****

**Yildirim Teknoloji – tfz.local**  
Active Directory Server

Sağlık Taraması Dokümanı

@Yildirim Teknoloji

Güncelleme Tablosu

|  |  |  |  |
| --- | --- | --- | --- |
| Sürüm | Tarih | Düzenleyen | Not |
| 1.0 |  |  | Doküman başlangıcı |
| 1.1 |  |  | Doküman taslağı tamamlandı |
| 1.2 |  |  | Doküman tamamlandı |
|  |  |  |  |

Kuruma Özeldir

İçindekiler

[1. Giriş 1](#_Toc59788845)

[1.1 Çalışmanın Amacı 1](#_Toc59788846)

[1.2 Active Directory Genel Sağlık Durumu 1](#_Toc59788847)

[1.3 Bulguların Özeti 2](#_Toc59788848)

[2. Active Directory Yapısı ve Mevcut Durum 3](#_Toc59788849)

[2.1 Active Directory Objeler 3](#_Toc59788850)

[2.2 Active Directory Site yapısı Raporu 3](#_Toc59788851)

[2.3 Active Directory Domain Controllers Raporu 3](#_Toc59788852)

[2.4 Active Directory DC Kritik Açıklar Raporu 3](#_Toc59788853)

[2.5 Active Directory Geçici Hesapların Raporu 3](#_Toc59788854)

[2.6 Active Directory Computers Description Raporu 3](#_Toc59788855)

[2.7 Domain controller üzerine kurulu 3th party servislerin listesi 3](#_Toc59788856)

[2.8 Yeni eklenen ve değiştirilmiş GPO’ler Raporu 3](#_Toc59788857)

[2.9 Active Directory CA Raporu 3](#_Toc59788858)

[2.10 Active Directory DC Windows Update 4](#_Toc59788859)

[2.11 Active Directory DC’lerin event log inceleme Raporu 4](#_Toc59788860)

[3. Active Directory Bulgular ve Öneriler 4](#_Toc59788861)

[3.1 Bulgular 4](#_Toc59788862)

[3.2 Active Directory Sonuç ve Ek Öneriler 5](#_Toc59788863)

# Giriş

## Çalışmanın Amacı

Bu doküman ile Yildirim Teknoloji Sistem takımının yönetiminde olana Active Directory altyapısının incelenmesi ile sağlık durumu hakkında bilgi vermesi amaçlanmıştır. “tfz.local” Active Directory mimarisi incelenerek sistemin genel sağlığı, performansı ve güvenliği perspektifinden Aylık olarak raporlanacaktır.

## Active Directory Genel Sağlık Durumu

Active Directory altyapısına ait genel sağlık durumu tabloda görülmektedir.

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Servis / Sağlık Durumu** | **Sistem** | **Yazılım** | **Yapılandırma** | **Süreklilik** | **Güvenlik** |
| **Active Directory “tfz.local”** | **Sağlıklı** | **Sağlıklı** | **Uyarı** | **Uyarı** | **Uyarı** |

Aşağıda her bir durumun ne anlama geldiği görülebilir

|  |  |
| --- | --- |
| **Sağlık Durumu** | **Açıklama** |
| **Sağlıklı** | Sistemin durumunun sağlıklı olduğunu belirtir. |
| **Uyarı** | Sistemin sağlık durumunun iyi olduğu fakat bazı uyarıların olduğunu belirtir. |
| **Kritik** | Sistemin sağlık durumunun kritik bir durumda olduğunu belirtir. |

## Bulguların Özeti

### Active Directory Özeti

# Active Directory Yapısı ve Mevcut Durum

## Active Directory Objeler

Haftalık eklenen user,Group,OU bulunmamaktadır.

## Active Directory Site yapısı Raporu

Haftalık eklenen site ve subnet bulunmamaktadır

Ekte Mevcuttur.

