Microsoft Active Directory As Built Report

Zen Pr Solutions

Author: Jonathan Colon
Date: Tuesday, May 23, 2023
Version: 1.0

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 Active Directory framework that holds the objects can be viewed at a number of levels. The forest, tree, and domain are the logical divisions in an Active Directory network. At the top of the structure is the forest. A forest is a collection of trees that share a common global catalog, directory schema, logical structure, and directory configuration. The forest represents the security boundary within which users, computers, groups, and other objects are accessible.

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

Table 1 - Forest Summary - PHARMAX.LOCAL

1.1.1 Optional Features

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

Table 2 - Optional Features - PHARMAX.LOCAL

1.1.2 Domain Sites

Site Name	Description	Subnets	Creation Date
ACAD	--	172.23.4.0/24	9/5/2021
Cayey-Branch	Site of Cayey, PR Branch	10.10.0.0/16	9/3/2021
Dead-Site	--	--	1/22/2022
Pharmax-HQ	Site of San Juan, PR HQ	10.9.1.0/24 192.168.0.0/16	6/10/2018
UIA	--	172.23.7.0/24	5/11/2022

Table 3 - Sites - PHARMAX.LOCAL

1.1.2.1 Site Subnets

Subnet	Description	Sites	Creation Date
10.10.0.0/16	Cayey-Networks	Cayey-Branch	9/12/2020
10.9.1.0/24	--	Pharmax-HQ	9/14/2021
172.23.4.0/24	--	ACAD	5/11/2022
172.23.7.0/24	--	UIA	5/11/2022
192.168.0.0/16	--	Pharmax-HQ	9/12/2020

Table 4 - Site Subnets - PHARMAX.LOCAL

1.1.2.2 Site Links

Site Link Name	Cost	Replication Frequency	Transport Protocol	Sites
PHARMAX-to-ACAD	100	15 min	IP	ACAD Pharmax-HQ
Pharmax-to-All	100	15 min	IP	UIA Dead-Site ACAD Cayey-Branch Pharmax-HQ

Table 5 - Site Links - PHARMAX.LOCAL

1.2 AD Domain Configuration

An Active Directory domain is a collection of objects within a Microsoft Active Directory network. An object can be a single user or a group or it can be a hardware component, such as a computer or printer.Each domain holds a database containing object identity information. Active Directory domains can be identified using a DNS name, which can be the same as an organization's public domain name, a sub-domain or an alternate version (which may end in .local).

1.2.1 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	8100
RID Available	1073733723

Table 6 - Domain Summary - PHARMAX.LOCAL

1.2.1.1 FSMO Roles

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

Table 7 - FSMO Roles - pharmax.local

1.2.1.2 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 8 - 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 9 - Trusts - uia.local

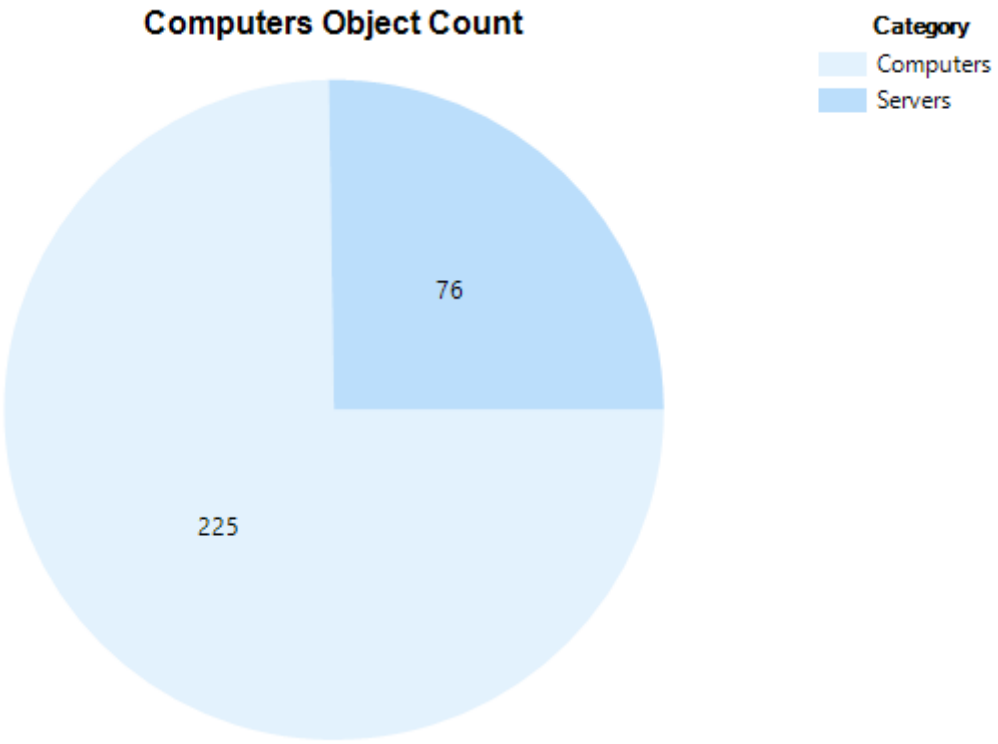
lab.local

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 10 - Trusts - lab.local

1.2.1.3 Domain Object Count

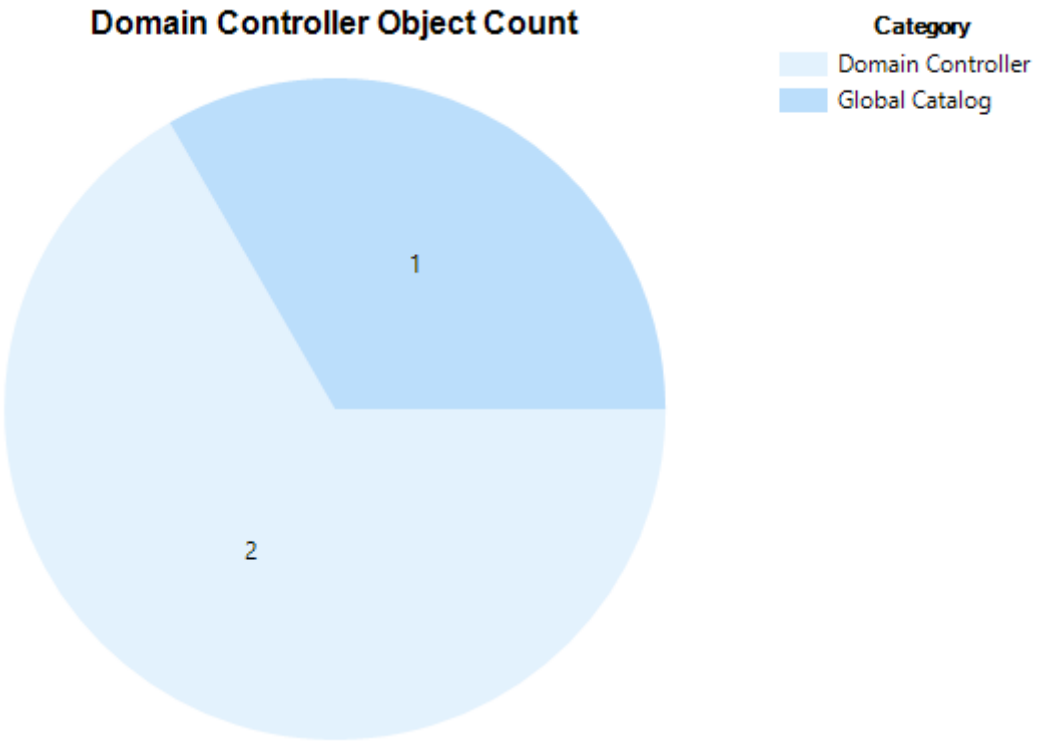
1.2.1.3.1 Computers Object



Computers	225
Servers	76

Table 11 - Computers Object - PHARMAX.LOCAL

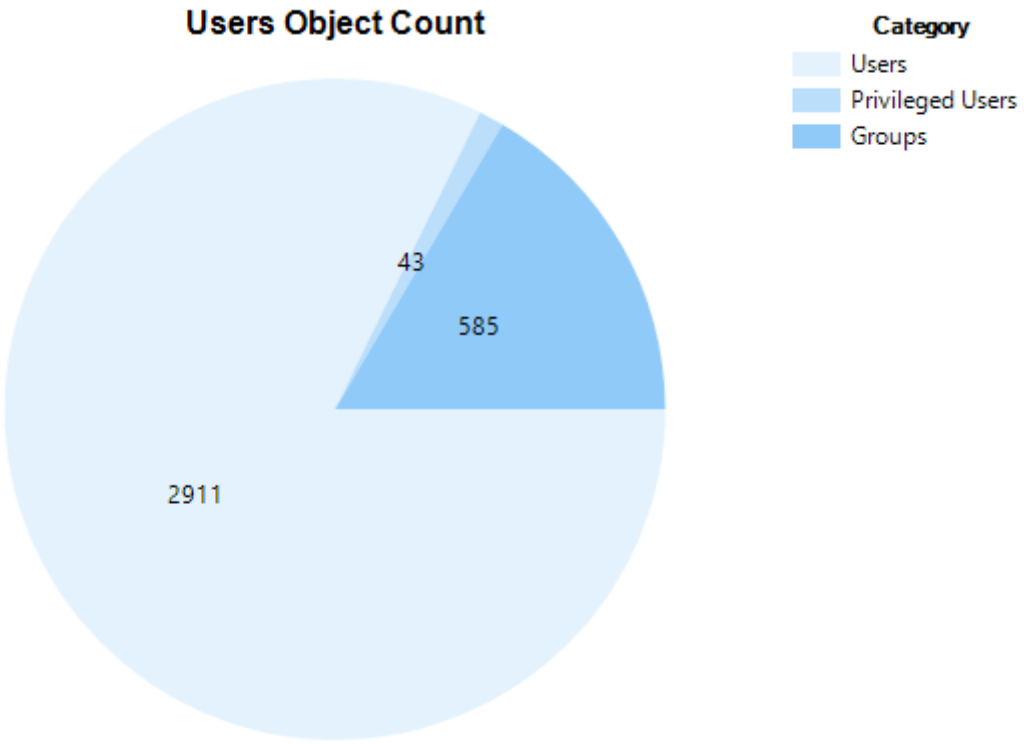
1.2.1.3.2 Domain Controller Object



Domain Controller	2
Global Catalog	1

Table 12 - Domain Controller Object - PHARMAX.LOCAL

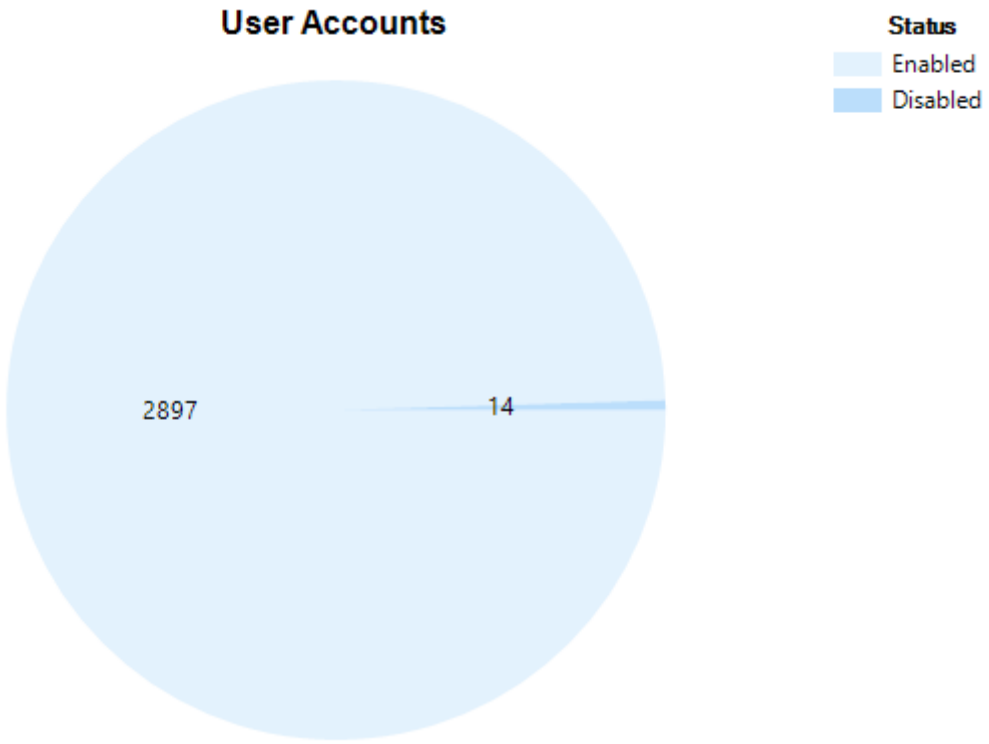
1.2.1.3.3 Users Object



Users	2911
Privileged Users	43
Groups	585

Table 13 - User Object - PHARMAX.LOCAL

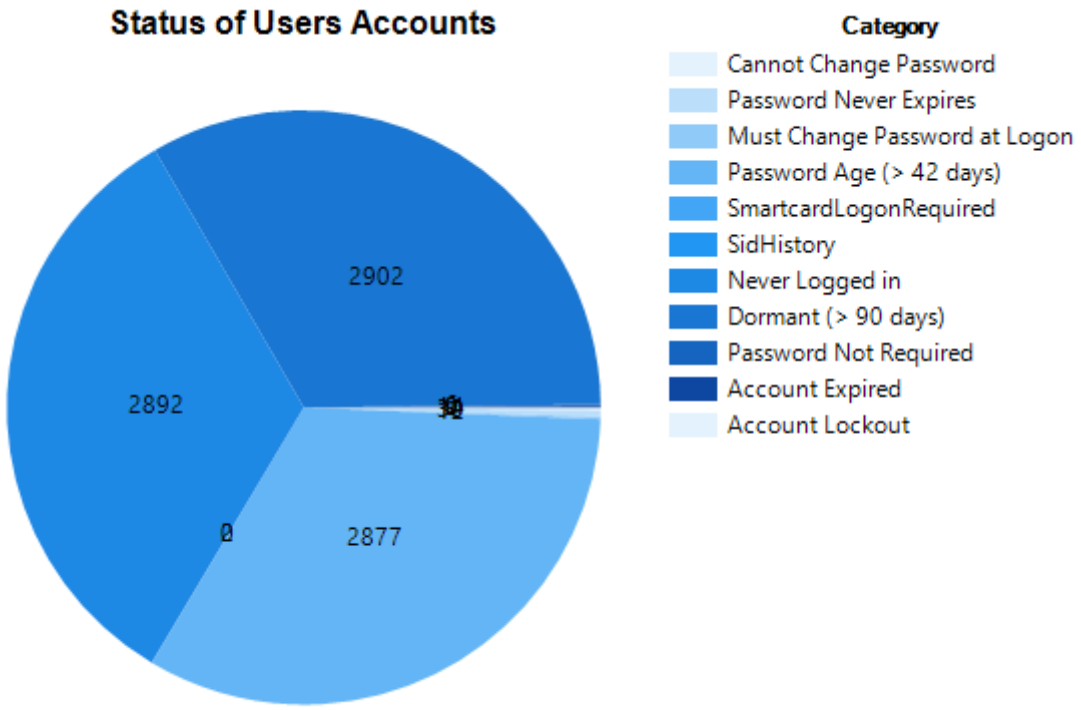
1.2.1.4 User Accounts in Domain



Status	Count	Percentage
Enabled	2897	100%
Disabled	14	0%

Table 14 - User Accounts in Domain - PHARMAX.LOCAL

1.2.1.5 Status of Users Accounts



Category	Enabled Count	Enabled %	Disabled Count	Disabled %	Total Count	Total %
Cannot Change Password	14	0	1	0	14	0
Password Never Expires	30	1	1	0	30	1
Must Change Password at Logon	12	0	1	0	12	0
Password Age (> 42 days)	2877	99	1	0	2877	99
SmartcardLogonRequired	2	0	1	0	2	0
SidHistory	0	0	1	0	0	0
Never Logged in	2892	99	1	0	2892	99
Dormant (> 90 days)	2902	100	1	0	2902	100
Password Not Required	6	0	1	0	6	0
Account Expired	9	0	1	0	9	0
Account Lockout	0	0	1	0	0	0

Table 15 - Status of User Accounts - PHARMAX.LOCAL

1.2.1.6 Privileged Group Count

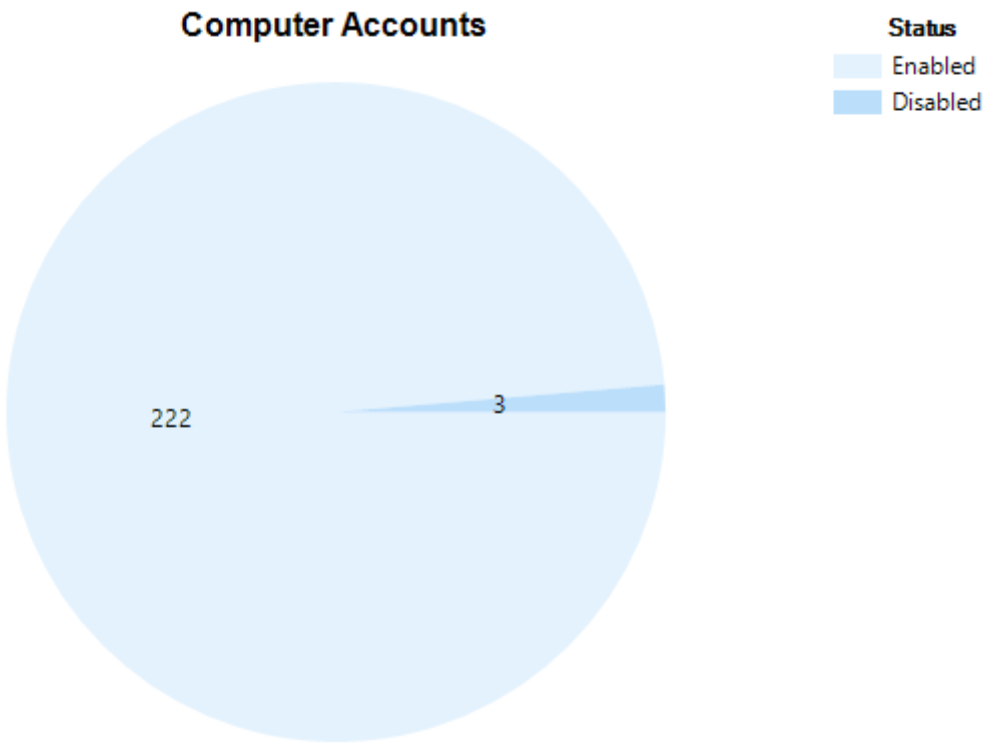
Group Name	Count
Account Operators	1
Administrators	6
Backup Operators	2

Group Name	Count
Cert Publishers	4
DnsAdmins	3
Domain Admins	5
Enterprise Admins	2
Incoming Forest Trust Builders	2
Key Admins	2
Print Operators	1
Remote Desktop Users	3
Schema Admins	25
Server Operators	3

Table 16 - Privileged Group Count - 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.

