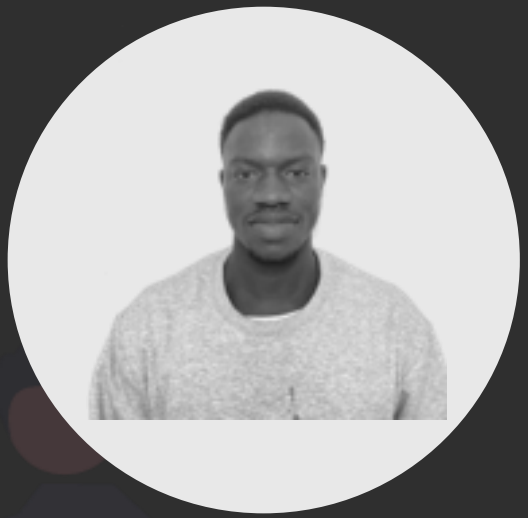
PROJET D'INTERGRATION

Groupe: Halim Jabbes et Alioune Diop

Institut supérieur d'informatique

WEZOOM

Présentation de l'équipe



Introduction

Nous sommes une petite entreprise de consultation informatique spécialisée dans le réseau et la sécurité ainsi qu'au développement we et applications.
On a récemment reçu une demande d'un projet
qui consiste à la réalisation d'un environnement de travail sécurisé spécialement pour une entreprise agissant dans le domaine pharmaceutique qui s’appelle Pharmed.

Topologie physique

Le schéma suivant présente la topologie qui a été mise en place spécialement pour l'entreprise Pharmed. d'une façon logique tout en utilisant une stratégie sécurisée.

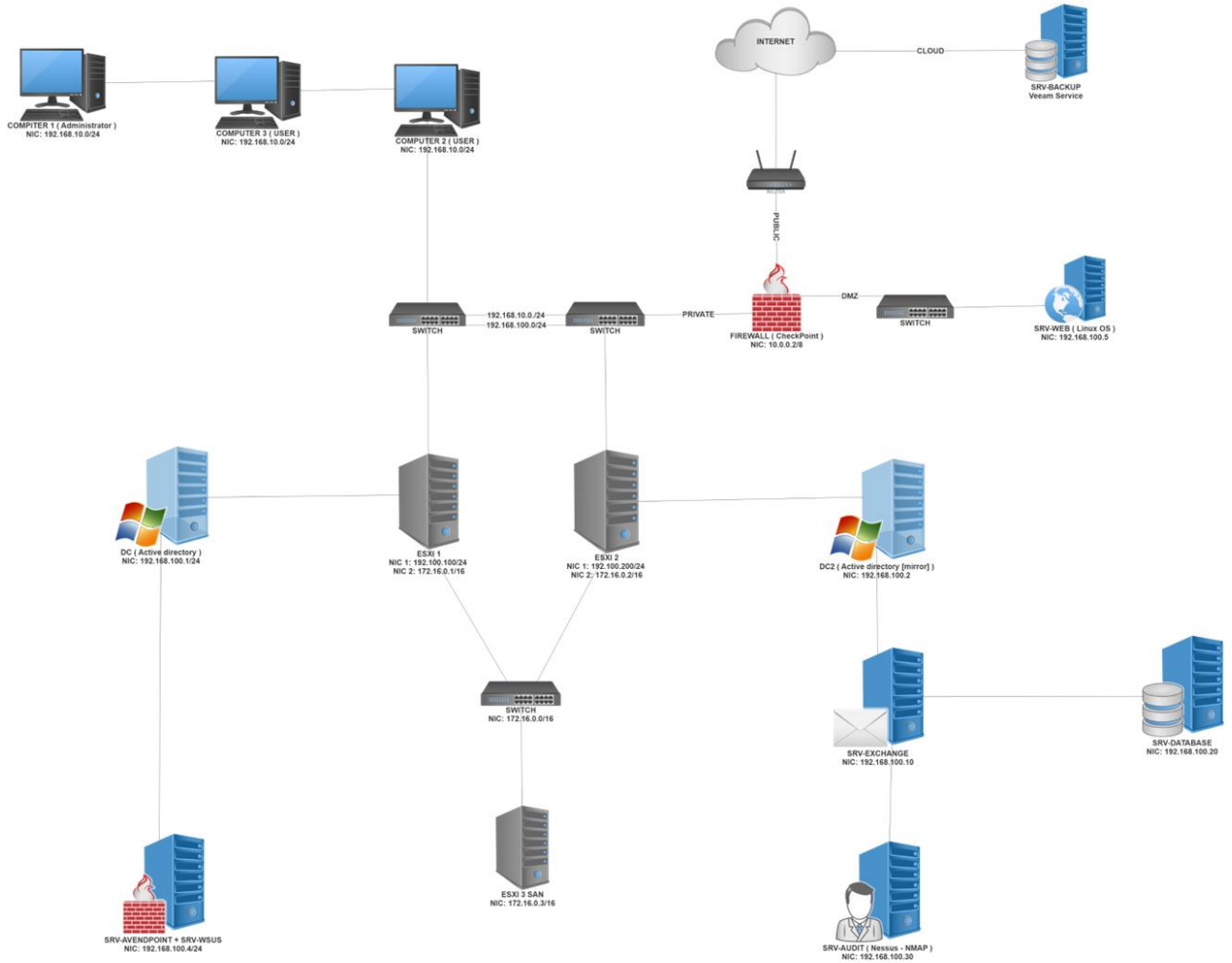

COMPITER 1 (Administrator)
NIC: 192.168.10.0/24
COMPUTER 3 (USER)
NIC: 192.168.10.0/24
COMPUTER 2 (USER)
NIC: 192.168.10.0/24
INTERNET
CLOUD
SRV-BACKUP
Veeam Service
PUBLIC
SWITCH
192.168.10.0./24
192.168.100.0/24
SWITCH
PRIVATE
FIREWALL (CheckPoint)
NIC: 10.0.0.2/8
DMZ
SWITCH
SRV-WEB (Linux OS)
NIC: 192.168.100.5
DC (Active directory)
NIC: 192.168.100.1/24
ESXI 1
NIC 1: 192.100.100/24
NIC 2: 172.16.0.1/16
ESXI 2
NIC 1: 192.100.200/24
NIC 2: 172.16.0.2/16
DC2 (Active directory [mirror])
NIC: 192.168.100.2
SWITCH
NIC: 172.16.0.0/16
SRV-EXCHANGE
NIC: 192.168.100.10
SRV-DATABASE
NIC: 192.168.100.20
SRV-AVENDPOINT + SRV-WSUS
NIC: 192.168.100.4/24
ESXI 3 SAN
NIC: 172.16.0.3/16
SRV-AUDIT (Nessus - NMAP)
NIC: 192.168.100.30

Tableau d'adressage

[+] SRV-ADFS
Guest OS: Microsoft Windows Server 2019 (64-bit)
DNS Name: srv-adfs.pharmed.ca
IP Addresses: 192.168.100.7
Host (EXSI): 192.168.100.200

[+] SRV-SDC
Guest OS: Microsoft Windows Server 2019 (64-bit)
DNS Name: srv-sdc.pharmed.ca
IP Addresses: 192.168.100.2
Host (EXSI): 192.168.100.100

[+] SRV-AVENDPOINT
Guest OS: Microsoft Windows Server 2019 (64-bit)
DNS Name: srv-avendpoint.pharmed.ca
IP Addresses: 192.168.100.4
Host (EXSI): 192.168.100.200

[+] SRV-EXCHANGE
Guest OS: Microsoft Windows Server 2019 (64-bit)
DNS Name: srv-exchange.pharmed.ca
IP Addresses: 192.168.100.3
Host (EXSI): 192.168.100.200

[+] SRV-PDC
Guest OS: Microsoft Windows Server 2019 (64-bit)
DNS Name: srv-pdc.pharmed.ca
IP Addresses: 192.168.100.1
Host (EXSI): 192.168.100.200

[+] SRV-VC
Guest OS: Microsoft Windows Server 2019 (64-bit)
DNS Name: srv-vc.pharmed.ca
IP Addresses: 192.168.100.10
Host (EXSI): 192.168.100.200

[+] SRV-BACKUP
Guest OS: Microsoft Windows Server 2019 (64-bit)
DNS Name: srv-backup.pharmed.ca
IP Addresses: 192.168.100.8
Host (EXSI): 192.168.100.100

[+] SRV-PENTESTING
Guest OS: Microsoft Windows Server 2019 (64-bit)
DNS Name: srv-pentesting.pharmed.ca
IP Addresses: 192.168.100.6
Host (EXSI): 192.168.100.100

[+] SRV-WORDPRESS
Guest OS: Microsoft Windows Server 2019 (64-bit)
DNS Name: srv-wordpress.pharmed.ca
IP Addresses: 192.168.100.5
Host (EXSI): 192.168.100.100

[+] SRV-NAS
Guest OS: Microsoft Windows Server 2019 (64-bit)
DNS Name: srv-wordpress.pharmed.ca
IP Addresses: 192.168.100.5
Host (EXSI): 192.168.100.100

Matériel & logiciel

Liste des équipements

[+] POWEREDGE R750
    [-] Deux serveurs EXI montés en cluster
    [-] Prix de l'unité $15,580.00

[+] DELL POWEREDGE R750
    [-] Réseau de stockage de type SAN
    [-] Prix de l'unité $15,450.00

[+] CheckPoint 770
    [-] Un pare-feu qui inspectent la couche réseau
    [-] Prix de l'unité $15,450.00

