JMS. Типовой сценарий развертывания (MSCA)

Версия ПО: JMS 2.x - 3.x

Токены: Любые

Проблема: Типовой сценарий развертывания для выпуска сертификатов на Microsoft CA

Решение:

1. Настройка УЦ МSCA.

1.1. Шаблон для оператора JMS.

Нажать на клавиатуре Win+R certsrv.msc. Откроется консоль MSCA

Необходимо зайти в управление шаблонами, на папке с шаблонами сертификатов нажать правой кнопкой мыши - "Управление / Manage":

📮 certsrv - [Ce	rtification Authority (Local)\test2-C	A1-CA\Certificate Templates] 🗕 🗖 🗙
File Action View Help		
🗢 🔿 🙍 🗟		
Certification Authority (Local) Lest2-CA1-CA Revoked Certificates Sisued Certificates Pending Requests Failed Requests Certificate New View Refresh Export Li Help	Name JMSOperator JMSUserTemplate Directory Email Replication Domain Controller Authentication S Authentication pvery Agent S Controller Ver st nate Certification Authority Administrator	Intended Purpose <all> Smart Card Logon Certificate Request Agent Directory Service Email Replication Client Authentication, Server Authentic Client Authentication, Server Authentic File Recovery Encrypting File System Client Authentication, Server Authentic Server Authentication Client Authentication, Server Authentic Server Authentication Client Authentication, Server Authentic Server Authentication, Server Authentic Client Authentication, Server Authentic Client Authentication, Server Authentic Client Authentication, Server Authentic Client Authentication, Server Faultentic Client Authentication, Server Authentic Client Authentication, Server Authentic Encrypting File System, Secure Email, Cl <all> Microsoft Trust List Signing, Encrypting</all></all>
Starts Certificate Templates snapin		

Откроется консоль управления шаблонами.

Найдите шаблон "Пользователь со смарт-картой", нажмите правой кнопкой мыши "Скопировать шаблон":

	Certificate Templates Console						
File Action View Help							
⇐ ➡ 🔲 🖬 📑 🖬							
Rertificate Templates (dc1.test2.	Template Display Name	Schema Version	Versi	Intended \land	Actions		
	Domain Controller Authentication	2	110.0	Client Au	Certificate Templates (dc 🔺		
	EFS Recovery Agent	1	6.1		Mars Artises		
	🗟 Enrollment Agent	1	4.1		More Actions 🔹		
	Enrollment Agent (Computer)	1	5.1		Smartcard User		
	Rxchange Enrollment Agent (Offline requ.	. 1	4.1		More Actions		
	Exchange Signature Only	1	6.1		More Actions		
	🗟 Exchange User	1	7.1				
	IPSec	1	8.1				
	IPSec (Offline request)	1	7.1				
	IMSOperator	2	100.2				
	IMSUserTemplate	2	6.2	Smart Car			
	Kerberos Authentication	2	110.0	Client Au			
	🚇 Key Recovery Agent	2	105.0	Key Recov			
	OCSP Response Signing	3	101.0	OCSP Sig			
	RAS and IAS Server	2	101.0	Client Au			
	Root Certification Authority	1	5.1	=			
	Router (Offline request)	1	4.1				
	🗷 Smartcard Logon	1	6.1				
	Smartcard User	o Tomplato	11.1				
	Subordinate Certification A	e rempiace	5.1				
	Trust List Signing All Tasks	; •	3.1				
	User Properti	ies	3.1				
	User Signature Only		4.1				
	Web Server		4.1				
	Workstation Authentication	2	101.0	Client Au 🗸			
< III >	<			>			
Using this template as a base, creates	a template that supports Windows Server 2003	Enterprise CAs					

Откроется окно настройки нового шаблона. Перейдите на вкладку **Основные** и задайте имя шаблона:

Properties of New Template							
Subject Name	Subject Name Server Issuance Requirements						
Superseded Templa	tes	Exte	nsions	Security			
Compatibility General	Request	Handling	Cryptography	Key Attestation			
Template display name:							
JMSOperator	2						
Template display name: IMSOperator Template name: JMSOperator Validity period: Renewal period: 1 years 6 weeks Publish certificate in Active Directory Do not automatically reenroll if a duplicate certificate exists in Active Directory Directory							
ок	(Cancel	Apply	Help			

Перейдите на вкладку **Имя субъекта**. Если у пользователя не предполагается наличия адреса Email в AD, уберите опции, указанные ниже:

Properties of New Template							
Supersed	led Templa	tes	nsions	Security			
Compatibility	General	Request	equest Handling Cryptography Key A				
Subject N	lame	Sen	/er	Issuance F	Requirements		
Supply in the request Use subject information from existing certificates for autoenrollment renewal requests (*)							
Build from	this Active	Directory	information	n			
Select this simplify ce	option to e rtificate adr	enforce co ministratior	nsistency a 1.	among subject i	names and to		
Subject na	ame format	:					
Fully disti	nguished n	ame			~		
Fully distinguished name ✓ Include e-mail name in subject name Include this information in alternate subject name: E-mail name DNS name ✓ User principal name (UPN) Service principal name (SPN)							
* Control is d	isabled due OK	to <u>compa</u>	atibility setti Cancel	ngs. Apply	Help		

1.2. Шаблон для выпуска сертификатов пользователям JMS.

