

MCSA Full Project Report

1. Introduction

1.1 Project Overview

This project demonstrates the design, implementation, and management of a Microsoft Active Directory infrastructure based on MCSA concepts. It includes multiple Domain Controllers, RODC, DNS, DHCP, WSUS, Group Policy Objects (GPOs), security restrictions, delegation, and user access control.

1.2 Project Objectives

- Deploy a multi-domain-controller Active Directory environment
 - Apply security policies using GPOs
 - Configure RODC and password replication policies
 - Implement DNS, DHCP, and WSUS services
 - Control user access and permissions based on roles
 - Apply delegation without granting full administrative privileges
-

2. Network Topology

2.1 Logical Topology Description

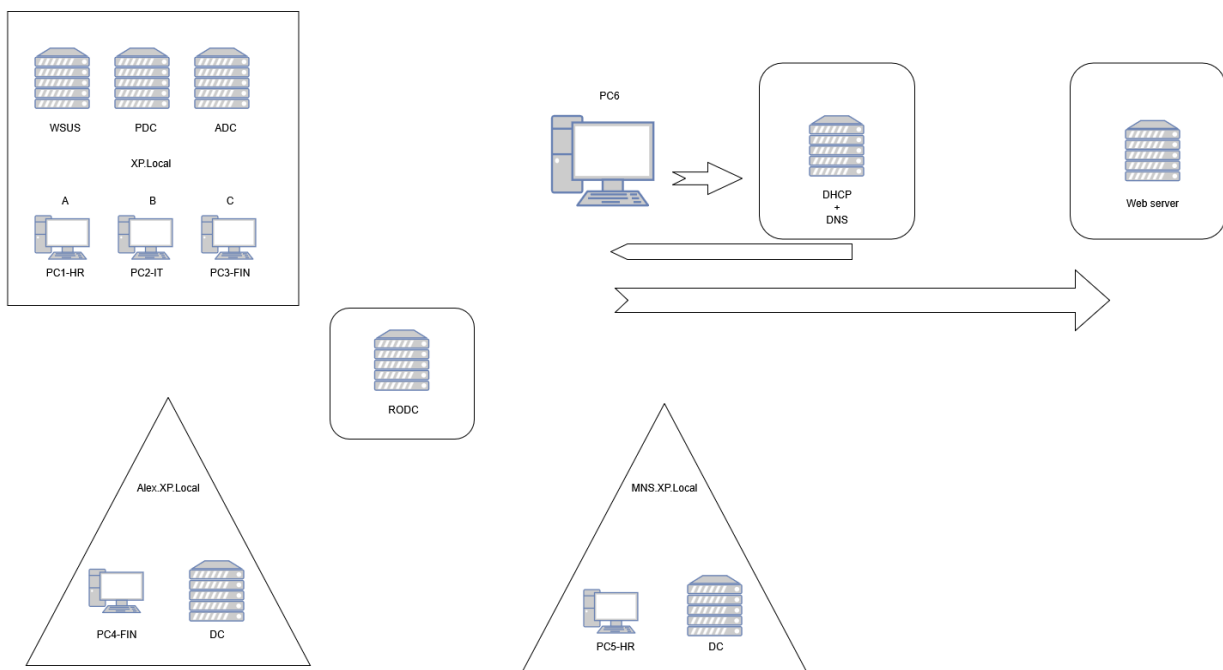
The environment consists of a primary domain controller, additional domain controllers, a Read-Only Domain Controller (RODC), child domains, client machines, and services such as WSUS, DNS, DHCP, and Web Servers.

2.2 Domain Structure

- **Root Domain:** xp.local
- **Child Domain:** alex.xp.local
- **Child Domain:** mns.xp.local

2.3 Domain Controllers

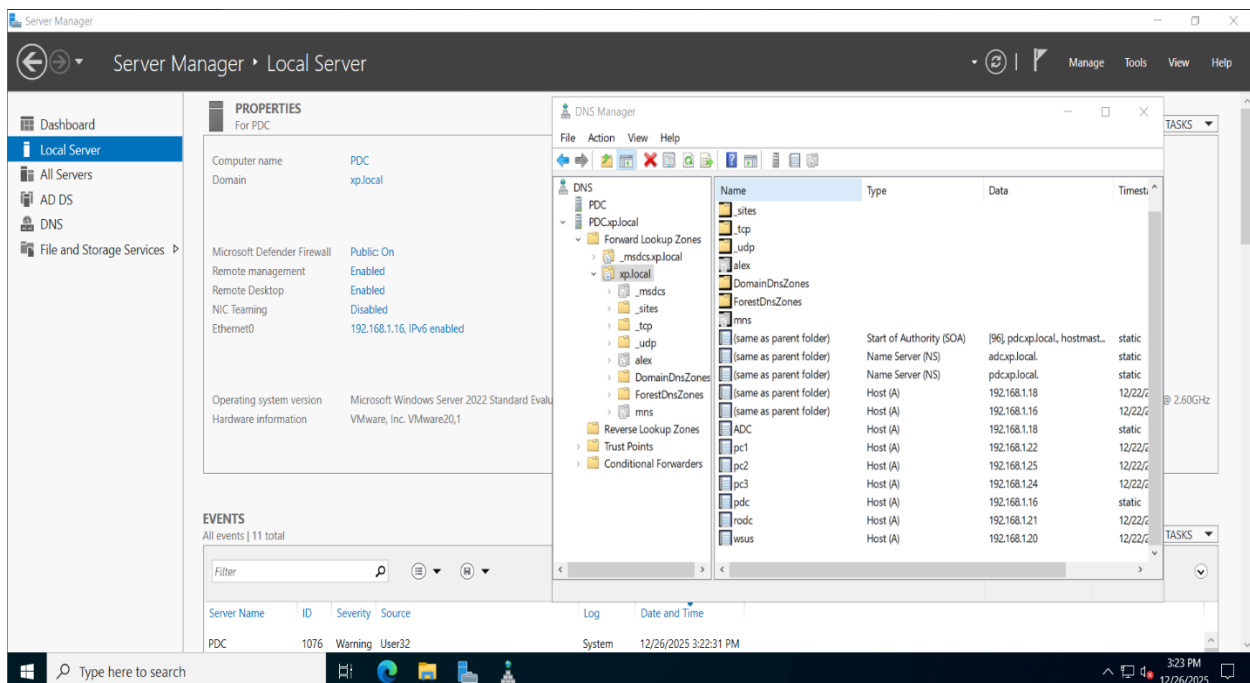
- DC1: Primary Domain Controller (PDC + DNS)
- DC2: Add additional Domain Controller
- DC3: Read-Only Domain Controller (RODC)
- DC4 & DC5: Child Domain Controllers