[+] TL-SG1016 | 16-Port Gigabit Rackmount Switch
    [-] Deux commutateurs de couche 3 pour but d'accélérer l'échange de données au sein d'un grand réseau local.
    [-] Prix de l'unité $76.99

[+] POWEREDGE R750
    [-] Deux serveurs EXI montés en cluster
    [-] Prix de l'unité $15,580.00

[+] DELL POWEREDGE R750
    [-] Réseau de stockage de type SAN
    [-] Prix de l'unité $15,450.00

[+] CheckPoint 770
    [-] Un pare-feu qui inspectent la couche réseau
    [-] Prix de l'unité $15,450.00

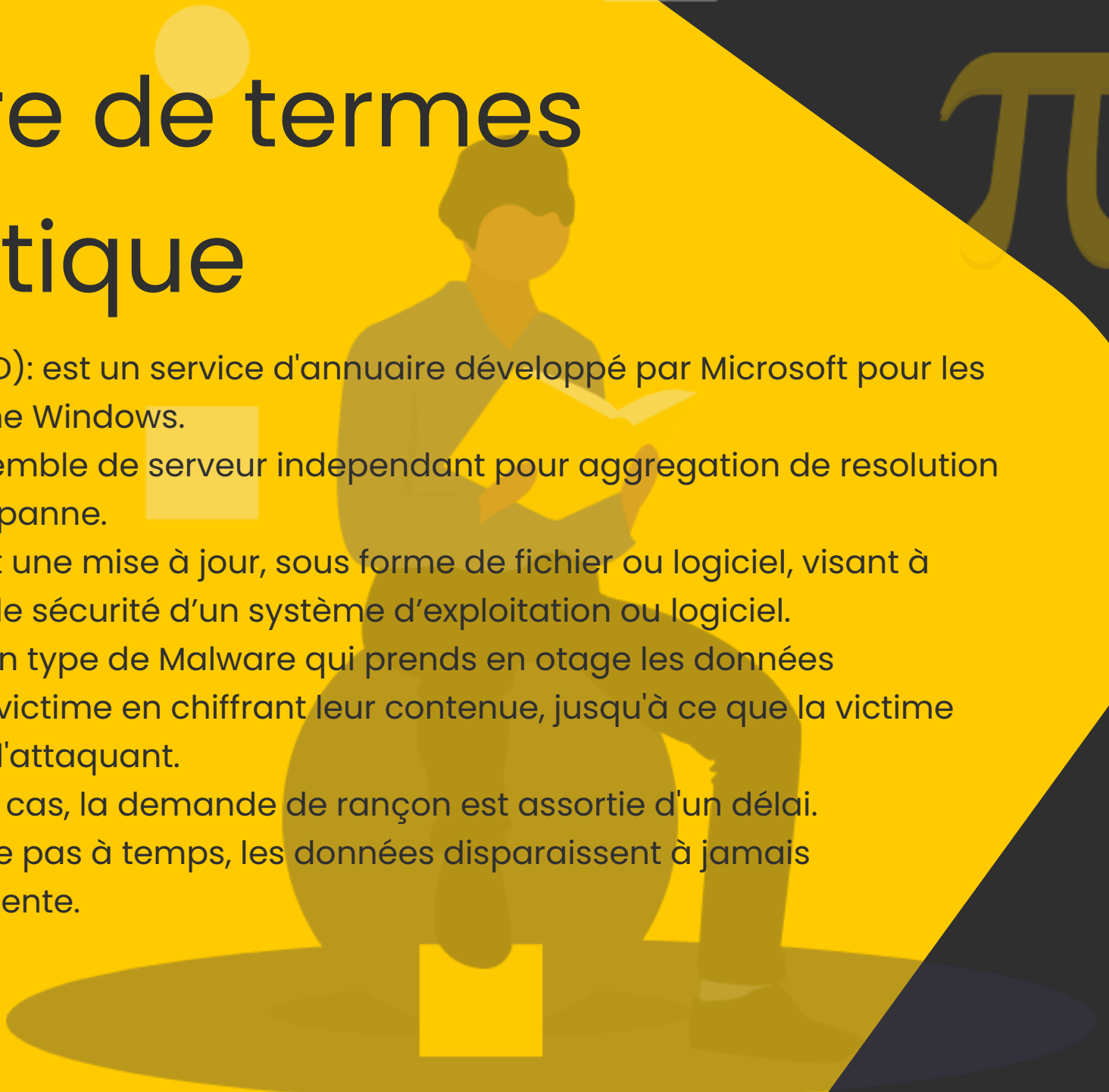
[+] TL-SG1016 | 16-Port Gigabit Rackmount Switch
    [-] Deux commutateurs de couche 3 pour but d'accélérer l'échange de données au sein d'un grand réseau local.
    [-] Prix de l'unité $76.99

Les technologies implantée

1. Dans le but d'avoir un environnement sécurisé on a mis en place un système de prévention contre les attaques ransomware ou de catastrophe naturelle, ce système consiste a mettre a jour chaque fin de journée les backups, tout cela se gère à partir du serveur backup (SRV-BACKUP) et stocké sur Google Cloud.
2. L'accès aux comptes sont sécurisé en utilisant la technologie double authentification (2FA).
3. Le serveur antivirus servira à faciliter les tâches au service d'administration lors d'un déploiement d'un des patchs et correctifs logiciels, les scans hebdomadaires ou les attaques malveillantes.

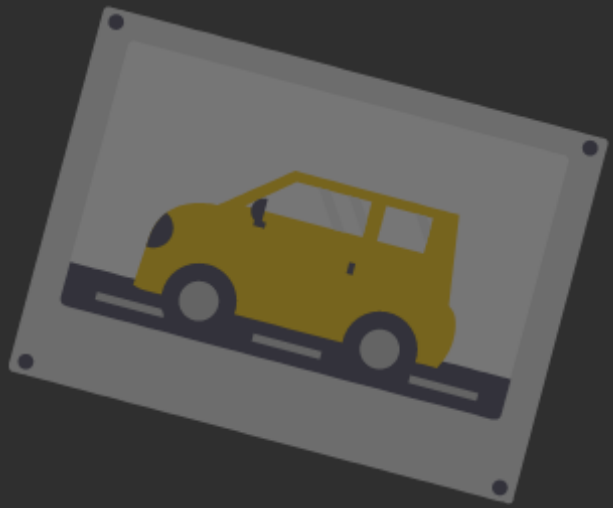
4. On a configuré notre firewall checkpoint, tout en mettant en place un ensemble de règles qui serviront à filtrer le trafique du réseau et en bloquant certaines applications.
5. On a installé et configuré un serveur Mail (Microsoft Exchange) relié directement avec le domaine "pharmed.ca" il est automatiquement synchronisé avec le serveur d'active directory. Il a pour but d'envoyer et recevoir des emails.
6. Le cluster est composé de deux serveurs ESXI "srv-esxione.pharmed.ca", "srv-esxitwo.pharmed.ca" qui travaillent ensemble pour une l'agrégation de résolution et de tolérance de panne.
7. On a mis en place un serveur SAN "srv-san.pharmed.ca" en tant que serveur de stockage qui sert à partager des fichiers et les données sur un réseau local, il est également relié avec le cluster.
8. Le site web est directement relié avec Cloudflare (WAF - Firewall d'applications Web) au niveau des Domaine Nom System (DNS), cela nous permet à cacher nos vrais DNS et d'avoir des statistiques détaillées concernant le trafic entrant, les attaques et mettre des règles de restrictions par exemple bloquer des pays ou des adresses ip.

