1. Configuring access, security, network infrastructure and customisations

* Mail Server Configuration

Table 1. Mail Server IP

|  |  |  |
| --- | --- | --- |
| **Server** | **Address/CIDR** | **Gateway** |
| Mail Server | 10.0.0.3/24 | 10.0.0.254 |

hMailServer software is used for the mail server.

ClamWin (Antivirus) is used for mail anti phishing.

A computer with a cd and a computer with a screen

Description automatically generated with medium confidence

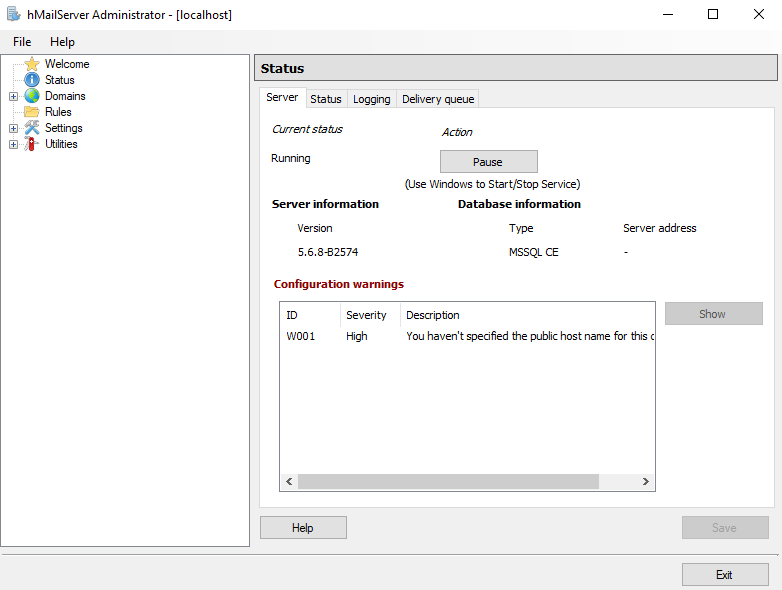


Figure 1 Mail Server (hMailServer)

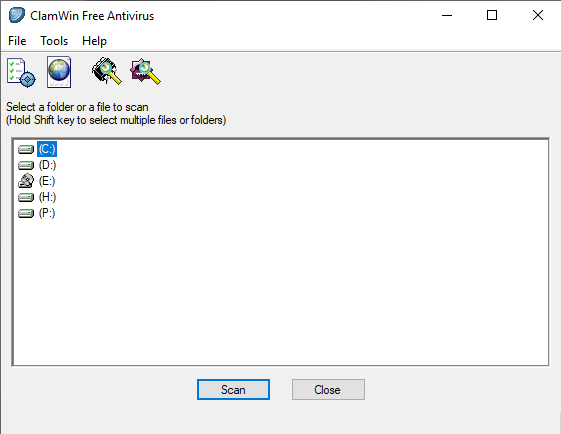


Figure 2 ClamWin (Antivirus)

