GOTOCLOUD
FROM VIRTUALIZATION TO CLOUD

# VDI on OpenStack with Leostream Connection Broker

**Bosung Lee, Ph.D.**

**(bs.lee@gotocloud.co.kr)**

openstack
CLOUD SOFTWARE

GOTOCLOUD
FROM VIRTUALIZATION TO CLOUD

# 목 차



openstack
CLOUD SOFTWARE

# 데스크탑 가상화 (Virtual Desktop Infrastructure, VDI) 개요

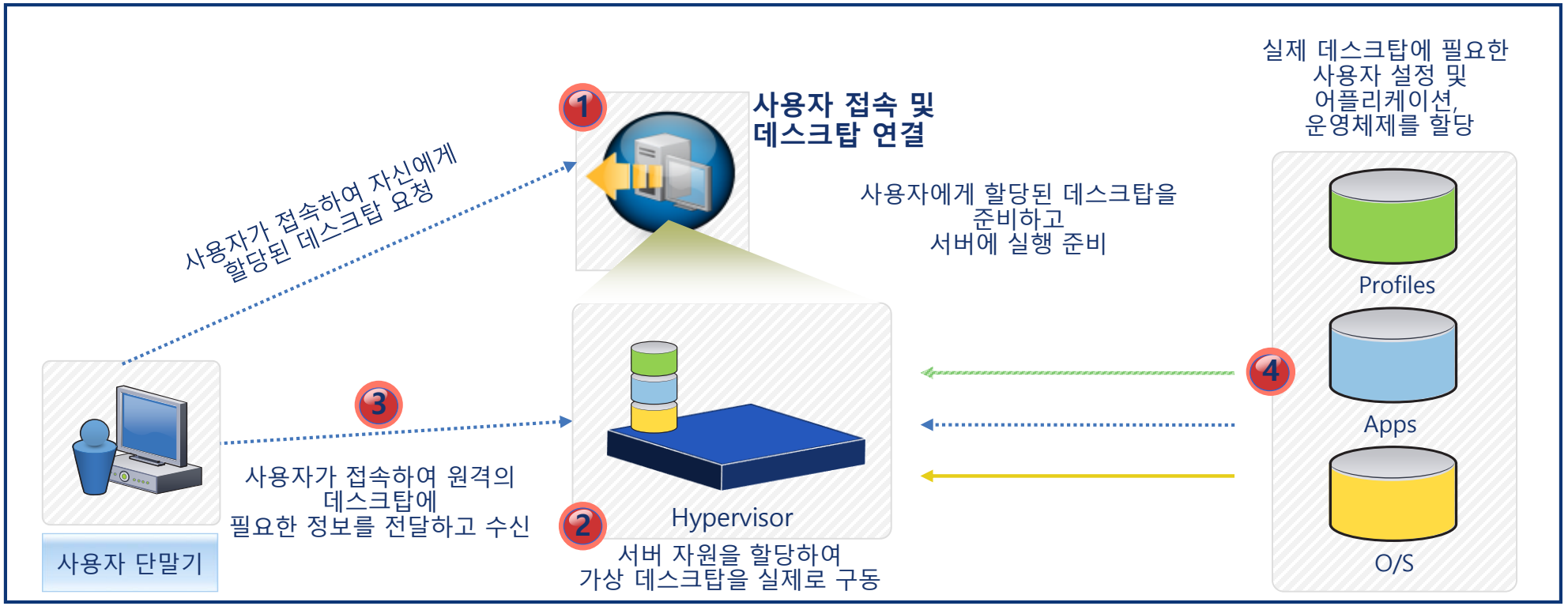
# 가상화 기술 분류

## • 가상화 기술 분류 및 특징

| | 서버가상화 | 프리젠테이션 가상화 | |
|---|---|---|---|
| | | 어플리케이션 가상화 (SBC) | 데스크탑 가상화 (VDI) |
| 주요 특징 | 여러 대의 물리적 서버를 고성능 서버의 가상머신(Virtual Machine)으로 통합 | 서버에 필요한 소프트웨어와 데이터가 준비되고 사용자의 PC는 입출력 장치로 사용됨 | 개인화된 데스크탑을 서버에서 제공, 사용자의 PC는 입출력 장치로 사용됨 |
| 장점 | •자원활용률 극대화<br>•신속한 서비스 제공 및 백업<br>•데이터 센터 비용 절감<br>•IT의 유연성 증대 | •한대의 서버에서 여러 개의 사용자 어플리케이션 사용<br>•신속한 사용자 환경 전개 | •부하 관리 자동화<br>•CPU, Memory, HDD, Network QoS<br>•가상 데스크탑 스케쥴 관리<br>•사용자별 개인화 환경 제공 |
| 유의점 | •데이터 센터 운영프로세스 전환<br>•가상화 도입과정에서 관리 포인트 증가 | •사용자 개인 환경의 제약 (Active-X 등)<br>•3D 환경 등 고성능 자원 제공 방안 (GPU Pass-through 등) 필요 | •3D 환경 등 고성능 시스템 자원 제공 방안 (GPU Pass-through 등) 필요 |
| 적용 업무 | •웹/포탈/데이터베이스 | •Task Worker 업무 | •Power & Knowledge Worker 업무 |
| 제품 | •Vmware vSphere<br>•Citrix XenServer<br>•Microsoft Hyper-V<br>•Red Hat RHEV<br>•Innogrid Cluoudit | •Citrix XenApp<br>•Microsoft RDS (Terminal Server)<br>•ThinApp (Vmware) | •Citrix XenDesktop / VDI-In-a-Box<br>•VMware Horizon View<br>•Microsoft RDS |

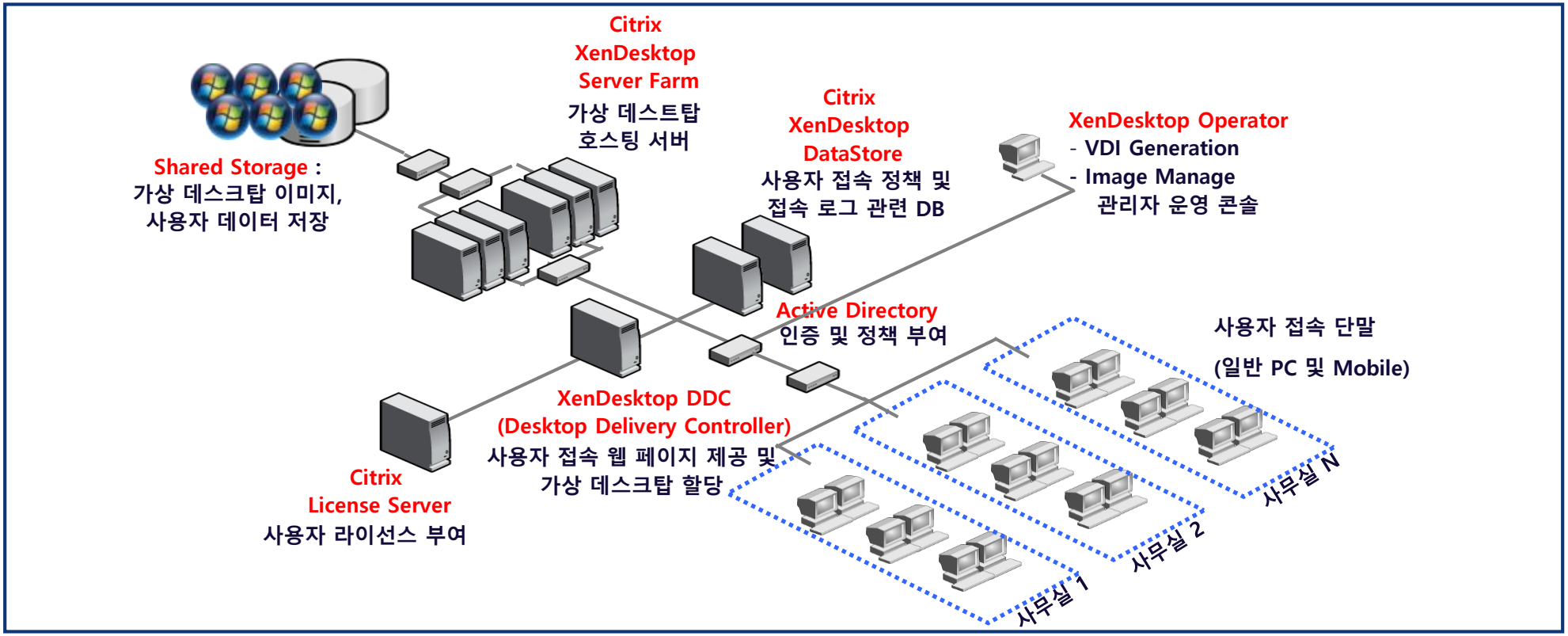
# 데스크탑 가상화 (VDI) 기본 구성 요소

- **데스크탑 가상화(VDI)는 Connection Broker, Hypervisor, Delivery, Provisioning으로 구성**
  - 사용자 접속 환경 및 할당된 데스크탑으로 연결(Broker)
  - 다수의 데스크탑이 실행되기 위한 VM 환경(Hypervisor)
  - 사용자 단말기와 가상 데스크탑을 연결하는 전송 기술(Delivery)
  - 다수의 데스크탑 환경을 보급, 관리(Provisioning)



# VDI 시스템 구성 예시 (Citrix XenDesktop)

- 관리서버 : **DDC, Active Directory, License Server**
- 가상데스크탑 호스팅 서버 : **XenServer, Hyper-V, ESXi 등 Hypervisor 구동**
- **Shared Storage** : 데스크탑 이미지 저장 및 사용자 데이터 저장
- **DataStore** : 가상데스크탑 정책 **DB**, 로그 저장