3. Server Roles and Configuration

3.1 DC1 – Primary Domain Controller

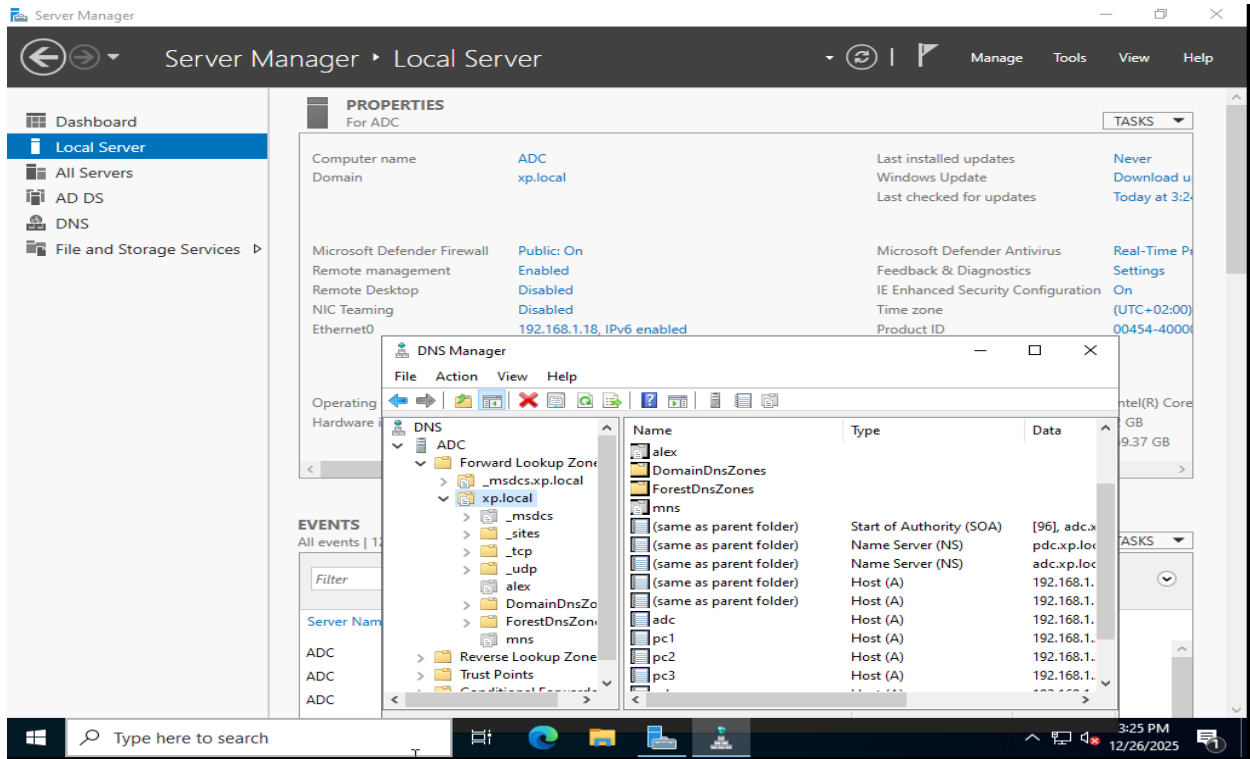
- Active Directory Domain Services
- DNS Server
- FSMO Roles



