

JaCarta PKI и VMware Horizon View 7

Руководство по настройке

Листов: 15 Автор: Александр Гриценко

Аннотация

Настоящий документ содержит сведения о настройке двухфакторной аутентификации в административном интерфейсе VMware Horizon 7 и входа на VDI-машину пользователя с использованием электронных ключей JaCarta PKI и вспомогательного программного обеспечения "Единый Клиент JaCarta".

Владельцем товарных знаков Аладдин, Aladdin, JaCarta, логотипов и правообладателем исключительных прав на их дизайн и использование, патентов на соответствующие продукты является ЗАО "Аладдин Р.Д.".

Сведения, приведённые в данном документе, актуальны на дату его публикации.

При перепечатке и использовании данных материалов либо любой их части ссылки на ЗАО "Аладдин Р.Д." обязательны.

© ЗАО "Аладдин Р.Д.", 1995–2017. Все права защищены.

Настоящий документ, включая подбор и расположение иллюстраций и материалов в нём, является объектом авторских прав и охраняется в соответствии с законодательством Российской Федерации. Обладателем исключительных авторских и имущественных прав является ЗАО "Аладдин Р.Д.". Использование этих материалов любым способом без письменного разрешения правообладателя запрещено и может повлечь ответственность, предусмотренную законодательством РФ.

Информация, приведённая в данном документе, предназначена исключительно для ознакомления и не является исчерпывающей. Состав продуктов, компонент, их функции, характеристики, версии, доступность и пр. могут быть изменены компанией "Аладдин Р.Д." без предварительного уведомления. Все указанные данные о характеристиках продуктов основаны на международных или российских стандартах и результатах тестирования, полученных в независимых тестовых или сертификационных лабораториях, либо на принятых в компании методиках. В данном документе компания "Аладдин Р.Д." не предоставляет никаких ни явных, ни подразумеваемых гарантий.

Владельцем товарного знака и др. — корпорация Microsoft (Microsoft Corporation). Названия прочих технологий, продуктов, компаний, упоминающихся в данном документе, могут являться товарными знаками своих законных владельцев.

1.0

Оглавление

О платформе VMware Horizon View 7	4
Настройка VMware Horizon View 7	5
Предварительные требования	5
Настройка сертификатов	5
Экспорт корневого сертификата	5
Создание файла-контейнера ключей JKS	7
Настройка входа по сертификату	8
Настройка проброса смарт-карты пользователя	9
Проверка входа	10
Вход в консоль администрирования	10
Вход на VDI-машину	11
Контакты, техническая поддержка	13
Регистрация изменений	14

О платформе VMware Horizon View 7

VMware View — продукт для виртуализации персональных компьютеров от VMware, Inc. Первые версии (2.0.0 и 2.1.0) продавались под именем VMware VDI, однако, начиная с версии 3.0.0, имя было изменено на VMware View. Начиная с версии 5.2, стал частью VMware Horizon Suite и получил название VMware Horizon View.

Настройка VMware Horizon View 7

Предварительные требования

Подразумевается использование OC семейства MS Windows. совместимых с программным обеспечением VMware Horizon View, а также с ПК "Единый Клиент JaCarta". Имеется работающая инфраструктура открытых ключей (PKI).

VMware Horizon View должен быть установлен и настроен в соответствии с требуемой конфигурацией.

Настройка сертификатов

Экспорт корневого сертификата

1. Откройте оснастку Certification Authority на корневом ЦС, выполнив команду certsrv.msc.

	Run 🗙			
	Type the name of a program, folder, document, or Internet resource, and Windows will open it for you.			
Open:	certsrv.msc v			
	OK Cancel Browse			

2. Откройте окно Certification Authority -> CA Name -> Properties.



3. На вкладке General выберите корневой сертификат и нажмите кнопку View Certificate.



4. Перейдите на вкладку **Details** и нажмите кнопку **Copy to File**.

R (Certificate	x
General Details Certification F	Path	
Show: <	~	
Field	Value ^	
Version	V3	1
Signature algorithm	19 f5 5c 10 cf 5a 06 b8 48 66 ≡ sha256RSA	
Signature hash algorithm	sha256	
🔲 Issuer	Virtlab Root CA, virtlab, space	
Valid from	7 сентября 2016 г. 13:25:25	
🔲 Valid to	7 сентября 2041 г. 13:35:25	
Subject	Virtlab Root CA, virtlab, space 🗸	
	2 Effe Dessarting	

5. На странице выбора формата файла выберите Base-64 encoded X.509 (.CER).

