搭建云桌面专有网络内 Windows AD 服务器

本文主要指导用户搭建基于专有网络(VPC)的 AD,并配置到云桌面环境设置中。

1. 云资源准备

1.1 创建 VPC 和交换机

此处创建的 VPC 将被设置到云桌面环境设置中,如已创建请忽略。

 在 <u>VPC 控制台</u>选中需要配置云桌面环境的区域(图 1.1.1),如选中 **华东 1**,并点击 创 建专有网络

专有网络	新出1 绿北2 标北3 华东1 标东2 标南1	香港 亚太东北1(东京) 3	亚太东南 1 (新加坡)	豆太东南 2 (悉尼)	美国东部 1 (弗吉尼亚)	美国西部1(硅谷)	中东东部1(迪拜) 欧洲中部1(法兰克林	0	新 创建专有网络
概范									
专有网络	VPC ID/名称	同段	状态	描述		创建时间	默认专有网络		操作



2. 创建 VPC(图 1.1.2)时请设置好其名称和网段,点击 创建 VPC

创建	专有网络 人名法尔 人名法尔尔 人名法尔尔 人名法尔尔 人名法尔尔 人名法尔尔 人名法尔尔 人名法尔尔 人名法尔尔 化合成合成 人名法尔尔 化合成合成 人名法尔尔 人名法尔尔尔 人名法尔尔尔尔 人名法尔尔尔尔 人名法尔尔尔尔 人名人名法尔尔尔尔 人名人名人名人名人名人名人名人名人名人名人名人名人名人名人名人名人名人	创建交换机	
*专有网络名称:	clouddesktop-vpc		
	名称为2-128个字符,以大小字母或中文开头,可包含数 字,"_"或"-"		
描述:			
	描述可以为空 : 或填写2-256个中英文字符 , 不能以http://和 https://开头		
*网段:	192.168.0.0/16 🔻		
	① 一旦创建成功,网段不能修改		

图 1.1.2

专有网络创建完成以后,请创建交换机,为了保证高可用,请至少在两个不同的可用区 创建两个交换机。在创建占有网络完成以后(图 1.1.3),点击 **管理交换机**

创建专有网络				×
	创建专有网络		前龍文冊肌	
0	创建专有网络成功 ^{生成:}			
	专有网络ID:	vpc-bplabyg7c4e98wxfld	2xa	
	路由器ID:	vrt-bplolxrhb0z3jke8h0p	an 管理語由器	
	下面您可以继续: 管理交换机			

下一步

 \times

图 1.1.3 3. 创建交换机时,请配置好其网段(图 1.1.4),点击 确定

创建交换机

*专有网络:	clouddesktop-vpc / vpc-bplabyg7c4e98wxfld2:
专有网络网段:	192 . 168 . 0 . 0 / 16 显示二进制
*名称:	clouddesktop-switcher-b 名称为2-128个字符,以大小字母或 中文开头,可包含数字,"_"或"-"
*可用区:	华东1可用区 B ▼ ① 创建后无法修改
*网段:	192 · 168 · 1 · 0 / 24 显示二进制 ① 创建后无法修改 必须等于或属于该专有网络的网段,网段掩码必须在16和29之间。 例如:192.168.88.0/24 交换机网络设置参考
可用IP数:	252 个
描述:	描述可以为空;或填写2-256个中英 文字符,不能以http://和https://开头
	确定 取消

图 1.1.4 交换机创建完成以后,可以在交换机列表里面查询到其配置,检查是否正确。

<	交換机列表							一个专有网络量的	FREE REPORT	CRIFF BILLOWER
专有同语洋情	xaerbo • Real-Asserbote/SNeeten	22								
	交接机 的/名称	ECSIRHIM	用段	83	可用回	可用私有问题	创建时间	新以交換机	描述	盛作
323671	vsw-bp19owelficy0yp11nnu0 clouddesktop	0	192.168.2.0/24	将用助	华东1可用区 D	252	2017-07-03 10:59:19	8		納理 一部除 创建共行+
	vsw-bpldwx7a7mdkrblo68ida clouddesktop	0	192.168.1.0/24	可用	华东1可用区8	252	2017-07-03 10:58:29	5		编辑 图除 创建实例 -
								共有2	条,每页显示:10条	4 4 <mark>1</mark> 4 4

图 1.1.5

1.2 创建安全组

此处创建的安全组将设置到云桌面环境配置中,如已创建请忽略。

1. 在 ECS 控制台选择 网络和安全 - 安全组,并选中刚才创建 VPC 的区域,如华东 1,点击 创建安全组 (图 1.2.1)

云服务器 ECS	安全组列表 \$#北1 \$#北2 \$#北3 \$ \$ \$ \$ \$	东 2 华南 1 香港 亚太东北 1 (东京)	亞太东南 1 (新加坡) 亞太东南 2 (思思	美国东部1(弗吉尼亚)	美国西部1(建谷) 中东东部1(迪拜)	(25)州中部1(法兰売福)		C 0000240
概范	安全組D · · · · · · · · · · · · · · · · · · ·	我家 ●标签						2 ?
面例	□ 安全组印/名称	所屋专有网络	相关实例	网络典型	自己就对力问	1815	标签	操作

图 1.2.1

2. 在安全组创建页面, 网络类型 选择 专有网络, 专有网络 选择 1.1 中创建完成的专有 网络(图 1.2.2), 点击 确定, 在没有特殊网络控制的情况下,可以不设置安全组规则。

201203010101011	clouddesktop-sg
	长度为2-128个字符,不能以特殊字符及数字开头,只可包含特殊字符中的".","_"或"-"。
描述:	
	长度为2-256个字符,不能以http://或https://并头。
网络类型:	长度为2-256个字符,不能以http://或https://卅头。 专有网络 ▼