Найдите шаблон "Пользователь со смарт-картой", нажмите правой кнопкой мыши "Скопировать шаблон":

	Certificate	e Templates Console			_ D X
File Action View Help					
◆ ⇒ 🖬 🗎 🗟 🖬					
Certificate Templates (dc1.test2.	Template Display Name	Schema Version	Versi	Intended ^	Actions
	Domain Controller Authentication	2	110.0	Client Au	Certificate Templates (dc 🔺
	🐵 EFS Recovery Agent	1	6.1		Certificate remplates (de
	🐵 Enrollment Agent	1	4.1		More Actions •
	🗵 Enrollment Agent (Computer)	1	5.1		Smartcard User
	🐵 Exchange Enrollment Agent (Offline requ	1	4.1		More Actions
	🚇 Exchange Signature Only	1	6.1		More Actions
	🗷 Exchange User	1	7.1		
	🗷 IPSec	1	8.1		
	IPSec (Offline request)	1	7.1		
	IMSOperator	2	100.2		
	IMSUserTemplate	2	6.2	Smart Ca	
	Rerberos Authentication	2	110.0	Client Au	
	🚇 Key Recovery Agent	2	105.0	Key Recov	
	Response Signing	3	101.0	OCSP Sig	
	RAS and IAS Server	2	101.0	Client Au	
	Root Certification Authority	1	5.1	=	
	Router (Offline request)	1	4.1		
	🗟 Smartcard Logon	1	6.1		
	Smartcard User	ta Tamalata	11.1		
	Bubordinate Certification A	ite i emplate	5.1		
	I Trust List Signing All Task	us ►	3.1		
	B User Proper	ties	3.1		
	User Signature Only		4.1		
	B Web Server		4.1		
	Reference Workstation Authentication	2	101.0	Client Au 🗸	
< III >	< 111			>	
Using this template as a base, creates	a template that supports Windows Server 200	3 Enterprise CAs			

Откроется окно настройки нового шаблона. Перейдите на вкладку Основные и задайте имя шаблона:

Properties of New Template								
Subject Name	Subject Name Server Issuance Requirements							
Superseded Templa	tes	Exte	nsions	Security				
Compatibility General	Request	Handling	Cryptography	Key Attestation				
Template display name:	Template display name:							
JMSOperator	2							
Template display name: IMSOperator Template name: JMSOperator Validity period: Renewal period: 1 years 6 weeks Publish certificate in Active Directory Do not automatically reenroll if a duplicate certificate exists in Active Directory								
ОК	(Cancel	Apply	Help				

Перейдите на вкладку **Имя субъекта**. Если у пользователя не предполагается наличия адреса Email в AD, уберите опции, указанные ниже:

Properties of New Template								
Superseded Templa	tes	Exte	ensions	Security				
Compatibility General	Request	Handling	Cryptograph	y Key Attestation				
Subject Name	Sen	ver	Issuance	Requirements				
Supply in the request Use subject information from existing certificates for autoenrollment renewal requests (*)								
Build from this Active	Directory	informatio	n					
Select this option to e simplify certificate adr	nforce co ninistratior	nsistency 1.	among subjec	t names and to				
Subject name format:								
Fully distinguished na	ame			~				
Include this information	on in alter ne (UPN) name (SPI	nate subjec N)	t name:					
*Control is disabled due ОК оейдите на вкладку Тре ке выберите из списка	e to <u>compa</u> (бования Полити	atibility sett Cancel н выдачи ка приме	ings. Аррlу н. Отметьте с енения и Се	Нер Нер опцию Количеств ортификат агента				

Pro	perties	of New	Template	e X
Superseded Templa	ites	Ext	ensions	Security
Compatibility General	Request	Handling	Cryptograpł	hy Key Attestation
Subject Name	Sen	ver	Issuance	e Requirements
Require the following fo	r enrollme	nt:		
CA certificate mana	ger approv	ral		
This number of auth	orized sign	natures:	1	
	onzoa olgi	lataros.	1	
If you require more	than one :	signature,	autoenrollmer	nt is not allowed.
Policy type required	in signatu	ire:		
Application policy				~
Application policy:				
Certificate Reques	t Agent			×
Issuance policies:				
				Add
				Remove
Require the following fo	r reenrollm	ent:		
 Same criteria as for 	enrollment			
O Valid existing certific	ate			
Allow key based	l renewal (5		
Requires subject in request.	formation t	o be provi	ded within the	e certificate
* Control is disabled du	e to <u>compa</u>	atibility set	tings.	
ОК	(Cancel	Apply	Help