* DNS Configuring in DC

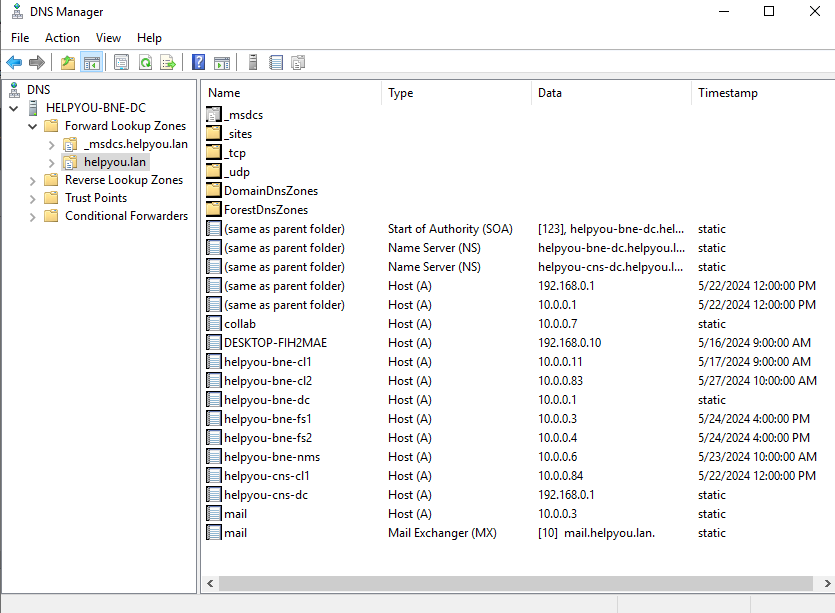


Figure 3 DNS Configuration

2. Email:

a) Users and mailboxes

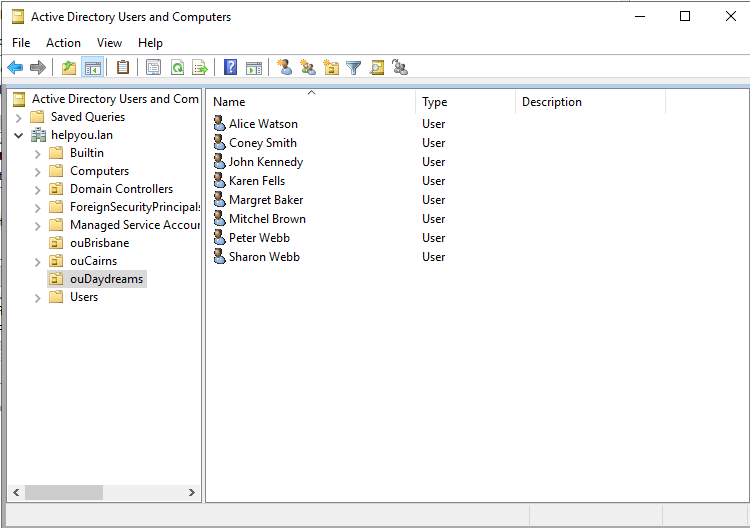


Figure 4 Users in Daydreams OU

A screenshot of a computer

Description automatically generated

Figure 5 Add Users to Mail Server

b) Remote email access

A screenshot of a computer

Description automatically generated

Figure 6 Nextcloud Mail (SnappyMail)

c) Address lists, distribution lists

A screenshot of a computer

Description automatically generated

Figure 7 Distribution list (Sales Distribution List)