确定

取消

1.3 创建云服务器实例

为了保证 AD 的高可用性,最好购买两台基于 VPC 的云主机实例。

1. 在 <u>ECS 控制台</u>,选择 **实例**,选中需要配置云桌面环境的区域(图 1.3.1),必须和创建的 VPC 在同一个区域,如 **华东 1**,点击 **创建实例**

云服务器 ECS	实例列表 非北1 非北2 年北3 ¥4	x1 参照2 参阅1	· 香港 亚太东北1(东京)	亚大东南1(新加坡)	豆太东南 2 (悉尼) 多	她国东郎 1 (弗吉尼亚)	美国西部1(社谷)	中东东部1(迪拜)	欧洲中部 1 (法兰克福		C	95	3RM
概范	实例名称 * 输入实例名称摄制查询		828 1055							,	國機業	2 0	?
政例	□ 实例0/宫称	<u>出投</u> 府	在可用区	IP384£	状态(全部) マ	网络	美型(全部) マ		配置	付繳方式(全部) ▼			操作

图 1.3.1

2. 在云服务器购买页面,请正确选择 地域,并选择前面创建的 网络 VPC、交换机、安全组(图 1.3.2),如遇到交换机对应的可用区无法购买实例,请返回 VPC 控制台重新选择新的可用区配置交换机。滚动页面,选择 实例类型、实例配置、镜像、存储等配置,假如需要管理的云桌面实例少于 1000,建议选择 系列 II、共享计算型 n1、2 核 4G 配置,镜像类型必须选择 Windows server 2008 R2 企业版 64 位中文版。继续滚动页面,在 安全设置 中输入 登陆密码 用于 Windows 登陆,请记住设置的密码。最后点击 立即购买。

🕜 计费方式	包年包月	按量付费	0			
♀ 地域	华北1 🚳	华北 2	华北 3 😂	华东 1	华东 2	华南1
		随机分配 ~	随机分配 ~	华东 1 可用区 E 🛛 🗸	随机分配 ~	随机分配 ~
	香港	亚太东南1(新加坡)	美国东部 1 (弗吉尼亚)	亚太东北 1 (东京)	美国西部 1 (硅谷)	欧洲中部1(法兰克福)
	随机分配 ~	随机分配 ~	美国东部1 可用区A ~	随机分配 🗸	美国西部1 可用区B ~	随机分配 ~
	中东东部 1 (迪拜)	亚太东南 2 (悉尼)				
	随机分配 ~	随机分配 🗸				
	不同地域的实例之间内网互不	相通;选择靠近忽客户的地域,下	可降低网络时延、提高您客户的;	方问速度, 教我选择>> 🕜		
◎ 网络	经典网络	专有网络 🔍	0			
	经典网络与专有网络不能互通	,购买后不能更换网络类型,请	」 ▲值选择			
	clouddesktop-vpc	 clouddesktop- 	switcher-e ~ 可用私	ム有 IP 252 个		
	如需使用其他专有网络,请选 当前虚拟交换机所在可用区为	择已有专有网络,也可以自行到: : 华东1可用区E	控制台创建>>			
	公网 IP 地址: 不分配		小网 ID #http://			
	不为美的方帽公网叶地址,如	繁切时公网,可能重开 那定理性				
			图 1.3.2			

实例	系列1	#391 II	乗列 Ⅲ	⑦ 1/0 优化实例	0							
申请更考配置	系列之间不能互批升舞蹈											
	共穿计算型 nl	共享通用型 n2	共享内存型 e3	计算型(原独享) sn1	通用型(原独享) sn2							
	1核1GB eccnltiny	1 核 2GB ecs.rd.small	2 検 4GB ecs.nL/medium	4 枝 8GB ecunilarge								
u ² 199	公共編集	自定义绕像	共享機働	镜像市场	Ø							
	📽 Windows Server 👻	2008 R2 企业版 64位中文8	ξ ×	載我法揮>>								
	🗹 安全加固 🕖											
₩ 存储	至统曲: 国 如何选择 55	欧天豊 - 40 の天豊 / 高次天豊 / 高速天豊 -	GB 1240 IOPS 重 调查 详细说明>>	统查设备名:/dev/xeda								
	8:84: 🕂 🗰	政援皇 即还可远起 4 快										
■ 购买量	1 1 1											

图 1.3.3

- 3. 重复步骤 2,并选择不同的交换机,购买另一台 ECS 实例作为备 AD 服务器,保证 AD 的 高可用性。
- 4. 在 ECS 控制台确认云服务器实例是否已经创建成功。如没有创建,请点击右上角的刷新 图标。

云服务器 ECS	实例列表 华北1 华北2 华北3 华东1	华东 2 华南	1 雪港 亚太东北1(东	(原) 亞太东南1(新加坡)	亚太东南 2 (紙尼) 美国东部	\$ 1 (弗吉尼亚) 美国西部	1 (後谷) 中东东部 1 (油坪) 欧洲中部 1 (法兰地福)	l	
概范	实例名称 * 输入实例名称燃料查询		225	2					***** <u>₹</u> • ?
卖例	東例D/名称	监控	所在可用区	IP地址	状态(退行中) 🗸	网络與型(全部) ▼	配置	付薨方式(全部) ▼	操作
▼ 存储 云盘	i-bp13cbiz72g5mat4imt0 iZ72g5mat4imt0Z	a 🗠	华东 1 可用区 E	192-168-1-134(私海)	 运行中 	专有网络	CPU: 2檢 內存:4 GB (I/O优化)	按量 17-07-03 14:36 创建	管理 這程连接 更多 -
文件存储 NAS	i-bp13cbiz72g5mat4imsy iZ72g5mat4imsyZ	a 🗠	华东 1 可用区 F	192.168.2.210(杭州)	• 运行中	专有网络	CPU: 2核 内存: 4 GB (I/O优化)	按量 17-07-03 14:35 创建	管理 远程连接 更多 +