Перейдите на вкладку **Безопасность**, нажмите **Добавить**, далее Типы объектов, оставьте только **Компьютеры**:

]		Certificate	e Templates	Console
Select Users, Comp	uters, Service Accounts	or Groups	x	
Select this object type:				~
Users, Groups, or Built-in security p	incipals	Object Types	plate	^
From this location:			ography	Key Attestation
test2.ru		Locations	suance F	Requirements
Enter the object names to select (ex	amples):			Security
		Check Name	s	
]				
Advanced	OF	Cancel		
			Add	Remove
	Object Types		x	Deny
Select the types of objects you wa	nt to find.			
Object to pass				
Built in security principals				
Service Accounts				
Computers				
				Advanced
-0				
		OK	0	Неір

Воспользуйтесь кнопкой **Дополнительно** и выберите свой сервер JMS. Установите ему полные права:

Properties of New Template							
Compatibility	General	Request	Handling	Cryptography	Key Attestation		
Subject N	lame	Sen	ver Issuance Requirements				
Supersec	ded Templa	tes	Exte	Extensions Security			
Group or use	rnames:						
Authenticated Users Administrator Common Admins (TEST2\Domain Admins) Common Admins (TEST2\Enterprise Admins) JMS1 (TEST2\JMS1\$)							
Permissions	for JMS1			Add	Remove Deny		
Full Contro	bl			✓			
Read				~			
Write				~			
Enroll				✓			
Autoenroll				✓			
For special p Advanced.	emissions	or advanc	ed setting:	s, click	Advanced		
[OK	(Cancel	Apply	Help		

Нажмите Применить и закройте окно.

1.3. Шаблон агента выпуска для сервера JMS.

Найдите шаблон "Агент регистрации (компьютер)", нажмите правой кнопкой мыши "Скопировать шаблон".

Откроется окно настройки нового шаблона. Перейдите на вкладку **Основные** и задайте имя шаблона.

Перейдите на вкладку **Безопасность**, нажмите **Добавить**, далее — Типы объектов, оставьте только **Компьютеры**:

Ð	Certifi	cate Templ	ates Console	
Select Users, Computers, Service	Accounts, or Groups	x		
Select this object type:				Y
Users, Groups, or Built-in security principals	Object T	ypes	ite l	
From this location:		ogr	aphy Key Attestat	tion
test2.ru	Locatio	ons	nce Requirements	[
Enter the object names to select (examples):		-	Security	
	Check N	lames		
Advanced	OK Car	ncel		
		Add	Remove	
Object T	ypes		X Deny	-
Select the types of objects you want to find.				
Object types:				
Service Accounts				
Computers				
			Advanced	
			avancea	- 1
	OK	Canool	Help	
	UK	Cancer		

Воспользуйтесь кнопкой **Дополнительно** и выберите свой сервер JMS. Установите ему полные права:

Prop	perties of	New	Template		x		
Compatibility General Subject Name	Request Ha	andling	Cryptography Issuance F	Key Attesta Requirements	tion		
Superseded Templa	tes	Exte	ensions	Security			
Group or user names:							
 Authenticated Users administrator Domain Admins (TEST2\Domain Admins) Enterprise Admins (TEST2\Enterprise Admins) IMS1 (TEST2\JMS1\$) 							
Permissions for JMS1			Add Allow	Remove Deny			
Full Control			~		ן ר		
Read			~				
Write			✓				
Enroll			\checkmark				
Autoenroll							
For special permissions of Advanced.	or advanced	setting	s, click	Advanced			
ОК	Car	ncel	Apply	Help			

Нажмите Применить и закройте окно.

1.4. Настройка доступа к MSCA.

В консоли MSCA поместите курсор на имя сервера, нажмите правой кнопкой мыши "Свойства":

ia)	certsrv	- [Certification Authority (Local)\test2-CA1	-CA]		
File Action View	Help				
🗢 🄿 🖄 🖾	🗟 🛛 🕨 🗖				
Certification Author	rity (Local) Name All Tasks View Refresh Export List Properties Help	oked Certificates led Certificates lding Requests ed Requests tificate Templates			
Opens the properties dialog box for the current selection.					

В открывшемся окне перейдите на вкладку **Безопасность**. Нажмите **Добавить** и выберите ваш сервер JMS.

