하여 CIP NIC 활성화 작업을 해야 합니다. 네트워크 인터페이스 정보를 등록 후 네트워크 재시작을 통해 인터페이스를 활성화 시켜줍니다.

```
[root@ test ~]# cd /etc/sysconfig/network-scripts/
[root@ test network-scripts]# cp ifcfg-eth0 ifcfg-eth1 ←ifcfg-eth0 내용 복사
[root@ test network-scripts]# vim ifcfg-eth1 → DEVICE="eth1"로 수정
[root@ test ~]# /etc/init.d/service network restart → 네트워크 재시작
```

[root@ test ~]# ifconfig -a → eth0 외에 eth1, eth2 등의 추가 인터페이스 및 CIP 정보가 보이는지 확인

마찬가지로 Private VM 의 CIP Interface 활성화 방법도 위의 내용과 동일합니다. (리눅스 서버의 경우에만 해당하며 윈도우 서버는 자동으로 Network Interface 가 활성화됨)
하지만 초기 시스템 구축 시 Private VM 은 외부에서 접근이 불가하여 직접 설정 또한 불가합니다. 이 경우에는 서버 생성 시에 userdata 를 이용하여 자동으로 CIP Interface 를 활성화하는 방법과 kt 고객센터에 작업요청을 하는 방법이 있겠습니다. Userdata 이용방법은 아래의 zoner 간 네트워크 라우팅 설정방법에서 확인하시면 되겠습니다. Kt 고객 센터에 요청하셔야 하는 경우에는 계정정보, 해당 VM 명, VM 의 root 패스워드를 공유해주셔야 합니다. 향후 VPN 구성 또는 Public Zone 의 네트워크 대역과 라우팅 처리를 통해 외부와 네트워크 연동이 되어 있다면 고객센터 요청은 불필요 해집니다.

2.9 DMZ Zone 과 Private Zone 간 네트워크 라우팅 설정

DMZ Zone 과 Private Zone 간 통신은 CIP 네트워크를 통해 가능합니다. ('2.4 상품 신청' 내용 참고) 실질적으로 각 Zone 의 서버에서 상대방 CIP 네트워크 대역을 Routing Table 에 등록해주어야 합니다. 예를 들어 DMZ Zone 의 DMZ 서버(10.64.X.2)에는 Private Zone 의 Private 서버의 네트워크 대역(10.65.X.0/24)을 등록하고, 반대로 Private 서버(10.65.X.2)에서는 DMZ 서버의 네트워크 대역(10.64.X.0/24)을 등록해야 합니다.

(DMZ 서버에서 Private Zone의 네트워크 대역 라우팅 정보를 등록)

```
[root@DMZ~]# route add –net 10.65.X.0 netmask 255.255.255.0 gw 10.64.X.1
[root@DMZ~]# route
Kernel IP routing table
Destination     Gateway         Genmask         Flags Metric Ref    Use Iface
10.64.X.0       *               255.255.255.0   U     0      0        0 eth1
10.65.X.0       10.64.X.1       255.255.255.0   UG    0      0        0 eth1
172.27.0.0      *               255.255.0.0     U     0      0        0 eth0
link-local      *               255.255.0.0     U     1002   0        0 eth0
link-local      *               255.255.0.0     U     1003   0        0 eth1
default         172.27.0.1      0.0.0.0         UG    0      0        0 eth0
```

(Private 서버에서 DMZ Zone의 네트워크 대역 라우팅 정보를 등록)

```
[root@Private~]# route add –net 10.64.X.0 netmask 255.255.255.0 gw 10.65.X.1
[root@Private~]# route
Kernel IP routing table
Destination     Gateway         Genmask         Flags Metric Ref    Use Iface
10.65.X.0       *               255.255.255.0   U     0      0        0 eth1
10.64.X.0       10.65.X.1       255.255.255.0   UG    0      0        0 eth1
172.27.0.0      *               255.255.0.0     U     0      0        0 eth0
link-local      *               255.255.0.0     U     1002   0        0 eth0
link-local      *               255.255.0.0     U     1003   0        0 eth1
default         172.27.0.1      0.0.0.0         UG    0      0        0 eth0
```