## Active Directory Domain Controllers Raporu

Disk Durumu

Server : SRUS005ADCVP03

OS : Microsoft Windows Server 2019 Standard

Drive : C:

Free Disk : 77

Total Disk : 99

Last Boot : 09-23-2020

Uptime/Day : 103

Socket : 1

Core : 4

Free VRam : 1.4

Free Ram : 0.1

Total Ram : 4

Server : SRUS005ADCVP04

OS : Microsoft Windows Server 2019 Standard

Drive : C:

Free Disk : 82

Total Disk : 99

Last Boot : 09-23-2020

Uptime/Day : 103

Socket : 1

Core : 4

Free VRam : 1.6

Free Ram : 0.9

Total Ram : 4

## Active Directory DC Kritik Açıklar Raporu

Haftalık CVE databaseleri üzerinden güvenlik açıkları listelenmelidir.

## Active Directory Geçici Hesapların Raporu

Haftalık oluşturulmuş Test user,computer hesapları ve Test veya POC OU bulunmamaktadır.

## Active Directory Computers Description Raporu

name whenCreated description

---- ----------- -----------

CRUS005D0084 12/4/2020 1:39:22 PM

CRUS005D0044 12/8/2020 9:48:45 AM

CRUS005D0008 12/8/2020 10:09:17 AM

CRUS005D0018 12/8/2020 1:58:15 PM

CRUS005D0094 12/8/2020 2:32:45 PM

CRUS005D0012 12/8/2020 3:29:28 PM

CRUS005D0098 12/8/2020 4:05:50 PM

CRUS005L0014 12/9/2020 8:45:20 AM

CRUS005D0061 12/9/2020 11:17:37 AM

CRUS005D0009 12/9/2020 1:28:02 PM

CRUS005D0085 12/9/2020 2:44:56 PM

CRUS005L0002 12/9/2020 3:13:40 PM

CRUS005D0110 12/10/2020 11:42:20 AM

CRUS005D0039 12/10/2020 1:41:51 PM

CRUS005D0104 12/11/2020 1:48:44 PM

CRUS005D0095 12/11/2020 2:04:59 PM

CRUS005D0030 12/11/2020 3:04:48 PM

CRUS005D0117 12/14/2020 12:15:20 PM

CRUS005D0076 12/16/2020 3:01:02 PM

CRUS005D0089 12/16/2020 3:08:05 PM

CRUS005D0057 12/17/2020 2:32:39 PM

CRUS005D0001 12/18/2020 2:17:25 PM

CRUS005D0037 12/21/2020 2:35:55 PM

CRUS005L0006 12/22/2020 11:44:49 AM

CRUS005D0050 12/22/2020 2:22:56 PM

CRUS005L0015 12/22/2020 4:43:40 PM

CRUS005D0073 12/23/2020 8:24:08 AM

CRUS005D0004 12/23/2020 9:04:20 AM

CRUS005D0113 12/23/2020 10:09:06 AM

CRUS005L0016 12/23/2020 1:16:20 PM

CRUS005L0017 12/23/2020 1:39:12 PM

CRUS005L0018 12/23/2020 1:58:57 PM

CRUS005L0019 12/23/2020 2:18:39 PM

CRUS005L0020 12/23/2020 2:47:17 PM

CRUS005L0010 12/24/2020 2:03:44 PM

CRUS005D0119 12/25/2020 12:16:48 PM

CRUS005D0048 12/25/2020 2:25:50 PM

CRUS005D0020 12/29/2020 9:35:56 AM

CRUS005D0021 12/29/2020 11:08:50 AM

CRUS005L0008 12/29/2020 11:12:26 AM

CRUS005D0046 12/29/2020 12:11:38 PM

CRUS005D0086 12/29/2020 1:14:59 PM

## Domain controller üzerine kurulu 3th party servislerin listesi

name vendor PSComputerName

---- ------ --------------

McAfee Endpoint Security Threat Prevention McAfee, LLC. SRUS005ADCVP03

McAfee Agent McAfee, Inc. SRUS005ADCVP03

McAfee Endpoint Security Adaptive Threat Protection McAfee, LLC. SRUS005ADCVP03

McAfee Active Response McAfee, LLC SRUS005ADCVP03

McAfee Endpoint Security Platform McAfee, LLC. SRUS005ADCVP03

McAfee Data Exchange Layer for MA McAfee LLC SRUS005ADCVP03

VMware Tools VMware, Inc. SRUS005ADCVP03

name vendor PSComputerName

---- ------ --------------

McAfee Endpoint Security Threat Prevention McAfee, LLC. SRUS005ADCVP04

McAfee Agent McAfee, Inc. SRUS005ADCVP04

McAfee Endpoint Security Adaptive Threat Protection McAfee, LLC. SRUS005ADCVP04

McAfee Active Response McAfee, LLC SRUS005ADCVP04

McAfee Endpoint Security Platform McAfee, LLC. SRUS005ADCVP04

McAfee Data Exchange Layer for MA McAfee LLC SRUS005ADCVP04

VMware Tools VMware, Inc. SRUS005ADCVP04

## Yeni eklenen ve değiştirilmiş GPO’ler Raporu

Son 1 ay içinde GPO üzerinde herhangi bir değişiklik yapılmamıştır.

## Active Directory CA Raporu

**SRUS005ADCVP03 – Expire olanlar**

DnsNameList NotAfter NotBefore

----------- -------- --------- --------------

12/31/1999 2:59:59 AM 5/13/1997 8:12:59 PM

12/31/1999 2:59:59 AM 5/13/1997 8:12:59 PM

{Microsoft Authenticode(tm) Root Authority} 1/1/2000 2:59:59 AM 1/1/1995 11:00:01 AM

{Microsoft Authenticode(tm) Root Authority} 1/1/2000 2:59:59 AM 1/1/1995 11:00:01 AM

{Microsoft Windows Hardware Compatibility} 12/31/2002 10:00:00 AM 10/1/1997 11:00:00 AM

{Microsoft Windows Hardware Compatibility} 12/31/2002 10:00:00 AM 10/1/1997 11:00:00 AM

