**CVAD 2203 POC Runbook**

微软基础架构环境安装

**目录**

[第一章 主要步骤 3](#_Toc105511389)

[第二章 安装参数 3](#_Toc105511390)

[第三章 域控与DNS角色安装与配置 3](#_Toc105511391)

[第四章 DHCP角色安装与配置 10](#_Toc105511392)

[第五章 活动目录用户和OU准备 22](#_Toc105511393)

[第六章 配置用户权限委派 24](#_Toc105511394)

[第七章 Windows CA服务器的安装与配置 27](#_Toc105511395)

[第八章 环境完成确认检查 35](#_Toc105511396)

[第九章 产品版本 35](#_Toc105511397)

1. 主要步骤

本章节介绍了Citrix虚拟化环境中Windows基础架构服务器安装的步骤，其中包括了

1. 准备Windows Server 2019 服务器
2. 域控和DNS角色的安装及配置
3. DHCP服务的安装和配置
4. AD用户及OU的准备
5. Windows CA服务器的安装及配置
6. 安装参数

|  |  |  |
| --- | --- | --- |
| **项目** | **配置** | **备注及注意事项** |
| AD服务器主机名 | CTXAD01 | 自定义AD服务器的机器名 |
| AD服务器IP地址 | IP: 192.168.101.100  DNS: 192.168.101.100  Gateway: 192.168.101.254 | AD服务器必须使用固定IP  服务器同时承载DNS角色  网关地址请按实际环境填写 |
| 活动目录域名 | FQDN:ctxdemo.local  NetBIOS:ctxdemo | 请按实际环境填写 |
| DNS转发地址 |  | 按实际环境，配置可以工作的内网或者公网DNS服务器，以使测试环境可以正常解析外部资源的域名。 |
| 反向DNS查找区域 | 192.168.101.x | 建立实际环境使用的IP地址段对应的反向查找区域 |
| DHCP 地址段 | 192.168.101.150-192.168.101.200 | 请根据环境具体修改 |
| DHCP Option | 子网掩码：255.255.255.0  DNS：192.168.101.100  默认网关:192.168.101.254 | 请根据环境具体修改 |

1. 域控与DNS角色安装与配置

在Citrix环境中，AD是必备的基础架构角色，AD用来实现用户身份验证而DNS服务用来实现系统全局FQDN.

AD 域控服务器通常与 DNS 和 DHCP 合设。建立域的方法是先安装一台独立服务器或成员服务器，然后再将其升级为域控制器。域控制要先修改好主机名称、设置固定 IP。

1. 准备一台Windows Server 2019 虚拟机，由于我们创建的这台虚拟机适用于活动目录服务器，所以首先将该服务器的IP地址改为静态IP。同时，活动目录服务器同时要承担DNS和DHCP的功能，所以DNS地址我们设置为本机。

图形用户界面, 文本

描述已自动生成

1. 运行服务器管理器的“添加角色和向导”

图形用户界面, 文本, 应用程序

描述已自动生成

1. 选择“基于角色或基于功能的安装”

图形用户界面, 文本, 应用程序, 电子邮件

描述已自动生成

1. 选择本机

图形用户界面, 文本, 应用程序

描述已自动生成

1. 选择“Active Directory域服务”

图形用户界面, 应用程序

描述已自动生成

1. 功能界面直接点击“下一步”