图 1.3.4

至此云资源都已准备完成,可以进行 AD 服务器搭建。

2.AD 服务器搭建

2.1 主 AD 服务器搭建

1. 在 ECS 控制台,选择需要作为主 AD 服务器的实例,点击 远程连接(图 2.1.1),跳转到

管理终端页面,复制 远程连接密码。通过输入远程连接密码,和云服务器进行连接,并通过左上角 发送远程命令 CTRUL+ALT+DELETE,输入服务器购买时设置的密码登陆 到 Windows 内部。

实例ID/名称		监控	所在可用区	IP地址	状态(运行中) 👻	网络类型(全部) ▼	配豐	付遡方式(全部) ▼	操作
i-bp13cbiz72g5mat4imt0 iZ72g5mat4imt0Z	° /4	R	华东 1 可用区 E	192.168.1.134(私有)	● 运行中	专有网络	CPU: 2核 内存:4GB(I/O优化)	按量 17-07-03 14:36 创建	管理 远程连接 更多▼
i-bp13cbiz72g5mat4imsy iZ72g5mat4imsyZ	• 🚑	¥	纵东 1 可用区 F	192.168.2.210(私有)	● 运行中	专有网络	CPU: 2核 内存:4 GB (I/O优化)	按量 17-07-03 14:35 创建	管理 远程连接 更多▼

图 2.1.1

2. 在 **开始**菜单--搜索程序和文件中输入 CMD,打开命令窗口,并输入 dcpromo,启动 AD 安装向导,图 2.1.2



图 2.1.2

3. 点击下一步至 选择某一部署配置 图 2.1.3,选择中 在新林中新建域,并点击下一步

る Active Directory 域服务安装向导	×
选择某一部署配置 您可为现有林或新林创建域控制器。	
○ 现有林 (2)	
○ 向现有域添加域控制器 (A)	
○ 在现有林中新建域 (C) 此服务器将成为新域中的第一个域控制器。	
◎ 在新林中新建域 @)	
有关可能的部署配置的详细信息	
<i>↓</i>	
〈上一步(33) 下一步(33) 〉	取消

图 2.1.3

4. 在 **命名林根域** 图 2.1.4,输入 AD 域名(如 vpc.clouddesktop.com),点击下一步,系统 自动验证创建 AD 相关的信息

Active Directory 域服务安装同导	
命名林根域 林中的第一个域是林根域。其名称也是该林的名称。	
键入新目录林根级域的完全限定的域名(FQDN)。	
vpc. clouddesktop. com	
初放口: corp. contoso. com	

图 2.1.4

5. 在 设置林功能级别 图 2.1.5 选择 Windows Server 2008 R2,点击下一步

■ Active Directory 域服务安装向导	×
设置林功能级别 选择林功能级别。	
林功能级别(?):	
Windows Server 2008 R2	•
详细信息 (D):	
Windows Server 2008 R2 林功能级别提供 Windows Server 2008 林功能 级别中可用的所有功能,以及以下附加功能: - 回收站,启用后,它提供运行 Active Directory 域服务时 完整还原删除的对象的功能。 默认情况下,在该林中创建的任何新域将在 Windows Server 2008 R2 域 功能级别下操作。	×
⚠️ 您将只能向该林添加运行 Windows Server 2008 R2 或更高版 本的域控制器。	
有关 <u>域和林功能级别的</u> 详细信息	
R	
〈上一步 (8) 下一步 (9) 〉	取消

图 2.1.5

6. 在 其他域控制器选项 图 2.1.6,选中 DNS 服务器(D),点击下一步

a Active Directory 域服务安装向导	×
其他域控制器选项	
为此域控制器选择其他选项。	
☑ DNS 服务器 (D)	
☑ 全局编录 (G)	
□ 只读域控制器 (RODC) (R)	
其他信息 (A):	
林中的第一个域控制器必须是全局编录服务器且不能是 RODC。	<u> </u>
建议您将 DWS 服务器服务安装在第一个域控制器上。	
	_
	<u>~</u>
有关其他城控制器洗项的详细信息	
<<上─歩 (8) 下─歩 (8) 入	取消

图 2.1.6

说明这里安装的 DNS 服务器只能被查找内网 IP 地址

7. 在 静态 IP 分配 图 2.1.7,选择 是

<u></u> 静和	态 IP 分配 🛛 🔀
\bigcirc	此计算机具有动态分配的 IP 地址
	此计算机上至少有一个物理网络适配器未将静态 IP 地址分配给其 IP 属 性。如果同时为某个网络适配器启用 IPv4 和 IPv6,则应将 IPv4 和 IPv6 静态 IP 地址分配给该物理网络适配器的 IPv4 和 IPv6 属性。应 对所有物理网络适配器执行此类静态 IP 地址分配,以便执行可靠的域名 系统 (DNS)操作。 是否要在未分配静态 IP 地址的情况下继续执行操作?
	→ 是(Y),该计算机将使用 DHCP 服务器自动分配的 IP 地址(不推荐)。
	→ 否(N),将静态 IP 地址分配给所有物理网络适配器。
()	有关配置 TCP/IP 和 DWS 客户端设置的详细信息。

图 2.1.7

8. 在 **域服务安装向导** 图 2.1.8,选择 是



图 2.1.8

9. 在 数据库、日志文件和 SYSVOL 的位置 图 2.1.9,设置文件存放路径,点击下一步

♂ Active Directory 域服务安装向导	×
数据库、日志文件和 SYSVOL 的位置 指定将包含 Active Directory 域控制器数据库、日志文件和 文件夹。	sysvol 的
为获得更好的性能和可恢复性,请将数据库和日志文件存储在不	下同的卷上。
数据库文件夹 (D):	
C:\Windows\NTDS	浏览(R)
日志文件文件夹 (L):	
C:\Windows\NTDS	浏览(0)
SYSVOL 文件夹(S):	
C:\Windows\SYSVOL	浏览(W)
	\mathbf{k}
有关 <u>放置 Active Directory 域服务文件</u> 的详细信息	
< 上一步 (B) 下一步 (30) > 取消