1/8/2004 2:59:59 AM 5/12/1997 4:00:00 AM

1/8/2004 2:59:59 AM 5/12/1997 4:00:00 AM

10/25/2016 2:59:59 AM 4/17/1997 4:00:00 AM

10/25/2016 2:59:59 AM 4/17/1997 4:00:00 AM

{Token Signing Public Key} 7/2/2018 12:10:37 AM 7/3/2013 1:10:37 AM

{Microsoft Corporation} 8/11/2018 11:20:24 PM 8/11/2017 11:20:24 PM

{Microsoft Corporation} 8/11/2018 11:20:24 PM 8/11/2017 11:20:24 PM

{VeriSign Class 3 Code Signing 2010 CA} 2/8/2020 2:59:59 AM 2/8/2010 3:00:00 AM

{VeriSign Class 3 Code Signing 2010 CA} 2/8/2020 2:59:59 AM 2/8/2010 3:00:00 AM

{AddTrust External CA Root} 5/30/2020 1:48:38 PM 5/30/2000 2:48:38 PM

{AddTrust External CA Root} 5/30/2020 1:48:38 PM 5/30/2000 2:48:38 PM

{AddTrust External CA Root} 5/30/2020 1:48:38 PM 5/30/2000 2:48:38 PM

{AddTrust External CA Root} 5/30/2020 1:48:38 PM 5/30/2000 2:48:38 PM

{Microsoft Root Authority} 12/31/2020 10:00:00 AM 1/10/1997 10:00:00 AM

{Microsoft Root Authority} 12/31/2020 10:00:00 AM 1/10/1997 10:00:00 AM

{Microsoft Test Root Authority} 12/31/2020 10:00:00 AM 1/10/1999 10:00:00 AM

{Thawte Timestamping CA} 1/1/2021 2:59:59 AM 1/1/1997 3:00:00 AM

{Thawte Timestamping CA} 1/1/2021 2:59:59 AM 1/1/1997 3:00:00 AM

**SRUS005ADCVP03 – Expire olacaklar**

DnsNameList NotAfter NotBefore

----------- -------- ---------

{SRUS005ADCVP03.tfz.local} 3/2/2021 3:24:18 PM 8/31/2020 3:24:18 PM

{Token Signing Public Key} 5/8/2021 11:40:55 PM 5/9/2016 11:40:55 PM

{Microsoft Root Certificate Authority} 5/10/2021 2:28:13 AM 5/10/2001 3:19:22 AM

{Microsoft Root Certificate Authority} 5/10/2021 2:28:13 AM 5/10/2001 3:19:22 AM

{GlobalSign} 12/15/2021 11:00:00 AM 12/15/2006 11:00:00 AM

{GlobalSign} 12/15/2021 11:00:00 AM 12/15/2006 11:00:00 AM

{GlobalSign} 12/15/2021 11:00:00 AM 12/15/2006 11:00:00 AM

{GlobalSign} 12/15/2021 11:00:00 AM 12/15/2006 11:00:00 AM

**SRUS005ADCVP04 – Expire olanlar**

DnsNameList NotAfter NotBefore

----------- -------- ---------

12/31/1999 2:59:59 AM 5/13/1997 8:12:59 PM

12/31/1999 2:59:59 AM 5/13/1997 8:12:59 PM

{Microsoft Authenticode(tm) Root Authority} 1/1/2000 2:59:59 AM 1/1/1995 11:00:01 AM