图形用户界面, 应用程序

描述已自动生成

1. 确认所选内容，点击安装

图形用户界面, 文本, 应用程序

描述已自动生成

1. 安装完成

图形用户界面, 文本, 应用程序

描述已自动生成

1. 现在进入AD配置，点击‘将此服务器提升为域控器‘

图形用户界面, 文本, 应用程序, 电子邮件

描述已自动生成

1. 这是POC环境里的第一台AD，所以选择‘添加新林‘，并指定域名。这里使用ctxdemo.local域名

图形用户界面, 应用程序

描述已自动生成

1. 保持默认设置，下一步

图形用户界面, 应用程序

描述已自动生成

1. DNS选项保持默认，下一步

图形用户界面, 文本, 应用程序

描述已自动生成

1. 输入NETBIOS域名:CTXDEMO

图形用户界面, 文本, 应用程序

描述已自动生成

1. 指定路径，保持默认或者按需修改

图形用户界面

描述已自动生成

1. 开始安装，安装完成后服务器会重启一次，至此，AD角色安装完毕。

图形用户界面, 文本, 应用程序, 电子邮件

描述已自动生成

1. DHCP角色安装与配置

在桌面虚拟化的环境中，所有的虚拟机都需要通过DHCP来获取IP地址

1. 在服务器角色里添加‘DHCP服务器‘角色

图形用户界面, 文本, 应用程序

描述已自动生成

1. 安装DHCP角色

图形用户界面, 文本, 应用程序, 电子邮件

描述已自动生成

1. 安装完毕后，进行初始配置

图形用户界面, 文本, 应用程序

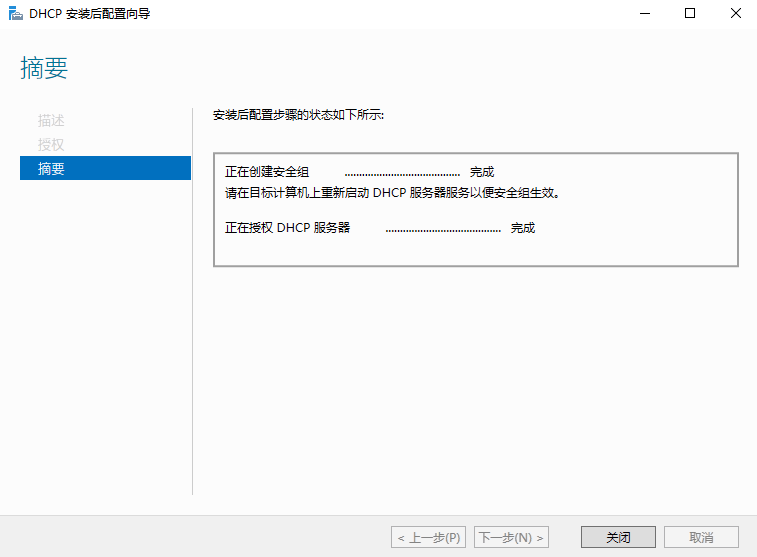
描述已自动生成

1. 指定用户账号

图形用户界面, 应用程序

描述已自动生成

1. 完成安装后初始配置



1. 现在进行DHCP 配置，打开DHCP配置界面，在 IPv4下，新建作用域

图形用户界面, 应用程序

描述已自动生成

1. 自定义作用域名称与描述

图形用户界面, 文本, 应用程序, 电子邮件

描述已自动生成

1. 自定义DHCP Scope起始IP与结束IP,可按实际情况填写

图形用户界面, 文本

描述已自动生成

1. 如有排除IP，可以在下一步的界面中填写



1. 租期保持默认



1. 继续进行配置DHCP

图形用户界面, 文本, 电子邮件

描述已自动生成

1. 指定默认网关和域名

图形用户界面, 应用程序

描述已自动生成

图形用户界面, 文本, 应用程序

描述已自动生成

1. 激活DHCP作用域，完成配置

图形用户界面, 文本, 应用程序, 电子邮件

描述已自动生成

图形用户界面, 文本, 应用程序

描述已自动生成

图形用户界面, 文本, 应用程序

描述已自动生成

1. 活动目录用户和OU准备

在活动目录AD内建立以下用户和OU，以备测试环境使用

|  |  |  |  |
| --- | --- | --- | --- |
| **AD类 别** | **名 称** | **位 置** | **备 注** |
| **OU**  **组织单元** | 请按右面结构创建相应的OU：  Citrix，  CTXUsers，  Infra，  XenApp，  XenDesktop  vWin10 | Domain Root  |--Citrix  |--Infra  |---CTXUsers  |---XenApp  |---XenDesktop  |--vWin10MCS  |--vWin10PVS | Citrix，存放所有本POC有关的对象  Infra，存放基础构架服务器的计算机账号，如DDC/SF/PVS等  CTXUsers，存放测试用户账号  XenApp，存放XenApp服务器计算机账号  XenDesktop，存放虚拟桌面计算机账号  vWin10MCS, 存放MCS Win10虚拟桌面计算机账号  vWin10PVS, 存放PVS Win10虚拟桌面计算机账号 |