图 2.1.9

10. 在 目录服务还原模式的 Administrator 密码 图 2.1.10,设置 Administrator 密码,必须 包含大写字母、小写字母、数字和特殊字符中的 3 种,点击下一步

on Active Directory 域服务安装向导	×
目录服务还原模式的 Administrator 密码	
目录服务还原模式 Administrator 帐户不同于域 Administrator 帐户。 为 Administrator 帐户分配一个密码,将在以目录服务还原模式启动此域控 制器时使用该帐户。我们建议您选择一个强密码。	
 密码 (P): 确认密码 (C): 关于目录服务还原模式密码的详细信息 	
< 上一步 (B) 下一步 (M) > 取	

图 2.1.10

```
11. 在"摘要" 图 2.1.11
```

可以选择 **导出设置(E)...**,用来保存 AD 创建的设置(保存到文件 vpc.cldouddesktop.com.txt),下次假如需要创建配置类似的 AD,只需要用以下 CM 命令进行无人值守创建 AD:

dcpromo /unattend:filepath/vpc.cldouddesktop.com.txt

点击下一步

a Active Directory 域服务安装向导	×
摘要	
检查您的选择(&): 将该服务器配置为新林中的第一个 Active Directory 域控制器。 新域名为"test.clouddesktop.com"。这也是新林的名称。 域的 NetBIOS 名称为"TEST"。 林功能级别: Windows Server 2008 R2 域功能级别: Windows Server 2008 R2 站点: Default=First=Site=Name 其他选项: 要更改选项,单击"上一步"。要开始操作,单击"下一步"。 可以将这些设置导出到一个应答文件中以用于其他无人 参与操作。 有关 <u>使用应答文件</u> 的详细信息	
< 上一步 (8) 下一步 (8) >	取消

图 2.1.11

12. 系统开始创建 AD 图 2.1.12, 创建完以后必须重启,因此可以选中 完成后重新启动

Active Directory 域服务安装向导
向导正在配置 Active Directory 域服务。此过程可能需要几分钟到几小时, 具体依您所选的环境和选项而定。
等待 DNS 安装完成
取消
☑ 完成后重新启动 (R)

图 2.1.12

13. 重启完成以后,可以看到在登陆界面 Administrator 前面多了一个域名第一个字段 图 2.1.12,说明 AD 已经创建成功,同时登陆到 Windows 内部,进行 **证书服务** 创建





14. 在 Windows 任务栏启动 服务器管理器 图 2.1.14



图 2.1.14

在 **服务器管理器** 窗口 图 2.1.15,选中 **服务器管理器**,点击右键,点击 **添加角** 色



图 2.1.15

15. 启动 **添加角色向导**,在 **开始之前**页面点击下一步,进入 **选择服务器角色** 图 2.1.16, 选中 Activity Directory 证书服务,点击下一步



图 2.1.16

16. 在 选择为 Activity Directory 证书服务安装的角色服务: 图 2.1.17, 选中 证书颁发机 构 Web 注册 ,并点击 添加所需的角色服务 图 2.1.18,点击下一步

选择为Active Directory 证书服务安装的角色服务: 角色服务(R):	描述:
 ✓ 证书颁发机构 ● 证书颁发机构 Web 注册 ● 联机响应程序 ● 网络设备注册服务 ● 证书注册 Web 服务 ● 证书注册策略 Web 服务 	证书颁发机构 Web 注册提供了简单 的 Web 界面,使用户可以执行诸如 请求和续订证书、检索证书吊销列 表(CRL)和执行智能卡证书注册等任 务。

图 2.1.17

添加角色的	向导		×
€ E	 是否添加 证书颁发机构 Web 注册 所需的角色. 无法安装 证书颁发机构 Web 注册,除非同时安装所需的角色 描述: □ Web 服务器 (TIS) □ Web 服务器 □ 管理工具 □ 远程服务器管理工具 □ 角色管理工具 	服务和功能? 务和功能。 <u>务器(IIS)</u> 提供可靠、同 的 Web 应用程序基础组	可管理并且 5构。
	添加	所需的角色服务(A)	取消
① 为值	可需要这些角色服务和功能?		

图 2.1.18

在 指定安装类型 图 2.1.19,选择 企业,点击下一步



图 2.1.19

在 指定 CA 类型 图 2.1.20,选择 根 CA(R),点击下一步

漆加用巴内寺	<u>^</u>
指定 CA 类型	
开始之前 服务器角色 AD CS 角色服务 安装类型 CA 类型	可以配置根 CA 和从属 CA 的组合来创建分层公钥基础结构 (PKI)。根 CA 是发布其自己的自签名证书 的 CA。从属 CA接收来自其他 CA 的证书。指定您需要设置根 CA 还是从属 CA。
私钥 加密 CA 名称 有效期	

图 2.1.20

在 设置私钥 图 2.1.21,选择 新建私钥

添加角色向导		×
设置私钥		
开始之前 服务器角色 AD CS 角色服务	若要生成证书并颁发给客户端,CA 必须有一个私钥。指定您要新建私钥还是使用现有私钥。 新建私钥(B) 如果您没有私钥或者要新建一个私钥以增强安全性,请使用此选项。系统将要求您选择加密服务提 供程序并指定私钥的密钥长度。若要颁发新证书,还必须选择一个哈希算法。 	
安裝类型 CA 类型 私钥	 ○ 使用现有私钥(0) 使用此选项可确保重新安装 CA 时与先前颁发的证书的连续性。 ◎ 选择一个证书并使用其关联私钥(0) 如果您在此计算机上有一个现有证书,或者如果您希望导入一个证书并使用其关联私钥,请洗 	
加密 CA 名称 有效期	择此选项。 C 选择此计算机上的现有私钥 (2) 如果您已保留来自以前安装的私钥或需要使用其他来源的私钥,请选择此选项。	