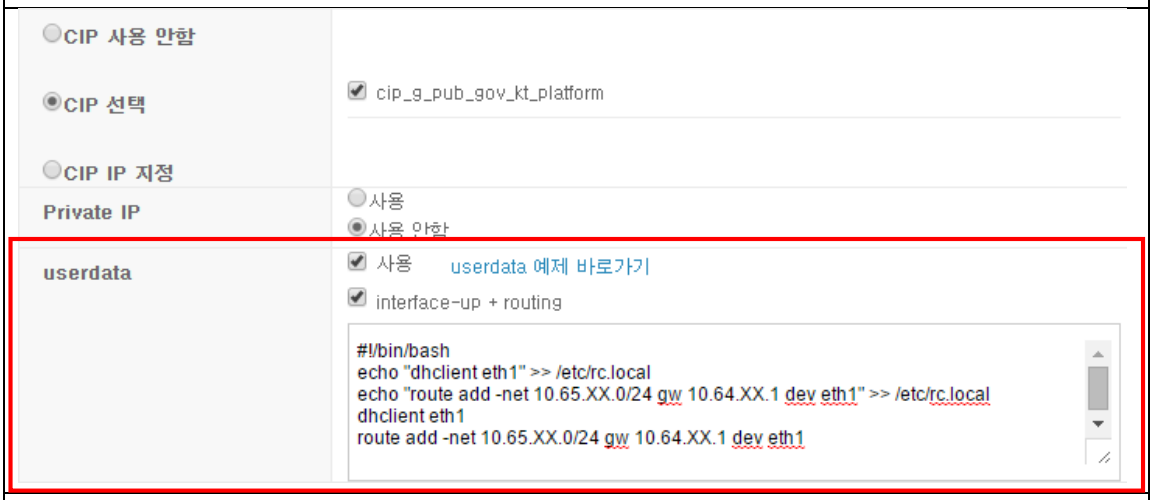
Routing Table 등록작업이 완료된 후에는 상대방 IP 를 target 으로 ping check 를 통해 정상통신 여부를 확인해볼 수 있습니다.

단, Private 서버의 경우 초기 시스템 구축 시에는 '2.9 Private VM CIP Interface 설정'에서의 상황과 같이 외부에서 접근이 불가하여 라우팅 직접 설정이 어렵습니다. 이 경우에는 마찬가지로 kt 고객센터에 작업요청을 하는 방법과 서버 생성단계에서 userdata 를 이용하여 자동설정을 하는 방법이 있겠습니다. 콘솔화면에서 userdata 를 이용하는 방법은 아래의 방법을 이용하시고 kt 고객센터로 작업 요청을 하실 경우에는 계정정보, 해당 VM 명, VM 의 root 패스워드를 공유해주셔야 합니다. (userdata 는 리눅스 OS 에서만 이용가능하므로 Windows OS 이용 시에는 고객센터로 요청을 주셔야 합니다.)

다음은 userdata 를 이용하는 방법입니다. 포탈에서 서버생성 시 'userdata 사용'과 'interface-up + routing'를 선택하면 관련 스크립트가 자동으로 입력됩니다.

** DMZ VM 과 Private VM 생성 시 입력 스크립트 내용은 상이하나 선택한 '위치(Zone)'에 따라 알맞은 스크립트가 자동으로 적용됩니다.*

Public VM 생성 시



Private VM 생성 시

2.10 VPN 이용

포탈의 사용자매뉴얼을 참고 바랍니다. (고객센터 > 서비스 이용 가이드 > 사용자 매뉴얼 > 네트워크 > VPN 연동가이드) https://gcloud.kt.com/manual/ucloud_VPN_Guide.pdf