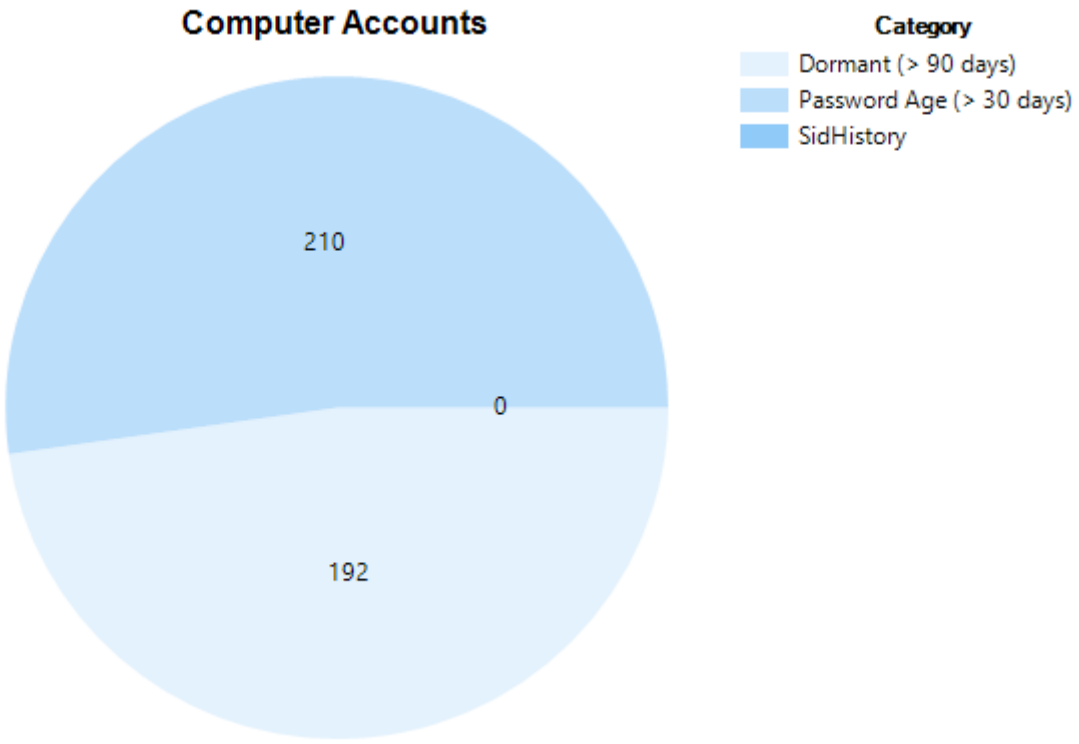
1.2.1.7 Computer Accounts in Domain



Status	Count	Percentage
Enabled	222	99%
Disabled	3	1%

Table 17 - Computer Accounts in Domain - PHARMAX.LOCAL

1.2.1.8 Status of Computer Accounts



Category	Enabled Count	Enabled %	Disabled Count	Disabled %	Total Count	Total %
Dormant (> 90 days)	192	85	1	0	192	85
Password Age (> 30 days)	210	93	1	0	210	93
SidHistory	0	0	1	0	0	0

Table 18 - Status of Computer Accounts - PHARMAX.LOCAL

1.2.1.9 Operating Systems Count

Operating System	Count
CentOS	1
Data Domain OS	1
EMC File Server	1
NetApp Release 9.5P6	1

Operating System	Count
NetApp Release 9.8	1
NetApp Release 9.8P7	1
NetApp Release 9.9.1P1	3
OneFS	1
pc-linux-gnu	2
redhat-linux-gnu	2
unknown	7
Unknown	105
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	42
Windows Server 2022 Datacenter	3
Windows Server 2022 Datacenter Evaluation	18
Windows Vista	1
Windows XP	1

Table 19 - 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

1.2.1.10 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 20 - Default Domain Password Policy - PHARMAX.LOCAL

1.2.1.11 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 21 - 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 22 - Fined Grained Password Policies - Test

1.2.1.12 Local Administrator Password Solution

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 23 - Local Administrator Password Solution - PHARMAX.LOCAL

1.2.1.13 gMSA identities

SQLServer

Name	SQLServer
SamAccountName	SQLServer$
Created	09/27/2020 14:14:22
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	09/27/2020 14:41:08
Locked Out	No
Logon Count	3
Password Expired	No
Password Last Set	09/27/2020 14:14:22

Table 24 - gMSA - SQLServer

adfsgmsa

Name	adfsgmsa
SamAccountName	adfsgmsa$
Created	10/07/2020 18:36:16
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	10/07/2020 18:36:17
Locked Out	No
Logon Count	40
Password Expired	No
Password Last Set	10/07/2020 18:36:16

Table 25 - gMSA - adfsgmsa

1.2.1.14 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	2023:02:20	91
CN=Schema,CN=Configuration,DC=pharmax,DC=local	2023:02:20	91
DC=DomainDnsZones,DC=pharmax,DC=local	2023:02:20	91
DC=ForestDnsZones,DC=pharmax,DC=local	2023:02:20	91
DC=pharmax,DC=local	2023:02:20	91

Table 26 - Naming Context Last Backup - PHARMAX.LOCAL

Health Check:
Corrective Actions: Ensure there is a recent (<180 days) Active Directory backup.

Sysvol Folder Status

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

Extension	File Count	Size
.aas	4	0.16 MB
.adm	3	0.04 MB
.adml	4684	75.08 MB
.admx	222	3.83 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	16	0.01 MB
.msi	3	150.78 MB
.pol	13	0.03 MB
.xml	4	0.01 MB
.zip	5	143.60 MB

Table 27 - Sysvol Folder Status - PHARMAX.LOCAL

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

Netlogon Folder Status

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

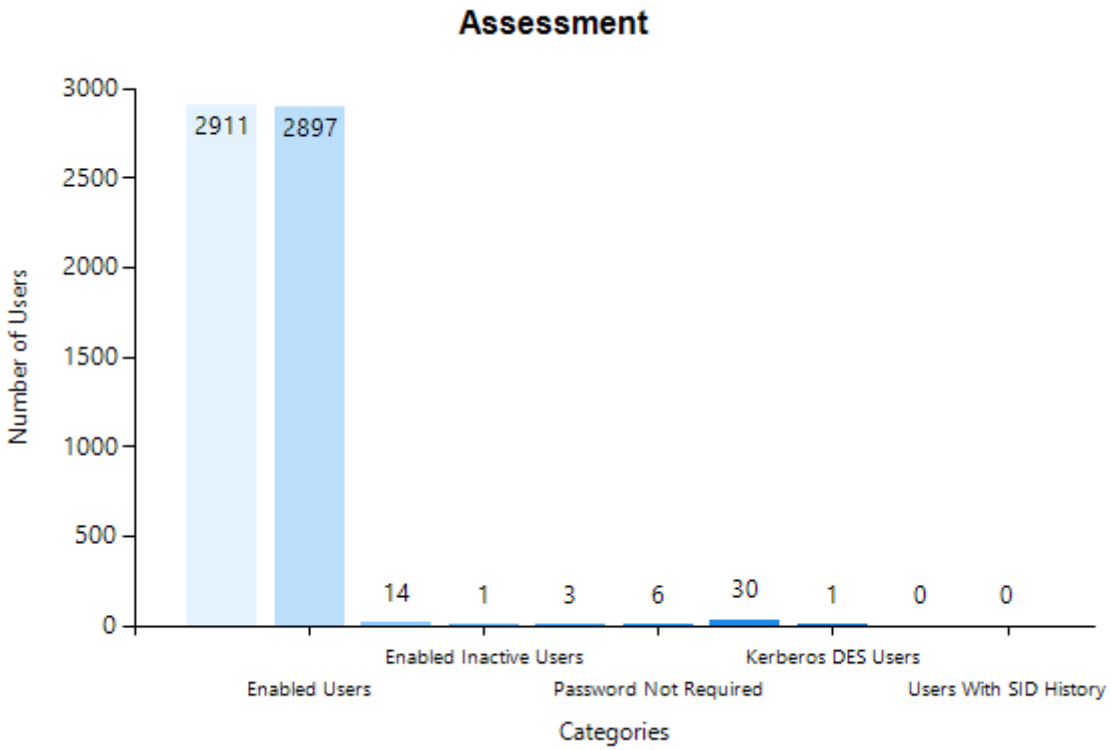
Extension	File Count	Size
.adm	1	0.01 MB
.adml	1	0.03 MB
.admx	1	0.02 MB
.config	7	0.03 MB
.dll	10	12.22 MB
.exe	18	85.80 MB
.ini	1	0.01 MB
.msi	3	150.78 MB
.xml	1	0.00 MB
.zip	5	143.60 MB

Table 28 - Netlogon Folder Status - PHARMAX.LOCAL

Health Check:
Corrective Actions: Make sure Netlogon content 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	2911
Enabled Users	2897
Disabled Users	14
Enabled Inactive Users	1
Users With Reversible Encryption Password	3
Password Not Required	6
Password Never Expires	30
Kerberos DES Users	1
Does Not Require Pre Auth	0
Users With SID History	0

Table 29 - 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

Username	Created	Password Last Set	Last Logon Date
jocolon	12/4/2019	11/30/2021	12/22/2043
svc_SCCM_ClientPush	9/12/2020	9/12/2020	9/14/2020
ELDON_THOMAS	4/5/2022	4/5/2022	-
LEROY_GARZA	4/5/2022	4/5/2022	-
EMILIO_HAMPTON	4/5/2022	4/5/2022	-
CRISTINA_BLACKBURN	4/5/2022	4/5/2022	-
BEULAH_HAYNES	4/5/2022	4/5/2022	-
DAMIAN_LEVY	4/5/2022	4/5/2022	-
MANUEL_KANE	4/5/2022	4/5/2022	-
JUDSON_BULLOCK	4/5/2022	4/5/2022	-
PETE_HOLT	4/5/2022	4/5/2022	-
LESLIE_CARSON	4/5/2022	4/5/2022	-
MABLE_WALTERS	4/5/2022	4/5/2022	-
RACHAEL_JOSEPH	4/5/2022	4/5/2022	-
JARVIS_BRADLEY	4/5/2022	4/5/2022	-
WADE_YOUNG	4/5/2022	4/5/2022	-
JUSTINE_MEYER	4/5/2022	4/5/2022	-
NETTIE_PETTY	4/5/2022	4/5/2022	-
AURORA_BRADSHAW	4/5/2022	4/5/2022	-
TREY_UNDERWOOD	4/5/2022	4/5/2022	-
PETRA_MILLS	4/5/2022	4/5/2022	-
BLANCA_BARNETT	4/5/2022	4/5/2022	-
MAE_BEST	4/5/2022	4/5/2022	-
KORY_HOPPER	4/5/2022	4/5/2022	-
PATRICIA_WYNN	4/5/2022	4/5/2022	-
LYDIA_GEORGE	4/5/2022	4/5/2022	-
DICK_COMPTON	4/5/2022	4/5/2022	-
ERVIN_ORTIZ	4/5/2022	4/5/2022	-
ANGELINA_CASE	4/5/2022	4/5/2022	-
MAJOR_MCMILLAN	4/5/2022	4/5/2022	-
KELLY_SALAZAR	4/5/2022	4/5/2022	-
DENVER_WEEKS	4/5/2022	4/5/2022	-
DICK_LESTER	4/5/2022	4/5/2022	-
RODRICK_HORNE	4/5/2022	4/5/2022	-
LUKE_HAHN	4/5/2022	4/5/2022	-
PASQUALE_BURCH	4/5/2022	4/5/2022	-
ANTWAN_WITT	4/5/2022	4/5/2022	-
MICHAEL_BARRON	4/5/2022	4/5/2022	-
SPENCER_MADDEN	4/5/2022	4/5/2022	-
LAWANDA_JOSEPH	4/5/2022	4/5/2022	-

Username	Created	Password Last Set	Last Logon Date
NICHOLAS_SCHROEDER	4/5/2022	4/5/2022	-

Table 30 - Privileged User Assessment - PHARMAX.LOCAL

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

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
7007675057SA	Yes	4/5/2022	-	CIFS/DR-DC-01V
AUGUST_REESE	Yes	4/5/2022	-	CIFS/ESMWAPPS1000002
ADRIANA_OBRIEN	Yes	4/5/2022	-	CIFS/ESMWWKS1000002
LUIS_SIMS	Yes	4/5/2022	-	CIFS/ESX-01A
MYRON_SINGLETON	Yes	4/5/2022	-	CIFS/FINWVIR1000000
HILDA_HOPKINS	Yes	4/5/2022	-	CIFS/FINWWKS1000001
MONTE_NEAL	Yes	4/5/2022	-	CIFS/HORIZON-MGT-01V
ANDREW_NOLAN	Yes	4/5/2022	-	CIFS/ISILON_NAS
EMMANUEL_HUBER	Yes	4/5/2022	-	CIFS/it1780782727
FLOSSIE_CHAN	Yes	4/5/2022	-	CIFS/NAS
DARWIN_MCKAY	Yes	4/5/2022	-	CIFS/NAS-DR
BRAD_SHIELDS	Yes	4/5/2022	-	CIFS/NAS-VEEAM
DOMINGO_JORDAN	Yes	4/5/2022	-	CIFS/NTAPWFA-01V
DOMINIC_FRAZIER	Yes	4/5/2022	-	CIFS/OGCWWEBS1000000
GREG_BUCKLEY	Yes	4/5/2022	-	CIFS/OGCWWKS1000002
LOUELLA_OCHOA	Yes	4/5/2022	-	CIFS/Pharmax-Cluster
MARY_VINCENT	Yes	4/5/2022	-	CIFS/SERVER-DC-01V
LAZARO_MAYNARD	Yes	4/5/2022	-	CIFS/VEEAM-EM
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
BETSY_MORGAN	Yes	4/5/2022	-	ftp/CAYEY-DC-01V
CESAR_FLOYD	Yes	4/5/2022	-	ftp/FSRWAPPS1000000
326142106SA	Yes	4/5/2022	-	ftp/HORIZON-CAP-01V
DIEGO_LEBLANC	Yes	4/5/2022	-	ftp/HV-SERVER-01V
PRESTON_CHARLES	Yes	4/5/2022	-	ftp/NFS
LANE_CASTANEDA	Yes	4/5/2022	-	ftp/NTAPWFA-01V
ELEANOR_ROSA	Yes	4/5/2022	-	ftp/OGCWVIR1000000
JAVIER_HEATH	Yes	4/5/2022	-	ftp/SCCM-DP-01V

Username	Enabled	Password Last Set	Last Logon Date	Service Principal Name
HEATHER_MUNOZ	Yes	4/5/2022	-	ftp/SCCM-PC-01V
CALVIN_DAVID	Yes	4/5/2022	-	ftp/SQLCluster
LAWRENCE_TANNER	Yes	4/5/2022	-	kafka/HORIZON-CP-01V ftp/VEEAM-DD
WALLACE_MARSH	Yes	4/5/2022	-	ftp/VEEAM-DXI
srmrecadmin	Yes	10/25/2021	-	ftp/VEEAM-EM
JORDAN_BURT	Yes	4/5/2022	-	ftp/VEEAM-VBR-10V
LUPE_BOYLE	Yes	4/5/2022	-	ftp/vm-01v
MEL_HERMAN	Yes	4/5/2022	-	https/ACAD-DNS-01V
JEANNINE_TERRY	Yes	4/5/2022	-	https/ESX-01B
horizon-ic	Yes	4/10/2023	5/1/2023	https/GOOWLPT1000001
DANIELLE_GALLAGHER	Yes	4/5/2022	-	https/HORIZON-JMP-01V
CHRIS_BOLTON	Yes	4/5/2022	-	https/HORIZON-MGT-01V POP3/SERVER-01V
LORENZO_GUZMAN	Yes	4/5/2022	-	https/HORIZON-RDS-01T
BRENTON_HAYDEN	Yes	4/5/2022	-	https/it131896688
ARACELI_CARLSON	Yes	4/5/2022	-	https/ITSWSECS1000000
9167612969SA	Yes	4/5/2022	-	https/NAS
KORY_PIERCE	Yes	4/5/2022	-	https/NTAPWIN-01V
JORDAN_ROSALES	Yes	4/5/2022	-	https/OGCWLPT1000002
HANK_BECKER	Yes	4/5/2022	-	https/SCCM-DB-01V
TRISHA_PRUITT	Yes	4/5/2022	-	https/SERVER-ADFS-02V
MAUREEN_KELLER	Yes	4/5/2022	-	https/server-rds-03v POP3/HORIZON-APV-01V
CYRUS_GRAHAM	Yes	4/5/2022	-	https/SQLCluster
BETTIE_MORRIS	Yes	4/5/2022	-	https/SQLSERVER-00V
SHELDON_ACOSTA	Yes	4/5/2022	-	https/TSTWWEBS1000000
ELINOR_AYALA	Yes	4/5/2022	-	https/VCENTER-01V
RICKEY_EDWARDS	Yes	4/5/2022	-	https/VEEAM-VBR-02V
FREDRICK_RHODES	Yes	4/5/2022	-	https/vm-02v
DEBORA_HANSEN	Yes	4/5/2022	-	kafka/AZRWAPPS1000000
MARLENE_ALBERT	Yes	4/5/2022	-	kafka/DR-DC-01V
JONAS_MOODY	Yes	4/5/2022	-	kafka/HORIZON-JMP-01V
BOBBIE_BRAY	Yes	4/5/2022	-	kafka/HORIZON-SQL-01V
DEBORA_OWEN	Yes	4/5/2022	-	kafka/HREWWKS1000000
MONA_MCLEOD	Yes	4/5/2022	-	kafka/ITSWLPT1000000
DOYLE_CASE	Yes	4/5/2022	-	kafka/NAS-DR
3527874691SA	Yes	4/5/2022	-	kafka/NAS-EDGE
GEORGIA_WEISS	Yes	4/5/2022	-	kafka/OGCWCTRX1000000

Username	Enabled	Password Last Set	Last Logon Date	Service Principal Name
ALTHEA_GUTHRIE	Yes	4/5/2022	-	kafka/ONTAP-7TT POP3/VEEAM-SQL
DOMINICK_VALDEZ	Yes	4/5/2022	-	kafka/SECWDBAS1000000
STAN_FORBES	Yes	4/5/2022	-	kafka/VEEAM-DD
MERVIN_WADE	Yes	4/5/2022	-	kafka/VEEAM-DXI
TESSA_ROGERS	Yes	4/5/2022	-	kafka/VEEAM-SP
RAUL_SANDOVAL	Yes	4/5/2022	-	kafka/vm-001v
RUDOLPH_WHITNEY	Yes	4/5/2022	-	MSSQL/AWSWVIR1000000
INEZ_CALDWELL	Yes	4/5/2022	-	MSSQL/FINWWKS1000000
4791895802SA	Yes	4/5/2022	-	MSSQL/HORIZON-APV-01V
CHARMAINE_RHODES	Yes	3/18/2023	3/18/2023	MSSQL/HORIZON-CAP-01V
MYLES_PETERSEN	Yes	4/5/2022	-	MSSQL/HORIZON-MGT-01V
JANELL_FITZGERALD	Yes	4/5/2022	-	MSSQL/ISILON_NAS
MARGO_HOBBS	Yes	4/5/2022	-	MSSQL/NTAPRHAT-01V
327437901SA	Yes	4/5/2022	-	MSSQL/NTAPWFA-01V
BRADLY_MCFARLAND	Yes	4/5/2022	-	MSSQL/OGCWVIR1000000
EMMA_PARKS	Yes	4/5/2022	-	MSSQL/SQL-CLUSTER-02V
SEBASTIAN_BARNES	Yes	4/5/2022	-	MSSQL/SQLSERVER-01
KELLY_PERKINS	Yes	4/5/2022	-	MSSQL/TSTWSECS1000001
LUKE_DYER	Yes	4/5/2022	-	MSSQL/VEEAM-PC
MICHAEL_LANG	Yes	4/5/2022	-	POP3/AZRWWKS1000000
CRISTINA_BLACKBURN	Yes	4/5/2022	-	POP3/ESX-01B
LAMONT_MORGAN	Yes	4/5/2022	-	POP3/FINWWKS1000000
DARIUS_STEIN	Yes	4/5/2022	-	POP3/HORIZON-FPC-01V
FEDERICO_FIELDS	Yes	4/5/2022	-	POP3/HORIZON-PROV-01
SASHA_PORTER	Yes	4/5/2022	-	POP3/HREWWEBS1000000
CLAUDIA_CARLSON	Yes	4/5/2022	-	POP3/ITSWVIR1000000
REX_FERGUSON	Yes	4/5/2022	-	POP3/SCCM-DP-01V
HARRY_DOTSON	Yes	4/5/2022	-	POP3/SQLSERVER-00V
BRENT_WILLIAMS	Yes	4/5/2022	-	POP3/TSTWWKS1000000
MARICELA_GARDNER	Yes	4/5/2022	-	POP3/VEEAM-HV-01
CLAUDE_BOYD	Yes	4/5/2022	-	POP3/vm-001v
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

Username	Enabled	Password Last Set	Last Logon Date	Service Principal Name
				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 31 - Service Accounts Assessment - PHARMAX.LOCAL

Health Check:
Corrective Actions: Service accounts are that gray area between regular user accounts and admin accounts that are often highly privileged. They are almost always over-privileged due to documented vendor requirements or because of operational challenges. Ensure there aren't any account with weak security posture.

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 32 - 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 33 - 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 34 - 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 35 - Duplicate Object - PHARMAX.LOCAL

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

1.2.1.15 Domain Controllers

A domain controller (DC) is a server computer that responds to security authentication requests within a computer network domain. It is a network server that is responsible for allowing host access to domain resources. It authenticates users, stores user account information and enforces security policy for a domain.

