

ООО Дигилабс

ОГРН: 1207700443532, ИНН: 7707445960, КПП: 770701001

Программный продукт ХантерЛог (HunterLog)

Документация, содержащая информацию, необходимую для эксплуатации экземпляра программного обеспечения, предоставленного для проведения экспертной оценки в Экспертном совете при Минцифры России

Москва
2022 г.

Оглавление

1.	ОПИСАНИЕ СИСТЕМЫ, ВХОД НА ПОРТАЛ	3
2.	ОБЩИЙ ВИД ПОРТАЛА.....	3
3.	ОСНОВНЫЕ РАЗДЕЛЫ И НАЗНАЧЕНИЕ.....	3
	События Active directory	3
	DNS & DHCP.....	6
	VMWare:.....	8
	«ESXi»	8
	«vCenter».....	10
	Exchange:	15
	«Мобильные клиенты».....	15
	«Системные события Exchange»	16
	«Отслеживание писем Exchange»	17
	«Linux»	19
	«Локальный компьютер».....	20
	«NetFlow».....	24
	«VPN».....	25
	«Сетевые папки».....	26
4.	ЮРИДИЧЕСКАЯ ИНФОРМАЦИЯ.....	27
	Авторские права	27
	Содержание документа	27

1. ОПИСАНИЕ СИСТЕМЫ, ВХОД НА ПОРТАЛ

Система ХантерЛог - централизованная система аудита для предприятий любого размера. Обеспечивает эффективный сбор, обработку и хранение событий с поддерживаемых сервисов. Отслеживание и своевременная реакция на соответствующие сообщения могут предсказать и предотвратить сбои, ошибки, низкую скорость работы и возможные атаки злоумышленников на ключевые корпоративные информационные системы.

Доступ к системе осуществляется через веб-интерфейс при помощи любого из поддерживаемых браузеров. У портала простая и интуитивно понятная навигация. Вход осуществляется через логин и пароль, выданный ранее.

2. ОБЩИЙ ВИД ПОРТАЛА

После аутентификации на портале открывается окно «События Active directory». Внешний вид представлен на рисунке 1.

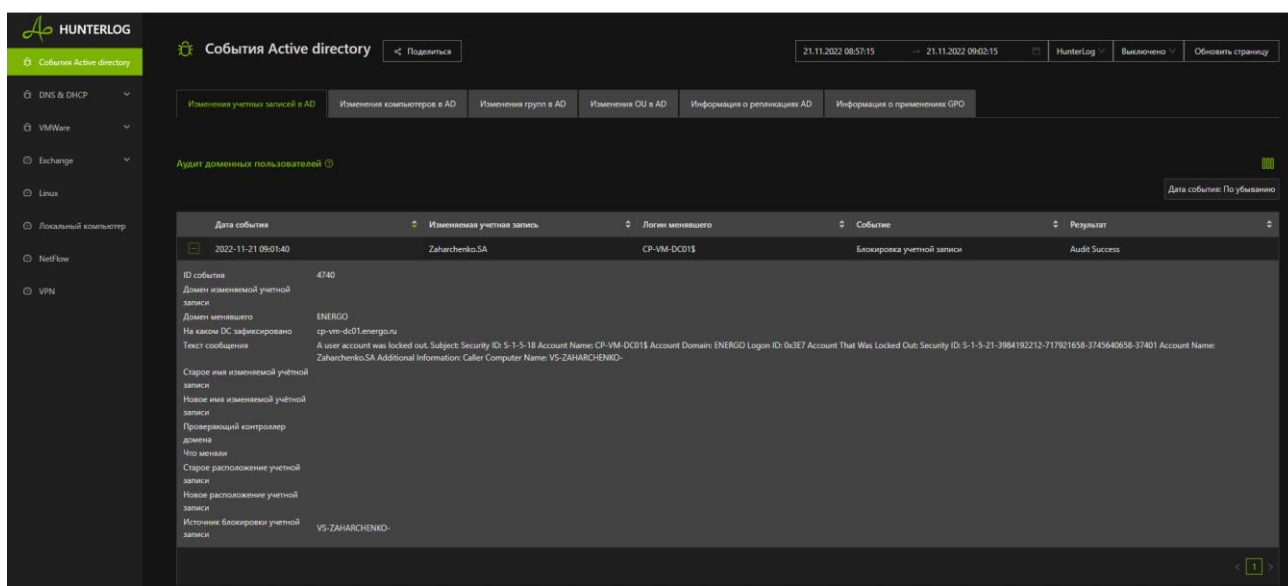


Рис.1 (общий вид портала)

Доступны следующие элементы навигации по portalу:

- Меню слева — перемещение в любой интересующий раздел;
- Выбор диапазона в верхнем правом углу — возможность конкретизации условий поиска с указанием временного диапазона и выбором нужного сервиса с автообновлением результатов;
- Команда «Поделиться» - возможность скопировать ссылку на конкретную выборку событий.

Далее в документе приводится детальная информация по каждому разделу портала, а также типовые сценарии работы в реальной инфраструктуре.

3. ОСНОВНЫЕ РАЗДЕЛЫ И НАЗНАЧЕНИЕ

В данном разделе приведено детальное описание всех экранов портала.

События Active directory

Экран представляет собой агрегированную информацию по следующим метрикам:

- Изменение учетных записей в AD;
- Изменения OU/CN;

- Изменения в группах;
- Изменения компьютеров;
- Репликация AD.

Информация выводится за выбранный период времени и для выбранного сервиса. Для автоматического обновления данных можно выставить период в секундах.

Внешний вид экрана «Изменение учетных записей в AD» представлен на рисунке 2. Показаны учетные записи, логин менявшего, событие, результат. При детализации строки представлена дополнительная информация по домену, тексту сообщения и т.п.

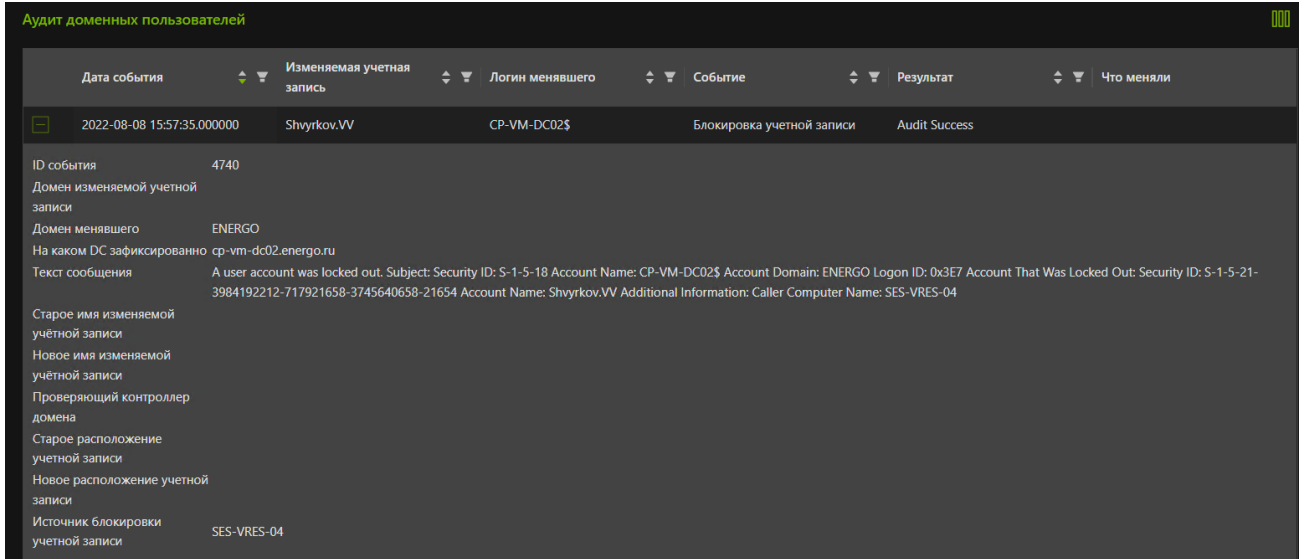


Рис. 2

На следующей вкладке «Изменения OU/CN» (рис.3) отображается информация об изменении подразделений и групп в Active directory. Доступна детализация каждой строки, с указанием логина менявшего, старое и новое расположение, старое и новое имя, а также событие.

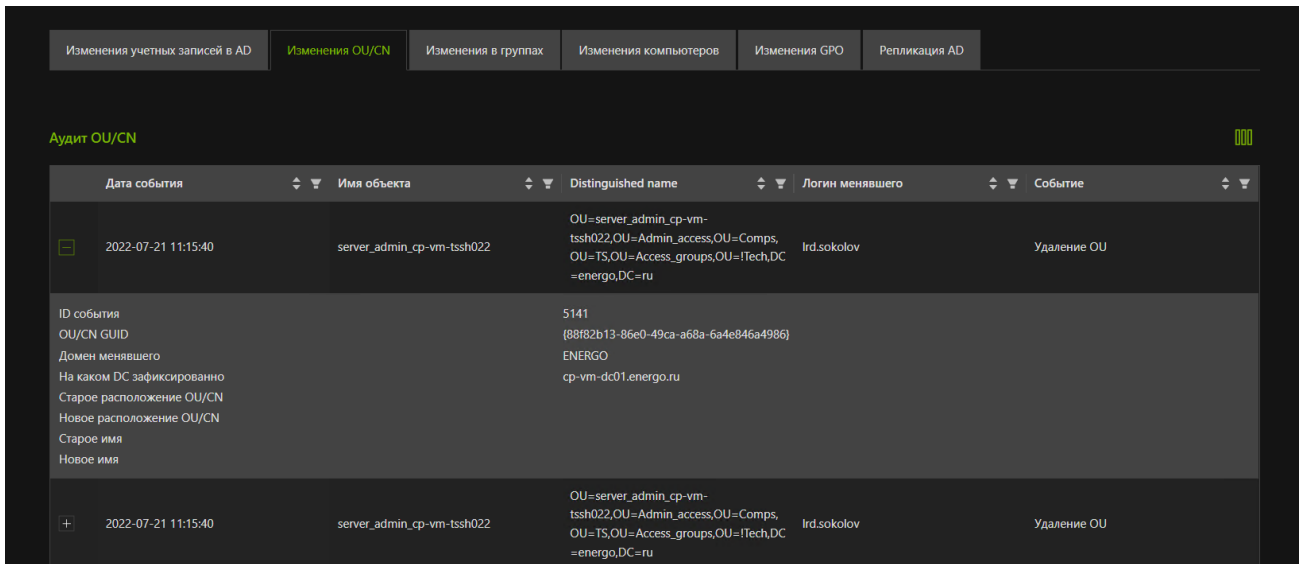


Рис. 3

На вкладке «Изменения в группах» (рис.4) отображаются данные по изменению доменных групп в разрезе имени группы, изменяющего пользователя, события, добавленного/удаленного в группу. При детализации строки отображается дополнительная развернутая информация, включающая текст сообщения, на каком DC зафиксировано изменение, и детальная информация по изменению.

