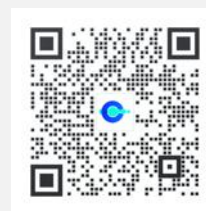


云联壹云 Meetup 19

Part 2：多云虚拟机统一监控

云联壹云核心产品融合云 云联壹云 秉承：简单、开放、融合、智能的产品理念，能够帮助企业实现异构IT基础设施的全面云化、统一管理及成本优化，提高运维效率的同时，降低企业运营成本。

2021-06 后端工程师 郑雨



扫码进技术交流群



更多资讯关注我

目录

CONTENTS

01 多云虚拟机统一监控

·意义 ·实现

02 监控Agent

·安装Agent ·采集数据 ·数据传输

03 总结与演示

·总结 ·演示

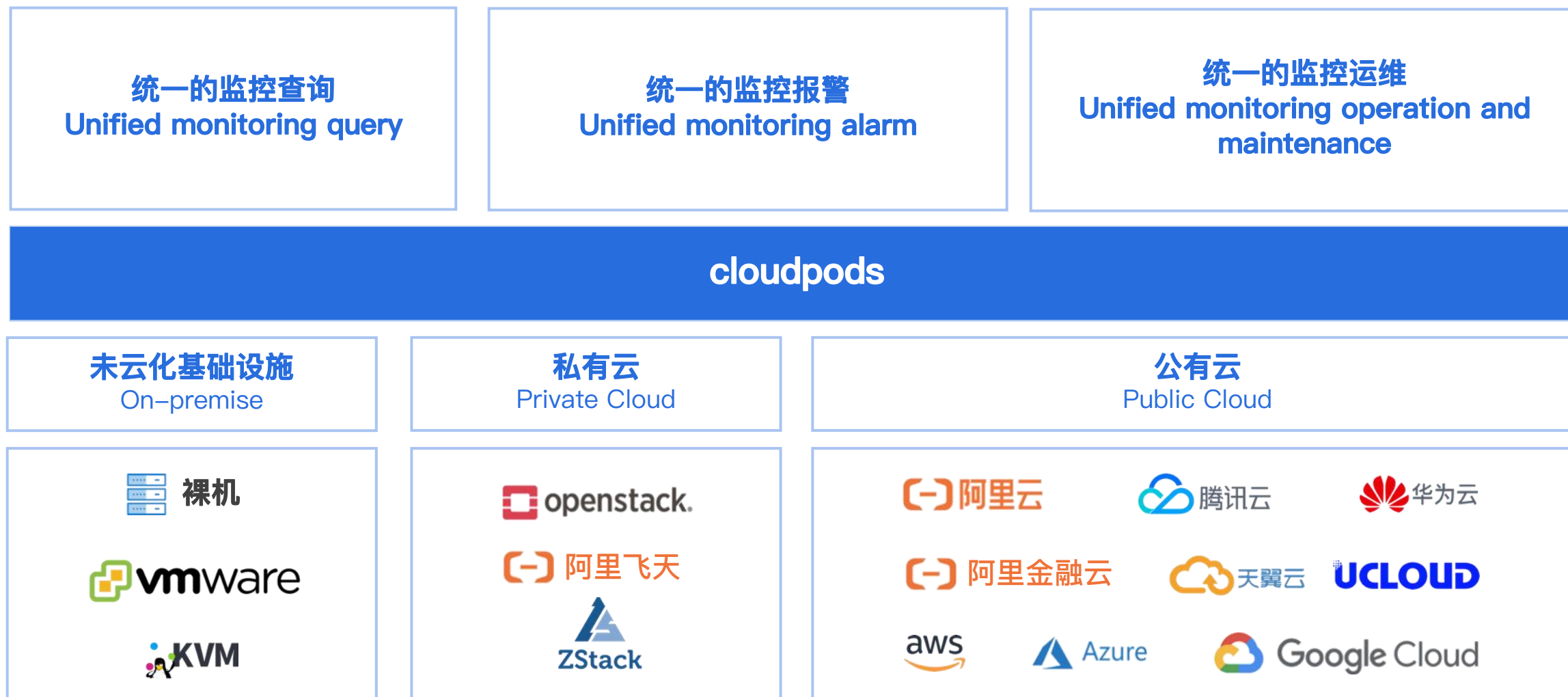
01

多云虚拟机统一监控

·架构 ·实现

架构

利用统一的监控数据进行统一的监控查询、报警以及运维。



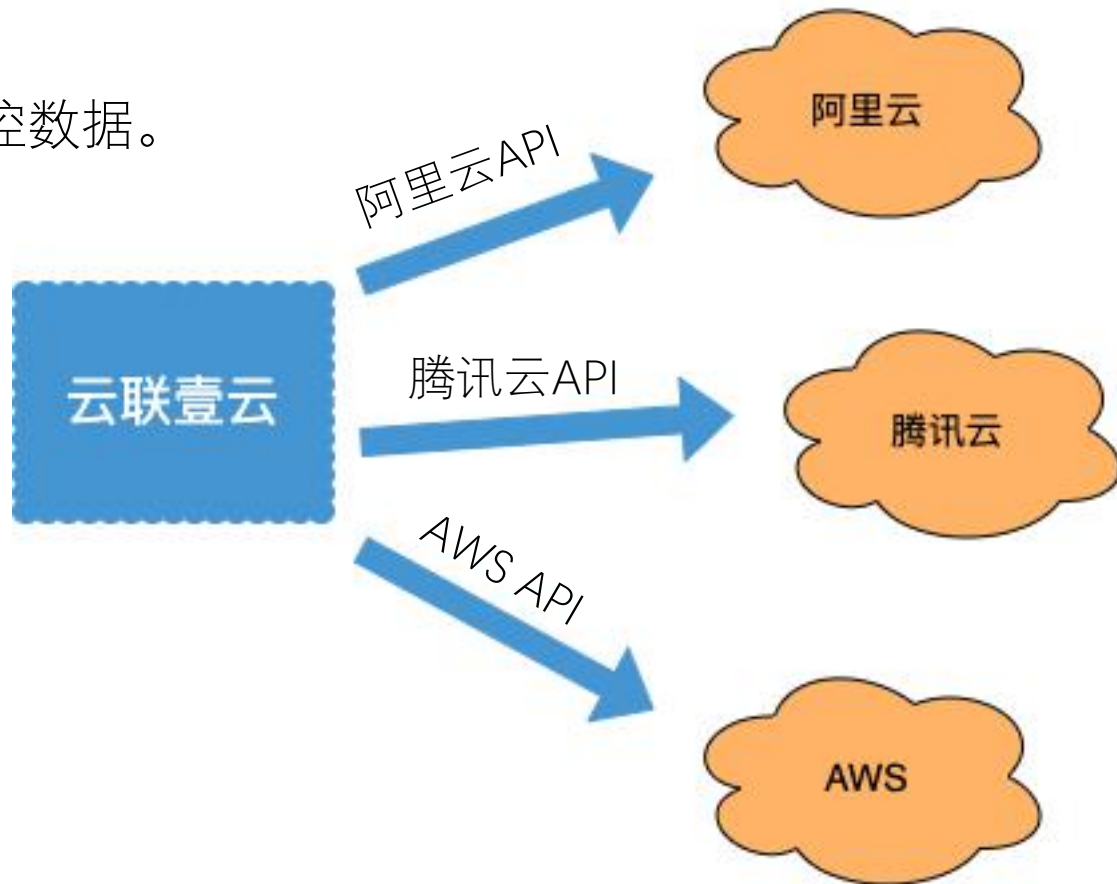
实现

过去的实现

