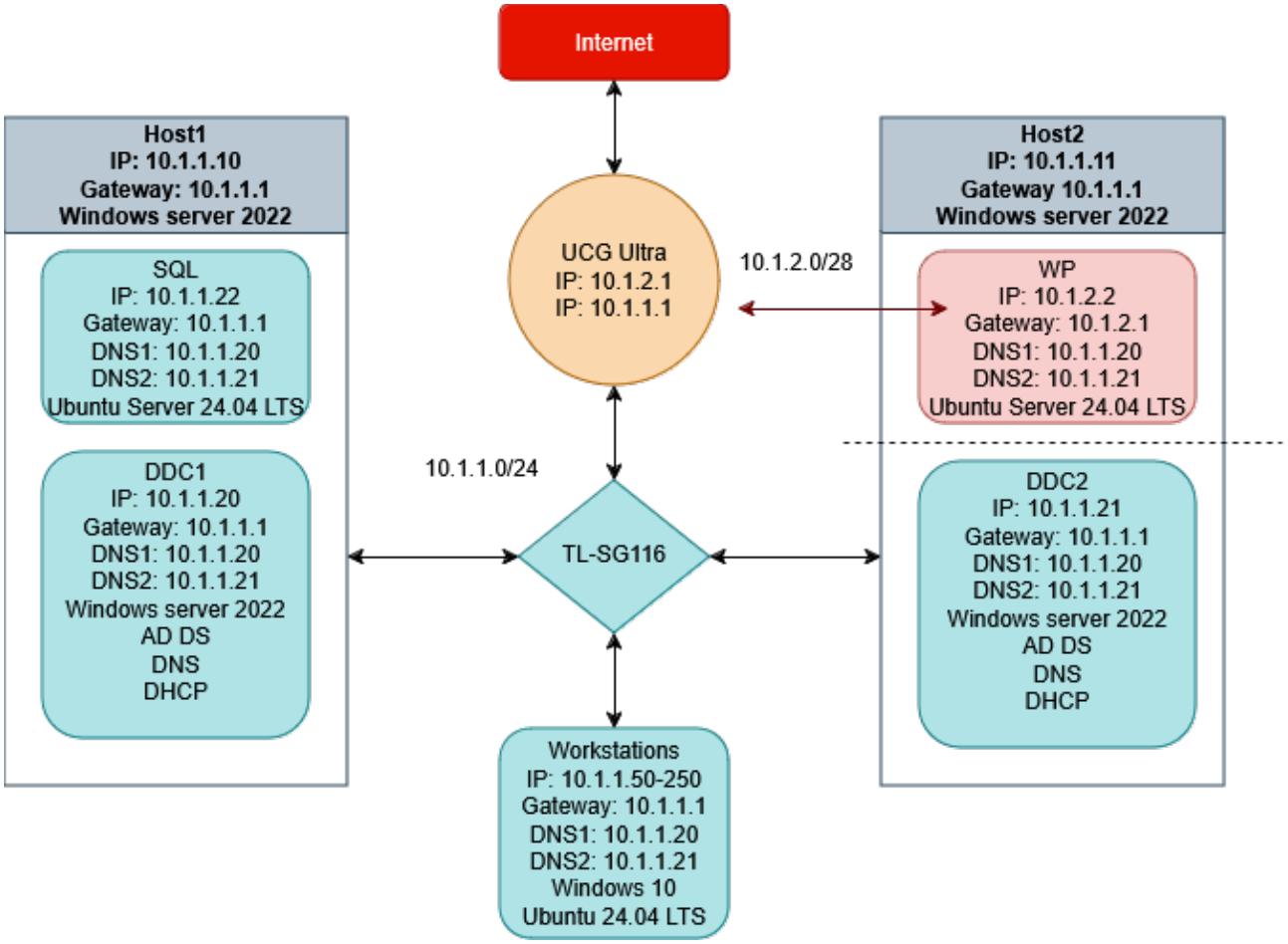
Technical Documentation



Network:

Gateway: Ubiquiti Unifi Cloud Gateway Ultra

WAN: ISP DHCP

Port 1: 10.1.1.1

Port 2: 10.1.2.1

Switch: TP-Link TL-SG116

Firewall rules: (Both means UDP and TCP)

Forward traffic from WAN to 10.1.2.2 on port 80 and 443.

