



# Microsoft AD As Built Report

Zen Pr Solutions

Author: Jonathan Colon  
Date: Sunday, September 4, 2022  
Version: 1.0

## Table of Contents

|  |    |
|--|----|
| 1 PHARMAX.LOCAL Active Directory Report.....           | 8  |
| 1.1 Forest Information.....                            | 8  |
| 1.1.1 Optional Features .....                          | 8  |
| 1.1.2 Domain Sites.....                                | 8  |
| 1.1.2.1 Site Subnets .....                             | 9  |
| 1.1.2.2 Site Links .....                               | 9  |
| 1.2 Active Directory Domain Information .....          | 9  |
| 1.2.1 PHARMAX.LOCAL Root Domain Configuration.....     | 9  |
| 1.2.1.1 Flexible Single Master Operations (FSMO) ..... | 10 |
| 1.2.1.2 Domain and Trusts .....                        | 10 |
| 1.2.1.3 Domain Object Count .....                      | 11 |
| 1.2.1.4 User Accounts in Active Directory .....        | 11 |
| 1.2.1.5 Status of Users Accounts .....                 | 11 |
| 1.2.1.6 Privileged Group Count .....                   | 11 |
| 1.2.1.7 Computer Accounts in Active Directory.....     | 12 |
| 1.2.1.8 Status of Computer Accounts.....               | 12 |
| 1.2.1.9 Operating Systems Count .....                  | 12 |
| 1.2.1.10 Default Domain Password Policy .....          | 13 |
| 1.2.1.11 Fined Grained Password Policies .....         | 13 |
| 1.2.1.12 Group Managed Service Accounts (GMSA) .....   | 14 |
| 1.2.1.13 Domain Controller Summary .....               | 15 |
| 1.2.1.13.1 Hardware Inventory .....                    | 15 |
| 1.2.1.13.2 NTDS Information .....                      | 16 |
| 1.2.1.13.3 Time Source Information .....               | 16 |
| 1.2.1.13.4 SRV Records Status .....                    | 17 |
| 1.2.1.13.5 Installed Software on DC .....              | 17 |
| 1.2.1.13.6 Roles.....                                  | 17 |
| 1.2.1.13.7 DC Diagnostic.....                          | 19 |
| 1.2.1.13.8 Infrastructure Services Status.....         | 20 |
| 1.2.1.13.9 Sites Replication Connection.....           | 21 |
| 1.2.1.13.10 Sites Replication Status.....              | 23 |
| 1.2.1.13.11 Group Policy Objects Summary .....         | 23 |
| 1.2.1.13.11.1 Central Store Repository .....           | 24 |
| 1.2.1.13.11.2 User Logon/Logoff Script.....            | 24 |
| 1.2.1.13.11.3 Computer Startup/Shutdown Script .....   | 24 |
| 1.2.1.13.11.4 Unlinked GPO .....                       | 25 |
| 1.2.1.13.11.5 Empty GPOs .....                         | 25 |
| 1.2.1.13.11.6 Enforced GPO .....                       | 25 |

## Microsoft AD As Built Report - v1.0

|   |    |
|---|----|
| 1.2.1.13.12 Organizational Units .....                    | 25 |
| 1.2.1.13.12.1 GPO Blocked Inheritance .....               | 31 |
| 1.2.2 ACAD.PHARMAX.LOCAL Child Domain Configuration ..... | 32 |
| 1.2.2.1 Flexible Single Master Operations (FSMO) .....    | 32 |
| 1.2.2.2 Domain and Trusts .....                           | 32 |
| 1.2.2.3 Domain Object Count .....                         | 33 |
| 1.2.2.4 User Accounts in Active Directory .....           | 33 |
| 1.2.2.5 Status of Users Accounts .....                    | 33 |
| 1.2.2.6 Privileged Group Count .....                      | 34 |
| 1.2.2.7 Computer Accounts in Active Directory .....       | 34 |
| 1.2.2.8 Status of Computer Accounts .....                 | 34 |
| 1.2.2.9 Operating Systems Count .....                     | 34 |
| 1.2.2.10 Default Domain Password Policy .....             | 34 |
| 1.2.2.11 Fined Grained Password Policies .....            | 35 |
| 1.2.2.12 Group Managed Service Accounts (GMSA) .....      | 35 |
| 1.2.2.13 Domain Controller Summary .....                  | 35 |
| 1.2.2.13.1 Hardware Inventory .....                       | 36 |
| 1.2.2.13.2 NTDS Information .....                         | 36 |
| 1.2.2.13.3 Time Source Information .....                  | 37 |
| 1.2.2.13.4 SRV Records Status .....                       | 37 |
| 1.2.2.13.5 Installed Software on DC .....                 | 37 |
| 1.2.2.13.6 Roles .....                                    | 37 |
| 1.2.2.13.7 DC Diagnostic .....                            | 38 |
| 1.2.2.13.8 Infrastructure Services Status .....           | 38 |
| 1.2.2.13.9 Sites Replication Connection .....             | 39 |
| 1.2.2.13.10 Sites Replication Status .....                | 40 |
| 1.2.2.13.11 Group Policy Objects Summary .....            | 40 |
| 1.2.2.13.11.1 Central Store Repository .....              | 41 |
| 1.2.2.13.11.2 User Logon/Logoff Script .....              | 41 |
| 1.2.2.13.11.3 Unlinked GPO .....                          | 41 |
| 1.2.2.13.11.4 Empty GPOs .....                            | 41 |
| 1.2.2.13.11.5 Enforced GPO .....                          | 42 |
| 1.2.2.13.12 Organizational Units .....                    | 42 |
| 1.2.2.13.12.1 GPO Blocked Inheritance .....               | 42 |
| 1.2.3 UIA.LOCAL Child Domain Configuration .....          | 42 |
| 1.2.3.1 Flexible Single Master Operations (FSMO) .....    | 43 |
| 1.2.3.2 Domain and Trusts .....                           | 43 |
| 1.2.3.3 Domain Object Count .....                         | 43 |
| 1.2.3.4 User Accounts in Active Directory .....           | 44 |

## Microsoft AD As Built Report - v1.0

|   |    |
|---|----|
| 1.2.3.5 Status of Users Accounts .....                  | 44 |
| 1.2.3.6 Privileged Group Count .....                    | 44 |
| 1.2.3.7 Computer Accounts in Active Directory .....     | 44 |
| 1.2.3.8 Status of Computer Accounts.....                | 45 |
| 1.2.3.9 Operating Systems Count .....                   | 45 |
| 1.2.3.10 Default Domain Password Policy .....           | 45 |
| 1.2.3.11 Domain Controller Summary .....                | 45 |
| 1.2.3.11.1 Hardware Inventory .....                     | 46 |
| 1.2.3.11.2 NTDS Information .....                       | 46 |
| 1.2.3.11.3 Time Source Information .....                | 46 |
| 1.2.3.11.4 SRV Records Status .....                     | 47 |
| 1.2.3.11.5 Installed Software on DC .....               | 47 |
| 1.2.3.11.6 Roles .....                                  | 47 |
| 1.2.3.11.7 DC Diagnostic .....                          | 48 |
| 1.2.3.11.8 Infrastructure Services Status.....          | 48 |
| 1.2.3.11.9 Sites Replication Connection.....            | 49 |
| 1.2.3.11.10 Sites Replication Status .....              | 50 |
| 1.2.3.11.11 Group Policy Objects Summary .....          | 50 |
| 1.2.3.11.11.1 Central Store Repository .....            | 50 |
| 1.2.3.11.12 Organizational Units .....                  | 51 |
| 1.3 Domain Name System Summary .....                    | 56 |
| 1.3.1 PHARMAX.LOCAL Root Domain DNS Configuration ..... | 56 |
| 1.3.1.1 Infrastructure Summary .....                    | 56 |
| 1.3.1.1.1 Domain Controller DNS IP Configuration .....  | 56 |
| 1.3.1.1.2 Application Directory Partition.....          | 56 |
| 1.3.1.1.3 Response Rate Limiting (RRL) .....            | 57 |
| 1.3.1.1.4 Scavenging Options.....                       | 57 |
| 1.3.1.1.5 Forwarder Options .....                       | 57 |
| 1.3.1.1.6 Root Hints .....                              | 57 |
| 1.3.1.1.7 Zone Scope Recursion .....                    | 58 |
| 1.3.1.2 SERVER-DC-01V DNS Zones .....                   | 58 |
| 1.3.1.2.1 Zone Delegation.....                          | 59 |
| 1.3.1.2.2 Zone Transfers.....                           | 59 |
| 1.3.1.2.3 Reverse Lookup Zone .....                     | 59 |
| 1.3.1.2.4 Conditional Forwarder .....                   | 59 |
| 1.3.1.2.5 Zone Scope Aging .....                        | 59 |
| 1.3.1.3 CAYEY-DC-01V DNS Zones.....                     | 60 |
| 1.3.1.3.1 Zone Delegation.....                          | 60 |
| 1.3.1.3.2 Reverse Lookup Zone .....                     | 60 |

