Microsoft AD As Built Report

Zen Pr Solutions

Author: Jonathan Colon
Date: Saturday, October 8, 2022
Version: 1.0

Table of Contents

1 PHARMAX.LOCAL Active Directory Report ... 9
1.1 Forest Information. ... 9
1.1.1 Optional Features ... 9
1.1.2 Domain Sites ... 9
1.1.2.1 Site Subnets ... 10
1.1.2.2 Site Links ... 10
1.2 Active Directory Domain Information ... 10
1.2.1 PHARMAX.LOCAL Root Domain Configuration ... 10
1.2.1.1 Flexible Single Master Operations (FSMO) ... 11
1.2.1.2 Domain and Trusts ... 11
1.2.1.3 Domain Object Count ... 12
1.2.1.3.1 Computers Object ... 12
1.2.1.3.2 Domain Controller Object ... 13
1.2.1.3.3 Users Object ... 14
1.2.1.4 User Accounts in Active Directory ... 15
1.2.1.5 Status of Users Accounts ... 16
1.2.1.6 Privileged Group Count ... 16
1.2.1.7 Computer Accounts in Active Directory ... 17
1.2.1.8 Status of Computer Accounts ... 18
1.2.1.9 Operating Systems Count ... 18
1.2.1.10 Default Domain Password Policy ... 19
1.2.1.11 Fined Grained Password Policies ... 19
1.2.1.12 Group Managed Service Accounts (GMSA) ... 20
1.2.1.13 Health Checks ... 21
1.2.1.14 Domain Controller Summary ... 27
1.2.1.14.1 Hardware Inventory ... 28
1.2.1.14.2 NTDS Information ... 29
1.2.1.14.3 Time Source Information ... 29
1.2.1.14.4 SRV Records Status ... 29
1.2.1.14.5 Installed Software ... 29
1.2.1.14.6 Roles ... 30
1.2.1.14.7 DC Diagnostic ... 32
1.2.1.14.8 Infrastructure Services Status ... 35
1.2.1.14.9 Sites Replication Connection ... 36
1.2.1.14.10 Sites Replication Status ... 38
1.2.1.14.11 Group Policy Objects Summary ... 38
1.2.1.14.11.1 Central Store Repository ... 41
1.2.1.14.11.2 User Logon/Logoff Script ... 41

1.2.1.14.11.3 Computer Startup/Shutdown Script 41
1.2.1.14.11.4 Unlinked GPO 42
1.2.1.14.11.5 Empty GPOs 42
1.2.1.14.11.6 Enforced GPO 42
1.2.1.14.12 Organizational Units 42
1.2.1.14.12.1 GPO Blocked Inheritance 49
1.2.2 ACAD.PHARMAX.LOCAL Child Domain Configuration 49
1.2.2.1 Flexible Single Master Operations (FSMO) 49
1.2.2.2 Domain and Trusts 50
1.2.2.3 Domain Object Count 50
1.2.2.3.1 Computers Object 50
1.2.2.3.2 Domain Controller Object 51
1.2.2.3.3 Users Object 52
1.2.2.4 User Accounts in Active Directory 53
1.2.2.5 Status of Users Accounts 54
1.2.2.6 Privileged Group Count 54
1.2.2.7 Computer Accounts in Active Directory 55
1.2.2.8 Status of Computer Accounts 56
1.2.2.9 Operating Systems Count 56
1.2.2.10 Default Domain Password Policy 56
1.2.2.11 Fined Grained Password Policies 57
1.2.2.12 Group Managed Service Accounts (GMSA) 57
1.2.2.13 Health Checks 58
1.2.2.14 Domain Controller Summary 60
1.2.2.14.1 Hardware Inventory 61
1.2.2.14.2 NTDS Information 61
1.2.2.14.3 Time Source Information 62
1.2.2.14.4 SRV Records Status 62
1.2.2.14.5 Installed Software 62
1.2.2.14.6 Roles 62
1.2.2.14.7 DC Diagnostic 63
1.2.2.14.8 Infrastructure Services Status 65
1.2.2.14.9 Sites Replication Connection 65
1.2.2.14.10 Sites Replication Status 66
1.2.2.14.11 Group Policy Objects Summary 67
1.2.2.14.11.1 Central Store Repository 68
1.2.2.14.11.2 User Logon/Logoff Script 68
1.2.2.14.11.3 Unlinked GPO 69
1.2.2.14.11.4 Empty GPOs 69

1.2.2.14.11.5 Enforced GPO 69
1.2.2.14.12 Organizational Units 69
1.2.2.14.12.1 GPO Blocked Inheritance 70
1.2.3 UIA.LOCAL Child Domain Configuration 70
1.2.3.1 Flexible Single Master Operations (FSMO) 70
1.2.3.2 Domain and Trusts 71
1.2.3.3 Domain Object Count 71
1.2.3.3.1 Computers Object 71
1.2.3.3.2 Domain Controller Object 72
1.2.3.3.3 Users Object 73
1.2.3.4 User Accounts in Active Directory 74
1.2.3.5 Status of Users Accounts 75
1.2.3.6 Privileged Group Count 75
1.2.3.7 Computer Accounts in Active Directory 76
1.2.3.8 Status of Computer Accounts 77
1.2.3.9 Operating Systems Count 77
1.2.3.10 Default Domain Password Policy 77
1.2.3.11 Health Checks 78
1.2.3.12 Domain Controller Summary 82
1.2.3.12.1 Hardware Inventory 82
1.2.3.12.2 NTDS Information 83
1.2.3.12.3 Time Source Information 83
1.2.3.12.4 SRV Records Status 83
1.2.3.12.5 Installed Software 84
1.2.3.12.6 Roles 84
1.2.3.12.7 DC Diagnostic 84
1.2.3.12.8 Infrastructure Services Status 86
1.2.3.12.9 Sites Replication Connection 87
1.2.3.12.10 Sites Replication Status 88
1.2.3.12.11 Group Policy Objects Summary 88
1.2.3.12.11.1 Central Store Repository 89
1.2.3.12.12 Organizational Units 89
1.3 Domain Name System Summary 94
1.3.1 PHARMAX.LOCAL Root Domain DNS Configuration 94
1.3.1.1 Infrastructure Summary 94
1.3.1.1.1 Domain Controller DNS IP Configuration 94
1.3.1.1.2 Application Directory Partition 94
1.3.1.1.3 Response Rate Limiting (RRL) 95
1.3.1.1.4 Scavenging Options 95

1.3.1.1.5 Forwarder Options 95
1.3.1.1.6 Root Hints 96
1.3.1.1.7 Zone Scope Recursion 96
1.3.1.2 SERVER-DC-01V DNS Zones 97
1.3.1.2.1 Zone Delegation 97
1.3.1.2.2 Zone Transfers 97
1.3.1.2.3 Reverse Lookup Zone 97
1.3.1.2.4 Conditional Forwarder 98
1.3.1.2.5 Zone Scope Aging 98
1.3.1.3 CAYEY-DC-01V DNS Zones 98
1.3.1.3.1 Zone Delegation 98
1.3.1.3.2 Reverse Lookup Zone 98
1.3.1.3.3 Conditional Forwarder 99
1.3.1.3.4 Zone Scope Aging 99
1.3.2 ACAD.PHARMAX.LOCAL Child Domain DNS Configuration 99
1.3.2.1 Infrastructure Summary 99
1.3.2.1.1 Domain Controller DNS IP Configuration 99
1.3.2.1.2 Application Directory Partition 100
1.3.2.1.3 Response Rate Limiting (RRL) 100
1.3.2.1.4 Scavenging Options 100
1.3.2.1.5 Forwarder Options 100
1.3.2.1.6 Root Hints 100
1.3.2.1.7 Zone Scope Recursion 101
1.3.2.2 ACADE-DC-01V DNS Zones 101
1.3.2.2.1 Zone Transfers 101
1.3.2.2.2 Reverse Lookup Zone 102
1.3.2.2.3 Conditional Forwarder 102
1.3.2.2.4 Zone Scope Aging 102
1.3.3 UIA.LOCAL Child Domain DNS Configuration 102
1.3.3.1 Infrastructure Summary 102
1.3.3.1.1 Domain Controller DNS IP Configuration 103
1.3.3.1.2 Application Directory Partition 103
1.3.3.1.3 Response Rate Limiting (RRL) 103
1.3.3.1.4 Scavenging Options 103
1.3.3.1.5 Forwarder Options 104
1.3.3.1.6 Root Hints 104
1.3.3.1.7 Zone Scope Recursion 104
1.3.3.2 DC-UIA-01V DNS Zones 104
1.3.3.2.1 Reverse Lookup Zone 104

1.3.3.2.2 Zone Scope Aging 105
1.4 Dynamic Host Configuration Protocol Summary 105
1.4.1 PHARMAX.LOCAL Root Domain DHCP Configuration 105
1.4.1.1 DHCP Servers In Active Directory 105
1.4.1.1.1 Service Database 106
1.4.1.1.2 Dynamic DNS credentials 106
1.4.1.2 IPv4 Scope Configuration 106
1.4.1.2.1 IPv4 Service Statistics 106
1.4.1.2.2 CAYEY-DC-01V IPv4 Scope Server Options 106
1.4.1.2.2.1 Scope DNS Setting 107
1.4.1.2.3 SERVER-DC-01V IPv4 Scopes 107
1.4.1.2.3.1 IPv4 Scope Statistics 107
1.4.1.2.3.2 IPv4 Network Interface Binding 108
1.4.1.2.4 SERVER-DC-01V IPv4 Scope Server Options 108
1.4.1.2.4.1 Scope DNS Setting 108
1.4.1.2.5 Scope Options 108
1.4.1.3 IPv6 Scope Configuration 110
1.4.1.3.1 IPv6 Service Statistics 110
1.4.2 ACAD.PHARMAX.LOCAL Child Domain DHCP Configuration 111
1.4.2.1 DHCP Servers In Active Directory 111
1.4.2.1.1 Service Database 111
1.4.2.1.2 Dynamic DNS credentials 111
1.4.2.2 IPv4 Scope Configuration 111
1.4.2.2.1 IPv4 Service Statistics 111
1.4.2.2.2 ACADE-DC-01V IPv4 Scopes 112
1.4.2.2.2.1 IPv4 Scope Statistics 112
1.4.2.2.2.2 IPv4 Network Interface Binding 112
1.4.2.2.3 ACADE-DC-01V IPv4 Scope Server Options 112
1.4.2.2.3.1 Scope DNS Setting 112
1.4.2.2.4 Scope Options 113
1.4.2.3 IPv6 Scope Configuration 113
1.4.2.3.1 IPv6 Service Statistics 113
1.4.2.3.2 ACADE-DC-01V IPv6 Scopes 113
1.4.2.3.2.1 IPv6 Scope Statistics 113
1.4.2.3.3 ACADE-DC-01V IPv6 Scope Server Options 114
1.4.2.3.3.1 Scope DNS Settings 114
1.4.2.3.4 Scope Options 114
1.4.3 UIA.LOCAL Child Domain DHCP Configuration 114
1.4.3.1 DHCP Servers In Active Directory 114

1.4.3.1.1 Service Database ... 115
1.4.3.1.2 Dynamic DNS credentials ... 115
1.4.3.2 IPv4 Scope Configuration ... 115
1.4.3.2.1 IPv4 Service Statistics ... 115
1.4.3.2.2 DC-UIA-01V IPv4 Scopes ... 115
1.4.3.2.2.1 IPv4 Scope Statistics ... 116
1.4.3.2.2.2 IPv4 Network Interface Binding ... 116
1.4.3.2.3 Scope Options ... 116
1.4.3.3 IPv6 Scope Configuration ... 116
1.4.3.3.1 IPv6 Service Statistics ... 116
1.5 Certificate Authority Summary ... 116
1.5.1 Enterprise Root Certificate Authority ... 117
1.5.2 Enterprise Subordinate Certificate Authority ... 117
1.5.3 pharmax-SERVER-DC-01V-CA Details ... 118
1.5.3.1 Certificate Validity Period ... 118
1.5.3.2 Access Control List (ACL) ... 118
1.5.3.2.1 Access Rights ... 118
1.5.3.3 Cryptography Configuration ... 119
1.5.3.4 Authority Information Access (AIA) ... 119
1.5.3.5 Certificate Revocation List (CRL) ... 120
1.5.3.5.1 CRL Validity Period ... 120
1.5.3.5.2 CRL Flags Settings ... 120
1.5.3.5.3 CRL Distribution Point ... 120
1.5.3.6 AIA and CDP Health Status ... 122
1.5.3.7 Certificate Template Summary ... 122
1.5.3.7.1 Issued Certificate Template ACLs ... 123
1.5.3.7.2 Certificate Template In Active Directory ... 128
1.5.3.8 Key Recovery Agent Certificate ... 130
1.5.4 acad-ACADE-DC-01V-CA Details ... 130
1.5.4.1 Certificate Validity Period ... 130
1.5.4.2 Access Control List (ACL) ... 130
1.5.4.2.1 Access Rights ... 131
1.5.4.3 Cryptography Configuration ... 131
1.5.4.4 Authority Information Access (AIA) ... 131
1.5.4.5 Certificate Revocation List (CRL) ... 132
1.5.4.5.1 CRL Validity Period ... 132
1.5.4.5.2 CRL Flags Settings ... 133
1.5.4.5.3 CRL Distribution Point ... 133
1.5.4.6 AIA and CDP Health Status ... 134

1.5.4.7 Certificate Template Summary 135
1.5.4.7.1 Issued Certificate Template ACLs 135
1.5.4.7.2 Certificate Template In Active Directory 138
1.5.4.8 Key Recovery Agent Certificate 140
1.5.5 pharmax-CAYEY-DC-01V-CA Details 140
1.5.5.1 Certificate Validity Period 140
1.5.5.2 Access Control List (ACL) 140
1.5.5.2.1 Access Rights 140
1.5.5.3 Cryptography Configuration 141
1.5.5.4 Authority Information Access (AIA) 141
1.5.5.5 Certificate Revocation List (CRL) 142
1.5.5.5.1 CRL Validity Period 142
1.5.5.5.2 CRL Flags Settings 142
1.5.5.5.3 CRL Distribution Point 142
1.5.5.6 AIA and CDP Health Status 144

1 PHARMAX.LOCAL Active Directory Report

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

1.1 Forest Information.

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	-

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

Site Name	Description	Subnets	Creation Date
UIA	-	172.23.7.0/24	5/11/2022

Table 3 - Sites - PHARMAX.LOCAL

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

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

Health Check:
Best Practices: Ensure that subnets has a defined description.

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 Active Directory Domain Information

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 Root Domain Configuration

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 Flexible Single Master Operations (FSMO)

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 Server - pharmax.local

1.2.1.2 Domain and Trusts

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 - PHARMAX.LOCAL

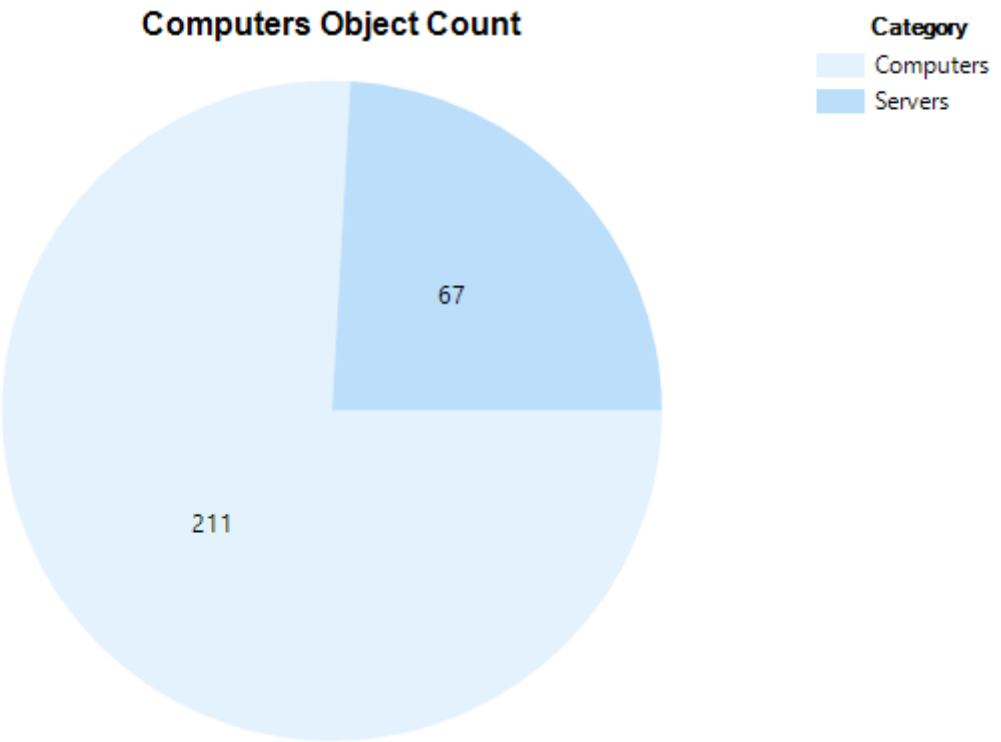
Name	uia.local
Path	pharmax.local/System/uia.local
Source	pharmax
Target	uia.local
Direction	BiDirectional
IntraForest	Yes
Selective Authentication	No

SID Filtering Forest Aware	No
SID Filtering Quarantined	No
Trust Type	Uplevel
Uplevel Only	No

Table 9 - Trusts - PHARMAX.LOCAL

1.2.1.3 Domain Object Count

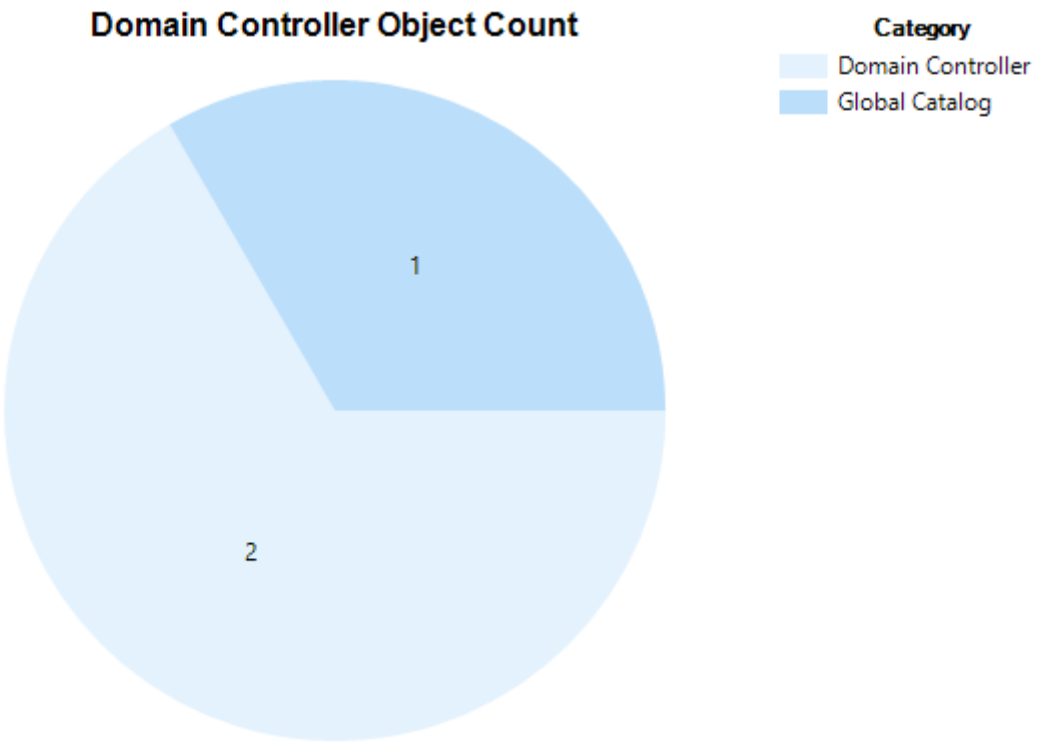
1.2.1.3.1 Computers Object



Computers	211
Servers	67

Table 10 - Computers Object - PHARMAX.LOCAL

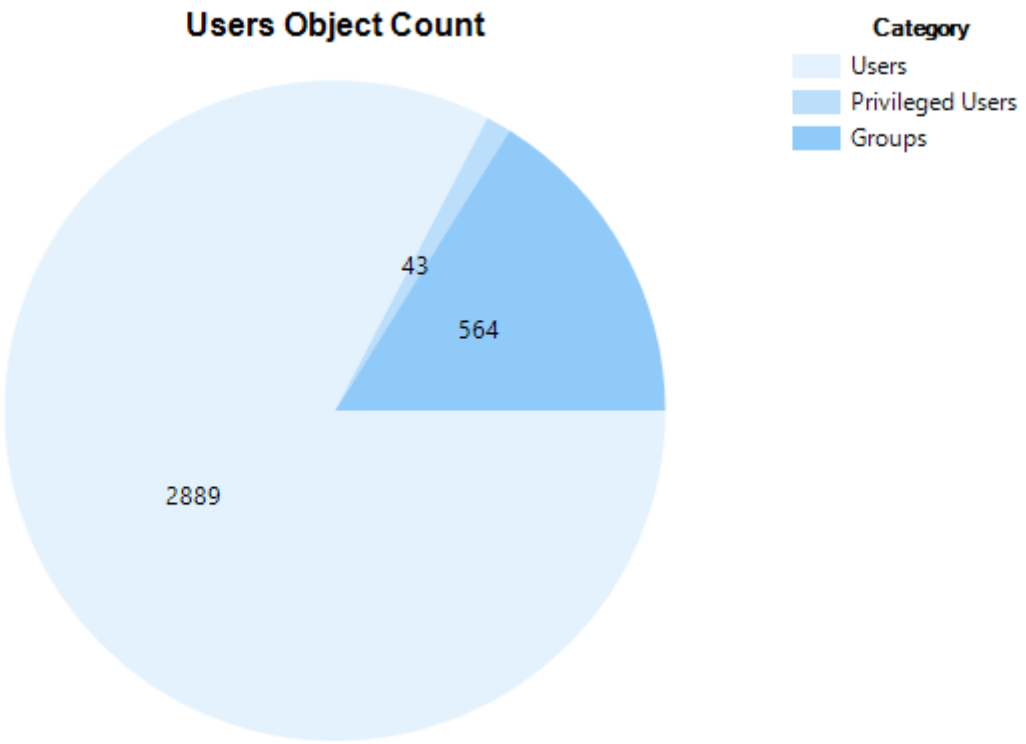
1.2.1.3.2 Domain Controller Object



Domain Controller	2
Global Catalog	1

Table 11 - Domain Controller Object - PHARMAX.LOCAL

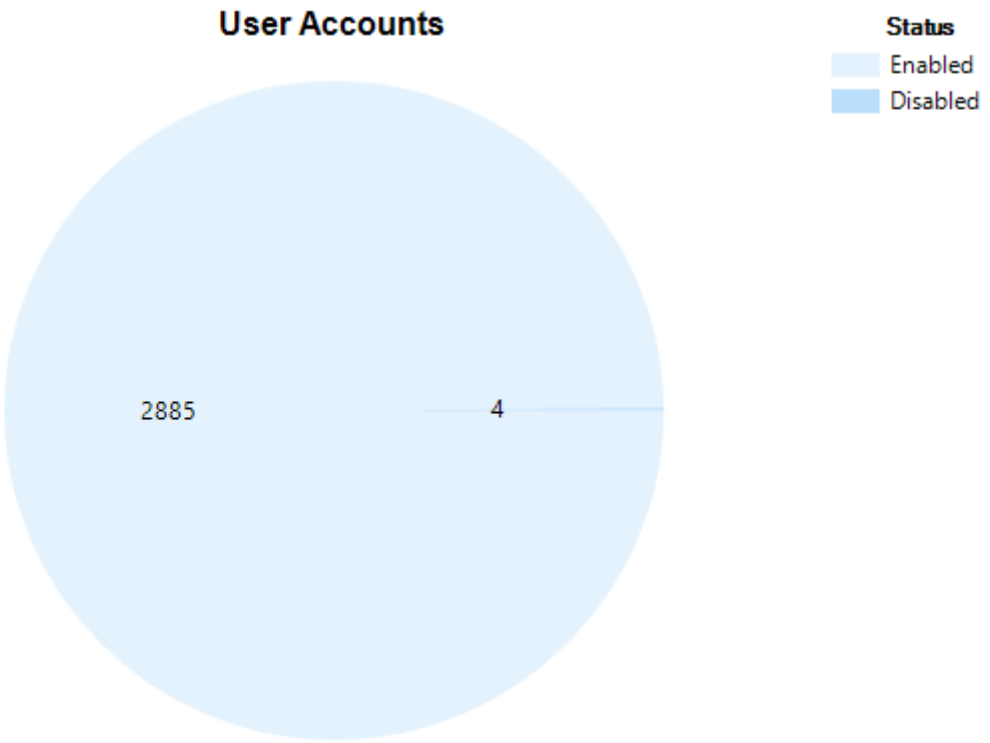
1.2.1.3.3 Users Object



Users	2889
Privileged Users	43
Groups	564

Table 12 - User Object - PHARMAX.LOCAL

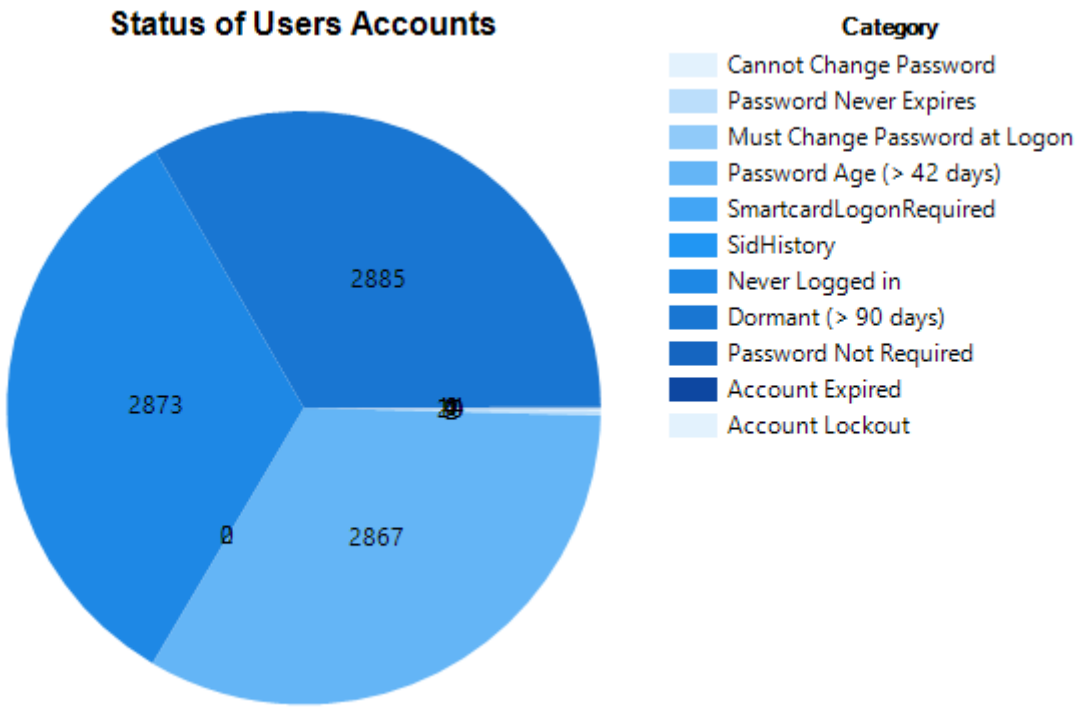
1.2.1.4 User Accounts in Active Directory