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 36 - Domain Controllers - PHARMAX.LOCAL

1.2.1.15.1 Hardware Inventory

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

SERVER-DC-01V

Name	SERVER-DC-01V
Windows Product Name	Windows Server 2019 Standard
Windows Current Version	6.3
Windows Build Number	10.0.17763
Windows Install Type	Server
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
Serial Number	
Bios Type	Uefi
BIOS Version	
Processor Manufacturer	GenuineIntel
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 37 - Hardware Inventory - SERVER-DC-01V

CAYEY-DC-01V

Name	CAYEY-DC-01V
Windows Product Name	Windows Server 2019 Standard Evaluation
Windows Current Version	6.3
Windows Build Number	10.0.17763
Windows Install Type	Server
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	Retail:TB:Eval
Partial Product Key	Y7XRX
Manufacturer	VMware, Inc.
Model	VMware7,1

Serial Number	
Bios Type	Uefi
BIOS Version	
Processor Manufacturer	GenuineIntel
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 38 - Hardware Inventory - CAYEY-DC-01V

1.2.1.15.2 NTDS Information

DC Name	Database File	Database Size	Log Path	SysVol Path
CAYEY-DC-01V	C:\Windows\NTDS\ntds.dit	124.00 MB	C:\Windows\NTDS	C:\Windows\SYSVOL\sysvol
SERVER-DC-01V	C:\Windows\NTDS\ntds.dit	130.00 MB	C:\Windows\NTDS	C:\Windows\SYSVOL\sysvol

Table 39 - NTDS Database File Usage - PHARMAX.LOCAL

1.2.1.15.3 Time Source Information

Name	Time Server	Type
CAYEY-DC-01V	Domain Hierarchy	DOMHIER
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)

Table 40 - Time Source Configuration - PHARMAX.LOCAL

1.2.1.15.4 SRV Records Status

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

Table 41 - SRV Records Status - PHARMAX.LOCAL

Health Check:

Best Practice: The SRV record is a Domain Name System (DNS) resource record. It's used to identify computers hosting specific services. SRV resource records are used to locate domain controllers for Active Directory.

1.2.1.15.5 Installed Software

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

SERVER-DC-01V

Name	Publisher	Install Date
7-Zip 19.00 (x64)	Igor Pavlov	--
DiskMax 6.21	KoshyJohn.com	17/11/2021
Google Chrome	Google LLC	20230518
Npcap	Nmap Project	--
RVTools	Robware	20220824
Veeam Agent for Microsoft Windows	Veeam Software Group GmbH	20230215
Veeam Backup Transport	Veeam Software Group GmbH	20230215
Veeam Backup VSS Integration	Veeam Software Group GmbH	20230215
Veeam Installer Service	Veeam Software Group GmbH	--
Veeam VSS Hardware Provider	Veeam Software Group GmbH	20230216

Table 42 - Installed Software - SERVER-DC-01V

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

CAYEY-DC-01V

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

Table 43 - Installed Software - CAYEY-DC-01V

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

1.2.1.15.6 Roles

The following section provides a summary of the Domain Controller Role & Features information.

SERVER-DC-01V

Name	Parent	InstallState
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.

Name	Parent	InstallState
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 44 - 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.

CAYEY-DC-01V

Name	Parent	InstallState
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

Name	Parent	InstallState
		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 45 - 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.

1.2.1.15.7 DC Diagnostic

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

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).

Test Name	Result	Impact	Description
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.
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.

Test Name	Result	Impact	Description
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 46 - DCDiag Test Status - SERVER-DC-01V

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.

Test Name	Result	Impact	Description
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.
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

Test Name	Result	Impact	Description
			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 47 - DCDiag Test Status - CAYEY-DC-01V

1.2.1.15.8 Infrastructure Services Status

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

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 48 - 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.

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
DFS Replication	DFSR	Running

Display Name	Short Name	Status
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 49 - 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.

1.2.1.15.9 Sites Replication Connection

The following section provides detailed information about Site Replication Connection.

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

GUID	d5a28ae4-ee92-47a4-872e-e4115bc8d1a5
Description	--
Replicate From Directory Server	ACADE-DC-01V
Replicate To Directory 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 50 - Site Replication - SERVER-DC-01V

From: CAYEY-DC-01V To: SERVER-DC-01V

GUID	9dd36d8c-c157-4886-b411-c316fdf19c86
Description	--

Replicate From Directory Server	CAYEY-DC-01V
Replicate To Directory 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	Tue, 07 Dec 2021 15:52:27 GMT

Table 51 - Site Replication - SERVER-DC-01V

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

GUID	aabfef5a-f968-4f1e-b02e-9625f6731933
Description	--
Replicate From Directory Server	DC-UIA-01V
Replicate To Directory 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 52 - Site Replication - SERVER-DC-01V

1.2.1.15.10 Sites Replication Status

Source DSA	Destination DSA	Source DSA Site	Last Success Time	Last Failure Status	Last Failure Time	Number of failures
ACADE-DC-01V	SERVER-DC-01V	ACAD	2023-05-23 16:46:45	0	0	0
ACADE-DC-01V	SERVER-DC-01V	ACAD	2023-05-23 16:46:45	0	0	0
ACADE-DC-01V	SERVER-DC-01V	ACAD	2023-05-23 16:46:45	0	0	0
ACADE-DC-01V	SERVER-DC-01V	ACAD	2023-05-23 16:46:45	0	0	0

Source DSA	Destination DSA	Source DSA Site	Last Success Time	Last Failure Status	Last Failure Time	Number of failures
ACADE-DC-01V	SERVER-DC-01V	ACAD	2023-05-23 16:46:45	0	0	0
CAYEY-DC-01V	SERVER-DC-01V	Cayey-Branch	2023-05-23 16:46:45	0	0	0
CAYEY-DC-01V	SERVER-DC-01V	Cayey-Branch	2023-05-23 16:46:45	0	0	0
CAYEY-DC-01V	SERVER-DC-01V	Cayey-Branch	2023-05-23 16:46:45	0	0	0
CAYEY-DC-01V	SERVER-DC-01V	Cayey-Branch	2023-05-23 16:46:45	0	0	0
CAYEY-DC-01V	SERVER-DC-01V	Cayey-Branch	2023-05-23 16:46:45	0	0	0
DC-UIA-01V	SERVER-DC-01V	UIA	2023-05-23 16:46:45	0	0	0
DC-UIA-01V	SERVER-DC-01V	UIA	2023-05-23 16:46:45	0	0	0
DC-UIA-01V	SERVER-DC-01V	UIA	2023-05-23 16:46:45	0	0	0
DC-UIA-01V	SERVER-DC-01V	UIA	2023-05-23 16:46:45	0	0	0
DC-UIA-01V	SERVER-DC-01V	UIA	2023-05-23 16:46:45	0	0	0

Table 53 - Site Replication Status - PHARMAX.LOCAL

1.2.1.15.11 Group Policy Objects

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

Assign-Applications

GPO Status	All Settings Enabled
Created	03/10/2021
Modified	04/10/2023
Description	
Owner	PHARMAX\Domain Admins

Table 54 - GPO - Assign-Applications

Certificate AutoEnrollment

GPO Status	User Settings Disabled
Created	01/25/2020

Modified	06/30/2021
Description	
Owner	PHARMAX\Domain Admins

Table 55 - GPO - Certificate AutoEnrollment

Default Domain Policy

GPO Status	All Settings Enabled
Created	06/10/2018
Modified	10/11/2022
Description	
Owner	PHARMAX\Domain Admins

Table 56 - GPO - Default Domain Policy

VEEAM_Disable_Firewall

GPO Status	All Settings Enabled
Created	12/13/2019
Modified	09/08/2020
Description	
Owner	PHARMAX\Domain Admins

Table 57 - GPO - VEEAM_Disable_Firewall

SET - KMS Server

GPO Status	All Settings Enabled
Created	08/31/2022
Modified	08/31/2022
Description	
Owner	PHARMAX\Domain Admins

Table 58 - GPO - SET - KMS Server

Default Domain Controllers Policy

GPO Status	All Settings Enabled
Created	06/10/2018
Modified	03/23/2023
Description	
Owner	PHARMAX\Domain Admins

Table 59 - GPO - Default Domain Controllers Policy

ProfileUnity

GPO Status	All Settings Enabled
Created	06/08/2020
Modified	10/05/2021
Description	
Owner	PHARMAX\Domain Admins

Table 60 - GPO - ProfileUnity

VEEAM_Local_Administrators

GPO Status	All Settings Enabled
Created	12/13/2019
Modified	05/20/2022
Description	
Owner	PHARMAX\Domain Admins

Table 61 - GPO - VEEAM_Local_Administrators

WSUS - Domain Policy

GPO Status	User Settings Disabled
Created	02/23/2020
Modified	03/10/2021
Description	
Owner	PHARMAX\Domain Admins

Table 62 - GPO - WSUS - Domain Policy

SCEP Configuration

GPO Status	All Settings Enabled
Created	09/14/2020
Modified	10/04/2020
Description	
Owner	PHARMAX\Domain Admins

Table 63 - GPO - SCEP Configuration

Dead Policy

GPO Status	All Settings Disabled
Created	10/05/2021
Modified	01/22/2022
Description	
Owner	PHARMAX\Domain Admins

Table 64 - GPO - Dead Policy

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

Horizon-DEM

GPO Status	All Settings Enabled
Created	03/01/2020
Modified	09/08/2020
Description	
Owner	PHARMAX\Domain Admins

Table 65 - GPO - Horizon-DEM

Linux-Settings-GPO

GPO Status	All Settings Disabled
Created	05/22/2021
Modified	02/04/2022
Description	
Owner	PHARMAX\Domain Admins

Table 66 - 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
Created	09/12/2020
Modified	09/12/2020
Description	
Owner	PHARMAX\Domain Admins

Table 67 - GPO - SCCM - Restricted Group and General Settings

LAPS Configuration

GPO Status	All Settings Enabled
Created	11/01/2020
Modified	11/01/2020
Description	
Owner	PHARMAX\Domain Admins

Table 68 - GPO - LAPS Configuration

1.2.1.15.11.1 Central Store Repository

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

Table 69 - GPO Central Store - PHARMAX.LOCAL

1.2.1.15.11.2 User 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
ProfileUnity	All Settings Enabled	Logoff	%systemdrive%\Program Files\ProfileUnity\Client.NET\LwL.ProfileUnity.Client.Logoff.exe

Table 70 - GPO with Logon/Logoff Script - PHARMAX.LOCAL

1.2.1.15.11.3 Computer Startup/Shutdown Script

GPO Name	GPO Status	Type	Script
Dead Policy	All Settings Disabled	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 71 - GPO with Startup/Shutdown Script - PHARMAX.LOCAL

1.2.1.15.11.4 Unlinked GPO

GPO Name	Created	Modified	Computer Enabled	User Enabled
Dead Policy	2021-10-05	2022-01-22	No	No

Table 72 - Unlinked GPO - PHARMAX.LOCAL

Health Check:
Corrective Actions: Remove Unused GPO from Active Directory.

1.2.1.15.11.5 Empty GPOs

GPO Name	Created	Modified	Description
Linux-Settings-GPO	2021-05-23	2022-02-04	--

Table 73 - Empty GPO - PHARMAX.LOCAL

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

1.2.1.15.11.6 Enforced GPO

GPO Name	Enforced	Order	Target
Linux-Settings-GPO	Yes	1	pharmax.local/LinuxMachines

Table 74 - Enforced GPO - PHARMAX.LOCAL

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

1.2.1.15.12 Organizational Units

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

Name	Path	Linked GPO
.SecFrame.com	pharmax.local/.SecFrame.com	--
Admin	pharmax.local/Admin	--
Staging	pharmax.local/Admin/Staging	--
Tier 0	pharmax.local/Admin/Tier 0	--
T0-Accounts	pharmax.local/Admin/Tier 0/T0-Accounts	--
T0-Devices	pharmax.local/Admin/Tier 0/T0-Devices	--
T0-Permissions	pharmax.local/Admin/Tier 0/T0-Permissions	--
T0-Roles	pharmax.local/Admin/Tier 0/T0-Roles	--
T0-Servers	pharmax.local/Admin/Tier 0/T0-Servers	--
Tier 1	pharmax.local/Admin/Tier 1	--
T1-Accounts	pharmax.local/Admin/Tier 1/T1-Accounts	--
T1-Devices	pharmax.local/Admin/Tier 1/T1-Devices	--
T1-Permissions	pharmax.local/Admin/Tier 1/T1-Permissions	--
T1-Roles	pharmax.local/Admin/Tier 1/T1-Roles	--
T1-Servers	pharmax.local/Admin/Tier 1/T1-Servers	--
Tier 2	pharmax.local/Admin/Tier 2	--

Name	Path	Linked GPO
T2-Accounts	pharmax.local/Admin/Tier 2/T2-Accounts	--
T2-Devices	pharmax.local/Admin/Tier 2/T2-Devices	--
T2-Permissions	pharmax.local/Admin/Tier 2/T2-Permissions	--
T2-Roles	pharmax.local/Admin/Tier 2/T2-Roles	--
T2-Servers	pharmax.local/Admin/Tier 2/T2-Servers	--
Admins PC	pharmax.local/Admins PC	--
Configuration Manager	pharmax.local/Configuration Manager	SCEP Configuration, SCCM - Restricted Group and General Settings
Configuration Manager Computers	pharmax.local/Configuration Manager Computers	LAPS Configuration, SCEP Configuration
Domain Controllers	pharmax.local/Domain Controllers	Default Domain Controllers Policy
EMC NAS servers	pharmax.local/EMC NAS servers	--
Computers	pharmax.local/EMC NAS servers/Computers	--
Fortinet EMS	pharmax.local/Fortinet EMS	--
Grouper-Groups	pharmax.local/Grouper-Groups	--
LinuxMachines	pharmax.local/LinuxMachines	Linux-Settings-GPO
Member Servers	pharmax.local/Member Servers	--
Microsoft Exchange Security Groups	pharmax.local/Microsoft Exchange Security Groups	--
People	pharmax.local/People	--
AWS	pharmax.local/People/AWS	--
AZR	pharmax.local/People/AZR	--
BDE	pharmax.local/People/BDE	--
Deprovisioned	pharmax.local/People/Deprovisioned	--
ESM	pharmax.local/People/ESM	--
FIN	pharmax.local/People/FIN	--
FSR	pharmax.local/People/FSR	--
GOO	pharmax.local/People/GOO	--
HRE	pharmax.local/People/HRE	--
ITS	pharmax.local/People/ITS	--
OGC	pharmax.local/People/OGC	--
SEC	pharmax.local/People/SEC	--
TST	pharmax.local/People/TST	--
Unassociated	pharmax.local/People/Unassociated	--
ProfileUnity VDI	pharmax.local/ProfileUnity VDI	VEEAM_Local_Administrators, VEEAM_Disable_Firewall
Computers	pharmax.local/ProfileUnity VDI/Computers	ProfileUnity

Name	Path	Linked GPO
Servers	pharmax.local/ProfileUnity VDI/Servers	--
Quarantine	pharmax.local/Quarantine	--
Stage	pharmax.local/Stage	--
AWS	pharmax.local/Stage/AWS	--
Devices	pharmax.local/Stage/AWS/Devices	--
Groups	pharmax.local/Stage/AWS/Groups	--
ServiceAccounts	pharmax.local/Stage/AWS/ServiceAccounts	--
Test	pharmax.local/Stage/AWS/Test	--
AZR	pharmax.local/Stage/AZR	--
Devices	pharmax.local/Stage/AZR/Devices	--
Groups	pharmax.local/Stage/AZR/Groups	--
ServiceAccounts	pharmax.local/Stage/AZR/ServiceAccounts	--
Test	pharmax.local/Stage/AZR/Test	--
BDE	pharmax.local/Stage/BDE	--
Devices	pharmax.local/Stage/BDE/Devices	--
Groups	pharmax.local/Stage/BDE/Groups	--
ServiceAccounts	pharmax.local/Stage/BDE/ServiceAccounts	--
Test	pharmax.local/Stage/BDE/Test	--
ESM	pharmax.local/Stage/ESM	--
Devices	pharmax.local/Stage/ESM/Devices	--
Groups	pharmax.local/Stage/ESM/Groups	--
ServiceAccounts	pharmax.local/Stage/ESM/ServiceAccounts	--
Test	pharmax.local/Stage/ESM/Test	--
FIN	pharmax.local/Stage/FIN	--
Devices	pharmax.local/Stage/FIN/Devices	--
Groups	pharmax.local/Stage/FIN/Groups	--
ServiceAccounts	pharmax.local/Stage/FIN/ServiceAccounts	--
Test	pharmax.local/Stage/FIN/Test	--
FSR	pharmax.local/Stage/FSR	--
Devices	pharmax.local/Stage/FSR/Devices	--
Groups	pharmax.local/Stage/FSR/Groups	--
ServiceAccounts	pharmax.local/Stage/FSR/ServiceAccounts	--
Test	pharmax.local/Stage/FSR/Test	--
GOO	pharmax.local/Stage/GOO	--
Devices	pharmax.local/Stage/GOO/Devices	--

Name	Path	Linked GPO
Groups	pharmax.local/Stage/GOO/Groups	--
ServiceAccounts	pharmax.local/Stage/GOO/ServiceAccounts	--
Test	pharmax.local/Stage/GOO/Test	--
HRE	pharmax.local/Stage/HRE	--
Devices	pharmax.local/Stage/HRE/Devices	--
Groups	pharmax.local/Stage/HRE/Groups	--
ServiceAccounts	pharmax.local/Stage/HRE/ServiceAccounts	--
Test	pharmax.local/Stage/HRE/Test	--
ITS	pharmax.local/Stage/ITS	--
Devices	pharmax.local/Stage/ITS/Devices	--
Groups	pharmax.local/Stage/ITS/Groups	--
ServiceAccounts	pharmax.local/Stage/ITS/ServiceAccounts	--
Test	pharmax.local/Stage/ITS/Test	--
OGC	pharmax.local/Stage/OGC	--
Devices	pharmax.local/Stage/OGC/Devices	--
Groups	pharmax.local/Stage/OGC/Groups	--
ServiceAccounts	pharmax.local/Stage/OGC/ServiceAccounts	--
Test	pharmax.local/Stage/OGC/Test	--
SEC	pharmax.local/Stage/SEC	--
Devices	pharmax.local/Stage/SEC/Devices	--
Groups	pharmax.local/Stage/SEC/Groups	--
ServiceAccounts	pharmax.local/Stage/SEC/ServiceAccounts	--
Test	pharmax.local/Stage/SEC/Test	--
TST	pharmax.local/Stage/TST	--
Devices	pharmax.local/Stage/TST/Devices	--
Groups	pharmax.local/Stage/TST/Groups	--
ServiceAccounts	pharmax.local/Stage/TST/ServiceAccounts	--
Test	pharmax.local/Stage/TST/Test	--
Testing	pharmax.local/Testing	--
Tier 1	pharmax.local/Tier 1	--
AWS	pharmax.local/Tier 1/AWS	--
Devices	pharmax.local/Tier 1/AWS/Devices	--
Groups	pharmax.local/Tier 1/AWS/Groups	--
ServiceAccounts	pharmax.local/Tier 1/AWS/ServiceAccounts	--

Name	Path	Linked GPO
Test	pharmax.local/Tier 1/AWS/Test	--
AZR	pharmax.local/Tier 1/AZR	--
Devices	pharmax.local/Tier 1/AZR/Devices	--
Groups	pharmax.local/Tier 1/AZR/Groups	--
ServiceAccounts	pharmax.local/Tier 1/AZR/ServiceAccounts	--
Test	pharmax.local/Tier 1/AZR/Test	--
BDE	pharmax.local/Tier 1/BDE	--
Devices	pharmax.local/Tier 1/BDE/Devices	--
Groups	pharmax.local/Tier 1/BDE/Groups	--
ServiceAccounts	pharmax.local/Tier 1/BDE/ServiceAccounts	--
Test	pharmax.local/Tier 1/BDE/Test	--
ESM	pharmax.local/Tier 1/ESM	--
Devices	pharmax.local/Tier 1/ESM/Devices	--
Groups	pharmax.local/Tier 1/ESM/Groups	--
ServiceAccounts	pharmax.local/Tier 1/ESM/ServiceAccounts	--
Test	pharmax.local/Tier 1/ESM/Test	--
FIN	pharmax.local/Tier 1/FIN	--
Devices	pharmax.local/Tier 1/FIN/Devices	--
Groups	pharmax.local/Tier 1/FIN/Groups	--
ServiceAccounts	pharmax.local/Tier 1/FIN/ServiceAccounts	--
Test	pharmax.local/Tier 1/FIN/Test	--
FSR	pharmax.local/Tier 1/FSR	--
Devices	pharmax.local/Tier 1/FSR/Devices	--
Groups	pharmax.local/Tier 1/FSR/Groups	--
ServiceAccounts	pharmax.local/Tier 1/FSR/ServiceAccounts	--
Test	pharmax.local/Tier 1/FSR/Test	--
GOO	pharmax.local/Tier 1/GOO	--
Devices	pharmax.local/Tier 1/GOO/Devices	--
Groups	pharmax.local/Tier 1/GOO/Groups	--
ServiceAccounts	pharmax.local/Tier 1/GOO/ServiceAccounts	--
Test	pharmax.local/Tier 1/GOO/Test	--
HRE	pharmax.local/Tier 1/HRE	--
Devices	pharmax.local/Tier 1/HRE/Devices	--
Groups	pharmax.local/Tier 1/HRE/Groups	--