# VDI 구성 요소 및 역할

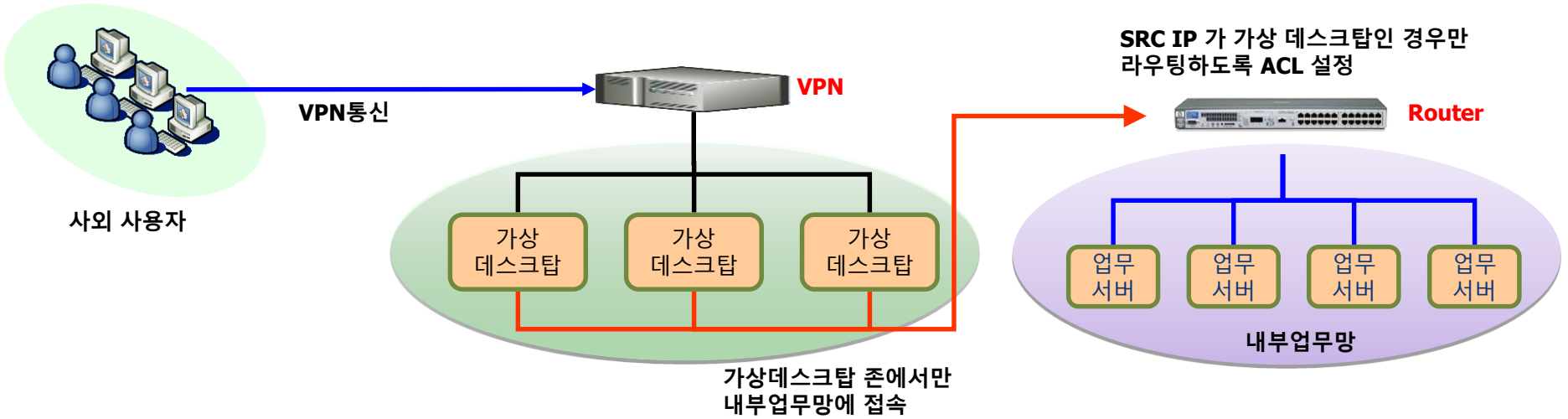
| 구성 요소 | 역할 | Citrix XenDesktop / VMware Horizon View | OpenStack에서의 VDI 구성 요소 |
|---|---|---|---|
| 가상데스크탑 호스팅 | • 사용자 가상데스크탑을 구동하는 서버<br>• Hypervisor 위에 Windows Desktop VM 구동<br>• 가상네트워크 구현 | • Citrix XenServer<br>• VMware ESXi<br>• Microsoft Hyper-V | • Nova<br>• Neutron |
| 웹인터페이스 | • 사용자가 Web browser나 전용 클라이언트를 통해 배포된 가상데스크탑을 이용할 수 있는 웹 인터페이스 제공 | • Web Interface | • 3rd Party Connection Broker<br>• OpenStack에 VM Provisioning<br>• 3rd Party Protocol<br>• User/Policy Mgmt. |
| 프로비저닝 | • 공통 이미지를 이용하여 다량의 가상데스크톱 이미지 생성 | • VM Provisioning on Hypervisor | |
| 데스크탑 전송 | • 가상 데스크탑 사용자 인증 후 사용자 별로 할당된 가상데스크톱을 중계하고 세션 정책을 적용<br>• 관리자는 중앙 콘솔에서 가상데스크톱 할당 정책 및 접속 현황을 실시간으로 확인 | • Desktop Delivery Controller<br>• User/Policy Mgmt.<br>• ICA / PCoIP /RDP | |
| 데이터베이스 | • 가상데스크탑 관리자 정책 및 가상데스크탑 설정 정보를 저장하는 데이터베이스 | • DataStore (MS-SQL) | • 3rd Party DB for Connection Broker |
| 인증서버 | • 가상데스크탑 사용자 인증 및 Windows 사용자 정책 | • Active Directory | • AD, LDAP, RADIUS 등 |
| Shared Storage | • 가상데스크탑 이미지 및 사용자 데이터를 저장하는 공유 스토리지 | • SAN/NAS/iSCSI<br>• Windows File Server<br>• Scale-out Storage | • Cinder, Ceph<br>• Swift |

# VDI 구현 사례

# VDI를 통한 사내 업무망 보안 접속

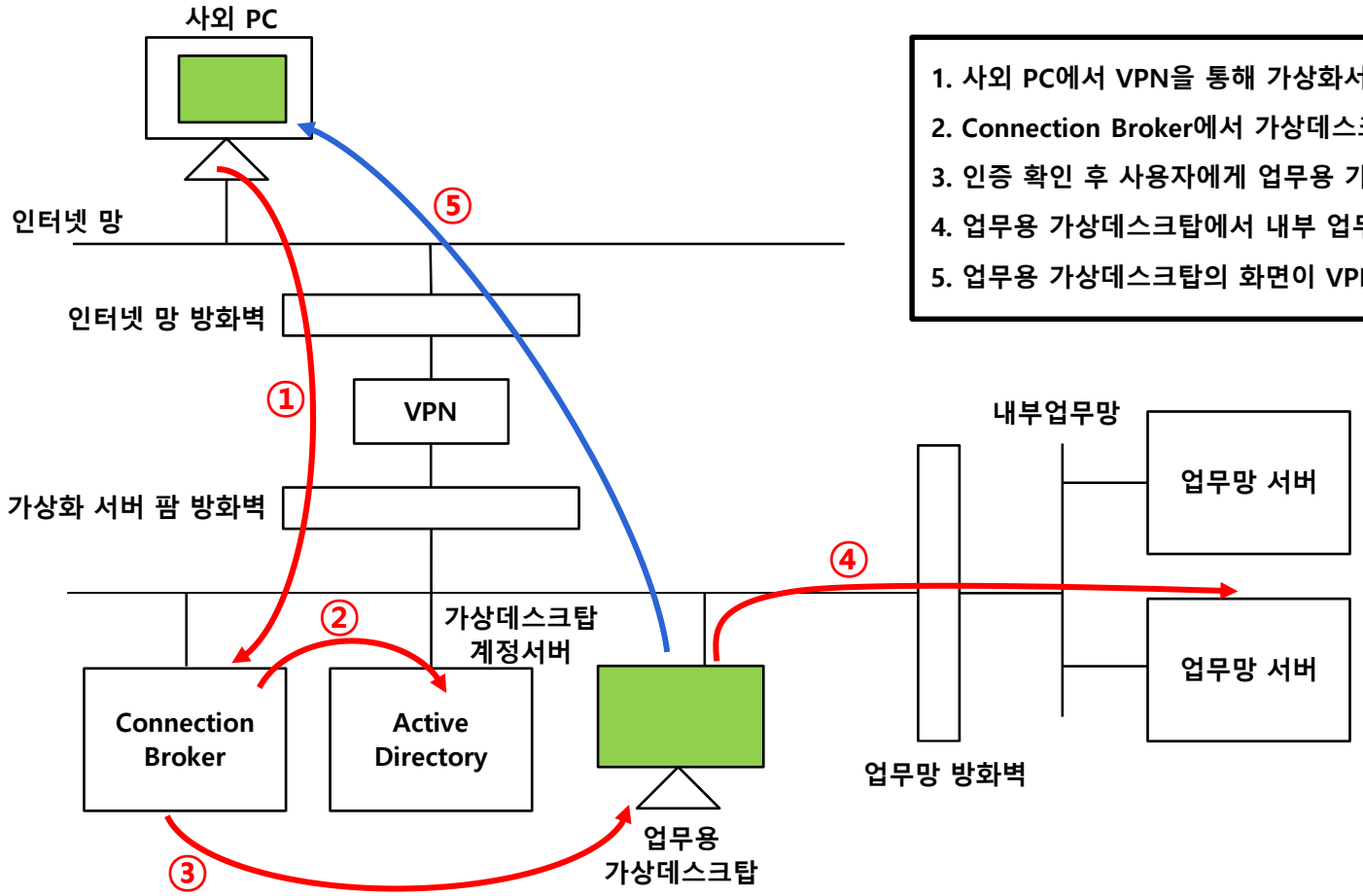
- **VDI를 이용한 사외에서 사내 업무망으로의 보안접속 구현**

| AS-IS | TO-BE | 장점 |
|---|---|---|
| • 내부 시스템의 보안을 위해 내부업무망과 인터넷망을 분리하여 운영 중<br>• 사외에서 내부의 업무망에는 VPN을 통해 접속이 가능하나 내부 정보의 다운로드 방지가 필요함 | • 사내망에 사외접속용 가상데스크탑 존을 구축하고, 가상데스크탑을 통해 내부업무망 접속 허용<br>• 가상데스크탑을 통해서만 내부업무망으로 접속이 가능하도록 가상데스크탑 존과 내부 업무망 사이에 ACL 적용 | • 별도의 물리적인 네트워크 재구축 없이 기존의 네트워크 구성을 통해 보안 접속<br>• 가상데스크탑에 대한 사외접속은 본사에서 제어<br>• 사외에서 내부업무망에 접속 후 내부 업무 가능, 업무 데이터는 가상데스크탑 내에만 저장되므로 데이터 유출 방지 구현 |