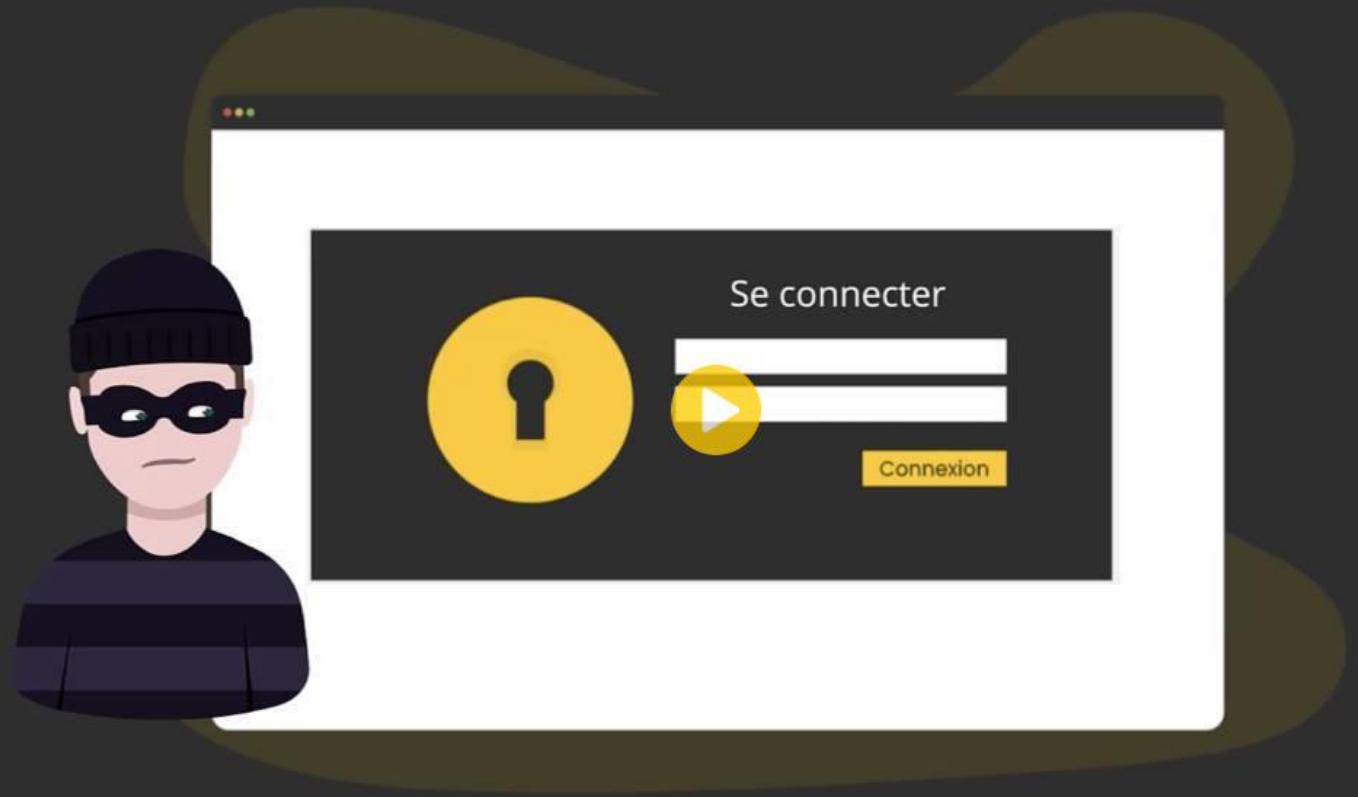
Glossaire de termes informatique



- Active Directory (AD): est un service d'annuaire développé par Microsoft pour les réseaux de domaine Windows.
- Cluster: est un ensemble de serveur independant pour aggregation de resolution et de tolerance de panne.
- Patch/Correctif: est une mise à jour, sous forme de fichier ou logiciel, visant à corriger les failles de sécurité d'un système d'exploitation ou logiciel.
- Ransomware: est un type de Malware qui prends en otage les données personnelles de la victime en chiffrant leur contenue, jusqu'à ce que la victime paie une rançon à l'attaquant.
  Dans de nombreux cas, la demande de rançon est assortie d'un délai.
  Si la victime ne paie pas à temps, les données disparaissent à jamais
  ou la rançon augmente.

Photos et vidéos




Se connecter
Connexion

Two-Factor Authentication | Settings

Two-Factor Authentication

Learn more about Two-Factor Authentication

Two-Factor Authentication, or 2FA, significantly improves login security for your website. Wordfence 2FA works with a number of TOTP-based apps like Google Authenticator, FreeOTP, and Authy. For a full list of tested TOTP-based apps, click here.

Editing User: example-user (you)

1. Scan Code or Enter Key

Scan the code below with your authenticator app to add this account. Some authenticator apps also allow you to type in the text version instead.

HCDLE3ELIYPXBXMLOPAKLGN7PGBOPLGA

2. Enter Code from Authenticator App

Download Recovery Codes *Optional*

Use one of these 5 codes to log in if you lose access to your authenticator device. Codes are 16 characters long plus optional spaces. Each one may be used only once.

```
0f2d 9b29 99ec 555b
e774 f5ae 799d 1959
5009 d881 f388 f3c1
b0cf 461b 0275 d525
68f1 3e94 98a2 c2c8
```

DOWNLOAD

Enter the code from your authenticator app below to verify and activate two-factor authentication for this account.

123456

For help on setting up an app, visit our help article.

ACTIVATE

Exchange admin center

recipients
permissions
compliance management
organization
protection
mail flow
mobile
public folders
servers
hybrid

mailboxes groups resources contacts shared migration

DISPLAY NAME	MAILBOX TYPE	EMAIL ADDRESS
Alice	**User**	**alice@pharmed.ca**
Administrator	User	Administrator@pharmed.ca

Alice

User mailbox
alice@pharmed.ca
Title:
Office:
Work phone:

Phone and Voice Features

Mobile Devices
Disable Exchange ActiveSync
Disable OWA for Devices
View details

In-Place Archive

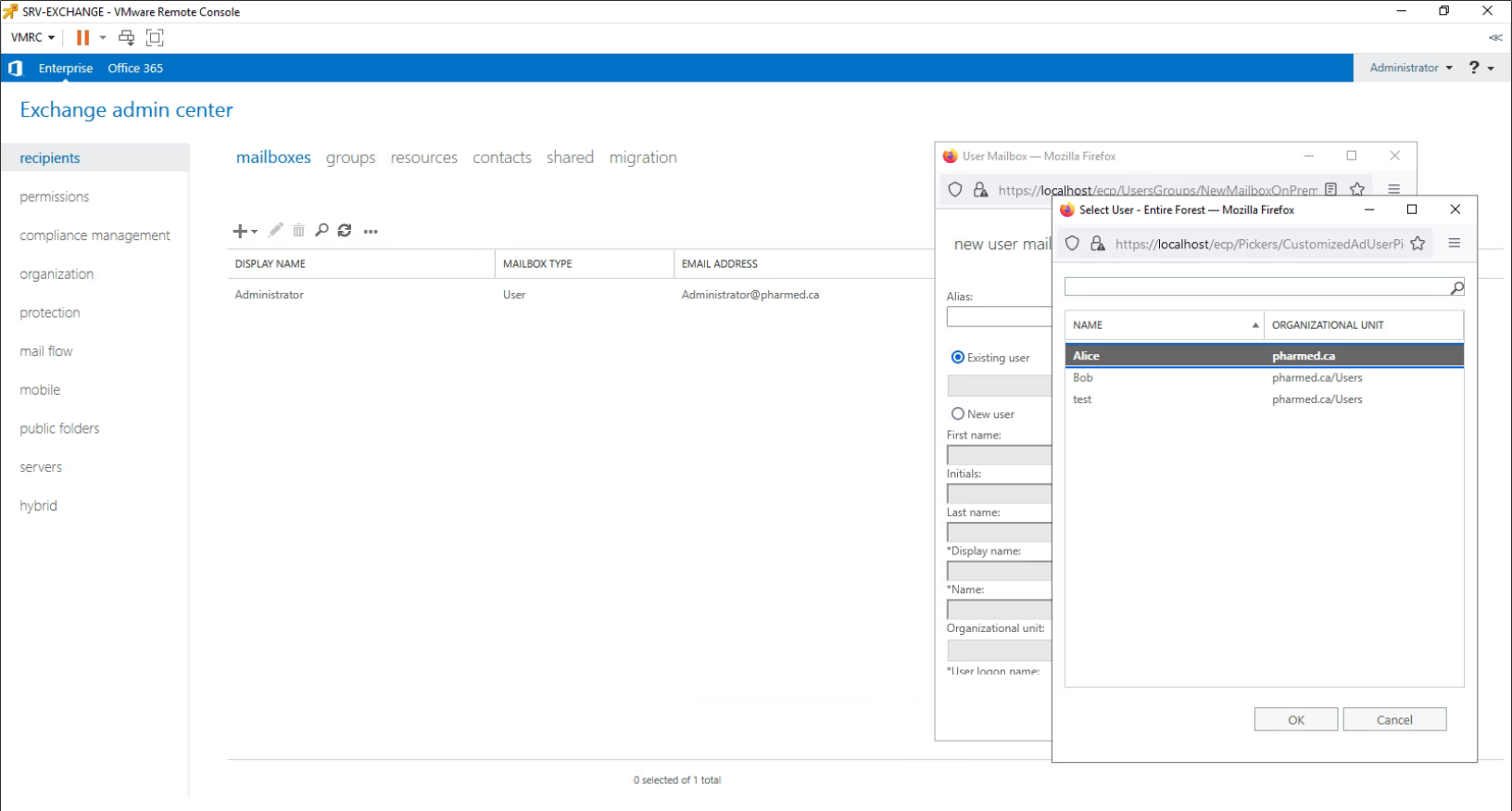
Archiving: Disabled
Enable

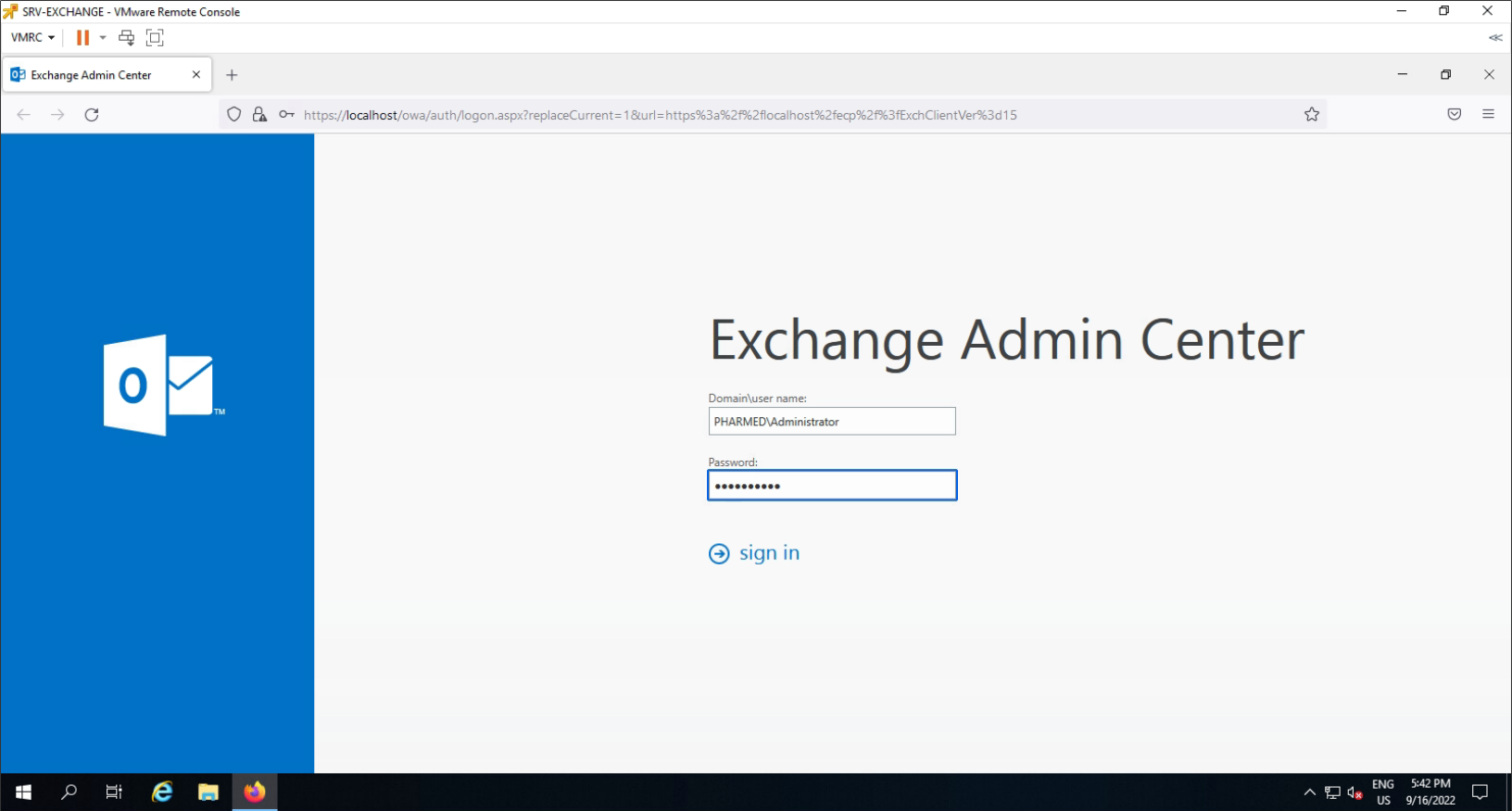
In-Place Hold

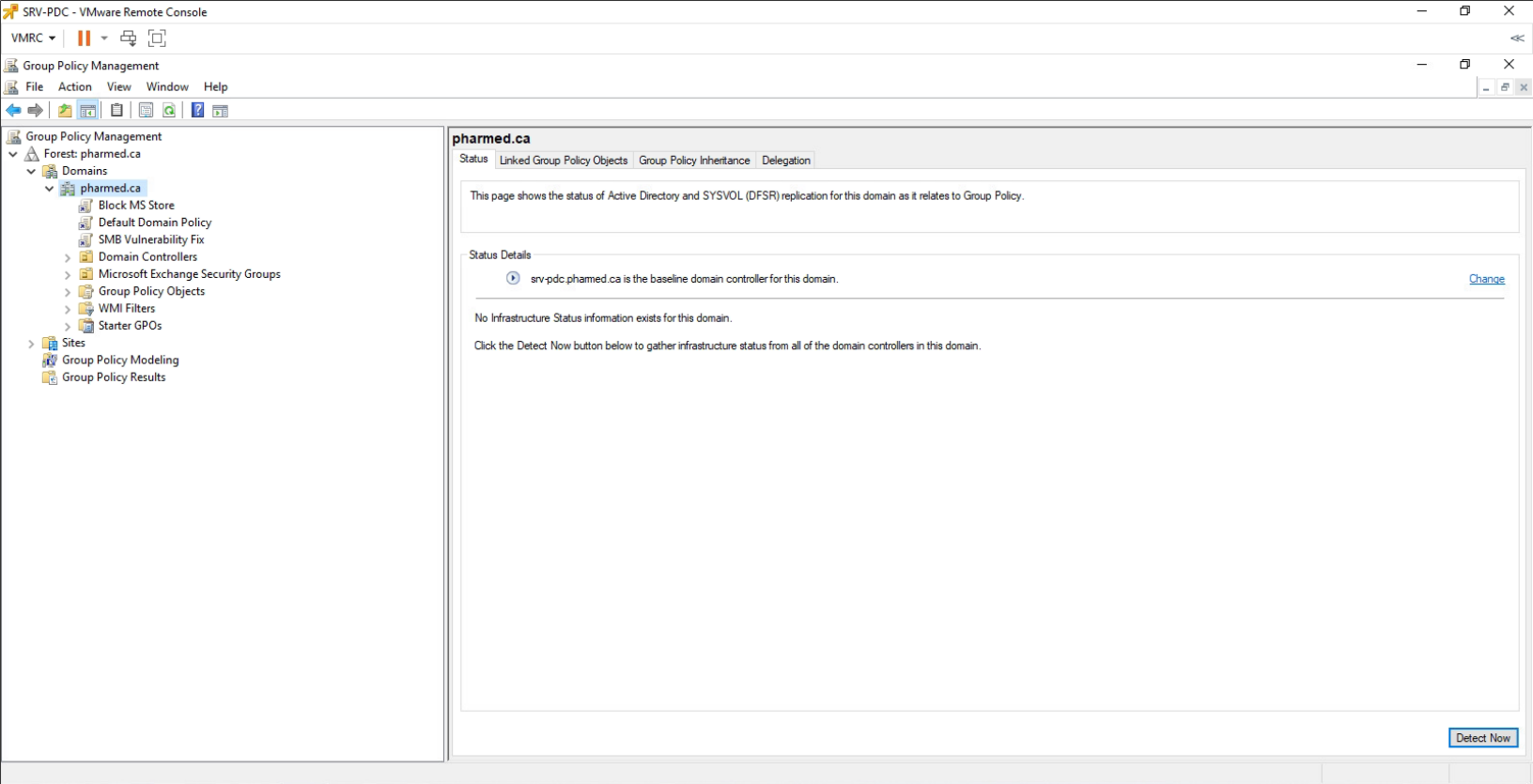
User isn't under hold

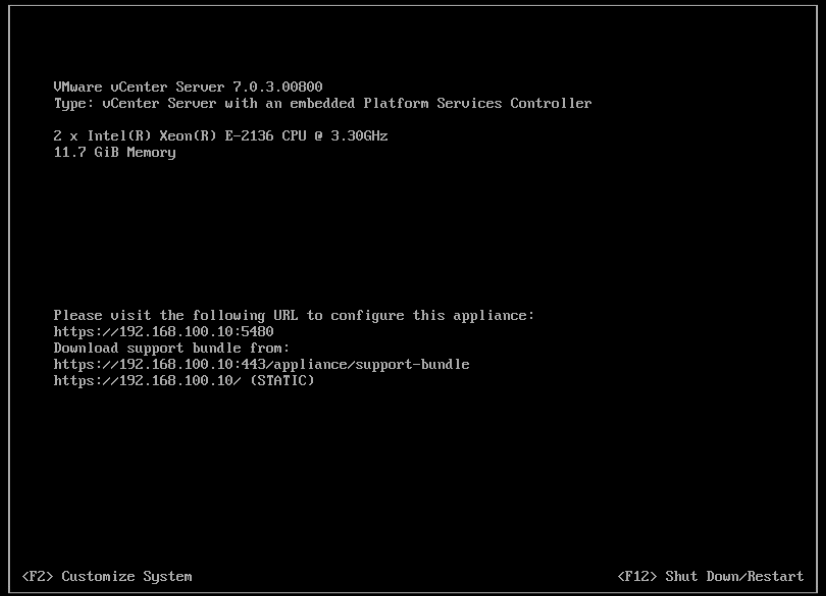
Email Connectivity

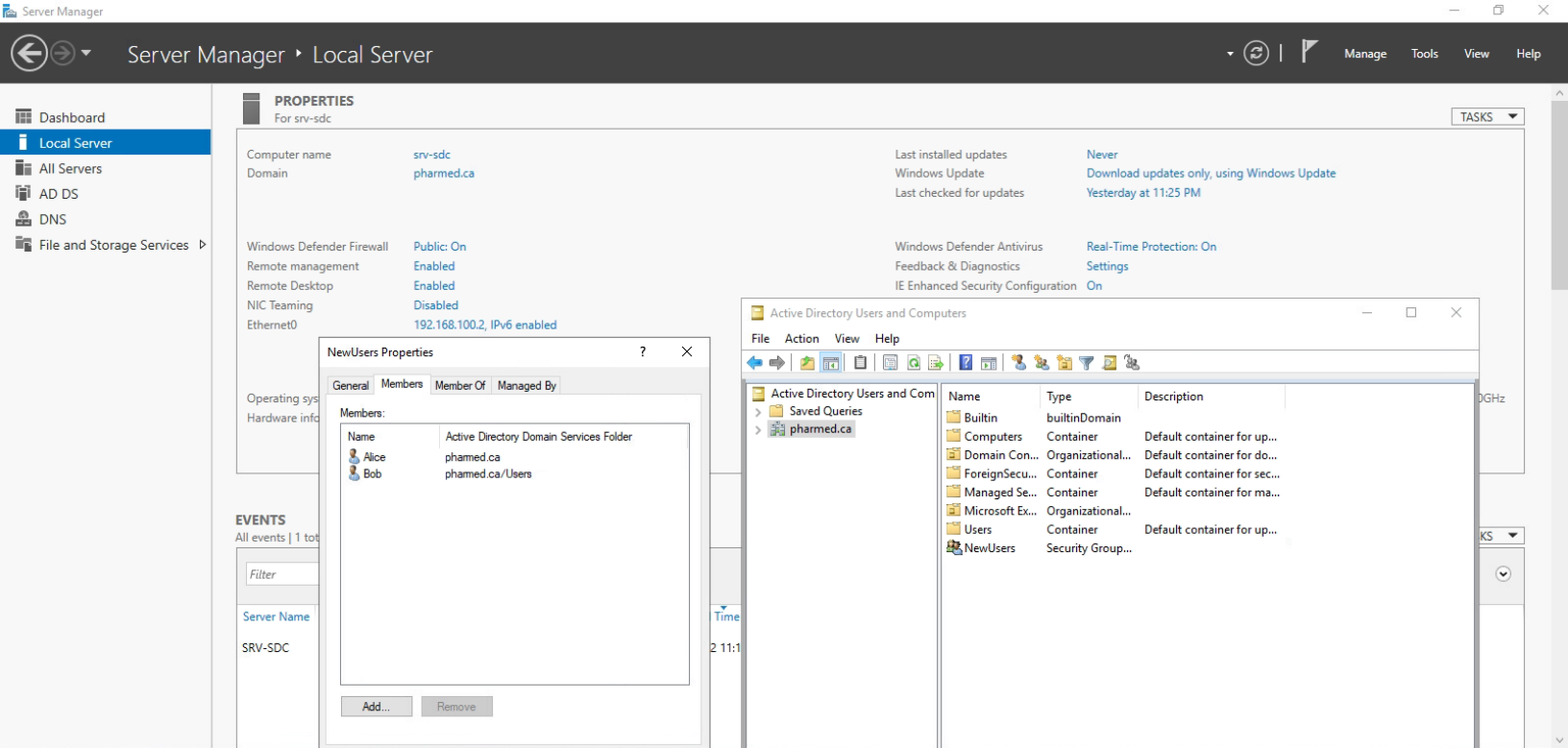
1 selected of 2 total

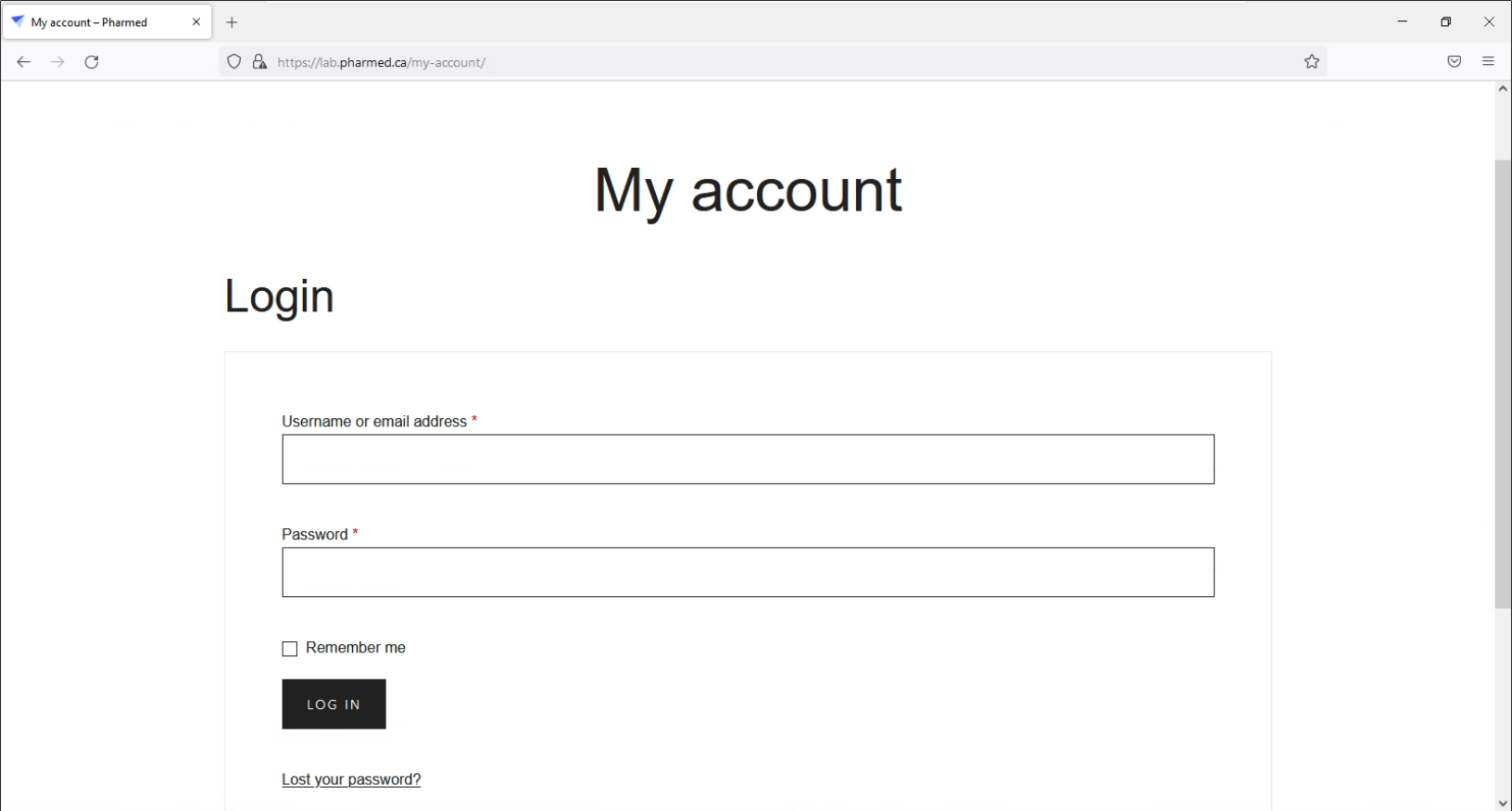

SRV-EXCHANGE - VMware Remote Console
VMRC
Enterprise
Office 365
Administrator
Exchange admin center
recipients
permissions
compliance management
organization
protection
mail flow
mobile
public folders
servers
hybrid
mailboxes
groups
resources
contacts
shared
migration
DISPLAY NAME
MAILBOX TYPE
EMAIL ADDRESS
Administrator
User
Administrator@pharmed.ca
0 selected of 1 total
User Mailbox — Mozilla Firefox
https://localhost/ecp/UsersGroups/NewMailboxOnPrem
new user mail
Alias:
Existing user
New user
First name:
Initials:
Last name:
*Display name:
*Name:
Organizational unit:
*User logon name:
Select User - Entire Forest — Mozilla Firefox
https://localhost/ecp/Pickers/CustomizedAdUserPi
NAME
ORGANIZATIONAL UNIT
Alice
