Sangfor в мире и СНГ

О компании Sangfor

- Основана в 2000 году
- HQ: Шэньчжэнь
- Shenzhen Stock Exchange 2018
- Общий оборот за 2024 год составил 1,5млрд $

Увеличение мирового присутствия

Новые хабы техподдержки – ОАЭ, Италия

Новые территории – СНГ (Казахстан, Узбекистан, Киргизия)

№1 по HCI в Китае

№2 по SDS в APAC

№3 по VDI в APAC

По объему продаж по версии IDC

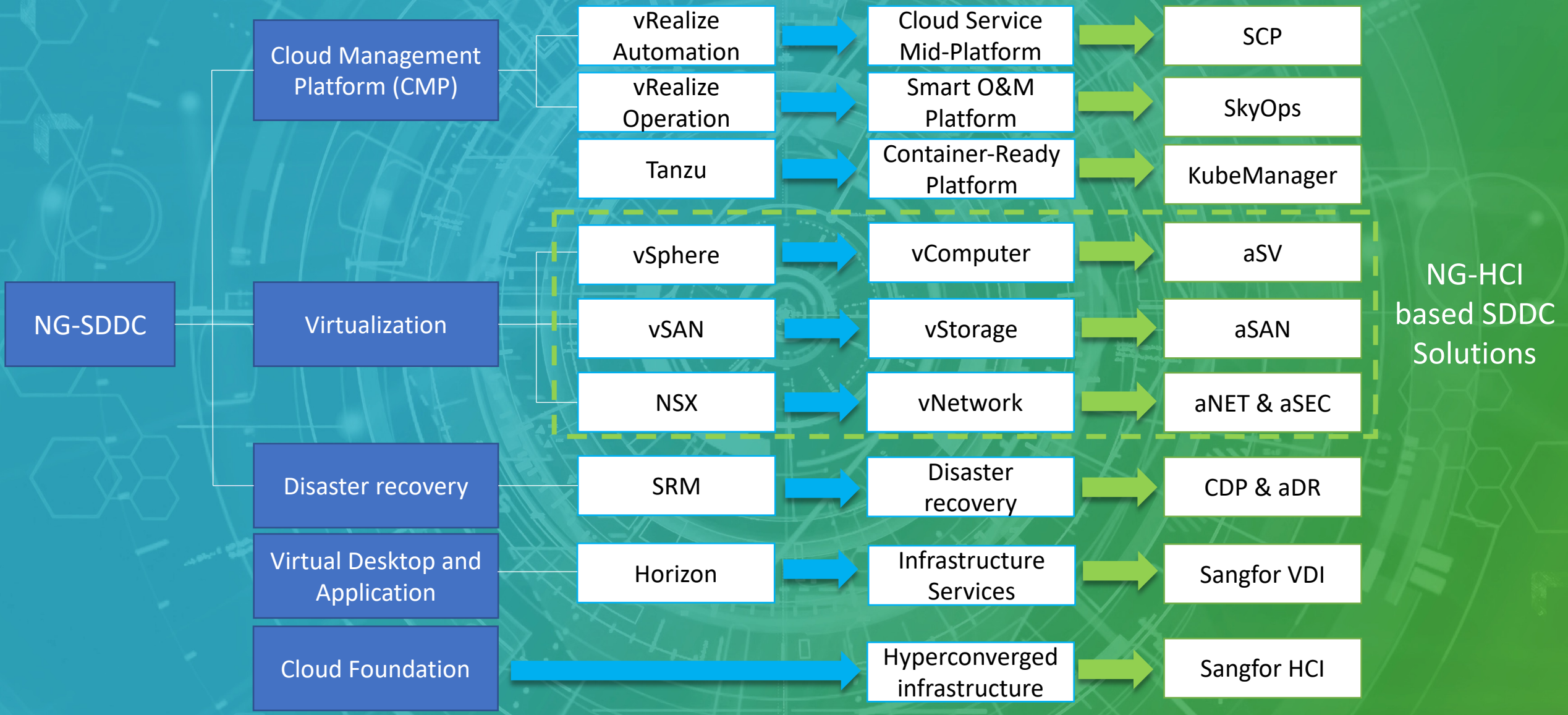
Sangfor HCI и VDI

HCI

VDI

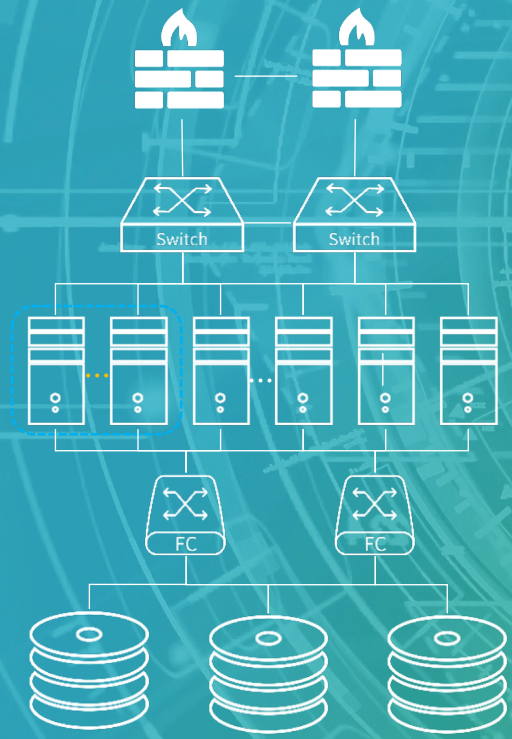
Наш софт действительно работает
Техническая поддержка оказывается на русском языке