云联壹云调用每个云的API，拿到他们的监控数据。

缺点：

1. 监控数据不统一
2. API 有调用次数限制
3. 监控数据延迟高

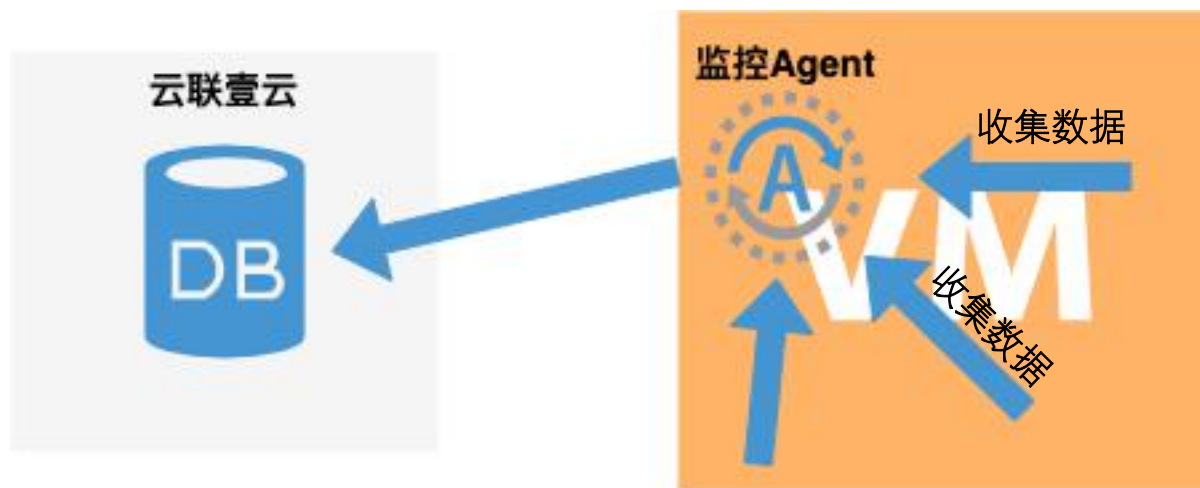


实现

现在的实现

给多云虚拟机安装监控 Agent，云联壹云 通过安装在虚拟机上 Agent 收集监控数据并存储在本数据库。

1. 统一的 Agent => 统一的监控数据
2. 不经过云厂商的API，所以没有监控API调用限制
3. push数据，可控的延迟



02


监控Agent

·安装Agent ·采集数据 ·数据传输

监控Agent

监控Agent是什么

监控 Agent 是运行在虚拟机上的 daemon，采集监控数据，并把数据传回 云联壹云 的 influxdb



如何安装Agent？

如何采集数据？

如何把数据传回来？

2.1

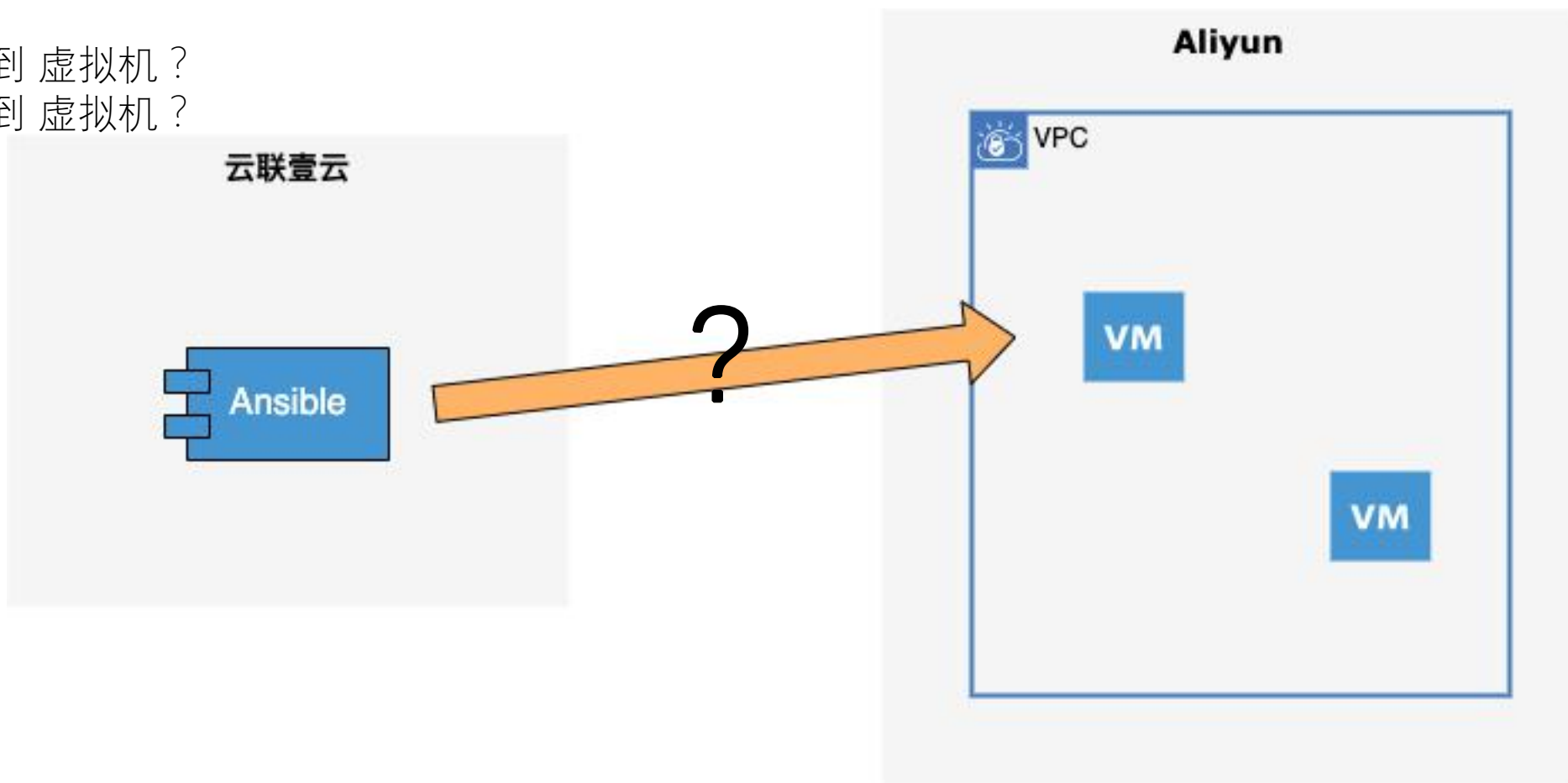
如何给虚拟机安装Agent?