Далее — Типы объектов, оставьте только Компьютеры:

Ð	Certifi	cate Templ	ates Console	
Select Users, Computers, Service	Accounts, or Groups	x		
Select this object type:				Y
Users, Groups, or Built-in security principals	Object T	ypes	ite l	
From this location:		ogr	aphy Key Attestat	tion
test2.ru	Locatio	ons	nce Requirements	[
Enter the object names to select (examples):		-	Security	
	Check N	lames		
Advanced	OK Car	ncel		
		Add	Remove	
Object T	ypes		X Deny	-
Select the types of objects you want to find.				
Object types:				
Service Accounts				
Computers				
			Advanced	
			avancea	- 1
	OK	Cancel	Help	
	UK	Cancer		

Дайте полные права серверу JMS:

te	est2-CA1-CA	A Prope	rties	? X
Extensions	Storage		Certificate Managers	
General	Policy Mo	dule	E	Exit Module
Enrollment Agents	Auditing	Recove	ery Agents	Security
Group or user names:				
& Authenticated Us	ers			
👗 JMS1\$				
🖓 Domain Admins (TEST2\Domain	Admins)		
Kenterprise Admins	(TEST2\Enterp	rise Admin	s)	
Administrators (C/	1\Administrators	5)		
		Ac	dd	Remove
Permissions for IMS1®			Allow	Denv
	Contificantes		 ✓ 	
Manage CA	centificates		 ▼ ▼ 	
Request Certificates			▼	
OK	Cance	el	Apply	Help

Нажмите Применить и закройте окно.

1.5. Добавление шаблонов в список выдаваемых.

В консоли сервера MSCA на папке шаблонов нажмите правой кнопкой мыши — "Новый" — "Выдаваемые шаблоны сертификатов".

<u>ت</u>	certsrv - [Cer	tificatio	on Authority (Local)\test2-CA	\1-CA\Certifi
File Action Vie	ew Help			
🗢 🔿 🖄 🙆	🔒 🛛			
🚋 Certification Au	thority (Local)	Name		Intended Purp
⊿ 🍶 test2-CA1-C	CA A	🖳 JMS	Operator	<all></all>
🧮 Revoked	l Certificates	🖳 JMSI	UserTemplate	Smart Card Lo
📔 Issued C	ertificates	🖳 Enro	llment Agent (Computer)	Certificate Req
📔 Pending	Requests	🚇 Dire	ctory Email Replication	Directory Servi
🧮 Failed Re	equests	🗵 Dom	Client Authent	
Certifica	Manage		eros Authentication	Client Authent
	New	۲	Certificate Template to Issue	ng File
	View	•	ain Controller	Client Authent
	Refresh		Server	Server Authent
	Evport List		puter	Client Authent
	Export List			Encrypting File
	Help		rdinate Certification Authority	<all></all>
Ľ		🗷 Adm	ninistrator	Microsoft Trus

Откроется окно с доступными шаблонами:

	Enable Certificate Templates					
S N ir A F	elect one Certificate Template to enable on thi lote: If a certificate template that was recently formation about this template has been replica If of the certificate templates in the organization for more information, see <u>Certificate Temp</u>	is Certification Authority. created does not appear on this list, you may need to wait until ted to all domain controllers. In may not be available to your CA. <u>plate Concepts.</u>				
Γ	Name	Intended Purpose	~			
	🗷 IPSec (Offline request)	IP security IKE intermediate				
	風 Key Recovery Agent	Key Recovery Agent				
	Response Signing	OCSP Signing				
	風 RAS and IAS Server	Client Authentication, Server Authentication				
	風 Router (Offline request)	Client Authentication				
	風 Smartcard Logon	Client Authentication, Smart Card Logon				
	🚇 Smartcard User	Secure Email, Client Authentication, Smart Card Logon				
	🚇 Trust List Signing	Microsoft Trust List Signing				
	🚇 User Signature Only	Secure Email, Client Authentication				
	🚇 Workstation Authentication	Client Authentication				
L			\mathbf{r}			
		OK Cance	ł			

Отметьте созданные нами шаблоны и нажмите ОК.

2. Настройка записей на сервере DNS.

Запустите консоль управления сервером DNS: dnsmgmt.msc. Перейдите в папку Зоны прямого просмотра\<Имя вашего домена>_tcp.



Нажмите правой кнопкой мыши на папке _tcp: "Другая новая запись". В появившемся окне найдите Расположение службы (SRV) и нажмите "Создать запись". В открывшемся окне введите данные:

	New Resource Record				
Service Location (SRV)					
Domain:	_tcp.test2.ru				
Service:	_eap_server v				
Protocol:	_tcp v				
Priority:	0				
Weight:	0				
Port number:	9010				
Host offering this s	ervice:				
Allow any authenticated user to update all DNS records with the same name. This setting applies only to DNS records for a new name.					
OK Cancel Help					

Аналогично создайте также записи для служб _eap_client, порт 9009 и _eap_sts, порт 9011.

В свойствах созданных записей на вкладке **Безопасность** дайте следующие права на чтение:

- для всех группе Authenticated users, для **_eap_client** и **_eap_sts** добавьте еще группу "Компьютеры домена";

- для проверки корректности записей DNS используйте команду:

nslookup -type=srv _eap_server._tcp.<?????? ??? ?????>

3. Подготовка сервера и установка JMS.

Действия производятся на сервере JMS.

3.1. Установка сертификата аутентификации.