Status	Count	Percentage
Enabled	2885	100%
Disabled	4	0%

Table 13 - User Accounts in Active Directory - 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	20	1	1	0	20	1
Must Change Password at Logon	2	0	1	0	2	0
Password Age (> 42 days)	2867	99	1	0	2867	99
SmartcardLogonRequired	2	0	1	0	2	0
SidHistory	0	0	1	0	0	0
Never Logged in	2873	99	1	0	2873	99
Dormant (> 90 days)	2885	100	1	0	2885	100
Password Not Required	4	0	1	0	4	0
Account Expired	1	0	1	0	1	0
Account Lockout	0	0	1	0	0	0

Table 14 - Status of User Accounts - PHARMAX.LOCAL

1.2.1.6 Privileged Group Count

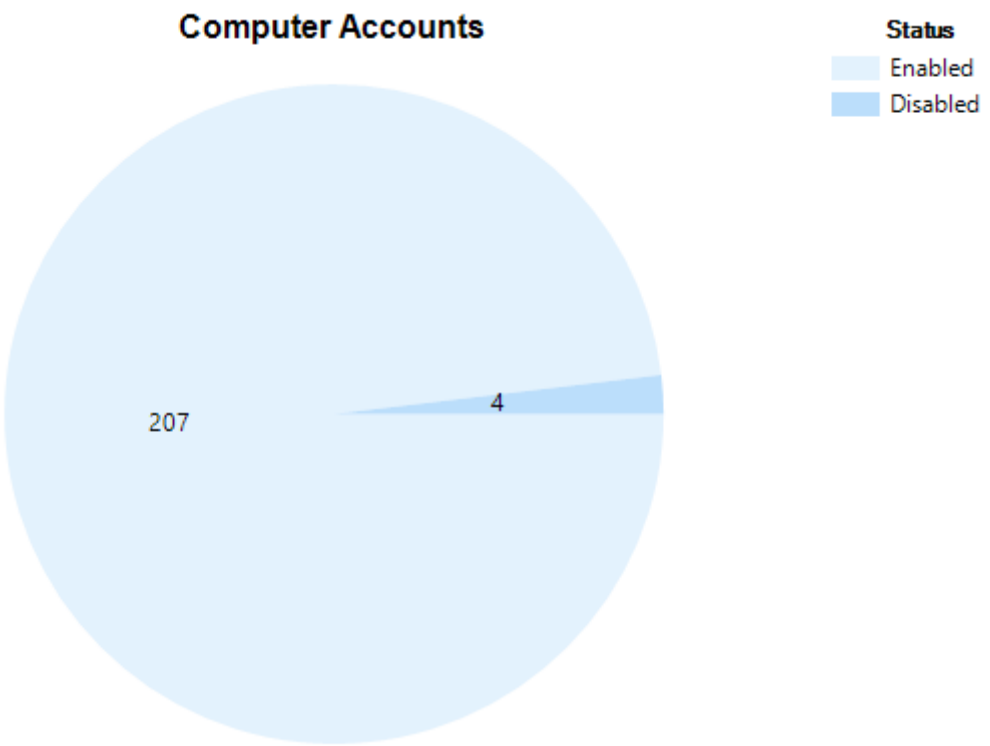
Group Name	Count
Account Operators	1
Administrators	6
Backup Operators	2
Cert Publishers	4

Group Name	Count
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 15 - 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.

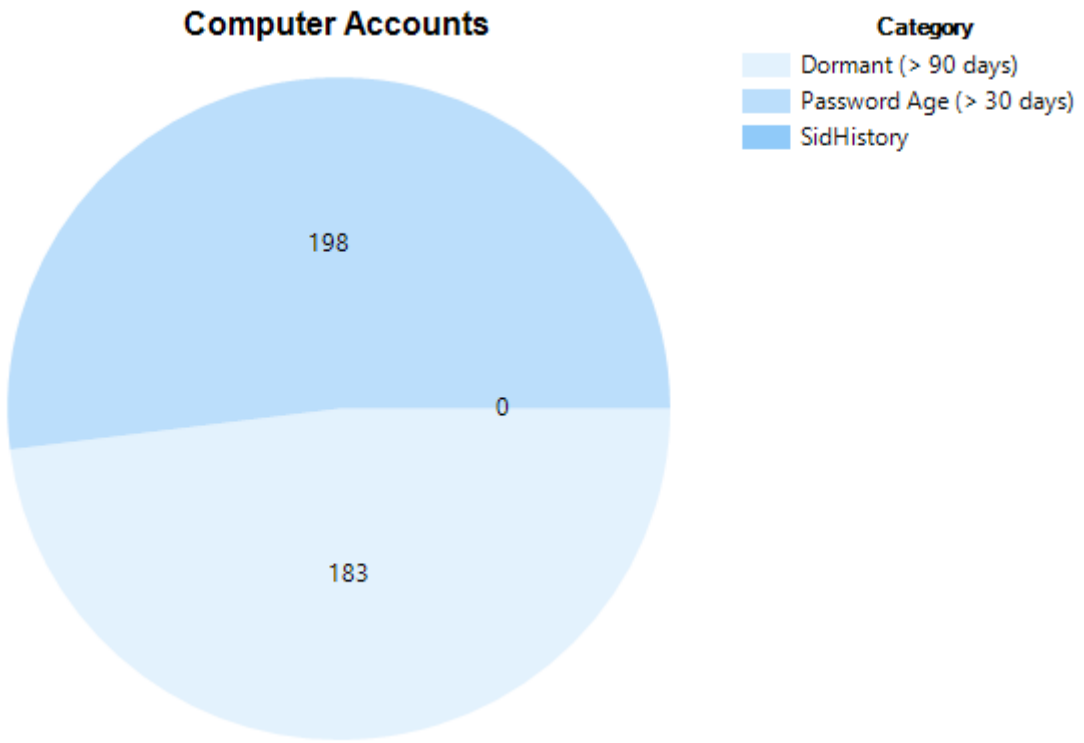
1.2.1.7 Computer Accounts in Active Directory



Status	Count	Percentage
Enabled	207	98%
Disabled	4	2%

Table 16 - Computer Accounts in Active Directory - PHARMAX.LOCAL

1.2.1.8 Status of Computer Accounts



Category	Enabled Count	Enabled %	Disabled Count	Disabled %	Total Count	Total %
Dormant (> 90 days)	183	87	1	0	183	87
Password Age (> 30 days)	198	94	1	0	198	94
SidHistory	0	0	1	0	0	0

Table 17 - 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
NetApp Release 9.8	1
NetApp Release 9.8P7	1
NetApp Release 9.9.1P1	3
OneFS	1
redhat-linux-gnu	1
unknown	7
Unknown	103
Windows 10 Education	1
Windows 10 Enterprise	1

Operating System	Count
Windows 10 Enterprise Evaluation	19
Windows Server 2003	1
Windows Server 2016 Standard Evaluation	10
Windows Server 2019 Standard	1
Windows Server 2019 Standard Evaluation	42
Windows Server 2022 Datacenter	3
Windows Server 2022 Datacenter Evaluation	10
Windows Vista	1
Windows XP	1

Table 18 - 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	00 days 00 hours 30 minutes 00 seconds
Lockout Threshold	0
Lockout Observation Window	00 days 00 hours 30 minutes 00 seconds
Max Password Age	42 days 00 hours 00 minutes 00 seconds
Min Password Age	01 days 00 hours 00 minutes 00 seconds
Min Password Length	7
Enforce Password History	24
Store Password using Reversible Encryption	No

Table 19 - Default Domain Password Policy - PHARMAX.LOCAL

1.2.1.11 Fined Grained Password Policies

Password Setting Name	Administrators
Domain Name	pharmax.local
Complexity Enabled	Yes
Path	pharmax.local/System/Password Settings Container/Administrators
Lockout Duration	00 days 00 hours 30 minutes 00 seconds
Lockout Threshold	0
Lockout Observation Window	00 days 00 hours 30 minutes 00 seconds
Max Password Age	42 days 00 hours 00 minutes 00 seconds
Min Password Age	05 days 00 hours 00 minutes 00 seconds
Min Password Length	12
Password History Count	90

Reversible Encryption Enabled	No
Precedence	1
Applies To	horizon-ic, dbuser, jocolon

Table 20 - Fined Grained Password Policies - Administrators

Password Setting Name	Test
Domain Name	pharmax.local
Complexity Enabled	Yes
Path	pharmax.local/System/Password Settings Container/Test
Lockout Duration	00 days 00 hours 30 minutes 00 seconds
Lockout Threshold	0
Lockout Observation Window	00 days 00 hours 30 minutes 00 seconds
Max Password Age	42 days 00 hours 00 minutes 00 seconds
Min Password Age	01 days 00 hours 00 minutes 00 seconds
Min Password Length	7
Password History Count	23
Reversible Encryption Enabled	No
Precedence	1
Applies To	vmuserro

Table 21 - Fined Grained Password Policies - Test

1.2.1.12 Group Managed Service Accounts (GMSA)

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 22 - Group Managed Service Accounts - SQLServer

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 23 - Group Managed Service Accounts - adfsgmsa

1.2.1.13 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	2022:05:13	148
CN=Schema,CN=Configuration,DC=pharmax,DC=local	2022:05:13	148
DC=DomainDnsZones,DC=pharmax,DC=local	2022:05:02	158
DC=ForestDnsZones,DC=pharmax,DC=local	2022:05:13	148
DC=pharmax,DC=local	2022:05:02	158

Table 24 - 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	3	0.09 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	103.04 MB
.pol	13	0.03 MB
.xml	4	0.01 MB
.zip	5	143.60 MB

Table 25 - 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.

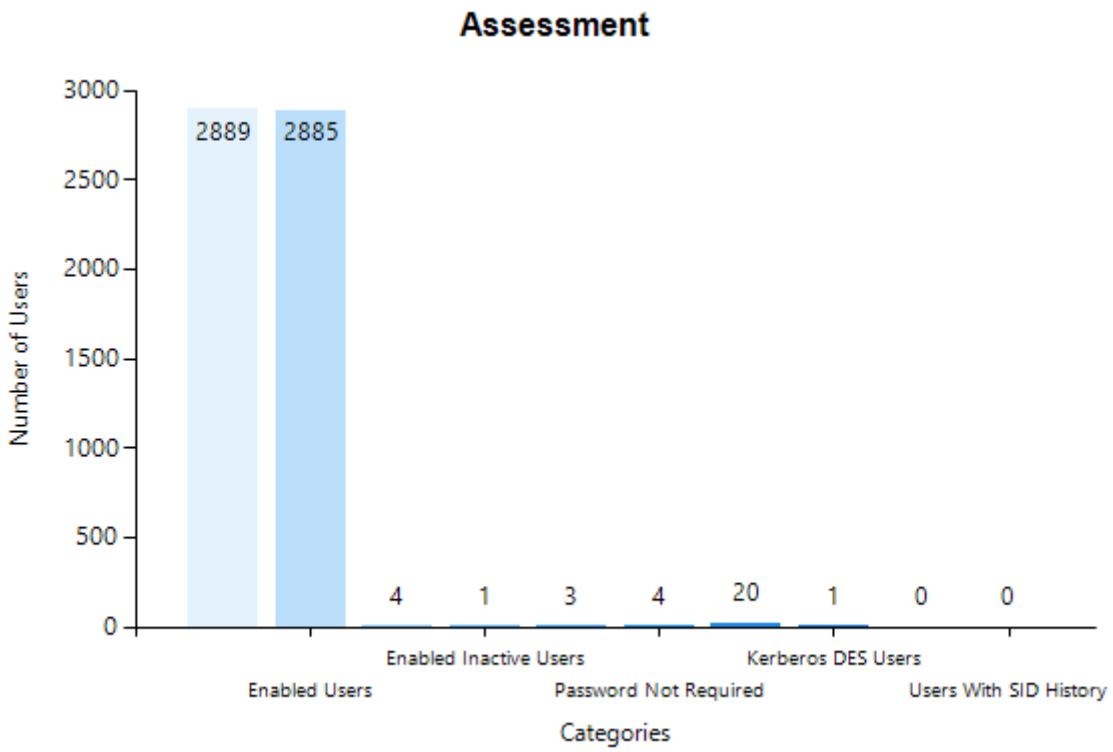
Extension	File Count	Size
.adm	1	0.01 MB
.adml	1	0.03 MB
.admx	1	0.02 MB
.config	7	0.03 MB
.dll	10	12.22 MB
.exe	18	85.80 MB
.ini	1	0.01 MB
.msi	3	103.04 MB
.xml	1	0.00 MB
.zip	5	143.60 MB

Table 26 - 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	2889
Enabled Users	2885

Disabled Users	4
Enabled Inactive Users	1
Users With Reversible Encryption Password	3
Password Not Required	4
Password Never Expires	20
Kerberos DES Users	1
Does Not Require Pre Auth	0
Users With SID History	0

Table 27 - Account Security Assessment - PHARMAX.LOCAL

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

Privileged Users Assessment

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

Username	Created	Password Last Set	Last Logon Date
krbtgt	6/10/2018	6/10/2018	-
Administrator	6/10/2018	6/10/2018	12/10/2053
jocolon	12/4/2019	11/30/2021	12/22/2043
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	-

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

Table 28 - 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

Username	Enabled	Password Last Set	Last Logon Date	Service Principal Name
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
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	8/10/2022	8/26/2022	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	4/5/2022	-	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

Table 29 - 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 30 - 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 31 - 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 32 - 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 33 - Duplicate Object - PHARMAX.LOCAL

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

1.2.1.14 Domain Controller Summary

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
CAYEY-DC-01V	pharmax.local	Cayey-Branch	No	No	10.10.33.1
SERVER-DC-01V	pharmax.local	Pharmax-HQ	Yes	No	192.168.5.1

Table 34 - Domain Controller Summary - PHARMAX.LOCAL

1.2.1.14.1 Hardware Inventory

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

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	
Number of CPU Cores	2
Number of Logical Cores	2
Physical Memory (GB)	4.00 GB

Table 35 - Hardware Inventory - SERVER-DC-01V

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	
Number of CPU Cores	2
Number of Logical Cores	2
Physical Memory (GB)	4.00 GB

Table 36 - Hardware Inventory - CAYEY-DC-01V

1.2.1.14.2 NTDS Information

DC Name	Database File	Database Size	Log Path	SysVol Path
CAYEY-DC-01V	C:\Windows\NTDS\ntds.dit	72.00 MB	C:\Windows\NTDS	C:\Windows\SYSVOL\sysvol
SERVER-DC-01V	C:\Windows\NTDS\ntds.dit	80.00 MB	C:\Windows\NTDS	C:\Windows\SYSVOL\sysvol

Table 37 - NTDS Database File Usage - PHARMAX.LOCAL

1.2.1.14.3 Time Source Information

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

Table 38 - Time Source Configuration - PHARMAX.LOCAL

1.2.1.14.4 SRV Records Status

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

Table 39 - 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.

1.2.1.14.5 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
Npcap	Nmap Project	-
RVTools	Robware	20220824
Veeam Agent for Microsoft Windows	Veeam Software Group GmbH	20220916
Veeam Backup Transport	Veeam Software Group GmbH	20220916
Veeam Backup VSS Integration	Veeam Software Group GmbH	20220916
Veeam Installer Service	Veeam Software Group GmbH	-
Veeam VSS Hardware Provider	Veeam Software Group GmbH	20220916

Table 40 - 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 41 - Installed Software - CAYEY-DC-01V

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

1.2.1.14.6 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.
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.
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 42 - 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 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 43 - 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.

1.2.1.14.7 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).
VerifyReplicas	Passed	High	Checks that all application directory partitions are fully instantiated on all replica servers.
DNS	Passed	Medium	DNS Includes six optional DNS-related tests, as well as the Connectivity test, which runs by default.
VerifyReferences	Passed	High	Validates that several attributes are present for the domain in the countainer and subcontainers in the DC objetcs. This test will fail if any attribute is missing.
SystemLog	Failed	Low	Checks if there is any erros in the Event Viewer > System event log in the past 60 minutes. Since the System event log records data from many places, errors reported here may lead to false positive and must be investigated further. The impact of this validation is marked as Low.
Topology	Passed	Medium	Topology Checks that the KCC has generated a fully connected topology for all domain controllers.
CutoffServers	Passed	Medium	Checks for any server that is not receiving replications because its partners are not running
FrsEvent	Passed	Medium	Checks if theres any errors in the event logs regarding FRS replication. If running Windows Server 2008 R2 or newer on all Domain Controllers is possible SYSVOL were already migrated to DFSR, in this case errors found here can be ignored.
CheckSecurityError	Passed	Medium	Reports on the overall health of replication with respect to Active Directory security in domain controllers running Windows Server 2003 SP1.

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

Table 44 - 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$. which can lead to failures in organizations that disable IPC$.

Test Name	Result	Impact	Description
Services	Passed	High	Validates if the core Active Directory services are running in this Domain Controller. The services verified are: RPCSS, EVENTSYSTEM, DNSCACHE, ISMSERV, KDC, SAMSS, WORKSTATION, W32TIME, NETLOGON, NTDS (in case Windows Server 2008 or newer) and DFSR (if SYSVOL is using DFSR).
VerifyReplicas	Passed	High	Checks that all application directory partitions are fully instantiated on all replica servers.
DNS	Passed	Medium	DNS Includes six optional DNS-related tests, as well as the Connectivity test, which runs by default.
VerifyReferences	Passed	High	Validates that several attributes are present for the domain in the countainer and subcontainers in the DC objetcs. This test will fail if any attribute is missing.
SystemLog	Failed	Low	Checks if there is any erros in the Event Viewer > System event log in the past 60 minutes. Since the System event log records data from many places, errors reported here may lead to false positive and must be investigated further. The impact of this validation is marked as Low.
Topology	Passed	Medium	Topology Checks that the KCC has generated a fully connected topology for all domain controllers.
CutoffServers	Passed	Medium	Checks for any server that is not receiving replications because its partners are not running
FrsEvent	Passed	Medium	Checks if theres any errors in the event logs regarding FRS replication. If running Windows Server 2008 R2 or newer on all Domain Controllers is possible SYSVOL were already migrated to DFSR, in this case errors found here can be ignored.
CheckSecurityError	Passed	Medium	Reports on the overall health of replication with respect to Active Directory security in domain controllers running Windows Server 2003 SP1.
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	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.

Test Name	Result	Impact	Description
KccEvent	Failed	High	Validates through KCC there were no errors in the Event Viewer > Applications and Services Logs > Directory Services event log in the past 15 minutes (default time).
SysVolCheck	Passed	High	Validates if the registry key HKEY_Local_Machine\System\CurrentControlSet\Services\Netlogon\Parameters\SysvolReady=1 exist. This registry has to exist with value 1 for the DCs SYSVOL to be advertised.
FrsSysVol	Passed	Medium	Checks that the file replication system (FRS) system volume (SYSVOL) is ready

Table 45 - DCDiag Test Status - CAYEY-DC-01V

1.2.1.14.8 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 46 - 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 47 - 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.

1.2.1.14.9 Sites Replication Connection

The following section provides detailed information about Site Replication Connection.

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
AutoGenerated	Yes
Enabled	Yes
Created	Tue, 07 Dec 2021 15:52:27 GMT

Table 48 - Site Replication - 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
AutoGenerated	Yes

Enabled	Yes
Created	Wed, 11 May 2022 17:54:53 GMT

Table 49 - Site Replication - 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
AutoGenerated	Yes
Enabled	Yes
Created	Sun, 05 Sep 2021 16:24:39 GMT

Table 50 - Site Replication - SERVER-DC-01V

CAYEY-DC-01V

GUID	25644f18-da4e-4c5a-887e-1b17b61e9d53
Description	-
Replicate From Directory Server	SERVER-DC-01V
Replicate To Directory Server	CAYEY-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
AutoGenerated	Yes
Enabled	Yes
Created	Tue, 07 Dec 2021 15:55:03 GMT

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

GUID	9d1d0689-b5e5-4bdf-b75d-9c8ca53a6fa2
Description	-
Replicate From Directory Server	ACADE-DC-01V
Replicate To Directory Server	CAYEY-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
AutoGenerated	Yes
Enabled	Yes
Created	Sat, 17 Sep 2022 13:54:49 GMT

Table 52 - Site Replication - CAYEY-DC-01V

1.2.1.14.10 Sites Replication Status

Destination DSA	Source DSA	Source DSA Site	Last Success Time	Last Failure Status	Last Failure Time	Number of failures
SERVER-DC-01V	CAYEY-DC-01V	Cayey-Branch	2022-10-08 19:22:29	0	0	0
SERVER-DC-01V	ACADE-DC-01V	ACAD	2022-10-08 19:22:29	0	0	0
SERVER-DC-01V	CAYEY-DC-01V	Cayey-Branch	2022-10-08 19:22:29	0	0	0
SERVER-DC-01V	DC-UIA-01V	UIA	2022-10-08 19:22:29	0	0	0
SERVER-DC-01V	ACADE-DC-01V	ACAD	2022-10-08 19:22:29	0	0	0
SERVER-DC-01V	CAYEY-DC-01V	Cayey-Branch	2022-10-08 19:22:29	0	0	0
SERVER-DC-01V	DC-UIA-01V	UIA	2022-10-08 19:22:29	0	0	0
SERVER-DC-01V	CAYEY-DC-01V	Cayey-Branch	2022-10-08 19:22:29	0	0	0
SERVER-DC-01V	ACADE-DC-01V	ACAD	2022-10-08 19:22:29	0	0	0
SERVER-DC-01V	DC-UIA-01V	UIA	2022-10-08 19:22:29	0	0	0
SERVER-DC-01V	CAYEY-DC-01V	Cayey-Branch	2022-10-08 19:22:29	0	0	0
SERVER-DC-01V	ACADE-DC-01V	ACAD	2022-10-08 19:22:29	0	0	0
SERVER-DC-01V	DC-UIA-01V	UIA	2022-10-08 19:22:29	0	0	0
SERVER-DC-01V	ACADE-DC-01V	ACAD	2022-10-08 19:22:29	0	0	0
SERVER-DC-01V	DC-UIA-01V	UIA	2022-10-08 19:22:29	0	0	0

Table 53 - Site Replication Status - PHARMAX.LOCAL

1.2.1.14.11 Group Policy Objects Summary

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

GPO Name	Assign-Applications
GPO Status	All Settings Enabled
Created	03/10/2021
Modified	03/10/2021
Description	
Owner	PHARMAX\Domain Admins

Table 54 - GPO - Assign-Applications

GPO Name	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

GPO Name	Default Domain Policy
GPO Status	All Settings Enabled
Created	06/10/2018
Modified	12/19/2021
Description	
Owner	PHARMAX\Domain Admins

Table 56 - GPO - Default Domain Policy

GPO Name	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

GPO Name	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

GPO Name	Default Domain Controllers Policy
GPO Status	All Settings Enabled
Created	06/10/2018
Modified	11/01/2020
Description	
Owner	PHARMAX\Domain Admins

Table 59 - GPO - Default Domain Controllers Policy

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

Table 60 - GPO - ProfileUnity

GPO Name	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

GPO Name	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

GPO Name	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

GPO Name	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

GPO Name	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

GPO Name	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

GPO Name	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

GPO Name	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

1.2.1.14.11.1 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

1.2.1.14.11.2 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

1.2.1.14.11.3 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

1.2.1.14.11.4 Unlinked GPO

GPO Name	Created	Modified	Computer Enabled	User Enabled
Assign-Applications	2021-03-11	2021-03-11	Yes	Yes
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.