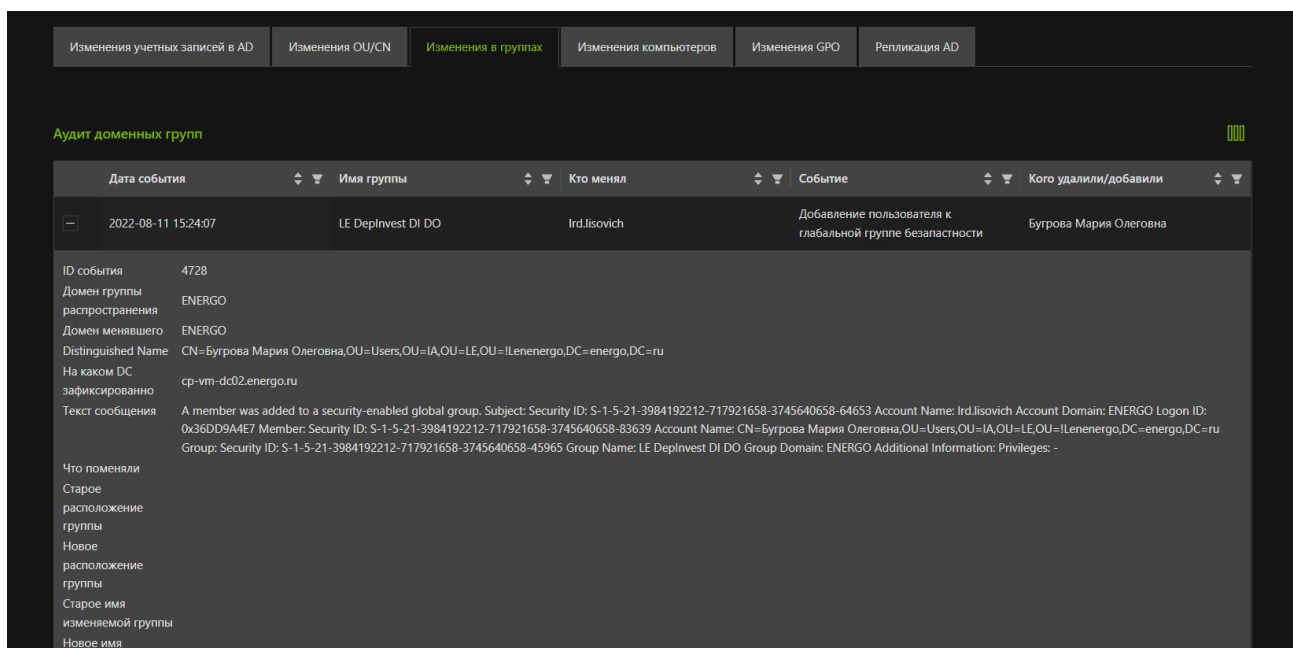


Рис. 4

На следующей вкладке «Изменения компьютеров» (рис.5) представлена информация об изменении данных, включающих такие события как: изменение учетных записей компьютера, добавление компьютера в домен, удаление компьютера из домена, перемещение учетной записи компьютера по структуре AD, переименование компьютера. Детализация строки содержит данные по старым/новым именам, результат события, текст сообщения.

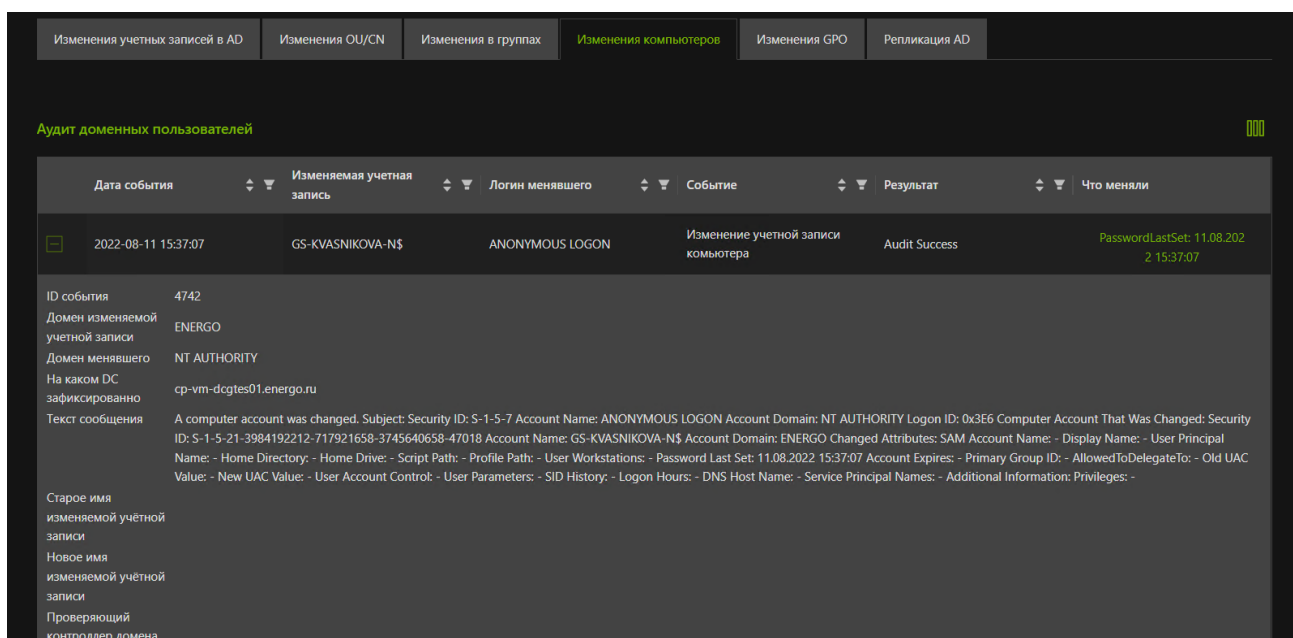


Рис. 5

Вкладка «Репликация AD» (рис.6) отображает информацию о проблемах в AD с описанием случившегося, включая тип сообщения, его текст и DC, где событие было зафиксировано.

Дата события	Тип сообщения	Что случилось	На каком DC зафиксировано
2022-08-11 13:59:49	information	Active Directory Domain Services encountered a write conflict when applying replicated changes to the following object	LEN-DC1.energo.ru
<p>ID события 1955</p> <p>Текст сообщения Active Directory Domain Services encountered a write conflict when applying replicated changes to the following object. Object: CN=Таранченко Анастасия Юрьевна,OU=2018,OU=UserOut,OU=ILenenergo,DC=energo,DC=ru Time in seconds: 0 Event log entries preceding this entry will indicate whether or not the update was accepted. A write conflict can be caused by simultaneous changes to the same object or simultaneous changes to other objects that have attributes referencing this object. This commonly occurs when the object represents a large group with many members, and the functional level of the forest is set to Windows 2000. This conflict triggered additional retries of the update. If the system appears slow, it could be because replication of these changes is occurring. User Action Use smaller groups for this operation or raise the forest functional level to Windows Server 2003.</p>			
2022-08-11 11:49:13	information	Active Directory Domain Services encountered a write conflict when applying replicated changes to the following object	cp-vm-dc02.energo.ru
2022-08-11 10:35:27	information	The following object was created on a remote directory service with an object name that already exists on the local directory service	cp-vm-dc04.energo.ru

Рис. 6

На всех вкладках в таблицах доступен отбор и сортировка записей каждой колонки для удобства сбора данных.

DNS & DHCP

Раздел «DNS & DHCP» раздел на два подраздела – DNS и DHCP, где выведена детальная информация по событиям, а также реализован удобный поиск по логам. **DHCP:**

На рисунке 7 представлена таблица с логами настроек DHCP Windows, где за выбранный период выводятся события в разрезе даты, описания области, логов менявшего, самого изменения, старых и новых значений, ip-адреса и имя DHCP- сервера.

Дата события	Событие	Область	Описание области	Логин менявшего
2022-11-09 13:01:45	EventID Старое значение срока аренды Новое значение срока аренды Что поменяли IP-адреса, добавленные или убранные из резервации IP-адреса, добавленные или убранные из исключения Имя DHCP-сервера	172.27.178.0	ecus2-lan-1-2	ENERGO\lrd.ozol
2022-11-09 13:01:45	EventID Старое значение срока аренды Новое значение срока аренды Что поменяли IP-адреса, добавленные или убранные из резервации IP-адреса, добавленные или убранные из исключения Имя DHCP-сервера	172.27.178.0	ecus2-lan-1-2	ENERGO\lrd.ozol
2022-11-09 13:01:44		172.27.178.0	ecus2-lan-1-2	ENERGO\lrd.ozol
2022-11-09 13:01:44		172.27.178.0	ecus2-lan-1-2	ENERGO\lrd.ozol
2022-11-09 13:01:44		172.27.178.0	ecus2-lan-1-2	ENERGO\lrd.ozol

Рис. 7

На следующей вкладке «Результаты работы службы DHCP Windows» (рис.8) отображается таблица, включающая следующие данные:

- Имя DHCP-сервера;
- Действие;
- Выданный/обновленный IP;

- Имя хоста клиента;
- MAC-адрес хоста-клиента.

Дата события	Имя DHCP-сервера	Действие	Выданный/обновленный IP	Имя хоста-клиента	MAC-адрес хоста-клиента
2022-11-21 09:40:19	sr-vm-dhcp01	Packet dropped because the server is in failover standby role or the hash of the client ID does not match	172.16.91.2		408D5CD4187E
Детали события Результат проверки, находится ли устройство в карантине: No Quarantine Information Время окончания карантина: No Quarantine Information ID объединяющий последовательность событий в логе: Общая информация о клиенте: Подробная информация о клиенте: ID связывающий все обновления IP клиентом: Ошибка обновления DNS:					
2022-11-21 09:40:15	sr-vm-dhcp01	Packet dropped because the server is in failover standby role or the hash of the client ID does not match	172.16.91.2		408D5CD4187E
2022-11-21 09:40:13	sr-vm-dhcp01	DNS update successful	172.26.248.61	39453.energo.ru	
2022-11-21 09:40:13	sr-vm-dhcp01	A lease was renewed by a client	172.26.248.61	39453.energo.ru	001AE8653AE7
2022-11-21 09:40:13	sr-vm-dhcp01	DNS update request to the named DNS server	172.26.248.61	39453.energo.ru	
2022-11-21 09:40:10	sr-vm-dhcp01	Packet dropped because the server is in failover standby role or the hash of the client ID does not match	172.16.91.34		001AE8D1A18F

Рис.8

DNS:

В подменю расположено две вкладки: «Аудит изменений DNS-записей» и «Запросы к DNS-серверам».

Аудит изменений DNS-записей (рис.9)

За выбранный период отображается информация о дате события, DNS-имени, событии, а также инициатора – кто менял.

Дата события	DNS имя	Событие	Кто менял
2022-12-01 08:36:52	DC=Tin-Fabrika.DC=energo.ru	Обновление DNS-записи	SYSTEM
Домен меньшего			
NT AUTHORITY			
2022-12-01 08:36:52	DC=229.129.DC=16.172.in-addr.arpa	Обновление DNS-записи	SYSTEM
Домен меньшего			
NT AUTHORITY			
2022-12-01 08:36:51	DC=A-KIRUMINA-V.DC=energo.ru	Обновление DNS-записи	SYSTEM
2022-12-01 08:36:34	DC=IG-Savenko.DC=energo.ru	Обновление DNS-записи	SYSTEM
2022-12-01 08:36:34	DC=85.161.DC=16.172.in-addr.arpa	Обновление DNS-записи	SYSTEM
2022-12-01 08:36:34	DC=IG-Savenko.DC=energo.ru	Обновление DNS-записи	SYSTEM
2022-12-01 08:36:34	DC=85.161.DC=16.172.in-addr.arpa	Обновление DNS-записи	SYSTEM
2022-12-01 08:36:21	DC=41.236.DC=28.172.in-addr.arpa	Обновление DNS-записи	dhcp_dns_updater
2022-12-01 08:36:11	DC=sr-vm-dhcp01.DC=energo.ru	Обновление DNS-записи	SYSTEM
2022-12-01 08:36:11	DC=35.238.DC=28.172.in-addr.arpa	Обновление DNS-записи	dhcp_dns_updater

Рис. 9

Запросы к DNS-серверам (рис.10)

Отображение информации в разрезе:

- Дата события;
- Имя DNS-сервера;
- Событие;
- Тип запроса;
- Запрашиваемое DNS-имя;
- Тип запрашиваемого имени;
- IP-адрес делавшего запрос.

По всем столбцам доступна сортировка данных.