Export File Format Certificates can be exp	orted in a variety of file formats.
Select the format you w	rant to use:
O DER encoded bir	ary X.509 (.CER)
Base-64 encode	1 X.509 (.CER)
Cryptographic M	essage Syntax Standard - PKCS #7 Certificates (.P7B)
Include all ce	rtificates in the certification path if possible
O Personal Informa	ation Exchange - PKCS #12 (.PFX)
Include all ce	rtificates in the certification path if possible
Delete the p	ivate key if the export is successful
Export all ex	tended properties
O Microsoft Serializ	ed Certificate Store (.SST)

6. Укажите путь экспорта файла, например, *C:\temp\RootCA.cer*.

		X
e 🦻	Certificate Export Wizard	
Fil	e to Export	
	specify the name of the life you want to export	
	File name:	
	C: \temp \RootCA.cer	Browse
		Next Cancel

Создание файла-контейнера ключей JKS

 На сервере VMware Horizon View откройте командную строку и перейдите в каталог с утилитой keytool.exe (C:\Program Files\VMware\VMware View\Server\jre\bin).

C:\Users\dcadmin>cd "C:\Program Files\VMware\UMware View\Server\jre\bin" C:\Program Files\VMware\UMware View\Server\jre\bin>_

 Импортируйте корневой сертификат в файл-хранилище с помощью команды keytool -import alias alias -file root_certificate -keystore truststorefile.key, где alias – псевдоним (любое значение), root_certificate – полный путь к файлу сертификата, truststorefile.key – имя файл-хранилища. В процессе импорта необходимо будет ввести парольную фразу для защиты хранилища и подтвердить доверие сертификату.

C:\Program Files\UMware\UMware Uieu\Server\jre\bin}keytool.exe -import -alias <mark>UirtlabRootCA</mark> -file <u>c:\temp\RootCA.ce</u> r - ystore_truststorefile.key	k
Enter Keystore password: Re-enter new password: Dunga: CH-Hiwitab Rest für DC-wintlab DC-sapage	
ometri on pirizian unut on portrian, porspace Issuer: CM-pirizian Docto, DC-pirizia, DC-space Serial number: 19755c10cf3a0608486674368bAha88 Jalid from: Wed Sep 07 13:25:25 MSK 2016 until: Sat Sep 07 13:35:25 MSK 2041	
Certificate fingerpints: MD5: 8B:AD:E4:F5:5D:BB:41:A5:9F:1E:04:7A:72:68:C8:0D SHA1: 5C:94:9A:DE:74:52:D8:23:79:D0:2E:BF:D5:D6:DD:80:2E:0F:78:14 SHA25: 2F:ED:C7:45:C3E:D0:89:45:C5:D8:25:CC:19:32:E4:E1:91:4E:EB:F6:BF:BF:54:EC:B2:A5:19:5E:73:90:C1:F6 Signature algorithm name: SHA256withMSA Version: 3	
Extensions:	
#1: ObjectId: 1.3.6.1.4.1.311.21.1 Criticality=false 0000: 02 01 00	
#2: ObjectId: 2.5.29.19 Criticality=true BasicConstraints:[CAttrue PathLen:2147483647]	
H3: ObjectId: 2.5.29.15 Criticality=false KeyUsage KeyUsatsi Key_CerteSign Cr1_Sign J	
#4: Object[d: 2.5.29.14 Criticality=false SubjectKeyldentifier [
ned01: 12 12 5 6 C C5 C1 C6 EB 95 10 F0 2E 28 84 2B 2D 73 .nl	
Trust this certificate? [no]: yes Certificate was added to keystore	
C:\Progran Files\UMware\UMware View\Server\jre\bin>_	А

- 3. Файл-хранилище **truststorefile.key** необходимо скопировать в директорию SSL Gateway: *install_directory\VMware\VMware View\Server\sslgateway\conf\truststorefile.key*.
- В директории SSL Gateway (install_directory\VMware\VMware View\Server\sslgateway\conf\locked.properties) необходимо создать файл с именем locked.properties и отредактировать его (например, в блокноте) до следующего содержимого:

trustKeyfile= truststorefile.key trustStoretype=JKS useCertAuth=true 5. Сохраните файл и перезагрузите службу View Connection Server.

Настройка входа по сертификату

1. Зайдите в Web-консоль VMware Horizon View.

vm ware [.]		
User name: Password: Domain:	↓ VIRTLAB ✓ Remember user name Log In	VMware Horizon=7 Administrator=

2. Перейдите в свойства сервера: Inventory -> View Configuration -> Servers -> Connections Servers -> Edit.