## Microsoft AD As Built Report - v1.0

|  |    |
|--|----|
| 1.3.1.3.3 Conditional Forwarder .....                        | 60 |
| 1.3.1.3.4 Zone Scope Aging .....                             | 61 |
| 1.3.2 ACAD.PHARMAX.LOCAL Child Domain DNS Configuration..... | 61 |
| 1.3.2.1 Infrastructure Summary .....                         | 61 |
| 1.3.2.1.1 Domain Controller DNS IP Configuration .....       | 61 |
| 1.3.2.1.2 Application Directory Partition.....               | 61 |
| 1.3.2.1.3 Response Rate Limiting (RRL) .....                 | 62 |
| 1.3.2.1.4 Scavenging Options.....                            | 62 |
| 1.3.2.1.5 Forwarder Options .....                            | 62 |
| 1.3.2.1.6 Root Hints .....                                   | 62 |
| 1.3.2.1.7 Zone Scope Recursion .....                         | 63 |
| 1.3.2.2 ACADE-DC-01V DNS Zones .....                         | 63 |
| 1.3.2.2.1 Zone Transfers.....                                | 63 |
| 1.3.2.2.2 Reverse Lookup Zone .....                          | 63 |
| 1.3.2.2.3 Conditional Forwarder .....                        | 63 |
| 1.3.2.2.4 Zone Scope Aging .....                             | 64 |
| 1.3.3 UIA.LOCAL Child Domain DNS Configuration .....         | 64 |
| 1.3.3.1 Infrastructure Summary .....                         | 64 |
| 1.3.3.1.1 Domain Controller DNS IP Configuration .....       | 64 |
| 1.3.3.1.2 Application Directory Partition.....               | 64 |
| 1.3.3.1.3 Response Rate Limiting (RRL) .....                 | 65 |
| 1.3.3.1.4 Scavenging Options.....                            | 65 |
| 1.3.3.1.5 Forwarder Options .....                            | 65 |
| 1.3.3.1.6 Root Hints .....                                   | 65 |
| 1.3.3.1.7 Zone Scope Recursion .....                         | 66 |
| 1.3.3.2 DC-UIA-01V DNS Zones .....                           | 66 |
| 1.3.3.2.1 Reverse Lookup Zone .....                          | 66 |
| 1.3.3.2.2 Zone Scope Aging .....                             | 66 |
| 1.4 Dynamic Host Configuration Protocol Summary .....        | 67 |
| 1.4.1 PHARMAX.LOCAL Root Domain DHCP Configuration.....      | 67 |
| 1.4.1.1 DHCP Servers In Active Directory.....                | 67 |
| 1.4.1.1.1 Service Database.....                              | 67 |
| 1.4.1.1.2 Dynamic DNS credentials.....                       | 67 |
| 1.4.1.2 IPv4 Scope Configuration.....                        | 67 |
| 1.4.1.2.1 IPv4 Service Statistics .....                      | 68 |
| 1.4.1.2.2 CAYEY-DC-01V IPv4 Scope Server Options .....       | 68 |
| 1.4.1.2.2.1 Scope DNS Setting .....                          | 68 |
| 1.4.1.2.3 SERVER-DC-01V IPv4 Scopes.....                     | 68 |
| 1.4.1.2.3.1 IPv4 Scope Statistics .....                      | 69 |

## Microsoft AD As Built Report - v1.0

|  |    |
|--|----|
| 1.4.1.2.3.2 IPv4 Network Interface Binding .....               | 69 |
| 1.4.1.2.4 SERVER-DC-01V IPv4 Scope Server Options .....        | 69 |
| 1.4.1.2.4.1 Scope DNS Setting .....                            | 70 |
| 1.4.1.2.5 Scope Options .....                                  | 70 |
| 1.4.1.3 IPv6 Scope Configuration.....                          | 72 |
| 1.4.1.3.1 IPv6 Service Statistics .....                        | 72 |
| 1.4.2 ACAD.PHARMAX.LOCAL Child Domain DHCP Configuration ..... | 72 |
| 1.4.2.1 DHCP Servers In Active Directory.....                  | 72 |
| 1.4.2.1.1 Service Database.....                                | 73 |
| 1.4.2.1.2 Dynamic DNS credentials .....                        | 73 |
| 1.4.2.2 IPv4 Scope Configuration.....                          | 73 |
| 1.4.2.2.1 IPv4 Service Statistics .....                        | 73 |
| 1.4.2.2.2 ACADE-DC-01V IPv4 Scopes .....                       | 73 |
| 1.4.2.2.2.1 IPv4 Scope Statistics .....                        | 73 |
| 1.4.2.2.2.2 IPv4 Network Interface Binding.....                | 74 |
| 1.4.2.2.3 ACADE-DC-01V IPv4 Scope Server Options .....         | 74 |
| 1.4.2.2.3.1 Scope DNS Setting .....                            | 74 |
| 1.4.2.2.4 Scope Options .....                                  | 74 |
| 1.4.2.3 IPv6 Scope Configuration.....                          | 75 |
| 1.4.2.3.1 IPv6 Service Statistics .....                        | 75 |
| 1.4.2.3.2 ACADE-DC-01V IPv6 Scopes .....                       | 75 |
| 1.4.2.3.2.1 IPv6 Scope Statistics .....                        | 75 |
| 1.4.2.3.3 ACADE-DC-01V IPv6 Scope Server Options .....         | 75 |
| 1.4.2.3.3.1 Scope DNS Settings .....                           | 75 |
| 1.4.2.3.4 Scope Options .....                                  | 76 |
| 1.4.3 UIA.LOCAL Child Domain DHCP Configuration .....          | 76 |
| 1.4.3.1 DHCP Servers In Active Directory.....                  | 76 |
| 1.4.3.1.1 Service Database.....                                | 76 |
| 1.4.3.1.2 Dynamic DNS credentials .....                        | 76 |
| 1.4.3.2 IPv4 Scope Configuration.....                          | 77 |
| 1.4.3.2.1 IPv4 Service Statistics .....                        | 77 |
| 1.4.3.2.2 DC-UIA-01V IPv4 Scopes.....                          | 77 |
| 1.4.3.2.2.1 IPv4 Scope Statistics .....                        | 77 |
| 1.4.3.2.2.2 IPv4 Network Interface Binding.....                | 77 |
| 1.4.3.2.3 Scope Options .....                                  | 77 |
| 1.4.3.3 IPv6 Scope Configuration.....                          | 78 |
| 1.4.3.3.1 IPv6 Service Statistics .....                        | 78 |
| 1.5 Certificate Authority Summary .....                        | 78 |
| 1.5.1 Enterprise Root Certificate Authority.....               | 78 |

## Microsoft AD As Built Report - v1.0

|  |    |
|--|----|
| 1.5.2 Enterprise Subordinate Certificate Authority ..... | 79 |
| 1.5.3 Certificate Validity Period .....                  | 79 |
| 1.5.3.1 Access Control List (ACL) .....                  | 80 |
| 1.5.3.1.1 pharmax-SERVER-DC-01V-CA Rights .....          | 80 |
| 1.5.3.1.2 acad-ACADE-DC-01V-CA Rights .....              | 80 |
| 1.5.3.1.3 pharmax-CAYEY-DC-01V-CA Rights .....           | 80 |
| 1.5.4 Cryptography Configuration .....                   | 80 |
| 1.5.5 Authority Information Access (AIA) .....           | 81 |
| 1.5.5.1 pharmax-SERVER-DC-01V-CA .....                   | 81 |
| 1.5.5.2 acad-ACADE-DC-01V-CA .....                       | 82 |
| 1.5.5.3 pharmax-CAYEY-DC-01V-CA .....                    | 83 |
| 1.5.6 Certificate Revocation List (CRL) .....            | 84 |
| 1.5.6.1 CRL Validity Period .....                        | 84 |
| 1.5.6.2 CRL Flags Settings .....                         | 85 |
| 1.5.6.3 CRL Distribution Point .....                     | 85 |
| 1.5.6.3.1 pharmax-SERVER-DC-01V-CA .....                 | 85 |
| 1.5.6.3.2 acad-ACADE-DC-01V-CA .....                     | 87 |
| 1.5.6.3.3 pharmax-CAYEY-DC-01V-CA .....                  | 88 |
| 1.5.7 AIA and CDP Health Status .....                    | 90 |
| 1.5.8 Certificate Template Summary .....                 | 90 |
| 1.5.8.1 pharmax-SERVER-DC-01V-CA .....                   | 90 |
| 1.5.8.2 Certificate Template In Active Directory .....   | 91 |
| 1.5.9 Certificate Template Summary .....                 | 92 |
| 1.5.9.1 acad-ACADE-DC-01V-CA .....                       | 92 |
| 1.5.9.2 Certificate Template In Active Directory .....   | 93 |
| 1.5.10 Certificate Template Summary .....                | 94 |
| 1.5.10.1 pharmax-CAYEY-DC-01V-CA .....                   | 94 |
| 1.5.10.2 Certificate Template In Active Directory .....  | 95 |
| 1.5.11 Key Recovery Agent Certificate .....              | 96 |