pharmed.ca
Bob
pharmed.ca/Users
test
pharmed.ca/Users
OK
Cancel


SRV-EXCHANGE - VMware Remote Console
VMRC
Exchange Admin Center
https://localhost/owa/auth/logon.aspx?replaceCurrent=1&url=https%3a%2f%2flocalhost%2fecp%2f%3fExchClientVer%3d15
Exchange Admin Center
Domain\user name:
PHARMED\Administrator
Password:
sign in
ENG
US
5:42 PM
9/16/2022


SRV-PDC - VMware Remote Console
VMRC
Group Policy Management
File Action View Window Help
Group Policy Management
Forest: pharmed.ca
Domains
pharmed.ca
Block MS Store
Default Domain Policy
SMB Vulnerability Fix
Domain Controllers
Microsoft Exchange Security Groups
Group Policy Objects
WMI Filters
Starter GPOs
Sites
Group Policy Modeling
Group Policy Results
pharmed.ca
Status
Linked Group Policy Objects
Group Policy Inheritance
Delegation
This page shows the status of Active Directory and SYSVOL (DFSR) replication for this domain as it relates to Group Policy.
Status Details
srv-pdc.pharmed.ca is the baseline domain controller for this domain.
Change
No Infrastructure Status information exists for this domain.
Click the Detect Now button below to gather infrastructure status from all of the domain controllers in this domain.
Detect Now