Дата события	Имя DNS-сервера	Событие	Тип запроса	Запрашиваемое DNS имя	Тип запрашиваемого имени	IP-адрес делегирующего запроса
2022-12-01 08:36:56	cr-vm-dcve01	Ответ	Стандартный запрос	len-term01.energo.ru	A	172.25.248.53
Направление запроса Протокол передачи						
2022-12-01 08:36:56	cr-vm-dcve01	Запрос	Стандартный запрос	len-term01.energo.ru	A	172.25.248.53
Направление запроса Протокол передачи						
2022-12-01 08:36:56	cr-vm-dcve01	Ответ	Стандартный запрос	len-term03.energo.ru	A	172.25.248.53
Направление запроса Протокол передачи						
2022-12-01 08:36:56	cr-vm-dcve01	Запрос	Стандартный запрос	len-term03.energo.ru	A	172.25.248.53
Направление запроса Протокол передачи						
2022-12-01 08:36:56	cr-vm-dcve01	Ответ	Стандартный запрос	yandex.ru	A	172.25.248.23
Направление запроса Протокол передачи						
2022-12-01 08:36:56	cr-vm-dcve01	Запрос	Стандартный запрос	yandex.ru	A	172.25.248.23

Рис.10

VMWare:

Раздел «VMWare» состоит из двух подразделов «ESXi» и «vCenter», в которых представлена общая аналитика по виртуализации, ошибкам, аудиту.

«ESXi»

Данный подраздел представлен в виде следующих вкладок:

- Аудит событий ESXi (рис.11):

Дата события	Имя сервера esxi	Тип сообщения	Кто делал	Имя VM	Действие
2022-12-01 08:33:06	cr-hws-hv024	info		cd-vm-dbgg06	Removed
Сообщение info hostd[100182] [Originator@6876 sub=Vimtools-eventmgr] Event 3418739: Removed cd-vm-dbgg06 on cr-hws-hv024 from ha-datacenter					
Описание: Ошибка подключения. Информация об анализе подключения					
2022-12-01 08:32:59	cr-hws-hv029	info	vrsular	cd-vm-dbgg06	Registered
Сообщение info hostd[100081] [Originator@6876 sub=Vimtools-eventmgr: opID=ho-8094679d3-659c3263-01-01-45-6a01 user=vrsular] Event 3415439: Registered cd-vm-dbgg06 on cr-hws-hv029 in ha-datacenter					

Рис.11

Пользователю доступны следующие данные:

- Дата события;
- Имя сервера ESXi;
- Тип сообщения;
- Кто делал;
- Имя VM;
- Действие.

При детализации каждой строки доступно сообщение.

- Аудит событий безопасности ESXi (рис.12):

Дата события	Имя сервера esxi	Тип сообщения	Кто делал	Событие	Объект изменения	Имя роли
2022-12-01 08:36:42	cr-hws-hv027	info	root	Accepted password		
Сообщение info hostd[2099961] [Originator@6876 sub=Default: opID=esxi-44-3ee6] Accepted password for user root from 127.0.0.1						
Описание: Ошибка подключения. Информация об анализе подключения						
2022-12-01 08:36:42	cr-hws-hv027	info	root	logged in		
Сообщение info hostd[210030] [Originator@6876 sub=Vimtools-eventmgr: opID=esxi-44-3ee6 user=root] Event 2370991: User root@127.0.0.1 logged in (login time: Thursday, 01 December, 2022 05:36:42 AM, number of API invocations: 7, user agent: python/Python/3.5.9 (VMware): 7.0.1, vrb_5d)						
Описание: Ошибка подключения. Информация об анализе подключения						
2022-12-01 08:36:41	cr-hws-hv027	info	root	Accepted password		
2022-12-01 08:36:41	cr-hws-hv027	info	root	logged in		
2022-12-01 08:36:41	cr-hws-hv027	info	root	logged out		
2022-12-01 08:36:40	cr-hws-hv027	info	root	Accepted password		

Рис.12

На странице представлена информация в разрезе:

- Дата события;
- Имя сервера ESXi;
- Тип сообщения;
- Кто делал;
- Событие;
- Объект изменения;
- Имя роли.

При детализации каждой строки пользователю доступны следующие данные:

- Сообщение;
- Откуда подключались;
- Права наследуются?
- Информация об агенте подключения.

- **Аудит ошибок ESXi (рис.13):**

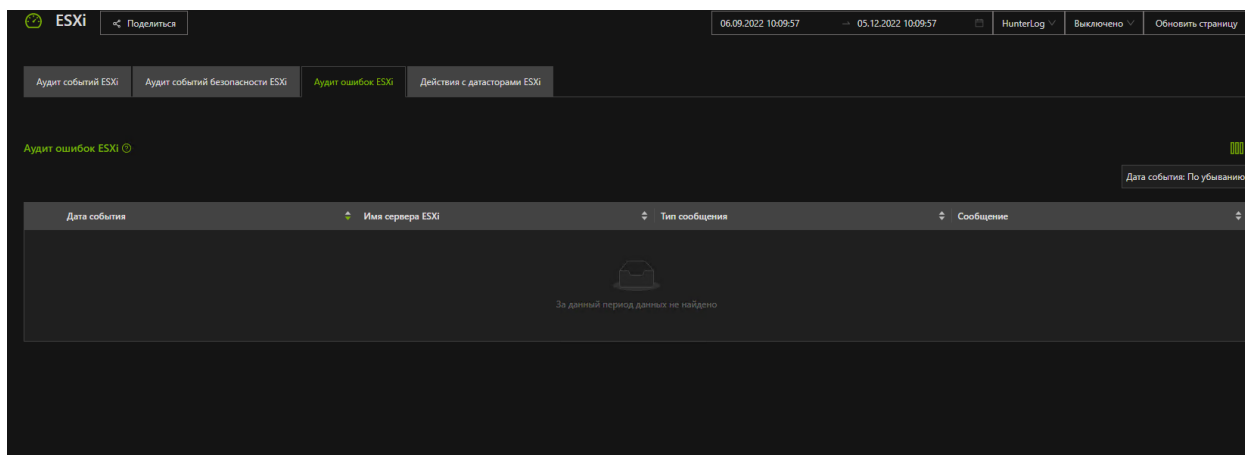


Рис.13

Аудит ошибок предоставляет информацию в разрезе:

- Дата события;
- Имя сервера ESXi;
- Тип сообщения;
- Сообщение.

За выбранный в примере период ошибок не обнаружено.

- **Действия с датасторами ESXi (рис.14):**

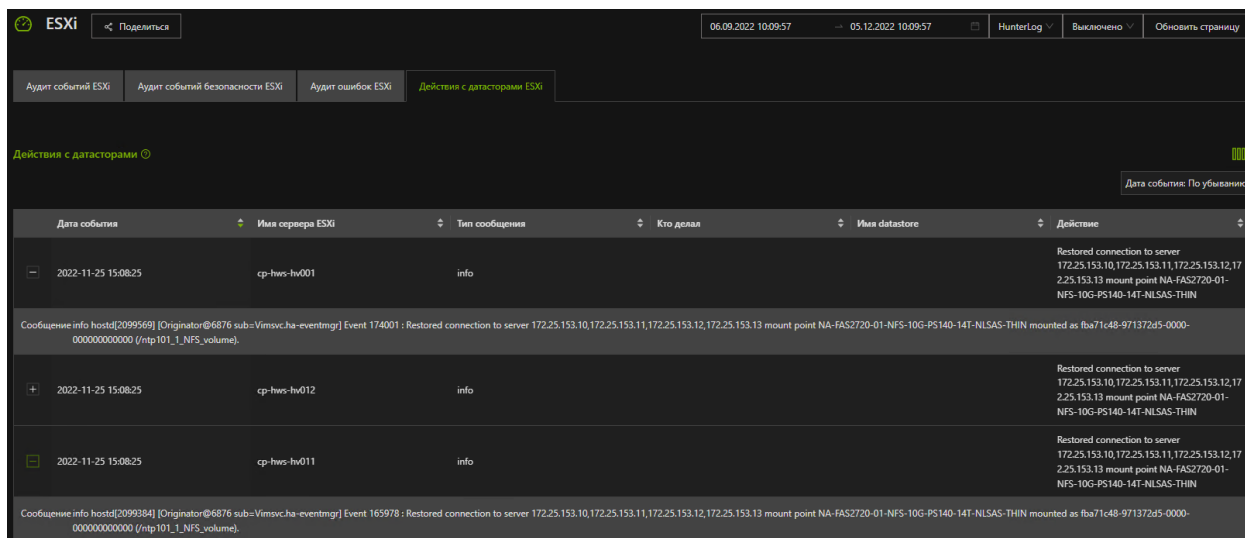


Рис.14

На данной вкладке представлена информация по действиям с датасторами в разрезе следующих полей:

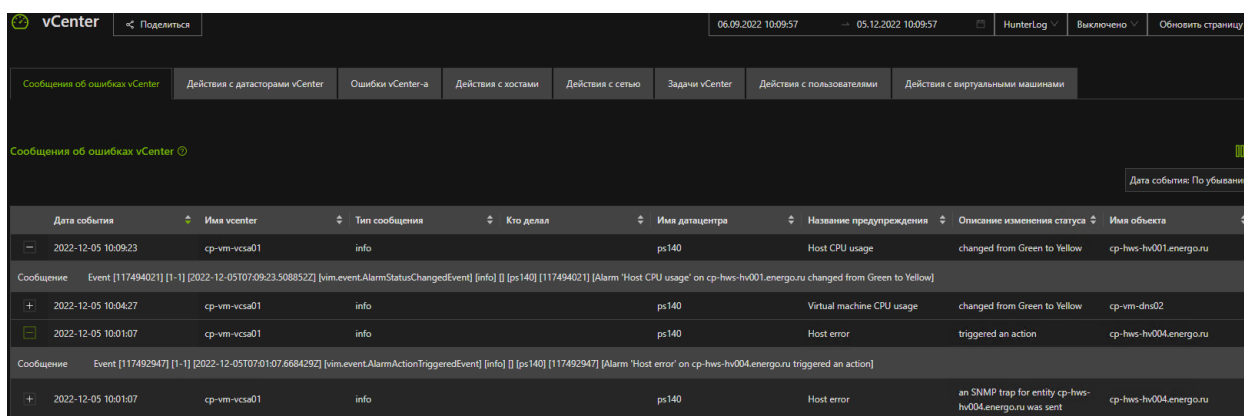
- Дата события;
- Имя сервера ESXi;
- Тип сообщения;
- Кто делал;
- Имя datastore;
- Действие.

При детализации строки есть возможность получить информацию о сообщении по этому событию.

«vCenter»

Данный подраздел представлен в виде следующих вкладок:

- Сообщения об ошибках vCenter (рис.15):



Дата события	Имя vcenter	Тип сообщения	Кто делал	Имя датацентра	Название предупреждения	Описание изменения статуса	Имя объекта
2022-12-05 10:09:23	cp-vm-vcsa01	info		ps140	Host CPU usage	changed from Green to Yellow	cp-hws-hv001.energo.ru
Сообщение Event [117494021] [1-1] [2022-12-05107:09:23.5088522] [vim.event.AlarmStatusChangedEvent] [info] [ps140] [117494021] [Alarm 'Host CPU usage' on cp-hws-hv001.energo.ru changed from Green to Yellow]							
2022-12-05 10:04:27	cp-vm-vcsa01	info		ps140	Virtual machine CPU usage	changed from Green to Yellow	cp-vm-dns02
2022-12-05 10:01:07	cp-vm-vcsa01	info		ps140	Host error	triggered an action	cp-hws-hv004.energo.ru
Сообщение Event [117492947] [1-1] [2022-12-05107:01:07.6684292] [vim.event.AlarmActionTriggeredEvent] [info] [ps140] [117492947] [Alarm 'Host error' on cp-hws-hv004.energo.ru triggered an action]							
2022-12-05 10:01:07	cp-vm-vcsa01	info		ps140	Host error	an SNMP trap for entity cp-hws-hv004.energo.ru was sent	cp-hws-hv004.energo.ru

Рис.15

На данной странице подробно представлена информация по ошибкам в виде следующих данных:

- Дата события;
- Имя vcenter;
- Тип сообщения;
- Кто делал;
- Имя датацентра;
- Название предупреждения;
- Описание изменения статуса;
- Имя объекта.

При детализации строки есть возможность получить информацию о сообщении по этому событию.

