Microsoft AD As Built Report

Zen PR Solutions

Author: Jonathan Colon
Date: Wednesday, January 24, 2024
Version: 1.0

DISCLAIMER

The information contained in this report has been obtained through automation and observations. Opinions, recommendations and conclusions are disseminated using insight, knowledge, training and experience. This assessment was not intended to be exhaustive. However, we have done our best to capture the most relevant opportunities for improvement. It is expected that responsibility for the implementation of these recommendations will be reviewed and implemented by a person with the necessary knowledge, experience or expertise. In no event shall the author(s) be liable for damages of any kind (including, but not limited to, damages for loss of business profits, business interruption, loss of business information, or other pecuniary loss) arising out of the use or inability to use these recommendations or the statements made in this documentation.

Table of Contents

1 PHARMAX.LOCAL

The following section provides a summary of the Active Directory Infrastructure configuration for PHARMAX.LOCAL.

1.1 Forest Configuration.

The following section provides a summary of the Active Directory Forest Information.

Forest Name	pharmax.local
Forest Functional Level	Windows2016Forest
Schema Version	ObjectVersion 88, Correspond to Windows Server 2019
Tombstone Lifetime (days)	180
Domains	acad.pharmax.local; pharmax.local; uia.local
Global Catalogs	Server-DC-01V.pharmax.local; acade-dc-01v.acad.pharmax.local; DC-UIA-01V.uia.local
Domains Count	3
Global Catalogs Count	3
Sites Count	5
Application Partitions	DC=DomainDnsZones,DC=acad,DC=pharmax,DC=local DC=ForestDnsZones,DC=pharmax,DC=local DC=DomainDnsZones,DC=uia,DC=local DC=DomainDnsZones,DC=pharmax,DC=local
PartitionsContainer	CN=Partitions,CN=Configuration,DC=pharmax,DC=local
SPN Suffixes	--
UPN Suffixes	pharmax, acad
Anonymous Access (dsHeuristics)	Disabled

Table 1 - Forest Summary - PHARMAX.LOCAL

1.1.1 Forest Diagram.

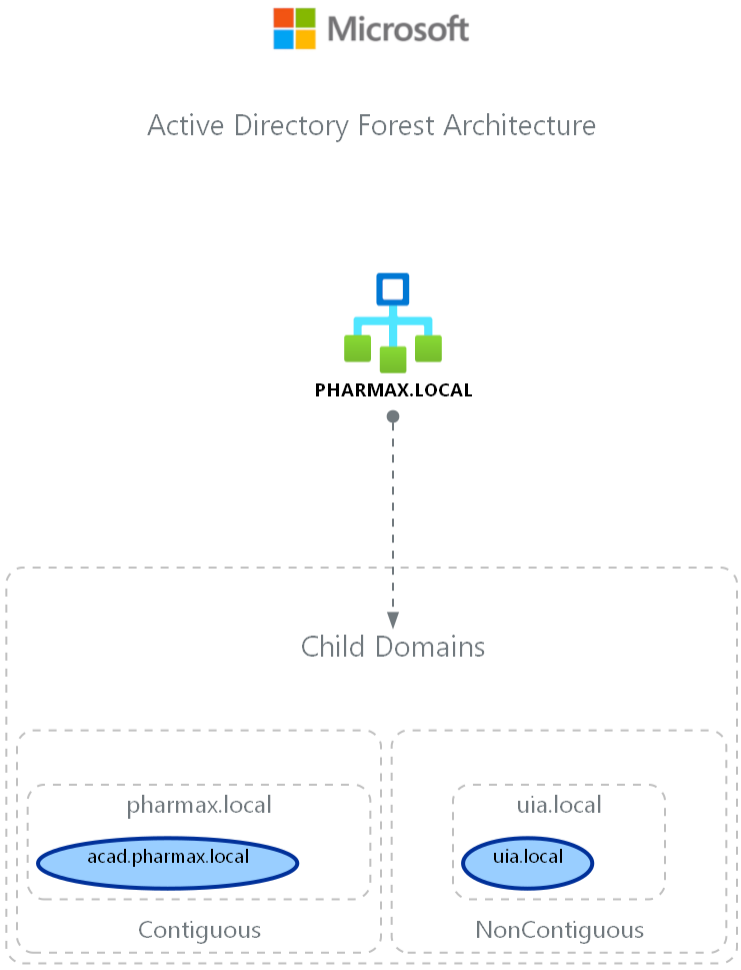


Image preview: Opens the image in a new tab to view it at full resolution.

1.1.2 Certificate Authority

The following section provides a summary of the Active Directory PKI Infrastructure Information.

Certification Authority Root(s)

Name	Distinguished Name
pharmax-SERVER-DC-01V-CA	CN=pharmax-SERVER-DC-01V-CA,CN=Certification Authorities,CN=Public Key Services,CN=Services,CN=Configuration,DC=pharmax,DC=local

Table 2 - Certificate Authority Root(s) - PHARMAX.LOCAL

Certification Authority Issuer(s)

Name	DNS Name
acad-ACADE-DC-01V-CA	acade-dc-01v.acad.pharmax.local
pharmax-CAYEY-DC-01V-CA	cayey-dc-01v.pharmax.local
pharmax-SERVER-DC-01V-CA	Server-DC-01V.pharmax.local

Table 3 - Certificate Authority Issuer(s) - PHARMAX.LOCAL

1.1.3 Optional Features

Name	Required Forest Mode	Enabled
Privileged Access Management Feature	Windows2016Forest	No
Recycle Bin Feature	Windows2008R2Forest	Yes

Table 4 - Optional Features - PHARMAX.LOCAL

1.1.4 Sites

Site Name	Description	Subnets	Domain Controllers
ACAD	--	172.23.4.0/24	ACADE-DC-01V
Cayey-Branch	Site of Cayey, PR Branch	10.10.0.0/16	CAYEY-DC-01V
Dead-Site	--	No subnet assigned	No DC assigned
Pharmax-HQ	Site of San Juan, PR HQ	192.168.7.0/24 192.168.5.0/24 10.9.1.0/24	SERVER-DC-01V
UIA	--	172.23.7.0/24	DC-UIA-01V

Table 5 - Sites - PHARMAX.LOCAL

Health Check:

Corrective Actions: Ensure Sites have an associated subnet. If subnets are not associated with AD Sites users in the AD Sites might choose a remote domain controller for authentication which in turn might result in excessive use of a remote domain controller.

Best Practice: It is a general rule of good practice to establish well-defined descriptions. This helps to speed up the fault identification process, as well as enabling better documentation of the environment.

Connection Objects

Name	From Server	To Server	From Site
<automatically generated>	ACADE-DC-01V	CAYEY-DC-01V	ACAD
<automatically generated>	ACADE-DC-01V	DC-UIA-01V	ACAD
<automatically generated>	ACADE-DC-01V	SERVER-DC-01V	ACAD
<automatically generated>	CAYEY-DC-01V	ACADE-DC-01V	Cayey-Branch
CAYEY-DC-01V	CAYEY-DC-01V	SERVER-DC-01V	Cayey-Branch
<automatically generated>	CAYEY-DC-01V	DC-UIA-01V	Cayey-Branch
<automatically generated>	SERVER-DC-01V	DC-UIA-01V	Pharmax-HQ
<automatically generated>	SERVER-DC-01V	ACADE-DC-01V	Pharmax-HQ
<automatically generated>	SERVER-DC-01V	CAYEY-DC-01V	Pharmax-HQ
<automatically generated>	DC-UIA-01V	ACADE-DC-01V	UIA
<automatically generated>	DC-UIA-01V	SERVER-DC-01V	UIA

Table 6 - Connection Objects - PHARMAX.LOCAL

Health Check:

Best Practice: By default, the replication topology is managed automatically and optimizes existing connections. However, manual connections created by an administrator are not modified or optimized. Verify that all topology information is entered for Site Links and delete all manual connection objects.

1.1.4.1 Site Subnets

Subnet	Description	Sites
10.10.0.0/16	Cayey-Networks	Cayey-Branch
10.9.1.0/24	--	Pharmax-HQ
172.23.4.0/24	--	ACAD
172.23.7.0/24	--	UIA
192.168.5.0/24	--	Pharmax-HQ
192.168.7.0/24	--	Pharmax-HQ

Subnet	Description	Sites
25.25.25.0/24	--	No site assigned

Table 7 - Site Subnets - PHARMAX.LOCAL

Health Check:

Best Practice: It is a general rule of good practice to establish well-defined descriptions. This helps to speed up the fault identification process, as well as enabling better documentation of the environment.

Corrective Actions: Ensure Subnet have an associated site. If subnets are not associated with AD Sites users in the AD Sites might choose a remote domain controller for authentication which in turn might result in excessive use of a remote domain controller.

Missing Subnets in AD

The following table list the NO_CLIENT_SITE entries found in the netlogon.log file at each DC in the forest.

DC	IP
cayey-dc-01v.pharmax.local	172.23.4.1
cayey-dc-01v.pharmax.local	172.23.9.11
cayey-dc-01v.pharmax.local	192.168.13.10

Table 8 - Missing Subnets - PHARMAX.LOCAL

Health Check:

Corrective Actions: Make sure that all the subnets at each Site are properly defined. Missing subnets can cause clients to not use the site's local DCs.

1.1.4.2 Site Links

Site Link Name	Pharmax-to-All
Cost	100
Replication Frequency	15 min
Transport Protocol	IP
Options	Change Notification is Disabled
Sites	UIA; Dead-Site; ACAD; Cayey-Branch; Pharmax-HQ
Protected From Accidental Deletion	No
Description	From Pharmax Forest to all Domains

Table 9 - Site Links - Pharmax-to-All

Health Check:

Best Practice: Enabling change notification treats an INTER-site replication connection like an INTRA-site connection. Replication between sites with change notification is almost instant. Microsoft recommends using an Option number value of 5 (Change Notification is Enabled without Compression).

Best Practice: If the Site Links in your Active Directory are not protected from accidental deletion, your environment can experience disruptions that might be caused by accidental bulk deletion of objects.

Site Link Name	PHARMAX-to-ACAD
Cost	100
Replication Frequency	15 min
Transport Protocol	IP
Options	(1)Change Notification is Enabled with Compression
Sites	ACAD; Pharmax-HQ
Protected From Accidental Deletion	Yes
Description	--

Table 10 - Site Links - PHARMAX-to-ACAD

Health Check:

Best Practice: It is a general rule of good practice to establish well-defined descriptions. This helps to speed up the fault identification process, as well as enabling better documentation of the environment.

1.1.4.3 Sysvol Replication

DC Name	Replication Status	Domain
acade-dc-01v	Normal	acad.pharmax.local
cayey-dc-01v		pharmax.local
Server-DC-01V	In error state	pharmax.local
DC-UIA-01V	Normal	uia.local

Table 11 - Sysvol Replication - UIA.LOCAL

Health Check:

Corrective Actions: SYSVOL is a special directory that resides on each domain controller (DC) within a domain. The directory comprises folders that store Group Policy objects (GPOs) and logon scripts that clients need to access and synchronize between DCs. For these logon scripts and GPOs to function properly, SYSVOL should be replicated accurately and rapidly throughout the domain. Ensure that proper SYSVOL replication is in place to ensure identical GPO/SYSVOL content for the domain controller across all Active Directory domains.