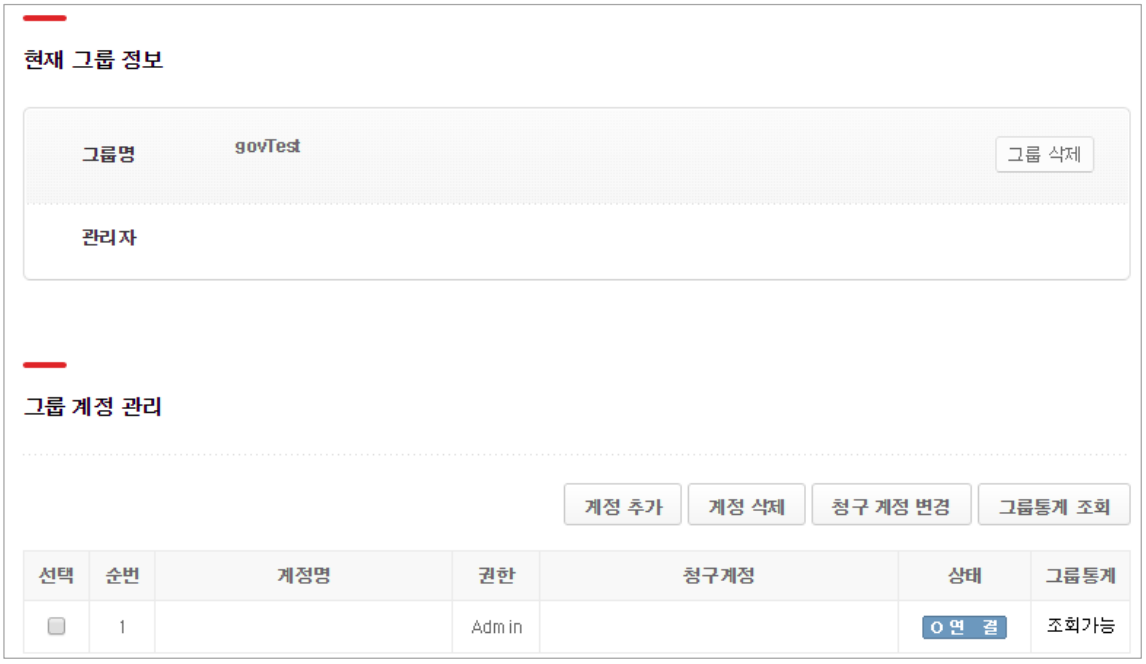
2.11 그룹계정 관리

동일 Domain 내 복수 개의 계정을 가질 경우 그룹계정 기능을 이용하여 편리하게 포탈을 이용할 수 있습니다.(통합 과금이 가능하며 이미지/NAS/LoadBalancer 등의 자원 및 기능을 조건부 공유할 수 있음)

포탈 메인 화면 우측 상단의 '내정보관리' 또는 콘솔화면 우측 상단에서 사용자명을 클릭하면 '그룹관리' 메뉴를 선택하실 수 있습니다.

그룹을 생성한 후 "계정 추가"를 통해 그룹 내에 추가할 계정정보를 입력합니다.

추가하려는 계정에서 "가입승인" 처리하면 하나의 그룹 계정으로서 이용하실 수 있습니다.



3. FAQ

Q . Private VM 에 관리용으로 접근(RDP, SSH)하려면 어떻게 해야 하나요?

- 두 가지 경로가 있을 수 있습니다.
  VPN 이나 전용 회선을 연동하여 접근하는 방법과 Enterprise Public VM 을 경유하여 접근하는 방법이 그 예시입니다.
  물론 각각의 경로상에 위치한 방화벽은 접근 전에 오픈 신청이 되어 있어야 합니다.
  이 때 Source IP 는 접근하려는 Client PC 나 시스템의 공인 IP 이어야 하며, Destination IP 는 DMZ IP 와 Private IP 입니다.

Q . 도메인 생성 절차가 누락되면 어떻게 되나요?

- 계정 생성 시 도메인을 입력하지 않으면, 해당 계정은 Public 사용자로 매핑 되어 G-Cloud 를 사용하지 않는 형태로 구성되고, 이후 사용자가 생성하는 자원들(VM 등)은 DMZ Zone 에 생성이 됩니다.
  따라서 G-Cloud 를 사용하기 위해서는 반드시 할당 받은 도메인을 지정하여 계정을 생성해야 합니다.

4. 서비스 상담 및 장애 신고

G-Cloud 상품의 모든 상담 및 장애 신고 방법은 전화 상담과 게시판 상담을 통해 이루어집니다.

4.1 FAQ 및 매뉴얼

각종 사용 매뉴얼 및 FAQ 는 G-Cloud 포탈 고객센터의 FAQ 게시판 및 자료실을 통하여 확인하실 수 있습니다.

- FAQ 게시판 : https://gcloud.kt.com/portal/portal.faq.html
- 사용자 매뉴얼 : https://gcloud.kt.com/portal/portal.portalinfo.html

4.2 전화 상담

상품 문의는 G-Cloud 고객센터(080-2580-005)를 통하여 상담 받으실 수 있습니다.

4.3 게시판 상담

G-Cloud 게시판에 문의사항 및 장애 상황을 작성 후 답변을 확인하시면 됩니다.

클라우드 기술 전문가가 해당 내용에 대해 기술적 문의사항을 지원해드립니다.