# 企业级虚拟专有网络统一认证解决方案及实战

## 0.背景

本文适用于办公以及研发环境的虚拟专有网络统一认证，适用于同时需要保障环境安全性，完整性以及可控性的情况。

内网的安全涉及到 wifi 准入，上网行为管理，网络出口防火墙等。基于 ZStack 平台私有云环境，需要一整套虚拟专有网准入以及日志审计的系统平台。

本次主要是使用 openldap 作为统一认证，Cisco ASA 作为 VPN 服务端，使用 syslog 进行日志审计。同时也提供了使用 snmp 的方式去定时轮训获取登录的用户以及 ip。

**说明：**

本文介绍的方案是新钛云服架构师在实际环境中实践总结而来，效果不错，所以整理分享出来

**实战环境：**

**AA.zstack+ASA8.42+Anyconnect+Ldap(CiscoPerson)+Syslog**

# 1.快速安装 openldap

https://github.com/osixia/docker-openldap

docker run --env LDAP_ORGANISATION="tyun" --env LDAP_DOMAIN="tyun.cn" --env LDAP_ADMIN_PASSWORD="ldap_passwd" --volume /data/slapd/database:/var/lib/ldap --volume /data/slapd/config:/etc/ldap/slapd.d --detach -it -p 389:389 -p 636:636 osixia/openldap:1.2.0

docker 快速安装（根据需要选择对应的版本，或者手工基于 dockerfile build 最新版本）或者手动安装，但需要加入 memberof 属性。

# 2.openldap 导入 CiscoPerson objectclass

## 2.1 下载 cisco.schema

wget

https://gist.github.com/jaseywang/041f76d03e2f43579d6f6984e3358774

cisco.schema(上面链接失效的化，使用本处)

将 85 行改为 MUST ( uid $ cn )， 86 行 delete 掉 telephoneNumber（否则会报错）

也可以直接使用已经修改好的

https://raw.githubusercontent.com/qingyufei/ubuntutools/master/Cisco_ASA_ldap/zhuxiang/cisco.schema

### 2.2 基于 cisco.schema 生成 cisco.ldif

新建配置文件以及目录

```
echo "include cisco.schema" >>cisco.conf
mkdir ldif_cisco
slaptest -f cisco.conf -F ldif_cisco
```

获取到 ldif 目录结构如下：

tree ldif

tree

.

├── cn=conflig

│ ├── cn=schema

│ │ └── cn={0}cisco.ldif

│ ├── cn=schema.ldif

│ ├── olcDatabase={0}config.ldif

│ └── olcDatabase={-1}frontend.ldif

└── cn=config.ldif

文件 cn=config/cn=schema/cn={0}cisco.ldif 就是生成的‘ldif’文件，编辑此文件，

前三行改为：

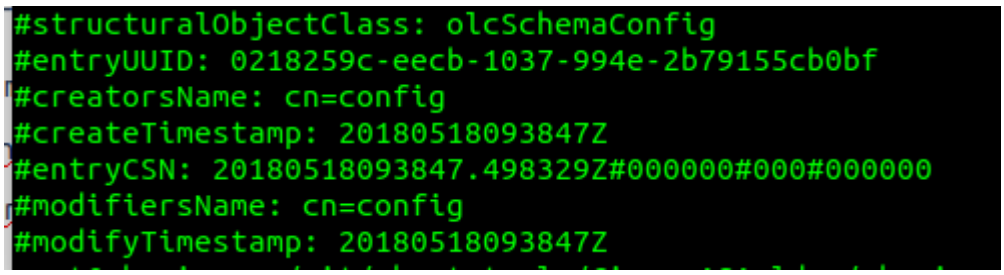
dn: cn=cisco,cn=schema,cn=config

objectClass: olcSchemaConfig

cn: cisco

```
root@zhuxiang:~/git/ubuntutools/Cisco_ASA_ldap/zhuxiang/ldif_dir/cn=config/cn=schema# cat cn\=\{0\}cisco.ldif
# AUTO-GENERATED FILE - DO NOT EDIT!! Use ldapmodify.
# CRC32 081a4f5f
dn: cn=cisco,cn=schema,cn=config
objectClass: olcSchemaConfig
cn: cisco
```