1.1.5 Exchange Infrastructure

The following section provides a summary of the Exchange Infrastructure configured on Active Directory.

EX16-SERVER-01V

Name	EX16-SERVER-01V
Dns Name	ex16-server-01v.pharmax.local
Server Roles	UM, CAS, MBX, HUB
Version	Version 15.1 (Build 32507.6)

Table 12 - Exchange Infrastructure - EX16-SERVER-01V

2 AD Domain Configuration

The following section provides a summary of the Active Directory Domain Information.

2.1 PHARMAX.LOCAL

The following section provides a summary of the Active Directory Domain Information.

Domain Name	pharmax
NetBIOS Name	PHARMAX
Domain SID	S-1-5-21-2867495315-1194516362-180967319
Domain Functional Level	Windows2016Domain
Domains	--
Forest	pharmax.local
Parent Domain	--
Replica Directory Servers	Server-DC-01V.pharmax.local cayey-dc-01v.pharmax.local
Child Domains	acad.pharmax.local
Domain Path	pharmax.local/
Computers Container	pharmax.local/Computers
Domain Controllers Container	pharmax.local/Domain Controllers
Systems Container	pharmax.local/System
Users Container	pharmax.local/Users
ReadOnly Replica Directory Servers	--
ms-DS-MachineAccountQuota	10
RID Issued/Available	351600 / 1073390223 (1% Issued)

Table 13 - Domain Summary - PHARMAX.LOCAL

2.1.1 FSMO Roles

Infrastructure Master	Server-DC-01V.pharmax.local
RID Master	Server-DC-01V.pharmax.local
PDC Emulator Name	Server-DC-01V.pharmax.local
Domain Naming Master	Server-DC-01V.pharmax.local
Schema Master	Server-DC-01V.pharmax.local

Table 14 - FSMO Roles - pharmax.local

Health Check:

Best Practice: The infrastructure master role in the domain PHARMAX.LOCAL should be held by a domain controller that is not a global catalog server. This issue does not affect forests that have a single domain.

Reference: http://go.microsoft.com/fwlink/?LinkId=168841

2.1.2 Domain and Trusts

acad.pharmax.local

Name	acad.pharmax.local
Path	pharmax.local/System/acad.pharmax.local
Source	pharmax
Target	acad.pharmax.local
Direction	BiDirectional
IntraForest	Yes
Selective Authentication	No
SID Filtering Forest Aware	No
SID Filtering Quarantined	No
Trust Type	Uplevel
Uplevel Only	No

Table 15 - Trusts - acad.pharmax.local

uia.local

Name	uia.local
Path	pharmax.local/System/uia.local
Source	pharmax
Target	uia.local
Direction	BiDirectional
IntraForest	Yes
Selective Authentication	No
SID Filtering Forest Aware	No
SID Filtering Quarantined	No
Trust Type	Uplevel

Uplevel Only	No

Table 16 - Trusts - uia.local

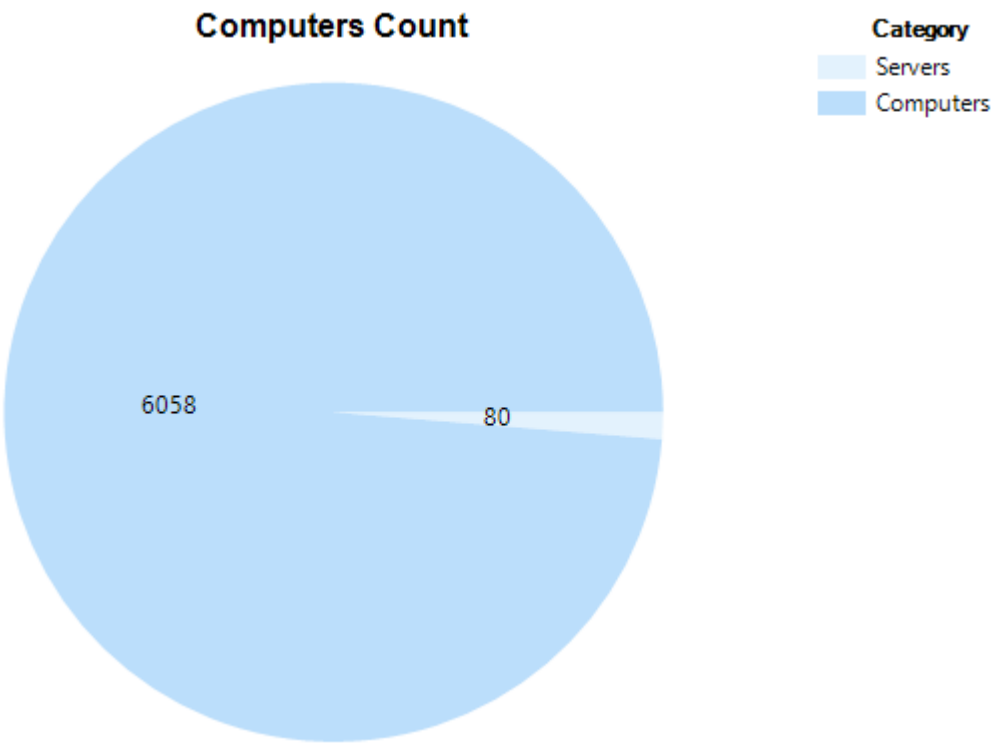
lab.local

Name	lab.local
Path	pharmax.local/System/lab.local
Source	pharmax
Target	lab.local
Direction	BiDirectional
IntraForest	No
Selective Authentication	No
SID Filtering Forest Aware	No
SID Filtering Quarantined	No
Trust Type	Uplevel
Uplevel Only	No