1.2.1.14.11.5 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.

1.2.1.14.11.6 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.

1.2.1.14.12 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	-

Name	Path	Linked GPO
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	-
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	-
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	-
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	-

Name	Path	Linked GPO
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	-
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	-

Name	Path	Linked GPO
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	-
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	-

Name	Path	Linked GPO
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	-
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	-

Name	Path	Linked GPO
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	-
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

1.2.1.14.12.1 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 Child Domain Configuration

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 Flexible Single Master Operations (FSMO)

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 Server - acad.pharmax.local

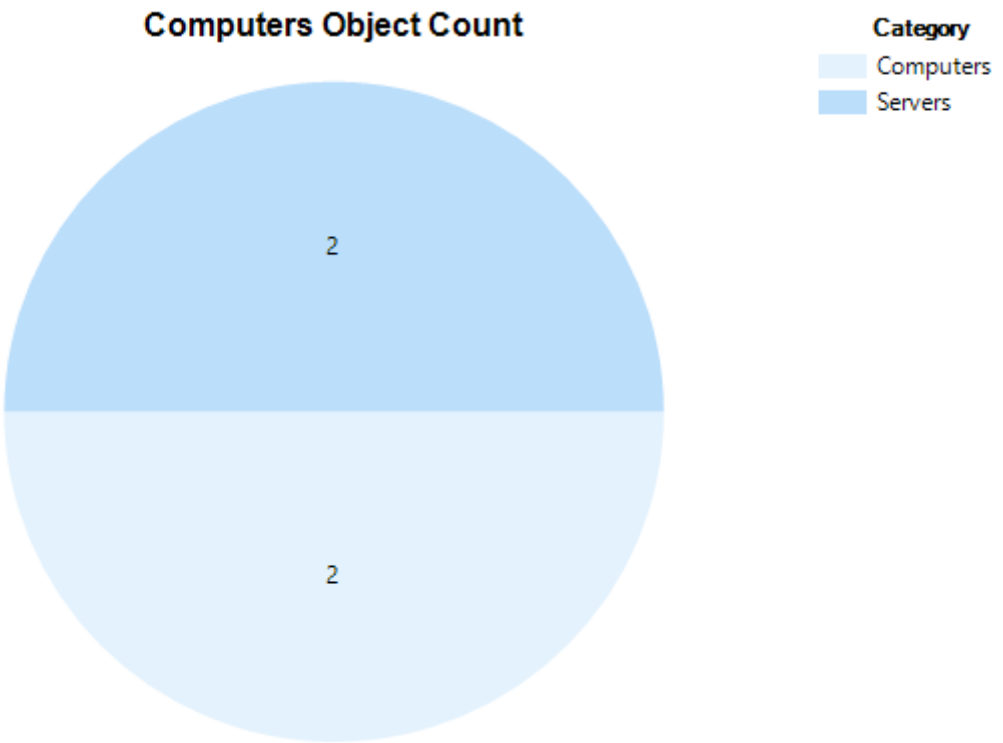
1.2.2.2 Domain and Trusts

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 - ACAD.PHARMAX.LOCAL

1.2.2.3 Domain Object Count

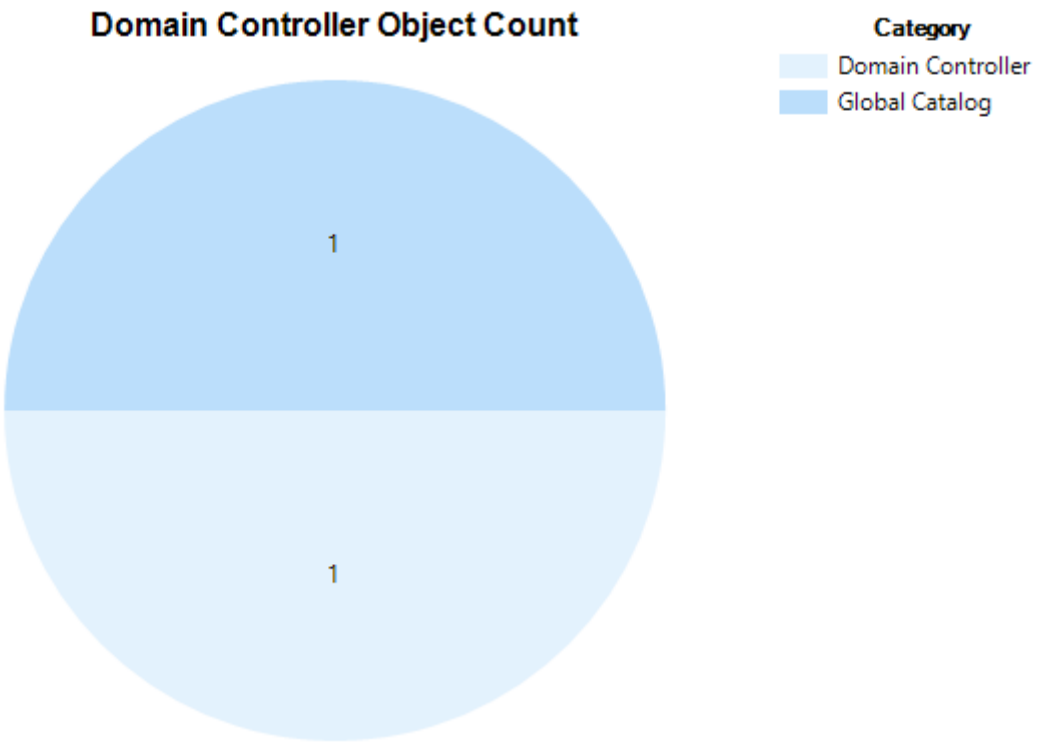
1.2.2.3.1 Computers Object



Computers	2
Servers	2

Table 80 - Computers Object - ACAD.PHARMAX.LOCAL

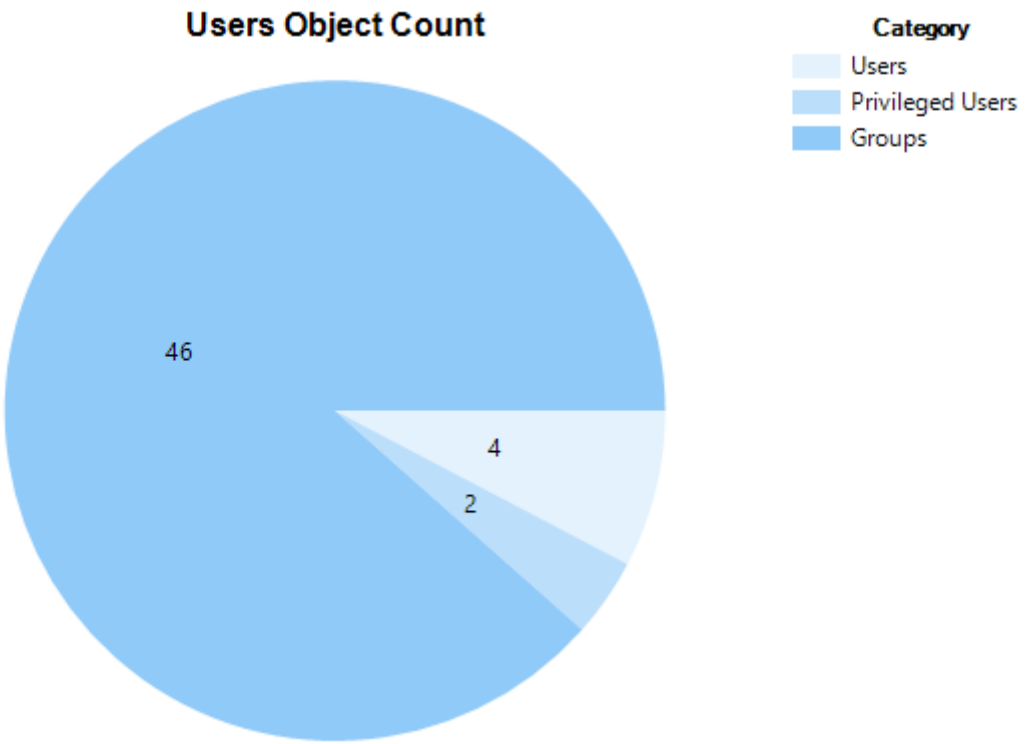
1.2.2.3.2 Domain Controller Object



Domain Controller	1
Global Catalog	1

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

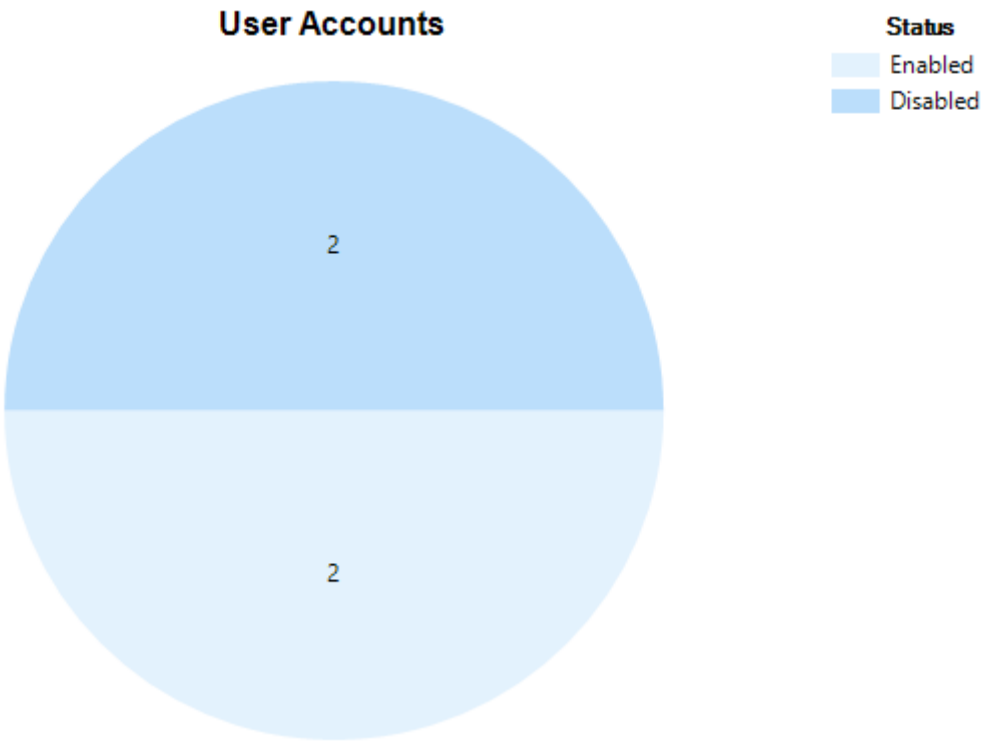
1.2.2.3.3 Users Object



Users	4
Privileged Users	2
Groups	46

Table 82 - User Object - ACAD.PHARMAX.LOCAL

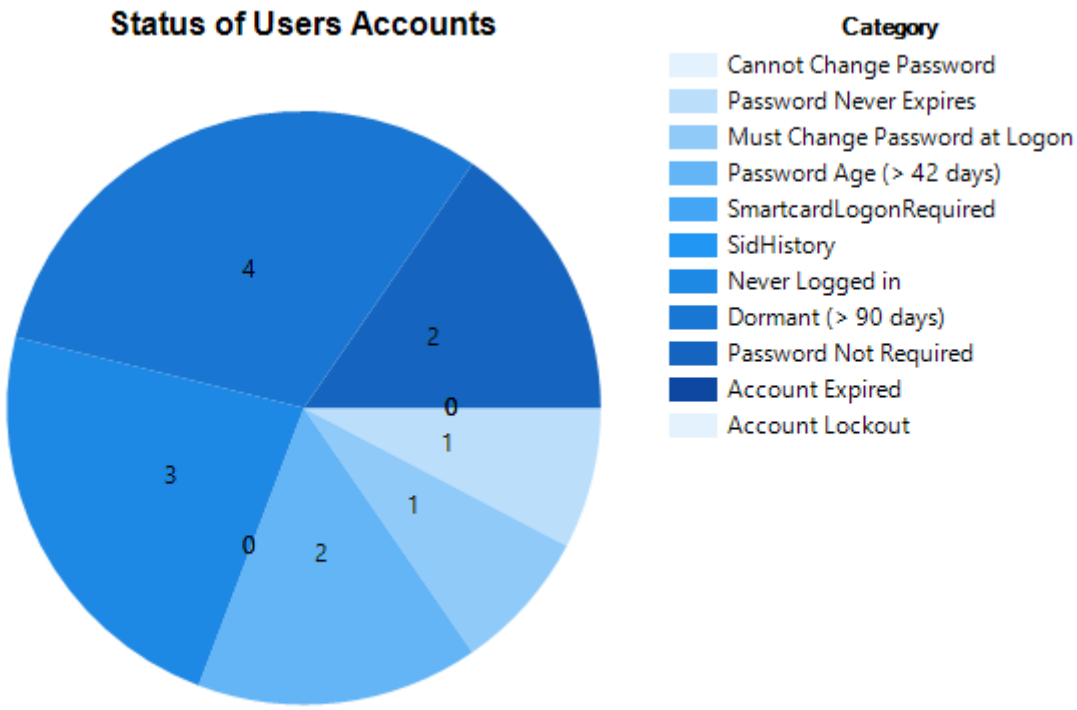
1.2.2.4 User Accounts in Active Directory



Status	Count	Percentage
Enabled	2	50%
Disabled	2	50%

Table 83 - User Accounts in Active Directory - 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

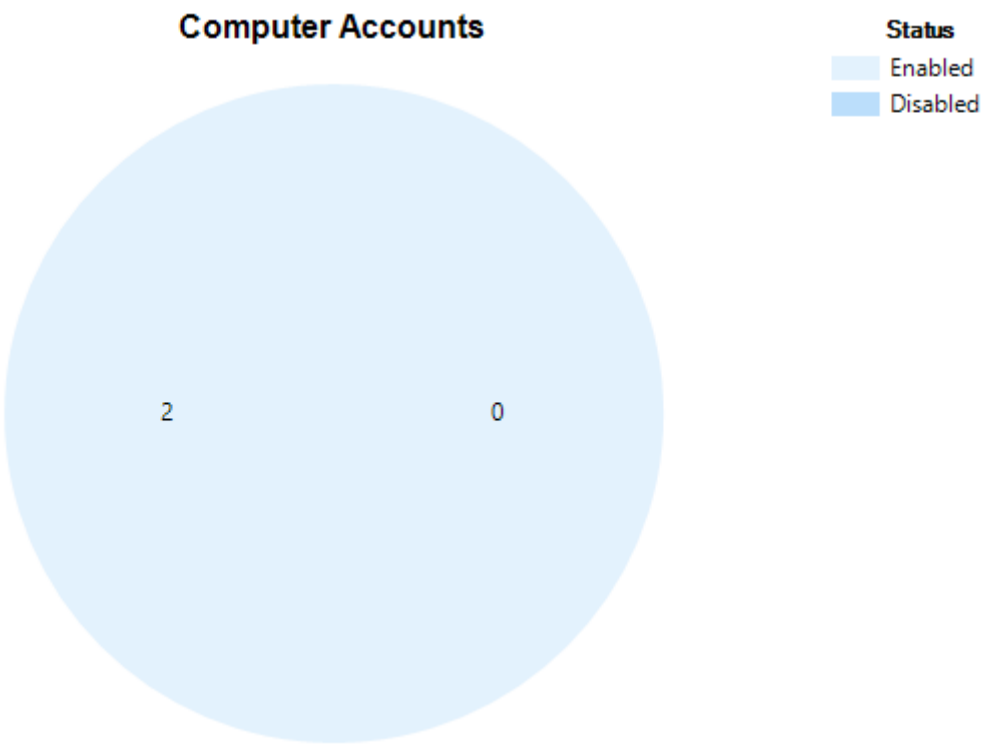
1.2.2.6 Privileged Group Count

Group Name	Count
Account Operators	0
Administrators	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

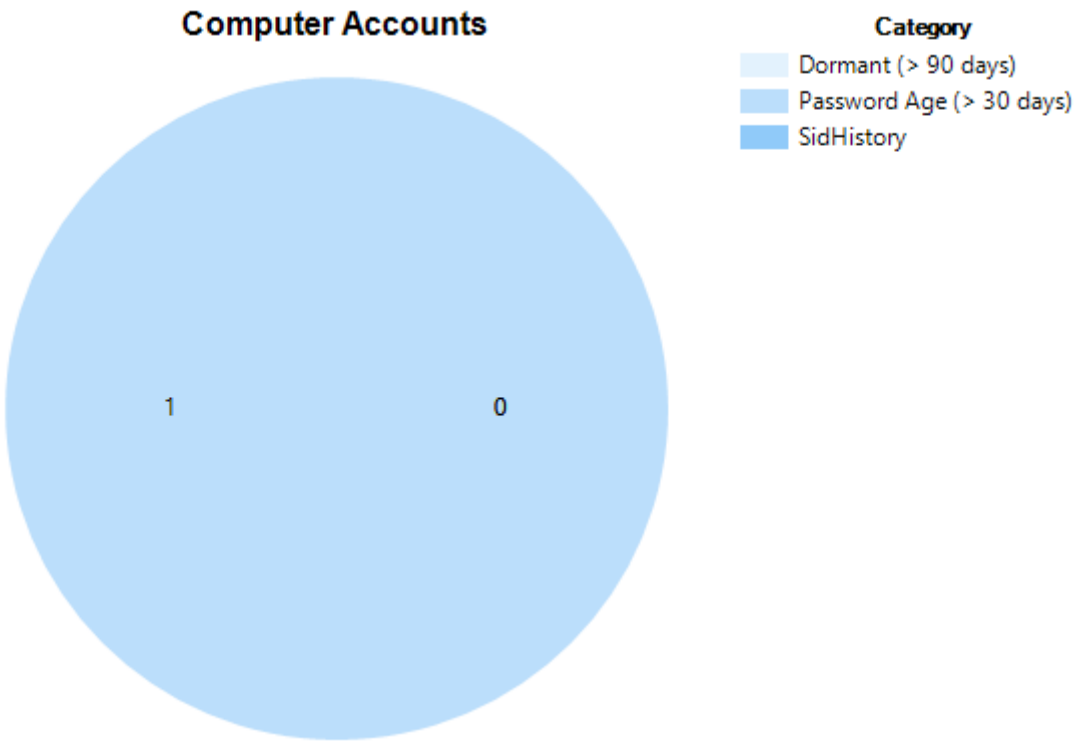
1.2.2.7 Computer Accounts in Active Directory



Status	Count	Percentage
Enabled	2	100%
Disabled	0	0%

Table 86 - Computer Accounts in Active Directory - ACAD.PHARMAX.LOCAL

1.2.2.8 Status of Computer Accounts



Category	Enabled Count	Enabled %	Disabled Count	Disabled %	Total Count	Total %
Dormant (> 90 days)	0	0	1	50	0	0
Password Age (> 30 days)	1	50	1	50	1	50
SidHistory	0	0	1	50	0	0

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

1.2.2.9 Operating Systems Count

Operating System	Count
Windows Server 2019 Standard	1
Windows Server 2019 Standard 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	00 days 00 hours 30 minutes 00 seconds
Lockout Threshold	0
Lockout Observation Window	00 days 00 hours 30 minutes 00 seconds

Max Password Age	42 days 00 hours 00 minutes 00 seconds
Min Password Age	01 days 00 hours 00 minutes 00 seconds
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

Password Setting Name	ACADTest
Domain Name	acad.pharmax.local
Complexity Enabled	Yes
Path	acad.pharmax.local/System/Password Settings Container/ACADTest
Lockout Duration	00 days 00 hours 30 minutes 00 seconds
Lockout Threshold	5
Lockout Observation Window	00 days 00 hours 30 minutes 00 seconds
Max Password Age	42 days 00 hours 00 minutes 00 seconds
Min Password Age	01 days 00 hours 00 minutes 00 seconds
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 Group Managed Service Accounts (GMSA)

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 - Group Managed Service Accounts - 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	2022:05:13	148
CN=Schema,CN=Configuration,DC=pharmax,DC=local	2022:05:13	148
DC=acad,DC=pharmax,DC=local	2021:09:05	398
DC=DomainDnsZones,DC=acad,DC=pharmax,DC=local	2021:09:05	398
DC=ForestDnsZones,DC=pharmax,DC=local	2022:05:13	148

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.

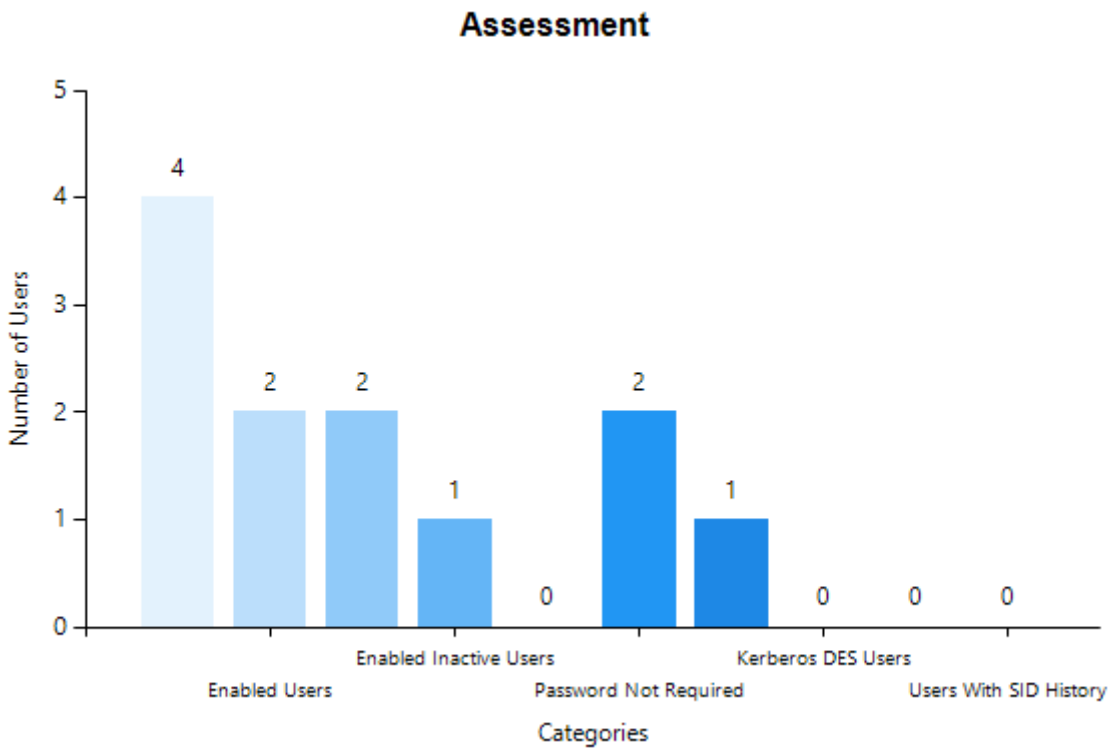
Extension	File Count	Size
.cab	12	2,866.91 MB
.esd	1	3,193.66 MB
.exe	119	1,117.91 MB

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 Controller Summary

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 Controller Summary - 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

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	
Number of CPU Cores	2
Number of Logical Cores	2
Physical Memory (GB)	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	64.00 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 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.

Name	Parent	InstallState
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 106 - 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.

1.2.2.14.7 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.
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	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	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	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 107 - DCDiag Test Status - ACADE-DC-01V

1.2.2.14.8 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
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 108 - 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.

1.2.2.14.9 Sites Replication Connection

The following section provides detailed information about Site Replication Connection.