d) Message integrity and antispam controls, antivirus controls and anti-phishing

A computer screen shot of a computer

Description automatically generated

Figure 8 Use ClamWin Antivirus to Mail Server

e) VOIP

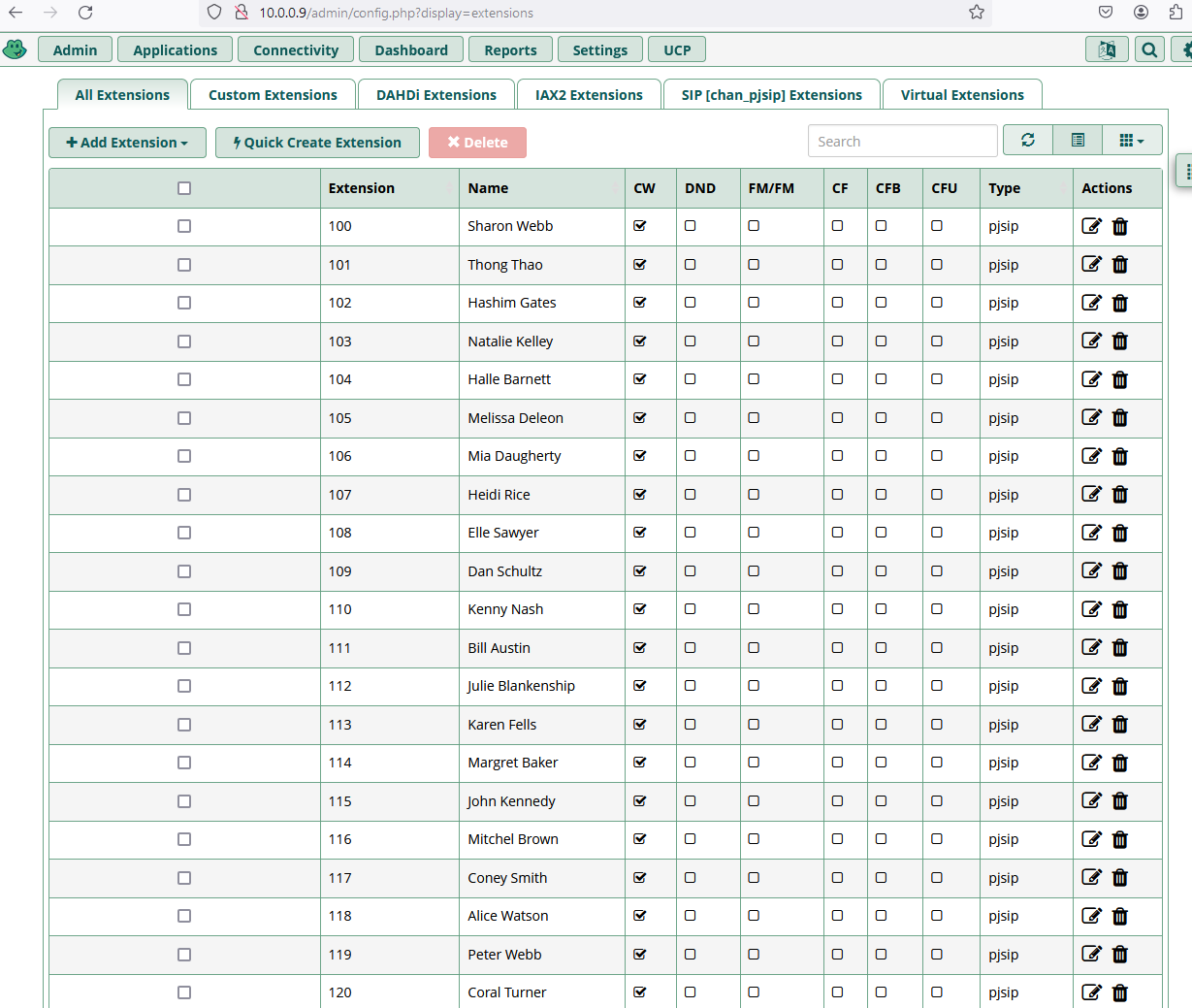


Figure 9 VoIP Extensions List

3. Collaboration tools:

a) Namespace and server roles

A screenshot of a computer

Description automatically generated

Figure 10 Configure trust domain

A screenshot of a computer

Description automatically generated

Figure 11 Configure DNS of Collaboration

b) User access, security, network infrastructure and customisations

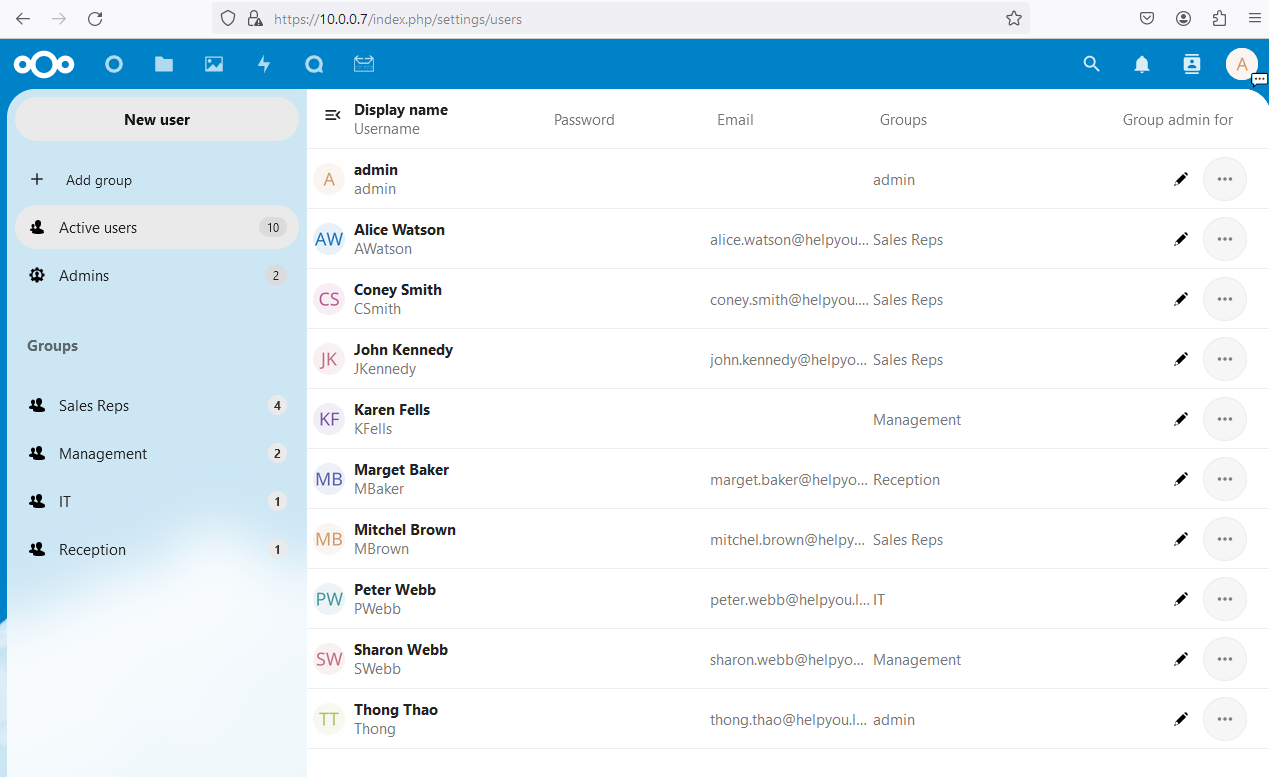


Figure 12 Collaboration Users

c) Providing high availability and disaster recovery

To provide high availability and disaster recovery for the collaboration server, a redundant configuration with multiple servers can