Table 17 - Trusts - lab.local

2.1.3 Domain Object Stats

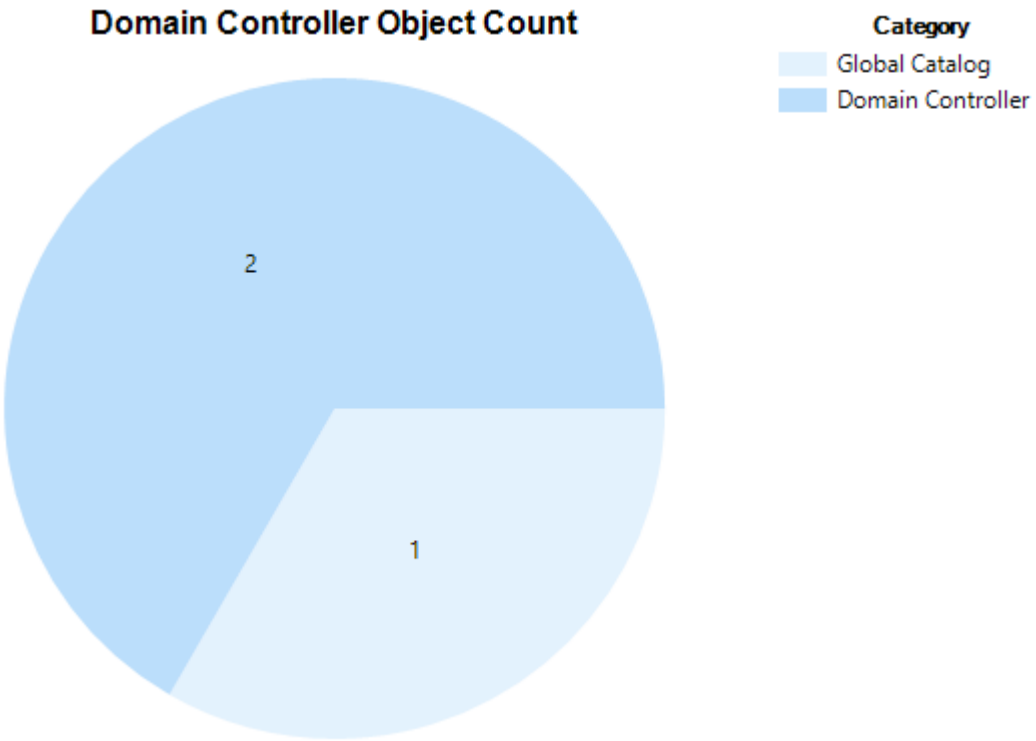
Computers



Computers	6058
Servers	80

Table 18 - Computers - PHARMAX.LOCAL

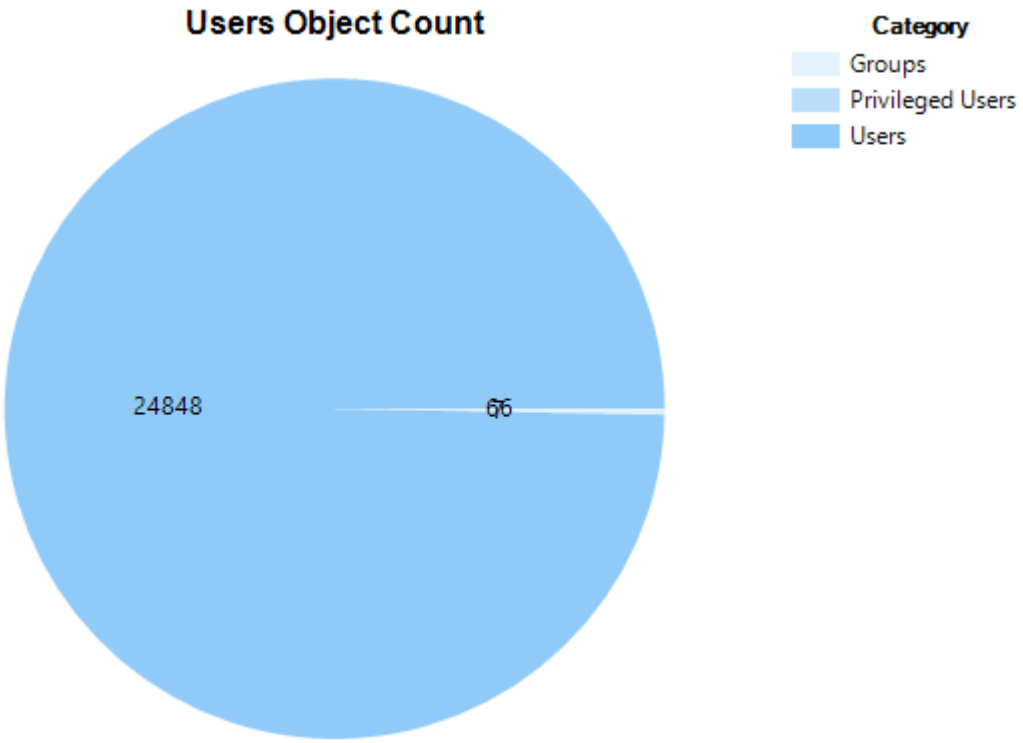
Domain Controller



Domain Controller	2
Global Catalog	1

Table 19 - Domain Controller - PHARMAX.LOCAL

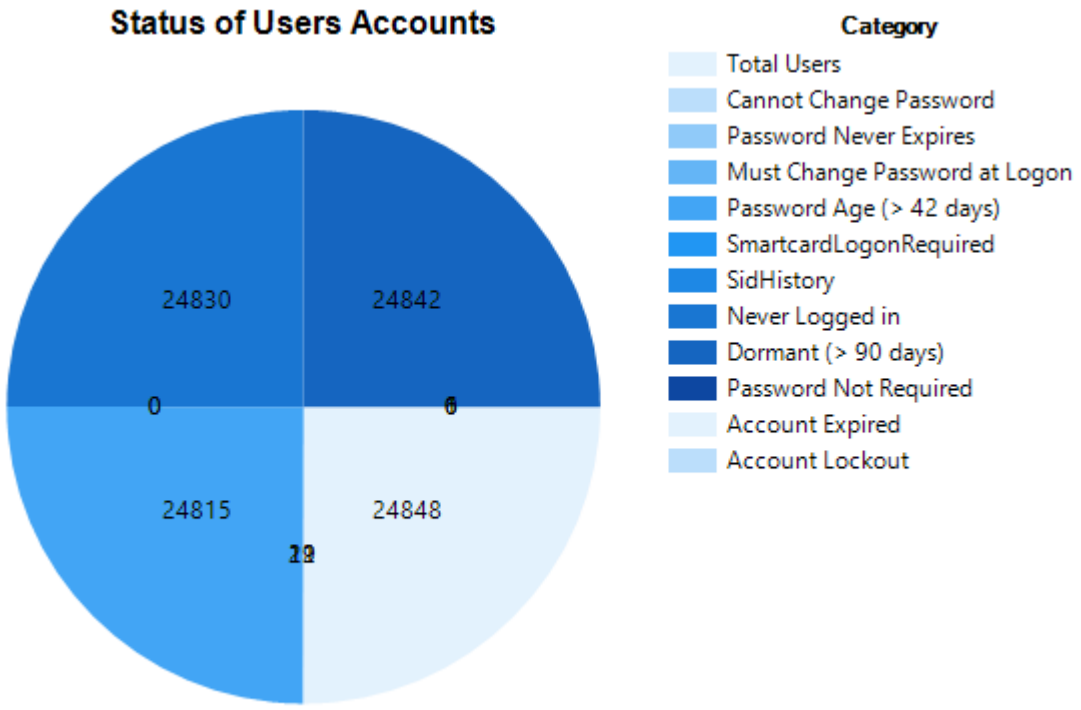
Users



Users	24848
Privileged Users	7
Groups	66

Table 20 - User - PHARMAX.LOCAL

2.1.4 Status of Users Accounts



Category	Enabled	Enabled %	Disabled	Disabled %	Total	Total %
Total Users	24835	99.95	13	0.05	24848	100
Cannot Change Password	11	0.04	0	0	11	0.04
Password Never Expires	27	0.11	2	0.01	29	0.12
Must Change Password at Logon	0	0	12	0.05	12	0.05
Password Age (> 42 days)	24805	99.83	10	0.04	24815	99.87
SmartcardLogonRequired	1	0	1	0	0	0
SidHistory	1	0	1	0	0	0
Never Logged in	24817	99.88	13	0.05	24830	99.93
Dormant (> 90 days)	24829	99.92	13	0.05	24842	99.98
Password Not Required	3	0.01	3	0.01	6	0.02
Account Expired	1	0	1	0	1	0
Account Lockout	1	0	1	0	0	0

Table 21 - Status of User Accounts - PHARMAX.LOCAL

2.1.5 Privileged Groups

The following session details the members users within the privilege groups.

Domain Admins (3 Members)

Name	Last Logon Date	Password Never Expires	Account Enabled
Administrator	12/10/2053	**Yes	Yes
jocolon	12/22/2043	**Yes	Yes
veeam_admin	12/26/2023	**Yes	Yes

Table 22 - Domain Admins - PHARMAX.LOCAL

Health Check:

Security Best Practice:

**Ensure there aren't any account with weak security posture.

Enterprise Admins (2 Members)

Name	Last Logon Date	Password Never Expires	Account Enabled
Administrator	12/10/2053	**Yes	Yes
jocolon	12/22/2043	**Yes	Yes

Table 23 - Enterprise Admins - PHARMAX.LOCAL

Health Check:

Security Best Practice:

Unless an account is doing specific tasks needing those highly elevated permissions, every account should be removed from Enterprise Admins (EA) group. A side benefit of having an empty Enterprise Admins group is that it adds just enough friction to ensure that enterprise-wide changes requiring Enterprise Admin rights are done purposefully and methodically.

**Ensure there aren't any account with weak security posture.

Administrators (4 Members)

Name	Last Logon Date	Password Never Expires	Account Enabled
Administrator	12/10/2053	**Yes	Yes
jocolon	12/22/2043	**Yes	Yes
svc_SCCM_ClientPush	*9/14/2020	**Yes	Yes
veeam_admin	12/26/2023	**Yes	Yes

Table 24 - Administrators - PHARMAX.LOCAL

Health Check:

Security Best Practice:

**Ensure there aren't any account with weak security posture.

*Regularly check for and remove inactive privileged user accounts in Active Directory.

Schema Admins (2 Members)

Name	Last Logon Date	Password Never Expires	Account Enabled
1227935471SA	--	No	Yes
Administrator	12/10/2053	**Yes	Yes

Table 25 - Schema Admins - PHARMAX.LOCAL

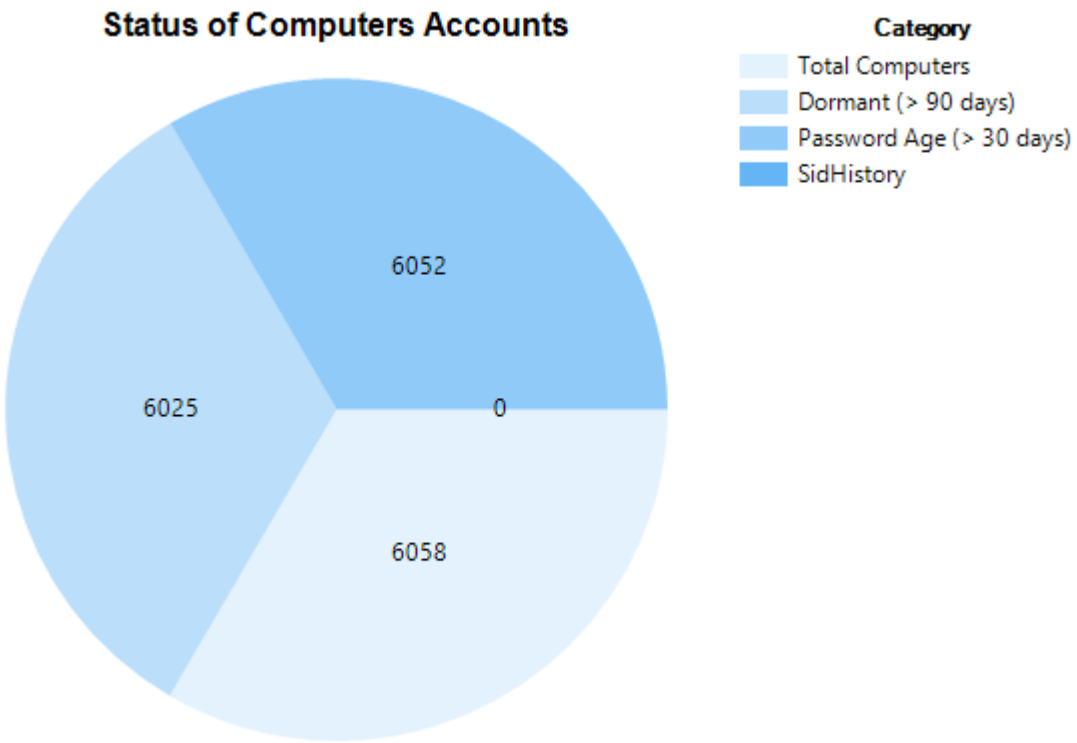
Health Check:

Security Best Practice:

The Schema Admins group is a privileged group in a forest root domain. Members of the Schema Admins group can make changes to the schema, which is the framework for the Active Directory forest. Changes to the schema are not frequently required. This group only contains the Built-in Administrator account by default. Additional accounts must only be added when changes to the schema are necessary and then must be removed.

**Ensure there aren't any account with weak security posture.

2.1.6 Status of Computer Accounts



Category	Enabled	Enabled %	Disabled	Disabled %	Total	Total %
Total Computers	6037	99.65	21	0.35	6058	100
Dormant (> 90 days)	6004	99.11	21	0.35	6025	99.46
Password Age (> 30 days)	6031	99.55	21	0.35	6052	99.9
SidHistory	1	0.02	1	0.02	0	0

Table 26 - Status of Computer Accounts - PHARMAX.LOCAL

2.1.7 Operating Systems Count

Operating System	Count
CentOS	1
Data Domain OS	1
EMC File Server	1
NetApp Release 9.5P6	1
NetApp Release 9.8	1
NetApp Release 9.8P7	1
NetApp Release 9.9.1P1	3
No OS Specified	5939
OneFS	1
pc-linux-gnu	2
redhat-linux-gnu	2
unknown	2
Windows 10 Education	1
Windows 10 Enterprise	1
Windows 10 Enterprise Evaluation	19
Windows Server 2003	1
Windows Server 2016 Standard Evaluation	11
Windows Server 2019 Standard	1
Windows Server 2019 Standard Evaluation	43
Windows Server 2022 Datacenter	3
Windows Server 2022 Datacenter Evaluation	21
Windows Vista	1
Windows XP	1

Table 27 - Operating System Count - PHARMAX.LOCAL

Health Check:

Security Best Practice: Operating systems that are no longer supported for security updates are not maintained or updated for vulnerabilities leaving them open to potential attack. Organizations must transition to a supported operating system to ensure continued support and to increase the organization security posture

2.1.8 Default Domain Password Policy

Password Must Meet Complexity Requirements	Yes
Path	pharmax.local/
Lockout Duration	30 minutes
Lockout Threshold	5
Lockout Observation Window	30 minutes
Max Password Age	42 days
Min Password Age	01 days
Min Password Length	7
Enforce Password History	24
Store Password using Reversible Encryption	No

Table 28 - Default Domain Password Policy - PHARMAX.LOCAL

2.1.9 Fined Grained Password Policies

Administrators

Name	Administrators
Domain Name	pharmax.local
Complexity Enabled	Yes
Path	pharmax.local/System/Password Settings Container/Administrators
Lockout Duration	30 minutes
Lockout Threshold	0
Lockout Observation Window	30 minutes
Max Password Age	42 days
Min Password Age	05 days
Min Password Length	12
Password History Count	90
Reversible Encryption Enabled	No
Precedence	1
Applies To	horizon-ic, dbuser, jocolon

Table 29 - Fined Grained Password Policies - Administrators

Test

Name	Test
Domain Name	pharmax.local
Complexity Enabled	Yes

Path	pharmax.local/System/Password Settings Container/Test
Lockout Duration	30 minutes
Lockout Threshold	0
Lockout Observation Window	30 minutes
Max Password Age	42 days
Min Password Age	01 days
Min Password Length	7
Password History Count	23
Reversible Encryption Enabled	No
Precedence	1
Applies To	vmuserro

Table 30 - Fined Grained Password Policies - Test

2.1.10 Windows LAPS

Name	ms-Mcs-AdmPwd
Domain Name	pharmax.local
Enabled	Yes
Distinguished Name	CN=ms-Mcs-AdmPwd,CN=Schema,CN=Configuration,DC=pharmax,DC=local

Table 31 - Windows LAPS - PHARMAX.LOCAL

2.1.11 gMSA Identities

SQLServer

Name	SQLServer
SamAccountName	SQLServer$
Created	9/27/2020
Enabled	Yes
DNS Host Name	SQL-Cluster
Host Computers	SQL-CLUSTER-02V, SQL-CLUSTER-01V
Retrieve Managed Password	SQL-CLUSTER-01V, SQL-CLUSTER-02V
Primary Group	Domain Computers
Last Logon Date	*9/27/2020
Locked Out	No
Logon Count	3
Password Expired	No
Password Last Set	9/27/2020

Table 32 - gMSA - SQLServer

Health Check:

Security Best Practice:

*Regularly check for and remove inactive group managed service accounts from Active Directory.

adfsgmsa

Name	adfsgmsa
SamAccountName	adfsgmsa$
Created	10/7/2020
Enabled	Yes
DNS Host Name	ADFS.pharmax.local
Host Computers	**--
Retrieve Managed Password	SERVER-ADFS-01V, SERVER-ADFS-02V
Primary Group	Domain Computers
Last Logon Date	*10/7/2020
Locked Out	No
Logon Count	40
Password Expired	No
Password Last Set	10/7/2020

Table 33 - gMSA - adfsgmsa

Health Check:

Security Best Practice:

*Regularly check for and remove inactive group managed service accounts from Active Directory.