| **用户** | ctxadmin | CTXUsers OU内 | citrix环境管理员账号, 同时作为citrix环境中的服务账号，POC时请将密码设置为不过期  记得将其加入XD和XA服务器的本地管理员组内。  使用该账号创建新的虚拟桌面时候，还需要赋予其将计算机加入域的权限。如  加入 Account  operation 组（POC中可把账号加入Domain Admins组） |
| **用户** | User01  User02  …  User05 | CTXUsers OU内 | 测试用户账号 |
| **用户组** | USB Allow  USB Deny  XenApp  VDI  … | CTXUsers OU | 测试用各种Group，  可按需求添加 |

图形用户界面, 文本, 电子邮件

描述已自动生成

图形用户界面, 文本

描述已自动生成

1. 配置用户权限委派

对于ctxadmin用户，由于在使用过程中需要操作AD创建计算机账号，我们需要提前委派响应权限给特定OU， 下面以ctxadmin账号为例，说明如何设置委派

1. 右键Citrix OU， 选择委派控制

图形用户界面, 应用程序

描述已自动生成

1. 添加ctxadmin账号

图形用户界面, 文本

描述已自动生成

1. 选择自定义任务去委派

图形用户界面, 文本, 应用程序

描述已自动生成

1. 选择这个文件，这个文件夹中的对象…

在实际项目中，如果用户对权限控制比较严格，可以选择‘只是在这个文件夹下的对象’，在权限为派中，自定义需要的权限，POC可以选择‘完全控制’

图形用户界面, 文本, 应用程序

描述已自动生成

图形用户界面, 文本, 应用程序

描述已自动生成

1. 完成委派

图形用户界面, 文本, 应用程序

描述已自动生成

1. Windows CA服务器的安装与配置

为了在域中实现HTTPS安全通信，我们需要为主机提供服务器证书。PoC项目所需要使用的证书都请通过Windows Certificate Authority（CA）服务来创建。本例中，我们将Windows CA搭建在当前的域控服务器上

1. 在当前服务器上添加‘Active Directory证书服务’

图形用户界面, 文本, 应用程序

描述已自动生成

1. 角色服务中选择“证书颁发机构”、“证书颁发机构Web注册”

图形用户界面, 应用程序

描述已自动生成

1. 之后的项目保持默认设置，直接进行角色安装

图形用户界面, 文本, 应用程序

描述已自动生成

1. 安装完成后，进入配置界面

图形用户界面, 文本, 应用程序

描述已自动生成

1. 选择“证书颁发机构”、“证书颁发机构Web注册”

图形用户界面, 文本, 应用程序

描述已自动生成

1. 选择‘独立CA’

图形用户界面, 文本, 应用程序, 电子邮件

描述已自动生成

1. 选择‘根CA’

图形用户界面, 文本, 应用程序, 电子邮件

描述已自动生成

1. 创建新的私钥

图形用户界面, 文本, 应用程序

描述已自动生成

1. 选择SHA256，密钥长度使用4096

图形用户界面, 应用程序

描述已自动生成

1. 指定CA名称

图形用户界面, 文本, 应用程序, 电子邮件

描述已自动生成

1. 指定有效期

图形用户界面, 文本, 应用程序

描述已自动生成

1. 完成配置

图形用户界面, 文本, 应用程序, 电子邮件

描述已自动生成

1. 打开浏览器，输入 http://localhost/certsrv，确认证书服务工作

图形用户界面, 文本, 应用程序, 电子邮件

描述已自动生成

1. 环境完成确认检查

本章结束后，请确认以下事项以：

* 活动目录环境建立完毕。AD、DNS、DHCP服务配置完毕，工作正常。
* IP地址主机名等配置均按表格配置，并且加入活动目录，登录域正常。
* Windows CA服务配置完毕，工作正常
* 相应的OU，用户账号在活动目录内建立完毕。

1. 产品版本

|  |  |
| --- | --- |
| **产品** | **版本** |
| Windows Server | 2019 |