Сопоставление продуктов Sangfor и VMware



Sangfor HCI

Традиционный DC



Firewall

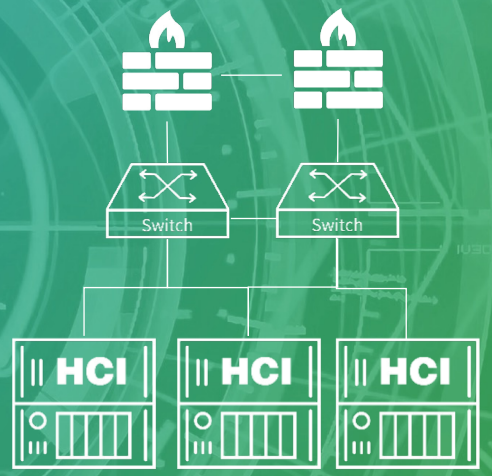
Switch

Server

FC Switch

SAN Storage

DC на базе HCI

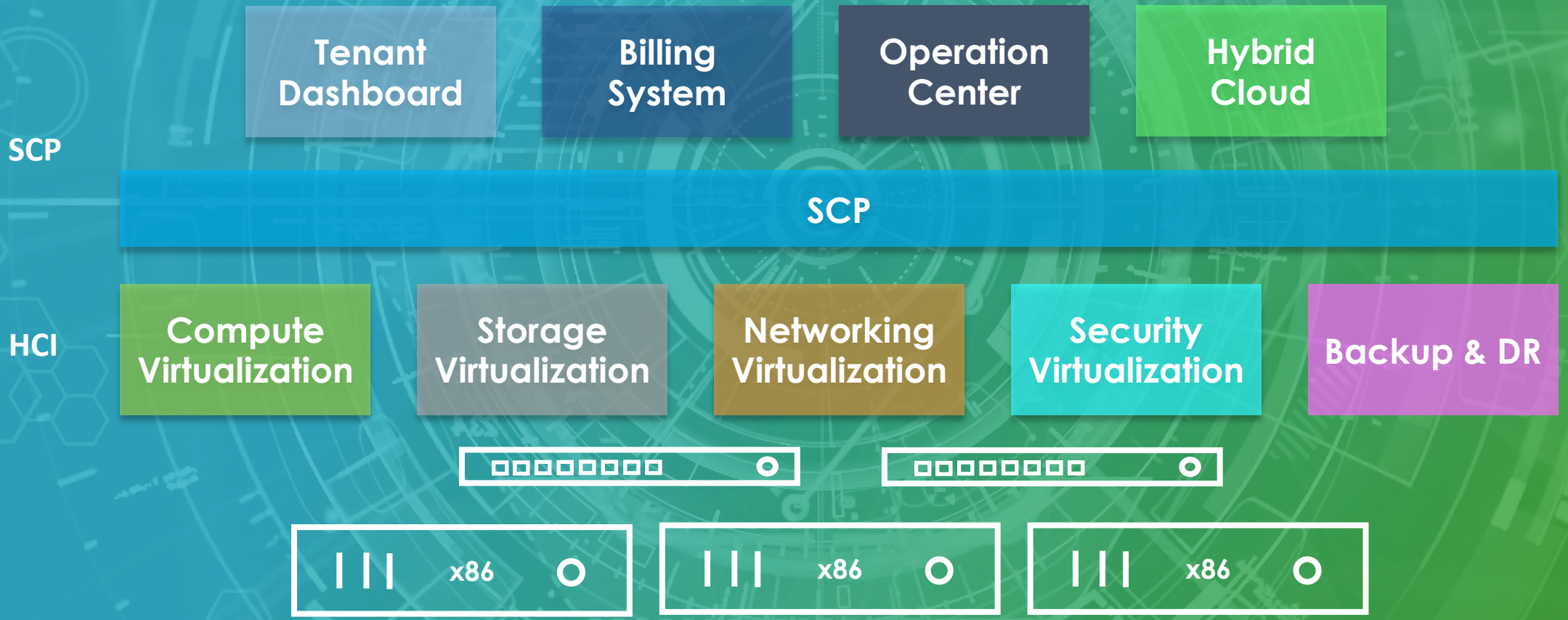


Firewall

Switch

Server

Виртуализация



Доставка приложений и рабочих столов

- 3 Основных компонента VDI решения
- Любой x86 Сервер+ VDI ПО+ Тонкий-Клиент/Агент

Virtual Desktop Controller

VM VM App

Сервер x86 с установленным гипервизором HCI

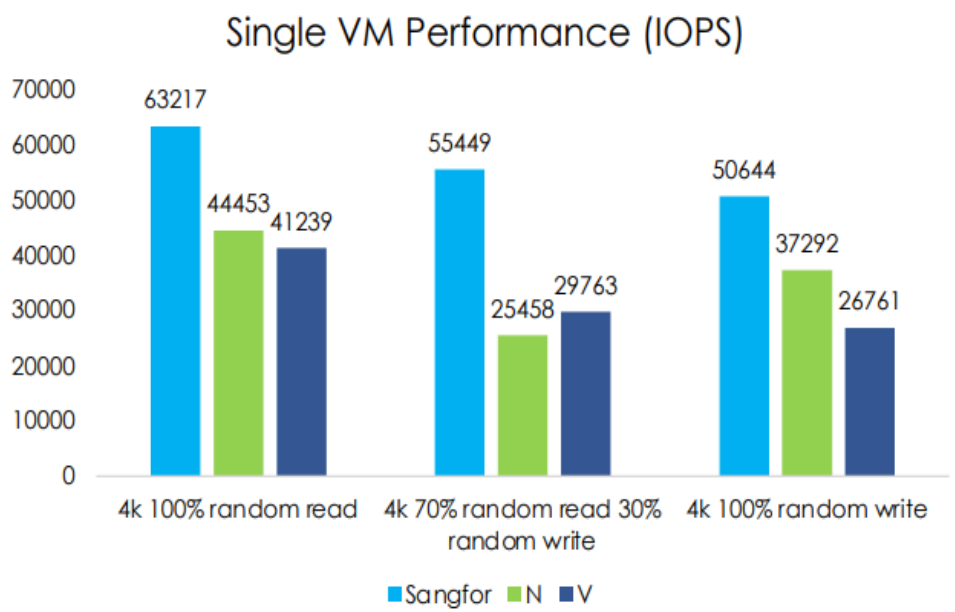
Взаимодействие с Virtual Desktop через сеть