**No 'Host Computers' has been defined, please validate that the gMSA is currently in use. If not, it is recommended to remove these unused resources from Active Directory.

ITFarm1

Name	ITFarm1
SamAccountName	ITFarm1$
Created	7/13/2023
Enabled	Yes
DNS Host Name	ITFarm1.pharmax.local
Host Computers	**--
Retrieve Managed Password	***--
Primary Group	Domain Computers
Last Logon Date	*--
Locked Out	No
Logon Count	0

Password Expired	No
Password Last Set	7/13/2023

Table 34 - gMSA - ITFarm1

Health Check:

Security Best Practice:

*Regularly check for and remove inactive group managed service accounts from Active Directory.

**No 'Host Computers' has been defined, please validate that the gMSA is currently in use. If not, it is recommended to remove these unused resources from Active Directory.

***No 'Retrieve Managed Password' has been defined, please validate that the gMSA is currently in use. If not, it is recommended to remove these unused resources from Active Directory.

2.1.12 Health Checks

Naming Context Last Backup

The following section details naming context last backup time for Domain PHARMAX.LOCAL.

Naming Context	Last Backup	Last Backup in Days
CN=Configuration,DC=pharmax,DC=local	2023:12:16	38
CN=Schema,CN=Configuration,DC=pharmax,DC=local	2023:12:16	38
DC=DomainDnsZones,DC=pharmax,DC=local	2023:12:16	38
DC=ForestDnsZones,DC=pharmax,DC=local	2023:12:16	38
DC=pharmax,DC=local	2023:12:16	38

Table 35 - Naming Context Last Backup - PHARMAX.LOCAL

Sysvol Replication Status

The following section details the sysvol folder replication status for Domain PHARMAX.LOCAL.

DC Name	Replication Status	GPO Count	Sysvol Count	Identical Count	Stop Replication On AutoRecovery
CAYEY-DC-01V		17	15	No	No
SERVER-DC-01V	In error state	17	17	Yes	No

Table 36 - Sysvol Replication Status - PHARMAX.LOCAL

Health Check:

Corrective Actions: SYSVOL is a special directory that resides on each domain controller (DC) within a domain. The directory comprises folders that store Group Policy objects (GPOs) and logon scripts that

clients need to access and synchronize between DCs. For these logon scripts and GPOs to function properly, SYSVOL should be replicated accurately and rapidly throughout the domain. Ensure that proper SYSVOL replication is in place to ensure identical GPO/SYSVOL content for the domain controller across all Active Directory domains.

Sysvol Content Status

The following section details domain PHARMAX.LOCAL sysvol health status.

Extension	File Count	Size
.aas	4	0.16 MB
.adm	4	0.05 MB
.adml	4684	75.08 MB
.admx	222	3.83 MB
.cmd	1	0.00 MB
.cmt	1	0.00 MB
.cmtx	6	0.00 MB
.config	7	0.03 MB
.dll	10	12.22 MB
.exe	18	85.80 MB
.inf	9	0.01 MB
.INI	18	0.01 MB
.msi	3	150.78 MB
.pol	15	0.03 MB
.ps1	2	0.02 MB
.xml	4	0.01 MB
.zip	5	143.60 MB

Table 37 - Sysvol Content Status - PHARMAX.LOCAL

Health Check:

Corrective Actions: Make sure Sysvol folder has no malicious extensions or unnecessary content.

Netlogon Content Status

The following section details domain PHARMAX.LOCAL netlogon health status.

Extension	File Count	Size
.adm	1	0.01 MB
.adml	1	0.03 MB
.admx	1	0.02 MB
.cmd	1	0.00 MB
.config	7	0.03 MB
.dll	10	12.22 MB

Extension	File Count	Size
.exe	18	85.80 MB
.ini	1	0.01 MB
.msi	3	150.78 MB
.ps1	2	0.02 MB
.xml	1	0.00 MB
.zip	5	143.60 MB

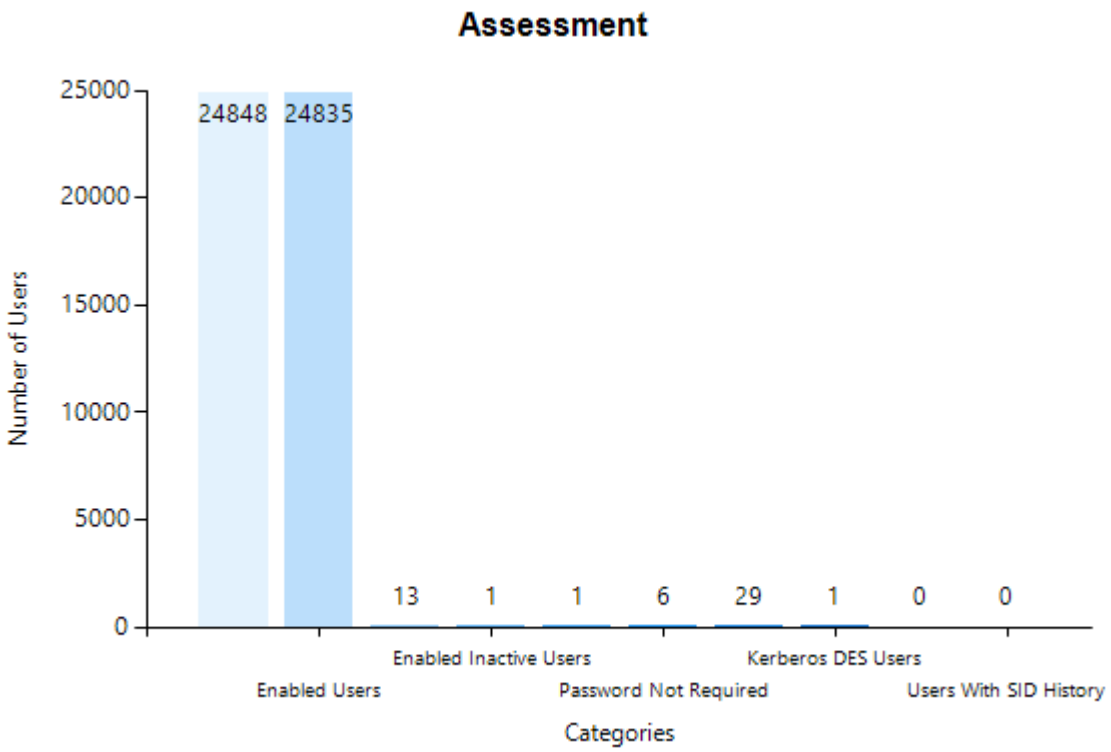
Table 38 - Netlogon Content Status - PHARMAX.LOCAL

Health Check:

Corrective Actions: Make sure Netlogon folder has no malicious extensions or unnecessary content.

Account Security Assessment

The following section provide a summary of the Account Security Assessment on Domain PHARMAX.LOCAL.



Total Users	24848
Enabled Users	24835
Disabled Users	13
Enabled Inactive Users	1
Users With Reversible Encryption Password	1

Password Not Required	6
Password Never Expires	29
Kerberos DES Users	1
Does Not Require Pre Auth	0
Users With SID History	0

Table 39 - Account Security Assessment - PHARMAX.LOCAL

Health Check:

Corrective Actions: Ensure there aren't any account with weak security posture.

Privileged Users Assessment

The following section details probable AD Admin accounts (user accounts with AdminCount set to 1) on Domain PHARMAX.LOCAL

Username	Created	Password Last Set	Last Logon Date
krbtgt	6/10/2018	6/10/2018	--
Administrator	6/10/2018	6/10/2018	12/10/2053
jocolon	12/4/2019	11/30/2021	12/22/2043
veeam_admin	12/13/2019	12/13/2019	12/26/2023
svc_SCCM_ClientPush	9/12/2020	9/12/2020	9/14/2020
1227935471SA	5/28/2023	5/28/2023	--
GERARDO_RICE	5/29/2023	5/29/2023	--

Table 40 - Privileged User Assessment - PHARMAX.LOCAL

Health Check:

Corrective Actions: Ensure there aren't any account with weak security posture.

Inactive Privileged Accounts

The following section details privileged accounts with the following filter (LastLogonDate >=30 days and PasswordLastSet >= 365 days) on Domain PHARMAX.LOCAL

Username	Created	Password Last Set	Last Logon Date
svc_SCCM_ClientPush	9/12/2020	9/12/2020	9/14/2020

Table 41 - Inactive Privileged Accounts - PHARMAX.LOCAL

Health Check:

Corrective Actions: Unused or underutilized accounts in highly privileged groups, outside of any break-glass emergency accounts like the default Administrator account, should have their AD Admin privileges removed.

Service Accounts Assessment

The following section details probable AD Service Accounts (user accounts with SPNs) on Domain PHARMAX.LOCAL

Username	Enabled	Password Last Set	Last Logon Date	Service Principal Name
vcenter	Yes	12/13/2019	12/13/2019	CIFS/ACAD-DNS-01V
DOYLE_BERG	Yes	5/28/2023	--	CIFS/OGCWVIR1000579
svc_SCCM_ClientPush	Yes	9/12/2020	9/14/2020	CIFS/VEEAM-HV-01
krbtgt	No	6/10/2018	--	CIFS/VEEAM-VBR-01V kadmin/changepw
srmrecadmin	Yes	10/25/2021	--	ftp/VEEAM-EM
horizon-ic	Yes	7/13/2023	12/14/2023	https/GOOWLPT1000001
8383246605SA	Yes	5/28/2023	--	kafka/AWSWCTRX1000046
LES_HYDE	Yes	5/28/2023	--	MSSQL/ESMWAPPS1000358
** GERARDO_RICE	Yes	5/29/2023	--	POP3/SECWVIR1000255
** Administrator	Yes	6/10/2018	12/10/2053	VeeamCdpSvc/VEEAM-VBR VeeamCdpSvc/VEEAM-VBR.pharmax.local VeeamCloudConnectSvc/VEEAM-VBR VeeamCloudConnectSvc/VEEAM-VBR.pharmax.local VeeamBackupSvc/VEEAM-VBR VeeamBackupSvc/VEEAM-VBR.pharmax.local VeeamCatalogSvc/VEEAM-VBR VeeamCatalogSvc/VEEAM-VBR.pharmax.local VeeamEnterpriseManagerSvc/VEEAM-EM VeeamEnterpriseManagerSvc/VEEAM-EM.pharmax.local VeeamCatalogSvc/VEEAM-EM VeeamCatalogSvc/VEEAM-EM.pharmax.local

Table 42 - Service Accounts Assessment - PHARMAX.LOCAL

Health Check:

Security Best Practice: **Attackers are most interested in Service Accounts that are members of highly privileged groups like Domain Admins. A quick way to check for this is to enumerate all user accounts with the attribute AdminCount equal to 1. This means an attacker may just ask AD for all user

accounts with a SPN and with AdminCount=1. Ensure that there are no privileged accounts that have SPNs assigned to them.