Name	Path	Linked GPO
ServiceAccounts	pharmax.local/Tier 1/HRE/ServiceAccounts	--
Test	pharmax.local/Tier 1/HRE/Test	--
ITS	pharmax.local/Tier 1/ITS	--
Devices	pharmax.local/Tier 1/ITS/Devices	--
Groups	pharmax.local/Tier 1/ITS/Groups	--
ServiceAccounts	pharmax.local/Tier 1/ITS/ServiceAccounts	--
Test	pharmax.local/Tier 1/ITS/Test	--
OGC	pharmax.local/Tier 1/OGC	--
Devices	pharmax.local/Tier 1/OGC/Devices	--
Groups	pharmax.local/Tier 1/OGC/Groups	--
ServiceAccounts	pharmax.local/Tier 1/OGC/ServiceAccounts	--
Test	pharmax.local/Tier 1/OGC/Test	--
SEC	pharmax.local/Tier 1/SEC	--
Devices	pharmax.local/Tier 1/SEC/Devices	--
Groups	pharmax.local/Tier 1/SEC/Groups	--
ServiceAccounts	pharmax.local/Tier 1/SEC/ServiceAccounts	--
Test	pharmax.local/Tier 1/SEC/Test	--
TST	pharmax.local/Tier 1/TST	--
Devices	pharmax.local/Tier 1/TST/Devices	--
Groups	pharmax.local/Tier 1/TST/Groups	--
ServiceAccounts	pharmax.local/Tier 1/TST/ServiceAccounts	--
Test	pharmax.local/Tier 1/TST/Test	--
Tier 2	pharmax.local/Tier 2	--
AWS	pharmax.local/Tier 2/AWS	--
Devices	pharmax.local/Tier 2/AWS/Devices	--
Groups	pharmax.local/Tier 2/AWS/Groups	--
ServiceAccounts	pharmax.local/Tier 2/AWS/ServiceAccounts	--
Test	pharmax.local/Tier 2/AWS/Test	--
AZR	pharmax.local/Tier 2/AZR	--
Devices	pharmax.local/Tier 2/AZR/Devices	--
Groups	pharmax.local/Tier 2/AZR/Groups	--
ServiceAccounts	pharmax.local/Tier 2/AZR/ServiceAccounts	--
Test	pharmax.local/Tier 2/AZR/Test	--
BDE	pharmax.local/Tier 2/BDE	--

Name	Path	Linked GPO
Devices	pharmax.local/Tier 2/BDE/Devices	--
Groups	pharmax.local/Tier 2/BDE/Groups	--
ServiceAccounts	pharmax.local/Tier 2/BDE/ServiceAccounts	--
Test	pharmax.local/Tier 2/BDE/Test	--
ESM	pharmax.local/Tier 2/ESM	--
Devices	pharmax.local/Tier 2/ESM/Devices	--
Groups	pharmax.local/Tier 2/ESM/Groups	--
ServiceAccounts	pharmax.local/Tier 2/ESM/ServiceAccounts	--
Test	pharmax.local/Tier 2/ESM/Test	--
FIN	pharmax.local/Tier 2/FIN	--
Devices	pharmax.local/Tier 2/FIN/Devices	--
Groups	pharmax.local/Tier 2/FIN/Groups	--
ServiceAccounts	pharmax.local/Tier 2/FIN/ServiceAccounts	--
Test	pharmax.local/Tier 2/FIN/Test	--
FSR	pharmax.local/Tier 2/FSR	--
Devices	pharmax.local/Tier 2/FSR/Devices	--
Groups	pharmax.local/Tier 2/FSR/Groups	--
ServiceAccounts	pharmax.local/Tier 2/FSR/ServiceAccounts	--
Test	pharmax.local/Tier 2/FSR/Test	--
GOO	pharmax.local/Tier 2/GOO	--
Devices	pharmax.local/Tier 2/GOO/Devices	--
Groups	pharmax.local/Tier 2/GOO/Groups	--
ServiceAccounts	pharmax.local/Tier 2/GOO/ServiceAccounts	--
Test	pharmax.local/Tier 2/GOO/Test	--
HRE	pharmax.local/Tier 2/HRE	--
Devices	pharmax.local/Tier 2/HRE/Devices	--
Groups	pharmax.local/Tier 2/HRE/Groups	--
ServiceAccounts	pharmax.local/Tier 2/HRE/ServiceAccounts	--
Test	pharmax.local/Tier 2/HRE/Test	--
ITS	pharmax.local/Tier 2/ITS	--
Devices	pharmax.local/Tier 2/ITS/Devices	--
Groups	pharmax.local/Tier 2/ITS/Groups	--
ServiceAccounts	pharmax.local/Tier 2/ITS/ServiceAccounts	--
Test	pharmax.local/Tier 2/ITS/Test	--

Name	Path	Linked GPO
OGC	pharmax.local/Tier 2/OGC	--
Devices	pharmax.local/Tier 2/OGC/Devices	--
Groups	pharmax.local/Tier 2/OGC/Groups	--
ServiceAccounts	pharmax.local/Tier 2/OGC/ServiceAccounts	--
Test	pharmax.local/Tier 2/OGC/Test	--
SEC	pharmax.local/Tier 2/SEC	--
Devices	pharmax.local/Tier 2/SEC/Devices	--
Groups	pharmax.local/Tier 2/SEC/Groups	--
ServiceAccounts	pharmax.local/Tier 2/SEC/ServiceAccounts	--
Test	pharmax.local/Tier 2/SEC/Test	--
TST	pharmax.local/Tier 2/TST	--
Devices	pharmax.local/Tier 2/TST/Devices	--
Groups	pharmax.local/Tier 2/TST/Groups	--
ServiceAccounts	pharmax.local/Tier 2/TST/ServiceAccounts	--
Test	pharmax.local/Tier 2/TST/Test	--
VDI-Computers	pharmax.local/VDI-Computers	Horizon-DEM
Finances	pharmax.local/VDI-Computers/Finances	--
HR	pharmax.local/VDI-Computers/HR	--
Marketing	pharmax.local/VDI-Computers/Marketing	--
Sales	pharmax.local/VDI-Computers/Sales	--
VEEAM Servers	pharmax.local/VEEAM Servers	VEEAM_Disable_Firewall, VEEAM_Local_Administrators
VEEAM WorkStations	pharmax.local/VEEAM WorkStations	VEEAM_Local_Administrators, VEEAM_Disable_Firewall

Table 75 - Organizational Unit - PHARMAX.LOCAL

1.2.1.15.12.1 GPO Blocked Inheritance

OU Name	Container Type	Inheritance Blocked	Path
fortinet ems	OU	Yes	pharmax.local/Fortinet EMS
linuxmachines	OU	Yes	pharmax.local/LinuxMachines

Table 76 - Blocked Inheritance GPO - PHARMAX.LOCAL

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

1.2.2 ACAD.PHARMAX.LOCAL

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

Domain Name	acad
NetBIOS Name	ACAD
Domain SID	S-1-5-21-370360276-377477351-3184454278
Domain Functional Level	Windows2016Domain
Domains	--
Forest	pharmax.local
Parent Domain	pharmax.local
Replica Directory Servers	acade-dc-01v.acad.pharmax.local
Child Domains	--
Domain Path	acad.pharmax.local/
Computers Container	acad.pharmax.local/Computers
Domain Controllers Container	acad.pharmax.local/Domain Controllers
Systems Container	acad.pharmax.local/System
Users Container	acad.pharmax.local/Users
ReadOnly Replica Directory Servers	--
ms-DS-MachineAccountQuota	10
RID Issued	1600
RID Available	1073740223

Table 77 - Domain Summary - ACAD.PHARMAX.LOCAL

1.2.2.1 FSMO Roles

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

Table 78 - FSMO Roles - acad.pharmax.local

1.2.2.2 Domain and Trusts

pharmax.local

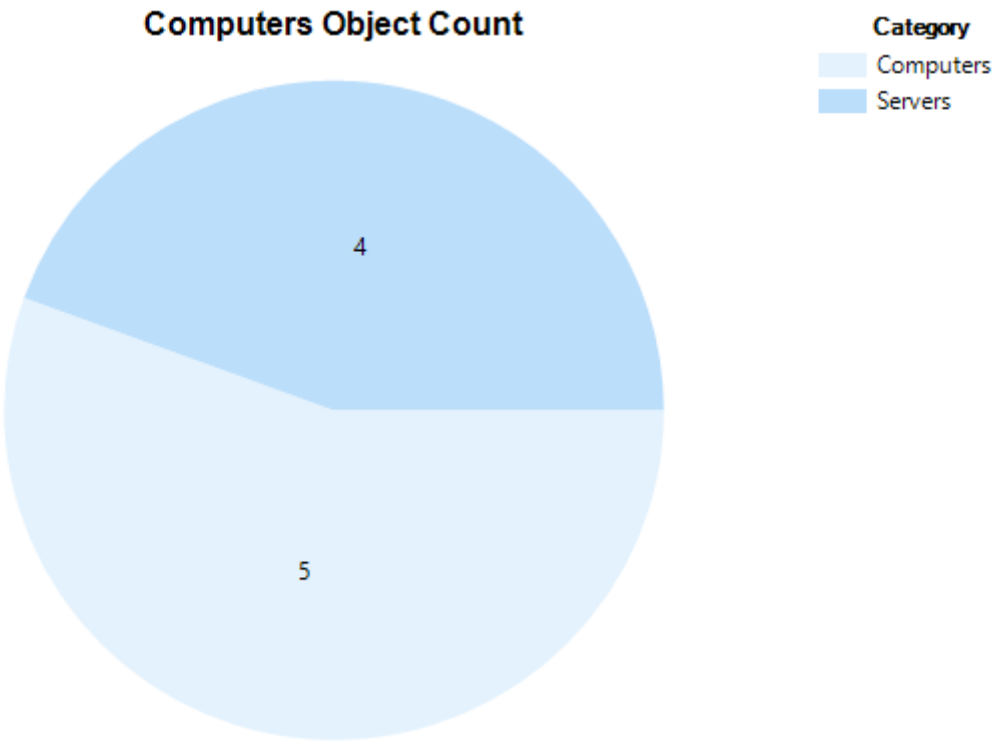
Name	pharmax.local
Path	acad.pharmax.local/System/pharmax.local
Source	acad
Target	pharmax.local

Direction	BiDirectional
IntraForest	Yes
Selective Authentication	No
SID Filtering Forest Aware	No
SID Filtering Quarantined	No
Trust Type	Uplevel
Uplevel Only	No

Table 79 - Trusts - pharmax.local

1.2.2.3 Domain Object Count

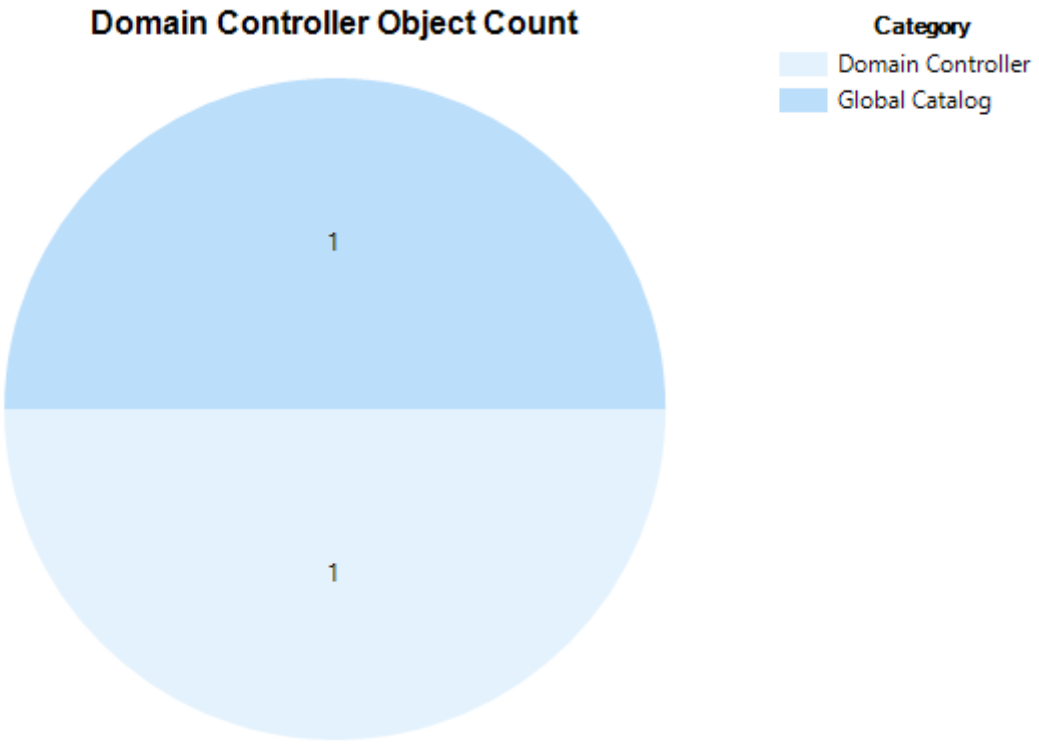
1.2.2.3.1 Computers Object



Computers	5
Servers	4

Table 80 - Computers Object - ACAD.PHARMAX.LOCAL

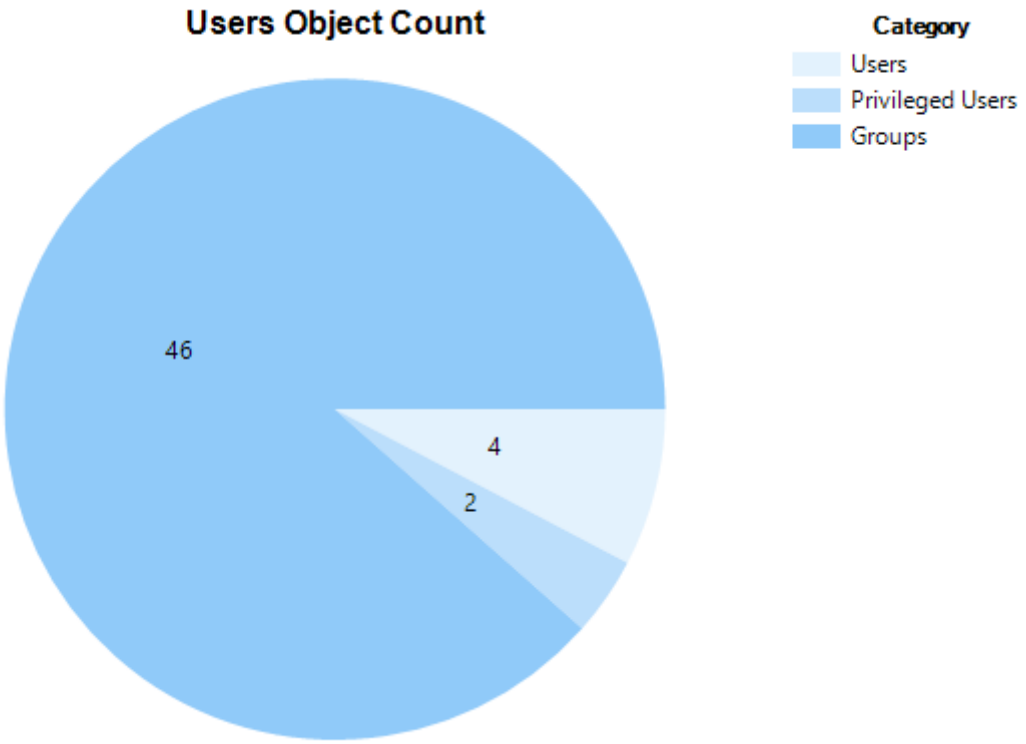
1.2.2.3.2 Domain Controller Object



Domain Controller	1
Global Catalog	1

Table 81 - Domain Controller Object - ACAD.PHARMAX.LOCAL

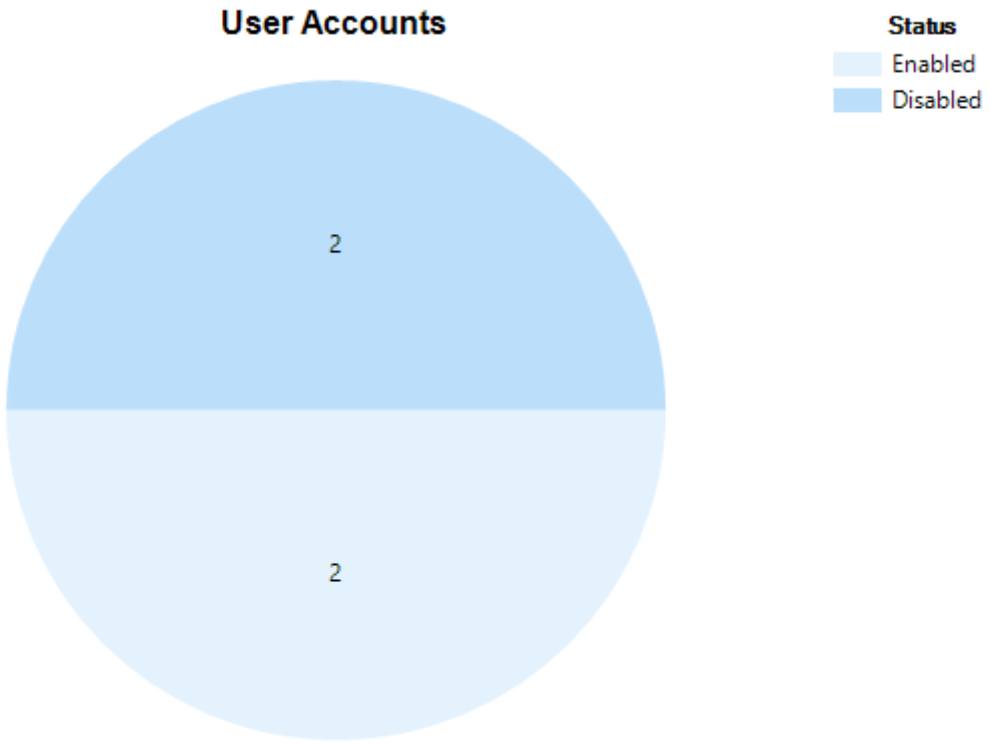
1.2.2.3.3 Users Object



Users	4
Privileged Users	2
Groups	46

Table 82 - User Object - ACAD.PHARMAX.LOCAL

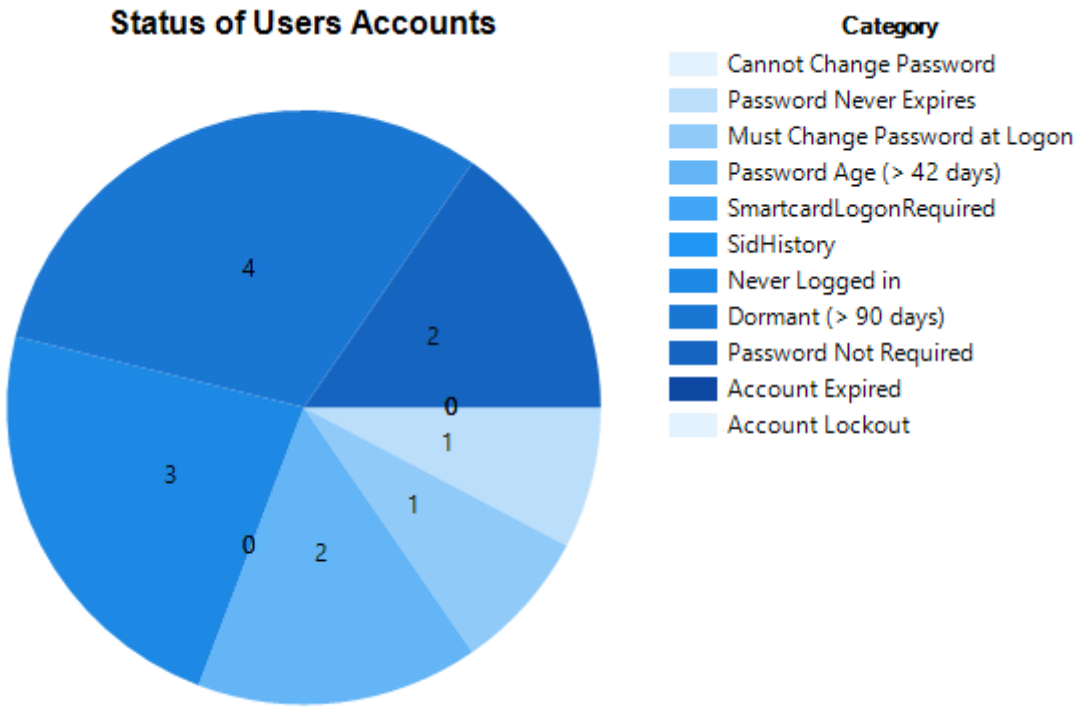
1.2.2.4 User Accounts in Domain



Status	Count	Percentage
Enabled	2	50%
Disabled	2	50%

Table 83 - User Accounts in Domain - ACAD.PHARMAX.LOCAL

1.2.2.5 Status of Users Accounts



Category	Enabled Count	Enabled %	Disabled Count	Disabled %	Total Count	Total %
Cannot Change Password	0	0	1	25	0	0
Password Never Expires	1	25	1	25	1	25
Must Change Password at Logon	1	25	1	25	1	25
Password Age (> 42 days)	2	50	1	25	2	50
SmartcardLogonRequired	0	0	1	25	0	0
SidHistory	0	0	1	25	0	0
Never Logged in	3	75	1	25	3	75
Dormant (> 90 days)	4	100	1	25	4	100
Password Not Required	2	50	1	25	2	50
Account Expired	0	0	1	25	0	0
Account Lockout	0	0	1	25	0	0