3.2 DC2 – Additional Domain Controller

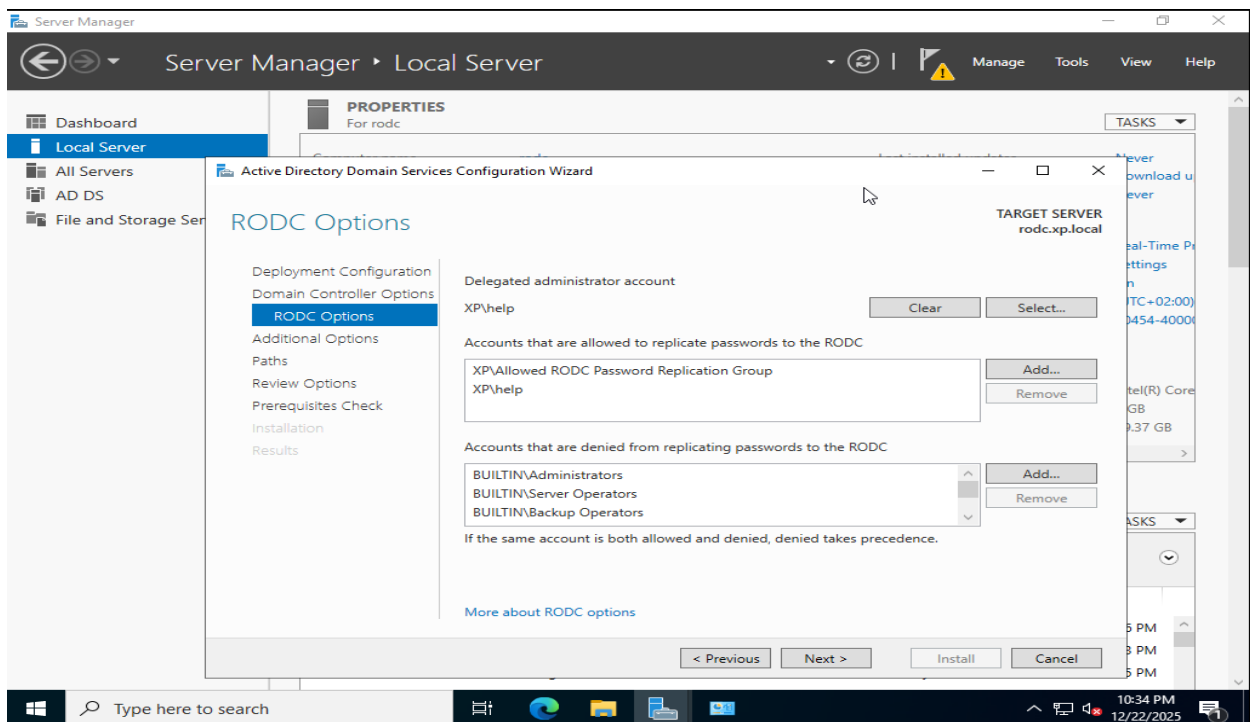
- AD DS Replication

- DNS Replication



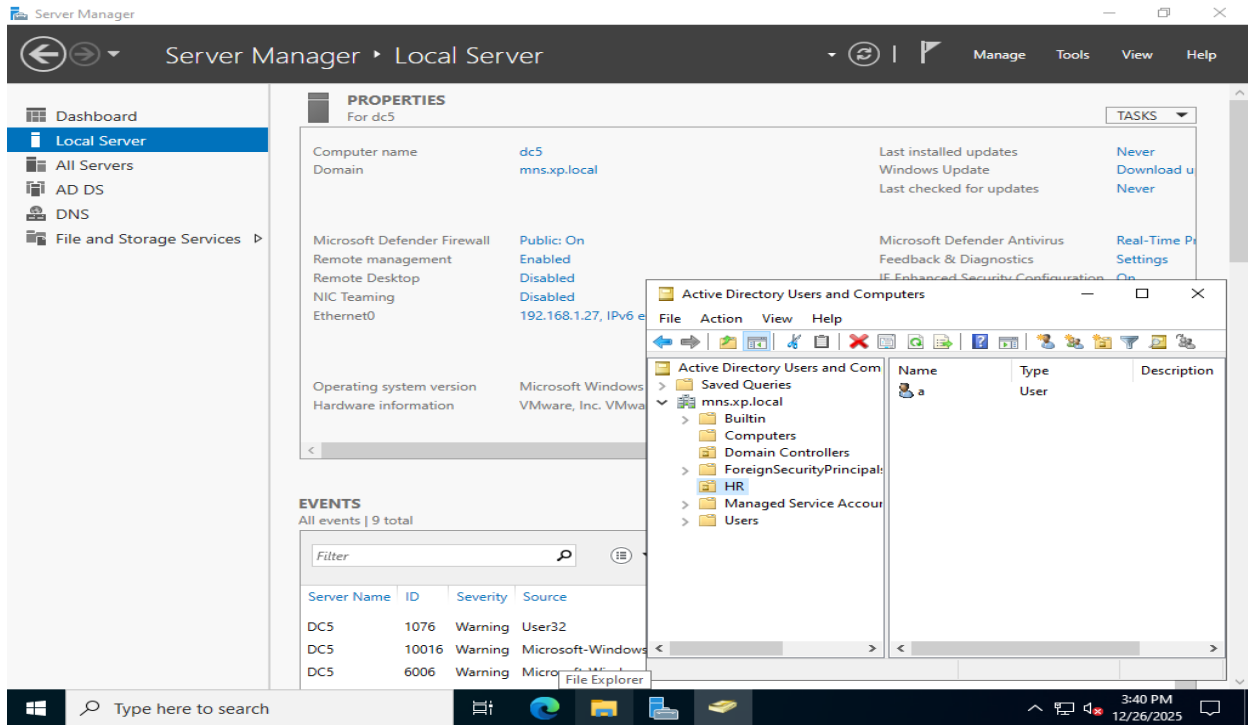
3.3 DC3 – RODC Configuration

- Read-Only Active Directory
- Password Replication Policy (PRP)



3.4 DC4 & DC5 – Child Domain Controllers

- Child domain setup
- Trust relationship with parent domain



The screenshot shows the Server Manager interface for a local server named 'dc5'. The left sidebar contains a navigation pane with 'Local Server' selected. The main area displays the 'PROPERTIES' for 'dc5', including computer name, domain, firewall settings, and operating system version. An 'EVENTS' pane at the bottom shows a list of events. A 'File Explorer' window is open, showing the 'Active Directory Users and Computers' console tree.

