EdgeADC

РУКОВОДСТВО ПО АДМИНИСТРИРОВАНИЮ

Содержание

Свойства документа

Номер документа: 2.0.6.16.21.18.06

Дата создания документа: 30 апреля 2021 г.

Последнее редактирование документа: June 16, 2021

Автор документа: Джей Савур

Документ Последний раз отредактирован:

Направление документа: EdgeADC - Версия 4.2.7.1895

Отказ от документа

Скриншоты и графика в данном руководстве могут незначительно отличаться от вашего продукта из-за различий в версии выпуска вашего продукта. Edgenexus гарантирует, что прилагает все разумные усилия для того, чтобы информация в этом документе была полной и точной. Edgenexus не несет ответственности за любые ошибки. Edgenexus вносит изменения и исправления в информацию в этом документе в будущих релизах, когда возникнет такая необходимость.

Авторские права

Товарные знаки

Логотип Edgenexus, Edgenexus, EdgeADC, EdgeWAF, EdgeGSLB, EdgeDNS являются торговыми марками или зарегистрированными торговыми марками компании Edgenexus Limited. Все другие торговые марки являются собственностью соответствующих владельцев и признаются.

Поддержка Edgenexus

Если у Вас возникли технические вопросы относительно данного продукта, пожалуйста, обратитесь в службу поддержки по адресу: support@edgenexus.io.

Установка EdgeADC

Продукт EdgeADC (в дальнейшем он будет называться ADC) доступен для установки несколькими способами. Для каждой целевой платформы требуется своя программа установки, и все они доступны для Вас.

Вот различные доступные модели установки.

- VMware ESXi
- KVM
- Microsoft Hyper-V
- Oracle VM
- ISO для аппаратного обеспечения BareMetal

Размер виртуальной машины, которую Вы будете использовать для размещения ADC, зависит от сценария использования и пропускной способности данных.

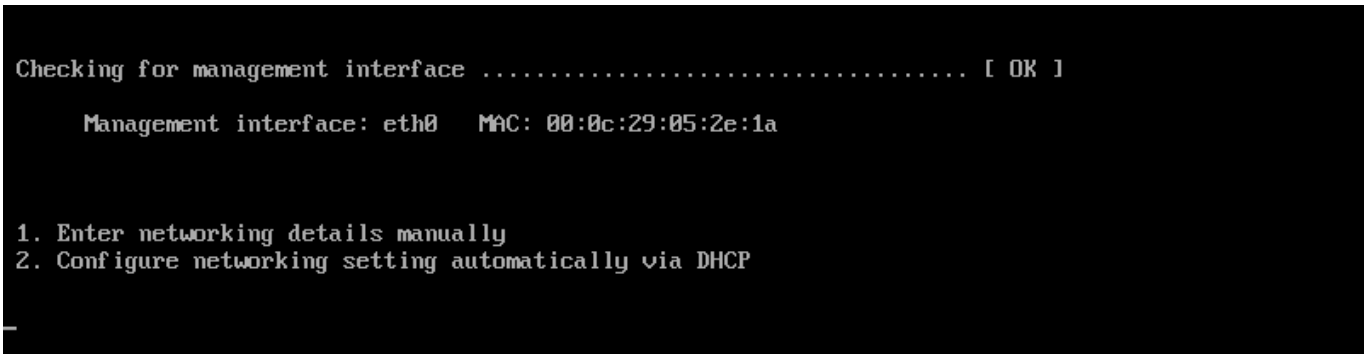
VMware ESXi

ADC доступен для установки на VMware ESXi версии 5.x и выше.

- Загрузите последнюю версию установочного OVA-пакета ADC, используя соответствующую ссылку, предоставленную в письме о загрузке.
- После загрузки, пожалуйста, распакуйте файл в подходящую директорию на Вашем ESXi хосте или SAN.
- В клиенте vSphere выберите File: Deploy OVA/OVF Template.
- Найдите и выберите место, где Вы сохранили свои файлы; выберите файл OVF и нажмите **NEXT**
- Сервер ESX запрашивает имя устройства. Введите подходящее имя и нажмите **NEXT**
- Выберите хранилище данных, с которого будет работать Ваше устройство ADC.
- Выберите хранилище данных с достаточным пространством и нажмите **NEXT**
- Затем Вам будет предоставлена информация о продукте; нажмите **NEXT**
- Нажмите **NEXT.**
- После того, как Вы скопировали файлы в хранилище данных, Вы можете установить виртуальное устройство.

Запустите клиент vSphere, чтобы увидеть новое виртуальное устройство ADC.

- Щелкните правой кнопкой мыши на VA и перейдите к пункту Power > Power-On
- После этого Ваш VA загрузится, и на консоли появится экран загрузки ADC.



Установка интерфейса VMXNET3

Драйвер VMXnet3 поддерживается, но сначала Вам необходимо внести изменения в настройки сетевой карты.

***Примечание** - НЕ обновляйте VMware-tools*

Включение интерфейса VMXNET3 на только что импортированном VA (никогда не запускался)

1. Удалите обе сетевые карты из виртуальной машины
2. Обновление аппаратного обеспечения виртуальной машины - - Щелкните правой кнопкой мыши на VA в списке и выберите Upgrade Virtual Hardware (не запускайте установку или обновление инструментов VMware, **а только** выполните обновление аппаратного обеспечения).
3. Добавьте две сетевые карты и выберите их в качестве VMXNET3
4. Запустите VA, используя стандартный метод. Он будет работать с VMXNET3

Включение интерфейса VMXNET3 на уже работающем VA

1. Остановите ВМ (команда выключения CLI или выключение питания GUI)
2. Получите MAC-адреса обеих сетевых карт (запомните порядок следования сетевых карт в списке!)
3. Удалите обе сетевые карты из виртуальной машины
4. Обновление аппаратного обеспечения ВМ (не запускайте установку или обновление инструментов VMware, выполните **только** обновление аппаратного обеспечения)
5. Добавьте две сетевые карты и выберите их в качестве VMXNET3
6. Установите MAC-адреса для новых сетевых карт в соответствии с шагом 2
7. Перезапустите VA

Мы поддерживаем VMware ESXi в качестве производственной платформы. Для ознакомительных целей Вы можете использовать VMware Workstation и Player.

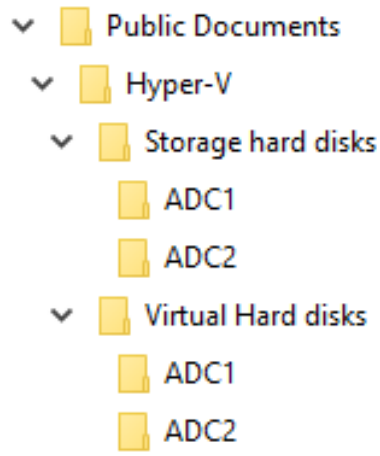
Пожалуйста, обратитесь к разделу **КОНФИГУРАЦИЯ ПЕРВОЙ ЗАГРУЗКИ,** чтобы продолжить.

Microsoft Hyper-V

Виртуальное устройство Edgenexus ADC Virtual может быть легко установлено в системе виртуализации Microsoft Hyper-V. Данное руководство предполагает, что Вы правильно указали и настроили систему Hyper-V и системные ресурсы для размещения ADC и его архитектуры балансировки нагрузки.

Обратите внимание, что каждому прибору требуется уникальный MAC-адрес.

- Распакуйте загруженный файл ADC-VA, совместимый с Hyper-V, на локальную машину или сервер.
- Откройте Hyper-V Manager.
- Создайте новую папку для виртуального жесткого диска ADC VA и другую новую папку для жесткого диска хранилища, например, C:\Users\Public\Documents\Hyper-V\Virtual hard disks\ADC1 и C:\Users\Public\Documents\Hyper-V\Storage hard disks\ADC1.
- **Примечание**: Для каждой установки виртуального экземпляра ADC необходимо создать новые подпапки ADC для виртуальных жестких дисков\ и жестких дисков для хранения данных\, как показано ниже:



- Скопируйте извлеченный файл EdgeADC .vhd в папку 'Storage hard disk', созданную выше.
- В клиенте Hyper-V Manager щелкните правой кнопкой мыши на сервере и выберите "Импорт виртуальной машины".
- Перейдите в папку, содержащую загруженный файл образа ADC VA, извлеченный ранее
- Выберите виртуальную машину - выделите виртуальную машину для импорта и нажмите Далее
- Выберите виртуальную машину - выделите виртуальную машину для импорта и нажмите Далее
- Выберите Тип импорта - выберите "**Копировать виртуальную машину (создать новый уникальный ID)**", нажмите далее
- Выберите папки для файлов виртуальной машины - Место назначения можно оставить по умолчанию Hyper-V или выбрать другое местоположение
- Найдите Virtual Hard Disks - найдите и выберите папку виртуальных жестких дисков, созданную выше, и нажмите далее
- Выберите папки для хранения виртуальных жестких дисков - найдите и выберите папку Storage hard disks, созданную ранее, и нажмите далее
- Проверьте правильность деталей в окне Completing Import Wizard Summary и нажмите Finish
- Щелкните правой кнопкой мыши на только что импортированной виртуальной машине **ADC** и выберите Пуск

ПРИМЕЧАНИЕ: В СООТВЕТСТВИИ С HTTP://SUPPORT.MICROSOFT.COM/KB/2956569 ВАМ СЛЕДУЕТ ИГНОРИРОВАТЬ СООБЩЕНИЕ О СОСТОЯНИИ "DEGRADED (INTEGRATION SERVICES UPGRADE REQUIRED)", КОТОРОЕ МОЖЕТ БЫТЬ ПОКАЗАНО НИЖЕ ПОСЛЕ ЗАПУСКА VA. НИКАКИХ ДЕЙСТВИЙ НЕ ТРЕБУЕТСЯ, И СЛУЖБА НЕ ДЕГРАДИРОВАНА

- Пока ВМ инициализируется, Вы можете щелкнуть правой кнопкой мыши на записи ВМ и выбрать Connect... Затем перед Вами откроется консоль EdgeADC.

- Как только Вы настроите свойства сети, VA перезагрузится и представит вход в консоль VA.

Пожалуйста, обратитесь к разделу **КОНФИГУРАЦИЯ ПЕРВОЙ ЗАГРУЗКИ,** чтобы продолжить.

Citrix XenServer

Виртуальное устройство ADC Virtual appliance можно установить на Citrix XenServer.

- Распакуйте файл ADC OVA ALB-VA на локальную машину или сервер.
- Откройте Citrix XenCenter Client.
- В клиенте XenCenter выберите **"Файл: Импорт"**.
- Найдите и выберите OVA-файл, затем нажмите **"Открыть далее".**
- В ответ на запрос выберите место создания виртуальной машины.
- Выберите, какой XenServer Вы хотите установить, и нажмите **"NEXT".**
- Выберите хранилище (SR) для размещения виртуального диска, когда появится соответствующий запрос.
- Выберите CP с достаточным пространством и нажмите **"NEXT".**
- Нанесите на карту интерфейсы виртуальной сети. На обоих интерфейсах будет написано Eth0; однако, обратите внимание, что нижний интерфейс - Eth1.
- Выберите целевую сеть для каждого интерфейса и нажмите **NEXT**
- **НЕ** ставьте галочку напротив "Использовать исправление операционной системы".
- Нажмите **"NEXT"**
- Выберите сетевой интерфейс, который будет использоваться для временной передачи VM.
- Выберите интерфейс управления, обычно Сеть 0, и оставьте сетевые настройки на DHCP. Имейте в виду, что Вы должны назначить статические IP-адреса, если у Вас нет работающего DHCP-сервера для переноса. Если этого не сделать, то в результате импорта будет написано Connecting constantly then failed. Нажмите **"NEXT"**
- Просмотрите всю информацию и проверьте правильность настроек. Нажмите **"FINISH".**
- Ваша ВМ начнет передавать виртуальный диск "ADC ADC" и, после завершения, отобразится под Вашим XenServer.
- Теперь в клиенте XenCenter Вы сможете увидеть новую виртуальную машину. Щелкните правой кнопкой мыши на VA и нажмите "**START**".
- Затем загрузится Ваша виртуальная машина, и появится экран загрузки ADC.

- После настройки вход в VA представляется сам собой.

Пожалуйста, обратитесь к разделу **КОНФИГУРАЦИЯ ПЕРВОЙ ЗАГРУЗКИ,** чтобы продолжить.

Конфигурация первой загрузки

При первой загрузке ADC VA отображает следующий экран с запросом конфигурации для производственных операций.

Первая загрузка - Детали сети вручную

При первой загрузке у Вас будет 10 секунд, чтобы прервать автоматическое назначение IP-данных через DHCP

Чтобы прервать этот процесс, щелкните в окне консоли и нажмите любую клавишу. Затем Вы можете ввести следующие данные вручную.

- IP-адрес
- Маска подсети
- Шлюз
- DNS-сервер

Эти изменения являются постоянными, они переживут перезагрузку и не требуют повторной настройки на VA.

Первая загрузка - DHCP успешно

Если Вы не прервете процесс назначения сети, то после тайм-аута Ваш АЦП свяжется с DHCP-сервером, чтобы получить данные о своей сети. Если контакт будет успешным, то Вашему аппарату будет присвоена следующая информация.

- IP-адрес
- Маска подсети
- Шлюз по умолчанию
- DNS-сервер

Мы советуем не использовать для работы ADC VA адрес DHCP, если только этот IP-адрес не связан постоянно с MAC-адресом VA на сервере DHCP. Мы всегда советуем использовать **фиксированный IP-адрес** при использовании VA. Выполняйте действия, описанные в разделе **Изменение IP-адреса управления** и последующих разделах, пока не завершите конфигурацию сети.

Первая загрузка - DHCP не работает

Если у Вас нет DHCP-сервера или соединение не удалось, будет назначен IP-адрес 192.168.100.100.
IP-адрес будет увеличиваться на '1' до тех пор, пока VA не найдет свободный IP-адрес. Кроме того, VA будет проверять, не используется ли IP-адрес в настоящее время, и если да, то будет увеличивать его снова и перепроверять.

Изменение IP-адреса управления

Вы можете изменить IP-адрес VA в любое время, используя команду **set greenside=n.n.n.n.n,** как показано ниже.

```
Command:set greenside=192.168.101.1_
```

Изменение маски подсети для eth0

Сетевые интерфейсы используют префикс 'eth'; базовый сетевой адрес называется eth0. Маску подсети или netmask можно изменить с помощью команды **set mask eth0 n.n.n.n.n**. Пример Вы можете увидеть ниже.

```
Command:set mask eth0 255.255.255.0_
```

Назначение шлюза по умолчанию

Для работы VA необходим шлюз по умолчанию. Чтобы установить шлюз по умолчанию, используйте команду **route add default gw n.n.n.n.n,** как показано в примере ниже.

```
Command:route add default gw 192.168.101.254_
```

Проверка значения шлюза по умолчанию

Чтобы проверить, добавлен ли шлюз по умолчанию и является ли он правильным, используйте команду **route**. Эта команда отобразит сетевые маршруты и значение шлюза по умолчанию. См. пример ниже.

```
Command:route
Kernel IP routing table
Destination     Gateway         Genmask         Flags Metric Ref    Use Iface
255.255.255.255 *               255.255.255.255 UH    0      0        0 eth0
192.168.101.0   *               255.255.255.0   U     0      0        0 eth0
default         192.168.101.254 0.0.0.0         UG    0      0        0 eth0
```

Теперь Вы можете получить доступ к графическому интерфейсу пользователя (GUI), чтобы настроить ADC для производственного или ознакомительного использования.

Доступ к веб-интерфейсу

Вы можете использовать любой интернет-браузер с поддержкой Javascript для настройки, мониторинга и развертывания АЦП в рабочем режиме.

В поле URL браузера введите либо **HTTPS://{IP ADDRESS}, либо HTTPS://{FQDN}.**

По умолчанию АЦП использует самоподписанный SSL-сертификат. Вы можете изменить АЦП, чтобы использовать SSL-сертификат по своему выбору.

Как только Ваш браузер достигнет АЦП, он покажет Вам экран входа в систему. Заводские учетные данные по умолчанию для АЦП следующие:

Имя пользователя по умолчанию = **admin** / Пароль по умолчанию = **jetnexus**

Справочная таблица команд

Команда	Параметр1	Параметр2	Описание	Пример
дата			Показывает настроенные в данный момент дату и время	Tue Sept 3 13:00 UTC 2013
по умолчанию			Назначьте заводские настройки по умолчанию для Вашего прибора	
выход			Выйдите из интерфейса командной строки	
помощь			Отображает все действующие команды	
ifconfig	[пустой].		Просмотр конфигурации интерфейса для всех интерфейсов	ifconfig
	eth0		Просмотрите конфигурацию интерфейса только eth0	ifconfig eth0
machineid			Эта команда предоставит machineid, используемый для лицензирования ADC ADC	EF4-3A35-F79
бросить			Выйдите из интерфейса командной строки	
перезагрузка			Разорвите все соединения и перезагрузите ADC ADC	перезагрузка
перезапустить			Перезапустите виртуальные службы ADC ADC	
маршрут	[пустой].		Просмотр таблицы маршрутизации	маршрут
	добавить	gw по умолчанию	Добавьте IP-адрес шлюза по умолчанию	route add default gw 192.168.100.254
установить	greenside		Установите IP-адрес управления для ADC	set greenside=192.168.101.1
	маска		Установите маску подсети для интерфейса. Имена интерфейсов: eth0, eth1....	установить маску eth0 255.255.255.0
показать			Отображает настройки глобальной конфигурации	
отключение			Завершите все соединения и отключите питание АЦП АЦП	
статус			Отображает текущую статистику данных	
топ			Просмотр информации о процессе, такой как ЦП и память	

viewlog	сообщения	Отображает необработанные сообщения syslog	Просмотр сообщений журнала

Обратите внимание: Команды не чувствительны к регистру. История команд отсутствует.

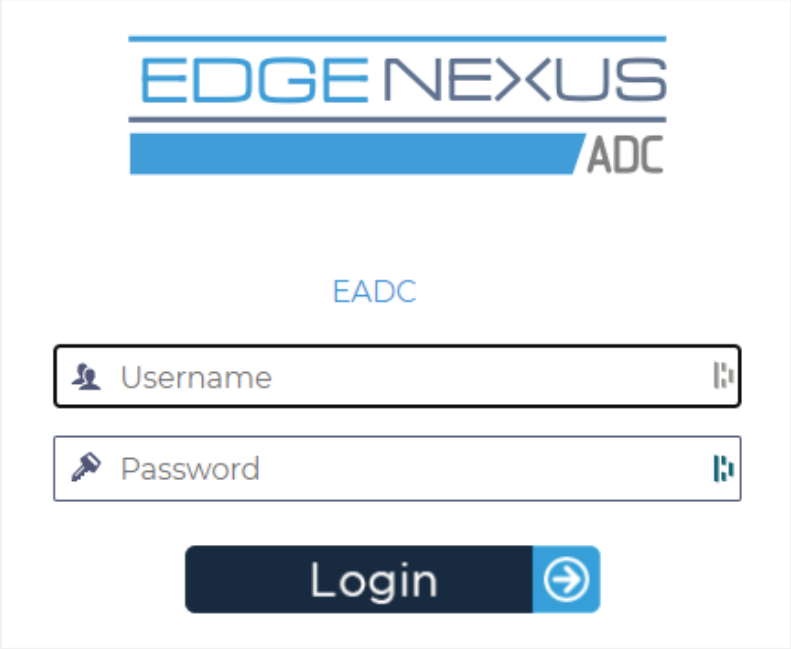
Запуск веб-консоли ADC

Все операции с АЦП (также называемым АЦП) настраиваются и выполняются с помощью веб-консоли. Доступ к веб-консоли осуществляется через любой браузер с поддержкой Javascript.

Чтобы запустить веб-консоль ADC, введите URL или IP-адрес ADC в поле URL. В качестве примера мы будем использовать adc.company.com:

https://adc.company.com

После запуска веб-консоль ADC выглядит так, как показано ниже, позволяя Вам войти в систему как пользователь admin.



Учетные данные для входа по умолчанию

Учетные данные для входа по умолчанию следующие:

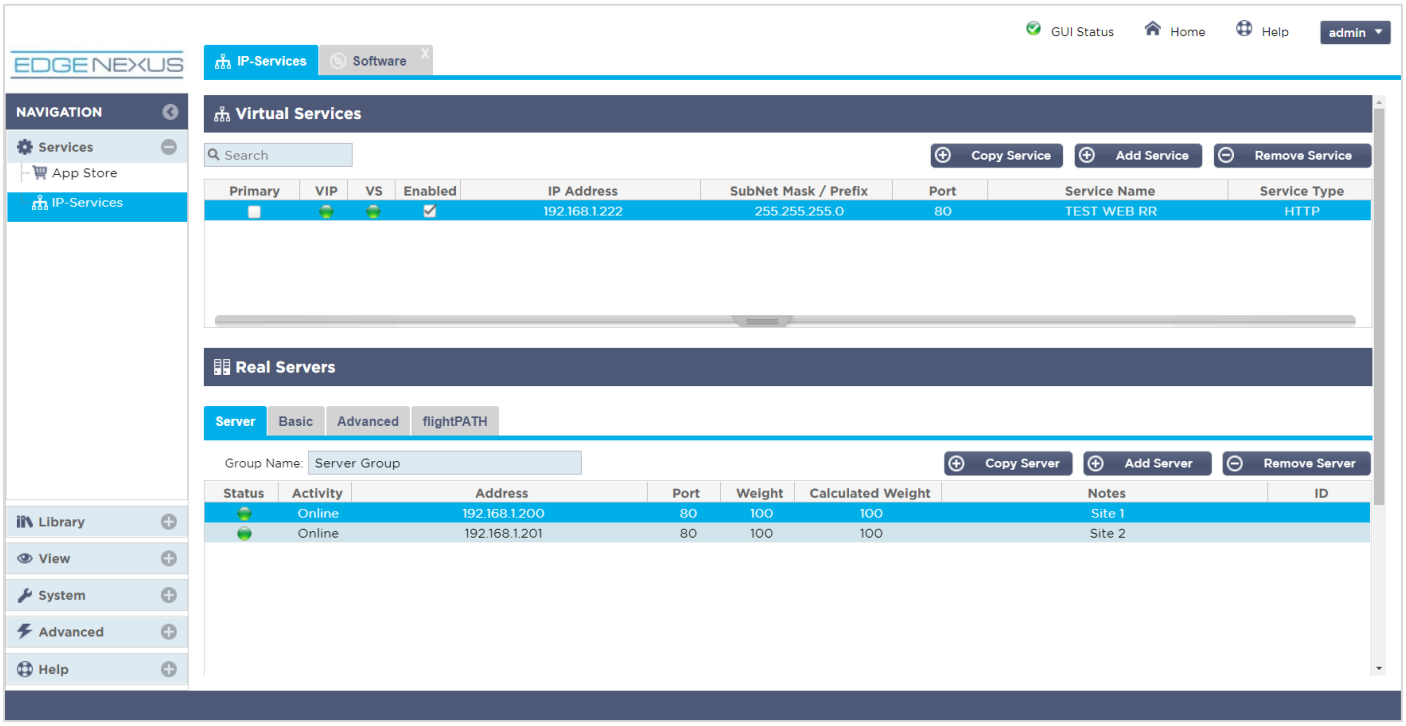
- Имя пользователя: admin
- Пароль: jetnexus

Вы можете изменить это в любое время, используя возможности конфигурации пользователя, расположенные по адресу *Система > Пользователи.*

После того, как Вы успешно вошли в систему, на экране появится главная приборная панель АЦП.

Главная приборная панель

На рисунке ниже показано, как выглядит главная приборная панель или "домашняя страница" АЦП. Время от времени мы можем вносить некоторые изменения по причинам улучшения, но все функции останутся.



Чтобы быть максимально краткими, мы предположим, что это первое знакомство с секциями экрана окажется достаточным для понимания различных разделов области конфигурации АЦП, поэтому мы не будем подробно описывать их по мере продвижения, а сосредоточимся на конфигурационных элементах.

Двигаясь слева направо, сначала мы видим раздел Навигация. Раздел Навигация состоит из различных областей внутри ADC. Когда Вы нажимаете на определенный выбор в разделе Навигация, это отобразит соответствующий раздел в правой части экрана. Вы также можете увидеть вкладку выбранного раздела конфигурации в верхней части экрана, рядом с логотипом продукта. Вкладки позволяют быстрее переходить к заранее используемым разделам конфигурации АЦП.

Услуги

Раздел услуг в АЦП имеет несколько областей. Когда Вы нажмете на пункт Услуги, он расширится и покажет доступные варианты.

IP-услуги

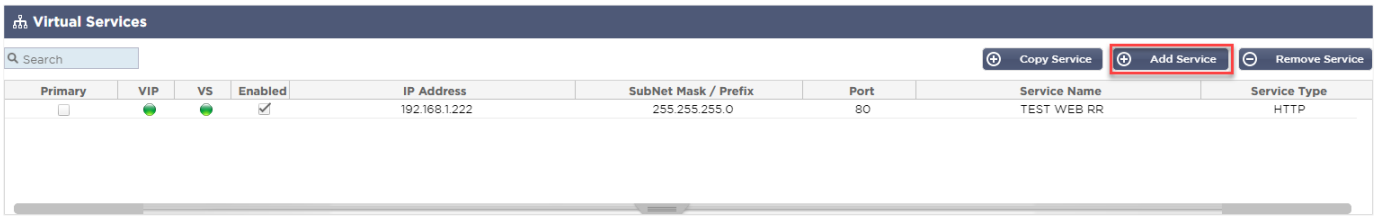
Раздел IP-служб ADC позволяет Вам добавлять, удалять и настраивать различные виртуальные IP-службы, необходимые для Вашего конкретного случая использования. Настройки и опции относятся к разделам, приведенным ниже. Эти разделы находятся в правой части экрана приложения.

Виртуальные услуги

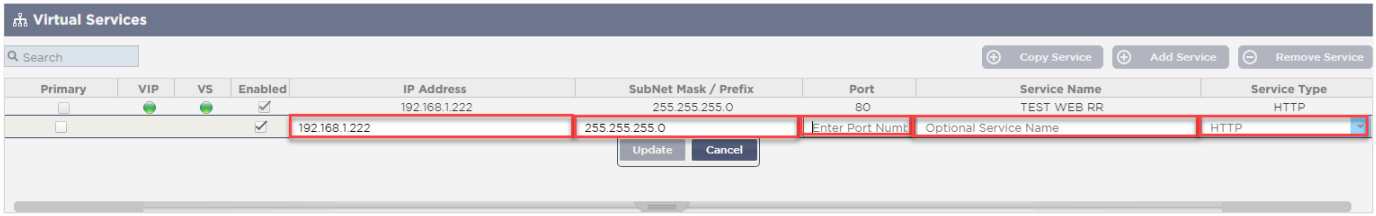
Виртуальная служба объединяет виртуальный IP-адрес (VIP) и порт TCP/UDP, на котором слушает ADC. Трафик, поступающий на IP-адрес виртуальной службы, перенаправляется на один из реальных серверов, связанных с этой службой. IP-адрес виртуальной службы не может совпадать с адресом управления АЦП. т.е. eth0, eth1 и т.д..

ADC определяет, как трафик перераспределяется между серверами на основе политики балансировки нагрузки, установленной на вкладке Basic в разделе Real Servers.

Создание новой виртуальной службы с использованием нового VIP-клиента



- Нажмите кнопку Добавить виртуальную службу, как указано выше.

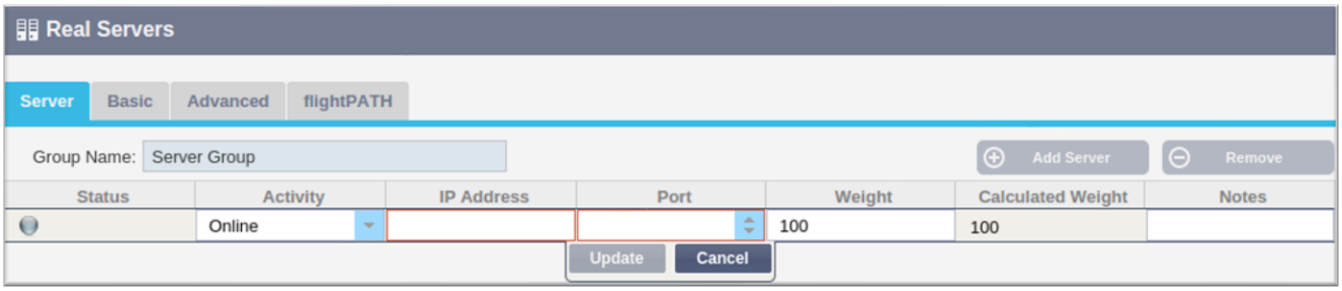


- Затем Вы войдете в режим **редактирования строки.**
- Заполните четыре выделенных поля, чтобы продолжить, а затем нажмите кнопку обновления.

Пожалуйста, используйте клавишу TAB для перемещения по полям.

Поле	Описание
IP-адрес	Введите новый виртуальный IP-адрес, который будет целевой точкой входа для доступа к реальному серверу. Этот IP-адрес является местом, на которое будут указывать пользователи или приложения для доступа к приложению с балансировкой нагрузки.
Маска подсети/Префикс	Это поле предназначено для маски подсети, относящейся к сети, в которой находится АЦП
Порт	Порт входа, используемый при доступе к VIP. Это значение не обязательно должно быть таким же, как у реального сервера, если Вы используете обратный прокси.
Название услуги	Название услуги - это текстовое представление назначения VIP-клиента. Оно необязательно, но мы рекомендуем Вам указать его для ясности.
Тип услуги	Существует множество различных типов услуг, которые Вы можете выбрать. Типы услуг уровня 4 не могут использовать технологию flightPATH.

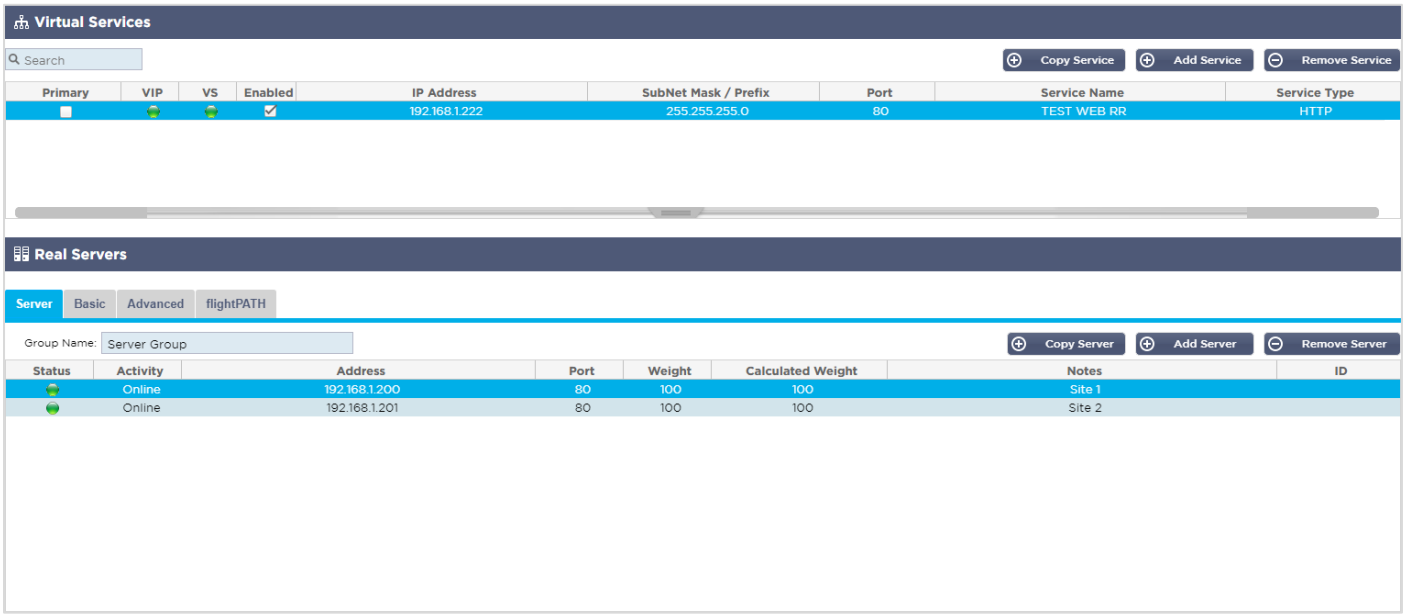
Теперь Вы можете нажать кнопку Update, чтобы сохранить этот раздел и автоматически перейти к разделу Real Server, описанному ниже:



Поле	Описание
Деятельность	Поле Activity можно использовать для отображения и изменения статуса реального сервера с балансировкой нагрузки. Online - Обозначает, что сервер активен и принимает запросы с балансировкой нагрузки Offline - Сервер находится в автономном режиме и не получает запросы. Drain - Сервер был переведен в режим drain, чтобы можно было промыть персистентность и перевести сервер в автономное состояние, не затрагивая пользователей. Standby - Сервер был переведен в состояние ожидания
IP-адрес	Это значение является IP-адресом реального сервера. Он должен быть точным и не должен быть адресом DHCP.
Порт	Целевой порт доступа на реальном сервере. При использовании обратного прокси-сервера он может отличаться от порта входа, указанного на VIP-сервере.
Взвешивание	Эта настройка обычно автоматически конфигурируется АЦП. Вы можете изменить его, если хотите изменить взвешивание приоритетов.

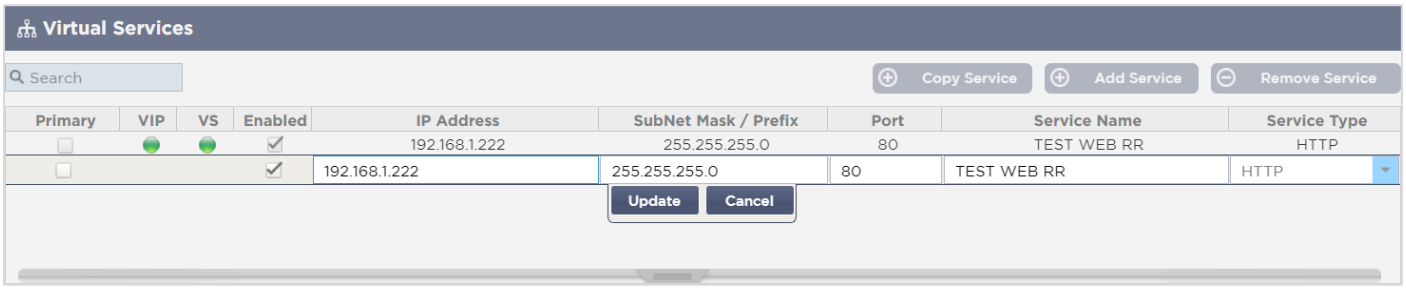
- Нажмите кнопку Обновить или нажмите Enter, чтобы сохранить изменения
- Индикатор состояния сначала станет серым, а затем зеленым, если проверка состояния сервера прошла успешно. Он станет красным, если монитор реального сервера не работает.
- Сервер, на котором горит красный индикатор состояния, не будет сбалансирован по нагрузке.

Пример завершенной виртуальной услуги

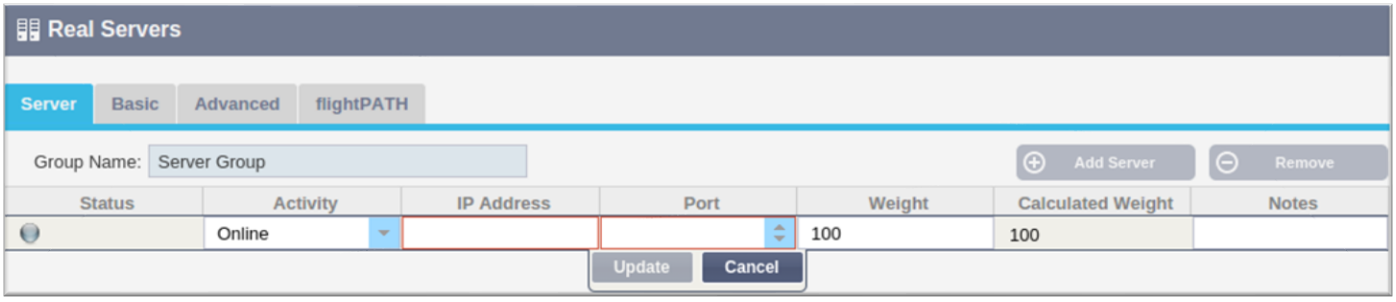


Создайте новую виртуальную службу, используя существующую VIP

- Выделите виртуальную услугу, которую Вы хотите скопировать
- Нажмите Добавить виртуальную услугу, чтобы войти в режим редактирования строки



- IP-адрес и маска подсети копируются автоматически
- Введите номер порта для Вашей услуги
- Введите необязательное Имя услуги
- Выберите тип услуги
- Теперь Вы можете нажать кнопку Обновить, чтобы сохранить этот раздел и автоматически перейти к разделу Реальный сервер ниже

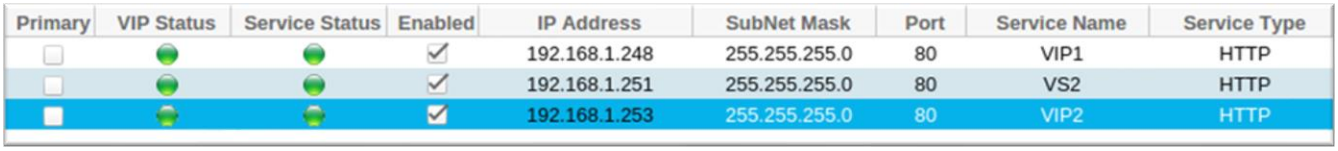


- Оставьте опцию Активность сервера как Онлайн - это означает, что нагрузка будет сбалансирована, если он пройдет стандартный монитор здоровья TCP Connect. Этот параметр может быть изменен позже, если потребуется.
- Введите IP-адрес сервера Real Server
- Введите номер порта для реального сервера
- Введите дополнительное имя для сервера Real Server
- Нажмите Обновить, чтобы сохранить изменения
- Индикатор состояния сначала станет серым, затем зеленым, если проверка здоровья сервера прошла успешно. Он станет красным, если монитор реального сервера не работает.
- Сервер, на котором горит красный индикатор состояния, не будет сбалансирован по нагрузке

Изменение IP-адреса виртуальной службы

Вы можете изменить IP-адрес существующей виртуальной службы или VIP в любое время.

- Выделите виртуальную службу, IP-адрес которой Вы хотите изменить



- Дважды щелкните по полю IP-адреса для этой службы

- Измените IP-адрес на тот, который Вы хотите использовать
- Нажмите кнопку Обновить, чтобы сохранить изменения.

Примечание: Изменение IP-адреса виртуальной службы приведет к изменению IP-адреса всех служб, связанных с VIP

Создание новой виртуальной службы с помощью Copy Service

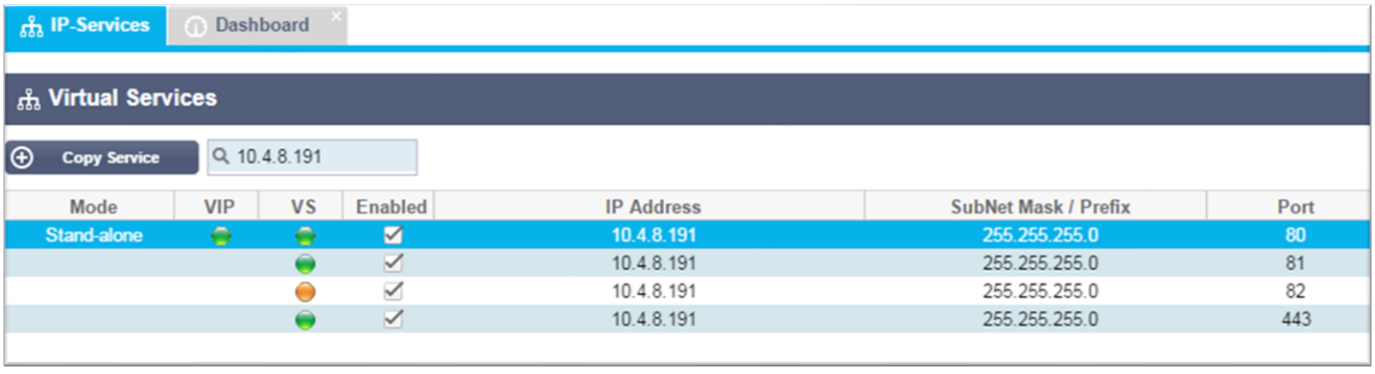
- Кнопка Копировать службу скопирует всю службу, включая все связанные с ней реальные серверы, основные настройки, расширенные настройки и правила flightPATH
- Выделите услугу, которую Вы хотите дублировать, и нажмите Копировать услугу
- Появится редактор строк с мигающим курсором в колонке IP-адрес
- Вы должны изменить IP-адрес, чтобы он был уникальным, или, если Вы хотите сохранить IP-адрес, Вы должны отредактировать Порт, чтобы он был уникальным для этого IP-адреса

Не забудьте отредактировать каждую вкладку, если Вы измените какой-либо параметр, например, политику балансировки нагрузки, монитор Real Server или удалите правило flightPATH.

Фильтрация отображаемых данных

Поиск определенного термина

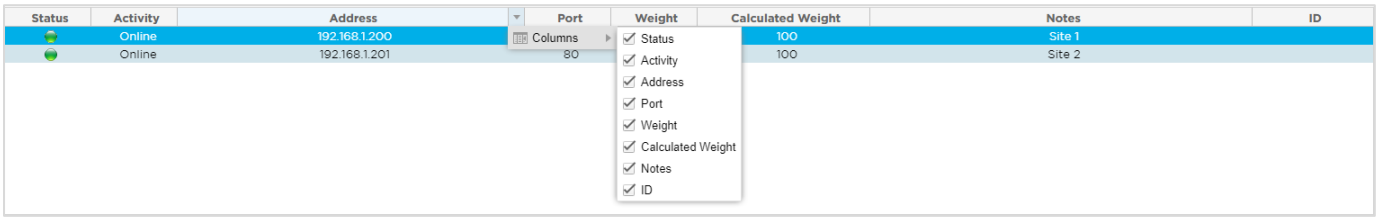
Поле Поиск позволяет Вам искать в таблице, используя любое значение, например, октеты IP-адреса или имя службы.



В примере выше показан результат поиска определенного IP-адреса 10.4.8.191.

Выбор видимости столбцов

Вы также можете выбрать столбцы, которые Вы хотите отобразить на приборной панели.

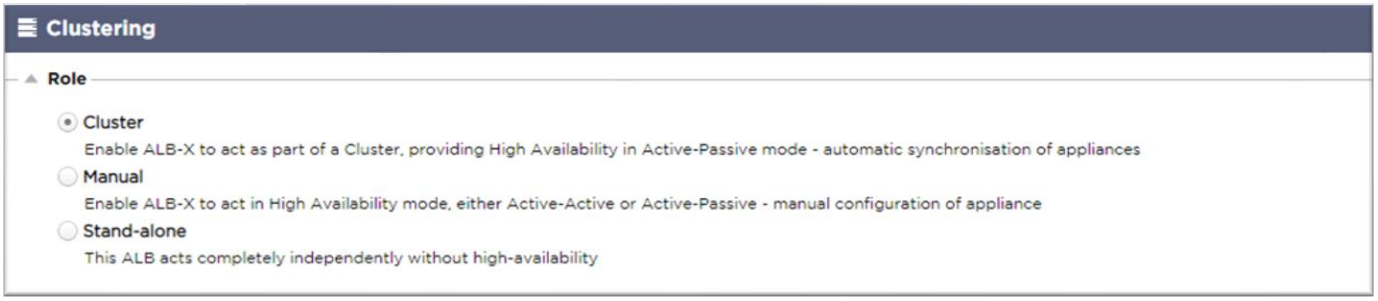


- Наведите курсор мыши на любой из столбцов
- Вы увидите небольшую стрелку, появившуюся с правой стороны колонки
- Щелкая по флажкам, Вы выбираете столбцы, которые Вы хотите видеть на приборной панели.

Понимание колонок виртуальных служб

Основной/режим

Колонка Primary/Mode указывает на роль высокой доступности, выбранную для текущего VIP. Для настройки этого параметра используйте опции, доступные в System > Clustering.



Вариант	Описание
Кластер	Кластер - это роль по умолчанию для ADC при установке, а в колонке Primary/Mode будет указан режим, в котором он работает в настоящее время. Если в Вашем датацентре есть пара устройств ADC в режиме HA, одно из них будет показывать Active, а другое Passive.
Руководство	Роль Manual позволяет паре ADC работать в режиме Active-Active для разных виртуальных IP-адресов. В таких случаях колонка Primary будет содержать поле рядом с каждым уникальным виртуальным IP, которое можно отметить для Active или оставить не отмеченным для Passive.
Автономный	АЦП работает как автономное устройство и не находится в режиме высокой доступности. Поэтому в колонке Primary будет указано Stand-alone.

VIP

Эта колонка предоставляет визуальную обратную связь о состоянии каждой виртуальной услуги. Индикаторы выделены цветом и выглядят следующим образом:

LED	Значение
●	Онлайн
●	Failover-Standby. Эта виртуальная служба работает в режиме горячего резервирования
●	Указывает на то, что "вторичный" задерживает "первичного".
●	Сервис требует внимания. Этот признак может быть результатом того, что реальный сервер не прошел проверку монитора здоровья или был вручную переведен в автономный режим.

	Трафик будет продолжать идти, но с уменьшенной пропускной способностью реального сервера.
●	Не в сети. Серверы содержимого недоступны, или ни один сервер содержимого не включен
●	Состояние находок
●	Не лицензированы или лицензированы Виртуальные IP превышены

Включено

По умолчанию эта опция включена, и флажок отображается как установленный. Вы можете отключить виртуальную службу, дважды щелкнув по строке, сняв флажок, а затем нажав кнопку Обновить.

IP-адрес

Добавьте свой IPv4-адрес в десятичной точечной нотации или IPv6-адрес. Это значение является виртуальным IP-адресом (VIP) для Вашей услуги. Пример IPv4 "192.168.1.100". Пример Ipv6 "2001:0db8:85a3:0000:0000:8a2e:0370:7334".

Маска подсети/Префикс

Добавьте маску подсети в десятичной точечной нотации. Пример "255.255.255.0". Или для IPv6 добавьте свой префикс. Более подробную информацию об IPv6 смотрите в **HTTPS://EN.WIKIPEDIA.ORG/WIKI/IPV6_ADDRESS**

Порт

Добавьте номер порта, связанный с Вашей услугой. Порт может быть номером TCP или UDP порта. Пример TCP "80" для веб-трафика и TCP "443" для защищенного веб-трафика.

Название услуги

Добавьте дружественное имя для идентификации Вашей службы. Пример "Производственные веб-серверы".