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
AutoGenerated	Yes
Enabled	Yes
Created	Sun, 05 Sep 2021 16:26:31 GMT

Table 109 - Site Replication - ACADE-DC-01V

GUID	4c26cbdb-51be-4426-ad5f-89d22029c6dd
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
AutoGenerated	Yes
Enabled	Yes
Created	Sat, 17 Sep 2022 13:54:46 GMT

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

GUID	9adda4f1-5c14-4dca-beef-a7a36d6d3609
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
AutoGenerated	Yes
Enabled	Yes
Created	Sat, 17 Sep 2022 13:54:46 GMT

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

1.2.2.14.10 Sites Replication Status

Destination DSA	Source DSA	Source DSA Site	Last Success Time	Last Failure Status	Last Failure Time	Number of failures
ACADE-DC-01V	SERVER-DC-01V	Pharmax-HQ	2022-09-11 20:35:10	-2146893022	2022-10-08 19:24:49	79
ACADE-DC-01V	CAYEY-DC-01V	Cayey-Branch	2022-09-17 13:04:46	-2146893022	2022-10-08 19:24:49	64
ACADE-DC-01V	DC-UIA-01V	UIA	2022-10-08 19:24:50	0	0	0
ACADE-DC-01V	SERVER-DC-01V	Pharmax-HQ	2022-09-11 20:35:10	-2146893022	2022-10-08 19:24:50	79
ACADE-DC-01V	CAYEY-DC-01V	Cayey-Branch	2022-09-17 13:04:46	-2146893022	2022-10-08 19:24:50	64
ACADE-DC-01V	DC-UIA-01V	UIA	2022-10-08 19:24:50	0	0	0
ACADE-DC-01V	SERVER-DC-01V	Pharmax-HQ	2022-09-11 20:35:10	1256	2022-10-08 19:24:49	79

Destination DSA	Source DSA	Source DSA Site	Last Success Time	Last Failure Status	Last Failure Time	Number of failures
ACADE-DC-01V	CAYEY-DC-01V	Cayey-Branch	2022-09-17 13:04:46	1256	2022-10-08 19:24:49	64
ACADE-DC-01V	DC-UIA-01V	UIA	2022-10-08 19:24:50	0	0	0
ACADE-DC-01V	SERVER-DC-01V	Pharmax-HQ	2022-09-11 20:35:10	1256	2022-10-08 19:24:49	79
ACADE-DC-01V	CAYEY-DC-01V	Cayey-Branch	2022-09-17 13:04:46	1256	2022-10-08 19:24:49	64
ACADE-DC-01V	DC-UIA-01V	UIA	2022-10-08 19:24:50	0	0	0
ACADE-DC-01V	SERVER-DC-01V	Pharmax-HQ	2022-09-11 20:35:10	1256	2022-10-08 19:24:49	79
ACADE-DC-01V	DC-UIA-01V	UIA	2022-10-08 19:24:50	0	0	0

Table 112 - Site Replication Status - ACAD.PHARMAX.LOCAL

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

1.2.2.14.11 Group Policy Objects Summary

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

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

Table 113 - GPO - Empty Policy ACAD

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

Table 114 - GPO - Default Domain Policy

GPO Name	Unlinked Policy ACAD
GPO Status	All Settings Disabled
Created	10/05/2021
Modified	10/05/2021
Description	
Owner	PHARMAX\Enterprise Admins

Table 115 - GPO - Unlinked Policy ACAD

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

Table 116 - GPO - Default Domain Controllers Policy

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

Table 117 - GPO - ACAD Certificate AutoEnrollment

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

Table 118 - GPO - Logon Script

1.2.2.14.11.1 Central Store Repository

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

Table 119 - GPO Central Store - ACAD.PHARMAX.LOCAL

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

1.2.2.14.11.2 User Logon/Logoff Script

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

Table 120 - GPO with Logon/Logoff Script - ACAD.PHARMAX.LOCAL

1.2.2.14.11.3 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 121 - Unlinked GPO - ACAD.PHARMAX.LOCAL

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

1.2.2.14.11.4 Empty GPOs

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

Table 122 - Empty GPO - ACAD.PHARMAX.LOCAL

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

1.2.2.14.11.5 Enforced GPO

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

Table 123 - Enforced GPO - ACAD.PHARMAX.LOCAL

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

1.2.2.14.12 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	-
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 124 - Organizational Unit - ACAD.PHARMAX.LOCAL

1.2.2.14.12.1 GPO Blocked Inheritance

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

Table 125 - 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 Child Domain Configuration

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 126 - Domain Summary - UIA.LOCAL

1.2.3.1 Flexible Single Master Operations (FSMO)

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 127 - FSMO Server - uia.local

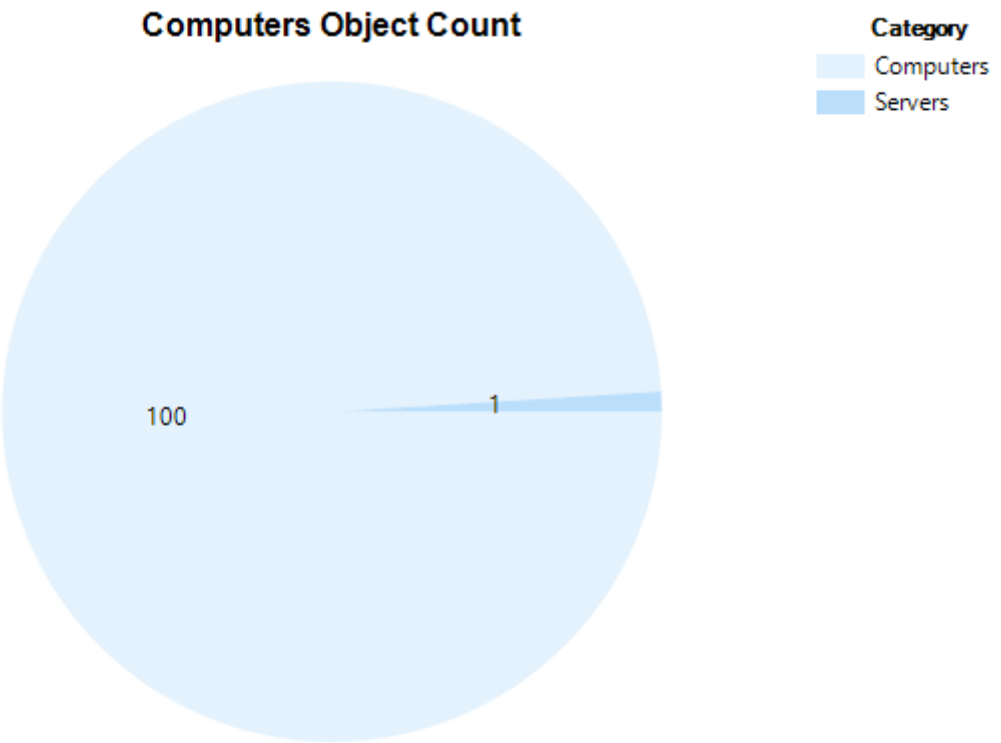
1.2.3.2 Domain and Trusts

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 128 - Trusts - UIA.LOCAL

1.2.3.3 Domain Object Count

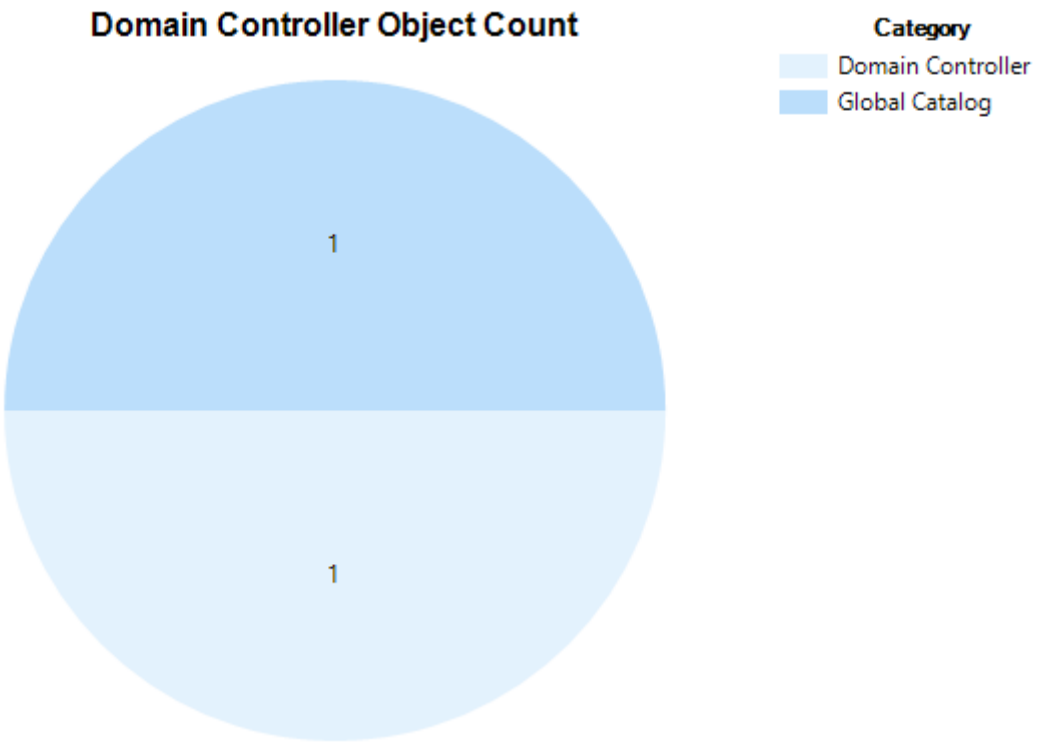
1.2.3.3.1 Computers Object



Computers	100
Servers	1

Table 129 - Computers Object - UIA.LOCAL

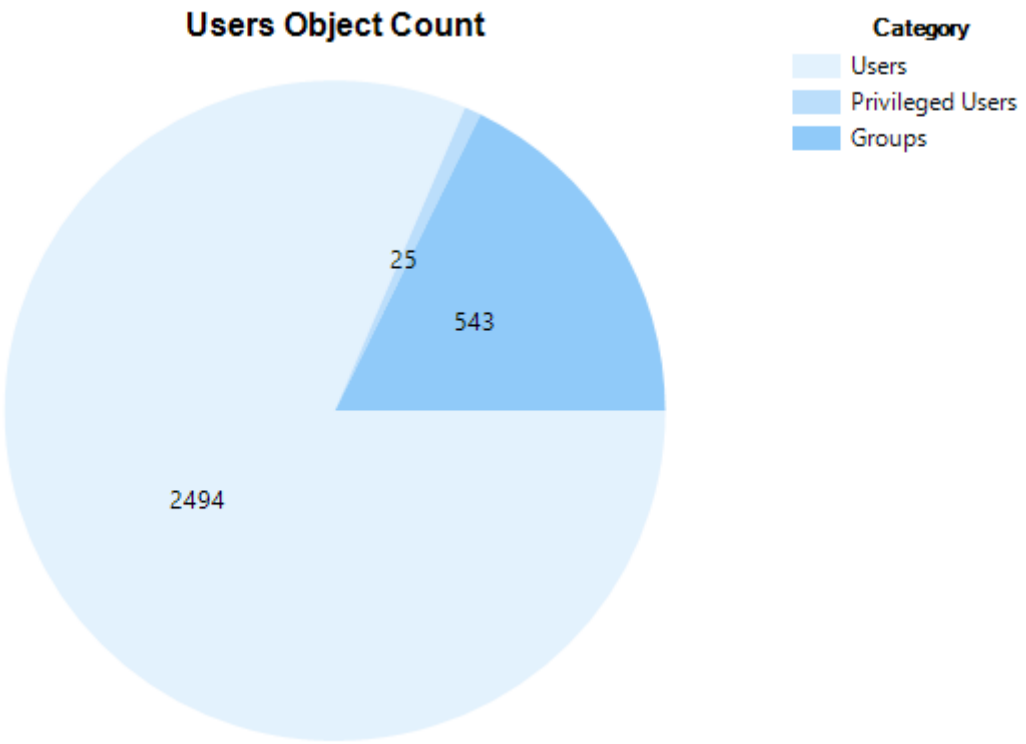
1.2.3.3.2 Domain Controller Object



Domain Controller	1
Global Catalog	1

Table 130 - Domain Controller Object - UIA.LOCAL

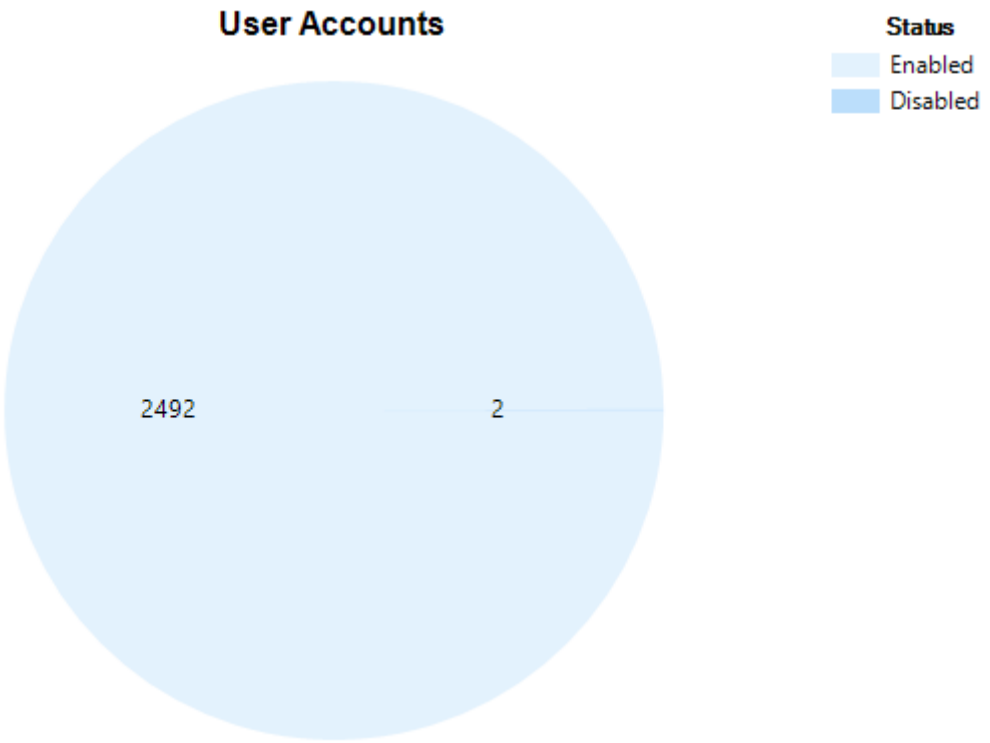
1.2.3.3.3 Users Object



Users	2494
Privileged Users	25
Groups	543

Table 131 - User Object - UIA.LOCAL

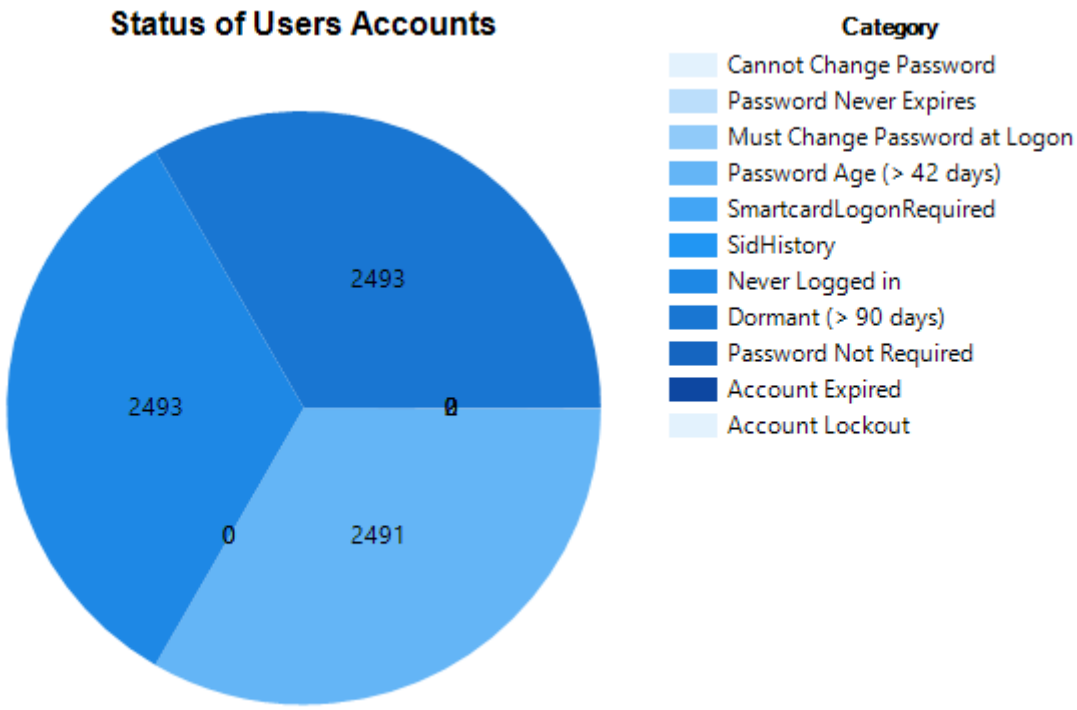
1.2.3.4 User Accounts in Active Directory



Status	Count	Percentage
Enabled	2492	100%
Disabled	2	0%

Table 132 - User Accounts in Active Directory - 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 133 - Status of User Accounts - UIA.LOCAL

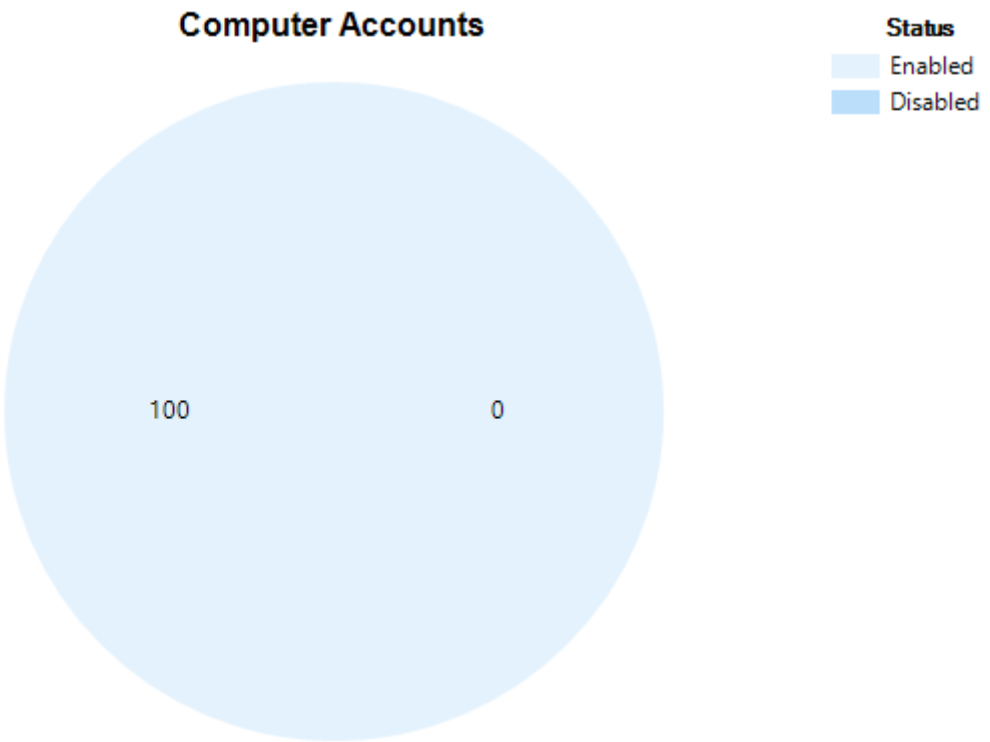
1.2.3.6 Privileged Group Count

Group Name	Count
Account Operators	1
Administrators	0
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 134 - Privileged Group Count - UIA.LOCAL

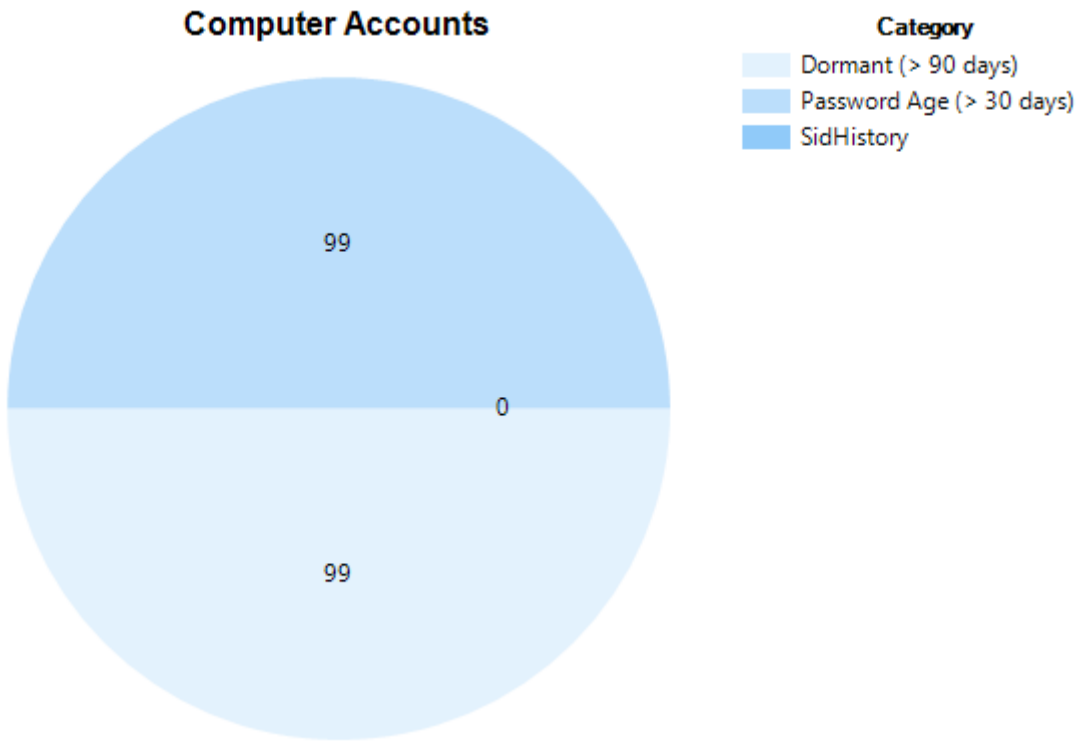
1.2.3.7 Computer Accounts in Active Directory



Status	Count	Percentage
Enabled	100	100%
Disabled	0	0%

Table 135 - Computer Accounts in Active Directory - 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 136 - 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 137 - Operating System Count - UIA.LOCAL

1.2.3.10 Default Domain Password Policy

Password Must Meet Complexity Requirements	Yes
Path	uia.local/
Lockout Duration	00 days 00 hours 30 minutes 00 seconds
Lockout Threshold	0
Lockout Observation Window	00 days 00 hours 30 minutes 00 seconds

Max Password Age	42 days 00 hours 00 minutes 00 seconds
Min Password Age	01 days 00 hours 00 minutes 00 seconds
Min Password Length	7
Enforce Password History	24
Store Password using Reversible Encryption	No

Table 138 - 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	2022:05:13	148
CN=Schema,CN=Configuration,DC=pharmax,DC=local	2022:05:13	148
DC=DomainDnsZones,DC=uia,DC=local	2022:05:13	148
DC=ForestDnsZones,DC=pharmax,DC=local	2022:05:13	148
DC=uia,DC=local	2022:05:13	148

Table 139 - 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 140 - 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.

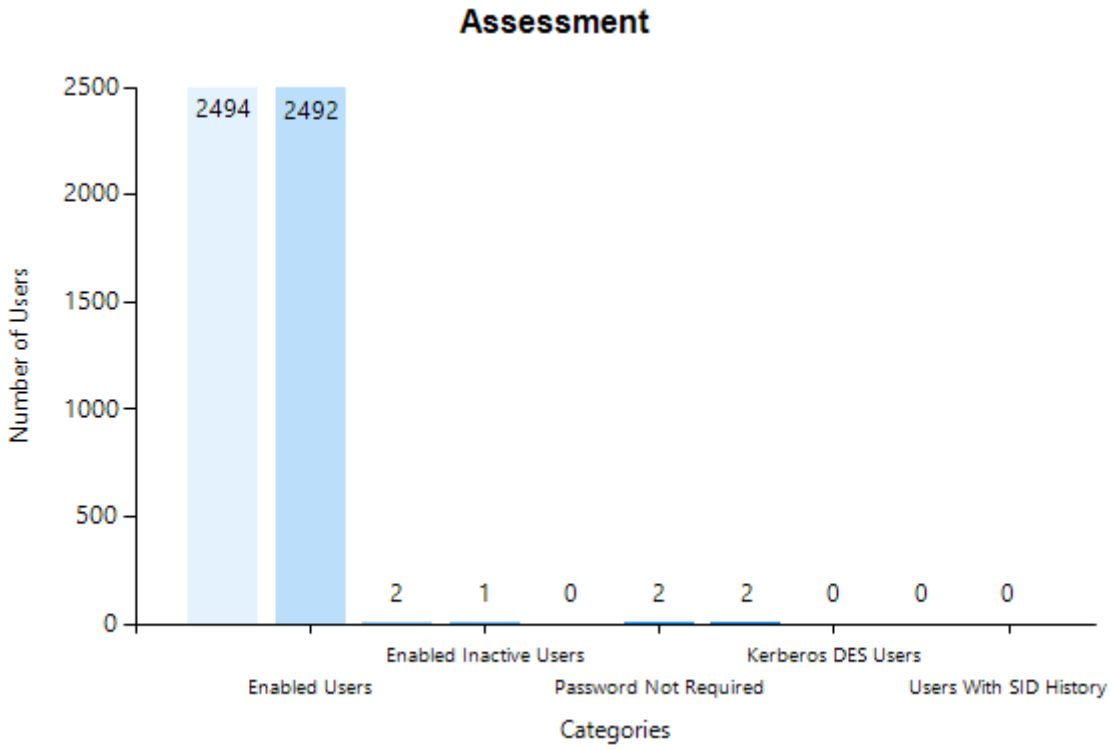
Extension	File Count	Size
.zip	80	4.72 MB

Table 141 - 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 142 - 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	10/3/2022
krbtgt	5/11/2022	5/11/2022	-

Username	Created	Password Last Set	Last Logon Date
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 143 - 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

Username	Enabled	Password Last Set	Last Logon Date	Service Principal Name
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
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 144 - 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 145 - 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	10/03/2022 20:36:37
Distinguished Name	CN=Administrator,CN=Users,DC=uia,DC=local

Table 146 - 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 Controller Summary

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 147 - Domain Controller Summary - 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

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	
Number of CPU Cores	2
Number of Logical Cores	2
Physical Memory (GB)	4.00 GB

Table 148 - 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	80.00 MB	C:\Windows\NTDS	C:\Windows\SYSVOL\sysvol

Table 149 - NTDS Database File Usage - UIA.LOCAL

1.2.3.12.3 Time Source Information

Name	Time Server	Type
DC-UIA-01V	Domain Hierarchy	MANUAL (NTP)

Table 150 - 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 151 - 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 152 - 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 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.
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 153 - 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.