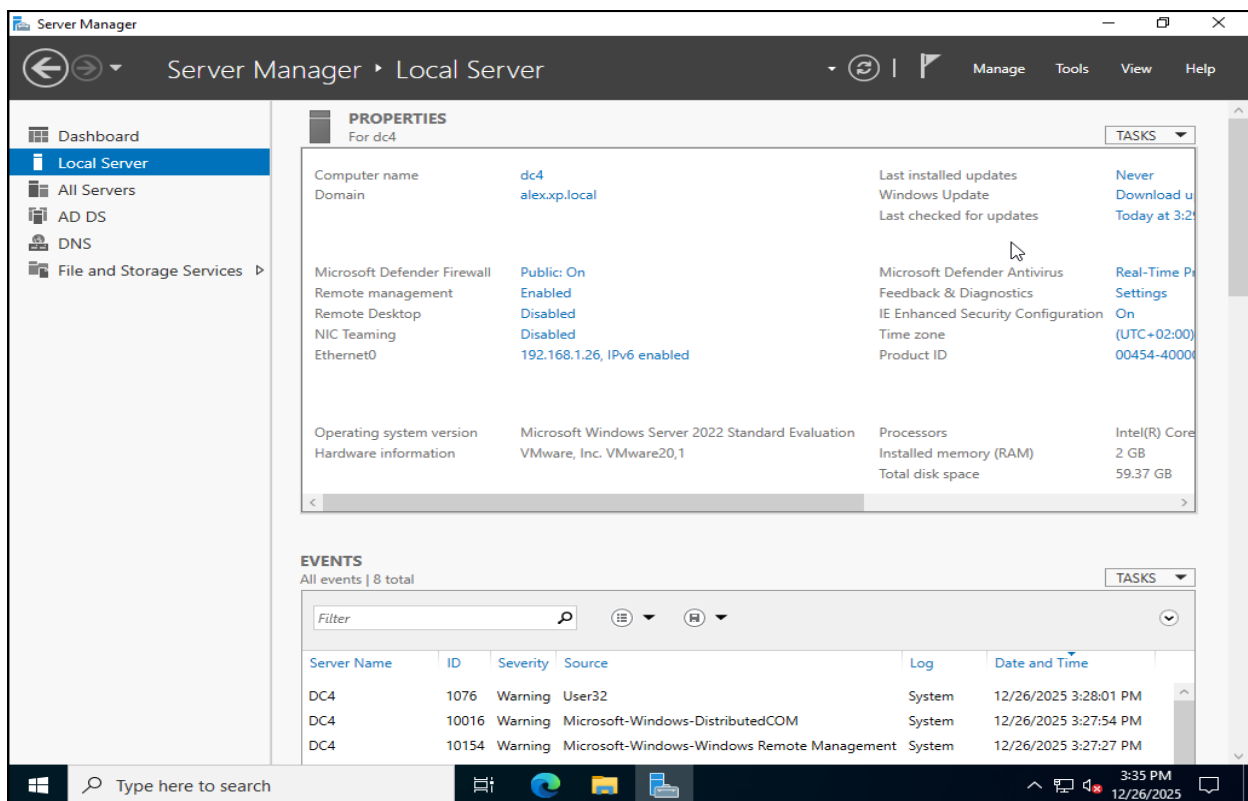
Server Manager - Local Server

PROPERTIES For dc5

Property	Value
Computer name	dc5
Domain	mns.xp.local
Microsoft Defender Firewall	Public: On
Remote management	Enabled
Remote Desktop	Disabled
NIC Teaming	Disabled
Ethernet0	192.168.1.27, IPv6 e
Operating system version	Microsoft Windows
Hardware information	VMware, Inc. VMwa

EVENTS
All events | 9 total

Server Name	ID	Severity	Source
DC5	1076	Warning	User32
DC5	10016	Warning	Microsoft-Windows
DC5	6006	Warning	Micro



The screenshot shows the Server Manager interface for a local server named 'dc4'. The left sidebar contains a navigation pane with 'Local Server' selected. The