be implemented. To set up a cluster of collaboration servers, where multiple servers are configured to work together and share the workload. If one server fails, the remaining servers in the cluster can automatically take over its responsibilities, ensuring continuous service availability[[1]](#footnote-1). Regular data backups and replication to a remote site or cloud storage can be implemented to enable disaster recovery in case of a catastrophic event, such as a natural disaster or a complete data centre failure.[[2]](#footnote-2)

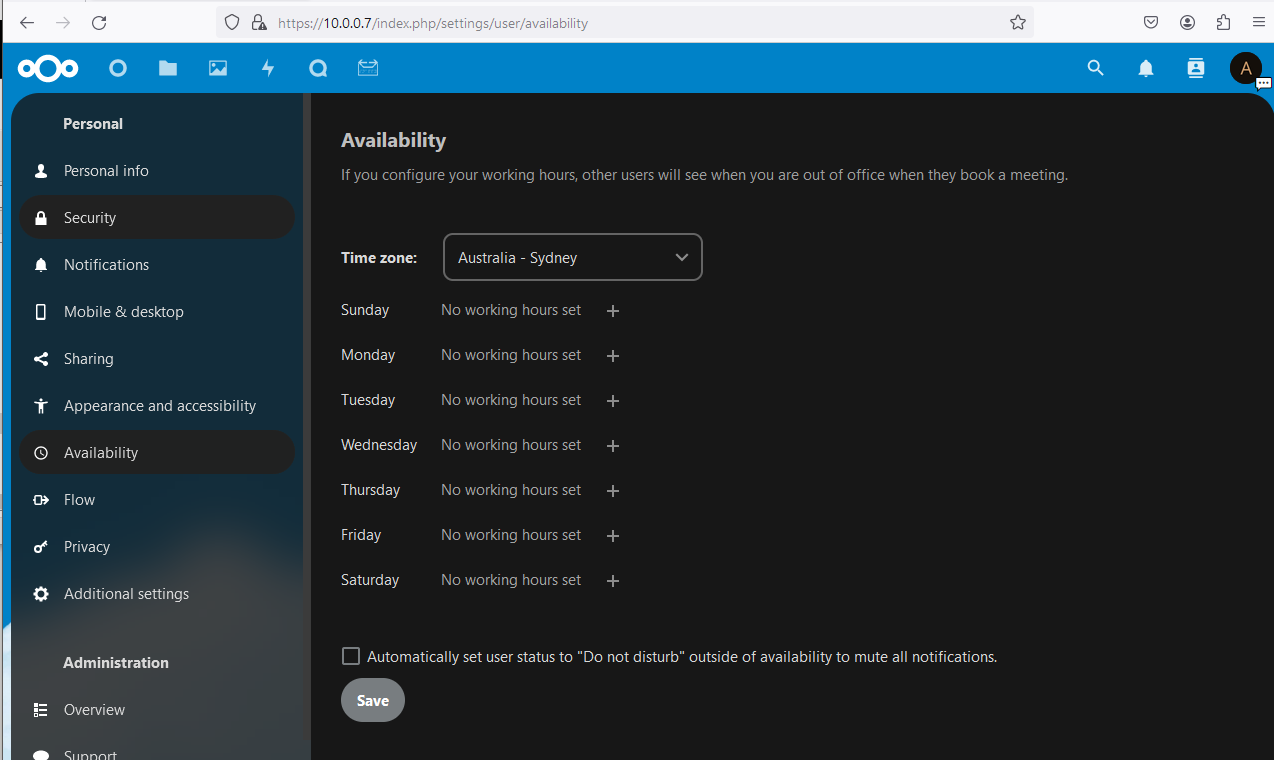


Figure 13 Nextcloud Availability

A screenshot of a computer

Description automatically generated

Figure 14 Backup Mail Server

1. https://www.site24x7.com/blog/failover-clusters-issues [↑](#footnote-ref-1)
2. https://www.investopedia.com/terms/d/disaster-recovery-site.asp [↑](#footnote-ref-2)