1.2.3.12.7 DC Diagnostic

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

DC-UIA-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	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	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	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	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	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 154 - DCDiag Test Status - DC-UIA-01V

1.2.3.12.8 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 155 - 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.

1.2.3.12.9 Sites Replication Connection

The following section provides detailed information about Site Replication Connection.

DC-UIA-01V

GUID	238a8b15-72f1-4794-ba2e-ca4399875c92
Description	-
Replicate From Directory Server	CAYEY-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
AutoGenerated	Yes
Enabled	Yes
Created	Sat, 08 Oct 2022 17:54:37 GMT

Table 156 - Site Replication - 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
AutoGenerated	Yes
Enabled	Yes
Created	Wed, 11 May 2022 17:57:17 GMT

Table 157 - Site Replication - 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
AutoGenerated	Yes

Enabled	Yes
Created	Wed, 11 May 2022 17:57:17 GMT

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

1.2.3.12.10 Sites Replication Status

Destination DSA	Source DSA	Source DSA Site	Last Success Time	Last Failure Status	Last Failure Time	Number of failures
DC-UIA-01V	ACADE-DC-01V	ACAD	2022-10-04 19:59:03	5	2022-10-08 19:24:48	17
DC-UIA-01V	SERVER-DC-01V	Pharmax-HQ	2022-10-04 19:59:03	5	2022-10-08 19:24:48	17
DC-UIA-01V	ACADE-DC-01V	ACAD	2022-10-04 19:59:03	5	2022-10-08 19:24:48	17
DC-UIA-01V	SERVER-DC-01V	Pharmax-HQ	2022-10-04 19:59:03	5	2022-10-08 19:24:48	17
DC-UIA-01V	ACADE-DC-01V	ACAD	2022-10-04 19:59:03	1256	2022-10-08 19:24:48	17
DC-UIA-01V	SERVER-DC-01V	Pharmax-HQ	2022-10-04 19:59:03	1256	2022-10-08 19:24:48	17
DC-UIA-01V	ACADE-DC-01V	ACAD	2022-10-04 19:59:03	1256	2022-10-08 19:24:48	17
DC-UIA-01V	SERVER-DC-01V	Pharmax-HQ	2022-10-04 19:59:03	1256	2022-10-08 19:24:48	17
DC-UIA-01V	ACADE-DC-01V	ACAD	2022-10-04 19:59:03	1256	2022-10-08 19:24:48	17
DC-UIA-01V	SERVER-DC-01V	Pharmax-HQ	2022-10-04 19:59:03	1256	2022-10-08 19:24:48	17

Table 159 - Site Replication Status - UIA.LOCAL

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

1.2.3.12.11 Group Policy Objects Summary

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

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

Table 160 - GPO - Default Domain Policy

GPO Name	Default Domain Controllers Policy
GPO Status	All Settings Enabled
Created	05/11/2022

Modified	05/11/2022
Description	
Owner	UIA\Domain Admins

Table 161 - GPO - Default Domain Controllers Policy

1.2.3.12.11.1 Central Store Repository

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

Table 162 - GPO Central Store - UIA.LOCAL

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

1.2.3.12.12 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	-

Name	Path	Linked GPO
ESM	uia.local/People/ESM	-
FIN	uia.local/People/FIN	-
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	-
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	-

Name	Path	Linked GPO
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	-
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	-

Name	Path	Linked GPO
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	-
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	-

Name	Path	Linked GPO
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	-
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	-

Name	Path	Linked GPO
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 163 - Organizational Unit - UIA.LOCAL

1.3 Domain Name System Summary

The Domain Name System (DNS) is a hierarchical and decentralized naming system for computers, services, or other resources connected to the Internet or a private network. It associates various information with domain names assigned to each of the participating entities. Most prominently, it translates more readily memorized domain names to the numerical IP addresses needed for locating and identifying computer services and devices with the underlying network protocols.

1.3.1 PHARMAX.LOCAL Root Domain DNS Configuration

The following section provides a configuration summary of the DNS service.

1.3.1.1 Infrastructure Summary

The following section provides a summary of the DNS Infrastructure configuration.

DC Name	Build Number	IPv6	DnsSec	ReadOnly DC	Listening IP
CAYEY-DC-01V	17763	Yes	No	No	10.10.33.1
SERVER-DC-01V	17763	Yes	No	No	192.168.5.1

Table 164 - Infrastructure Summary - PHARMAX.LOCAL

1.3.1.1.1 Domain Controller DNS IP Configuration

DC Name	Interface	DNS IP 1	DNS IP 2	DNS IP 3	DNS IP 4
CAYEY-DC-01V	Ethernet0	10.10.33.1	192.168.5.1	127.0.0.1	-
SERVER-DC-01V	Ethernet0	192.168.5.1	127.0.0.1	8.8.8.8	-

Table 165 - DNS IP Configuration - PHARMAX.LOCAL

1.3.1.1.2 Application Directory Partition

The following section provides Directory Partition information.

SERVER-DC-01V

Name	State	Flags	Zone Count
DomainDnsZones.acad.pharmax.local	-	Not-Enlisted	0
DomainDnsZones.pharmax.local	DNS_DP_OKAY	Enlisted Auto Domain	8
DomainDnsZones.uia.local	-	Not-Enlisted	0
ForestDnsZones.pharmax.local	DNS_DP_OKAY	Enlisted Auto Forest	4

Table 166 - Directory Partitions - SERVER-DC-01V

CAYEY-DC-01V

Name	State	Flags	Zone Count
DomainDnsZones.acad.pharmax.local	-	Not-Enlisted	0
DomainDnsZones.pharmax.local	DNS_DP_OKAY	Enlisted Auto Domain	8
DomainDnsZones.uia.local	-	Not-Enlisted	0
ForestDnsZones.pharmax.local	DNS_DP_OKAY	Enlisted Auto Forest	3

Table 167 - Directory Partitions - CAYEY-DC-01V

1.3.1.1.3 Response Rate Limiting (RRL)

DC Name	Status	Responses Per Sec	Errors Per Sec	Window In Sec	Leak Rate	Truncate Rate
CAYEY-DC-01V	Disable	5	5	5	3	2
SERVER-DC-01V	Disable	5	5	5	3	2

Table 168 - Response Rate Limiting - PHARMAX.LOCAL

1.3.1.1.4 Scavenging Options

DC Name	NoRefresh Interval	Refresh Interval	Scavenging Interval	Last Scavenge Time	Scavenging State
CAYEY-DC-01V	7.00:00:00	7.00:00:00	00:00:00	-	Disabled
SERVER-DC-01V	7.00:00:00	7.00:00:00	7.00:00:00	-	Enabled

Table 169 - Scavenging - PHARMAX.LOCAL

Health Check:
Best Practices: Microsoft recommends to enable aging/scavenging on all DNS servers. However, with AD-integrated zones ensure to enable DNS scavenging on one DC at main site. The results will be replicated to other DCs.

1.3.1.1.5 Forwarder Options

DC Name	IP Address	Timeout	Use Root Hint	Use Recursion
CAYEY-DC-01V	192.168.5.1	3/s	Yes	Yes
SERVER-DC-01V	8.8.8.8 10.0.0.138	3/s	Yes	Yes

Table 170 - Forwarders - PHARMAX.LOCAL

1.3.1.1.6 Root Hints

The following section provides Root Hints information.

SERVER-DC-01V

Name	IP Address
a.root-servers.net.	System.Object[]
b.root-servers.net.	199.9.14.201
c.root-servers.net.	192.33.4.12
d.root-servers.net.	199.7.91.13
e.root-servers.net.	192.203.230.10
f.root-servers.net.	192.5.5.241
g.root-servers.net.	192.112.36.4
h.root-servers.net.	198.97.190.53
i.root-servers.net.	192.36.148.17
j.root-servers.net.	192.58.128.30
k.root-servers.net.	193.0.14.129
l.root-servers.net.	199.7.83.42
m.root-servers.net.	202.12.27.33

Table 171 - Root Hints - PHARMAX.LOCAL

CAYEY-DC-01V

Name	IP Address
a.root-servers.net.	System.Object[]
b.root-servers.net.	199.9.14.201
c.root-servers.net.	192.33.4.12
d.root-servers.net.	199.7.91.13
e.root-servers.net.	192.203.230.10
f.root-servers.net.	192.5.5.241
g.root-servers.net.	192.112.36.4
h.root-servers.net.	198.97.190.53
i.root-servers.net.	192.36.148.17
j.root-servers.net.	192.58.128.30
k.root-servers.net.	193.0.14.129
l.root-servers.net.	199.7.83.42
m.root-servers.net.	202.12.27.33

Table 172 - Root Hints - PHARMAX.LOCAL

1.3.1.1.7 Zone Scope Recursion

DC Name	Zone Name	Forwarder	Use Recursion
CAYEY-DC-01V	Root	192.168.5.1	Yes
SERVER-DC-01V	Root	8.8.8.8 10.0.0.138	Yes

Table 173 - Zone Scope Recursion - PHARMAX.LOCAL

1.3.1.2 SERVER-DC-01V DNS Zones

Zone Name	Zone Type	Replication Scope	Dynamic Update	DS Integrated	Read Only	Signed
_msdcs.pharmax.local	Primary	Forest	Secure	Yes	No	No
pharmax.local	Primary	Domain	Secure	Yes	No	No
TrustAnchors	Primary	Forest	None	Yes	No	No
uia.local	Stub	Domain	-	Yes	No	-
zenprsolutions.local	Stub	Domain	-	Yes	No	-

Table 174 - Zones - PHARMAX.LOCAL

1.3.1.2.1 Zone Delegation

Zone Name	Child Zone	Name Server	IP Address
pharmax.local	acad.pharmax.local.	ACADE-DC-01V.acad.pharmax.local.	172.23.4.1
pharmax.local	_msdcs.pharmax.local.	server-dc-01v.pharmax.local.	192.168.5.1

Table 175 - Zone Delegations - PHARMAX.LOCAL

1.3.1.2.2 Zone Transfers

Zone Name	Secondary Servers	Notify Servers	Secure Secondaries
pharmax.local	172.23.4.1	-	Send zone transfers only to name servers that are authoritative for the zone.

Table 176 - Zone Transfers - pharmax.local

1.3.1.2.3 Reverse Lookup Zone

Zone Name	Zone Type	Replication Scope	Dynamic Update	DS Integrated	Read Only	Signed
0.in-addr.arpa	Primary	None	None	No	No	No
10.10.in-addr.arpa	Primary	Domain	Secure	Yes	No	No
127.in-addr.arpa	Primary	None	None	No	No	No
168.192.in-addr.arpa	Primary	Domain	Secure	Yes	No	No
23.172.in-addr.arpa	Primary	Domain	Secure	Yes	No	No
255.in-addr.arpa	Primary	None	None	No	No	No
70.23.172.in-addr.arpa	Primary	Forest	Secure	Yes	No	No

Table 177 - Zones - PHARMAX.LOCAL

1.3.1.2.4 Conditional Forwarder

Zone Name	Zone Type	Replication Scope	Master Servers	DS Integrated
b12.local	Forwarder	Forest	10.10.30.1	Yes
zenprsolutions.gov	Forwarder	Domain	8.8.8.8	Yes

Table 178 - Conditional Forwarders - PHARMAX.LOCAL

1.3.1.2.5 Zone Scope Aging

Zone Name	Aging Enabled	Refresh Interval	NoRefresh Interval	Available For Scavenge
_msdcs.pharmax.local	Yes	7.00:00:00	7.00:00:00	Sat, 15 Oct 2022 21:00:00 GMT
pharmax.local	Yes	7.00:00:00	7.00:00:00	Sat, 15 Oct 2022 21:00:00 GMT
TrustAnchors	Yes	7.00:00:00	7.00:00:00	Sat, 15 Oct 2022 21:00:00 GMT

Table 179 - Zone Aging Properties - PHARMAX.LOCAL

1.3.1.3 CAYEY-DC-01V DNS Zones

Zone Name	Zone Type	Replication Scope	Dynamic Update	DS Integrated	Read Only	Signed
_msdcs.pharmax.local	Primary	Forest	Secure	Yes	No	No
pharmax.local	Primary	Domain	Secure	Yes	No	No
TrustAnchors	Primary	Forest	None	Yes	No	No
uia.local	Stub	Domain	-	Yes	No	-
zenpr.local	Secondary	-	-	No	No	-
zenprsolutions.local	Stub	Domain	-	Yes	No	-

Table 180 - Zones - PHARMAX.LOCAL

1.3.1.3.1 Zone Delegation

Zone Name	Child Zone	Name Server	IP Address
pharmax.local	acad.pharmax.local.	ACADE-DC-01V.acad.pharmax.local.	172.23.4.1
pharmax.local	_msdcs.pharmax.local.	server-dc-01v.pharmax.local.	192.168.5.1

Table 181 - Zone Delegations - PHARMAX.LOCAL

1.3.1.3.2 Reverse Lookup Zone

Zone Name	Zone Type	Replication Scope	Dynamic Update	DS Integrated	Read Only	Signed
0.in-addr.arpa	Primary	None	None	No	No	No
10.10.in-addr.arpa	Primary	Domain	Secure	Yes	No	No
127.in-addr.arpa	Primary	None	None	No	No	No
168.192.in-addr.arpa	Primary	Domain	Secure	Yes	No	No

Zone Name	Zone Type	Replication Scope	Dynamic Update	DS Integrated	Read Only	Signed
23.172.in-addr.arpa	Primary	Domain	Secure	Yes	No	No
255.in-addr.arpa	Primary	None	None	No	No	No
70.23.172.in-addr.arpa	Primary	Forest	Secure	Yes	No	No

Table 182 - Zones - PHARMAX.LOCAL

1.3.1.3.3 Conditional Forwarder

Zone Name	Zone Type	Replication Scope	Master Servers	DS Integrated
zenprsolutions.edu	Forwarder	None	1.1.1.1	No
zenprsolutions.gov	Forwarder	Domain	8.8.8.8	Yes

Table 183 - Conditional Forwarders - PHARMAX.LOCAL

1.3.1.3.4 Zone Scope Aging

Zone Name	Aging Enabled	Refresh Interval	NoRefresh Interval	Available For Scavenge
_msdcs.pharmax.local	Yes	7.00:00:00	7.00:00:00	Sat, 29 Jan 2022 18:00:00 GMT
pharmax.local	Yes	7.00:00:00	7.00:00:00	Fri, 24 Sep 2021 23:00:00 GMT
TrustAnchors	Yes	7.00:00:00	7.00:00:00	Thu, 07 Jan 2021 16:00:00 GMT

Table 184 - Zone Aging Properties - PHARMAX.LOCAL

1.3.2 ACAD.PHARMAX.LOCAL Child Domain DNS Configuration

The following section provides a configuration summary of the DNS service.

1.3.2.1 Infrastructure Summary

The following section provides a summary of the DNS Infrastructure configuration.

DC Name	Build Number	IPv6	DnsSec	ReadOnly DC	Listening IP
ACADE-DC-01V	17763	Yes	No	No	172.23.4.1

Table 185 - Infrastructure Summary - ACAD.PHARMAX.LOCAL

1.3.2.1.1 Domain Controller DNS IP Configuration

DC Name	Interface	DNS IP 1	DNS IP 2	DNS IP 3	DNS IP 4
ACADE-DC-01V	Ethernet0	172.23.4.1	192.168.5.1	10.10.33.1	127.0.0.1

Table 186 - DNS IP Configuration - ACAD.PHARMAX.LOCAL

1.3.2.1.2 Application Directory Partition

The following section provides Directory Partition information.

ACADE-DC-01V

Name	State	Flags	Zone Count
DomainDnsZones.acad.pharmax.local	DNS_DP_OKAY	Enlisted Auto Domain	3
DomainDnsZones.pharmax.local	-	Not-Enlisted	0
DomainDnsZones.uia.local	-	Not-Enlisted	0
ForestDnsZones.pharmax.local	DNS_DP_OKAY	Enlisted Auto Forest	3

Table 187 - Directory Partitions - ACADE-DC-01V

1.3.2.1.3 Response Rate Limiting (RRL)

DC Name	Status	Responses Per Sec	Errors Per Sec	Window In Sec	Leak Rate	Truncate Rate
ACADE-DC-01V	Disable	5	5	5	3	2

Table 188 - Response Rate Limiting - ACAD.PHARMAX.LOCAL

1.3.2.1.4 Scavenging Options

DC Name	NoRefresh Interval	Refresh Interval	Scavenging Interval	Last Scavenge Time	Scavenging State
ACADE-DC-01V	7.00:00:00	7.00:00:00	00:00:00	-	Disabled

Table 189 - Scavenging - ACAD.PHARMAX.LOCAL

Health Check:
Best Practices: Microsoft recommends to enable aging/scavenging on all DNS servers. However, with AD-integrated zones ensure to enable DNS scavenging on one DC at main site. The results will be replicated to other DCs.

1.3.2.1.5 Forwarder Options

DC Name	IP Address	Timeout	Use Root Hint	Use Recursion
ACADE-DC-01V	192.168.5.1	3/s	Yes	Yes

Table 190 - Forwarders - ACAD.PHARMAX.LOCAL

1.3.2.1.6 Root Hints

The following section provides Root Hints information.

ACADE-DC-01V

Name	IP Address
a.root-servers.net.	System.Object[]
b.root-servers.net.	199.9.14.201
c.root-servers.net.	2001:500:2::c
d.root-servers.net.	2001:500:2d::d
e.root-servers.net.	2001:500:a8::e
f.root-servers.net.	2001:500:2f::f
g.root-servers.net.	2001:500:12::d0d
h.root-servers.net.	2001:500:1::53
i.root-servers.net.	2001:7fe::53
j.root-servers.net.	2001:503:c27::2:30
k.root-servers.net.	2001:7fd::1
l.root-servers.net.	2001:500:9f::42
m.root-servers.net.	2001:dc3::35

Table 191 - Root Hints - ACAD.PHARMAX.LOCAL

1.3.2.1.7 Zone Scope Recursion

DC Name	Zone Name	Forwarder	Use Recursion
ACADE-DC-01V	Root	192.168.5.1	Yes

Table 192 - Zone Scope Recursion - ACAD.PHARMAX.LOCAL

1.3.2.2 ACADE-DC-01V DNS Zones

Zone Name	Zone Type	Replication Scope	Dynamic Update	DS Integrated	Read Only	Signed
_msdcs.pharmax.local	Primary	Forest	Secure	Yes	No	No
acad.pharmax.local	Primary	Domain	Secure	Yes	No	No
TrustAnchors	Primary	Forest	None	Yes	No	No
zenpr.local	Secondary	-	-	No	No	-

Table 193 - Zones - ACAD.PHARMAX.LOCAL

1.3.2.2.1 Zone Transfers

Zone Name	Secondary Servers	Notify Servers	Secure Secondaries
acad.pharmax.local	172.23.4.2, 10.10.40.2	172.23.4.2	Send zone transfers only to servers you specify in Secondary Servers.
zenpr.local	172.23.4.2	172.24.4.2	Send zone transfers to all secondary servers that request them.

Table 194 - Zone Transfers - zenpr.local

Health Check:
Best Practices: Configure all DNS zones only to allow zone transfers from Trusted IP addresses.

1.3.2.2.2 Reverse Lookup Zone

Zone Name	Zone Type	Replication Scope	Dynamic Update	DS Integrated	Read Only	Signed
0.23.172.in-addr.arpa	Primary	Domain	Secure	Yes	No	No
0.in-addr.arpa	Primary	None	None	No	No	No
127.in-addr.arpa	Primary	None	None	No	No	No
255.in-addr.arpa	Primary	None	None	No	No	No
70.23.172.in-addr.arpa	Primary	Forest	Secure	Yes	No	No

Table 195 - Zones - ACAD.PHARMAX.LOCAL

1.3.2.2.3 Conditional Forwarder

Zone Name	Zone Type	Replication Scope	Master Servers	DS Integrated
zenprsolutions.local	Forwarder	None	8.8.8.8	No

Table 196 - Conditional Forwarders - ACAD.PHARMAX.LOCAL

1.3.2.2.4 Zone Scope Aging

Zone Name	Aging Enabled	Refresh Interval	NoRefresh Interval	Available For Scavenge
_msdcs.pharmax.local	Yes	7.00:00:00	7.00:00:00	Sat, 29 Jan 2022 18:00:00 GMT
acad.pharmax.local	No	7.00:00:00	7.00:00:00	-
TrustAnchors	Yes	7.00:00:00	7.00:00:00	Thu, 07 Jan 2021 16:00:00 GMT

Table 197 - Zone Aging Properties - ACAD.PHARMAX.LOCAL

Health Check:
Best Practices: Microsoft recommends to enable aging/scavenging on all DNS servers. However, with AD-integrated zones ensure to enable DNS scavenging on one DC at main site. The results will be replicated to other DCs.

1.3.3 UIA.LOCAL Child Domain DNS Configuration

The following section provides a configuration summary of the DNS service.

1.3.3.1 Infrastructure Summary

The following section provides a summary of the DNS Infrastructure configuration.

DC Name	Build Number	IPv6	DnsSec	ReadOnly DC	Listening IP
DC-UIA-01V	20348	Yes	Yes	No	fe80::fc0b:52e5:4931:6229 172.23.7.1

Table 198 - Infrastructure Summary - UIA.LOCAL

1.3.3.1.1 Domain Controller DNS IP Configuration

DC Name	Interface	DNS IP 1	DNS IP 2	DNS IP 3	DNS IP 4
DC-UIA-01V	Ethernet0	127.0.0.1	192.168.5.1	-	-

Table 199 - DNS IP Configuration - UIA.LOCAL

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

1.3.3.1.2 Application Directory Partition

The following section provides Directory Partition information.

DC-UIA-01V

Name	State	Flags	Zone Count
DomainDnsZones.acad.pharmax.local	-	Not-Enlisted	0
DomainDnsZones.pharmax.local	-	Not-Enlisted	0
DomainDnsZones.uia.local	DNS_DP_OKAY	Enlisted Auto Domain	2
ForestDnsZones.pharmax.local	DNS_DP_OKAY	Enlisted Auto Forest	3

Table 200 - Directory Partitions - DC-UIA-01V

1.3.3.1.3 Response Rate Limiting (RRL)

DC Name	Status	Responses Per Sec	Errors Per Sec	Window In Sec	Leak Rate	Truncate Rate
DC-UIA-01V	Disable	5	5	5	3	2

Table 201 - Response Rate Limiting - UIA.LOCAL

1.3.3.1.4 Scavenging Options

DC Name	NoRefresh Interval	Refresh Interval	Scavenging Interval	Last Scavenge Time	Scavenging State
DC-UIA-01V	7.00:00:00	7.00:00:00	00:00:00	-	Disabled

Table 202 - Scavenging - UIA.LOCAL

Health Check:
Best Practices: Microsoft recommends to enable aging/scavenging on all DNS servers. However, with AD-integrated zones ensure to enable DNS scavenging on one DC at main site. The results will be replicated to other DCs.

1.3.3.1.5 Forwarder Options

DC Name	IP Address	Timeout	Use Root Hint	Use Recursion
DC-UIA-01V	192.168.5.1	3/s	Yes	Yes

Table 203 - Forwarders - UIA.LOCAL

1.3.3.1.6 Root Hints

The following section provides Root Hints information.

DC-UIA-01V

Name	IP Address
a.root-servers.net.	2001:503:ba3e::2:30
b.root-servers.net.	2001:500:200::b
c.root-servers.net.	2001:500:2::c
d.root-servers.net.	2001:500:2d::d
e.root-servers.net.	2001:500:a8::e
f.root-servers.net.	2001:500:2f::f
g.root-servers.net.	2001:500:12::d0d
h.root-servers.net.	2001:500:1::53
i.root-servers.net.	2001:7fe::53
j.root-servers.net.	2001:503:c27::2:30
k.root-servers.net.	2001:7fd::1
l.root-servers.net.	2001:500:9f::42
m.root-servers.net.	2001:dc3::35

Table 204 - Root Hints - UIA.LOCAL

1.3.3.1.7 Zone Scope Recursion

DC Name	Zone Name	Forwarder	Use Recursion
DC-UIA-01V	Root	192.168.5.1	Yes

Table 205 - Zone Scope Recursion - UIA.LOCAL

1.3.3.2 DC-UIA-01V DNS Zones

Zone Name	Zone Type	Replication Scope	Dynamic Update	DS Integrated	Read Only	Signed
_msdcs.pharmax.local	Primary	Forest	Secure	Yes	No	No
TrustAnchors	Primary	Forest	None	Yes	No	No
uia.local	Primary	Domain	Secure	Yes	No	No

Table 206 - Zones - UIA.LOCAL

1.3.3.2.1 Reverse Lookup Zone

Zone Name	Zone Type	Replication Scope	Dynamic Update	DS Integrated	Read Only	Signed
0.in-addr.arpa	Primary	None	None	No	No	No
127.in-addr.arpa	Primary	None	None	No	No	No
255.in-addr.arpa	Primary	None	None	No	No	No
70.23.172.in-addr.arpa	Primary	Forest	Secure	Yes	No	No

Table 207 - Zones - UIA.LOCAL

1.3.3.2.2 Zone Scope Aging

Zone Name	Aging Enabled	Refresh Interval	NoRefresh Interval	Available For Scavenge
_msdcs.pharmax.local	Yes	7.00:00:00	7.00:00:00	Sat, 29 Jan 2022 18:00:00 GMT
TrustAnchors	Yes	7.00:00:00	7.00:00:00	Thu, 07 Jan 2021 16:00:00 GMT
uia.local	No	7.00:00:00	7.00:00:00	-

Table 208 - Zone Aging Properties - UIA.LOCAL

Health Check:
Best Practices: Microsoft recommends to enable aging/scavenging on all DNS servers. However, with AD-integrated zones ensure to enable DNS scavenging on one DC at main site. The results will be replicated to other DCs.