main area displays the 'PROPERTIES' for 'dc4', including computer name, domain, firewall settings, and operating system version. An 'EVENTS' pane at the bottom shows a list of events.

Server Manager - Local Server

PROPERTIES For dc4

Property	Value
Computer name	dc4
Domain	alex.xp.local
Microsoft Defender Firewall	Public: On
Remote management	Enabled
Remote Desktop	Disabled
NIC Teaming	Disabled
Ethernet0	192.168.1.26, IPv6 enabled
Operating system version	Microsoft Windows Server 2022 Standard Evaluation
Hardware information	VMware, Inc. VMware20,1

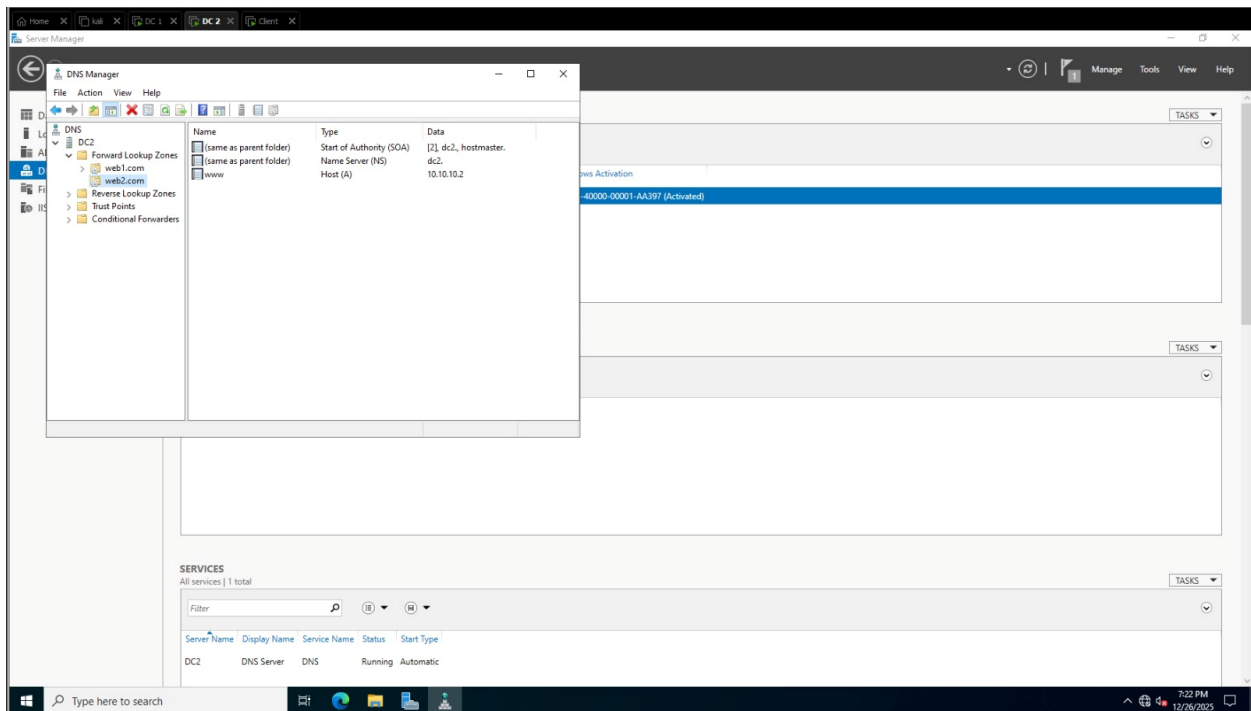
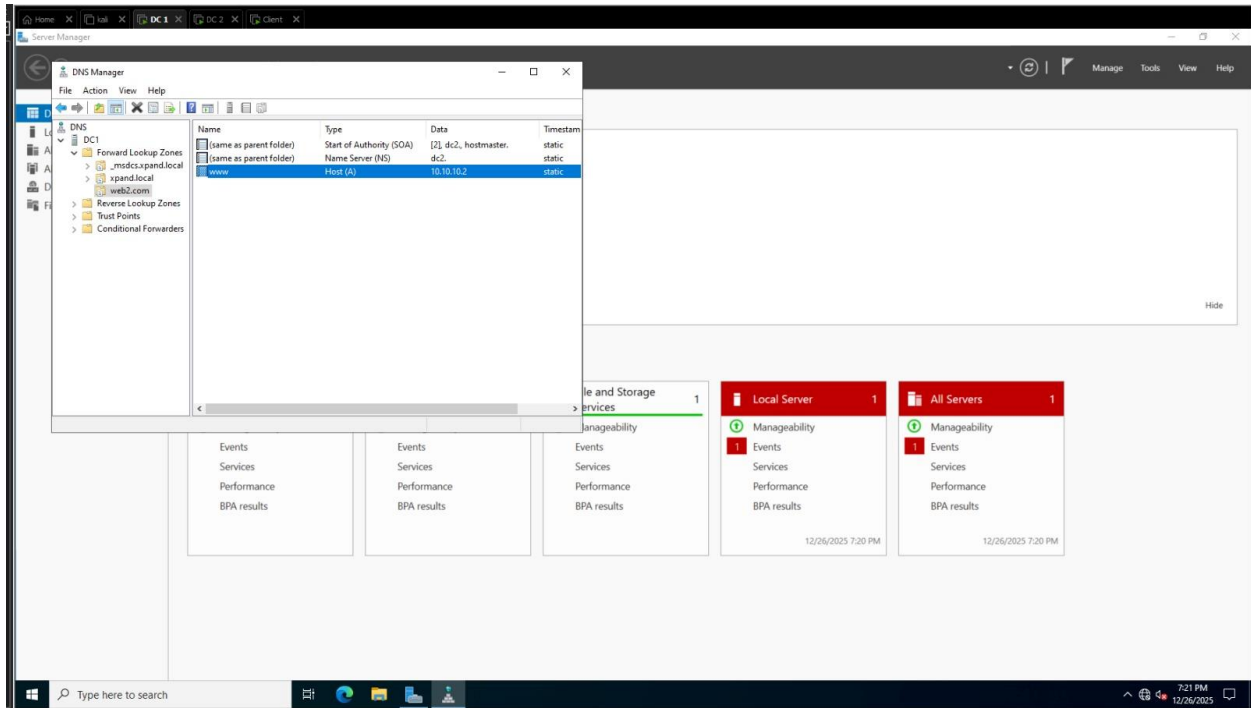
EVENTS
All events | 8 total