安装Agent

云联壹云使用 Ansible 给虚拟机安装 Agent。

这个过程需要解决的两个问题：

1. 云联壹云怎么连接到 虚拟机？
2. 云联壹云怎么登录到 虚拟机？

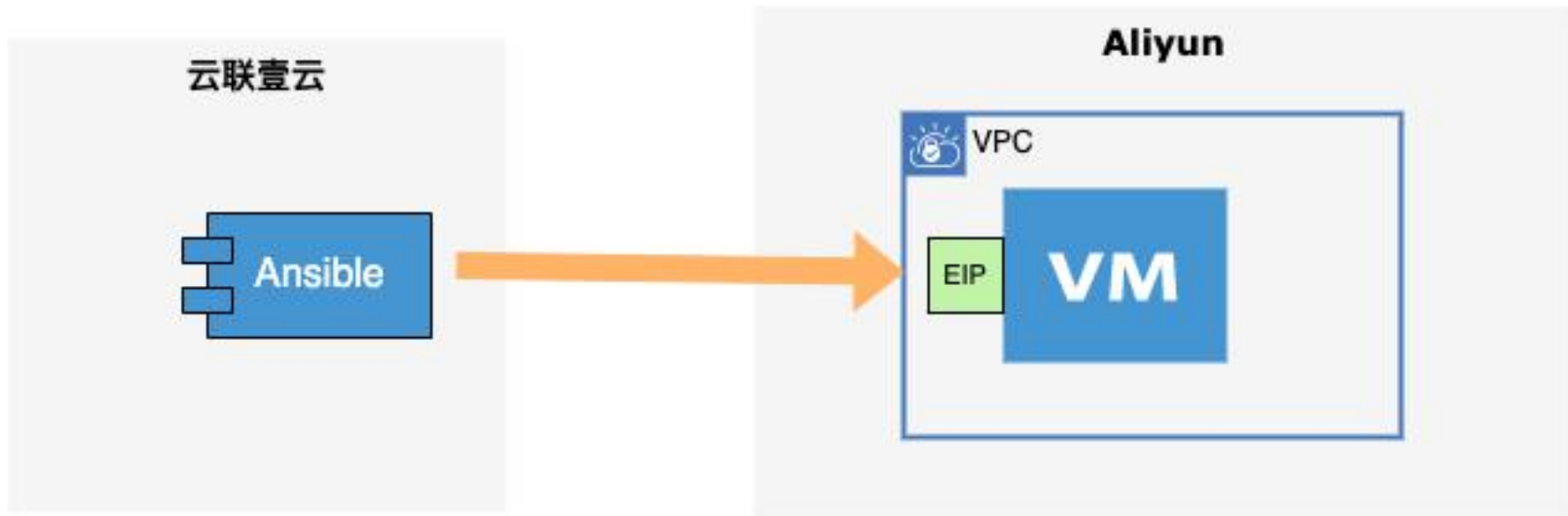


安装Agent

如何登录?

假设云联壹云已经能够连接到 VPC 内部的虚拟机，比如说通过 NAT网关或者虚拟机已经绑定了 EIP 等。

1. 使用云联壹云创建的虚拟机本身是满足这种条件的，云联壹云会在虚拟机上自动创建一个可以通过公钥登录的 cloudroot 用户，私钥存储在本地数据库。
2. 否则，需要用户帮助 cloudpods 配置免密登录。



安装Agent

用户协助配置免密登录

用户在前端输入虚拟机的用户名和密钥/密码，以使云联壹云能够暂时登录到目标虚拟机，云联壹云会使用 ansible 在目标虚拟机上创建 cloudroot 用户，并设置公钥登录，以达到刚才的第一种情况。

设置方式：

密钥

密码

脚本

设置方式：

密钥

密码

脚本

* 用户名： ②:

root

* 密码：

请输入密码



安装Agent

用户协助配置免密登录

那其实也可以直接让用户在虚拟机上执行脚本，以达到创建 cloudroot 用户以及配置公钥登录的目的。

设置方式：

密钥

密码

脚本

脚本：

❗ 请使用root或具有sudo权限的用户在虚拟机中执行以下脚本，执行完成后，单击探测，测试虚拟机免密登录状态

```
1 user="cloudroot"
2 adminpub="ssh-rsa
  AAAAB3NzaC1yc2EAAAADAQABAAQCsCKpYsS0vpMFLEaeNzgMd321kcPwRmlCljXM
  T17BFHZ4cWylc//iwZrWO4RatDZ6RbHLi5r5exXPEPL6SazAaeoODZhMjeKEqr0y5ieEe5cH
  g5aK4aa4g0GvsuFuP+v/wCaUGZU7qyPLn32oFCc/GRGq3GzO23P0xc5SKpvLHFQ9qwZU
  sTy8qD9CJzEE5vJWYSvCRDpNt8iDYi7BmlzzwPnanr2UNVCLTMg9e0vdckysMRy7bc2b/gB
  gOyDB5MO8cJ1Wg1vVyMhDSicGutf0OGZldhAJQ/YKoJ0lcnuafxAWZmGI07YLBsOGBqm6f8
  55UKh1NyJJc67ck7dHTuD"
3 projpub="ssh-rsa
  AAAAB3NzaC1yc2EAAAADAQABAAQCs2avuo6rutxph2l+yUQeVQYFVFSZRqDCLTO27U
  2/TiDOHXLg4v+Fb8pHQnPQUE4qy7fnUgyW2UNkrFto70H3dM9ULVGzv5mETWb4k24mLF
  wq6srteV7ACkOz/jEhmuev6jgHXx+dOkYMlta34nzbUj/xCsZvBzA8fVlkvpclThqEMXBwwl6V
  Y4p1voLQlexo4CA9O07V1g0Vtmjr2F6mCtJfuPUD4HsyvBplQsCBihsc3QuP8iMbb8t7f7FbFS
  3ZpbjH8rAr43vkiXqfxZFq4T6QgVnJNDDGbuY55/EHeYp7LRrLw4f/YRZw31yY2Lr7G2rumS
```