10.1.1.0:

Inbound:

Allow Both/53 to any from 10.1.2.0 - DNS
Allow Both/88 to any from 10.1.2.0 - Kerberos
Allow Both/135 to any from 10.1.2.0 - RPC Handler
Allow Both/389 to any from 10.1.2.0 - LDAP
Allow TCP/445 to any from 10.1.2.0 - SMB
Allow TCP/3306 to any from 10.1.2.0 - SQL
Deny all

Outbound:

None

10.1.2.0:

Inbound:

Allow TCP/22 to any from 10.1.1.0 - SSH
Allow TCP/80 to any from any - HTTP
Allow TCP/443 to any from any - HTTPS
Allow Both/49152-65535 to any from 10.1.1.0 - RPC
Deny all

Outbound:

None

DNS:

Scavenge stale resource records:

No-refresh interval: 4 days
Refresh Interval: 4 days

Forward Lookup Zones:

Zone name: dd.com

Records:

- ddc1.dd.com A 10.1.1.20
- ddc2.dd.com A 10.1.1.21
- sql.dd.com A 10.1.1.22
- wp.dd.com A 10.1.2.2

SOA:

Expires after: 7 days

Reverse Lookup Zones:

Zone name: 1.1.10.in-addr.arpa

Records:

- 10.1.1.20 PTR ddc1.dd.com
- 10.1.1.21 PTR ddc2.dd.com
- 10.1.1.22 PTR sql.dd.com

Zone name: 2.1.10.in-addr.arpa

Records:

- 10.1.2.2 PTR wp.dd.com

DHCP:

IPv4:

Properties→Advanced:

Conflict detection attempts: 1

Scope:

Name: DDHCP
Range: 10.1.1.50-250
Subnet mask: 255.255.255.0
Lease duration: 8 days
Default Gateway: 10.1.1.1

DNS Servers:
10.1.1.20
10.1.1.21

Failover:
Name: ddc1.dd.com-ddc2.dd.com
Maxiumum Client Lead Time: 1h
Mode: Hot standby
Role of partner server:
DDC1: Active, 10% Address reservation
DDC2: Standby, 10% Address reservation
State switchover Interval: 30m
Enable Message Authentication: True
Shared Secret: *See passwords.md*

Physical servers:

Server 1:

Hostname: Host1
Operating System: Windows Server 2022 Standard Edition 21H2
Specs:

- CPU: Intel Xeon W-1350, 6c/12t 5Ghz
- RAM: 2x16 GB DDR4 ECC RAM 3200 Mhz
- HDD: 2x512GB NVME SSD (Raid 1)

Location: Server Room
Network:
IP: 10.1.1.10
Subnet mask: 255.255.255.0
Default Gateway: 10.1.1.1
DNS: 1.1.1.1, 8.8.8.8
Hyper-V settings:
Virtual Switches:
DD-SW:
External:
Intel 82579LM Gigabit Ethernet

Server 2:

Hostname: Host2
Operating System: Windows Server 2022 Standard Edition 21H2
Specs:

- CPU: Intel Xeon E-2144G, 4c/8t 4,5Ghz
- RAM: 2x16 GB DDR4 ECC RAM 2666 Mhz
- HDD: 2x256 GB SATA SSD (Raid 1)
- NIC2: TP-Link TX201

Location: Server Room

Network:

IP: 10.1.1.11

Subnet mask: 255.255.255.0

Default Gateway: 10.1.1.1

DNS: 1.1.1.1, 8.8.8.8

Hyper-V settings:

Virtual Switches:

DD-SW:

External:

Intel 82579LM Gigabit Ethernet

DDMZ-SW:

External:

TP-TX201

Allow management operating system to share this network adapter: False

Virtual servers:

Domain Controller 1:

Hostname: DDC1

Operating System: Windows Server 2022 Standard Edition 21H2

Specs:

- 4 vCPU
- 4 GB RAM
- 60 GB Storage

Location: Host1 (VM)

Network:

IP: 10.1.1.20

Subnet mask: 255.255.255.0

Default Gateway: 10.1.1.1

DNS: 10.1.1.20, 10.1.1.21

Roles/Features:

- Active Directory Domain Services
- DNS Server
- DHCP Server

Remote Desktop: Enabled

Database:

Hostname: SQL
Operating System: Ubuntu Server 24.04 LTS
Specs:

- 4 vCPU
- 8 GB RAM (fixed)
- 80 GB Storage

Location: Host1 (VM)
Network:

IP: 10.1.1.22
Subnet mask: 255.255.255.0
Default Gateway: 10.1.1.1
DNS: 10.1.1.20, 10.1.1.21

Packages: (main packages installs dependencies)

- realmd
- krb5-user
- adsys
- openssh-server
- mariadb-server

Domain Controller 2:

Hostname: DDC2
Operating System: Windows Server 2022 Standard Edition 21H2
Specs:

- CPU: 4 vCPU
- RAM: 4 GB
- HDD: 60 GB

Location: Host2 (VM)
Network:

IP: 10.1.1.21
Subnet mask: 255.255.255.0
Default Gateway: 10.1.1.1
DNS: 10.1.1.20, 10.1.1.21

Roles/Features:

- Active Directory Domain Services
- DNS Server

Remote Desktop: Enabled

WordPress:

Hostname: WP

Operating System: Ubuntu Server 24.04 LTS

Specs:

- 4 vCPU
- 8 GB RAM
- 120 GB Storage

Location: Host2 (VM)

Network:

IP: 10.1.2.2

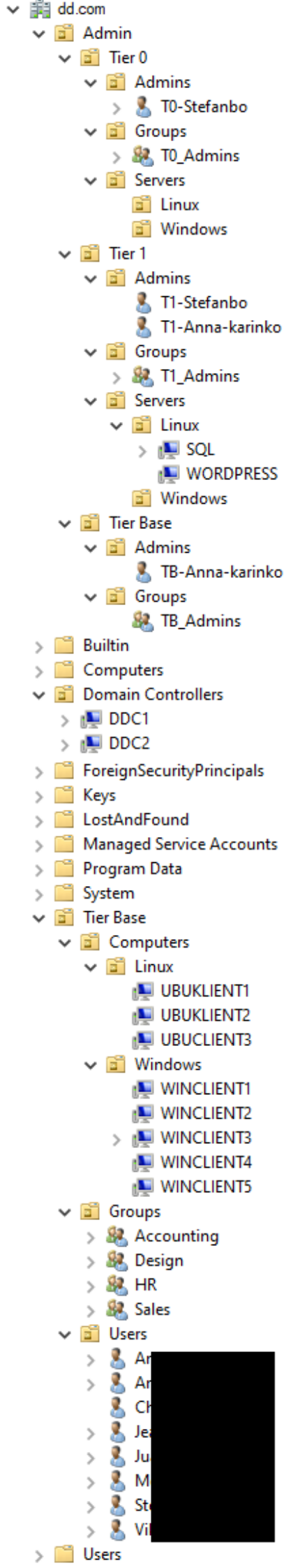
Subnet mask: 255.255.255.240

Default gateway: 10.1.2.1

DNS: 10.1.1.20, 10.1.1.21

Packages: (main packages installs dependencies)

- realmd
- krb5-user
- adsys
- openssh-server
- apache2
- libapache2-mod-php
- php-mysql, php-mbstring, php-ldap, php-gd, php-curl, php-imagick, php-xml, php-zip, php-intl



OU Structure:

OU Delegations:

OU: dd.com/Tier Base

Users and groups: TB_Admins

Tasks to Delegate:

- Create, delete and manage user accounts
- Reset user passwords and force password change at next logon
- Read all user information
- Create, delete and manage groups

OU: dd.com/Tier 0/Servers/Linux:

Block Inheritance: True

OU: dd.com/Tier 1/Servers/Linux:

Block Inheritance: True

Users:

Administrator:

OU: dd.com/Users

Properties→Account:

- Account is sensitive and cannot be delegated

T0-Stefanbo:

OU: dd.com/Admin/Tier 0/Admins

Group Memberships:

- T0_Admins

Properties→Account:

- Account is sensitive and cannot be delegated

T1-Stefanbo:

OU: dd.com/Admin/Tier 1/Admins

Group Memberships:

- T1_Admins

Properties→Account:

- Account is sensitive and cannot be delegated

T1-Anna-karinko:

OU: dd.com/Admin/Tier 1/Admins

Group Memberships:

- T1_Admins

Properties→Account:

- Account is sensitive and cannot be delegated

TB-Anna-karinko:

OU: dd.com/Admin/Tier Base/Admins

Group Memberships:

- TB_Admins

Properties→Account:

- Account is sensitive and cannot be delegated

WP-Read:

OU: dd.com/Managed Service Accounts

Groups:

Global Groups:

T0_Admins	- Manage AD, domain controllers and T0 servers.
T1_Admins	- Manage T1 servers.
TB_Admins	- Manage users and workstations.
Accounting	- Manage financial records.
Design	- Designing sites.
Sales	- Promotion and sales.
HR	- Manage employees.

GPOs:

Ubuntu ADMX-files: https://github.com/ubuntu/adsys/tree/main/policies/Ubuntu/all

T0 Linux Access Rights:

OU: dd.com/Admin/Tier 0/Servers/Linux

Computer Settings:

Windows Settings/Security Settings/Local Policies/User Rights/Allow log on locally:

BUILTIN/Administrators

DD/Domain Admins

Windows Settings/Security Settings/Local Policies/User Rights/Allow log on terminal serv.:

BUILTIN/Administrators

DD/Domain Admins

Administrative Templates/Ubuntu/Client Management/Privilege Authorization:

Allow local administrators: Disabled

Client administrators: %Domain Admins@dd.com

Administrative Templates/Ubuntu/Client Management/Computer Scripts:

Startup Scripts: Enabled

t0-polkit-1.sh

T0 Restricted Groups:

OU: dd.com/Admin/Tier 0/Servers/Windows

Computer Settings:

Windows Settings/Security Settings/Restricted Groups:

BUILTIN/Administrators

Members:

DD/Domain Admins

T1 Linux Access Rights:

OU: dd.com/Admin/Tier 1/Servers/Linux

Computer Settings:

Windows Settings/Security Settings/Local Policies/User Rights/Allow log on locally:

BUILTIN/Administrators

DD/T1_Admins

Windows Settings/Security Settings/Local Policies/User Rights/Allow log on terminal serv.:

BUILTIN/Administrators

DD/T1_Admins

Administrative Templates/Ubuntu/Client Management/Privilege Authorization:

Allow local administrators: Disabled

Client administrators: %T1_Admins@dd.com

Administrative Templates/Ubuntu/Client Management/Computer Scripts:

Startup Scripts: Enabled

t1-polkit-1.sh

T1 Restricted Groups:

OU: dd.com/Admin/Tier 1/Servers/Windows

Computer Settings:

Windows Settings/Security Settings/Restricted Groups:

BUILTIN/Administrators

Members:

DD/T1_Admins

TB Linux Access Rights:

OU: dd.com/Tier Base/Computers/Linux

Computer Settings:

Administrative Templates/Ubuntu/Client Management/Privilege Authorization:

Allow local administrators: Disabled

Client administrators: %TB_Admins@dd.com

Administrative Templates/Ubuntu/Client Management/Computer Scripts:

Startup Scripts: Enabled

tb-polkit-1.sh

TB Computers Access Rights:

OU: dd.com/Tier Base/Computers

Computer Settings:

Windows Settings/Security Settings/Local Policies/User Rights/Deny log on locally

DD/T0_Admins

DD/T1_Admins

DD/Domain Admins

DD/Enterprise Admins

Windows Settings/Security Settings/Local Policies/User Rights/Deny log on terminal serv.