最后注释掉最后七行：




**2.3 将‘’cn={0}cisco.ldif"文件内容导入 ldap 数据库**

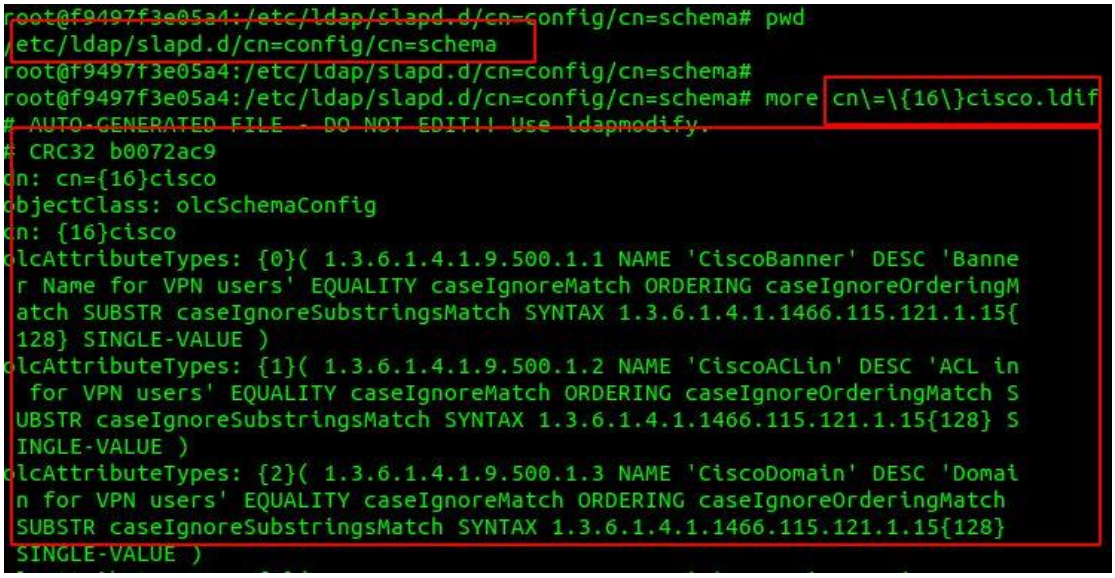
进入对应的目录，导入数据库(如果使用 docker 安装，则通过 docker cp 复制配置文件到容器里执行,当然也可以安装 openldap-clients,openldap-devel，通过-H 指定 ldap 主机)：

```
cd  ldif_cisco/cn=config/cn=schema
sudo ldapadd -Q -Y EXTERNAL -H ldapi:/// -f cn={0}cisco.ldif
```

查看是否导入成功：

```
ldapsearch -Q -LLL -Y EXTERNAL -H ldapi:/// -b cn=schema,cn=config dn
```

直接查看生成的文件(/etc/ldap/slapd.d/cn=config/cn=schema/cn={16}cisco.ldif)：




# 3.Cisco ASA

**3.1 商业购买 ASA 硬件+ Anyconnect vpn 的 liscence （推荐）**

**3.2 模拟器 vMware 或在 Esxi 版本的 ASA8.42(或者 ASA931 等其他版本都可以)**

**+Cisco ASA Keygen（网上教程比较多，仅作为测试学习使用，请勿商业使用。）**

**3.3 KVM 版本的 ASA8.42（仅作为测试学习使用）。**

解压 vmware 的 ova 文件(iso 文件为启动引导文件，qcow2 为 disk0:或者 flash 文件，最重要的是 iso 文件，qcow2 可以重新生成):

convert vmware to qcow2

root@zhuxiang:~/cisco# tar -xvf asa842.ova

WOLF-ASA842-adv.ovf

WOLF-ASA842-adv.mf

WOLF-ASA842-adv-disk1.vmdk

WOLF-ASA842-adv-file1.iso

root@zhuxiang:~/cisco# ls

asa842.ova WOLF-ASA842-adv-disk1.vmdk WOLF-ASA842-adv-file1.iso WOLF-ASA842-adv.mf WOLF-ASA842-adv.ovf

root@zhuxiang:~/cisco# mkdir -pv ASA_qcow2

mkdir: created directory 'ASA_qcow2'

root@zhuxiang:~/cisco# qemu-img convert -f vmdk -O qcow2 WOLF-ASA842-adv-disk1.vmdk ASA_qcow2/ASA842-adv-disk1.qcow2

root@zhuxiang:~/cisco# cp WOLF-ASA842-adv-file1.iso ASA_qcow2/ASA842-adv-file1.iso