📋 点击复制

安装Agent

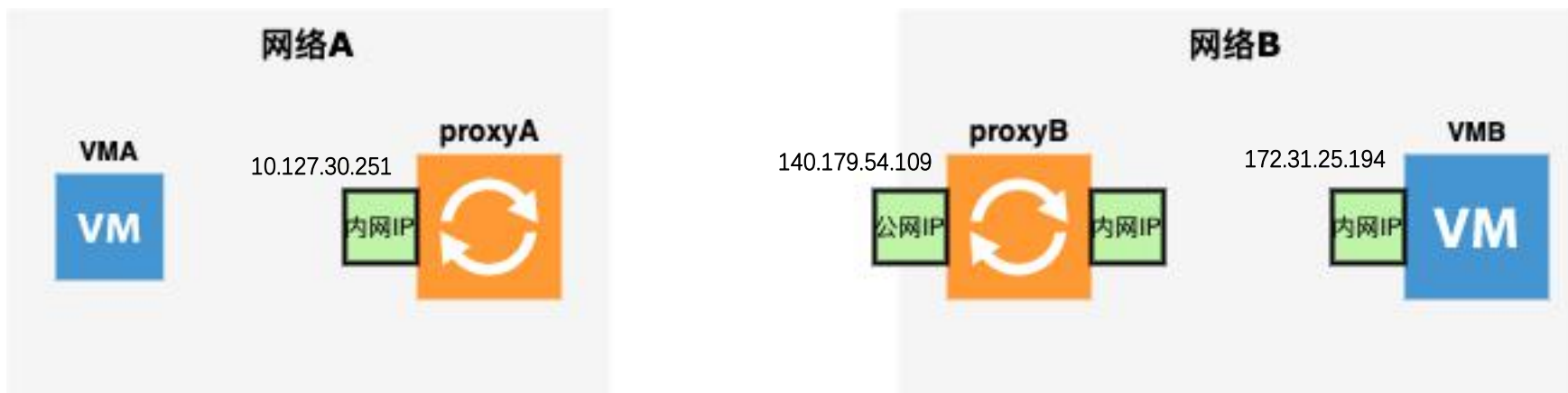
无法直接连接

上面假设了云联壹云是可以直接连接到VPC内部的虚拟机，如果不行呢？

使用 SSH 代理，Local Port Forwarding。

安装Agent

SSH Local Port Forwarding



假设网络A和网络B是两个隔离的网络，如果能让VMA能够访问VMB上监听在 80 端口的web服务应该怎么办呢？

在 proxyA 上执行 `ssh -NfL 10.127.30.251:12345:172.31.25.194:80 cloudroot@140.179.54.109`

执行上面的命令要求 proxyA 能够以 cloudroot 用户正常登录到 proxyB 上，这个可以通过前面讲到的登录方法来解决。

然后 VMA 只要访问 10.127.30.251:12345 就能够访问 VMB 上的 web 服务。

安装Agent

SSH Local Port Forwarding



在 proxyA 上执行 `ssh -NfL 10.127.30.251:12345:172.31.25.194:80 cloud` root@140.179.54.109

会在 proxyA 和 proxyB 之间建立 SSH 隧道，并在 proxyA 上创建一个 port forwarding，它将监听 10.127.30.251:12345，一旦有请求发来，就会通过 SSH 隧道转发到 proxyB，proxyB 会把请求转发到 172.31.25.194:80

然后 VMA 只要访问 10.127.30.251:12345 就能够访问 VMB 上的 web 服务。

安装Agent

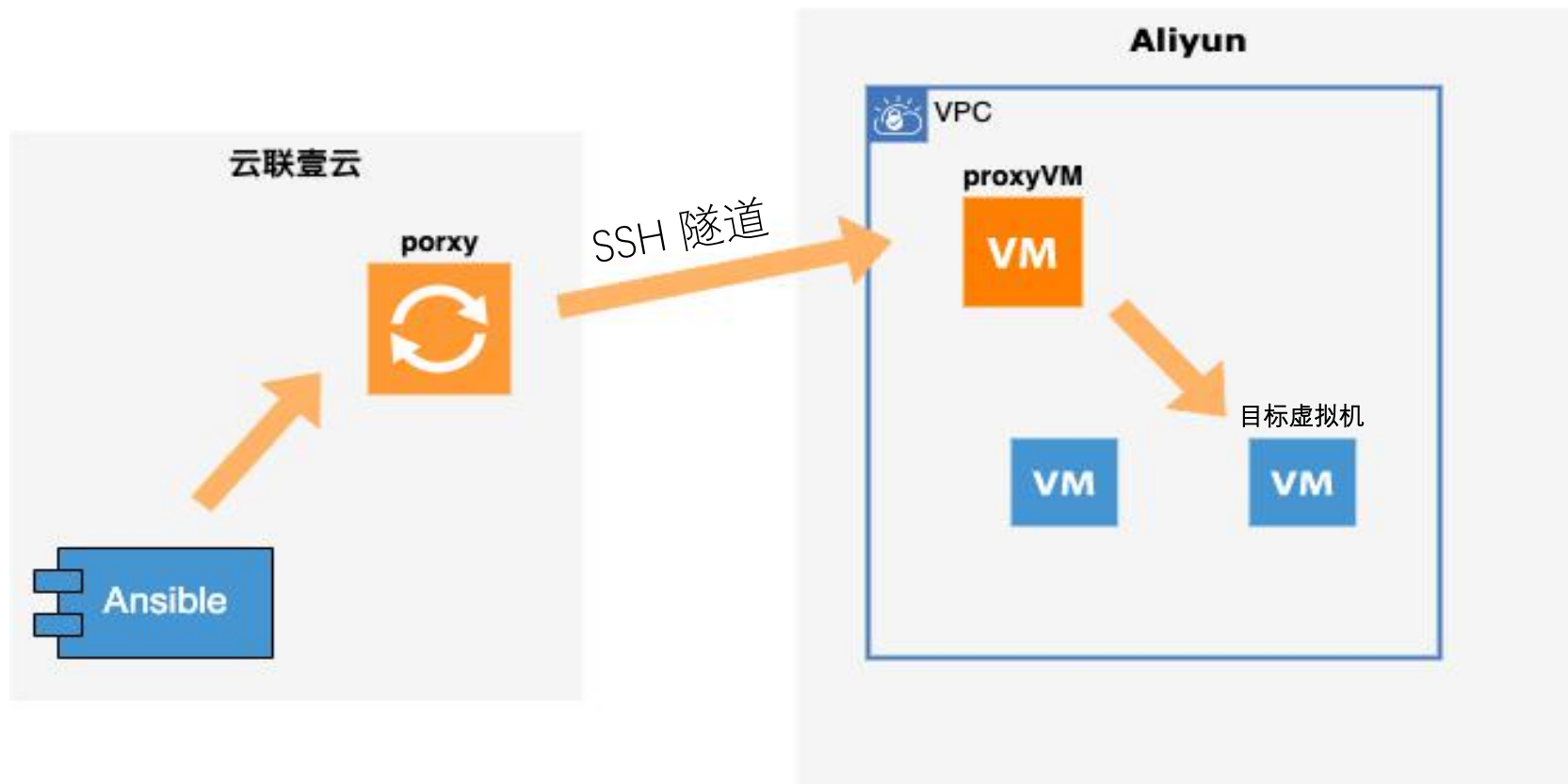
云联壹云连接到VPC内部虚拟机

用上面的 SSH Local Port Forwarding：在 VPC 内部找一个即可以被云联壹云访问到，又可以访问目标虚拟机的 proxyVM；在云联壹云上启用一个 proxy 服务。

在 proxy 和 proxyVM 之间
建立 SSH 隧道

并在 proxy 上建立 local
fowarding 对应到目标虚拟
机的 22 端口

Ansible 就可以通过连接
proxy，进而连接到目标虚
拟机



A blue parallelogram graphic with a white dot in the center, tilted at an angle.