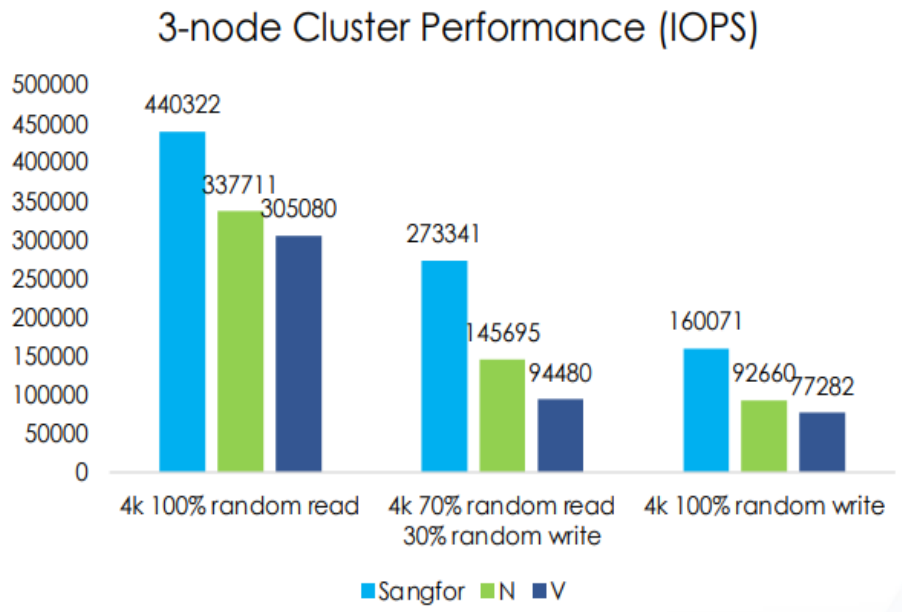
Тонкий клиент

ПК-Клиент

Смартфон

Производительный aSAN





Hosts	3
CPU	2*Intel® Xeon® CPU E5-2680 v4® 2.4Hz
RAM	128GB
Disk	2*Intel S4600 SSD , 6*1T HDD
NIC	2* 10GE

aCloud ver.	HCI 5.8.6
VSAN ver.	VSAN6.6
Tool	IOmeter
IO depth	32

Performance v.s. vSAN:

IOPS avg.: **50%** ↑

Throughput avg.: **90%** ↑

Производительный aSAN

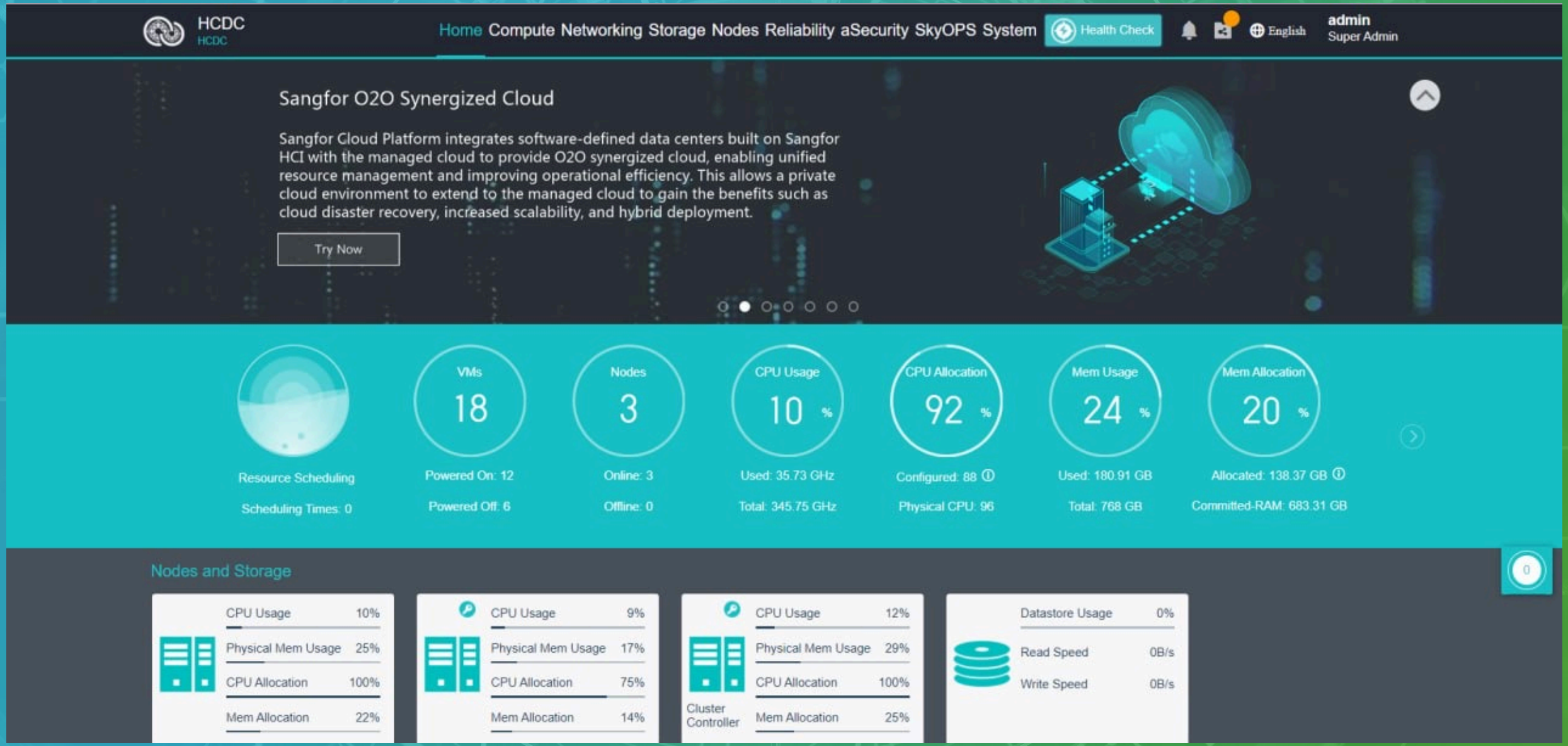
```
[root@localhost ~]# sysbench cpu --cpu-max-prime=10000 --threads=2 --time=10 --events=0 run
sysbench 1.0.20 (using bundled LuaJIT 2.1.0-beta2)

Running the test with following options:
Number of threads: 2
Initializing random number generator from current time


Prime numbers limit: 10000

Initializing worker threads...

Threads started!

CPU speed:
    events per second:  1578.05

General statistics:
    total time:                          10.0006s
    total number of events:              15785

Latency (ms):
         min:                                    1.19
         avg:                                    1.27
         max:                                   11.20
         95th percentile:                        1.58
         sum:                                19986.10

Threads fairness:
    events (avg/stddev):           7892.5000/74.50
    execution time (avg/stddev):   9.9931/0.00
```