- Действия с датасторами vCenter (рис.16):

Дата события	Имя vcenter	Тип сообщения	Кто делал	Окружение	Действие	Имя датастора	Имя хоста VMWare
2022-11-21 16:54:05	cr-vm-vcsa01	info		ecus	Renamed datastore from datastore1 to hv056-DAS-ECUS-7T-NVME-01	datastore1	
Сообщение Event [114897286] [1-1] [2022-11-21T16:54:05.205833Z] [vim.event.DatastoreRenamedEvent] [info] [] [ecus] [114897286] [Renamed datastore from datastore1 to hv056-DAS-ECUS-7T-NVME-01 in ecus]							
2022-11-21 16:47:03	cr-vm-vcsa01	info		ecus	Discovered datastore	datastore1	cr-hws-hv056.energo.ru
2022-11-17 12:11:13	cr-vm-vcsa01	info		ecus	Renamed datastore from datastore1 to hv059-DAS-ECUS-7T-NVME-01	datastore1	
Сообщение Event [114113954] [1-1] [2022-11-17T09:11:13.746815Z] [vim.event.DatastoreRenamedEvent] [info] [] [ecus] [114113954] [Renamed datastore from datastore1 to hv059-DAS-ECUS-7T-NVME-01 in ecus]							
2022-11-17 12:10:53	cr-vm-vcsa01	info		ecus	Renamed datastore from datastore1 (1) to hv058-DAS-ECUS-7T-NVME-01	datastore1 (1)	

Рис.16

На странице представлены следующие данные:

- Дата события;
- Имя vCenter;
- Тип сообщения;
- Кто делал;
- Окружение;
- Действие;
- Имя датастора;
- Имя хоста VMWare.

По каждой строке выводится информация в виде сообщения. Пользователю доступна сортировка по каждой представленной колонке.

- Ошибки vCenter-a (рис.17):

Дата события	Тип сообщения	Кто делал
За данный период данных не найдено		

Рис.17

Все выявленные ошибки за указанный период отображаются на странице в разрезе:

- Дата события;
- Тип сообщения;
- Кто делал.

На рисунке отсутствует информация, так как за выбранный период ошибок не обнаружено.

- Действия с хостами (рис.18):

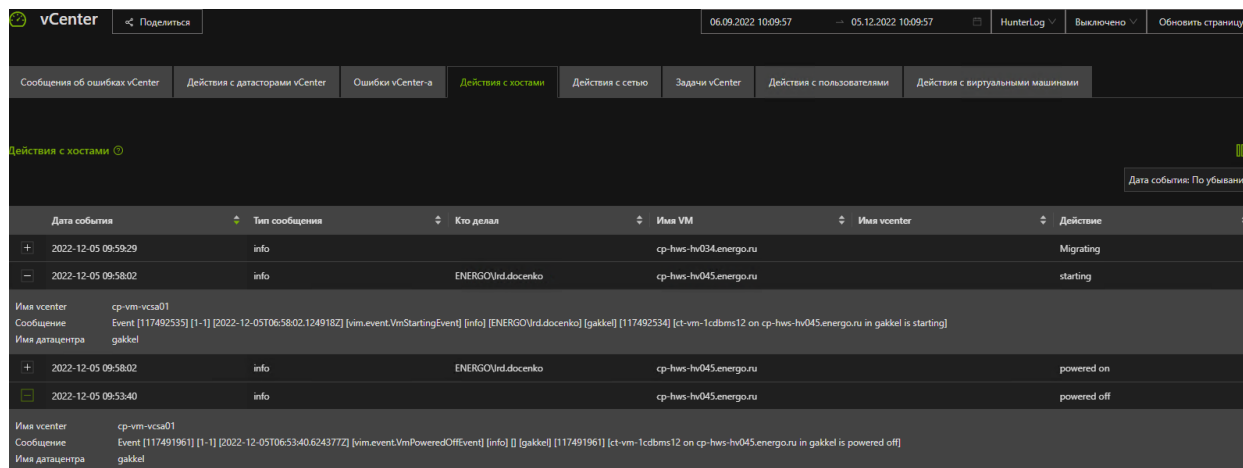


Рис.18

На текущей вкладке пользователю представлена детальная, подробная информация по событиям действий с хостами в разрезе:

- Дата события;
- Тип сообщения;
- Кто делал;
- Имя VM;
- Имя vcenter;
- Действие.

При детализации строки выводится информация, содержащая:

- Имя vcenter;
- Сообщение;
- Имя датацентра.

По всем колонкам доступна сортировка данных для удобства пользования.

- Действия с сетью (рис.19):

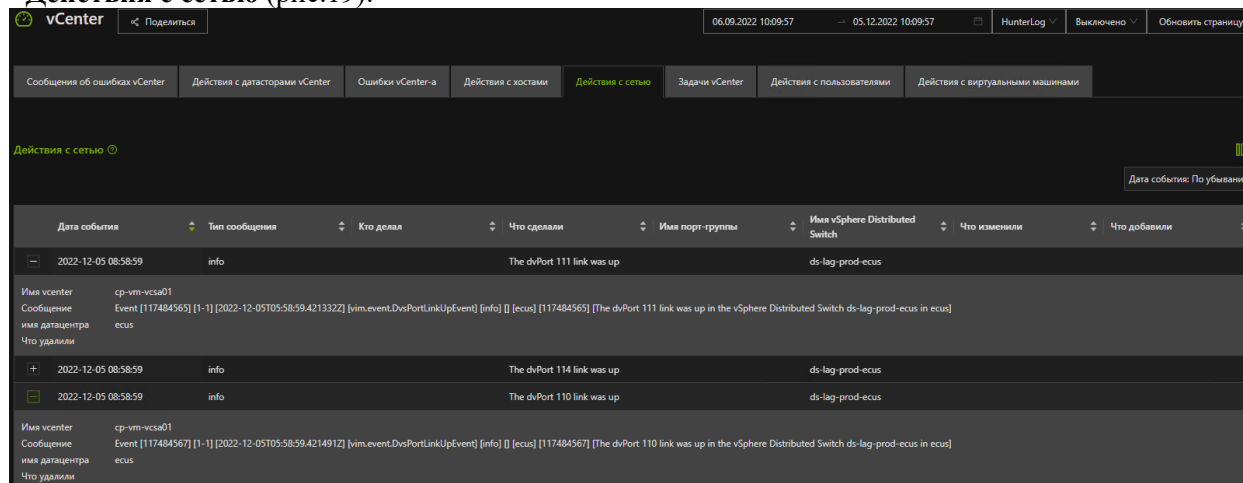


Рис.19

На вкладке отображаются все действия с сетью за выбранный период. Вся информация сгруппирована по следующим полям:

- Дата события;
- Тип сообщения;
- Кто делал;
- Что сделано;
- Имя порт-группы;
- Имя vSphere Distributed Switch;

- Что изменили;
- Что добавили.

При детализации строки выводится дополнительная информация:

- Имя vcenter;
- Сообщение;
- Имя датацентра;
- Что удалили.

По всем колонкам доступна сортировка данных для удобства пользования.

- Задачи vCenter (рис.20):

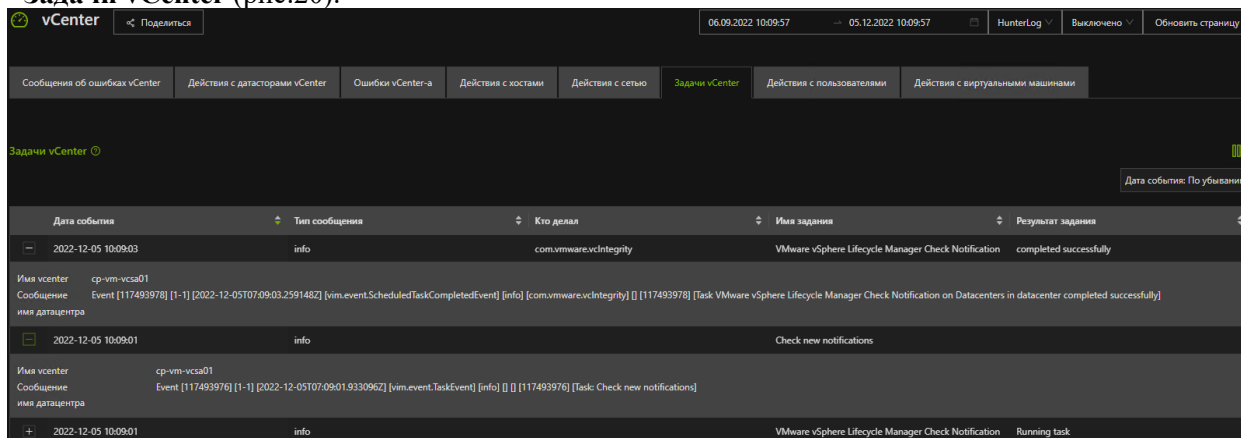


Рис.20

На вкладке отображаются все задачи за выбранный период. Вся информация сгруппирована по следующим полям:

- Дата события;
- Тип сообщения;
- Кто делал;
- Имя задания;
- Результат задания.

При детализации строки выводится дополнительная информация:

- Имя vcenter;
- Сообщение;
- Имя датацентра.

По всем колонкам доступна сортировка данных для удобства пользования.

- Действия с пользователями (рис.21):

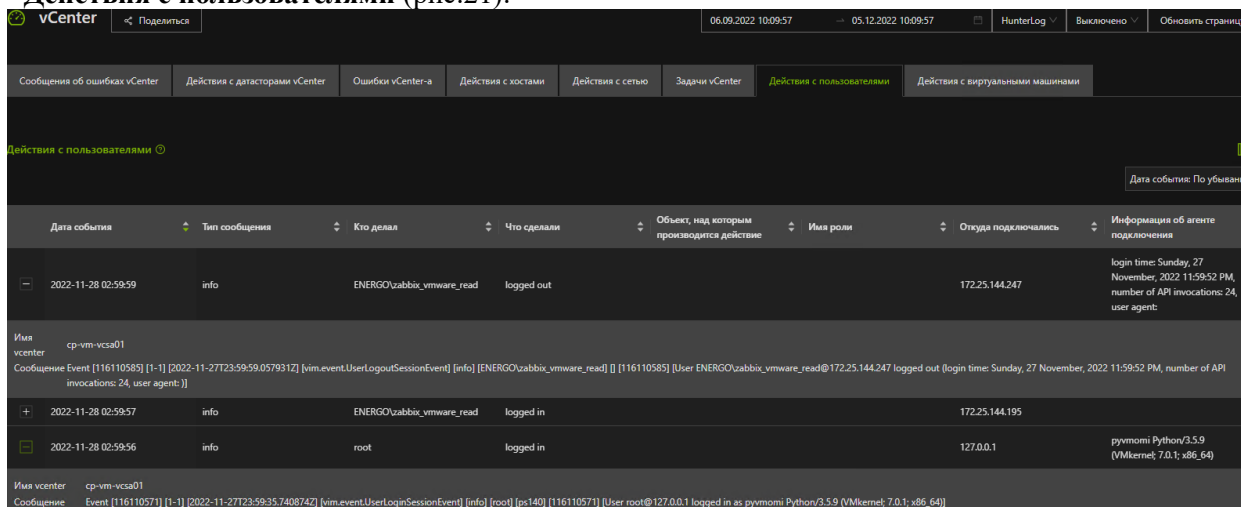


Рис.21

На странице действий с пользователями представлены данные за выбранный период с группировкой по следующим полям:

- Дата события;
- Тип сообщения;
- Кто делал;
- Что сделали;
- Объект, над которым производится действие;
- Имя роли;
- Откуда подключались;
- Информация об агенте подключения.

При детализации строки выводится дополнительная информация:

- Имя vcenter;
- Сообщение.

По всем колонкам доступна сортировка данных для удобства пользования.