# 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; acad-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<br>DC=ForestDnsZones,DC=pharmax,DC=local<br>DC=DomainDnsZones,DC=uia,DC=local<br>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<br>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<br>Cayey-Branch<br>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

|                   |      |
|-------------------|------|
| Computers         | 211  |
| Servers           | 67   |
| Domain Controller | 2    |
| Global Catalog    | 1    |
| Users             | 2889 |
| Privileged Users  | 43   |
| Groups            | 564  |

Table 10 - Object Count - PHARMAX.LOCAL

## 1.2.1.4 User Accounts in Active Directory

| Status   | Count | Percentage |
|----------|-------|------------|
| Enabled  | 2885  | 100%       |
| Disabled | 4     | 0%         |

Table 11 - 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        | 13            | 0         | 1              | 0          | 14          | 0       |
| Password Never Expires        | 17            | 1         | 3              | 0          | 20          | 1       |
| Must Change Password at Logon | 0             | 0         | 2              | 0          | 2           | 0       |
| Password Age (> 42 days)      | 2865          | 99        | 1              | 0          | 2866        | 99      |
| SmartcardLogonRequired        | 1             | 0         | 1              | 0          | 2           | 0       |
| SidHistory                    | 1             | 0         | 1              | 0          | 0           | 0       |
| Never Logged in               | 2869          | 99        | 4              | 0          | 2873        | 99      |
| Dormant (> 90 days)           | 2881          | 100       | 4              | 0          | 2885        | 100     |
| Password Not Required         | 2             | 0         | 2              | 0          | 4           | 0       |
| Account Expired               | 1             | 0         | 1              | 0          | 1           | 0       |
| Account Lockout               | 1             | 0         | 1              | 0          | 0           | 0       |

Table 12 - 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         |
| DnsAdmins                      | 3         |
| Domain Admins                  | 5         |
| Enterprise Admins              | 2         |
| Incoming Forest Trust Builders | 2         |
| Key Admins                     | 2         |
| Print Operators                | 1         |
| Remote Desktop Users           | 3         |
| <b>Schema Admins</b>           | <b>25</b> |
| Server Operators               | 3         |

Table 13 - 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 14 - 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)      | 176           | 83        | 4              | 2          | 180         | 85      |
| Password Age (> 30 days) | 179           | 85        | 4              | 2          | 183         | 87      |
| SidHistory               | 1             | 0         | 1              | 0          | 0           | 0       |

Table 15 - 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     |

| Operating System                          | Count |
|---|-------|
| NetApp Release 9.9.1P1                    | 3     |
| OneFS                                     | 1     |
| redhat-linux-gnu                          | 1     |
| unknown                                   | 7     |
| Unknown                                   | 103   |
| Windows 10 Education                      | 1     |
| Windows 10 Enterprise                     | 1     |
| 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 16 - 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 17 - 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 |

# Microsoft AD As Built Report - v1.0

|                               |  |
|-------------------------------|--|
| 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 18 - 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 19 - 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 20 - Group Managed Service Accounts - SQLServer*

|                |             |
|----------------|-------------|
| Name           | adfsghmsa   |
| SamAccountName | adfsghmsa\$ |

|                           |                                  |
|---------------------------|----------------------------------|
| 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 21 - Group Managed Service Accounts - adfsgmsa

### 1.2.1.13 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 22 - Domain Controller Summary - PHARMAX.LOCAL

#### 1.2.1.13.1 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              |  |

Microsoft AD As Built Report - v1.0

|                         |   |
|-------------------------|---|
| 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 23 - 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 24 - Hardware Inventory - CAYEY-DC-01V

### 1.2.1.13.2 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 25 - NTDS Database File Usage - PHARMAX.LOCAL

### 1.2.1.13.3 Time Source Information

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



| Name          | Time Server  | Type         |
|---------------|--|--------------|
| SERVER-DC-01V | 192.168.5.254 0.pool.ntp.org 1.pool.ntp.org<br>2.pool.ntp.org 3.pool.ntp.org | MANUAL (NTP) |

Table 26 - Time Source Configuration - PHARMAX.LOCAL

#### 1.2.1.13.4 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 27 - 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.

#### 1.2.1.13.5 Installed Software on DC

The following section provides a summary of additional software running on PHARMAX.LOCAL.

##### SERVER-DC-01V

| Name                        | Publisher                 | Install Date |
|-----------------------------|---------------------------|--------------|
| Veeam VSS Hardware Provider | Veeam Software Group GmbH | 20220502     |

Table 28 - 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 29 - Installed Software - CAYEY-DC-01V

#### **Health Check:**

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

#### 1.2.1.13.6 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   |

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

Table 30 - 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.  |

| Name             | Parent | InstallState   |
|------------------|--------|--|
| Web Server (IIS) | Role   | Web Server (IIS) provides a reliable, manageable, and scalable Web application infrastructure. |

Table 31 - 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**

## 1.2.1.13.7 DC Diagnostic

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

## SERVER-DC-01V

| Test Name          | Result |
|--------------------|--------|
| Advertising        | passed |
| CheckSDRefDom      | passed |
| CheckSDRefDom      | passed |
| CheckSDRefDom      | passed |
| CheckSDRefDom      | passed |
| CheckSDRefDom      | passed |
| Connectivity       | passed |
| CrossRefValidation | passed |
| CrossRefValidation | passed |
| CrossRefValidation | passed |
| DFSREvent          | failed |
| FrsEvent           | passed |
| Intersite          | passed |
| KccEvent           | passed |
| KnowsOfRoleHolders | passed |
| LocatorCheck       | passed |
| MachineAccount     | passed |
| NCSecDesc          | passed |
| NetLogons          | passed |
| ObjectsReplicated  | passed |
| Replications       | failed |
| RidManager         | passed |
| Services           | passed |
| SystemLog          | failed |
| SysVolCheck        | passed |
| VerifyReferences   | passed |

Table 32 - Domain Controller DCDiag - SERVER-DC-01V

## CAYEY-DC-01V

## Microsoft AD As Built Report - v1.0

| Test Name          | Result |
|--------------------|--------|
| Advertising        | passed |
| CheckSDRefDom      | passed |
| CheckSDRefDom      | passed |
| CheckSDRefDom      | passed |
| CheckSDRefDom      | passed |
| CheckSDRefDom      | passed |
| Connectivity       | passed |
| CrossRefValidation | passed |
| CrossRefValidation | passed |
| CrossRefValidation | passed |
| DFSREvent          | failed |
| FrsEvent           | passed |
| Intersite          | passed |
| KccEvent           | failed |
| KnowsOfRoleHolders | passed |
| LocatorCheck       | passed |
| MachineAccount     | passed |
| NCSecDesc          | passed |
| NetLogons          | passed |
| ObjectsReplicated  | passed |
| Replications       | failed |
| RidManager         | passed |
| Services           | passed |
| SystemLog          | failed |
| SysVolCheck        | passed |
| VerifyReferences   | passed |

Table 33 - Domain Controller DCDiag - CAYEY-DC-01V

### 1.2.1.13.8 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 |
| DFS Replication                       | DFSR       | Running |
| DHCP Server                           | DHCPServer | Running |
| DNS Server                            | DNS        | Running |
| Intersite Messaging                   | IsmServ    | Running |
| Kerberos Key Distribution Center      | Kdc        | Running |
| NetLogon                              | Netlogon   | Running |
| Windows Time                          | W32Time    | Running |

Table 34 - Infrastructure Services Status - SERVER-DC-01V

## 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 |
| DFS Replication                       | DFSR       | Running |
| DHCP Server                           | DHCPServer | Running |
| DNS Server                            | DNS        | Running |
| Intersite Messaging                   | IsmServ    | Running |
| Kerberos Key Distribution Center      | Kdc        | Running |
| NetLogon                              | Netlogon   | Running |
| Windows Time                          | W32Time    | Running |

Table 35 - Infrastructure Services Status - CAYEY-DC-01V

## 1.2.1.13.9 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<br>DC=ForestDnsZones,DC=pharmax,DC=local<br>CN=Schema,CN=Configuration,DC=pharmax,DC=local<br>CN=Configuration,DC=pharmax,DC=local<br>DC=pharmax,DC=local |
| Transport Protocol              | IP  |
| AutoGenerated                   | Yes   |
| Enabled                         | Yes   |
| Created                         | Tue, 07 Dec 2021 15:52:27 GMT   |