Тип услуги

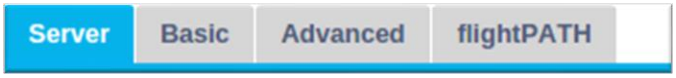
Обратите внимание, что со всеми типами услуг "Layer 4" ADC не будет взаимодействовать или изменять поток данных, поэтому flightPATH недоступен с типами услуг Layer 4. Службы 4-го уровня просто балансируют трафик в соответствии с политикой балансировки нагрузки:

Тип услуги	**Порт/Протокол**	**Уровень обслуживания**	**Комментарий**
TCP 4-го уровня	Любой порт TCP	Уровень 4	АЦП не изменяет никакой информации в потоке данных и выполняет стандартную балансировку нагрузки на трафик в соответствии с политикой балансировки нагрузки
Уровень 4 UDP	Любой UDP-порт	Уровень 4	Как и в случае с TCP 4-го уровня, ADC не изменяет никакой информации в потоке данных и выполняет стандартную балансировку нагрузки трафика в

			соответствии с политикой балансировки нагрузки
Уровень 4 TCP/UDP	Любой порт TCP или UDP	Уровень 4	Это идеальный вариант, если Ваша служба имеет основной протокол, такой как UDP, но будет возвращаться к TCP. ADC не изменяет никакой информации в потоке данных и выполняет стандартную балансировку трафика в соответствии с политикой балансировки нагрузки
DNS	!!!		
HTTP	Протокол HTTP или HTTPS	Уровень 7	АЦП может взаимодействовать, манипулировать и изменять поток данных с помощью flightPATH.
FTP	Протокол передачи файлов Протокол	Уровень 7	Использование отдельных соединений управления и данных между клиентом и сервером
SMTP	Простой протокол передачи почты	Уровень 4	Используйте при балансировке нагрузки на почтовые серверы
POP3	Протокол почтового отделения	Уровень 4	Используйте при балансировке нагрузки на почтовые серверы
IMAP	Протокол доступа к интернет-сообщениям	Уровень 4	Используйте при балансировке нагрузки на почтовые серверы
RDP	Протокол удаленного рабочего стола	Уровень 4	Используйте при балансировке нагрузки серверов служб терминалов
RPC	Удаленный вызов процедуры	Уровень 4	Используйте при балансировке нагрузки систем, использующих вызовы RPC
RPC/ADS	Exchange 2010 Статический RPC для службы адресной книги	Уровень 4	Используйте при балансировке нагрузки серверов Exchange
RPC/CA/PF	Exchange 2010 Static RPC для клиентского доступа и общих папок	Уровень 4	Используйте при балансировке нагрузки серверов Exchange
DICOM	Цифровая визуализация и коммуникации в медицине	Уровень 4	Используйте при балансировке нагрузки серверов, использующих протоколы DICOM

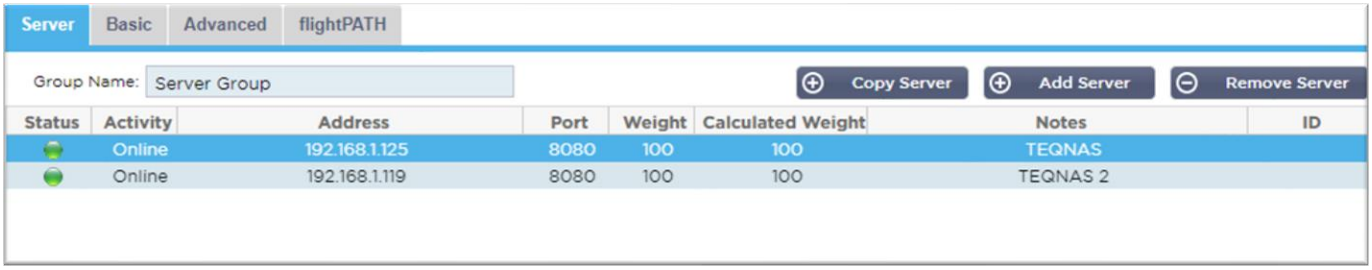
Реальные серверы

В разделе Real Servers приборной панели есть несколько вкладок: Сервер, Базовый, Расширенный и flightPATH.



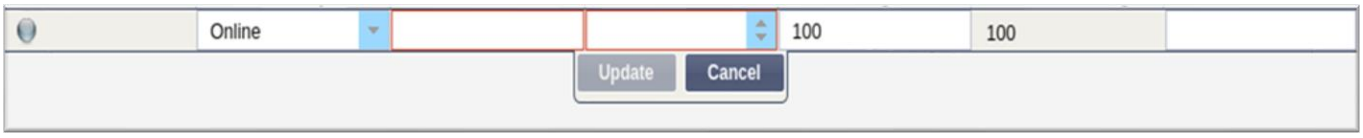
Сервер

Вкладка "Сервер" содержит определения реальных внутренних серверов, сопряженных с выбранной в данный момент виртуальной службой. Вам необходимо добавить хотя бы один сервер в раздел Реальные серверы.



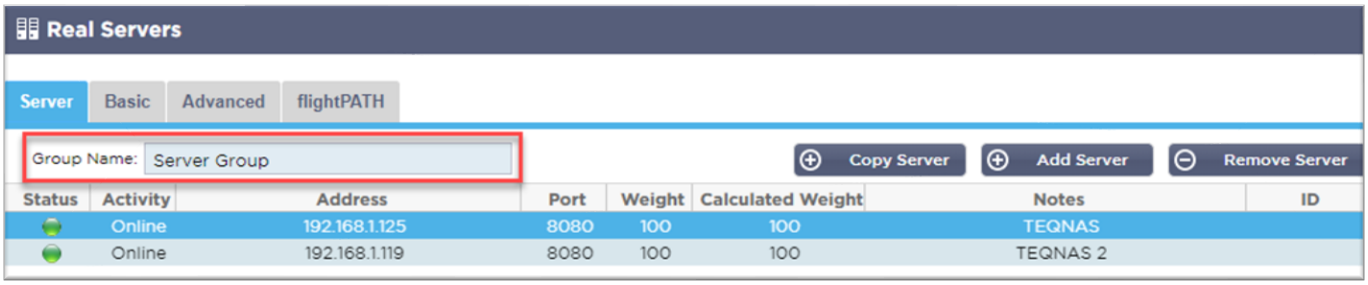
Добавить сервер

- Выберите соответствующий VIP, который Вы ранее определили.
- Нажмите Добавить сервер
- Появится новая строка с мигающим курсором в колонке IP-адрес



- Введите IPv4-адрес Вашего сервера в точечной десятичной системе счисления. Реальный сервер может находиться в той же сети, что и Ваша виртуальная служба, в любой непосредственно подключенной локальной сети или в любой сети, которую может маршрутизировать Ваш ADC. Пример "10.1.1.1".
- Перейдите в колонку Порт и введите номер порта TCP/UDP для Вашего сервера. Номер порта может быть таким же, как номер порта виртуальной службы, или другим номером порта для подключения обратного прокси. ADC будет автоматически переводить на этот номер.
- Перейдите к разделу Примечания, чтобы добавить все необходимые детали для сервера. Пример: "IIS Web Server 1"

Название группы



Когда Вы добавили серверы, составляющие набор для балансировки нагрузки, Вы также можете присвоить им имя группы. После редактирования этого поля его содержимое сохраняется без необходимости нажимать кнопку Обновить.

Индикаторы состояния реального сервера

Вы можете увидеть статус реального сервера по светлому цвету в колонке "Статус". См. ниже:

LED	Значение

●	Подключено
◎	Не контролируется
●	Слив
●	Offline
●	В режиме ожидания
●	Не подключено
●	Статус находки
●	Не лицензировано или превышено количество лицензированных серверов Real Servers

Деятельность

Вы можете изменить Активность реального сервера в любое время, используя выпадающее меню. Для этого дважды щелкните на строке Реального сервера, чтобы перевести ее в режим редактирования.

Вариант	Описание
Онлайн	Все Real Servers, назначенные Online, будут получать трафик в соответствии с политикой балансировки нагрузки, установленной на вкладке Basic.
Слив	Все реальные серверы, назначенные как "Слив", будут продолжать обслуживать существующие соединения, но не будут принимать новые соединения. Индикатор состояния будет мигать зеленым/синим цветом, пока идет процесс слива. Как только существующие соединения естественным образом закроются, реальные серверы перейдут в автономный режим, а индикатор состояния будет гореть синим цветом. Вы также можете просмотреть эти соединения, перейдя в раздел Навигация > Монитор > Статус.
Offline	Все реальные серверы, установленные как Offline, будут немедленно переведены в автономный режим и не будут получать трафик.
В режиме ожидания	Все реальные серверы, установленные как резервные, будут оставаться в автономном режиме до тех пор, пока **ВСЕ** серверы группы Online не пройдут проверку Server Health Monitor. Трафик будет приниматься резервной группой в соответствии с политикой балансировки нагрузки, когда это произойдет. Если один сервер в группе Online пройдет проверку Server Health Monitor, этот сервер Online будет получать весь трафик, а группа Standby перестанет получать трафик.

IP-адрес

Это поле - IP-адрес Вашего сервера Real Server. Пример "192.168.1.200".

Порт

Номер порта TCP или UDP, который прослушивает Real Server для данной службы. Пример "80" для веб-трафика.

Вес

Эта колонка станет редактируемой, когда будет указана соответствующая политика балансировки нагрузки.

Вес по умолчанию для Real Server равен 100, и Вы можете ввести значения от 1 до 100. Значение 100 означает максимальную нагрузку, а 1 - минимальную.

Пример для трех серверов может выглядеть примерно так:

- Вес сервера 1 = 100
- Вес сервера 2 = 50
- Вес сервера 3 = 50

Если учесть, что политика балансировки нагрузки установлена на Least Connections, и всего имеется 200 клиентских подключений;

- Сервер 1 получит 100 одновременных соединений
- Сервер 2 получит 50 одновременных соединений
- Сервер 3 получит 50 одновременных соединений

Если бы мы использовали Round Robin в качестве метода балансировки нагрузки, который ротирует запросы через набор серверов с балансировкой нагрузки, изменение весов влияет на то, как часто серверы выбираются в качестве цели.

Если мы считаем, что политика балансировки нагрузки Fastest использует наименьшее время, необходимое для ПОЛУЧЕНИЯ ответа, то корректировка весов изменяет смещение аналогично Least Connections.

Рассчитанный вес

Расчетный вес каждого сервера можно просматривать динамически, он рассчитывается автоматически и не редактируется. Поле показывает фактический вес, который ADC использует при учете ручного взвешивания и политики балансировки нагрузки.

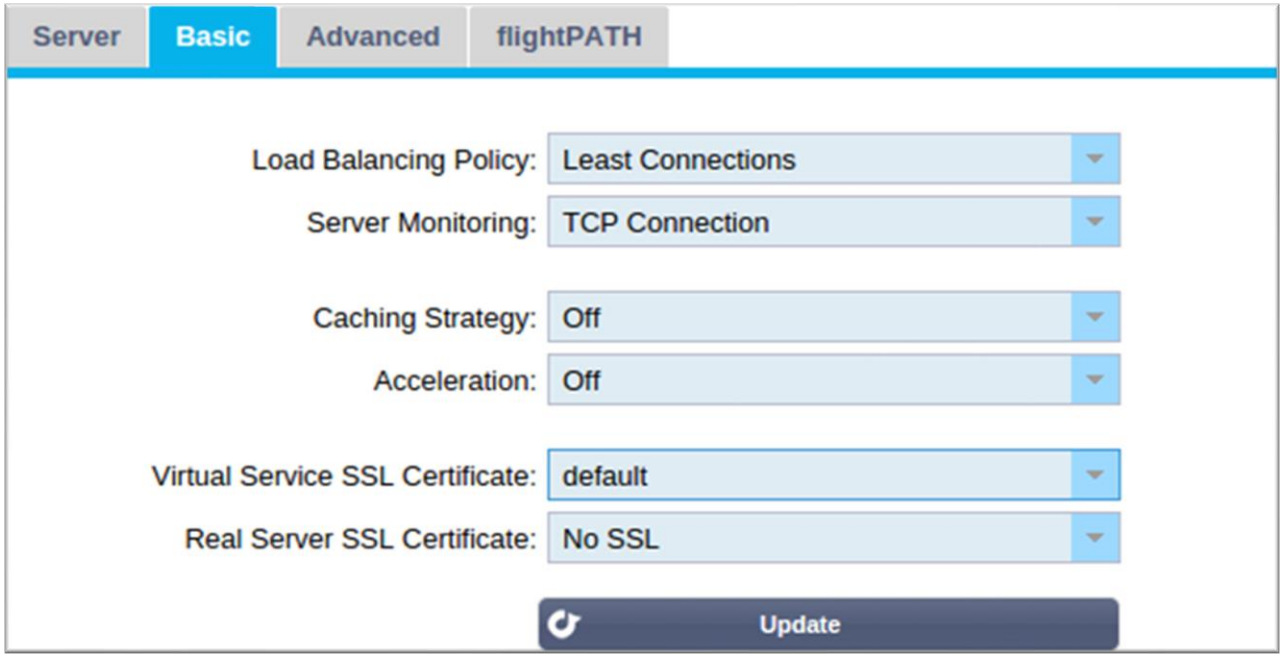
Примечания

Введите в поле Примечания любые особые заметки, полезные для описания определяемой записи. Пример "IIS Server1 - London DC".

ID

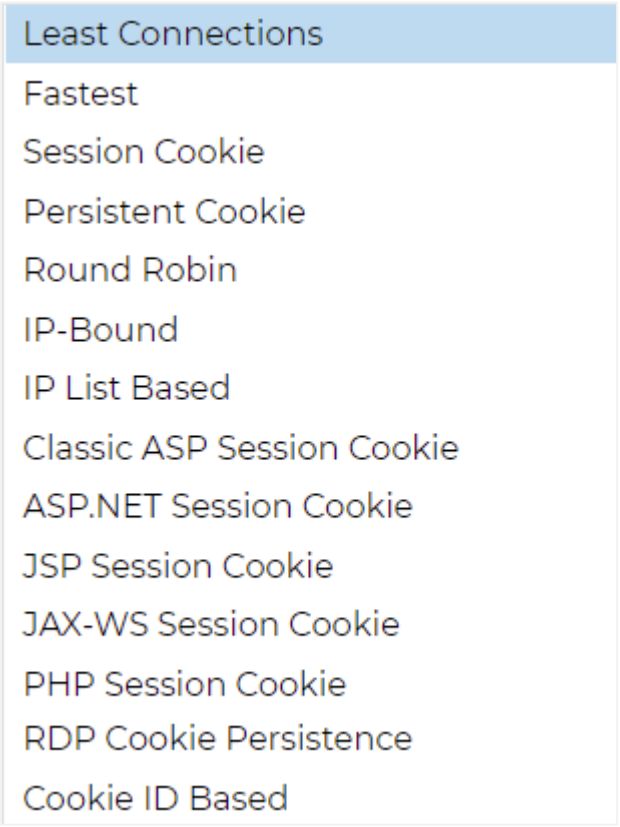
Поле ID используется в рамках политики балансировки нагрузки Cookie ID. ID номер, размещенный здесь, используется для идентификации

Базовый



Политика балансировки нагрузки

Выпадающий список показывает Вам поддерживаемые в настоящее время политики балансировки нагрузки, доступные для использования. Список политик балансировки нагрузки вместе с пояснениями приведен ниже.



Вариант	Описание

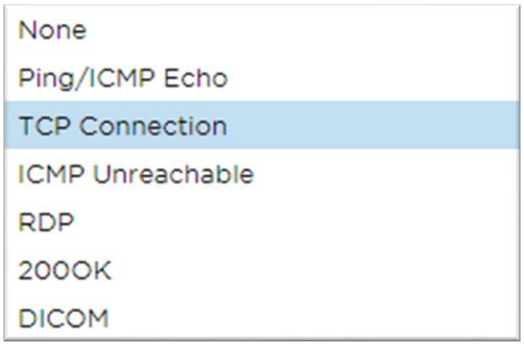
Самый быстрый	Политика балансировки нагрузки Fastest автоматически рассчитывает время ответа на все запросы для каждого сервера, сглаженное по времени. Колонка Рассчитанный вес содержит автоматически рассчитанное значение. Ручной ввод возможен только при использовании этой политики балансировки нагрузки.
Раунд Робин	Round Robin обычно используется в брандмауэрах и базовых балансировщиках нагрузки и является самым простым методом. Каждый реальный сервер получает новый запрос по порядку. Этот метод подходит только тогда, когда Вам нужно равномерно распределить нагрузку запросов на серверы; примером могут служить поисковые веб-серверы. Однако, когда Вам нужно сбалансировать нагрузку на основе нагрузки приложения или нагрузки сервера, или даже обеспечить использование одного и того же сервера для сессии, метод Round Robin неуместен.
Наименьшие связи	Балансировщик нагрузки будет отслеживать количество текущих подключений к каждому Real Server. Сервер Real Server с наименьшим количеством соединений получает последующий новый запрос.
Layer 3 Session Affinity/Persistence - IP Bound	В этом режиме IP-адрес клиента формирует основу для выбора того, какой Real Server получит запрос. Это действие обеспечивает постоянство. HTTP и протоколы 4-го уровня могут использовать этот режим. Этот метод полезен для внутренних сетей, где топология сети известна, и Вы можете быть уверены, что нет "супер-прокси" выше по течению. При использовании Layer 4 и прокси-серверов все запросы могут выглядеть так, как будто они исходят от одного клиента, и поэтому нагрузка будет неравномерной. В HTTP информация заголовка (X-Forwarder-For) используется при наличии, чтобы справиться с прокси.
Слияние/сохранение сеансов 3-го уровня - на основе списка IP-адресов	Соединение с Real Server инициируется с использованием "Наименьшего количества соединений", затем на основе IP-адреса клиента достигается привязка к сеансу. По умолчанию список ведется в течение 2 часов, но его можно изменить с помощью jetPACK.
Уровень 7 Принадлежность/ постоянство сеанса - Куки сеанса	Этот режим является наиболее популярным методом балансировки нагрузки для HTTP. В этом режиме ADC использует балансировку нагрузки на основе IP-списков для каждого первого запроса. Он вставляет cookie в заголовки первого HTTP-ответа. После этого ADC использует cookie клиента для маршрутизации трафика на один и тот же внутренний сервер. Этот файл cookie используется для постоянства, когда клиенту необходимо каждый раз обращаться к одному и тому же внутреннему серверу. Срок действия куки истекает после закрытия сессии.
Уровень 7 Принадлежность/постоянство сеанса - Постоянный файл cookie	Режим балансировки нагрузки на основе списка IP используется для каждого первого запроса. АЦП вставляет cookie в заголовки первого HTTP-ответа. После этого ADC использует cookie клиента для маршрутизации трафика на один и тот же внутренний сервер. Этот файл cookie используется для постоянства, когда клиент должен каждый раз обращаться к одному и тому же внутреннему серверу. Срок действия cookie истечет через 2 часа, и соединение будет сбалансировано по нагрузке в соответствии с алгоритмом, основанным на списке IP-адресов. Это время истечения срока действия можно настроить с помощью jetPACK.

Cookie сессии - Классическая Cookie сессии ASP	Active Server Pages (ASP) - это технология Microsoft на стороне сервера. При выборе этой опции ADC будет поддерживать постоянство сеанса на одном и том же сервере, если ASP cookie будет обнаружен и найден в его списке известных cookie. При обнаружении нового файла cookie ASP нагрузка будет сбалансирована с использованием алгоритма наименьших подключений.
Cookie сессии - ASP.NET Cookie сессии	Этот режим применяется к **ASP.net.** При выборе этого режима ADC будет поддерживать постоянство сессии на одном и том же сервере, если куки ASP.NET обнаружены и найдены в его списке известных куки. При обнаружении нового куки ASP, нагрузка будет сбалансирована с использованием алгоритма наименьших подключений.
Cookie сессии - Cookie сессии JSP	Java Server Pages (JSP) - это серверная технология Oracle. При выборе этого режима ADC будет поддерживать постоянство сеанса на одном и том же сервере, если куки JSP будут обнаружены и найдены в списке известных куки. При обнаружении нового JSP cookie, нагрузка будет сбалансирована с использованием алгоритма наименьших соединений.
Cookie сессии - JAX-WS Cookie сессии	Веб-сервисы Java (JAX-WS) - это технология Oracle на стороне сервера. При выборе этого режима АЦП будет поддерживать постоянство сеанса на одном и том же сервере, если куки JAX-WS будут обнаружены и найдены в его списке известных куки. При обнаружении нового куки-файла JAX-WS, нагрузка будет сбалансирована с использованием алгоритма наименьших подключений.
Cookie сессии - PHP Cookie сессии	Personal Home Page (PHP) - это технология с открытым исходным кодом на стороне сервера. При выборе этого режима АЦП будет поддерживать постоянство сессии на одном и том же сервере при обнаружении куки PHP.
Сессионный куки - постоянство куки RDP	Этот метод балансировки нагрузки использует созданный Microsoft RDP Cookie на основе имени пользователя/домена для обеспечения постоянства соединения с сервером. Преимущество этого метода заключается в том, что поддержание соединения с сервером возможно даже при изменении IP-адреса клиента.
На основе идентификатора cookie	Новый метод, очень похожий на "PhpCookieBased" и другие методы балансировки нагрузки, но использующий CookieIDBased и cookie RegEx h=[^;]+ Этот метод будет использовать значение, установленное в поле примечаний реального сервера "ID=X;" в качестве значения cookie для идентификации сервера. Таким образом, это означает, что этот метод аналогичен методу CookieListBased, но использует другое имя cookie и хранит уникальное значение cookie, не зашифрованный IP, а ID с реального сервера (считывается при загрузке). Значение по умолчанию - CookieIDName="h"; однако, если в конфигурации расширенных настроек виртуального сервера есть переопределенное значение, используйте его вместо этого. **ПРИМЕЧАНИЕ**: Если это значение установлено, мы перезаписываем приведенное выше выражение cookie, чтобы заменить h= на новое значение.

	Последний бит заключается в том, что если приходит неизвестное значение cookie и совпадает с одним из идентификаторов реального сервера, следует выбрать этот сервер; в противном случае используйте следующий метод (делегирование).

Мониторинг сервера

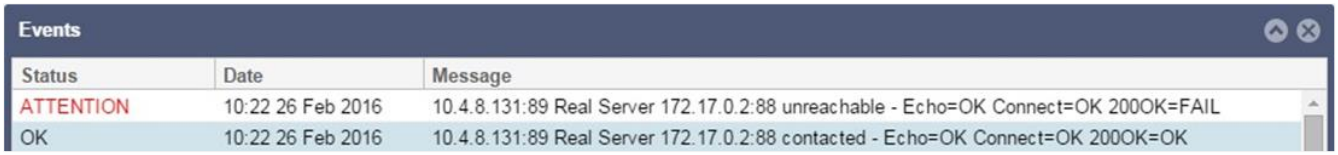
Ваш ADC содержит шесть стандартных методов мониторинга реального сервера, перечисленных ниже.



Выберите метод мониторинга, который Вы хотите применить к виртуальной службе (VIP).

Очень важно выбрать правильный монитор для службы. Например, если Real Server является RDP-сервером, монитор 200OK не подходит. Если Вы не уверены в том, какой монитор выбрать, то TCP Connection по умолчанию - отличное место для начала.

Вы можете выбрать несколько мониторов, поочередно нажимая на каждый монитор, который Вы хотите применить к службе. Выбранные мониторы выполняются в том порядке, в котором Вы их выбрали; поэтому сначала начните с мониторов нижних уровней. Например, установка мониторов Ping/ICMP Echo, TCP Connection и 200OK будет отображаться в Событиях приборной панели, как показано на рисунке ниже:



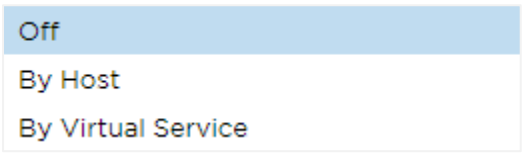
Мы видим, что Layer 3 Ping и Layer 4 TCP Connect прошли успешно, если мы посмотрим на верхнюю строку, но Layer 7 200OK потерпел неудачу. Эти результаты мониторинга дают достаточно информации, чтобы показать, что маршрутизация в порядке и есть служба, запущенная на соответствующем порту, но веб-сайт не отвечает правильно на запрошенную страницу. Теперь пришло время взглянуть на веб-сервер и раздел Library > Real Server Monitor, чтобы увидеть детали отказавшего монитора.

Вариант	**Описание**
Нет	В этом режиме мониторинг реального сервера не ведется, и он всегда работает правильно. Настройка None полезна в ситуациях, когда мониторинг расстраивает сервер, а также для служб, которые не должны участвовать в отказоустойчивом действии ADC. Это маршрут для размещения ненадежных или устаревших систем, которые не являются основными для операций H/A. Используйте этот метод мониторинга с любым типом службы.

Ping/ICMP Echo	В этом режиме АЦП посылает эхо-запрос ICMP на IP-адрес сервера контента. Если получен правильный эхо-ответ, ADC считает, что реальный сервер работает, и пропускная способность трафика к серверу продолжается. Он также будет поддерживать доступность услуги на паре H/A. Этот метод мониторинга можно использовать с любым типом услуги.
TCP-соединение	В этом режиме устанавливается TCP-соединение с реальным сервером и сразу же разрывается без отправки каких-либо данных. Если соединение успешно установлено, АЦП считает, что Реальный сервер работает. Этот метод мониторинга можно использовать с любым типом сервиса. Только службы UDP в настоящее время не подходят для мониторинга TCP-соединения.
ICMP Unreachable	ADC отправит проверку работоспособности UDP на сервер и пометит Real Server как недоступный, если получит сообщение ICMP port unreachable. Этот метод может быть полезен, когда Вам нужно проверить, доступен ли служебный порт UDP на сервере, например, порт DNS 53.
RDP	В этом режиме TCP-соединение инициализируется, как описано в методе ICMP Unreachable. После инициализации соединения запрашивается RDP-соединение уровня 7. Если соединение подтверждается, ADC считает, что Real Server работает. Этот метод мониторинга можно использовать с любым сервером терминалов Microsoft.
200 OK	В этом методе инициализируется TCP-соединение с реальным сервером. После успешного соединения АЦП отправляет Реальному серверу HTTP-запрос. Ожидается ответ HTTP, который проверяется на наличие кода ответа "200 OK". Если получен код ответа "200 OK", АЦП считает, что Реальный сервер работает. Если ADC не получает код ответа "200 OK" по какой-либо причине, включая таймаут, невозможность подключения и другие причины, ADC считает Реальный сервер недоступным. Этот метод мониторинга действителен только для использования с типами служб HTTP и ускоренного HTTP. Если для HTTP-сервера используется тип сервиса 4-го уровня, он может использоваться, если SSL не используется на реальном сервере или обрабатывается соответствующим образом с помощью средства "Content SSL".
DICOM	TCP-соединение инициализируется с Real Server в режиме DICOM, и Echoscu "Associate Request" выполняется на Real Server при подключении. Разговор, включающий "Associate Accept" от сервера содержимого, передачу небольшого количества данных, за которым следует "Release Request", а затем "Release Response", успешно завершает монитор. Если по какой-либо причине монитор не завершается успешно, то Реальный сервер считается отключенным.
Определяется пользователем	Любой монитор, настроенный в разделе Мониторинг реального сервера, появится в списке.

Стратегия кэширования

По умолчанию стратегия кэширования отключена и установлена как Выкл. Если тип Вашего сервиса - HTTP, то Вы можете применить два типа стратегии кэширования.



Обратитесь к странице Настроить кэш для детальной настройки параметров кэша. Обратите внимание, что когда кэширование применяется к VIP с типом сервиса Accelerated "HTTP", сжатые объекты не кэшируются.

Вариант	Описание
Ведущий	Кэширование на хост основано на приложении на имя хоста. Для каждого домена/имени хоста будет существовать отдельный кэш. Этот режим идеально подходит для веб-серверов, которые могут обслуживать несколько веб-сайтов в зависимости от домена.
Виртуальной службой	Кэширование для каждой виртуальной службы доступно при выборе этой опции. Только один кэш будет существовать для всех доменов/хост-имен, которые проходят через виртуальную службу. Эта опция является специализированной настройкой для использования с несколькими клонами одного сайта.

Ускорение

Вариант	Описание
На сайте	Отключите сжатие для виртуальной службы
Компрессия	Когда эта опция выбрана, она включает сжатие для выбранной Виртуальной службы. АЦП динамически сжимает поток данных, передаваемый клиенту по запросу. Этот процесс применяется только к объектам, содержащим заголовок content-encoding: gzip. Пример содержимого включает HTML, CSS или Javascript. Вы также можете исключить определенные типы контента, используя раздел Глобальные исключения.

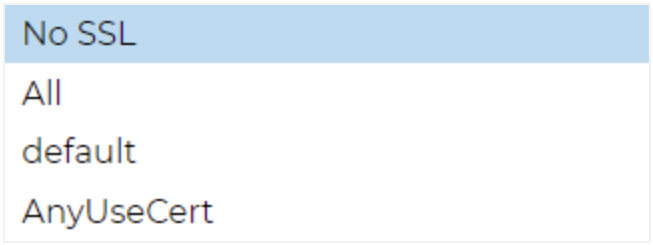
Примечание: Если объект является кэшируемым, ADC будет хранить сжатую версию и обслуживать ее статически (из памяти) до тех пор, пока срок действия содержимого не истечет и оно не будет повторно проверено.

SSL-сертификат виртуальной службы (шифрование между клиентом и ADC)

По умолчанию установлено значение Нет SSL. Если тип Вашей службы "HTTP" или "Layer4 TCP", Вы можете выбрать сертификат из выпадающего списка, чтобы применить его к Виртуальной службе. В этом списке появятся сертификаты, которые были созданы или импортированы. Вы можете выделить несколько сертификатов для применения к службе. Эта операция автоматически включит расширение SNI, чтобы разрешить сертификат на основе "Доменного имени", запрошенного клиентом.

Индикация имени сервера

Эта опция является расширением сетевого протокола TLS, с помощью которого клиент указывает имя хоста, к которому он пытается подключиться, в начале процесса квитирования. Эта настройка позволяет ADC представлять несколько сертификатов на одном виртуальном IP-адресе и TCP-порту.

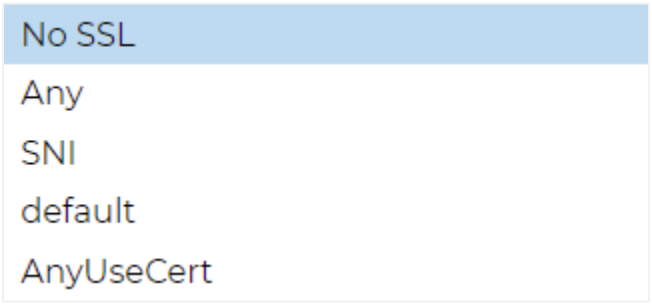


Вариант	Описание

Нет SSL	Трафик от источника к АЦП не шифруется.
Все	Загружает все доступные сертификаты для использования
По умолчанию	Эта опция приводит к применению локально созданного сертификата под названием "Default" на стороне канала браузера. Используйте эту опцию для тестирования SSL, если сертификат не был создан или импортирован.
AnyUseCert	Используйте любой сертификат, имеющийся на АЦП, который пользователь загрузил или сгенерировал

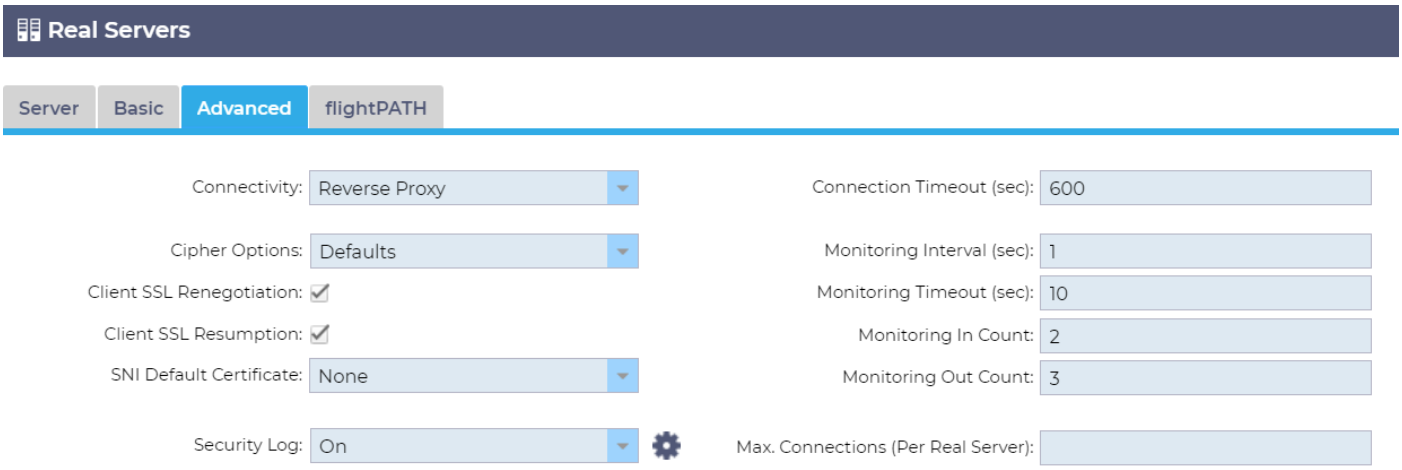
SSL-сертификат реального сервера (шифрование между АЦП и реальным сервером)

По умолчанию для этой опции установлено значение No SSL. Если Ваш сервер требует зашифрованного соединения, это значение должно быть любым другим, кроме No SSL. Сертификаты, которые были созданы или импортированы, появятся в этом списке.



Вариант	**Описание**
Нет SSL	Трафик от АЦП к Реальному серверу не шифруется. Выбор сертификата на стороне браузера означает, что "No SSL" может быть выбран на стороне клиента для обеспечения того, что известно как "SSL Offload".
Любой	ADC действует как клиент и примет любой сертификат, который представит Real Server. Трафик от АЦП к Реальному серверу шифруется, когда выбрана эта опция. Используйте опцию "Любой", когда сертификат указан на стороне Виртуальной службы, обеспечивая так называемое "SSL Bridging" или "SSL Re-Encryption".
SNI	ADC действует как клиент и примет любой сертификат, который представит Real Server. Трафик от АЦП к Реальному серверу шифруется, если выбрана эта опция. Используйте опцию "Любой", когда сертификат указан на стороне Виртуальной службы, обеспечивая так называемое "SSL Bridging" или "SSL Re-Encryption". Выберите эту опцию, чтобы включить SNI на стороне сервера.
AnyUseCert	Здесь отображаются любые сертификаты, которые Вы создали или импортировали в ADC.

Расширенный



Связь

Ваша виртуальная услуга может быть сконфигурирована с четырьмя различными типами подключения. Пожалуйста, выберите режим подключения, который будет применяться к услуге.

Вариант	**Описание**
Обратный прокси-сервер	Обратный прокси является значением по умолчанию и работает на Layer7 со сжатием и кэшированием. И на Уровне 4 без кэширования и сжатия. В этом режиме Ваш ADC действует как обратный прокси и становится адресом источника, который видят реальные серверы.
Прямой возврат сервера	Прямой возврат сервера или DSR, как он широко известен (DR - Direct Routing в некоторых кругах), позволяет серверу за балансировщиком нагрузки отвечать клиенту напрямую, минуя ADC при ответе. DSR подходит только для использования с балансировкой нагрузки 4-го уровня. Поэтому кэширование и сжатие недоступны при выборе этой опции. Балансировка нагрузки на уровне 7 не работает с этим DSR. Также нет поддержки постоянства, кроме IP List Based. SSL/TLS балансировка нагрузки с помощью этого метода не идеальна, так как поддержка Source IP persistence является единственным доступным типом. DSR также требует изменений Реального сервера. Пожалуйста, обратитесь к разделу Изменения реального сервера.
Шлюз	Режим шлюза позволяет Вам направлять весь трафик через ADC, позволяя трафику от Real Servers направляться через ADC в другие сети через виртуальные машины ADC или аппаратные интерфейсы. Использование устройства в качестве шлюза для Real Servers идеально при работе в многоинтерфейсном режиме. Балансировка нагрузки на уровне 7 с помощью этого метода не работает, так как нет поддержки постоянства, кроме как на основе IP-списка. Этот метод требует, чтобы Real Server установил свой шлюз по умолчанию на локальный адрес интерфейса (eth0, eth1 и т.д.) ADC. Пожалуйста, обратитесь к разделу Изменения реального сервера. ***Обратите внимание, что режим шлюза не поддерживает обход отказа в кластерной среде.***

Параметры шифра

Вы можете установить шифры на уровне каждой услуги, и это актуально только для услуг с включенным SSL/TLS. ADC выполняет автоматический выбор шифра, и Вы можете добавлять

различные шифры с помощью jetPACKS. Добавив соответствующий jetPACK, Вы можете установить параметры шифра для каждой услуги. Преимуществом этого является то, что Вы можете создать несколько служб с различными уровнями безопасности. Имейте в виду, что старые клиенты не совместимы с новыми шифрами, чтобы уменьшить количество клиентов, чем более безопасна служба.

Переговоры SSL клиента

Отметьте это поле, если Вы хотите разрешить инициируемое клиентом пересогласование SSL. Запретите клиентское пересогласование SSL для предотвращения возможных DDOS-атак на SSL-уровень, сняв галочку с этой опции.

Возобновление SSL клиента

Отметьте это поле, если Вы хотите включить SSL Resumption Server сессий, добавленных в кэш сессий. Когда клиент предлагает повторное использование сессии, сервер попытается повторно использовать сессию, если она будет найдена. Если флажок "Возобновление" не установлен, кэширование сессий для клиента или сервера не происходит.

SNI Сертификат по умолчанию

Во время SSL-соединения с включенной функцией SNI на стороне клиента, если запрашиваемый домен не соответствует ни одному из сертификатов, назначенных службе, ADC представит сертификат SNI по умолчанию. По умолчанию для этого параметра установлено значение Нет, что приведет к обрыву соединения в случае отсутствия точного совпадения. Выберите любой из установленных сертификатов из выпадающего списка для представления в случае, если точное совпадение SSL-сертификата не будет достигнуто.

Журнал безопасности

'On' - это значение по умолчанию, которое используется для каждой службы и позволяет службе записывать информацию об аутентификации в журналы W3C. Щелкнув на значке Cog, Вы перейдете на страницу System > Logging, где Вы можете проверить настройки протоколирования W3C.

Таймаут соединения

По умолчанию тайм-аут соединения составляет 600 секунд или 10 минут. Этот параметр регулирует время тайм-аута соединения при отсутствии активности. Уменьшите это значение для недолговечного веб-трафика без статических данных, который обычно составляет 90 секунд или меньше. Увеличьте этот показатель для соединений с активным состоянием, таких как RDP, до 7200 секунд (2 часа) или более, в зависимости от Вашей инфраструктуры. Пример с тайм-аутом RDP означает, что если у пользователя период бездействия составляет 2 часа или меньше, соединения останутся открытыми.

Настройки мониторинга

Эти настройки относятся к параметру Мониторы реального сервера на вкладке Основные. В конфигурации есть глобальные записи для подсчета количества успешных или неудачных мониторингов, прежде чем статус сервера будет отмечен как онлайн или неудачный.

Интервал

Интервал - это время в секундах между мониторами. По умолчанию интервал составляет 1 секунду. Хотя 1 с является приемлемым для большинства приложений, может быть полезно увеличить это значение для других приложений или во время тестирования.

Тайм-аут мониторинга

Значение тайм-аута - это время, в течение которого АЦП будет ждать ответа сервера на запрос соединения. Значение по умолчанию составляет 2 с. Увеличьте это значение для загруженных серверов.

Мониторинг В графе

Значение по умолчанию для этой настройки равно 2. Значение 2 указывает на то, что Real Server должен пройти две успешные проверки монитора здоровья, прежде чем он начнет работать. Увеличение этого показателя увеличит вероятность того, что сервер сможет обслуживать трафик, но в зависимости от интервала ему потребуется больше времени для приведения в рабочее состояние. Уменьшение этого значения приведет к более быстрому вводу сервера в эксплуатацию.

Счетчик выходов мониторинга

Значение по умолчанию для этого параметра равно 3, что означает, что монитор Real Server должен отказать три раза, прежде чем ADC прекратит отправку трафика на сервер, и он будет помечен как RED и Unreachable. Увеличение этого показателя приведет к улучшению и повышению надежности обслуживания за счет времени, которое требуется ADC для прекращения отправки трафика на этот сервер.

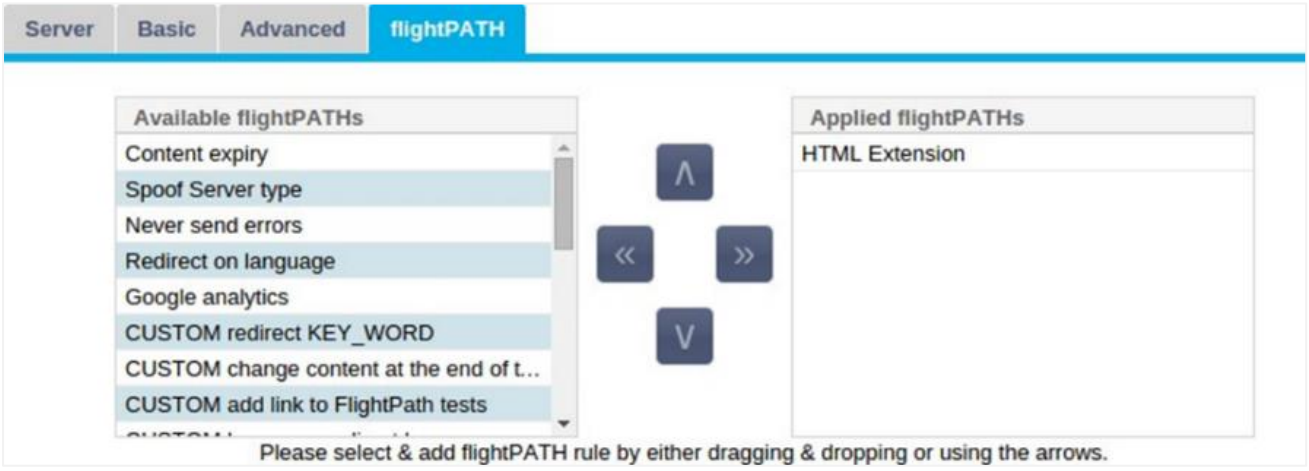
Переход в автономный режим при сбое

Когда этот флажок установлен, реальные серверы, которые не прошли проверку здоровья, переводятся в автономный режим и могут быть включены только вручную.

Макс. Соединения

Ограничивает количество одновременных соединений Real Server и устанавливается для каждой службы. Например, если Вы настроите значение 1000 и у Вас есть два сервера Real Server, ADC ограничит **каждый** сервер Real Server до 1000 одновременных соединений. Вы также можете выбрать отображение страницы "Сервер слишком занят" при достижении этого предела на всех серверах, чтобы помочь пользователям понять причину отсутствия ответа или задержки. Оставьте этот параметр пустым для неограниченного количества соединений. То, что Вы установите здесь, зависит от ресурсов Вашей системы.

flightPATH



flightPATH - это система, разработанная компанией Edgenexus и доступная исключительно в рамках ADC. В отличие от движков на основе правил других производителей, flightPATH не работает через командную строку или консоль ввода сценариев. Вместо этого он использует графический интерфейс пользователя для выбора различных параметров, условий и действий, которые необходимо выполнить для достижения требуемого результата. Эти особенности делают flightPATH

чрезвычайно мощным и позволяют сетевым администраторам манипулировать HTTPS-трафиком очень эффективными способами.

flightPATH доступен только для использования с соединениями HTTPS, и этот раздел не виден, если тип виртуальной службы не HTTP.

Как видно из изображения выше, слева находится список доступных правил, а справа - правила, применяемые к виртуальной службе.

Добавьте доступное правило, перетащив его с левой стороны на правую или выделив правило и нажав стрелку вправо, чтобы переместить его на правую сторону.

Порядок выполнения важен и начинается с верхнего правила, выполняемого первым. Чтобы изменить порядок выполнения, выделите правило и перемещайтесь вверх и вниз с помощью стрелок.

Чтобы удалить правило, перетащите его обратно в инвентарь правил слева или выделите правило и нажмите стрелку влево.

Вы можете добавлять, удалять и редактировать правила flightPATH в разделе Настроить flightPATH данного руководства.

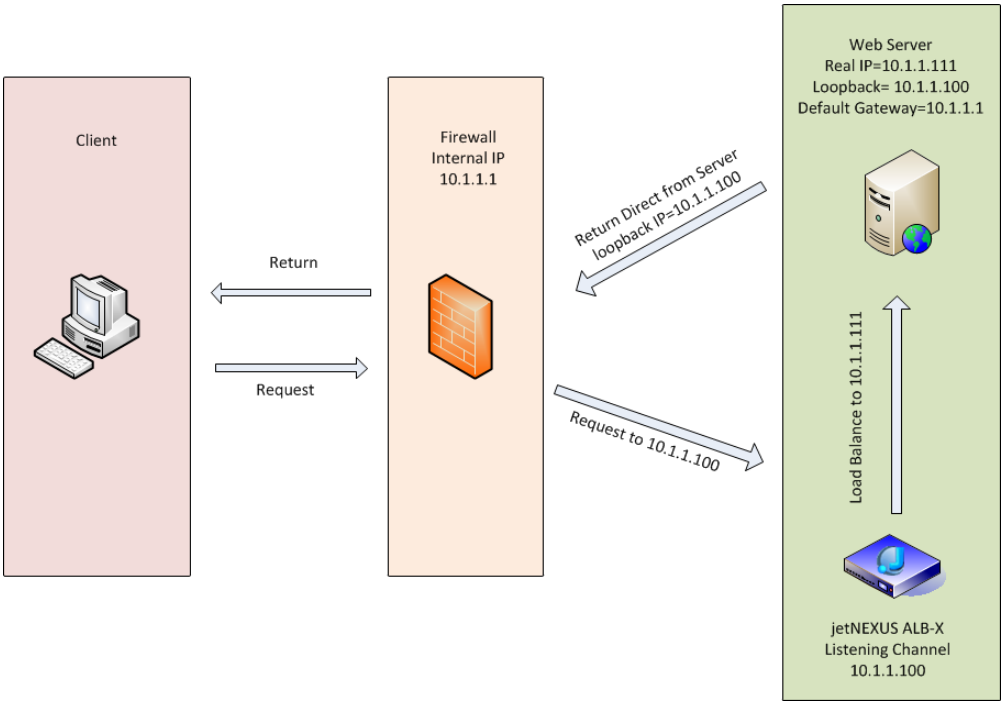
Реальные изменения сервера для прямого возврата сервера

Прямой возврат сервера или DSR, как он широко известен (DR - Direct Routing в некоторых кругах), позволяет серверу за ADC отвечать клиенту напрямую, минуя ADC при ответе. DSR подходит только для использования с балансировкой нагрузки 4-го уровня. Кэширование и сжатие недоступны, если они включены.

Балансировка нагрузки на уровне 7 с помощью этого метода не будет работать, так как нет поддержки постоянства, кроме IP источника. Балансировка нагрузки SSL/TLS с помощью этого метода не является идеальной, поскольку поддерживается только постоянство IP-адреса источника.

Как это работает

- Клиент отправляет запрос на jetNEXUS ALB-X
- Запрос получен edgeNEXUS
- Запрос направляется на серверы контента
- Ответ отправляется непосредственно клиенту без прохождения через edgeNEXUS



Необходимая конфигурация сервера содержимого

Общие сведения

- Шлюз по умолчанию сервера содержимого должен быть настроен как обычно. (Не через ADC)
- Сервер контента и балансировщик нагрузки должны находиться в одной подсети

Windows

- Сервер контента должен иметь loopback или Alias, настроенный на IP-адрес канала или VIP.
  - Метрика сети должна быть 254 для предотвращения ответа на ARP-запросы
  - Добавление адаптера обратной петли в Windows Server 2012 - Нажмите здесь
  - Добавление адаптера обратной петли в Windows Server 2003/2008 - Нажмите здесь
- Выполните следующее в командной строке для каждого сетевого интерфейса, который Вы настроили на серверах Windows Real Servers

netsh interface ipv4 set interface "Имя сетевого интерфейса Windows" weakhostreceive=enable

netsh interface ipv4 set interface "Windows loopback interface name" weakhostreceive=enable

netsh interface ipv4 set interface "Windows loopback interface name" weakhostsend=enable

Linux

- Добавьте постоянный интерфейс обратной петли
- Отредактируйте "/etc/sysconfig/network-scripts"

ifcfg-lo:1DEVICE=lo
:1IPADDR=x
.x.x.xNETMASK=255
.255.255.255BROADCAST=x
.x.x.xONBOOT=yes

- Отредактируйте "/etc/sysctl.conf"

```
net.ipv4.conf.all.arp_ignore = 1net
.ipv4.conf.eth0.arp_ignore = 1net
.ipv4.conf.eht1.arp_ignore = 1net
.ipv4.conf.all.arp_announce = 2net
.ipv4.conf.eth0.arp_announce = 2net
.ipv4.conf.eth1.arp_announce = 2
```

- Выполните команду "sysctl - p".

Изменения реального сервера - Режим шлюза

Режим шлюза позволяет Вам направлять весь трафик через ADC, и это позволяет трафику, исходящему от серверов контента, направляться через ADC в другие сети через интерфейсы на устройстве ADC. Использование устройства в качестве шлюза для серверов контента должно применяться при работе в многоинтерфейсном режиме.