Откройте консоль сертификатов локального компьютера: certlm.msc.

На папке "Личные" нажать правой кнопкой мыши — "Все задачи" — "Запросить новый сертификат":

1		C	ertlm - [Certificates - Local Co	omputer\Personal]			
File Action	View Help						
🗢 🔿 🙋							
Gertificates	- Local Computer Obje	ct Ty	be and a second s				
Persona		rtific	ates				
b 🚞 Tri	Find Certificates			_			
▷ 📫 En'	All Tasks		Find Certificates				
⊳ 🚞 Int	View		Request New Certificate	1			
D 📔 Tri	VIEW P		Request New Certificate	J			
⊳ 🚞 Un	Refresh		Import				
þ 📔 Th	Export List		Advanced Operations				
👂 🧮 Tri		L					
👂 🚞 Cli	Help						
Remote Desktop							
Smart Card Trusted Roots							
Trusted Devices							

Откроется мастер запроса сертификатов. Два раза нажимаем "Далее" и выбираем шаблон **Компьютер**. Нажимаем **Выпустить** и дожидаемся сообщения об успешном выпуске.

		_ □	x
📮 Certificate Enrollment			
Request Certificates			
You can request the following click Enroll.	types of certificates. Select the certificates you want to reque	est, and then	
Active Directory Enrollme	nt Policy		
Computer	🔅 STATUS: Available	Details	~
Show all templates			
	Enro	oll Can	cel

3.2. Выпуск сертификата агента запроса.

Откройте консоль сертификатов локального компьютера: certlm.msc.

На папке "Личные" нажать правой кнопкой мыши — "Все задачи" — "Запросить новый

сертификат":

.		C	ertlm - [Certificates - Loc	al Co	mputer\Personal]			
File Action	File Action View Help							
🗢 🔿 🖄								
🗟 Certificates	s - Local Computer Obje	ct Ty	pe					
Percon:	al 📫 🗠 🗠	rtific	ates					
þ 📔 Tri	Find Certificates							
⊳ 📔 En	All Tasks 🕨		Find Certificates					
D Int D Int	View 🕨		Request New Certificate					
⊳ 🧰 Un	Refresh		Import					
⊳ 📫 Th ⊳ 📫 Tri	Export List		Advanced Operations	•				
þ 🧰 Cli	Help							
N 🦰 Remote Desktop								
Smart Card Trusted Poets								
Trusted Devices								

Откроется мастер запроса сертификатов. Два раза нажимаем "Далее" и выбираем шаблон агента запроса сертификатов.

			_ D X
🗐 Cei	rtificate Enrollment		
	Request Certificates		
	You can request the following types of certin click Enroll.	ficates. Select the certificates you w	ant to request, and then
	Active Directory Enrollment Policy		
	Computer	i STATUS: Available	Details 🗸
	Enrollment Agent (Computer)	🤃 STATUS: Available	Details 🗸
	Show all templater		
			Enroll Cancel

Нажмите "Выпустить" и дождитесь сообщение об успешном выпуске.

3.3. Установка и конфигурация сервера JMS.

Запустите установку серверной части JMS. После установки запустится мастер начальной конфигурации. Выберите "Установить только на этом компьютере":

S	Мастер первоначальной настройки
Выбор к Дальней выбранно	онфигурации шие шаги Мастера помогут осуществить развертывание в ой конфигурации.
Выб	берите вариант развертывания:
0	Использовать настройки от предыдущей установки
	Выберите данный вариант в случае выполнения обновления
۲	Установить только на этом компьютере
-	Конфигурация для работы на одном компьютере
0	Развернуть новый кластер
-	Выберите данный вариант в случае развертывания первого узла кластера
0	<u>Добавить новый узел в существующий кластер</u>
	Вариант для развертывания второго и последующих узлов кластера
0	Дополнительные опции развертывания
	В данном режиме требуется вручную выбирать опции развертывания
	< Назад Далее > Отмена

Тип каталога — Active Directory:

S Мастер перв	воначальной настройки
Тип каталога учетных записей Укажите тип каталога учетных записе	a.
Тип каталога учетных записей:	Active Directory V Подключение к локальному контроллеру домена Microsoft Active Directory из текущего домена или леса.
	< Назад Далее > Отмена

Параметры привязки — выберите свой домен:

S Масте	р первоначальной настройки	1 ×
Настройка подключения Укажите настройки подключе	я к серверу Active Directory ения к серверу Active Directory.	
Параметры привязки:	LDAP://test2.ru иальную сервисную учетную запись:	
Логин:		
Пароль:		
🗌 Указать контроллер	домена для чтения схемы вручную:	
Контроллер домена:		¥
	< Назад Дале	е > Отмена

Следующий экран оставьте без изменений.