Unconstrained Kerberos Delegation

The following section provide a summary of unconstrained kerberos delegation on Domain PHARMAX.LOCAL.

Name	Distinguished Name
HV-SERVER-01V	CN=HV-SERVER-01V,OU=Member Servers,DC=pharmax,DC=local

Table 43 - Unconstrained Kerberos Delegation - PHARMAX.LOCAL

Health Check:

Corrective Actions: Ensure there aren't any unconstrained kerberos delegation in Active Directory.

KRBTGT Account Audit

The following section provide a summary of KRBTGT account on Domain PHARMAX.LOCAL.

Name	krbtgt
Created	06/10/2018 21:00:49
Password Last Set	06/10/2018 21:00:49
Distinguished Name	CN=krbtgt,CN=Users,DC=pharmax,DC=local

Table 44 - KRBTGT Account Audit - PHARMAX.LOCAL

Health Check:

Best Practice: Microsoft advises changing the krbtgt account password at regular intervals to keep the environment more secure.

Administrator Account Audit

The following section provide a summary of Administrator account on Domain PHARMAX.LOCAL.

Name	Administrator
Created	06/10/2018 21:00:05
Password Last Set	06/10/2018 04:01:50
Last Logon Date	12/10/2053 19:01:07
Distinguished Name	CN=Administrator,CN=Users,DC=pharmax,DC=local

Table 45 - Administrator Account Audit - PHARMAX.LOCAL

Health Check:

Best Practice: Microsoft advises changing the administrator account password at regular intervals to keep the environment more secure.

Duplicate Objects

The following section details Duplicate Objects discovered on Domain PHARMAX.LOCAL.

Name	Created	Changed	Conflict Changed
SCCM-DP-01V-Remote-Installation-Services CNF:0b206bf4-6c39-47b2-bd69-3694aa657d76	2020:09:13	2020:09:13	2020:09:13

Table 46 - Duplicate Object - PHARMAX.LOCAL

Health Check:

Corrective Actions: Ensure there aren't any duplicate object.

2.1.13 Domain Controllers

The following section provides a summary of the Active Directory Domain Controllers.

DC Name	Domain Name	Site	Global Catalog	Read Only	IP Address
SERVER-DC-01V	pharmax.local	Pharmax-HQ	Yes	No	192.168.5.1

Table 47 - Domain Controllers - PHARMAX.LOCAL

Health Check:

Best Practice: All domains should have at least two functioning domain controllers for redundancy. In the event of a failure on the domain's only domain controller, users will not be able to log in to the domain or access domain resources.

2.1.13.1 Hardware Inventory

The following section provides detailed Domain Controller hardware information for domain PHARMAX.LOCAL.

CAYEY-DC-01V

Name	CAYEY-DC-01V
Windows Product Name	Windows Server 2019 Standard Evaluation
Windows Build Number	10.0.17763
AD Domain	pharmax.local
Windows Installation Date	09/03/2021 20:36:55
Time Zone	(UTC-04:00) Georgetown, La Paz, Manaus, San Juan
License Type	
Partial Product Key	
Manufacturer	VMware, Inc.

Model	VMware7,1
Processor Model	Intel(R) Core(TM) i7-6700 CPU @ 3.40GHz
Number of Processors	1
Number of CPU Cores	2
Number of Logical Cores	2
Physical Memory	4.00 GB

Table 48 - Hardware Inventory - CAYEY-DC-01V

Health Check:

Best Practice: Microsoft recommend putting enough RAM 8GB+ to load the entire DIT into memory, plus accommodate the operating system and other installed applications, such as anti-virus, backup software, monitoring, and so on.

SERVER-DC-01V

Name	SERVER-DC-01V
Windows Product Name	Windows Server 2019 Standard
Windows Build Number	10.0.17763
AD Domain	pharmax.local
Windows Installation Date	09/08/2020 21:20:17
Time Zone	(UTC-04:00) Georgetown, La Paz, Manaus, San Juan
License Type	Volume:GVLK
Partial Product Key	J464C
Manufacturer	VMware, Inc.
Model	VMware7,1
Processor Model	Intel(R) Core(TM) i7-6700 CPU @ 3.40GHz
Number of Processors	1
Number of CPU Cores	2
Number of Logical Cores	2
Physical Memory	4.00 GB

Table 49 - Hardware Inventory - SERVER-DC-01V

Health Check:

Best Practice: Microsoft recommend putting enough RAM 8GB+ to load the entire DIT into memory, plus accommodate the operating system and other installed applications, such as anti-virus, backup software, monitoring, and so on.

2.1.13.2 DNS IP Configuration

DC Name	Interface	Prefered DNS	Alternate DNS	DNS 3	DNS 4
CAYEY-DC-01V	Ethernet0	10.10.33.1	--	--	--
CAYEY-DC-01V	Ethernet1	192.168.5.1	10.10.33.1	--	--
SERVER-DC-01V	Ethernet0	127.0.0.1	192.168.5.1	8.8.8.8	--

Table 50 - DNS IP Configuration - PHARMAX.LOCAL

Health Check:

Best Practices: DNS configuration on network adapter should include the loopback address, but not as the first entry.

Best Practices: DNS configuration on network adapter shouldn't include the Domain Controller own IP address as the first entry.

Best Practices: For redundancy reasons, the DNS configuration on the network adapter should include an Alternate DNS address.

Corrective Actions: Network interfaces must be configured with DNS servers that can resolve names in the forest root domain. The following DNS server did not respond to the query for the forest root domain PHARMAX.LOCAL: 8.8.8.8

2.1.13.3 NTDS Information

DC Name	Database File	Database Size	Log Path	SysVol Path
CAYEY-DC-01V	C:\Windows\NTDS\ntds.dit	2.68 GB	C:\Windows\NTDS	C:\Windows\SYSVOL\sysvol
SERVER-DC-01V	C:\Windows\NTDS\ntds.dit	2.68 GB	C:\Windows\NTDS	C:\Windows\SYSVOL\sysvol

Table 51 - NTDS Database File Usage - PHARMAX.LOCAL

2.1.13.4 Time Source Information

Name	Time Server	Type
SERVER-DC-01V	192.168.5.254 0.pool.ntp.org 1.pool.ntp.org 2.pool.ntp.org 3.pool.ntp.org	MANUAL (NTP)
CAYEY-DC-01V	Domain Hierarchy	DOMHIER

Table 52 - Time Source Configuration - PHARMAX.LOCAL

2.1.13.5 SRV Records Status

Name	A Record	KDC SRV	PDC SRV	GC SRV	DC SRV
SERVER-DC-01V	OK	OK	OK	OK	OK

Table 53 - SRV Records Status - PHARMAX.LOCAL

2.1.13.6 File Shares

The following domain controllers have non-default file shares.

SERVER-DC-01V

Name	Path	Description
UEMConfig	E:\UEMConfig	--
UEMProfiles	E:\UEMProfiles	--
UpdateServicesPackages	E:\wsus\UpdateServicesPackages	A network share to be used by client systems for collecting all software packages (usually applications) published on this WSUS system.
WsusContent	E:\wsus\WsusContent	A network share to be used by Local Publishing to place published content on this WSUS system.

Table 54 - File Shares - SERVER-DC-01V

Health Check:

Best Practice: Only netlogon, sysvol and the default administrative shares should exist on a Domain Controller. If possible, non default file shares should be moved to another server, preferably a dedicated file server.

2.1.13.7 Installed Software

The following section provides a summary of additional software running on Domain Controllers from domain PHARMAX.LOCAL.

CAYEY-DC-01V

Name	Publisher	Install Date
7-Zip 21.07 (x64 edition)	Igor Pavlov	20220122

Table 55 - Installed Software - CAYEY-DC-01V

Health Check:

Best Practices: Do not run other software or services on a Domain Controller.

SERVER-DC-01V

Name	Publisher	Install Date
7-Zip 19.00 (x64)	Igor Pavlov	--
DiskMax 6.21	KoshyJohn.com	17/11/2021
Git	The Git Development Community	20240124
Google Chrome	Google LLC	20240118

Name	Publisher	Install Date
Graphviz	Graphviz	--
MEM Patching Optimizer	Patch My PC	20231104
Npcap	Nmap Project	--
RVTools	Robware	20220824
Veeam Agent for Microsoft Windows	Veeam Software Group GmbH	20231222
Veeam Backup Transport	Veeam Software Group GmbH	20231222
Veeam Backup VSS Integration	Veeam Software Group GmbH	20231222
Veeam Installer Service	Veeam Software Group GmbH	--
Veeam VSS Hardware Provider	Veeam Software Group GmbH	20231222

Table 56 - Installed Software - SERVER-DC-01V

Health Check:

Best Practices: Do not run other software or services on a Domain Controller.

2.1.13.8 Roles

The following section provides a summary of installed role & features on pharmax.local DCs.

CAYEY-DC-01V

Name	Parent	Description
Active Directory Certificate Services	Role	Active Directory Certificate Services (AD CS) is used to create certification authorities and related role services that allow you to issue and manage certificates used in a variety of applications.
Active Directory Domain Services	Role	Active Directory Domain Services (AD DS) stores information about objects on the network and makes this information available to users and network administrators. AD DS uses domain controllers to give network users access to permitted resources anywhere on the network through a single logon process.
DHCP Server	Role	Dynamic Host Configuration Protocol (DHCP) Server enables you to centrally configure, manage, and provide temporary IP addresses and related information for client computers.
DNS Server	Role	Domain Name System (DNS) Server provides name resolution for TCP/IP networks. DNS Server is easier to manage when it is installed on the same server as Active Directory Domain Services. If you select the Active Directory Domain Services role, you can install and configure DNS Server and Active Directory Domain Services to work together.
File and Storage Services	Role	File and Storage Services includes services that are always installed, as well as functionality that you can install to help manage file servers and storage.
Web Server (IIS)	Role	Web Server (IIS) provides a reliable, manageable, and scalable Web application infrastructure.

Table 57 - Roles - CAYEY-DC-01V

Health Check:

Best Practices: Domain Controllers should have limited software and agents installed including roles and services. Non-essential code running on Domain Controllers is a risk to the enterprise Active Directory environment. A Domain Controller should only run required software, services and roles critical to essential operation.