# VDI를 통한 사내 업무망 보안 접속

- 사내 업무망 보안 접속 개념도

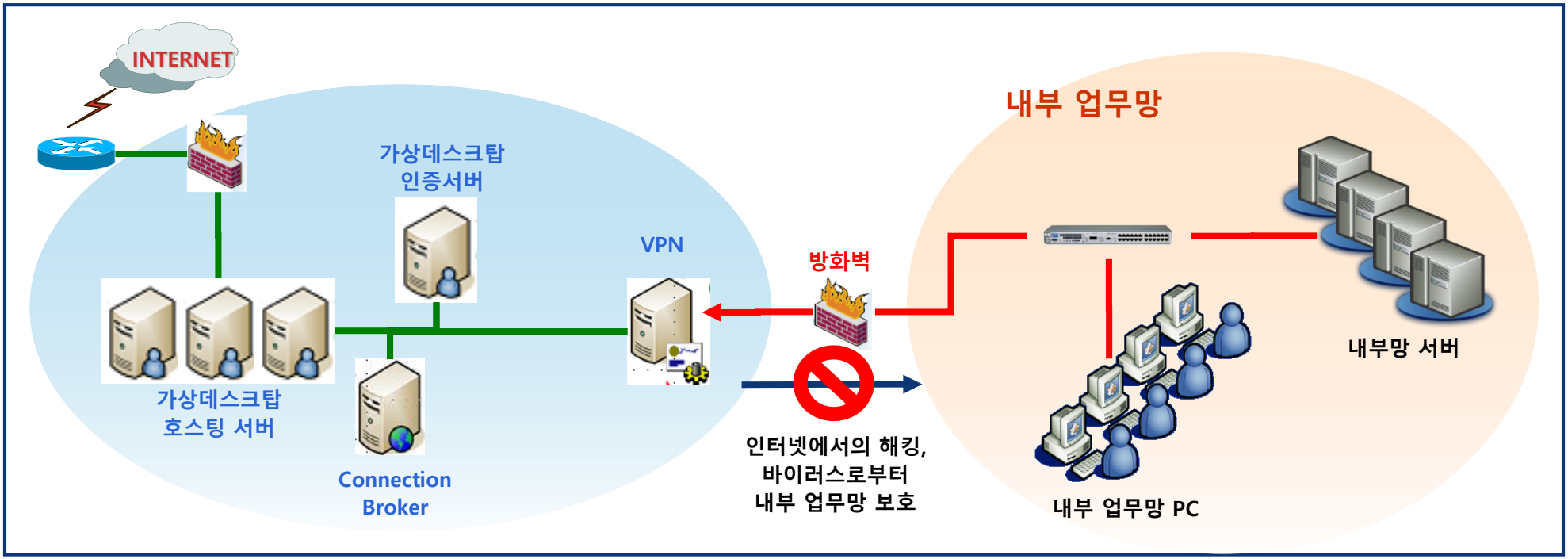



1. 사외 PC에서 VPN을 통해 가상화서버팜의 Connection Broker 접속
2. Connection Broker에서 가상데스크탑 계정서버에 인증 확인
3. 인증 확인 후 사용자에게 업무용 가상데스크탑 할당
4. 업무용 가상데스크탑에서 내부 업무망서버에 접속
5. 업무용 가상데스크탑의 화면이 VPN을 통해 사외 PC에 전송

# VDI를 통한 인터넷 망분리

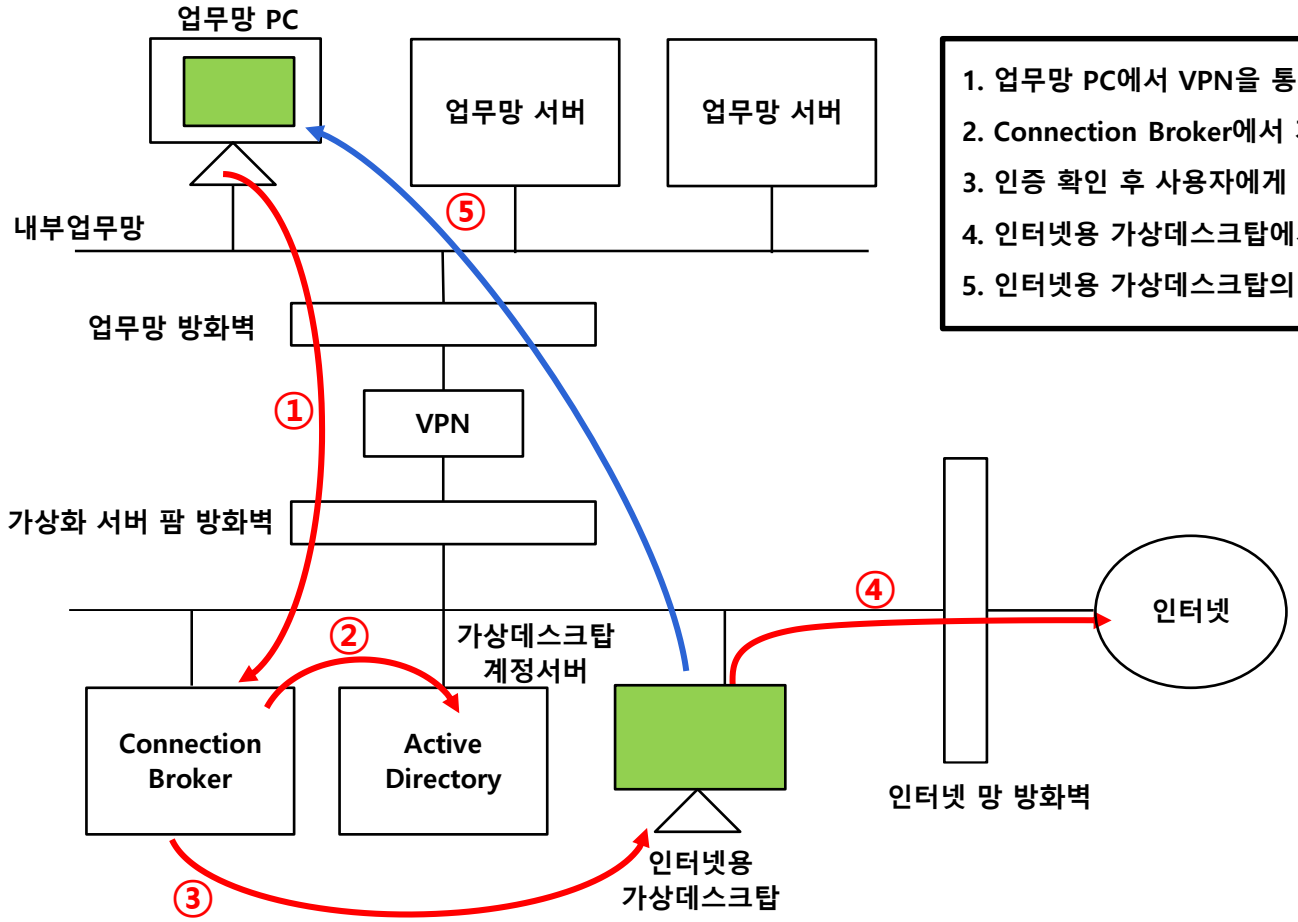
- **악성코드에 의한 내부망 공격을 방지하기 위한 인터넷용 VDI 구현**

| AS-IS | TO-BE | 장점 |
|---|---|---|
| • 물리적인 망분리의 경우 사용자당 2대의 PC 필요<br>• 사용자 PC의 증가로 인한 데스크탑 관리 부하 증가<br>• 전력 및 공간 확보 등 망분리로 인한 시설투자 증가<br>• 물리적인 망분리를 위한 네트워크 투자 비용 증가<br>• 사용률이 낮은 PC의 증가로 인한 IT 자원 비효율화 | • 가상화를 통한 망분리로 사용자당 1대의 PC 유지<br>• 기존의 PC를 이용, 안터넷용 가상데스크탑에 연결<br>• 기존 네트워크 망을 활용 가상화 서버에 접속 | • 물리적 망분리에 비해 데스크탑 관리 부하 감소<br>• 전력 및 공간 확보 불필요로 인한 시설투자비 감소<br>• 논리적인 망분리를 통한 네트워크 투자 비용 절감<br>• 사용률이 낮은 PC에 대한 가상화로 인한 IT 자원 효율화 추구 |



# VDI를 통한 인터넷 망분리

- 인터넷 망분리 개념도




1. 업무망 PC에서 VPN을 통해 가상화서버팜의 Connection Broker 접속
2. Connection Broker에서 가상데스크탑 계정서버에 인증 확인
3. 인증 확인 후 사용자에게 인터넷용 가상데스크탑 할당
4. 인터넷용 가상데스크탑에서 인터넷 접속
5. 인터넷용 가상데스크탑의 화면이 VPN을 통해 업무망 PC에 전송