Table 36 - 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<br>DC=ForestDnsZones,DC=pharmax,DC=local<br>CN=Schema,CN=Configuration,DC=pharmax,DC=local<br>CN=Configuration,DC=pharmax,DC=local<br>DC=pharmax,DC=local |
| Transport Protocol              | IP  |
| AutoGenerated                   | Yes   |
| Enabled                         | Yes   |
| Created                         | Wed, 11 May 2022 17:54:53 GMT   |

Table 37 - 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<br>DC=ForestDnsZones,DC=pharmax,DC=local<br>CN=Schema,CN=Configuration,DC=pharmax,DC=local<br>CN=Configuration,DC=pharmax,DC=local<br>DC=pharmax,DC=local |
| Transport Protocol              | IP  |
| AutoGenerated                   | Yes   |
| Enabled                         | Yes   |
| Created                         | Sun, 05 Sep 2021 16:24:39 GMT   |

Table 38 - Site Replication - SERVER-DC-01V

#### CAYEY-DC-01V

|                                 |   |
|---------------------------------|---|
| GUID                            | 14c5d35b-e285-4bdb-a044-c75e0a22558a  |
| Description                     | -   |
| Replicate From Directory Server | ACADE-DC-01V  |
| Replicate To Directory Server   | CAYEY-DC-01V  |
| Replicated Naming Contexts      | DC=DomainDnsZones,DC=pharmax,DC=local<br>DC=ForestDnsZones,DC=pharmax,DC=local<br>CN=Schema,CN=Configuration,DC=pharmax,DC=local<br>CN=Configuration,DC=pharmax,DC=local<br>DC=pharmax,DC=local |
| Transport Protocol              | IP  |
| AutoGenerated                   | Yes   |
| Enabled                         | Yes   |
| Created                         | Wed, 31 Aug 2022 15:03:09 GMT   |

Table 39 - Site Replication - 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<br>DC=ForestDnsZones,DC=pharmax,DC=local<br>CN=Schema,CN=Configuration,DC=pharmax,DC=local<br>CN=Configuration,DC=pharmax,DC=local<br>DC=pharmax,DC=local |
| Transport Protocol              | IP  |
| AutoGenerated                   | Yes   |
| Enabled                         | Yes   |
| Created                         | Tue, 07 Dec 2021 15:55:03 GMT   |

Table 40 - Site Replication - CAYEY-DC-01V

## 1.2.1.13.10 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    | 2022-09-04 17:39:45 | 0                   | 0                   | 0                  |
| SERVER-DC-01V   | ACADE-DC-01V | ACAD            | 2022-09-04 17:39:45 | 0                   | 0                   | 0                  |
| SERVER-DC-01V   | CAYEY-DC-01V | Cayey-Branch    | 2022-09-04 17:39:45 | 0                   | 0                   | 0                  |
| SERVER-DC-01V   | DC-UIA-01V   | UIA             | 2022-09-04 15:51:21 | 8524                | 2022-09-04 17:39:52 | 7                  |
| SERVER-DC-01V   | ACADE-DC-01V | ACAD            | 2022-09-04 17:39:52 | 0                   | 0                   | 0                  |
| SERVER-DC-01V   | CAYEY-DC-01V | Cayey-Branch    | 2022-09-04 17:39:52 | 0                   | 0                   | 0                  |
| SERVER-DC-01V   | DC-UIA-01V   | UIA             | 2022-09-04 15:51:21 | 8524                | 2022-09-04 17:39:58 | 7                  |
| SERVER-DC-01V   | DC-UIA-01V   | UIA             | 2022-09-04 15:51:21 | 1256                | 2022-09-04 17:39:52 | 7                  |
| SERVER-DC-01V   | CAYEY-DC-01V | Cayey-Branch    | 2022-09-04 17:39:58 | 0                   | 0                   | 0                  |
| SERVER-DC-01V   | ACADE-DC-01V | ACAD            | 2022-09-04 17:39:58 | 0                   | 0                   | 0                  |
| SERVER-DC-01V   | CAYEY-DC-01V | Cayey-Branch    | 2022-09-04 17:39:58 | 0                   | 0                   | 0                  |
| SERVER-DC-01V   | DC-UIA-01V   | UIA             | 2022-09-04 15:51:21 | 1256                | 2022-09-04 17:39:52 | 6                  |
| SERVER-DC-01V   | ACADE-DC-01V | ACAD            | 2022-09-04 17:39:58 | 0                   | 0                   | 0                  |
| SERVER-DC-01V   | DC-UIA-01V   | UIA             | 2022-09-04 15:51:21 | 1256                | 2022-09-04 17:39:52 | 6                  |
| SERVER-DC-01V   | ACADE-DC-01V | ACAD            | 2022-09-04 17:39:58 | 0                   | 0                   | 0                  |

Table 41 - Site Replication Status - PHARMAX.LOCAL

**Health Check:**

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

## 1.2.1.13.11 Group Policy Objects Summary

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

| GPO Name                          | GPO Status             | Owner                 |
|-----------------------------------|------------------------|-----------------------|
| Assign-Applications               | All Settings Enabled   | PHARMAX\Domain Admins |
| Certificate AutoEnrollment        | User Settings Disabled | PHARMAX\Domain Admins |
| Dead Policy                       | All Settings Disabled  | PHARMAX\Domain Admins |
| Default Domain Controllers Policy | All Settings Enabled   | PHARMAX\Domain Admins |
| Default Domain Policy             | All Settings Enabled   | PHARMAX\Domain Admins |

| GPO Name                                     | GPO Status             | Owner                 |
|--|------------------------|-----------------------|
| Horizon-DEM                                  | All Settings Enabled   | PHARMAX\Domain Admins |
| LAPS Configuration                           | All Settings Enabled   | PHARMAX\Domain Admins |
| Linux-Settings-GPO                           | All Settings Disabled  | PHARMAX\Domain Admins |
| ProfileUnity                                 | All Settings Enabled   | PHARMAX\Domain Admins |
| SCCM - Restricted Group and General Settings | All Settings Enabled   | PHARMAX\Domain Admins |
| SCEP Configuration                           | All Settings Enabled   | PHARMAX\Domain Admins |
| SET - KMS Server                             | All Settings Enabled   | PHARMAX\Domain Admins |
| VEEAM_Disable_Firewall                       | All Settings Enabled   | PHARMAX\Domain Admins |
| VEEAM_Local_Administrators                   | All Settings Enabled   | PHARMAX\Domain Admins |
| WSUS - Domain Policy                         | User Settings Disabled | PHARMAX\Domain Admins |

Table 42 - GPO - PHARMAX.LOCAL

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

## 1.2.1.13.11.1 Central Store Repository

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

Table 43 - GPO Central Store - PHARMAX.LOCAL

## 1.2.1.13.11.2 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 44 - GPO with Logon/Logoff Script - PHARMAX.LOCAL

## 1.2.1.13.11.3 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 45 - GPO with Startup/Shutdown Script - PHARMAX.LOCAL



## 1.2.1.13.11.4 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 46 - Unlinked GPO - PHARMAX.LOCAL

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

## 1.2.1.13.11.5 Empty GPOs

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

Table 47 - Empty GPO - PHARMAX.LOCAL

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

## 1.2.1.13.11.6 Enforced GPO

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

Table 48 - Enforced GPO - PHARMAX.LOCAL

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

## 1.2.1.13.12 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                | -          |

Microsoft AD As Built Report - v1.0

| 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   |

Microsoft AD As Built Report - v1.0

| 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          | -          |

Microsoft AD As Built Report - v1.0

| 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                 | -          |

Microsoft AD As Built Report - v1.0

| 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                 | -          |

Microsoft AD As Built Report - v1.0

| 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            | -          |

Microsoft AD As Built Report - v1.0

| 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,<br>VEEAM_Local_Administrators |
| VEEAM WorkStations | pharmax.local/VEEAM WorkStations         | VEEAM_Local_Administrators,<br>VEEAM_Disable_Firewall |

Table 49 - Organizational Unit - PHARMAX.LOCAL

#### 1.2.1.13.12.1 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 50 - 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 51 - 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 52 - FSMO Server - acad.pharmax.local

### 1.2.2.2 Domain and Trusts

|        |   |
|--------|---|
| Name   | pharmax.local                           |
| Path   | acad.pharmax.local/System/pharmax.local |
| Source | acad                                    |



## Microsoft AD As Built Report - v1.0

|                            |               |
|----------------------------|---------------|
| 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 53 - Trusts - ACAD.PHARMAX.LOCAL