2.2

监控Agent如何收集数据？

监控Agent

实际上是Telegraf

第一版的监控 Agent 其实是 Telegraf。

定制了下配置文件以采集云联壹云需要的数据。



Telegraf 是收集、处理、聚合和编写指标的Agent。

Telegraf 是开源的。

Telegraf 可以灵活地配置，采集什么样的数据，把数据送到哪里。

[glo

```
#####
#                                OUTPUTS                                #
#####

[[outputs.influxdb]]
  urls = ["https://192.168.12.251:50041"]
  database = "telegraf"
  insecure_skip_verify = true

#####
#                                INPUTS                                #
#####

[[inputs.cpu]]
  name_prefix = "agent_"
  percpu = true
  totalcpu = true
  collect_cpu_time = false
  report_active = true
[[inputs.disk]]
  name_prefix = "agent_"
  ignore_fs = ["tmpfs", "devtmpfs", "overlay", "squashfs", "iso9660"]
[[inputs.diskio]]
  name_prefix = "agent_"
  skip_serial_number = false
[[inputs.kernel]]
  name_prefix = "agent_"
[[inputs.kernel_vmstat]]
  name_prefix = "agent_"
[[inputs.mem]]
  name_prefix = "agent_"
[[inputs.processes]]
  name_prefix = "agent_"
[[inputs.swap]]
  name_prefix = "agent_"
[[inputs.system]]
  name_prefix = "agent_"
[[inputs.net]]
  name_prefix = "agent_"
[[inputs.netstat]]
  name_prefix = "agent_"
[[inputs.nstat]]
  name_prefix = "agent_"
[[inputs.ntpq]]
  name_prefix = "agent_"
  dns_lookup = false
[[inputs.internal]]
  name_prefix = "agent_"
  collect_memstats = false
```

78"
"
d1"

2.3

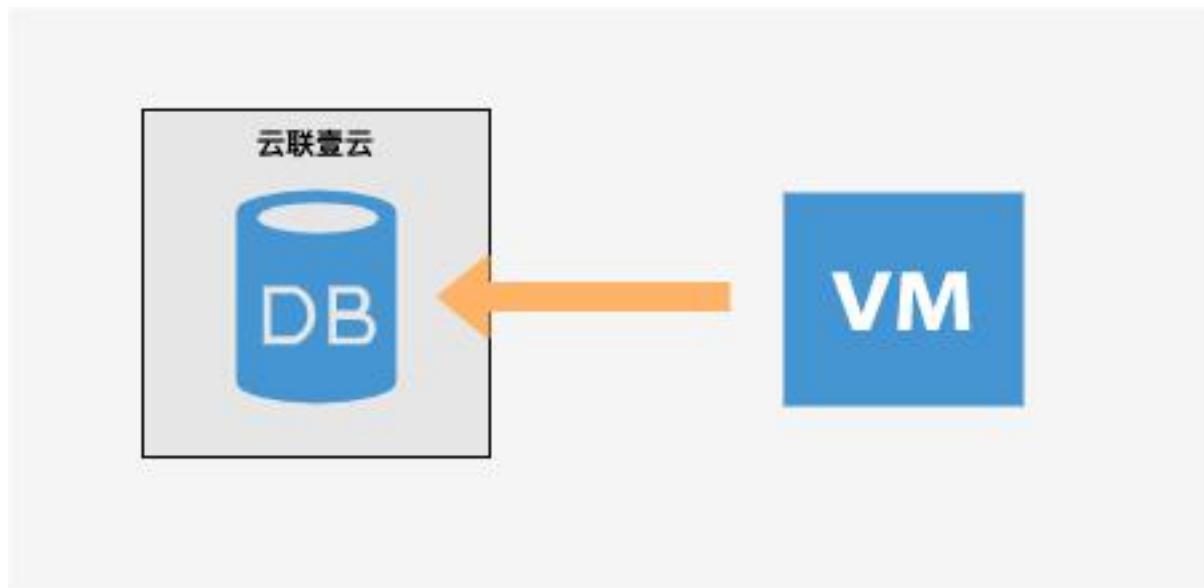
监控Agent将数据传回来?