GOTOCLOUD
FROM VIRTUALIZATION TO CLOUD

# OpenStack과 VDI 환경 통합

openstack
CLOUD SOFTWARE

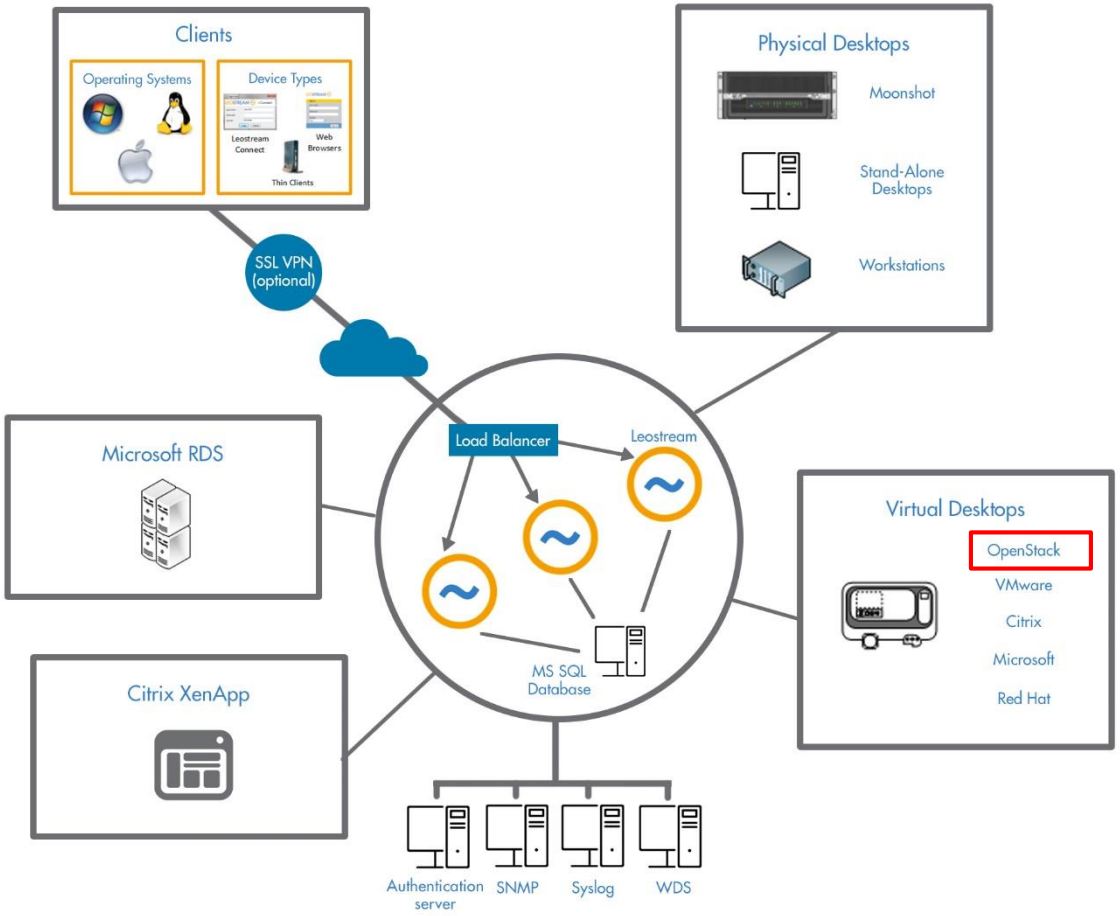
# OpenStack 환경에서 VDI 구현 필요성

- **기존 데스크탑 가상화 솔루션의 한계**
  - 특정 Hypervisor에 종속
    - Citrix XenDesktop : XenServer / Microsoft Hyper-V / Vmware ESX
    - Vmware Horizon View : VMware ESXi
    - Microsoft RDS : Microsoft Hyper-V
    - Red Hat VDI, Verde VirtualBridge : KVM
  - 특정 네트워크 장비(VPN)에서 최적의 성능 발휘
    - Citrix NetScalar / VMware Secure Gateway
  - 데스크탑 가상화 인프라와 IaaS 클라우드와의 통합 어려움
    - IaaS 클라우드 인프라와 데스크탑 가상화 인프라 별도 운영으로 인한 인력, 투자 비용, 리소스의 낭비 발생 우려
    - OpenStack은 Linux 기반, VDI 솔루션은 Windows 서버 기반

# OpenStack과 VDI 환경 통합

| 구성 요소 | 역할 | OpenStack에서의 VDI 구성 요소 | 요구 사항 |
|---|---|---|---|
| 가상데스크탑 호스팅 | • 사용자 가상데스크탑을 구동하는 서버<br>• Hypervisor 위에 Windows Desktop VM 구동<br>• 가상네트워크 구현 | • Nova<br>• Neutron | 만족 |
| 웹인터페이스 | • 사용자가 Web browser나 전용 클라이언트를 통해 배포된 가상데스크탑을 이용할 수 있는 웹 인터페이스 제공 | • 3rd Party Connection Broker<br>• OpenStack에 VM Provisioning<br>• 3rd Party Protocol<br>• User/Policy Mgmt. | **• OpenStack Nova에 가상데스크탑 생성 및 삭제 지원** |
| 프로비저닝 | • 공통 이미지를 이용하여 다량의 가상데스크톱 이미지 생성 | | |
| 데스크탑 전송 | • 가상 데스크탑 사용자 인증 후 사용자 별로 할당된 가상데스크톱을 중계하고 세션 정책을 적용<br>• 관리자는 중앙 콘솔에서 가상데스크톱 할당 정책 및 접속 현황을 실시간으로 확인 | | |
| 데이터베이스 | • 가상데스크탑 관리자 정책 및 가상데스크탑 설정 정보를 저장하는 데이터베이스 | • 3rd Party DB for Connection Broker | **• 다양한 DB 지원** |
| 인증서버 | • 가상데스크탑 사용자 인증 및 Windows 사용자 정책 | • AD, LDAP, RADIUS 등 | **• 다양한 사용자 인증 방식 지원**<br>**• Keystone 통합** |
| Shared Storage | • 가상데스크탑 이미지 및 사용자 데이터를 저장하는 공유 스토리지 | • Cinder, Ceph<br>• Swift | 만족 |

# Leostream Connection Broker




## Leostream 주요 특징

- **Connection Broker**
  - 가상데스크탑 및 어플리케이션 할당 및 관리
  - 웹 인터페이스를 통한 자원관리 및 사용자 정책 관리
  - OpenStack 가상데스크탑 지원
- **Leostream Connect**
  - 가상데스크탑 접속 용 클라이언트
  - Single Sign-on 지원
  - Windows / Linux / OS X 지원
- **Leostream Agent**
  - 가상데스크탑에 설치
  - Connection Broker와 가상데스크탑 간의 정보 교환
  - USB Redirection
  - User idle time monitoring

출처: http://www.leostream.com/product/how_it_works

GOTOCLOUD
FROM VIRTUALIZATION TO CLOUD

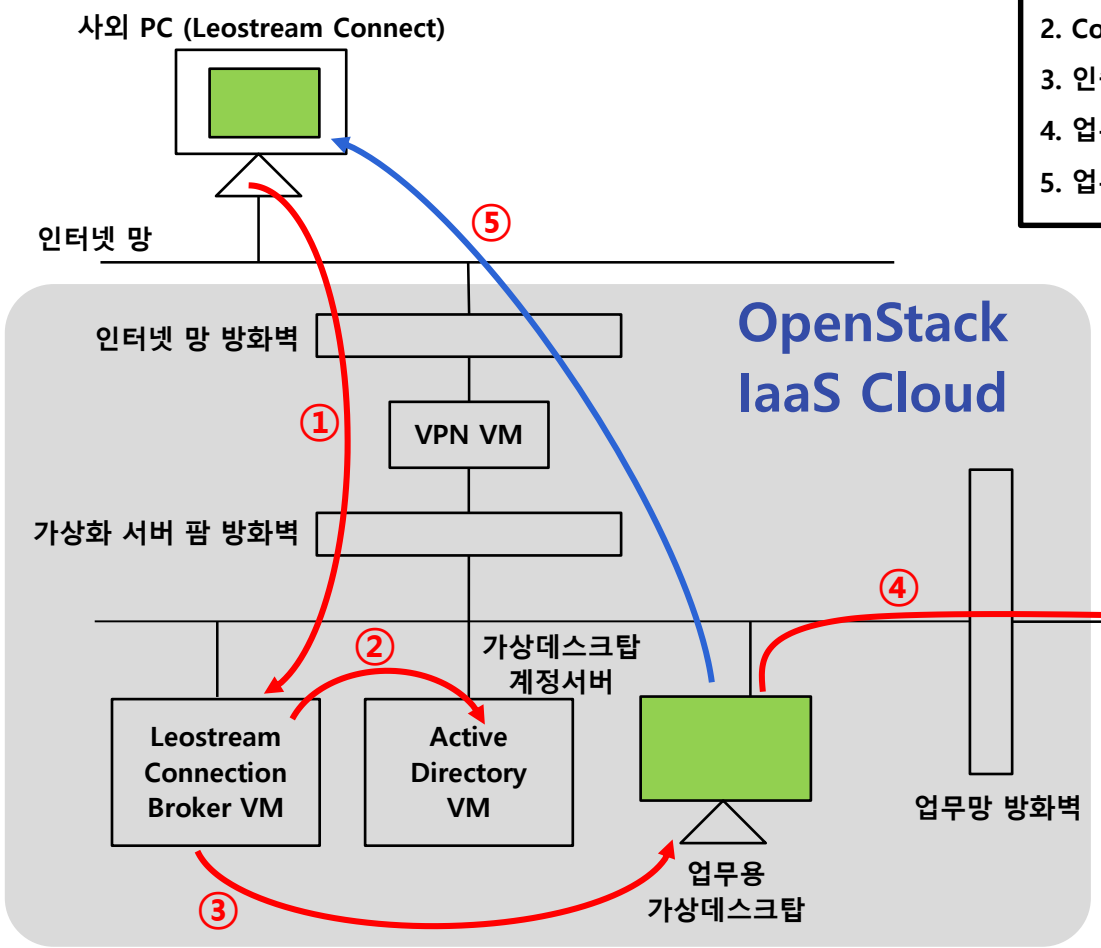
# VDI on OpenStack 환경 구성

openstack
CLOUD SOFTWARE

# OpenStack 기반 VDI를 통한 사내 업무망 보안 접속 구현

- **OpenStack 기반 VDI 사내 업무망 보안 접속 개념도**

1. 사외 PC에서 VPN을 통해 가상화서버팜의 Connection Broker 접속
2. Connection Broker에서 가상데스크탑 계정서버에 인증 확인
3. 인증 확인 후 사용자에게 업무용 가상데스크탑 할당
4. 업무용 가상데스크탑에서 내부 업무망서버에 접속
5. 업무용 가상데스크탑의 화면이 VPN을 통해 사외 PC에 전송




