

AVSOFT KAIROS

Система защиты от спама и фишинга

Руководство по развертыванию

Москва 2022г.

Контактная информация

127106, г. Москва, ул. Гостиничная, д.5 Тел.: +7 (495) 988-92-25 E-mail: office@avsw.ru www.avsw.ru/about/contacts

Авторское право

OOO «AB Coфт» www.avsw.ru © 2010-2022 ООО «AB Coфт»

Версия документа

Июнь 9, 2022.

Настоящий документ является собственностью ООО «АВ Софт» (далее — «АВ Софт») и защищен законодательством Российской Федерации и международными соглашениями об авторских правах и интеллектуальной собственности.

Копирование документа либо его фрагментов в любой форме, распространение, в том числе в переводе, а также их передача третьим лицам возможны только с письменного разрешения «АВ Софт».

Документ может быть изменен без предварительного уведомления.

СОДЕРЖАНИЕ

1 Термины и определения	. 4
2 Описание поставки ПО системы KAIROS	. 4
3 Описание развертывания комплекса	. 5
4 Настройка сервиса менеджмента	10
5 Настройки в веб-интерфейсе	11

1 Термины и определения

В настоящем документе используются термины и определения, представленные в таблице 1.

Таблица	1.	Te	рмин	ыи	ОП	реде.	пения
	-	-	-		-		-

Nº	Термин	Определение
1.	Primary interface	Основной интерфейс для общения между сенсором и сервисом менеджмента.
2.	Load interface	Интерфейс для загрузки данных

В настоящем документе используется перечень сокращений, представленный в таблице 2.

Таблица 2. Перечень сокращений

N⁰	Сокращение	Значение
1.	APM	Автоматизированное рабочее место
2.	ПО	Программное обеспечение
3.	BM	Виртуальная машина
4.	VLAN	Virtual Local Area Network

2 Описание поставки ПО KAIROS

Программное обеспечение (далее – ПО) системы KAIROS состоит из программных модулей, описанных в таблице 3.

Талица 3. Описание модулей ПО

N⁰	Описание модуля	Описание	Формат файлов
1.	Модуль управления	Управление комплексом	kairos.ova

3 Описание развертывания комплекса

Для установки системы KAIROS в среде виртуализации ESXi, необходимо выделить сетевой интерфейс со свободным ID (выбранный ID необходимо будет вписать в настройки разворачиваемой виртуальной машины Kairos). Для этого в интерфейсе ESXi в разделе «Networking > Port groups» необходимо создать VLAN_(выбранный ID)_ TAGGED, «Add port group», со следующими настройками безопасности, как показано на рисунке 1. По завершении ввода данных необходимо нажать «Add».

Name	VLAN_0_TAGGED
VLAN ID	0
Virtual switch	vSwitch0 ~
Security	
Promiscuous mode	○ Accept ○ Reject
MAC address changes	○Accept ○ Reject
Forged transmits	○ Accept ○ Reject

Рисунок 1. Настройка сетевого интерфейса модуля управления

В данном VLAN будет располагаться модуль управления системой KAIROS. Вторую Port Group по аналогии нужно сделать так, как показано на рисунке 2.

Name	VLAN_660_PROMISC
VLAN ID	660
Virtual switch	vSwitch0 ~
Security	
Promiscuous mode	Accept Reject Inherit from vSwitch
MAC address changes	OAccept Reject OInherit from vSwitch
Forged transmits	Accept Reject Inherit from vSwitch

Рисунок 2. Настройка сетевого интерфейса

Далее необходимо создать ещё одну выделенную PortGroup «VLAN_(выбранный ID)_PROMISC» чтобы было как минимум две PortGroup: например, «VLAN_660_PROMISC» и «VLAN_661_PROMISC».

Далее необходимо создать виртуальную машину для развертывания образа дистрибутива сервиса менеджмента системы KAIROS. Для этого нужно перейти в раздел «Virtual Machines», нажать «Create / Register VM», в пункте 1 «Select creation type» выбрать «Deploy a virtual machine from an OVF or OVA file». Далее нажать кнопку «Next» (Рисунок 3).

Select creation type	Select creation type	
Select OVF and VMDK files Select storage	How would you like to create a Virtual Machine?	
License agreements Deployment options Additional settings Ready to complete	Create a new virtual machine Deploy a virtual machine from an OVF or OVA file	This option guides you through the process of creating a virtual machine from an OVF and VMDK files.
vmware.		
VIIIVale		

Рисунок 3. Выбор типа файла для развертывания

Далее необходимо в пункте 2 «Select OVF and VMDK files» присвоить имя виртуальной машине и выбрать файл для загрузки (Рисунок 4).



Рисунок 4. Импорт файла в виртуальную машину

Далее в пункте 3 «Select storage» необходимо выбрать хранилище, в котором будет размещен образ и нажать кнопку «Next» (Рисунок 5).

1 Select creation type	Select storage						
2 Select OVF and VMDK files	Select the storage type and datastore						
3 Select storage	e 						
4 License agreements	Standard Persistent Memory						
5 Deployment options							
6 Additional settings	Select a datastore for the virtual machine's o	configuration files	s and all of its' v	irtual disks.			
7 Ready to complete							
			-	-			
	Name	Capacity ~	Free ~	Туре	V Thin pro V	Access	×
	datastore1	1.62 TB	59.94 GB	VMFS6	Supported	Single	
						11	tem
						11	tem

Рисунок 5. Выбор хранилища для размещения образа

Далее в пункте 4 **«Deployment options»** необходимо выбрать VLAN, способ размещения на диске (по умолчанию рекомендуется «тонкий», в случае необходимости — перезагрузите страницу) и автоматический способ запуска. Нажать кнопку **«Next**» (Рисунок 6).

