Instalando o Active Directory Certificate Services (AD CS)

Breve descrição

Um servidor designado como autoridade de certificação (CA) é responsável por emitir certificados de infraestrutura de chave pública [PKI] e gerenciar listas de revogação de certificados (CRLs, Certificate Revogation Lists). Servidores que executam o Windows Server podem ser configurados como autoridades de certificação com a instalação do Serviços de Certificados do Active Directory [AD CS]. (Stanek, 2009, p. 191) Além de proteger o aplicativo e o tráfego HTTP, os certificados que o AD CS fornece podem ser usados para autenticação de contas de computador, usuário ou dispositivo em uma rede com base nos requisitos de segurança da infraestrutura. — Fonte: *eduardomozartdeoliveira.wordpress.com*

Passo 1

Abrir o Gerenciador de Servidor » Gerenciar » Adicionar Funções e Recursos



Passo 2

Selecionar tipo de instalação » Instalação baseada em função ou recurso



Passo 3

Selecionar o servidor de destino » **Selecionar um servidor no pool de servidor**

눰 Add Roles and Features Wiz	ard			-		×
Select destination	on server			DESTINA	TION SER\ ugainfo.lo	/ER ocal
Before You Begin Installation Type Server Selection	Select a server or a virtual Select a server from th Select a virtual hard di	hard disk on which t <mark>e server pool</mark> sk	o install roles and features.			
Server Roles Features Confirmation	Server Pool					
Results	Name (1997) Jugainfo.local	IP Address	Operating System Microsoft Windows Server 2019 S	itandard		

Passo 4

Selecionar Funções do Servidor » Active Directory Certificate Services

2024/05/24 12:59	3/8	Instalando o J	Active Directory C	ertificate S	Services	(AD CS)
눰 Add Roles and Features Wiz	ard			—		×
Select server ro	les			DESTINA	ITION SERV gugainfo.lo	/ER xcal
Before You Begin	Sele	ct one or more roles to install on the selected server.				
Installation Type	Role	5	Description			
Server Selection		Active Directory Certificate Services	Active Directo	ory Certifica	te Service	es
Server Roles		 Active Directory Domain Services (Installed) 	(AD CS) is used to create			
Features		Active Directory Federation Services	role services that allow you		ind relate ou to issu	.d Je
AD CS		Active Directory Rights Management Services	and manage (ertificates	used in a	
Role Services		Device Health Attestation	variety of app	lications.		

Passo 5

Avança até » Serviços de Função marcando "Certification Authority"

📥 Add Roles and Features Wizard		– 🗆 X
Select role service	2S	DESTINATION SERVER
Before You Begin	Select the role services to install for Active Directory Certification	te Services
Installation Type	Role services	Description
Server Selection	Certification Authority	Certification Authority (CA) is used
Server Roles	Certificate Enrollment Policy Web Service	to issue and manage certificates. Multiple CAs can be linked to form a
Features	Certificate Enrollment Web Service	public key infrastructure.
AD CS	Network Device Enrollment Service	
Role Services		

Passo 6

Avançar até concluir, não é necessário reiniciar o servidor.

Passo 7

Realizar configuração inicial para tornar o servidor uma autoridade certificadora. Será necessário credencial de um usuário com privilégios administrativos, clique em **ALTERAR** e entre com as credenciais.

📥 AD CS Configuration	- 🗆 X
Credentials	DESTINATION SERVER
Credentials Role Services	Specify credentials to configure role services
Confirmation	To install the following role services you must belong to the local Administrators group:
Progress	Standalone certification authority Cartification Authority Web Facelly and
Results	Online Responder
	To install the following role services you must belong to the Enterprise Admins group:
	Enterprise certification authority Certificate Enrollment Policy Web Service Certificate Enrollment Web Service Network Device Enrollment Service
	To install remotely you must enter credentials.
	Credentials: GUGAINFO\gustavo Change

Passo 8

Selecionar o serviço a configurar, marcar somente "Certification Authority"

📥 AD CS Configuration		—		×
Role Services		DESTINATI	ION SER Igainfo.lo	VER ocal
Credentials	Select Role Services to configure			
Role Services				
Setup Type	Certification Authority			
СА Туре	Certification Authority Web Enrollment			
Private Key	Network Device Enrollment Service			
Cryptography	Certificate Enrollment Web Service			
CA Name	Certificate Enrollment Policy Web Service			

Passo 9

Especificar o tipo de instalação da autoridade de certificação. Em nosso caso como será integrada ao AD escolheremos **AC Corporativa**

2024/05/24 12:59	i/8 Instalando o Active Directory Certificate Services (AD CS)		
📥 AD CS Configuration	- D ×		
Setup Type	DESTINATION SERVER		
Credentials Role Services	Specify the setup type of the CA		
Setup Type	Enterprise certification authorities (CAs) can use Active Directory Domain Services (AD DS) to		
СА Туре	simplify the management of certificates. Standalone CAs do not use AD DS to issue or manage certificates.		
Private Key	Enterprise CA		
Cryptography	Enterprise CAs must be domain members and are typically online to issue certificates or		
CA Name	certificate policies.		
Validity Period	○ Standalone CA		
Certificate Database	Standalone CAs can be members or a workgroup or domain. Standalone CAs do not require AD		
Confirmation	DS and can be used without a network connection (offline).		

Passo 10

2024/05/24 12:59

5/8

Especificar o tipo de autoridade de certificação como "AC Raiz"



Passo 11

Especificar o tipo da chave privada. Neste caso precisamos "Criar uma nova chave privada"

📥 AD CS Configuration	- 🗆 X
Private Key	DESTINATION SERVER
Credentials Role Services	Specify the type of the private key
Setup Type CA Type	To generate and issue certificates to clients, a certification authority (CA) must have a private key.
Private Key	Use this option if you do not have a private key or want to create a new private key.
Cryptography CA Name Validity Period Certificate Database Confirmation Progress Results	 Use existing private key Use this option to ensure continuity with previously issued certificates when reinstalling a CA. Select a certificate and use its associated private key Select this option if you have an existing certificate on this computer or if you want to import a certificate and use its associated private key. Select an existing private key on this computer Select this option if you have retained private keys from a previous installation or want to use a private key from an alternate source.

Passo 12

Especificar as opções criptográficas, podemos deixar o padrão e avançar.

📥 AD CS Configuration		- 🗆 X
Cryptography for	CA	DESTINATION SERVER
Credentials	Specify the cryptographic options	
Role Services		
Setup Type	Select a cryptographic provider:	Key length:
CA Type	RSA#Microsoft Software Key Storage Provider Y	2048 ~
Private Key	Select the bash algorithm for signing certificates issued by this CA:	_
Cryptography	SHA256	
CA Name	SHA384	
Validity Period	SHA512	
Certificate Database	SHA1	
Confirmation	MD5	
Progress	Allow administrator interaction when the private key is accessed	by the CA.

Passo 13

Especificar o nome da Autoridade de Certificação. Pode usar o padrão que já vem preenchido ou personalizar para facilitar a identificação. Caso decida personalizar o nome, alterar somente o campo

"Nome comum da autoridade de certificação. Os temais campos serão atualizados automaticamente.



Passo 14

Definir o período de validade dos certificados gerados para esta AC.



Passo 15

Avançar com as opções padrão até concluir e receber a mensagem de sucesso.



From: https://gugainfo.com.br/ - GugaInfo

Permanent link: https://gugainfo.com.br/doku.php?id=windows:win_server_2019:certificate_services

Last update: 2022/03/19 13:30