내부업무망

업무망 서버

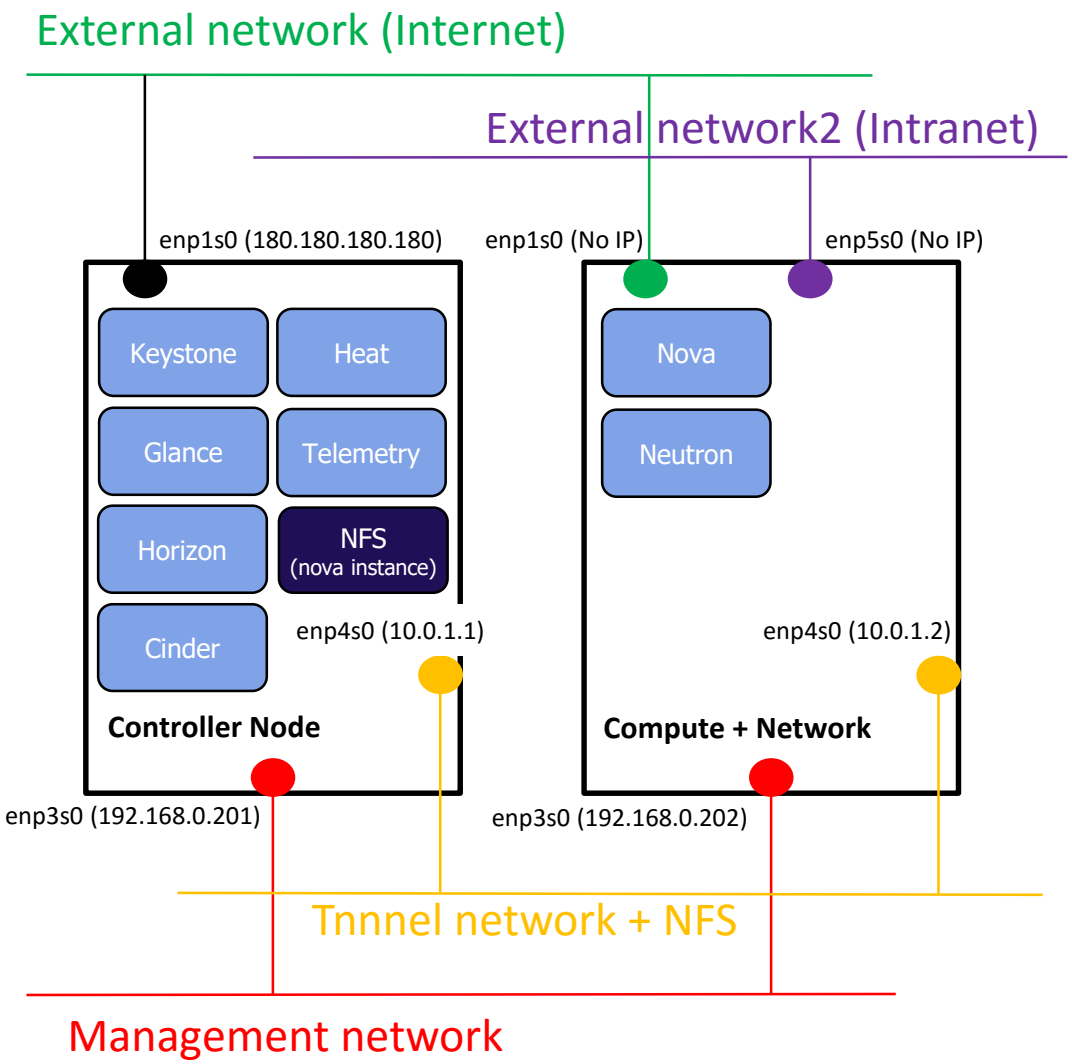
업무망 서버

**Key Concepts**

- Leostream Connection Broker
- Active Directory 인증
- VPN VM
- OpenStack Security Group으로 방화벽 대체
- Leostream Connect로 접속

# GotoCloud OpenStack Configuration

- **서버 구성**
  - 1 Controller, 1 Compute + Network
  - CentOS 7 64bit (KVM)
  - OpenStack Kilo
  - Controller에 OS HDD + Data HDD 설치
    - glance image, cinder volume service
    - nova instance는 controller의 NFS volume에 저장
- **네트워크 구성**
  - 서버당 4개의 NIC 장착
  - enp1s0 : External Network 1 (internet) 연결
    - Controller는 Internet에서 Dashboard 접속용
  - enp3s0 : Management Network
  - enp4s0 : Tunnel network와 NFS network
    - Compute 노드가 늘어날 경우 Tunnel로 사용
    - NFS Network는 분리하는 것을 권장함
  - enp5s0 : External Network 2 (intranet) 연결



# External network2 추가

- **Intranet 연결용 External network2 추가**
  - Neutron L3 Agent 설정
    - /etc/neutron/l3_agent.ini 수정 (Controller node Only!)

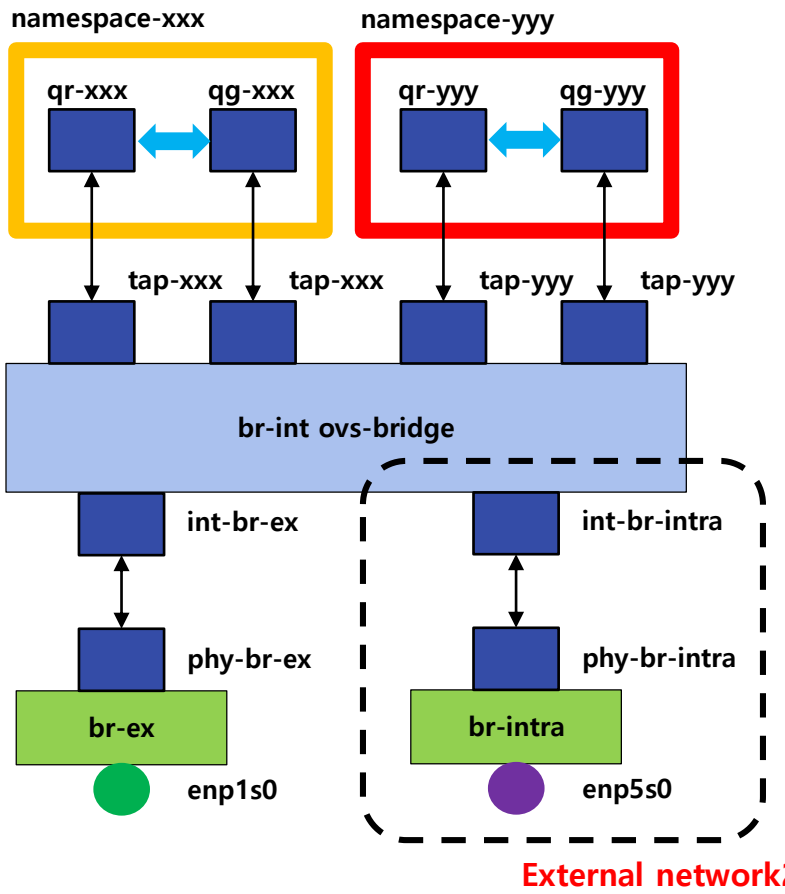
```
external_network_bridge =
gateway_external_network_id =
```

  - Openvswitch Plugin 설정
    - /etc/neutron/plugin.ini (Controller+Compute node)

```
[ml2]
type_drivers = flat, vlan, gre, vxlan
[ml2_type_flat]
flat_networks = *
[ovs]
bridge_mappings = external:br-ex,intranet:br-intra
network_vlan_range = external,intranet
```

  - Bridge 추가

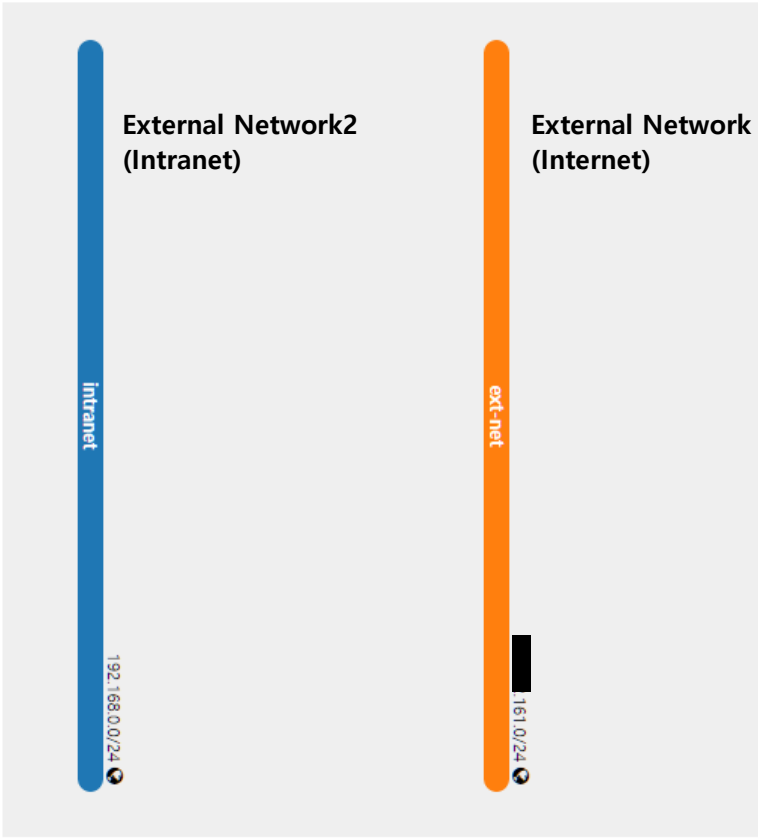
```
# ovs-vsctl add-br br-intra
# ovs-vsctl add-port br-intra enp5s0
# ovs-vsctl add-port br-intra phy-by-intra
# ovs-vsctl set interface phy-by-intra type=patch
# ovs-vsctl set interface phy-by-intra options:peer=int-br-intra
```



# Multiple External Networks – Internet & Intranet

## Network Topology

Small | Normal | Launch Instance | + Create Network | + Create Router




## Networks

Filter | + Create Network | Delete Networks

| Name | Subnets Associated | Shared | Status | Admin State | Actions |
|---|---|---|---|---|---|
| intranet | **intranet-subnet** 192.168.0.0/24 | No | Active | UP | Edit Network |
| ext-net | **ext-subnet** [redacted]161.0/24 | No | Active | UP | Edit Network |

Displaying 2 items

## Subnets

+ Create Subnet | Delete Subnets

| Name | Network Address | IP Version | Gateway IP | Actions |
|---|---|---|---|---|
| ext-subnet | [redacted]161.0/24 | IPv4 | [redacted]161.1 | Edit Subnet |

Displaying 1 item

## Subnets

+ Create Subnet | Delete Subnets

| Name | Network Address | IP Version | Gateway IP | Actions |
|---|---|---|---|---|
| intranet-subnet | 192.168.0.0/24 | IPv4 | 192.168.0.1 | Edit Subnet |

Displaying 1 item

# Default Security Group Rule

- **Internet 에서 VM 접속 (Ingress)**
  - 172.16.100.0 내부의 VM에 대해서는 RDP(3389 tcp) 접속만 허용
  - 172.16.100.1 Router를 통해 내부로 연결
    - Default GW : 172.16.100.1

