업데이트일 : 2018-11-01

IV. 엔터프라이즈

2. enterprise cloud

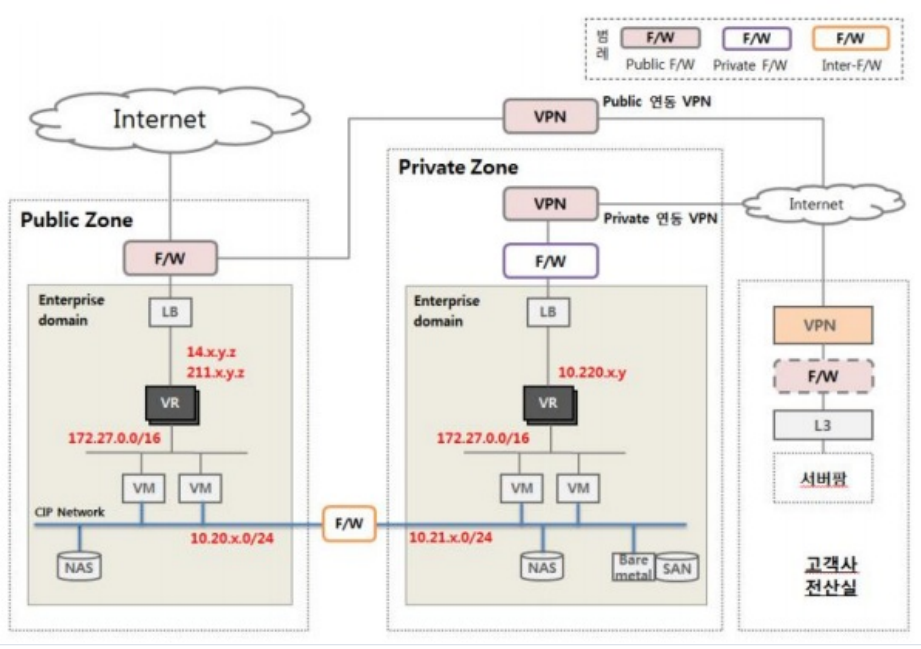
목차

2.1 Enterprise Cloud 서비스소개

2.1.1 목적/용도

Enterprise Cloud 서비스는 Public Zone 과 Private Zone으로 구분하여, 일반 클라우드 서비스에 비해 더욱 강화된 보안을 요구하는 기업, 공공기관, 금융기관 등이 사용하기에 적합합니다.
IPS(침입방지시스템), FW(방화벽), VPN, 보안관제서비스를 기본으로 제공합니다.
하드웨어기반 보안 장비를 통해 강력한 NW 보안 및 성능을 제공 합니다.

2.1.2 구조/원리



▫ Public Zone / Private Zone 구조

- Public Zone VM과 Private Zone VM(또는 Bare Metal(물리머신)) 간에는 Inter-F/W 에 의해 차단되며 CIP 네트워크 이용하여 연동

- Public Zone에는 웹서버등 Public으로 노출되는 VM 배치 (표준)

- Private Zone에는 WAS 및 DB 등 배치 (표준)

- Private Zone에 배치되는 시스템은 VM 또는 Bare Metal(물리머신)

- 웹서비스를 이용하는 최종 사용자는 IPS → Public F/W → Public LB (옵션) → VR → VM 의 경로로 접근

- 고객사 전산실 또는 Collocation 시스템은 VPN 또는 전용회선을 이용하여 Public Zone VM 또는 Private Zone VM으로 연동 (고객사 서버팜 → VPN/전용회선 → Private F/W → VR → Private VM 또는 Bare Metal)