DD/T0_Admins

DD/T1_Admins

DD/Domain Admins

DD/Enterprise Admins

Windows Settings/Security Settings/Local Policies/User Rights/Deny log on locally

DD/T0_Admins

DD/T1_Admins

DD/Domain Admins

DD/Enterprise Admins

Windows Settings/Security Settings/Local Policies/User Rights/Deny log on as a service

DD/T0_Admins

DD/T1_Admins

DD/Domain Admins

DD/Enterprise Admins

TB Restricted Groups:

OU: dd.com/Admin/Tier Base/Computers/Windows

Computer Settings:

Windows Settings/Security Settings/Restricted Groups:

BUILTIN/Administrators

Members:

DD/TB_Admins

Default Domain Policy:

OU: dd.com

Computer Settings:

Policies/Windows Settings/Security Settings/Account Policies/Password Policy:

Enforce password history: Not Defined

Maximum password age: Not Defined

Minimum password age: Not Defined

Minimum password length: Not Defined

Password must meet complexity requirements: Not Defined

Store password using reversible encryption: Not Defined

Beyond these handmade GPOs Windows Server 2022 Security Baselines are also installed.
https://www.microsoft.com/en-us/download/details.aspx?id=55319

They are linked according to:
MSFT Windows Server 2022 – Domain Security
    OU: dd.com

MSFT Windows Server 2022 – Defender Antivirus
    OU: dd.com

MSFT Windows Server 2022 – Member Server
    OU: dd.com/Tier 0/Servers/Windows
    OU: dd.com/Tier 1/Servers/Windows