Subnet Name

vdi-network

Network Address

172.16.100.0/24

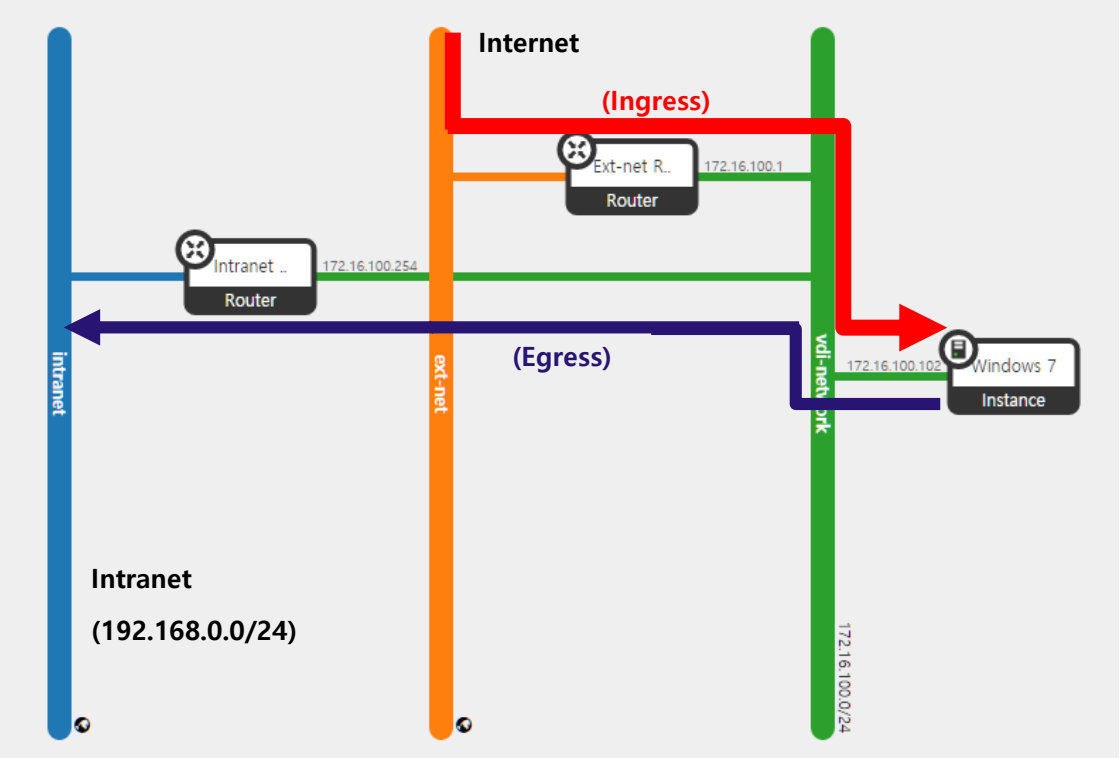
Gateway IP (optional)

172.16.100.1

- **VM에서 Intranet 접속 (Egress)**
  - 172.16.100.0 에서는 192.168.0.0 네트워크로만 접속
    - 192.168.0.0/24 GW : 172.16.100.254

Host Routes

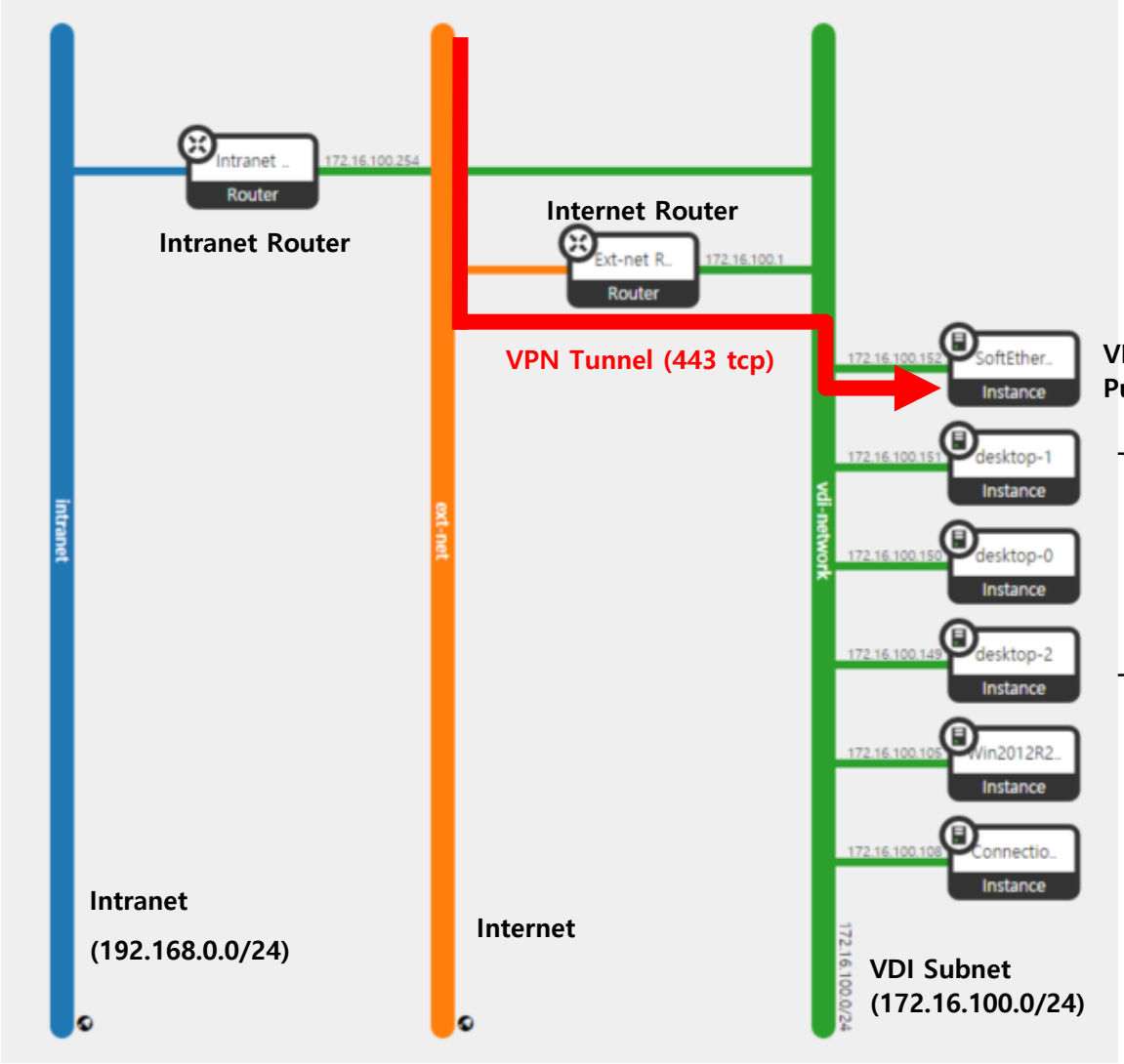
192.168.0.0/24,172.16.100.254




Manage Security Group Rules: default

| Direction | Ether Type | IP Protocol | Port Range | Remote IP Prefix |
|---|---|---|---|---|
| Ingress | IPv4 | TCP | 3389 (RDP) | 0.0.0.0/0 |
| Egress | IPv4 | Any | Any | 192.168.0.0/24 |

# Final Network Topology




1. 사외 PC에서 VPN VM Public IP로 VPN Tunnel 생성
2. Leostream Connection Broker에 로그인
3. Active Directory 에서 사용자 인증
4. 인증 후 desktop-0 ~ desktop-2 VM 할당
5. Desktop VM에서 Intranet (192.168.0.0/24) 접속
6. Desktop VM의 화면이 사외 PC에 전송

VPN VM (SoftEther VPN)
Public IP Association

Virtual Desktops
(Windows 7 32 bit)

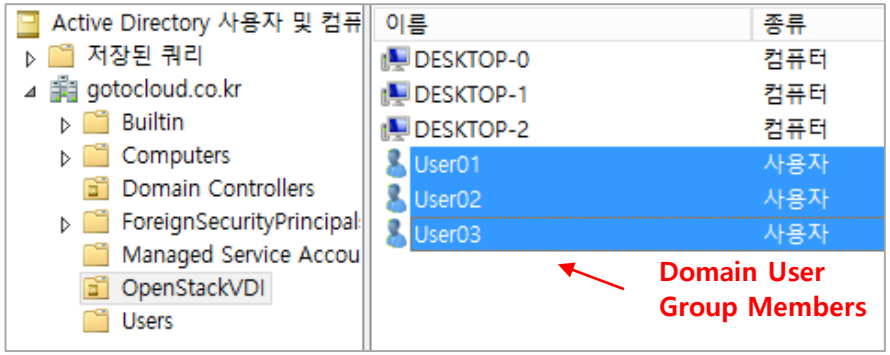
Active Directory
(DNS Server)