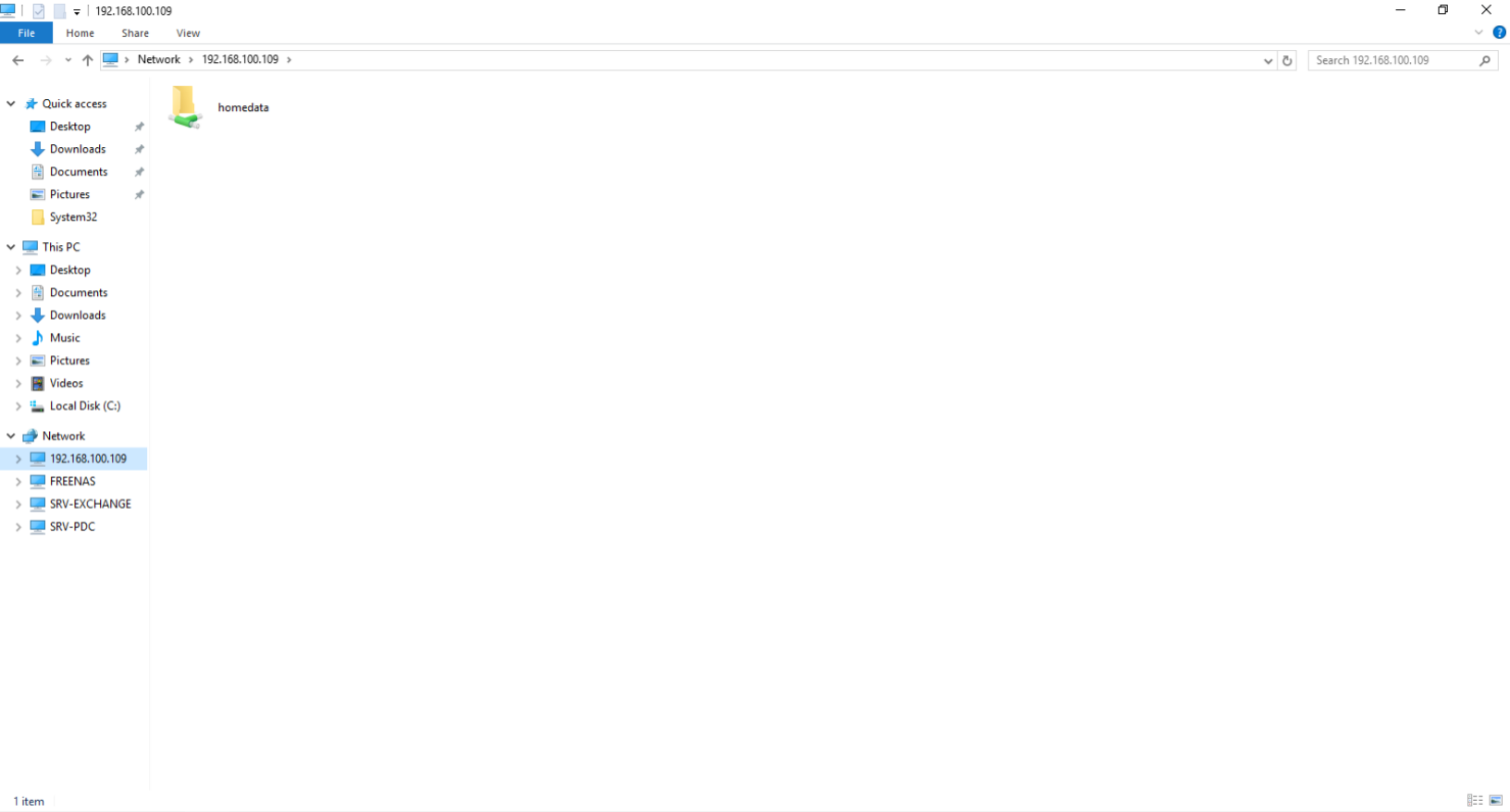

VMware vCenter Server 7.0.3.00800
Type: vCenter Server with an embedded Platform Services Controller
2 x Intel(R) Xeon(R) E-2136 CPU @ 3.30GHz
11.7 GiB Memory
Please visit the following URL to configure this appliance:
https://192.168.100.10:5480
Download support bundle from:
https://192.168.100.10:443/appliance/support-bundle
https://192.168.100.10/ (STATIC)
<F2> Customize System
<F12> Shut Down/Restart

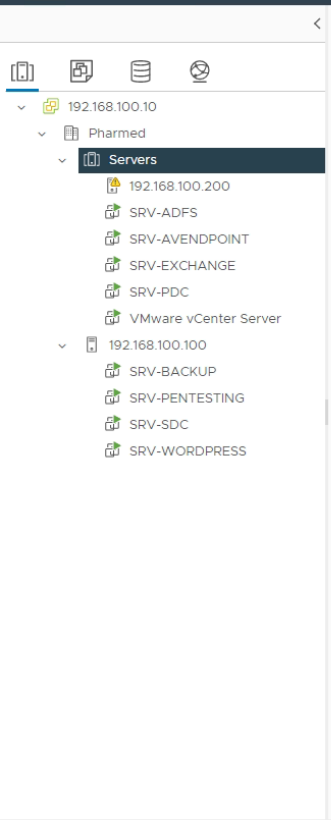

Server Manager
Server Manager ▸ Local Server
Manage
Tools
View
Help
Dashboard
Local Server
All Servers
AD DS
DNS
File and Storage Services
PROPERTIES
For srv-sdc
TASKS
Computer name
srv-sdc
Domain
pharmed.ca
Last installed updates
Never
Windows Update
Download updates only, using Windows Update
Last checked for updates
Yesterday at 11:25 PM
Windows Defender Firewall
Public: On
Remote management
Enabled
Remote Desktop
Enabled
NIC Teaming
Disabled
Ethernet0
192.168.100.2, IPv6 enabled
Windows Defender Antivirus
Real-Time Protection: On
Feedback & Diagnostics
Settings
IE Enhanced Security Configuration
On
Operating sys
Hardware info
EVENTS
All events | 1 tot
Filter
Server Name
Time
SRV-SDC
2 11:1
NewUsers Properties
General
Members
Member Of
Managed By
Members:
Name
Active Directory Domain Services Folder
Alice
pharmed.ca
Bob
pharmed.ca/Users
Add...
Remove
Active Directory Users and Computers
File
Action
View
Help
Active Directory Users and Com
Saved Queries
pharmed.ca
Name
Type
Description
Builtin
builtinDomain
Computers
Container
Default container for up...
Domain Con...
Organizational...
Default container for do...
ForeignSecu...
Container
Default container for sec...
Managed Se...
Container
Default container for ma...
Microsoft Ex...
Organizational...
Users
Container
Default container for up...
NewUsers
Security Group...


My account – Pharmed
https://lab.pharmed.ca/my-account/
My account
Login
Username or email address *
Password *
Remember me
LOG IN
Lost your password?

Nos gammes de produits cosmétiques et de beauté

ACHETEZ MAINTENANT


192.168.100.109
File
Home
Share
View
Network
192.168.100.109
Search 192.168.100.109
Quick access
Desktop
Downloads
Documents
Pictures
System32
This PC
Desktop
Documents
Downloads
Music
Pictures
Videos
Local Disk (C:)
Network
192.168.100.109
FREENAS
SRV-EXCHANGE
SRV-PDC
homedata
1 item



Servers

ACTIONS

Summary | Monitor | Configure | Permissions | Hosts | VMs | Datastores | Networks | Updates

Total Processors: 6
Total vMotion Migrations: 0

CPU — Free: 18.17 GHz — Used: 1.7 GHz — Capacity: 19.87 GHz
Memory — Free: 4.63 GB — Used: 27.1 GB — Capacity: 31.72 GB
Storage — Free: 98.32 GB — Used: 832.93 GB — Capacity: 931.25 GB

Related Objects

Datacenter	Pharmed

Cluster Services

Custom Attributes

Attribute	Value
com.vmware.vcenter.cluster.edrs.upgradeHos...	

1 items

Edit...

