

epati

Active Directory - Kerberos SSO Entegrasyonu

Ürün: Antikor v2 - Yeni Nesil Güvenlik Duvarı
Yapılandırma Örnekleri

Active Directory - Kerberos SSO Entegrasyonu

Kerberos, ağ üzerinde iletişim gerçekleştiren kaynakların kimliklerini ispatlamak için geliştirilmiş kimlik doğrulama protokolüdür. SSO (Single Sign On), tek bir kullanıcı kimliği ile oturum açma işlemi gerçekleştirilerek erişim sağlamaktadır.

Active Directory Tarafında Yapılması Gerekenler

1. Domain Controller makinesinde DNS sunucuya A kaydı oluşturulmalıdır.

Name	Type	Data	Timestamp
(same as parent folder)	Start of Authority (SOA)	[57], epatitest.sunucu.local...	static
(same as parent folder)	Name Server (NS)	epatitest.sunucu.local.	static
(same as parent folder)	Host (A)	192.168.100.10	6.05.2019 13:00:00
antikor	Host (A)	192.168.100.10	static
epatitest	Host (A)	192.168.100.10	static
testlocal	Host (A)	192.168.100.100	22.04.2019 16:00:00

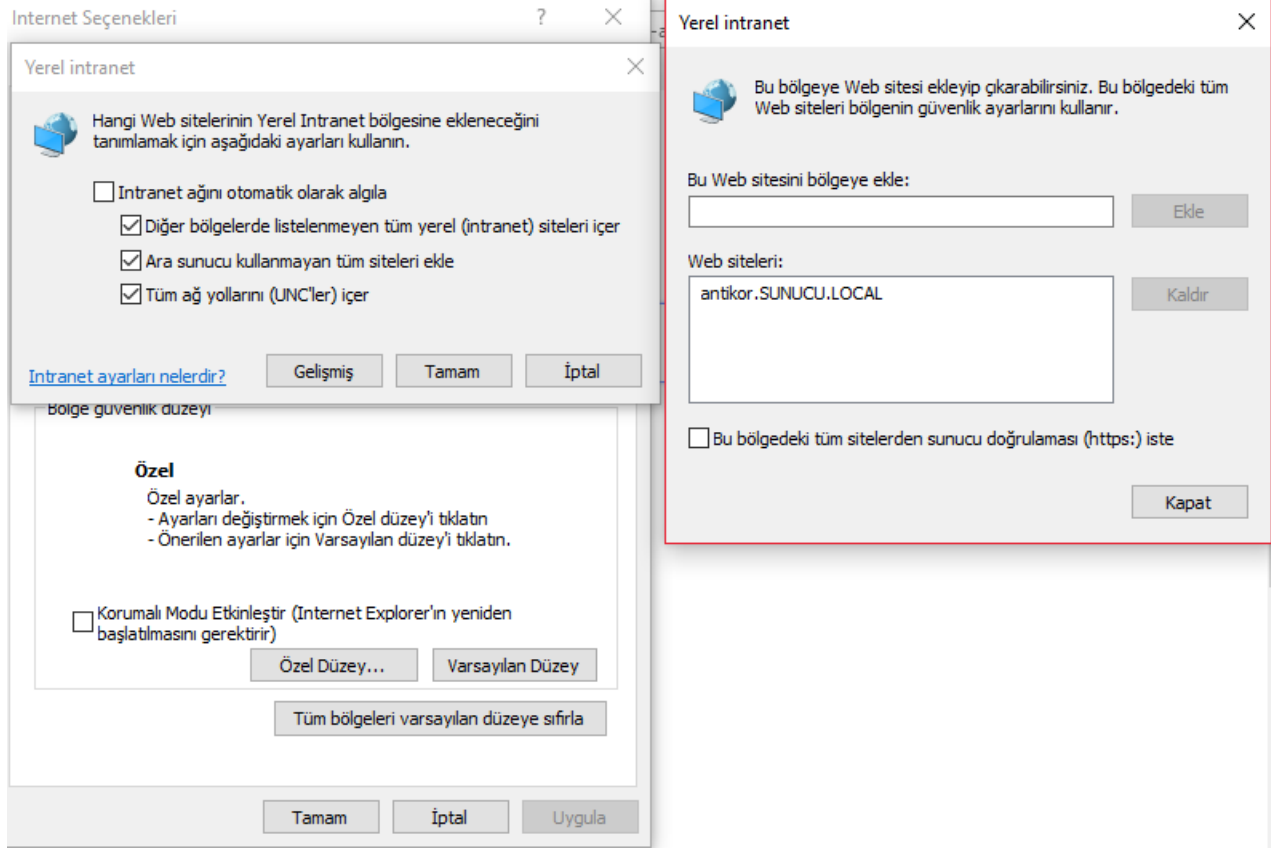
2. DC makinesinde antikor adında user oluşturulmalıdır.