最重要的是 iso 文件，每次虚拟机启动都要重 iso 启动:

root@zhuxiang:~/cisco# ls ASA_qcow2/

ASA842-adv-disk1.qcow2 ASA842-adv-file1.iso

查看 qcow2 文件:

root@zhuxiang:~/cisco/ASA_qcow2# virt-list-filesystems -a ASA842-adv-disk1.qcow2

/dev/sda1

通过 guestmount 工具查看 asa 磁盘里的信息。

root@zhuxiang:~/cisco/ASA_qcow2# guestmount -a ASA842-adv-disk1.qcow2 -m /dev/sda1 /mnt
root@zhuxiang:~/cisco/ASA_qcow2# ls /mnt/
anyconnect-win-3.0.0629-k9.pkg boot csco_config rdp2-plugin.090211.jar ssh-plugin.080430.jar
asdm-645-206.bin coredumpinfo csd_3.6.181-k9.pkg rdp-plugin.101215.jar vnc-plugin.080130.jar

可以生成 kvm 系统（网卡必须选择 e1000,把 iso 作为第一启动项），或者导入 ISO ZStack，然后直接运行(导入 ASA8.42.iso，格式必须是 iso，平台是 other)：


创建虚拟机，根云盘规格选择 10G，计算规格 2 核 4G 以上，网络按照需求选择，选择对应的 ASA8.42 iso 镜像。创建虚拟机成功。(Network Anti-Spoofing 功能注意关闭)

由于 zstack2.3.2 不支持 serial 重定向，查看 ASA8.42 所在的计算节点，通过在宿主机上直接运行命令 virsh console ASA8.42_domain 进入 console 控制台，配置基础管理功能

（其他版本 ASA 可能支持直接从页面 console 口登陆）

修改云主机启动顺序(CdRom,HardDisk)：


asa

[root@bjm8-zscns-10-0-3-16 ~]# virsh list --all

Id 名称 状态

---

6 687ba60019f04a5fa71b3f1501560d3a running

7 3459d91402c247ca8fabf0e7d922af7b running

9 09cabc8ca969429c9505fafaf14071eb running

34 fb4550f382fb496cbb03d77ca5f2456e running

42 8af69ae1236e4827880f6684987d9438 running

43 zstack10310 running

[root@bjm8-zscns-10-0-3-16 ~]# virsh console 8af69ae1236e4827880f6684987d9438

连接到域 8af69ae1236e4827880f6684987d9438

换码符为 ^]

ASAGW7>

ASAGW7> ena

Password:

ASAGW7# show version

Cisco Adaptive Security Appliance Software Version 8.4(2)

Device Manager Version 6.4(5)206

Compiled on Wed 15-Jun-11 18:17 by builders

System image file is "Unknown, monitor mode tftp booted image"

Config file at boot was "startup-config"

ASAGW7 up 1 day 20 hours

Hardware: ASA 5520, 3072 MB RAM, CPU Pentium II 2095 MHz

Internal ATA Compact Flash, 131072MB

BIOS Flash unknown @ 0x0, 0KB

0: Ext: GigabitEthernet0 : address is fa1a.6c10.8800, irq 0

1: Ext: GigabitEthernet1 : address is fa03.b8ec.3001, irq 0

Licensed features for this platform:

| | | |
|---|---|---|
| Maximum Physical Interfaces | : Unlimited | perpetual |
| Maximum VLANs | : 100 | perpetual |
| Inside Hosts | : Unlimited | perpetual |
| Failover | : Active/Active | perpetual |
| VPN-DES | : Enabled | perpetual |
| VPN-3DES-AES | : Enabled | perpetual |
| Security Contexts | : 20 | perpetual |
| GTP/GPRS | : Enabled | perpetual |
| AnyConnect Premium Peers | : 10000 | perpetual |
| AnyConnect Essentials | : 0 | perpetual |
| Other VPN Peers | : 5000 | perpetual |
| Total VPN Peers | : 0 | perpetual |
| Shared License | : Enabled | perpetual |
| AnyConnect for Mobile | : Enabled | perpetual |
| AnyConnect for Cisco VPN Phone | : Enabled | perpetual |
| Advanced Endpoint Assessment | : Enabled | perpetual |
| UC Phone Proxy Sessions | : 5000 | perpetual |
| Total UC Proxy Sessions | : 10000 | perpetual |
| Botnet Traffic Filter | : Enabled | perpetual |
| Intercompany Media Engine | : Disabled | perpetual |

This platform has an ASA 5520 VPN Plus license.