1.4 Dynamic Host Configuration Protocol Summary

The Dynamic Host Configuration Protocol (DHCP) is a network management protocol used on Internet Protocol (IP) networks for automatically assigning IP addresses and other communication parameters to devices connected to the network using a client/server architecture.

1.4.1 PHARMAX.LOCAL Root Domain DHCP Configuration

The following section provides a summary of the Dynamic Host Configuration Protocol.

1.4.1.1 DHCP Servers In Active Directory

The following section provides a summary of the DHCP servers information on PHARMAX.LOCAL.

DC Name	IP Address	Domain Name	Domain Joined	Authorized	Conflict Detection Attempts
cayey-dc-01v	10.10.33.1	pharmax.local	Yes	Yes	0
server-dc-01v	192.168.5.1	pharmax.local	Yes	Yes	1

Table 209 - DHCP Servers In Active Directory - PHARMAX.LOCAL

1.4.1.1.1 Service Database

DC Name	File Path	Backup Path	Backup Interval	Logging Enabled
cayey-dc-01v	C:\Windows\system32\dhcp\dhcp.mdb	C:\Windows\system32\dhcp\backup	60 min	Yes
server-dc-01v	C:\Windows\system32\dhcp\dhcp.mdb	C:\Windows\system32\dhcp\backup	60 min	Yes

Table 210 - DHCP Servers Database - PHARMAX.LOCAL

1.4.1.1.2 Dynamic DNS credentials

DC Name	User Name	Domain Name
cayey-dc-01v	-	-
server-dc-01v	administrator	PHARMAX.LOCAL

Table 211 - DHCP Servers Dynamic DNS Credentials - PHARMAX.LOCAL

Health Check:
Best Practice: Credentials for DNS update should be configured if secure dynamic DNS update is enabled and the domain controller is on the same host as the DHCP server.

1.4.1.2 IPv4 Scope Configuration

The following section provides a IPv4 configuration summary of the Dynamic Host Configuration Protocol.

1.4.1.2.1 IPv4 Service Statistics

DC Name	Total Scopes	Total Addresses	Addresses In Use	Addresses Available	Percentage In Use	Percentage Available
cayey-dc-01v	0	0	0	0	0	0
server-dc-01v	10	2118	221	1897	10	90

Table 212 - DHCP Server IPv4 Statistics - PHARMAX.LOCAL

1.4.1.2.2 CAYEY-DC-01V IPv4 Scope Server Options

Name	Option Id	Value	Policy Name
Time Offset	2	0	-
Time Server	4	10.10.33.1	-
Name Servers	5	10.10.33.1	-
DNS Servers	6	10.10.33.1 192.168.5.1	-

Table 213 - IPv4 Scopes Server Options - CAYEY-DC-01V

1.4.1.2.2.1 Scope DNS Setting

The following section provides a summary of the DHCP servers IPv4 Scope DNS Setting information.

Dynamic Updates	OnClientRequest
Dns Suffix	-
Name Protection	No
Update Dns RR For Older Clients	No
Disable Dns Ptr RR Update	No
Delete Dns RR On Lease Expiry	Yes

Table 214 - IPv4 Scopes DNS Setting - cayey-dc-01v

Health Check:
Best Practice: 'Always dynamically update dns records' should be configured if secure dynamic DNS update is enabled and the domain controller is on the same host as the DHCP server.

1.4.1.2.3 SERVER-DC-01V IPv4 Scopes

The following section provides detailed information of the IPv4 Scope configuration.

Scope Id	Scope Name	Scope Range	Lease Duration	State
10.10.32.0/24	ESXi-vMotion-DR	10.10.32.10 - 10.10.32.250	8.00:00:00	Active
10.10.33.0/24	ESX-VM-NETWORK-DR	10.10.33.40 - 10.10.33.253	100.00:00:00	Active
10.10.34.0/24	ESXi-ISCSI-BLOCK-A-DR	10.10.34.10 - 10.10.34.253	8.00:00:00	Active
10.10.35.0/24	ESXi-ISCSI-BLOCK-B-DR	10.10.35.10 - 10.10.35.253	8.00:00:00	Active
192.168.10.0/24	ESX-vSAN-NET	192.168.10.10 - 192.168.10.253	8.00:00:00	Active
192.168.12.0/24	ESXi-ISCSI-BLOCK-B	192.168.12.10 - 192.168.12.240	8.00:00:00	Active
192.168.2.0/24	ESXi-vMotion	192.168.2.10 - 192.168.2.253	8.00:00:00	Active
192.168.4.0/24	ESXi-NFS-File	192.168.4.10 - 192.168.4.20	8.00:00:00	Active
192.168.6.0/24	ESXi-ISCSI-BLOCK-A	192.168.6.10 - 192.168.6.240	8.00:00:00	Active
192.168.7.0/24	ESX-VM-NETWORK	192.168.7.40 - 192.168.7.253	Unlimited	Active

Table 215 - IPv4 Scopes - SERVER-DC-01V

1.4.1.2.3.1 IPv4 Scope Statistics

Scope Id	Free IP	In Use IP	Percentage In Use	Reserved IP
10.10.32.0	239	2	1	0
10.10.33.0	210	4	2	3
10.10.34.0	242	2	1	0
10.10.35.0	242	2	1	0

Scope Id	Free IP	In Use IP	Percentage In Use	Reserved IP
192.168.10.0	244	0	0	0
192.168.12.0	228	3	1	3
192.168.2.0	244	0	0	0
192.168.4.0	11	0	0	0
192.168.6.0	229	2	1	2
192.168.7.0	8	206	96	17

Table 216 - IPv4 Scope Statistics - SERVER-DC-01V

1.4.1.2.3.2 IPv4 Network Interface Binding

Interface Alias	IP Address	Subnet Mask	State
Ethernet0	192.168.5.1	255.255.255.0	Enabled

Table 217 - IPv4 Network Interface binding - SERVER-DC-01V

1.4.1.2.4 SERVER-DC-01V IPv4 Scope Server Options

Name	Option Id	Value	Policy Name
Time Server	4	192.168.5.1	-
Name Servers	5	192.168.5.1	-
DNS Servers	6	192.168.5.1	-
NTP Servers	42	192.168.5.1	-
Simple Mail Transport Protocol (SMTP) Servers	69	192.168.7.21	-
Post Office Protocol (POP3) Servers	70	192.168.7.21	-
	81	55	-

Table 218 - IPv4 Scopes Server Options - SERVER-DC-01V

1.4.1.2.4.1 Scope DNS Setting

The following section provides a summary of the DHCP servers IPv4 Scope DNS Setting information.

Dynamic Updates	Always
Dns Suffix	-
Name Protection	Yes
Update Dns RR For Older Clients	Yes
Disable Dns Ptr RR Update	No
Delete Dns RR On Lease Expiry	Yes

Table 219 - IPv4 Scopes DNS Setting - server-dc-01v

1.4.1.2.5 Scope Options

The following section provides a summary of the DHCP servers IPv4 Scope Server Options information.

10.10.32.0

Name	Option Id	Value	Policy Name
Router	3	10.10.32.254	-
DNS Domain Name	15	pharmax.local	-
Lease	51	691200	-

Table 220 - IPv4 Scopes Options - 10.10.32.0

10.10.33.0

Name	Option Id	Value	Policy Name
Router	3	10.10.33.254	-
Lease	51	8640000	-
Boot Server Host Name	66	192.168.5.2	-
Bootfile Name	67	snponly64.efi.vmw-hardwired	-
	81	23	-

Table 221 - IPv4 Scopes Options - 10.10.33.0

10.10.34.0

Name	Option Id	Value	Policy Name
DNS Servers	6	192.168.5.1 192.168.5.1	-
DNS Domain Name	15	pharmax.local	-
Lease	51	691200	-

Table 222 - IPv4 Scopes Options - 10.10.34.0

10.10.35.0

Name	Option Id	Value	Policy Name
DNS Servers	6	192.168.5.1 192.168.5.1	-
DNS Domain Name	15	pharmax.local	-
Lease	51	691200	-

Table 223 - IPv4 Scopes Options - 10.10.35.0

192.168.2.0

Name	Option Id	Value	Policy Name
Router	3	192.168.2.254	-
DNS Domain Name	15	pharmax.local	-
Lease	51	691200	-

Table 224 - IPv4 Scopes Options - 192.168.2.0

192.168.4.0

Name	Option Id	Value	Policy Name
Router	3	192.168.4.254	-

Name	Option Id	Value	Policy Name
DNS Domain Name	15	pharmax.local	-
Lease	51	691200	-

Table 225 - IPv4 Scopes Options - 192.168.4.0

192.168.6.0

Name	Option Id	Value	Policy Name
DNS Domain Name	15	pharmax.local	-
Lease	51	691200	-

Table 226 - IPv4 Scopes Options - 192.168.6.0

192.168.7.0

Name	Option Id	Value	Policy Name
Router	3	192.168.7.254	-
DNS Domain Name	15	pharmax.local	-
Lease	51	4294967295	-
Boot Server Host Name	66	192.168.5.2	-
Bootfile Name	67	snponly64.efi.vmw-hardwired	-
	81	23	-

Table 227 - IPv4 Scopes Options - 192.168.7.0

192.168.10.0

Name	Option Id	Value	Policy Name
Router	3	192.168.10.254	-
DNS Servers	6	192.168.5.1 192.168.5.1	-
DNS Domain Name	15	pharmax.local	-
Lease	51	691200	-

Table 228 - IPv4 Scopes Options - 192.168.10.0

192.168.12.0

Name	Option Id	Value	Policy Name
DNS Domain Name	15	pharmax.local	-
Lease	51	691200	-

Table 229 - IPv4 Scopes Options - 192.168.12.0

1.4.1.3 IPv6 Scope Configuration

The following section provides a IPv6 configuration summary of the Dynamic Host Configuration Protocol.

1.4.1.3.1 IPv6 Service Statistics

DC Name	Total Scopes	Total Addresses	Addresses In Use	Addresses Available	Percentage In Use	Percentage Available
cayey-dc-01v	0	0	0	0	0	0
server-dc-01v	0	0	0	0	0	0

Table 230 - DHCP Server IPv6 Statistics - PHARMAX.LOCAL

1.4.2 ACAD.PHARMAX.LOCAL Child Domain DHCP Configuration

The following section provides a summary of the Dynamic Host Configuration Protocol.

1.4.2.1 DHCP Servers In Active Directory

The following section provides a summary of the DHCP servers information on ACAD.PHARMAX.LOCAL.

DC Name	IP Address	Domain Name	Domain Joined	Authorized	Conflict Detection Attempts
acade-dc-01v	172.23.4.1	acad.pharmax.local	Yes	Yes	0

Table 231 - DHCP Servers In Active Directory - ACAD.PHARMAX.LOCAL

1.4.2.1.1 Service Database

DC Name	File Path	Backup Path	Backup Interval	Logging Enabled
acade-dc-01v	C:\Windows\system32\dhcp\dhcp.mdb	C:\Windows\system32\dhcp\backup	60 min	Yes

Table 232 - DHCP Servers Database - ACAD.PHARMAX.LOCAL

1.4.2.1.2 Dynamic DNS credentials

DC Name	User Name	Domain Name
acade-dc-01v	-	-

Table 233 - DHCP Servers Dynamic DNS Credentials - ACAD.PHARMAX.LOCAL

Health Check:
Best Practice: Credentials for DNS update should be configured if secure dynamic DNS update is enabled and the domain controller is on the same host as the DHCP server.

1.4.2.2 IPv4 Scope Configuration

The following section provides a IPv4 configuration summary of the Dynamic Host Configuration Protocol.

1.4.2.2.1 IPv4 Service Statistics

DC Name	Total Scopes	Total Addresses	Addresses In Use	Addresses Available	Percentage In Use	Percentage Available
acade-dc-01v	1	233	0	233	0	100

Table 234 - DHCP Server IPv4 Statistics - ACAD.PHARMAX.LOCAL

1.4.2.2.2 ACADE-DC-01V IPv4 Scopes

The following section provides detailed information of the IPv4 Scope configuration.

Scope Id	Scope Name	Scope Range	Lease Duration	State
172.23.5.0/24	Dept-B Clients	172.23.5.10 - 172.23.5.253	1.00:00:00	Active

Table 235 - IPv4 Scopes - ACADE-DC-01V

1.4.2.2.2.1 IPv4 Scope Statistics

Scope Id	Free IP	In Use IP	Percentage In Use	Reserved IP
172.23.5.0	233	0	0	0

Table 236 - IPv4 Scope Statistics - ACADE-DC-01V

1.4.2.2.2.2 IPv4 Network Interface Binding

Interface Alias	IP Address	Subnet Mask	State
Ethernet0	172.23.4.1	255.255.255.0	Enabled

Table 237 - IPv4 Network Interface binding - ACADE-DC-01V

1.4.2.2.3 ACADE-DC-01V IPv4 Scope Server Options

Name	Option Id	Value	Policy Name
DNS Servers	6	172.23.4.1 192.168.5.1 10.10.33.1	-
DNS Domain Name	15	acad.pharmax.local	-

Table 238 - IPv4 Scopes Server Options - ACADE-DC-01V

1.4.2.2.3.1 Scope DNS Setting

The following section provides a summary of the DHCP servers IPv4 Scope DNS Setting information.

Dynamic Updates	OnClientRequest
Dns Suffix	-
Name Protection	No

Update Dns RR For Older Clients	No
Disable Dns Ptr RR Update	No
Delete Dns RR On Lease Expiry	Yes

Table 239 - IPv4 Scopes DNS Setting - acade-dc-01v

Health Check:
Best Practice: 'Always dynamically update dns records' should be configured if secure dynamic DNS update is enabled and the domain controller is on the same host as the DHCP server.

1.4.2.2.4 Scope Options

The following section provides a summary of the DHCP servers IPv4 Scope Server Options information.

172.23.5.0

Name	Option Id	Value	Policy Name
Router	3	172.23.5.254	-
Lease	51	86400	-

Table 240 - IPv4 Scopes Options - 172.23.5.0

1.4.2.3 IPv6 Scope Configuration

The following section provides a IPv6 configuration summary of the Dynamic Host Configuration Protocol.

1.4.2.3.1 IPv6 Service Statistics

DC Name	Total Scopes	Total Addresses	Addresses In Use	Addresses Available	Percentage In Use	Percentage Available
acade-dc-01v	1	18446744073709551614	0	18446744073709551614	0	100

Table 241 - DHCP Server IPv6 Statistics - ACAD.PHARMAX.LOCAL

1.4.2.3.2 ACADE-DC-01V IPv6 Scopes

The following section provides a summary of the DHCP servers IPv6 Scope Configuration.

Scope Id	Scope Name	Lease Duration	State
fd99:9971::/64	Dept-C Clients	8.00:00:00	Active

Table 242 - IPv6 Scopes - ACADE-DC-01V

1.4.2.3.2.1 IPv6 Scope Statistics

Scope Id	Free IP	In Use IP	Percentage In Use	Reserved IP
fd99:9971::	18446744073709551614	0	0	0

Table 243 - IPv6 Scope Statistics - ACADE-DC-01V

1.4.2.3.3 ACADE-DC-01V IPv6 Scope Server Options

The following section provides a summary of the DHCP servers IPv6 Scope Server Options information.

Name	Option Id	Type	Value
Domain Search List	24	String	fd99:9971::1

Table 244 - IPv6 Scopes Server Options - ACADE-DC-01V

1.4.2.3.3.1 Scope DNS Settings

Dynamic Updates	OnClientRequest
Name Protection	No
Delete Dns RR On Lease Expiry	Yes

Table 245 - IPv6 Scopes DNS Setting - acade-dc-01v

1.4.2.3.4 Scope Options

The following section provides a summary 6 Scope Server Options information.

fd99:9971::

The following section provides a summary of the DHCP servers IPv6 Scope Server Options information.

Name	Option Id	Type	Value
DNS Recursive Name Server IPv6 Address List	23	IPv6Address	fd99:9971::1

Table 246 - IPv6 Scopes Options - fd99:9971::

1.4.3 UIA.LOCAL Child Domain DHCP Configuration

The following section provides a summary of the Dynamic Host Configuration Protocol.

1.4.3.1 DHCP Servers In Active Directory

The following section provides a summary of the DHCP servers information on UIA.LOCAL.

DC Name	IP Address	Domain Name	Domain Joined	Authorized	Conflict Detection Attempts
dc-uia-01v	172.23.7.1	uia.local	Yes	Yes	0

Table 247 - DHCP Servers In Active Directory - UIA.LOCAL

1.4.3.1.1 Service Database

DC Name	File Path	Backup Path	Backup Interval	Logging Enabled
dc-uia-01v	C:\Windows\system32\dhcp\dhcp.mdb	C:\Windows\system32\dhcp\backup	60 min	Yes

Table 248 - DHCP Servers Database - UIA.LOCAL

1.4.3.1.2 Dynamic DNS credentials

DC Name	User Name	Domain Name
dc-uia-01v	-	-

Table 249 - DHCP Servers Dynamic DNS Credentials - UIA.LOCAL

Health Check:
Best Practice: Credentials for DNS update should be configured if secure dynamic DNS update is enabled and the domain controller is on the same host as the DHCP server.

1.4.3.2 IPv4 Scope Configuration

The following section provides a IPv4 configuration summary of the Dynamic Host Configuration Protocol.

1.4.3.2.1 IPv4 Service Statistics

DC Name	Total Scopes	Total Addresses	Addresses In Use	Addresses Available	Percentage In Use	Percentage Available
dc-uia-01v	1	244	0	244	0	100

Table 250 - DHCP Server IPv4 Statistics - UIA.LOCAL

1.4.3.2.2 DC-UIA-01V IPv4 Scopes

The following section provides detailed information of the IPv4 Scope configuration.

Scope Id	Scope Name	Scope Range	Lease Duration	State
172.23.7.0/24	UIA Admin Scope	172.23.7.10 - 172.23.7.253	8.00:00:00	Active

Table 251 - IPv4 Scopes - DC-UIA-01V

1.4.3.2.2.1 IPv4 Scope Statistics

Scope Id	Free IP	In Use IP	Percentage In Use	Reserved IP
172.23.7.0	244	0	0	0

Table 252 - IPv4 Scope Statistics - DC-UIA-01V

1.4.3.2.2.2 IPv4 Network Interface Binding

Interface Alias	IP Address	Subnet Mask	State
Ethernet0	172.23.7.1	255.255.255.0	Enabled

Table 253 - IPv4 Network Interface binding - DC-UIA-01V

1.4.3.2.3 Scope Options

The following section provides a summary of the DHCP servers IPv4 Scope Server Options information.

172.23.7.0

Name	Option Id	Value	Policy Name
Router	3	172.23.7.254	-
DNS Servers	6	172.23.7.1 192.168.5.1	-
DNS Domain Name	15	uia.local	-
Lease	51	691200	-

Table 254 - IPv4 Scopes Options - 172.23.7.0

1.4.3.3 IPv6 Scope Configuration

The following section provides a IPv6 configuration summary of the Dynamic Host Configuration Protocol.

1.4.3.3.1 IPv6 Service Statistics

DC Name	Total Scopes	Total Addresses	Addresses In Use	Addresses Available	Percentage In Use	Percentage Available
dc-uia-01v	0	0	0	0	0	0

Table 255 - DHCP Server IPv6 Statistics - UIA.LOCAL

1.5 Certificate Authority Summary

In cryptography, a certificate authority or certification authority (CA) is an entity that issues digital certificates. A digital certificate certifies the ownership of a public key by the named subject of the certificate. This allows others (relying parties) to rely upon signatures or on assertions made about the private key that corresponds to the certified public key. A CA acts as a trusted third party trusted both

by the subject (owner) of the certificate and by the party relying upon the certificate. The format of these certificates is specified by the X.509 or EMV standard.

CA Name	Server Name	Type	Status
acad-ACADE-DC-01V-CA	ACADE-DC-01V	Enterprise Subordinate CA	Running
pharmax-CAYEY-DC-01V-CA	CAYEY-DC-01V	Enterprise Subordinate CA	Running
pharmax-SERVER-DC-01V-CA	SERVER-DC-01V	Enterprise Root CA	Running

Table 256 - Certification Authority - PHARMAX.LOCAL

1.5.1 Enterprise Root Certificate Authority

The following section provides the Enterprise Root CA information.

CA Name	pharmax-SERVER-DC-01V-CA
Server Name	SERVER-DC-01V
Type	Enterprise Root CA
Config String	Server-DC-01V.pharmax.local\pharmax-SERVER-DC-01V-CA
Operating System	Microsoft Windows Server 2019 Standard
Certificate	[Subject] CN=pharmax-SERVER-DC-01V-CA, DC=pharmax, DC=local [Issuer] CN=pharmax-SERVER-DC-01V-CA, DC=pharmax, DC=local [Serial Number] 5D2E25D9AFFDE4904A05D70BEB7ACBD2 [Not Before] 1/25/2020 7:35:16 PM [Not After] 1/25/2025 7:45:15 PM [Thumbprint] 0F6D4D3B8C71290E76B6B6C0661275F6F37B9CE0
Status	Running

Table 257 - Enterprise Root CA - PHARMAX.LOCAL

1.5.2 Enterprise Subordinate Certificate Authority

The following section provides the Enterprise Subordinate CA information.

CA Name	acad-ACADE-DC-01V-CA
Server Name	ACADE-DC-01V
Type	Enterprise Subordinate CA
Config String	acade-dc-01v.acad.pharmax.local\acad-ACADE-DC-01V-CA
Operating System	Microsoft Windows Server 2019 Standard Evaluation
Certificate	[Subject] CN=acad-ACADE-DC-01V-CA, DC=acad, DC=pharmax, DC=local [Issuer] CN=pharmax-SERVER-DC-01V-CA, DC=pharmax, DC=local [Serial Number] 61000000F5B20F8367F4837C6A0000000000F5 [Not Before] 9/22/2021 8:59:36 PM [Not After] 9/22/2023 9:09:36 PM [Thumbprint] 89532761827821E1B102CC8B86C529A6D2E92AC6
Status	Running

Table 258 - Enterprise Subordinate CA - acad-ACADE-DC-01V-CA

CA Name	pharmax-CAYEY-DC-01V-CA
Server Name	CAYEY-DC-01V
Type	Enterprise Subordinate CA
Config String	cayey-dc-01v.pharmax.local\pharmax-CAYEY-DC-01V-CA
Operating System	Microsoft Windows Server 2019 Standard Evaluation
Certificate	[Subject] CN=pharmax-CAYEY-DC-01V-CA, DC=pharmax, DC=local [Issuer] CN=pharmax-SERVER-DC-01V-CA, DC=pharmax, DC=local [Serial Number] 61000000F60DE0C8AB312FB51E0000000000F6 [Not Before] 10/4/2021 10:33:08 AM [Not After] 10/4/2023 10:43:08 AM [Thumbprint] CB2AC03DDA5A793DACAFC1EDC048CB1123D94B4B
Status	Running

Table 259 - Enterprise Subordinate CA - pharmax-CAYEY-DC-01V-CA

1.5.3 pharmax-SERVER-DC-01V-CA Details

1.5.3.1 Certificate Validity Period

The following section provides the Certification Authority Certificate Validity Period information.

CA Name	pharmax-SERVER-DC-01V-CA
Server Name	Server-DC-01V.pharmax.local
Validity Period	2 Years

Table 260 - Certificate Validity Period - PHARMAX.LOCAL

1.5.3.2 Access Control List (ACL)

DC Name	Owner	Group
pharmax-SERVER-DC-01V-CA	BUILTIN\Administrators	BUILTIN\Administrators

Table 261 - Access Control List - PHARMAX.LOCAL

1.5.3.2.1 Access Rights

Identity	Access Control Type	Rights
BUILTIN\Administrators	Allow	ManageCA, ManageCertificates
NT AUTHORITY\Authenticated Users	Allow	Enroll
PHARMAX\Domain Admins	Allow	ManageCA, ManageCertificates
PHARMAX\Enterprise Admins	Allow	ManageCA, ManageCertificates
PHARMAX\jocolon	Allow	ManageCA, ManageCertificates, Read, Enroll

Table 262 - Access Rights - pharmax-SERVER-DC-01V-CA

1.5.3.3 Cryptography Configuration

The following section provides the Certification Authority Cryptography Configuration information.

CA Name	pharmax-SERVER-DC-01V-CA
Server Name	SERVER-DC-01V
PublicKey Algorithm	RSA
Hashing Algorithm	SHA256
Provider Name	Microsoft Software Key Storage Provider
Alternate Signature Algorithm	No
Provider Is CNG	Yes

Table 263 - Cryptography Configuration - PHARMAX.LOCAL

1.5.3.4 Authority Information Access (AIA)

The following section provides the Certification Authority Authority Information Access information.