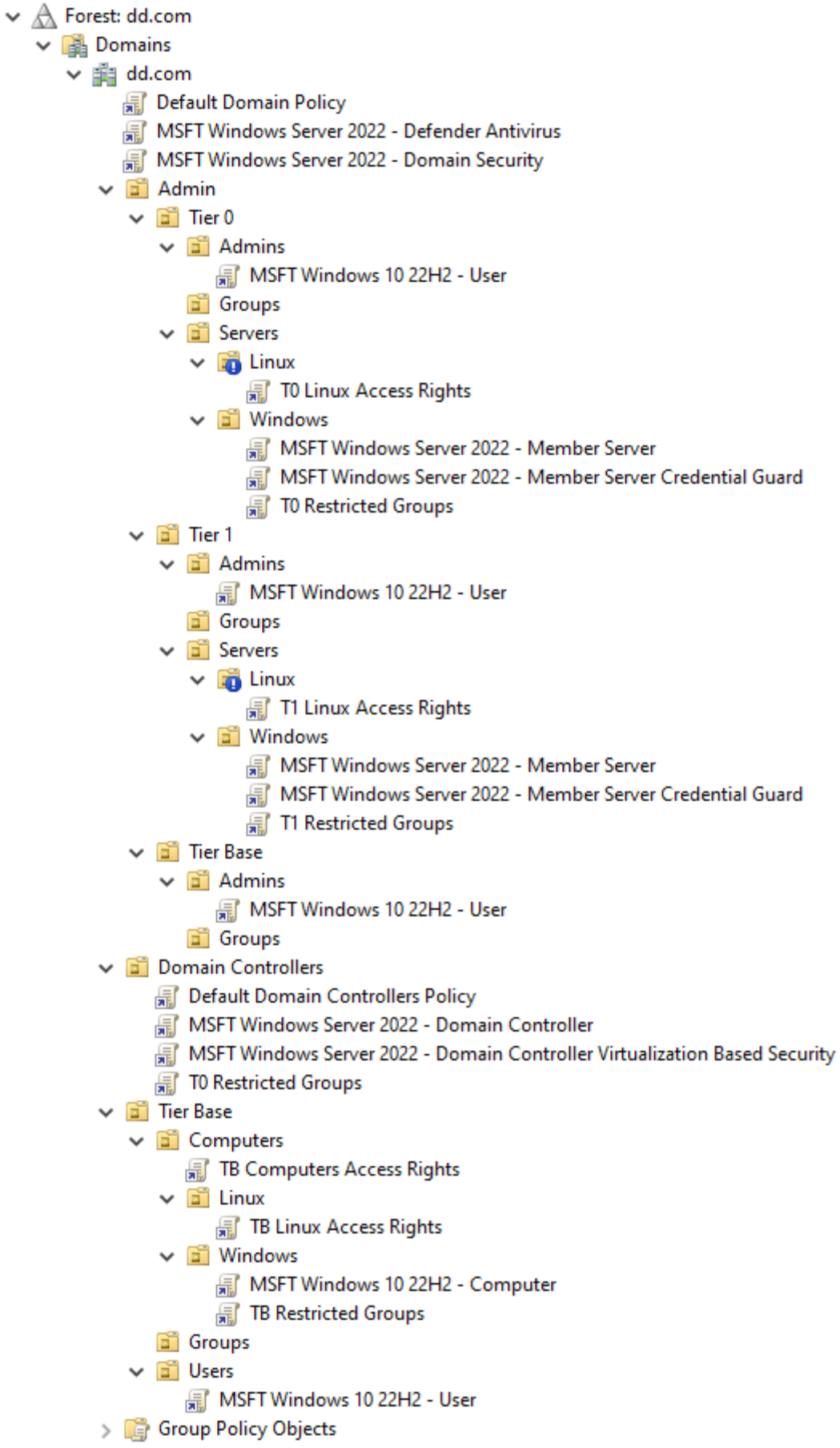
MSFT Windows Server 2022 – Member Server Credential Guard
    OU: dd.com/Tier 0/Servers/Windows
    OU: dd.com/Tier 1/Servers/Windows

MSFT Windows Server 2022 – Domain Controller
    OU: dd.com/Domain Controllers

MSFT Windows Server 2022 – Domain Controller Virtualization Based Security
    OU: dd.com/Domain Controllers

MSFT Windows 10 22H2 – Computer
    OU: dd.com/Tier Base/Computers/Windows

MSFT Windows 10 22H2 – User
    OU: dd.com/Admin/Tier 0/Admins
    OU: dd.com/Admin/Tier 1/Admins
    OU: dd.com/Admin/Tier Base/Admins
    OU: dd.com/Tier Base/Users


Forest: dd.com
Domains
dd.com
Default Domain Policy
MSFT Windows Server 2022 - Defender Antivirus
MSFT Windows Server 2022 - Domain Security
Admin
Tier 0
Admins
MSFT Windows 10 22H2 - User
Groups
Servers
Linux
T0 Linux Access Rights
Windows
MSFT Windows Server 2022 - Member Server
MSFT Windows Server 2022 - Member Server Credential Guard
T0 Restricted Groups
Tier 1
Admins
MSFT Windows 10 22H2 - User
Groups
Servers
Linux
T1 Linux Access Rights
Windows
MSFT Windows Server 2022 - Member Server
MSFT Windows Server 2022 - Member Server Credential Guard
T1 Restricted Groups
Tier Base
Admins
MSFT Windows 10 22H2 - User
Groups
Domain Controllers
Default Domain Controllers Policy
MSFT Windows Server 2022 - Domain Controller
MSFT Windows Server 2022 - Domain Controller Virtualization Based Security
T0 Restricted Groups
Tier Base
Computers
TB Computers Access Rights
Linux
TB Linux Access Rights
Windows
MSFT Windows 10 22H2 - Computer
TB Restricted Groups
Groups
Users
MSFT Windows 10 22H2 - User
Group Policy Objects