数据传输

直接传输到InfluxBD

现在，虚拟机里面已经正常安装了监控Agent，那么如果传回到云联壹云中的InfluxDB？

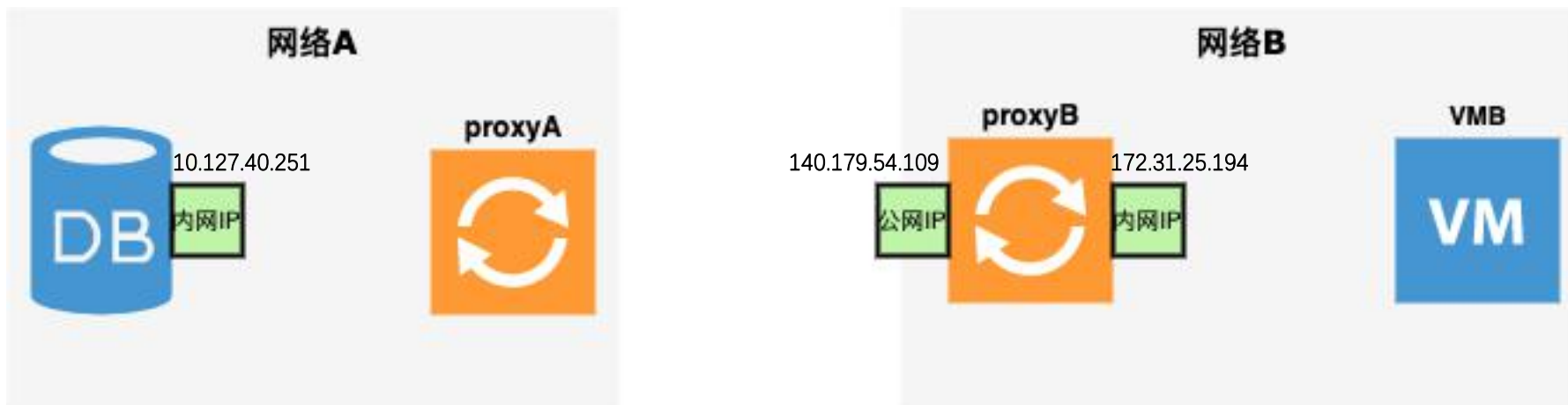
最简单的，就是虚拟机可以直连云联壹云中的InfluxDB？



否则，还是使用 SSH 代理，Remote Port Forwarding。

数据传输

SSH Remote Port Forwarding



网络A和网络B是两个隔离的网络，proxyB 具有公网IP，所以proxyA可以访问到proxyB，如何让 VMB 访问 DB？

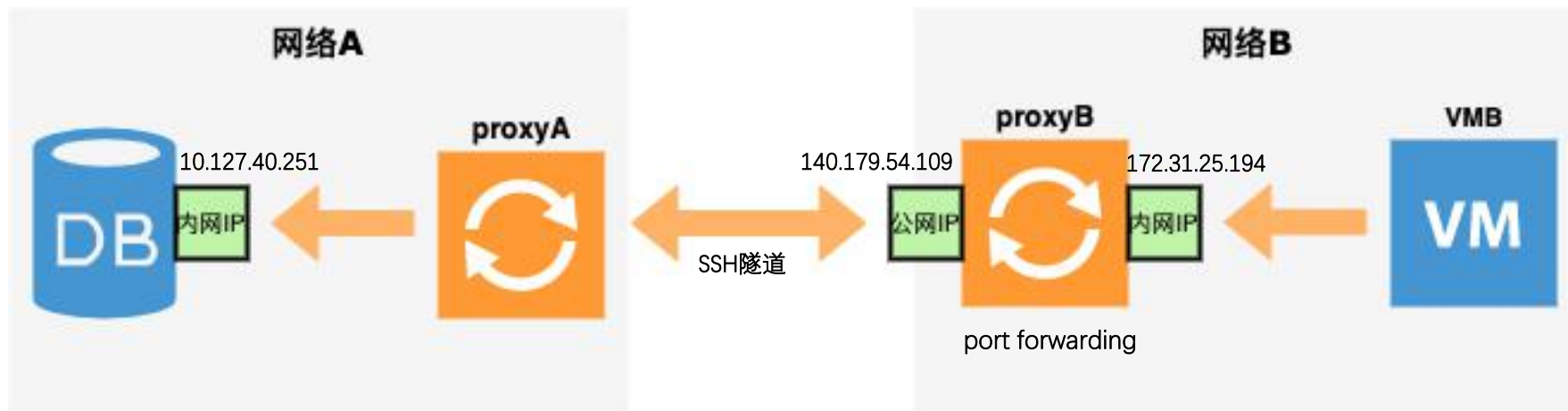
在 proxyA 上执行 `ssh -NfR 172.31.25.194:12345:10.127.40.251:30086 cloudroot@140.179.54.109`

执行上面的命令要求 proxyA 能够以 cloudroot 用户正常登录到 proxyB 上，这个可以通过前面讲到的登录方法来解决。

通过上面的方式，网络B 内部的 VMB 只要访问 172.31.25.194:12345 就可以访问到 DB。

数据传输

SSH Remote Port Forwarding



在 proxyA 上执行 `ssh -NfR 172.31.25.194:12345:10.127.40.251:30086 cloudroot@140.179.54.109`

会在 proxyA 和 proxyB 之间建立 SSH隧道，并在 proxyB 上创建一个 port forwarding，它将监听 172.31.25.194:12345，一旦有请求发来，就会通过 SSH 隧道转发到 proxyA，proxyA 会把请求转发到 10.127.40.251:80