- Действия с виртуальными машинами (рис.22):

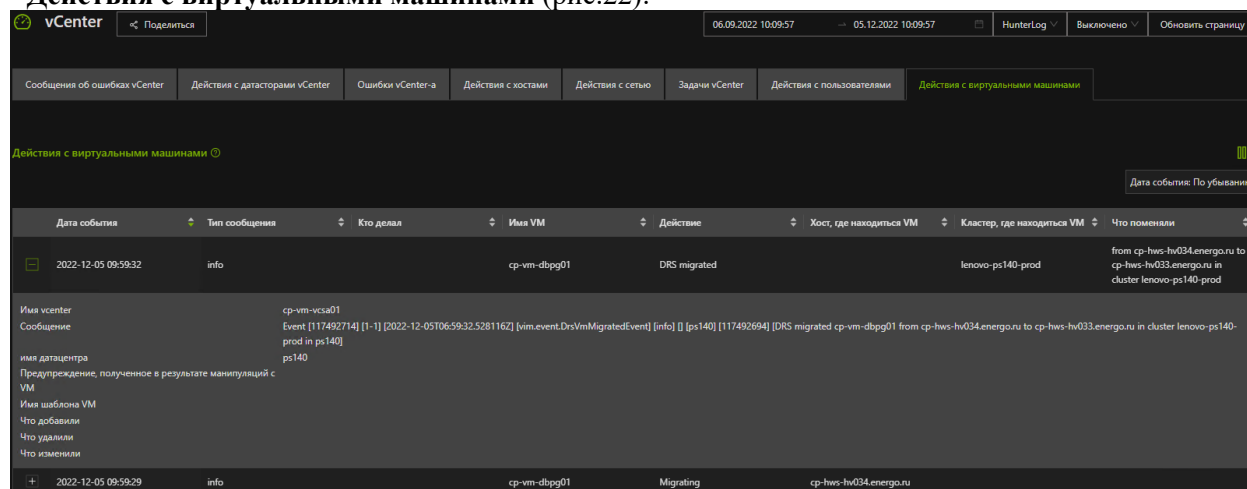


Рис.22

На странице представлены все действия с виртуальными машинами за выбранный период. Пользователю доступна информация по следующим полям:

- Дата события;
- Тип сообщения;
- Кто делал;
- Имя VM;
- Действие;
- Хост, где находится VM;
- Кластер, где находится VM;
- Что поменяли.

При детализации строки пользователю доступна более подробная информация по каждому событию, представленная следующими данными:

- Имя vcenter;
- Сообщение;
- Имя датацентра;
- Предупреждение, полученное в результате манипуляций с VM;
- Имя шаблона VM;
- Что добавили;
- Что удалили;
- Что изменили.

По всем колонкам доступна сортировка данных для удобства пользования.

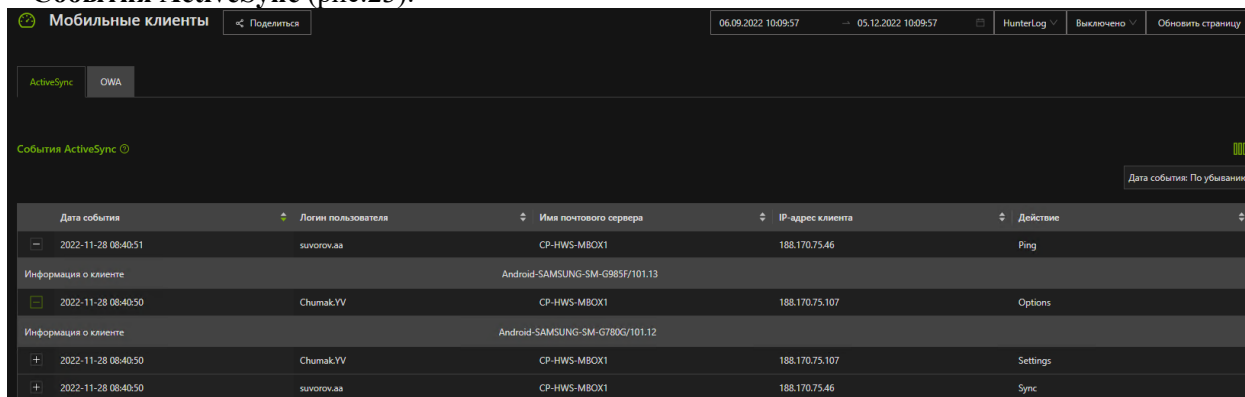
Exchange:

Раздел «Exchange» состоит из трех подразделов «Мобильные клиенты», «Системные события Exchange» и «Отслеживание писем Exchange». Подробная информация о каждом разделе представлена ниже.

«Мобильные клиенты»

Данный подраздел представлен в виде следующих вкладок:

- События ActiveSync (рис.23):



Дата события	Логин пользователя	Имя почтового сервера	IP-адрес клиента	Действие
2022-11-28 08:40:51	suvtovov.as	CP-HWS-MBOX1	188.170.75.46	Ping
Информация о клиенте: Android-SAMSUNG-SM-G985F/101.13				
2022-11-28 08:40:50	Chumak.YV	CP-HWS-MBOX1	188.170.75.107	Options
Информация о клиенте: Android-SAMSUNG-SM-G780G/101.12				
2022-11-28 08:40:50	Chumak.YV	CP-HWS-MBOX1	188.170.75.107	Settings
2022-11-28 08:40:50	suvtovov.as	CP-HWS-MBOX1	188.170.75.46	Sync

Рис.23

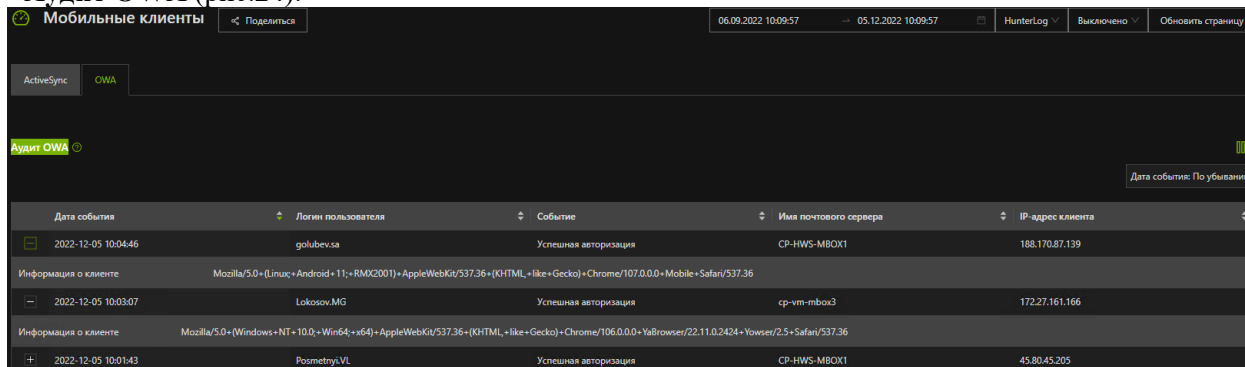
Данные события – это, подключения к Microsoft Exchange OWA от мобильных клиентов по протоколу ActiveSync.

Информация на странице представлена в разрезе следующих полей:

- Дата события;
- Логин пользователя;
- Имя почтового сервера;
- IP-адрес клиента;
- Действие.

При детализации строки, отображается информация о клиенте, которое участвует в событии.

- Аудит OWA (рис.24):



Дата события	Логин пользователя	Событие	Имя почтового сервера	IP-адрес клиента
2022-12-05 10:04:46	golubev.sa	Успешная авторизация	CP-HWS-MBOX1	188.170.87.139
Информация о клиенте: Mozilla/5.0+(Linux;+Android;+11;+RMX2001)+AppleWebKit/537.36+(KHTML;+Ike+Gecko)+Chrome/107.0.0.0+Mobile+Safari/537.36				
2022-12-05 10:03:07	Lokosov.MG	Успешная авторизация	cp-vm-mbox3	172.27.161.166
Информация о клиенте: Mozilla/5.0+(Windows+NT+10.0;+Win64;+x64)+AppleWebKit/537.36+(KHTML;+Ike+Gecko)+Chrome/106.0.0.0+YaBrowser/22.11.0.2424+Yowser/2.5+Safari/537.36				
2022-12-05 10:01:43	Rozmetny.VL	Успешная авторизация	CP-HWS-MBOX1	45.80.45.205

Рис.24

На странице представлены события по подключению к Microsoft Exchange OWA через веб-интерфейс.

Представление информации по следующим полям:

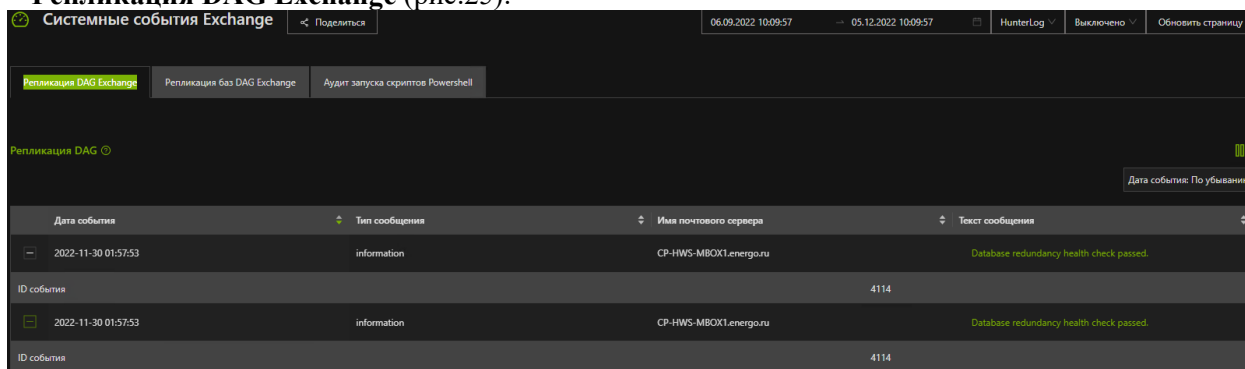
- Дата события;
- Логин пользователя;
- Событие;
- Имя почтового сервера;
- IP-адрес клиента.

При детализации строки, отображается информация о клиенте, которое участвует в событии.

«Системные события Exchange»

Данный подраздел представлен в виде следующих вкладок:

- Репликация DAG Exchange (рис.25):



The screenshot shows the 'Системные события Exchange' console with the 'Репликация DAG Exchange' tab selected. The table below represents the data visible in the log entries.

Дата события	Тип сообщения	Имя почтового сервера	Текст сообщения
2022-11-30 01:57:53	information	CP-HWS-MBOX1.energo.ru	Database redundancy health check passed.
ID события			4114
2022-11-30 01:57:53	information	CP-HWS-MBOX1.energo.ru	Database redundancy health check passed.
ID события			4114

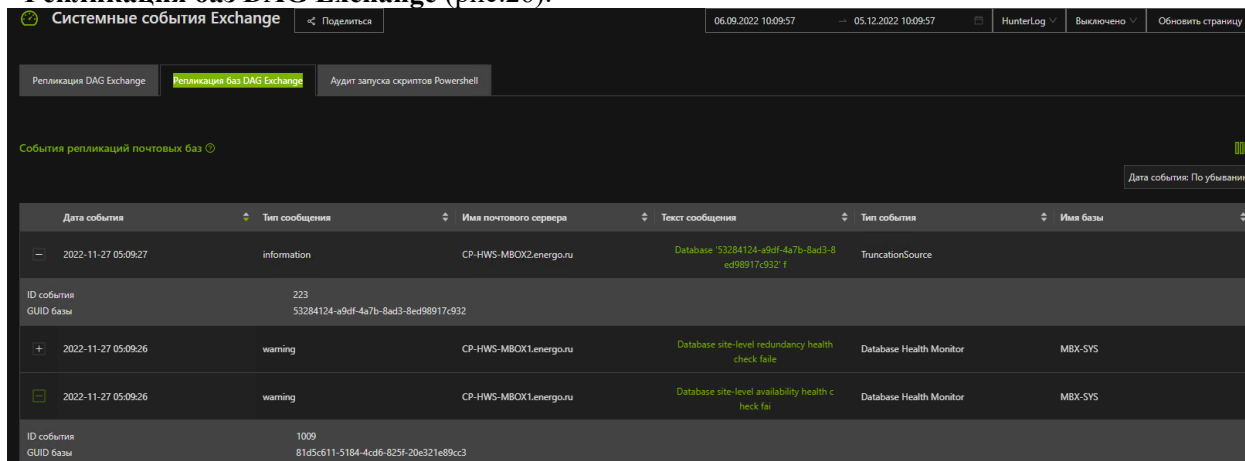
Рис.25

На данной странице представлены логи репликации групп доступности (DAG). Данные представлены в виде:

- Дата события;
- Тип сообщения;
- Имя почтового сервера;
- Текст сообщения.