Updated 12.05.2017 18/00 Servers Sessions Problem KDS Hots System Health 9 Other Problem KDS Hots System Health 9 Other Problem KDS Hots Problem KDS Ho	VMware Horizon 7 Adm	inistrator					About	Help Logo		
Sessions A Problem RDS Hots A System Health Diable Events Diable System Health Diable Educations Severes System Health Diable Connection Server Version Problem KOS Hots Connection Server Version Connection Server Version PCLP Secure State Secure tunoid connection Version PCLP Secure State Secure tunoid connection Version PCLP Secure State Secure tunoid connection Version Problem State Secure tunoid connection Problem Secure tunoid connection	Updated 12.05.2017 16:08	Servers								
Problem RDS Hots Versition Versition Versition Versition • More Commands • More Commands • More C	Sessions 1 Problem vCenter VMs 0	vCenter Servers	Security Sec	ervers Conne	ection Server	s 🔶	- 3			
System Hadming 1 1 1 0 1 1 0 1 1 1 0 1	Problem RDS Hosts 0 Events 0 1 0	Enable Disable	Edit	Backup Now	 More Co 	ommands				æ
Visit-View-01 Bushboard Dabboard Catalog Resources Private Torison Catalog Resources Private Torison Resources Private Torison Resources Resources Private Torison Resources Private Torison Resources Resour	19 1 1 0	Connection Server	Version	PCoIP Secure	State	Settings		Last Backup		
Inventory VSRV-VVEW-02		VSRV-VIEW-01	7.0.1-39889	! Installed	Enabled	Secure tunnel connection,	 12.05.201 	7 0:00:10		
Costalog	Inventory	VSRV-VIEW-02	Enable			Secure tunnel connection,	 12.05.201 	7 0:00:10		
Lotatag Lotatag Reserves Advings Reserves Protection Protection Protection Reserve Reserves	🔗 Dashboard		Disable			5				
	👸 Users and Groups		Edit			5				
Resources General Security Server Fusing Resource. General Security Server Fusing Resource. Figure Attachings Products Prod	► Catalog	1	Backup Nov	v		-				
Image: Marine Service Eport table contents Refresh table contents Refresh table contents Policine Service Refresh table contents Policine Service Refresh table contents Instant Close Domain Admins Policine Service Product Licencing and Usage 2 Global Statings Registered Machines Administrors ThinApp Configuration Cloud Pod Architecture Point Configuration Event Configuration Image: Configuration	▼ Resources	-	Specify Sec	urity Server Pairing	p Password					
Refresh table content Refresh table Refresh table Refresh table Refresh tab	Farms 1		Export table	e contents						
La effetive Colos Monitoring Policies View Configuration Several Instart Cone Domain Admins Product Licensing and Uage Global Settings Registered Machines Administrators ThinApp Configuration Cload Ped Architecture Event Configuration	Machines		Refresh tab	ole content		-				
Policies View Configuration Server Instant Clone Domain Admins Product Licensing and Usage Global Settings Registred Meshines Administrators ThirdspC Configuration Cloud Pol Architecture Event Configuration	Persistent Disks									
View Configuration	Policies									
Scruer 2 Instant Clone Domain Admins 2 Product Liceraring and Usage 2 Global Settings 8 Registered Weshines 4 Administrators 1 ThriApp Configuration 1 Cloud Pol Architecture 1 Event Configuration 1	View Configuration									
Indiat Clove Domain Adminis Product Uncerning and Usage Cibabil Statings Registated Machines Administrators ThinAps Configuration Cloud Pid Architecture Event Configuration	Servers d									_
Product Literation and Usage 2 Global Settings Registered Machines Administrators ThinApp Configuration Cloud Pod Architecture Event Configuration	Instant Clone Domain Admins	2								
Global Settings Registeral Methines Administrators Thirkape Configuration Cloud Pid Architecture Event Configuration	Product Licensing and Usage	2								_
Registered Machines	Global Settings									
Administrators ThirApp Configuration Cloud Pol Architecture Event Configuration	Registered Machines									
ThinApp Configuration Cloud Field Architecture Event Configuration	Administrators									
Cloud Pod Architecture Event Configuration	ThinApp Configuration									
Event Computation	Cloud Pod Architecture									
	Event Configuration									
									_	_

- 3. Перейдите на вкладку Authentication и выберите предпочтительный режим аутентификации. Аутентификация в административную консоль по смарт-карте настраивается из выпадающего списка Smart card authentication for administrators:
 - Not Allowed не использовать смарт-карту;
 - Optional смешанная аутентификация (или по паролю или по смарт-карте);
 - Required обязательное использование смарт-карты.

Аутентификация пользователя в VDI по смарт-карте настраивается из выпадающего списка Smart card authentication for users:

- Not Allowed не использовать смарт-карту;
- Optional смешанная аутентификация (или по паролю или по смарт-карте);
- Required обязательное использование смарт-карты.