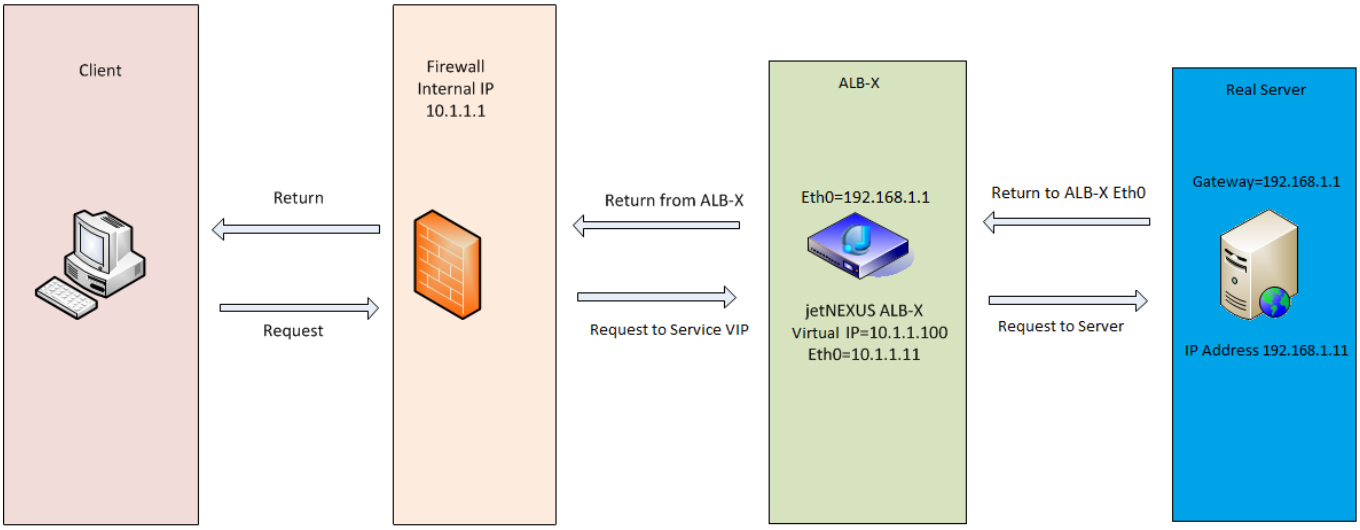
Как это работает

- Клиент отправляет запрос на jetNEXUS ALB-X
- Запрос получен компанией edgeNEXUS
- Запрос, отправленный на серверы контента
- Ответ отправлен на edgeNEXUS
- ADC направляет ответ клиенту

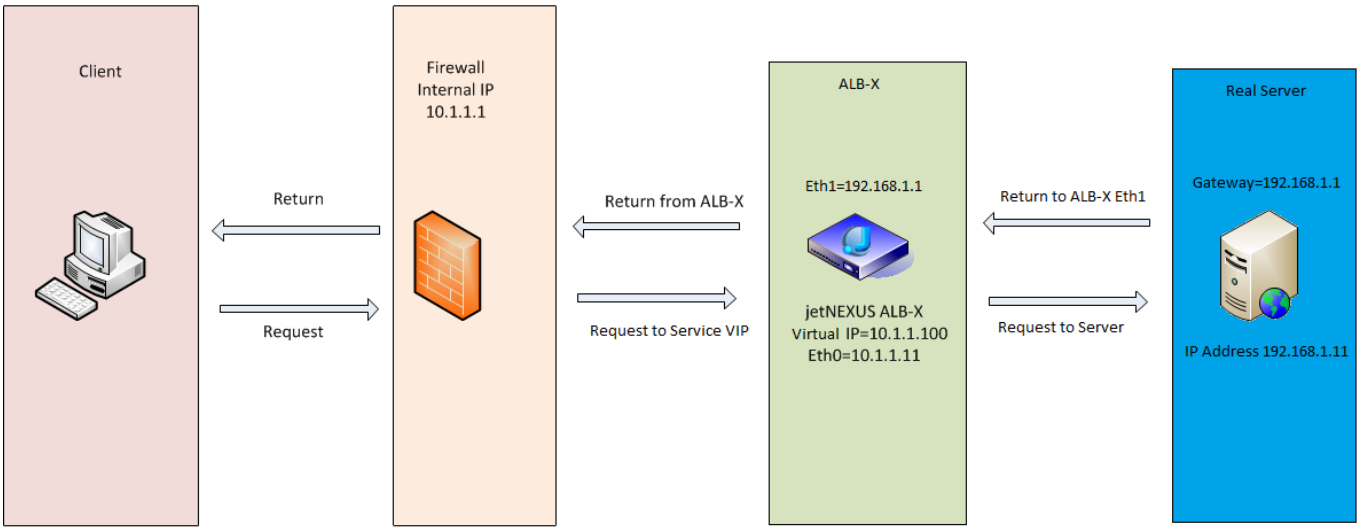
Необходимая конфигурация сервера содержимого

- Режим Single Arm Mode - используется один интерфейс, но служебный VIP и реальные серверы должны находиться в разных подсетях.
- Режим Dual Arm Mode - используются два интерфейса, но служебный VIP и реальный серверы должны находиться в разных подсетях.
- В каждом случае, Single и Dual Arm, Real Servers должны настроить свой шлюз по умолчанию на адрес интерфейса ADC в соответствующей подсети.

Пример с одной рукой



Пример двойного рычага



Библиотека

Дополнения

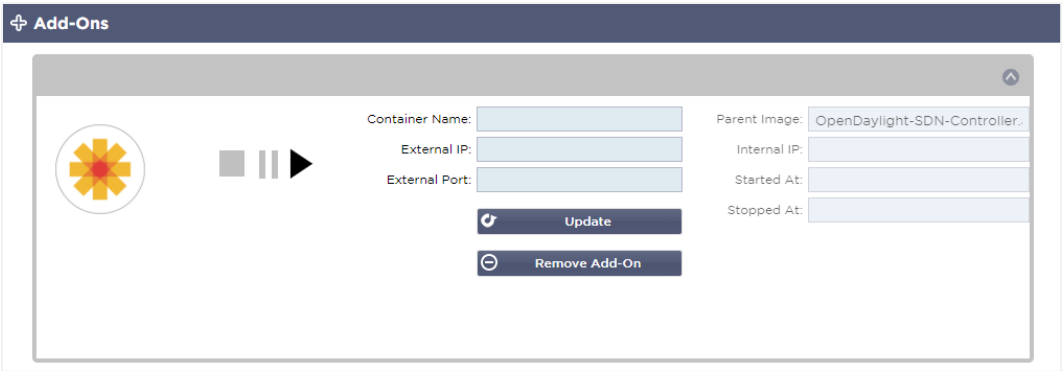
Дополнения - это контейнеры на базе Docker, которые могут работать в изолированном режиме внутри ADC. Примерами дополнений могут быть брандмауэр приложений или даже микро экземпляр самого ADC.

Приложения

Раздел Apps в Add-Ons содержит подробную информацию о приложениях, которые Вы приобрели, загрузили и развернули.

Если приложений нет, в этом разделе появится сообщение, предлагающее Вам перейти в раздел "Приложения", загрузить и установить приложение.

Как только Вы развернете приложение, оно появится в области Apps.



Приобретение дополнения

Чтобы приобрести приложение, Вам необходимо зарегистрироваться в App Store. Покупка осуществляется с помощью самого АЦП. Вы найдете

Перейдите на страницу Библиотека > Приложения приборной панели ADC.

Здесь Вы можете выбрать приложение, которое Вы хотите загрузить, а затем установить.

Если Вы делаете это с приборной панели ADC, выберите только 1 элемент. Вы можете владеть несколькими наборами ADC, и приложения должны быть связаны с ADC, на котором они развернуты.

Если Вы заходите в App Store через настольный компьютер и браузер, Вы можете загрузить столько экземпляров, сколько пожелаете. Например, четыре экземпляра WAF или GSLB. Они появятся в области Purchased Apps Вашего ADC, и Вы сможете их загрузить.

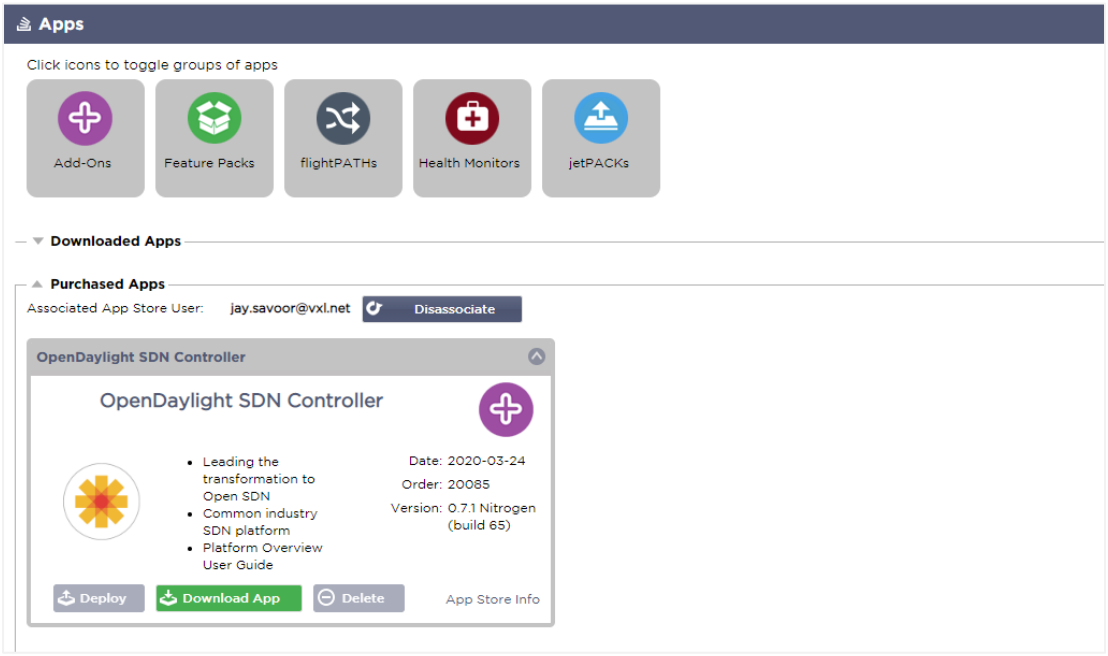
Приложения ассоциируются с принадлежащими Вам и зарегистрированными ADC.

Когда Вы решите загрузить приложение, Вам будет предложено ввести идентификатор машины, после чего приложение будет зашифровано и связано с идентификатором машины ADC.

Ссылки на App Store следующие:

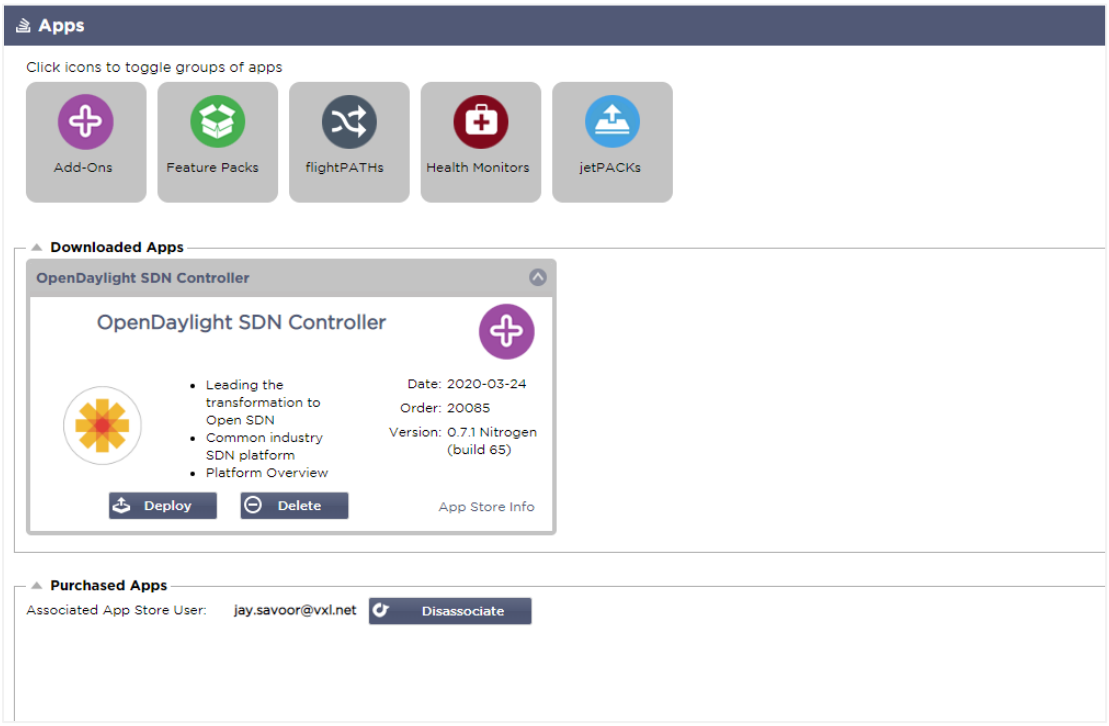
- Дополнения: **HTTPS://APPSTORE.EDGENEXUS.IO/PRODUCT-CATEGORY/ADD-ONS/**
- Мониторы здоровья: **HTTPS://APPSTORE.EDGENEXUS.IO/PRODUCT-CATEGORY/SERVER-HEALTH-MONITORS/**
- jetPACKS: **HTTPS://APPSTORE.EDGENEXUS.IO/PRODUCT-CATEGORY/JETPACKS/**

- Пакеты функций: HTTPS://APPSTORE.EDGENEXUS.IO/PRODUCT-CATEGORY/EDGENEXUS-FEATURE-PACK/
- Правила flightPATH: HTTPS://APPSTORE.EDGENEXUS.IO/PRODUCT-CATEGORY/FLIGHTPATH/
- Обновления программного обеспечения: HTTPS://APPSTORE.EDGENEXUS.IO/PRODUCT-CATEGORY/EDGENEXUS-SOFTWARE-UPDATE/



Развертывание приложения

После загрузки на ADC приложение будет перемещено в раздел Загруженные приложения и развернуто на ADC с помощью кнопки Развернуть. Этот процесс занимает некоторое время в зависимости от ресурсов, доступных для ADC. После развертывания приложение появится в разделе Загруженные приложения.



Аутентификация

Страница Библиотека > Аутентификация позволяет Вам настроить серверы аутентификации и создать правила аутентификации с опциями для Basic или Forms на стороне клиента и NTLM или BASIC на стороне сервера.

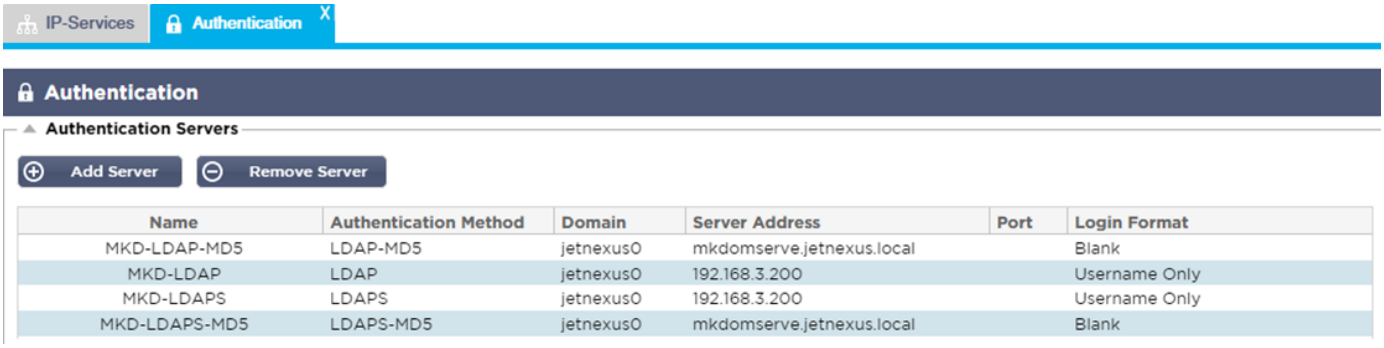
Настройка аутентификации - рабочий процесс

Пожалуйста, выполните следующие минимальные шаги, чтобы применить аутентификацию к Вашей услуге.

1. Создайте сервер аутентификации.
2. Создайте правило аутентификации, которое использует сервер аутентификации.
3. Создайте правило flightPATH, которое использует правило аутентификации.
4. Примените правило flightPATH к Службе

Серверы аутентификации

Чтобы установить рабочий метод аутентификации, мы должны сначала настроить сервер аутентификации.



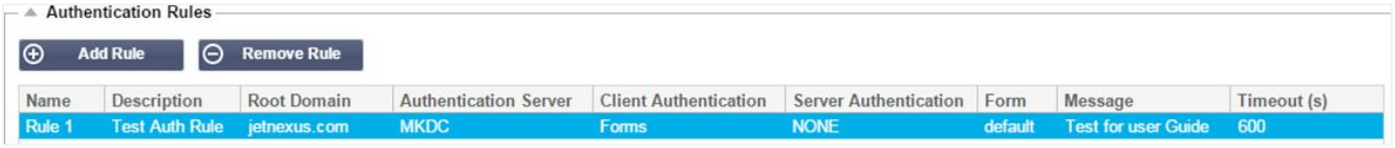
- Нажмите кнопку Добавить сервер.
- Это действие приведет к созданию пустой строки, готовой к заполнению.

Вариант	Описание
Имя	Дайте своему серверу имя в целях идентификации - это имя используется в правилах
Описание	Добавить описание
Метод аутентификации	Выберите метод аутентификации LDAP - базовый LDAP с именами пользователей и паролями, отправляемыми открытым текстом на сервер LDAP. LDAP-MD5 - базовый LDAP с именем пользователя открытым текстом и паролем, хешированным MD5 для повышения безопасности. LDAPS - LDAP через SSL. Отправляет пароль открытым текстом в зашифрованном туннеле между АЦП и LDAP-сервером. LDAPS-MD5 - LDAP через SSL. Пароль хешируется MD5 для дополнительной безопасности в зашифрованном туннеле между АЦП и сервером LDAP.
Домен	Добавьте доменное имя для сервера LDAP.
Адрес сервера	Добавьте IP-адрес или имя хоста сервера аутентификации LDAP - IPv4-адрес или имя хоста. LDAP-MD5 - только имя хоста (IPv4-адрес не работает) LDAPS - IPv4-адрес или имя хоста. LDAPS-MD5 - только имя хоста (IPv4-адрес не работает).
Порт	По умолчанию используйте порт 389 для LDAP и порт 636 для LDAPS. Нет необходимости добавлять номер порта для LDAP и LDAPS. Когда станут доступны другие методы, Вы сможете настроить их здесь

Условия поиска	Условия поиска должны соответствовать RFC 4515. Пример: (MemberOf=CN=Phone- VPN,CN=Users,DC=mycompany,DC=local).
База поиска	Это значение является отправной точкой для поиска в базе данных LDAP. Пример *dc=mycompany,dc=local*
Формат входа в систему	Используйте тот формат входа, который Вам нужен. Имя пользователя - при выборе этого формата Вам необходимо ввести только имя пользователя. Любая информация о пользователе и домене, введенная пользователем, удаляется, и используется информация о домене с сервера. Имя пользователя и домен - Пользователь должен ввести весь синтаксис домена и имени пользователя. Пример: *mycompany\gchristie ИЛИ someone@mycompany*. Информация о домене, введенная на уровне сервера, игнорируется. Пустой - АЦП примет все, что введет пользователь, и отправит это на сервер аутентификации. Эта опция используется при использовании MD5.
Парольная фраза	Эта опция не используется в данной версии.
Мертвое время	Не используется в данной версии

Правила аутентификации

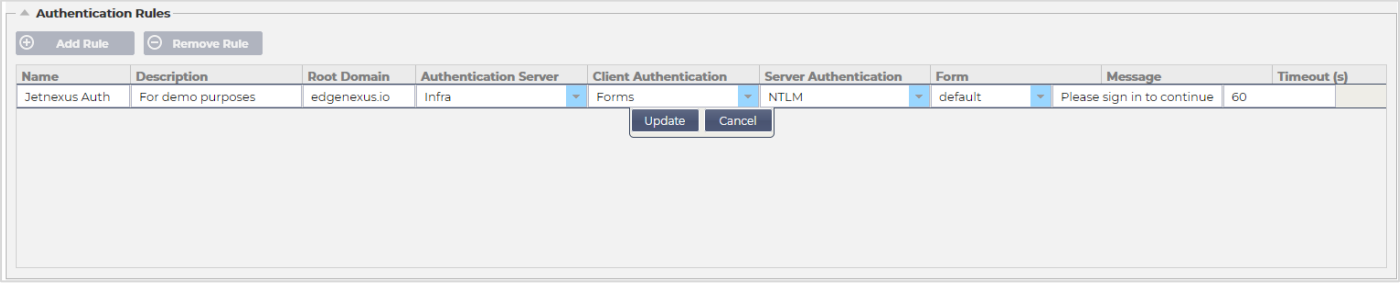
На следующем этапе необходимо создать правила аутентификации для использования с определением сервера.



Поле	**Описание**
Имя	Добавьте подходящее имя для Вашего правила аутентификации.
Описание	Добавьте подходящее описание.
Корневой домен	Этот параметр следует оставить пустым, если Вам не нужен единый вход в систему на поддоменах.
Сервер аутентификации	Это выпадающее окно, содержащее серверы, которые Вы настроили.
Аутентификация клиента:	Выберите значение, соответствующее Вашим потребностям: Базовый (401) - Этот метод использует стандартный метод аутентификации 401 Формы - здесь пользователю будет представлена форма ADC по умолчанию. Внутри формы Вы можете добавить сообщение. Вы можете выбрать форму, которую Вы загрузили, используя раздел ниже.
Аутентификация сервера	Выберите соответствующее значение. Нет - если Ваш сервер не имеет никакой существующей аутентификации, выберите эту настройку. Эта настройка означает, что Вы можете добавить возможности аутентификации на сервер, который ранее не имел таковых. Basic - если на Вашем сервере включена базовая аутентификация (401), выберите BASIC. NTLM - если на Вашем сервере включена аутентификация NTLM, выберите NTLM.
Форма	Выберите соответствующее значение По умолчанию - Выбор этой опции приведет к тому, что АЦП будет использовать свою встроенную форму. Пользовательская - Вы можете добавить форму, которую Вы разработали, и выбрать ее здесь.

Сообщение	Добавьте личное сообщение в форму.
Тайм-аут	Добавьте к правилу тайм-аут, после которого пользователь должен будет повторно пройти аутентификацию. Обратите внимание, что параметр Тайм-аут действителен только для аутентификации на основе форм.

Единая регистрация



Если Вы хотите обеспечить единый вход для пользователей, заполните колонку Корневой домен своим доменом. В данном примере мы использовали edgenexus.io. Теперь мы можем иметь несколько служб, которые будут использовать edgenexus.io в качестве корневого домена, и Вам нужно будет войти в систему только один раз. Если мы рассмотрим следующие сервисы:

- Sharepoint.mycompany.com
- usercentral. mycompany.com
- appstore. mycompany.com

Эти службы могут располагаться на одном VIP или могут быть распределены между 3 VIP. Пользователь, впервые заходящий на usercentral. mycompany.com, получит форму с просьбой войти в систему в зависимости от используемого правила аутентификации. Этот же пользователь может затем подключиться к appstore. mycompany.com и будет автоматически аутентифицирован ADC. Вы можете установить тайм-аут, который заставит пройти аутентификацию по достижении указанного периода бездействия.

Формы

Этот раздел позволит Вам загрузить пользовательскую форму.

Как создать свою пользовательскую форму

Хотя базовая форма, которую предоставляет ADC, достаточна для большинства целей, бывают случаи, когда компании хотят представить пользователю свою собственную личность. Вы можете создать свою собственную форму, которая будет предложена пользователям для заполнения в таких случаях. Эта форма должна быть в формате HTM или HTML.

Вариант	**Описание**
Имя	имя формы = loginform действие = %JNURL% Метод = POST
Имя пользователя	Синтаксис: name = "JNUSER"
Пароль:	name="JNPASS"
Необязательное сообщение1:	%JNMESSAGE%
Необязательное сообщение2:	%JNAUTHMESSAGE%

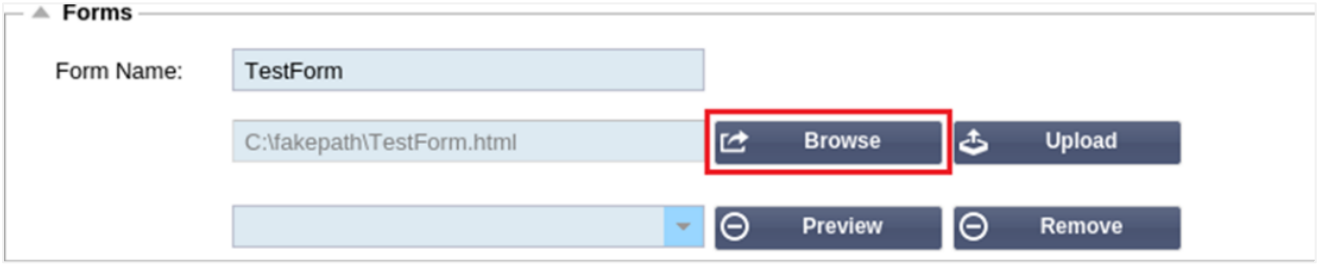
Изображения	Если Вы хотите добавить изображение, то, пожалуйста, добавьте его в строку, используя кодировку Base64.

Пример html-кода очень простой и базовой формы

```
<HTML>
<HEAD>
<TITLE>ОБРАЗЕЦ ФОРМЫ АВТОРИЗАЦИИ</TITLE>
</HEAD>
<BODY>
%JNMESSAGE%<br>
<form name="loginform" action="%JNURL%" method="post"> USER: <input type="text" name="JNUSER" size="20" value=""></br>
PASS: <input type="password" name="JNPASS" size="20" value=""></br>
<input type="submit" name="submit" value="OK">.
</form>
</BODY>
</HTML>
```

Добавление пользовательской формы

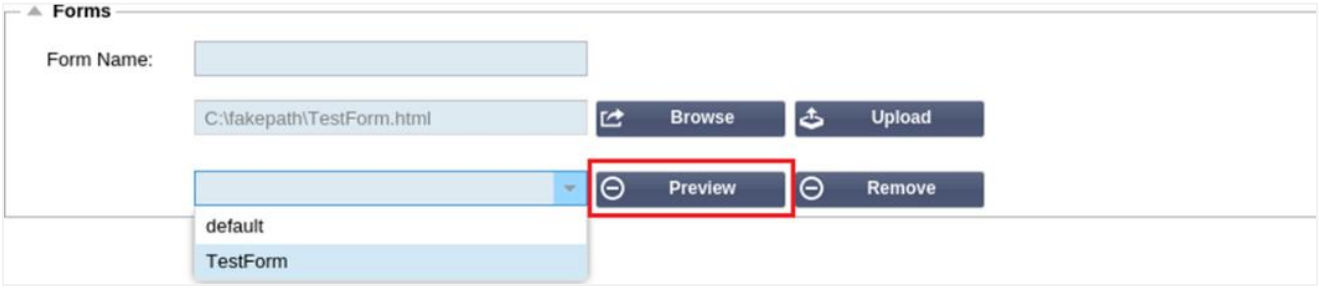
После того, как Вы создали пользовательскую форму, Вы можете добавить ее с помощью раздела Формы.



1. Выберите имя для Вашей формы
2. Найдите местную форму
3. Нажмите кнопку Загрузить

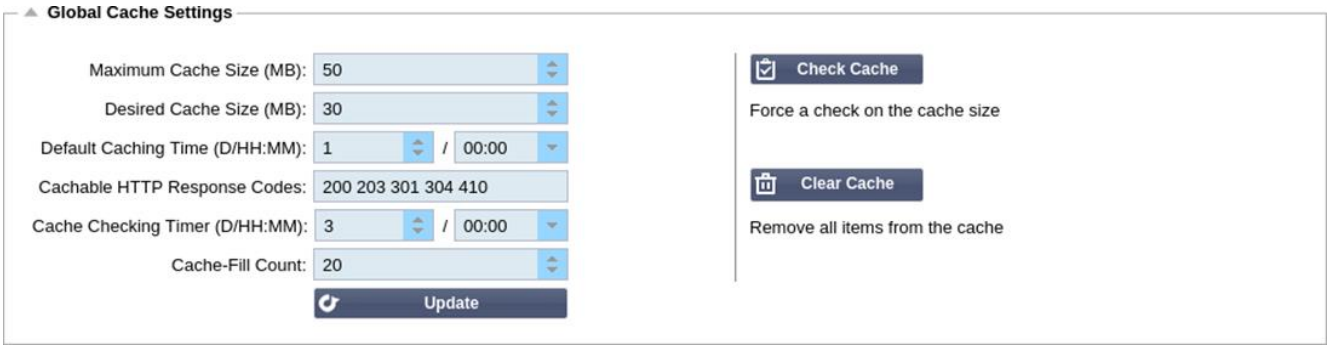
Предварительный просмотр Вашей пользовательской формы

Чтобы просмотреть пользовательскую форму, которую Вы только что загрузили, Вы выбираете ее и нажимаете кнопку Preview. Вы также можете использовать этот раздел для удаления форм, которые больше не нужны.



Кэш

АЦП способен кэшировать данные в своей внутренней памяти и периодически сбрасывать этот кэш во внутреннее хранилище АЦП. Настройки, управляющие этой функциональностью, приведены в этом разделе.



Глобальные настройки кэша

Максимальный размер кэша (МБ)

Это значение определяет максимальный объем оперативной памяти, который может занимать кэш. Кэш ADC - это кэш в памяти, который также периодически сбрасывается на носитель для поддержания постоянства кэша после перезагрузки, перезагрузки и выключения. Эта функциональность означает, что максимальный размер кэша должен соответствовать объему памяти устройства (а не дискового пространства) и составлять не более половины доступной памяти.

Желаемый размер кэша (МБ)

Это значение обозначает оптимальный размер оперативной памяти, до которого будет обрезаться кэш. В то время как максимальный размер кэша представляет собой абсолютную верхнюю границу кэша, желаемый размер кэша предназначен как оптимальный размер, который кэш должен пытаться достичь всякий раз, когда производится автоматическая или ручная проверка размера кэша. Промежуток между максимальным и желаемым размером кэша существует для того, чтобы учесть поступление и перекрытие нового содержимого между периодическими проверками размера кэша для удаления просроченного содержимого. И снова, возможно, будет более эффективным принять значение по умолчанию (30 МБ) и периодически проверять размер кэша в разделе "Монитор -> Статистика" для определения подходящего размера.

Время кэширования по умолчанию (Д/ЧЧ:ММ)

Введенное здесь значение представляет собой срок жизни контента без явного срока годности. Время кэширования по умолчанию - это период, в течение которого хранится контент без директивы "no-store" или явного времени истечения срока действия в заголовке трафика.

Запись в поле принимает форму "D/HH:MM" - таким образом, запись "1/01:01" (по умолчанию 1/00:00) означает, что АЦП будет хранить содержимое в течение одного дня, "01:00" - одного часа, и "00:01" - одной минуты.

Кэшируемые коды ответов HTTP

Одним из наборов кэшированных данных являются HTTP-ответы. Коды ответов HTTP, которые кэшируются, следующие:

- 200 - Стандартный ответ для успешных HTTP-запросов
- 203 - Заголовки не являются окончательными, а собраны из местной или сторонней копии
- 301 - Запрашиваемому ресурсу был присвоен новый постоянный URL-адрес

- 304 - Не изменен с момента последнего запроса и вместо него следует использовать локально кэшированную копию
- 410 - Ресурс больше не доступен на сервере, и адрес пересылки неизвестен

Это поле следует редактировать с осторожностью, поскольку наиболее распространенные кэшируемые коды ответа уже перечислены.

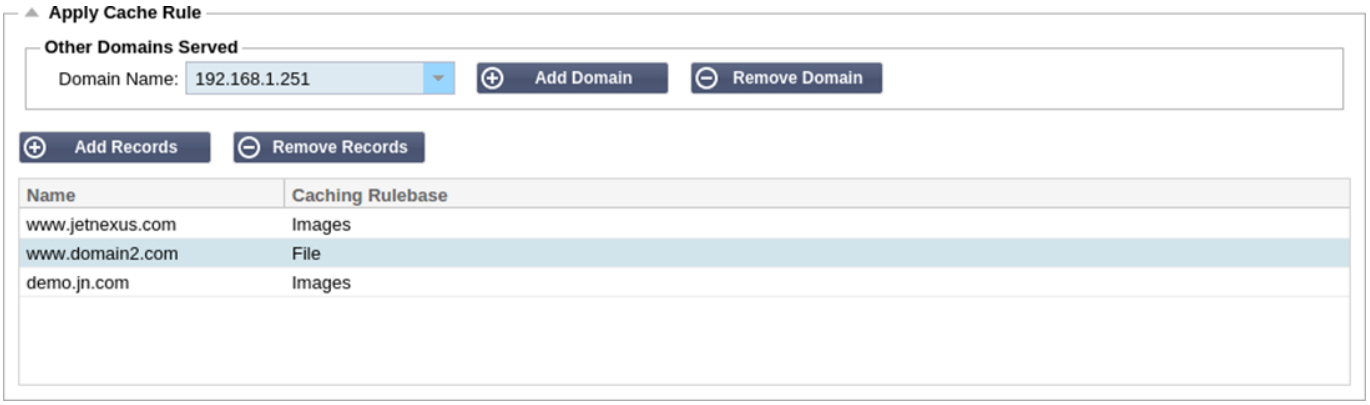
Время проверки кэша (Д/ЧЧ:ММ)

Эта настройка определяет временной интервал между операциями обрезки кэша.

Подсчет заполнения кэш-памяти

Этот параметр является вспомогательным средством, помогающим заполнить кэш при обнаружении определенного количества 304.

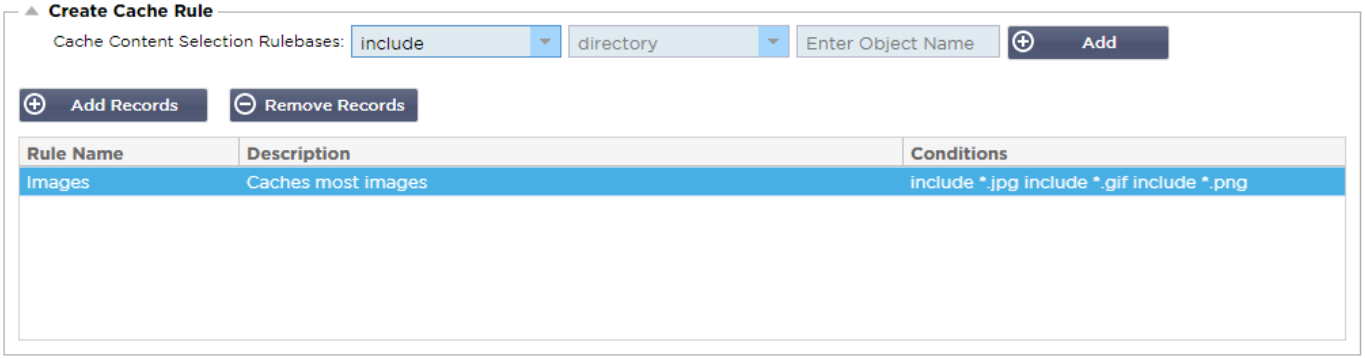
Применить правило кэширования



Этот раздел позволяет Вам применить правило кэширования к домену:

- Добавьте домен вручную с помощью кнопки Добавить записи. Вы должны использовать полное доменное имя или IP-адрес в точечно-десятичной системе счисления. Пример www.mycompany.com или 192.168.3.1:80
- Щелкните на выпадающей стрелке и выберите свой домен из списка
- Список будет заполнен до тех пор, пока трафик проходит через виртуальную службу и к виртуальной службе была применена стратегия кэширования
- Выберите свое правило кэширования, дважды щелкнув на колонке Caching Rulebase и выбрав из списка

Создайте правило кэширования



Этот раздел позволяет Вам создать несколько различных правил кэширования, которые затем могут быть применены к домену:

- Нажмите Добавить записи и дайте своему правилу имя и описание
- Вы можете ввести свои условия вручную или использовать функцию Добавить условие

Чтобы добавить условие с помощью базы правил выбора:

- Выберите Включить или Исключить
- Выберите все изображения JPEG
- Нажмите на символ + Добавить
- Вы увидите, что 'include *.jpg' теперь добавлено к условиям
- Вы можете добавить больше условий. Если Вы решили сделать это вручную, Вам необходимо добавить каждое условие на НОВУЮ строку. Обратите внимание, что Ваши правила будут отображаться на одной строке, пока Вы не щелкните в поле Условия, тогда они будут отображаться на отдельной строке

flightPATH

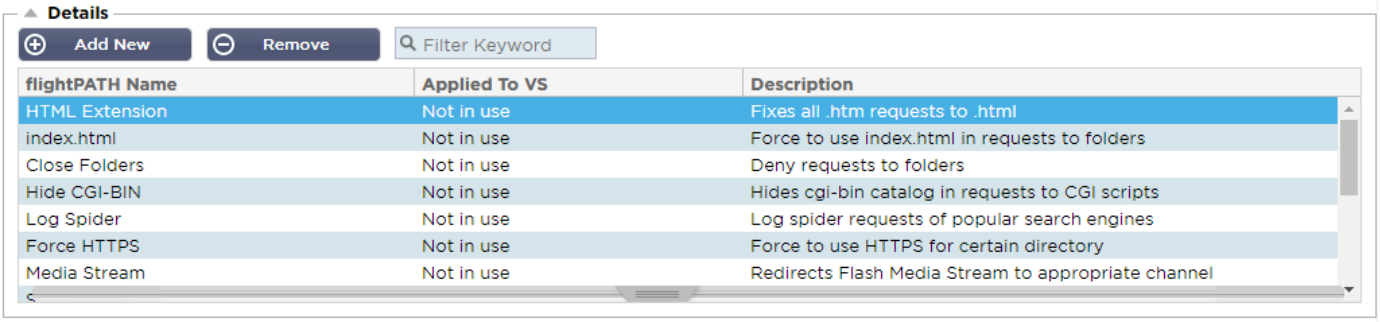
flightPATH - это технология управления трафиком, встроенная в ADC. flightPATH позволяет Вам проверять HTTP и HTTPS трафик в режиме реального времени и выполнять действия в зависимости от условий.

Правила flightPATH должны применяться к VIP, если в правилах используются объекты IP.

Правило траектории полета состоит из четырех элементов:

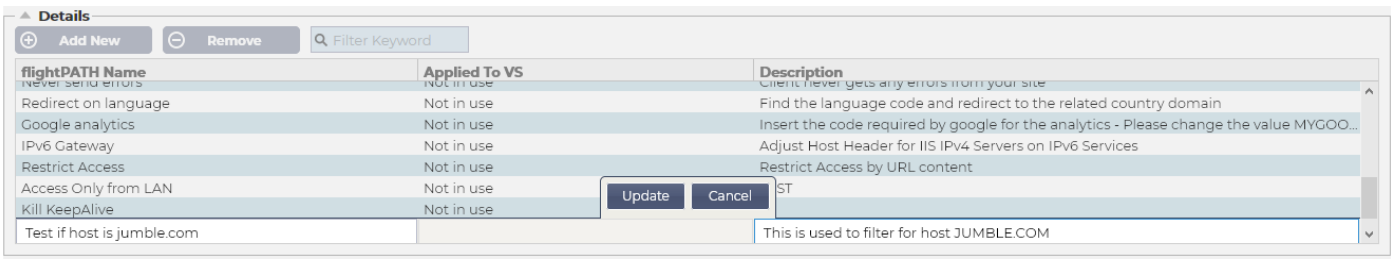
1. Details, где Вы определяете Имя flightPATH и Сервис, к которому он прикреплен.
2. Условие(я), которые могут быть определены, чтобы вызвать срабатывание правила.
3. Оценка, позволяющая определить переменные, которые могут быть использованы в рамках Действий
4. Действия, которые используются для управления тем, что должно произойти при выполнении условий

Подробности



В разделе "Подробности" показаны доступные правила flightPATH. В этом разделе Вы можете добавлять новые правила flightPATH и удалять определенные.

Добавление нового правила flightPATH



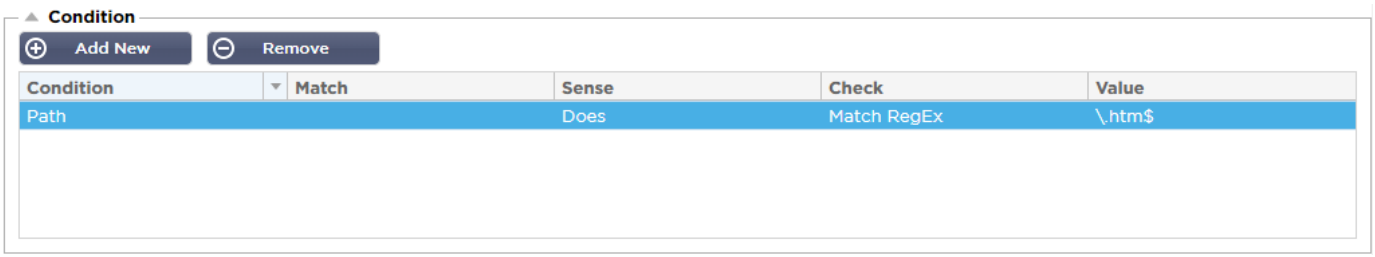
Поле	Описание
Имя FlightPATH	Это поле предназначено для имени правила flightPATH. Имя, которое Вы здесь указываете, появляется в других частях ADC и на него ссылаются.
Применяется к VS	Этот столбец доступен только для чтения и показывает VIP, к которому применяется правило flightPATH.
Описание	Значение, представляющее описание, предоставленное для удобства чтения.

Шаги для добавления правила flightPATH

1. Сначала нажмите кнопку Добавить новую, расположенную в разделе Подробности.
2. Введите имя для Вашего правила. Пример Auth2
3. Введите описание Вашего правила
4. Как только правило будет применено к службе, Вы увидите, что в колонке Applied To автоматически заполняются IP-адрес и значение порта
5. Не забудьте нажать кнопку Обновить, чтобы сохранить изменения, или, если Вы ошиблись, просто нажмите кнопку Отменить, чтобы вернуться к предыдущему состоянию.

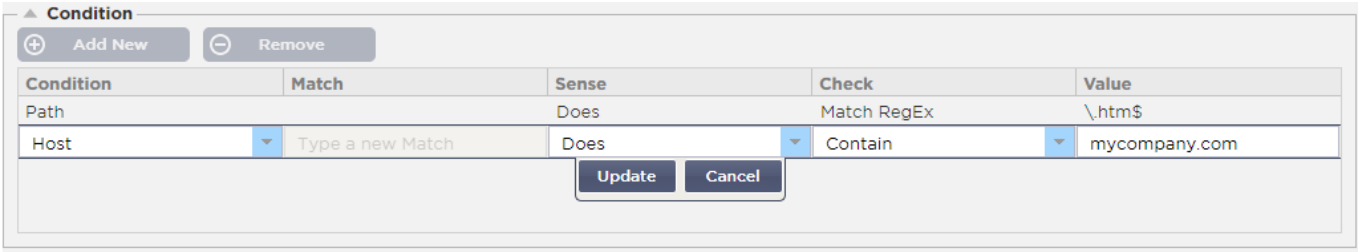
Состояние

Правило flightPATH может содержать любое количество условий. Условия, работающие по принципу И, позволяют Вам установить условие, при котором срабатывает действие. Если Вы хотите использовать условие OR, создайте дополнительное правило flightPATH и примените его к VIP в правильном порядке.



Вы также можете использовать RegEx, выбрав Match RegEx в поле Check и значение RegEx в поле Value. Включение оценки RegEx значительно расширяет возможности flightPATH.

Создание нового условия flightPATH



Состояние

Мы предоставляем несколько Условий, предварительно заданных в выпадающем списке, которые охватывают все предусмотренные сценарии. Когда будут добавлены новые условия, они будут доступны через обновления Jetpack.

Доступны следующие варианты:

КОНДИЦИЯ	ОПИСАНИЕ	ПРИМЕР
<form>	HTML-формы используются для передачи данных на сервер	Пример "форма не имеет длины 0".

Местонахождение ГЕО	Сравнивает IP-адрес источника с кодами стран ISO 3166	ГЕО местоположение равно GB, ИЛИ ГЕО местоположение равно Германия
Хозяин	Хост, извлеченный из URL	www.mywebsite.com или 192.168.1.1
Язык	Язык, извлеченный из языкового HTTP-заголовка	Это условие приведет к появлению выпадающего списка с перечнем языков
Метод	Выпадающий список методов HTTP	Выпадающий список, включающий GET, POST и т.д.
Происхождение IP	Если восходящий прокси поддерживает X-Forwarded-for (XFF), он будет использовать истинный адрес происхождения	IP-адрес клиента. Он также может использовать несколько IP или подсетей. 10\.1\.2\.* - это 10.1.2.0 /24 подсеть10\ .1\.2\.3|10\.1\.2\.4 Используйте | для нескольких IP-адресов
Путь	Путь к сайту	/mywebsite/index.asp
ПОСТ	Метод запроса POST	Проверка данных, загружаемых на веб-сайт
Запрос	Имя и значение запроса, и может принимать либо имя запроса, либо также значение	"Best=jetNEXUS", где соответствие - Best, а значение - edgeNEXUS
Строка запроса	Вся строка запроса после символа ?	
Запрос Cookie	Имя файла cookie, запрошенного клиентом	MS-WSMAN=afYfn1CDqqCDqUD::
Заголовок запроса	Любой заголовок HTTP	Referrer, User-Agent, From, Date
Версия для запроса	Версия HTTP	HTTP/1.0 ИЛИ HTTP/1.1
Орган реагирования	Определяемая пользователем строка в теле ответа	Сервер UP
Код ответа	Код HTTP для ответа	200 OK, 304 Not Modified
Ответное печенье	Имя файла cookie, отправленного сервером	MS-WSMAN=afYfn1CDqqCDqUD::
Заголовок ответа	Любой заголовок HTTP	Referrer, User-Agent, From, Date
Версия ответа	Версия HTTP, отправленная сервером	HTTP/1.0 ИЛИ HTTP/1.1
Источник IP	Либо IP-адрес источника, IP-адрес прокси-сервера, либо какой-то другой агрегированный IP-адрес	ClientIP , Proxy IP, Firewall IP. Можно также использовать несколько IP и подсетей. Вы должны исключить точки, так как они являются RegEX. Пример 10\.1\.2\.3 - 10.1.2.3

Матч

Поле Match может быть выпадающим или текстовым и определяется в зависимости от значения в поле Condition. Например, если Условие установлено на Host, поле Match недоступно. Если Условие

установлено на <form>, поле Match отображается как текстовое поле, а если Условие - POST, поле Match представлено как выпадающий список, содержащий соответствующие значения.

Доступны следующие варианты:

МАТЧ	ОПИСАНИЕ	ПРИМЕР
Принять	Типы содержимого, которые допустимы	Принять: текст/plain
Accept-Encoding	Допустимые кодировки	Accept-Encoding: <compress | gzip | deflate | sdch | identity>.
Accept-Language	Приемлемые языки для ответа	Язык приема: en-US
Accept-Ranges	Какие типы диапазонов частичного содержимого поддерживает этот сервер	Accept-Ranges: bytes
Авторизация	Учетные данные для аутентификации по протоколу HTTP	Авторизация: Basic QWxhZGRpbjpvcGVuIHNlc2FtZQ==
Зарядка -	Содержит информацию о расходах, связанных с применением запрашиваемого метода	
Content-Encoding	Тип используемого кодирования	Content-Encoding: gzip
Content-Length	Длина тела ответа в октетах (8-битных байтах)	Content-Length: 348
Content-Type	Тип mime тела запроса (используется с запросами POST и PUT)	Content-Type: application/x-www-form-urlencoded
Печенье	HTTP cookie, ранее отправленный сервером с помощью Set-Cookie (ниже).	Cookie: $Version=1; Skin=new;
Дата	Дата и время, когда было отправлено сообщение	Дата = "Дата" ":" HTTP-дата
ETag	Идентификатор для конкретной версии ресурса, часто дайджест сообщения	ETag: "aed6bdb8e090cd1:0".
С сайта	Адрес электронной почты пользователя, делающего запрос	От: user@example.com
If-Modified-Since	Позволяет возвращать сообщение 304 Not Modified, если содержимое не изменилось	If-Modified-Since: Sat, 29 Oct 1994 19:43:31 GMT
Last-Modified	Дата последнего изменения для запрашиваемого объекта, в формате RFC 2822	Last-Modified: Tue, 15 Nov 1994 12:45:26 GMT
Pragma	Реализация: Специфические заголовки, которые могут иметь различные эффекты в любой точке цепочки запрос-ответ.	Pragma: no-cache
Реферрер	Адрес предыдущей веб-страницы, с которой была получена ссылка на текущую запрашиваемую страницу	Реферер: HTTP://www.edgenexus.io
Сервер	Имя для сервера	Сервер: Apache/2.4.1 (Unix)

Set-Cookie	HTTP-куки	Set-Cookie: UserID=JohnDoe; Max-Age=3600; Version=1
User-Agent	Строка агента пользователя	User-Agent: Mozilla/5.0 (совместимый; MSIE 9.0; Windows NT 6.1; WOW64; Trident/5.0)
Варьировать	Сообщает нижестоящим прокси-серверам, как сопоставить заголовки будущих запросов, чтобы решить, можно ли использовать кэшированный ответ, а не запрашивать новый с исходного сервера.	Vary: User-Agent
X-Powered-By	Указывает технологию (например, ASP.NET, PHP, JBoss), поддерживающую веб-приложение	X-Powered-By: PHP/5.4.0

Чувства

Поле Sense является выпадающим булевым полем и содержит варианты Does или Doesn't.