- NAS, Backup Service, Bare Metal(물리머신) 연결은 각 존의 CIP를 통해 연결

2.1.3 유의사항/제약사항

▫ F/W 제공

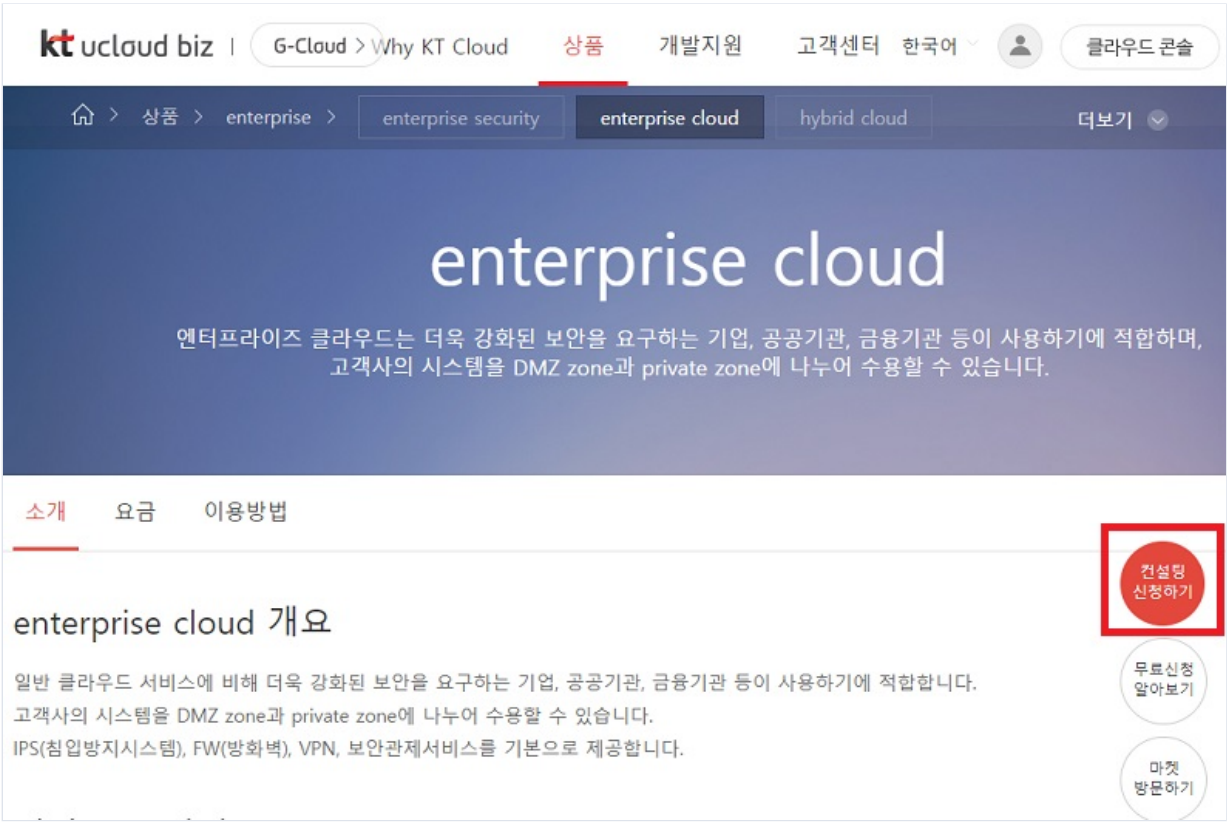
- Public-F/W, Private F/W, Inter-F/W 의 세가지 방화벽을 제공하고 방화벽 및 IPS 의 관리 및 관제는 보안 매니지드 서비스 담당자가 수행

2.2 enterprise cloud 이용방법

이번 장은 서비스 이용을 위해 고객사에서 수행할 단계별 처리방법을 설명합니다.

컨설팅 신청

고객은 포탈을 통하여 서비스 컨설팅 요청을 합니다. Enterprise Cloud는 컨설팅을 통해서만 서비스가 활성화됩니다.



위 화면에서 컨설팅 신청 버튼을 눌러 컨설팅을 신청합니다.

위 화면에서 각각의 항목을 입력하고 신청버튼을 누르시면 기재된 연락번호로 컨설팅 담당자가 고객께 연락하여 컨설팅을 진행합니다.

고객 컨설팅

컨설팅 담당자의 오프라인으로 시스템 수요 및 서비스 이용 프로세스에 대한 가이드를 제공합니다. 고객사에서 서비스 이용을 희망하실 경우 고객사 전용의 도메인생성 및 계정생성 단계로 넘어갑니다.