### 1.2.2.3 Domain Object Count

|                   |    |
|-------------------|----|
| Computers         | 2  |
| Servers           | 2  |
| Domain Controller | 1  |
| Global Catalog    | 1  |
| Users             | 4  |
| Privileged Users  | 2  |
| Groups            | 46 |

Table 54 - Object Count - ACAD.PHARMAX.LOCAL

### 1.2.2.4 User Accounts in Active Directory

| Status   | Count | Percentage |
|----------|-------|------------|
| Enabled  | 2     | 50%        |
| Disabled | 2     | 50%        |

Table 55 - 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        | 13            | 325       | 1              | 25         | 14          | 350     |
| Password Never Expires        | 1             | 25        | 1              | 25         | 1           | 25      |
| Must Change Password at Logon | 1             | 25        | 1              | 25         | 1           | 25      |
| Password Age (> 42 days)      | 1             | 25        | 1              | 25         | 2           | 50      |
| SmartcardLogonRequired        | 1             | 25        | 1              | 25         | 0           | 0       |
| SidHistory                    | 1             | 25        | 1              | 25         | 0           | 0       |
| Never Logged in               | 1             | 25        | 2              | 50         | 3           | 75      |
| Dormant (> 90 days)           | 2             | 50        | 2              | 50         | 4           | 100     |
| Password Not Required         | 1             | 25        | 1              | 25         | 2           | 50      |
| Account Expired               | 1             | 25        | 1              | 25         | 0           | 0       |
| Account Lockout               | 1             | 25        | 1              | 25         | 0           | 0       |

Table 56 - Status of User Accounts - ACAD.PHARMAX.LOCAL

## 1.2.2.6 Privileged Group Count

| Group Name           | Count |
|----------------------|-------|
| Account Operators    | 0     |
| Administrators       | 6     |
| Backup Operators     | 1     |
| Cert Publishers      | 1     |
| DnsAdmins            | 0     |
| Domain Admins        | 1     |
| Key Admins           | 0     |
| Print Operators      | 0     |
| Remote Desktop Users | 0     |
| Server Operators     | 0     |

Table 57 - 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 58 - 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)      | 1             | 50        | 1              | 50         | 0           | 0       |
| Password Age (> 30 days) | 1             | 50        | 1              | 50         | 0           | 0       |
| SidHistory               | 1             | 50        | 1              | 50         | 0           | 0       |

Table 59 - 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 60 - 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 61 - 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 62 - 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 63 - Group Managed Service Accounts - SCCMMSA

## 1.2.2.13 Domain Controller Summary

## Microsoft AD As Built Report - v1.0

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 64 - Domain Controller Summary - ACAD.PHARMAX.LOCAL

### 1.2.2.13.1 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 65 - Hardware Inventory - ACADE-DC-01V

### 1.2.2.13.2 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 66 - NTDS Database File Usage - ACAD.PHARMAX.LOCAL

### 1.2.2.13.3 Time Source Information

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

Table 67 - Time Source Configuration - ACAD.PHARMAX.LOCAL

### 1.2.2.13.4 SRV Records Status

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

Table 68 - 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.

### 1.2.2.13.5 Installed Software on DC

The following section provides a summary of additional software running on ACAD.PHARMAX.LOCAL.

### 1.2.2.13.6 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.   |
| 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.  |

| Name             | Parent | InstallState   |
|------------------|--------|--|
| Web Server (IIS) | Role   | Web Server (IIS) provides a reliable, manageable, and scalable Web application infrastructure. |

Table 69 - 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**

## 1.2.2.13.7 DC Diagnostic

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

## ACADE-DC-01V

| Test Name          | Result |
|--------------------|--------|
| Advertising        | failed |
| CheckSDRefDom      | passed |
| CheckSDRefDom      | passed |
| CheckSDRefDom      | passed |
| CheckSDRefDom      | passed |
| CheckSDRefDom      | passed |
| Connectivity       | passed |
| CrossRefValidation | passed |
| CrossRefValidation | passed |
| CrossRefValidation | passed |
| DFSREvent          | passed |
| FrsEvent           | passed |
| Intersite          | passed |
| KccEvent           | failed |
| KnowsOfRoleHolders | passed |
| LocatorCheck       | failed |
| MachineAccount     | passed |
| NCSecDesc          | failed |
| NetLogons          | failed |
| ObjectsReplicated  | passed |
| Replications       | failed |
| RidManager         | passed |
| Services           | passed |
| SystemLog          | failed |
| SysVolCheck        | failed |
| VerifyReferences   | passed |

Table 70 - Domain Controller DCDiag - ACADE-DC-01V

## 1.2.2.13.8 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 |
| DFS Replication                       | DFSR       | Running |
| DHCP Server                           | DHCPServer | Running |
| DNS Server                            | DNS        | Running |
| Intersite Messaging                   | IsmServ    | Running |
| Kerberos Key Distribution Center      | Kdc        | Running |
| NetLogon                              | Netlogon   | Running |
| Windows Time                          | W32Time    | Running |

Table 71 - Infrastructure Services Status - ACADE-DC-01V

#### 1.2.2.13.9 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<br>DC=acad,DC=pharmax,DC=local<br>DC=ForestDnsZones,DC=pharmax,DC=local<br>CN=Schema,CN=Configuration,DC=pharmax,DC=local<br>CN=Configuration,DC=pharmax,DC=local |
| Transport Protocol              | IP  |
| AutoGenerated                   | Yes   |
| Enabled                         | Yes   |
| Created                         | Sun, 05 Sep 2021 16:26:31 GMT   |

Table 72 - Site Replication - ACADE-DC-01V

|                                 |   |
|---------------------------------|---|
| GUID                            | ad51f64a-c0be-46ff-9cc8-af3fb05bfe7c  |
| 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<br>DC=acad,DC=pharmax,DC=local<br>DC=ForestDnsZones,DC=pharmax,DC=local<br>CN=Schema,CN=Configuration,DC=pharmax,DC=local<br>CN=Configuration,DC=pharmax,DC=local |
| Transport Protocol              | IP  |
| AutoGenerated                   | Yes   |

|         |                               |
|---------|-------------------------------|
| Enabled | Yes                           |
| Created | Thu, 01 Sep 2022 11:32:16 GMT |

Table 73 - Site Replication - ACADE-DC-01V

|                                 |   |
|---------------------------------|---|
| GUID                            | 056708d1-2630-487d-a25e-a9b837f860e6  |
| 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<br>DC=acad,DC=pharmax,DC=local<br>DC=ForestDnsZones,DC=pharmax,DC=local<br>CN=Schema,CN=Configuration,DC=pharmax,DC=local<br>CN=Configuration,DC=pharmax,DC=local |
| Transport Protocol              | IP  |
| AutoGenerated                   | Yes   |
| Enabled                         | Yes   |
| Created                         | Thu, 01 Sep 2022 11:32:16 GMT   |

Table 74 - Site Replication - ACADE-DC-01V

#### 1.2.2.13.10 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      | 2022-08-31 19:59:38 | 5                   | 2022-09-04 17:46:03 | 92                 |
| ACADE-DC-01V    | SERVER-DC-01V | Pharmax-HQ      | 2022-08-31 19:59:38 | 5                   | 2022-09-04 17:46:03 | 92                 |
| ACADE-DC-01V    | SERVER-DC-01V | Pharmax-HQ      | 2022-08-31 19:59:38 | 1256                | 2022-09-04 17:46:03 | 92                 |
| ACADE-DC-01V    | SERVER-DC-01V | Pharmax-HQ      | 2022-08-31 19:59:38 | 1256                | 2022-09-04 17:46:03 | 92                 |
| ACADE-DC-01V    | SERVER-DC-01V | Pharmax-HQ      | 2022-08-31 19:59:38 | 1256                | 2022-09-04 17:46:03 | 92                 |

Table 75 - Site Replication Status - ACAD.PHARMAX.LOCAL

#### **Health Check:**

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

#### 1.2.2.13.11 Group Policy Objects Summary

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

| GPO Name                          | GPO Status           | Owner                     |
|-----------------------------------|----------------------|---------------------------|
| ACAD Certificate AutoEnrollment   | All Settings Enabled | PHARMAX\Enterprise Admins |
| Default Domain Controllers Policy | All Settings Enabled | ACAD\Domain Admins        |
| Default Domain Policy             | All Settings Enabled | ACAD\Domain Admins        |



| GPO Name             | GPO Status            | Owner                     |
|----------------------|-----------------------|---------------------------|
| Empty Policy ACAD    | All Settings Enabled  | PHARMAX\Enterprise Admins |
| Logon Script         | All Settings Enabled  | PHARMAX\Enterprise Admins |
| Unlinked Policy ACAD | All Settings Disabled | PHARMAX\Enterprise Admins |