Проверьте

Поле Проверка позволяет установить контрольные значения против Условия.

Доступны следующие варианты: Содержать, Конец, Равный, Существующий, Имеет длину, Соответствует RegEx, Соответствует списку, Начало, Превышает длину

ПРОВЕРЬТЕ	ОПИСАНИЕ	ПРИМЕР
Существовать	Здесь не важны детали условия, только то, что оно существует/не существует	Host - Does - Exist
Начало	Строка начинается со значения	Путь - Does - Start - /secure
Конец	Строка заканчивается значением	Путь - Делает - Конец - .jpg
Содержите	Строка содержит Значение	Заголовок запроса - Принимать - Есть - Содержит - изображение
Равный	Строка равна значению	Host - Does - Equal - www.jetnexus.com
Иметь длину	Строка имеет длину, равную значению	Host - Does - Have Length - 16www.jetnexus.com = TRUEwww.jetnexus.co.uk = FALSE
Соответствие RegEx	Позволяет Вам ввести полное регулярное выражение, совместимое с Perl	Origin IP - Does - Match Regex - 10\...* | 11\...*

Шаги для добавления условия

Добавить новое условие flightPATH очень просто. Пример показан выше.

1. Нажмите кнопку Добавить новую в области Условие.
2. Выберите условие из выпадающего списка. В качестве примера возьмем Хост. Вы также можете ввести текст в поле, и ADC покажет значение в выпадающем списке.
3. Выберите чувство. Например, Does
4. Выберите Проверку. Например, Содержать

5. Выберите значение. Например, mycompany.com

Приведенный выше пример показывает, что есть два условия, которые оба должны быть ИСТИНОЙ, чтобы правило было выполнено

- Первое - это проверка того, что запрашиваемый объект является изображением
- Второй проверяет, является ли хост в URL www.imagepool.com.

Оценка

Возможность добавлять определяемые переменные является привлекательной возможностью. Обычные АЦП предлагают такую возможность, используя сценарии или опции командной строки, которые не являются идеальными для всех. АЦП позволяет Вам определить любое количество переменных с помощью простого в использовании графического интерфейса, как показано и описано ниже.

Определение переменной flightPATH состоит из четырех записей, которые необходимо сделать.

- Переменная - это имя переменной
- Источник - выпадающий список возможных точек источника
- Деталь - выберите значения из выпадающего списка или наберите вручную.
- Значение - значение, которое хранит переменная, может быть буквенно-цифровым значением или RegEx для точной настройки.

Встроенные переменные:

Встроенные переменные уже жестко закодированы, поэтому Вам не нужно создавать для них оценочную запись.

Вы можете использовать любую из переменных, перечисленных ниже в разделе "Действие".

Объяснение каждой переменной находится в таблице "Условия" выше.

- Метод = $method$
- Path = $path$
- Querystring = $querystring$
- Sourceip = $sourceip$
- Код ответа (текст также включает "200 OK") = $resp$
- Host = $host$
- Версия = $version$
- Клиентский порт = $clientport$
- Clientip = $clientip$
- Геолокация = $geolocation$"

ДЕЙСТВИЕ	ЦЕЛЬ
Действие = Перенаправление 302	Цель = HTTPs://$host$/404.html

Действие = Журнал	Target = Клиент из $sourceip$:$sourceport$ только что сделал запрос $path$ page

Объяснение:

- Клиент, обращающийся к несуществующей странице, обычно получает в браузере страницу "Ошибка 404".
- Вместо этого пользователь перенаправляется на исходное имя хоста, которое он использовал, но неверный путь заменяется на 404.html
- В Syslog добавляется запись: "Клиент с 154.3.22.14:3454 только что запросил страницу wrong.html".

Действие

Следующим этапом процесса является добавление действия, связанного с правилом и условием flightPATH.

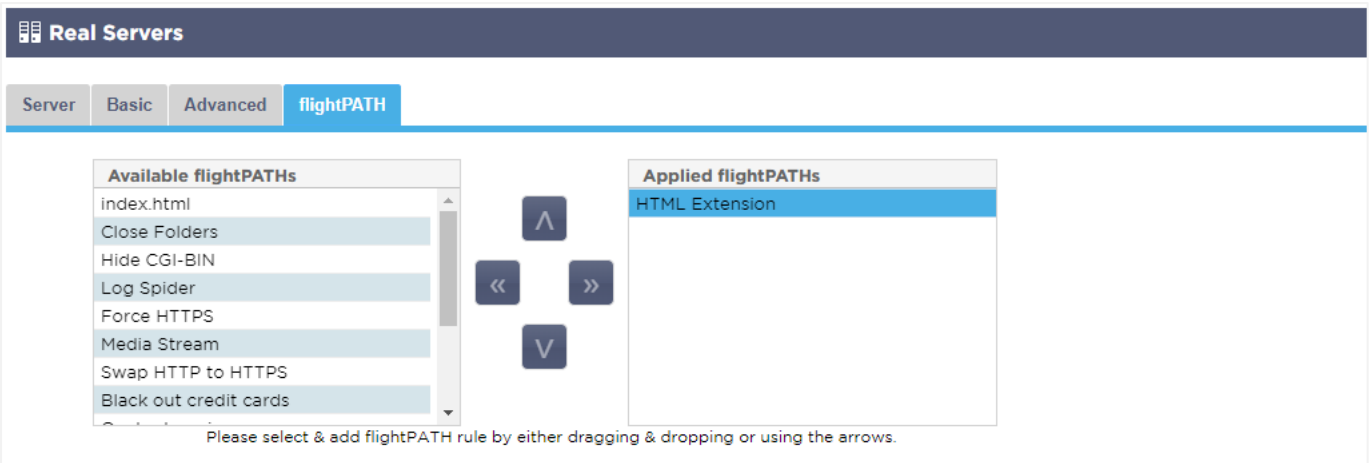
В этом примере мы хотим переписать часть пути URL, чтобы отразить URL, набранный пользователем.

- Нажмите кнопку Добавить новый
- Выберите Переписать путь из выпадающего меню Действие
- В поле Цель введите $path$/myimages
- Нажмите Обновить

Это действие добавит /myimages к пути, так что окончательный URL станет www.imagepool.com/myimages.

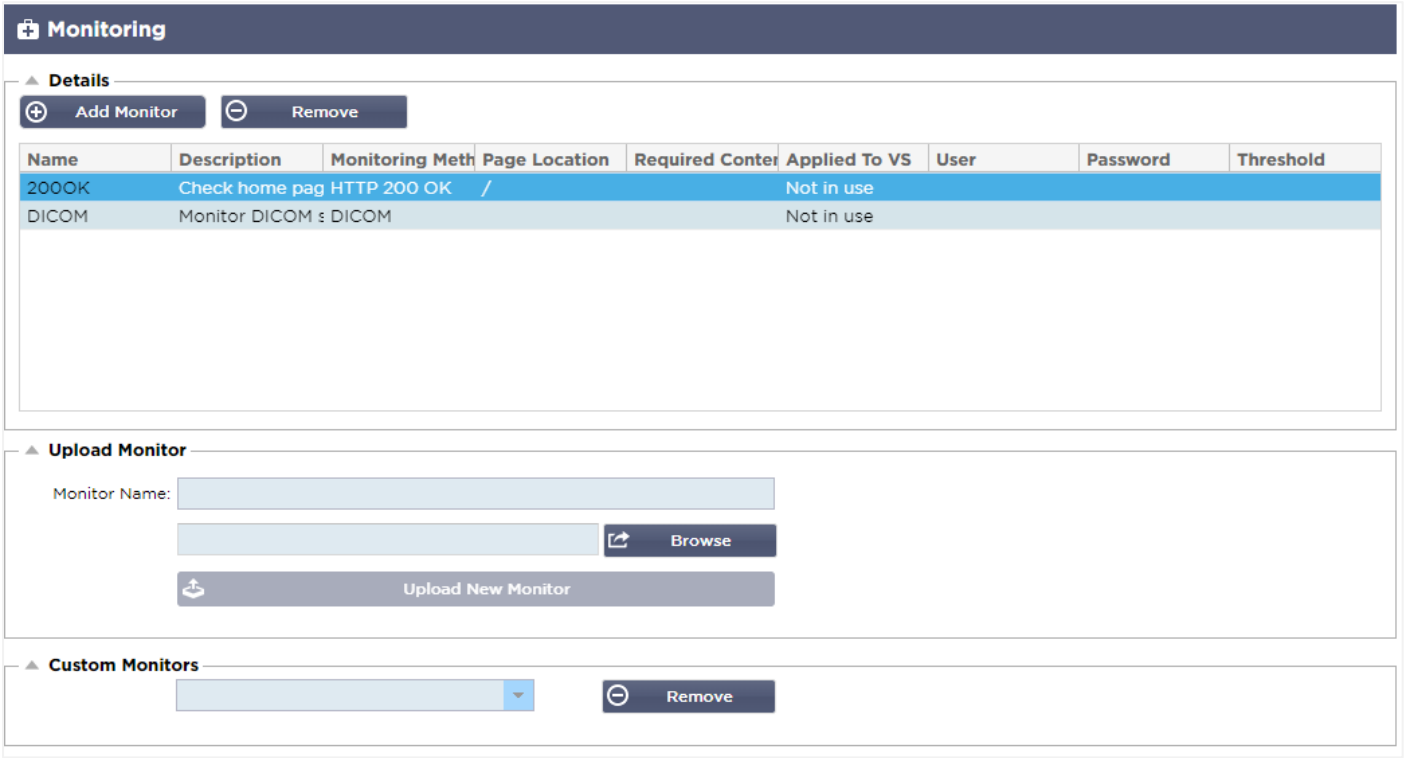
Применение правила flightPATH

Применение любого правила flightPATH осуществляется на вкладке flightPATH каждого VIP/VS.



- Перейдите в раздел Services > IP Services и выберите VIP, которому Вы хотите назначить правило flightPATH.
- Вы увидите список реальных серверов, показанный ниже
- Перейдите на вкладку flightPATH
- Выберите правило flightPATH, которое Вы настроили, или одно из предварительно созданных правил. При необходимости Вы можете выбрать несколько правил flightPATH.
- Перетащите выбранный набор в раздел Applied flightPATHs или нажмите кнопку со стрелкой >>.
- Правило будет перемещено в правую часть и автоматически применено.

Мониторы реальных серверов



Когда балансировка нагрузки настроена, полезно следить за состоянием реальных серверов и приложений, работающих на них. Например, в веб-серверах Вы можете настроить определенную страницу, с помощью которой Вы сможете следить за состоянием, или использовать одну из других систем мониторинга, которыми располагает ADC.

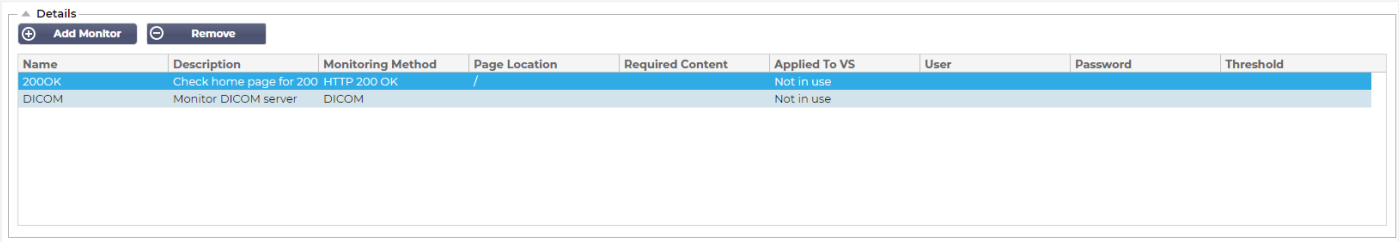
Страница Library > Real Server Monitors позволяет Вам добавлять, просматривать и редактировать пользовательский мониторинг. Это "Проверки здоровья" сервера 7-го уровня, которые выбираются из поля Мониторинг сервера на вкладке Основные для определенной Вами виртуальной службы.

Страница Мониторы реального сервера разделена на три раздела.

- Подробности
- Загрузить
- Индивидуальные мониторы

Подробности

Раздел Подробности используется для добавления новых мониторов и удаления тех, которые Вам не нужны. Вы также можете редактировать существующий монитор, дважды щелкнув на нем.



Имя

Название по Вашему выбору для Вашего монитора.

Описание

Текстовое описание для этого Монитора, и мы рекомендуем сделать его как можно более описательным.

Метод мониторинга

Выберите метод мониторинга из выпадающего списка. Доступны следующие варианты:

Метод мониторинга	**Описание**	**Пример**
HTTP 200 OK	Создается TCP-соединение с реальным сервером. После установления соединения на реальный сервер отправляется короткий HTTP-запрос. Ожидается HTTP-ответ от сервера, который затем проверяется на наличие кода ответа "200 OK". Если получен код ответа "200 OK", считается, что Реальный сервер работает. Если по какой-либо причине код ответа "200 OK" не получен, включая тайм-ауты или невозможность подключения, то считается, что Реальный сервер не работает и недоступен. Этот метод мониторинга действительно можно использовать только с типами услуг HTTP и Accelerated HTTP. Однако, если для HTTP-сервера используется тип сервиса 4-го уровня, он все равно может быть использован, если SSL не используется на реальном сервере или обрабатывается соответствующим образом средством "Content SSL".	Название: 200OK Описание: Проверка производственного веб-сайта Метод мониторинга: HTTP 200 OK Расположение страницы: /main/index.html ИЛИ HTTP://www.edgenexus.io/main/index.html Требуемое содержание: Н/Д
HTTP-ответ	Соединение и HTTP запрос/ответ выполняется с реальным сервером и проверяется, как описано в предыдущем примере. Но вместо того, чтобы проверять код ответа "200 OK", заголовок HTTP-ответа проверяется на наличие пользовательского текстового содержимого. Текст может быть	Название: Сервер поднят Описание: Проверьте содержимое страницы на наличие "Server Up. " Метод мониторинга: HTTP-ответ Расположение страницы: /main/index.html ИЛИ HTTP://www.edgenexus.io/main/index.html Требуемое содержание: Загрузка сервера

	полным заголовком, частью заголовка, строкой из части страницы или просто одним словом. Если текст найден, считается, что Real Server работает. Этот метод мониторинга действительно можно использовать только с типами служб HTTP и Accelerated HTTP. Однако, если для HTTP-сервера используется тип сервиса 4-го уровня, его все равно можно использовать, если SSL не используется на реальном сервере или обрабатывается соответствующим образом средством "Content SSL".	
DICOM	Мы отправляем DICOM-эхо, используя значение "Source Calling" AE Title в колонке требуемого содержания. Вы также можете установить значение AE Title "Destination Called" в разделе Notes каждого сервера. Вы можете найти колонку Notes в IP Services-. -Виртуальные службы - Страница сервера.	Название: DICOM Описание: Проверка здоровья L7 для службы DICOM Метод мониторинга: DICOM Расположение страницы: N/A Необходимое содержание: Значение AET
TCP вне диапазона	Метод TCP Out of Band похож на TCP Connect, за исключением того, что Вы можете указать порт, который Вы хотите контролировать, в колонке требуемого содержимого. Этот порт обычно не совпадает с портом трафика и используется, когда Вы хотите связать службы вместе	Название: TCP вне диапазона Описание: Мониторинг порта вне диапазона/трафика Расположение страницы: N/A Необходимое содержание: 555
Многопортовый монитор TCP	Этот метод похож на описанный выше, за исключением того, что у Вас может быть несколько разных портов. Монитор считается успешным, только если все порты, указанные в разделе требуемого содержимого, отвечают правильно.	Название: Многопортовый монитор Описание: Контролируйте несколько портов для успешной работы Расположение страницы: N/A Необходимое содержание: 135,59534,59535

Расположение страницы

URL Расположение страницы для HTTP-монитора. Это значение может быть относительной ссылкой, такой как /folder1/folder2/page1.html. Вы также можете использовать абсолютную ссылку, где веб-сайт привязан к имени хоста.

Необходимое содержание

Это значение содержит любое содержимое, которое монитор должен обнаружить и использовать. Представленное здесь значение будет меняться в зависимости от выбранного метода мониторинга.

Применяется к VS

Это поле автоматически заполняется IP/портом виртуальной службы, к которой применяется монитор. Вы не сможете удалить монитор, который был использован с виртуальной службой.

Пользователь

Некоторые пользовательские мониторы могут использовать это значение вместе с полем пароля для входа на Real Server.

Пароль

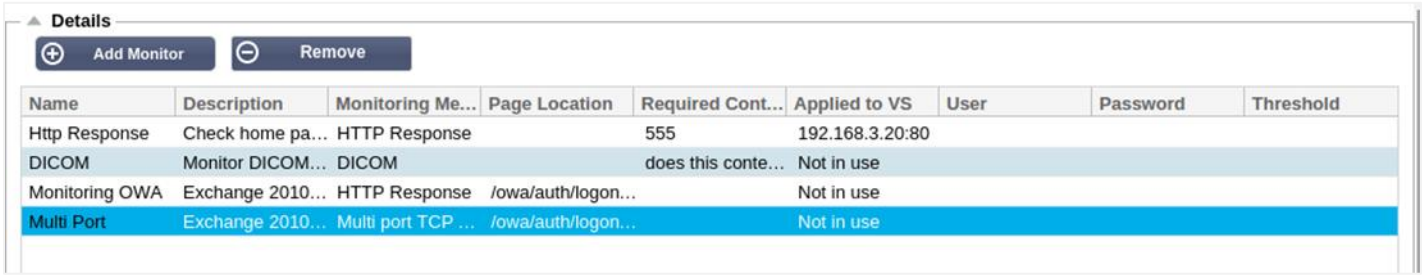
Некоторые пользовательские мониторы могут использовать это значение вместе с полем User для входа в Real Server.

Порог

Поле Threshold - это общее целое число, используемое в пользовательских мониторах, где требуется порог, например, уровень ЦП.

ПРИМЕЧАНИЕ: Пожалуйста, убедитесь, что ответ сервера приложений не является "Chunked" ответом.

Примеры Монитора реального сервера



Монитор загрузки

Во многих случаях пользователи захотят создать свои собственные мониторы, и этот раздел позволяет загрузить их в АЦП.

Пользовательские мониторы пишутся с помощью сценариев PERL и имеют расширение файла .pl.

- Дайте своему монитору имя, чтобы Вы могли идентифицировать его в списке Метод мониторинга
- Найдите файл .pl
- Нажмите Загрузить новый монитор
- Ваш файл будет загружен в нужное место и будет виден как новый Метод мониторинга.

Индивидуальные мониторы

В этом разделе Вы можете просмотреть загруженные пользовательские мониторы и удалить их, если они больше не нужны.

- Нажмите на выпадающее поле
- Выберите имя пользовательского монитора
- Нажмите кнопку Удалить
- Ваш пользовательский монитор больше не будет виден в списке Метод мониторинга

Создание пользовательского Perl-сценария монитора

ВНИМАНИЕ: Этот раздел предназначен для людей, имеющих опыт использования и написания текстов на языке Perl

В этом разделе показаны команды, которые Вы можете использовать в своем Perl-скрипте.

Команда #Monitor-Name: - это имя, используемое для Perl-скрипта, хранящегося на АЦП. Если Вы не включите эту строку, то Ваш сценарий не будет найден!

Следующие пункты являются обязательными:

- #Monitor-Name
- используйте строго;
- предупреждение об использовании;

Скрипты Perl выполняются в среде CHROOTED. Они часто вызывают другое приложение, такое как WGET или CURL. Иногда их нужно обновить для определенных функций, например, SNI.

Динамические ценности

- my $host = $_[0]; - Здесь используется "Адрес" из раздела "IP Services--Real Server".
- my $port = $_[1]; - Здесь используется "Порт" из раздела "IP Services--Real Server".
- my $content = $_[2]; - Здесь используется значение "Требуемое содержание" из раздела Библиотека - Мониторинг реального сервера
- my $notes = $_[3]; - Здесь используется колонка "Notes" в разделе Real Server раздела IP Services
- my $page = $_[4]; - Здесь используются значения "Расположение страницы" из раздела Библиотека - Монитор реального сервера
- my $user = $_[5]; - Здесь используется значение "User" из раздела Библиотека - Монитор реального сервера
- my $password = $_[6]; - Здесь используется значение "Password" из раздела Библиотека - Монитор реального сервера

Пользовательские проверки здоровья имеют два результата

- Успешный
  Возвращаемое значение 1Печатать
  сообщение об успехе в SyslogОтметить
  реальный сервер в режиме онлайн (при условии совпадения IN COUNT)
- Unsuccessful
  Возвращаемое значение 2Печатать
  сообщение о неудаче в SyslogМаркировка
  реального сервера в автономном режиме (при условии совпадения OUT Count)

Пример пользовательского монитора здоровья

```
#Monitor-Name HTTPS_SNI
используйте строго:
предупреждения по использованию;
# Имя монитора, как указано выше, отображается в выпадающем списке Доступные проверки здоровья
# В этот скрипт передано 6 значений (см. ниже)
# Сценарий вернет следующие значения
# 1 - тест прошел успешно
# 2, если тест не удался sub monitor
{
my Shost=       $_[0]; ### IP или имя хоста
my Sport=       $_[1]; ### Порт хоста
my Scontent=    $_[2]; ### Содержание, которое нужно искать (в веб-странице и HTTP-заголовках)
my Snotes=      $_[3]; ### Имя виртуального хоста
my Spage=       $_[4]; ### Часть URL после адреса хоста
my Suser=       $_[5]: ### домен/имя пользователя (необязательно)
my Spassword=           $_[6]; ### пароль (необязательно)
my $resolve;
my $auth        =;
если ($port)
{
        $resolve = "$notes:$port:$host":
}
else {
        $resolve = "$notes:$host";
}
if ($user && $password) {
        $auth = "-u $user:$password :
}
my @lines = 'curl -s -i -retry 1 -max-time 1 -k -H "Host:$notes --resolve $resolve $auth HTTPs://${notes}${page} 2>&1';
if(join(""@lines)=~/$content/)
        {
        print "HTTPs://$notes}${page} ищет - $content - Health check successful.\n";
        return(1);
        }
else
        {
        print "HTTPs://${notes}${page} ищет - $content - Health check failed.\n";
        возврат(2)
        }
}
monitor(@ARGV):
```

ПРИМЕЧАНИЕ: Пользовательский мониторинг - Использование глобальных переменных невозможно. Используйте только локальные переменные - переменные, определенные внутри функций

SSL-сертификаты

Чтобы успешно использовать балансировку нагрузки уровня 7 с серверами, использующими зашифрованные соединения с помощью SSL, ADC должен быть оснащен сертификатами SSL, используемыми на целевых серверах. Это требование необходимо для того, чтобы поток данных можно было расшифровать, изучить, управлять, а затем повторно зашифровать перед отправкой на целевой сервер.

SSL сертификаты могут варьироваться от самоподписанных сертификатов, которые может генерировать ADC, до традиционных сертификатов (с подстановочным знаком), доступных от надежных поставщиков. Вы также можете использовать сертификаты с доменной подписью, которые генерируются из Active Directory.

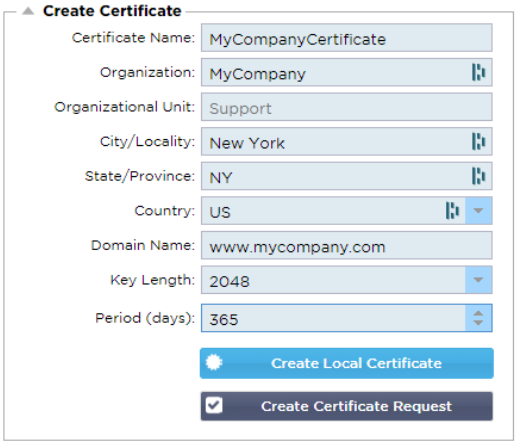
Что делает АЦП с SSL-сертификатом?

ADC может выполнять правила управления трафиком (flightPATH) в зависимости от того, что содержат данные. Это управление не может быть выполнено для зашифрованных данных SSL. Когда ADC должен проверить данные, ему необходимо сначала расшифровать их, а для этого ему нужен SSL-сертификат, используемый сервером. После расшифровки ADC сможет изучить и выполнить правила flightPATH. После этого данные будут повторно зашифрованы с помощью SSL-сертификата и отправлены на конечный Real Server.

Создать сертификат

Хотя АЦП может использовать глобально доверенный SSL сертификат, он может генерировать самоподписанный SSL сертификат. Самоподписанный SSL идеально подходит для внутренних требований балансировки нагрузки. Однако Ваши ИТ-политики могут потребовать доверенный сертификат или сертификат ЦС домена.

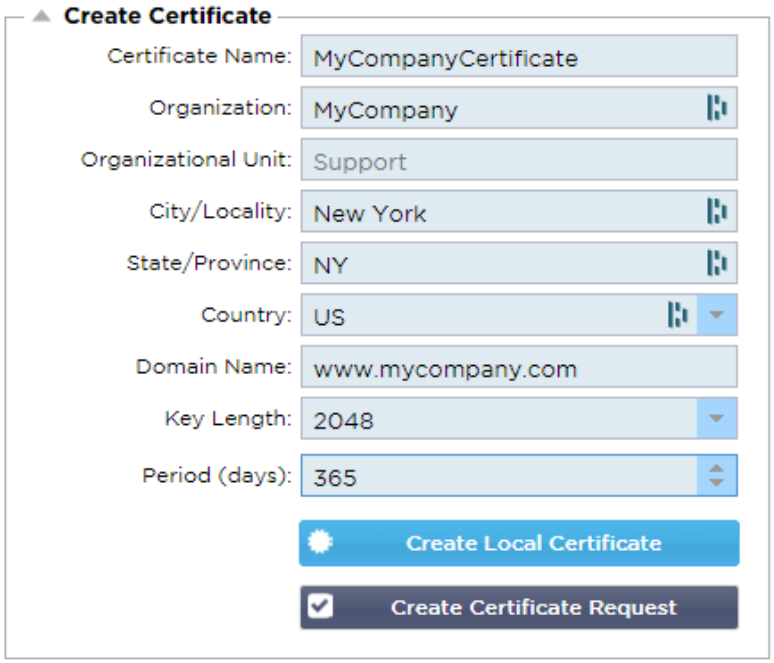
Как создать локальный SSL сертификат



- Заполните все детали, как в примере выше
- Нажмите на кнопку Создать локальный сертификат
- После этого Вы можете применить сертификат к **ВИРТУАЛЬНОЙ СЛУЖБЕ.**

Создайте запрос на сертификат (CSR)

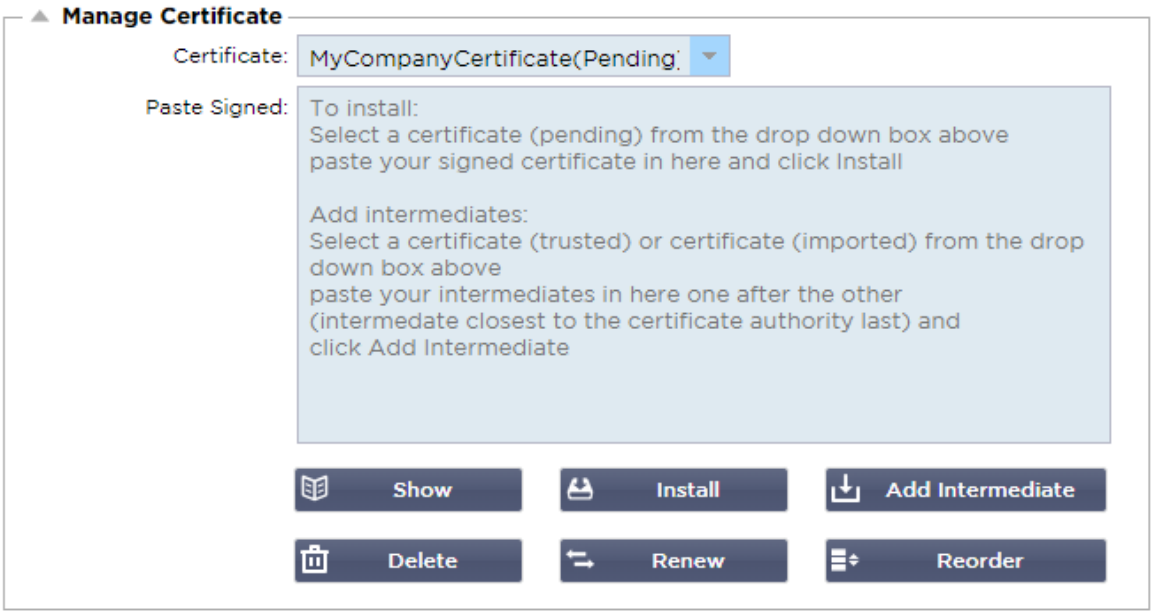
Когда Вам необходимо получить глобально доверенный SSL от внешнего провайдера, Вам необходимо создать CSR для генерации SSL сертификата.



Заполните форму, как показано выше, всеми соответствующими данными, а затем нажмите кнопку Запрос сертификата. Перед Вами появится всплывающее окно, соответствующее предоставленным Вами данным.

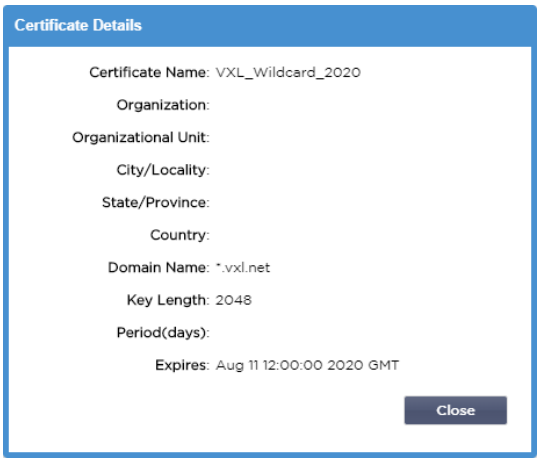
Вам нужно будет вырезать и вставить содержимое в ТЕКСТОВЫЙ файл и назвать его с расширением файла CSR, например, *mycert.csr*. Этот файл CSR затем нужно будет предоставить в Ваш центр сертификации для создания SSL-сертификата.

Управление сертификатом



Этот подраздел содержит различные инструменты, позволяющие управлять SSL-сертификатами, имеющимися в ADC.

Показать

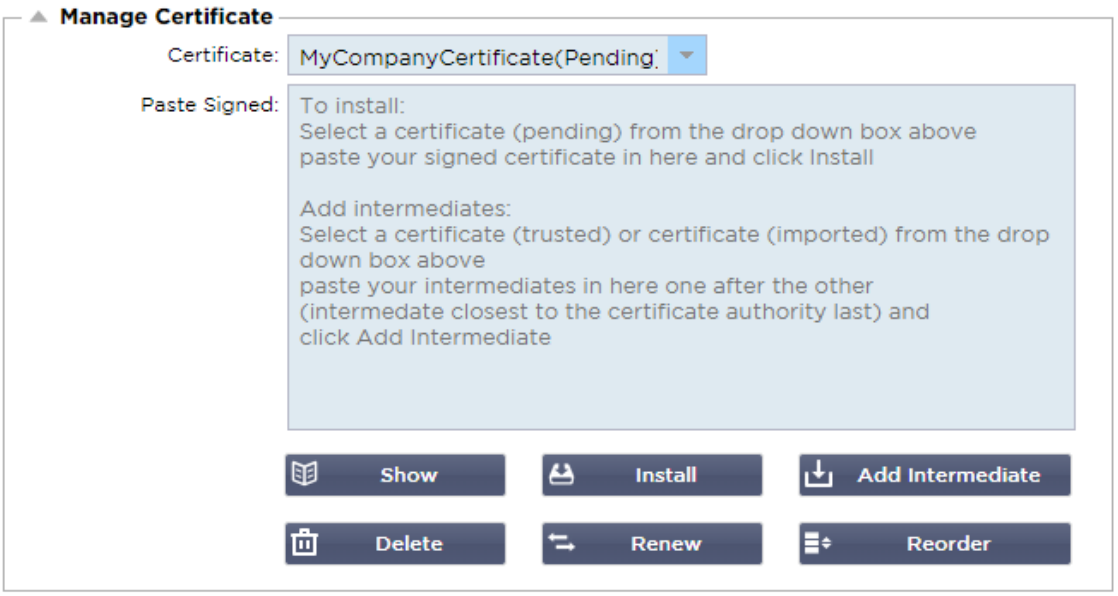


Бывают случаи, когда Вы хотите просмотреть детали установленного SSL-сертификата.

- Выберите сертификат из выпадающего меню
- Нажмите на кнопку Показать
- Во всплывающем окне, показанном ниже, будет представлена информация о сертификате.

Установка сертификата

Как только Вы получите сертификат от доверенного центра сертификации, Вам нужно будет сопоставить его со сгенерированным CSR и установить его в ADC.



- Выберите сертификат, который Вы сгенерировали в описанных выше шагах. В строке будет зафиксирован статус (Pending). В примере, MyCompanyCertificate показан на изображении выше.
- Откройте файл сертификата в текстовом редакторе
- Скопируйте все содержимое файла в буфер обмена
- Вставьте содержимое подписанного SSL-сертификата, который Вы получили от доверенного органа, в поле с надписью Paste Signed.
- Вы также можете вставить Промежуточные ниже этого, соблюдая правильный порядок:
    1. (TOP) Ваш подписанный сертификат
    2. (2-й сверху) Промежуточный 1
    3. (3-я сверху) Промежуточный 2
    4. (Внизу) Промежуточный 3
    5. Корневой центр сертификации Нет необходимости добавлять их, так как они существуют на клиентских машинах.
       (ADC также содержит корневой пучок для повторного шифрования, когда он действует как клиент Real Server)
- Нажмите кнопку Установить
- Как только Вы установили сертификат, Вы должны увидеть статус (Trusted) рядом с Вашим сертификатом

Если Вы допустили ошибку или ввели неправильный промежуточный порядок, то выберите Сертификат (Доверенный) и добавьте сертификаты (включая подписанный сертификат) снова в правильном порядке и нажмите Установить

Добавить промежуточный

В некоторых случаях требуется добавлять промежуточные сертификаты отдельно. Например, Вы могли импортировать сертификат, не имеющий промежуточных сертификатов.

- Выделите сертификат (доверенный) или сертификат (импортированный)
- Вставьте промежуточные элементы один под другим, следя за тем, чтобы промежуточный элемент, расположенный ближе всего к Центру сертификации, был вставлен последним.
- Нажмите Добавить промежуточный.

Если Вы ошиблись в заказе, Вы можете повторить процесс и добавить промежуточные продукты снова. Это действие только перезапишет предыдущие промежуточные продукты.

Удаление сертификата

Вы можете удалить сертификат с помощью кнопки Удалить. После удаления сертификат будет полностью удален из ADC и его необходимо будет заменить, а затем снова применить к виртуальным службам, если это потребуется.

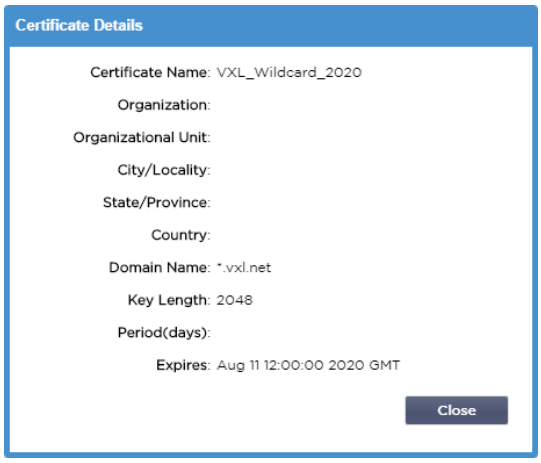
Примечание: Перед удалением сертификата убедитесь, что он не прикреплен к действующему VIP-клиенту.

Продлить сертификат

Кнопка Renew позволяет Вам получить новый запрос на подписание сертификата. Это действие требуется, когда срок действия сертификата истекает и его необходимо обновить.

- Выберите сертификат из выпадающего списка; Вы можете выбрать любой сертификат со статусом (Ожидающий), (Доверенный) или (Импортированный).
- Нажмите кнопку Обновить
- Скопируйте данные нового CSR, чтобы Вы могли получить новый сертификат

- Когда Вы получите новый сертификат, выполните действия, подробно описанные в разделе **Показать**



- **Бывают случаи,** когда Вы хотите просмотреть детали установленного SSL-сертификата.
- Выберите сертификат из выпадающего меню
- Нажмите на кнопку Показать
- Во всплывающем окне, показанном ниже, будет представлена информация о сертификате.

- Установка сертификата.
- Теперь новый и обновленный сертификат будет установлен в ADC.

Импорт сертификата

Во многих случаях корпоративным предприятиям необходимо использовать свои сертификаты, подписанные доменом, как часть внутреннего режима безопасности. Сертификаты должны быть в формате PKCS#12, и такие сертификаты неизменно защищаются паролями.

На рисунке ниже показан подраздел для импорта одного SSL-сертификата.

- Дайте своему сертификату дружественное имя. Это имя идентифицирует его в выпадающих списках, используемых в ADC. Оно не обязательно должно совпадать с именем домена сертификата, но должно быть буквенно-цифровым без пробелов. Не допускается использование специальных символов, кроме _ и -.
- Введите пароль, который Вы использовали для создания сертификата PKCS#12
- Найдите файл {имя сертификата}.pfx
- Нажмите кнопку Импорт.
- Теперь Ваш сертификат будет находиться в соответствующих выпадающих меню SSL в ADC

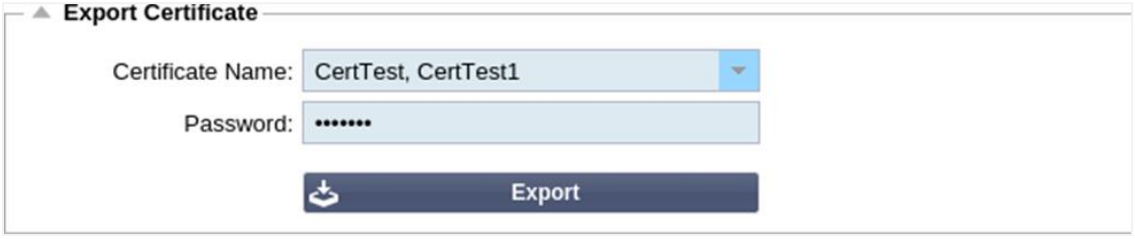
Импорт нескольких сертификатов

Этот раздел позволяет Вам импортировать файл JNBK, содержащий несколько сертификатов. Файл JNBK шифруется и создается ADC при экспорте нескольких сертификатов.

- Найдите свой файл JNBK - Вы можете создать один из них, экспортируя несколько сертификатов
- Введите пароль, который Вы использовали для создания файла JNBK
- Нажмите кнопку Импорт.
- Теперь Ваши сертификаты будут находиться в соответствующих выпадающих меню SSL в ADC

Экспорт сертификата

Время от времени Вы можете захотеть экспортировать один из сертификатов, хранящихся в АЦП. В АЦП предусмотрена возможность сделать это.



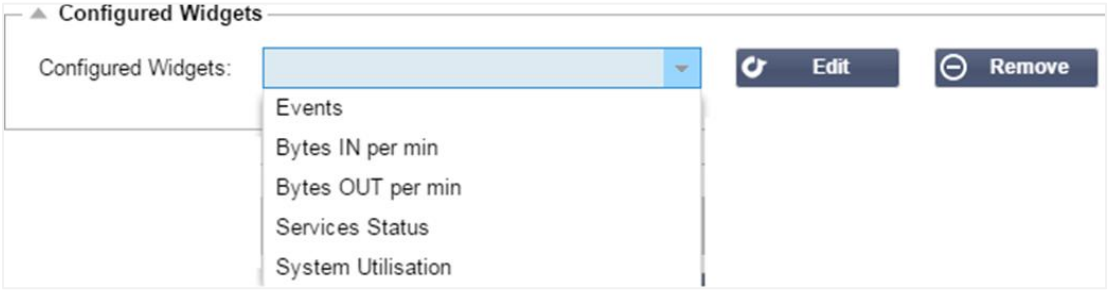
- Щелкните сертификат или сертификаты, которые Вы хотите установить. Вы можете выбрать опцию Все, чтобы выбрать все перечисленные сертификаты.
- Введите пароль для защиты экспортируемого файла. Пароль должен состоять не менее чем из шести символов. Можно использовать буквы, цифры и некоторые символы. Следующие символы недопустимы: < > " ' ( ) ; \ | \A3 % &
- Нажмите кнопку Экспорт
- Если Вы экспортируете один сертификат, результирующий файл будет иметь имя sslcert_{certname}.pfx. Например, sslcert_Test1Cert.pfx
- В случае экспорта нескольких сертификатов, результирующий файл будет файлом JNBK. Имя файла будет sslcert__pack.jnbk.

Примечание: Файл JNBK - это зашифрованный файл контейнера, созданный АЦП и действительный только для импорта в АЦП

Виджеты

Страница Библиотека > Виджеты позволяет Вам настраивать различные легкие визуальные компоненты, отображаемые на Вашей пользовательской приборной панели.

Настроенные виджеты

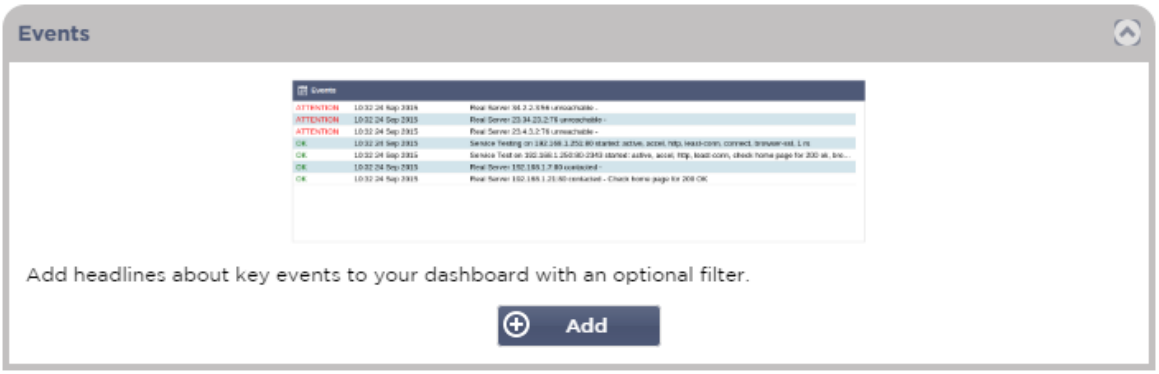


Раздел Настроенные виджеты позволяет Вам просматривать, редактировать или удалять любые виджеты, созданные из раздела доступных виджетов.

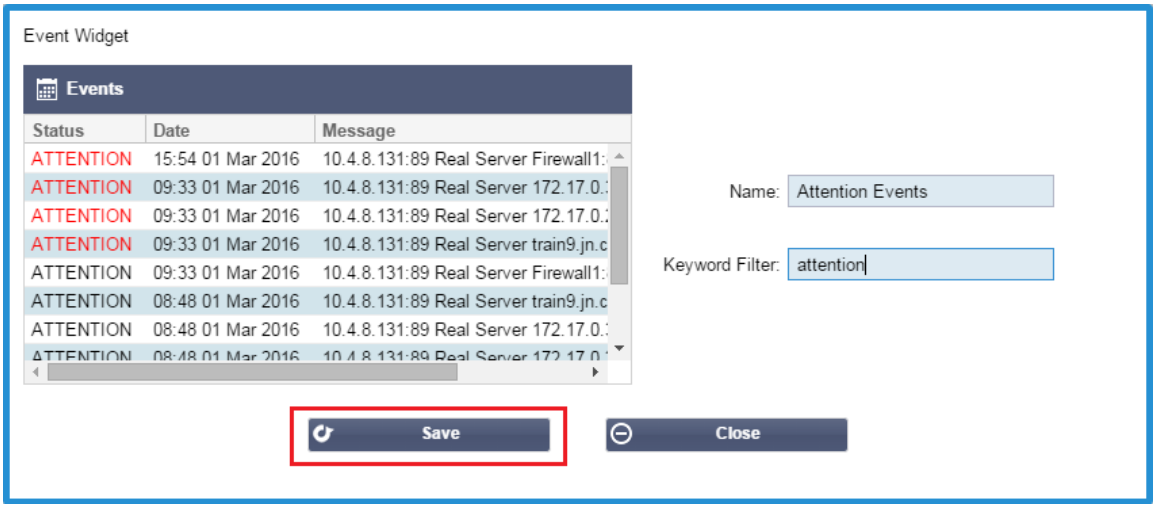
Доступные виджеты

В АЦП предусмотрено пять различных виджетов, и Вы можете настроить их в соответствии со своими требованиями.

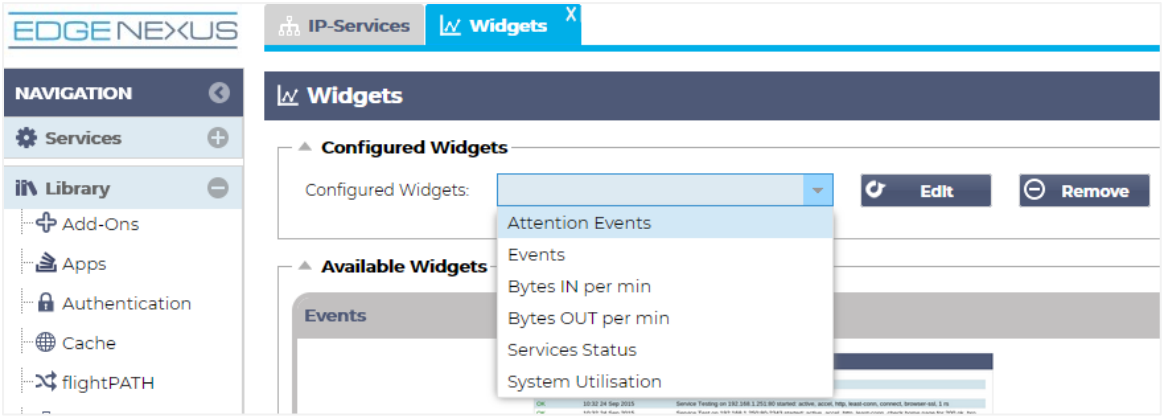
Виджет событий



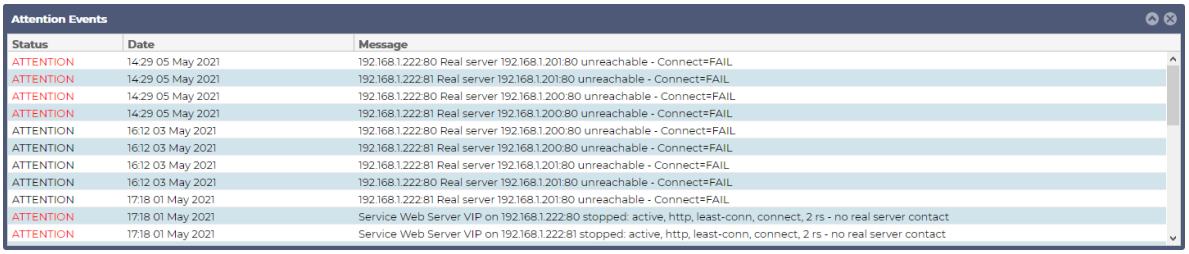
- Чтобы добавить событие в виджет "События", нажмите кнопку Добавить.
- Укажите название для Вашего события. В нашем примере мы добавили Attention Events в качестве названия события.
- Добавьте фильтр ключевых слов. Мы также добавили значение фильтра Внимание



- Нажмите Сохранить, затем Закрыть
- Теперь Вы увидите дополнительный виджет под названием Attention Events в выпадающем списке Настроенные виджеты.