Reg URI	1:C:\Windows\system32\CertSrv\CertEnroll\%1_%3%4.crt
Config URI	1:C:\Windows\system32\CertSrv\CertEnroll\<ServerDNSName>_<CaName><CertificateName>.crt
Flags	1
Server Publish	Yes
Include To Extension	No
OCSP	No

Table 264 - Authority Information Access - pharmax-SERVER-DC-01V-CA

Reg URI	3:ldap:///CN=%7,CN=AIA,CN=Public Key Services,CN=Services,%6%11
Config URI	3:ldap:///CN=<CATruncatedName>,CN=AIA,CN=Public Key Services,CN=Services,<ConfigurationContainer><CAObjectClass>
Flags	1, 2
Server Publish	Yes
Include To Extension	Yes
OCSP	No

Table 265 - Authority Information Access - pharmax-SERVER-DC-01V-CA

Reg URI	0:http://%1/CertEnroll/%1_%3%4.crt
Config URI	0:http://<ServerDNSName>/CertEnroll/<ServerDNSName>_<CaName><CertificateName>.crt
Flags	-
Server Publish	No
Include To Extension	No
OCSP	No

Table 266 - Authority Information Access - pharmax-SERVER-DC-01V-CA

Reg URI	0:file://%1/CertEnroll/%1_%3%4.crt
Config URI	0:file://<ServerDNSName>/CertEnroll/<ServerDNSName>_<CaName><CertificateName>.crt

Flags	-
Server Publish	No
Include To Extension	No
OCSP	No

Table 267 - Authority Information Access - pharmax-SERVER-DC-01V-CA

Reg URI	2:http://acade-dc-01v.acad.pharmax.local/CertData/%1_%3%4.crt
Config URI	2:http://acade-dc-01v.acad.pharmax.local/CertData/<ServerDNSName>_<CaName><CertificateName>.crt
Flags	2
Server Publish	No
Include To Extension	Yes
OCSP	No

Table 268 - Authority Information Access - pharmax-SERVER-DC-01V-CA

1.5.3.5 Certificate Revocation List (CRL)

The following section provides the Certification Authority CRL Distribution Point information.

1.5.3.5.1 CRL Validity Period

CA Name	Base CRL	Base CRL Overlap	Delta CRL	Delta CRL Overlap
pharmax-SERVER-DC-01V-CA	50 Weeks	0 Hours	0 Days	0 Minutes

Table 269 - CRL Validity Preriod - PHARMAX.LOCAL

1.5.3.5.2 CRL Flags Settings

CA Name	Server Name	CRL Flags
pharmax-SERVER-DC-01V-CA	SERVER-DC-01V	DeleteExpiredCRLs

Table 270 - CRL Flags - PHARMAX.LOCAL

1.5.3.5.3 CRL Distribution Point

The following section provides the Certification Authority CRL Distribution Point information.

Reg URI	65:C:\Windows\system32\CertSrv\CertEnroll\%3%8%9.crl
Config URI	65:C:\Windows\system32\CertSrv\CertEnroll\<CaName><CRLNameSuffix><DeltaCRLAllowed>.crl
Url Scheme	Unknown
ProjectedURI	65:C:\Windows\system32\CertSrv\CertEnroll\pharmax-SERVER-DC-01V-CA.crl 65:C:\Windows\system32\CertSrv\CertEnroll\pharmax-SERVER-DC-01V-CA+.crl

Flags	1, 64
CRL Publish	-
Delta CRL Publish	Yes
Add To Cert CDP	No
Add To Fresh est CRL	No
Add To Crl cdp	No

Table 271 - CRL Distribution Point - pharmax-SERVER-DC-01V-CA

Reg URI	79:ldap:///CN=%7%8,CN=%2,CN=CDP,CN=Public Key Services,CN=Services,%6%10
Config URI	79:ldap:///CN=<CATruncatedName><CRLNameSuffix>,CN=<ServerShortName>,CN=CDP,CN=Public Key Services,CN=Services,<ConfigurationContainer><CDPObjectClass>
Url Scheme	LDAP
ProjectedURI	79:ldap:///CN=pharmax-SERVER-DC-01V-CA,CN=Server-DC-01V,CN=CDP,CN=Public Key Services,CN=Services,CN=Configuration,DC=pharmax,DC=local?certificateRevocationList?base?objectClass=cRLDistributionPoint
Flags	1, 2, 4, 8, 64
CRL Publish	-
Delta CRL Publish	Yes
Add To Cert CDP	Yes
Add To Fresh est CRL	Yes
Add To Crl cdp	Yes

Table 272 - CRL Distribution Point - pharmax-SERVER-DC-01V-CA

Reg URI	0:http://%1/CertEnroll/%3%8%9.crl
Config URI	0:http://<ServerDNSName>/CertEnroll/<CaName><CRLNameSuffix><DeltaCRLAllowed>.crl
Url Scheme	HTTP
ProjectedURI	0:http:///CertEnroll/pharmax-SERVER-DC-01V-CA.crl 0:http:///CertEnroll/pharmax-SERVER-DC-01V-CA+.crl
Flags	-
CRL Publish	-
Delta CRL Publish	No
Add To Cert CDP	No
Add To Fresh est CRL	No
Add To Crl cdp	No

Table 273 - CRL Distribution Point - pharmax-SERVER-DC-01V-CA

Reg URI	0:file://%1/CertEnroll/%3%8%9.crl
Config URI	0:file://<ServerDNSName>/CertEnroll/<CaName><CRLNameSuffix><DeltaCRLAllowed>.crl
Url Scheme	UNC
ProjectedURI	0:file:///CertEnroll/pharmax-SERVER-DC-01V-CA.crl 0:file:///CertEnroll/pharmax-SERVER-DC-01V-CA+.crl
Flags	-
CRL Publish	-

Delta CRL Publish	No
Add To Cert CDP	No
Add To Fresh est CRL	No
Add To Crl cdp	No

Table 274 - CRL Distribution Point - pharmax-SERVER-DC-01V-CA

Reg URI	6:http://acade-dc-01v.acad.pharmax.local/CertData/%3%8%9.crl
Config URI	6:http://acade-dc-01v.acad.pharmax.local/CertData/<CaName><CRLNameSuffix><DeltaCRLAllowed>.crl
Url Scheme	HTTP
ProjectedURI	6:http://acade-dc-01v.acad.pharmax.local/CertData/pharmax-SERVER-DC-01V-CA.crl 6:http://acade-dc-01v.acad.pharmax.local/CertData/pharmax-SERVER-DC-01V-CA+.crl
Flags	2, 4
CRL Publish	-
Delta CRL Publish	No
Add To Cert CDP	Yes
Add To Fresh est CRL	Yes
Add To Crl cdp	No

Table 275 - CRL Distribution Point - pharmax-SERVER-DC-01V-CA

1.5.3.6 AIA and CDP Health Status

The following section is intended to perform Certification Authority health status checking by CA certificate chain status and validating all CRL Distribution Point (CDP) and Authority Information Access (AIA) URLs for each certificate in the chain.

CA Name	Childs	Health
pharmax-SERVER-DC-01V-CA	pharmax-SERVER-DC-01V-CA	Error

Table 276 - Certification Authority Health - PHARMAX.LOCAL

1.5.3.7 Certificate Template Summary

The following section provides the certificate templates that are assigned to a specified Certification Authority (CA). CA server can issue certificates only based on assigned templates.

Template Name	Schema Version	Supported CA	Autoenrollment
Administrator	1	Windows 2000 Server	No
Basic EFS	1	Windows 2000 Server	No
Computer	1	Windows 2000 Server	No
ConfigMgr Client Distribution	2	Windows Server 2003 Enterprise Edition	Yes
Directory Email Replication	2	Windows Server 2003 Enterprise Edition	Yes

Template Name	Schema Version	Supported CA	Autoenrollment
Domain Controller	1	Windows 2000 Server	No
Domain Controller Authentication	2	Windows Server 2003 Enterprise Edition	Yes
EFS Recovery Agent	1	Windows 2000 Server	No
Kerberos Authentication	2	Windows Server 2003 Enterprise Edition	Yes
Pharmax Key Recovery Agent	2	Windows Server 2003 Enterprise Edition	Yes
Pharmax Labs Key Archive	2	Windows Server 2003 Enterprise Edition	Yes
Pharmax Web Server	2	Windows Server 2003 Enterprise Edition	No
Pharmax Workstation Authentication	2	Windows Server 2003 Enterprise Edition	Yes
Subordinate Certification Authority	1	Windows 2000 Server	No
User	1	Windows 2000 Server	No
Web Server	1	Windows 2000 Server	No
Web Server - ADFS	2	Windows Server 2003 Enterprise Edition	No
Web Server - Horizon	2	Windows Server 2003 Enterprise Edition	No
Web Server - Parallel	2	Windows Server 2003 Enterprise Edition	No
Web Server - WSUS SSL	2	Windows Server 2003 Enterprise Edition	No

Table 277 - Issued Certificate Template - pharmax-SERVER-DC-01V-CA

1.5.3.7.1 Issued Certificate Template ACLs

The following section provides the certificate templates Access Control List that are assigned to a specified Certification Authority (CA).

Pharmax Labs Key Archive

Identity	Access Control Type	Rights	Inherited
NT AUTHORITY\Authenticated Users	Allow	Read	No
PHARMAX\Administrator	Allow	Read, Write	No
PHARMAX\Domain Admins	Allow	Read, Write, Enroll	No
PHARMAX\Domain Users	Allow	Enroll	No
PHARMAX\Enterprise Admins	Allow	Read, Write, Enroll	No

Table 278 - Certificate Template ACL - Pharmax Labs Key Archive

Pharmax Key Recovery Agent

Identity	Access Control Type	Rights	Inherited
NT AUTHORITY\Authenticated Users	Allow	Read	No
PHARMAX\Administrator	Allow	Read, Write	No
PHARMAX\Domain Admins	Allow	Read, Write, Enroll	No
PHARMAX\Enterprise Admins	Allow	Read, Write, Enroll	No

Table 279 - Certificate Template ACL - Pharmax Key Recovery Agent

Pharmax Workstation Authentication

Identity	Access Control Type	Rights	Inherited
NT AUTHORITY\Authenticated Users	Allow	Read	No
PHARMAX\Administrator	Allow	Read, Write	No
PHARMAX\Domain Admins	Allow	Read, Write, Enroll	No
PHARMAX\Domain Computers	Allow	Read, Enroll, Autoenroll	No
PHARMAX\Enterprise Admins	Allow	Read, Write, Enroll	No

Table 280 - Certificate Template ACL - Pharmax Workstation Authentication

Web Server - ADFS

Identity	Access Control Type	Rights	Inherited
NT AUTHORITY\Authenticated Users	Allow	Read	No
PHARMAX\Administrator	Allow	Read, Write	No
PHARMAX\Domain Admins	Allow	Read, Write, Enroll	No
PHARMAX\Enterprise Admins	Allow	Read, Write, Enroll	No
PHARMAX\SERVER-ADFS-01V$	Allow	Read, Enroll	No
PHARMAX\SERVER-ADFS-02V$	Allow	Read, Enroll	No

Table 281 - Certificate Template ACL - Web Server - ADFS

Web Server - Parallel

Identity	Access Control Type	Rights	Inherited
NT AUTHORITY\Authenticated Users	Allow	Read	No
PHARMAX\Administrator	Allow	Read, Write	No
PHARMAX\Domain Admins	Allow	Read, Write, Enroll	No
PHARMAX\Enterprise Admins	Allow	Read, Write, Enroll	No
PHARMAX\SCCM_SiteServers	Allow	Read, Enroll, Autoenroll	No

Table 282 - Certificate Template ACL - Web Server - Parallel

ConfigMgr Client Distribution

Identity	Access Control Type	Rights	Inherited
NT AUTHORITY\Authenticated Users	Allow	Read	No
PHARMAX\Administrator	Allow	Read, Write	No
PHARMAX\Domain Admins	Allow	Read, Write, Enroll	No
PHARMAX\Enterprise Admins	Allow	Read, Write, Enroll	No
PHARMAX\SCCM-DB-01V$	Allow	Read, Enroll, Autoenroll	No
PHARMAX\SCCM-DP-01V$	Allow	Read, Enroll, Autoenroll	No
PHARMAX\SCCM-PRI-01V$	Allow	Read, Enroll, Autoenroll	No

Table 283 - Certificate Template ACL - ConfigMgr Client Distribution

Pharmax Web Server

Identity	Access Control Type	Rights	Inherited
NT AUTHORITY\Authenticated Users	Allow	Read	No
PHARMAX\Domain Admins	Allow	Read, Write, Enroll	No
PHARMAX\Enterprise Admins	Allow	Read, Write, Enroll	No
PHARMAX\jocolon	Allow	Read, Write	No

Table 284 - Certificate Template ACL - Pharmax Web Server

Web Server - Horizon

Identity	Access Control Type	Rights	Inherited
NT AUTHORITY\Authenticated Users	Allow	Read	No
PHARMAX\Administrator	Allow	Read, Write	No
PHARMAX\Domain Admins	Allow	Read, Write, Enroll	No
PHARMAX\Domain Computers	Allow	Read, Write, Enroll	No
PHARMAX\Enterprise Admins	Allow	Read, Write, Enroll	No

Table 285 - Certificate Template ACL - Web Server - Horizon

Web Server - WSUS SSL

Identity	Access Control Type	Rights	Inherited
NT AUTHORITY\Authenticated Users	Allow	Read	No
PHARMAX\Administrator	Allow	Read, Write	No
PHARMAX\Domain Admins	Allow	Read, Write, Enroll	No
PHARMAX\Domain Computers	Allow	Read, Write, Enroll	No
PHARMAX\Domain Controllers	Allow	Read, Write, Enroll	No
PHARMAX\Enterprise Admins	Allow	Read, Write, Enroll	No

Table 286 - Certificate Template ACL - Web Server - WSUS SSL

Directory Email Replication

Identity	Access Control Type	Rights	Inherited
NT AUTHORITY\Authenticated Users	Allow	Read	No
NT AUTHORITY\ENTERPRISE DOMAIN CONTROLLERS	Allow	Enroll, Autoenroll	No
PHARMAX\Domain Admins	Allow	Read, Write, Enroll	No
PHARMAX\Domain Controllers	Allow	Enroll, Autoenroll	No
PHARMAX\Enterprise Admins	Allow	Read, Write, Enroll	No
PHARMAX\Enterprise Read-only Domain Controllers	Allow	Enroll, Autoenroll	No

Table 287 - Certificate Template ACL - Directory Email Replication

Domain Controller Authentication

Identity	Access Control Type	Rights	Inherited
NT AUTHORITY\Authenticated Users	Allow	Read	No
NT AUTHORITY\ENTERPRISE DOMAIN CONTROLLERS	Allow	Enroll, Autoenroll	No
PHARMAX\Domain Admins	Allow	Read, Write, Enroll	No
PHARMAX\Domain Controllers	Allow	Enroll, Autoenroll	No
PHARMAX\Enterprise Admins	Allow	Read, Write, Enroll	No
PHARMAX\Enterprise Read-only Domain Controllers	Allow	Enroll, Autoenroll	No

Table 288 - Certificate Template ACL - Domain Controller Authentication

Kerberos Authentication

Identity	Access Control Type	Rights	Inherited
NT AUTHORITY\Authenticated Users	Allow	Read	No
NT AUTHORITY\ENTERPRISE DOMAIN CONTROLLERS	Allow	Enroll, Autoenroll	No
PHARMAX\Domain Admins	Allow	Read, Write, Enroll	No
PHARMAX\Domain Controllers	Allow	Enroll, Autoenroll	No
PHARMAX\Enterprise Admins	Allow	Read, Write, Enroll	No
PHARMAX\Enterprise Read-only Domain Controllers	Allow	Enroll, Autoenroll	No

Table 289 - Certificate Template ACL - Kerberos Authentication

EFS Recovery Agent

Identity	Access Control Type	Rights	Inherited
NT AUTHORITY\Authenticated Users	Allow	Read	No
PHARMAX\Domain Admins	Allow	Read, Write, Enroll	No

Identity	Access Control Type	Rights	Inherited
PHARMAX\Enterprise Admins	Allow	Read, Write, Enroll	No

Table 290 - Certificate Template ACL - EFS Recovery Agent

Basic EFS

Identity	Access Control Type	Rights	Inherited
NT AUTHORITY\Authenticated Users	Allow	Read	No
PHARMAX\Domain Admins	Allow	Read, Write, Enroll	No
PHARMAX\Domain Users	Allow	Enroll	No
PHARMAX\Enterprise Admins	Allow	Read, Write, Enroll	No

Table 291 - Certificate Template ACL - Basic EFS

Domain Controller

Identity	Access Control Type	Rights	Inherited
NT AUTHORITY\Authenticated Users	Allow	Read	No
NT AUTHORITY\ENTERPRISE DOMAIN CONTROLLERS	Allow	Enroll	No
PHARMAX\Domain Admins	Allow	Read, Write, Enroll	No
PHARMAX\Domain Controllers	Allow	Enroll	No
PHARMAX\Enterprise Admins	Allow	Read, Write, Enroll	No
PHARMAX\Enterprise Read-only Domain Controllers	Allow	Enroll	No

Table 292 - Certificate Template ACL - Domain Controller

Web Server

Identity	Access Control Type	Rights	Inherited
NT AUTHORITY\Authenticated Users	Allow	Read	No
PHARMAX\Domain Admins	Allow	Read, Write, Enroll	No
PHARMAX\Enterprise Admins	Allow	Read, Write, Enroll	No

Table 293 - Certificate Template ACL - Web Server

Computer

Identity	Access Control Type	Rights	Inherited
NT AUTHORITY\Authenticated Users	Allow	Read	No
PHARMAX\Domain Admins	Allow	Read, Write, Enroll	No
PHARMAX\Domain Computers	Allow	Enroll	No

Identity	Access Control Type	Rights	Inherited
PHARMAX\Enterprise Admins	Allow	Read, Write, Enroll	No

Table 294 - Certificate Template ACL - Computer

User

Identity	Access Control Type	Rights	Inherited
NT AUTHORITY\Authenticated Users	Allow	Read	No
PHARMAX\Domain Admins	Allow	Read, Write, Enroll	No
PHARMAX\Domain Users	Allow	Enroll	No
PHARMAX\Enterprise Admins	Allow	Read, Write, Enroll	No

Table 295 - Certificate Template ACL - User

Subordinate Certification Authority

Identity	Access Control Type	Rights	Inherited
NT AUTHORITY\Authenticated Users	Allow	Read	No
PHARMAX\Domain Admins	Allow	Read, Write, Enroll	No
PHARMAX\Enterprise Admins	Allow	Read, Write, Enroll	No

Table 296 - Certificate Template ACL - Subordinate Certification Authority

Administrator

Identity	Access Control Type	Rights	Inherited
NT AUTHORITY\Authenticated Users	Allow	Read	No
PHARMAX\Domain Admins	Allow	Read, Write, Enroll	No
PHARMAX\Enterprise Admins	Allow	Read, Write, Enroll	No

Table 297 - Certificate Template ACL - Administrator

1.5.3.7.2 Certificate Template In Active Directory

The following section provides registered certificate templates from Active Directory.

Template Name	Schema Version	Supported CA	Autoenrollment
Administrator	1	Windows 2000 Server	No
Authenticated Session	1	Windows 2000 Server	No
Basic EFS	1	Windows 2000 Server	No
CA Exchange	2	Windows Server 2003 Enterprise Edition	No
CEP Encryption	1	Windows 2000 Server	No

Template Name	Schema Version	Supported CA	Autoenrollment
Code Signing	1	Windows 2000 Server	No
Computer	1	Windows 2000 Server	No
ConfigMgr Client Distribution	2	Windows Server 2003 Enterprise Edition	Yes
Cross Certification Authority	2	Windows Server 2003 Enterprise Edition	No
Directory Email Replication	2	Windows Server 2003 Enterprise Edition	Yes
Domain Controller	1	Windows 2000 Server	No
Domain Controller Authentication	2	Windows Server 2003 Enterprise Edition	Yes
EFS Recovery Agent	1	Windows 2000 Server	No
Enrollment Agent	1	Windows 2000 Server	No
Enrollment Agent (Computer)	1	Windows 2000 Server	No
Exchange Enrollment Agent (Offline request)	1	Windows 2000 Server	No
Exchange Signature Only	1	Windows 2000 Server	No
Exchange User	1	Windows 2000 Server	No
IPSec	1	Windows 2000 Server	No
IPSec (Offline request)	1	Windows 2000 Server	No
Kerberos Authentication	2	Windows Server 2003 Enterprise Edition	Yes
Key Recovery Agent	2	Windows Server 2003 Enterprise Edition	Yes
OCSP Response Signing	3	Windows Server 2008 Enterprise Edition	No
Pharmax Key Recovery Agent	2	Windows Server 2003 Enterprise Edition	Yes
Pharmax Labs Key Archive	2	Windows Server 2003 Enterprise Edition	Yes
Pharmax Web Server	2	Windows Server 2003 Enterprise Edition	No
Pharmax Workstation Authentication	2	Windows Server 2003 Enterprise Edition	Yes
RAS and IAS Server	2	Windows Server 2003 Enterprise Edition	Yes
Root Certification Authority	1	Windows 2000 Server	No
Router (Offline request)	1	Windows 2000 Server	No
Smartcard Logon	1	Windows 2000 Server	No
Smartcard User	1	Windows 2000 Server	No
Subordinate Certification Authority	1	Windows 2000 Server	No
Trust List Signing	1	Windows 2000 Server	No
User	1	Windows 2000 Server	No
User Signature Only	1	Windows 2000 Server	No
Web Server	1	Windows 2000 Server	No
Web Server - ADFS	2	Windows Server 2003 Enterprise Edition	No

Template Name	Schema Version	Supported CA	Autoenrollment
Web Server - Horizon	2	Windows Server 2003 Enterprise Edition	No
Web Server - Parallel	2	Windows Server 2003 Enterprise Edition	No
Web Server - WSUS SSL	2	Windows Server 2003 Enterprise Edition	No
Workstation Authentication	2	Windows Server 2003 Enterprise Edition	Yes

Table 298 - Certificate Template in AD - PHARMAX.LOCAL

1.5.3.8 Key Recovery Agent Certificate

The following section provides the Key Recovery Agent certificate used to encrypt user's certificate private key and store it in CA database. In the case when user cannot access his or her certificate private key it is possible to recover it by Key Recovery Agent if Key Archival procedure was taken against particular certificate.

CA Name	pharmax-SERVER-DC-01V-CA
Server Name	SERVER-DC-01V
Certificate	[Subject] CN=Administrator, CN=Users, DC=pharmax, DC=local [Issuer] CN=pharmax-SERVER-DC-01V-CA, DC=pharmax, DC=local [Serial Number] 61000001068FABBB1D8B7B986A000000000106 [Not Before] 11/16/2021 8:11:55 PM [Not After] 11/16/2023 8:11:55 PM [Thumbprint] 0C65947128A94A0209907127D13F81AD5840CA37

Table 299 - Key Recovery Agent Certificate - pharmax-SERVER-DC-01V-CA

1.5.4 acad-ACADE-DC-01V-CA Details

1.5.4.1 Certificate Validity Period

The following section provides the Certification Authority Certificate Validity Period information.

CA Name	acad-ACADE-DC-01V-CA
Server Name	acade-dc-01v.acad.pharmax.local
Validity Period	2 Years

Table 300 - Certificate Validity Period - PHARMAX.LOCAL

1.5.4.2 Access Control List (ACL)

DC Name	Owner	Group
acad-ACADE-DC-01V-CA	BUILTIN\Administrators	BUILTIN\Administrators

Table 301 - Access Control List - PHARMAX.LOCAL

1.5.4.2.1 Access Rights

Identity	Access Control Type	Rights
ACAD\Domain Admins	Allow	ManageCA, ManageCertificates
BUILTIN\Administrators	Allow	ManageCA, ManageCertificates
NT AUTHORITY\Authenticated Users	Allow	Enroll
PHARMAX\Enterprise Admins	Allow	ManageCA, ManageCertificates

Table 302 - Access Rights - acad-ACADE-DC-01V-CA

1.5.4.3 Cryptography Configuration

The following section provides the Certification Authority Cryptography Configuration information.

CA Name	acad-ACADE-DC-01V-CA
Server Name	ACADE-DC-01V
PublicKey Algorithm	RSA
Hashing Algorithm	SHA256
Provider Name	Microsoft Software Key Storage Provider
Alternate Signature Algorithm	No
Provider Is CNG	Yes

Table 303 - Cryptography Configuration - PHARMAX.LOCAL

1.5.4.4 Authority Information Access (AIA)

The following section provides the Certification Authority Authority Information Access information.

