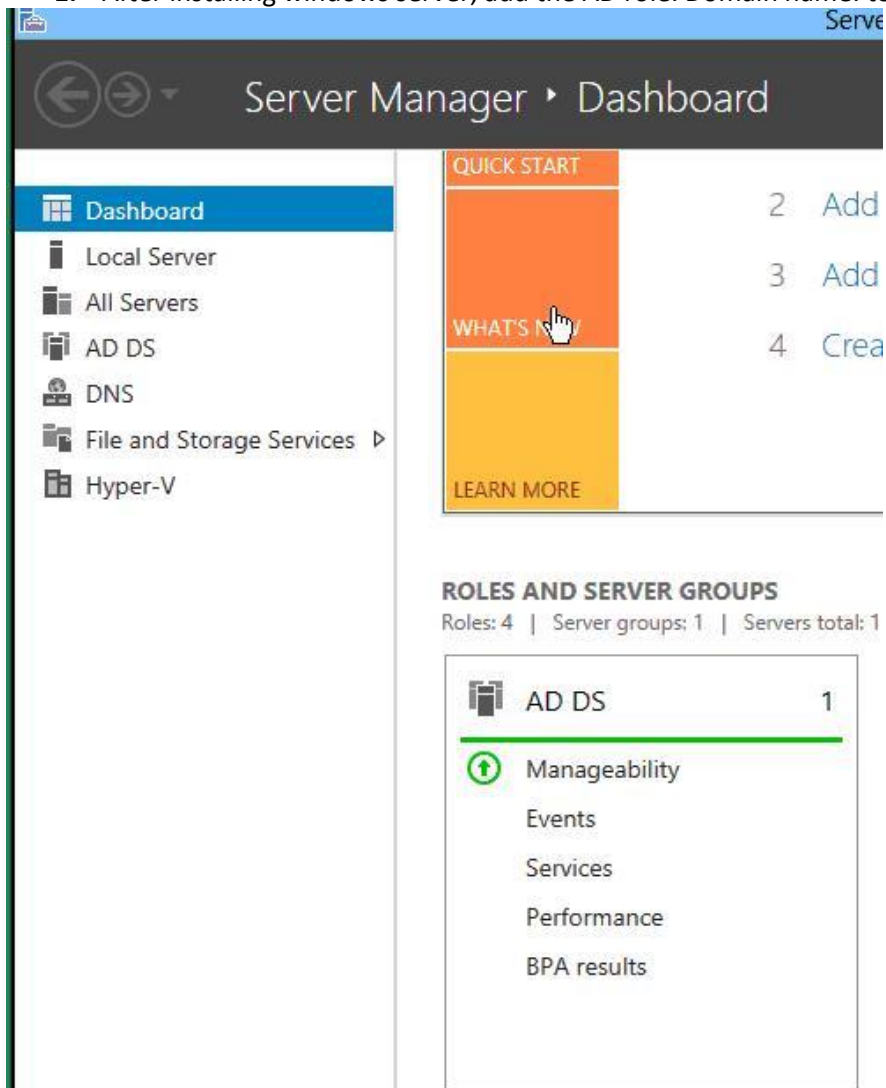
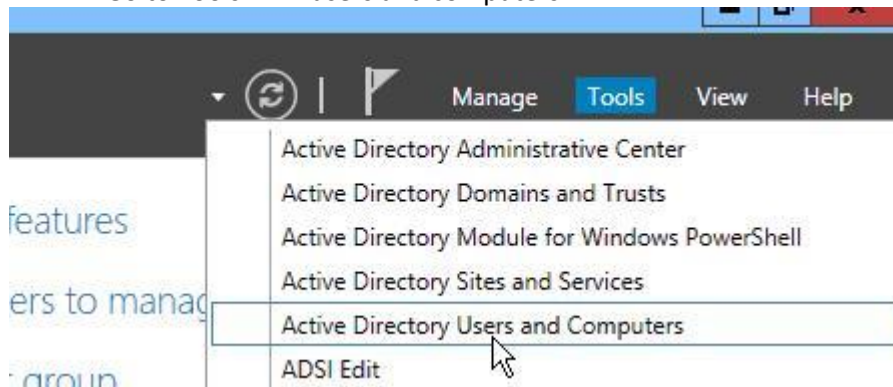


1. After installing windows server, add the AD role. Domain name: test.ts



2. Go to Tools > AD users and computers



3. Navigate to test.ts, then add users, create password for users

New Object - User

Create in: test.ts/Users

Password: [masked]

Confirm password: [masked]