PSO:

Admin Password Policy:

- Precedence: 1
- Enforce minimum password length: 16 characters
- Enforce maximum password age: 900 days
- Enforce account lockout policy:
  - Number of failed logon attempts allowed: 5
  - Reset failed logon attempts count after (mins): 30
  - Account will be locked out:
    - For a duration of (mins): 30
- Directly applies to:
  - Domain Admins
  - T0_Admins
  - T1_Admins
  - TB_Admins

Sysvol:

To deploy scripts through GPOs, a folder named Ubuntu need to be created inside the domains SYSVOL directory. Inside this folder, a scripts directory need to be created along with a GPT.ini file. The GPT.ini should contain:

- [General]
- Version=<int>
- displayName=UbuntuAssetsDirectory

Scripts intended for execution via GPOs are to be placed in the scripts folder. Each time a script is modified, the version number in the GPO.ini file must be incremented.

Scripts:

importUsers.ps1:

Imports users based on a predefined template format, which includes the following fields: **First Name, Surname, Department, Phone, City** and **Mail**.

For each unique department listed in the import file, a corresponding group is created within the **Groups OU** under **Tier Base**, and the relevant users are added to these groups. If a user belongs to multiple departments (separated by a whitespace) in the CSV file, they will be added to all the applicable groups.

Users sAMAccountName is calculated by their first name and first two letters in their surname. The UPN becomes the sAMAccountName@dd.com. If a mail column is not present the mail attribute will be created by the username@domain.

Each user is assigned a unique, randomized 14-character password, which must be changed on their first login. The user information, along with their generated password, is saved back to a new CSV file named userpass.csv for easy distribution.

linuxJoin.sh:

This script joins a computer to a domain using realmd. It accepts two key parameters:

-domain Specifies domain name.

-server Installs OpenSSH server for management.

Alongside domain integration, the script also configures the system timezone to GMT+1 and ensures the NTP server matches the one used by Windows. To enable features like GPO integration, the script prompts for an Ubuntu Pro key.

t%-polkit-1.sh:

Create a Polkit rule on Linux clients that enables GNOME to authenticate administrative actions using an AD admin account specific to the clients tier.

Apache2:

HTTPS enabled with a self-signed certificate.
Redirection from HTTP to HTTPS enabled.

wordpress.conf

```
<VirtualHost _default_:443>
    SSLEngine On
    SSLCertificateFile /etc/apache2/certs/wp-cert.pem
    SSLCertificateKeyFile /etc/apache2/certs/wp-key.pem
    DocumentRoot /var/www/wordpress
    <Directory /var/www/wordpress>
        Options FollowSymLinks
        AllowOverride Limit Options FileInfo
        DirectoryIndex index.php
        Require all granted
    </Directory>
    <Directory /var/www/wordpress/wp-content>
        Options FollowSymLinks
        Require all granted
    </Directory>
</VirtualHost>

<VirtualHost *:80>
        Redirect 301 / https://wordpress.dd.com
</VirtualHost>
```

WordPress:

Settings:

Permalinks:

Permalink structure: Post name

Next Active Directory Integration:

Configuration:

Environment:

Domain controllers:

- DDC1.dd.com
- DDC2.dd.com

Use encryption: STARTTLS

Base DN: dc=doman,dc=nu

Username: WP-Read@dd.com

Password: *See passwords.md*

User:

Account Suffix: @dd.com

Prevent email change: True

Display name: CN

Permissions:

Authorize by group memberships: True

Authorization groups:

- T1_Admins
- Design
- Sales

Role equivalent groups:

- T1_Admins → administrator
- Design → editor
- Sales → author

References:

Integrating RHEL systems directly with Windows Active Directory

System-Level Authentication Guide

ADSys Documentation

Active Directory Tiering

Domain Join Ubuntu 22.04 to Active Directory

Install and configure WordPress

WP-CLI

polkit

Next Active Directory Integration