Table 84 - Status of User Accounts - ACAD.PHARMAX.LOCAL

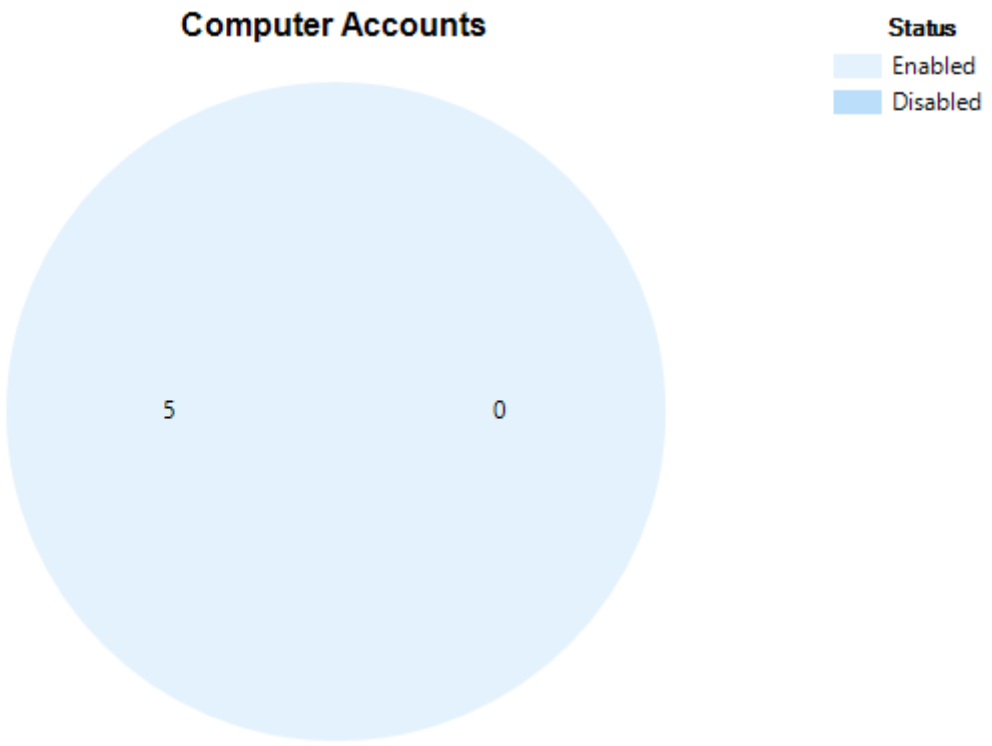
1.2.2.6 Privileged Group Count

Group Name	Count
Account Operators	0
Backup Operators	1
Cert Publishers	1

Group Name	Count
DnsAdmins	0
Domain Admins	1
Key Admins	0
Print Operators	0
Remote Desktop Users	0
Server Operators	0

Table 85 - Privileged Group Count - ACAD.PHARMAX.LOCAL

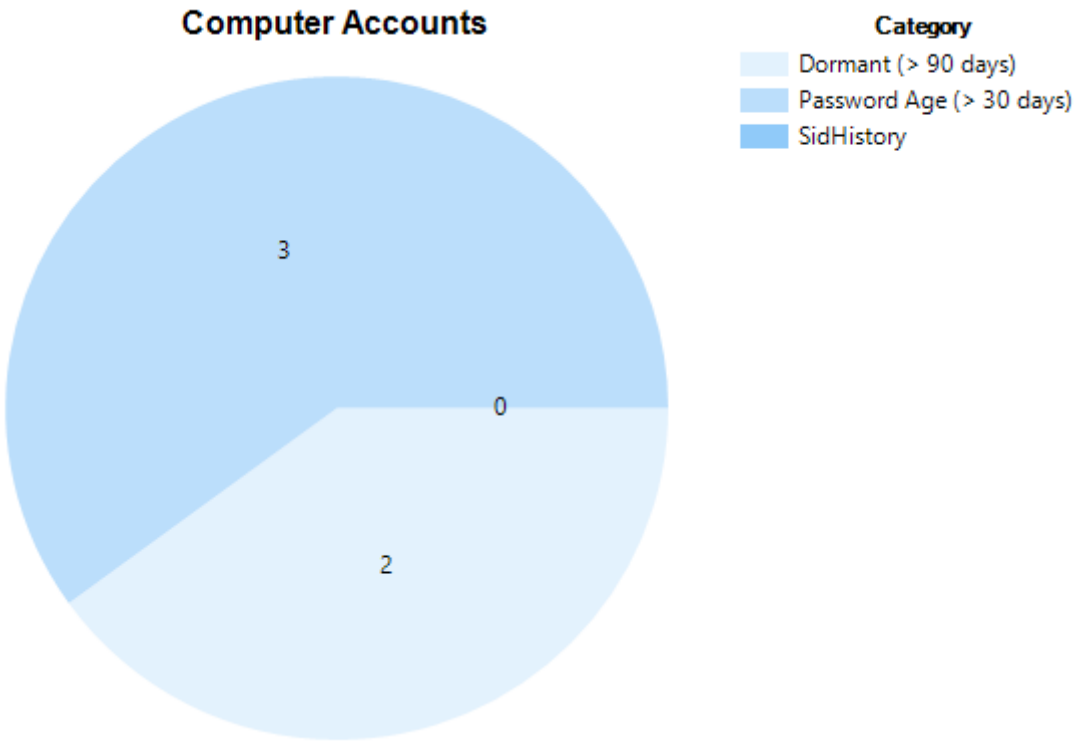
1.2.2.7 Computer Accounts in Domain



Status	Count	Percentage
Enabled	5	100%
Disabled	0	0%

Table 86 - Computer Accounts in Domain - ACAD.PHARMAX.LOCAL

1.2.2.8 Status of Computer Accounts



Category	Enabled Count	Enabled %	Disabled Count	Disabled %	Total Count	Total %
Dormant (> 90 days)	2	40	1	20	2	40
Password Age (> 30 days)	3	60	1	20	3	60
SidHistory	0	0	1	20	0	0

Table 87 - Status of Computer Accounts - ACAD.PHARMAX.LOCAL

1.2.2.9 Operating Systems Count

Operating System	Count
Unknown	1
Windows Server 2019 Standard	1
Windows Server 2019 Standard Evaluation	2
Windows Server 2022 Datacenter Evaluation	1

Table 88 - Operating System Count - ACAD.PHARMAX.LOCAL

1.2.2.10 Default Domain Password Policy

Password Must Meet Complexity Requirements	Yes
Path	acad.pharmax.local/

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
Enforce Password History	24
Store Password using Reversible Encryption	No

Table 89 - Default Domain Password Policy - ACAD.PHARMAX.LOCAL

1.2.2.11 Fined Grained Password Policies

ACADTest

Name	ACADTest
Domain Name	acad.pharmax.local
Complexity Enabled	Yes
Path	acad.pharmax.local/System/Password Settings Container/ACADTest
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	14
Password History Count	24
Reversible Encryption Enabled	No
Precedence	1
Applies To	SCCM-GMSA

Table 90 - Fined Grained Password Policies - ACADTest

1.2.2.12 gMSA identities

SCCMMSA

Name	SCCMMSA
SamAccountName	SCCMMSA$
Created	09/11/2021 21:01:33
Enabled	Yes
DNS Host Name	acad.pharmax.local
Host Computers	

Retrieve Managed Password	SCCM-GMSA
Primary Group	Domain Computers
Last Logon Date	
Locked Out	No
Logon Count	0
Password Expired	No
Password Last Set	09/11/2021 21:01:33

Table 91 - gMSA - SCCMMSA

1.2.2.13 Health Checks

Naming Context Last Backup

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

Naming Context	Last Backup	Last Backup in Days
CN=Configuration,DC=pharmax,DC=local	2023:02:20	91
CN=Schema,CN=Configuration,DC=pharmax,DC=local	2023:02:20	91
DC=acad,DC=pharmax,DC=local	2021:09:05	625
DC=DomainDnsZones,DC=acad,DC=pharmax,DC=local	2021:09:05	625
DC=ForestDnsZones,DC=pharmax,DC=local	2023:02:20	91

Table 92 - Naming Context Last Backup - ACAD.PHARMAX.LOCAL

Health Check:
Corrective Actions: Ensure there is a recent (<180 days) Active Directory backup.

Sysvol Folder Status

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

Extension	File Count	Size
.cab	12	2,866.91 MB
.cmtx	1	0.00 MB
.esd	1	3,193.66 MB
.exe	119	1,117.91 MB
.inf	3	0.01 MB
.INI	6	0.00 MB
.pol	3	0.01 MB

Table 93 - Sysvol Folder Status - ACAD.PHARMAX.LOCAL

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

Netlogon Folder Status

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

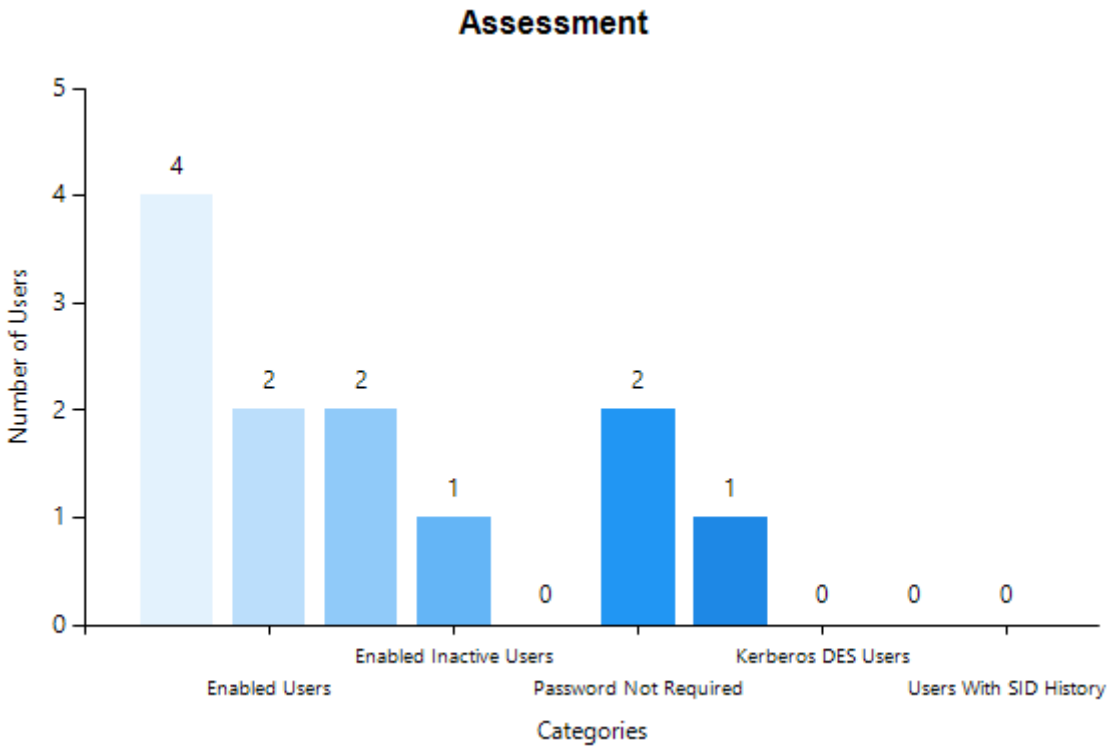
Extension	File Count	Size
.cab	12	2,866.91 MB
.esd	1	3,193.66 MB
.exe	119	1,117.91 MB

Table 94 - Netlogon Folder Status - ACAD.PHARMAX.LOCAL

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

Account Security Assessment

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



Total Users	4
Enabled Users	2
Disabled Users	2
Enabled Inactive Users	1
Users With Reversible Encryption Password	0

Password Not Required	2
Password Never Expires	1
Kerberos DES Users	0
Does Not Require Pre Auth	0
Users With SID History	0

Table 95 - Account Security Assessment - ACAD.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 ACAD.PHARMAX.LOCAL

Username	Created	Password Last Set	Last Logon Date
Administrator	9/5/2021	9/5/2021	9/18/2021
krbtgt	9/5/2021	9/5/2021	-

Table 96 - Privileged User Assessment - ACAD.PHARMAX.LOCAL

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

Service Accounts Assessment

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

Username	Enabled	Password Last Set	Last Logon Date	Service Principal Name
krbtgt	No	9/5/2021	-	kadmin/changepw

Table 97 - Service Accounts Assessment - ACAD.PHARMAX.LOCAL

Health Check:
Corrective Actions: Service accounts are that gray area between regular user accounts and admin accounts that are often highly privileged. They are almost always over-privileged due to documented vendor requirements or because of operational challenges. Ensure there aren't any account with weak security posture.

KRBTGT Account Audit

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

Name	krbtgt
Created	09/05/2021 12:25:21
Password Last Set	09/05/2021 12:25:21
Distinguished Name	CN=krbtgt,CN=Users,DC=acad,DC=pharmax,DC=local

Table 98 - KRBTGT Account Audit - ACAD.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 ACAD.PHARMAX.LOCAL.

Name	Administrator
Created	09/05/2021 12:24:39
Password Last Set	09/05/2021 10:35:45
Last Logon Date	09/18/2021 22:28:55
Distinguished Name	CN=Administrator,CN=Users,DC=acad,DC=pharmax,DC=local

Table 99 - Administrator Account Audit - ACAD.PHARMAX.LOCAL

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

1.2.2.14 Domain Controllers

A domain controller (DC) is a server computer that responds to security authentication requests within a computer network domain. It is a network server that is responsible for allowing host access to domain resources. It authenticates users, stores user account information and enforces security policy for a domain.

DC Name	Domain Name	Site	Global Catalog	Read Only	IP Address
ACADE-DC-01V	acad.pharmax.local	ACAD	Yes	No	172.23.4.1

Table 100 - Domain Controllers - ACAD.PHARMAX.LOCAL

1.2.2.14.1 Hardware Inventory

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

ACADE-DC-01V

Name	ACADE-DC-01V
Windows Product Name	Windows Server 2019 Standard Evaluation
Windows Current Version	6.3
Windows Build Number	10.0.17763

Windows Install Type	Server
AD Domain	acad.pharmax.local
Windows Installation Date	09/05/2021 10:35:50
Time Zone	(UTC-04:00) Georgetown, La Paz, Manaus, San Juan
License Type	Retail:TB:Eval
Partial Product Key	Y7XRX
Manufacturer	VMware, Inc.
Model	VMware7,1
Serial Number	
Bios Type	Uefi
BIOS Version	
Processor Manufacturer	GenuineIntel
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 101 - Hardware Inventory - ACADE-DC-01V

1.2.2.14.2 NTDS Information

DC Name	Database File	Database Size	Log Path	SysVol Path
ACADE-DC-01V	C:\Windows\NTDS\ntds.dit	116.00 MB	C:\Windows\NTDS	C:\Windows\SYSVOL\sysvol

Table 102 - NTDS Database File Usage - ACAD.PHARMAX.LOCAL

1.2.2.14.3 Time Source Information

Name	Time Server	Type
ACADE-DC-01V	Domain Hierarchy	DOMHIER

Table 103 - Time Source Configuration - ACAD.PHARMAX.LOCAL

1.2.2.14.4 SRV Records Status

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

Table 104 - SRV Records Status - ACAD.PHARMAX.LOCAL

Health Check:

Best Practice: The SRV record is a Domain Name System (DNS) resource record. It's used to identify computers hosting specific services. SRV resource records are used to locate domain controllers for Active Directory.

1.2.2.14.5 Installed Software

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

ACADE-DC-01V

Name	Publisher	Install Date
7-Zip 22.01 (x64)	Igor Pavlov	--

Table 105 - Installed Software - ACADE-DC-01V

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

1.2.2.14.6 Missing Windows Updates

The following section provides a summary of pending/missing windows updates on Domain Controllers from domain ACAD.PHARMAX.LOCAL.

ACADE-DC-01V

KB Article	Name
KB5022782	2023-02 Cumulative Update for .NET Framework 3.5, 4.7.2 and 4.8 for Windows Server 2019 for x64 (KB5022782)
KB5026362	2023-05 Cumulative Update for Windows Server 2019 for x64-based Systems (KB5026362)

Table 106 - Missing Windows Updates - ACADE-DC-01V

Health Check:
Security Best Practices: It is critical to install security updates to protect your systems from malicious attacks. In the long run, it is also important to install software updates, not only to access new features, but also to be on the safe side in terms of security loop holes being discovered in outdated programs. And it is in your own best interest to install all other updates, which may potentially cause your system to become vulnerable to attack.

1.2.2.14.7 Roles

The following section provides a summary of the Domain Controller Role & Features information.

ACADE-DC-01V

Name	Parent	InstallState
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 107 - Roles - ACADE-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.

1.2.2.14.8 DC Diagnostic

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

ACADE-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.

Test Name	Result	Impact	Description
NCSecDesc	Failed	Medium	Validates if permissions are correctly set in this Domain Controller for all naming contexts. Those permissions directly affect replications health.
NetLogons	Failed	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	Passed	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	Failed	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.

Test Name	Result	Impact	Description
Advertising	Failed	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	Passed	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	Failed	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	Failed	Medium	Checks that the file replication system (FRS) system volume (SYSVOL) is ready

Table 108 - DCDiag Test Status - ACADE-DC-01V

1.2.2.14.9 Infrastructure Services Status

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

ACADE-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

Display Name	Short Name	Status
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 109 - Infrastructure Services Status - ACADE-DC-01V

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

1.2.2.14.10 Sites Replication Connection

The following section provides detailed information about Site Replication Connection.