Далее выберите атрибуты пользователя. Если сомневаетесь, выберите все:

S Мастер первоначальной настройки							
łастройка атрибут Укажите атрибуты поль регистрации из каталог	ов пользователя зователя, которые будут с а учетных записей.	охранятся при его					
Код атрибута	Имя атрибута	Описание атрибута	~				
✓ objectSID	test2.ru.objectSID	Идентификатор безопасн					
✓ objectGUID	test2.ru.objectGUID	Уникальный идентификатор					
✓ sAMAccountName	test2.ru.sAMAccountNa	Учетная запись					
✓ userPrincipalName	test2.ru.userPrincipalNa	UPN					
✓ canonicalName	test2.ru.canonicalName	CN					
✓ distinguishedName	test2.ru.distinguishedNa	Выделенное имя					
✓ displayName	test2.ru.displayName	Отображаемое имя					
🖌 cn	test2.ru.cn	Полное имя					
🖌 sn	test2.ru.sn	Фамилия					
✓ givenName	test2.ru.givenName	Имя	~				
Изменить Выделить все Снять выделение							
		< Назад Далее > О	тмена				

Добавьте вашу лицензию JMS:

S	Мастер	о первоначально	ой настройки	x
Выбор ли Укажите :	ц ензии лицензию, необходим	мую для работы продук	та 3	
Лицензии	для регистрации:			
Ключ	Продукт	Параметры	Срок действия	Статус
			Добави	ть Удалить
		< H	азад Далее :	> Отмена

Выберите поставщика криптографии:

S	Мастер первоначальной настройки	x
Настр Выбор	ойка параметров поставщиков криптографии	
	Iоступные поставщики криптографии: Microsoft Enhanced CSP	
	< Назад Далее >	Отмена

В следующем экране ничего не менять.

Выбрать сертификат оператора. Указать сертификат на токене, шаблон для которого подготовили в п.1.1.

	E	5	Cer	рвер JMS (TES	T2\jmsadmin)		_ [1 X					
						1							
	Г	Статус	Мастер-ключ БЛ	Криптография	Пицензии К	аталоги	8			Выбер	ите сертификат	г	
Aladdin.JM		Прив	зязки каталогов учет	ных записей	Настройка			🔪 Cor	тифи	(2711.112.000		TIQUO.	
S			Мастер первон	ачальной нас	тройки			p cer	пифи	аты на эле	ктронном к	ЭРОНС	
Настро	ойка	парам	етров криптогр	афии		4	Выб	ерите серт	іфикат:				Обновить
	copii		и резервное кониров	anine macrop Killore		1000	Ko	чу выдан		Кем выдан	Срок действия	Поставщик кр	иптографии
^							Adn	inistrator		test2-SDE-SERV	23.05.2019	Microsoft Enhar	nced CSP
Cont							JMS	Admin		test2-CA1-CA	02.05.2020	Microsoft Enhar	iced CSP
Cepi	ифик		тора										
	кому	выдан.	-										
	Кем	выдан:											
A	Срок	действия	R: -										
	Пост	авщик кр	иптографии: -										
Резе	рвно	е копиров	вание мастер-ключа	БД	<u>Выбрать серт</u>	тификат	Πρ	осмотр сер	тификата]		ОК	Отмена
	Стат	vc: He e	зыполнено										
	Фай	л: -						крыть					
				Выполнит	ъ резервное копир	рование							
				< Назад	Далее >	Отме	ia						

Выполните резервное копирование ключа шифрования:

S Мастер первоначальной настройки							
Настройка параметров кри Выбор сертификата и резервное ко	птографии опирование мастер-ключа БД						
Сертификат оператора							
Кому выдан:	JMSAdmin						
Кем выдан:	test2-CA1-CA						
Срок действия:	02.05.2020 8:29						
Поставщик криптографии:	Microsoft Enhanced CSP						
	Выбрать сертификат						
Резервное копирование мастер-	ключа БД						
Статус: Не выполнено							
Файл: -							
	Выполнить резервное копирование						
	< Назад Далее > Отмена						

После этого будет доступна кнопка "Далее".

Укажите сертификат для аутентификации сервера, выпущенный согласно п.3.1.

	Windows Security	< _
	Выбор сертификата Выберите сертификат свойства которого будут использоваться как критерии поиска сертификата для работы с УЦ	
Aladdin.JM.	jms1.test2.ru Issuer: test2-CA1-CA Valid From: 03.05.2018 to 03.05.2019 Click here to view certificate properties	ых за ектор
Парам Для ра рабоче Критер	ОК Cancel рии поиска сертификата:]
Спосо	б поиска: 🔿 По отпечатку 💿 По параметрам	
Кем в	ыдан:	J
Улучш	енный ключ:	1
	Просмотр сертификата	2
		й
		K
	< Назад Далее > Отмена	3

Укажите учётную запись службы, оставив "Системную учётную запись":