고객 도메인 생성 (KT 운영센터) 및 고객 계정 생성 (고객사)

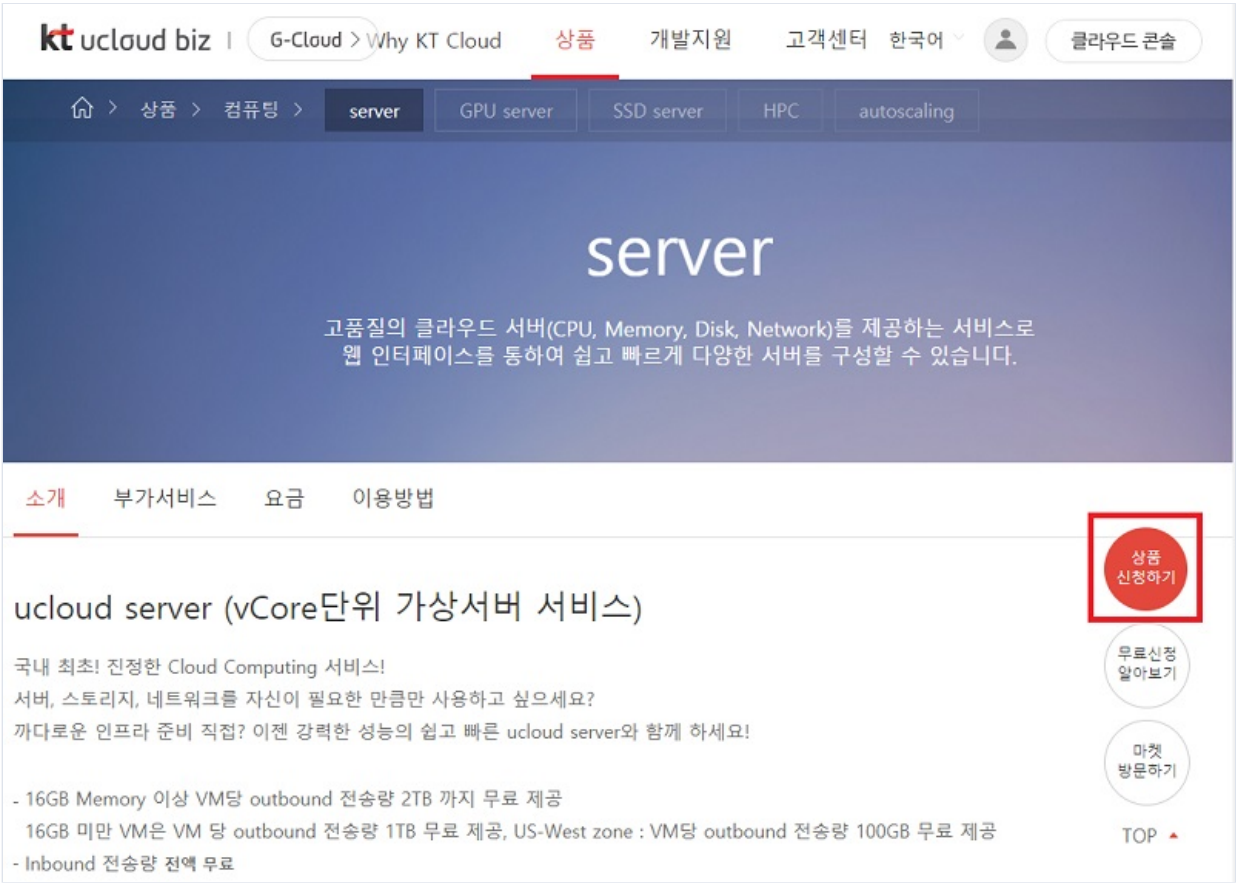
컨설팅 담당자의 요청으로 KT 운영센터에서 해당 고객사에 해당하는 도메인을 생성합니다. 도메인을 생성하면 고유의 도메인 네임이 만들어지며 이를 고객사에 전달합니다. 고객사는 전달받은 도메인 명을 기준으로 회원가

입을 수행합니다. ucloudbiz portal (https://ucloudbiz.olleh.com)에서 회원가입 시 도메인입력란에 전달받은 도메인 명을 입력합니다.