图 2.1.21

在为CA配置加密 图 2.1.22,设置秘钥相关内容,点击下一步

涂加用巴回导	
🎼 为 CA 配置加密	
开始之前	若要新建私钥,您必须首先选择加密服务提供程序、哈希算法和适合您颁发的证书的特定用途的密
服务器角色	钥长度。为密钥长度选择更高的值将导致更强的安全性,但会增加完成签名操作所需的时间。
AD CS	选择加密服务提供程序(CSP)(C):
角色服务	RSA#Microsoft Software Key Storage Provider ▼ 2008 ▼
安装类型	选择此 CA 颁发的签名证书的哈希算法 CH):
CA 类型	SHA256
私钥	SHA384
加密	SHA512
CA 名称	SHA1
有效期	◀
证书数据库	■ 当 CA 访问该私钥时,允许管理员交互操作(A)。

图 2.1.22

在 配置 CA 名称 ,设置证书名称,点击下一步

添加角色向导		×
📭 配置 CA 名称		
开始之前 服务器角色 AD CS 角色服务 安装类型 CA 类型 AA钥	 键入公用名称以识别此 CA,此名称会被添加到由该 CA 颁发的所有证书中。可分辨名称的后缀值是自动生成的,但可以修改。 此 CA 的公用名称 (C): test=iZxjes9zn9ntfbZ=CA 可分辨名称后缀 (D): DC=test, DC=clouddesktop, DC=com 	
CA 名称	可分辨名称的预览(V): 「Withouts Swiss	
有效期	Currest Issjessinghting of, burrest, burrested desktop, burrom	
证书数据库		
Web 服务器(IIS)		

图 2.1.23 在 **设置有效期** 图 2.1.24,设置证书有效期,点击下一步

添加角色向导		x
设置有效期		
开始之前 服务器角色 AD CS 角色服务 安装类型 CA 类型 私钥 加密 CA 名称	会招一个证书颁发给此 CA 以保护与其他 CA 和请求证书的客户端之间的通信。CA 证书的有效期可以 基于许多因素,包括 CA 的预期目的以及为保护 CA 您已采取的安全措施。 为此 CA 生成的证书选择有效期(V): 10 年 CA 过期日期: 2027/5/23 16:31 请注意,CA 仅在其过期日期之前才能颁发有效的证书。	
有效期 证书数据库 Web 服务器(IIS)		

图 2.1.24

在 配置证书数据库 图 2.1.25,设置数据库位置,点击下一步

添加角色向导		X
配置证书数据库		
开始之前 服务器角色	证书数据库记录所有证书请求、已颁发的证书以及已吊销或过期的证书。CA 可使用该 视管理活动。	数据库日志来监
AD CS 角色服务 安装类型 CA 类型	 证书数据库位置 (C): C:\Windows\system32\CertLog □ 在此位置使用来自上次安装的现有证书数据库 (0) 证书数据库日志位置 (C): 	浏览(0)
私钥 加密 CA 名称 有效期 江口#Mgc	C:\Windows\system32\CertLog	浏览(8)
uttyygg年 Web 服务器(IIS)		

图 2.1.25 在 选择角色服务 图 2.1.26,选择系统默认的服务即可,点击下一步



图 2.1.26

17. 在 **确认安装选择** 图 2.1.27,可以检查配置是否正确,如果没有问题,点击安装,进行 证书安装



图 2.1.27

18. 证书服务安装完成以后,可以在 **服务器管理器** 窗口 图 **2.1.28**,确认证书服务是否安装 成功。

同时,我们可以通过 LDAP SSL 协议访问 AD。



图 2.1.28

19. 为了确保 AD 服务器可以正确设置到云桌面系统中,请手动重置一下管理员密码(图 2.1.29),重置密码时,请不要勾选 用户下次登录时需更改密码(图 2.1.30)

	?		
 服务器管理器 (iZibcimutfetf7Z) 角色 Active Directory 域服务 Active Directory 用户和计算机 wpc. clouddesktop.com t Domain Controllers t Domain Controllers t PoreignSecurityPrincipal t Managed Service Accounts Users t Active Directory 证书服务 t DNS 服务器 t Web 服务器 (IIS) t 酸 t 奇绪 	Users 19 个对象 名称 Administrator Administrator Administrator Allowed RODC Passw Cert Publishers Denied RODC Passw Denied RODC Passw DnsAdmins Domain S Domain Admins Domain Computers Domain Computers Domain Guests Domain Guests Domain Users Enterprise Admins Enterprise Read-o: Group Policy Crea Guest RAS and IAS Serve: Read-only Domain I Schema Admins WinRMRemoteWMIUsers	[启动筛选器] 要型 田户 夏制(C) 添加到组(G) 漆加到组(G) 禁用帐户(S) 重置密码(R) 移动(V) 打开主页(0) 发送邮件(A) 所有任务(K) 鄭切(T) 刪除(0) 重命名(M) 属性(R) 帮助(H) 安全组 - 1 安全组 - 2	推管允此不或允指加域域所企该这供这此架。