# 4.AnyConnect VPN 配置

## 41. webvpn 配置

webvpn

webvpn

enable Outside

no anyconnect-essentials

anyconnect image disk0:/anyconnect-win-3.0.0629-k9.pkg 1

anyconnect enable

tunnel-group-list enable

sysopt connection permit-vpn

## 4.2 aaa-server ldap 配置

aaa-server ldap

ASAGW7# sho running-config aaa-server

aaa-server LdapServerGroup0 protocol ldap

aaa-server LdapServerGroup0 (Inside) host XXXXXXXXXX

ldap-base-dn dc=tyun,dc=cn

ldap-scope subtree

ldap-naming-attribute uid

ldap-login-password *****

ldap-login-dn cn=admin,dc=tyun,dc=cn

server-type openldap

ldap-attribute-map LdapMapClass0

### 4.3 ldap attribute-map 配置

ldap attreibute-map

ASAGW7# sho run ldap

ldap attribute-map LdapMapClass0

map-name CiscoACLin Cisco-AV-Pair

map-name CiscoBanner Banner1

map-name CiscoDNS Primary-DNS

map-name CiscoDomain IPSec-Default-Domain

map-name CiscoGroupPolicy IETF-Radius-Class

map-name CiscoIPAddress IETF-Radius-Framed-IP-Address

map-name CiscoIPNetmask IETF-Radius-Framed-IP-Netmask

map-name CiscoSplitACL IPSec-Split-Tunnel-List

map-name CiscoSplitTunnelPolicy IPSec-Split-Tunneling-Policy

ldap 用户 ciscoperson objectclass 添加，以及 ASA 关键配置

ciscoperson

根据需要配置 ciscoperson，案例如下，本次案例可以直接只使用 group-policy

cat users.ldiff

# User account

dn: uid=zhuxiang,ou=operations,ou=users,dc=tyun,dc=cn

cn: zhu xiang

givenName: zhuxiang

sn: zhuxiang

uid: zhuxiang

uidNumber: 10000

gidNumber: 10000

homeDirectory: /home/zhuxiang

mail: zhuxiang@tyun.cn

objectClass: top

objectClass: posixAccount

objectClass: shadowAccount

objectClass: inetOrgPerson

objectClass: organizationalPerson

objectClass: person

objectClass: CiscoPerson

loginShell: /bin/bash

userPassword: {CRYPT}*

CiscoBanner: This is banner 1

CiscoIPAddress: 10.1.1.1

CiscoIPNetmask: 255.255.255.128

CiscoDomain: xtstack.com

CiscoDNS: 223.5.5.5

CiscoACLin: ip:inacl#1=permit ip 10.255.0.200 255.255.255.255 10.0.3.14 255.255.255.255

ip:inacl#2=permit ip 10.255.0.200 255.255.255.255 10.0.3.10 255.255.255.255

CiscoSplitACL: DefaultSplitVPNAcl0

CiscoSplitTunnelPolicy: 1

CiscoGroupPolicy: DefaultGroupPolicy0

ASA 上对应配置

ASAGW47# show running-config access-list

access-list DefaultSplitVPNAcl0 standard permit 10.0.0.0 255.0.0.0

access-list DefaultSplitVPNAcl1 standard permit 10.0.5.0 255.255.255.0

ip local pool DefaultVPNPool0 10.255.0.11-10.255.0.64 mask 255.255.255.0

新建用户 group-policy ， 以及默认 denyall 的 group-policy

ASAGW47# sho running-config group-policy

group-policy DefaultGroupPolicy0 internal

group-policy DefaultGroupPolicy0 attributes

vpn-simultaneous-logins 10

vpn-idle-timeout 9999

vpn-session-timeout none

vpn-tunnel-protocol ikev1 ikev2 l2tp-ipsec ssl-client ssl-clientless

split-tunnel-policy tunnelspecified

split-tunnel-network-list value DefaultSplitVPNAcl0

default-domain value tyun.cn

address-pools value DefaultVPNPool0

group-policy NoAccessGroupPolicy internal

group-policy NoAccessGroupPolicy attributes

vpn-simultaneous-logins 0

vpn-tunnel-protocol ikev1 ikev2 l2tp-ipsec ssl-client ssl-clientless

default-domain value tyun.cn

address-pools none

LDAP 用户匹配上 group-policy DefaultGroupPolicy0 才可以访问，其他用户默认匹配 group-policy NoAccessGroupPolicy，该策略默认不可以访问 vpn