{Microsoft Authenticode(tm) Root Authority} 1/1/2000 2:59:59 AM 1/1/1995 11:00:01 AM

{Microsoft Windows Hardware Compatibility} 12/31/2002 10:00:00 AM 10/1/1997 11:00:00 AM

{Microsoft Windows Hardware Compatibility} 12/31/2002 10:00:00 AM 10/1/1997 11:00:00 AM

1/8/2004 2:59:59 AM 5/12/1997 4:00:00 AM

1/8/2004 2:59:59 AM 5/12/1997 4:00:00 AM

10/25/2016 2:59:59 AM 4/17/1997 4:00:00 AM

10/25/2016 2:59:59 AM 4/17/1997 4:00:00 AM

{Token Signing Public Key} 7/2/2018 12:10:37 AM 7/3/2013 1:10:37 AM

{VeriSign Class 3 Code Signing 2010 CA} 2/8/2020 2:59:59 AM 2/8/2010 3:00:00 AM

{VeriSign Class 3 Code Signing 2010 CA} 2/8/2020 2:59:59 AM 2/8/2010 3:00:00 AM

{AddTrust External CA Root} 5/30/2020 1:48:38 PM 5/30/2000 2:48:38 PM

{AddTrust External CA Root} 5/30/2020 1:48:38 PM 5/30/2000 2:48:38 PM

{AddTrust External CA Root} 5/30/2020 1:48:38 PM 5/30/2000 2:48:38 PM

{AddTrust External CA Root} 5/30/2020 1:48:38 PM 5/30/2000 2:48:38 PM

{Microsoft Test Root Authority} 12/31/2020 10:00:00 AM 1/10/1999 10:00:00 AM

{Microsoft Root Authority} 12/31/2020 10:00:00 AM 1/10/1997 10:00:00 AM

{Microsoft Root Authority} 12/31/2020 10:00:00 AM 1/10/1997 10:00:00 AM

{Thawte Timestamping CA} 1/1/2021 2:59:59 AM 1/1/1997 3:00:00 AM

{Thawte Timestamping CA} 1/1/2021 2:59:59 AM 1/1/1997 3:00:00 AM

**SRUS005ADCVP04 – Expire olacaklar**

DnsNameList NotAfter NotBefore

----------- -------- ---------

{SRUS005ADCVP04.tfz.local} 3/2/2021 3:21:14 PM 8/31/2020 3:21:14 PM

{Token Signing Public Key} 5/8/2021 11:40:55 PM 5/9/2016 11:40:55 PM

{Microsoft Root Certificate Authority} 5/10/2021 2:28:13 AM 5/10/2001 3:19:22 AM

{Microsoft Root Certificate Authority} 5/10/2021 2:28:13 AM 5/10/2001 3:19:22 AM

{GlobalSign} 12/15/2021 11:00:00 AM 12/15/2006 11:00:00 AM

{GlobalSign} 12/15/2021 11:00:00 AM 12/15/2006 11:00:00 AM

{GlobalSign} 12/15/2021 11:00:00 AM 12/15/2006 11:00:00 AM

{GlobalSign} 12/15/2021 11:00:00 AM 12/15/2006 11:00:00 AM

## Active Directory DC Windows Update

Aylık DC’lerin Security ve critical patch gereksinim listesini içermelidir.