VMware

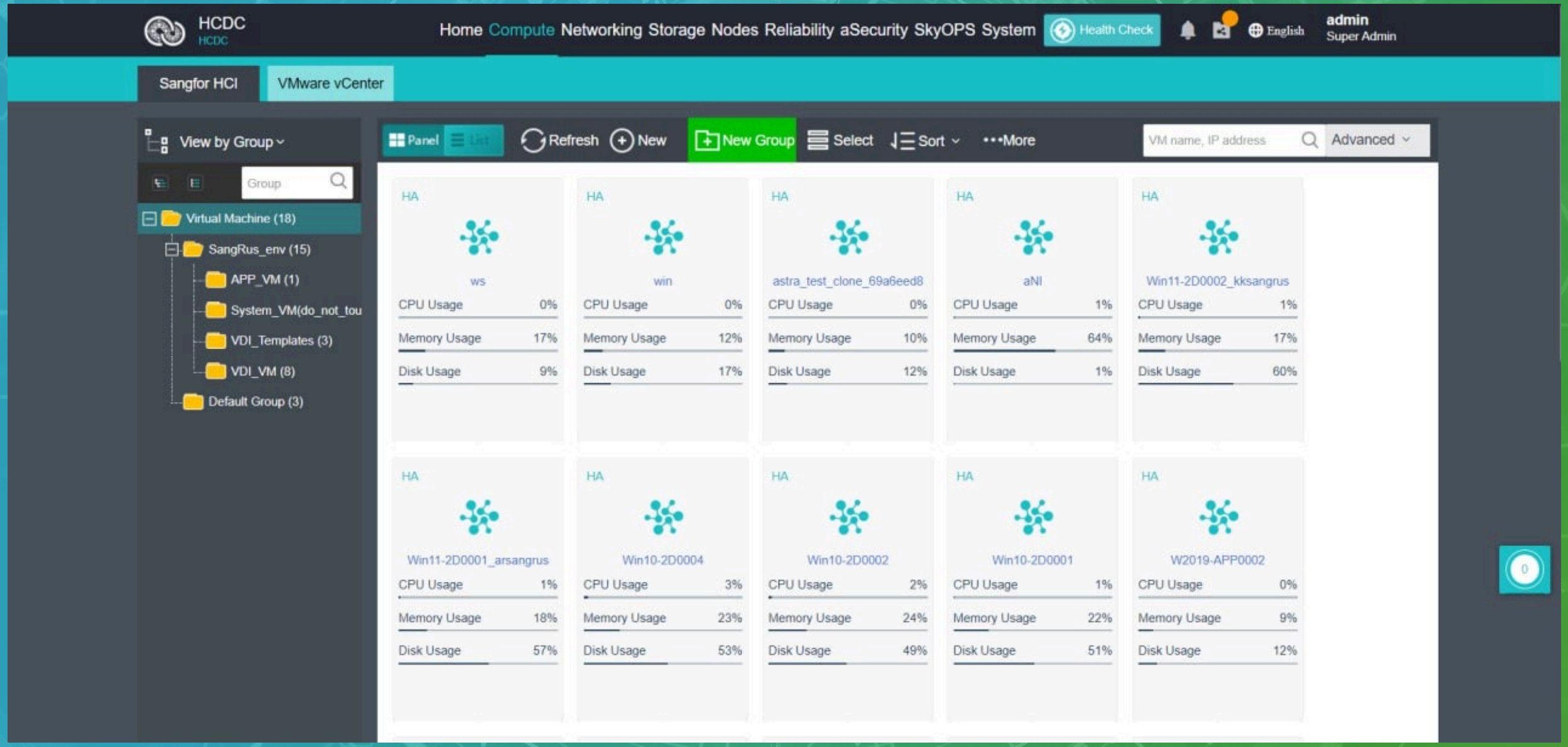
```
Initializing worker threads...

Threads started!

CPU speed:
    events per second:  2365.06

General statistics:
    total time:                          10.0007s
    total number of events:              23656

Latency (ms):
         min:                                    0.79
         avg:                                    0.84
         max:                                   12.89
         95th percentile:                        1.04
         sum:                                19985.76

Threads fairness:
    events (avg/stddev):           11828.0000/186.00
    execution time (avg/stddev):   9.9929/0.00

[test@localhost ~]$
```