SERVER-DC-01V

Name	Parent	Description
Active Directory Certificate Services	Role	Active Directory Certificate Services (AD CS) is used to create certification authorities and related role services that allow you to issue and manage certificates used in a variety of applications.
Active Directory Domain Services	Role	Active Directory Domain Services (AD DS) stores information about objects on the network and makes this information available to users and network administrators. AD DS uses domain controllers to give network users access to permitted resources anywhere on the network through a single logon process.
DHCP Server	Role	Dynamic Host Configuration Protocol (DHCP) Server enables you to centrally configure, manage, and provide temporary IP addresses and related information for client computers.
DNS Server	Role	Domain Name System (DNS) Server provides name resolution for TCP/IP networks. DNS Server is easier to manage when it is installed on the same server as Active Directory Domain Services. If you select the Active Directory Domain Services role, you can install and configure DNS Server and Active Directory Domain Services to work together.
File and Storage Services	Role	File and Storage Services includes services that are always installed, as well as functionality that you can install to help manage file servers and storage.
Web Server (IIS)	Role	Web Server (IIS) provides a reliable, manageable, and scalable Web application infrastructure.
Windows Server Update Services	Role	Windows Server Update Services allows network administrators to specify the Microsoft updates that should be installed, create separate groups of computers for different sets of updates, and get reports on the compliance levels of the computers and the updates that must be installed.

Table 58 - Roles - SERVER-DC-01V

Health Check:

Best Practices: Domain Controllers should have limited software and agents installed including roles and services. Non-essential code running on Domain Controllers is a risk to the enterprise Active Directory environment. A Domain Controller should only run required software, services and roles critical to essential operation.

2.1.13.9 DC Diagnostic

The following section provides a summary of the Active Directory DC Diagnostic.

CAYEY-DC-01V

Test Name	Result	Impact	Description
Replications	Failed	High	Makes a deep validation to check the main replication for all naming contexts in this Domain Controller.
RidManager	Passed	High	Validates this Domain Controller can locate and contact the RID Master FSMO role holder. This test is skipped in RODCs.
ObjectsReplicated	Passed	High	Checks the replication health of core objects and attributes.
NCSecDesc	Passed	Medium	Validates if permissions are correctly set in this Domain Controller for all naming contexts. Those permissions directly affect replications health.
NetLogons	Passed	High	Validates if core security groups (including administrators and Authenticated Users) can connect and read NETLOGON and SYSVOL folders. It also validates access to IPC$. which can lead to failures in organizations that disable IPC$.
Services	Passed	High	Validates if the core Active Directory services are running in this Domain Controller. The services verified are: RPCSS, EVENTSYSTEM, DNSCACHE, ISMSERV, KDC, SAMSS, WORKSTATION, W32TIME, NETLOGON, NTDS (in case Windows Server 2008 or newer) and DFSR (if SYSVOL is using DFSR).
VerifyReplicas	Passed	High	Checks that all application directory partitions are fully instantiated on all replica servers.
DNS	Failed	Medium	DNS Includes six optional DNS-related tests, as well as the Connectivity test, which runs by default.
VerifyReferences	Passed	High	Validates that several attributes are present for the domain in the countainer and subcontainers in the DC objetcs. This test will fail if any attribute is missing.
SystemLog	Failed	Low	Checks if there is any erros in the Event Viewer > System event log in the past 60 minutes. Since the System event log records data from many places, errors reported here may lead to false positive and must be investigated further. The impact of this validation is marked as Low.
Topology	Passed	Medium	Topology Checks that the KCC has generated a fully connected topology for all domain controllers.
CutoffServers	Passed	Medium	Checks for any server that is not receiving replications because its partners are not running

Test Name	Result	Impact	Description
FrsEvent	Passed	Medium	Checks if theres any errors in the event logs regarding FRS replication. If running Windows Server 2008 R2 or newer on all Domain Controllers is possible SYSVOL were already migrated to DFSR, in this case errors found here can be ignored.
CheckSecurityError	Passed	Medium	Reports on the overall health of replication with respect to Active Directory security in domain controllers running Windows Server 2003 SP1.
Connectivity	Passed	Medium	Initial connection validation, checks if the DC can be located in the DNS, validates the ICMP ping (1 hop), checks LDAP binding and also the RPC connection. This initial test requires ICMP, LDAP, DNS and RPC connectivity to work properly.
Advertising	Passed	High	Validates this Domain Controller can be correctly located through the KDC service. It does not validate the Kerberos tickets answer or the communication through the TCP and UDP port 88.
DFSREvent	Failed	Medium	Checks if theres any errors in the event logs regarding DFSR replication. If running Windows Server 2008 or older on all Domain Controllers is possible SYSVOL is still using FRS, and in this case errors found here can be ignored. Obs. is highly recommended to migrate SYSVOL to DFSR.
KnowsOfRoleHolders	Passed	High	Checks if this Domain Controller is aware of which DC (or DCs) hold the FSMOs.
MachineAccount	Passed	High	Checks if this computer account exist in Active Directory and the main attributes are set. If this validation reports error. the following parameters of DCDIAG might help: /RecreateMachineAccount and /FixMachineAccount.
KccEvent	Failed	High	Validates through KCC there were no errors in the Event Viewer > Applications and Services Logs > Directory Services event log in the past 15 minutes (default time).
SysVolCheck	Passed	High	Validates if the registry key HKEY_Local_Machine\System\CurrentControlSet\Services\Netlogon\Parameters\SysvolReady=1 exist. This registry has to exist with value 1 for the DCs SYSVOL to be advertised.
FrsSysVol	Passed	Medium	Checks that the file replication system (FRS) system volume (SYSVOL) is ready

Table 59 - DCDiag Test Status - CAYEY-DC-01V

SERVER-DC-01V

Test Name	Result	Impact	Description
Replications	Passed	High	Makes a deep validation to check the main replication for all naming contexts in this Domain Controller.
RidManager	Passed	High	Validates this Domain Controller can locate and contact the RID Master FSMO role holder. This test is skipped in RODCs.
ObjectsReplicated	Passed	High	Checks the replication health of core objects and attributes.
NCSecDesc	Passed	Medium	Validates if permissions are correctly set in this Domain Controller for all naming contexts. Those permissions directly affect replications health.
NetLogons	Passed	High	Validates if core security groups (including administrators and Authenticated Users) can connect and read NETLOGON and SYSVOL folders. It also validates access to IPC$. which can lead to failures in organizations that disable IPC$.
Services	Passed	High	Validates if the core Active Directory services are running in this Domain Controller. The services verified are: RPCSS, EVENTSYSTEM, DNSCACHE, ISMSERV, KDC, SAMSS, WORKSTATION, W32TIME, NETLOGON, NTDS (in case Windows Server 2008 or newer) and DFSR (if SYSVOL is using DFSR).
VerifyReplicas	Passed	High	Checks that all application directory partitions are fully instantiated on all replica servers.
DNS	Passed	Medium	DNS Includes six optional DNS-related tests, as well as the Connectivity test, which runs by default.
VerifyReferences	Passed	High	Validates that several attributes are present for the domain in the countainer and subcontainers in the DC objetcs. This test will fail if any attribute is missing.
SystemLog	Failed	Low	Checks if there is any erros in the Event Viewer > System event log in the past 60 minutes. Since the System event log records data from many places, errors reported here may lead to false positive and must be investigated further. The impact of this validation is marked as Low.
Topology	Passed	Medium	Topology Checks that the KCC has generated a fully connected topology for all domain controllers.
CutoffServers	Passed	Medium	Checks for any server that is not receiving replications because its partners are not running
FrsEvent	Passed	Medium	Checks if theres any errors in the event logs regarding FRS replication. If running Windows Server 2008 R2 or newer on all Domain Controllers is possible SYSVOL were already migrated to DFSR, in this case errors found here can be ignored.
CheckSecurityError	Passed	Medium	Reports on the overall health of replication with respect to Active Directory security in domain controllers running Windows Server 2003 SP1.

Test Name	Result	Impact	Description
Connectivity	Passed	Medium	Initial connection validation, checks if the DC can be located in the DNS, validates the ICMP ping (1 hop), checks LDAP binding and also the RPC connection. This initial test requires ICMP, LDAP, DNS and RPC connectivity to work properly.
Advertising	Passed	High	Validates this Domain Controller can be correctly located through the KDC service. It does not validate the Kerberos tickets answer or the communication through the TCP and UDP port 88.
DFSREvent	Failed	Medium	Checks if theres any errors in the event logs regarding DFSR replication. If running Windows Server 2008 or older on all Domain Controllers is possible SYSVOL is still using FRS, and in this case errors found here can be ignored. Obs. is highly recommended to migrate SYSVOL to DFSR.
KnowsOfRoleHolders	Passed	High	Checks if this Domain Controller is aware of which DC (or DCs) hold the FSMOs.
MachineAccount	Passed	High	Checks if this computer account exist in Active Directory and the main attributes are set. If this validation reports error. the following parameters of DCDIAG might help: /RecreateMachineAccount and /FixMachineAccount.
KccEvent	Passed	High	Validates through KCC there were no errors in the Event Viewer > Applications and Services Logs > Directory Services event log in the past 15 minutes (default time).
SysVolCheck	Passed	High	Validates if the registry key HKEY_Local_Machine\System\CurrentControlSet\Services\Netlogon\Parameters\SysvolReady=1 exist. This registry has to exist with value 1 for the DCs SYSVOL to be advertised.
FrsSysVol	Passed	Medium	Checks that the file replication system (FRS) system volume (SYSVOL) is ready

Table 60 - DCDiag Test Status - SERVER-DC-01V

2.1.13.10 Infrastructure Services

The following section provides a summary of the Domain Controller Infrastructure services status.

CAYEY-DC-01V

Display Name	Short Name	Status
Active Directory Certificate Services	CertSvc	Running
Active Directory Domain Services	NTDS	Running
Active Directory Web Services	ADWS	Running
COM+ Event System	EVENTSYSTEM	Running

Display Name	Short Name	Status
DFS Replication	DFSR	Running
DHCP Server	DHCPServer	Running
DNS Client	DNSCACHE	Running
DNS Server	DNS	Running
Intersite Messaging	IsmServ	Running
Kerberos Key Distribution Center	Kdc	Running
NetLogon	Netlogon	Running
Print Spooler	Spooler	Running
Remote Procedure Call (RPC)	RPCSS	Running
Security Accounts Manager	SAMSS	Running
Windows Time	W32Time	Running
WORKSTATION	LanmanWorkstation	Running

Table 61 - Infrastructure Services Status - CAYEY-DC-01V

Health Check:

Corrective Actions: Disable Print Spooler service on DCs and all servers that do not perform Print services.

SERVER-DC-01V

Display Name	Short Name	Status
Active Directory Certificate Services	CertSvc	Running
Active Directory Domain Services	NTDS	Running
Active Directory Web Services	ADWS	Running
COM+ Event System	EVENTSYSTEM	Running
DFS Replication	DFSR	Running
DHCP Server	DHCPServer	Running
DNS Client	DNSCACHE	Running
DNS Server	DNS	Running
Intersite Messaging	IsmServ	Running
Kerberos Key Distribution Center	Kdc	Running
NetLogon	Netlogon	Running
Print Spooler	Spooler	Running
Remote Procedure Call (RPC)	RPCSS	Running
Security Accounts Manager	SAMSS	Running
Windows Time	W32Time	Running
WORKSTATION	LanmanWorkstation	Running

Table 62 - Infrastructure Services Status - SERVER-DC-01V

Health Check:

Corrective Actions: Disable Print Spooler service on DCs and all servers that do not perform Print services.

2.1.13.11 Replication Connection

The following section provides detailed information about Replication Connection.

