epati

Hotspot SSO:Negotiate Kerberos - Active Directory Yapılandırması

Ürün: Antikor v2 - Yeni Nesil Güvenlik Duvarı

Yapılandırma Örnekleri

www.epati.com.tr

ераті



Hotspot SSO:Negotiate Kerberos - Active Directory Yapılandırması

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.

횳 DNS Manager						
File Action View Help						
🗢 🄿 🖄 📷 🗙 🗊 🗟 🛛	7 🖬 🕺 🗐 🖓					
 DNS DNS Forward Lookup Zones antikor.local path.local hotspotlocalad yabanci.local meverse Lookup Zones Conditional Forwarders 	Name msdcs sites tcp udp com DomainDnsZones ForestDnsZones ForestDnsZones f	Type Start of Authority (SO Name Server (NS) Host (A) Host (A) Host (A)	Data [35], epatitest.hotspot.local epatitest.hotspot.local.ad. 192.168.58.11 192.168.58.11 192.168.58.11	Timestamp static static 30.04.2022 21:00:00 static static	antikor Properties ? × Hott (A) Security Hott (A) Security Hott (A) Fittle Fully qualified domain name (FQDN): artikor/hottpot/local ad IP address: 192.168.58.1 192.168.58.1 Update associated pointer (PTR) record	

2. DC makinesinde antikor adında user oluşturulmalıdır.

Active Directory Users and Computers			- U X
File Action View Help			
🗢 🔿 🙍 💼 📋 📾 🧟 🕞 🛛 🖬 🗏 📚 🖆 🍞 🧕	Se .		
Active Directory Users and Com Saved Queries Mew Object - User Builtin Computers Domain Controllers ForeignSecurityPrincipal:	Type ot local.ad/Users	Description X for administering the c group can have their p	^
 Managed Service Accour personel Users Last name: antikor Full name: antikor User logon name: 	Initials:	group are permitted to group that are domain nanaged by the system. group cannot have the ors Group are permitted to perfor nistrators of the domain	
antikor	@hotspot.local.ad	 and servers joined to t 	
User logon name (pre-Window	s 2000):	ollers in the domain	
HOTSPOT	antikor		
a Guest Key Admins	< Back Next > User Security Group - Global	nistrators of the enterp group can perform ad group are Read-Only group can modify gro Built-in account for guest access to the Members of this group can perform ad	
< >> Retmon Users	Security Group - Domain Local	Netmon Users can capture network traf	¥

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

ktpass -princ HTTP/antikor.hotspot.local@hotspot.local -mapuser antikor@hotspot.LOCAL	-crypto
ll -ptype KRB5_NT_PRINCIPAL -pass SIFRE -out antikor.krb.keytab	

4. Internet Explorer > Güvenlik > Yerel Intranet > Siteler > Gelişmiş penceresinde antikor.hotspot.local yazılmalıdır.

Internet Options ?	? ×	
Local intranet	×	Local intranet X
Use the settings below to define which websites are include the local intranet zone.	ed in	You can add and remove websites from this zone. All websites in this zone will use the zone's security settings.
Automatically detect intranet network Indude all local (intranet) sites not listed in other zor Indude all sites that bypass the proxy server Indude all network paths (UNCs)	nes	Add this website to the zone: http:// Add Websites:
What are intranet settings? Advanced OK Security level for this zone Allowed levels for this zone: All -	Cancel	Require server verification (https:) for all sites in this zone
- Same as Medium level without prompts Enable Protected Mode (requires restarting Internet Explo Custom level Default le Reset all zones to default le	evel	
OK Cancel	Apply	

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 hotspot.local.ad kaydı oluşturulur.

Aktif	
hotspot.local.ad	
IPv4 192.168.58.11	
	Aktif hotspot.local.ad IPv4 192.168.58.11

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 / Ker Oturum Açma (SSO) baş senkronizasyonu yapıld	beros Key Distribution Center ile saat uyuşmazlığı halinde Te sarısız olabilir. Lütfen Tarih Saat Ayarları menüsünden NTP ığından emin olun.	k			
Etki Alanı	HOTSPOT.LOCAL.AD				
KDC / DC DNS Adı	epatitest.HOTSPOT.LOCAL.AD				
Antikora atanan DNS Adı	antikor.HOTSPOT.LOCAL.AD				
	Ø İptal 🛛 🖺 Kayd	let			

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	HOTSPOT.LOCAL.AD	C Düzenle	💼 Sil	🛓 Yükle	📥 Kök Sertifi

Keytab dosyası yüklendiğinde aşağıdaki gibi bilgiler görülecektir;

±	Yükle		✓ Kerberos SSO Test
/anti	ikor/etc/kerberos/krb_Win	R52N_RHLJ.keytab:	
Vno	Туре	Principal	Aliases
69	des-cbc-crc	HTTP/antikor.HOTSPOT.LOCAL.AD@HOTSPOT.LOCAL.AD	
69	des-cbc-md5	HTTP/antikor.HOTSPOT.LOCAL.AD@HOTSPOT.LOCAL.AD	
69	arcfour-hmac-md5	HTTP/antikor.HOTSPOT.LOCAL.AD@HOTSPOT.LOCAL.AD	
69	aes256-cts-hmac-sha1-96	HTTP/antikor.HOTSPOT.LOCAL.AD@HOTSPOT.LOCAL.AD	

Not: Kerberos SSO Test butonu ile test işlemi gerçekleştirilebilir.