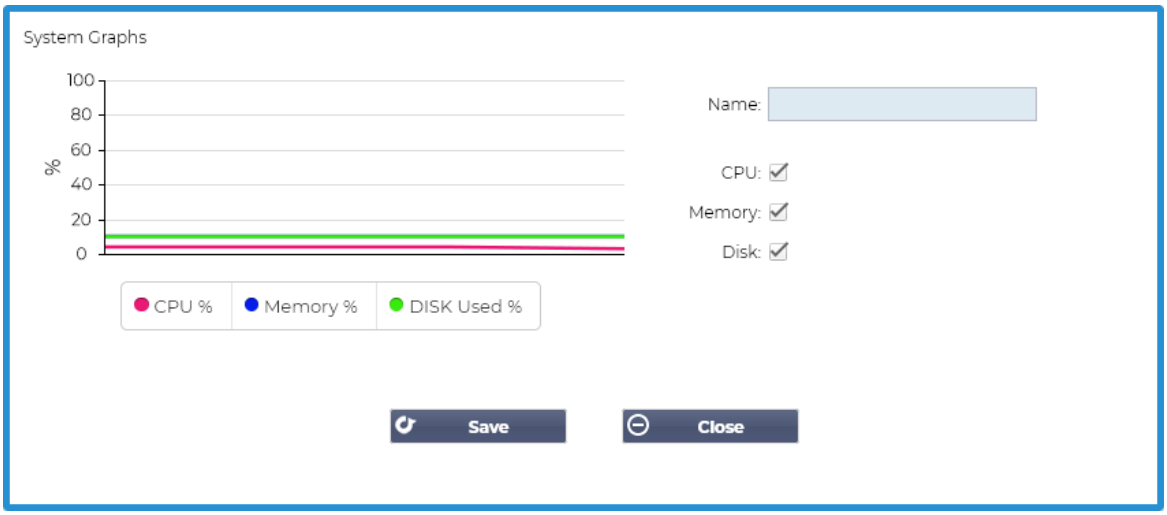


- Вы можете видеть, что теперь мы добавили этот виджет в раздел View > Dashboard.
- Выберите виджет "События внимания", чтобы отобразить его на приборной панели. См. ниже.



Вы также можете приостановить и возобновить подачу данных в реальном времени, нажав на кнопку Pause Live Data. Кроме того, Вы можете в любой момент вернуться к приборной панели по умолчанию, нажав кнопку Default Dashboard.

Виджет системных графиков

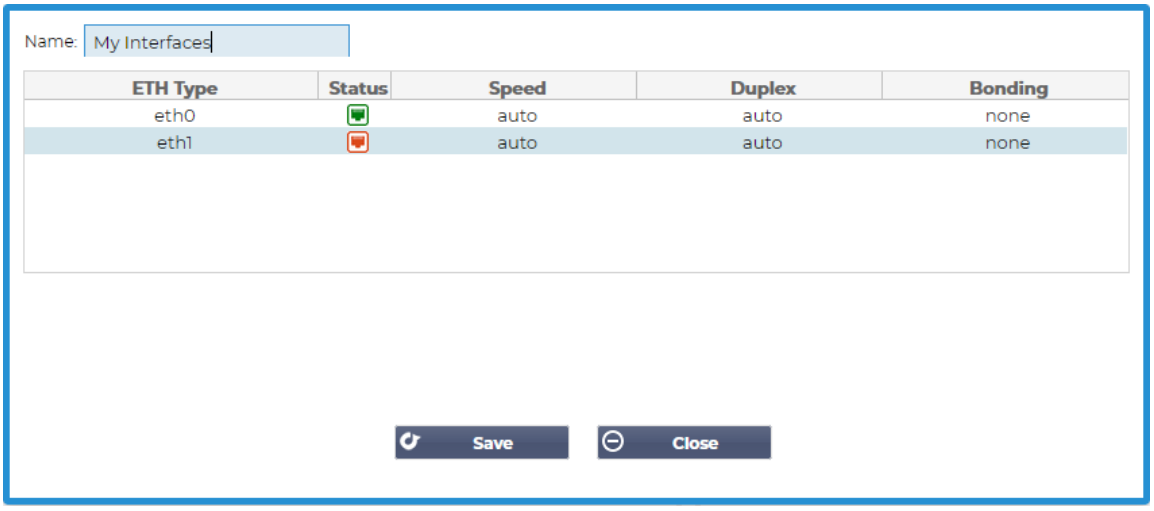


АЦП имеет настраиваемый виджет System Graph. Нажав кнопку Добавить на виджете, Вы можете добавить следующие графики мониторинга для отображения.

- CPU
- ПАМЯТЬ
- ДИСК

После того, как Вы их добавите, они будут доступны по отдельности в меню виджетов приборной панели.

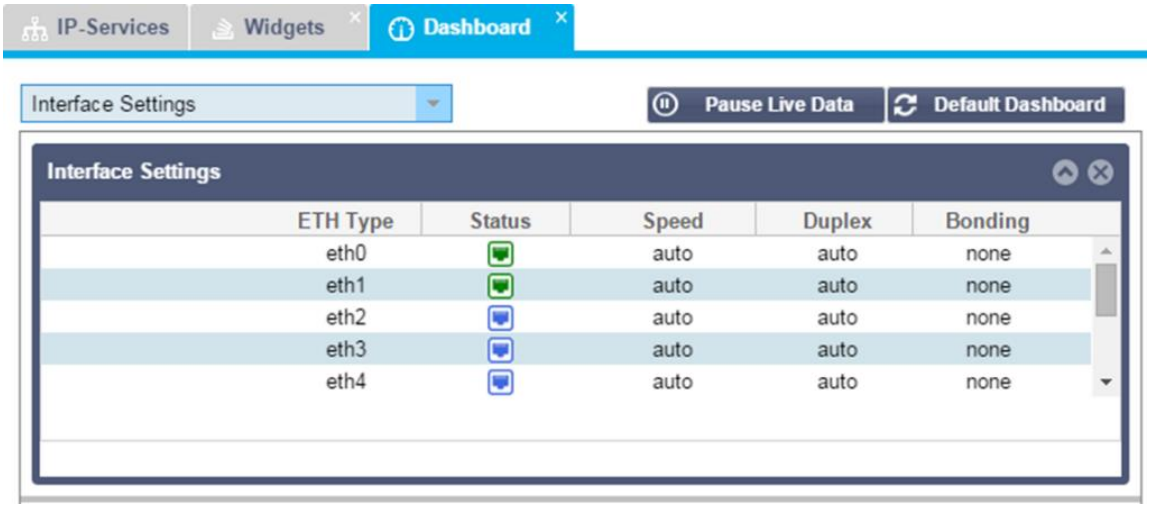
Виджет интерфейса



Виджет Интерфейс позволяет Вам отобразить данные для выбранного сетевого интерфейса, например, ETH0, ETH1 и так далее. Количество доступных интерфейсов для добавления зависит от того, сколько сетевых интерфейсов Вы определили для виртуального устройства или обеспечили в аппаратном устройстве.

Когда Вы закончите, нажмите кнопку Сохранить, а затем кнопку Закрыть.

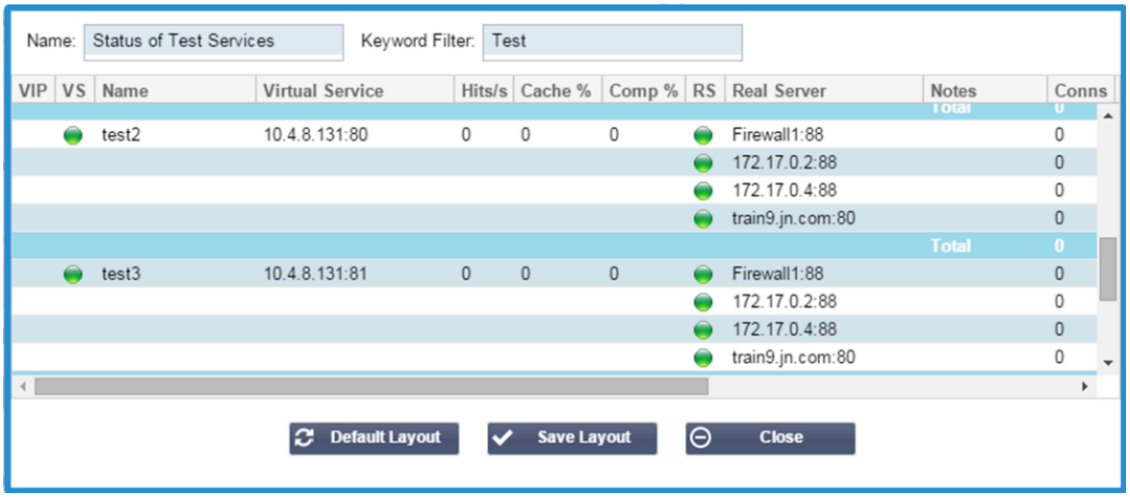
Выберите виджет, который Вы только что настроили, из выпадающего меню виджетов в панели инструментов. Вы увидите окно, как показано ниже.



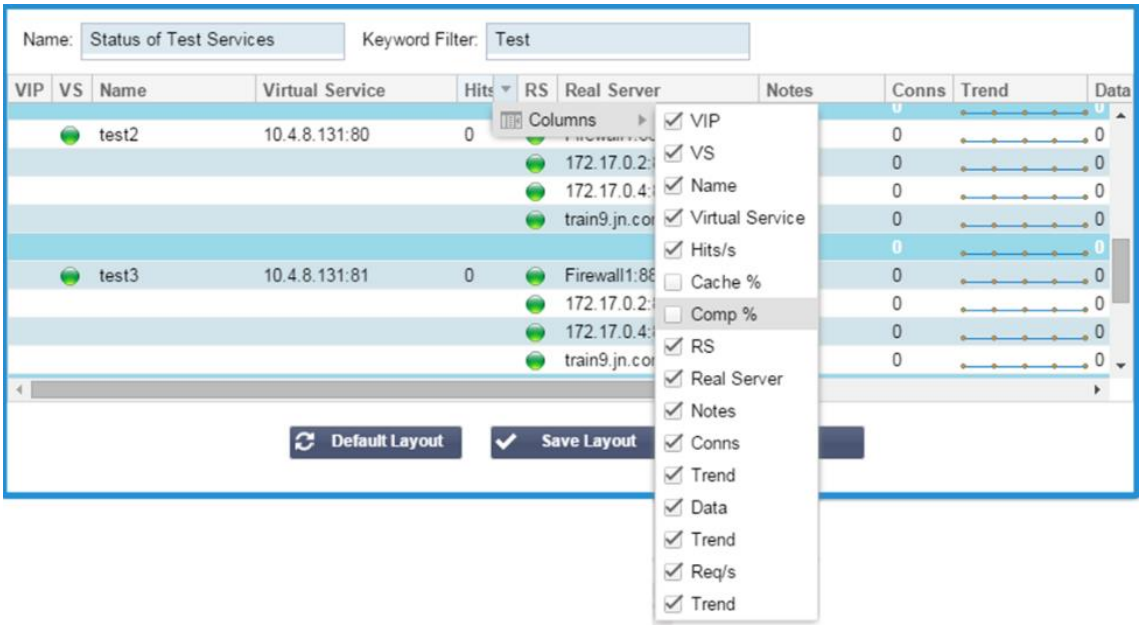
Виджет состояния

Виджет Status позволяет Вам увидеть балансировку нагрузки в действии. Вы также можете фильтровать представление, чтобы показать конкретную информацию.

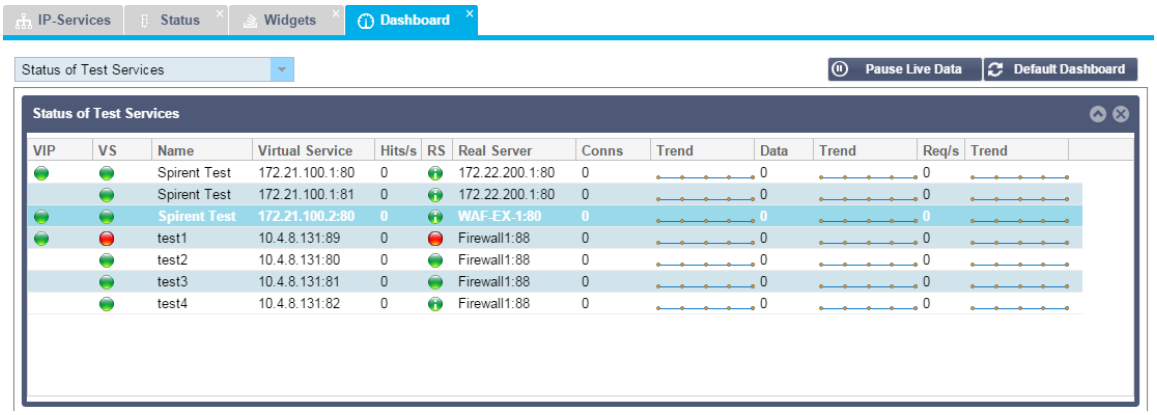
- Нажмите кнопку Добавить.



- Введите имя для услуги, которую Вы хотите контролировать
- Вы также можете выбрать, какие колонки Вы хотите отобразить в виджете.

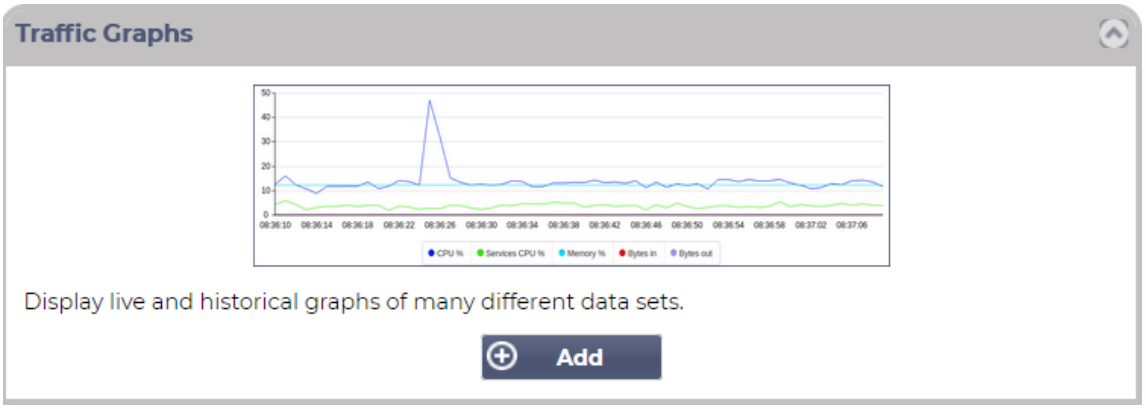


- Когда Вы будете удовлетворены, нажмите Сохранить, а затем Закрыть.
- Выбранный виджет Status будет доступен в разделе Dashboard.



Виджет графики трафика

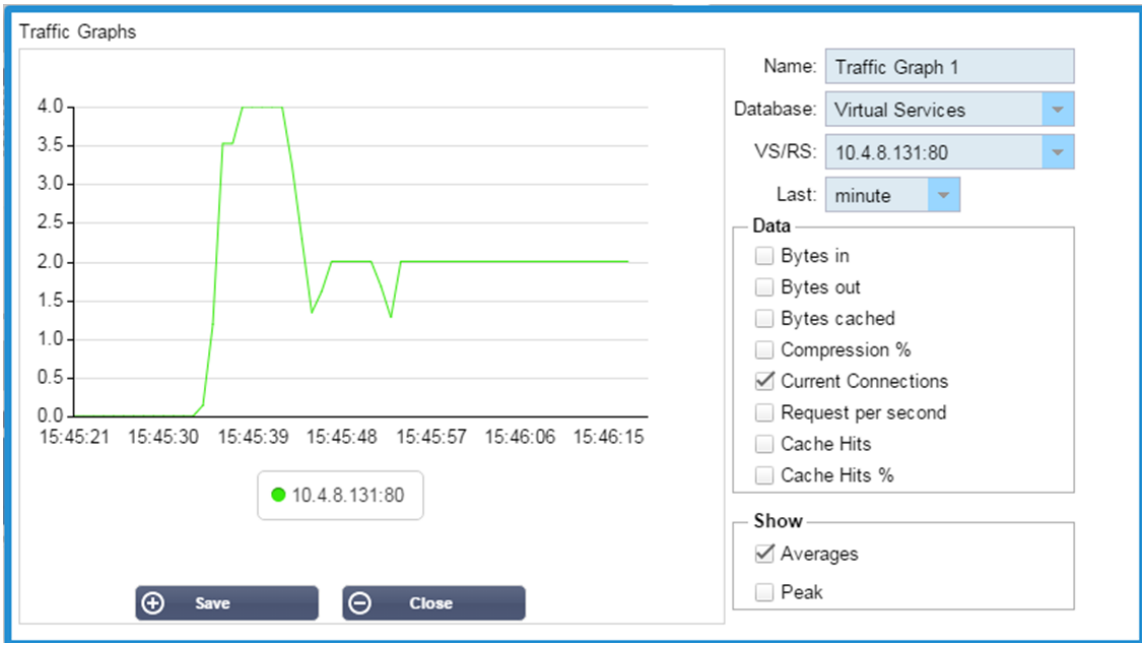
Этот виджет может быть настроен на отображение текущих и исторических данных трафика по виртуальным службам и реальным серверам. Кроме того, Вы можете увидеть общие текущие и исторические данные по глобальному трафику



- Нажмите кнопку Добавить
- Назовите свой виджет.
- Выберите базу данных из Виртуальных служб, Реальных серверов или Системы.

- Если Вы выбрали Виртуальные службы, Вы можете выбрать виртуальную службу из раскрывающегося списка VS/RS.
- Выберите временной интервал из раскрывающегося списка Последний.
    - Минута - последние 60
    - Час - агрегированные данные с каждой минуты за последние 60 минут
    - День - агрегированные данные за каждый час за предыдущие 24 часа
    - Неделя - агрегированные данные за каждый день в течение предыдущих семи дней
    - Месяц - агрегированные данные за каждую неделю за последние семь дней
    - Год - агрегированные данные за каждый месяц в течение предыдущих 12 месяцев
- Выберите Доступные данные в зависимости от выбранной Вами базы данных
    - База данных виртуальных служб
    - Байты в
    - Вывод байтов
    - Кэшированные байты
    - Сжатие %
    - Текущие соединения
    - Запросы в секунду
    - Хиты кэша
    - Хиты кэша %
- Реальные серверы
    - Байты в
    - Вывод байтов
    - Текущие соединения
    - Запрос в секунду
    - Время ответа
- Система
    - CPU %
    - Услуги ЦП
    - Память %
    - Свободный % на диске
    - Байты в
    - Вывод байтов
- Выбор отображения средних или пиковых значений
- После того, как Вы выбрали все параметры, нажмите Сохранить и закрыть

Пример графика трафика



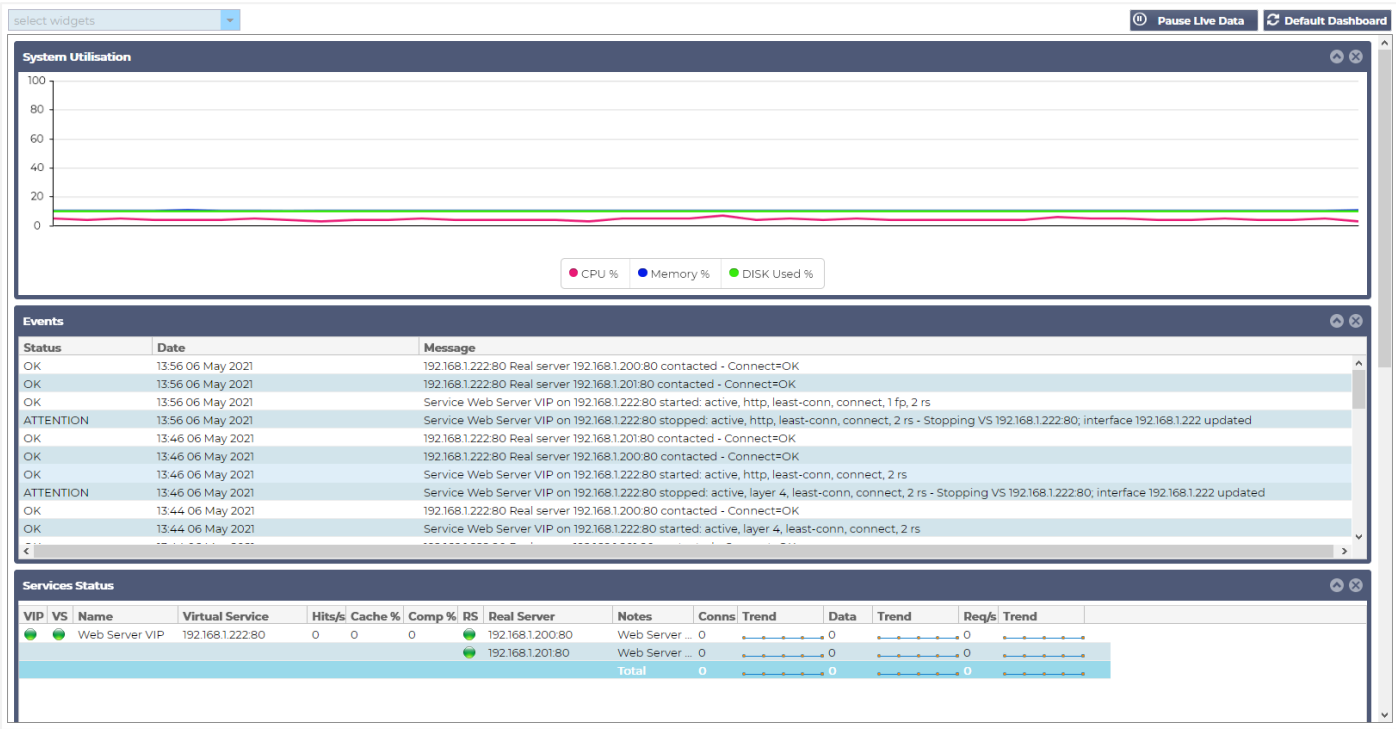
Теперь Вы можете добавить свой виджет Traffic Graph в меню View > Dashboard.

Посмотреть

Приборная панель

Как и во всех интерфейсах управления ИТ-системами, часто возникают ситуации, когда Вам необходимо просмотреть показатели производительности и данные, которые обрабатывает ADC. Мы предоставляем настраиваемую приборную панель для того, чтобы Вы могли сделать это простым и содержательным образом.

Приборная панель доступна с помощью сегмента Вид на панели навигатора. Когда она выбрана, она показывает несколько виджетов по умолчанию и позволяет Вам выбрать любые настроенные виджеты, которые Вы определили.



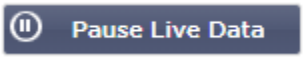
Использование приборной панели

Приборная панель U состоит из четырех элементов: меню виджетов, кнопка паузы/воспроизведения и кнопка "Приборная панель по умолчанию".

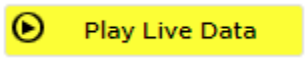
Меню виджетов

Меню "Виджеты", расположенное в верхней левой части приборной панели, позволяет Вам выбрать и добавить любые стандартные или настроенные виджеты, которые Вы определили. Чтобы воспользоваться этим меню, выберите виджет из выпадающего списка.

Кнопка приостановки данных в реальном времени

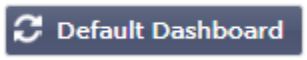


Эта кнопка позволяет Вам выбрать, должен ли АЦП обновлять приборную панель в режиме реального времени. После приостановки ни один виджет приборной панели не будет обновляться, что позволит Вам изучать содержимое в свое удовольствие. Кнопка меняет состояние на отображение Play Live Data, как только инициируется пауза.



Когда Вы закончите, просто нажмите кнопку Play Live Data, чтобы возобновить сбор данных и обновить приборную панель.

Кнопка приборной панели по умолчанию



Может случиться так, что Вы захотите сбросить макет приборной панели на макет по умолчанию. В этом случае нажмите кнопку Default Dashboard. После нажатия все изменения, внесенные в приборную панель, будут потеряны.

Изменение размера, минимизация, переупорядочивание и удаление виджетов

Изменение размера виджета

Вы можете очень легко изменить размер виджета. Нажмите и удерживайте строку заголовка виджета и перетащите его в левую или правую часть области Приборной панели. Вы увидите пунктирный прямоугольник, который представляет собой новый размер виджета. Поместите виджет в прямоугольник и отпустите кнопку мыши. Если Вы хотите поместить виджет с измененным размером рядом с виджетом, размер которого был изменен ранее, Вы увидите, что прямоугольник появляется рядом с виджетом, который Вы хотите поместить рядом.

Минимизация виджета

Вы можете свернуть виджеты в любое время, щелкнув по строке заголовка виджета. Это действие свернет виджет и отобразит только строку заголовка.

Перемещение порядка виджетов

Чтобы переместить виджет, Вы можете перетащить его, нажав и удерживая кнопку мыши на строке заголовка и перемещая мышь.

Удаление виджета

Вы можете удалить виджет, нажав на ⊗значок в строке заголовка виджета.

История

Опция История, выбираемая из навигатора, позволяет администратору изучить исторические показатели работы ADC. Исторические представления могут быть созданы для виртуальных служб, реальных серверов и системы.

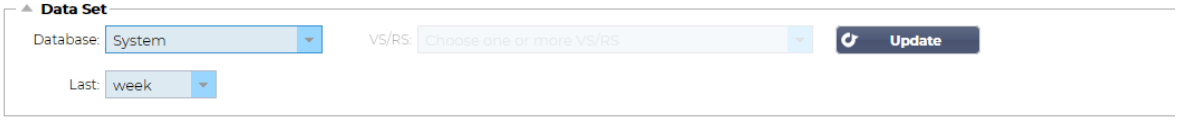
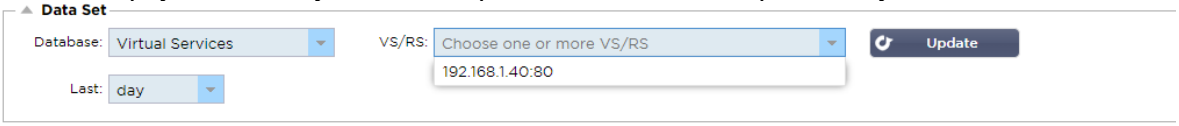
Это также позволит Вам увидеть балансировку нагрузки в действии и поможет выявить любые ошибки или закономерности, которые необходимо исследовать. Обратите внимание, что для использования этой функции Вы должны включить ведение журнала в System > History.

Просмотр графических данных

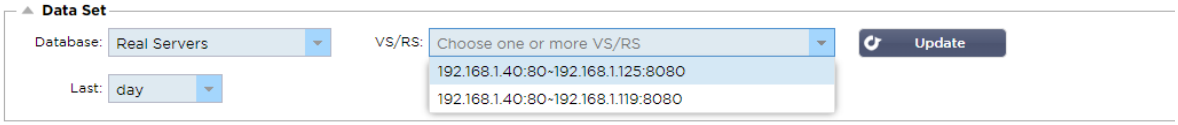
Набор данных

Чтобы просмотреть исторические данные в графическом формате, пожалуйста, выполните следующие действия:

Первым шагом является выбор базы данных и периода, относящегося к информации, которую Вы хотите просмотреть. Период, который Вы можете выбрать в раскрывающемся списке "Последний", - это минута, час, день, неделя, месяц и год.

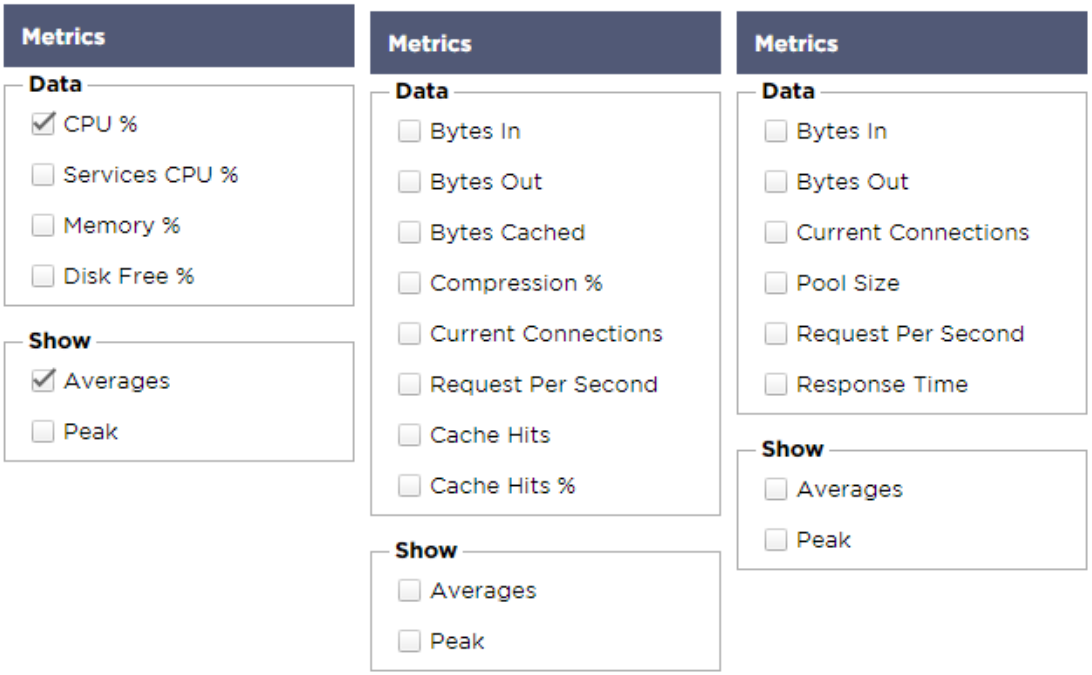
База данных	**Описание**
Система	Выбрав эту базу данных, Вы сможете просмотреть данные о процессоре, памяти и дисковом пространстве с течением времени 
Виртуальные услуги	Выбрав эту базу данных, Вы сможете выбрать все виртуальные службы в базе данных с того момента, когда Вы начали регистрировать данные. Вы увидите список виртуальных служб, из которого Вы можете выбрать одну. 

Реальные услуги	Выбрав эту базу данных, Вы сможете выбрать все Real Servers в базе данных с того момента, когда Вы начали регистрировать данные. Вы увидите список Real Servers, из которого Вы можете выбрать один.

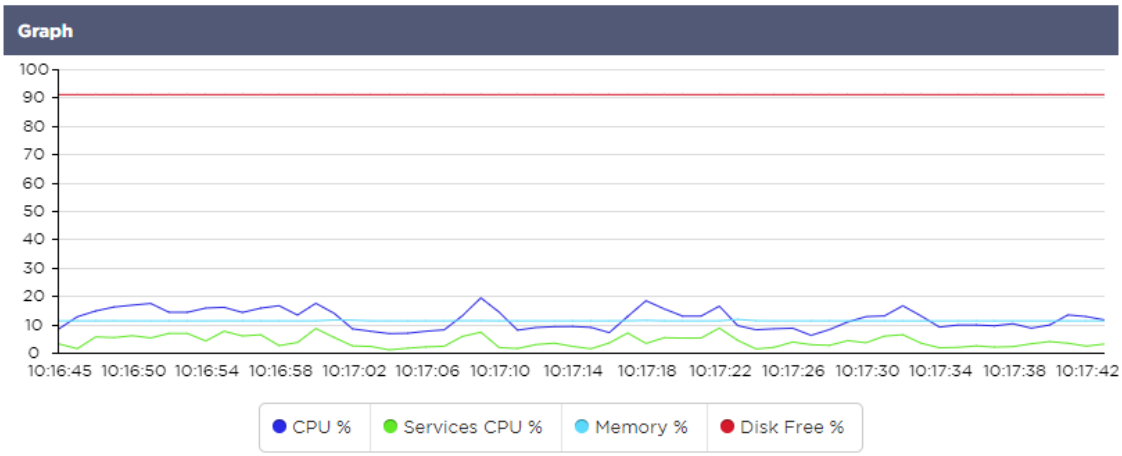


Метрика

После того, как Вы выбрали набор данных, который Вы будете использовать, пришло время выбрать метрики, которые Вы хотите отобразить. На изображении ниже показаны метрики, доступные для выбора администратором: эти выборки соответствуют Системе, Виртуальным службам и Реальным серверам (слева направо).



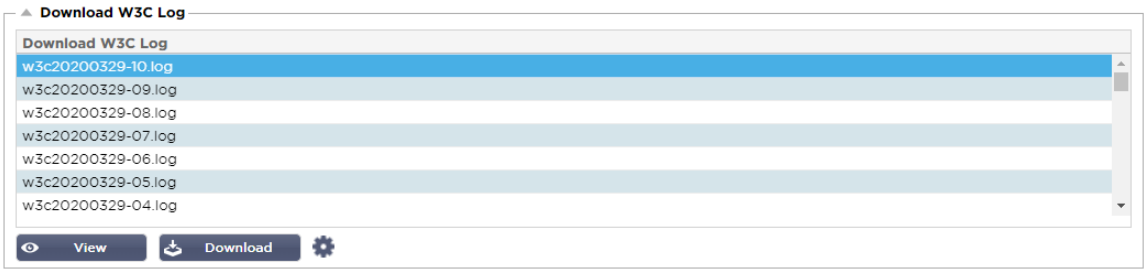
Образец графика



Журналы

Страница Журналы в разделе Вид позволяет Вам просматривать и загружать журналы W3C и Системы. Страница организована в два раздела, как подробно описано ниже.

Скачать журналы W3C



Ведение журнала W3C включается в разделе Система > Ведение журнала. Журнал W3C - это журнал доступа для веб-серверов, в котором создаются текстовые файлы, содержащие данные о каждом запросе доступа, включая адрес источника Интернет-протокола (IP), версию HTTP, тип браузера, ссылающуюся страницу и метку времени. Журналы W3C могут стать очень большими в зависимости от объема данных и категории регистрируемого журнала.

В разделе W3C Вы можете выбрать нужный Вам журнал, а затем просмотреть или скачать его.

Посмотреть кнопку

Кнопка Просмотр позволяет Вам просмотреть выбранный журнал в окне текстового редактора, например, Блокнота.

Скачать кнопку

Эта кнопка позволяет Вам загрузить журнал в локальное хранилище для последующего просмотра.

Значок шестеренки

Щелкнув на этом значке, Вы перейдете в раздел настроек журнала W3C, расположенный в System > Logging. Мы подробно обсудим это в разделе "Ведение журнала" данного руководства.

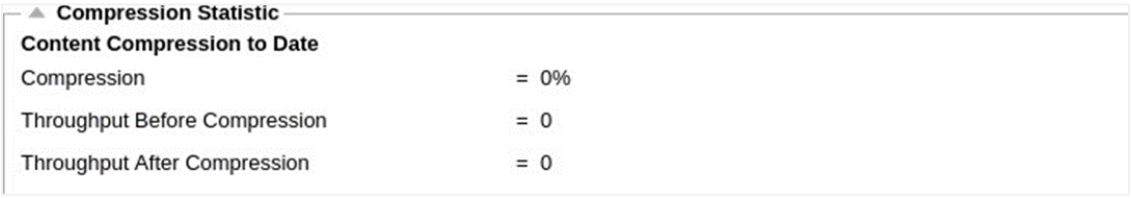
Статистика

Раздел Статистика ADC - это часто используемая область системными администраторами, которые хотят убедиться, что производительность ADC соответствует их ожиданиям.

Компрессия

Вся цель АЦП - отслеживать данные и направлять их на реальные серверы, настроенные на их получение. Функция сжатия данных предусмотрена в ADC для повышения производительности ADC. Бывают случаи, когда администраторы хотят протестировать и проверить информацию о сжатии данных в АЦП; эти данные предоставляются панелью Сжатие в Статистике.

Сжатие контента на сегодняшний день



Данные, приведенные в этом разделе, подробно описывают уровень сжатия, достигнутый АЦП на сжимаемом содержимом. Значение 60-80% - это то, что мы считаем типичным.

Общая компрессия на сегодняшний день

Overall Compression to Date			Current Values
Compression	= 0%		= 0%
Throughput Before Compression	= 1.93 GB		= 7.32 Mbps (data)
Throughput After Compression	= 1.93 GB		= 7.32 Mbps (data)
Throughput From Cache	= 0		= 0.00 Mbps (data)
		Total	= 14.64 Mbps (data)

Значения, представленные в этом разделе, сообщают, какой степени сжатия достиг АЦП для всего содержимого. Типичный процент для этого зависит от того, сколько предварительно сжатых изображений содержится в Ваших услугах. Чем больше количество изображений, тем меньше будет общий процент сжатия.

Общий ввод/вывод

Total Input	= 2.13 GB	Input/s	= 9.10 Mbps
Total Output	= 2.18 GB	Output/s	= 9.24 Mbps

Показатели общего входа/выхода представляют собой количество необработанных данных, прошедших в АЦП и из него. Единица измерения будет меняться по мере роста размера от Кбит/с до Мбит/с и Гбит/с.

Удары и соединения

Hits and Connections

Overall Hits Counted	= 185033	95 Hits/sec
Total Connection	= 208194	94 / 42 connections/sec
Peak Connections	= 29	1 current connections

Раздел "Хиты и соединения" содержит общую статистику хитов и транзакций, прошедших через АЦП. Итак, что означают хиты и соединения?

- Хит определяется как транзакция 7-го уровня. Обычно используется для веб-серверов, это GET-запрос на объект, например, изображение.
- Соединение определяется как TCP-соединение 4-го уровня. Многие транзакции могут происходить через 1 TCP-соединение.

Общее количество подсчитанных хитов

Цифры в этом разделе показывают кумулятивное количество некэшированных просмотров с момента последнего сброса. С правой стороны на рисунке будет показано текущее количество обращений в секунду.

Общее количество подключений

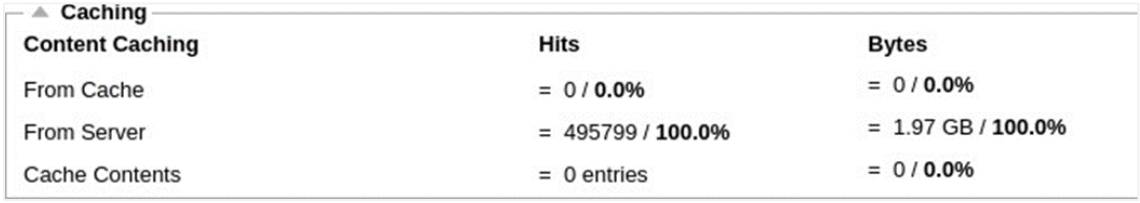
Значение Total Connections представляет собой кумулятивное количество TCP-соединений с момента последнего сброса. Цифра во втором столбце указывает на количество TCP-соединений, совершаемых в секунду с АЦП. Цифра в правом столбце - это количество TCP-соединений в секунду, выполненных с Реальными серверами. Пример 6/8 соединений/сек. В показанном примере мы имеем 6 TCP-соединений в секунду к Виртуальной службе и 6 TCP-соединений в секунду к Реальным серверам.

Пиковые соединения

Пиковое значение Connections представляет собой максимальное количество TCP-соединений, выполненных с АЦП. Число в крайнем правом столбце указывает на текущее количество активных TCP-соединений.

Кэширование

Как Вы помните, АЦП оснащен функциями сжатия и кэширования. В этом разделе показана общая статистика, связанная с кэшированием, когда оно применяется к каналу. Если кэширование не было применено к каналу и настроено правильно, Вы увидите 0 содержимого кэша.



Из кэша

Удары: В первом столбце указано общее количество транзакций, обслуживаемых из кэша АЦП с момента последнего сброса. Также представлен процент от общего количества транзакций.

Байты: Во втором столбце указан общий объем данных в килобайтах, обслуживаемых из кэша АЦП. Также указывается процент от общего объема данных.

От сервера

Удары: В столбце 1 указано общее количество транзакций, обслуживаемых с реальных серверов с момента последнего сброса. Также приводится процент от общего количества транзакций.

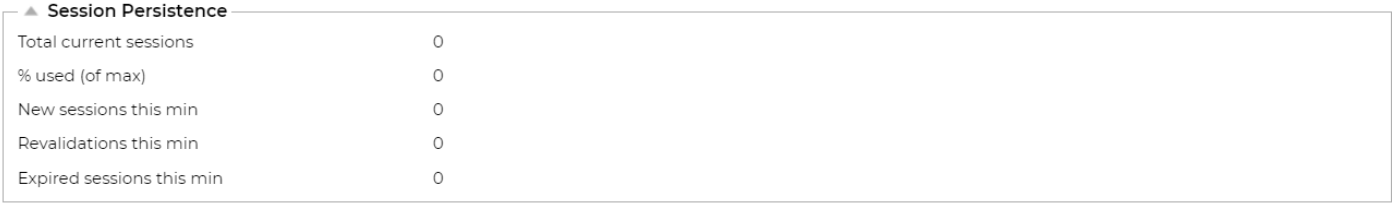
Байты: Во втором столбце указан общий объем данных в килобайтах, переданных с реальных серверов. Также указывается процент от общего объема данных.

Содержимое кэша

Хиты: Это число показывает общее количество объектов, содержащихся в кэше ADC.

Байты: Первое число показывает общий размер в мегабайтах кэшированных объектов ADC. Также указывается процент от максимального размера кэша.

Постоянство сессии



Раздел Session Persistence предоставляет информацию по нескольким параметрам.

Поле	Описание
Общее количество текущих сессий	Это показывает, сколько сеансов персистенции находится в процессе - обновляется каждую минуту
% Использованный (от максимального)	Это показывает, насколько используется общее пространство, отведенное для информации о сеансе.
Новая сессия в эти минуты	Это показывает, в течение последней минуты, сколько новых сеансов персистенции было добавлено
Переоцените этот мин	Это показывает, в течение последней минуты, сколько существующих сеансов персистентности было подтверждено большим количеством трафика
Просроченные сеансы в течение этой минуты	Это показывает, в течение последней минуты, сколько существующих сессий персистенции истекло из-за отсутствия дальнейшего трафика в течение тайм-аута

Аппаратное обеспечение

Независимо от того, используете ли Вы ADC в виртуальной среде или в составе аппаратного обеспечения, этот раздел предоставит Вам ценную информацию о производительности устройства.

Использование диска

Значение, представленное в колонке 2, дает процент используемого в настоящее время дискового пространства и включает информацию о файлах журнала и кэш-данных, которые периодически сохраняются на накопителе.

Использование памяти

Во втором столбце указан процент памяти, используемой в настоящее время. Более значимое число в скобках - это общий объем памяти, выделенный для АЦП. Рекомендуется выделять АЦП не менее 2 Гб оперативной памяти.

Использование процессора

Одним из критических значений является процент CPU, используемый в настоящее время ADC. Естественно, что этот показатель может колебаться.

Статус

На странице Вид > Статус отображается живой трафик, проходящий через ADC для определенных Вами виртуальных Служб. Она также показывает количество подключений и данных к каждому реальному серверу, чтобы Вы могли оценить балансировку нагрузки в режиме реального времени.

Детали виртуальной услуги

Колонка VIP

Цвет индикатора указывает на состояние виртуального IP-адреса, связанного с одной или многими виртуальными службами.

Статус	Описание
●	Онлайн
●	Failover-Standby. Эта виртуальная служба работает в режиме горячего резервирования
●	Указывает на то, что "пассив" задерживает "актив".
●	Не в сети. Реальные серверы недоступны, или ни один из реальных серверов не включен
●	Состояние находок
●	Не лицензированы или лицензированы Виртуальные IP превышены

Колонка состояния VS

Цвет индикатора указывает на состояние виртуальной службы.

Статус	Описание
●	Онлайн
●	Failover-Standby. Эта виртуальная служба работает в режиме горячего резервирования
●	Указывает на то, что "пассив" задерживает "актив".
●	Сервис требует внимания. Этот индикатор состояния может быть результатом того, что реальный сервер не прошел мониторинг здоровья или был вручную переведен в состояние Offline. Трафик будет продолжать идти, но с уменьшенной пропускной способностью реального сервера.
●	Не в сети. Реальные серверы недоступны, или ни один из реальных серверов не включен
●	Состояние находок
●	Не лицензированы или лицензированы Виртуальные IP превышены

Имя

Имя виртуальной службы

Виртуальная услуга (VIP)

Виртуальный IP-адрес и порт для службы, а также адрес, который будут использовать пользователи или приложения.

Хит/сек

Уровень 7 транзакций в секунду на стороне клиента.

Кэш%

Приведенный здесь показатель представляет собой процент объектов, которые были обслужены из кэша оперативной памяти АЦП.

Сжатие%

Этот показатель представляет собой процент объектов, которые были сжаты между клиентом и АЦП.

Статус RS (Удаленный сервер)

В таблице ниже описано значение статуса реальных серверов, связанных с VIP.

Статус	Описание
●	Подключено
●	Не контролируется
●	Слив или отключение
●	В режиме ожидания
●	Не подключено
●	Состояние находок
●	Не лицензированы или лицензированы Виртуальные IP превышены

Реальный сервер

IP-адрес и порт сервера Real Server.

Примечания

Это значение может быть любым полезным примечанием, чтобы другие поняли цель записи.

Conns (Соединения)

Представление количества подключений к каждому Real Server позволяет Вам увидеть балансировку нагрузки в действии. Очень полезно для проверки правильности работы Вашей политики балансировки нагрузки.

Данные

Значение в этой колонке показывает количество данных, отправляемых на каждый Real Server.

Req/Sec (Запросы в секунду)

Количество запросов в секунду, отправляемых на каждый Real Server.

Система

Сегмент System пользовательского интерфейса АЦП позволяет Вам получить доступ и управлять всеми общесистемными аспектами АЦП.

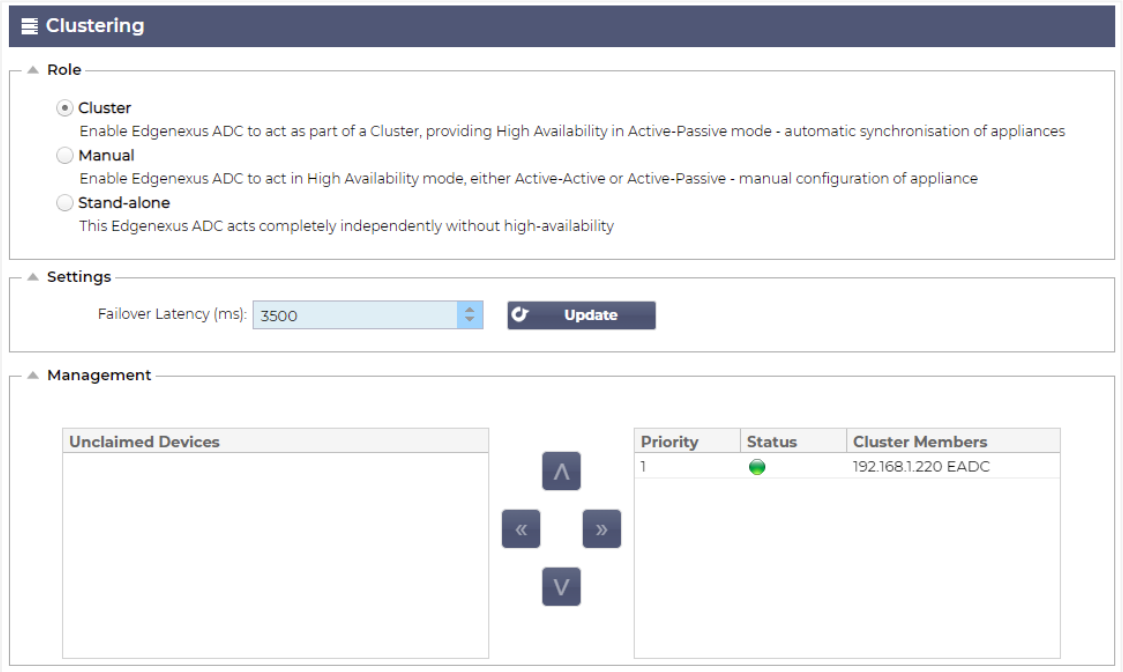
Кластеризация

ADC можно использовать как одиночное автономное устройство, и он будет прекрасно работать в этом качестве. Однако, если учесть, что назначение ADC - балансировать нагрузку множества серверов, необходимость кластеризации самого ADC становится очевидной. Легко ориентируемый дизайн пользовательского интерфейса ADC делает настройку системы кластеризации простой и понятной.

На странице Система > Кластеризация Вы сможете настроить высокую доступность Ваших устройств ADC. Этот раздел состоит из нескольких частей.