Sangfor

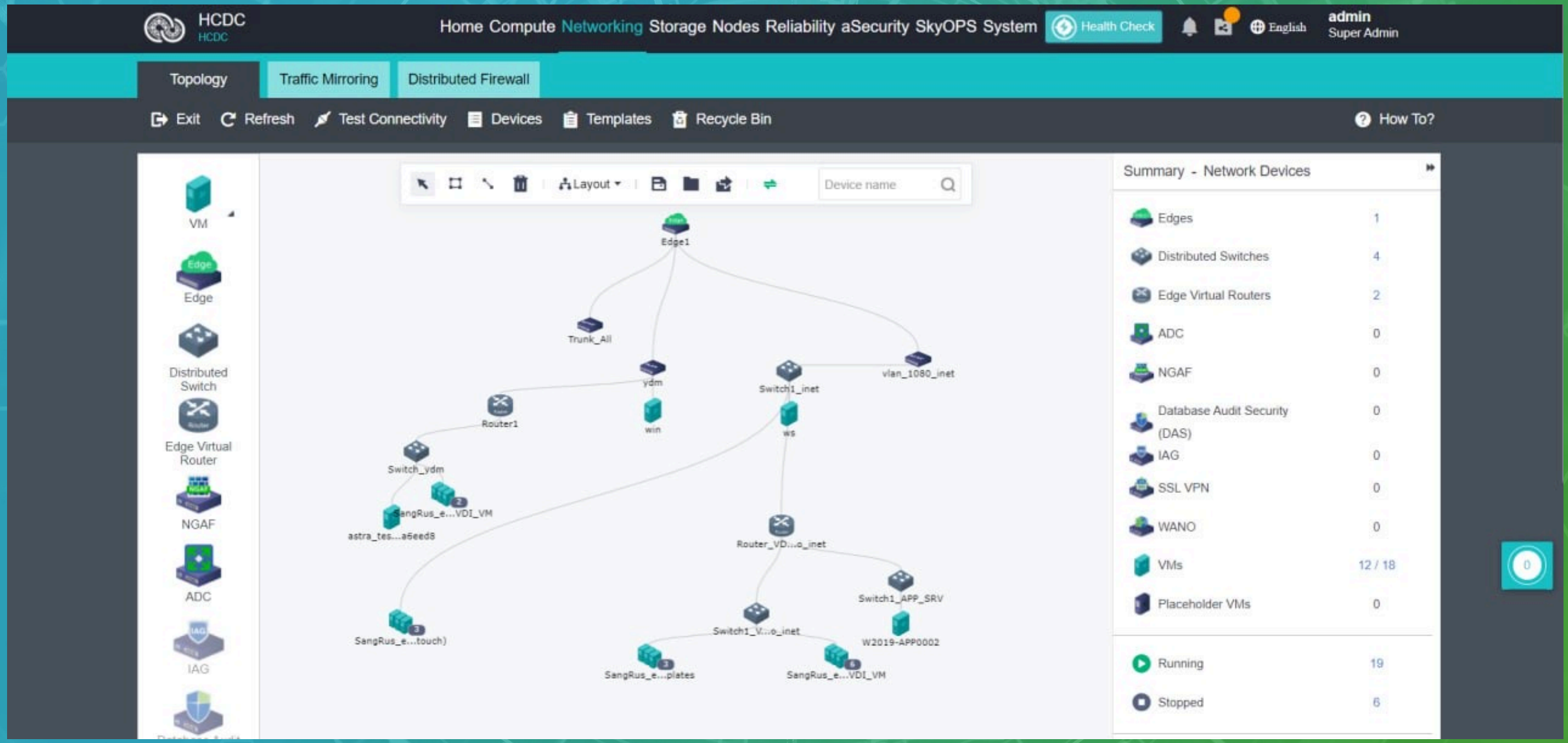
Просто и удобно



Просто и удобно

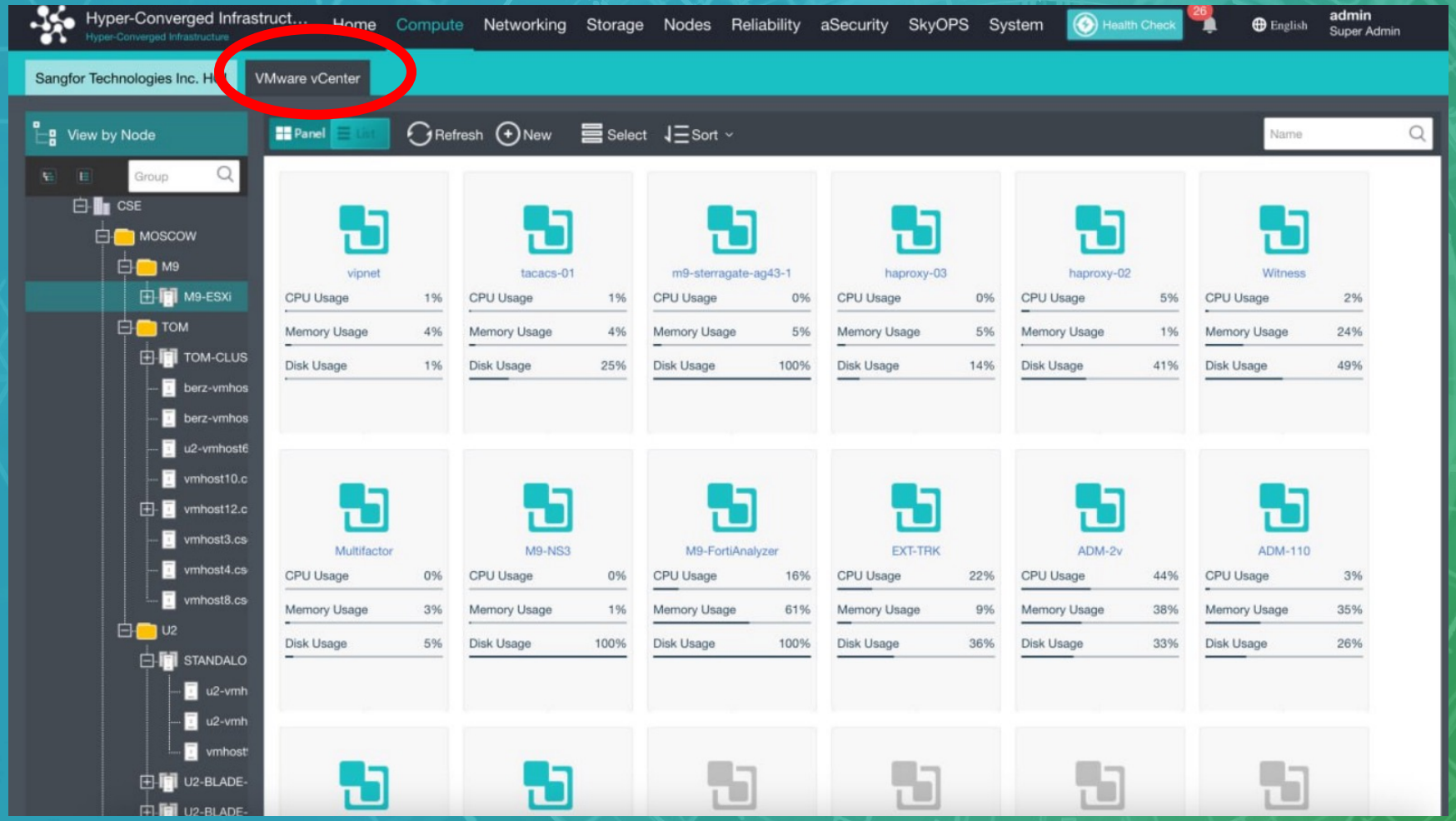


Просто и удобно



Встроенный Backup и DR

Управление VMware из Sangfor HCI+миграция



Возможность миграции виртуальных машин, подключенных к vCenter

Конвертация и миграция виртуальных машин и физических серверов в HCI с помощью агента

Миграция с различных платформ

- **P2V Для Windows OS**

  P2V Миграция Windows с физического хоста Windows на Sangfor HCI через сетевое взаимодействие.