Cluster Consumers

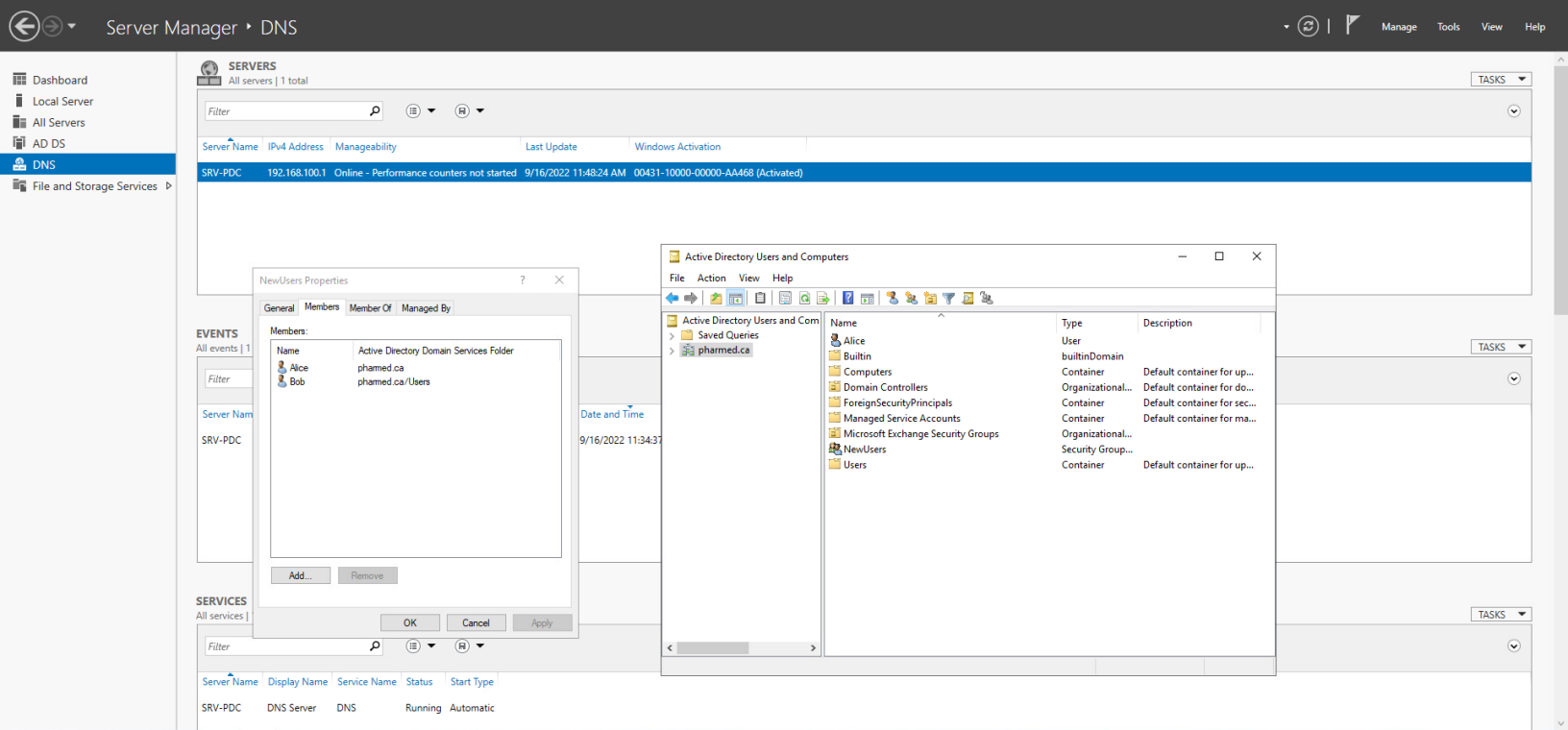
Tags

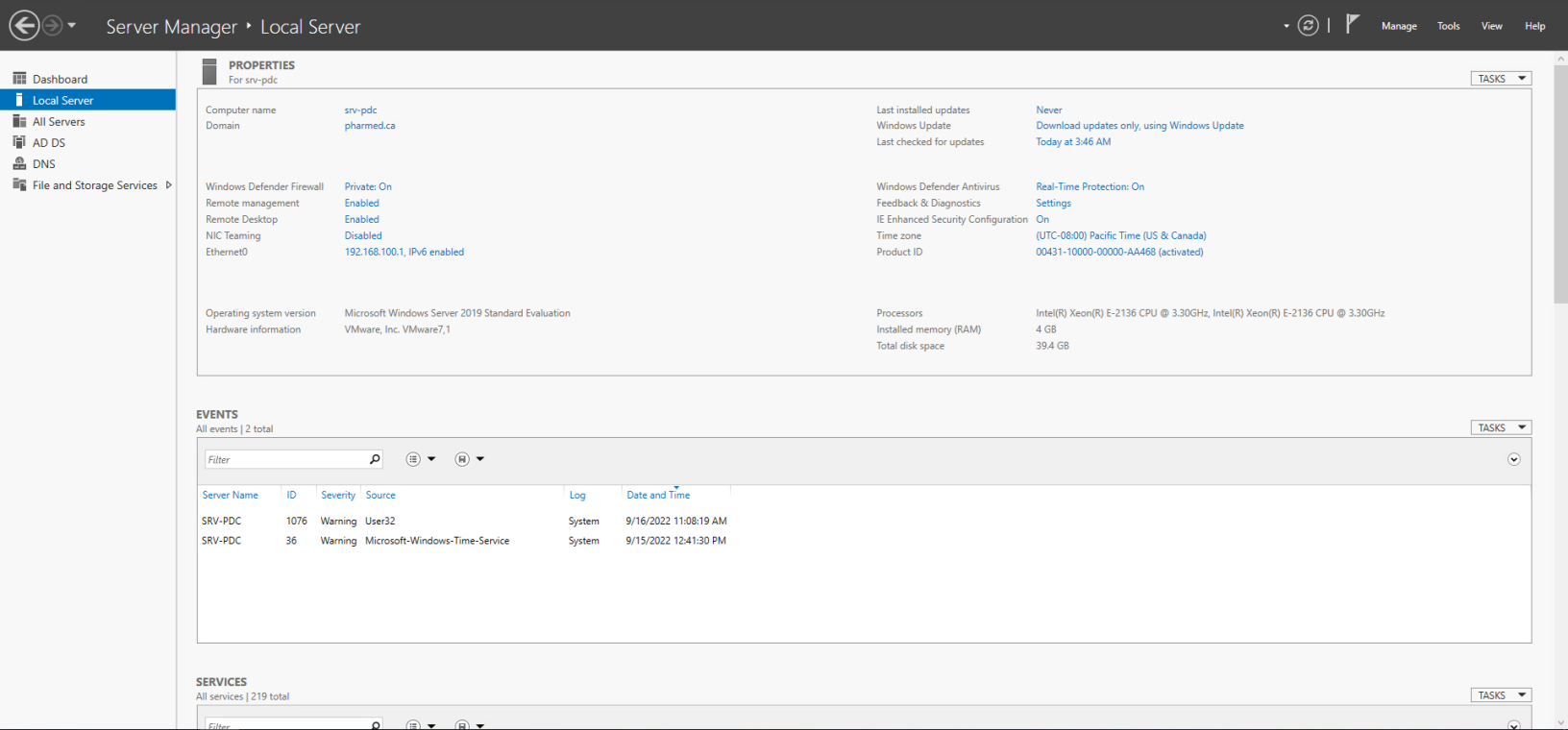
Assigned Tag	Category	Description

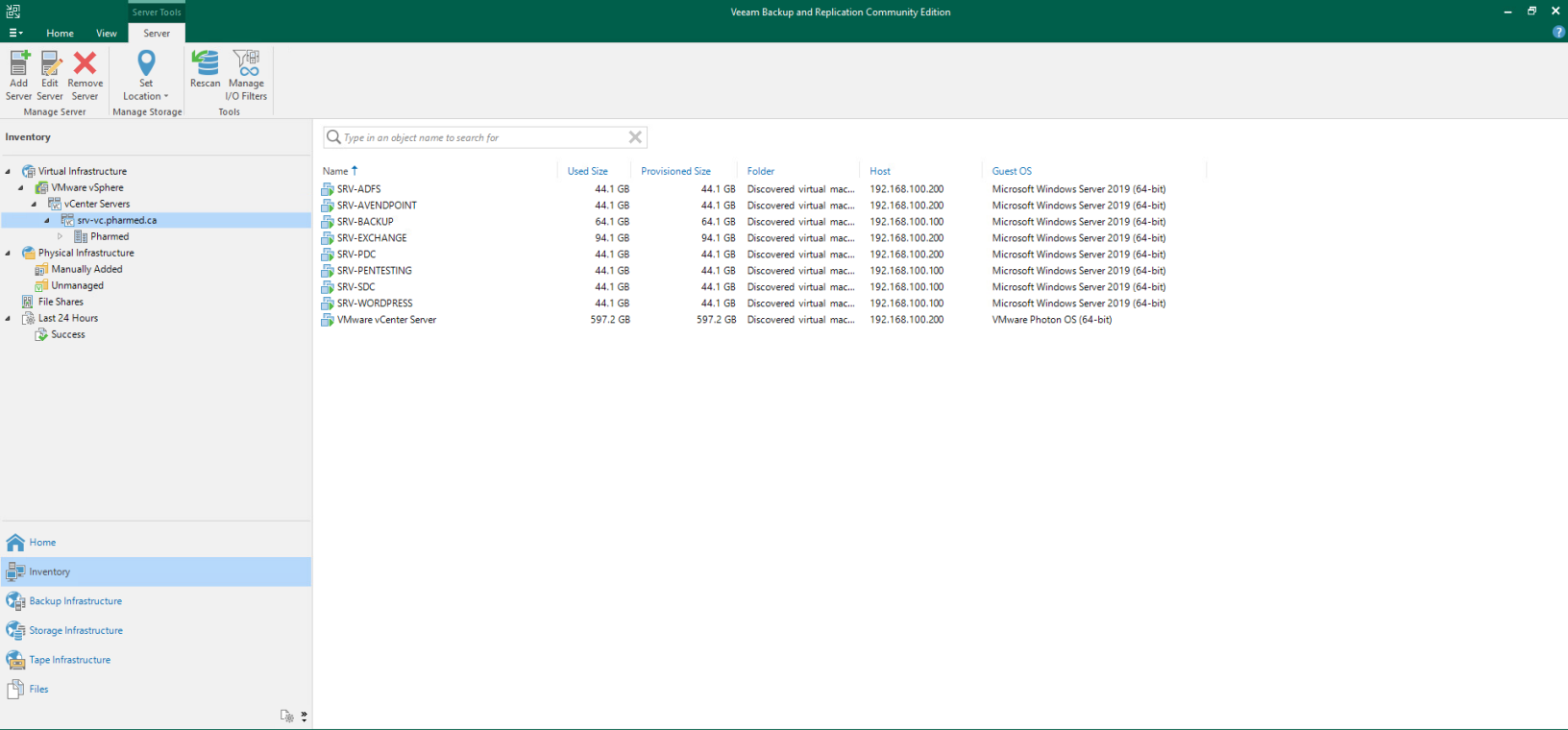
No items to display

Assign... Remove...

Cluster Resources


Server Manager ▸ DNS
Manage
Tools
View
Help
Dashboard
Local Server
All Servers
AD DS
DNS
File and Storage Services
SERVERS
All servers | 1 total
TASKS
Filter
Server Name
IPv4 Address
Manageability
Last Update
Windows Activation
SRV-PDC
192.168.100.1
Online - Performance counters not started
9/16/2022 11:48:24 AM
00431-10000-00000-AA468 (Activated)
EVENTS
All events | 1
TASKS
Filter
Server Nam
Date and Time
SRV-PDC
9/16/2022 11:34:37
SERVICES
All services |
TASKS
Filter
Server Name
Display Name
Service Name
Status
Start Type
SRV-PDC
DNS Server
DNS
Running
Automatic
NewUsers Properties
General
Members
Member Of
Managed By
Members:
Name
Active Directory Domain Services Folder
Alice
phamed.ca
Bob
phamed.ca/Users
Add...
Remove
OK
Cancel
Apply
Active Directory Users and Computers
File
Action
View
Help
Active Directory Users and Com
Saved Queries
pharmed.ca
Name
Type
Description
Alice
User
Builtin
builtinDomain
Computers
Container
Default container for up...
Domain Controllers
Organizational...
Default container for do...
ForeignSecurityPrincipals
Container
Default container for sec...
Managed Service Accounts
Container
Default container for ma...
Microsoft Exchange Security Groups
Organizational...
NewUsers
Security Group...
Users
Container
Default container for up...