Site: Cayey-Branch: From: CAYEY-DC-01V To: SERVER-DC-01V

Name	CAYEY-DC-01V
From Site	Cayey-Branch
GUID	df73ca5c-2ca4-4b7b-9797-f23968c000cc
Description	--
From Server	CAYEY-DC-01V
To Server	SERVER-DC-01V
Replicated Naming Contexts	DC=DomainDnsZones,DC=pharmax,DC=local DC=ForestDnsZones,DC=pharmax,DC=local CN=Schema,CN=Configuration,DC=pharmax,DC=local CN=Configuration,DC=pharmax,DC=local DC=pharmax,DC=local
Transport Protocol	IP
Auto Generated	No
Enabled	Yes
Created	Sat, 17 Jun 2023 01:12:08 GMT

Table 63 - Replication Connection - SERVER-DC-01V

Site: ACAD: From: ACADE-DC-01V To: SERVER-DC-01V

Name	<automatically generated>
From Site	ACAD
GUID	d5a28ae4-ee92-47a4-872e-e4115bc8d1a5
Description	--
From Server	ACADE-DC-01V
To Server	SERVER-DC-01V
Replicated Naming Contexts	DC=DomainDnsZones,DC=pharmax,DC=local DC=ForestDnsZones,DC=pharmax,DC=local CN=Schema,CN=Configuration,DC=pharmax,DC=local CN=Configuration,DC=pharmax,DC=local DC=pharmax,DC=local
Transport Protocol	IP
Auto Generated	Yes
Enabled	Yes
Created	Sun, 05 Sep 2021 16:24:39 GMT

Table 64 - Replication Connection - SERVER-DC-01V

Site: UIA: From: DC-UIA-01V To: SERVER-DC-01V

Name	<automatically generated>
From Site	UIA
GUID	aabfef5a-f968-4f1e-b02e-9625f6731933
Description	--
From Server	DC-UIA-01V
To Server	SERVER-DC-01V
Replicated Naming Contexts	DC=DomainDnsZones,DC=pharmax,DC=local DC=ForestDnsZones,DC=pharmax,DC=local CN=Schema,CN=Configuration,DC=pharmax,DC=local CN=Configuration,DC=pharmax,DC=local DC=pharmax,DC=local
Transport Protocol	IP
Auto Generated	Yes
Enabled	Yes
Created	Wed, 11 May 2022 17:54:53 GMT

Table 65 - Replication Connection - SERVER-DC-01V

2.1.13.12 Replication Status

From Server	To Server	From Site	Last Success Time	Last Failure Status	Last Failure Time	Failures
CAYEY-DC-01V	SERVER-DC-01V	Cayey-Branch	2024-01-24 10:31:53	0	0	0
ACADE-DC-01V	SERVER-DC-01V	ACAD	2024-01-24 10:31:53	0	0	0
CAYEY-DC-01V	SERVER-DC-01V	Cayey-Branch	2024-01-24 10:31:53	0	0	0
DC-UIA-01V	SERVER-DC-01V	UIA	2024-01-24 10:31:53	0	0	0
ACADE-DC-01V	SERVER-DC-01V	ACAD	2024-01-24 10:31:53	0	0	0
DC-UIA-01V	SERVER-DC-01V	UIA	2024-01-24 10:31:53	0	0	0
ACADE-DC-01V	SERVER-DC-01V	ACAD	2024-01-24 10:31:53	0	0	0
DC-UIA-01V	SERVER-DC-01V	UIA	2024-01-24 10:31:53	0	0	0
CAYEY-DC-01V	SERVER-DC-01V	Cayey-Branch	2024-01-24 10:31:53	0	0	0

From Server	To Server	From Site	Last Success Time	Last Failure Status	Last Failure Time	Failures
ACADE-DC-01V	SERVER-DC-01V	ACAD	2024-01-24 10:31:53	0	0	0
CAYEY-DC-01V	SERVER-DC-01V	Cayey-Branch	2024-01-24 10:31:53	0	0	0
DC-UIA-01V	SERVER-DC-01V	UIA	2024-01-24 10:31:53	0	0	0
ACADE-DC-01V	SERVER-DC-01V	ACAD	2024-01-24 10:31:53	0	0	0
DC-UIA-01V	SERVER-DC-01V	UIA	2024-01-24 10:31:53	0	0	0
CAYEY-DC-01V	SERVER-DC-01V	Cayey-Branch	2024-01-24 10:31:53	0	0	0

Table 66 - Replication Status - PHARMAX.LOCAL

2.1.13.13 Group Policy Objects

The following section provides a summary of the Group Policy Objects for domain PHARMAX.LOCAL.

Deleted GPO in Sysvol

GPO Status	All Settings Enabled
GUID	09e68095-8cfc-4174-81ed-afb52597dd7f
Created	06/20/2023
Modified	06/20/2023
Owner	PHARMAX\Domain Admins
Computer Version	0 (AD), 0 (SYSVOL)
User Version	0 (AD), 0 (SYSVOL)
WMI Filter	--
Security Filtering	Authenticated Users
Linked Target	--
Description	--

Table 67 - GPO - Deleted GPO in Sysvol

Health Check:

Corrective Actions: Ensure unused or unlinked GPOs are removed from Active Directory.

Assign-Applications

GPO Status	All Settings Enabled
GUID	2168b63b-4bd0-4627-99a8-835aea402534

Created	03/10/2021
Modified	07/18/2023
Owner	PHARMAX\Domain Admins
Computer Version	7 (AD), 7 (SYSVOL)
User Version	0 (AD), 0 (SYSVOL)
WMI Filter	--
Security Filtering	jocolon Authenticated Users
Linked Target	pharmax.local/LinuxMachines pharmax.local
Description	This is a bad description example

Table 68 - GPO - Assign-Applications

Certificate AutoEnrollment

GPO Status	User Settings Disabled
GUID	27fa05c8-7c50-4994-9f95-29c4aa3971ed
Created	01/25/2020
Modified	06/30/2021
Owner	PHARMAX\Domain Admins
Computer Version	28 (AD), 28 (SYSVOL)
User Version	0 (AD), 0 (SYSVOL)
WMI Filter	--
Security Filtering	Authenticated Users
Linked Target	pharmax.local
Description	--

Table 69 - GPO - Certificate AutoEnrollment

Default Domain Policy

GPO Status	All Settings Enabled
GUID	31b2f340-016d-11d2-945f-00c04fb984f9
Created	06/10/2018
Modified	10/11/2022
Owner	PHARMAX\Domain Admins
Computer Version	112 (AD), 112 (SYSVOL)
User Version	0 (AD), 0 (SYSVOL)
WMI Filter	--
Security Filtering	Authenticated Users
Linked Target	pharmax.local
Description	--

Table 70 - GPO - Default Domain Policy

VEEAM_Disable_Firewall

GPO Status	All Settings Enabled
GUID	4b2e42eb-2100-4a94-b4b0-7822e30634f6
Created	12/13/2019
Modified	09/08/2020
Owner	PHARMAX\Domain Admins
Computer Version	12 (AD), 12 (SYSVOL)
User Version	0 (AD), 0 (SYSVOL)
WMI Filter	--
Security Filtering	Authenticated Users
Linked Target	pharmax.local/VEEAM Servers pharmax.local/VEEAM WorkStations pharmax.local/ProfileUnity VDI
Description	--

Table 71 - GPO - VEEAM_Disable_Firewall

SET - KMS Server

GPO Status	All Settings Enabled
GUID	502c4398-dc59-49ee-b567-47656f08e09e
Created	08/31/2022
Modified	08/31/2022
Owner	PHARMAX\Domain Admins
Computer Version	8 (AD), 8 (SYSVOL)
User Version	0 (AD), 0 (SYSVOL)
WMI Filter	--
Security Filtering	Authenticated Users
Linked Target	pharmax.local
Description	--

Table 72 - GPO - SET - KMS Server

Default Domain Controllers Policy

GPO Status	All Settings Enabled
GUID	6ac1786c-016f-11d2-945f-00c04fb984f9
Created	06/10/2018
Modified	06/25/2023
Owner	PHARMAX\Domain Admins
Computer Version	21 (AD), 21 (SYSVOL)
User Version	0 (AD), 0 (SYSVOL)
WMI Filter	--
Security Filtering	Authenticated Users

Linked Target	pharmax.local/Domain Controllers
Description	--

Table 73 - GPO - Default Domain Controllers Policy

ProfileUnity

GPO Status	All Settings Enabled
GUID	8f11a3fa-3b68-476d-99fc-32064f696ebe
Created	06/08/2020
Modified	10/05/2021
Owner	PHARMAX\Domain Admins
Computer Version	1 (AD), 1 (SYSVOL)
User Version	1 (AD), 1 (SYSVOL)
WMI Filter	--
Security Filtering	Authenticated Users
Linked Target	pharmax.local/ProfileUnity VDI/Computers
Description	--

Table 74 - GPO - ProfileUnity

VEEAM_Local_Administrators

GPO Status	All Settings Enabled
GUID	96cb9511-a88c-45ab-b10c-05b0441b1057
Created	12/13/2019
Modified	05/20/2022
Owner	PHARMAX\Domain Admins
Computer Version	8 (AD), 8 (SYSVOL)
User Version	0 (AD), 0 (SYSVOL)
WMI Filter	--
Security Filtering	Authenticated Users
Linked Target	pharmax.local/VEEAM Servers pharmax.local/VEEAM WorkStations pharmax.local/ProfileUnity VDI
Description	--

Table 75 - GPO - VEEAM_Local_Administrators

WSUS - Domain Policy

GPO Status	User Settings Disabled
GUID	a9ec1b8c-3520-4e19-b11c-babb27c6da1a
Created	02/23/2020
Modified	03/10/2021
Owner	PHARMAX\Domain Admins

Computer Version	26 (AD), 26 (SYSVOL)
User Version	0 (AD), 0 (SYSVOL)
WMI Filter	--
Security Filtering	Authenticated Users
Linked Target	pharmax.local
Description	--

Table 76 - GPO - WSUS - Domain Policy

SCEP Configuration

GPO Status	All Settings Enabled
GUID	d6187a9f-118c-4ee7-a18f-6889a0a657f4
Created	09/14/2020
Modified	10/04/2020
Owner	PHARMAX\Domain Admins
Computer Version	6 (AD), 6 (SYSVOL)
User Version	0 (AD), 0 (SYSVOL)
WMI Filter	--
Security Filtering	Authenticated Users
Linked Target	pharmax.local/Configuration Manager pharmax.local/Configuration Manager Computers
Description	--

Table 77 - GPO - SCEP Configuration

Dead Policy

GPO Status	All Settings Disabled
GUID	e360fece-8631-4749-b1a4-e55d0e48aa5e
Created	10/05/2021
Modified	06/19/2023
Owner	PHARMAX\Domain Admins
Computer Version	1 (AD), 1 (SYSVOL)
User Version	1 (AD), 1 (SYSVOL)
WMI Filter	ByUser
Security Filtering	Authenticated Users
Linked Target	--
Description	--

Table 78 - GPO - Dead Policy

Health Check:

Best Practices: Ensure 'All Settings Disabled' GPO are removed from Active Directory.

Corrective Actions: Ensure unused or unlinked GPOs are removed from Active Directory.