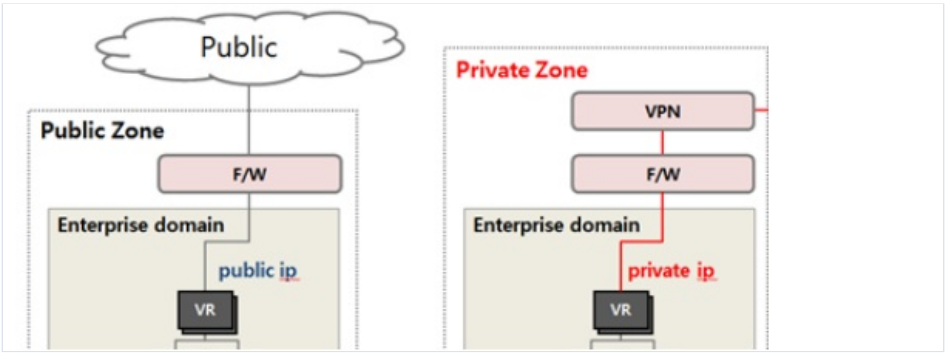
회원가입신청이 완료되면 등록하신 이메일 계정으로 인증메일이 발송됩니다. 접속하시어 '회원가입 완료하러 가기'를 클릭합니다.

상품 신청

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



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

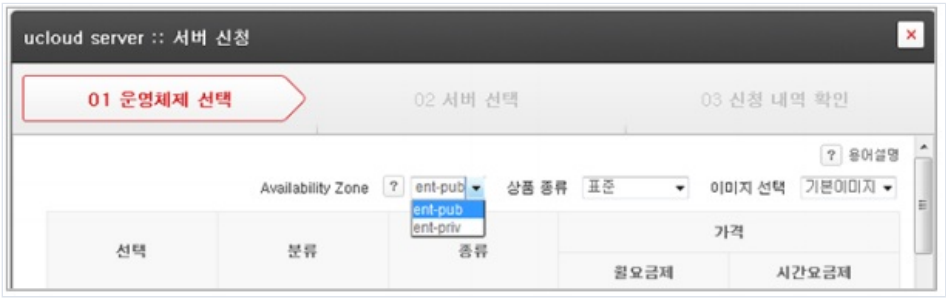


위 그림에서 Public IP는 천안의 경우 14.63.0.0/16 또는 211.253.0.0/16 IP 가 할당되고 Private IP 는 10.220.0.0/16가 할당됩니다. Private IP 는 VPN이나 전용회선을 연동하지 않으면 실제 사용하지 않게 됩니다. 할당 받은 네트워크 자원에 대해 운용센터에서의 별도의 작업(CIP Inter-AZ)이 필요하며 처리되는데 Business Day 기준 약 3일의 시간이 소요됩니다.

VM 생성

상품 신청이 완료되면 다음과 같은 ucloudbiz 서비스 포탈의 클라우드 콘솔 화면을 보실 수 있겠습니다.