Reg URI	1:C:\Windows\system32\CertSrv\CertEnroll\%1_%3%4.crt
Config URI	1:C:\Windows\system32\CertSrv\CertEnroll\<ServerDNSName>_<CaName><CertificateName>.crt
Flags	1
Server Publish	Yes
Include To Extension	No
OCSP	No

Table 304 - Authority Information Access - acad-ACADE-DC-01V-CA

Reg URI	3:ldap:///CN=%7,CN=AIA,CN=Public Key Services,CN=Services,%6%11
Config URI	3:ldap:///CN=<CATruncatedName>,CN=AIA,CN=Public Key Services,CN=Services,<ConfigurationContainer><CAObjectClass>
Flags	1, 2
Server Publish	Yes
Include To Extension	Yes
OCSP	No

Table 305 - Authority Information Access - acad-ACADE-DC-01V-CA

Reg URI	0:http://%1/CertEnroll/%1_%3%4.crt

Config URI	0:http://<ServerDNSName>/CertEnroll/<ServerDNSName>_<CaName><CertificateName>.crt
Flags	-
Server Publish	No
Include To Extension	No
OCSP	No

Table 306 - Authority Information Access - acad-ACADE-DC-01V-CA

Reg URI	0:file://%1/CertEnroll/%1_%3%4.crt
Config URI	0:file://<ServerDNSName>/CertEnroll/<ServerDNSName>_<CaName><CertificateName>.crt
Flags	-
Server Publish	No
Include To Extension	No
OCSP	No

Table 307 - Authority Information Access - acad-ACADE-DC-01V-CA

Reg URI	2:http://acade-dc-01v.acad.pharmax.local/CertEnroll/%1_%3%4.crt
Config URI	2:http://acade-dc-01v.acad.pharmax.local/CertEnroll/<ServerDNSName>_<CaName><CertificateName>.crt
Flags	2
Server Publish	No
Include To Extension	Yes
OCSP	No

Table 308 - Authority Information Access - acad-ACADE-DC-01V-CA

Reg URI	32:http://acade-dc-01v.acad.pharmax.local/ocsp
Config URI	32:http://acade-dc-01v.acad.pharmax.local/ocsp
Flags	32
Server Publish	No
Include To Extension	No
OCSP	Yes

Table 309 - Authority Information Access - acad-ACADE-DC-01V-CA

1.5.4.5 Certificate Revocation List (CRL)

The following section provides the Certification Authority CRL Distribution Point information.

1.5.4.5.1 CRL Validity Period

CA Name	Base CRL	Base CRL Overlap	Delta CRL	Delta CRL Overlap
acad-ACADE-DC-01V-CA	1 Weeks	0 Hours	1 Days	0 Minutes

Table 310 - CRL Validity Preriod - PHARMAX.LOCAL

1.5.4.5.2 CRL Flags Settings

CA Name	Server Name	CRL Flags
acad-ACADE-DC-01V-CA	ACADE-DC-01V	DeleteExpiredCRLs

Table 311 - CRL Flags - PHARMAX.LOCAL

1.5.4.5.3 CRL Distribution Point

The following section provides the Certification Authority CRL Distribution Point information.

Reg URI	65:C:\Windows\system32\CertSrv\CertEnroll\%3%8%9.crl
Config URI	65:C:\Windows\system32\CertSrv\CertEnroll\<CaName><CRLNameSuffix><DeltaCRLAllowed>.crl
Url Scheme	Unknown
ProjectedURI	65:C:\Windows\system32\CertSrv\CertEnroll\acad-ACADE-DC-01V-CA.crl 65:C:\Windows\system32\CertSrv\CertEnroll\acad-ACADE-DC-01V-CA+.crl
Flags	1, 64
CRL Publish	-
Delta CRL Publish	Yes
Add To Cert CDP	No
Add To Fresh est CRL	No
Add To Crl cdp	No

Table 312 - CRL Distribution Point - acad-ACADE-DC-01V-CA

Reg URI	79:ldap:///CN=%7%8,CN=%2,CN=CDP,CN=Public Key Services,CN=Services,%6%10
Config URI	79:ldap:///CN=<CATruncatedName><CRLNameSuffix>,CN=<ServerShortName>,CN=CDP,CN=Public Key Services,CN=Services,<ConfigurationContainer><CDPObjectClass>
Url Scheme	LDAP
ProjectedURI	79:ldap:///CN=acad-ACADE-DC-01V-CA,CN=acade-dc-01v,CN=CDP,CN=Public Key Services,CN=Services,CN=Configuration,DC=pharmax,DC=local?certificateRevocationList?base?objectClass=cRLDistributionPoint
Flags	1, 2, 4, 8, 64
CRL Publish	-
Delta CRL Publish	Yes
Add To Cert CDP	Yes
Add To Fresh est CRL	Yes
Add To Crl cdp	Yes

Table 313 - CRL Distribution Point - acad-ACADE-DC-01V-CA

Reg URI	0:http://%1/CertEnroll/%3%8%9.crl
Config URI	0:http://<ServerDNSName>/CertEnroll/<CaName><CRLNameSuffix><DeltaCRLAllowed>.crl

Url Scheme	HTTP
ProjectedURI	0:http:///CertEnroll/acad-ACADE-DC-01V-CA.crl 0:http:///CertEnroll/acad-ACADE-DC-01V-CA+.crl
Flags	-
CRL Publish	-
Delta CRL Publish	No
Add To Cert CDP	No
Add To Fresh est CRL	No
Add To Crl cdp	No

Table 314 - CRL Distribution Point - acad-ACADE-DC-01V-CA

Reg URI	0:file://%1/CertEnroll/%3%8%9.crl
Config URI	0:file://<ServerDNSName>/CertEnroll/<CaName><CRLNameSuffix><DeltaCRLAllowed>.crl
Url Scheme	UNC
ProjectedURI	0:file:///CertEnroll/acad-ACADE-DC-01V-CA.crl 0:file:///CertEnroll/acad-ACADE-DC-01V-CA+.crl
Flags	-
CRL Publish	-
Delta CRL Publish	No
Add To Cert CDP	No
Add To Fresh est CRL	No
Add To Crl cdp	No

Table 315 - CRL Distribution Point - acad-ACADE-DC-01V-CA

Reg URI	6:http://acade-dc-01v.acad.pharmax.local/CertEnroll/%3%8%9.crl
Config URI	6:http://acade-dc-01v.acad.pharmax.local/CertEnroll/<CaName><CRLNameSuffix><DeltaCRLAllowed>.crl
Url Scheme	HTTP
ProjectedURI	6:http://acade-dc-01v.acad.pharmax.local/CertEnroll/acad-ACADE-DC-01V-CA.crl 6:http://acade-dc-01v.acad.pharmax.local/CertEnroll/acad-ACADE-DC-01V-CA+.crl
Flags	2, 4
CRL Publish	-
Delta CRL Publish	No
Add To Cert CDP	Yes
Add To Fresh est CRL	Yes
Add To Crl cdp	No

Table 316 - CRL Distribution Point - acad-ACADE-DC-01V-CA

1.5.4.6 AIA and CDP Health Status

The following section is intended to perform Certification Authority health status checking by CA certificate chain status and validating all CRL Distribution Point (CDP) and Authority Information Access (AIA) URLs for each certificate in the chain.

CA Name	Childs	Health
acad-ACADE-DC-01V-CA	acad-ACADE-DC-01V-CA pharmax-SERVER-DC-01V-CA	Error

Table 317 - Certification Authority Health - PHARMAX.LOCAL

1.5.4.7 Certificate Template Summary

The following section provides the certificate templates that are assigned to a specified Certification Authority (CA). CA server can issue certificates only based on assigned templates.

Template Name	Schema Version	Supported CA	Autoenrollment
Administrator	1	Windows 2000 Server	No
Basic EFS	1	Windows 2000 Server	No
Computer	1	Windows 2000 Server	No
Directory Email Replication	2	Windows Server 2003 Enterprise Edition	Yes
Domain Controller	1	Windows 2000 Server	No
Domain Controller Authentication	2	Windows Server 2003 Enterprise Edition	Yes
EFS Recovery Agent	1	Windows 2000 Server	No
Kerberos Authentication	2	Windows Server 2003 Enterprise Edition	Yes
Pharmax Workstation Authentication	2	Windows Server 2003 Enterprise Edition	Yes
Subordinate Certification Authority	1	Windows 2000 Server	No
User	1	Windows 2000 Server	No
Web Server	1	Windows 2000 Server	No

Table 318 - Issued Certificate Template - acad-ACADE-DC-01V-CA

1.5.4.7.1 Issued Certificate Template ACLs

The following section provides the certificate templates Access Control List that are assigned to a specified Certification Authority (CA).

Pharmax Workstation Authentication

Identity	Access Control Type	Rights	Inherited
NT AUTHORITY\Authenticated Users	Allow	Read	No
PHARMAX\Administrator	Allow	Read, Write	No
PHARMAX\Domain Admins	Allow	Read, Write, Enroll	No
PHARMAX\Domain Computers	Allow	Read, Enroll, Autoenroll	No
PHARMAX\Enterprise Admins	Allow	Read, Write, Enroll	No

Table 319 - Certificate Template ACL - Pharmax Workstation Authentication

Directory Email Replication

Identity	Access Control Type	Rights	Inherited
NT AUTHORITY\Authenticated Users	Allow	Read	No
NT AUTHORITY\ENTERPRISE DOMAIN CONTROLLERS	Allow	Enroll, Autoenroll	No
PHARMAX\Domain Admins	Allow	Read, Write, Enroll	No
PHARMAX\Domain Controllers	Allow	Enroll, Autoenroll	No
PHARMAX\Enterprise Admins	Allow	Read, Write, Enroll	No
PHARMAX\Enterprise Read-only Domain Controllers	Allow	Enroll, Autoenroll	No

Table 320 - Certificate Template ACL - Directory Email Replication

Domain Controller Authentication

Identity	Access Control Type	Rights	Inherited
NT AUTHORITY\Authenticated Users	Allow	Read	No
NT AUTHORITY\ENTERPRISE DOMAIN CONTROLLERS	Allow	Enroll, Autoenroll	No
PHARMAX\Domain Admins	Allow	Read, Write, Enroll	No
PHARMAX\Domain Controllers	Allow	Enroll, Autoenroll	No
PHARMAX\Enterprise Admins	Allow	Read, Write, Enroll	No
PHARMAX\Enterprise Read-only Domain Controllers	Allow	Enroll, Autoenroll	No

Table 321 - Certificate Template ACL - Domain Controller Authentication

Kerberos Authentication

Identity	Access Control Type	Rights	Inherited
NT AUTHORITY\Authenticated Users	Allow	Read	No
NT AUTHORITY\ENTERPRISE DOMAIN CONTROLLERS	Allow	Enroll, Autoenroll	No
PHARMAX\Domain Admins	Allow	Read, Write, Enroll	No
PHARMAX\Domain Controllers	Allow	Enroll, Autoenroll	No
PHARMAX\Enterprise Admins	Allow	Read, Write, Enroll	No
PHARMAX\Enterprise Read-only Domain Controllers	Allow	Enroll, Autoenroll	No

Table 322 - Certificate Template ACL - Kerberos Authentication

EFS Recovery Agent

Identity	Access Control Type	Rights	Inherited
NT AUTHORITY\Authenticated Users	Allow	Read	No

Identity	Access Control Type	Rights	Inherited
PHARMAX\Domain Admins	Allow	Read, Write, Enroll	No
PHARMAX\Enterprise Admins	Allow	Read, Write, Enroll	No

Table 323 - Certificate Template ACL - EFS Recovery Agent

Basic EFS

Identity	Access Control Type	Rights	Inherited
NT AUTHORITY\Authenticated Users	Allow	Read	No
PHARMAX\Domain Admins	Allow	Read, Write, Enroll	No
PHARMAX\Domain Users	Allow	Enroll	No
PHARMAX\Enterprise Admins	Allow	Read, Write, Enroll	No

Table 324 - Certificate Template ACL - Basic EFS

Domain Controller

Identity	Access Control Type	Rights	Inherited
NT AUTHORITY\Authenticated Users	Allow	Read	No
NT AUTHORITY\ENTERPRISE DOMAIN CONTROLLERS	Allow	Enroll	No
PHARMAX\Domain Admins	Allow	Read, Write, Enroll	No
PHARMAX\Domain Controllers	Allow	Enroll	No
PHARMAX\Enterprise Admins	Allow	Read, Write, Enroll	No
PHARMAX\Enterprise Read-only Domain Controllers	Allow	Enroll	No

Table 325 - Certificate Template ACL - Domain Controller

Web Server

Identity	Access Control Type	Rights	Inherited
NT AUTHORITY\Authenticated Users	Allow	Read	No
PHARMAX\Domain Admins	Allow	Read, Write, Enroll	No
PHARMAX\Enterprise Admins	Allow	Read, Write, Enroll	No

Table 326 - Certificate Template ACL - Web Server

Computer

Identity	Access Control Type	Rights	Inherited
NT AUTHORITY\Authenticated Users	Allow	Read	No
PHARMAX\Domain Admins	Allow	Read, Write, Enroll	No

Identity	Access Control Type	Rights	Inherited
PHARMAX\Domain Computers	Allow	Enroll	No
PHARMAX\Enterprise Admins	Allow	Read, Write, Enroll	No

Table 327 - Certificate Template ACL - Computer

User

Identity	Access Control Type	Rights	Inherited
NT AUTHORITY\Authenticated Users	Allow	Read	No
PHARMAX\Domain Admins	Allow	Read, Write, Enroll	No
PHARMAX\Domain Users	Allow	Enroll	No
PHARMAX\Enterprise Admins	Allow	Read, Write, Enroll	No

Table 328 - Certificate Template ACL - User

Subordinate Certification Authority

Identity	Access Control Type	Rights	Inherited
NT AUTHORITY\Authenticated Users	Allow	Read	No
PHARMAX\Domain Admins	Allow	Read, Write, Enroll	No
PHARMAX\Enterprise Admins	Allow	Read, Write, Enroll	No

Table 329 - Certificate Template ACL - Subordinate Certification Authority

Administrator

Identity	Access Control Type	Rights	Inherited
NT AUTHORITY\Authenticated Users	Allow	Read	No
PHARMAX\Domain Admins	Allow	Read, Write, Enroll	No
PHARMAX\Enterprise Admins	Allow	Read, Write, Enroll	No

Table 330 - Certificate Template ACL - Administrator

1.5.4.7.2 Certificate Template In Active Directory

The following section provides registered certificate templates from Active Directory.

Template Name	Schema Version	Supported CA	Autoenrollment
Administrator	1	Windows 2000 Server	No
Authenticated Session	1	Windows 2000 Server	No
Basic EFS	1	Windows 2000 Server	No
CA Exchange	2	Windows Server 2003 Enterprise Edition	No

Template Name	Schema Version	Supported CA	Autoenrollment
CEP Encryption	1	Windows 2000 Server	No
Code Signing	1	Windows 2000 Server	No
Computer	1	Windows 2000 Server	No
ConfigMgr Client Distribution	2	Windows Server 2003 Enterprise Edition	Yes
Cross Certification Authority	2	Windows Server 2003 Enterprise Edition	No
Directory Email Replication	2	Windows Server 2003 Enterprise Edition	Yes
Domain Controller	1	Windows 2000 Server	No
Domain Controller Authentication	2	Windows Server 2003 Enterprise Edition	Yes
EFS Recovery Agent	1	Windows 2000 Server	No
Enrollment Agent	1	Windows 2000 Server	No
Enrollment Agent (Computer)	1	Windows 2000 Server	No
Exchange Enrollment Agent (Offline request)	1	Windows 2000 Server	No
Exchange Signature Only	1	Windows 2000 Server	No
Exchange User	1	Windows 2000 Server	No
IPSec	1	Windows 2000 Server	No
IPSec (Offline request)	1	Windows 2000 Server	No
Kerberos Authentication	2	Windows Server 2003 Enterprise Edition	Yes
Key Recovery Agent	2	Windows Server 2003 Enterprise Edition	Yes
OCSP Response Signing	3	Windows Server 2008 Enterprise Edition	No
Pharmax Key Recovery Agent	2	Windows Server 2003 Enterprise Edition	Yes
Pharmax Labs Key Archive	2	Windows Server 2003 Enterprise Edition	Yes
Pharmax Web Server	2	Windows Server 2003 Enterprise Edition	No
Pharmax Workstation Authentication	2	Windows Server 2003 Enterprise Edition	Yes
RAS and IAS Server	2	Windows Server 2003 Enterprise Edition	Yes
Root Certification Authority	1	Windows 2000 Server	No
Router (Offline request)	1	Windows 2000 Server	No
Smartcard Logon	1	Windows 2000 Server	No
Smartcard User	1	Windows 2000 Server	No
Subordinate Certification Authority	1	Windows 2000 Server	No
Trust List Signing	1	Windows 2000 Server	No
User	1	Windows 2000 Server	No
User Signature Only	1	Windows 2000 Server	No
Web Server	1	Windows 2000 Server	No
Web Server - ADFS	2	Windows Server 2003 Enterprise Edition	No

Template Name	Schema Version	Supported CA	Autoenrollment
Web Server - Horizon	2	Windows Server 2003 Enterprise Edition	No
Web Server - Parallel	2	Windows Server 2003 Enterprise Edition	No
Web Server - WSUS SSL	2	Windows Server 2003 Enterprise Edition	No
Workstation Authentication	2	Windows Server 2003 Enterprise Edition	Yes

Table 331 - Certificate Template in AD - PHARMAX.LOCAL

1.5.4.8 Key Recovery Agent Certificate

The following section provides the Key Recovery Agent certificate used to encrypt user's certificate private key and store it in CA database. In the case when user cannot access his or her certificate private key it is possible to recover it by Key Recovery Agent if Key Archival procedure was taken against particular certificate.

CA Name	acad-ACADE-DC-01V-CA
Server Name	ACADE-DC-01V
Certificate	[Subject] CN=Administrator, CN=Users, DC=pharmax, DC=local [Issuer] CN=pharmax-SERVER-DC-01V-CA, DC=pharmax, DC=local [Serial Number] 610000011FC4B5F75727EEAB0800000000011F [Not Before] 1/23/2022 10:30:44 PM [Not After] 1/23/2024 10:30:44 PM [Thumbprint] 4883ED66CAB909725F89D7483E97DBF69C4CDA9B

Table 332 - Key Recovery Agent Certificate - acad-ACADE-DC-01V-CA

1.5.5 pharmax-CAYEY-DC-01V-CA Details

1.5.5.1 Certificate Validity Period

The following section provides the Certification Authority Certificate Validity Period information.

CA Name	pharmax-CAYEY-DC-01V-CA
Server Name	cayey-dc-01v.pharmax.local
Validity Period	2 Years

Table 333 - Certificate Validity Period - PHARMAX.LOCAL

1.5.5.2 Access Control List (ACL)

DC Name	Owner	Group
pharmax-CAYEY-DC-01V-CA	BUILTIN\Administrators	BUILTIN\Administrators

Table 334 - Access Control List - PHARMAX.LOCAL

1.5.5.2.1 Access Rights

Identity	Access Control Type	Rights
BUILTIN\Administrators	Allow	ManageCA, ManageCertificates
NT AUTHORITY\Authenticated Users	Allow	Enroll
PHARMAX\Domain Admins	Allow	ManageCA, ManageCertificates
PHARMAX\Enterprise Admins	Allow	ManageCA, ManageCertificates

Table 335 - Access Rights - pharmax-CAYEY-DC-01V-CA

1.5.5.3 Cryptography Configuration

The following section provides the Certification Authority Cryptography Configuration information.

CA Name	pharmax-CAYEY-DC-01V-CA
Server Name	CAYEY-DC-01V
PublicKey Algorithm	RSA
Hashing Algorithm	SHA256
Provider Name	Microsoft Software Key Storage Provider
Alternate Signature Algorithm	No
Provider Is CNG	Yes

Table 336 - Cryptography Configuration - PHARMAX.LOCAL

1.5.5.4 Authority Information Access (AIA)

The following section provides the Certification Authority Authority Information Access information.

Reg URI	1:C:\Windows\system32\CertSrv\CertEnroll\%1_%3%4.crt
Config URI	1:C:\Windows\system32\CertSrv\CertEnroll\<ServerDNSName>_<CaName><CertificateName>.crt
Flags	1
Server Publish	Yes
Include To Extension	No
OCSP	No

Table 337 - Authority Information Access - pharmax-CAYEY-DC-01V-CA

Reg URI	3:ldap:///CN=%7,CN=AIA,CN=Public Key Services,CN=Services,%6%11
Config URI	3:ldap:///CN=<CATruncatedName>,CN=AIA,CN=Public Key Services,CN=Services,<ConfigurationContainer><CAObjectClass>
Flags	1, 2
Server Publish	Yes
Include To Extension	Yes
OCSP	No

Table 338 - Authority Information Access - pharmax-CAYEY-DC-01V-CA

Reg URI	0:http://%1/CertEnroll/%1_%3%4.crt
Config URI	0:http://<ServerDNSName>/CertEnroll/<ServerDNSName>_<CaName><CertificateName>.crt

Flags	-
Server Publish	No
Include To Extension	No
OCSP	No

Table 339 - Authority Information Access - pharmax-CAYEY-DC-01V-CA

Reg URI	0:file://%1/CertEnroll/%1_%3%4.crt
Config URI	0:file://<ServerDNSName>/CertEnroll/<ServerDNSName>_<CaName><CertificateName>.crt
Flags	-
Server Publish	No
Include To Extension	No
OCSP	No

Table 340 - Authority Information Access - pharmax-CAYEY-DC-01V-CA

1.5.5.5 Certificate Revocation List (CRL)

The following section provides the Certification Authority CRL Distribution Point information.

1.5.5.5.1 CRL Validity Period

CA Name	Base CRL	Base CRL Overlap	Delta CRL	Delta CRL Overlap
pharmax-CAYEY-DC-01V-CA	1 Weeks	0 Hours	1 Days	0 Minutes

Table 341 - CRL Validity Preriod - PHARMAX.LOCAL

1.5.5.5.2 CRL Flags Settings

CA Name	Server Name	CRL Flags
pharmax-CAYEY-DC-01V-CA	CAYEY-DC-01V	DeleteExpiredCRLs

Table 342 - CRL Flags - PHARMAX.LOCAL

1.5.5.5.3 CRL Distribution Point

The following section provides the Certification Authority CRL Distribution Point information.

Reg URI	65:C:\Windows\system32\CertSrv\CertEnroll\%3%8%9.crl
Config URI	65:C:\Windows\system32\CertSrv\CertEnroll\<CaName><CRLNameSuffix><DeltaCRLAllowed>.crl
Url Scheme	Unknown
ProjectedURI	65:C:\Windows\system32\CertSrv\CertEnroll\pharmax-CAYEY-DC-01V-CA.crl 65:C:\Windows\system32\CertSrv\CertEnroll\pharmax-CAYEY-DC-01V-CA+.crl
Flags	1, 64

CRL Publish	-
Delta CRL Publish	Yes
Add To Cert CDP	No
Add To Fresh est CRL	No
Add To Crl cdp	No

Table 343 - CRL Distribution Point - pharmax-CAYEY-DC-01V-CA

Reg URI	79:ldap:///CN=%7%8,CN=%2,CN=CDP,CN=Public Key Services,CN=Services,%6%10
Config URI	79:ldap:///CN=<CATruncatedName><CRLNameSuffix>,CN=<ServerShortName>,CN=CDP,CN=Public Key Services,CN=Services,<ConfigurationContainer><CDPObjectClass>
Url Scheme	LDAP
ProjectedURI	79:ldap:///CN=pharmax-CAYEY-DC-01V-CA,CN=cayey-dc-01v,CN=CDP,CN=Public Key Services,CN=Services,CN=Configuration,DC=pharmax,DC=local?certificateRevocationList?base?objectClass=cRLDistributionPoint
Flags	1, 2, 4, 8, 64
CRL Publish	-
Delta CRL Publish	Yes
Add To Cert CDP	Yes
Add To Fresh est CRL	Yes
Add To Crl cdp	Yes

Table 344 - CRL Distribution Point - pharmax-CAYEY-DC-01V-CA

Reg URI	0:http://%1/CertEnroll/%3%8%9.crl
Config URI	0:http://<ServerDNSName>/CertEnroll/<CaName><CRLNameSuffix><DeltaCRLAllowed>.crl
Url Scheme	HTTP
ProjectedURI	0:http:///CertEnroll/pharmax-CAYEY-DC-01V-CA.crl 0:http:///CertEnroll/pharmax-CAYEY-DC-01V-CA+.crl
Flags	-
CRL Publish	-
Delta CRL Publish	No
Add To Cert CDP	No
Add To Fresh est CRL	No
Add To Crl cdp	No

Table 345 - CRL Distribution Point - pharmax-CAYEY-DC-01V-CA

Reg URI	0:file://%1/CertEnroll/%3%8%9.crl
Config URI	0:file://<ServerDNSName>/CertEnroll/<CaName><CRLNameSuffix><DeltaCRLAllowed>.crl
Url Scheme	UNC
ProjectedURI	0:file:///CertEnroll/pharmax-CAYEY-DC-01V-CA.crl 0:file:///CertEnroll/pharmax-CAYEY-DC-01V-CA+.crl
Flags	-
CRL Publish	-
Delta CRL Publish	No

Add To Cert CDP	No
Add To Fresh est CRL	No
Add To Crl cdp	No

Table 346 - CRL Distribution Point - pharmax-CAYEY-DC-01V-CA

1.5.5.6 AIA and CDP Health Status

The following section is intended to perform Certification Authority health status checking by CA certificate chain status and validating all CRL Distribution Point (CDP) and Authority Information Access (AIA) URLs for each certificate in the chain.

CA Name	Childs	Health
pharmax-CAYEY-DC-01V-CA	pharmax-CAYEY-DC-01V-CA pharmax-SERVER-DC-01V-CA	Error

Table 347 - Certification Authority Health - PHARMAX.LOCAL