- **P2V Linux OS**

  P2V Миграция Linux с физического хоста на Sangfor HCI через сетевое взаимодействие.

- **V2V system migration**

  Миграция виртуальных машин с других платформ таких как VMware на Sangfor HCI платформу через сетевое взаимодействие.

Лицензирование

Тип	Описание продукта	Дополнительно
HCI Software	Server Virtualization - **Mandatory**	Per CPU Socket
	Storage Virtualization - **Optional**	Per CPU Socket
	Network Virtualization - **Optional**	Per CPU Socket
SCP Cloud Management	Private / Public Cloud	Per CPU Socket
Heterogenous Management	Manage VMware Machines	Per VM
Disaster Recovery	Disaster Recovery	Per VM
CDP	Continuous / Realtime Backup	Per VM
NFV	Security Virtualization	Per Appliance
Container	Kubernetes	Per Instance/Node

Почему нужно менять VMware

Нейро
На основе источников, возможны неточности

Изначально установленная дата окончания общей поддержки (End of General Support, EoGS) для продуктов VMware vSphere 7.x и VMware vSAN 7.x была назначена на 2 апреля 2025 года. Но теперь она продлена на 6 месяцев, до 2 октября 2025 года. 1

После этой даты для пользователей больше не будет доступных обновлений и патчей продукта, в том числе по информационной безопасности. Апдейты версии 7.0 можно будет получить только в рамках Technical Guidance Phase, то есть в виде кастомной платной доработки от самого вендора. В России она будет недоступна. 3

Также известно, что срок жизни версии VMware ESXi 7.0 истечёт **2 апреля 2027 года**. 4

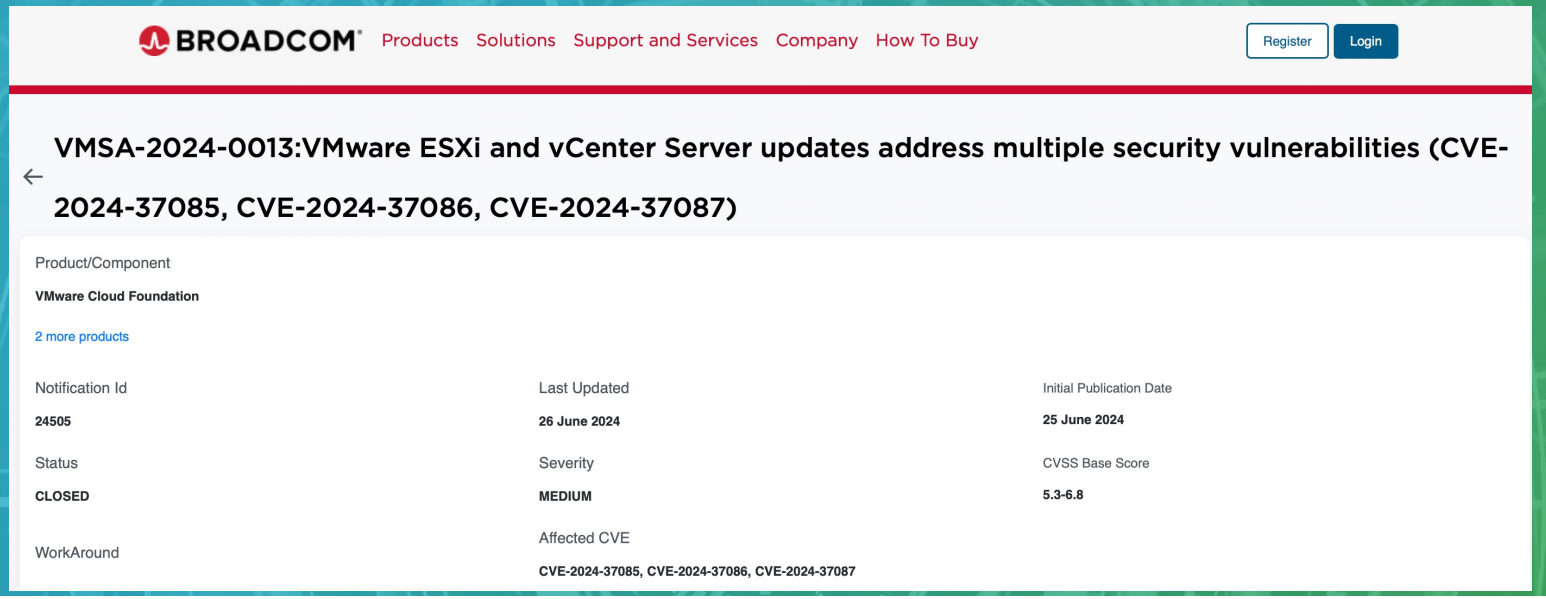
vm-guru.com 1 | internet-lab.ru 2 | habr.com 3

Окончание поддержки текущих версий производителем

13 найденных уязвимостей за последние 3 года, из них
Critical – 5
High – 3
https://cve.mitre.org/cgi-bin/cvekey.cgi?keyword=Vmware+ESXi