При детализации строки выводится ID события.

- Репликация баз DAG Exchange (рис.26):



The screenshot shows the 'Системные события Exchange' console with the 'Репликация баз DAG Exchange' tab selected. The table below represents the data visible in the log entries.

Дата события	Тип сообщения	Имя почтового сервера	Текст сообщения	Тип события	Имя базы
2022-11-27 05:09:27	information	CP-HWS-MBOX2.energo.ru	Database '53284124-a9df-4a7b-8ac3-8ed98917c932'	TruncationSource	
ID события			223		
GUID базы			53284124-a9df-4a7b-8ac3-8ed98917c932		
2022-11-27 05:09:26	warning	CP-HWS-MBOX1.energo.ru	Database site-level redundancy health check failed	Database Health Monitor	MBX-SYS
2022-11-27 05:09:26	warning	CP-HWS-MBOX1.energo.ru	Database site-level availability health check failed	Database Health Monitor	MBX-SYS
ID события			1009		
GUID базы			81d5c611-5184-4cd6-825f-20e321e89cc3		

Рис.26

На данной странице представлены логи репликации групп доступности (DAG). Данные представлены в виде:

- Дата события;
- Тип сообщения;
- Имя почтового сервера;
- Текст сообщения;
- Тип события;
- Имя базы.

При детализации строки выводятся ID события и GUID базы.

- Аудит запуска скриптов Powershell (рис.27):

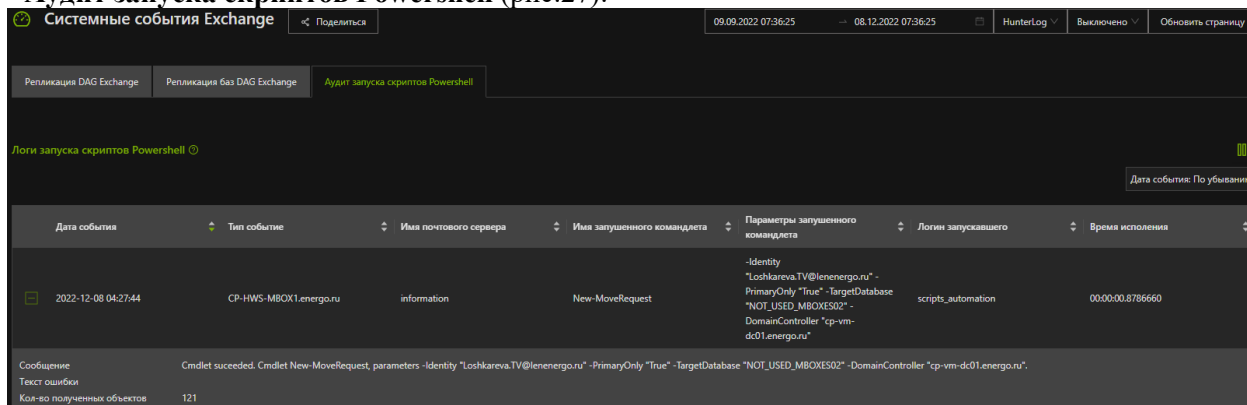


Рис.27

На данной странице представлены все логи запускаемых скриптов Powershell. Данные представлены в виде:

- Дата события;
- Тип события;
- Имя почтового сервера;
- Имя запущенного командлета;
- Параметры запущенного командлета;
- Логин запускавшего;
- Время исполнения.

При детализации строки пользователю доступны дополнительные данные:

- Сообщение;
- Текст ошибки;
- Количество полученных объектов.

«Отслеживание писем Exchange»

Данный подраздел представлен в виде следующих вкладок:

- Отслеживание писем Exchange (рис.28):

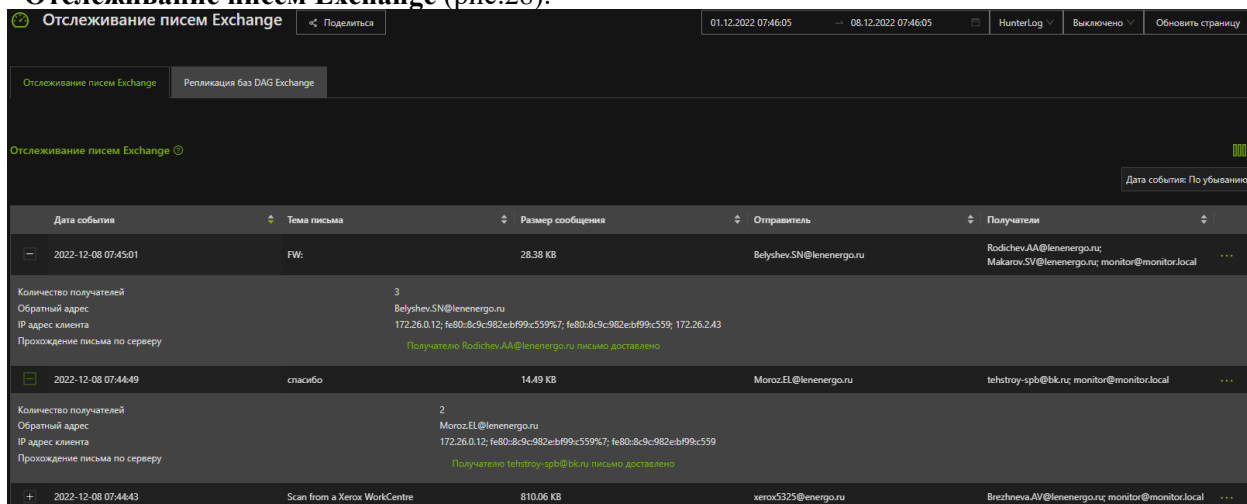


Рис. 28

На данной странице пользователю представлена подробная информация об отправляемых письмах:

- Дата события;
- Тема события;

- Размер сообщения;
- Отправитель;
- Получатель.

В конце каждой строки при наведении курсора мыши на «...» выводится ID сообщения, при нажатии на них автоматически происходит переход на вкладку с логами по выбранному message id (рис.29):

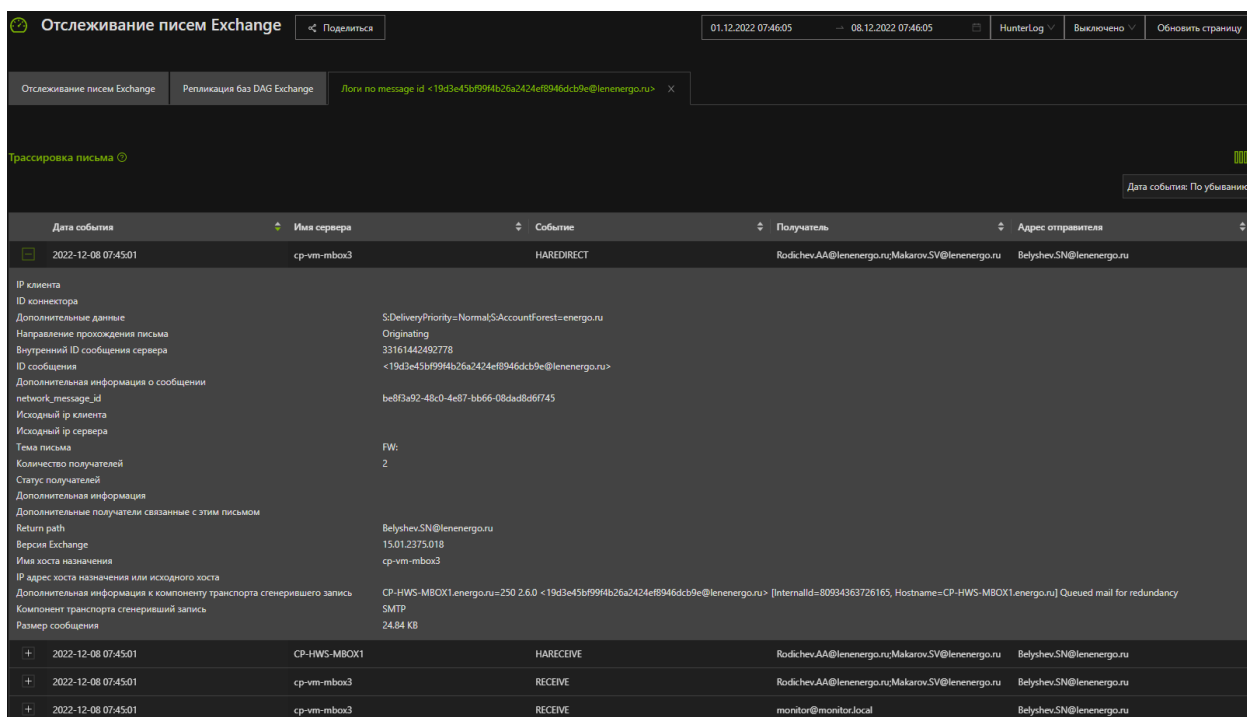


Рис.29

При детализации строки выводится дополнительная информация:

- Количество получателей;
- Обратный адрес;
- IP-адрес клиента;
- Прохождение письма по серверу – при нажатии на данные, открывается окно, в котором перечислены статусы по каждому получателю письма;

- Репликация баз DAG Exchange (рис.30):

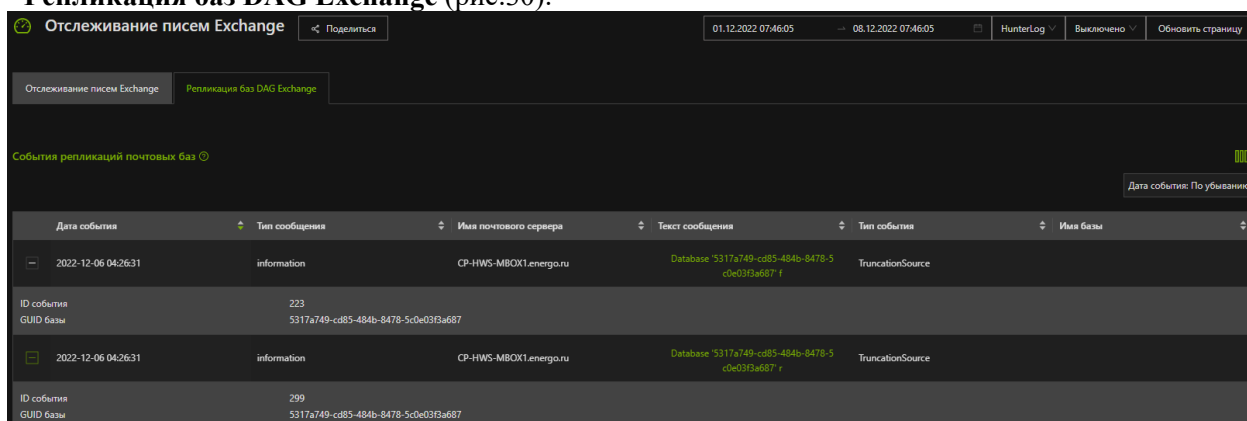


Рис. 30

На данной странице представлены логи событий репликаций почтовых баз (DAG):

- Дата события;
- Тип сообщения;
- Имя почтового сервера;
- Текст сообщения – при нажатии на сообщение, открывается полный запрос;

- Тип события;
- Имя базы.

При детализации строки отображается ID события, а также, GUID базы.

«Linux»

Данный подраздел включает в себя информацию по аудиту подключений к Linux, аудиту изменений файловой системы, истории выполняемых команд и изменению учетных записей:

- Аудит подключений к Linux (рис.31):

Дата события	Имя хоста	Логин	Событие	Результат
2022-11-29 12:32:52	cr-vm-traefik02	lrd.docenko	Окончание сеанса	
IP-адрес клиента			172.25.170.64	
Терминал			pts/0	
2022-11-29 11:36:53	cr-vm-traefik02	lrd.docenko	Аутентификация	Ошибка аутентификации
IP-адрес клиента			172.25.170.64	
Терминал			pts/0	

Рис.31

На странице представлены все события подключений за выбранный период:

- Дата события;
- Имя хоста;
- Логин;
- Событие;
- Результат.

При детализации строки выводится информация по IP-адресу клиента и терминале.