Name	Type	Description
Administrator	User	Built-in account for ad...
Allowed RODC Password Replication Group	Security Group...	Members in this group c...
Cert Publishers	Security Group...	Members of this group ...
Cloneable Domain Controllers	Security Group...	Members of this group t...
DefaultAccount	User	A user account manage...
Denied RODC Password Replication Group	Security Group...	Members in this group c...
DnsAdmins	Security Group...	DNS Administrators Gro...
DnsUpdateProxy	Security Group...	DNS clients who are per...
Domain Admins	Security Group...	Designated administrato...
Domain Computers	Security Group...	All workstations and ser...
Domain Controllers	Security Group...	All domain controllers i...
Domain Guests	Security Group...	All domain guests
Domain Users	Security Group...	All domain users
Enterprise Admins	Security Group...	Designated administrato...
Enterprise Key Admins	Security Group...	Members of this group ...
Enterprise Read-only Domain Controllers	Security Group...	Members in this group ...
Group Policy Creator Owners	Security Group...	Members in this group c...
Guest	User	Built-in account for gue...
Key Admins	Security Group...	Members of this group ...
Protected Users	Security Group...	Members of this group ...
RAS and IAS Servers	Security Group...	Servers in this group can...
Read-only Domain Controllers	Security Group...	Members of this group ...
Schema Admins	Security Group...	Designated administrato...
test	User	

3. Yönetici olarak CMD açılarak aşağıdaki komut ile keytab dosyası oluşturulmalıdır.

```
ktpass -princ HTTP/antikor.SUNUCU.LOCAL@SUNUCU.LOCAL -mapuser antikor@SUNUCU.LOCAL -crypto al  
-ptype KRB5_NT_PRINCIPAL -pass SIFRE -out antikor.krb.keytab
```

4. Internet Explorer > Güvenlik > Yerel Intranet > Siteler > Gelişmiş penceresinde antikor.SUNUCU.LOCAL yazılmalıdır.



5. Group Policy ayarları ile Antikor SSL sertifikası tüm istemcilere dağıtılmalıdır.

To add trusted sites using a GPO (Group Policy Objects), Launch Active Directory Users and Computers (ADUC), right click on the domain the clients are in, select Properties > Group Policy > New, type in a name for the GPO (like "IE Security Settings") and then select Edit > User Configuration > Windows Settings > Internet Explorer Maintenance > Security > Security Zones and Content Ratings. Select Import the current security zones and privacy settings > Modify Settings > Trusted Sites > Sites and add your Plexcel protected websites just as you would on a client. Then wait for the policy to propagate throughout the domain.

Antikor Tarafında Yapılması Gerekenler

1. Antikor Domain Tanımları sayfasında SUNUCU.LOCAL kaydı oluşturulur.

Domain Tanımları - Kayıt Düzeltme

Durum

Aktif

Alan Adı

sunucu.local

DNS Sunucusu

IPv4

10.2.2.50

İptal

Kaydet

2. Kimlik Sağlayıcı Tanımları sayfasında Sağlayıcı Türü SSO: Negotiate/Kerberos - Active Directory seçilerek kayıt girilir.

Kimlik Sağlayıcı Tanımları - Kayıt Düzeltme ×

Durum Aktif ☐

Sağlayıcı Türü SSO: Negotiate/Kerberos - Active Directory ▼

Domain Controller / Kerberos Key Distribution Center ile saat uyumsuzluğu halinde Tek Oturum Açma (SSO) başarısız olabilir. Lütfen Tarih Saat Ayarları menüsünden NTP senkronizasyonu yapıldığından emin olun.