四 2.1.29	冬	2.1	29
----------	---	-----	----

新密码 ON):	•••••
角认密码(C):	•••••
用户下次登录时	「須更改密码の」
更佳面改生动,田	日户心湎注销,然后重新登录。

图 2.1.30

20. 主 AD 服务器已经安装和配置完成,重启 AD 服务器。

2.2 备 AD 服务器搭建

1. 在 ECS 控制台查看主 AD 服务器的 IP 地址(图 2.2.1),并记录。选择另一台需要搭建备 AD 服务器,通过远程连接登陆到 Windows 内部。

E	〕 实例ID/名称		监控	所在可用区	IP地址	状态(运行中) ▼	网络类型(全部) ▼	配證	付腸方式(全部) ▼	操作
6	i-bp13cbiz72g5mat4imt0 iZ72g5mat4imt0Z	° //	ĸ	华东 1 可用区 E	192.168.1.134(私有)	● 還行中	专有网络	CPU: 2核 内存:4GB(I/O优化)	按量 17-07-03 14:36 创建	管理 远程连接 更多▼
6	i-bp13cbiz72g5mat4imsy iZ72g5mat4imsyZ	•	ĸ	纵东 1 可用区 F	192.168.2.210(私有)	● 运行中	专有网络	CPU: 2核 内存:4 GB (I/O优化)	按量 17-07-03 14:35 创建	管理 远程连接 更多・

图 2.2.1

2. 在 Windows 中,打开命令窗口,输入 c:\windows\system32\sysprep\sysprep.exe, 打开 系 统准备工具 (图 2.2.2),选中 进入系统全新体验 勾选 通用,点击 确定。等系统清理完成后重启系统(有可能会提示 尝试使用 Sysprep 处理计算机时出错,直接手动重启即可)。系统重启后,需要重新设置登录密码。

系统准备工具 3.14	×
系统准备工具(Sysprep)为硬件独立和清理准备计算机。	
┌系统清理操作 ⑷	
→ 送入系统全新体验(OOBE)	
☑ 通用 ⓒ	
● 新自动	
确定 取消	
	_



在 Windows 中,打开 网络连接 - 本地连接 - Internet 协议版本 4 (TCP/IPV4)属性(图 2.2.3),选中 使用下面的 DNS 服务器地址,在 首先 DNS 服务器 中填入主域控的 IP 地址,点击 确定。DNS 配置完成以后,可以打开命令窗口,ping 主域控设置的域名。

假如域名成功转换成解析成主域控的 IP 地址,并收到回复,说明 DNS 设置正确,否则 请检查 AD 服务器和 DNS 配置是否正确。

🧧 网络连接	
🌀 ◯∽ 😰 → 控制面板 → 网络和 Internet → 网络连接 →	▼ 😝 捜索 网络连接
组织 ▼ 禁用此网络设备 诊断这个连接 重命名此连接 查看此连	接的状态 更改此连接的设置 📑 🔻 🛄 🥑
本地注接 4 内容 2 Red Hat VirtIO Ethernet ● 本地注接 4 既在 四络 注接时使用: ● Red Hat VirtIO Ethernet 此注接使用下列项目 0): ● Microsoft 网络客户 ● QoS 数据包计划程序 ● Microsoft 网络客户 ● Microsoft 网络名 ● Microsoft 网络名 ● Microsoft 网络名 ● Microsoft 网络客户 ● Microsoft 网络客户 ● Microsoft 网络客户 ● Microsoft 网络名 ● Microsoft Macha ● Microsoft	Internet 协议版本 4 (TCP/IIP+4) 厘性 ? × 常规 备用配置 如果网络支持此功能,则可以获取自动指派的 IP 设置。否则, 您需要从网络系统管理员处获得适当的 IP 设置。 • 自动获得 IP 地址(0) ● 使用下面的 IP 地址(S): IP 地址(I): 子网撩码(0):
атта 🍇 🗾 🚝 🕎	

图 2.2.3

 打开一个命令窗口,并输入 dcpromo,打开 Activity Directory 域服务安装向导 (图 2.2.4), 点击下一步至 选择某一部署配置 中 现有林 – 向现有域添加域控制器 (图 2.2.5),点 击下一步

🚮 Active Directory 域服	务安装向导
	 次迎使用 Active Directory 域服务 安装向导 此向导有助于在该服务器上安装 Active Directory 域服务(AD DS),从而使该服务器成为 Active Directory 域控制器。单击"下一步"继续。 □ 使用高级模式安装(A) □ 使用高级模式安装(A) □ 了解有关高级模式安装中可用的其他选项的详细 信息。
	<上一步(B) 下一步(M) > 取消
	图 2.2.4
圆Active Directory 域服	务安装向导
选择某一部署配置 您可为现有林或新林创	建域控制器。
 现有林 (2) 同现有域添加地 	
○ 在现有林中新建 此服务器将成注	赴域℃) 为新域中的第一个域控制器。
C 在新林中新建域 (D)	
有关可能的部署配置的	洋细信息
	< 上一步 (B) 下一步 (M) > 取消 图 2.2.5

5. 在 网络凭据 (图 2.2.6) 窗口, 输入 AD 的域名, 选择 备用凭据, 点击 设置, 在 网络凭据 (图 2.2.7) 窗口中输入 AD 的管理员用户名和密码, 点击确定, 并点击下一步。

🖥 Active Directory 域服务安装向导	×
网络凭据 指定将在其上执行安装的林的名称,以及具有执行安装所需的足够权限的 帐户凭据。	
键 入位于计划安装此域控制器的林中任何域的名称(T):	
vpc. clouddesktop. com	
请指定用于执行安装的帐户凭据: ○ 我的当前登录凭据(WINALIY-7QTKFIE\Administrator)(C) ● 备用凭据(A):]
<上一步(B) 下一步(D) > 取消	ŧ.