Server Name	ID	Severity	Source	Log	Date and Time
DC4	1076	Warning	User32	System	12/26/2025 3:28:01 PM
DC4	10016	Warning	Microsoft-Windows-DistributedCOM	System	12/26/2025 3:27:54 PM
DC4	10154	Warning	Microsoft-Windows-Windows Remote Management	System	12/26/2025 3:27:27 PM

4. DNS and DHCP Configuration

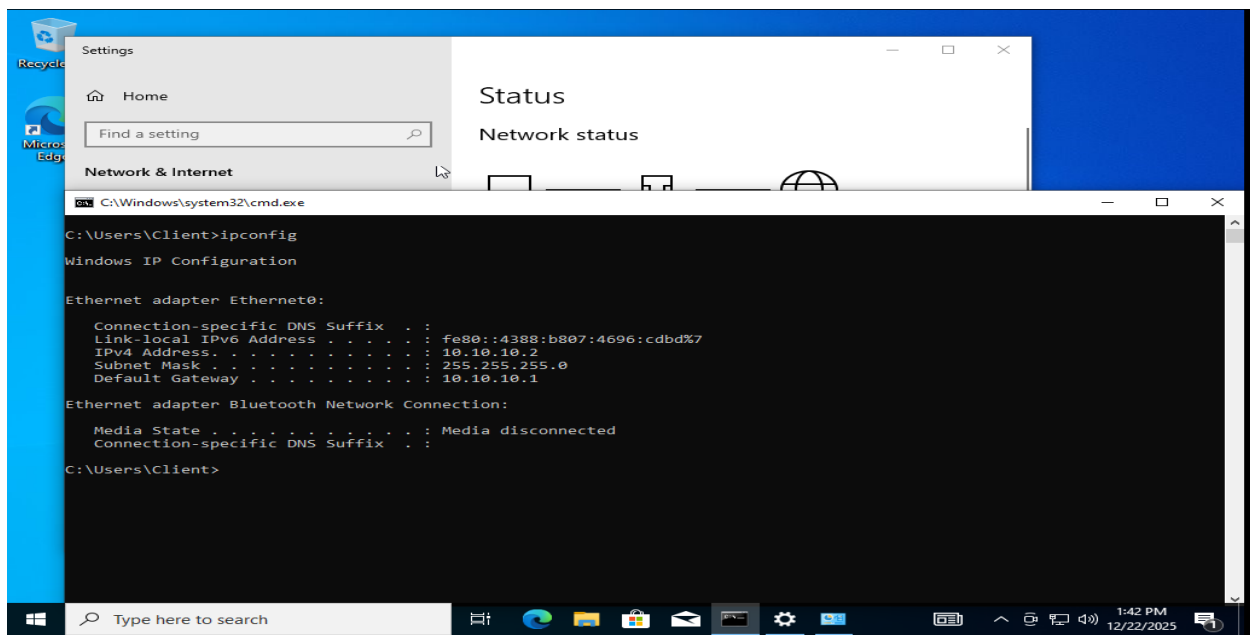
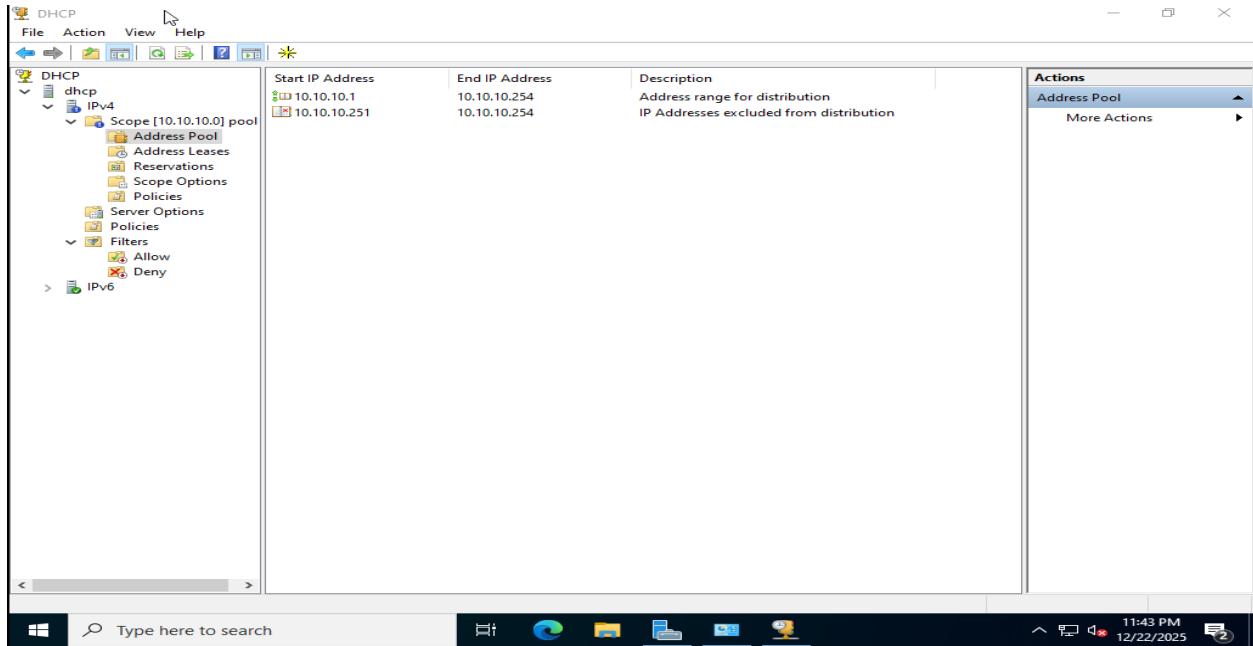
4.1 DNS Zones