Важное замечание

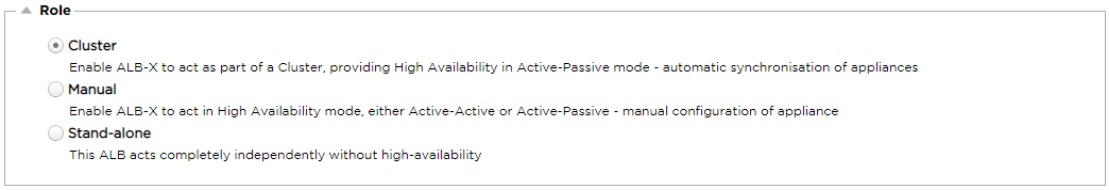
- Нет необходимости в выделенном кабеле между парой АЦП для поддержания высокой доступности сердцебиения.
- Сердцебиение происходит в той же сети, что и виртуальная служба, которой требуется высокая доступность.
- Между устройствами ADC не происходит обхода отказа по состоянию.
- Когда высокая доступность включена на двух или более ADC, каждый блок будет транслировать через UDP виртуальные услуги, которые он настроен предоставлять.
- При отказоустойчивости высокой доступности используется одноадресная передача сообщений и Gratuitous ARP для информирования новых коммутаторов Active load balancer.



Роль

При настройке ADC для высокой доступности доступны три роли кластера.

Кластер



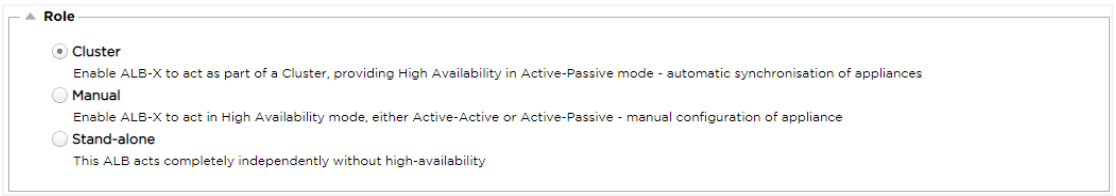
- По умолчанию новый АЦП включается с ролью Кластер. В этой роли каждый член кластера будет иметь одинаковую "рабочую конфигурацию", и, таким образом, только один АЦП в кластере будет активным в любой момент времени.
- Рабочая конфигурация" означает все параметры конфигурации, за исключением элементов, которые должны быть уникальными, например, IP-адрес управления, имя ALB Name, сетевые настройки, детали интерфейса и т.д.
- ADC с приоритетом 1, самая верхняя позиция, в блоке Cluster Members является владельцем кластера и активным балансировщиком нагрузки, в то время как все остальные ADC являются пассивными членами.
- Вы можете редактировать любой АЦП в кластере, и изменения будут синхронизированы со всеми членами кластера.
- Когда Вы удаляете ADC из кластера, все виртуальные службы будут удалены из этого ADC.
- Вы не можете удалить последнего члена кластера в Невостребованные устройства. Чтобы удалить последнего участника, измените роль на Manual или Stand-alone.
- Следующие объекты не синхронизируются:
    - Ручная секция Дата и время - (Секция NTP синхронизирована)
    - Задержка обхода отказа (мс)
    - Раздел "Оборудование
    - Раздел "Приборы
    - Раздел сети

Отказ владельца кластера

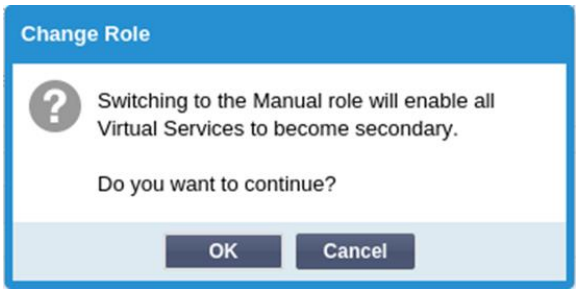
- Когда владелец кластера выходит из строя, один из оставшихся членов кластера автоматически берет на себя его обязанности и продолжает балансировать нагрузку трафика.
- Когда владелец кластера вернется, он возобновит балансировку нагрузки и возьмет на себя роль владельца.
- Предположим, что владелец вышел из строя, и балансировку нагрузки взял на себя один из участников. Если Вы хотите, чтобы Член, который принял на себя трафик балансировки нагрузки, стал новым владельцем, выделите его и нажмите стрелку вверх, чтобы переместить его в позицию Приоритет 1.
- Если Вы редактируете один из оставшихся членов кластера, а владелец не работает, отредактированный член автоматически перейдет на место владельца без потери трафика

Изменение роли с роли Кластера на роль Руководителя

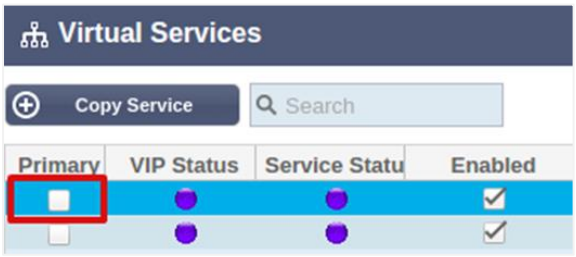
- Если Вы хотите изменить роль с Кластерной на Ручную, нажмите на радиокнопку рядом с опцией Ручная роль



- После того, как Вы нажмете на радиокнопку, Вы увидите следующее сообщение:



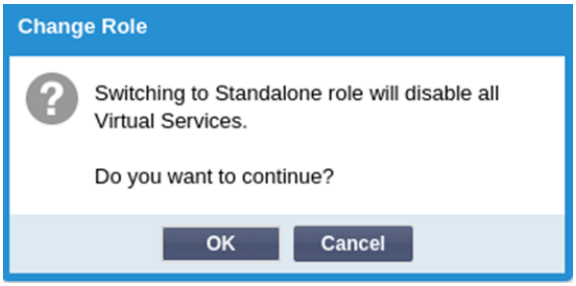
- Нажмите кнопку OK
- Проверьте раздел Виртуальные службы. Вы увидите, что в столбце Primary теперь стоит галочка.



- Это функция безопасности и означает, что если у Вас есть другой ADC с теми же виртуальными службами, то поток трафика не будет прерван.

Изменение роли с кластерной на автономную

- Если Вы хотите изменить роль с Кластера на Автономную, нажмите на радиокнопку рядом с опцией Автономная.
- Вам будет предложено следующее сообщение:



- Нажмите OK, чтобы изменить роли.
- Проверьте свои Виртуальные службы. Вы увидите, что колонка Primary изменила название на Stand-alone
- Вы также увидите, что все виртуальные службы отключены (не отмечены) по соображениям безопасности.
- Когда Вы убедитесь, что ни один другой ADC в той же сети не имеет дублирующих виртуальных служб, Вы можете включить каждую из них по очереди.

Роль руководства

ADC в роли Manual будет работать с другими ADC в роли Manual для обеспечения высокой доступности. Основным преимуществом по сравнению с ролью Cluster является возможность установить, какой ADC является активным для виртуального IP. Недостатком является отсутствие синхронизации конфигурации между ADC. Любые изменения должны быть реплицированы вручную

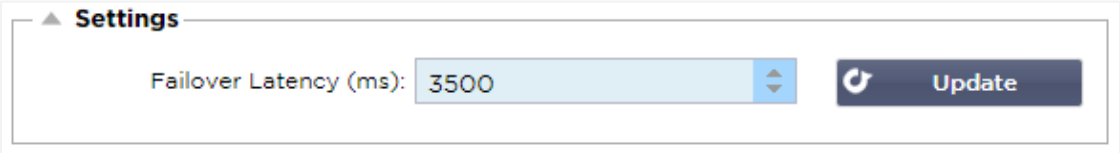
на каждой коробке через графический интерфейс, или при большом количестве изменений Вы можете создать jetPACK с одного ADC и отправить его на другой.

- Чтобы сделать виртуальный IP-адрес "Активным", установите флажок в основной колонке (страница IP Services).
- Чтобы сделать виртуальный IP-адрес "Пассивным", оставьте флажок пустым в основной колонке (страница IP Services).
- В случае, если активная служба переходит в пассивную:
  - Если обе колонки Primary отмечены галочками, то происходит процесс выборов, и наименьший MAC-адрес будет Active
  - Если оба флажка не установлены, то происходит тот же процесс выборов. Кроме того, если обе галочки сняты, то автоматического возврата к исходному активному АЦП не происходит.

Отдельная роль

ADC в роли автономного не будет взаимодействовать с другими ADC относительно своих услуг, и поэтому все виртуальные службы будут оставаться в зеленом статусе и подключенными. Вы должны убедиться, что все Виртуальные службы имеют уникальные IP-адреса, иначе в Вашей сети возникнет конфликт.

Настройки

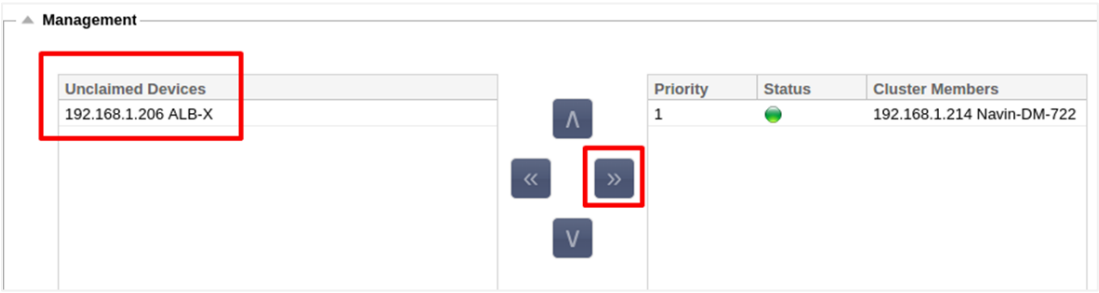


В разделе "Настройки" Вы можете установить Failover Latency в миллисекундах, время, которое пассивный ADC будет ждать, прежде чем взять на себя управление виртуальными службами после отказа активного ADC.

Мы рекомендуем установить значение 10000 мс или 10 секунд, но Вы можете уменьшить или увеличить это значение в соответствии с Вашей сетью и требованиями. Приемлемые значения находятся в диапазоне от 1500 мс до 20000 мс. Если Вы испытываете нестабильность в кластере при более низкой задержке, Вам следует увеличить это значение.

Менеджмент

В этом разделе Вы можете добавлять и удалять членов кластера, а также изменять приоритет АЦП в кластере. Раздел состоит из двух панелей и набора клавиш со стрелками между ними. Область слева - это Невостребованные устройства, а самая правая область - это сам кластер.

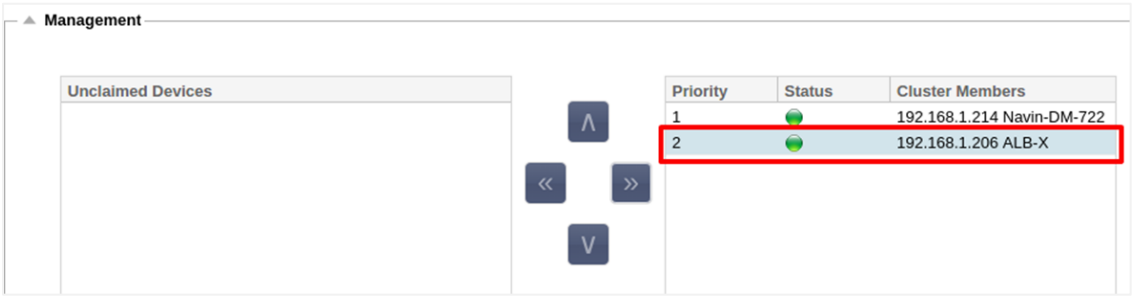


Добавление АЦП в кластер

- Перед добавлением ADC в кластер, Вы должны убедиться, что всем устройствам ADC предоставлен уникальный набор имен в разделе Система > Сеть.

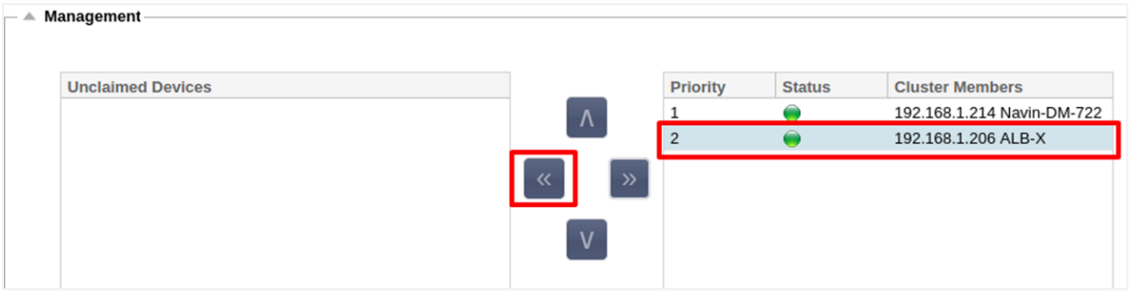
- Вы должны увидеть ADC как Приоритет 1 со статусом зеленого цвета и его имя в колонке Члены кластера в разделе управления. Этот ADC является основным устройством по умолчанию.
- Все остальные доступные ADC будут отображаться в окне Невостребованные устройства в разделе управления. Невостребованное устройство - это ADC, который был назначен в роли кластера, но не имеет настроенных виртуальных служб.
- Выделите АЦП из окна Невостребованные устройства и нажмите кнопку со стрелкой вправо.
- Теперь Вы увидите следующее сообщение:

- Нажмите OK, чтобы повысить ADC в кластере.
- Теперь Ваш ADC должен отображаться как Приоритет 2 в списке членов кластера.



Удаление члена кластера

- Выделите члена кластера, которого Вы хотите удалить из кластера.
- Нажмите кнопку со стрелкой влево.

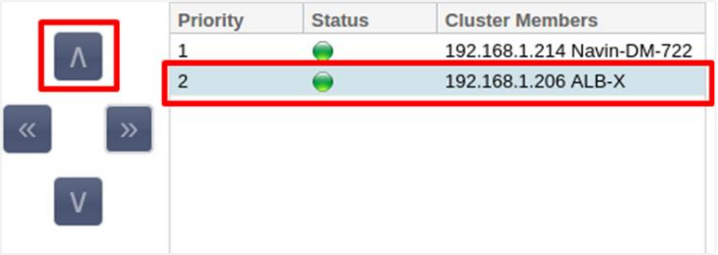


- Вам будет представлен запрос на подтверждение.
- Нажмите OK для подтверждения.
- Ваш ADC будет удален и отображен в разделе "Невостребованные устройства".

Изменение приоритета АЦП

Бывают случаи, когда Вы хотите изменить приоритет АЦП в списке членов.

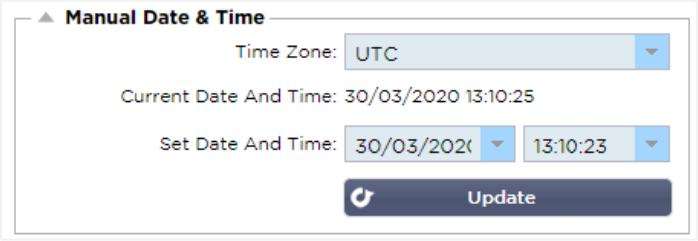
- ADC в верхней части списка членов кластера имеет приоритет 1 и является активным ADC для всех виртуальных служб.
- ADC, который является вторым в списке, получает приоритет 2 и является пассивным ADC для всех виртуальных служб.
- Чтобы изменить, какой АЦП является активным, просто выделите АЦП и нажмите стрелку вверх, пока он не окажется в верхней части списка



Дата и время

Раздел "Дата и время" позволяет установить характеристики даты/времени АЦП, включая часовой пояс, в котором находится АЦП. Вместе с часовым поясом дата и время играют важную роль в криптографических процессах, связанных с шифрованием SSL.

Дата и время вручную



Часовой пояс

Значение, которое Вы установили в этом поле, представляет собой часовой пояс, в котором находится АЦП.

- Нажмите на выпадающее поле для Часового пояса и начните вводить свое местоположение. Например, Лондон
- Когда Вы начнете вводить текст, АЦП автоматически отобразит места, содержащие букву L.
- Продолжайте вводить 'Lon,' и так далее - список мест будет сужен до тех, которые содержат 'Lon. '
- Если Вы находитесь, скажем, в Лондоне, то выберите Европа/Лондон, чтобы установить свое местоположение

Если после вышеуказанного изменения Дата и время все еще неправильные, пожалуйста, измените дату вручную

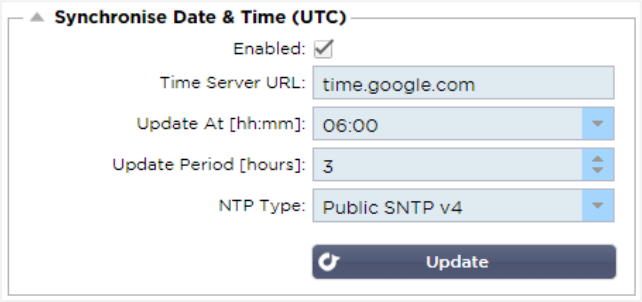
Установите дату и время

Эта настройка представляет собой фактическую дату и время.

- Выберите правильную дату из первого выпадающего списка или, альтернативно, Вы можете ввести дату в следующем формате ДД/ММ/ГГГГ
- Добавьте время в следующем формате hh: mm: ss, например, 06:00:10 для 6 часов утра и 10 секунд.
- После того, как Вы введете его правильно, пожалуйста, нажмите Обновить, чтобы подать заявку.
- После этого Вы должны увидеть новые Дата и Время, выделенные жирным шрифтом.

Синхронизация даты и времени (UTC)

Вы можете использовать NTP-серверы для точной синхронизации даты и времени. Серверы NTP расположены по всему миру, и Вы также можете иметь свой собственный внутренний сервер NTP, если Ваша инфраструктура имеет ограничения на внешний доступ.



URL сервера времени

Введите действительный IP-адрес или полное доменное имя (FQDN) для сервера NTP. Если сервер является глобально расположенным сервером в Интернете, рекомендуется использовать FQDN.

Обновление в [чч:мм]

Выберите запланированное время, в которое Вы хотите, чтобы АЦП синхронизировался с NTP-сервером.

Период обновления [часы]:

Выберите, как часто Вы хотите, чтобы происходила синхронизация.

Тип NTP:

- Public SNTP V4 - Это текущий и предпочтительный метод при синхронизации с NTP-сервером. **RFC 5905**
- NTP v1 Over TCP - Устаревшая версия NTP через TCP. **RFC 1059**
- NTP v1 Over UDP - Устаревшая версия NTP через UDP. **RFC 1059**

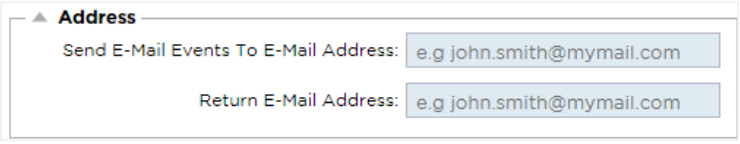
Примечание: Обратите внимание, что синхронизация осуществляется только по Гринвичу. Если Вы хотите установить местное время, это можно сделать только вручную. Это ограничение будет изменено в последующих версиях, чтобы включить возможность выбора часового пояса.

События по электронной почте

ADC является критически важным устройством, и, как любая важная система, он оснащен возможностью информировать системную администрацию о любых проблемах, которые могут потребовать внимания.

Страница Система > События электронной почты позволяет Вам настроить подключение к серверу электронной почты и отправку уведомлений системным администраторам. Страница организована в следующие разделы.

Адрес



Отправить по электронной почте События по адресам электронной почты

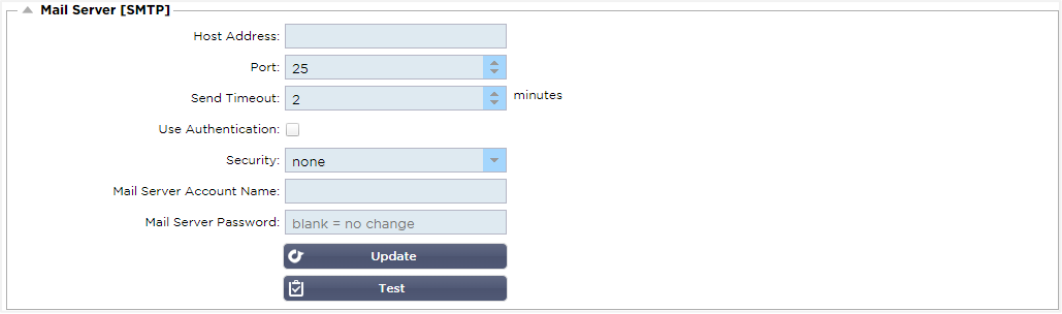
Добавьте действующий адрес электронной почты для отправки на него оповещений, уведомлений и событий. Пример support@domain.com. Вы также можете добавить несколько адресов электронной почты, используя разделитель-запятую.

Обратный адрес электронной почты:

Добавьте адрес электронной почты, который будет отображаться в папке входящих сообщений. Пример adc@domain.com.

Почтовый сервер (SMTP)

В этом разделе Вы должны добавить данные SMTP-сервера, который будет использоваться для отправки писем. Пожалуйста, убедитесь, что адрес электронной почты, который Вы используете для отправки, авторизован для этого.



Адрес хоста

Добавьте IP-адрес Вашего SMTP-сервера.

Порт

Добавьте порт Вашего SMTP-сервера. Порт по умолчанию для SMTP - 25 или 587, если Вы используете SSL.

Таймаут отправки

Добавьте тайм-аут SMTP. По умолчанию установлено значение 2 минуты.

Используйте аутентификацию

Поставьте галочку, если Ваш SMTP-сервер требует аутентификации.

Безопасность

- Нет
- По умолчанию установлено значение "нет".
- SSL - Используйте эту настройку, если Ваш SMTP-сервер требует аутентификации Secure Sockets Layer.
- TLS - Используйте эту настройку, если Ваш SMTP-сервер требует аутентификации Transport Layer Security.

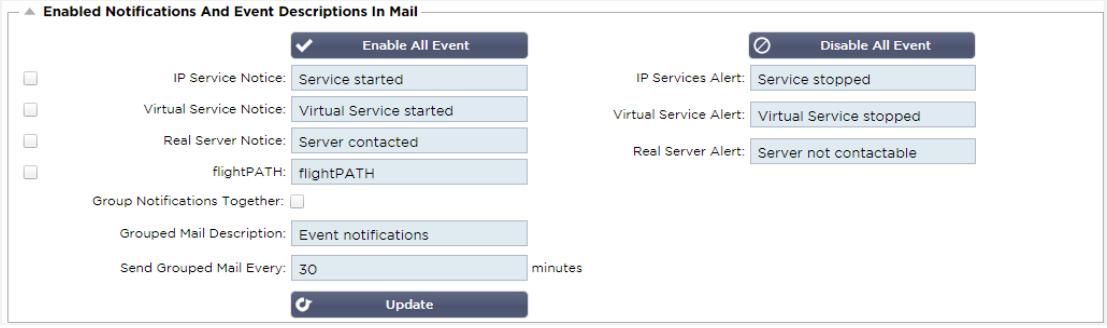
Имя учетной записи основного сервера

Добавьте имя пользователя, необходимое для аутентификации.

Пароль почтового сервера

Добавьте пароль, необходимый для аутентификации.

Уведомления и оповещения



Существует несколько типов уведомлений о событиях, которые АЦП будет отправлять лицам, настроенным на их получение. Вы можете отметить и включить уведомления и оповещения, которые должны рассылаться. Уведомления возникают, когда происходит контакт с реальными серверами или запускаются каналы. Оповещения возникают, когда с Реальными серверами невозможно связаться или каналы перестают работать.

IP-служба

Уведомление IP-службы сообщит Вам, когда какой-либо Виртуальный IP-адрес находится в сети или перестал работать. Это действие выполняется для всех Виртуальных служб, принадлежащих VIP.

Виртуальная служба

Информирует получателя о том, что виртуальная служба находится в режиме онлайн или перестала работать.

Реальный сервер

Когда Real Sever и Port подключены или не могут связаться, ADC отправит уведомление Real Server.

flightPATH

Это уведомление - электронное письмо, отправляемое при выполнении какого-либо условия, и при наличии настроенного действия, инструктирующего ADC отправить это событие по электронной почте.

Групповые уведомления

Поставьте галочку, чтобы сгруппировать уведомления. Если этот флажок установлен, все уведомления и предупреждения будут объединены в одно письмо.

Описание групповой почты

Укажите соответствующую тему для группового уведомления по электронной почте.

Интервал групповой отправки

Задайте количество времени, которое Вы хотите подождать перед отправкой группового уведомления по электронной почте. Минимальное время составляет 2 минуты.

Предупреждения

Существует два типа предупреждающих писем, и ни одно из них не следует игнорировать.

Дисковое пространство

Установите процент свободного дискового пространства, до достижения которого будет отправлено предупреждение. Когда этот показатель будет достигнут, Вам будет отправлено электронное письмо.

Истечение срока действия лицензии

Этот параметр позволяет Вам включить или отключить предупреждение об истечении срока действия лицензии, отправляемое по электронной почте системному администратору. Когда это значение будет достигнуто, Вам будет отправлено электронное письмо.

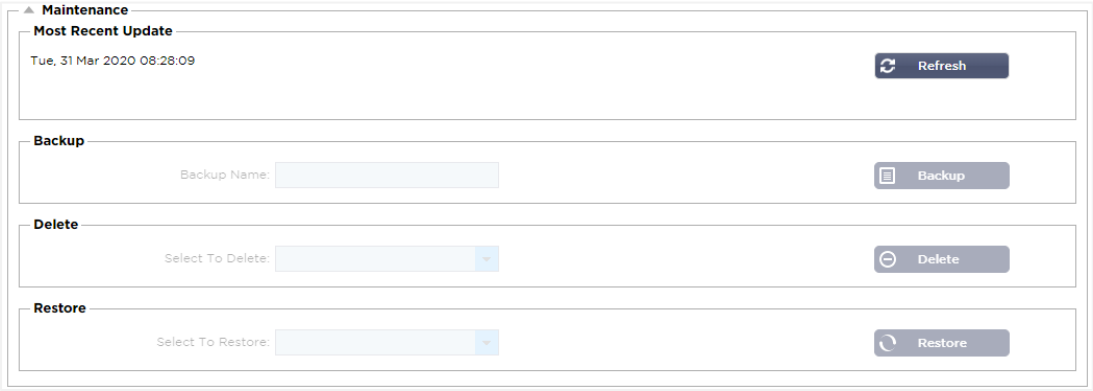
История системы

В разделе Система находится опция История системы, позволяющая предоставлять исторические данные для таких элементов, как ЦП, память, запросы в секунду и другие характеристики. После включения этой опции Вы можете просмотреть результаты в графическом виде на странице Вид > История. Эта страница также позволит Вам создать резервную копию или восстановить файлы истории на локальном ADC.

Сбор данных

- Чтобы разрешить сбор данных, поставьте, пожалуйста, галочку.
- Затем установите временной интервал, через который АЦП будет собирать данные. Это значение времени может находиться в диапазоне 1-60 секунд.

Техническое обслуживание



Этот раздел будет выделен серым цветом, если Вы включили ведение исторических журналов. Пожалуйста, снимите флажок Enabled в разделе Collect Data и нажмите Update, чтобы разрешить ведение исторических журналов.

Резервное копирование

Дайте своей резервной копии описательное имя. Нажмите Резервное копирование, чтобы создать резервную копию всех файлов на ADC

Удалить

Выберите файл резервной копии из выпадающего списка. Нажмите Удалить, чтобы удалить файл резервной копии из ADC

Восстановить

Выберите ранее сохраненный файл резервной копии. Нажмите кнопку Восстановить, чтобы заполнить данные из этого файла резервной копии.

Лицензия

АЦП лицензируется для использования либо с помощью одной из следующих моделей, что зависит от параметров покупки и типа клиента.

Тип лицензии	Описание
Вечный	Вы, клиент, имеете право использовать АЦП и другое программное обеспечение бессрочно. Это не исключает того, что Вам придется приобрести поддержку для получения помощи и обновлений.
SaaS	SaaS или Software-as-a-Service означает, что Вы, по сути, арендуете программное обеспечение на постоянной или платной основе. В этой модели Вы платите ежегодную аренду за программное обеспечение. У Вас нет бессрочных прав на использование программного обеспечения.
MSP	Поставщики управляемых услуг могут предлагать ADC в качестве услуги и приобретать лицензию по принципу "на каждого VIP", начисляемую и оплачиваемую ежегодно.

Лицензия Подробнее

Каждая лицензия включает конкретные детали, относящиеся к лицу или организации, приобретающей ее.

Идентификатор лицензии

Этот идентификатор лицензии напрямую связан с идентификатором машины и другими деталями, специфичными для Вашей покупки и ADC. Эта информация очень важна и требуется, когда Вы хотите получить обновления и другие элементы из App Store.

Идентификатор машины

Machine ID генерируется с использованием IP-адреса eth0 виртуального устройства ADC и MAC ID аппаратного ADC. Если Вы измените IP-адрес виртуального устройства ADC, лицензия больше не будет действительна. Вам придется обратиться за помощью в службу поддержки. Мы рекомендуем, чтобы Ваши виртуальные устройства ADC имели фиксированные IP-адреса с инструкциями не менять их. Техническая поддержка доступна путем создания заявки на сайте HTTPs://edgenexus.io.

Примечание: Вы не должны изменять IP-адрес или MAC ID Ваших устройств ADC. Если Вы работаете в виртуализированной среде, то, пожалуйста, исправьте MAC ID и IP-адрес.

Выдано

Это значение содержит имя покупателя, связанное с идентификатором машины АЦП.

Контактное лицо

Это значение содержит контактное лицо, с которым необходимо связаться в компании клиента, связанной с идентификатором машины

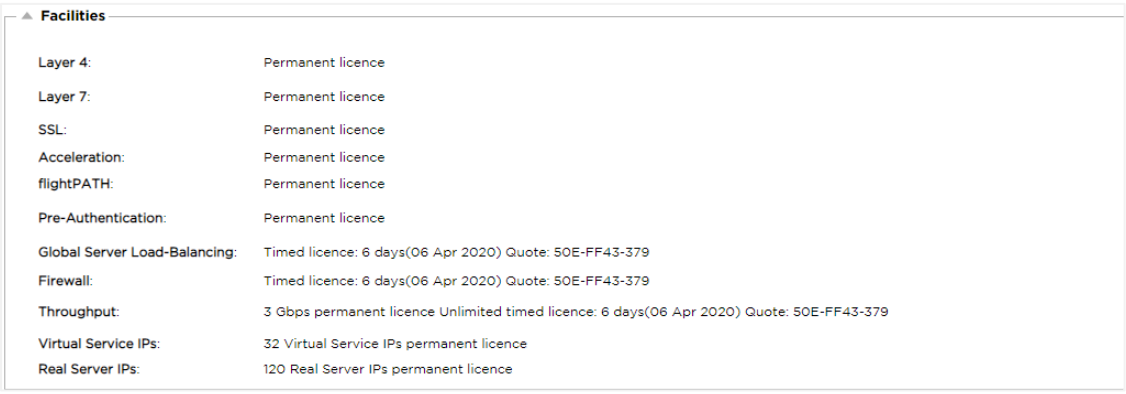
Проблемы с датой

Дата, на которую была выдана лицензия

Имя

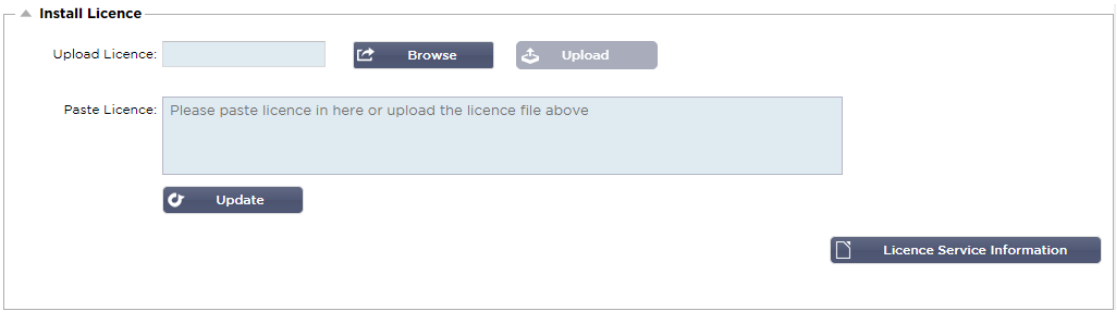
Это значение показывает описательное имя для ADC Appliance, которое Вы предоставили.

Удобства



Раздел средств предоставляет Вам информацию о том, какие функции в ADC были лицензированы для использования и срок действия лицензии. Также отображается пропускная способность, лицензированная для ADC, и количество Real Servers. Эта информация зависит от приобретенной Вами лицензии.

Установите лицензии



- Установка новой лицензии очень проста. Когда Вы получите от Edgenexus новую или запасную лицензию, она будет отправлена в виде текстового файла. Вы можете открыть этот файл, а затем скопировать и вставить его содержимое в поле Paste License.
- Вы также можете загрузить его в ADC, если копирование/вставка не является для Вас подходящим вариантом.
- Как только Вы это сделаете, пожалуйста, нажмите кнопку обновления
- Теперь лицензия установлена.

Информация о лицензионной службе

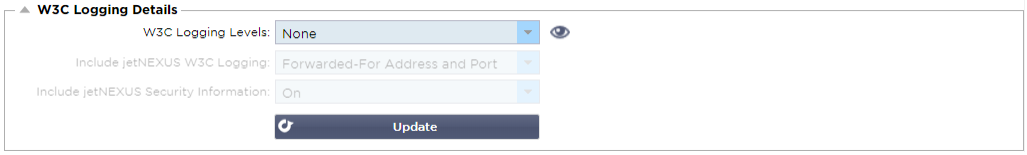
При нажатии на кнопку Информация об обслуживании лицензии отобразится вся информация о лицензии. Эта функция может быть использована для отправки сведений персоналу службы поддержки.

Ведение журнала

Страница Система > Ведение журнала позволяет Вам установить уровни ведения журнала W3C и указать удаленный сервер, на который будут автоматически экспортироваться журналы. Страница состоит из четырех разделов, приведенных ниже.

Детали протоколирования W3C

Включение регистрации W3C приведет к тому, что АЦП начнет записывать файл журнала, совместимый с W3C. Журнал W3C - это журнал доступа для веб-серверов, в котором создаются текстовые файлы, содержащие данные о каждом запросе доступа, включая исходный IP-адрес, версию HTTP, тип браузера, ссылающуюся страницу и отметку времени. Формат был разработан World Wide Web Consortium (W3C), организацией, которая продвигает стандарты для развития Интернета. Файл представляет собой текст в формате ASCII с колонками, разделенными пробелами. В файле содержатся строки комментариев, начинающиеся с символа #. Одна из этих строк комментариев - это строка, указывающая поля (дающая имена столбцов), чтобы данные можно было добывать. Существуют отдельные файлы для протоколов HTTP и FTP.



Уровни протоколирования W3C

Существуют различные уровни протоколирования, и в зависимости от типа услуги предоставляемые данные различаются.

В таблице ниже описаны уровни протоколирования для W3C HTTP.

Значение	Описание
Нет	Журналирование W3C выключено.
Кратко	Присутствуют следующие поля: #Поля: time c-ip c-port s-ip method uri x-c-version x-r-version sc-status cs-bytes sr-bytes rs-bytes sc-bytes x-percent time-taken x- round-trip-time cs(User-Agent) x-sc(Content-Type).
Полный	Это более совместимый с процессором формат с отдельными полями даты и времени. Информацию о значении полей см. ниже. Присутствуют следующие поля: #Поля: дата время c-ip c-port cs-username s-ip s-port cs-method cs-uri-stem cs-ur- -query sc-status cs(User-Agent) referer x-c-version x-r-version cs-bytes sr-bytes rs-bytes sc-bytes x-percent time-taken x-roun-trip-time x-sc(Content-Type).
Сайт	Этот формат очень похож на "Полный", но имеет дополнительное поле. Смотрите краткое описание полей ниже для получения информации о том, что эти поля означают. Присутствуют следующие поля: #Поля: дата время x-mil c-ip c-port cs-username s-ip s-port cs-host cs-method cs-uri-stem cs-ur--query sc-status cs(User-Agent) referer x-c-version x-r-version cs-bytes sr-bytes rs-bytes sc-bytes x-percent time-taken x-round-trip-time x-sc(Content-Type).
Диагностика	Этот формат заполняется всевозможной информацией, имеющей отношение к развитию и вспомогательному персоналу. Информацию о том, что означают те или иные поля, см. в кратком описании полей ниже. Присутствуют следующие поля: #Поля: дата время c-ip c-port cs-username s-ip s-port x-xff x-xffcustom cs-host x-r-ip x-r-port cs-method cs-uri-stem cs-uri-query sc-status cs(User-Agent) referer x-c-version x-r-version cs-bytes sr-bytes rs-bytes sc-bytes x-percent time-taken x-round-trip-time x-trip-times(new,rcon,rqf,rql,tqf,tql,rsf,rsl,tsf,tsl,dis,log) x-closed-by x- compress-action x-sc(Content-Type) x-cache-action X-finish

В таблице ниже описаны уровни протоколирования для W3C FTP.

Значение	Описание
Кратко	#Поля: дата время c-ip c-port s-ip s-port r-ip r-port cs-method cs-param sc-status sc-param sr-method sr-param rs-status rs-param
Полный	#Поля: дата время c-ip c-port s-ip s-port r-ip r-port cs-method cs-param cs-bytes sc-status sc-param sc-bytes sr-method sr-param sr-bytes rs-status rs-param rs-bytes
Диагностика	#Поля: дата время c-ip c-port s-ip s-port r-ip r-port cs-method cs-param cs-bytes sc-status sc-param sc-bytes sr-method sr-param sr-bytes rs-status rs-param rs-bytes

Включить протоколирование W3C

Эта опция позволяет Вам установить, какая информация об АЦП должна быть включена в журналы W3C.

Значение	Описание
Сетевой адрес и порт клиента	Значение, показанное здесь, отображает фактический IP-адрес клиента вместе с портом.
Сетевой адрес клиента	Эта опция будет включать и показывать только фактический IP-адрес клиента.
Адрес и порт для переадресации	Эта опция покажет детали, содержащиеся в заголовке XFF, включая адрес и порт.
Адрес для переадресации	Эта опция покажет детали, содержащиеся в заголовке XFF, включая только адрес.

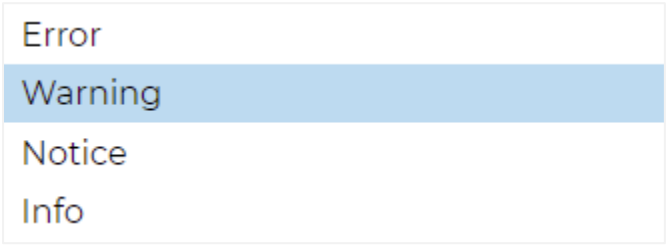
Включите информацию о безопасности

Это меню состоит из двух опций:

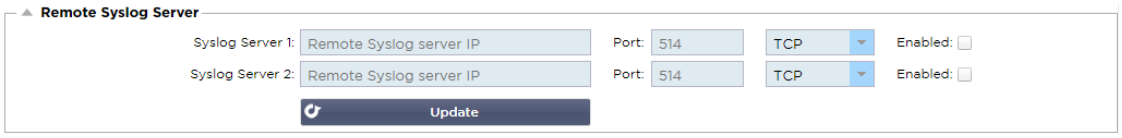
Значение	Описание
На сайте	Этот параметр является глобальным. Если установлено значение on, имя пользователя будет добавлено в журнал W3C, когда любая виртуальная служба использует аутентификацию и у нее включено ведение журнала W3C.
На сайте	Это отключит возможность регистрировать имя пользователя в журнале W3C на глобальном уровне.

Сервер Syslog

Этот раздел позволяет Вам установить уровень регистрации сообщений, передаваемых на сервер SYSLOG. Доступны следующие опции.



Удаленный сервер Syslog



В этом разделе Вы можете настроить два внешних сервера Syslog для отправки всех системных журналов.

- Добавьте IP-адрес Вашего сервера Syslog
- Добавить порт
- Выберите, что Вы хотите использовать: TCP или UDP
- Поставьте галочку в поле Включено, чтобы начать ведение журнала
- Нажмите Обновить

Удаленное хранение журналов

Все журналы W3C сохраняются в сжатом виде на ADC каждый час. Самые старые файлы будут удалены, когда останется 30% дискового пространства. Если Вы хотите экспортировать их на удаленный сервер для хранения, Вы можете настроить это с помощью общего ресурса SMB. Обратите внимание, что журнал W3C не будет передан на удаленное место, пока файл не будет завершен и сжат. Поскольку журналы записываются каждый час, это может занять до двух часов в устройстве на виртуальной машине и до пяти часов в аппаратном устройстве.

Мы включим кнопку тестирования в будущие релизы, чтобы обеспечить обратную связь, чтобы убедиться, что Ваши настройки верны.

Col1	Col2
Удаленное хранение журналов	Поставьте галочку, чтобы включить удаленное хранение журналов
IP-адрес	Укажите IP-адрес Вашего SMB-сервера. Он должен быть указан в десятичной точечной системе счисления. Пример: 10.1.1.23
Имя акции	Укажите имя общего ресурса на SMB-сервере. Пример: w3c.
Каталог	Укажите каталог на SMB-сервере. Пример: /log.
Имя пользователя	Укажите имя пользователя для общего ресурса SMB.
Пароль	Укажите пароль для общего ресурса SMB

Краткое описание поля

Состояние	Описание
Дата	Не локализовано = всегда ГГГГ-ММ-ДД (GMT/UTC)
Время	Не локализовано = HH:MM:SS или HH:MM:SS.ZZZ (GMT/UTC) * Примечание - к сожалению, это имеет два формата (Сайт
	не имеет .ZZZ миллисекунд).
x-mil	Только формат сайта = миллисекунда метки времени
c-ip	IP-адрес клиента, насколько это возможно определить из сети или заголовка X-Forwarded-For
c-port	Порт клиента, насколько это возможно определить из сети или заголовка X-Forwarded-For
cs-username	Поле запроса имени пользователя клиента
s-ip	Порт прослушивания ALB
s-port	ALB's listening VIP
x-xff	Значение заголовка X-Forwarded-For
x-xffcustom	Значение заголовка запроса типа X-Forwarded-For типа configured-named
cs-host	Имя хоста в запросе
x-r-ip	IP-адрес используемого сервера Real Server
x-r-port	Используемый порт реального сервера
cs-метод	Метод запроса HTTP * кроме формата Brief
метод	* Только в кратком формате используется это имя для cs-метода
cs-uri-stem	Путь запрашиваемого ресурса * кроме формата Brief
cs-uri-query	Запрос на запрашиваемый ресурс * кроме формата Brief
uri	* краткий формат регистрирует комбинированный путь и запрос-строку
sc-status	Код ответа HTTP
cs(User-Agent)	Строка User-Agent браузера (как отправлено клиентом)
референт	Ссылающаяся страница (как отправлено клиентом)
x-c-версия	Запрос клиента Версия HTTP
x-r-version	Содержание-Ответ сервера Версия HTTP
cs-bytes	Байты от клиента, в запросе
sr-bytes	Байты, переданные серверу Real Server, в запросе
rs-bytes	Байты с реального сервера, в ответе
sc-bytes	Байты, отправленные клиенту, в ответе
x-процент	Процент сжатия * = 100 * (1 - выход / вход), включая заголовки
по времени	Сколько времени занял сервер Real Server в секундах
x-trip-times new pcon	миллисекунда с момента подключения до публикации в "списке новичков" миллисекунда с момента подключения до установки соединения с сервером Real Server

acon	миллисекунда с момента подключения до завершения установки соединения с сервером Real Server
rcon	миллисекунда с момента подключения до установления соединения с реальным сервером
rqf	миллисекунда с момента подключения до получения первого байта запроса от клиента
rql	миллисекунда с момента подключения до получения последнего байта запроса от клиента
tqf	миллисекунда с момента подключения до отправки первого байта запроса на Real Server
tql	миллисекунда с момента подключения до отправки последнего байта запроса на Real Server
pcф	миллисекунда с момента подключения до получения первого байта ответа от Реального сервера
rsl	миллисекунда с момента подключения до получения последнего байта ответа от Реального сервера
цф	миллисекунда с момента подключения до отправки первого байта ответа клиенту
цл	миллисекунда с момента подключения до отправки последнего байта ответа клиенту
dis	миллисекунда от подключения до отключения (обе стороны - последняя отключилась)
журнал	миллисекунд с момента подключения к этой записи журнала обычно следует (Политика балансировки нагрузки и обоснование)
x-round-trip-time	Сколько времени занял ALB в секундах
x-closed-by	Какое действие вызвало закрытие (или сохранение открытым) соединения
x-compress-action	Как осуществлялось или предотвращалось сжатие
x-sc(Content-Type)	Content-Type ответа
x-cache-action	Как реагировало или было предотвращено кэширование
x-finish	Триггер, который вызвал эту строку журнала

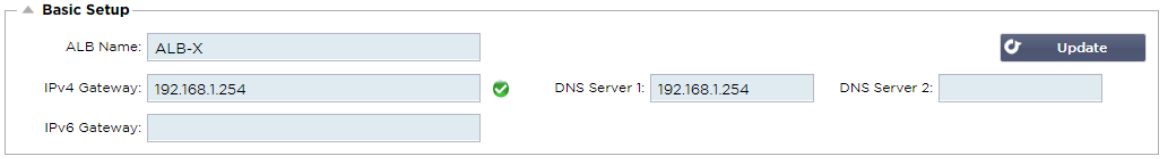
Очистить файлы журнала

Эта функция позволяет Вам очистить файлы журналов с АЦП. Вы можете выбрать тип журнала, который Вы хотите удалить, из выпадающего меню, а затем нажмите кнопку Очистить.

Сеть

Раздел Сеть в Библиотеке позволяет конфигурировать сетевые интерфейсы АЦП и их поведение.

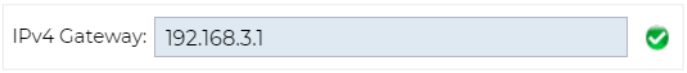
Основная настройка



Название АЛБ

Укажите имя для Вашего устройства ADC. Обратите внимание, что его нельзя изменить, если в кластере более одного участника. См. раздел "Кластеризация".

Шлюз IPv4



Укажите адрес шлюза IPv4. Этот адрес должен находиться в той же подсети, что и существующий адаптер. Если Вы неправильно добавили шлюз, Вы увидите белый крестик в красном круге. Когда Вы добавите правильный шлюз, Вы увидите зеленый баннер успеха внизу страницы и белую галочку в зеленом круге рядом с IP-адресом.

Шлюз IPv6

Укажите адрес шлюза IPv6. Этот адрес должен находиться в той же подсети, что и существующий адаптер. Если Вы неправильно добавили шлюз, Вы увидите белый крестик в красном круге. Когда Вы добавите правильный шлюз, Вы увидите зеленый баннер успеха внизу страницы и белую галочку в зеленом круге рядом с IP-адресом.

DNS-сервер 1 и DNS-сервер 2

Добавьте IPv4-адрес Вашего первого и второго (по желанию) DNS-сервера.

Адаптер Подробнее

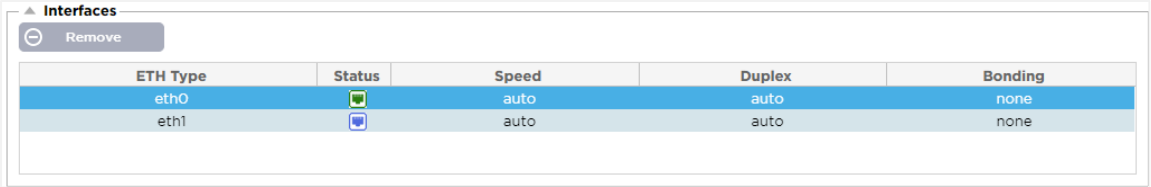
В этом разделе панели Сеть показаны сетевые интерфейсы, установленные в Вашем устройстве ADC. Вы можете добавлять и удалять адаптеры по мере необходимости.