Leostream
Connection Broker

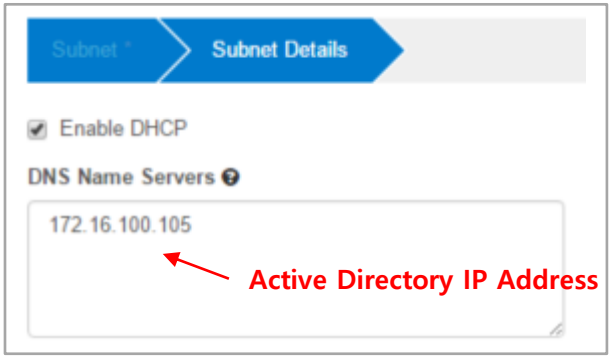
# VDI 구성

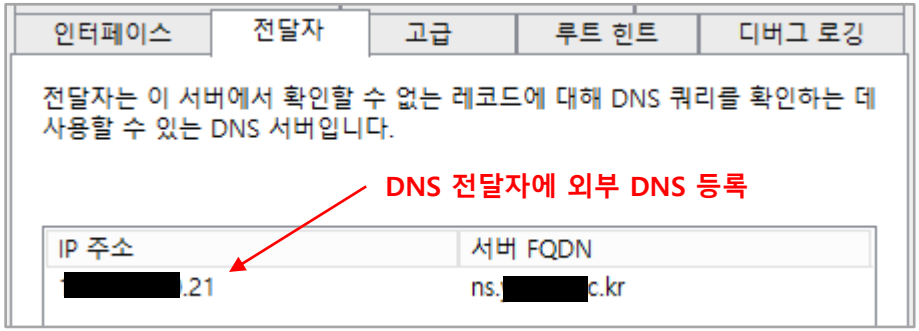
# Active Directory 서버 설치

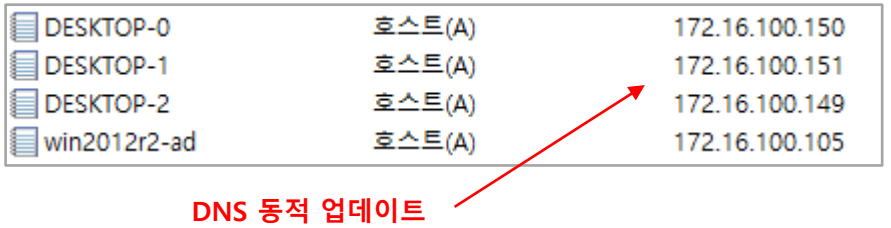
- **DNS 서비스 설치**
  - VDI Subnet 설정에서 DNS 주소를 Active Directory로 지정
    - DNS가 AD로 지정되지 않을 경우 Desktop VM의 AD Join이 실패함
    - 외부 DNS는 DNS 전달자에서 설정
    - DNS 동적 업데이트 설정 (가상데스크탑 자동 추가)
- **VDI User 생성**
  - 조직단위 (Organizational Unit)




- **Domain 방화벽 정책 설정**
  - AD의 도메인 방화벽 정책 가상 데스크탑에 적용

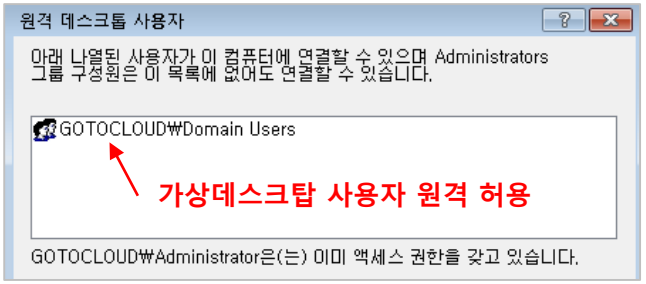


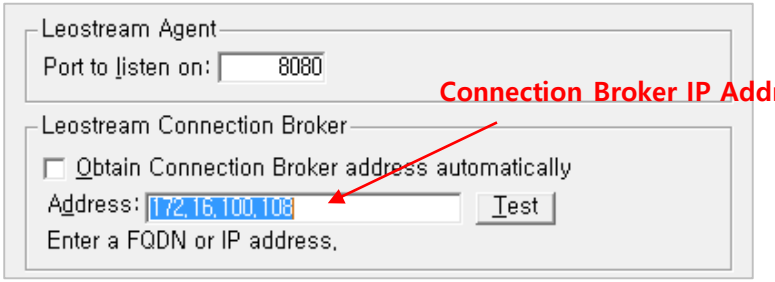



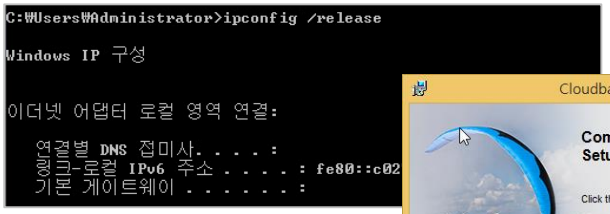



# 가상데스크탑 Master Image 생성

- **VirtIO 드라이버를 포함한 가상데스크탑 OS 설치**
  - OS Update 및 필요한 응용프로그램 설치
- **가상데스크탑 OS 설정**
  - Domain Join 및 원격데스크탑 허용 설정
    - 원격데스크탑 사용자에 Domain User 추가
- **Leostream Agent 설치**
  - Connection Broker 주소와 Port 지정
- **기존 IP해제**
  - DHCP에서 할당된 IP 주소 해제
    - 해제하지 않을 경우 신규 생성 VM에서 IP를 할당받지 못함
- **Cloudbase-Init 설치**
  - Cloudbase-Init 설치 및 Sysprep 초기화 수행
    - Windows OS를 복제할 경우 SID (Security Identifier)가 중복 되면 Domain에 Join에 실패
- **Glance Image 등록**



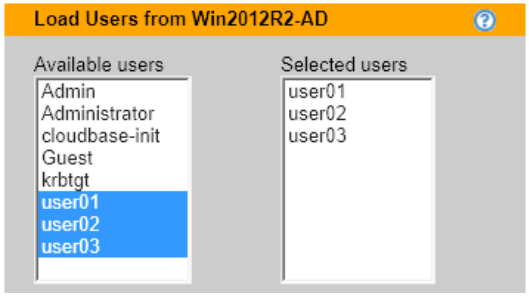





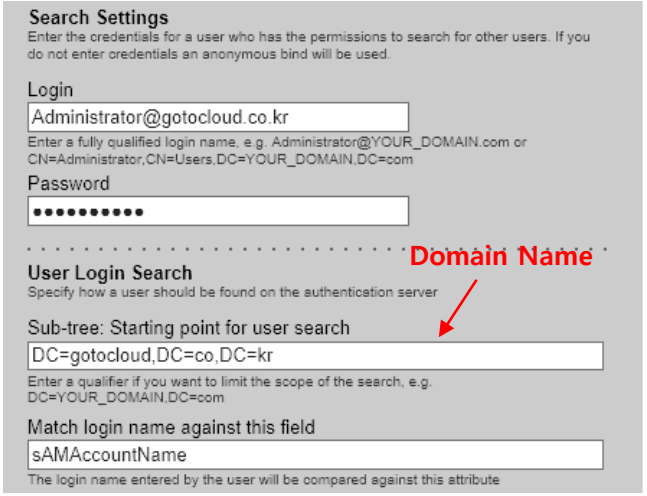
| Image Name | Type | Status | Public | Protected | Format | Size | Actions |
|---|---|---|---|---|---|---|---|
| Win7 VDI Master AD Joined | Snapshot | Active | No | Yes | QCOW2 | 10.2 GB | Launch Instance |

# Connection Broker 설정

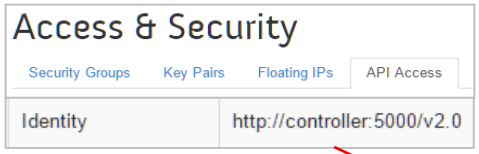
- **Authentication Server 추가**
  - Active Directory 서버 인증서버로 추가
  - AD의 사용자를 VDI 사용자로 추가



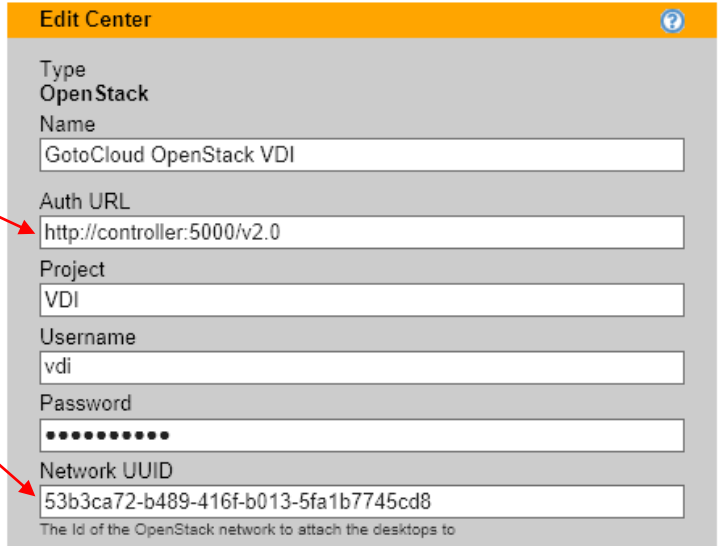





- **OpenStack Center 추가**
  - Auth URL 설정
    - Auth URL을 통해 Connection Broker에서 OpenStack에 연결
  - OpenStack Project, User 설정
  - VDI subnet 추가
    - 가상데스크탑이 연결될 Subnet ID