图 2.2.6

нарена.	110411543	MUMAN JU	149.		
	a	dministrat	or		
			•••••		
	198	vpc. clou	iddesktop. (zom	

图 2.2.7

6. 在 其他域控制器选项 窗口(图 2.2.8),默认选中 DNS 服务器和全局编录,点击下一步, 在 静态 IP 分配 (图 2.2.9)中点击 否(是),点击下一步。在图 2.2.9 显示窗口中单 击 是。



图 2.2.8



图 2.2.9

■ Active Directory 域服务安装向导	×
无法创建该 DNS 服务器的委派,因为无法找到有机 域或者它未运行 Windows DNS 服务器。如果您要与 基础结构集成,应在父区域中手动创建对该 DNS 用 派,以确保来自域 "vpc. clouddesktop. com"以外 称解析。否则,不需要执行任何操作。 是否要继续?	又威的父区 亏现有 DNS 陨务器的委 的可靠名
是(17)	否(10)

图 2.2.10

7. 在 **数据库、日志文件和 SYSVOL 的位置** (图 2.2.11)窗口中设置这几个文件的保存位置。

■ Active Directory 域服务安装向导	X
教据库、日志文件和 SYSVOL 的位置 指定将包含 Active Directory 域控制器数据库、日志文件和 SY 文件夹。	rsvol.的
为获得更好的性能和可恢复性,请将数据库和日志文件存储在不同	同的卷上。
数据库文件夹 (D):	
C:\Windows\NTDS	浏览(R)
日志文件文件夹 (L):	
C:\Windows\NTDS	浏览 (0)
SYSVOL 文件夹(S):	,
C:\Windows\SYSVOL	浏览(W)
有关 <u>放置 Active Directory 域服务文件</u> 的详细信息	
< 上一步 (8) 下一步 (8)) >

图 2.2.11

8. 在 目录服务还原模式的 Administrator 密码 (图 2.2.12)中设置还原密码。点击下一步,等待备 AD 服务器配置完成后重启。

	J	女装问诗	<u>×</u>
目录服务	还原模式的 Admin	istrator 密码	
目录用	服务还原模式 Admini	strator 帐户不同于域 Administrator 呐	k户。
为 Ad 制器明	ministrator 帐户分 时使用该帐户。我们建	配一个密码,将在以目录服务还原模式启 【议您选择一个强密码。	动此域控
密码	œ):		
确认额	答码(C):	•••••	
关于	目录服务还原模式密码	的详细信息	
			-
		<u>〈上一步(B)</u> 下一步(M) 〉	
		图 2.2.12	
ctive I	lirectory 域服务す	安装向导	×
摘要			
尚 要			
尚安 检查()	购选择 (R) :		
商豊 检查 終 域控	函的选择(R): Active Directory	域服务安装向导	
簡要 检查您 将域控 站点	函的选择 (R): Active Directory 向导正在配置 Activ 具体依您所选的环境	· 域服务安装向导 ve Directory 域服务。此过程可能需要厂 氧和选项而定。	1分钟到几小时,
简要步 检将域。 站 其 只	a的选择 (R): Active Directory 向导正在配置 Activ 具体依您所选的环境	<mark>域服务安装向导</mark> ve Directory 域服务。此过程可能需要厂 和选项而定。	山 山分钟到几小时,
简要步 检将域站 其一位公式 这一位一个公式	题的选择 (R): Active Directory 向导正在配置 Activ 具体依您所选的环境	<mark>域服务安装向导</mark> ve Directory 域服务。此过程可能需要厂 和选项而定。	山 山分钟到几小时,
简要要 检将域站 其一一更 新	驱的选择 (R): Active Directory 向导正在配置 Activ 具体依您所选的环境	<mark>域服务安装向导</mark> ve Directory 域服务。此过程可能需要厂 和选项而定。	山 分钟到几小时,
简音要检将域站一样一更源。 查该控点他口公子 亚新域。	函的选择 (R): Active Directory 向导正在配置 Activ 具体依您所选的环境	<mark>域服务安装向导</mark> ve Directory 域服务。此过程可能需要厂 和选项而定。	1分钟到几小时,
简明要。 检将域站其一更源。要一 查该控点他。公子派新域更。	函的选择 (R): Active Directory 向导正在配置 Activ 具体依您所选的环境	<mark>域服务安装向导</mark> ve Directory 域服务。此过程可能需要厂 和选项而定。 NALLY-7QTKFIE\$ 的域 vpc. clouddesktop	L分钟到几小时, .com 查找域控制
简为要检将域站,其一更源要,可 查该控点,他只全观新域更见。	a的选择(R): Active Directory 向导正在配置 Activ 具体依您所选的环境	域服务安装向导 ve Directory 域服务。此过程可能需要厂 和选项而定。 NALIY-7QTKFIE\$ 的域 vpc. clouddesktop	L分钟到几小时, .com 查找域控制
简为要检将域站,其一更源。要要可参考查。 语按点 化只全比亚新域 更以与圣道。"	a的选择 (R): Active Directory 向导正在配置 Activ 具体依您所选的环境	域服务安装向导 ve Directory 域服务。此过程可能需要厂 和选项而定。 NALIY-7QTKFIE\$ 的域 vpc. clouddesktop 取消	L分钟到几小时, .com 查找域控制
简为要检将域站,其一更源。要一可参有查。该控点,他只全现新域,更以与关	SAD Directory Active Directory Active Directory 向导正在配置 Activ 具体依您所选的环境 正在为含有帐户 WII 器	<mark>域服务安装向导</mark> ve Directory 域服务。此过程可能需要厂 和选项而定。 NALIY-7QTKFIE\$ 的域 vpc. clouddesktop 取消	业 L分钟到几小时, . com 查找域控制
简为要检将一域站,其一一更源。要要可参有一步查该,控点。他只全见"新"域更一以与关系。	a的选择 (R): Active Directory 向导正在配置 Activ 具体依您所选的环境 正在为含有帐户 WII 器	<mark>域服务安装向导</mark> ve Directory 域服务。此过程可能需要厂 和选项而定。 NALIY-7QTKFIE\$ 的域 vpc. clouddesktop 取消 (R)	业 L分钟到几小时, . com 查找域控制
简为要检将域站,其一更源。要一可参有查。 道该控点 他已全弧 新域更一以与关系	a的选择 (R): Active Directory 向导正在配置 Activ 具体依您所选的环境 正在为含有帐户 WII 器	域服务安装向导 ve Directory 域服务。此过程可能需要厂 和选项而定。 NALIY-7QTKFIE\$ 的域 vpc. clouddesktop 取消 (R) (R)	L分钟到几小时, . com 查找域控制

