用户更改证书服务模板有效期后使用BYOD快速部署工具时无法申请用户证书的处理办法?

BYOD 罗孝晨 2016-06-01 发表

用户更改证书服务模板以及用户证书模板有效期后使用BYOD快速部署工具时无法申请用户证书,并且 重启了CA SERVER



在CA SERVER直接访问<u>http://172.18.95.1/certsrv/mscep/mscep.dll/pkiclient.exe</u> 失败, Windows有告 警"Network Device Enrollment Service cannot started"

wes Web Sice Galery *	
S Detailed Error - 500.0 - Internal Server Error	Sin + 🖸 - 🗆 📾 + Page + Safety + 1
rver Error in Application "DE	FAULT WEB SITE/CERTSRV/MSCEP"
	Internet Information Service
Error Summary	
HTTP Error E00.0 Internal Corpus	r Error
HTTP Erfor 500.0 - Internal Serve	I EITOI
The page cannot be displayed because an	internal server error has occurred.
Detailed Error Information	
ModuleIsapiModule	Requested URLhttp://10.10.32.110:80/certsrv/mscep/mscep.dll/pkiclient.exe
ModuleIsapiModule NotificationExecuteRequestMandler	Requested URLhttp://10.10.32.110/80/certsrv/mscep/mscep.dll/pkiclient.exe Physical PathC:\Windows\system32\CertSrv\mscep\mscep.dll\pkiclient.exe
NotiveIsapiModule NotificationExecuteRequestMandler HandlerISAPI-dll	Requested Villahter//15.13.23.11080/certsv/mscep/mscep/ml/pkiclient.exe Physical Pat/S:\Windows\system32\CertSv/mscep\mscep\mscep.dll\pkiclient.exe Logon Metodasymmous
ModuleIsapiHodule NotificationExecuteRequestNandler HondlerISAPI-dll Error Codebx80070057	Reported (URIMING/IAB.33.21.1040/certers/inscep/inscep.dll/phichent.exe Physical Pat/C (Windows knythem31(CertSrv/inscep/inscep.dll/phichent.exe Logon Unit-Monoperature Logon Unit-Monoperature
ModuleSapiHodule Nofication ExerciseReguesElfandlier Hindle ESAFF-dil Ener Codebx80070057	Registed ULURIA (/ 16.3.2.3.1.100/certixi/imscog/imscog.dll/pik/climit.exe im/pip/lim/climites/states/states/states/states/imscog.dll/pik/climit.exe Login Methodologymene Login UserAssingenees
Holds Experiedade Indicator Exceeding input Handler Hondro: SAVF.edl Error Codebed0076657 Mint Marky Codebed076657 Itili Streament for mount in process on internal of the same state in the process on internal to the same state is the process configuration for the the same state is the process configuration for the Itili was not able to process configuration for the the Itili was not able to process configuration for the the Itili was not able to process configuration for the the Itili was not able to process configuration for the the	Requested URURING/16.1.3.2.1.100//certix/imrceg/imrceg.dll/pikclient.exe Physical Introl:Vimideen/exeten3/1 Certix/imrceg/imrceg.dll/pikclient.exe Logon Introl/Wimdeen Logon User/Attemption Logon User/Attemption User/Attem
Hodol Experiedade Nedication Executive/puestion Nedication Nedicat	Required ULURAPY/16.1.3.2.1.100/certory/mecog/mecog.dll/pikclient.exe Physical Dirtic/UltideAcomprises Logen MethodeAcomprises Logen MethodeAcomprises Logen List/Acomprises Logen List/Acomprises Physical Dirtic/List/Acomprises Physical Dirtic/List/Acomprise