User must change password at next logon

User cannot change password

Password never expires

Account is disabled

< Back   Next >   Cancel

4. Create group: test, add the users (test1,test2,test3) to group: test

Server Manager

Server Manager Dashboard

Active Directory Users and Computers

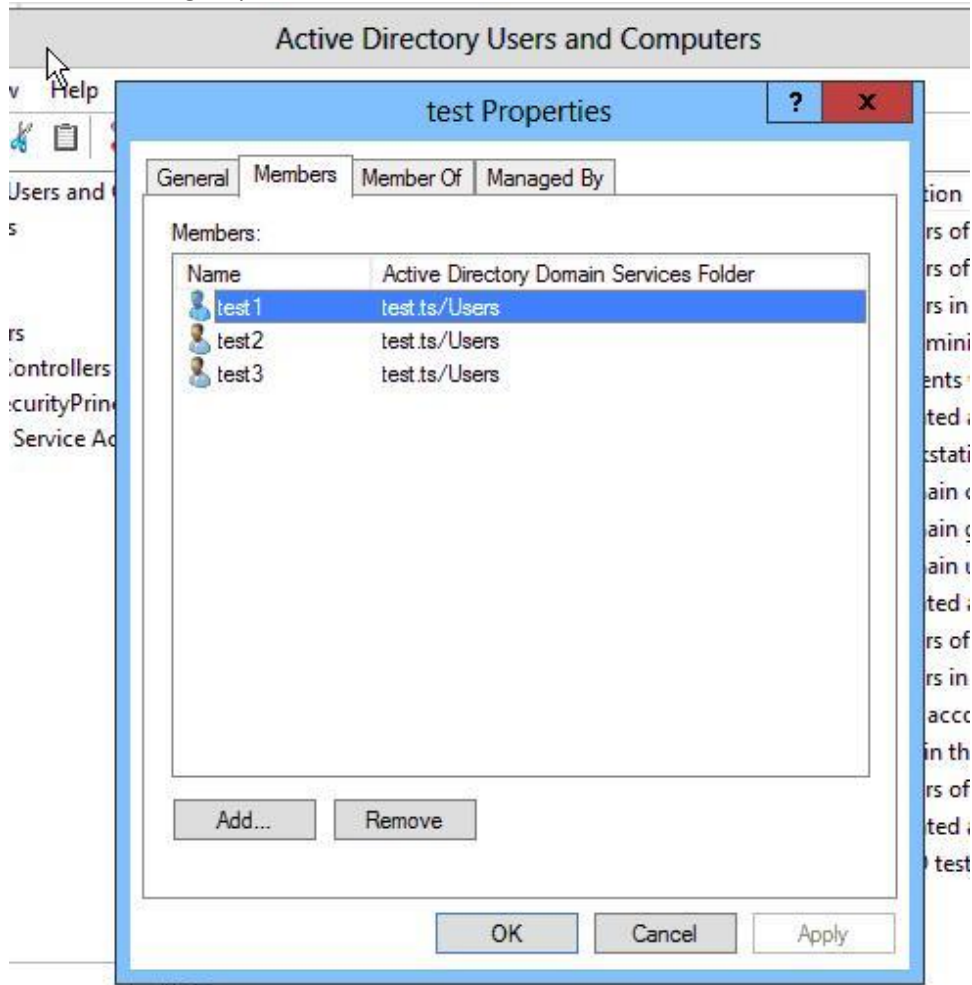
Name	Type	Description
Cert Publish...	Security Group - Domain Local	Members of this group ...
Cloneable D...	Security Group - Global	Members of this group t...
Denied ROD...	Security Group - Domain Local	Members in this group c...
DnsAdmins	Security Group - Domain Local	DNS Administrators Gro...
DnsUpdateP...	Security Group - Global	DNS clients who are per...
Domain Ad...	Security Group - Global	Designated administrato...
Read-only D...	Security Group - Global	Members of this group ...
Schema Ad...	Security Group - Universal	Designated administrato...
test	Security Group - Global	IPMI AD test
test1	User	
test2	User	
test3	User	

Active Directory Domain Services

The Add to Group operation was successfully completed.

OK

5. Check group – see all three test users



In the IPMI on X9SRH-7F system with fw 2.26:

6. In IPMI, check Configuration > AD > Advance Settings
  - a. User Domain Name = test.ts
  - b. Port 389 default
  - c. Time out = 0 -> 10
  - d. Domain Controller Server Address is the IP address of the Windows Server with the AD, in this example 172.31.8.236

The screenshot shows the IPMI web interface. At the top, a 'Host Identification' box displays 'Server: 172.031.009.026' and 'User: ADMIN (Administrator)'. Below this is a navigation bar with tabs for 'System Health', 'Configuration', 'Remote Control', 'Virtual Media', and 'Maintenance'. The 'Configuration' tab is active, leading to the 'Active Directory - Advanced Settings' page. A light blue instruction box states: 'Check the box below to enable Active Directory authentication and enter the required information to access Active Directory server. Press the Save button to save your changes.' The settings are as follows:

- Enable Active Directory Authentication
- Active Directory Authentication over SSL
- Port: 389
- User Domain Name: test.ts
- Time Out: 10
- Domain Controller Server Address1: 172.31.8.236
- Domain Controller Server Address2: 0.0.0.0
- Domain Controller Server Address3: 0.0.0.0

At the bottom left are 'Save' and 'Cancel' buttons. A blue dialog box titled 'The page at 172.31.9.26 says:' displays the message 'The requested configuration has been successfully set.' with an 'OK' button.