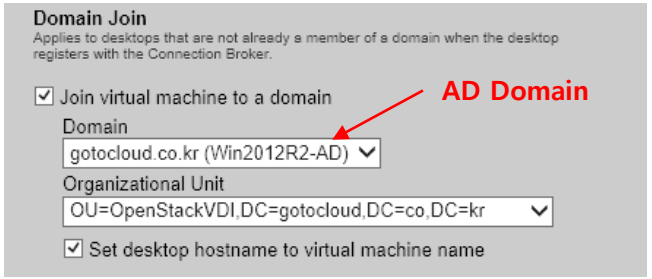




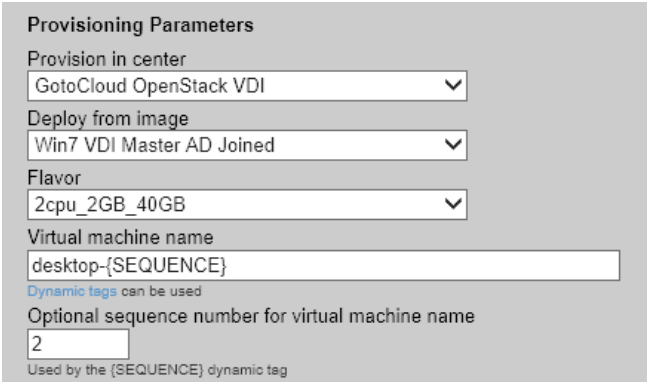


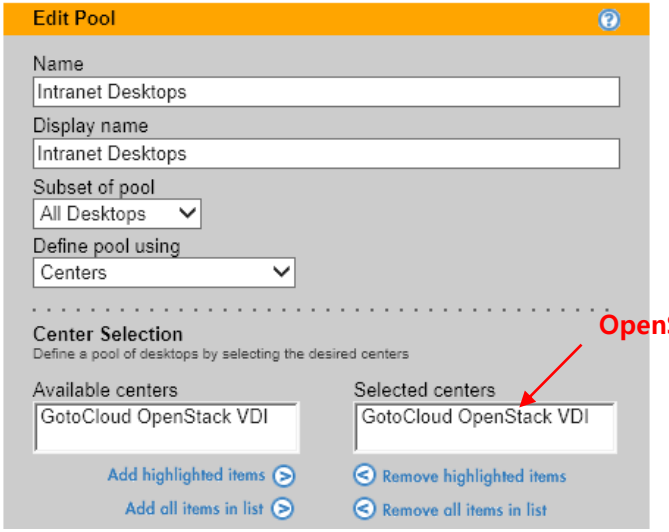
# Connection Broker 설정

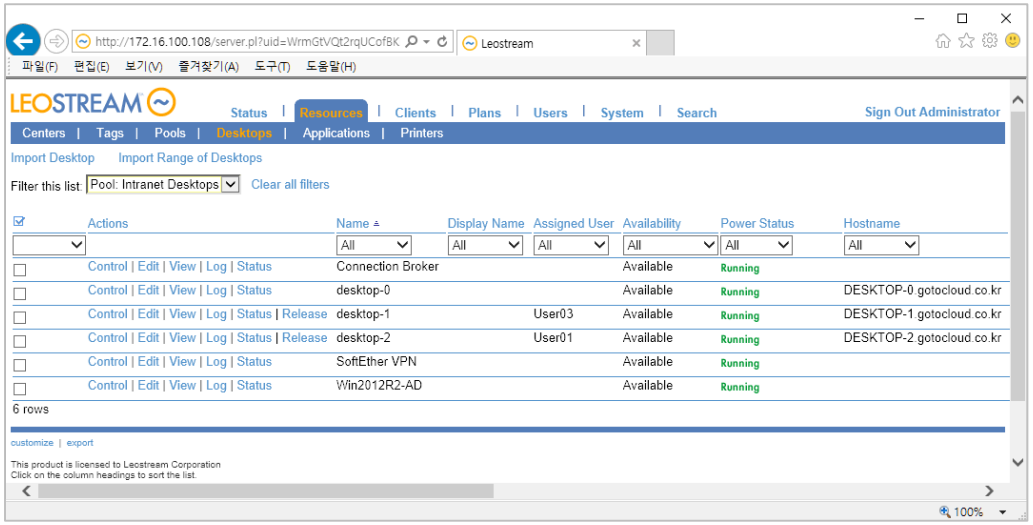
- **가상데스크탑 Pool 설정**
  - Pool에 OpenStack Center추가
    - Center 목록에서 선택
  - 생성되는 가상데스크탑을 Domain에 추가
    - 인증서버에 추가한 AD의 도메인 지정
    - AD가 먼저 추가되어 있어야 함




  - Provisioning Parameter 설정

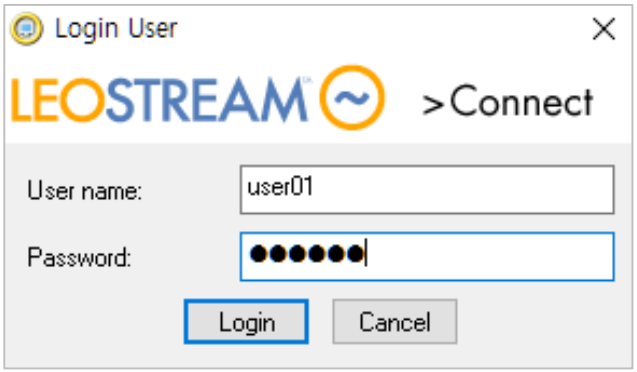


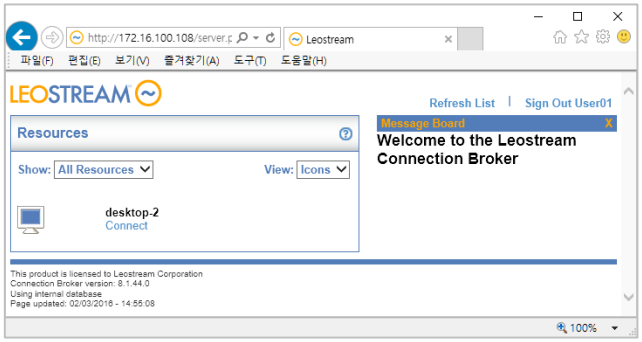



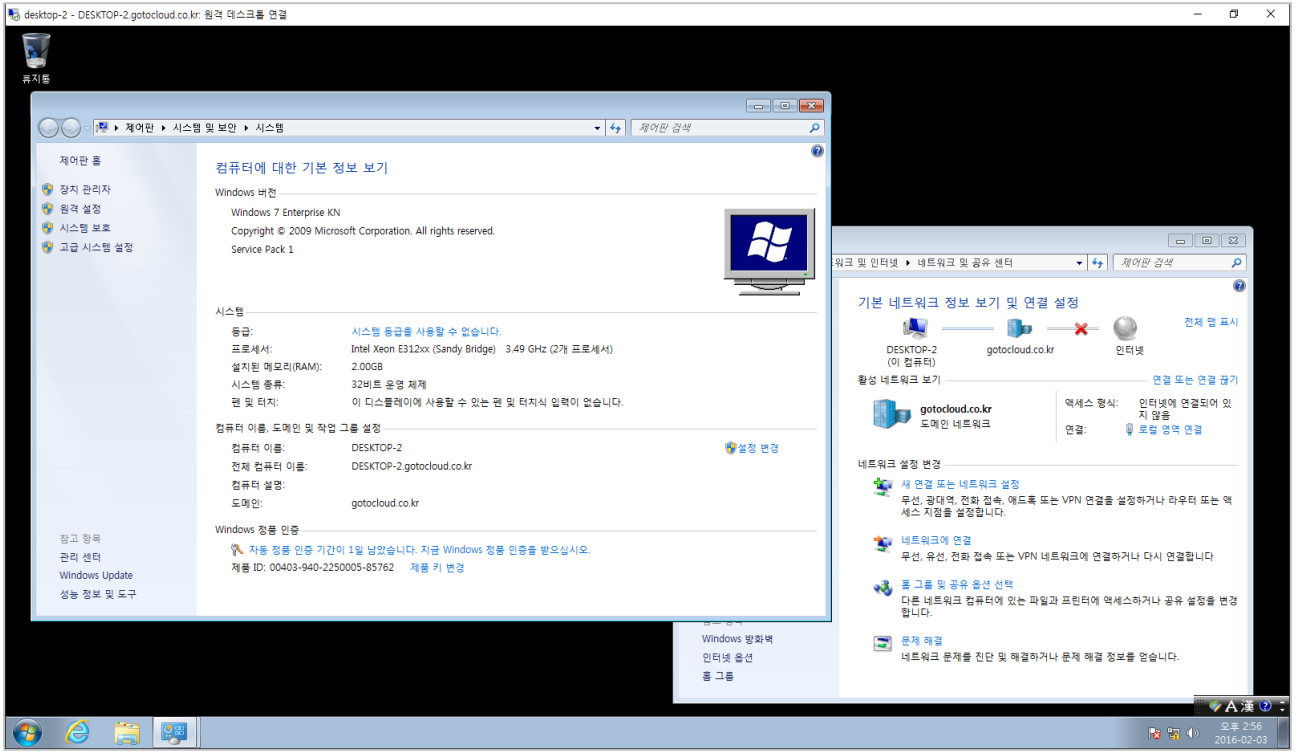



# VDI 접속

- **Leostream Connect 또는 웹인터페이스 접속**



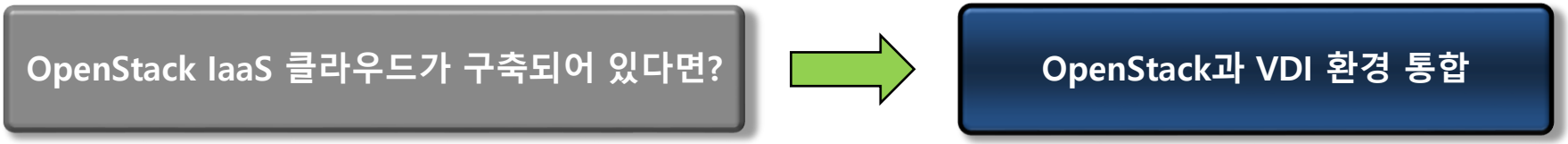



# Conclusions & Future Works

# Conclusions & Future Works

- **OpenStack 환경에서 VDI 구현**
  - OpenStack 환경에서 VDI를 구현함으로써 특정 Hypervisor에 종속 해결
  - 데스크탑 가상화 인프라와 IaaS 클라우드와의 통합
    - IaaS 클라우드 인프라와 데스크탑 가상화 인프라 통합 운영으로 인한 인력, 투자 비용, 리소스의 낭비 감소




- **Leostream Connection Broker**
  - OpenStack을 지원하는 Connection Broker
- **Future Works**
  - 가상데스크탑 Master Image 생성 방식 개선 필요
    - Master Image 생성 : OS 설치 -> 가상데스크탑 구성 -> 일반화 -> OpenStack Image 등록
    - Master Image 변경 : Master Image로부터 VM 생성 -> 변경 작업 -> 일반화 -> OpenStack Image 등록
    - 개선필요 사항 : Connection Broker에서 가상데스크탑 복제 실행 -> Agent 에서 일반화 명령 전송 -> 새로운 데스크탑 복제
  - Swift 등 Object Storage를 가상데스크탑의 사용자 데이터 저장 공간으로 활용
    - VDI에서의 Storage 병목 현상 개선
  - VPN 연동, 모바일 디바이스 지원 Client 개발

# Q & A


GOTOCLOUD
From Virtualization To Cloud

**Bosung Lee, Ph.D.**

e-mail: bs.lee@gotocloud.co.kr
blog: http://gotocloud.co.kr

openstack
CLOUD SOFTWARE



GOTOCLOUD
FROM VIRTUALIZATION TO CLOUD