通过上面的方式，网络B 内部的 VMB 只要访问 172.31.25.194:12345 就可以访问到 DB。

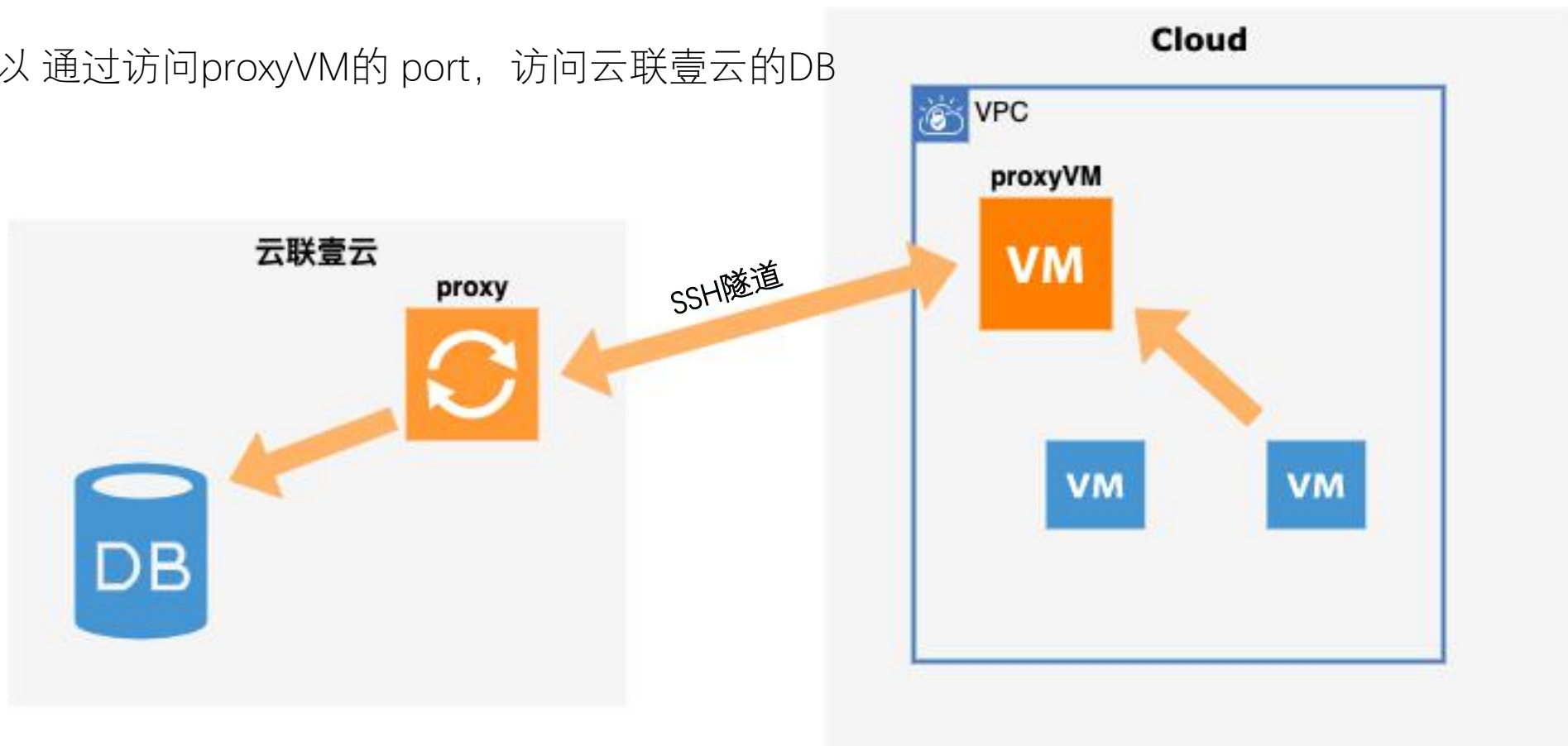
数据传输

通过代理传输数据

在 proxy 和 proxyVM 之间建立 SSH 隧道

并在 proxy 执行命令以在 proxyVM 上建立 port forwarding，对 proxy 来说就是 remote port forwarding。

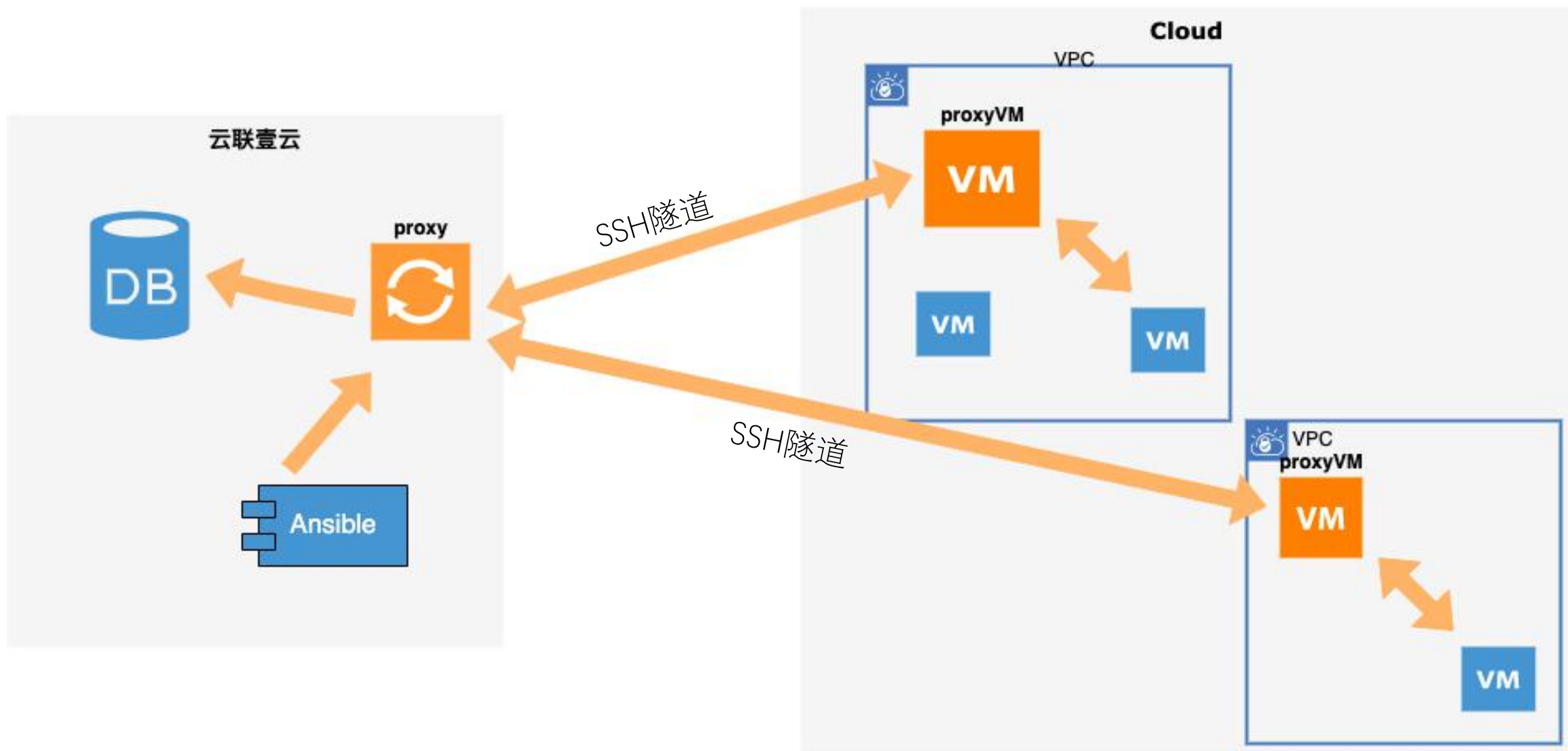
VPC 内部的虚拟机就可以通过访问 proxyVM 的 port，访问云联壹云的 DB 以把数据传输回来



03

总结与演示

总结



演示

Q & A

演示

新建VPC

网络

地域

区域

可用区

基础网络

全局VPC

VPC

二层网络

IP子网

网络服务

弹性公网IP

NAT网关

DNS解析

SSH代理服务

SSH代理节点

SSH代理服务

负载均衡

新建VPC

本地IDC

私有云

公有云

域:

Default

* 区域:

平台: 阿里云

区域: 阿里云 华北2 (北京)

* 名称:

agent-test

* 目标网段:

172.31.25.0/24

一旦创建成功, 网段不能修改。

允许外网访问:



启用该项后, VPC下的IP子网可以通过绑定EIP的方式访问外网

* 指定云订阅:

aliyun 云账号: aliyun



演示

新建IP子网

网络

地域

区域

可用区

基础网络

全局VPC

VPC

二层网络

IP子网

网络服务

弹性公网IP

NAT网关

DNS解析

SSH代理服务

SSH代理节点

SSH代理服务

负载均衡

新建IP子网

本地IDC

私有云

公有云

项目:

域: Default

项目: system

* 区域:

平台: 阿里云

区域: 阿里云 华北2 (北京)

* 名称:

agent-test

* VPC:

agent-test (172.31.25.0/24) 云账号: aliyun

* 可用区:

阿里云 华北 2 可用区 A

同一 VPC 下可以有不同可用区的子网，同一 VPC 下不同可用区的子网默认可以内网互通。

* 子网网段:

172.31.25.0/26

子网的 CIDR 必须是所在 VPC CIDR 的一部分，且不能和该 VPC 下已有子网的 CIDR 重叠。

自动调度:

☐

启用后，用户创建虚拟机网络指定自动调度时，将从启用自动调度的IP子网中为虚拟机分配IP地址。

演示

新建带有EIP的VM以作为proxyVM

虚拟机

全部

新建

开机

添加筛选选项

名称

proxyVM

p0-32ca-monkey...

lxj-test-vm

wangwenlong-vm...

lxj-test-vm2

interface-vmware...

mj-test-01-1

mj-test-01

interface-templat...

wcl-test

新建虚拟机

虚拟机

proxyVM

远程控制

更多

详情

安全组

网络

磁盘

快照

监控

报警

操作日志

基本信息

ID

2ec72e7e-6125-458d-891b-4e800f73f4d6

名称

proxyVM

状态

运行中

域

Default

项目

system

CPU架构

x86_64

用户标签

编辑标签

关联密钥

-

平台

计费方式

按量付费

1小时后到期

区域

阿里云 华北2（北京）

可用区

阿里云 华北2 可用区 A

云账号

alitest

云订阅

alitest

创建时间

2021-06-30 15:45:28

更新时间

2021-06-30 15:46:23

备注

-

配置信息

操作系统

CentOS

IP

182.92.223.33(弹性)

172.31.25.60(私有)