4. Doğrulama kuralları Hotspot sekmesinde sağlayıcı olarak SSO:Negotiate Kerberos - Active Directory seçilir.

Vetwork	xy Kayıt Servisi							
Vetwork		LZTP7 PPTP VPN SSL VPN	RADIUS İstemci Değişikliği	Formu				
	Tümü	٣						
0	V Tek Oturum Açma 5	so Seçiniz	Ŧ					
1	✓ Mernis							
2	SMS							
3	IP Bil	gi mesajı					🖺 Kaydet	
4	Sağlayıcılar	SSO: Negotiate/Kerberos - Activ 🔻						
	## Adı	Etki Alanı	Kullanımda	>	Adı Sağ	ayıcı Türü	Etki Alanı	İşlemler
ma Kuralları								
ma Kuralları ətspot Pro	oxy Kayıt Servisi	LZTP / PPTP VPN SSL VPN	RADIUS İstemci Değişikliği	Formu				
na Kuralları otspot Pro	oxy Køyıt Servîsî Tûmû	L2TP / PPTP VPN SSL VPN	RADIUS İstemci Değişikliği	Formu				
otspot Pro	oxy Kayıt Servisi Tümü ✓ Tek Oturum Açma S	LZTP / PPTP VPN SSL VPN * 50 Seçiniz	RADIUS İstemci Değişikliği	Formu				
ma Kuralları otspot Pro Network	oxy Kayıt Servisi Tümü ✓ Tek Oturum Açma Sı ✓ Mernis	LZTP / PPTP VPN SSL VPN	RADIUS İstemci Değişikliği	Formu				
ma Kuralları otspot Pro Network	axy Kayıt Servisi Tümü Tak Oturum Açma S Mernis SMS	SO Seçiniz	RADIUS İstemci Değişikliği	Formu				
ma Kuralları otspot Pro Network	ary Kayıt Servisi Tümü ✓ Tek Oturum Açma S ✓ Mernis SMS	LZTP / PPTP VPN SSL VPN	RADIUS İstemci Değişikliği	Formu			B kaydet	
ma Kuralları otspot Pro Network	oxy Kayıt Servisi Tümü ✓ Tek Oturum Açma S ✓ Mernis SMS IP Bil Sağlayıcılar	LZTP / PPTP VPN SSL VPN	RADIUS İstemci Değişikliği	Formu			B kaydet	

ogrulama Kurallari								-
Hotspot Prov	cy Kayıt Servisi	L2TP / PPTP VPN SSL V	PN RADIUS İstemci Değişikliği f	ormu				
Network	Tümü		*					
٥	✓ Tek Oturum Açm	na SSO HOTSPOT	LOCAL.AD Y					
۵	✓ Mernis							
2	SMS							
3	IP	Bilgi mesajı				n 2	aydet	
4	Sağlayıcılar	SSO: Negotiate/Kerberos - Activ	, v					
	## Adı	Etki Alanı HOTSPOT.LOCAL.AD	Kullanımda Evet	*	Adı s	Sağlayıcı Türü SSO: Negotiate/Kerberos - Active Directory	Etki Alanı HOTSPOT.LOCAL.AD	İşlemler

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

Antikor Tarafında Dikkat Edilmesi Gerekenler

1. NTP Sunucu ayarı yapılmalıdır.

	04.05	.2020	NTP Sunucula	ir	_			2 Yenile
			XLS C	SV PDF	⊞G	öster/Gizle - Sayfa Başı Kayıt Sayısı	Tamam Tiltrele	🥒 Filtreyi T
	16:3	1 29 +3	# D	urum 🕸	Sunucu Adresi	Jî İşlemler		
Otomatik Al	Akter		1 Ai	ttif	192.168.58.11	🕼 Düzenle 📄 🖬 🖉 Senkro	nize Et	
Saat Dilimleri	+3	v						
	С Каз	ydet				« < 1 > »		
#	Kimlik Bilgileri	J↑ Kullanıcı Ad	i ti	şlem Adı	τ	İşlem Zamanı	17	
1	Antikor Admin	admin		Güncelleme		2020-04-30 23:44:35.292484+03		
2	Antikor Admin	admin		Güncelleme		2020-04-30 23:44:25.333333+03		
3	Antikor Admin	admin		Güncelleme		2020-04-30 23:44:21.104845+03		
4	Antikor Admin	admin		Güncelleme		2020-04-30 21:51:20.539566+03		
	Antikor Admin	admin		Güncelleme		2020-04-30 21:51:08.428983+03		

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

Do	ğrulama Kuralla	ari		^
	Hotspot	Proxy Kayıt Servisi L2TP / PPTP VPN SSL VPN	RADIUS İstemci Değişikliği Formu	
	Network	Tũmũ v		
	٥	Tek Oturum Açma SSO		

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