Колонка	Описание
Адаптер	В этой колонке отображаются физические адаптеры, установленные на Вашем устройстве. Выберите адаптер из списка доступных адаптеров, щелкнув по нему - двойной щелчок переведет строку списка в режим редактирования.
VLAN	Дважды щелкните, чтобы добавить идентификатор VLAN для адаптера. VLAN - это виртуальная локальная сеть, которая создает отдельный широковещательный домен. VLAN имеет те же атрибуты, что и физическая локальная сеть, но позволяет более легко группировать конечные станции, если они не находятся на одном сетевом коммутаторе.
IP-адрес	Дважды щелкните, чтобы добавить IP-адрес, связанный с интерфейсом адаптера. Вы можете добавить несколько IP-адресов к одному и тому же

	интерфейсу. Это должно быть 32-битное число IPv4 в четырех точечной десятичной системе счисления. Пример 192.168.101.2
Маска подсети	Дважды щелкните, чтобы добавить маску подсети, назначенную интерфейсу адаптера. Это должно быть 32-битное число IPv4 в четырехточечной десятичной системе счисления. Пример 255.255.255.0
Шлюз	Добавьте шлюз для интерфейса. При его добавлении ADC установит простую политику, которая позволит соединениям, инициированным с этого интерфейса, возвращаться через этот интерфейс на указанный шлюз-маршрутизатор. Это позволяет устанавливать ADC в более сложных сетевых средах без необходимости вручную настраивать сложную маршрутизацию на основе политики.
Описание	Дважды щелкните, чтобы добавить описание для Вашего адаптера. Пример Публичный интерфейс. Примечание: АЦП автоматически назовет первый интерфейс "Зеленая сторона", второй интерфейс "Красная сторона", третий интерфейс "Сторона 3" и т.д. Пожалуйста, не стесняйтесь изменять эти соглашения об именовании по своему усмотрению.
Веб-консоль	Дважды щелкните по столбцу, затем установите флажок, чтобы назначить этот интерфейс в качестве адреса управления для Web-консоли графического интерфейса пользователя. Пожалуйста, будьте очень внимательны при изменении интерфейса, на котором будет прослушиваться Web-консоль. Вам потребуется правильная настройка маршрутизации или нахождение в той же подсети, что и новый интерфейс, чтобы после изменения можно было связаться с Web-консолью. Единственный способ изменить это обратно - зайти в командную строку и выполнить команду set greenside. Это приведет к удалению всех интерфейсов, кроме eth0.

Интерфейсы

Раздел Интерфейсы на панели Сеть позволяет настроить определенные элементы, относящиеся к сетевому интерфейсу. Вы также можете удалить сетевой интерфейс из списка, нажав кнопку Удалить. При использовании виртуального устройства интерфейсы, которые Вы видите здесь, ограничены базовой структурой виртуализации.



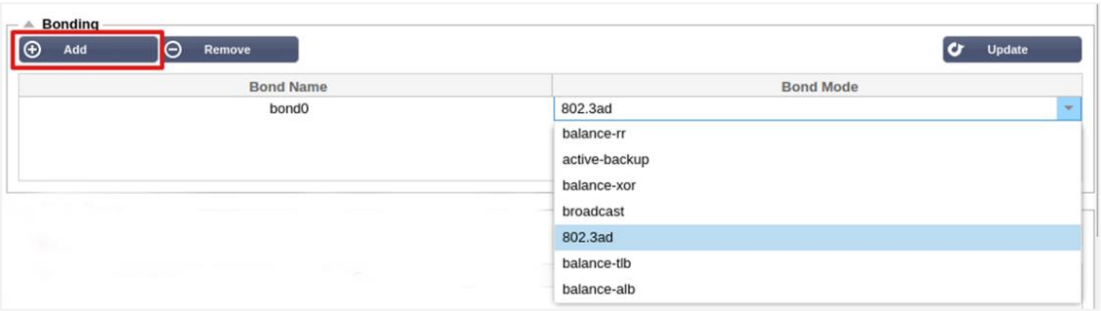
Колонка	Описание
Тип ETH	Это значение указывает на внутреннюю ссылку ОС на сетевой интерфейс. Это поле не может быть настроено. Значения начинаются с ETH0 и далее по порядку в зависимости от количества сетевых интерфейсов.
Статус	Эта графическая индикация показывает текущее состояние сетевого интерфейса. Зеленый статус показывает, что интерфейс подключен и работает. Другие индикаторы состояния показаны ниже.  **Адаптер UP**  Адаптер вниз  Адаптер отключен от сети  Отсутствие адаптера
Скорость	По умолчанию это значение установлено на автосогласование скорости. Но Вы можете изменить сетевую скорость интерфейса на любое значение, доступное в выпадающем списке (10/100/1000/AUTO).
Дуплекс	Значение этого поля настраивается, и Вы можете выбрать между Авто (по умолчанию), Полнодуплексный и Полудуплексный.
Связывание	Вы можете выбрать один из типов связывания, которые Вы определили. Более подробную информацию смотрите в разделе "Связывание".

Связывание

Для обозначения объединения сетевых интерфейсов используется множество названий: Port Trunking, Channel Bonding, Link Aggregation, NIC teaming и другие. Объединение объединяет или агрегирует несколько сетевых соединений в один интерфейс с объединенным каналом. Объединение позволяет двум или более сетевым интерфейсам действовать как один, увеличивать пропускную способность, обеспечивать избыточность или отказоустойчивость.

Ядро ADC имеет встроенный драйвер Bonding для объединения нескольких физических сетевых интерфейсов в один логический интерфейс (например, объединение eth0 и eth1 в bond0). Для каждого объединенного интерфейса Вы можете определить режим работы и параметры мониторинга соединения. Существует семь различных режимов, каждый из которых обеспечивает определенные характеристики балансировки нагрузки и отказоустойчивости. Они показаны на изображении ниже.

ПРИМЕЧАНИЕ: СВЯЗЫВАНИЕ МОЖЕТ БЫТЬ НАСТРОЕНО ТОЛЬКО ДЛЯ АППАРАТНЫХ УСТРОЙСТВ АЦП.



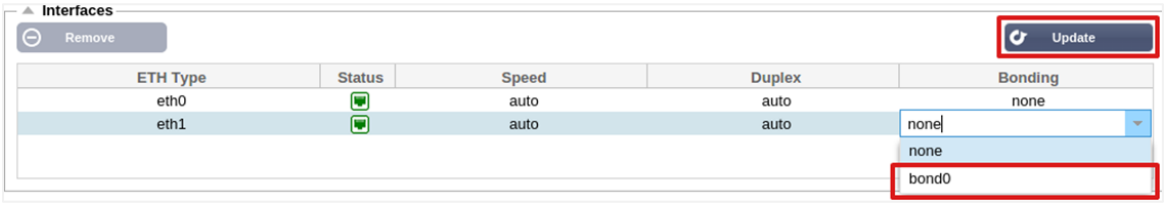
Создание профиля Bonding

- Нажмите на кнопку Добавить, чтобы добавить новую облигацию
- Укажите имя для конфигурации связывания

- Выберите, какой режим склеивания Вы хотите использовать

Затем в разделе Interfaces выберите режим Bonding, который Вы хотите использовать, в раскрывающемся поле Bond для сетевого интерфейса.

В приведенном ниже примере eth0, eth1 и eth2 теперь являются частью bond0. В то время как Eth0 остается сам по себе в качестве интерфейса управления.

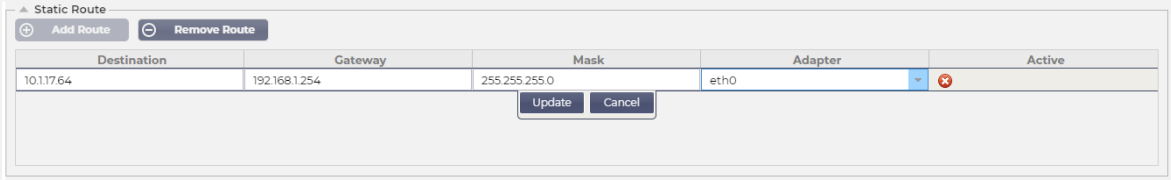


Режимы связывания

Режим скрепления	Описание
баланс-рр:	Пакеты последовательно передаются/принимаются через каждый интерфейс один за другим.
активное резервное копирование:	В этом режиме один интерфейс будет активным, а второй интерфейс будет находиться в режиме ожидания. Этот вторичный интерфейс становится активным только в случае сбоя активного соединения на первом интерфейсе.
баланс - иксор:	Передача на основе MAC-адреса источника, XOR'd с MAC-адресом назначения. Эта опция выбирает одного и того же ведомого для каждого Mac-адреса назначения.
трансляция:	В этом режиме все данные будут передаваться по всем ведомым интерфейсам.
802.3ad:	Создает группы агрегации, которые имеют одинаковые настройки скорости и дуплекса и используют все ведомые устройства в активном агрегаторе в соответствии со спецификацией 802.3ad.
баланс - ТЛБ:	Режим склеивания с адаптивной балансировкой нагрузки на передачу: Обеспечивает объединение каналов, не требующее специальной поддержки коммутатора. Исходящий трафик распределяется в соответствии с текущей нагрузкой (вычисленной относительно скорости) на каждом ведомом устройстве. Текущий ведомый получает входящий трафик. Если принимающее ведомое устройство выходит из строя, другое ведомое устройство принимает MAC-адрес вышедшего из строя принимающего ведомого устройства.
balance-alb:	Адаптивный режим балансировки нагрузки: также включает balance-tlb плюс балансировку принимаемой нагрузки (rlb) для трафика IPV4 и не требует специальной поддержки коммутатора. Балансировка нагрузки на прием достигается путем ARP переговоров. Драйвер бондинга перехватывает ARP-ответы, отправленные локальной системой, и перезаписывает аппаратный адрес источника уникальным аппаратным адресом одного из ведомых устройств в бондинге, таким образом, что разные ведомые устройства используют разные аппаратные адреса для сервера.

Статический маршрут

Бывают случаи, когда Вам необходимо создать статические маршруты для определенных подсетей в Вашей сети. ADC предоставляет Вам возможность сделать это с помощью модуля Статические маршруты.



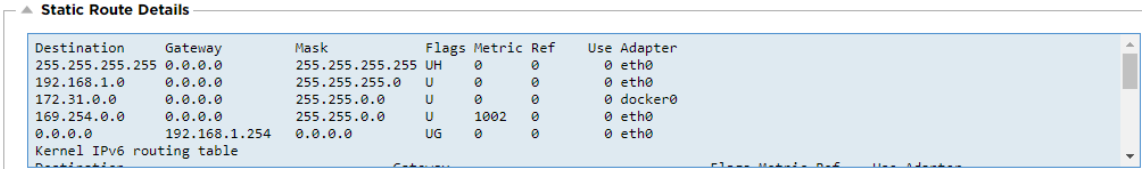
Добавление статического маршрута

- Нажмите кнопку Добавить маршрут
- Заполните поле, используя в качестве руководства данные, приведенные в таблице ниже.
- Нажмите кнопку Обновить, когда закончите.

Поле	Описание
Место назначения	Введите сетевой адрес назначения в десятичной точечной нотации. Пример 123.123.123.5
Шлюз	Введите IPv4-адрес шлюза в десятичной точечной нотации. Пример 10.4.8.1
Маска	Введите маску подсети назначения в десятичной точечной нотации. Пример 255.255.255.0
Адаптер	Введите адаптер, через который можно связаться со шлюзом. Пример eth1.
Активный	Зеленая галочка означает, что шлюз может быть достигнут. Красный крестик будет означать, что шлюз не может быть достигнут на данном интерфейсе. Убедитесь, что Вы настроили интерфейс и IP-адрес в той же сети, что и шлюз.

Детали статического маршрута

В этом разделе будет представлена информация обо всех маршрутах, настроенных на АЦП.



Расширенные сетевые настройки

Что такое Нагле?

Алгоритм Нагла повышает эффективность сетей TCP/IP за счет уменьшения количества пакетов, которые необходимо пересылать по сети. См. **СТАТЬЮ ВИКИПЕДИИ О НАГЛЕ**

Сервер Нагл

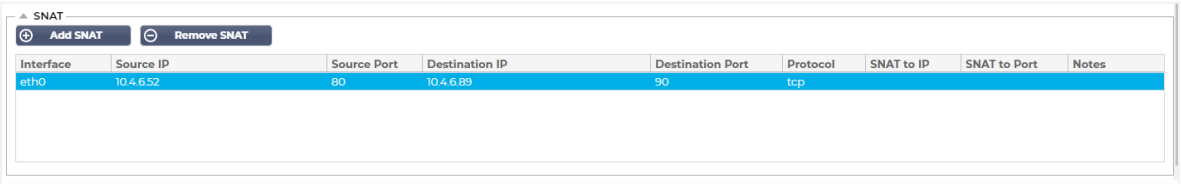
Поставьте галочку в этом поле, чтобы включить настройку Server Nagle. Server Nagle - это средство повышения эффективности сетей TCP/IP путем уменьшения количества пакетов, которые должны быть отправлены по сети. Эта настройка применяется к серверной стороне транзакции. С

настройками сервера следует быть осторожным, так как Nagle и отложенный ACK могут сильно повлиять на производительность.

Клиент Нагле

Поставьте галочку, чтобы включить настройку Client Nagle. Как и выше, но применяется к клиентской стороне транзакции.

SNAT



SNAT расшифровывается как Source Network Address Translation, и разные производители имеют небольшие различия в реализации SNAT. Простое объяснение SNAT для EdgeADC может быть следующим.

При нормальных обстоятельствах входящие запросы будут направлены на VIP, который будет видеть IP-адрес источника запроса. Так, например, если конечная точка браузера имеет IP-адрес 81.71.61.51, это будет видно VIP-клиенту.

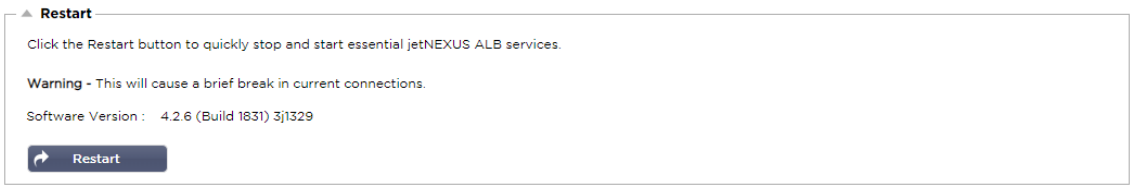
Когда SNAT в действии, исходный IP-адрес источника запроса будет скрыт от VIP, и вместо него он будет видеть IP-адрес, указанный в правиле SNAT. Таким образом, SNAT можно использовать в режимах балансировки нагрузки 4-го и 7-го уровней.

Поле	**Описание**
Источник IP	IP-адрес источника является необязательным и может быть либо сетевым IP-адресом (с /mask), либо обычным IP-адресом. Маска может быть либо сетевой маской, либо обычным числом, указывающим количество единиц в левой части сетевой маски. Таким образом, маска /24 эквивалентна 255.255.255.0.
IP-адрес назначения	IP-адрес назначения является необязательным и может быть либо сетевым IP-адресом (с /mask), либо обычным IP-адресом. Маска может быть либо сетевой маской, либо обычным числом, указывающим количество единиц в левой части сетевой маски. Таким образом, маска /24 эквивалентна 255.255.255.0.
Порт источника	Порт источника необязателен, он может быть одним числом, в этом случае он определяет только этот порт, или он может включать двоеточие, что определяет диапазон портов. Примеры: 80 или 5900:5905.
Порт назначения	Порт назначения является необязательным, он может быть одним числом, в этом случае он определяет только этот порт, или он может включать двоеточие, которое определяет диапазон портов. Примеры: 80 или 5900:5905.
Протокол	Вы можете выбрать, использовать SNAT на одном протоколе или на всех протоколах. Мы рекомендуем быть конкретными, чтобы быть более точными.
SNAT - IP	SNAT to IP - это обязательный IP-адрес или диапазон IP-адресов. Примеры: 10.0.0.1 или 10.0.0.1-10.0.0.3.
SNAT к порту	SNAT to Port является необязательным, он может быть одним числом, в этом случае он определяет только этот порт, или он может включать тире, что определяет диапазон портов. Примеры: 80 или 5900-5905.
Примечания	Используйте это, чтобы дать дружественное имя, чтобы напомнить себе, почему правила существуют. Это также полезно для отладки в Syslog.

Мощность

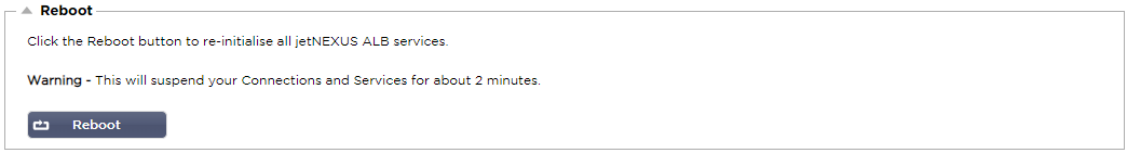
Эта функция системы АЦП также позволяет Вам выполнять несколько задач, связанных с питанием Вашего АЦП.

Перезапустите



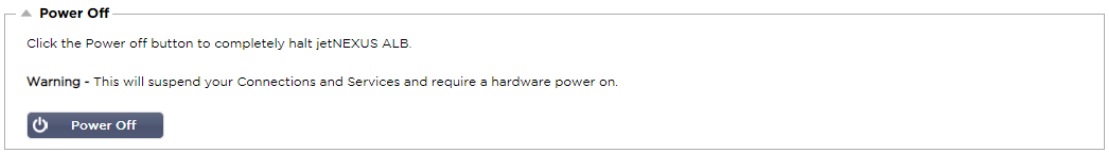
Эта настройка инициирует глобальный перезапуск всех Служб и, соответственно, разрывает все активные в данный момент соединения. Все Службы автоматически возобновят работу через некоторое время, но время будет зависеть от того, сколько Служб настроено. Появится всплывающее окно, запрашивающее подтверждение действия перезапуска.

Перезагрузка



Нажатие кнопки Перезагрузка приведет к циклу питания АЦП и автоматически вернет его в активное состояние. Появится всплывающее окно с запросом подтверждения действия перезагрузки.

Выключение питания



Нажатие на кнопку Выключить питание выключит АЦП. Если это аппаратное устройство, Вам потребуется физический доступ к устройству, чтобы включить его снова. Появится всплывающее окно с запросом подтверждения действия выключения.

Безопасность

Этот раздел позволяет Вам изменить пароль веб-консоли, а также включить или отключить доступ к Secure Shell. Он также позволяет включить возможность REST API.

SSH

Вариант	Описание
Удаленное подключение Secure Shell	Поставьте галочку, если Вы хотите получить доступ к АЦП с помощью SSH. "Putty" - отличное приложение для этого.

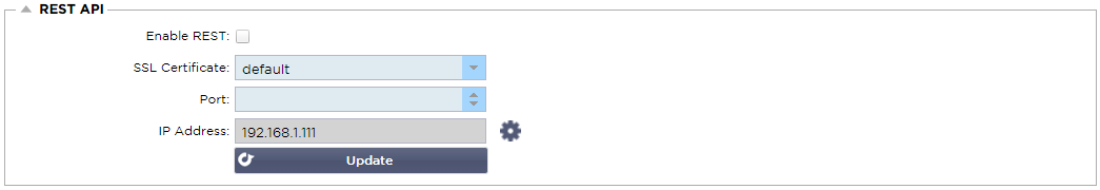
Веб-консоль

SSL-сертификат Выберите сертификат из выпадающего списка. Выбранный Вами сертификат будет использоваться для защиты Вашего соединения с пользовательским веб-интерфейсом АЦП. Вы можете создать самоподписанный сертификат в АЦП или импортировать его из раздела **SSL-СЕРТИФИКАТЫ**.

Вариант	Описание
Защищенный порт	Порт по умолчанию для веб-консоли - TCP 443. Если Вы хотите использовать другой порт по соображениям безопасности, Вы можете изменить его здесь.

REST API

REST API, также известный как RESTful API, является интерфейсом прикладного программирования, который соответствует архитектурному стилю REST и позволяет конфигурировать АЦП или извлекать данные из АЦП. Термин REST расшифровывается как representational state transfer и был создан компьютерным ученым Роем Филдингом.



Вариант	Описание
Включить REST	Поставьте галочку в этом поле, чтобы включить доступ с помощью REST API. Обратите внимание, что Вам также придется настроить, на каком адаптере включен REST. См. примечание по ссылке Cog ниже.
SSL-сертификат	Выберите сертификат для службы REST. В раскрывающемся списке будут показаны все сертификаты, установленные на ADC.
Порт	Установите порт для службы REST. Хорошей идеей будет использовать порт, отличный от 443.
IP-адрес	Здесь будет показан IP-адрес, к которому привязана служба REST. Вы можете нажать на ссылку Cog для доступа к странице Сеть, чтобы изменить, на каком адаптере включена служба REST.
Зубчатое звено	Щелкнув по этой ссылке, Вы перейдете на страницу Сеть, где Вы можете настроить адаптер для REST.

Документация для REST API

Документация по использованию REST API доступна: **jetAPI | 4.2.3 | jetNEXUS | SwaggerHub**

Примечание: Если Вы получаете ошибки на странице Swagger, это связано с тем, что у них есть проблемы с поддержкой строк запросов.
Прокрутите страницу мимо ошибок, чтобы перейти к jetNEXUS REST API

Примеры

GUID с помощью CURL:

- Команда

curl -k HTTPs://<rest ip>/POST/32 -H "Content-Type: application/json" -X POST -d '{"<rest username>":"<password>"}''

- вернется

{ "Loginstatus": "OK", "Username": "<имя пользователя>", "GUID": "<guid>"}

- Валидность
  - GUID действителен в течение 24 часов

Детали лицензии

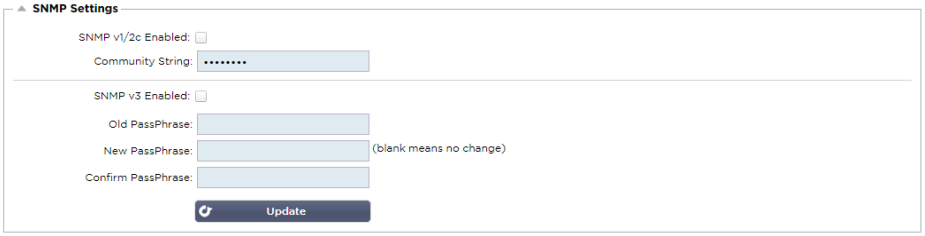
- Команда

curl -k HTTPs://<rest ip>/GET/39 -GET -b 'GUID=<guid;>

SNMP

Раздел SNMP позволяет конфигурировать SNMP MIB, находящуюся внутри АЦП. Затем MIB может быть запрошена сторонним программным обеспечением, способным взаимодействовать с устройствами, оснащенными SNMP.

Настройки SNMP



Вариант	Описание
SNMP v1 / V2C	Поставьте галочку, чтобы включить V1/V2C MIB. SNMP v1 соответствует RFC-1157. SNMP V2c соответствует RFC-1901-1908.
SNMP v3	Поставьте галочку, чтобы включить V3 MIB. RFC-3411-3418. Имя пользователя для v3 - admin. Пример:- snmpwalk -v3 -u admin -A jetnexus -l authNoPriv 192.168.1.11 1.3.6.1.4.1.38370
Строка сообщества	Это строка только для чтения, установленная на агенте и используемая менеджером для получения информации SNMP. Строка сообщества по умолчанию - jetnexus
PassPhrase	Это пароль, необходимый при включенном SNMP v3, который должен состоять не менее чем из 8 символов и содержать только буквы Aa-Zz и цифры 0-9. Парольная фраза по умолчанию - **jetnexus**

SNMP MIB

Информация, доступная для просмотра по SNMP, определяется базой управленческой информации (MIB). MIB описывают структуру данных управления и используют иерархические идентификаторы объектов (OID). Каждый OID может быть прочитан через приложение управления SNMP.

Скачать MIB

MIB можно загрузить здесь:

OID АЦП

КОРНЕВОЙ ИДЕНТИФИКАТОР

iso.org.dod.internet.private.enterprise = .1.3.6.1.4.1

Наши OID

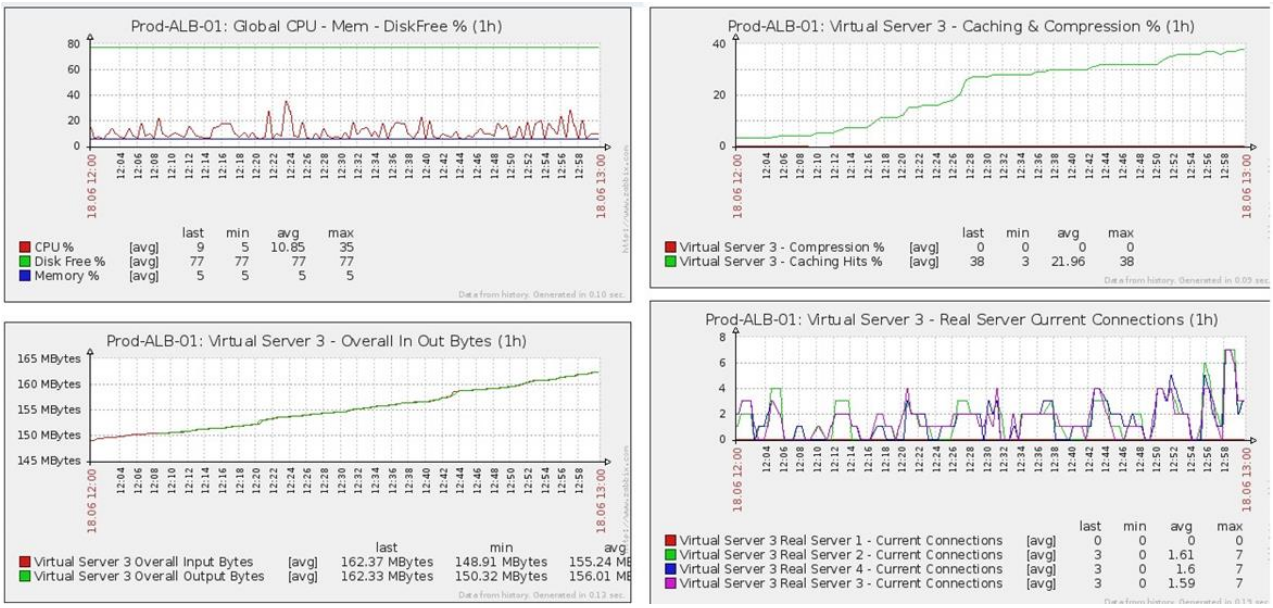
.38370 jetnexusMIB
.1 **jetnexusData (1**.3.6.1.4.1.38370.1)
.1 **jetnexusGlobal (1**.3.6.1.4.1.38370.1.1)
.2 **jetnexusVirtualServices (1**.3.6.1.4.1.38370.1.2)
.3 **jetnexusServers (1**.3.6.1.4.1.38370.1.3)
.1 **jetnexusGlobal (1**.3.6.1.4.1.38370.1.1)
.1 **jetnexusOverallInputBytes (1**.3.6.1.4.1.38370.1.1.1.0)
.2 **jetnexusOverallOutputBytes (1**.3.6.1.4.1.38370.1.1.2.0)
.3 **jetnexusCompressedInputBytes (1**.3.6.1.4.1.38370.1.1.3.0)
. 4 **jetnexusCompressedOutputBytes (1**.3.6.1.4.1.38370.1.1.4.0)
. 5 **jetnexusVersionInfo (1**.3.6.1.4.1.38370.1.1.5.0)
.6 **jetnexusTotalClientConnections (1**.3.6.1.4.1.38370.1.1.6.0)
.7 **jetnexusCpuPercent (1**.3.6.1.4.1.38370.1.1.7.0)
.8 **jetnexusDiskFreePercent (1**.3.6.1.4.1.38370.1.1.8.0)
.9 **jetnexusMemoryPercent (1**.3.6.1.4.1.38370.1.1.9.0)
.10 **jetnexusCurrentConnections (1**.3.6.1.4.1.38370.1.1.10.0)

.2 **jetnexusVirtualServices (1**.3.6.1.4.1.38370.1.2)
.1 **jnvirtualserviceEntry (1**.3.6.1.4.1.38370.1.2.1)
.1 **jnvirtualserviceIndexvirtualservice (1**.3.6.1.4.1.38370.1.2.1.**1**)
.2 **jnvirtualserviceVSAddrPort (1**.3.6.1.4.1.38370.1.2.1.**2**)
.3 **jnvirtualserviceOverallInputBytes (1**.3.6.1.4.1.38370.1.2.1.**3**)
.4 **jnvirtualserviceOverallOutputBytes (1**.3.6.1.4.1.38370.1.2.1.**4**)
. 5 **jnvirtualserviceCacheBytes (1**.3.6.1.4.1.38370.1.2.1.**5**)
.6 **jnvirtualserviceCompressionPercent (1**.3.6.1.4.1.38370.1.2.1.**6**)
.7 **jnvirtualservicePresentClientConnections (1**.3.6.1.4.1.38370.1.2.1.**7**)
.8 **jnvirtualserviceHitCount (1**.3.6.1.4.1.38370.1.2.1.**8**)
.9 jnvirtualserviceCacheHits (1.3.6.1.4.1.38370.1.2.1.**9**)
. 10 **jnvirtualserviceCacheHitsPercent (1**.3.6.1.4.1.38370.1.2.1.**10**)
.11 **jnvirtualserviceVSStatus (1**.3.6.1.4.1.38370.1.2.1.**11**)

.3 **jetnexusRealServers (1**.3.6.1.4.1.38370.1.3)
.1 **jnrealserverEntry (1**.3.6.1.4.1.38370.1.3.**1**)
.1 **jnrealserverIndexVirtualService (1**.3.6.1.4.1.38370.1.3.1.**1**)
.2 **jnrealserverIndexRealServer (1**.3.6.1.4.1.38370.1.3.1.**2**)
.3 **jnrealserverChAddrPort (1**.3.6.1.4.1.38370.1.3.1.**3**)
. 4 **jnrealserverCSAddrPort (1**.3.6.1.4.1.38370.1.3.1.**4**)
.5 **jnrealserverOverallInputBytes (1**.3.6.1.4.1.38370.1.3.1.**5**)
.6 **jnrealserverOverallOutputBytes (1**.3.6.1.4.1.38370.1.3.1.**6**)
.7 **jnrealserverCompressionPercent (1**.3.6.1.4.1.38370.1.3.1.**7**)
.8 **jnrealserverPresentClientConnections (1**.3.6.1.4.1.38370.1.3.1.**8**)
. 9 **jnrealserverPoolUsage (1**.3.6.1.4.1.38370.1.3.1.**9**)
.10 **jnrealserverHitCount (1**.3.6.1.4.1.38370.1.3.1.**10**)
. 11 **jnrealserverRSStatus (1**.3.6.1.4.1.38370.1.3.1.**11**)

Исторические графики

Лучшее применение для пользовательской SNMP MIB АЦП - это возможность выгрузить исторические графики на консоль управления по Вашему выбору. Ниже приведены примеры из Zabbix, которые опрашивают АЦП для различных значений OID, перечисленных выше.



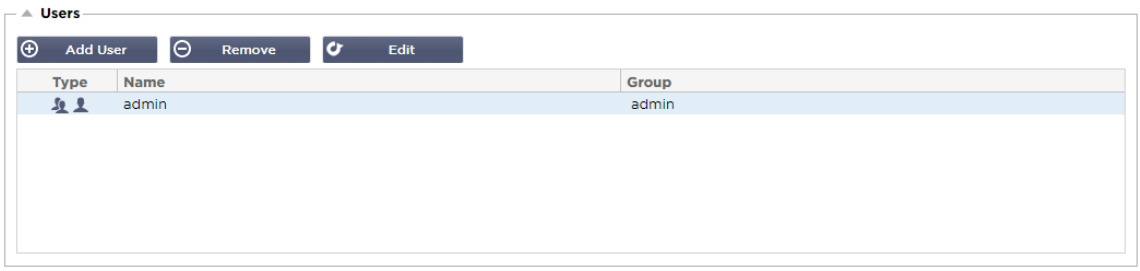
Пользователи и журналы аудита

АЦП предоставляет возможность иметь внутренний набор пользователей для настройки и определения того, что делает АЦП. Пользователи, определенные в АЦП, могут выполнять различные операции в зависимости от закрепленной за ними роли.

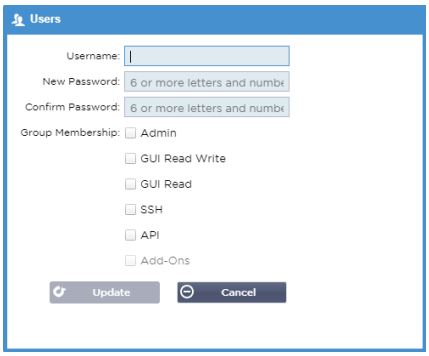
Существует пользователь по умолчанию под именем **admin**, которого Вы используете при первой настройке ADC. Пароль по умолчанию для admin - **jetnexus**.

Пользователи

Раздел Пользователи предназначен для создания, редактирования и удаления пользователей из ADC.



Добавить пользователя



Нажмите кнопку Добавить пользователя, показанную на изображении выше, чтобы открыть диалоговое окно добавления пользователя.

Параметр	Описание/использование
Имя пользователя	Введите имя пользователя по своему выбору Имя пользователя должно соответствовать следующим требованиям: • Минимальное количество символов 1 • Максимальное количество символов 32 • Буквы могут быть в верхнем и нижнем регистре • Можно использовать цифры • Символы не допускаются
Пароль	Введите **надежный** пароль, который соответствует приведенным ниже требованиям • Минимальное количество символов 6 • Максимальное количество символов 32 • Должны использовать хотя бы комбинацию букв и цифр • Буквы могут быть в верхнем или нижнем регистре • Символы разрешены, за исключением тех, которые приведены в примере ниже **£**, **%**, **& , < , >**
Подтверждение пароля	Подтвердите пароль еще раз, чтобы убедиться в его правильности
Членство в группе	Отметьте группу, к которой Вы хотите, чтобы принадлежал пользователь. • Администратор - Эта группа может делать все • GUI Read Write - Пользователи в этой группе могут получить доступ к графическому интерфейсу пользователя и вносить изменения через него. • GUI Read - Пользователи в этой группе могут получить доступ к графическому интерфейсу только для просмотра информации. Никакие изменения не могут быть сделаны • SSH - Пользователи этой группы могут получить доступ к АЦП через Secure Shell. Этот выбор даст доступ к командной строке, в которой имеется минимальный набор команд • API - Пользователи этой группы будут иметь доступ к программируемому интерфейсу SOAP и REST. REST будет доступен с версии программного обеспечения 4.2.1

Тип пользователя

Местный пользователь
ADC в роли Stand-Alone или Manual H/A будет создавать только локальных пользователей
По умолчанию локальный пользователь под именем "admin" **является членом группы admin. Для обратной совместимости этот пользователь никогда не может быть удален**
Вы можете изменить пароль этого пользователя или удалить его, **но Вы не можете удалить последнего локального администратора**

Пользователь кластера
Роль ADC в кластере будет создавать только пользователей кластера
Пользователи кластера синхронизируются по всем АЦП в кластере
Любое изменение пользователя кластера будет изменено для всех членов кластера
Если Вы вошли в систему как пользователь кластера, Вы не сможете переключать роли с кластера на Manual или Stand-Alone

Кластер и локальный пользователь
Любые пользователи, созданные в роли Stand-Alone или Manual, будут скопированы в кластер.
Если ADC впоследствии покинет кластер, то останутся только Локальные пользователи
Последний настроенный пароль для пользователя будет действительным

Удаление пользователя

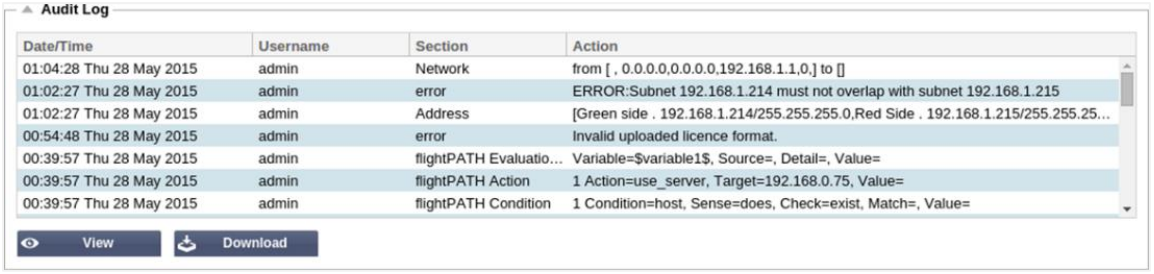
- Выделите существующего пользователя
- Нажмите кнопку Удалить
- Вы не сможете удалить пользователя, который в настоящее время входит в систему
- Вы не сможете удалить последнего локального пользователя в группе администраторов
- Вы не сможете удалить последнего оставшегося пользователя кластера в группе администраторов
- Вы не сможете удалить пользователя admin для обратной совместимости
- Если Вы удалите ADC из кластера, все пользователи, кроме локальных, будут удалены

Редактирование пользователя

- Выделите существующего пользователя
- Нажмите Редактировать
- Вы можете изменить членство пользователя в группе, отметив соответствующие поля и обновив
- Вы также можете изменить пароль пользователя, если у Вас есть права администратора

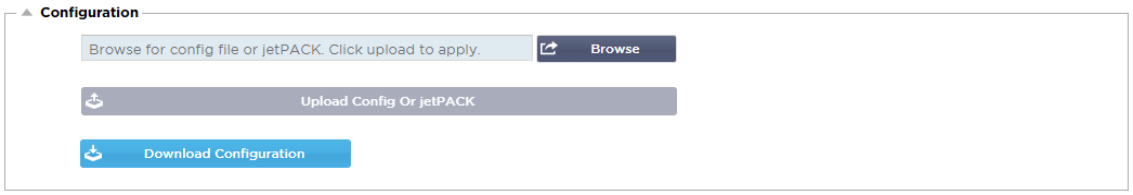
Журнал аудита

АЦП регистрирует изменения, внесенные в конфигурацию АЦП отдельными пользователями. В журнале аудита будут представлены последние 50 действий, выполненных всеми пользователями. Вы также можете увидеть ВСЕ записи в разделе **Журналы**. Например:



Расширенный

Конфигурация



Наилучшей практикой всегда является загрузка и сохранение конфигурации АЦП после того, как он полностью настроен и работает в соответствии с требованиями. Вы можете использовать модуль Configuration как для загрузки, так и для выгрузки конфигурации.

Jetpacks - это файлы конфигурации для стандартных приложений, которые предоставляются Edgenexus для упрощения Вашей работы. Их также можно загрузить в ADC с помощью модуля Configuration.

Файл конфигурации - это, по сути, текстовый файл, и как таковой, может быть отредактирован Вами с помощью текстового редактора, такого как Notepad++ или VI. После редактирования, файл конфигурации может быть загружен в АЦП.

Загрузка конфигурации

- Чтобы загрузить текущую конфигурацию АЦП, нажмите кнопку Загрузить конфигурацию.
- Появится всплывающее окно с предложением открыть или сохранить файл .conf.
- Сохраните в удобном месте.
- Вы можете открыть его с помощью любого текстового редактора, например, Notepad++.

Загрузка конфигурации

- Вы можете загрузить сохраненный файл конфигурации, найдя сохраненный файл .conf.
- Нажмите кнопку 'Upload Config или Jetpack'.
- АЦП загрузит и применит конфигурацию, а затем обновит браузер. Если браузер не обновляется автоматически, пожалуйста, нажмите кнопку обновить в браузере.
- После завершения Вы будете перенаправлены на страницу Dashboard.

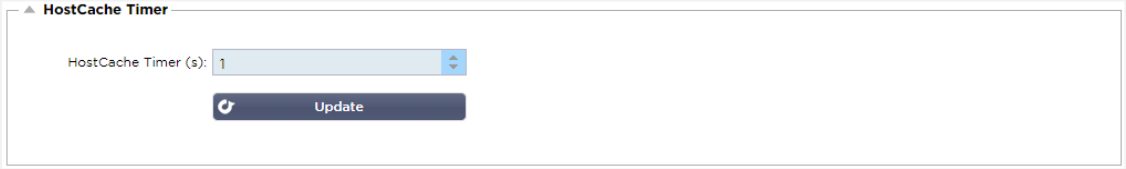
Загрузить jetPACK

- JetPACK - это набор обновлений конфигурации к существующей конфигурации.
- JetPACK может быть настолько мал, как изменение значения тайм-аута TCP, вплоть до полной конфигурации для конкретного приложения, например, Microsoft Exchange или Microsoft Lync.
    - Вы можете получить jetPACK на портале поддержки, указанном в конце данного руководства.
- Найдите файл jetPACK.txt.
- Нажмите кнопку Загрузить.
- После загрузки браузер обновится автоматически.
- После завершения Вы будете перенаправлены на страницу Dashboard.
- Импорт может занять больше времени для более сложных развертываний, таких как Microsoft Lync и т.д.

Глобальные настройки

Раздел Глобальные настройки позволяет Вам изменять различные элементы, включая криптографическую библиотеку SSL.

Таймер кэша хоста



Таймер кэша хоста - это параметр, который сохраняет IP-адрес реального сервера в течение определенного периода времени, когда вместо IP-адреса используется доменное имя. Кэш очищается при отказе реального сервера. Установка этого значения на ноль предотвратит очистку кэша. Для этого параметра нет максимального значения.

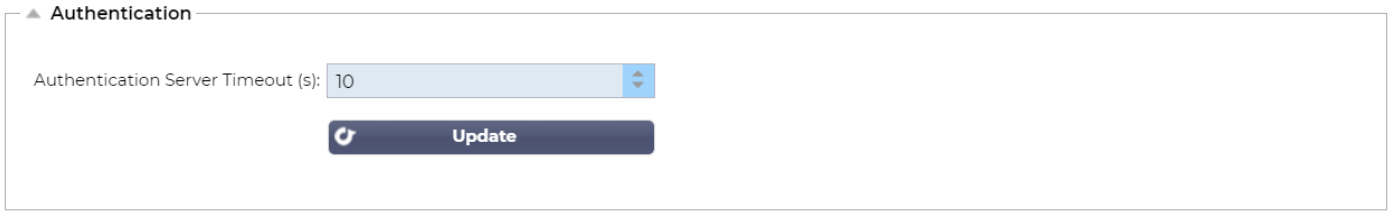
Слив

Функция Drain настраивается для каждого реального сервера, связанного с виртуальной службой. По умолчанию параметр Drain Clears Persistence включен, что позволяет серверам, переведенным в режим Drain, завершать сеансы изящно, чтобы их можно было перевести в автономный режим для обслуживания.

SSL

Эта глобальная настройка позволяет изменять библиотеку SSL по мере необходимости. По умолчанию АЦП использует криптографическую библиотеку SSL от OpenSSL. Если Вы хотите использовать другую криптографическую библиотеку, это можно изменить здесь.

Аутентификация

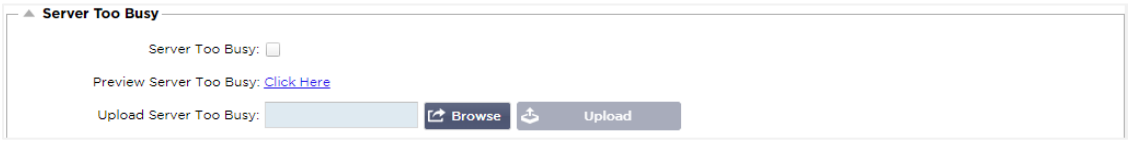


Это значение устанавливает значение тайм-аута для аутентификации, по истечении которого попытка аутентификации будет считаться неудачной.

Протокол

Раздел Протокол используется для установки многих дополнительных настроек для протокола HTTP.

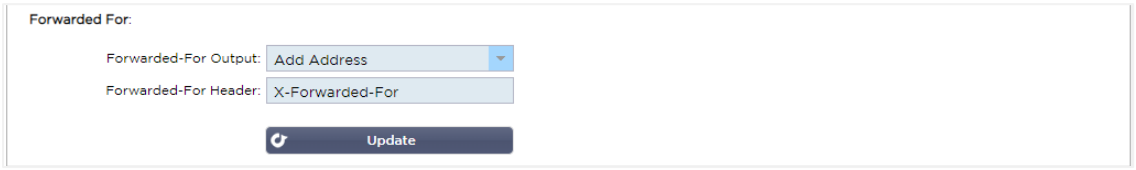
Сервер слишком занят



Предположим, Вы ограничили максимальное количество подключений к Вашим реальным серверам; Вы можете выбрать отображение дружественной веб-страницы, когда этот лимит будет достигнут.

- Создайте простую веб-страницу с Вашим сообщением. Вы можете включить внешние ссылки на объекты на других веб-серверах и сайтах. В качестве альтернативы, если Вы хотите, чтобы на Вашей веб-странице были изображения, используйте встроенные изображения в кодировке base64
- Найдите файл HTM(L) Вашей недавно созданной веб-страницы
- Нажмите кнопку Загрузить
- Если Вы хотите предварительно просмотреть страницу, Вы можете сделать это с помощью ссылки Click Here

Направлено для



Forwarded For - это стандарт де-факто для идентификации IP-адреса клиента, подключающегося к веб-серверу через балансировщики нагрузки 7-го уровня и прокси-серверы.

Переданный-переданный выход

Вариант	Описание
На сайте	ADC не изменяет заголовок Forwarded-For.
Добавить адрес и порт	Этот выбор добавит IP-адрес и порт устройства или клиента, подключенного к АЦП, к заголовку Forwarded-For.
Добавить адрес	Этот выбор добавит IP-адрес устройства или клиента, подключенного к АЦП, к заголовку Forwarded-For.
Замените адрес и порт	Этот выбор заменит значение заголовка Forwarded-For на IP-адрес и порт устройства или клиента, подключенного к АЦП.
Заменить адрес	Этот выбор заменит значение заголовка Forwarded-For на IP-адрес устройства или клиента, подключенного к ADC.

Заголовок для переадресации

Это поле позволяет Вам указать имя, присвоенное заголовку Forwarded-For. Обычно это "X-Forwarded-For", но для некоторых сред оно может быть изменено.

Расширенное ведение журнала для IIS - Пользовательское ведение журнала

Вы можете получить информацию X-Forwarded-For, установив приложение IIS Advanced logging 64-bit. После загрузки создайте пользовательское поле регистрации под названием X-Forwarded-For с приведенными ниже настройками.

Выберите Default в списке Source Type в списке Category, выберите Request Header в поле Source Name и введите X-Forwarded-For.

HTTP://www.iis.net/learn/extensions/advanced-logging-module/advanced-logging-for-iis-custom-logging

Изменения в Apache HTTPd.conf

Вы захотите внести несколько изменений в формат по умолчанию, чтобы регистрировать IP-адрес клиента X-Forwarded-For или фактический IP-адрес клиента, если заголовок X-Forwarded-For не существует.

Эти изменения приведены ниже:

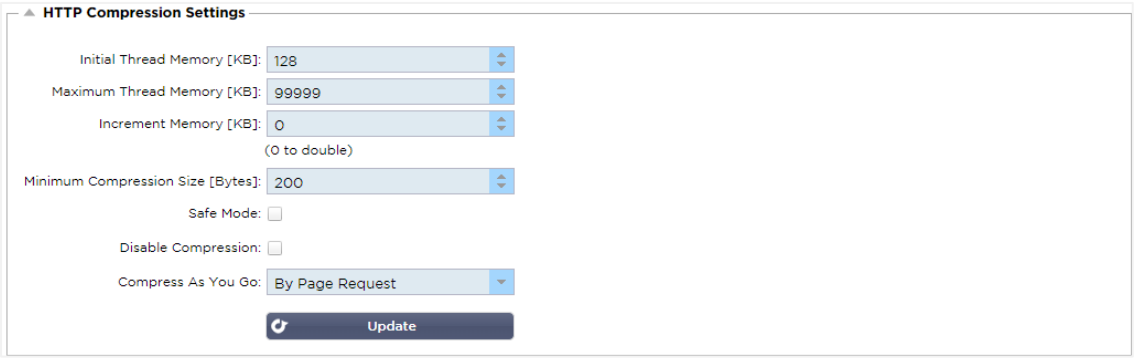
Тип	Значение
LogFormat:	"%h %l %u %t \"%r\" %>s %b \"%{Referer}i\" \"%{User-Agent}i\"" комбинированный
LogFormat:	"%{X-Forwarded-For}i %l %u %t \"%r\" %>s %b \"%{Referer}i\" \"%{User-Agent}i\"" proxy SetEnvIf X- Forwarded-For "^.*\..*\..*\..*\..*" forwarded
CustomLog:	"logs/access_log" комбинированный env=!forwarded
CustomLog:	"logs/access_log" proxy env=forwarded

Этот формат использует преимущества встроенной поддержки Apache для условного протоколирования на основе переменных окружения.