From: CAYEY-DC-01V To: ACADE-DC-01V

GUID	e67df374-0002-4e2f-9bef-e023dff2901c
Description	--
Replicate From Directory Server	CAYEY-DC-01V
Replicate To Directory Server	ACADE-DC-01V
Replicated Naming Contexts	DC=DomainDnsZones,DC=acad,DC=pharmax,DC=local DC=acad,DC=pharmax,DC=local DC=ForestDnsZones,DC=pharmax,DC=local CN=Schema,CN=Configuration,DC=pharmax,DC=local CN=Configuration,DC=pharmax,DC=local
Transport Protocol	IP
Auto Generated	Yes
Enabled	Yes
Created	Tue, 23 May 2023 15:13:50 GMT

Table 110 - Site Replication - ACADE-DC-01V

From: DC-UIA-01V To: ACADE-DC-01V

GUID	6ae00374-f928-46ec-890c-bc495e2b6da7
Description	--
Replicate From Directory Server	DC-UIA-01V
Replicate To Directory Server	ACADE-DC-01V
Replicated Naming Contexts	DC=DomainDnsZones,DC=acad,DC=pharmax,DC=local DC=acad,DC=pharmax,DC=local

	DC=ForestDnsZones,DC=pharmax,DC=local CN=Schema,CN=Configuration,DC=pharmax,DC=local CN=Configuration,DC=pharmax,DC=local
Transport Protocol	IP
Auto Generated	Yes
Enabled	Yes
Created	Tue, 23 May 2023 15:13:50 GMT

Table 111 - Site Replication - ACADE-DC-01V

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

GUID	739a49db-275b-4d09-81c8-ab9e5f393977
Description	--
Replicate From Directory Server	SERVER-DC-01V
Replicate To Directory Server	ACADE-DC-01V
Replicated Naming Contexts	DC=DomainDnsZones,DC=acad,DC=pharmax,DC=local DC=acad,DC=pharmax,DC=local DC=ForestDnsZones,DC=pharmax,DC=local CN=Schema,CN=Configuration,DC=pharmax,DC=local CN=Configuration,DC=pharmax,DC=local
Transport Protocol	IP
Auto Generated	Yes
Enabled	Yes
Created	Sun, 05 Sep 2021 16:26:31 GMT

Table 112 - Site Replication - ACADE-DC-01V

1.2.2.14.11 Sites Replication Status

Source DSA	Destination DSA	Source DSA Site	Last Success Time	Last Failure Status	Last Failure Time	Number of failures
CAYEY-DC-01V	ACADE-DC-01V	Cayey-Branch	2023-05-23 16:38:44	0	0	0
CAYEY-DC-01V	ACADE-DC-01V	Cayey-Branch	2023-05-23 16:38:44	0	0	0
CAYEY-DC-01V	ACADE-DC-01V	Cayey-Branch	2023-05-23 16:38:44	0	0	0
CAYEY-DC-01V	ACADE-DC-01V	Cayey-Branch	2023-05-23 16:38:44	0	0	0
SERVER-DC-01V	ACADE-DC-01V	Pharmax-HQ	2023-05-22 20:44:52	1256	2023-05-23 16:38:44	28
SERVER-DC-01V	ACADE-DC-01V	Pharmax-HQ	2023-05-22 20:44:52	1256	2023-05-23 16:38:44	28

Source DSA	Destination DSA	Source DSA Site	Last Success Time	Last Failure Status	Last Failure Time	Number of failures
SERVER-DC-01V	ACADE-DC-01V	Pharmax-HQ	2023-05-22 20:44:52	5	2023-05-23 16:38:44	28
SERVER-DC-01V	ACADE-DC-01V	Pharmax-HQ	2023-05-22 20:44:52	5	2023-05-23 16:38:44	28
SERVER-DC-01V	ACADE-DC-01V	Pharmax-HQ	2023-05-22 20:44:52	1256	2023-05-23 16:38:44	28

Table 113 - Site Replication Status - ACAD.PHARMAX.LOCAL

Health Check:
Best Practices: Replication failure can lead to object inconsistencies and major problems in Active Directory.

1.2.2.14.12 Group Policy Objects

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

Empty Policy ACAD

GPO Status	All Settings Enabled
Created	10/05/2021
Modified	10/05/2021
Description	
Owner	PHARMAX\Enterprise Admins

Table 114 - GPO - Empty Policy ACAD

Default Domain Policy

GPO Status	All Settings Enabled
Created	09/05/2021
Modified	10/19/2021
Description	
Owner	ACAD\Domain Admins

Table 115 - GPO - Default Domain Policy

Unlinked Policy ACAD

GPO Status	All Settings Disabled
Created	10/05/2021
Modified	10/05/2021
Description	

Owner	PHARMAX\Enterprise Admins

Table 116 - GPO - Unlinked Policy ACAD

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

Default Domain Controllers Policy

GPO Status	All Settings Enabled
Created	09/05/2021
Modified	09/22/2021
Description	
Owner	ACAD\Domain Admins

Table 117 - GPO - Default Domain Controllers Policy

ACAD Certificate AutoEnrollment

GPO Status	All Settings Enabled
Created	09/22/2021
Modified	09/22/2021
Description	
Owner	PHARMAX\Enterprise Admins

Table 118 - GPO - ACAD Certificate AutoEnrollment

Logon Script

GPO Status	All Settings Enabled
Created	10/07/2021
Modified	10/07/2021
Description	
Owner	PHARMAX\Enterprise Admins

Table 119 - GPO - Logon Script

1.2.2.14.12.1 Central Store Repository

Domain	Configured	Central Store Path
ACAD.PHARMAX.LOCAL	No	\\acad.pharmax.local\SYSVOL\acad.pharmax.local\Policies\PolicyDefinitions

Table 120 - GPO Central Store - ACAD.PHARMAX.LOCAL

Health Check:
Best Practices: Ensure Central Store is deployed to centralized GPO repository.

1.2.2.14.12.2 User Logon/Logoff Script

GPO Name	GPO Status	Type	Script
Logon Script	All Settings Enabled	Logon	\\acad.pharmax.local\NETLOGON\enroll.exe

Table 121 - GPO with Logon/Logoff Script - ACAD.PHARMAX.LOCAL

1.2.2.14.12.3 Unlinked GPO

GPO Name	Created	Modified	Computer Enabled	User Enabled
Logon Script	2021-10-07	2021-10-07	Yes	Yes
Unlinked Policy ACAD	2021-10-06	2021-10-06	No	No

Table 122 - Unlinked GPO - ACAD.PHARMAX.LOCAL

Health Check:
Corrective Actions: Remove Unused GPO from Active Directory.

1.2.2.14.12.4 Empty GPOs

GPO Name	Created	Modified	Description
Empty Policy ACAD	2021-10-06	2021-10-06	--

Table 123 - Empty GPO - ACAD.PHARMAX.LOCAL

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

1.2.2.14.12.5 Enforced GPO

GPO Name	Enforced	Order	Target
Empty Policy ACAD	Yes	1	acad.pharmax.local/Acad Computers/SCCM Computers

Table 124 - Enforced GPO - ACAD.PHARMAX.LOCAL

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

1.2.2.14.13 Organizational Units

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

Name	Path	Linked GPO
Acad Computers	acad.pharmax.local/Acad Computers	--

Name	Path	Linked GPO
SCCM Computers	acad.pharmax.local/Acad Computers/SCCM Computers	Empty Policy ACAD
Domain Controllers	acad.pharmax.local/Domain Controllers	Default Domain Controllers Policy
Member Servers	acad.pharmax.local/Member Servers	--

Table 125 - Organizational Unit - ACAD.PHARMAX.LOCAL

1.2.2.14.13.1 GPO Blocked Inheritance

OU Name	Container Type	Inheritance Blocked	Path
sccm computers	OU	Yes	acad.pharmax.local/Acad Computers/SCCM Computers

Table 126 - Blocked Inheritance GPO - ACAD.PHARMAX.LOCAL

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

1.2.3 UIA.LOCAL

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

Domain Name	uia
NetBIOS Name	UIA
Domain SID	S-1-5-21-658426745-1048856031-3787862735
Domain Functional Level	Windows2016Domain
Domains	--
Forest	pharmax.local
Parent Domain	--
Replica Directory Servers	DC-UIA-01V.uia.local
Child Domains	--
Domain Path	uia.local/
Computers Container	uia.local/Computers
Domain Controllers Container	uia.local/Domain Controllers
Systems Container	uia.local/System
Users Container	uia.local/Users
ReadOnly Replica Directory Servers	--
ms-DS-MachineAccountQuota	10
RID Issued	4600
RID Available	1073737223

Table 127 - Domain Summary - UIA.LOCAL

1.2.3.1 FSMO Roles

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

Table 128 - FSMO Roles - uia.local

1.2.3.2 Domain and Trusts

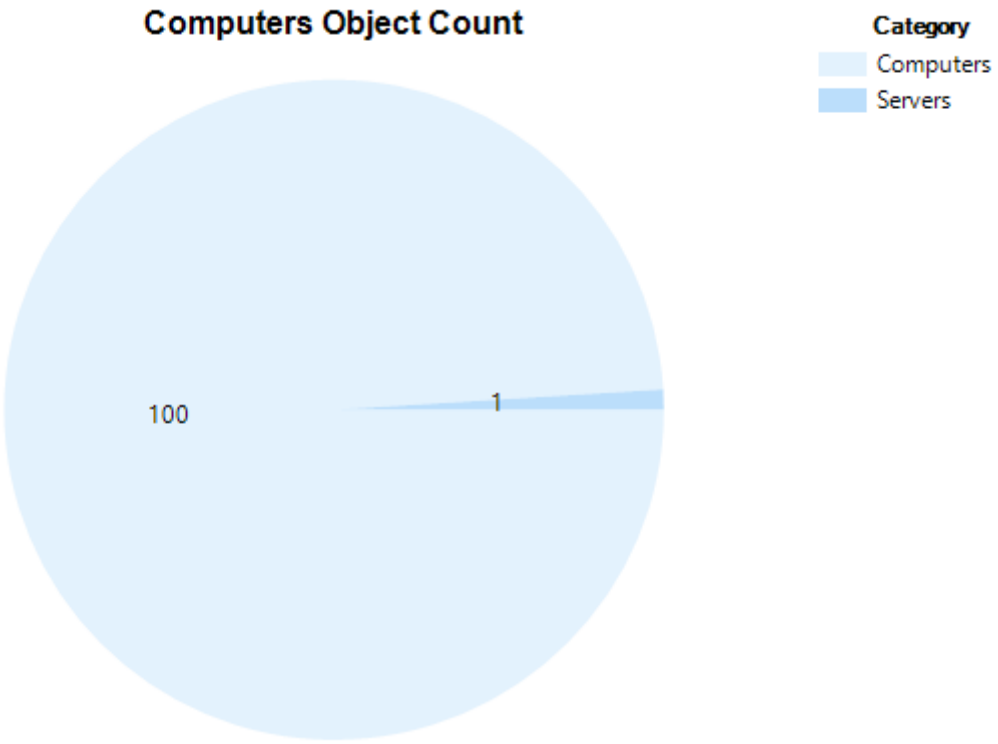
pharmax.local

Name	pharmax.local
Path	uia.local/System/pharmax.local
Source	uia
Target	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 129 - Trusts - pharmax.local

1.2.3.3 Domain Object Count

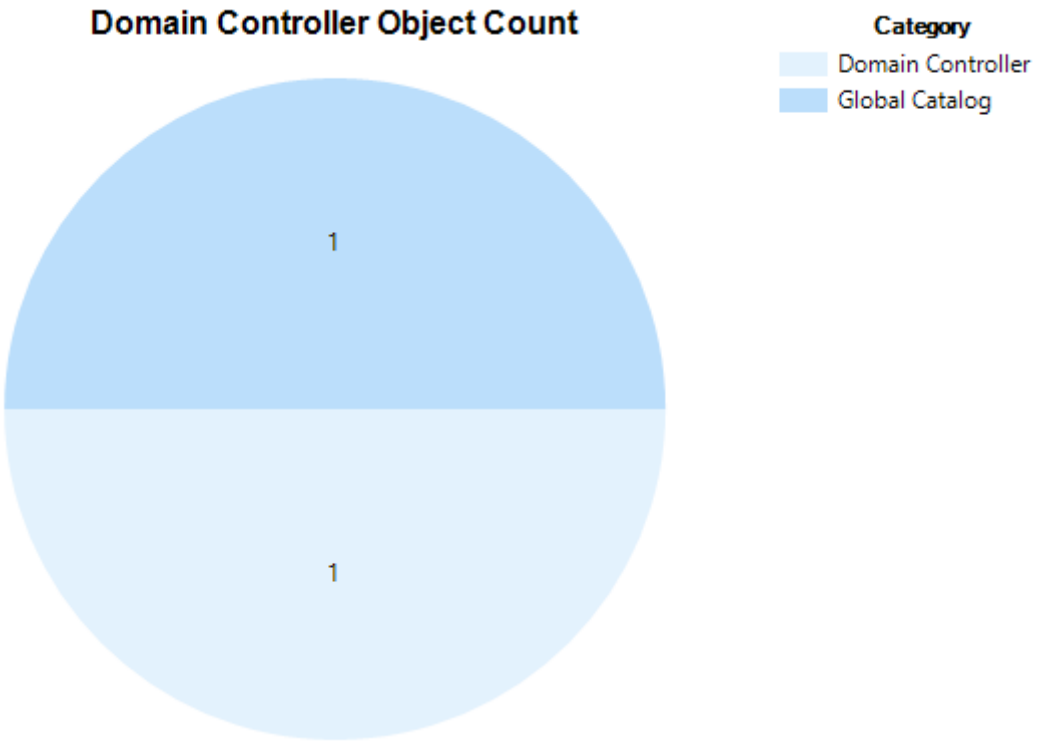
1.2.3.3.1 Computers Object



Computers	100
Servers	1

Table 130 - Computers Object - UIA.LOCAL

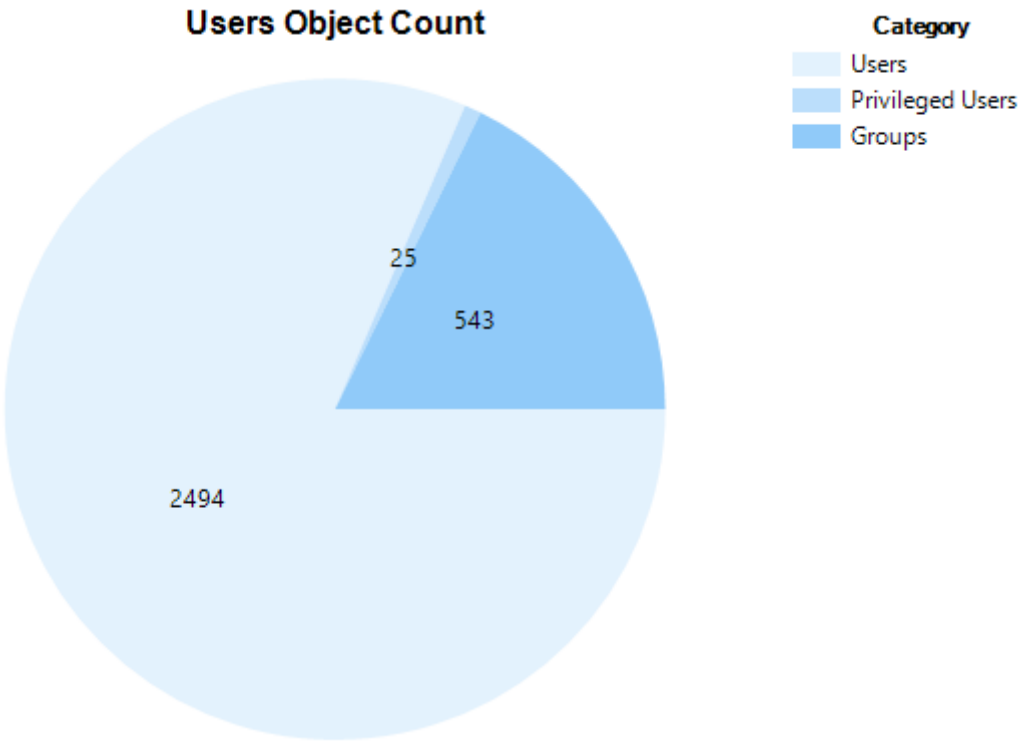
1.2.3.3.2 Domain Controller Object



Domain Controller	1
Global Catalog	1

Table 131 - Domain Controller Object - UIA.LOCAL

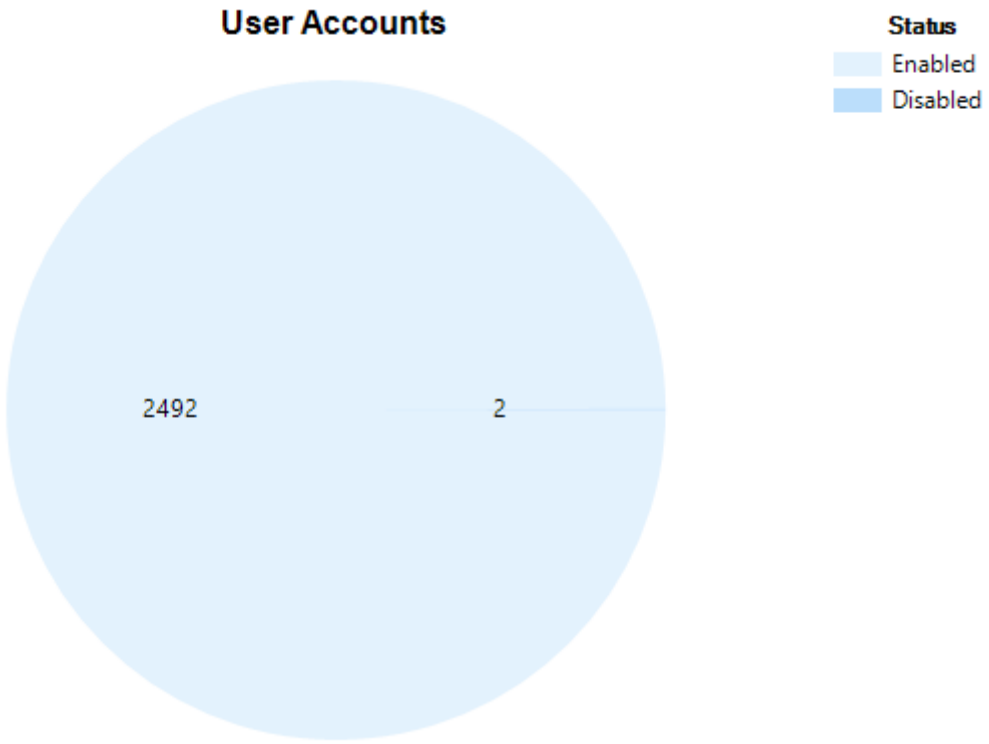
1.2.3.3.3 Users Object



Users	2494
Privileged Users	25
Groups	543

Table 132 - User Object - UIA.LOCAL

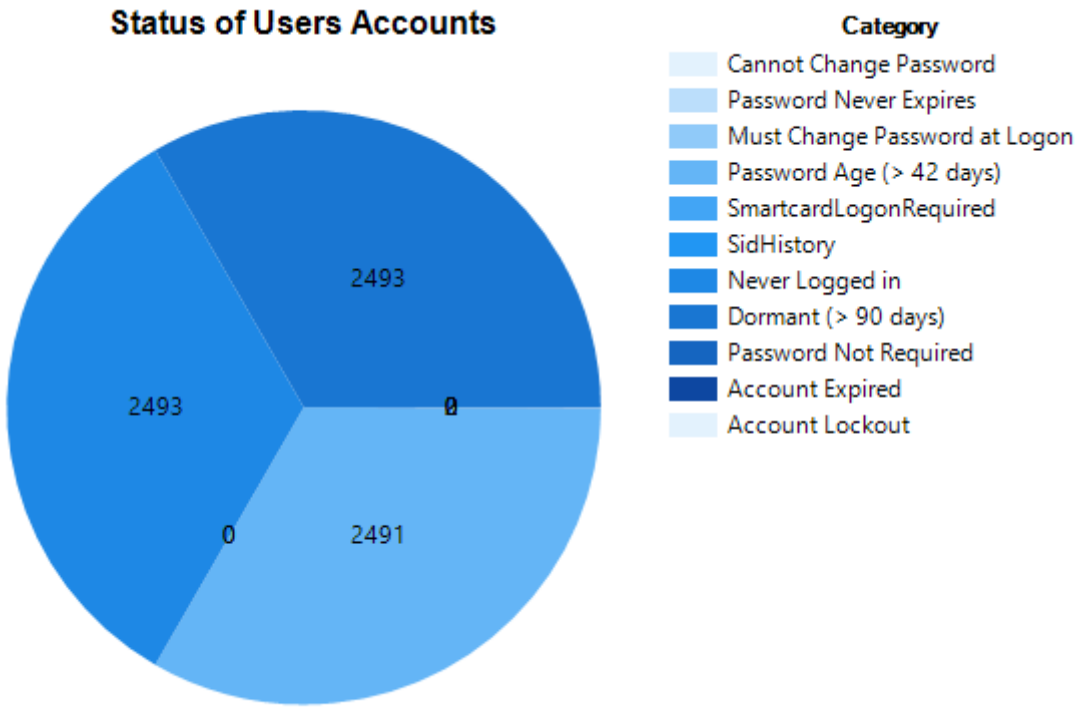
1.2.3.4 User Accounts in Domain



Status	Count	Percentage
Enabled	2492	100%
Disabled	2	0%

Table 133 - User Accounts in Domain - UIA.LOCAL

1.2.3.5 Status of Users Accounts



Category	Enabled Count	Enabled %	Disabled Count	Disabled %	Total Count	Total %
Cannot Change Password	0	0	1	0	0	0
Password Never Expires	2	0	1	0	2	0
Must Change Password at Logon	2	0	1	0	2	0
Password Age (> 42 days)	2491	100	1	0	2491	100
SmartcardLogonRequired	0	0	1	0	0	0
SidHistory	0	0	1	0	0	0
Never Logged in	2493	100	1	0	2493	100
Dormant (> 90 days)	2493	100	1	0	2493	100
Password Not Required	2	0	1	0	2	0
Account Expired	0	0	1	0	0	0
Account Lockout	0	0	1	0	0	0