S Мастер пе	рвоначальной настройки
Настройка учетной записи Необходимо выбрать из-под какой служба бизнес-логики	учетной записи будет работать
Выберите учтеную запись от им бизнес-логики JMS Системная учетная запис Встроенная учетная за 	аени которой будет работать служба а пись компьютера по-умолчанию
 Учетная запись пользова Выделенная учетная з 	ателя апись пользователя в домене
Выбрать пользователя	a:
Пароль:	
	< Назад Далее > Отмена

Укажите сервер БД и учётные данные для него. Нажмите "Тест соединения", убедитесь, что соединение успешно:

-		Мастер п	ервоначальной настройки 🛛 🗴	
Aladd	inJM	Соединен	ие с сервером успешно установлено.	четных : Коннект
	ыбор нас Укажите им подлинностит	ри подулючении	ОК	
	Настройки Укажите	и административного п е сервер БД	юдключения Macтера к БД SQL-SERVER\SQLEXPRESS 🗸 🗘	
		Использовать SSL		
۹.	Укажите O Wind	е способ проверки под Jows NT Security	линности для административного соединения: Логин:	
	SQL	Server Security	sa	
			Пароль:	
			•••••	
			Тест соединения	
			< Назад Далее > Отмен	а

Укажите имя БД и учётные данные при необходимости:

S	Мастер первоначальной настройки							
Вы б Ук	бор базы данных ажите базу данных и настройки подключения							
	Настройки подключения сервера к БД Укажите имя БД Использовать SSL	EAPDB						
	Укажите способ проверки подлинности ○ Windows NT Security ● SQL Server Security ▼ Создать новый логин	Логин: EAPDB Пароль: •••••••••	n					
		Подтверждение пароля: •••••						
		< Назад Далее > Отмен	a					

Дождитесь запуска службы:



Запустите мастер приложения и дождитесь его завершения:

S	Мастер первоначальной настройки
Настройка Создание об	параметров приложения ъектов, необходимых для устанавливаемого приложения
- Мастер пр Стату	иложения ис: Не выполнен <u>Запустить Мастер приложения</u>
	< Назад Далее > Отмена

Далее будет предложено смонтировать криптохранилище и работа мастера завершится.

4. Настройка и выпуск сертификата в JMS.

4.1. Подготовка системы к выпуску.

Для работы с JMS установите консоль JMS из файла вида Aladdin.JMS.Admin-*.msi

Запустите консоль управления JMS.

Перейдите на вкладку (в левой части окна) "Пользователи". Сверху перейдите на вкладку "Действия над контейнером", включите вид "Отображать вложенные". Нажмите кнопку "Зарегистрировать".



В появившемся окне отметьте необходимых пользователей и нажмите «Зарегистрировать»:

Действия над контей	и́нером	Дейс	твия					
	8		••			Ľ	0	
Варегистрировать Зар	регистрир всех	овать	Установить принудительную Отм смену PIN-кода	енить принудительную смену PIN-кода	Экспорт	Отображать вложенные	О программе	
Регистраци	я	4	Принудительная смена	PIN-кода 🛛	Резер	Содерж 🖌	Помощь	
🎎 Пользователи	\$		Регис	трация новых пол	ьзователей		-	
۹	a 06	новить	🐈 Отображать вложенные 🖌	Исключить зарегистрир	ованные			
↓ test2.ru	test2.ru							
Computers	٩							
ForeignSecu		/ Учет	ная запись	Отображаемое имя		Департамент		
📄 Managed Se		Admir	nistrator					
📄 Users	8	🚺 JMSA	dmin	JMSAdmin				
🥦 Рабочие станции	_			N A F N	Стр. 1	из 1 1 - 2 из	2 Показывать	опо 25 ▼
🛷 Ключевые носите					1	Зарегистриро	вать С	Отмена
Полключенные к	_							

Эти пользователи будут отображаться в основном окне.

Перейдите на вкладку "Профили", выберите пункт "Профили". Установите указатель на "Выпуск сертификатов — УЦ Microsoft CA". На верхней панели нажмите "Создать". Откроется окно нового профиля. Введите имя профиля.



Перейдите на вкладку "Подключение". Выберите сертификат агента запроса, выпущенный согласно п.3.2. В обоих полях шаблонов сертификатов укажите шаблон, созданный согласно п.1.2.

👗 Создание профиля 🗙							
Ключевой контейнер Печать			ать запроса на сер	гь запроса на сертификат Печать сертификат			
Общие	бщие Подключение Приложения Параметры режимов выпус			ы режимов выпуска			
Microsoft	CA						
	Имя центра	Имя центра сертификации Microsoft CA:					
	test2-CA1-C	test2-CA1-CA 🔹					
	Тип подписи	і запр	оса для админист	ративного в	ыпуска:		
	Общий (под	цпись	запроса на сервер	oe)	-		
	Критерии по	Критерии поиска сертификата Enrollment Agent:					
Способ поиска: 🥥 По отпечатку 🛛 По параметрам				параметрам			
Отпечаток сертификата:							
	35886263334ED32840F8D74BB312970306333434						
	Просмотр сертификата						
Шаблонн	о сертификато	в					
	6						
e	пользовате	ль:					
	JMSUserTen	JMSUserTemplate 🔹					
	Администратор:						
	JMSUserTen	JMSUserTemplate					

Перейдите на вкладку "Приложения". Отметьте апплет РКІ.