- Primary Zone: web1.com
- Secondary Zone: web2.com



4.2 DHCP Configuration

- Scope creation
- IP address assignment to clients



5. User and Computer Accounts

5.1 User Accounts

- A@xp.local
- help@xp.local
- c@xp.local
- b@xp.local
- d (Local User)

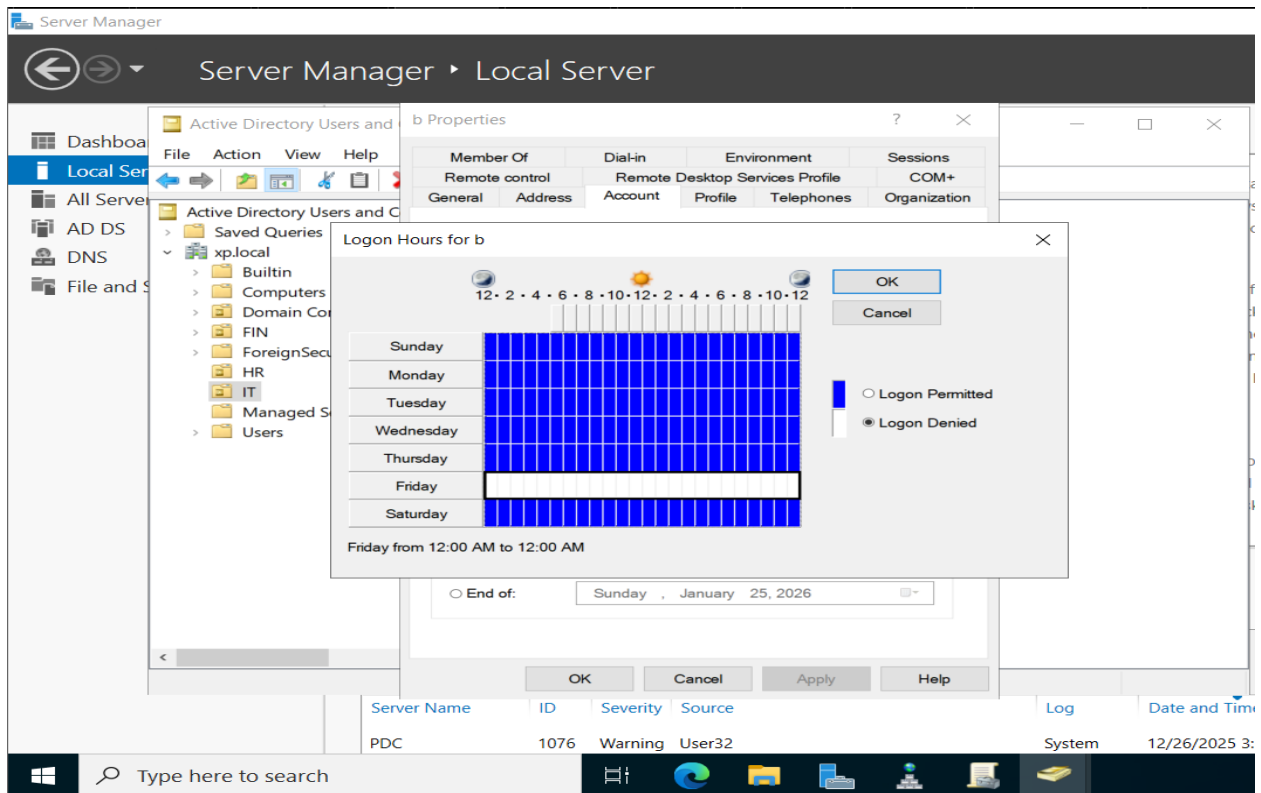
5.2 Computer Accounts

- PC1-HR
- PC2-IT
- PC3-FIN
- PC4-FIN
- PC5-HR
- PC6

6. Group Policy Objects (GPOs)

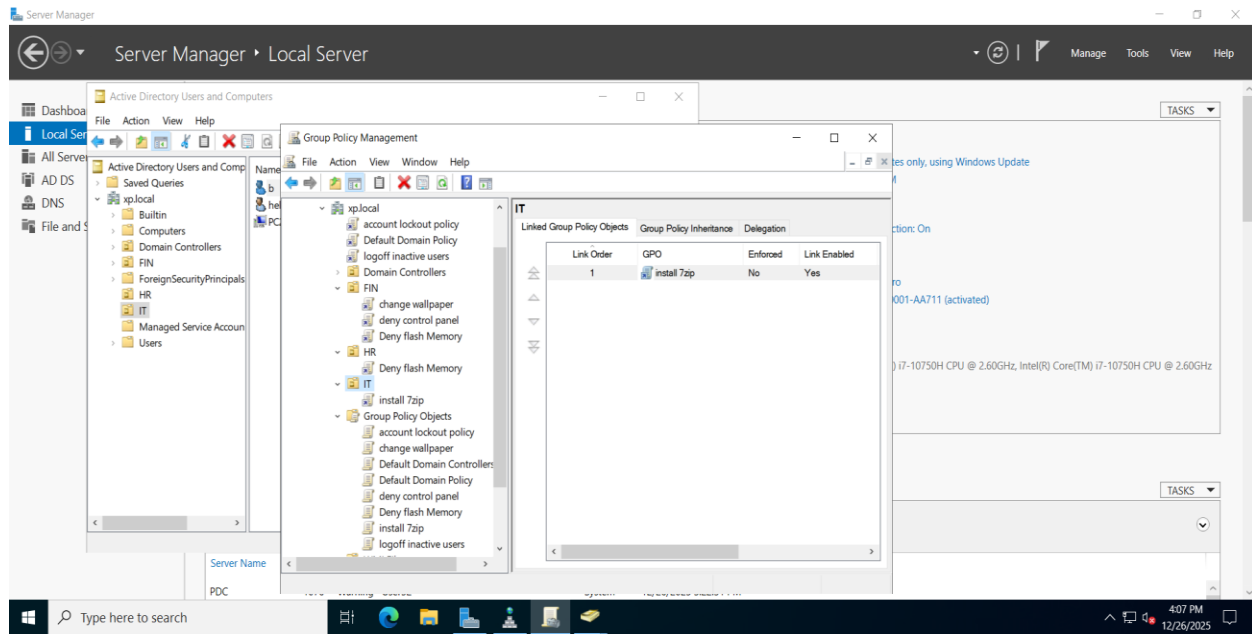
6.1 Login Restrictions

- A@xp.local allowed to log in only on PC1
- Login denied on Fridays



6.2 Desktop and Control Panel Restrictions

- Disable Control Panel access for c@xp.local
- Disable Flash memory access
- Apply XP logo as desktop wallpaper
- Install 7-zip on PC2 using GPO
- Account lockout
- Logoff inactive users



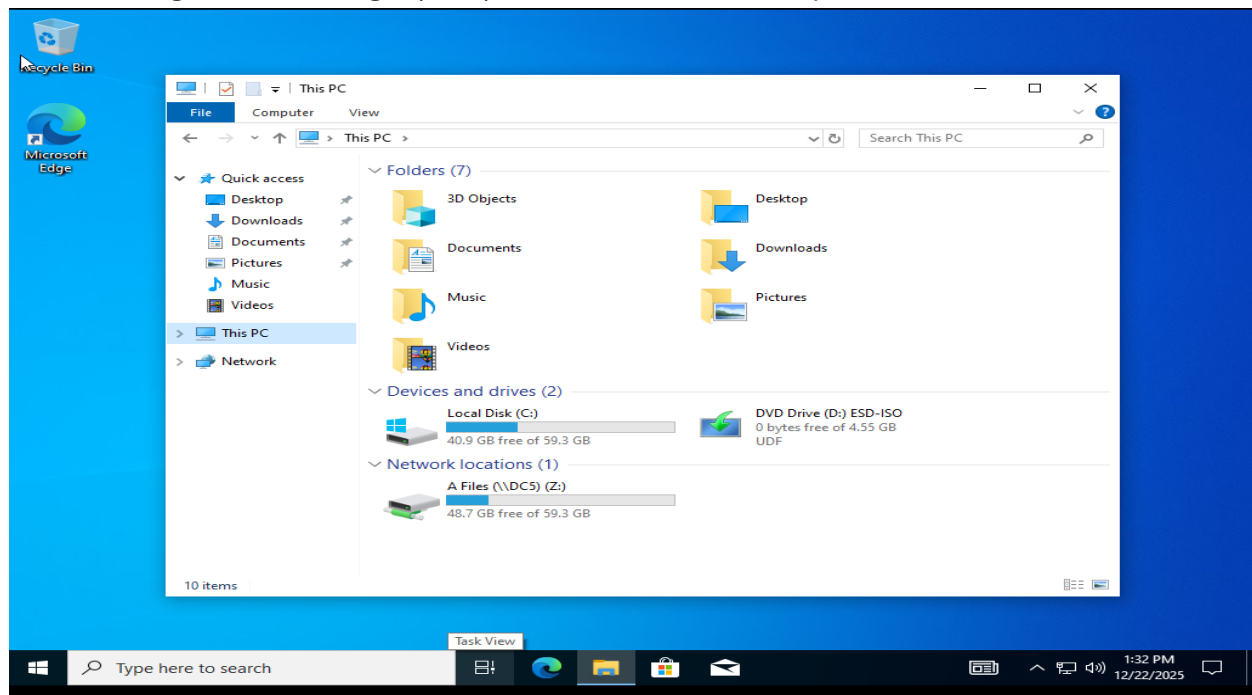
7. Roaming Profiles

- Configure roaming profile for A@Mns.XP.local
- Allow access to PC1, PC4, and PC5