Table 134 - Status of User Accounts - UIA.LOCAL

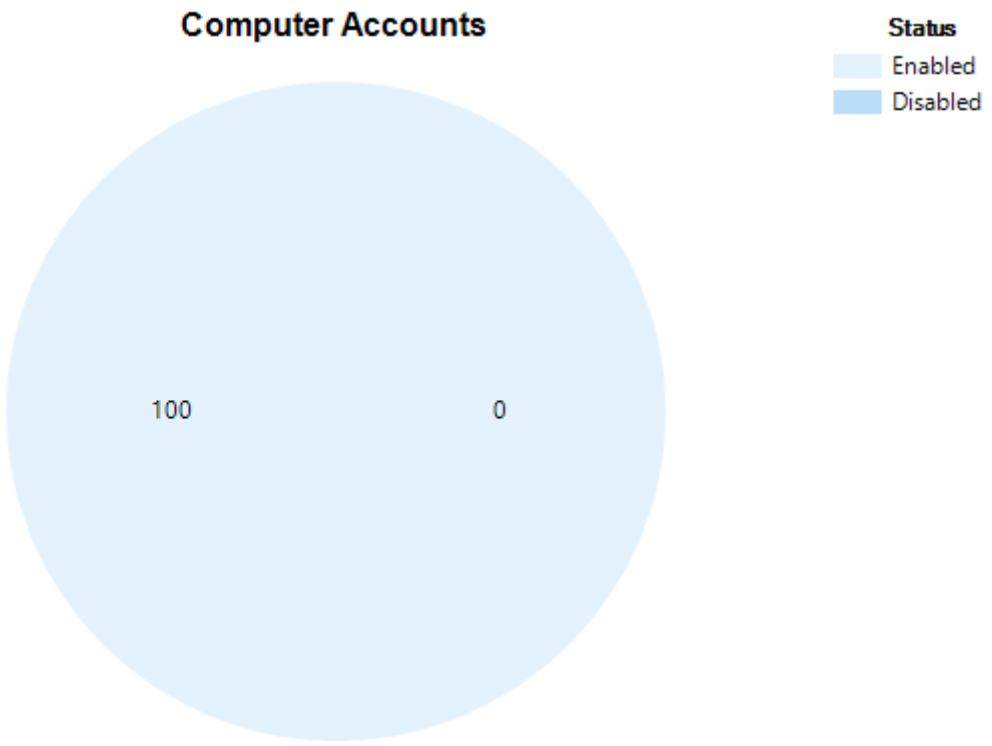
1.2.3.6 Privileged Group Count

Group Name	Count
Account Operators	1
Backup Operators	2
Cert Publishers	1

Group Name	Count
DnsAdmins	3
Domain Admins	6
Key Admins	5
Print Operators	3
Remote Desktop Users	2
Server Operators	2

Table 135 - Privileged Group Count - UIA.LOCAL

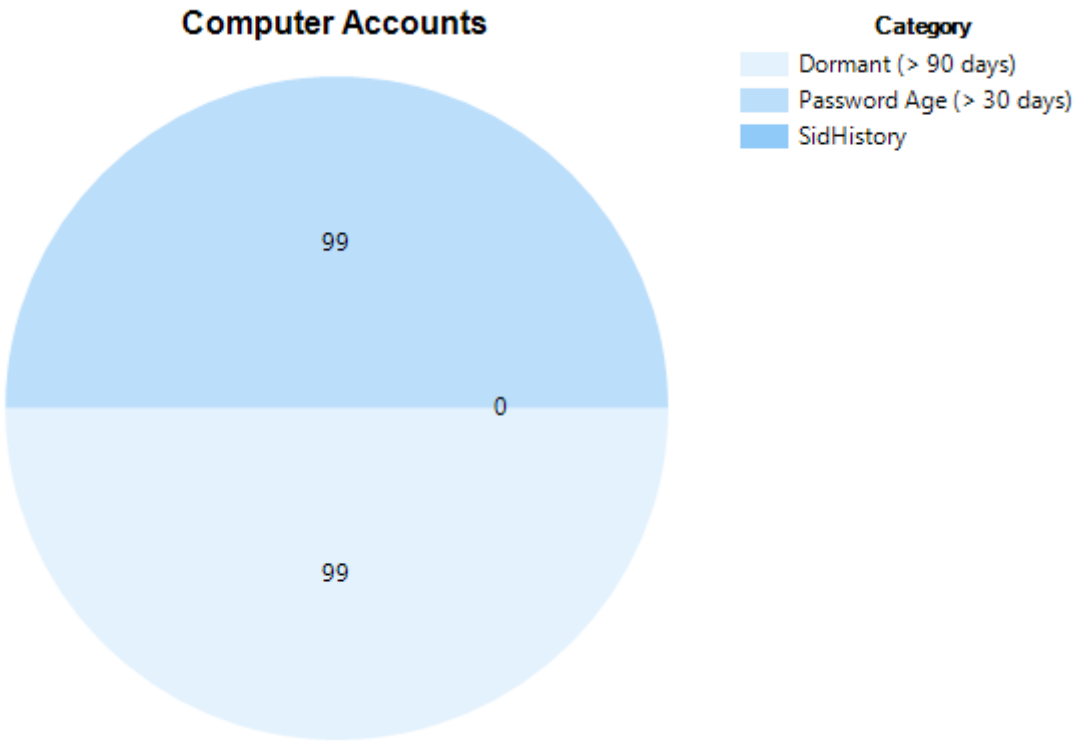
1.2.3.7 Computer Accounts in Domain



Status	Count	Percentage
Enabled	100	100%
Disabled	0	0%

Table 136 - Computer Accounts in Domain - UIA.LOCAL

1.2.3.8 Status of Computer Accounts



Category	Enabled Count	Enabled %	Disabled Count	Disabled %	Total Count	Total %
Dormant (> 90 days)	99	99	1	1	99	99
Password Age (> 30 days)	99	99	1	1	99	99
SidHistory	0	0	1	1	0	0

Table 137 - Status of Computer Accounts - UIA.LOCAL

1.2.3.9 Operating Systems Count

Operating System	Count
Unknown	99
Windows Server 2022 Datacenter Evaluation	1

Table 138 - Operating System Count - UIA.LOCAL

1.2.3.10 Default Domain Password Policy

Password Must Meet Complexity Requirements	Yes
Path	uia.local/
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
Enforce Password History	24
Store Password using Reversible Encryption	No

Table 139 - Default Domain Password Policy - UIA.LOCAL

1.2.3.11 Health Checks

Naming Context Last Backup

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

Naming Context	Last Backup	Last Backup in Days
CN=Configuration,DC=pharmax,DC=local	2023:02:20	91
CN=Schema,CN=Configuration,DC=pharmax,DC=local	2023:02:20	91
DC=DomainDnsZones,DC=uia,DC=local	2022:05:13	375
DC=ForestDnsZones,DC=pharmax,DC=local	2023:02:20	91
DC=uia,DC=local	2022:05:13	375

Table 140 - Naming Context Last Backup - UIA.LOCAL

Health Check:
Corrective Actions: Ensure there is a recent (<180 days) Active Directory backup.

Sysvol Folder Status

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

Extension	File Count	Size
.inf	2	0.00 MB
.INI	2	0.00 MB
.pol	1	0.00 MB
.zip	80	4.72 MB

Table 141 - Sysvol Folder Status - UIA.LOCAL

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

Netlogon Folder Status

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

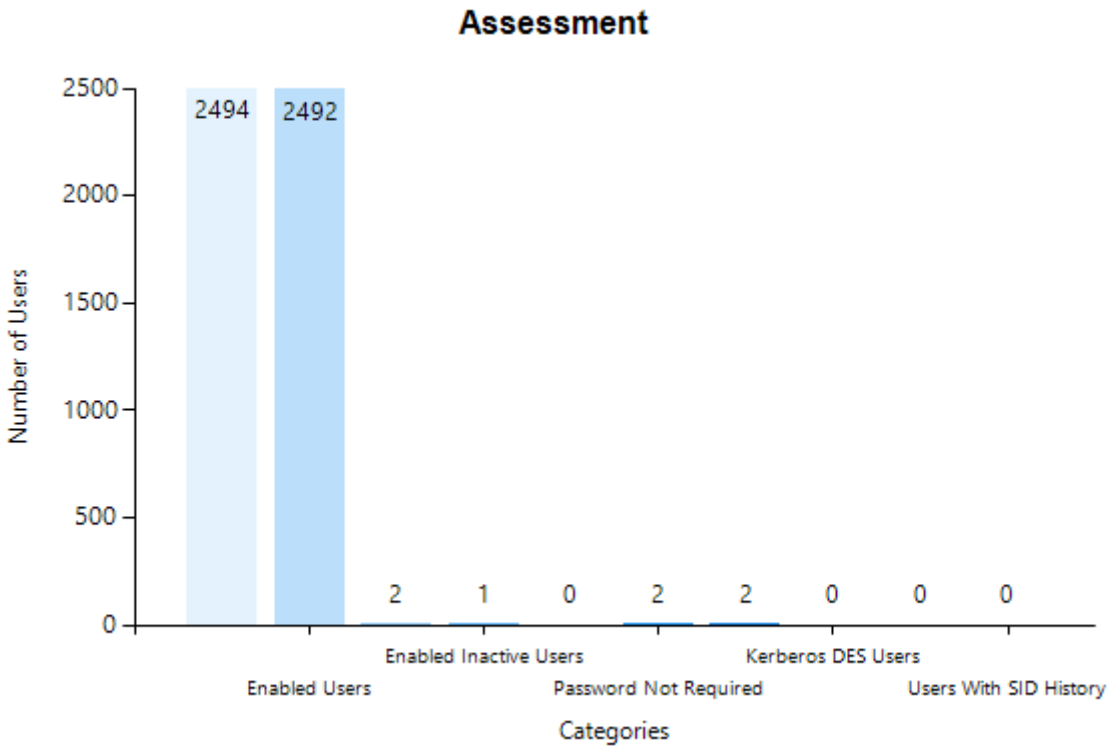
Extension	File Count	Size
.zip	80	4.72 MB

Table 142 - Netlogon Folder Status - UIA.LOCAL

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

Account Security Assessment

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



Total Users	2494
Enabled Users	2492
Disabled Users	2
Enabled Inactive Users	1
Users With Reversible Encryption Password	0
Password Not Required	2
Password Never Expires	2
Kerberos DES Users	0
Does Not Require Pre Auth	0
Users With SID History	0

Table 143 - Account Security Assessment - UIA.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 UIA.LOCAL

Username	Created	Password Last Set	Last Logon Date
Administrator	5/11/2022	1/26/2022	5/21/2023
krbtgt	5/11/2022	5/11/2022	-
ERNEST_WALLACE	5/14/2022	5/14/2022	-
SYBIL_BIRD	5/14/2022	5/14/2022	-
SASHA_PRESTON	5/14/2022	5/14/2022	-
MONA_SYKES	5/14/2022	5/14/2022	-
KENDRICK_RAYMOND	5/14/2022	5/14/2022	-
ADA_MARSHALL	5/14/2022	5/14/2022	-
ELISABETH_GOMEZ	5/14/2022	5/14/2022	-
AVA_MERRILL	5/14/2022	5/14/2022	-
HUGO_MERRITT	5/14/2022	5/14/2022	-
AMELIA_VALENCIA	5/14/2022	5/14/2022	-
CAROLE_COLEMAN	5/14/2022	5/14/2022	-
SARAH_GREER	5/14/2022	5/14/2022	-
ANGEL_MCDANIEL	5/14/2022	5/14/2022	-
THOMAS_CASH	5/14/2022	5/14/2022	-
ALISSA_SHAW	5/14/2022	5/14/2022	-
JESSE_WHEELER	5/14/2022	5/14/2022	-
DARRIN_KLEIN	5/14/2022	5/14/2022	-
JOSIE_WHEELER	5/14/2022	5/14/2022	-
LEONARDO_TALLEY	5/14/2022	5/14/2022	-
RAYMOND_HENDERSON	5/14/2022	5/14/2022	-
LINA_BEASLEY	5/14/2022	5/14/2022	-
RACHELLE_ADAMS	5/14/2022	5/14/2022	-
LENA_HENDRICKS	5/14/2022	5/14/2022	-

Table 144 - Privileged User Assessment - UIA.LOCAL

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

Service Accounts Assessment

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

Username	Enabled	Password Last Set	Last Logon Date	Service Principal Name
DEAN_WILEY	Yes	5/14/2022	-	CIFS/ESMWWEBS1000001
MICHELE_WILCOX	Yes	5/14/2022	-	CIFS/ESMWWKS1000000
ELISABETH_GOMEZ	Yes	5/14/2022	-	CIFS/FSRWWKS1000001
VILMA_KEY	Yes	5/14/2022	-	CIFS/HREWDBAS1000000
WILLA_CLARKE	Yes	5/14/2022	-	CIFS/ITSWVIR1000000
JESSE_WHEELER	Yes	5/14/2022	-	CIFS/SECWWEBS1000000
CHRISTINE_HARMON	Yes	5/14/2022	-	CIFS/TSTWCTRX1000000
KERMIT_KINNEY	Yes	5/14/2022	-	ftp/AWSWLPT1000000
IRMA_RODGERS	Yes	5/14/2022	-	ftp/AZRWCTRX1000000
NUMBERS_CHEN	Yes	5/14/2022	-	ftp/AZRWSECS1000000
CLAYTON_HEWITT	Yes	5/14/2022	-	ftp/BDEWVIR1000000
AMOS_DAUGHERTY	Yes	5/14/2022	-	ftp/ESMWLPT1000001
JAIME_DAWSON	Yes	5/14/2022	-	ftp/ESMWVIR1000000
TIM_HUMPHREY	Yes	5/14/2022	-	ftp/FINWWKS1000001
GLENDA_PATE	Yes	5/14/2022	-	ftp/ITSWVIR1000000
ROYCE_BERNARD	Yes	5/14/2022	-	ftp/TSTWWKS1000002
BARBARA_SKINNER	Yes	5/14/2022	-	https/AWSWAPPS1000000
KATE_CARR	Yes	5/14/2022	-	https/AWSWVIR1000000
CHUCK_MANNING	Yes	5/14/2022	-	https/BDEWSECS1000001
DEBBIE_FORD	Yes	5/14/2022	-	https/DC-UIA-01V
ISSAC_BUCK	Yes	5/14/2022	-	https/FINWLPT1000002
JOHN_YOUNG	Yes	5/14/2022	-	https/GOOWWEBS1000000
RITA_SPARKS	Yes	5/14/2022	-	https/HREWWEBS1000000
COLEMAN_KENNEDY	Yes	5/14/2022	-	https/TSTWLPT1000001
krbtgt	No	5/11/2022	-	kadmin/changepw
NEWTON_PENNINGTON	Yes	5/14/2022	-	kafka/AWSWWKS1000000
NANETTE_GARRETT	Yes	5/14/2022	-	kafka/AZRWWEBS1000000
TAMI_MULLINS	Yes	5/14/2022	-	kafka/ESMWWKS1000001
NIGEL_FARMER	Yes	5/14/2022	-	kafka/ESMWWKS1000002
CURT_POOLE	Yes	5/14/2022	-	kafka/FINWAPPS1000001
LUCIANO_KINNEY	Yes	5/14/2022	-	kafka/FINWCTRX1000000
HARRIS_DAVENPORT	Yes	5/14/2022	-	kafka/FSRWWKS1000001
6182398383SA	Yes	5/14/2022	-	kafka/SECWSECS1000000
JACQUELINE_MANN	Yes	5/14/2022	-	kafka/SECWWKS1000000
FRANKLIN_SMITH	Yes	5/14/2022	-	kafka/TSTWCTRX1000000
KITTY_CLARKE	Yes	5/14/2022	-	MSSQL/BDEWLPT1000001 POP3/AZRWAPPS1000000
LEONARDO_VAUGHAN	Yes	5/14/2022	-	MSSQL/ESMWWEBS1000002
CELIA_MUNOZ	Yes	5/14/2022	-	MSSQL/FSRWDBAS1000000
KAREEM_HAHN	Yes	5/14/2022	-	MSSQL/HREWVIR1000000

Username	Enabled	Password Last Set	Last Logon Date	Service Principal Name
MATILDA_RAMSEY	Yes	5/14/2022	-	MSSQL/HREWVIR1000001
GILDA_COOPER	Yes	5/14/2022	-	MSSQL/OGCWAPPS1000000
NATALIA_HOUSTON	Yes	5/14/2022	-	MSSQL/TSTWLPT1000000
ELIZA_WALTERS	Yes	5/14/2022	-	POP3/AWSWAPPS1000000
AMALIA_MCLAUGHLIN	Yes	5/14/2022	-	POP3/AWSWLPT1000000
GERRY_HUFF	Yes	5/14/2022	-	POP3/AWSWVIR1000000
MIRANDA_KIRKLAND	Yes	5/14/2022	-	POP3/BDEWWKS1000000
CORNELIA_WASHINGTON	Yes	5/14/2022	-	POP3/ESMWWEBS1000001
ADOLFO_MCNEIL	Yes	5/14/2022	-	POP3/FINWCTRX1000000
WINSTON_BAILEY	Yes	5/14/2022	-	POP3/FINWLPT1000003
LAMONT_JUAREZ	Yes	5/14/2022	-	POP3/HREWWKS1000000

Table 145 - Service Accounts Assessment - UIA.LOCAL

Health Check:
Corrective Actions: Service accounts are that gray area between regular user accounts and admin accounts that are often highly privileged. They are almost always over-privileged due to documented vendor requirements or because of operational challenges. Ensure there aren't any account with weak security posture.

KRBTGT Account Audit

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

Name	krbtgt
Created	05/11/2022 13:56:07
Password Last Set	05/11/2022 13:56:07
Distinguished Name	CN=krbtgt,CN=Users,DC=uia,DC=local

Table 146 - KRBTGT Account Audit - UIA.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 UIA.LOCAL.

Name	Administrator
Created	05/11/2022 13:54:55
Password Last Set	01/26/2022 20:44:53
Last Logon Date	05/21/2023 22:34:07
Distinguished Name	CN=Administrator,CN=Users,DC=uia,DC=local

Table 147 - Administrator Account Audit - UIA.LOCAL

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

1.2.3.12 Domain Controllers

A domain controller (DC) is a server computer that responds to security authentication requests within a computer network domain. It is a network server that is responsible for allowing host access to domain resources. It authenticates users, stores user account information and enforces security policy for a domain.

DC Name	Domain Name	Site	Global Catalog	Read Only	IP Address
DC-UIA-01V	uia.local	UIA	Yes	No	172.23.7.1

Table 148 - Domain Controllers - UIA.LOCAL

1.2.3.12.1 Hardware Inventory

The following section provides detailed Domain Controller Hardware information for domain UIA.LOCAL.