- Аудит изменений файловой системы (рис.32):

Дата события	Имя хоста	Что меняли	Логин	Событие	Результат
2022-11-29 02:59:01	cr-vm-smobile01		root	wrote-to-file	success
Команда /usr/sbin/CRON -f					
2022-11-29 02:58:48	cr-vm-logstn04			violated-apparmor-policy	success
Команда /usr/libexec/sss/sss_nss --uid 0 --gid 0 --logger-files					
2022-11-29 02:58:44	cr-vm-alka01			violated-apparmor-policy	success
Команда /usr/libexec/sss/sss_nss --uid 0 --gid 0 --logger-files					
2022-11-29 02:58:15	cr-vm-conf01			violated-apparmor-policy	success

Рис.32

На странице представлены события изменений файловой системы за выбранный период:

- Дата события;
- Имя хоста;
- Что меняли;
- Логин;
- Событие;
- Результат.

При детализации строки выводится выполненная команда.

- История выполненных команд (рис.33):

Дата события	Имя хоста	Логин	sudo user	Терминал
2022-11-30 15:00:55	cr-vm-zabrn04			sh -c /usr/lib/zabbix/externalscripts/jitter.sh 172.23.224.76
2022-11-30 15:00:55	cr-vm-zabrn04			/bin/bash /usr/lib/zabbix/externalscripts/jitter.sh 172.23.224.76
2022-11-30 15:00:55	cr-vm-zabrn04			/bin/ping -c 10 -i 0.3 172.23.224.76
2022-11-30 15:00:55	cr-vm-zabrn04			cut -f1 -d

Рис.33

На странице представлена вся история выполненных команд за выбранный период:

- Дата события;
- Имя хоста;
- Логин;
- sudo user;
- Терминал.

- Аудит изменений учетных записей (рис.34):

Рис.34

На странице представлена вся информация по изменению учетных записей за выбранный период:

- Дата события;
- Событие;
- Имя хоста;
- Логин изменяемого.

За текущий период изменений учетных записей не происходило.

«Локальный компьютер»

Данный подраздел включает в себя всю информацию по аудиту действий на локальных компьютерах и состоит из следующих подразделов:

- События приложений (рис.35):

Дата события	Имя компьютера	Тип события	Сообщение	Дополнительная информация о событии	Кто делал
2022-12-02 10:58:16	CP-HWS-MBOX1.energo.ru	information	Database redundancy health check passed.	Service	4114
ID события Домен пользователя					
2022-12-02 10:58:16	CP-HWS-MBOX1.energo.ru	information	Database redundancy health check passed.	Service	4114
ID события Домен пользователя					

Рис.35

На странице представлены все события журнала приложений Windows за выбранный период:

- Дата события;
- Имя компьютера;
- Тип события;
- Сообщение – при нажатии на текст, открывается окно с текстом запроса и возможностью его копирования;
- Дополнительная информация о событии;
- Кто делал.

При детализации строки выводится информация по ID события и домену пользователя.

- Аудит Firewall (рис.36):

Дата события	Событие	На каком компьютере зафиксировано	Имя правила	Список профилей, к которым применяется правило	
2022-11-30 11:40:25	Создание правила	cp-vm-tssh023.energo.ru	@(Microsoft.Windows.Cortana_1.11.6.17763_neutral_neutral_cw5n1h2byewy?ms-resource://Microsoft.Windows.Cortana/resources/PackagedDisplayName)	All	
ID события Имя измененного параметра Значение измененного параметра В каком профиле сработало правило Заблокированное приложение					
2022-11-30 11:40:25	Создание правила	cp-vm-tssh023.energo.ru	@(Microsoft.Windows.Cortana_1.11.6.17763_neutral_neutral_cw5n1h2byewy?ms-resource://Microsoft.Windows.Cortana/resources/PackagedDisplayName)	All	

Рис.36

На странице представлены все события брандмауэра Windows за выбранный период:

- Дата события;
- Событие;
- На каком компьютере зафиксировано;
- Имя правила;
- Список профилей, к которым применяется правило.

При детализации строки выводится дополнительная информация по событию:

- ID события;
- Имя измененного параметра;
- Значение измененного параметра;
- В каком профиле сработало правило;
- Заблокированное приложение.

- Аудит исполнения GPO (рис.37):

The screenshot shows the Windows Event Viewer interface for 'Локальный компьютер'. The 'Аудит исполнения GPO' log is selected. The main pane displays a list of events with columns for 'Дата события', 'Событие', 'На каком компьютере зафиксировано', and 'Тип сообщения'. Two events are visible:

Дата события	Событие	На каком компьютере зафиксировано	Тип сообщения
2022-11-30 03:13:08	Выполнение системного вызова для доступа к указанному файлу	cd-vm-1capp07.energo.ru	information
2022-11-30 03:13:08	Системные вызовы для доступа к указанному файлу завершены успешно	cd-vm-1capp07.energo.ru	information

Below the main pane, the details for the selected event (ID 4017) are shown:

Сообщения: Making LDAP calls to connect and bind to Active Directory. cp-vm-dc02.energo.ru

Рис.37

На странице представлены аудит всех событий изменения групповых политик за выбранный период:

- Дата события;
- Событие;
- На каком компьютере зафиксировано;
- Тип сообщения.

При детализации строки выводится дополнительная информация по ID события и сообщению.

- Аудит локальных групп (рис.38):

The screenshot shows the Windows Event Viewer interface for 'Локальный компьютер'. The 'Аудит локальных групп' log is selected. The main pane displays a list of events with columns for 'Дата события', 'Имя группы', 'Кто менял', 'Событие', and 'Кого удалили/добавили'. Two events are visible:

Дата события	Имя группы	Кто менял	Событие	Кого удалили/добавили
2022-12-03 22:44:27	IIS_IUSRS	ips_srsadm	Удаление пользователя из локальной группы безопасности	
2022-12-03 22:44:26	IIS_IUSRS	ips_srsadm	Добавление пользователя к локальной группе безопасности	

Below the main pane, the details for the selected event (ID 4733) are shown:

Домен меньшего: ENERGO
На каком компьютере зафиксировано: len-ips-arr.energo.ru
Текст сообщения: Удален член локальной группы с включенной безопасностью. Субъект: Идентификатор безопасности: S-1-5-21-3984192212-717921658-3745640658-43064 Имя учетной записи: ips_srsadm Домен учетной записи: ENERGO Идентификатор входа: 0x22E3AC8A7 Член: Идентификатор безопасности: S-1-5-20 Имя учетной записи: - Группа: Идентификатор безопасности: S-1-5-32-568 Имя группы: IIS_IUSRS Домен группы: BuiltIn Дополнительные сведения: Привилегии: -
Старое имя изменяемой группы:
Новое имя изменяемой группы:

Рис.38

На странице представлены аудит всех изменений локальных групп на компьютере за выбранный период:

- Дата события;
- Имя группы;
- Кто менял;
- Событие;
- Кого удалили/добавили.

При детализации строки выводится дополнительная информация:

- ID события;
- Домен меньшего;
- На каком компьютере зафиксировано;
- Текст сообщения;
- Старое имя изменяемой группы;
- Новое имя изменяемой группы.

- Аудит выполнения Powershell команд (рис.39):

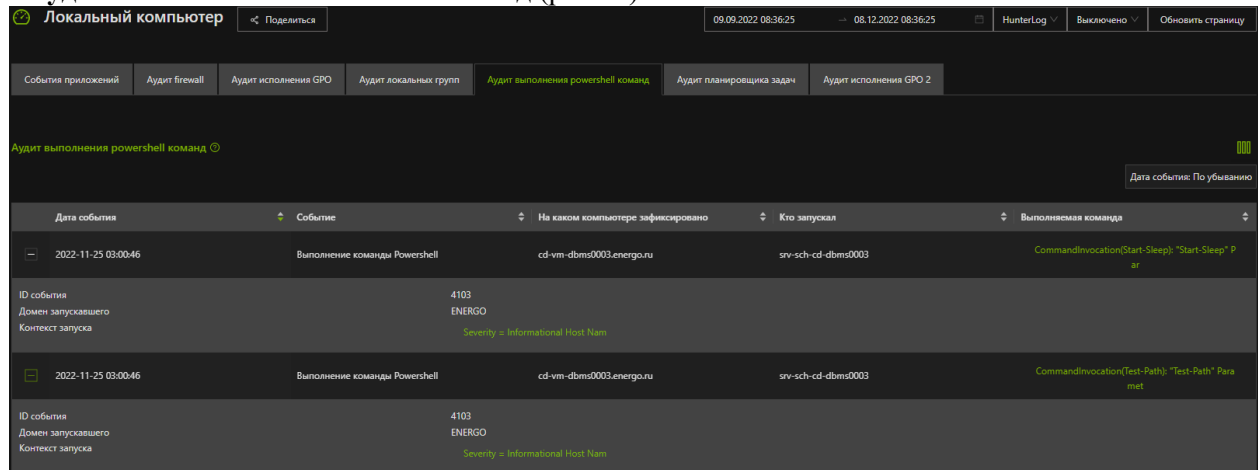


Рис.39

На странице представлены аудит всех выполняемых команд в командной строке на компьютере за выбранный период:

- Дата события;
- Событие;
- На каком компьютере зафиксировано;
- Кто запускал;
- Выполняемая команда – при нажатии на текст команды, откроется окно с полным текстом команды и возможностью его копирования.

При детализации строки выводится дополнительная информация:

- ID события;
- Домен запускавшего;
- Контекст запуска – при нажатии на контекст команды, откроется окно с полным текстом и возможностью его копирования.

- Аудит планировщика задач (рис.40):

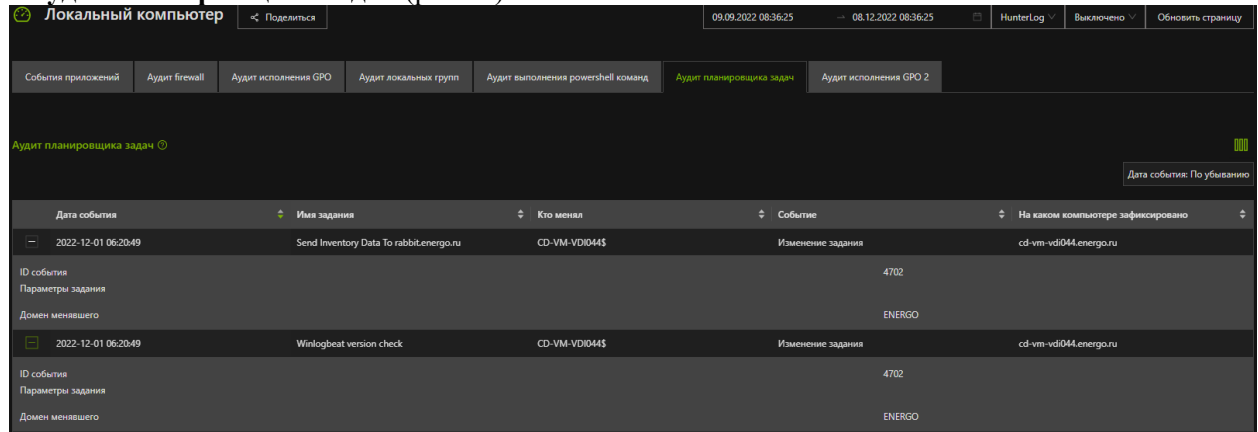


Рис.40

На странице представлены аудит всех зафиксированных событий в планировщике задач на компьютере за выбранный период:

- Дата события;
- Имя задания;
- Кто менял;
- Событие;
- На каком компьютере зафиксировано.

При детализации строки выводится дополнительная информация:

- ID события;
- Параметры задания;
- Домен менявшего.