Name	Description
CVE-2024-37086	VMware ESXi contains an out-of-bounds read vulnerability. A malicious actor with local administrative privileges on a virtual machine with an existing snapshot may trigger an out-of-bounds read leading to a denial-of-service condition of the host.
CVE-2024-37085	VMware ESXi contains an authentication bypass vulnerability. A malicious actor with sufficient Active Directory (AD) permissions can gain full access to an ESXi host that was previously configured to use AD for user management https://blogs.vmware.com/vsphere/2012/09/joining-vsphere-hosts-to-active-directory.html by re-creating the configured AD group ('ESXi Admins' by default) after it was deleted from AD.
CVE-2024-22273	The storage controllers on VMware ESXi, Workstation, and Fusion have out-of-bounds read/write vulnerability. A malicious actor with access to a virtual machine with storage controllers enabled may exploit this issue to create a denial of service condition or execute code on the hypervisor from a virtual machine in conjunction with other issues.
CVE-2024-22255	VMware ESXi, Workstation, and Fusion contain an information disclosure vulnerability in the UHCI USB controller. A malicious actor with administrative access to a virtual machine may be able to exploit this issue to leak memory from the vmx process.
CVE-2024-22254	VMware ESXi contains an out-of-bounds write vulnerability. A malicious actor with privileges within the VMX process may trigger an out-of-bounds write leading to an escape of the sandbox.
CVE-2024-22253	VMware ESXi, Workstation, and Fusion contain a use-after-free vulnerability in the UHCI USB controller. A malicious actor with local administrative privileges on a virtual machine may exploit this issue to execute code as the virtual machine's VMX process running on the host. On ESXi, the exploitation is contained within the VMX sandbox whereas, on Workstation and Fusion, this may lead to code execution on the machine where Workstation or Fusion is installed.
CVE-2024-22252	VMware ESXi, Workstation, and Fusion contain a use-after-free vulnerability in the XHCI USB controller. A malicious actor with local administrative privileges on a virtual machine may exploit this issue to execute code as the virtual machine's VMX process running on the host. On ESXi, the exploitation is contained within the VMX sandbox whereas, on Workstation and Fusion, this may lead to code execution on the machine where Workstation or Fusion is installed.
CVE-2023-36628	A flaw exists in VASA which allows users with access to a vSphere/ESXi VMware admin on a FlashArray to gain root access through privilege escalation.
CVE-2023-20867	A fully compromised ESXi host can force VMware Tools to fail to authenticate host-to-guest operations, impacting the confidentiality and integrity of the guest virtual machine.
CVE-2022-31705	VMware ESXi, Workstation, and Fusion contain a heap out-of-bounds write vulnerability in the USB 2.0 controller (EHCI). A malicious actor with local administrative privileges on a virtual machine may exploit this issue to execute code as the virtual machine's VMX process running on the host. On ESXi, the exploitation is contained within the VMX sandbox whereas, on Workstation and Fusion, this may lead to code execution on the machine where Workstation or Fusion is installed.
CVE-2022-31699	VMware ESXi contains a heap-overflow vulnerability. A malicious local actor with restricted privileges within a sandbox process may exploit this issue to achieve a partial information disclosure.
CVE-2022-31696	VMware ESXi contains a memory corruption vulnerability that exists in the way it handles a network socket. A malicious actor with local access to ESXi may exploit this issue to corrupt memory leading to an escape of the ESXi sandbox.
CVE-2022-31681	VMware ESXi contains a null-pointer deference vulnerability. A malicious actor with privileges within the VMX process only, may create a denial of service condition on the host.

Патчинг уязвимостей?



Response Matrix:

VMware Product	Version	Running On	CVE	CVSSv3	Severity	Fixed Version	Workarounds	Additional Documentation
ESXi	8.0	Any	CVE-2024-37085	6.8	Moderate	ESXi80U3-24022510	KB369707	None
ESXi	7.0	Any	CVE-2024-37085	6.8	Moderate	No Patch Planned	KB369707	None
VMware Cloud Foundation	5.x	Any	CVE-2024-37085	6.8	Moderate	Patch Pending	KB369707	None
VMware Cloud Foundation	4.x	Any	CVE-2024-37085	6.8	Moderate	No Patch Planned	KB369707	None

А где версия 6.x?

https://support.broadcom.com/web/ecx/support-content-notification/-/external/content/SecurityAdvisories/0/24505

Что говорит ФСТЭК

Банк данных угроз безопасности информации

Федеральная служба по техническому и экспортному контролю

ФСТЭК России

Государственный научно-исследовательский испытательный институт проблем технической защиты информации

ФАУ «ГНИИИ ПТЗИ ФСТЭК России»

Угрозы | Уязвимости | Тестирование обновлений | Документы | Обратная связь | Обновления | Участники | Обучение | БДУ АСУ ТП | ФСТЭК России

Поиск

Главная / Список уязвимостей / BDU:2024-05045

BDU:2024-05045: Уязвимость гипервизора VMware ESXi, связанная с недостатками процедуры аутентификации, позволяющая нарушителю обойти процедуру аутентификации

Вид

Описание уязвимости	Уязвимость гипервизора VMware ESXi связана с недостатками процедуры аутентификации. Эксплуатация уязвимости может позволить нарушителю, действующему удаленно, обойти процедуру аутентификации
Вендор	VMware Inc.
Наименование ПО	VMware Cloud Foundation, VMware ESXi
Версия ПО	4.0 (VMware Cloud Foundation) 7.0 (VMware ESXi) 5.0 (VMware Cloud Foundation) от 8.0 до ESXi80U3-24022510 (VMware ESXi)

ПОСЛЕДНИЕ ИЗМЕНЕНИЯ

29.07.2024
Уязвимость системы работы с заявками и инцидентами GLPI, связанная с неправильным управлением привилегиями, позволяющая нарушителю раскрыть защищаемую информацию

29.07.2024
Уязвимость системы работы с заявками и инцидентами GLPI, связанная с неправильной нейтрализацией входных данных во время генерации веб-страницы, позволяющая нарушителю создавать вредоносную внешнюю ссылку

https://bdu.fstec.ru/vul/2024-05045

Всего 146 записей об уязвимостях в Vmware с 1 марта 2022 по 29 июля 2024 на сейте ФСТЭК