No Security Filtering Applied

GPO Status	All Settings Enabled
GUID	ecbc276e-0e38-42f5-b6e0-6c133b08203c
Created	06/18/2023
Modified	06/20/2023
Owner	PHARMAX\Domain Admins
Computer Version	1 (AD), 1 (SYSVOL)
User Version	1 (AD), 1 (SYSVOL)
WMI Filter	--
Security Filtering	No Security Filtering
Linked Target	--
Description	--

Table 79 - GPO - No Security Filtering Applied

Health Check:

Corrective Actions: Determine which 'No Security Filtering' Group Policies should be deleted and delete them.

Corrective Actions: Ensure unused or unlinked GPOs are removed from Active Directory.

Horizon-DEM

GPO Status	All Settings Enabled
GUID	f33e9036-4496-4323-9d5a-3011dfd8f1f7
Created	03/01/2020
Modified	06/18/2023
Owner	PHARMAX\Domain Admins
Computer Version	14 (AD), 14 (SYSVOL)
User Version	12 (AD), 12 (SYSVOL)
WMI Filter	--
Security Filtering	Authenticated Users
Linked Target	pharmax.local/VDI-Computers
Description	--

Table 80 - GPO - Horizon-DEM

Linux-Settings-GPO

GPO Status	All Settings Disabled
GUID	f46abddd-4ae2-457d-b933-849b164fb3f8

Created	05/22/2021
Modified	02/04/2022
Owner	PHARMAX\Domain Admins
Computer Version	0 (AD), 0 (SYSVOL)
User Version	6 (AD), 6 (SYSVOL)
WMI Filter	--
Security Filtering	Authenticated Users
Linked Target	pharmax.local/LinuxMachines
Description	--

Table 81 - GPO - Linux-Settings-GPO

Health Check:

Best Practices: Ensure 'All Settings Disabled' GPO are removed from Active Directory.

SCCM - Restricted Group and General Settings

GPO Status	All Settings Enabled
GUID	fc8443e6-43cb-4ea4-9862-47b19813596b
Created	09/12/2020
Modified	09/12/2020
Owner	PHARMAX\Domain Admins
Computer Version	6 (AD), 6 (SYSVOL)
User Version	0 (AD), 0 (SYSVOL)
WMI Filter	--
Security Filtering	Authenticated Users
Linked Target	pharmax.local/Configuration Manager
Description	--

Table 82 - GPO - SCCM - Restricted Group and General Settings

LAPS Configuration

GPO Status	All Settings Enabled
GUID	fe43b055-4f61-4fa1-b387-0fc3e2b5915e
Created	11/01/2020
Modified	11/01/2020
Owner	PHARMAX\Domain Admins
Computer Version	15 (AD), 15 (SYSVOL)
User Version	0 (AD), 0 (SYSVOL)
WMI Filter	--
Security Filtering	Authenticated Users
Linked Target	pharmax.local/Configuration Manager Computers
Description	--

Table 83 - GPO - LAPS Configuration

2.1.13.13.1 WMI Filters

Name	ByUser
Author	Administrator@pharmax.local
Query	1;3;10;81;WQL;root\CIMv2;Select * from Win32_OperatingSystem where Version like "10.%" and ProductType="1";
Description	User Filter

Table 84 - WMI Filter - ByUser

Name	ByIP
Author	Administrator@pharmax.local
Query	1;3;10;78;WQL;root\CIMv2;Select * from WIN32_ComputerSystem where TotalPhysicalMemory >= 1073741824 ;
Description	Filter by IP

Table 85 - WMI Filter - ByIP

2.1.13.13.2 Central Store Repository

Domain	Configured	Central Store Path
PHARMAX.LOCAL	Yes	\\pharmax.local\SYSVOL\pharmax.local\Policies\PolicyDefinitions

Table 86 - GPO Central Store - PHARMAX.LOCAL

2.1.13.13.3 Logon/Logoff Script

GPO Name	GPO Status	Type	Script
Dead Policy	All Settings Disabled	Logoff	%systemdrive%\Program Files\ProfileUnity\Client.NET\LwL.ProfileUnity.Client.Logoff.exe
Horizon-DEM	All Settings Enabled	Logoff	C:\Program Files\Immidio\Flex Profiles\FlexEngine.exe
No Security Filtering Applied	All Settings Enabled	Logoff	%systemdrive%\Program Files\ProfileUnity\Client.NET\LwL.ProfileUnity.Client.Logoff.exe

GPO Name	GPO Status	Type	Script
ProfileUnity	All Settings Enabled	Logoff	%systemdrive%\Program Files\ProfileUnity\Client.NET\LwL.ProfileUnity.Client.Logoff.exe

Table 87 - GPO with Logon/Logoff Script - PHARMAX.LOCAL

2.1.13.13.4 Startup/Shutdown Script

GPO Name	GPO Status	Type	Script
Dead Policy	All Settings Disabled	Startup	\\pharmax.local\netlogon\profileunity\LwL.ProfileUnity.Client.Startup.exe
No Security Filtering Applied	All Settings Enabled	Startup	\\pharmax.local\netlogon\profileunity\LwL.ProfileUnity.Client.Startup.exe
ProfileUnity	All Settings Enabled	Startup	\\pharmax.local\netlogon\profileunity\LwL.ProfileUnity.Client.Startup.exe

Table 88 - GPO with Startup/Shutdown Script - PHARMAX.LOCAL

2.1.13.13.5 Unlinked GPO

GPO Name	Created	Modified	Computer Enabled	User Enabled
Dead Policy	2021-10-05	2023-06-20	No	No
Deleted GPO in Sysvol	2023-06-20	2023-06-20	Yes	Yes
No Security Filtering Applied	2023-06-19	2023-06-20	Yes	Yes

Table 89 - Unlinked GPO - PHARMAX.LOCAL

Health Check:

Corrective Actions: Remove Unused GPO from Active Directory.

2.1.13.13.6 Empty GPOs

GPO Name	Created	Modified	Description
Deleted GPO in Sysvol	2023-06-20	2023-06-20	--
Linux-Settings-GPO	2021-05-23	2022-02-04	--

Table 90 - Empty GPO - PHARMAX.LOCAL

Health Check:

Corrective Actions: No User and Computer parameters are set: Remove Unused GPO in Active Directory.

2.1.13.13.7 Enforced GPO

GPO Name	Target
Certificate AutoEnrollment	pharmax.local/
SET - KMS Server	pharmax.local/
LAPS Configuration	pharmax.local/Configuration Manager Computers
Linux-Settings-GPO	pharmax.local/LinuxMachines

Table 91 - Enforced GPO - PHARMAX.LOCAL

Health Check:

Corrective Actions: Review use of enforcement and blocked policy inheritance in Active Directory.

2.1.13.13.8 Orphaned GPO

The following table summarizes the group policy objects that are orphaned or missing in the AD database or in the SYSVOL directory.

Name	Unknown
Guid	A8DF92D3-BDAF-479E-8C0C-9D78AAE058E4
AD DN Database	Missing
AD DN Path	CN={A8DF92D3-BDAF-479E-8C0C-9D78AAE058E4},CN=Policies,CN=System,DC=pharmax,DC=local (Missing)
SYSVOL Guid Directory	Valid
SYSVOL Guid Path	\\pharmax.local\SYSVOL\pharmax.local\Policies\{A8DF92D3-BDAF-479E-8C0C-9D78AAE058E4} (Valid)

Table 92 - Orphaned GPO - PHARMAX.LOCAL

Health Check:

Corrective Actions: Evaluate orphaned group policies objects that exist in SYSVOL but not in AD or the Group Policy Management Console (GPMC). These take up space in SYSVOL and bandwidth during replication.

Name	Deleted GPO in Sysvol
Guid	09E68095-8CFC-4174-81ED-AFB52597DD7F
AD DN Database	Valid
AD DN Path	CN={09E68095-8CFC-4174-81ED-AFB52597DD7F},CN=Policies,CN=System,DC=pharmax,DC=local (Valid)
SYSVOL Guid Directory	Missing
SYSVOL Guid Path	\\pharmax.local\SYSVOL\pharmax.local\Policies\{09E68095-8CFC-4174-81ED-AFB52597DD7F} (Missing)

Table 93 - Orphaned GPO - PHARMAX.LOCAL

Health Check:

Corrective Actions: Evaluate orphaned group policies folders and files that exist in AD or the Group Policy Management Console (GPMC) but not in SYSVOL. These take up space in the AD database and bandwidth during replication.

2.1.13.14 Organizational Units

The following section provides a summary of Active Directory Organizational Unit information.

Name	Linked GPO	Protected
Admin	--	Yes
Admins PC	--	Yes
Configuration Manager	SCEP Configuration, SCCM - Restricted Group and General Settings	Yes
Configuration Manager Computers	LAPS Configuration, SCEP Configuration	Yes
Domain Controllers	Default Domain Controllers Policy	No
EMC NAS servers	--	No
EMC NAS servers/Computers	--	No
LinuxMachines	Assign-Applications, Linux-Settings-GPO	Yes
Member Servers	--	Yes
Microsoft Exchange Security Groups	--	No
People	--	Yes
ProfileUnity VDI	VEEAM_Local_Administrators, VEEAM_Disable_Firewall	Yes
ProfileUnity VDI/Computers	ProfileUnity	Yes
ProfileUnity VDI/Servers	--	Yes
Tier 2	--	Yes
Tier 2/BDE	--	No
Tier 2/BDE/Devices	--	Yes
Tier 2/BDE/Groups	--	Yes
Tier 2/BDE/ServiceAccounts	--	Yes
Tier 2/BDE/Test	--	Yes
Tier 2/FIN	--	No
Tier 2/FIN/Devices	--	Yes
Tier 2/FIN/Groups	--	Yes
Tier 2/FIN/ServiceAccounts	--	Yes
Tier 2/FIN/Test	--	Yes
Tier 2/HRE	--	No
Tier 2/HRE/Devices	--	Yes

Name	Linked GPO	Protected
Tier 2/HRE/Groups	--	Yes
Tier 2/HRE/ServiceAccounts	--	Yes
Tier 2/HRE/Test	--	Yes
Tier 2/OGC	--	No
Tier 2/OGC/Devices	--	Yes
Tier 2/OGC/Groups	--	Yes
Tier 2/OGC/ServiceAccounts	--	Yes
Tier 2/OGC/Test	--	Yes
VDI-Computers	Horizon-DEM	Yes
VDI-Computers/Finances	--	Yes
VDI-Computers/HR	--	Yes
VDI-Computers/Marketing	--	Yes
VDI-Computers/Sales	--	Yes
VEEAM Servers	VEEAM_Disable_Firewall, VEEAM_Local_Administrators	Yes
VEEAM WorkStations	VEEAM_Local_Administrators, VEEAM_Disable_Firewall	Yes

Table 94 - Organizational Unit - PHARMAX.LOCAL

Health Check:

Best Practice: If the Organizational Units in your Active Directory are not protected from accidental deletion, your environment can experience disruptions that might be caused by accidental bulk deletion of objects. All OUs in this domain should be protected from accidental deletion

GPO Blocked Inheritance

OU Name	Container Type	Inheritance Blocked	Path
linuxmachines	OU	Yes	pharmax.local/LinuxMachines

Table 95 - Blocked Inheritance GPO - PHARMAX.LOCAL

Health Check:

Corrective Actions: Review use of enforcement and blocked policy inheritance in Active Directory.