Table 76 - GPO - ACAD.PHARMAX.LOCAL

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

## 1.2.2.13.11.1 Central Store Repository

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

Table 77 - GPO Central Store - ACAD.PHARMAX.LOCAL

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

## 1.2.2.13.11.2 User Logon/Logoff Script

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

Table 78 - GPO with Logon/Logoff Script - ACAD.PHARMAX.LOCAL

## 1.2.2.13.11.3 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 79 - Unlinked GPO - ACAD.PHARMAX.LOCAL

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

## 1.2.2.13.11.4 Empty GPOs

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

Table 80 - Empty GPO - ACAD.PHARMAX.LOCAL

**Health Check:**

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

#### 1.2.2.13.11.5 Enforced GPO

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

Table 81 - Enforced GPO - ACAD.PHARMAX.LOCAL

**Health Check:**

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

#### 1.2.2.13.12 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 82 - Organizational Unit - ACAD.PHARMAX.LOCAL

#### 1.2.2.13.12.1 GPO Blocked Inheritance

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

Table 83 - 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 84 - 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 85 - 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 86 - Trusts - UIA.LOCAL

### 1.2.3.3 Domain Object Count

|                   |      |
|-------------------|------|
| Computers         | 100  |
| Servers           | 1    |
| Domain Controller | 1    |
| Global Catalog    | 1    |
| Users             | 2494 |
| Privileged Users  | 25   |

|        |     |
|--------|-----|
| Groups | 543 |
|--------|-----|

Table 87 - Object Count - UIA.LOCAL

## 1.2.3.4 User Accounts in Active Directory

| Status   | Count | Percentage |
|----------|-------|------------|
| Enabled  | 2492  | 100%       |
| Disabled | 2     | 0%         |

Table 88 - 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        | 13            | 1         | 1              | 0          | 14          | 1       |
| Password Never Expires        | 1             | 0         | 1              | 0          | 2           | 0       |
| Must Change Password at Logon | 1             | 0         | 1              | 0          | 2           | 0       |
| Password Age (> 42 days)      | 2490          | 100       | 1              | 0          | 2491        | 100     |
| SmartcardLogonRequired        | 1             | 0         | 1              | 0          | 0           | 0       |
| SidHistory                    | 1             | 0         | 1              | 0          | 0           | 0       |
| Never Logged in               | 2491          | 100       | 2              | 0          | 2493        | 100     |
| Dormant (> 90 days)           | 2492          | 100       | 2              | 0          | 2494        | 100     |
| Password Not Required         | 1             | 0         | 1              | 0          | 2           | 0       |
| Account Expired               | 1             | 0         | 1              | 0          | 0           | 0       |
| Account Lockout               | 1             | 0         | 1              | 0          | 0           | 0       |

Table 89 - Status of User Accounts - UIA.LOCAL

## 1.2.3.6 Privileged Group Count

| Group Name           | Count |
|----------------------|-------|
| Account Operators    | 1     |
| Administrators       | 10    |
| Backup Operators     | 2     |
| Cert Publishers      | 1     |
| DnsAdmins            | 3     |
| Domain Admins        | 6     |
| Key Admins           | 5     |
| Print Operators      | 3     |
| Remote Desktop Users | 2     |
| Server Operators     | 2     |

Table 90 - Privileged Group Count - UIA.LOCAL

## 1.2.3.7 Computer Accounts in Active Directory

| Status   | Count | Percentage |
|----------|-------|------------|
| Enabled  | 100   | 100%       |
| Disabled | 0     | 0%         |

Table 91 - 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        | 0              | 0          | 99          | 99      |
| Password Age (> 30 days) | 99            | 99        | 0              | 0          | 99          | 99      |
| SidHistory               | 1             | 1         | 1              | 1          | 0           | 0       |

Table 92 - 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 93 - 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 94 - Default Domain Password Policy - UIA.LOCAL

### 1.2.3.11 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 95 - Domain Controller Summary - UIA.LOCAL

### 1.2.3.11.1 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 96 - Hardware Inventory - DC-UIA-01V

### 1.2.3.11.2 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 97 - NTDS Database File Usage - UIA.LOCAL

### 1.2.3.11.3 Time Source Information

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

Table 98 - Time Source Configuration - UIA.LOCAL

#### 1.2.3.11.4 SRV Records Status

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

Table 99 - 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.

#### 1.2.3.11.5 Installed Software on DC

The following section provides a summary of additional software running on UIA.LOCAL.

#### 1.2.3.11.6 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 100 - 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

### 1.2.3.11.7 DC Diagnostic

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

#### DC-UIA-01V

| Test Name          | Result |
|--------------------|--------|
| Advertising        | failed |
| CheckSDRefDom      | passed |
| CheckSDRefDom      | passed |
| CheckSDRefDom      | passed |
| CheckSDRefDom      | passed |
| CheckSDRefDom      | passed |
| Connectivity       | passed |
| CrossRefValidation | passed |
| CrossRefValidation | passed |
| CrossRefValidation | passed |
| DFSREvent          | failed |
| FrsEvent           | passed |
| Intersite          | passed |
| KccEvent           | failed |
| KnowsOfRoleHolders | passed |
| LocatorCheck       | failed |
| MachineAccount     | passed |
| NCSecDesc          | failed |
| NetLogons          | failed |
| ObjectsReplicated  | passed |
| Replications       | failed |
| RidManager         | passed |
| Services           | passed |
| SystemLog          | failed |
| SysVolCheck        | failed |
| VerifyReferences   | passed |

Table 101 - Domain Controller DCDiag - DC-UIA-01V

### 1.2.3.11.8 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 |
| DFS Replication                  | DFSR       | Running |
| DHCP Server                      | DHCPServer | Running |
| DNS Server                       | DNS        | Running |
| Intersite Messaging              | Ismserv    | Running |



| Display Name                     | Short Name | Status  |
|----------------------------------|------------|---------|
| Kerberos Key Distribution Center | Kdc        | Running |
| NetLogon                         | Netlogon   | Running |
| Windows Time                     | W32Time    | Running |

Table 102 - Infrastructure Services Status - DC-UIA-01V

### 1.2.3.11.9 Sites Replication Connection

The following section provides detailed information about Site Replication Connection.

#### DC-UIA-01V

|                                 |  |
|---------------------------------|--|
| GUID                            | f1926927-cf11-4b5c-a070-3a1151f7c1e2   |
| 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<br>DC=ForestDnsZones,DC=pharmax,DC=local<br>CN=Schema,CN=Configuration,DC=pharmax,DC=local<br>CN=Configuration,DC=pharmax,DC=local |
| Transport Protocol              | IP   |
| AutoGenerated                   | Yes  |
| Enabled                         | Yes  |
| Created                         | Thu, 01 Sep 2022 12:01:59 GMT  |

Table 103 - 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<br>DC=ForestDnsZones,DC=pharmax,DC=local<br>CN=Schema,CN=Configuration,DC=pharmax,DC=local<br>CN=Configuration,DC=pharmax,DC=local |
| Transport Protocol              | IP   |
| AutoGenerated                   | Yes  |
| Enabled                         | Yes  |
| Created                         | Wed, 11 May 2022 17:57:17 GMT  |

Table 104 - 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<br>DC=ForestDnsZones,DC=pharmax,DC=local<br>CN=Schema,CN=Configuration,DC=pharmax,DC=local<br>CN=Configuration,DC=pharmax,DC=local |
| Transport Protocol              | IP   |

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

Table 105 - Site Replication - DC-UIA-01V

## 1.2.3.11.10 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      | SERVER-DC-01V | Pharmax-HQ      | 2022-08-31 21:14:31 | 5                   | 2022-09-04 17:46:00 | 89                 |
| DC-UIA-01V      | ACADE-DC-01V  | ACAD            | 2022-08-31 21:14:31 | 5                   | 2022-09-04 17:46:00 | 89                 |
| DC-UIA-01V      | SERVER-DC-01V | Pharmax-HQ      | 2022-08-31 21:14:31 | 5                   | 2022-09-04 17:46:00 | 89                 |
| DC-UIA-01V      | ACADE-DC-01V  | ACAD            | 2022-08-31 21:14:31 | 5                   | 2022-09-04 17:46:00 | 89                 |
| DC-UIA-01V      | SERVER-DC-01V | Pharmax-HQ      | 2022-08-31 21:14:31 | 1256                | 2022-09-04 17:46:00 | 89                 |
| DC-UIA-01V      | ACADE-DC-01V  | ACAD            | 2022-08-31 21:14:31 | 1256                | 2022-09-04 17:46:00 | 89                 |
| DC-UIA-01V      | SERVER-DC-01V | Pharmax-HQ      | 2022-08-31 21:14:31 | 1256                | 2022-09-04 17:46:00 | 89                 |
| DC-UIA-01V      | ACADE-DC-01V  | ACAD            | 2022-08-31 21:14:31 | 1256                | 2022-09-04 17:46:00 | 89                 |
| DC-UIA-01V      | SERVER-DC-01V | Pharmax-HQ      | 2022-08-31 21:14:31 | 1256                | 2022-09-04 17:46:00 | 89                 |
| DC-UIA-01V      | ACADE-DC-01V  | ACAD            | 2022-08-31 21:14:31 | 1256                | 2022-09-04 17:46:00 | 89                 |