DC-UIA-01V

Name	DC-UIA-01V
Windows Product Name	Windows Server 2022 Datacenter Evaluation
Windows Current Version	6.3
Windows Build Number	10.0.20348
Windows Install Type	Server
AD Domain	uia.local
Windows Installation Date	01/26/2022 20:44:54
Time Zone	(UTC-04:00) Georgetown, La Paz, Manaus, San Juan
License Type	Retail:TB:Eval
Partial Product Key	37CYR
Manufacturer	VMware, Inc.
Model	VMware7,1
Serial Number	
Bios Type	Uefi
BIOS Version	
Processor Manufacturer	GenuineIntel
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 149 - Hardware Inventory - DC-UIA-01V

1.2.3.12.2 NTDS Information

DC Name	Database File	Database Size	Log Path	SysVol Path
DC-UIA-01V	C:\Windows\NTDS\ntds.dit	132.00 MB	C:\Windows\NTDS	C:\Windows\SYSVOL\sysvol

Table 150 - NTDS Database File Usage - UIA.LOCAL

1.2.3.12.3 Time Source Information

Name	Time Server	Type
DC-UIA-01V	Domain Hierarchy	DOMHIER

Table 151 - Time Source Configuration - UIA.LOCAL

1.2.3.12.4 SRV Records Status

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

Table 152 - SRV Records Status - UIA.LOCAL

Health Check:
Best Practice: The SRV record is a Domain Name System (DNS) resource record. It's used to identify computers hosting specific services. SRV resource records are used to locate domain controllers for Active Directory.

1.2.3.12.5 Installed Software

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

DC-UIA-01V

Name	Publisher	Install Date
Mozilla Firefox (x64 en-US)	Mozilla	--
Mozilla Maintenance Service	Mozilla	--

Table 153 - Installed Software - DC-UIA-01V

Health Check:

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

1.2.3.12.6 Missing Windows Updates

The following section provides a summary of pending/missing windows updates on Domain Controllers from domain UIA.LOCAL.

DC-UIA-01V

KB Article	Name
KB5026370	2023-05 Cumulative Update for Microsoft server operating system version 21H2 for x64-based Systems (KB5026370)
KB2267602	Security Intelligence Update for Microsoft Defender Antivirus - KB2267602 (Version 1.389.2214.0)
KB890830	Windows Malicious Software Removal Tool x64 - v5.113 (KB890830)

Table 154 - Missing Windows Updates - DC-UIA-01V

Health Check:
Security Best Practices: It is critical to install security updates to protect your systems from malicious attacks. In the long run, it is also important to install software updates, not only to access new features, but also to be on the safe side in terms of security loop holes being discovered in outdated programs. And it is in your own best interest to install all other updates, which may potentially cause your system to become vulnerable to attack.

1.2.3.12.7 Roles

The following section provides a summary of the Domain Controller Role & Features information.

DC-UIA-01V

Name	Parent	InstallState
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.

Name	Parent	InstallState
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.

Table 155 - Roles - DC-UIA-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.

1.2.3.12.8 DC Diagnostic

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

DC-UIA-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	Failed	Medium	Validates if permissions are correctly set in this Domain Controller for all naming contexts. Those permissions directly affect replications health.
NetLogons	Failed	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.

Test Name	Result	Impact	Description
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	Passed	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.
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	Failed	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).

Test Name	Result	Impact	Description
SysVolCheck	Failed	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	Failed	Medium	Checks that the file replication system (FRS) system volume (SYSVOL) is ready

Table 156 - DCDiag Test Status - DC-UIA-01V

1.2.3.12.9 Infrastructure Services Status

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

DC-UIA-01V

Display Name	Short Name	Status
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 157 - Infrastructure Services Status - DC-UIA-01V

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

1.2.3.12.10 Sites Replication Connection

The following section provides detailed information about Site Replication Connection.

From: ACADE-DC-01V To: DC-UIA-01V

GUID	26fe30d7-5edb-4acd-8098-f0695eac1e26
Description	--
Replicate From Directory Server	ACADE-DC-01V
Replicate To Directory Server	DC-UIA-01V
Replicated Naming Contexts	DC=DomainDnsZones,DC=uia,DC=local DC=uia,DC=local DC=ForestDnsZones,DC=pharmax,DC=local CN=Schema,CN=Configuration,DC=pharmax,DC=local CN=Configuration,DC=pharmax,DC=local
Transport Protocol	IP
Auto Generated	Yes
Enabled	Yes
Created	Wed, 11 May 2022 17:57:17 GMT

Table 158 - Site Replication - DC-UIA-01V

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

GUID	c73a836c-1dbc-43de-a918-ae91f8ea29c6
Description	--
Replicate From Directory Server	SERVER-DC-01V
Replicate To Directory Server	DC-UIA-01V
Replicated Naming Contexts	DC=DomainDnsZones,DC=uia,DC=local DC=uia,DC=local DC=ForestDnsZones,DC=pharmax,DC=local CN=Schema,CN=Configuration,DC=pharmax,DC=local CN=Configuration,DC=pharmax,DC=local
Transport Protocol	IP
Auto Generated	Yes
Enabled	Yes
Created	Wed, 11 May 2022 17:57:17 GMT

Table 159 - Site Replication - DC-UIA-01V

1.2.3.12.11 Sites Replication Status

Source DSA	Destination DSA	Source DSA Site	Last Success Time	Last Failure Status	Last Failure Time	Number of failures
ACADE-DC-01V	DC-UIA-01V	ACAD	2023-05-23 16:52:55	0	0	0
ACADE-DC-01V	DC-UIA-01V	ACAD	2023-05-23 16:52:55	0	0	0
ACADE-DC-01V	DC-UIA-01V	ACAD	2023-05-23 16:52:55	0	0	0

Source DSA	Destination DSA	Source DSA Site	Last Success Time	Last Failure Status	Last Failure Time	Number of failures
ACADE-DC-01V	DC-UIA-01V	ACAD	2023-05-23 16:52:55	0	0	0
ACADE-DC-01V	DC-UIA-01V	ACAD	2023-05-23 16:52:55	0	0	0
SERVER-DC-01V	DC-UIA-01V	Pharmax-HQ	2023-05-23 16:52:55	0	0	0
SERVER-DC-01V	DC-UIA-01V	Pharmax-HQ	2023-05-23 16:52:55	0	0	0
SERVER-DC-01V	DC-UIA-01V	Pharmax-HQ	2023-05-23 16:52:55	0	0	0
SERVER-DC-01V	DC-UIA-01V	Pharmax-HQ	2023-05-23 16:52:55	0	0	0
SERVER-DC-01V	DC-UIA-01V	Pharmax-HQ	2023-05-23 16:52:55	0	0	0

Table 160 - Site Replication Status - UIA.LOCAL

1.2.3.12.12 Group Policy Objects

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

Default Domain Policy

GPO Status	All Settings Enabled
Created	05/11/2022
Modified	05/11/2022
Description	
Owner	UIA\Domain Admins

Table 161 - GPO - Default Domain Policy

Default Domain Controllers Policy

GPO Status	All Settings Enabled
Created	05/11/2022
Modified	05/11/2022
Description	
Owner	UIA\Domain Admins

Table 162 - GPO - Default Domain Controllers Policy

1.2.3.12.12.1 Central Store Repository

Domain	Configured	Central Store Path
UIA.LOCAL	No	\\uia.local\SYSVOL\uia.local\Policies\PolicyDefinitions

Table 163 - GPO Central Store - UIA.LOCAL

Health Check:
Best Practices: Ensure Central Store is deployed to centralized GPO repository.

1.2.3.12.13 Organizational Units

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

Name	Path	Linked GPO
.SecFrame.com	uia.local/.SecFrame.com	--
Admin	uia.local/Admin	--
Staging	uia.local/Admin/Staging	--
Tier 0	uia.local/Admin/Tier 0	--
T0-Accounts	uia.local/Admin/Tier 0/T0-Accounts	--
T0-Devices	uia.local/Admin/Tier 0/T0-Devices	--
T0-Permissions	uia.local/Admin/Tier 0/T0-Permissions	--
T0-Roles	uia.local/Admin/Tier 0/T0-Roles	--
T0-Servers	uia.local/Admin/Tier 0/T0-Servers	--
Tier 1	uia.local/Admin/Tier 1	--
T1-Accounts	uia.local/Admin/Tier 1/T1-Accounts	--
T1-Devices	uia.local/Admin/Tier 1/T1-Devices	--
T1-Permissions	uia.local/Admin/Tier 1/T1-Permissions	--
T1-Roles	uia.local/Admin/Tier 1/T1-Roles	--
T1-Servers	uia.local/Admin/Tier 1/T1-Servers	--
Tier 2	uia.local/Admin/Tier 2	--
T2-Accounts	uia.local/Admin/Tier 2/T2-Accounts	--
T2-Devices	uia.local/Admin/Tier 2/T2-Devices	--
T2-Permissions	uia.local/Admin/Tier 2/T2-Permissions	--
T2-Roles	uia.local/Admin/Tier 2/T2-Roles	--
T2-Servers	uia.local/Admin/Tier 2/T2-Servers	--
Domain Controllers	uia.local/Domain Controllers	Default Domain Controllers Policy
Grouper-Groups	uia.local/Grouper-Groups	--
People	uia.local/People	--
AWS	uia.local/People/AWS	--
AZR	uia.local/People/AZR	--
BDE	uia.local/People/BDE	--
Deprovisioned	uia.local/People/Deprovisioned	--
ESM	uia.local/People/ESM	--
FIN	uia.local/People/FIN	--

Name	Path	Linked GPO
FSR	uia.local/People/FSR	--
GOO	uia.local/People/GOO	--
HRE	uia.local/People/HRE	--
ITS	uia.local/People/ITS	--
OGC	uia.local/People/OGC	--
SEC	uia.local/People/SEC	--
TST	uia.local/People/TST	--
Unassociated	uia.local/People/Unassociated	--
Quarantine	uia.local/Quarantine	--
Stage	uia.local/Stage	--
AWS	uia.local/Stage/AWS	--
Devices	uia.local/Stage/AWS/Devices	--
Groups	uia.local/Stage/AWS/Groups	--
ServiceAccounts	uia.local/Stage/AWS/ServiceAccounts	--
Test	uia.local/Stage/AWS/Test	--
AZR	uia.local/Stage/AZR	--
Devices	uia.local/Stage/AZR/Devices	--
Groups	uia.local/Stage/AZR/Groups	--
ServiceAccounts	uia.local/Stage/AZR/ServiceAccounts	--
Test	uia.local/Stage/AZR/Test	--
BDE	uia.local/Stage/BDE	--
Devices	uia.local/Stage/BDE/Devices	--
Groups	uia.local/Stage/BDE/Groups	--
ServiceAccounts	uia.local/Stage/BDE/ServiceAccounts	--
Test	uia.local/Stage/BDE/Test	--
ESM	uia.local/Stage/ESM	--
Devices	uia.local/Stage/ESM/Devices	--
Groups	uia.local/Stage/ESM/Groups	--
ServiceAccounts	uia.local/Stage/ESM/ServiceAccounts	--
Test	uia.local/Stage/ESM/Test	--
FIN	uia.local/Stage/FIN	--
Devices	uia.local/Stage/FIN/Devices	--
Groups	uia.local/Stage/FIN/Groups	--
ServiceAccounts	uia.local/Stage/FIN/ServiceAccounts	--
Test	uia.local/Stage/FIN/Test	--
FSR	uia.local/Stage/FSR	--
Devices	uia.local/Stage/FSR/Devices	--
Groups	uia.local/Stage/FSR/Groups	--
ServiceAccounts	uia.local/Stage/FSR/ServiceAccounts	--
Test	uia.local/Stage/FSR/Test	--

Name	Path	Linked GPO
GOO	uia.local/Stage/GOO	--
Devices	uia.local/Stage/GOO/Devices	--
Groups	uia.local/Stage/GOO/Groups	--
ServiceAccounts	uia.local/Stage/GOO/ServiceAccounts	--
Test	uia.local/Stage/GOO/Test	--
HRE	uia.local/Stage/HRE	--
Devices	uia.local/Stage/HRE/Devices	--
Groups	uia.local/Stage/HRE/Groups	--
ServiceAccounts	uia.local/Stage/HRE/ServiceAccounts	--
Test	uia.local/Stage/HRE/Test	--
ITS	uia.local/Stage/ITS	--
Devices	uia.local/Stage/ITS/Devices	--
Groups	uia.local/Stage/ITS/Groups	--
ServiceAccounts	uia.local/Stage/ITS/ServiceAccounts	--
Test	uia.local/Stage/ITS/Test	--
OGC	uia.local/Stage/OGC	--
Devices	uia.local/Stage/OGC/Devices	--
Groups	uia.local/Stage/OGC/Groups	--
ServiceAccounts	uia.local/Stage/OGC/ServiceAccounts	--
Test	uia.local/Stage/OGC/Test	--
SEC	uia.local/Stage/SEC	--
Devices	uia.local/Stage/SEC/Devices	--
Groups	uia.local/Stage/SEC/Groups	--
ServiceAccounts	uia.local/Stage/SEC/ServiceAccounts	--
Test	uia.local/Stage/SEC/Test	--
TST	uia.local/Stage/TST	--
Devices	uia.local/Stage/TST/Devices	--
Groups	uia.local/Stage/TST/Groups	--
ServiceAccounts	uia.local/Stage/TST/ServiceAccounts	--
Test	uia.local/Stage/TST/Test	--
Testing	uia.local/Testing	--
Tier 1	uia.local/Tier 1	--
AWS	uia.local/Tier 1/AWS	--
Devices	uia.local/Tier 1/AWS/Devices	--
Groups	uia.local/Tier 1/AWS/Groups	--
ServiceAccounts	uia.local/Tier 1/AWS/ServiceAccounts	--
Test	uia.local/Tier 1/AWS/Test	--
AZR	uia.local/Tier 1/AZR	--
Devices	uia.local/Tier 1/AZR/Devices	--
Groups	uia.local/Tier 1/AZR/Groups	--

Name	Path	Linked GPO
ServiceAccounts	uia.local/Tier 1/AZR/ServiceAccounts	--
Test	uia.local/Tier 1/AZR/Test	--
BDE	uia.local/Tier 1/BDE	--
Devices	uia.local/Tier 1/BDE/Devices	--
Groups	uia.local/Tier 1/BDE/Groups	--
ServiceAccounts	uia.local/Tier 1/BDE/ServiceAccounts	--
Test	uia.local/Tier 1/BDE/Test	--
ESM	uia.local/Tier 1/ESM	--
Devices	uia.local/Tier 1/ESM/Devices	--
Groups	uia.local/Tier 1/ESM/Groups	--
ServiceAccounts	uia.local/Tier 1/ESM/ServiceAccounts	--
Test	uia.local/Tier 1/ESM/Test	--
FIN	uia.local/Tier 1/FIN	--
Devices	uia.local/Tier 1/FIN/Devices	--
Groups	uia.local/Tier 1/FIN/Groups	--
ServiceAccounts	uia.local/Tier 1/FIN/ServiceAccounts	--
Test	uia.local/Tier 1/FIN/Test	--
FSR	uia.local/Tier 1/FSR	--
Devices	uia.local/Tier 1/FSR/Devices	--
Groups	uia.local/Tier 1/FSR/Groups	--
ServiceAccounts	uia.local/Tier 1/FSR/ServiceAccounts	--
Test	uia.local/Tier 1/FSR/Test	--
GOO	uia.local/Tier 1/GOO	--
Devices	uia.local/Tier 1/GOO/Devices	--
Groups	uia.local/Tier 1/GOO/Groups	--
ServiceAccounts	uia.local/Tier 1/GOO/ServiceAccounts	--
Test	uia.local/Tier 1/GOO/Test	--
HRE	uia.local/Tier 1/HRE	--
Devices	uia.local/Tier 1/HRE/Devices	--
Groups	uia.local/Tier 1/HRE/Groups	--
ServiceAccounts	uia.local/Tier 1/HRE/ServiceAccounts	--
Test	uia.local/Tier 1/HRE/Test	--
ITS	uia.local/Tier 1/ITS	--
Devices	uia.local/Tier 1/ITS/Devices	--
Groups	uia.local/Tier 1/ITS/Groups	--
ServiceAccounts	uia.local/Tier 1/ITS/ServiceAccounts	--
Test	uia.local/Tier 1/ITS/Test	--
OGC	uia.local/Tier 1/OGC	--
Devices	uia.local/Tier 1/OGC/Devices	--
Groups	uia.local/Tier 1/OGC/Groups	--

Name	Path	Linked GPO
ServiceAccounts	uia.local/Tier 1/OGC/ServiceAccounts	--
Test	uia.local/Tier 1/OGC/Test	--
SEC	uia.local/Tier 1/SEC	--
Devices	uia.local/Tier 1/SEC/Devices	--
Groups	uia.local/Tier 1/SEC/Groups	--
ServiceAccounts	uia.local/Tier 1/SEC/ServiceAccounts	--
Test	uia.local/Tier 1/SEC/Test	--
TST	uia.local/Tier 1/TST	--
Devices	uia.local/Tier 1/TST/Devices	--
Groups	uia.local/Tier 1/TST/Groups	--
ServiceAccounts	uia.local/Tier 1/TST/ServiceAccounts	--
Test	uia.local/Tier 1/TST/Test	--
Tier 2	uia.local/Tier 2	--
AWS	uia.local/Tier 2/AWS	--
Devices	uia.local/Tier 2/AWS/Devices	--
Groups	uia.local/Tier 2/AWS/Groups	--
ServiceAccounts	uia.local/Tier 2/AWS/ServiceAccounts	--
Test	uia.local/Tier 2/AWS/Test	--
AZR	uia.local/Tier 2/AZR	--
Devices	uia.local/Tier 2/AZR/Devices	--
Groups	uia.local/Tier 2/AZR/Groups	--
ServiceAccounts	uia.local/Tier 2/AZR/ServiceAccounts	--
Test	uia.local/Tier 2/AZR/Test	--
BDE	uia.local/Tier 2/BDE	--
Devices	uia.local/Tier 2/BDE/Devices	--
Groups	uia.local/Tier 2/BDE/Groups	--
ServiceAccounts	uia.local/Tier 2/BDE/ServiceAccounts	--
Test	uia.local/Tier 2/BDE/Test	--
ESM	uia.local/Tier 2/ESM	--
Devices	uia.local/Tier 2/ESM/Devices	--
Groups	uia.local/Tier 2/ESM/Groups	--
ServiceAccounts	uia.local/Tier 2/ESM/ServiceAccounts	--
Test	uia.local/Tier 2/ESM/Test	--
FIN	uia.local/Tier 2/FIN	--
Devices	uia.local/Tier 2/FIN/Devices	--
Groups	uia.local/Tier 2/FIN/Groups	--
ServiceAccounts	uia.local/Tier 2/FIN/ServiceAccounts	--
Test	uia.local/Tier 2/FIN/Test	--
FSR	uia.local/Tier 2/FSR	--
Devices	uia.local/Tier 2/FSR/Devices	--

Name	Path	Linked GPO
Groups	uia.local/Tier 2/FSR/Groups	--
ServiceAccounts	uia.local/Tier 2/FSR/ServiceAccounts	--
Test	uia.local/Tier 2/FSR/Test	--
GOO	uia.local/Tier 2/GOO	--
Devices	uia.local/Tier 2/GOO/Devices	--
Groups	uia.local/Tier 2/GOO/Groups	--
ServiceAccounts	uia.local/Tier 2/GOO/ServiceAccounts	--
Test	uia.local/Tier 2/GOO/Test	--
HRE	uia.local/Tier 2/HRE	--
Devices	uia.local/Tier 2/HRE/Devices	--
Groups	uia.local/Tier 2/HRE/Groups	--
ServiceAccounts	uia.local/Tier 2/HRE/ServiceAccounts	--
Test	uia.local/Tier 2/HRE/Test	--
ITS	uia.local/Tier 2/ITS	--
Devices	uia.local/Tier 2/ITS/Devices	--
Groups	uia.local/Tier 2/ITS/Groups	--
ServiceAccounts	uia.local/Tier 2/ITS/ServiceAccounts	--
Test	uia.local/Tier 2/ITS/Test	--
OGC	uia.local/Tier 2/OGC	--
Devices	uia.local/Tier 2/OGC/Devices	--
Groups	uia.local/Tier 2/OGC/Groups	--
ServiceAccounts	uia.local/Tier 2/OGC/ServiceAccounts	--
Test	uia.local/Tier 2/OGC/Test	--
SEC	uia.local/Tier 2/SEC	--
Devices	uia.local/Tier 2/SEC/Devices	--
Groups	uia.local/Tier 2/SEC/Groups	--
ServiceAccounts	uia.local/Tier 2/SEC/ServiceAccounts	--
Test	uia.local/Tier 2/SEC/Test	--
TST	uia.local/Tier 2/TST	--
Devices	uia.local/Tier 2/TST/Devices	--
Groups	uia.local/Tier 2/TST/Groups	--
ServiceAccounts	uia.local/Tier 2/TST/ServiceAccounts	--
Test	uia.local/Tier 2/TST/Test	--

Table 164 - Organizational Unit - UIA.LOCAL