- Аудит исполнения GPO 2 (рис.41):

Начало работы GPO	Конец работы GPO	На каком компьютере зафиксировано	Сообщение
2022-11-09 07:17:24	2022-11-09 07:17:28	cd-vm-vc01b.energo.ru	2022-11-09 04:17:24.569: Starting periodic policy processing for user ENERGO\rd.litvinov. Activity id: {d2fad802-9472-4371-a597-03ac11997738}
2022-11-09 07:17:23	2022-11-09 07:17:28	cp-vm-tsh01b.energo.ru	2022-11-09 04:17:23.813: Starting periodic policy processing for computer ENERGO\CP-VM-TSSH01BS. Activity id: {6b7ea8e4-e6-8f-4d9b-99aa-50a407d9d99e}
2022-11-09 07:17:18	2022-11-09 07:17:20	ct-vm-dbms0001.energo.ru	2022-11-09 04:17:18.194: Starting periodic policy processing for computer ENERGO\CT-VM-DBMS0001S. Activity id: {a950a83f-6-53b-4bee-09aa-7d9f7a23ae7c}

Рис.41

На странице представлен расширенный аудит всех событий изменения групповых политик за выбранный период:

- Начало работы GPO;
- Конец работы GPO;
- На каком компьютере зафиксировано;
- Сообщение – при нажатии на часть текста сообщения, откроется окно с полным текстом данного сообщения и возможностью его копирования (рис.42).

```

2022-11-09 04:17:24.569: Starting periodic policy processing for user ENERGO\rd.litvinov. Activity id: {d2fad802-9472-4371-a597-03ac11997738}
2022-11-09 04:17:24.569: Starting periodic policy processing for user ENERGO\rd.litvinov. Activity id: {d2fad802-9472-4371-a597-03ac11997738}
2022-11-09 04:17:24.572: The Group Policy processing mode is Background.
2022-11-09 04:17:24.572: Attempting to retrieve the account information.
2022-11-09 04:17:24.572: Making system call to get account information.
2022-11-09 04:17:24.572: The system call to get account information completed. CN=rd.litvinov,OU=Admin_accounts,OU=Tech,DC=energo,DC=ru The call completed in 0 milliseconds.
2022-11-09 04:17:24.572: Retrieved account information.
2022-11-09 04:17:24.572: The Group Policy processing mode is Background.
2022-11-09 04:17:24.572: Attempting to retrieve the account information.
2022-11-09 04:17:24.572: Making system call to get account information.
2022-11-09 04:17:24.572: The system call to get account information completed. CN=rd.litvinov,OU=Admin_accounts,OU=Tech,DC=energo,DC=ru The call completed in 0 milliseconds.
2022-11-09 04:17:24.572: Retrieved account information.
2022-11-09 04:17:24.730: Group Policy is trying to discover the Domain Controller information.
2022-11-09 04:17:24.730: Retrieving Domain Controller details.
2022-11-09 04:17:24.730: Group Policy is trying to discover the Domain Controller information.
2022-11-09 04:17:24.730: Retrieving Domain Controller details.
    
```

Рис.42

«NetFlow»

Данный подраздел включает в себя всю информацию по учету сетевого трафика (рис.43).

Передано данных	Source IP	Source Port	Dest IP	Dest Port	Протокол	Количество
738.57 MB	172.26.2.142	Postgres (5432)	172.26.2.126	34194	TCP	11
167.68 MB	172.26.0.152	MSSQL (1433)	172.26.0.3	55433	TCP	2
118.08 MB	172.26.2.47	51662	172.26.2.89	ClickHouse HTTP (8123)	TCP	6
111.66 MB	172.26.2.47	34440	172.26.0.101	ClickHouse HTTP (8123)	TCP	7
105.1 MB	172.26.2.43	SMB 6es NetBios (445)	172.23-225.55	9693	TCP	7
100.47 MB	172.26.2.47	43348	172.26.0.101	ClickHouse HTTP (8123)	TCP	5

Рис.43

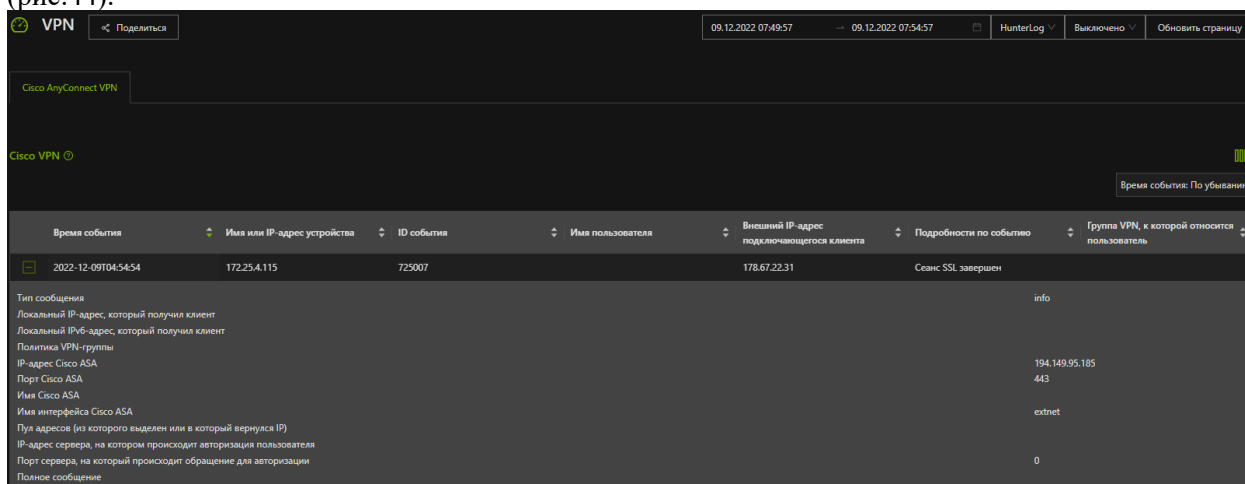
На странице сгруппированы данные по следующим полям:

- Передано данных (MB);
- Source IP;
- Source Port;
- Dest IP;
- Dest Port;
- Протокол;
- Количество.

Для удобства использования, по каждой колонке доступна сортировка данных.

«VPN»

Данный подраздел включает в себя всю информацию по учету трафика подключений по VPN (рис.44).



The screenshot shows the Cisco AnyConnect VPN management interface. At the top, there is a navigation bar with 'VPN', a 'Поделиться' button, and a date range from '09.12.2022 07:49:57' to '09.12.2022 07:54:57'. Below this, there are tabs for 'Cisco AnyConnect VPN' and 'Cisco VPN'. A search bar contains 'Время события: По убыванию'. The main area displays a table of VPN events with the following columns: 'Время события', 'Имя или IP-адрес устройства', 'ID события', 'Имя пользователя', 'Внешний IP-адрес подключающегося клиента', 'Подробности по событию', and 'Группа VPN, к которой относится пользователь'. The first row shows an event with ID '2022-12-09T04:54:54', device '172.25.4.115', ID '725007', user 'HunterLog', and details 'Сессия SSL завершена'. Below the table, there is a 'Полное сообщение' section with details such as 'Тип сообщения: info', 'Локальный IP-адрес, который получил клиент', 'Локальный IPv6-адрес, который получил клиент', 'Политика VPN-группы', 'IP-адрес Cisco ASA: 194.149.95.185', 'Порт Cisco ASA: 443', 'Имя Cisco ASA', 'Имя интерфейса Cisco ASA: extnet', 'Пул адресов (из которого выделен или в который вернулся IP)', 'IP-адрес сервера, на котором происходит авторизация пользователя', 'Порт сервера, на который происходит обращение для авторизации: 0', and 'Полное сообщение'.

Рис.44

На странице сгруппированы данные по следующим полям:

- Время события;
- Имя или IP-адрес устройства;
- ID события;
- Имя пользователя;
- Внешний IP-адрес подключающегося клиента;
- Подробности по событию;
- Группа VPN, к которой относится пользователь.

При детализации строки реализован дополнительный свод информации, состоящий из:

- Тип сообщения;
- Локальный IP-адрес, который получил клиент;
- Локальный IPv6-адрес, который получил клиент;
- Политика VPN-группы;
- IP-адрес Cisco ASA;
- Порт Cisco ASA;
- Имя Cisco ASA;
- Имя интерфейса Cisco ASA;
- Пул адресов (из которого выделен или в который вернулся IP);
- IP-адрес сервера, на котором происходит авторизация пользователя;
- Порт сервера, на который происходит обращение для авторизации;
- Полное сообщение.

«Сетевые папки»

Данный подраздел включает в себя всю информацию по учету действий с сетевыми папками (рис.45).

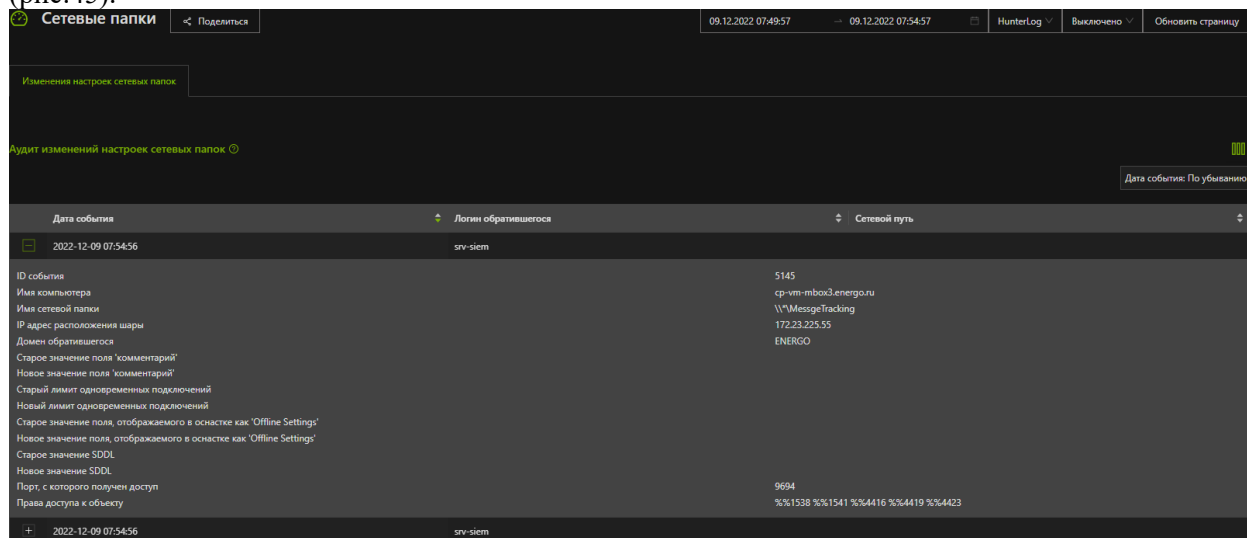


Рис.45

События выводятся за выбранный пользователем период с группировкой по дате события, логину обратившегося и сетевому пути. При детализации каждой строки реализовано получение подробных данных по выбранному событию:

- ID события;
- Имя компьютера;
- Имя сетевой папки;
- IP адрес расположения шары;
- Домен обратившегося;
- Старое значение поля 'комментарий';
- Новое значение поля 'комментарий';
- Старый лимит одновременных подключений;
- Старое значение поля, отображаемого в оснастке как 'Offline Settings';
- Новое значение поля, отображаемого в оснастке как 'Offline Settings';
- Старое значение SDDL;
- Новое значение SDDL;
- Порт, с которого получен доступ;
- Права доступа к объекту.

Для удобства использования информации реализована сортировка, как по колонкам, так и по дате.

4. ЮРИДИЧЕСКАЯ ИНФОРМАЦИЯ

Авторские права

Материалы, приведенные в настоящем документе, являются собственностью ООО «Дигилабс» и могут быть использованы только специалистами для целей экспертной проверки Системы в рамках процедуры включения в Единый реестр российских программ для электронных вычислительных машин и баз данных, а также для личных целей приобретателей программного обеспечения.

Запрещается воспроизведение отдельных частей документа, внесение правок в него, размещение на сетевых ресурсах, распространение в любой форме (в том числе в переводе) на бумажных и электронных носителях, посредством каналов связи и средств массовой информации или каким-либо другим способом без специального письменного разрешения ООО «Дигилабс» и ссылки на источник.

Программное обеспечение и товарные знаки, указанные в настоящем документе, принадлежат ООО «Дигилабс» и охраняются законом.

Содержание документа

Содержание данного документа может изменяться без предварительного уведомления. ООО «Дигилабс» не несёт ответственности за неточности и/или ошибки, допущенные в данном документе и возможный ущерб, связанный с этим.