Table 106 - Site Replication Status - UIA.LOCAL

**Health Check:**

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

## 1.2.3.11.11 Group Policy Objects Summary

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

| GPO Name                          | GPO Status           | Owner             |
|-----------------------------------|----------------------|-------------------|
| Default Domain Controllers Policy | All Settings Enabled | UIA\Domain Admins |
| Default Domain Policy             | All Settings Enabled | UIA\Domain Admins |

Table 107 - GPO - UIA.LOCAL

## 1.2.3.11.11.1 Central Store Repository

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

Table 108 - GPO Central Store - UIA.LOCAL

**Health Check:****Best Practices: Ensure Central Store is deployed to centralized GPO repository.****1.2.3.11.12 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        | -                                 |
| 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                  | -                                 |

Microsoft AD As Built Report - v1.0

| Name            | Path                                | Linked GPO |
|-----------------|-------------------------------------|------------|
| 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            | -          |
| 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          | -          |

Microsoft AD As Built Report - v1.0

| Name            | Path                                 | Linked GPO |
|-----------------|--------------------------------------|------------|
| 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            | -          |
| 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          | -          |

Microsoft AD As Built Report - v1.0

| Name            | Path                                 | Linked GPO |
|-----------------|--------------------------------------|------------|
| 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                 | -          |
| 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 | -          |

Microsoft AD As Built Report - v1.0

| Name            | Path                                 | Linked GPO |
|-----------------|--------------------------------------|------------|
| 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          | -          |
| 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 109 - 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 110 - 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 111 - 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 | 3          |

*Table 112 - 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 113 - 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 114 - 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 115 - 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<br>10.0.0.138 | 3/s     | Yes           | Yes           |

Table 116 - 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. | 198.41.0.4   |
| b.root-servers.net. | 199.9.14.201 |

| Name                | IP Address     |
|---------------------|----------------|
| 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 117 - Root Hints - PHARMAX.LOCAL

## CAYEY-DC-01V

| Name                | IP Address     |
|---------------------|----------------|
| a.root-servers.net. | 198.41.0.4     |
| 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 118 - 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 119 - 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     |

| Zone Name            | Zone Type | Replication Scope | Dynamic Update | DS Integrated | Read Only | Signed |
|----------------------|-----------|-------------------|----------------|---------------|-----------|--------|
| uia.local            | Stub      | Domain            | -              | Yes           | No        | -      |
| zenprsolutions.local | Stub      | Domain            | -              | Yes           | No        | -      |

Table 120 - 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 121 - 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 122 - 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 123 - Zones - PHARMAX.LOCAL

## 1.3.1.2.4 Conditional Forwarder

| Zone Name          | Zone Type | Replication Scope | Master Servers | DS Integrated |
|--------------------|-----------|-------------------|----------------|---------------|
| zenprsolutions.gov | Forwarder | Domain            | 8.8.8.8        | Yes           |

Table 124 - 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         | Sun, 11 Sep 2022 19:00:00 GMT |
| pharmax.local        | Yes           | 7.00:00:00       | 7.00:00:00         | Sun, 11 Sep 2022 19:00:00 GMT |
| TrustAnchors         | Yes           | 7.00:00:00       | 7.00:00:00         | Sun, 11 Sep 2022 19:00:00 GMT |

Table 125 - 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 126 - 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 127 - 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     |
| 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 128 - 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 129 - 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 130 - 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 131 - 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 132 - 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 133 - 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 134 - 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 135 - 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 136 - 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. | 198.41.0.4         |
| 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 137 - 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 138 - Zone Scope Recursion - ACAD.PHARMAX.LOCAL

## 1.3.2.2 ACAD-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 139 - 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,<br>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 140 - 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 141 - 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 142 - 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 143 - 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<br>172.23.7.1 |

Table 144 - 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 145 - 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 146 - 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 147 - 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 148 - 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 149 - 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. | 201:503:ba3e::2:30 |
| b.root-servers.net. | 201:500:200::b     |
| c.root-servers.net. | 201:500:2::c       |
| d.root-servers.net. | 201:500:2d::d      |
| e.root-servers.net. | 201:500:a8::e      |
| f.root-servers.net. | 201:500:2f::f      |

## Microsoft AD As Built Report - v1.0

| Name                | IP Address         |
|---------------------|--------------------|
| 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 150 - 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 151 - 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 152 - 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 153 - 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 154 - 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 155 - 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 156 - 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 157 - 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            | 220              | 1898                | 10                | 90                   |

Table 158 - 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<br>192.168.5.1 | -           |

Table 159 - 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 160 - 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 |

# Microsoft AD As Built Report - v1.0

| Scope Id        | Scope Name            | Scope Range                    | Lease Duration | State  |
|-----------------|-----------------------|--------------------------------|----------------|--------|
| 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 161 - 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   | 241     | 0         | 0                 | 0           |
| 10.10.33.0   | 210     | 4         | 2                 | 3           |
| 10.10.34.0   | 244     | 0         | 0                 | 0           |
| 10.10.35.0   | 244     | 0         | 0                 | 0           |
| 192.168.10.0 | 244     | 0         | 0                 | 0           |
| 192.168.12.0 | 226     | 5         | 2                 | 3           |
| 192.168.2.0  | 243     | 1         | 0                 | 0           |
| 192.168.4.0  | 11      | 0         | 0                 | 0           |
| 192.168.6.0  | 227     | 4         | 2                 | 2           |
| 192.168.7.0  | 8       | 206       | 96                | 17          |

Table 162 - 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 163 - 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 | -           |

| Name  | Option Id | Value        | Policy Name |
|---|-----------|--------------|-------------|
| 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 164 - 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 165 - 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 166 - 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 167 - IPv4 Scopes Options - 10.10.33.0

##### 10.10.34.0

Microsoft AD As Built Report - v1.0

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

Table 168 - IPv4 Scopes Options - 10.10.34.0

10.10.35.0

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

Table 169 - 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 170 - IPv4 Scopes Options - 192.168.2.0

192.168.4.0

| Name            | Option Id | Value         | Policy Name |
|-----------------|-----------|---------------|-------------|
| Router          | 3         | 192.168.4.254 | -           |
| DNS Domain Name | 15        | pharmax.local | -           |
| Lease           | 51        | 691200        | -           |

Table 171 - 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 172 - 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-<br>hardwired | -           |
|                       | 81        | 23                              | -           |

Table 173 - 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<br>192.168.5.1 | -           |
| DNS Domain Name | 15        | pharmax.local              | -           |
| Lease           | 51        | 691200                     | -           |

Table 174 - 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 175 - 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 176 - 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 177 - 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 178 - DHCP Servers Database - ACAD.PHARMAX.LOCAL

#### 1.4.2.1.2 Dynamic DNS credentials

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

Table 179 - 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 180 - 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 181 - 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 182 - IPv4 Scope Statistics - ACADE-DC-01V

## 1.4.2.2.2 IPv4 Network Interface Binding

| Interface Alias | IP Address | Subnet Mask   | State   |
|-----------------|------------|---------------|---------|
| Ethernet0       | 172.23.4.1 | 255.255.255.0 | Enabled |

Table 183 - 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<br>192.168.5.1<br>10.10.33.1 | -           |
| DNS Domain Name | 15        | acad.pharmax.local                      | -           |

Table 184 - 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 185 - IPv4 Scopes DNS Setting - acad-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 186 - 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 187 - 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 188 - 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 189 - 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 190 - 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 191 - 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 192 - 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 193 - 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 194 - DHCP Servers Database - UIA.LOCAL*

##### 1.4.3.1.2 Dynamic DNS credentials

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

*Table 195 - 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 196 - 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 197 - 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 198 - 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 199 - 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<br>192.168.5.1 | -           |

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

Table 200 - 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 201 - 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 202 - 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]<br>0F6D4D3B8C71290E76B6B6C0661275F6F37B9CE0 |
| Status | Running  |

Table 203 - 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    | acad-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 204 - 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 205 - Enterprise Subordinate CA - pharmax-CAYEY-DC-01V-CA

### 1.5.3 Certificate Validity Period

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

| CA Name                  | Server Name   | Validity Period |
|--------------------------|---------------|-----------------|
| acad-ACADE-DC-01V-CA     | ACADE-DC-01V  | 2 Years         |
| pharmax-CAYEY-DC-01V-CA  | CAYEY-DC-01V  | 2 Years         |
| pharmax-SERVER-DC-01V-CA | SERVER-DC-01V | 2 Years         |