MAC

00:16:3e:34:02:d0

系统镜像

CentOS 8.3 64位

宿主机

-

安全组

Default

VPC

agent-test

CPU

1核

内存

2GB

系统盘

40GB（高效云盘）

数据盘

-

ISO

-

GPU

-

备份机的宿主机

-

其他设置

删除保护

开

演示

本身就是免密登录

通过云联壹云平台创建出来的虚拟机本身就是满足免密登录的。

探测免密登录

名称 ▾	状态 ▾	免密登录状态 ▾	操作
proxyVM 品	● 运行中	● 可免密登录	查看

确定

取消

演示

转化为 proxy

网络

地域

区域

可用区

基础网络

全局VPC

VPC

二层网络

IP子网

网络服务

弹性公网IP

NAT网关

DNS解析

SSH代理服务

SSH代理节点

SSH代理服务

负载均衡

实例

新建SSH代理节点

1 选择虚拟机

2 探测虚拟机可用状态

域:

Default

* 名称:

proxyVM

区域:

平台: 阿里云

区域: 阿里云 华北2 (北京)

网络:

VPC: agent-test (172.31.25.0/24) 云订阅: alitest

IP子网: agent-test (172.31.25.1 - 172.31.25.60) 可用: 58

* 虚拟机:

添加筛选项

名称	状态	IP	免密登录状态
proxyVM	运行中	182.92.223.33(弹性) 172.31.25.60(私有)	可免密登录

没有您想要的? 可以[新建](#),虚拟机具体配置请参考[虚拟机配置要求](#)

演示

创建VPC内的普通虚拟机

虚拟机

全部

虚拟机

normalVM

远程控制

更多

详情

安全组

网络

磁盘

快照

监控

报警

操作日志

刷新

新建

开机

添加筛选项

名称

normalVM

proxyVM

p0-32ca-monkey...

lxj-test-vm

wangwenlong-vm...

lxj-test-vm2

interface-vmware...

mj-test-01-1

mj-test-01

interface-templat...

wcl-test

基本信息

ID

2f227272-430c-49b7-86b8-e68bf2acc6c6

名称

normalVM

状态

运行中

域

Default

项目

system

CPU架构

x86_64

用户标签

编辑标签

关联密钥

-

平台

计费方式

按量付费

1小时后到期

区域

阿里云 华北2（北京）

可用区

阿里云 华北2 可用区 A

云账号

alitest

云订阅

alitest

创建时间

2021-06-30 15:50:53

更新时间

2021-06-30 15:51:29

备注

-

配置信息

操作系统

CentOS

IP

172.31.25.59(私有)

MAC

00:16:3e:2c:8b:85

系统镜像

CentOS 8.3 64位

宿主机

-

安全组

Default

VPC

agent-test

CPU

1核

内存

2GB

系统盘

40GB（高效云盘）

数据盘

-

ISO

-

GPU

-

备份机的宿主机

-

其他设置

删除保护

开

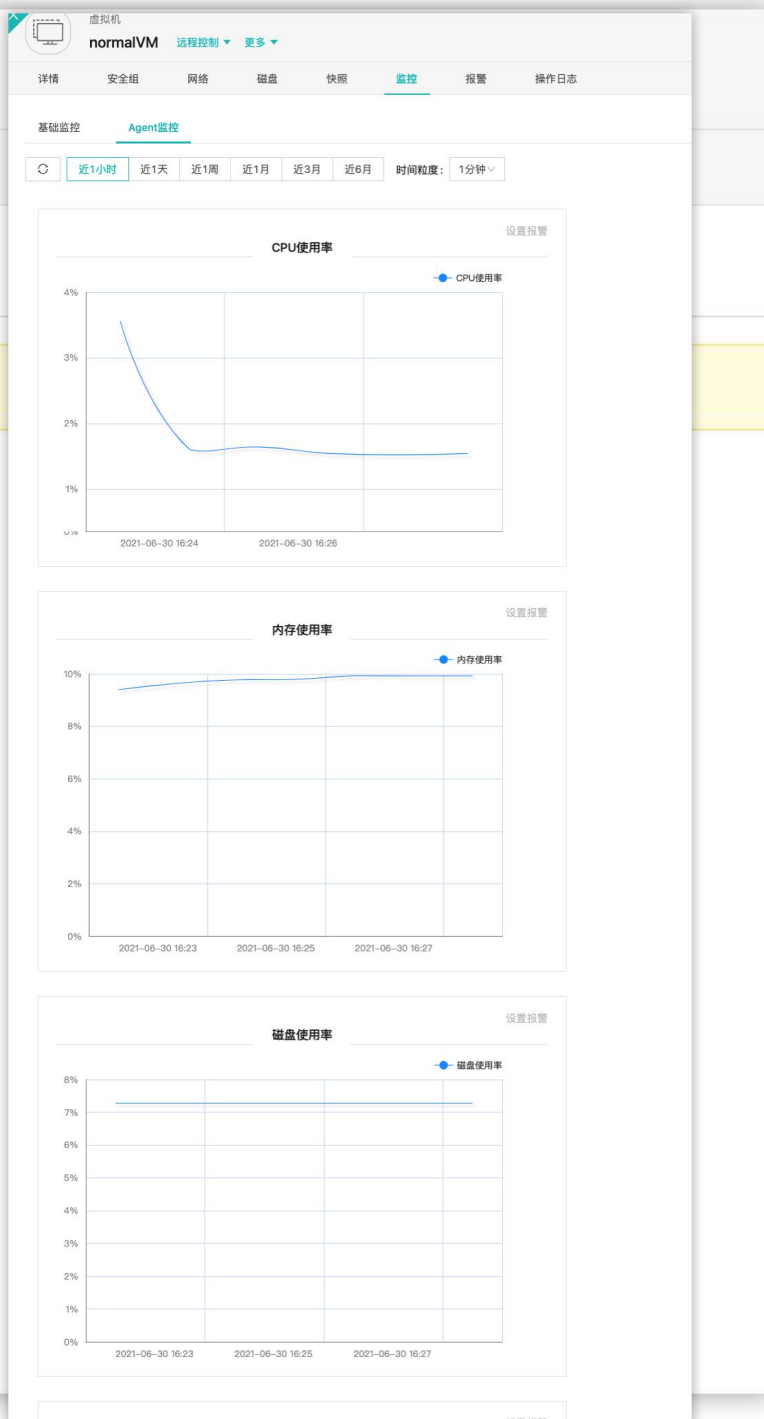
演示

监控

基础监控是通过调用云API拿到的监控数据。

Agent监控是运行在虚拟机上的监控Agent传回来的监控数据。

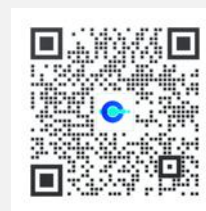
Agent监控需要手动触发安装。



2021 THANK YOU

云联壹云核心产品融合云 云联壹云 秉承：简单、开放、融合、智能的产品理念，能够帮助企业实现异构IT基础设施的全面云化、统一管理及成本优化，提高运维效率的同时，降低企业运营成本。

宋登举&郑雨 2021-06



扫码进技术交流群



更多资讯关注我