Еще немного про уязвимости

VMware предупреждает клиентов о начале эксплуатации **критической CVE-2024-38812 в vCenter Server,** которая была **отнесена поставщиком к категории Hard-to-Fix**.
VMware выпустила срочное обновление своего бюллетеня VMSA-2024-0019, в котором признал факт активных атак, нацеленных на CVE-2024-38812 и CVE-2024-38813, призывая клиентов отдать высокий приоритет развертыванию доступных исправлений.
Уязвимость была впервые обнаружена еще пять месяцев назад командой **TZL** на китайском хакерском конкурсе **Matrix Cup 2024,** организованном **Qihoo 360 и Beijing Huayun'an Information Technology,** и имеет CVSS 9,8/10.
Уязвимость описывается как переполнение кучи в реализации протокола распределенной вычислительной среды/удалённого вызова процедур (DCERPC) в **vCenter Server.**
Компания **VMware** отметила, что злоумышленник, имеющий сетевой доступ к **vCenter Server,** может активировать эту уязвимость, отправив специально созданный сетевой пакет, потенциально приводящий к RCE.
На протяжении четырех месяцев компания предпринимала попытки исправить опасную ошибку.
Так, как признались в VMware, исправления 17 сентября 2024 года не в полной мере смогли закрыть влияние CVE-2024-38812.
Гигант виртуализации устранил уязвимости, выпустив: vCenter Server 8.0 U3b и 7.0 U3s, VMware Cloud Foundation 5.x (Исправлено в 8.0 U3b) и VMware Cloud Foundation 4.x (исправлено в 7.0 U3s).

А можно и мне Sangfor?

Использование иностранного программного обеспечения виртуализации в Российской Федерации в настоящее время имеет определенные ограничения.

Ограничения связанны с необходимостью использования сертифицированного программного обеспечения, невозможности использования иностранного программного обеспечения и необходимости согласования использования иностранного программного обеспечения в некоторых областях применения.

В случае, если вы являетесь оператором ИСПДн, то вы имеете право приобретать и использовать средство виртуализации Sangfor, при этом вы имеете право принять решение и провести оценку его соответствия в форме приемки и испытаний.

В случае, если вы являетесь субъектом КИИ, и в процессе категорирования определили, что вы используете незначимые объекты КИИ, то вы имеете право приобретать и использовать средство виртуализации Sangfor без ограничений.

В случае, если вы являетесь субъектом КИИ, и используете значимые объекты КИИ но при этом НЕ являетесь заказчиком, осуществляющим закупки в соответствии с Федеральным законом от 18 июля 2011 г. N 223-ФЗ "О закупках товаров, работ, услуг отдельными видами юридических лиц" или являетесь организацией-заказчиком с муниципальным участием, осуществляющей закупки в соответствии с Федеральным законом от 18 июля 2011 г. N 223-ФЗ "О закупках товаров, работ, услуг отдельными видами юридических лиц" **вы имеете право приобретать и использовать средство виртуализации Sangfor. При этом имеете право принять решение и провести оценку его соответствия в форме приемки и испытаний.**

Более подробная информация об ограничениях применения несертифицированного и иностранного программного обеспечения приведена в приложении №1.

Сравнение цен

	5 двухсокетных серверов по 32 ядра, 100 Тб SDS									
	Sangfor (лицензии постоянные, продлеватеся только техническая поддержка)					Vmware (подписка)				
	лицензируется по процессорам					лицензируется по ядрам, vSan по объему				
				Виртуализация						
aSV	Server virtualization, HA, DRS, Automated Hot Add, backup, clone, ...	10	$5 624	$56 240		VCF-VSP-STD-8-3Y	VMware vSphere Standard 8	320	$339,06	$108 499,20
aNET	Network virtualization, Distributed Firewall, Drawable topology, visualized network, aSwitch, aRouter...	0	$2 704	$0						**$108 499,20**
aSAN	Storage virtualization, 2-3 copies, SSD read and write acceleration, data locality, Striping.	0	$11 368	$0						
HCISS-1Y	Software license subscription & upgrade, upgrade license included for 1 year, CTI technical support 7*24 for 1 year, 10% of HCI License	3	$5 624	$16 872						
RSHCI-1Y	Russian Technical Support for HCI Software 8*5, 20% of HCI License	3	$11 248	$33 744						
				$106 856						
				Виртуализация + SDS						
aSV	Server virtualization, HA, DRS, Automated Hot Add, backup, clone, ...	10	$5 624	$56 240		VCF-VSP-FND-8-3Y	VMware vSphere Foundation 8	320	$915,48	$292 953,60
aNET	Network virtualization, Distributed Firewall, Drawable topology, visualized network, aSwitch, aRouter...	0	$2 704	$0		VCF-VSAN-8-3Y	VMware vSAN 8	100	$1 424,08	$142 408,00
aSAN	Storage virtualization, 2-3 copies, SSD read and write acceleration, data locality, Striping.	10	$11 368	$113 680						**$435 361,60**
HCISS-1Y	Software license subscription & upgrade, upgrade license included for 1 year, CTI technical support 7*24 for 1 year, 10% of HCI License	3	$16 992	$50 976						
RSHCI-1Y	Russian Technical Support for HCI Software 8*5, 20% of HCI License	3	$33 984	$101 952						
				$322 848						
				Гиперконвергенция						
aSV	Server virtualization, HA, DRS, Automated Hot Add, backup, clone, ...	10	$5 624	$56 240		VCF-CLD-FND-5-3Y	VMware Cloud Foundation 5	320	$2 373,46	$759 507,20
aNET	Network virtualization, Distributed Firewall, Drawable topology, visualized network, aSwitch, aRouter...	10	$2 704	$27 040						**$759 507,20**
aSAN	Storage virtualization, 2-3 copies, SSD read and write acceleration, data locality, Striping.	10	$11 368	$113 680						
HCISS-1Y	Software license subscription & upgrade, upgrade license included for 1 year, CTI technical support 7*24 for 1 year, 10% of HCI License	3	$19 696	$59 088						
RSHCI-1Y	Russian Technical Support for HCI Software 8*5, 20% of HCI License	3	$39 392	$118 176						
				$374 224						

Sangfor HCI и VDI

HCI

VDI

Спасибо!

CIS@sangrus.com