Server Manager ‣ Local Server
Manage
Tools
View
Help
Dashboard
Local Server
All Servers
AD DS
DNS
File and Storage Services
PROPERTIES
For srv-pdc
TASKS
Computer name
srv-pdc
Domain
pharmed.ca
Last installed updates
Never
Windows Update
Download updates only, using Windows Update
Last checked for updates
Today at 3:46 AM
Windows Defender Firewall
Private: On
Remote management
Enabled
Remote Desktop
Enabled
NIC Teaming
Disabled
Ethernet0
192.168.100.1, IPv6 enabled
Windows Defender Antivirus
Real-Time Protection: On
Feedback & Diagnostics
Settings
IE Enhanced Security Configuration
On
Time zone
(UTC-08:00) Pacific Time (US & Canada)
Product ID
00431-10000-00000-AA468 (activated)
Operating system version
Microsoft Windows Server 2019 Standard Evaluation
Hardware information
VMware, Inc. VMware7,1
Processors
Intel(R) Xeon(R) E-2136 CPU @ 3.30GHz, Intel(R) Xeon(R) E-2136 CPU @ 3.30GHz
Installed memory (RAM)
4 GB
Total disk space
39.4 GB
EVENTS
All events | 2 total
TASKS
Filter
Server Name
ID
Severity
Source
Log
Date and Time
SRV-PDC
1076
Warning
User32
System
9/16/2022 11:08:19 AM
SRV-PDC
36
Warning
Microsoft-Windows-Time-Service
System
9/15/2022 12:41:30 PM
SERVICES
All services | 219 total
TASKS
Filter


Server Tools
Veeam Backup and Replication Community Edition
Home
View
Server
Add Server
Edit Server
Remove Server
Manage Server
Set Location
Manage Storage
Rescan
Manage I/O Filters
Tools
Inventory
Type in an object name to search for
Virtual Infrastructure
VMware vSphere
vCenter Servers
srv-vc.pharmed.ca
Pharmed
Physical Infrastructure
Manually Added
Unmanaged
File Shares
Last 24 Hours
Success
Name
Used Size
Provisioned Size
Folder
Host
Guest OS
SRV-ADFS 44.1 GB 44.1 GB Discovered virtual mac... 192.168.100.200 Microsoft Windows Server 2019 (64-bit)
SRV-AVENDPOINT 44.1 GB 44.1 GB Discovered virtual mac... 192.168.100.200 Microsoft Windows Server 2019 (64-bit)
SRV-BACKUP 64.1 GB 64.1 GB Discovered virtual mac... 192.168.100.100 Microsoft Windows Server 2019 (64-bit)
SRV-EXCHANGE 94.1 GB 94.1 GB Discovered virtual mac... 192.168.100.200 Microsoft Windows Server 2019 (64-bit)
SRV-PDC 44.1 GB 44.1 GB Discovered virtual mac... 192.168.100.200 Microsoft Windows Server 2019 (64-bit)
SRV-PENTESTING 44.1 GB 44.1 GB Discovered virtual mac... 192.168.100.100 Microsoft Windows Server 2019 (64-bit)
SRV-SDC 44.1 GB 44.1 GB Discovered virtual mac... 192.168.100.100 Microsoft Windows Server 2019 (64-bit)
SRV-WORDPRESS 44.1 GB 44.1 GB Discovered virtual mac... 192.168.100.100 Microsoft Windows Server 2019 (64-bit)
VMware vCenter Server 597.2 GB 597.2 GB Discovered virtual mac... 192.168.100.200 VMware Photon OS (64-bit)
Home
Inventory
Backup Infrastructure
Storage Infrastructure
Tape Infrastructure
Files

root
freenas.local

Dashboard
Accounts
System
Tasks
Network
Storage
Directory Services
Sharing
Services
Plugins
Jails
Reporting
Virtual Machines
Display System Processes

FreeNAS

CHECK FOR UPDATES

System Information

Overview

Platform: Generic

Version: FreeNAS-11.3-RELEASE

HostName: freenas.local

Uptime: 2:23PM up 3 days, 3:18, 0 users

CPU

Intel(R) Xeon(R) E-2136 CPU @ 3.30GHz

LOAD

0%

12
Threads

Stats Per Thread

Usage

Temperature

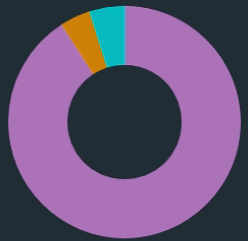
Memory

31.6GiB
total memory installed

Free: 28.1 GiB

ZFS Cache: 1.3 GiB

Services: 1.5 GiB



Pool

mypool

ONLINE

Overview

Path: /mnt/mypool

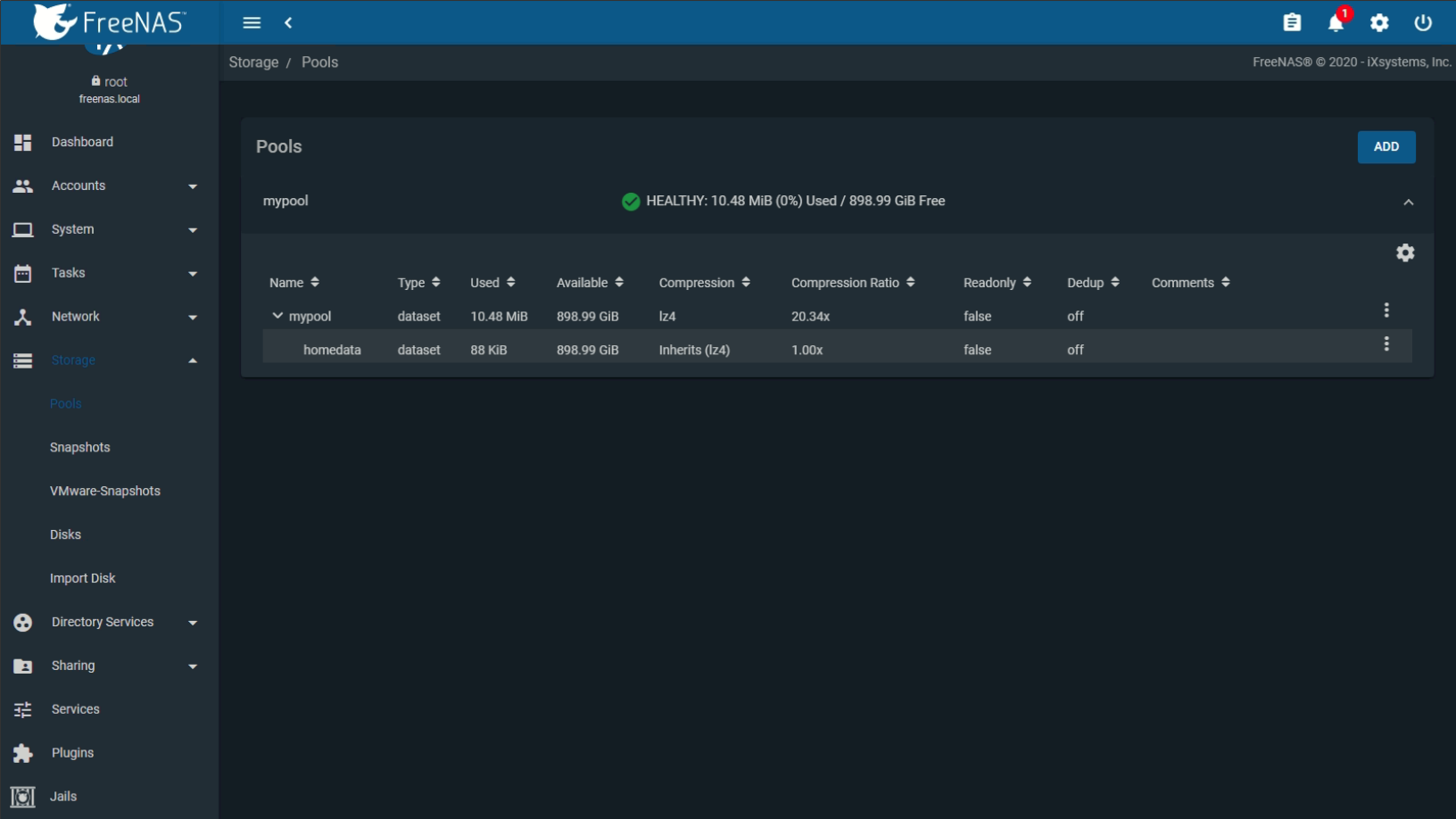
Available Space: 898.99GiB (0% used)

Data: 1 vdev

Caches: 0

Spares: 0

Logs: 0


FreeNAS
root
freenas.local
Dashboard
Accounts
System
Tasks
Network
Storage
Pools
Snapshots
VMware-Snapshots
Disks
Import Disk
Directory Services
Sharing
Services
Plugins
Jails
Storage / Pools
FreeNAS® © 2020 - iXsystems, Inc.
Pools
ADD
mypool
HEALTHY: 10.48 MiB (0%) Used / 898.99 GiB Free
Name
Type
Used
Available
Compression
Compression Ratio
Readonly
Dedup
Comments
mypool
dataset
10.48 MiB
898.99 GiB
lz4
20.34x
false
off
homedata
dataset
88 KiB
898.99 GiB
Inherits (lz4)
1.00x
false
off