图 2.2.13

重启完成以后,可以看到在登陆界面 Administrator 前面多了一个域名第一个字段 图
 2.2.14,说明 AD 已经创建成功,同时登陆到 Windows 内部,进行"证书服务"创建





10. 打开 服务器管理器 - 添加角色 - 添加角色向导,点击下一步到选择服务器角色(图 2.2.15),点击下一步到选择角色服务(图 2.2.16),选中 证书颁发机构 Web 注册,在添加角色向导 弹框中,点击 添加手续的角色服务(图 2.2.17),点击下一步

添加角色向导		×
选择服务器角色		
 开始之前 服务器角色 AD CS 角色服务 安装类型 CA 类型 私钥 加密 CA 名称 证书申请 证书数据库 确认 进度 结果 	 法择要安装在此服务器上的一个或多个角色。 角色 (R): Active Directory Kights Management Services Active Directory 联合身份验证服务 Active Directory 轻型目录服务 Active Directory 短期(P)(P)(P)(P)(P) Active Directory 证明服务 DISE 服务器 (D)(P)(P)(P)(P)(P) Web 服务器 (D)(P)(P)(P)(P) Web 服务器 (D)(P)(P)(P)(P)(P) Web 服务器 (D)(P)(P)(P)(P)(P)(P) Web 服务器 (D)(P)(P)(P)(P)(P)(P)(P)(P) Web 服务器 (D)(P)(P)(P)(P)(P)(P)(P)(P)(P)(P)(P)(P)(P)	描述: Active_Directory 证书服务(AD CS)用于创建证书颁发机构和相关的 角色服务,可以使您颁发和管理在 各种应用程序中所使用的证书。

图 2.2.15



图 2.2.17

11. 在接下来的配置窗口中都选择系统默认配置,下一步直到 向父 CA 申请证书 窗口(图 2.2.18),选中 将证书请求发送给父级 CA ,点击 父 CA 后面的 浏览,弹出 选择证书 颁发机构,在弹框中过会列出主域控的 CA,选中,点击确定即可。最后点击下一步直 到 安装,并点击安装。

下 前父 са в	申请证书					
开始之前 服务器角色	您可以直接从您的 它发送给父级 CA	网络中的父级 CA 请求	¢此子级 CA 的证书,或者将请求保存到某个5	之件中并稍后将		
AD CS 角色服务	 将证书请求发送 浏览方式(0): 	送给父级 CA(E) ④ CA 名称	○ 计算机名称			
安装类型 CA 类型	52 CA:	父 CA: iZibcimutfetf7Z.vpc.clouddesktop.com/vpc-iZibcimutfetf7Z 浏览(3)				
私钥	○ 将证书请求保存	F到某个文件中并稍后:	手动将它发送给父级 CA(V):			
加密	文件名:	C:\ABCD123458QSCDE vpc elouddesktop.com_vpc=ABCD123458QS 测造())				
CA 名称	 愈必须手a 	b从父级 CA 取回证书。	以使此 CA 可操作。			
证书申请						



12. 等服务器安装 证书服务和 Web 服务器 完成以后, 备 AD 服务器的证书服务也安装完成。13. 重启 AD 服务器, 重启完成以后,可以进行云桌面环境设置了。

3.云桌面环境设置

- 进入<u>云桌面控制台</u>,选中需要配置的区域(如华东1),点击 桌面管理 创建,弹出 云 桌面环境设置 窗口。
- 2. 在 云桌面环境设置 选择专用网络 (图 3.1)中选择创建好的专有网络。点击下一步 云桌面环境设置 [华东 1] ×

选择专用网络	选择安全组	AD设置
选择专有网络	vpc-bp1bh4dx9tmu06qv6u 🗸	
	如需使用其他专有网络,请选择已有	

-			1	1	
- 1		e	3	2	

3. 在 **云桌面环境设置 – 选择安全组**(图 3.2)中,选中域控服务器对应的安全组,点击下一步。

云桌面环境设置[华东7	1]		×
医择身用网络	选择安全组		ADige
安全组10 🗸		搜索	
安全组名称	安全组ID	创建时间	
OnEcs-Gust	sg-bp17vkyzh9iktp4nbch9	2017-06-21 10:14:46	宣吾规则>>





 \times

图 3.2

4. 在**云桌面环境设置 – AD 设置**中,选择 AD 网络类型 为 专有网络,并根据 ECS 控制台 上面的 IP 地址,填写到主 AD 服务器 IP 和备 AD 服务器 IP 中,最后填写好 AD 域名和管 理员账号、密码,点击确定。

云桌面环境设置[华东1]

选择专用网络	选择安全组	AD设置
L)	「下信息为您企业自建域控服务器的信息	
* AD网络类型:	专有网络	/ ?
* 主AD服务器IP:	192.168.1.134	\bigcirc
备AD服务器IP:	192.168.2.210	(?)
DNS服务器IP:		(?)
备DNS服务器IP:		(?)
* AD域名:	vpc.clouddesktop.com	
* 管理员帐号:	Administrator	
* 管理员密码:	•••••	