👗 Создание профиля 🗙							
Ключевой контейнер	Печать запроса на се	ртификат П	ечать сертификата				
Общие Подключение Приложения Параметры режимов выпуска							
Типы приложений							
Список определяет прим выбранной комбинацией	Список определяет применимость данного профиля к ключевым носителям с выбранной комбинацией апплетов						
Комбинация аппле	стов		<u>ـ</u>				
V PKI							
PKI + FOCT + STO	RAGE						
РКІ + ГОСТ 2							
PKI/BIO							
PKI/BIO + FOCT							
PKI/BIO + FOCT 2							
PRO							
PRO (Java) / PKI (с обратной совместимос	гью)					
PRO (Java) / PKI (с обратной совместимост	гью) + РКІ					
PRO (Java) / PKI (PRO (Java) / РКІ (с обратной совместимостью) + ГОСТ						
	PRO (Java) / PKI (с обратной совместимостью) + ГОСТ 2						
RuToken Lite							
RuToken S							
STORAGE	STORAGE						
О ГОСТ							
COCT + STORAGE							
ГОСТ 2	C FOCT 2						
ФКН	ФКН						
Найдено криптопровайдеров: 1							
		ОК	Отмена				

Перейдите на вкладку "Ключевой контейнер". При необходимости измените размер ключа. Он должен совпадать с размером в шаблоне согласно п.1.2.

A		Созд	ание про	филя		X
Общие	Подключени	1е При	ложения	Параметры	и режимов вы	пуска
Ключевой	Ключевой контейнер Печать запроса на сертификат Печать сертификата					тификата
Параметры	ы криптограф	оии				
	Криптопровайдер для генерации ключевой пары:					
	Athena ASE	Card Crypto	CSP			•
	Алгоритм дл	ля генерац	ии ключевой	пары:		
	RSA					•
	Применять PIN-код подписи					
Применени	е и размер к	люча				
۶	Key Exchange O Digital Signature					
	Размер ключа, бит: 2 048 💲					
Ключевой	контейнер					
	О Использо	рвать назва	ание профил	9		
	О Использо	овать суще	ствующий к	онтейнер		
	О Использовать указанное имя:					
					ок	Отмена

Нажмите "ОК".

Перейдите к пункту "Привязка профилей". Выберите нужный контейнер в AD и нажмите "Привязать". Откроется окно профилей. Выберите профиль выпуска сертификатов, профиль выпуска по умолчанию, профиль инициализации и нажмите OK.



4.2. Выпуск сертификата на токен.

Перейдите в раздел **Пользователи**. Подключите чистый токен, который будем привязывать и выпускать для этого пользователя. Найдите нужного пользователя, кликните на него. В верхней панели нажмите кнопку "Выпустить токен". Откроется мастер выпуска:



На следующем этапе дождитесь, когда отобразится ваш токен. Кликните на него и нажмите "Далее".

Мастер выпуска ключевого носителя					x
Вы	Выбор ключевого носителя Выберите ключевой носитель для выпуска.				
	Список подключе	нных ключевых носителе	й:		φ.
	Модель	Идентификатор	Метка	Состояние	
	JaCarta PKI	0C50000427129613	My token	Не зарегистрир	o
			< Назад	Далее > От	мена

Следующие 4 экрана оставьте без изменений.

Далее отобразятся параметры предполагаемого выпуска токена.

Мастер выпуска ключевого носителя				
Подтверждение параметров Подтвердите параметры выпускаемого ключевого носителя.				
Подтвердите введенные парамет	ры:			
Общие		~		
Владелец:	Administrator			
Модель:	JaCarta PKI	=		
Идентификатор:	0C50000427129613			
Номер корпуса:				
Номер СКЗИ:				
Номер СЗИ:				
Профили выпуска объектов:	msca-jacarta	~		
	< Назад Далее >	Отмена		

Далее начнется процесс выпуска токена:

Мастер выпуска к	лючевого носителя
Выпуск ключевого носителя Выпуск ключевого носителя	
Выполняется выпуск ключевого носителя	
Инициализация ключевого носителя	
	< Назад Далее > Отмена

В последнем окне вы увидите ссылку на окно отчёта о выпуске. Если она синего цвета, значит процесс прошёл успешно. Если ссылка красного цвета, значит имели место ошибки.



ID статьи: 285

Последнее обновление: 09 Jul, 2018

Ревизия: 1

JaCarta Management System -> JMS. Типовой сценарий развертывания (MSCA)

https://kbp-6.aladdin-rd.ru/index.php?View=entry&EntryID=285