	Active Directory Certificat	te Services Number of	fleventsi 303			
Custom Views	Number of events 30	8				
E Server Roles	Level	Date and Time			anatomin .	
Active Directory Doma	Error	5/27/2016 3:28:4	AS EM	NetworkD	weetrealm	10
T DHCP Server	Error	5/27/2016 3:28:	38 PM	NetworkD	eviceErrolm	
T DNS Server	Error	5/27/2016 3:28:	38 PM	Networks	evictivolm	
Web Server (LIS)	Error	5/27/2016 3:78	:06 PM	Network	evicetrola	10
Admissibative Events	Error	5/27/2016 3:28	1:06 PM	Network	Constanting the second	2
Windows Logs	Error	5/27/2016 3:15	1:48 PM	Network	Ontering	80
CH Security	O Error	5/27/2016 3:15	9:48 PM	Percentor	CA ILLEST CA	
Setup System	Event 2, NetworkDeviceE	nrollmentService				
Forwarded Events Forwarded	General Details	Enrollment Service ca	annot be started (0	s80004005). Umspi	cified error	
ONS Server Hardware Events Internet Explorer Key Management Servic Windows PowerShel Windows PowerShel One Server Shel Coconterpart + A	e chication Pools		-			
File Mene Mich						
The New Hep						
Start Page CACERTP 1 (CNCEICAlsysadmin)	Application Per This page lets you view and ma provide isolation among differen	ools mage the lat of application p int applications.	cools on the server. Appl	ution peak are associa		
Application Pools	Filter:	- All Go - Show Al	Group by: No Group			
H Sides	Name A	Status NET Frame	Managed Pipeli	Ser By		
	DefaultAcoPool	Started v2.0	Entery ated	And about soldering		
	OCSPISAPIADOPool	Started v2.0	Classic	Change A perpadent		
	SCEP	Started v2.0	Integrated	Apple abord tool don the		
and the state of the second	WSEnrolmentPolicyServer	Started V2.0	Integrated	CALLER PROPERTY.		
and the second se	WSEnrolmentServer	514 100				
a second and a second second second						
the second se						

一、通过对用户进行的操作进行分析,用户进行了如下操作:

In CA Server:

<complex-block>



le Action View Help				
🔿 📷 🗙 🗊 😼 🖬 🕯	1			
Certificate Templates (CACERTP1.c	Template Display Name Administrator	Minimum Supported CAs Version Intended Purposes Windows 2000 4.1		Actions Certificate Templat
	Authenticated Session Basic BFS Received and and and and and and and and and an	yodserver Properties ? × Superseded Templates Extensions Security Server		More Actions
	CA Exchange	General Request Handling Subject Name Issuance Requirements		byodserver More Actions
	Code Signing	1 griptiste display nome: byodserver		
	Cross Certification Authority	Minimum Supported CAa: Windows Server 2003 Enterprise		
	Domain Controller	I emplate name: Byodserver	milcation, Smart Card Logon	
	Enrolment Agent Enrolment Agent (Computer) Exchange Enrolment Agent (Offine reque	Validity period: Benewal period:		
	Exchange Signature Only Exchange User imdErvol	Bublish certificate in Active Directory	Authentication	
	IPSec (Offine request)	Denot automatically reenrol if a duplicate certificate exists in Active Directory	ntication, Smart Card Logon, KDC Authentic	
	at Key Recovery Agent COSP Response Signing RAS and IAS Server Root Certification Authority Root Certification Authority	For automatic renewal of amat card certificates, use the existing key If a new key cannot be created	ntication	
	Smartcard Logon			
	Trust List Signing	OK Cancel Apply Help		
	User Signature Only Web Server	Windows 2000 4.1 Windows 2000 4.1		



4、重启CA服务器

根据类似的处理经验,以及网页上报出"HTTP Error500.0"错误,怀疑是网络设备注册服务出现异常,导致无法申请证书。为了尽快解决问题,建议删除"网络设备注册服务"角色后重新添加该角色。删除该角色后不会丢失已申请的证书,但注册表中配置需要重新修改。

一、删除网络设备注册服务,并重新安装网络设备注册服务



二、打开注册表

位置为HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Cryptography\MECEP,将其中三个参数修 改为证书模板的模板名(图中的模板名为AppleEnroll,注意是模板名,不是模板显示名称,现场需要 根据实际模板名进行修改),然后再修改enforecepassword,将其值改为0.

板的属性				
服务器 】 常规	发布要求 请求处理	取代模板 2 加密	扩展	安全 使用者名称
【仮显示白術 AppleEnroll	1 0).			
最低支持的 0	A: Windows :	Server 2008 Ent	erprise	
糞 板名(T):				
AppleEnroll				
与效期 (V):		续订期(R):		
2 年	•	6 周	<u>-</u>	
▼ 在 Active	Directory F	中发布证书(P)		
「如果 A 注册 0	ctive Direct)	ory 中有一个重复	夏证书,:	不要自动重新
			In the short star is a	



1、在处理该问题时可以多参考网上的类似经验,网页上报出的500错误一般都是由于CA证书服务器异 常导致的,和iMC本身没有太大关系。现场按照指导方案修改之后可以正常申请用户证书。