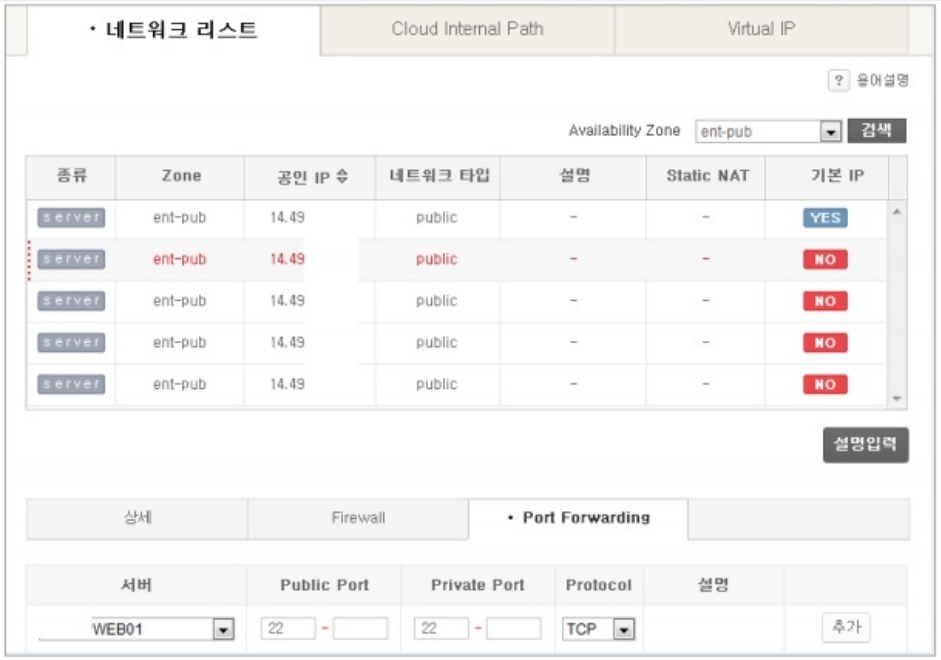
Ucloud server 메뉴에서 '서버 신청'을 이용하여 zone 별로 필요한 VM을 생성합니다. Enterprise Public Zone은 ent-pub, Enterprise Private Zone은 ent-priv로 표시됩니다.



- VM 을 생성할 Zone (Public/Private)을 선택하여 VM을 생성합니다.

Public VR에서 VM으로 Port Forwarding 설정

VR은 Public Zone이나 Private Zone이나 모두 NAT 방식으로 동작합니다. 때문에 Public IP 또는 Private IP 에서 내부 guest network으로 접근하기 위해 Port Forwarding이 설정되어 있어야 합니다. 아래는 Public IP (14.49.X.X)/22번포트 에서 Public VM (web01)/22번 포트로 Port Forwarding을 설정하는 화면입니다.



Private Zone의 VM에 대해서도 VPN이나 전용회선으로 연결하는 경우는 위 그림의 Availability Zone 을 ent-priv로 전환하고 같은 방식으로 설정이 필요합니다.

VM 방화벽 정책 설정 요청

방화벽(Public F/W, Private F/W, Inter-F/W)의 정책설정은 보안 매니지드 서비스를 통해 이용 가능합니다. 서비스 이용을 위해서는 이메일 또는 전화로 연락을 하셔야 하며 첨부양식(첨부#1. 방화벽 정책 신청서)을 참고하여 신청합니다. (Email: mss1@wins21.co.kr, 전화: 031-622-8592~4) 정책설정은 각 방화벽마다 Source/Destination IP에 대해 IP와 Port 단위로 허용/차단 정책 설정이 가능합니다.

고객의 시스템으로부터 public VM에 접속하는 경로는 다음과 같습니다.

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

따라서 고객사가 Public VM에 접근하기 위해서는 Public F/W이 오픈되어 있어야 합니다. 이 때 Source IP는 고객이 접속을 시도하려는 Client IP이고 Destination IP는 2.4 절에서 명시한 Public IP입니다. 예를 들어, 사용자 VM에 원격접속을 하고자 할 때 포탈에서 SSH(22번 포트) 또는 RDP(3389 포트)를 Open 해야 하며 추가로 Public F/W에 Source IP:any → 14.63.XX.XX:22 와 같은 형태로 Open 정책을 요청해야 합니다

Public/Private VM CIP interface 설정

(Public Zone의 CIP는 10.20.0.0/16 내에서 Private Zone의 CIP는 10.21.0.0/16 내에서 할당됨)