Опция "Disconnect user sessions on smart card removal" определяет политику при отключении смарт-карты. Установите галочку, если необходимо производить отключение сессии при изъятии смарт-карты.

dit Connection Server Settings
General Authentication Backup
Disabled Delegation of authentication to VMware Horizon (SAML 2.0 Authenticator) SAML Authenticator: No Enabled Authenticator configured Manage SAML Authenticators
View Authentication
Changes to authentication settings will take effect on next user login
Smart card authentication for users: Required 💌
☑ Disconnect user sessions on smart card removal 3 Advanced Authentication 3
2-factor authentication Disabled V
View Administrator Authentication
Changes to authentication settings will take effect on next user login
Smart card authentication for administrators: Not allowed Vot allowed Optional Required

4. Нажмите кнопку ОК.

Настройка проброса смарт-карты пользователя

Проброс смарт-карты пользователя позволяет производить прозрачную аутентификацию в виртуальную машину с вводом PIN-кода один раз.

При использовании тонких клиентов Teradici настройка, как правило, не требуется.

При использовании программных клиентов Windows, macOS, Linux необходимо выполнить установку VMware View Agent с активацией опции Smartcard Redirection.

ок

Cancel

🕞 VMware Horizon Agent	×
Custom Setup Select the program features you want installed.	日
Click on an icon in the list below to change how a feat	ure is installed. Feature Description Enables the Smartcard Redirection feature.
This feature will be installed on lo	cal hard drive.
This feature will not be available.	
Install to:	Change
Help Space < Ba	ck Next > Cancel

Проверка входа

Вход в консоль администрирования

- 1. Вставьте смарт-карту и перейдите в консоль администрирования.
- 2. В появившемся окне формы входа выберите сертификат администратора и нажмите кнопку ОК.

← → @ https://vsrv-view-0	01.virtlab.space/admin/		X - ۵	O vsrv-view-01.virtlab.space	×
Windo	ws Security		×		
Sele	ct a Certificate				
Site v	vsrv-view-01.virtlab.space	needs your credentials:			
	dcadmin				
	Issuer: Virtlab Root CA	4			
	Valid From: 15.05.201	7 to 15.05.2018			
	Click here to view cert	tificate properties			
More	choices				
	ОК	Cancel			

3. Отобразится запрос на ввод PIN-кода. После успешной проверки PIN будет произведена аутентификация в Web-интерфейс.

🗲 🔿 <i> ि</i> ht	tps://vsrv-view-01.virtlab.space/admin/		Ø ▼ X C Waiting for vsrv-view-01.vir ×
	Windows Security		×
	Smart Card		
	Please enter your authentication	on PIN.	
	PIN	୕	
	Click here for more in	formation	
	ОК	Cancel	

Вход на VDI-машину

1. Запустите VMware Horizon Client и выберите подключение.

Ø VMware Horizon Client	-	×
+ New Server		≡ -
view-cert.virtiab.s pace		_

2. Отобразится запрос на ввод PIN-кода.

VMware Hori	zon Client	_	\times
🖋 Cancel	Loading		
	🚱 Login — 🗆 🗙		
	vmware Horizon PColP		
	Enter your PIN.		
	Server: 🏠 https://view-cert.virtlab.space		
	PIN: ••••••		
	Login Cancel		

3. После успешной аутентификации отобразятся доступные ресурсы.

I VMware Horizon Clie	nt ab.space			- □ 🛧 🌣	× • 9
Windows 7 01	Windows 7 02	Windows 7 03	Windows 8.1 01	Windows 8.1 02	

Контакты, техническая поддержка

Офис (общие вопросы)

Адрес: 129226, Москва, ул. Докукина, д. 16, стр. 1, компания "Аладдин Р.Д." Телефоны: +7 (495) 223-00-01 (многоканальный), +7 (495) 988-46-40 Факс: +7 (495) 646-08-82 E-mail: aladdin@aladdin-rd.ru (общий) Web: www.aladdin-rd.ru Время работы: ежедневно с 10:00 до 19:00, кроме выходных и праздничных дней.

Техподдержка

Служба техподдержки принимает запросы только в письменном виде через Web-сайт:

www.aladdin-rd.ru/support/index.php

Для оперативного решения Вашей проблемы укажите используемый Вами продукт, его версию, подробно опишите условия и сценарии применения, по возможности, снабдите сообщение снимками экрана, примерами исходного кода.

Регистрация изменений

Версия	Изменения
1.0	Исходная версия документа



Лицензии ФСТЭК России № 0037 и № 0054 от 18.02.03, № 2874 от 18.05.12 Лицензии ФСБ России № 12632 H от 20.12.12, № 24530 от 25.02.14 Система менеджмента качества компании соответствует требованиям стандарта ISO/ИСО 9001-2011 Сертификат СМК ГОСТ Р ИСО 9001-2011 № РОСС RU.ИС72.К00082 от 10.07.15 Аррle Developer

© ЗАО "Аладдин Р.Д.", 1995–2017. Все права защищены.

Тел. +7 (495) 223-00-01 Email: <u>aladdin@aladdin-rd.ru</u> Web: <u>www.aladdin-rd.ru</u>