Select creation type	Deployment options			
Select OVF and VMDK files Select storage	Select deployment options			
Deployment options Ready to complete	Network mappings	VM Network	VM Network ~	
	Disk provisioning	● Thin ○ Th	nick	
	Power on automatically			

Рисунок 6. Выбор настроек установки

Далее в пункте 5 «**Ready to complete**» необходимо выполнить перепроверку настроек импорта и развертывания. Если все корректно, то нажать кнопку «**Finish**» (Рисунок 7).

2 Select OVF and VMDK files 3 Select storage	Ready to complete Review your settings selection b	efore finishing the wizard
4 Deployment options 5 Ready to complete	Product	Kairos
	VM Name	kairos
	Files	kairos.vmdk
	Datastore	datastore1
	Provisioning type	Thin
	Network mappings	VM Network: VM Network
	Guest OS Name	Unknown
	Do not refresh yo	our browser while this VM is being deployed.

Рисунок 7. Перепроверка настроек установки и ее запуск

После завершения импорта в таблице заданий «**Recent tasks**» в столбце «**Result**» статус следующих заданий должен быть «Completed successfully»:

- Upload disk (Загрузка диска)
- Create VM (Создание виртуальной машины)
- Import VApp (Импорт образов)
- Power On VM (Запуск на виртуальной машине)

4 Настройка сервиса менеджмента

После успешного импортирования необходимо осуществить настройку сервера. Для этого необходимо перейти в консоль терминала (Рисунок 8):

mware ESXi		Aller			rootg(192.168.0.192 + Help + Q Search
T Navigator	E LOKI_Managment				
Best Manage Monitor Global Constraints Global Constraints	Console Monitor Console Monitor Console Monitor Control Console Control Control Control Control Contro	Power of a Suspent © Reset / Edit © Referent LOK Management Overs 05 Compatibility ESX55 Sinitial machine Univers 06 Compatibility ESX55 Sinitial machine Univers 06 A A A A A A A A A A A A A A A A A A	Actions	size you to perform operations on the	233 MHZ 10.05 68 1004 28 1005 68 1004 28 1004 28 1
	General Information			- Hardware Configuration	
	Networking			▶ □ CPU	4 vCPUs
	+ 📾 VMware Tools	VMware Tools is not installed.	Actions	Memory	10 GB
	► 🗐 Storage	1 disk		+ I Hard disk 1	200 GB
	E Notes		/ Edit notes	ININ Network adapter 1	VLAN_0_TAGGED (Connected)
				Floppy drive 1	Remote Floppy 0
	· Performance summary last	hour		Video card	4 MB
		Consumed host CPU Consumed host memory.	Ready	>)III Others	Additional Hardware
	3 100		10	+ Resource Consumption	
	5 80		8 Cons	Consumed host CPU	233 MHz
			1 C C C C C C C C C C C C C C C C C C C		
	Rea		Ime	Consumed host memory	10.05 GB
	82 CO		6 for	Consumed host memory	10.05 OB
	eeg / ndo see		amed host me	Consumed host memory Active guest memory The Storage	10.05 OB 1.8 OB
	ned heat CPU/ Rea		uned host memory 6 4	Consumed host memory Active guest memory Consumed Active guest	10.05 08 1.8 08 200 08
	oreumed feat CPU/Rea		6 4 2	Consumed host memory Active guest memory Consumed Provisioned Uncommitted	10.05 08 1.8 08 200 08 192 58 08
	Octamined test		6 4 memory (CEI)	Consumed host memory Active guest memory Consumed host memory Consumed Uncommitted Not-shared	10.5 08 18 08 200 08 152 58 08 55 15 08

Рисунок 8. Переход в консоль терминала для настройки сервиса менеджмента

Далее необходимо авторизоваться под пользователем avsoft_shell, пароль от которого будет выдан вендором, чтобы попасть в консоль управления.

Для просмотра доступных сетевых интерфейсов нужно воспользоваться следующей командой:

interface info

Далее необходимо настроить сетевые интерфейсы. В случае, если в сети имеется DHCP-сервер, следует ввести команду:

interface edit INTERFACE dynamic

INTERFACE — имя настраиваемого интерфейса

В ином случае интерфейсы нужно настроить вручную, воспользовавшись следующей командой:

interface edit INTERFACE static --ip IP_ADDR --nm NETMASK --gw GATEWAY

INTERFACE — имя настраиваемого интерфейса;

NETMASK — маска подсети;

GATEWAY — шлюз (необязательный параметр).

Для проверки настроек сетевого интерфейса можно использовать команду:

interface info INTERFACE

INTERFACE — имя интерфейса

Сервису менеджмента также необходимо задать управляющий интерфейс. Сделать это можно следующей командой:

interface primary INTERFACE

INTERFACE — имя интерфейса

5 Настройки в веб-интерфейсе

Далее необходимо перейти в веб-интерфейс и выполнить авторизацию в нем (логин и пароль выдается вендором) (Рисунок 9).



Рисунок 9. Авторизация в веб-интерфейсе