7. Add group role
  - a. Role group name: test
  - b. Role group domain: test.ts
  - c. Group privilege: Administrator

## ➔ Add New Role Group

Enter the information for the new role group below and press Add. Press Cancel to re

Role Group Name:

Role Group Domain:

Role Group Privilege:

8. Check, see group ID 1 is for test group, in test.ts domain

## ➔ Active Directory Settings

To enable or configure the Active Directory server, please click [here](#)

The list below shows the current list of configured Role Groups. If you would like to delete or modify a role group, select the name in the list and press Delete Role Group or Modify Role Group. To add a new Role Group, select an unconfigured slot and press Add Role Group.

Number of configured role groups:

Role Group ID	Group Name	Group Domain	Network Privilege
1	test	test.ts	Administrator
2	~	~	Reserved
3	~	~	Reserved
4	~	~	Reserved
5	~	~	Reserved

9. Log out, then login as one of the test users in the test group
  - a. test1@test.ts
  - b. test2@test.ts
  - c. test3@test.ts



**SUPERMICR**®

**Please Login**

Username

Password

10. login successful, you can see up top the User: test1@test.ts

← → ↻ 172.31.9.26/cgi/url\_redirect.cgi?url\_name=mainmenu

**SUPERMICR**®

Host Identification  
Server: 172.031.009.026  
User: test1@test.ts

System	Server Health	Configuration	Remote Control	Virtual Media	Maintenance
--------	---------------	---------------	----------------	---------------	-------------

→ System

→ **System Information**

→ FRU Reading

### → Summary

Firmware Revision : 02.26  
Firmware Build Time : 2013-04-24

IP address : 172.031.009.026  
BMC MAC address : 00:25:90:cc:53:77  
System LAN1 MAC address : 00:25:90:c1:c0:a8  
System LAN2 MAC address : 00:25:90:c1:c0:a8

Remote Console Preview

Refresh Preview Image

Power Control via IPMI

Host is currently on

Power On Power Down Reset

In the IPMI of the X9SRD-F microcloud we have setup, using fw 1.89, it also works



#### Host Identification

Server: 172.031.009.177

User: ADMIN (Administrator)

System	Server Health	Configuration	Remote Control	Virtual Media
--------	---------------	---------------	----------------	---------------

→ System

→ System Information

→ FRU Reading

### → Summary

Firmware Revision : 01.89

Firmware Build Time : 2012-11-28

IP address : 172.03

BMC MAC address :

System LAN1 MAC :

System LAN2 MAC :

→ Configuration

→ Alerts

→ Date and Time

→ LDAP

→ Active Directory

### → Active Directory Settings

To enable or configure the Active Directory server, please click [here](#)

The list below shows the current list of configured Role Groups. If you want to select the name in the list and press Delete Role Group or Modify Role Group on an unconfigured slot and press Add Role Group.



## ➔ Active Directory - Advanced Settings

Check the box below to enable Active Directory authentication and enter the required information for the Active Directory server. Press the Save button to save your changes.

Enable Active Directory Authentication

Active Directory Authentication over SSL

Port

User Domain Name

Time Out

Domain Controller Server Address1

Domain Controller Server Address2

Domain Controller Server Address3



Host Identification  
Server: 172.031.009.177  
User: ADMIN (Administrator)

 Critical  Refresh  Logout

- Health
- Configuration
- Remote Control
- Virtual Media
- Maintenance
- Miscellaneous

## ➔ Active Directory Settings

To enable or configure the Active Directory server, please click [here](#)

The list below shows the current list of configured Role Groups. If you would like to delete or modify a role group, select the name in the list and press Delete Role Group or Modify Role Group. To add a new Role Group, select an unconfigured slot and press Add Role Group.

Role Group ID	Group Name	Group Domain	Number of configured role	Network Privilege
1	test	test.ts		Administrator
2	~	~		Reserved
3	~	~		Reserved
4	~	~		Reserved
5	~	~		Reserved

[Add Role Group](#) [Modify Role Group](#) [Delete Role Group](#)



172.31.9.177

# SUPERMICR<sup>®</sup>

## Please Login

Username

Password

[login](#)



172.31.9.177/cgi/url\_redirect.cgi?url\_name=mainmenu

# SUPERMICR<sup>®</sup>

### Host Identification

Server: 172.031.009.177

User: test2@test.ts

System

Server Health

Configuration

Remote Control

Virtual Media

Maintenance

[System](#)

[System Information](#)

[FRU Reading](#)

## Summary

Firmware Revision : 01.89

Firmware Build Time : 2012-11-28

IP address : 172.031.009.177

BMC MAC address : 00:25:90:7d:14:f3

System LAN1 MAC address : 00:25:90:96:8b:d0

System LAN2 MAC address : 00:25:90:96:8b:d1