PSComputerName Description HotFixID InstalledOn

-------------- ----------- -------- -----------

SRUS005ADCVP03 Security Update KB4512577 9/7/2019 12:00:00 AM

SRUS005ADCVP03 Security Update KB4523204 2/28/2020 12:00:00 AM

SRUS005ADCVP03 Security Update KB4537759 2/28/2020 12:00:00 AM

SRUS005ADCVP03 Security Update KB4549947 4/21/2020 12:00:00 AM

SRUS005ADCVP03 Security Update KB4549949 4/21/2020 12:00:00 AM

PSComputerName Description HotFixID InstalledOn

-------------- ----------- -------- -----------

SRUS005ADCVP04 Security Update KB4512577 9/7/2019 12:00:00 AM

SRUS005ADCVP04 Security Update KB4523204 2/28/2020 12:00:00 AM

SRUS005ADCVP04 Security Update KB4537759 2/28/2020 12:00:00 AM

SRUS005ADCVP04 Security Update KB4549947 4/21/2020 12:00:00 AM

SRUS005ADCVP04 Security Update KB4549949 4/21/2020 12:00:00 AM

## Active Directory DC’lerin event log inceleme Raporu

**SRUS005ADCVP03**

**Error** - Session "SensorFramework-{d61722cd-d3ce-0897-1694-d917cab88c2a}" failed to start with the following error: 0xC0000035

**Warning** - The DFS Replication service is stopping communication with partner SRUS005ADCVP04 for replication group Domain System Volume due to an error. The service will retry the connection periodically.

**Warning** - Windows Management Instrumentation has stopped WMIPRVSE.EXE because a quota reached a warning value. Quota: HandleCount Value: 4102 Maximum value: 4096 WMIPRVSE PID: 30960 Providers hosted in this process: %systemroot%\system32\wbem\cimwin32.dll, %SystemRoot%\system32\tscfgwmi.dll, %systemroot%\system32\wbem\ntevt.dll, %SystemRoot%\system32\wbem\policman.dll

**Warning** - The maximum file size for session "NetCfgTrace" has been reached. As a result, events might be lost (not logged) to file "C:\Windows\Logs\NetSetup\service.0.etl". The maximum files size is currently set to 5242880 bytes.

**SRUS005ADCVP04**

**Error** – The DFS Replication service failed to register the WMI providers. Replication is disabled until the problem is resolved.

Additional Information:

Error: 2147749902 (100e)

**Error** - The DFS Replication service failed to communicate with partner CONTROLLER1 for replication group Domain System Volume. This error can occur if the host is unreachable, or if the DFS Replication service is not running on the server.

Partner DNS Address: controller1.tfz.local

Optional data if available:

Partner WINS Address: controller1

Partner IP Address: 10.31.100.110

The service will retry the connection periodically.

Additional Information:

Error: 1722 (The RPC server is unavailable.)

Connection ID: 50B0CDDB-471D-4968-B5A1-11A0103DF095

Replication Group ID: BA93AF3E-48A7-47DC-A194-82CF6EA0B524

# Active Directory Bulgular ve Öneriler

## Bulgular

Organizasyonundaki Active Directory Mimarisine ait Bulgular aşağıdaki gibidir.

### Bulgu 1

|  |  |
| --- | --- |
| **Bulgu** | GPO üzerinde Enforce password history 0 değerindedir |
| **Önem derecesi** | **Orta** |
| **Etkisi** | Güvenlik açığı yaratabilir |
| **Düzeltici aksiyon** | GPO üzerinden en az 3 olarak düzeltilmelidir |

### Bulgu 2

|  |  |
| --- | --- |
| **Bulgu** | GPO üzerinde windows updateler için 4 - Auto download and schedule the install işaretlidir. |
| **Önem derecesi** | **Düşük** |
| **Etkisi** | Test edilmediği için PC ler üzerinde sorun yaşanabilir. |
| **Düzeltici aksiyon** | Default Domain Controller Policy’si üzerinde yükleme seçeneği kulanıcıya verilmelidir. |

## Active Directory Sonuç ve Ek Öneriler

* Genel olarak Active Directory Servisleri hata almadan çalışmaktadır.