CIP를 연결하고자 하는 서버를 서버리스트에서 선택한 후 'Action - CIP 연결'을 해줍니다. 서버에 CIP 연결을 완료하면 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 CIP정보가 보이는지 확인
```

마찬가지로 Private VM의 CIP Interface 활성화 방법도 위의 내용과 동일합니다. (리눅스 서버의 경우에만 해당하며 윈도우 서버는 자동으로 Network Interface가 활성화됨)

하지만 초기 시스템 구축 시 Private VM은 외부에서 접근이 불가하여 직접 설정 또한 불가합니다. 이 경우에는 서버 생성 시에 userdata를 이용하여 자동으로 CIP Interface를 활성화하는 방법과 kt 고객센터에 작업요청을 하는 방법이 있겠습니다. userdata 이용방법은 아래의 zone간 네트워크 라우팅 설정방법에서 확인하시면 되겠습니다. Kt 고객센터에 요청하셔야 하는 경우에는 계정정보, 해당 VM명, VM의 root 패스워드를 공유해주셔야 합니다. 향후 VPN 구성 또는 Public Zone의 네트워크 대역과 라우팅 처리를 통해 외부와 네트워크 연동이 되어있다면 고객센터 요청은 불필요해집니다.

Public Zone 과 Private Zone간 네트워크 라우팅 설정

Public Zone과 Private Zone간 CIP 네트워크 연동은 CIP Inter-AZ 작업을 통해 가능합니다. ('2.4 상품 신청' 내용 참고) 고객센터를 통해 CIP Inter-AZ 작업이 완료되면 실질적으로 각 Zone의 서버에서 상대방 CIP 네트워크 대역을 Routing Table에 등록해주어야 합니다. 예를 들어 Public Zone의 Public 서버(10.20.X.2)에는 Private Zone의 Private 서버의 네트워크 대역(10.21.X.0/24)을 등록하고, 반대로 Private 서버(10.21.X.2)에서는 DMZ 서버의 네트워크 대역(10.20.X.0/24)을 등록해야 합니다.

(Public 서버에서 Private Zone의 네트워크 대역 라우팅 정보를 등록)[root@Public~]# route add –net 10.21.X.0 netmask 255.255.255.0 gw 10.20.X.1[root@ Public ~]# routeKernel IP routing tableDestination Gateway Genmask Flags Metric Ref Use Iface10.20.X.0 * 255.255.255.0 U 0 0 0 eth110.21.X.0 10.20.X.1 255.255.255.0 UG 0 0 0 eth1172.27.0.0 * 255.255.0.0 U 0 0 0 eth0link-local * 255.255.0.0 U 1002 0 0 eth0link-local * 255.255.0.0 U 1003 0 0 eth1default 172.27.0.1 0.0.0.0 UG 0 0 0 eth0(Private 서버에서 Public Zone의 네트워크 대역 라우팅 정보를 등록)[root@Private~]# route add –net 10.20.X.0 netmask 255.255.255.0 gw 10.21.X.1[root@Private~]# routeKernel IP routing tableDestination Gateway Genmask Flags Metric Ref Use Iface10.21.X.0 * 255.255.255.0 U 0 0 0 eth110.20.X.0 10.21.X.1 255.255.255.0 UG 0 0 0 eth1172.27.0.0 * 255.255.0.0 U 0 0 0 eth0link-local * 255.255.0.0 U 1002 0 0 eth0link-local * 255.255.0.0 U 1003 0 0 eth1default 172.27.0.1 0.0.0.0 UG 0 0 0 eth0