Table 206 - Certificate Validity Period - PHARMAX.LOCAL

### 1.5.3.1 Access Control List (ACL)

| DC Name                  | Owner                  | Group                  |
|--------------------------|------------------------|------------------------|
| acad-ACADE-DC-01V-CA     | BUILTIN\Administrators | BUILTIN\Administrators |
| pharmax-CAYEY-DC-01V-CA  | BUILTIN\Administrators | BUILTIN\Administrators |
| pharmax-SERVER-DC-01V-CA | BUILTIN\Administrators | BUILTIN\Administrators |

Table 207 - Access Control List - PHARMAX.LOCAL

#### 1.5.3.1.1 pharmax-SERVER-DC-01V-CA 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 208 - ACL Rights - pharmax-SERVER-DC-01V-CA

#### 1.5.3.1.2 acad-ACADE-DC-01V-CA 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 209 - ACL Rights - acad-ACADE-DC-01V-CA

#### 1.5.3.1.3 pharmax-CAYEY-DC-01V-CA 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 210 - ACL Rights - pharmax-CAYEY-DC-01V-CA

## 1.5.4 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 211 - Cryptography Configuration - PHARMAX.LOCAL

|                               |   |
|-------------------------------|---|
| 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 212 - Cryptography Configuration - PHARMAX.LOCAL

|                               |   |
|-------------------------------|---|
| 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 213 - Cryptography Configuration - PHARMAX.LOCAL

### 1.5.5 Authority Information Access (AIA)

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

#### 1.5.5.1 pharmax-SERVER-DC-01V-CA

|                      |   |
|----------------------|---|
| 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 214 - 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><CAObject Class> |

|                      |      |
|----------------------|------|
| Flags                | 1, 2 |
| Server Publish       | Yes  |
| Include To Extension | Yes  |
| OCSP                 | No   |

Table 215 - 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 216 - 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 217 - Authority Information Access - pharmax-SERVER-DC-01V-CA

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

Table 218 - Authority Information Access - pharmax-SERVER-DC-01V-CA

#### 1.5.5.2 acad-ACADE-DC-01V-CA

|                      |  |
|----------------------|--|
| 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 219 - 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><CAObject Class> |
| Flags                | 1, 2  |
| Server Publish       | Yes   |
| Include To Extension | Yes   |
| OCSP                 | No  |

Table 220 - 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 221 - 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 222 - Authority Information Access - acad-ACADE-DC-01V-CA

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

Table 223 - Authority Information Access - acad-ACADE-DC-01V-CA

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

Table 224 - Authority Information Access - acad-ACADE-DC-01V-CA

### 1.5.5.3 pharmax-CAYEY-DC-01V-CA

|         |  |
|---------|--|
| 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 225 - 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><CAObject Class> |
| Flags                | 1, 2  |
| Server Publish       | Yes   |
| Include To Extension | Yes   |
| OCSP                 | No  |

Table 226 - 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 227 - 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 228 - Authority Information Access - pharmax-CAYEY-DC-01V-CA

## 1.5.6 Certificate Revocation List (CRL)

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

### 1.5.6.1 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         |
| pharmax-CAYEY-DC-01V-CA  | 1 Weeks  | 0 Hours          | 1 Days    | 0 Minutes         |
| pharmax-SERVER-DC-01V-CA | 50 Weeks | 0 Hours          | 0 Days    | 0 Minutes         |

Table 229 - CRL Validity Period - PHARMAX.LOCAL

### 1.5.6.2 CRL Flags Settings

| CA Name                  | Server Name   | CRL Flags         |
|--------------------------|---------------|-------------------|
| acad-ACADE-DC-01V-CA     | ACADE-DC-01V  | DeleteExpiredCRLs |
| pharmax-CAYEY-DC-01V-CA  | CAYEY-DC-01V  | DeleteExpiredCRLs |
| pharmax-SERVER-DC-01V-CA | SERVER-DC-01V | DeleteExpiredCRLs |

Table 230 - CRL Flags - PHARMAX.LOCAL

### 1.5.6.3 CRL Distribution Point

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

#### 1.5.6.3.1 pharmax-SERVER-DC-01V-CA

|                      |   |
|----------------------|---|
| 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<br>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 231 - 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 232 - 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<br>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 233 - 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<br>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 234 - 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 235 - CRL Distribution Point - pharmax-SERVER-DC-01V-CA

## 1.5.6.3.2 acad-ACADE-DC-01V-CA

|                      |   |
|----------------------|---|
| 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<br>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 236 - 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 237 - 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<br>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 238 - 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<br>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 239 - CRL Distribution Point - acad-ACADE-DC-01V-CA

|                      |  |
|----------------------|--|
| Reg URI              | 6:http://acad-dc-01v.acad.pharmax.local/CertEnroll/%3%8%9.crl  |
| Config URI           | 6:http://acad-dc-01v.acad.pharmax.local/CertEnroll/<CaName><CRLNameSuffix><DeltaCRLAllowed>.crl  |
| Url Scheme           | HTTP   |
| ProjectedURI         | 6:http://acad-dc-01v.acad.pharmax.local/CertEnroll/acad-ACADE-DC-01V-CA.crl 6:http://acad-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 240 - CRL Distribution Point - acad-ACADE-DC-01V-CA

## 1.5.6.3.3 pharmax-CAYEY-DC-01V-CA

|                   |   |
|-------------------|---|
| 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<br>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 241 - 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><CDPObjctClass>  |
| 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 242 - 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<br>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 243 - 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<br>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 244 - CRL Distribution Point - pharmax-CAYEY-DC-01V-CA

### 1.5.7 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  |
| pharmax-CAYEY-DC-01V-CA  | pharmax-CAYEY-DC-01V-CA<br>pharmax-SERVER-DC-01V-CA | Error  |
| pharmax-SERVER-DC-01V-CA | pharmax-SERVER-DC-01V-CA                            | Error  |

Table 245 - Certification Authority Health - PHARMAX.LOCAL

### 1.5.8 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.

#### 1.5.8.1 pharmax-SERVER-DC-01V-CA

| 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            |
| 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             |

| Template Name         | Schema Version | Supported CA                           | Autoenrollment |
|-----------------------|----------------|--|----------------|
| 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 246 - Issued Certificate Template - pharmax-SERVER-DC-01V-CA

### 1.5.8.2 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             |
| 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            |

| Template Name                       | Schema Version | Supported CA                           | Autoenrollment |
|-------------------------------------|----------------|--|----------------|
| 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             |
| 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 247 - Certificate Template in AD - PHARMAX.LOCAL

### 1.5.9 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.

#### 1.5.9.1 acad-ACADE-DC-01V-CA

| 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             |

| Template Name                       | Schema Version | Supported CA                           | Autoenrollment |
|-------------------------------------|----------------|--|----------------|
| 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 248 - Issued Certificate Template - acad-ACADE-DC-01V-CA

### 1.5.9.2 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             |
| 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             |

| Template Name                       | Schema Version | Supported CA                           | Autoenrollment |
|-------------------------------------|----------------|--|----------------|
| 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             |
| 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 249 - Certificate Template in AD - PHARMAX.LOCAL

### 1.5.10 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.

#### 1.5.10.1 pharmax-CAYEY-DC-01V-CA

| Template Name | Schema Version | Supported CA        | Autoenrollment |
|---------------|----------------|---------------------|----------------|
| Administrator | 1              | Windows 2000 Server | No             |

| Template Name                       | Schema Version | Supported CA                           | Autoenrollment |
|-------------------------------------|----------------|--|----------------|
| 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            |
| Subordinate Certification Authority | 1              | Windows 2000 Server                    | No             |
| User                                | 1              | Windows 2000 Server                    | No             |
| Web Server                          | 1              | Windows 2000 Server                    | No             |

Table 250 - Issued Certificate Template - pharmax-CAYEY-DC-01V-CA

### 1.5.10.2 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             |
| 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             |

| Template Name                       | Schema Version | Supported CA                           | Autoenrollment |
|-------------------------------------|----------------|--|----------------|
| 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             |
| 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 251 - Certificate Template in AD - PHARMAX.LOCAL

### 1.5.11 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, |



Microsoft AD As Built Report - v1.0

|  |  |
|--|--|
|  | DC=pharmax, DC=local [Serial Number]<br>61000001068FABBB1D8B7B986A000000000106 [Not<br>Before] 11/16/2021 8:11:55 PM [Not After] 11/16/2023<br>8:11:55 PM [Thumbprint]<br>0C65947128A94A0209907127D13F81AD5840CA37 |
|--|--|

*Table 252 - Key Recovery Agent Certificate - pharmax-SERVER-DC-01V-CA*

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

*Table 253 - Key Recovery Agent Certificate - acad-ACADE-DC-01V-CA*