ASAGW7# sho run tunnel-group

tunnel-group DefaultTunnelGroup0 type remote-access

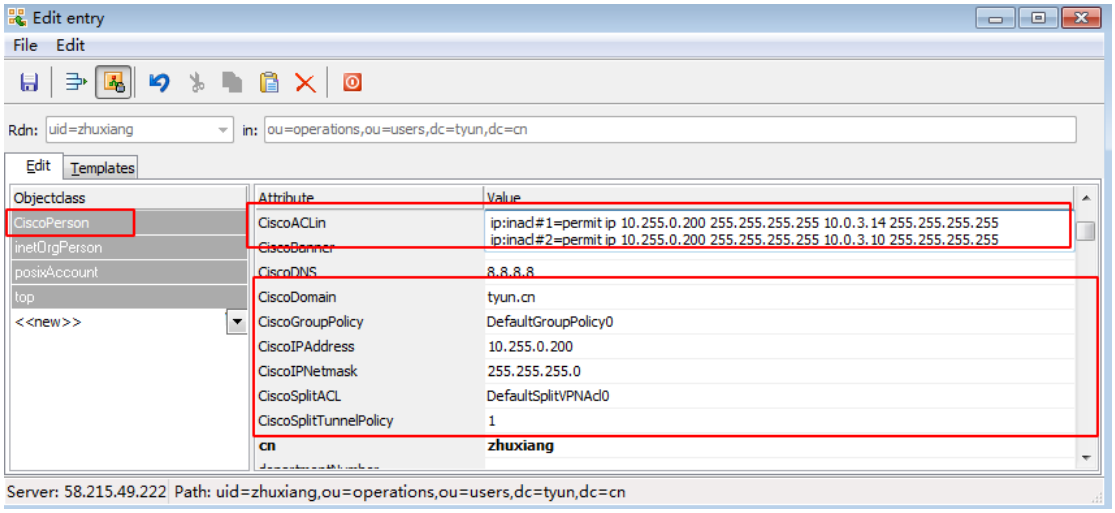
tunnel-group DefaultTunnelGroup0 general-attributes

authentication-server-group LdapServerGroup0

default-group-policy NoAccessGroupPolicy

tunnel-group DefaultTunnelGroup0 webvpn-attributes

group-alias OperationsAdmin enable




ldap objectclass ciscoperson 常见

https://www.cisco.com/c/en/us/td/docs/security/asa/asa90/configuration/guide/asa_90_cli_config/ref_extserver.pdf

| | | | | | | |
|---|---|---|---|---|---|---|
| IPsec-Split-Tunneling-Policy | Y | Y | Y | Integer | Single | 0 = Tunnel everything<br>1 = Split tunneling<br>2 = Local LAN permitted |

# 5.log 配置

开启 ASA vpn 以及 auth log

asa syslog

logging enable

logging timestamp

logging buffer-size 1048576

logging buffered notifications

logging class vpn buffered notifications

logging class auth buffered notifications

日志可以查看登录用户历史记录

log

ASAGW7# show logging | include zhuxiang

May 23 2018 17:54:02: %ASA-4-722041: TunnelGroup <DefaultTunnelGroup0> GroupPolicy <DefaultGroupPolicy0> User <zhuxiang> IP <58.215.49.222> No IPv6 address available for SVC connection

May 23 2018 17:54:02: %ASA-5-722033: Group <DefaultGroupPolicy0> User <zhuxiang> IP <58.215.49.222> First TCP SVC connection established for SVC session.

May 23 2018 17:54:02: %ASA-4-722051: Group <DefaultGroupPolicy0> User <zhuxiang> IP <58.215.49.222> Address <10.255.0.13> assigned to session

May 23 2018 17:57:20: %ASA-5-722012: Group <DefaultGroupPolicy0> User <zhuxiang> IP <58.215.49.222> SVC Message: 16/NOTICE: Aborted by caller.