Routing Table 등록작업이 완료된 후에는 상대방 IP를 target으로 ping check를 통해 정상통신 여부를 확인해볼 수 있습니다.

단, Private 서버의 경우 초기 시스템 구축 시에는 '2.8 Public/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 userdata를 이용하여 자동설정을 하는 방법이 있겠습니다. 콘솔화면에서 userdata를 이용하는 방법은 아래의 방법을 이용하시고 kt 고객센터로 작업 요청을 하실 경우에는 계정정보, 해당 VM명, VM의 root 패스워드를 공유해주셔야 합니다. (userdata는 리눅스 OS에서만 이용가능하므로 Windows OS 이용 시에는 고객센터로 요청을 주셔야 합니다.)

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

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

Load Balancer 이용 방법

Load Balancer는 Public-LB, Private-LB, Inter-LB를 선택하여 이용할 수 있습니다. Public-LB는 Public Zone에서 생성 가능한 LB로 인터넷망으로부터 들어오는 트래픽에 대한 분산처리를 합니다. Private-LB와 Inter-LB는 Private Zone에서 생성 가능한 LB로 Private-LB는 외부의 고객사전산실에서 VPN/전용회선을 통해 Private Zone으로 전송되는 트래픽에 대한 분산처리를 합니다. Inter-LB는 Public Zone으로부터 Private Zone으로 전송되는 트래픽에 대한 분산처리를 합니다.

LB 신규생성 시 할당되는 서비스 IP는 기본적으로 방화벽에서 차단하고 있으므로 이용을 위해서는 윈스테크넷으로 방화벽 오픈요청을 하셔야 합니다. Public-LB 신규생성 시 할당되는 서비스 IP(14.49.X.X)는 Public F/W에서 차단하고 있습니다. Private-LB 신규생성 시 할당되는 서비스 IP(10.220.X.X)는 Private F/W에서 차단하고 있습니다. Inter-LB 신규생성 시 할당되는 서비스 IP(10.21.X.X)는 Private F/W에서 차단하고 있습니다. LB 방화벽 오픈요청도 '2.7 VM 방화벽 정책 설정 요청'에서와 같이 첨부양식(첨부#1. 방화벽 정책 신청서)을 참고하여 보안매니지드 업체에 이메일 또는 전화(Email: mss1@wins21.co.kr, 전화: 031-622-8592~4)로 신청합니다.

VPN 이용

포탈 화면에서 VPN 이용 신청이 가능합니다. ucloud server 의 네트워크 메뉴에서 세부 메뉴 중 'VPN' 탭을 선택합니다.

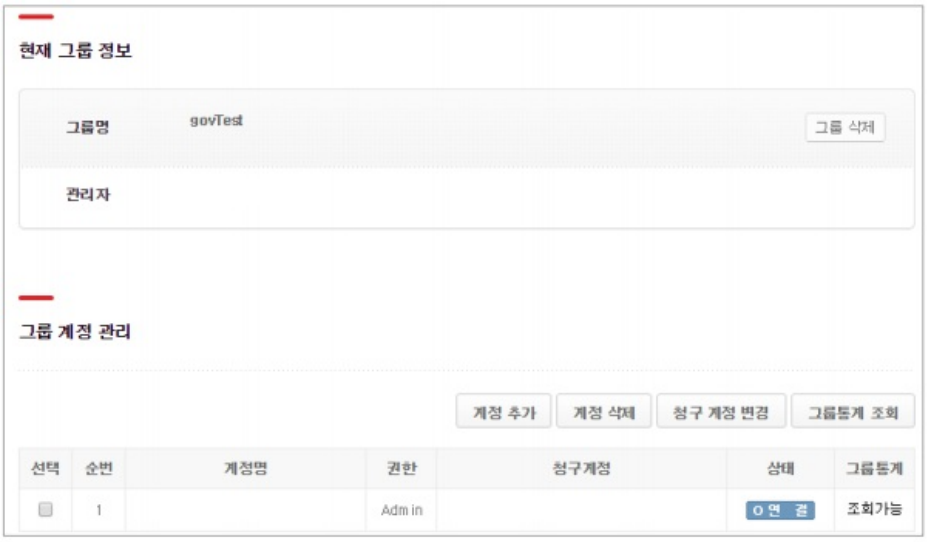
VPN 신청을 클릭하여 VPN 터널링 구성에 필요한 기본 정보를 기입합니다. 신청 이후의 개통 프로세스 및 단계별 점검사항은 포탈의 사용자매뉴얼을 참고바랍니다. (고객센터 > 서비스 이용 가이드 > 사용자 매뉴얼 > 네트워크 > VPN 연동가이드)

https://ucloudbiz.olleh.com/manual/ucloud_VPN_Guide.pdf

그룹계정 관리

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

포탈 메인화면 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 그룹계정으로서 이용하실 수 있습니다.



첨부#1. 방화벽 정책 신청서