Etki Alanı SUNUCU.LOCAL

KDC / DC DNS Adı dc.SUNUCU.LOCAL

Antikora atanmış DNS Adı antikor.SUNUCU.LOCAL

İptal Kaydet

3. Oluşturulan Keytab dosyası Yükle butonu aracılığıyla yüklenecektir. Kök Sertifika butonu, Doğrulama Kuralları sayfasında “Tek Oturum Açma SSO” seçeneği aktif edilmesi halinde görülecektir.

2	Aktif	SSO: Negotiate/Kerberos - Active Directory	SUNUCU.LOCAL	Düzenle	Sil	Yükle	Kök Sertifika
---	-------	--	--------------	----------------------	------------------	--------------------	----------------------------

Keytab dosyası yüklendiğinde aşağıdaki gibi bilgiler görülecektir;

Kerberos Keytab ×

Yükle Kerberos SSO Test

```
/antikor/etc/kerberos/krb_6.keytab:
Vno  Type                Principal                                Aliases
7    des-cbc-crc          HTTP/antikor.SUNUCU.LOCAL@SUNUCU.LOCAL
7    des-cbc-md5          HTTP/antikor.SUNUCU.LOCAL@SUNUCU.LOCAL
7    arcfour-hmac-md5     HTTP/antikor.SUNUCU.LOCAL@SUNUCU.LOCAL
7    aes256-cts-hmac-sha1-96 HTTP/antikor.SUNUCU.LOCAL@SUNUCU.LOCAL
7    aes128-cts-hmac-sha1-96 HTTP/antikor.SUNUCU.LOCAL@SUNUCU.LOCAL
```

Kerberos SSO Test butonu ile test işlemi gerçekleştirilebilir.

4. Bütün adımlar gerçekleştirildikten sonra oturum açma işlemi başarı ile gerçekleştirilecektir.

Antikor Tarafında Dikkat Edilmesi Gerekenler

1. NTP Sunucu ayarı yapılmalıdır.

02.07.2019

09:07 10

Otomatik Al

Ayar

Saat Dilimleri

Seçiniz...

Güncelle

NTP Sunucular

Yenile

+Ekle

XLS CSV PDF

Filtrele

Temizle

#	Durum	Sunucu Adresi	İşlemler
1	Aktif	0.tr.pool.ntp.org	Düzenle Sil Güncelle
2	Aktif	1.tr.pool.ntp.org	Düzenle Sil Güncelle

< 1 >

#	Kimlik Bilgileri	Kullanıcı Adı	İşlem Adı	İşlem Zamanı
1	Antikor Admin	admin	Ekleme	2019-07-02 11:58:57+00
2	Antikor Admin	admin	Ekleme	2019-07-02 11:58:48+00
3	Antikor Admin	admin	Silme	2019-07-02 11:58:04+00
4	Antikor Admin	admin	Ekleme	2019-07-02 11:57:59+00
5	Antikor Admin	admin	Güncelleme	2019-07-02 08:57:41.930586+00

2. Doğrulama Kuralları sayfasında Hotspot sekmesinde Tek Oturum Açma SSO özelliği aktif edilmelidir.

Doğrulama Kuralları

Hotspot Proxy Kayıt Servisi L2TP / PPTP VPN SSL VPN RADIUS İstemci Değişikliği Formu

Network

Tümü

0

✓

Tek Oturum Açma SSO

Seçiniz...

1

□

Mernis

3. Domain Sunucu, İstemci ve Antikor için tarih/saat ayarları aynı olmalıdır.

4. SSO doğrulama yapılmak istenen IP adresleri veya IP blokları Hotspot İstemcileri sayfasına eklenmelidir.

ePati Siber Güvenlik Teknolojileri A.Ş.

Mersin Üniversitesi Çiftlikköy Kampüsü

Teknopark İdari Binası Kat: 4 No: 411

Posta Kodu: 33343 Yenişehir / MERSİN

www.epati.com.tr

bilgi@epati.com.tr

+90 324 361 02 33

+90 324 361 02 39