May 23 2018 17:57:20: %ASA-5-722037: Group <DefaultGroupPolicy0> User <zhuxiang> IP <58.215.49.222> SVC closing connection: User Requested.

May 23 2018 17:57:20: %ASA-4-113019: Group = DefaultTunnelGroup0, Username = zhuxiang, IP = 58.215.49.222, Session disconnected. Session Type: AnyConnect-Parent, Duration: 0h:03m:18s, Bytes xmt: 8592, Bytes rcv: 1053, Reason: User Requested

May 23 2018 18:45:44: %ASA-5-722037: Group <DefaultGroupPolicy0> User <zhuxiang> IP <101.81.238.100> SVC closing connection: Transport closing.

May 23 2018 18:48:15: %ASA-5-722037: Group <DefaultGroupPolicy0> User <zhuxiang> IP <101.81.238.100> SVC closing connection: Transport closing.

通通过 snmp 获取 用户以及访问的来源 ip 地址

asa snmp

[root@zabbix55 ~]# snmpwalk -v 2c -c tyun11325 10.0.5.7 enterprises.9.9.392.1.3.21.1.10

SNMPv2-SMI::enterprises.9.9.392.1.3.21.1.10.8.122.104.117.120.105.97.110.103.53249 = STRING: "124.78.135.29"

SNMPv2-SMI::enterprises.9.9.392.1.3.21.1.10.8.122.104.117.120.105.97.110.103.57345 = STRING: "101.81.238.100"

重量级的 Graylog

https://blog.csdn.net/liukuan73/article/details/52525431

商业 kiwi syslog

## 6.后记

以下的方法是直接通过 ldap memberof (ldapsearch -x -h "127.0.0.1" -b dc=tyun,dc=cn -D "cn=admin,dc=tyun,dc=cn" -W '(uid=zhuxiang)' memberOf)属性映射的方式，8.4.2 没有测试成功，估计要更高的版本

**参考文档：**

https://www.cisco.com/c/zh_cn/support/docs/security/asa-5500-x-series-next-generation-firewalls/91831-mappingsvctovpn.html#anc6

https://www.tunnelsup.com/cisco-asa-vpn-authorize-user-based-on-ldap-group/

https://www.cisco.com/c/en/us/support/docs/security/asa-5500-x-series-next-generation-firewalls/98625-asa-ldap-authentication.html

**作者：祝祥 新钛云服运维架构师**

十年运维经验，曾任刻通云运维工程师、微烛云和某互联网金融平台首席运维架构师。拥有 OpenStack、CCIE、阿里云、ZStack 等技术认证。有上万台云主机，PB 级别分布式存储运维经验。熟悉各种虚拟化技术，软硬件，网络，容器编排等技术，拥有 python 开发经验。热爱各种开源技术。

**ZStack 是谁?**

大道至简·极速部署，ZStack 致力于产品化私有云和混合云。

ZStack 是新一代创新开源的云计算 IaaS 软件，由英特尔、微软、CloudStack 等世界上最早一批虚拟化工程师创建，拥有 KVM、Xen、Hyper-V 等成熟的技术背景。

ZStack 创新提出了云计算 4S 理念，即 Simple (简单)、Strong (健壮)、Smart (智能)、Scalable (弹性)，通过全异步架构，无状态服务架构，无锁架构等核心技术，完美解决云

计算执行效率低，系统不稳定，不能支撑高并发等问题，实现 HA 和轻量化管理。

ZStack 发起并维护着国内最大的自主开源 IaaS 社区——zstack.io，吸引了 6000 多名社区用户，对外公开的 API 超过 1000 个。基于这 1000 多个 API，用户可以自由组装出自己的私有云、混合云，甚至利用 ZStack 搭建公有云对外提供服务。

ZStack 拥有充足的知识产权储备，积极申报多项软著和专利，参与业内标准、白皮书的撰写，入选云计算行业方案目录，还通过了工信部云服务能力认证和信通院可信云认证。

ZStack 面向企业用户提供基于 IaaS 的私有云和混合云，是业内唯一一家实现产品化，并领先业内首家推出同时打通数据面和控制面无缝混合云的云服务商。选择 ZStack，用户可以官网直接下载、1 台 PC 也可上云、30 分钟完成从裸机的安装部署。

目前已有 1000 多家企业用户选择了 ZStack 云平台。