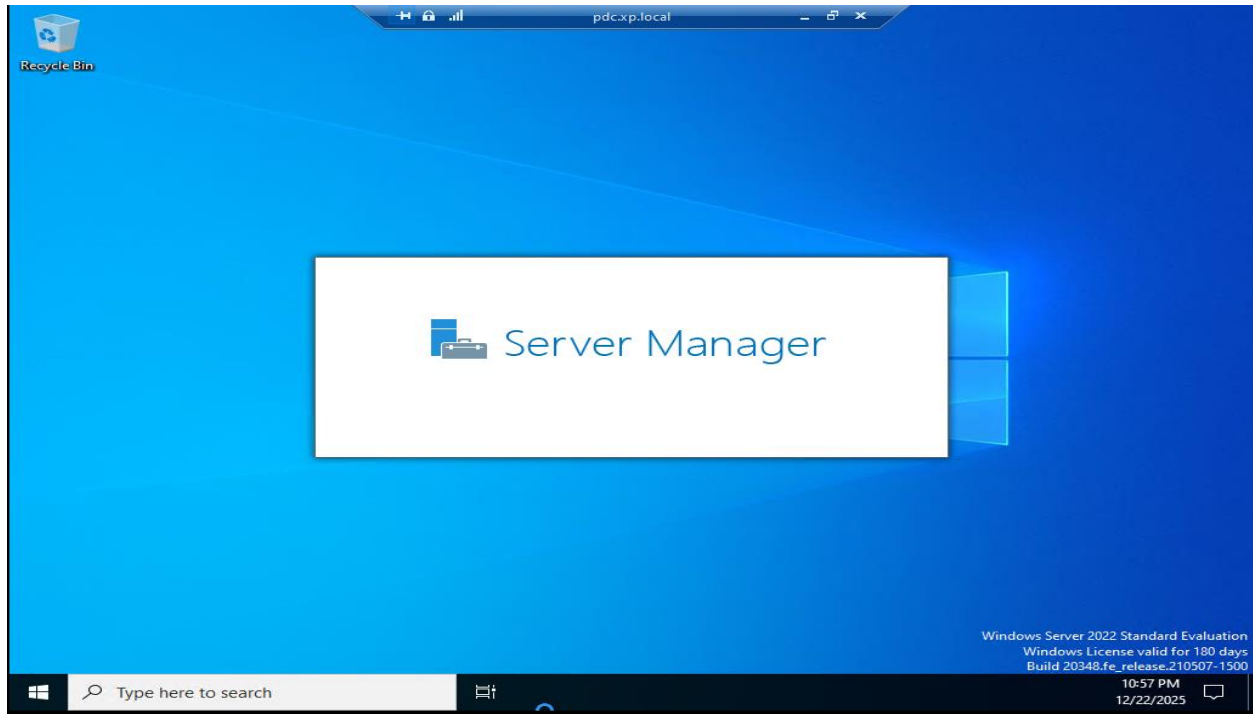
8. Delegation and Permissions

8.1 Administrative Delegation

- Delegate remote login (RDP) access to DC1 for b@xp.local

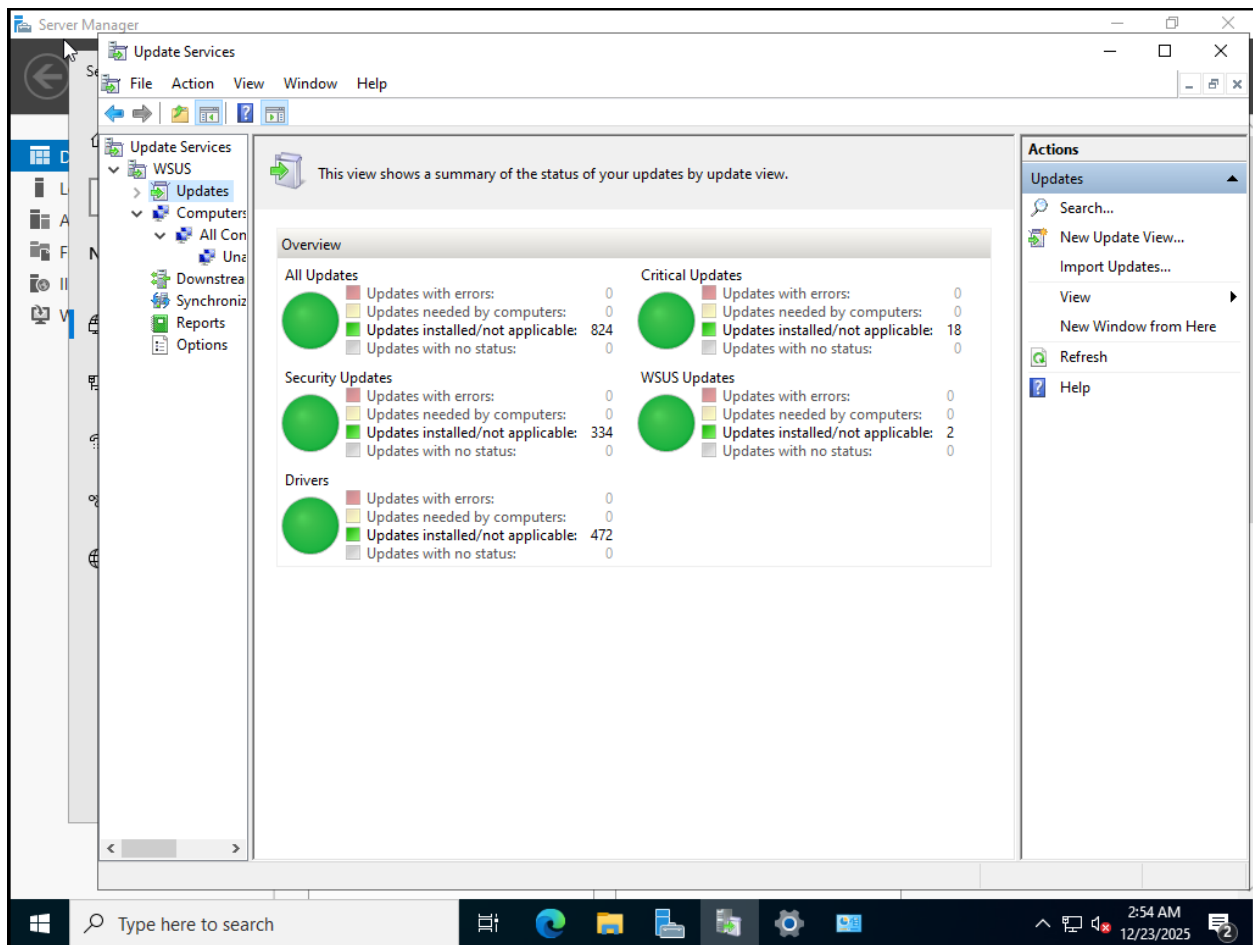


- User is NOT a member of Domain Admins



9. WSUS Configuration

- Install and configure WSUS on DC6
- Approved updates for clients
- Verify update status



10. Web Server Access and Verification

10.1 Website Access

- Verify access to:
 - <http://www.web1.com>
 - <http://www.web2.com>