- Строка 1 - это стандартная строка комбинированного журнала, отформатированная по умолчанию.
- Строка 2 заменяет поле %h (удаленный хост) на значение(я), взятое из заголовка X-Forwarded-For, и устанавливает имя этого шаблона файла журнала на "proxy".
- Строка 3 - это настройка для переменной окружения "forwarded", которая содержит свободное регулярное выражение, соответствующее IP-адресу, что в данном случае нормально, поскольку нас больше волнует, существует ли IP-адрес в заголовке X-Forwarded-For.
- Кроме того, строка 3 может быть прочитана как: "Если есть значение X-Forwarded-For, используйте его".
- Строки 4 и 5 указывают Apache, какой шаблон журнала использовать. Если существует значение X-Forwarded-For, используйте шаблон "прокси", в противном случае используйте шаблон "комбинированный" для данного запроса. Для удобочитаемости строки 4 и 5 не используют преимущества функции Apache по вращению журналов (piped), но мы предполагаем, что почти все ее используют.

Эти изменения приведут к регистрации IP-адреса для каждого запроса.

Настройки сжатия HTTP



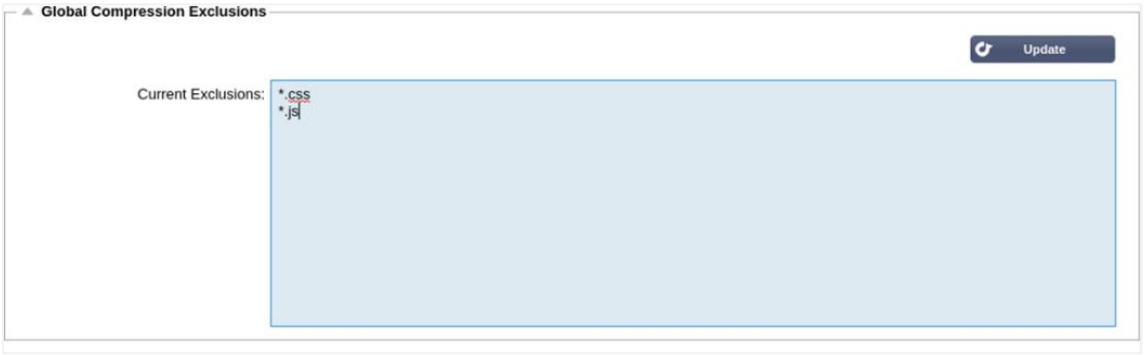
Сжатие является функцией ускорения и включается для каждой службы на странице IP-служб.

ПРЕДУПРЕЖДЕНИЕ - Будьте предельно внимательны при настройке этих параметров, так как неправильные настройки могут негативно повлиять на работу АЦП

Вариант	Описание
Начальная потоковая память [KB]	Это значение - объем памяти, который может первоначально выделить каждый запрос, полученный ADC. Для наиболее эффективной работы, это значение должно быть установлено на величину, чуть превышающую самый большой несжатый HTML файл, который, скорее всего, будут отправлять веб-серверы.
Максимальная потоковая память [KB]	Это значение - максимальный объем памяти, который АЦП выделит на один запрос. Для обеспечения максимальной производительности АЦП обычно хранит и сжимает все содержимое в памяти. Если обрабатывается исключительно большой файл содержимого, превышающий этот объем, АЦП будет записывать данные на диск и сжимать их там.
Память инкремента [КБ]	Это значение устанавливает объем памяти, добавляемый к начальному распределению памяти потоков, когда требуется больше памяти. По умолчанию значение равно нулю. Это означает, что ADC будет удваивать объем выделенной памяти, когда данные превысят текущий объем (например, 128 Кб, затем 256 Кб, затем 512 Кб и т.д.) до предела, установленного параметром Maximum Memory Usage per Thread. Это эффективно, когда большинство страниц имеют постоянный размер, но иногда встречаются файлы большего размера. (Например, большинство страниц имеют размер 128 Кб или меньше, но иногда встречаются ответы размером 1 Мб). В сценарии, когда есть большие файлы переменного размера, эффективнее установить линейное увеличение значительного размера (например, ответы размером от 2Мб до 10Мб, более эффективным будет начальное значение 1Мб с увеличением на 1Мб).
Минимальный размер сжатия [Байт]	Это значение - размер в байтах, при котором АЦП не будет пытаться сжимать данные. Это полезно, поскольку все, что меньше 200 байт, плохо сжимается и может даже увеличиться в размере из-за накладных расходов на заголовки сжатия.
Безопасный режим	Отметьте эту опцию, чтобы предотвратить применение ADC сжатия к таблицам стилей и JavaScript. Причина этого в том, что хотя ADC знает, какие отдельные браузеры могут обрабатывать сжатое содержимое, некоторые другие прокси-серверы, даже если они утверждают, что соответствуют стандарту HTTP/1.1, не могут

	корректно передавать сжатые таблицы стилей и JavaScript. Если возникают проблемы с таблицами стилей или JavaScript через прокси-сервер, то используйте эту опцию, чтобы отключить сжатие этих типов. Однако это уменьшит общий объем сжатия содержимого.
Отключить сжатие	Поставьте галочку, чтобы остановить ADC от сжатия любого ответа.
Компресс по мере выполнения	ON - Используйте Compress as You Go на этой странице. Это сжимает каждый блок данных, полученных от сервера, в дискретный кусок, который полностью декомпрессируется. OFF - Не использовать Compress As You Go на этой странице. По запросу страницы - Использовать Compress as You Go по запросу страницы.

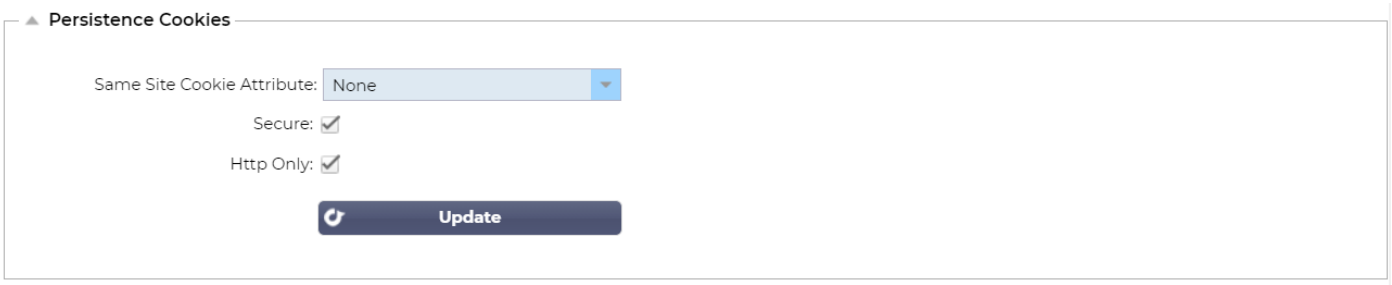
Исключения глобального сжатия



Любые страницы с добавленным расширением в списке исключений не будут сжиматься.

- Введите имя индивидуального файла.
- Нажмите кнопку обновить.
- Если Вы хотите добавить тип файла, просто введите "*.css" для исключения всех каскадных таблиц стилей.
- Каждый файл или тип файла должен быть добавлен в новую строку.

Постоянные файлы cookie



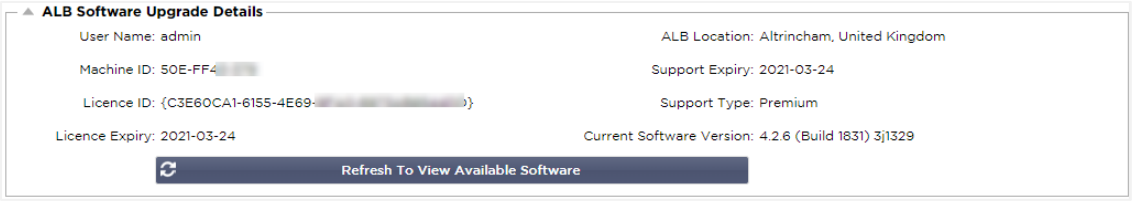
Этот параметр позволяет Вам указать, как будут обрабатываться Persistence Cookies.

Поле	Описание
Атрибут Кука того же сайта	**Нет**: Все файлы cookie доступны для скриптов **Небрежный**: Предотвращает доступ к файлам cookie на разных сайтах, но они сохраняются, чтобы стать доступными и передаваться на принадлежащий сайт, если его посещают **Строгий**: предотвращает доступ или сохранение любых файлов cookie для другого сайта **Выкл**: возврат к поведению браузера по умолчанию
Безопасный	Этот флажок, если он установлен, применяет постоянство к безопасному трафику
Только HTTP	Если флажок установлен, это разрешает постоянные куки только для HTTP-трафика

Программное обеспечение

Раздел "Программное обеспечение" позволяет Вам обновить конфигурацию и микропрограмму Вашего АЦП.

Детали обновления программного обеспечения



Информация в этом разделе будет заполнена, если у Вас есть работающее подключение к Интернету. Если в Вашем браузере нет соединения с Интернетом, этот раздел будет пустым. После подключения Вы получите баннерное сообщение, показанное ниже.

We have successfully connected to Cloud Services Manager to retrieve your Software Update Details

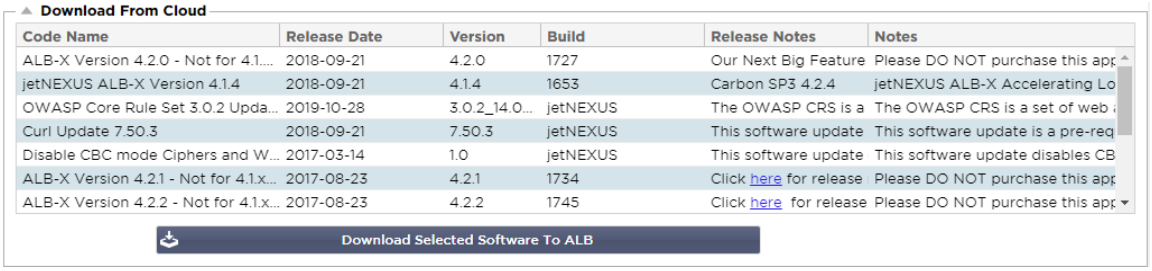
В разделе Download from Cloud, показанном ниже, будет размещена информация, показывающая обновления, доступные Вам в рамках Вашего плана поддержки. Вам следует обратить внимание на Тип поддержки и Срок действия поддержки.

Примечание: Мы используем интернет-соединение Вашего браузера для просмотра того, что доступно в Edgenexus Cloud. Вы сможете загрузить обновления программного обеспечения только в том случае, если АЦП имеет подключение к Интернету.

Чтобы проверить это:

- Дополнительно--Устранение неполадок--Ping
- IP-адрес - appstore.edgenexus.io
- Нажмите Ping
- Если результат показывает "ping: неизвестный хост appstore.edgenexus.io. "
- ADC НЕ сможет загрузить что-либо из облака

Скачать из Облака



Если Ваш браузер подключен к Интернету, Вы увидите подробную информацию о программном обеспечении, доступном в облаке.

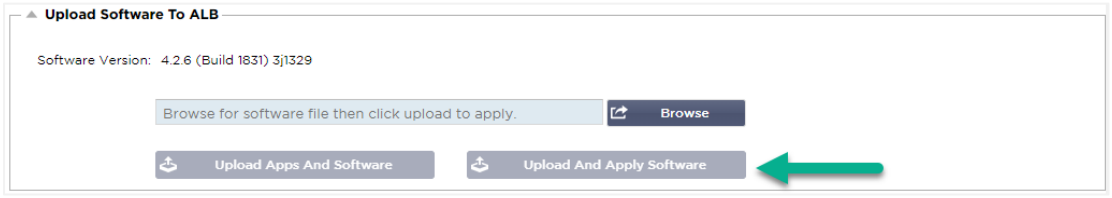
- Выделите интересующую Вас строку и нажмите кнопку "Загрузить выбранное программное обеспечение в ALB. " кнопку
- Выбранное программное обеспечение загрузится на Ваш ALB после щелчка, которое можно применить в разделе "Применить программное обеспечение, хранящееся на ALB" ниже.

Примечание: Если АДЦ не имеет прямого доступа в Интернет, Вы получите ошибку, как показано ниже:

Ошибка загрузки, ALB не может получить доступ к ADC Cloud Services для файла build1734-3236-v4.2.1-Sprint2-update-64.software.alb

Загрузка программного обеспечения в ALB

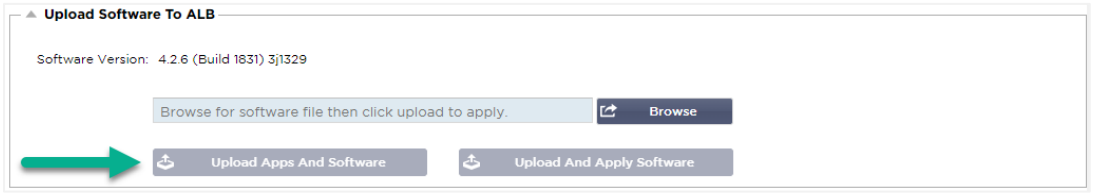
Загрузка приложений



Если у Вас есть файл App, который заканчивается <apptype>.alb, Вы можете использовать этот метод для его загрузки.

- Существует пять типов приложений
  - <Имя приложения>flightpath.alb
  - <имя приложения>.monitor.alb
  - <имя приложения>.jetpack.alb
  - <appname>.addons.alb
  - <имя приложения>.featurepack.alb
- После загрузки каждое приложение можно будет найти в разделе Библиотека> Приложения.
- Затем Вы должны развернуть каждое приложение в этом разделе по отдельности.

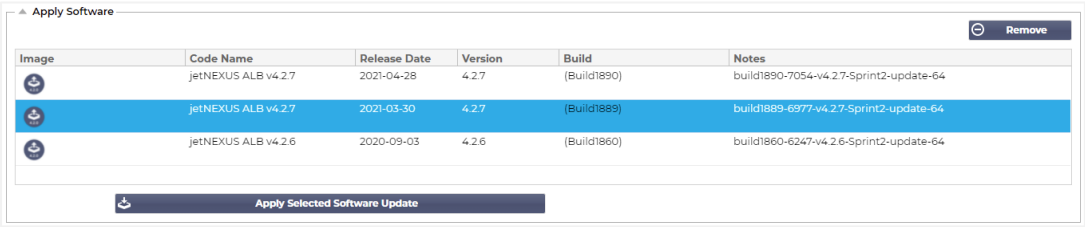
Программное обеспечение



- Если Вы хотите загрузить программное обеспечение без его применения, то используйте выделенную кнопку.

- Файл программного обеспечения - <имя программного обеспечения>.software.alb.
- Затем он появится в разделе "Программное обеспечение, хранящееся на ALB", откуда Вы сможете применить его в удобное для Вас время.

Применять программное обеспечение, хранящееся на ALB



В этом разделе будут показаны все файлы Программного обеспечения, хранящиеся на ALB и доступные для развертывания. Список будет включать обновленные сигнатуры Web Application Firewall (WAF).

- Выделите строку Программное обеспечение, которое Вы хотите использовать.
- Нажмите "Применить программное обеспечение из выбранных"
- Если это обновление программного обеспечения ALB, пожалуйста, имейте в виду, что оно будет загружено, а затем перезагружено ALB для применения.
- Если обновление, которое Вы применяете, является обновлением сигнатуры OWASP, оно будет применено автоматически без перезагрузки.

Устранение неполадок

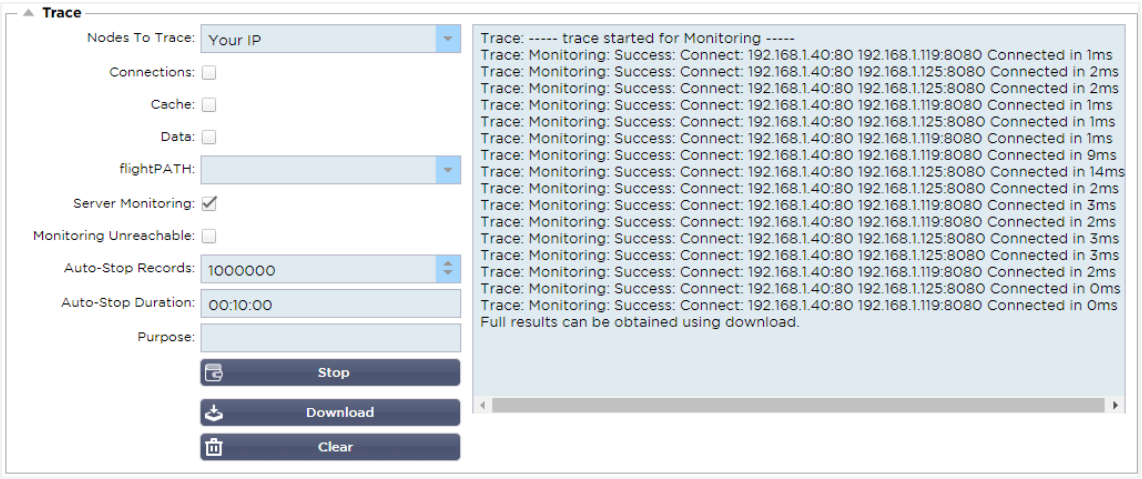
Всегда есть проблемы, которые требуют поиска неисправностей, чтобы найти первопричину и решение. Данный раздел позволяет Вам это сделать.

Файлы поддержки

Если у Вас возникла проблема с ADC и Вам необходимо открыть тикет поддержки, служба технической поддержки часто запрашивает несколько различных файлов с устройства ADC. Теперь эти файлы объединены в один единственный файл .dat, который можно загрузить через этот раздел.

- Выберите временной интервал из выпадающего списка: Вы можете выбрать 3, 7, 14 и Все дни.
- Нажмите "Загрузить файлы поддержки"
- Будет загружен файл в формате Support-jetNEXUS-yyymmddhh-NAME.dat
- Поднимите тикет на портале поддержки, подробная информация о котором приведена в конце данного документа.
- Убедитесь, что Вы подробно описали проблему и приложили файл .dat к билету.

След



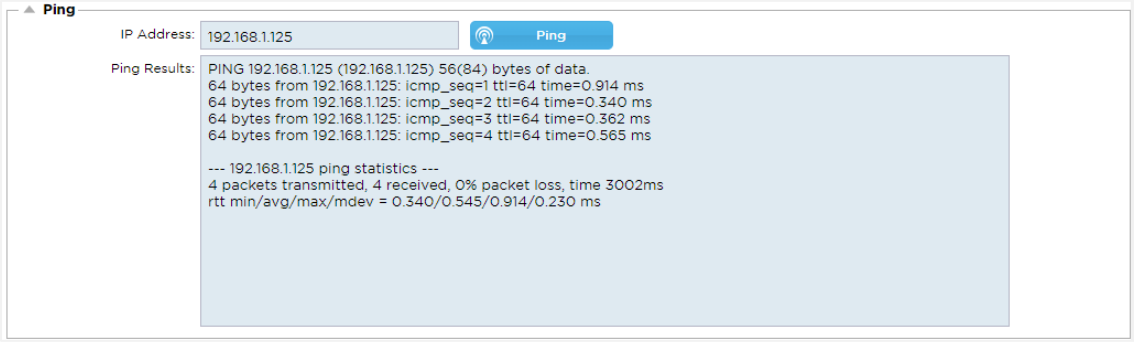
Раздел "Трассировка" позволит Вам изучить информацию, позволяющую отладить проблему. Предоставляемая информация зависит от опций, которые Вы выбираете из выпадающих списков и отмеченных галочками полей.

Вариант	**Описание**
Узлы для отслеживания	**Ваш IP**: Это отфильтрует вывод, чтобы использовать IP-адрес, с которого Вы получаете доступ к графическому интерфейсу (Примечание, не выбирайте эту опцию для мониторинга, так как мониторинг будет использовать адрес интерфейса АЦП). **Все IP**: Фильтр не будет применяться. Следует отметить, что на загруженном блоке это отрицательно скажется на производительности.
Соединения	Этот флажок, если он установлен, покажет Вам информацию о соединениях на стороне клиента и сервера.
Кэш	Этот флажок будет показывать Вам информацию о кэшированных объектах.
Данные	Когда этот флажок отмечен, он будет включать необработанные байты данных, обработанные на входе и выходе АЦП.
flightPATH	Меню flightPATH позволяет Вам выбрать конкретное правило flightPATH для мониторинга или Все правила flightPATH.
Мониторинг сервера	Этот флажок, если он установлен, покажет мониторы здоровья сервера, активные на ADC, и их соответствующие результаты.
Мониторинг Недоступно	Когда эта опция выбрана, поведение очень похоже на мониторинг сервера, за исключением того, что он будет показывать только неудачные мониторы и поэтому действует как фильтр только для этих сообщений.
Записи автостопа	Значение по умолчанию составляет 1,000,000 записей, после чего функция Trace автоматически останавливается. Эта настройка является мерой предосторожности, чтобы предотвратить случайное включение функции Trace и влияние на работу Вашего АЦП.
Продолжительность автостопа	По умолчанию время установлено на 10 минут, после чего функция Trace автоматически останавливается. Эта функция является мерой предосторожности, чтобы предотвратить случайное включение функции Trace и влияние на работу АЦП.

Начало	Щелкните здесь, чтобы запустить средство трассировки вручную.
Остановитесь	Нажмите, чтобы вручную остановить средство Трассировки до того, как будет достигнута автоматическая запись или время.
Скачать	Хотя Вы можете видеть программу просмотра в реальном времени с правой стороны, информация может отображаться слишком быстро. Вместо этого Вы можете загрузить Trace.log, чтобы просмотреть всю информацию, собранную во время различных трасс в тот день. Эта функция представляет собой отфильтрованный список информации о трассировке. Если Вы хотите просмотреть информацию о трассировке за предыдущие дни, Вы можете загрузить Syslog за этот день, но фильтровать придется вручную.
Очистить	Очищает журнал трассировки

Пинг

Вы можете проверить сетевое подключение к серверам и другим сетевым объектам в Вашей инфраструктуре с помощью инструмента Ping.



Введите IP-адрес узла, который Вы хотите проверить, например, шлюз по умолчанию, используя десятичную систему счисления, или адрес IPv6. Возможно, Вам придется подождать несколько секунд, чтобы получить результат после нажатия кнопки "Ping".

Если Вы настроили DNS-сервер, то Вы можете ввести полное доменное имя. Вы можете настроить DNS-сервер в разделе **DNS Server 1 & DNS Server 2**. Возможно, Вам придется подождать несколько секунд, чтобы получить результат после нажатия кнопки "Ping".

Захват

Для захвата сетевого трафика следуйте простым инструкциям, приведенным ниже.

- Заполните параметры в форме
- Нажмите кнопку Генерировать
- После запуска захвата в Вашем браузере появится окно с вопросом, куда Вы хотите сохранить файл. Он будет иметь формат "jetNEXUS.cap.gz".
- Поднимите тикет на портале поддержки, подробная информация о котором приведена в конце данного документа.
- Убедитесь, что Вы подробно описали проблему и прикрепили файл к билету.

- Вы также можете просмотреть содержимое с помощью Wireshark

Вариант	Описание
Адаптер	Выберите свой адаптер из выпадающего списка, обычно это eth0 или eth1. Вы также можете захватить все интерфейсы с помощью "any"
Пакеты	Это значение - максимальное количество пакетов для захвата. Как правило, 99999
Продолжительность	Выберите максимальное время, в течение которого будет выполняться захват. Типичное время - 15 секунд для сайтов с высокой посещаемостью. GUI будет недоступен в течение периода захвата.
Адрес	Это значение будет фильтровать любой IP-адрес, введенный в поле. Оставьте это значение пустым для отсутствия фильтрации.

Для поддержания производительности мы ограничили размер загружаемого файла до 10 МБ. Если Вы обнаружите, что этого недостаточно для получения всех необходимых данных, мы можем увеличить эту цифру.

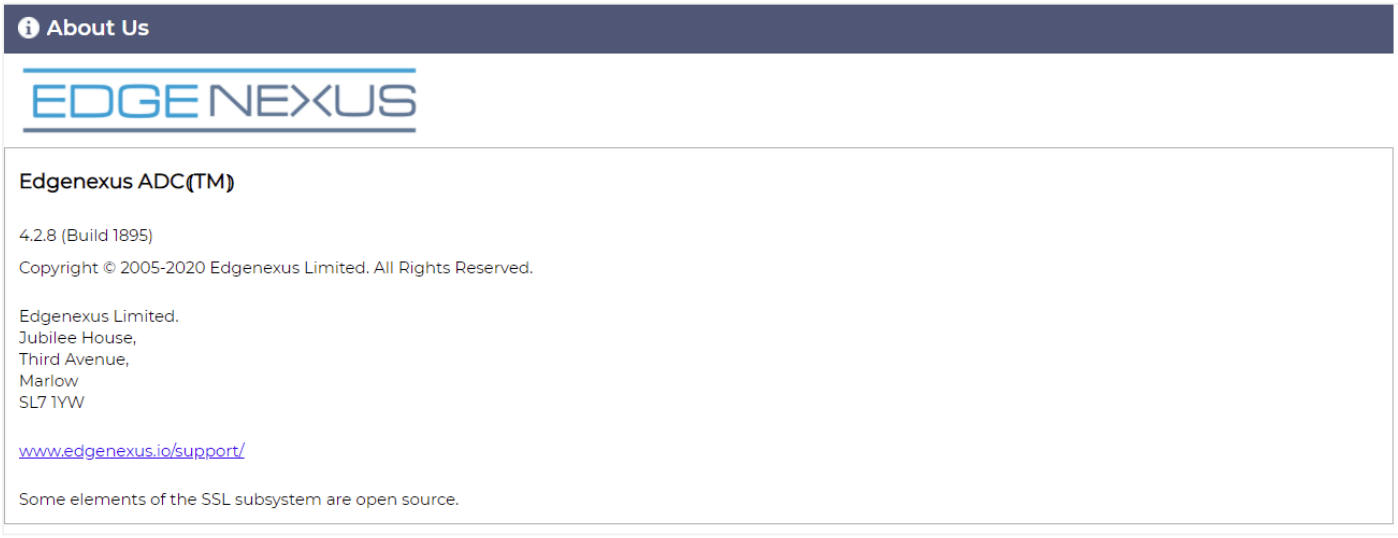
Примечание: Это повлияет на производительность живых сайтов. Для увеличения доступного размера захвата, пожалуйста, примените глобальную настройку jetPACK для увеличения размера захвата.

Помощь

Раздел "Помощь" предоставляет доступ к информации об Edgenexus, а также доступ к руководствам пользователя и другой полезной информации.

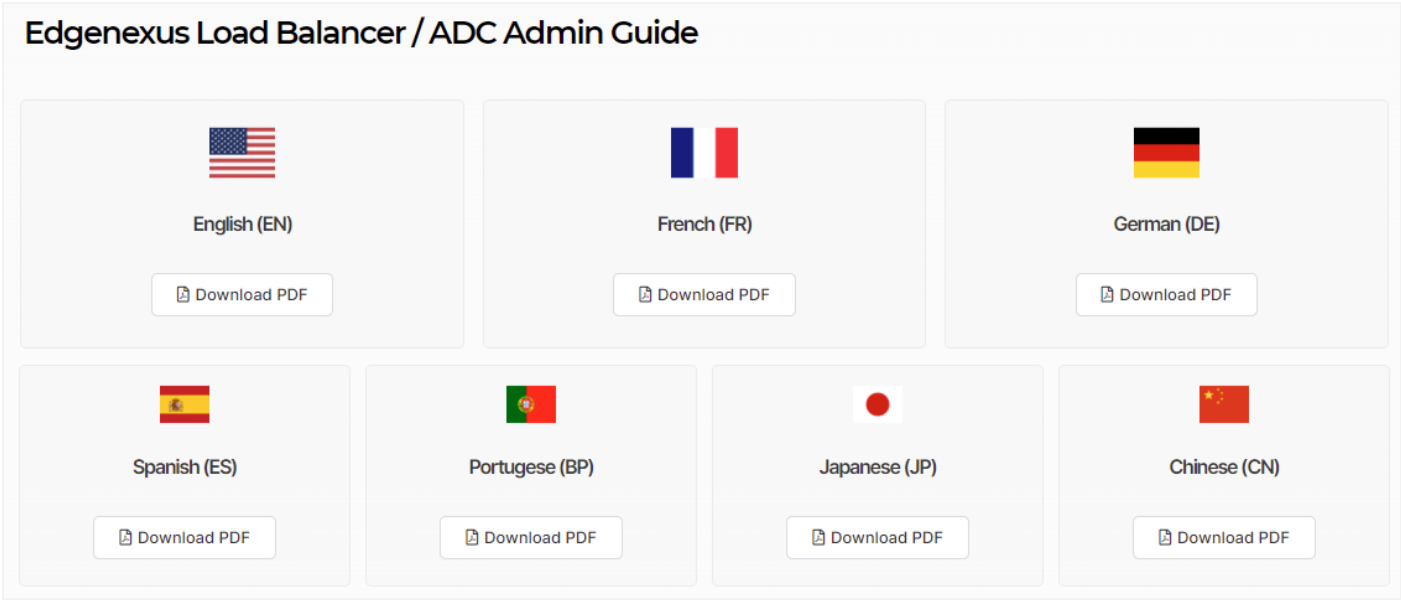
О нас

Щелкнув на опции "О нас", Вы увидите информацию о компании Edgenexus и ее корпоративном офисе.



Ссылка

Опция справки откроет страницу, содержащую руководства пользователя и другие полезные документы.



Если Вы не нашли то, что ищете, пожалуйста, свяжитесь с support@edgenexus.io.

Что такое jetPACK

jetPACKs - это уникальный метод мгновенной настройки Вашего ADC для конкретных приложений. Эти простые в использовании шаблоны поставляются предварительно сконфигурированными и полностью настроенными со всеми специфическими для конкретного приложения параметрами, которые необходимы Вам для получения оптимизированных услуг от Вашего ADC. Некоторые из jetPACK используют flightPATH для манипулирования трафиком, и для работы этого элемента у Вас должна быть лицензия flightPATH. Чтобы узнать, есть ли у Вас лицензия на flightPATH, пожалуйста, обратитесь к странице **Лицензия**.

Загрузка пакета jetPACK

- Каждый jetPACK, представленный ниже, был создан с уникальным Виртуальным IP-адресом, содержащимся в названии jetPACK. Например, первый jetPACK ниже имеет Виртуальный IP-адрес 1.1.1.1
- Вы можете либо загрузить этот jetPACK как есть и изменить IP-адрес в графическом интерфейсе, либо отредактировать jetPACK с помощью текстового редактора, такого как Notepad++, и найти и заменить 1.1.1.1 на Ваш виртуальный IP-адрес.
- Кроме того, каждый jetPACK был создан с 2 реальными серверами с IP адресами 127.1.1.1 и 127.2.2.2. Опять же, Вы можете изменить их в графическом интерфейсе после загрузки или заранее, используя Notepad++.
- Нажмите на ссылку jetPACK ниже и сохраните ссылку как файл jetPACK-VIP-Application.txt в выбранном Вами месте

Microsoft Exchange

Применение	Ссылка на скачивание	Что он делает?	Что включено?
Exchange 2010	jetPACK-1.1.1.1-Exchange-2010	Этот jetPACK добавит основные настройки для балансировки нагрузки Microsoft Exchange 2010. Включено правило flightPATH для перенаправления трафика на службе HTTP на HTTPS, но это опция. Если у Вас нет лицензии на flightPATH, этот jetPACK все равно будет работать.	Глобальные настройки: Тайм-аут обслуживания 2 часа Мониторы: Монитор уровня 7 для веб-приложения Outlook и внеполосный монитор уровня 4 для службы клиентского доступа IP-адрес виртуальной службы: 1.1.1.1 Порты виртуальных служб: 80, 443, 135, 59534, 59535 Реальные серверы: 127.1.1.1 127.2.2.2 flightPATH: Добавляет перенаправление с HTTP на HTTPS
	jetPACK-1.1.1.2-Exchange-2010-SMTP-RP	То же самое, что и выше, но добавляется служба SMTP на порт 25 в режиме обратного прокси. SMTP-сервер будет видеть адрес интерфейса ALB-X в качестве IP-адреса источника.	Глобальные настройки: Тайм-аут обслуживания 2 часа Мониторы: Монитор уровня 7 для веб-приложения Outlook. Внеполосный монитор уровня 4 для службы клиентского доступа

			IP-адрес виртуальной службы: 1.1.1.1 Порты виртуальных служб: 80, 443, 135, 59534, 59535, 25 (обратный прокси) Реальные серверы: 127.1.1.1 127.2.2.2 flightPATH: Добавляет перенаправление с HTTP на HTTPS
	jetPACK-1.1.1.3-Exchange-2010-SMTP-DSR	То же самое, что и выше, за исключением того, что этот jetPACK настроит службу SMTP на использование прямого возврата сервера. Этот jetPACK необходим, если Ваш SMTP-сервер должен видеть фактический IP-адрес клиента.	Глобальные настройки: Тайм-аут обслуживания 2 часа Мониторы: Монитор уровня 7 для веб-приложения Outlook. Внеполосный монитор уровня 4 для службы клиентского доступа IP-адрес виртуальной службы: 1.1.1.1 Порты виртуального сервиса: 80, 443, 135, 59534, 59535, 25 (прямой возврат сервера) Реальные серверы: 127.1.1.1 127.2.2.2 flightPATH: Добавляет перенаправление с HTTP на HTTPs
Exchange 2013	jetPACK-2.2.2.1-Exchange-2013-Low-Resource	Эта установка добавляет 1 VIP и две службы для HTTP и HTTPS трафика и требует меньше всего CPU. Можно добавить несколько проверок состояния VIP, чтобы проверить, что каждая из отдельных служб находится в рабочем состоянии	Глобальные настройки: Мониторы: Монитор уровня 7 для OWA, EWS, OA, EAS, ECP, OAB и ADS IP-адрес виртуальной службы: 2.2.2.1 Порты виртуальных служб: 80, 443 Реальные серверы: 127.1.1.1 127.2.2.2 flightPATH: Добавляет перенаправление с HTTP на HTTPS
	jetPACK-2.2.3.1-Exchange-2013-Med-Resource	Эта настройка использует уникальный IP-адрес для каждой службы и поэтому использует больше ресурсов, чем выше. Вы должны настроить каждую службу как отдельную запись DNS Пример owa.jetnexus.com, ews.jetnexus.com и т.д. Монитор для каждой службы будет добавлен и применен к соответствующей службе	Глобальные настройки: Мониторы: Монитор уровня 7 для OWA, EWS, OA, EAS, ECP, OAB, ADS, MAPI и PowerShell IP виртуальной службы: 2.2.3.1, 2.2.3.2, 2.2.3.3, 2.2.3.4, 2.2.3.5, 2.2.3.6, 2.2.3.7, 2.2.3.8, 2.2.3.9, 2.2.3.10 Порты виртуальных служб: 80, 443

			Реальные серверы: 127.1.1.1 127.2.2.2 flightPATH: Добавляет перенаправление с HTTP на HTTPs
	jetPACK-2.2.2.3-Exchange2013-HIgh-Resource	Этот jetPACK добавит один уникальный IP-адрес и несколько виртуальных служб на разных портах. flightPATH затем будет осуществлять контекстное переключение на основе пути назначения к нужной виртуальной службе. Этот пакет jetPACK требует наибольшего количества CPU для выполнения контекстного переключения	Глобальные настройки: Мониторы: Монитор уровня 7 для OWA, EWS, OA, EAS, ECP, OAB, ADS, MAPI и PowerShell IP-адрес виртуальной службы: 2.2.2.3 Порты виртуальных служб: 80, 443, 1, 2, 3, 4, 5, 6, 7 Реальные серверы: 127.1.1.1 127.2.2.2 flightPATH: Добавляет перенаправление с HTTP на HTTPS

Microsoft Lync 2010/2013

Обратный прокси-сервер	Фронт-энд	Край внутренний	Край внешний
jetPACK-3.3.3.1-Lync-Reverse-Proxy	jetPACK-3.3.3.2-Lync-Front -End	jetPACK-3.3.3.3-Lync-Edge-Internal	jetPACK-3.3.3.4-Lync-Edge-External

Веб-услуги

Обычный HTTP	SSL разгрузка	Повторное шифрование SSL	SSL Passthrough
jetPACK-4.4.4.1-Web-HTTP	jetPACK-4.4.4.2-Web-SSL Offload	jetPACK-4.4.4.3-Web-SSL-Re-Encryption	jetPACK-4.4.4.4-Web-SSL Passthrough

Удаленный рабочий стол Microsoft

Нормальный
jetPACK-5.5.5.1-Remote-Desktop

DICOM - Цифровая визуализация и коммуникация в медицине

Обычный HTTP
jetPACK-6.6.6.1-DICOM

Oracle e-Business Suite

SSL разгрузка
jetPACK-7.7.7..1-Oracle-EBS

VMware Horizon View

Серверы соединений - SSL разгрузка	Серверы безопасности - повторное шифрование SSL

jetPACK-8.8.8.1-View-SSL-Offload jetPACK-8.8.8.2-View-SSL-Re-encryption

Глобальные настройки

- GUI Secure Port 443 - этот jetPACK изменит Ваш безопасный порт GUI с 27376 на 443. HTTPs://x.x.x.x
- GUI Timeout 1 day - GUI будет запрашивать Вас ввести пароль каждые 20 минут. Эта настройка увеличит время запроса до 1 дня
- ARP Refresh 10 - во время обхода отказа между устройствами HA, эта настройка увеличит количество **Gratuitous ARP'ов,** чтобы помочь коммутаторам во время перехода.
- Размер захвата 16MB - размер захвата по умолчанию составляет 2MB. Это значение увеличит размер до максимального значения 16MB

Параметры шифра

- Сильные шифры - Это добавит возможность выбрать "Сильные шифры" из списка опций шифров:
  - Шифр = ALL:RC4+RSA:+RC4:+HIGH:!DES-CBC3-SHA:!SSLv2:!ADH:!EXP:!ADHexport:!MD5
- Anti-Beast - Это добавит возможность выбрать "Anti Beast" из списка опций шифра:
  - Шифр = ECDHE-RSA-AES128-SHA256:AES128-GCM-SHA256:RC4:HIGH:!MD5:!aNULL:!EDH
- No SSLv3 - Это добавит возможность выбрать "No SSLv3" из списка Cipher Options:
  - Шифр = ECDHE-RSA-AES128-SHA256:AES128-GCM-SHA256:HIGH:!MD5:!aNULL:!EDH:!RC4
- No SSLv3 no TLSv1 No RC4 - Это добавит возможность выбрать "No-TLSv1 No-SSLv3 No-RC4" из списка Cipher Options:
  - Шифр = ECDHE-RSA-AES128-SHA256:AES128-GCM-SHA256:HIGH:!MD5:!aNULL:!EDH:!RC4
- NO_TLSv1.1 -Это добавит возможность выбрать "NO_TLSv1.1" из списка опций шифра:
  - Шифр= ECDH+AESGCM:DH+AESGCM:ECDH+AES256:DH+AES256:ECDH+AES128:DH+AES:RSA+AESGCM:RSA+AES:HIGH:!3DES:!aNULL:!MD5:!DSS:!MD5:!aNULL:!EDH:!RC4

flightPATHs

- X-Content-Type-Options - добавьте этот заголовок, если он не существует, и установите его в значение "nosniff" - предотвращает автоматический "MIME-Sniffing" браузера.
- X-Frame-Options - добавьте этот заголовок, если он не существует, и установите его в значение "SAMEORIGIN" - страницы Вашего сайта могут быть включены во фреймы, но только на других страницах того же сайта.
- X-XSS-Protection - добавьте этот заголовок, если он не существует, и установите его значение "1; mode=block" - включите защиту браузера от межсайтовых скриптов
- Strict-Transport-Security - добавьте заголовок, если он не существует, и установите его на "max-age=31536000 ; includeSubdomains" - гарантирует, что клиент должен соблюдать, что все ссылки должны быть HTTPs:// для max-age

Применение jetPACK

Вы можете применять любой jetPACK в любом порядке, но будьте осторожны, чтобы не использовать jetPACK с одним и тем же виртуальным IP-адресом. Это действие приведет к

дублированию IP-адреса в конфигурации. Если Вы сделали это по ошибке, Вы можете изменить это в графическом интерфейсе.

- Перейдите в меню Дополнительно > Обновить программное обеспечение
- Раздел конфигурации
- Загрузите новую конфигурацию или jetPACK
- Просмотреть для jetPACK
- Нажмите кнопку Загрузить
- Как только экран браузера станет белым, пожалуйста, нажмите обновить и дождитесь появления страницы Приборной панели

Создание пакета jetPACK

Одна из замечательных особенностей jetPACK заключается в том, что Вы можете создавать свои собственные. Возможно, Вы создали идеальную конфигурацию для какого-либо приложения и хотите использовать ее для нескольких других коробок независимо друг от друга.

- Начните с копирования текущей конфигурации из имеющейся у Вас ALB-X
  - Расширенный
  - Обновление программного обеспечения
  - Загрузить текущую конфигурацию
- Отредактируйте этот файл с помощью Notepad++
- Откройте новый документ txt и назовите его "yourname-jetPACK1.txt".
- Скопируйте все соответствующие разделы из файла конфигурации в файл "yourname-jetPACK1.txt".
- Сохраните после завершения

ВАЖНО: Каждый jetPACK разделен на различные разделы, но все jetPACK должны иметь #!jetpack в верхней части страницы.

Ниже перечислены разделы, которые рекомендуется редактировать/копировать.

Раздел 0:

```
#!jetpack
```

Эта строка должна находиться в верхней части jetPACK, иначе Ваша текущая конфигурация будет перезаписана.

Раздел1:

```
[jetnexusdaemon].
```

Этот раздел содержит глобальные настройки, которые после изменения будут применяться ко всем службам. Некоторые из этих настроек можно изменить из веб-консоли, но другие доступны только здесь.

Примеры:

```
ConnectionTimeout=600000
```

В данном примере значение тайм-аута TCP в миллисекундах. Эта настройка означает, что TCP-соединение будет закрыто после 10 минут бездействия

```
ContentServerCustomTimer=20000
```

Этот пример представляет собой задержку в миллисекундах между проверками состояния сервера содержимого для пользовательских мониторов, таких как DICOM

```
jnCookieHeader="MS-WSMAN"
```

Этот пример изменит имя заголовка cookie, используемого при постоянной балансировке нагрузки, со стандартного "jnAccel" на "MS-WSMAN". Это конкретное изменение необходимо для обратного прокси Lync 2010/2013.

Раздел 2:

[jetnexusdaemon-Csm-Rules].

Этот раздел содержит пользовательские правила мониторинга сервера, которые обычно настраиваются здесь с веб-консоли.

Пример:

[jetnexusdaemon-Csm-Rules-0].

Content="Server Up"

Desc="Монитор 1

Method="CheckResponse"

Name="Проверка здоровья - работает ли сервер"

Url="HTTP://demo.jetneus.com/healthcheck/healthcheck.html"

Раздел 3:

[jetnexusdaemon-LocalInterface].

Этот раздел содержит все детали раздела IP Services. Каждый интерфейс пронумерован и включает в себя подинтерфейсы для каждого канала. Если к Вашему каналу применено правило flightPATH, то он также будет содержать раздел Path.

Пример:

[jetnexusdaemon-LocalInterface1].

1.1=”443″

1.2=”104″

1.3=”80″

1.4=”81″

Включено=1

Netmask="255.255.255.0″

PrimaryV2="{A28B2C99-1FFC-4A7C-AAD9-A55C32A9E913}"

[jetnexusdaemon-LocalInterface1.1].

1=">,""Secure Group"",2000,""

2="192.168.101.11:80,Y,""IIS WWW Server 1″"""

3="192.168.101.12:80,Y,""IIS WWW Server 2″"""

AddressResolution=0

CachePort=0

CertificateName="default"

ClientCertificateName="No SSL"

Compress=1

ConnectionLimiting=0

DSR=0

DSRProto="tcp"

Включено=1

LoadBalancePolicy="CookieBased"

MaxConnections=10000

MonitoringPolicy="1″

PassThrough=0

Protocol="Accelerate HTTP"

ServiceDesc="Secure Servers VIP"

SNAT=0

SSL=1

SSLClient=0

SSLInternalPort=27400

[jetnexusdaemon-LocalInterface1.1-Path]

1=”6″

Раздел 4:

[jetnexusdaemon-Path]

Этот раздел содержит все правила flightPATH. Номера должны совпадать с тем, что было применено к интерфейсу. В примере выше мы видим, что правило flightPATH "6" было применено к каналу, включая это в качестве примера ниже.

Пример:

[jetnexusdaemon-Path-6].

Desc="Принудительное использование HTTPS для определенного каталога"

Name="Gary - Force HTTPS"

[jetnexusdaemon-Path-6-Condition-1].

Check="contain"

Условие="путь"

Соответствие=

Sense="does"

Value="/secure/"

[jetnexusdaemon-Path-6-Evaluate-1].

Подробнее=

Source="host"

Значение=

Переменная="$host$"[jetnexusdaemon-Path-6-Function-1]

Action="redirect"

Target="HTTPs://$host$$path$$querystring$"

Значение=

Введение в flightPATH

Что такое flightPATH?

flightPATH - это интеллектуальный механизм правил, разработанный компанией Edgenexus для управления и маршрутизации HTTP и HTTPS трафика. Он очень настраиваемый, очень мощный и в то же время очень простой в использовании.

Хотя некоторые компоненты flightPATH являются объектами IP, например, Source IP, flightPATH может быть применен только к **типу службы,** равному HTTP. Если Вы выберете любой другой тип службы, то вкладка flightPATH в IP Services будет пустой.

Правило flightPATH состоит из трех компонентов:

Вариант	Описание
Состояние	Установите несколько критериев для запуска правила flightPATH.
Оценка	Позволяет использовать переменные, которые могут быть использованы в области действий.
Действие	Поведение после срабатывания правила.

Что может сделать flightPATH?

flightPATH может быть использован для изменения входящего и исходящего HTTP(s) содержимого и запросов.

Помимо использования простых строковых соответствий, таких как, например, "Начинается с" и "Заканчивается с", можно реализовать полный контроль с помощью мощных Perl-совместимых регулярных выражений (RegEx).

Подробнее о RegEx смотрите на этом полезном сайте https://www.regexbuddy.com/regex.html.

Кроме того, пользовательские переменные могут быть созданы и использованы в области **действий, что позволяет использовать** множество различных возможностей.

Состояние

Состояние	Описание	Пример
<form>	HTML-формы используются для передачи данных на сервер	Пример "форма не имеет длины 0".
Местонахождение ГЕО	При этом IP-адрес источника сравнивается с кодом страны ISO 3166	ГЕО местоположение равно GB ИЛИ ГЕО местоположение равно Германия
Хозяин	Это хост, извлеченный из URL	www.mywebsite.com или 192.168.1.1
Язык	Вот язык, извлеченный из HTTP-заголовка language	Это условие приведет к появлению выпадающего списка с перечнем языков
Метод	Это выпадающий список методов HTTP	Это выпадающий список, который включает GET, POST и т.д.
Происхождение IP	Если восходящий прокси поддерживает X-Forwarded-for (XFF),	IP-адрес клиента. Можно также использовать несколько IP или подсетей.

	он будет использовать истинный адрес происхождения	10\.1\.2\.* - это 10.1.2.0 /24 подсеть10\ .1\.2\.3|10\.1\.2\.4 Используйте | для нескольких IP-адресов
Путь	Это путь к сайту	/mywebsite/index.asp
ПОСТ	Метод запроса POST	Проверка данных, загружаемых на веб-сайт
Запрос	Это имя и значение запроса, поэтому он может принимать либо имя запроса, либо значение.	"Best=jetNEXUS", где соответствие - Best, а значение - edgeNEXUS
Строка запроса	Вся строка запроса после символа ?	
Запрос Cookie	Это имя файла cookie, запрашиваемого клиентом	MS-WSMAN=afYfn1CDqqCDqUD::
Заголовок запроса	Это может быть любой HTTP-заголовок	Referrer, User-Agent, From, Date
Версия для запроса	Это версия HTTP	HTTP/1.0 ИЛИ HTTP/1.1
Орган реагирования	Определяемая пользователем строка в теле ответа	Сервер UP
Код ответа	Код HTTP для ответа	200 OK, 304 Not Modified
Ответное печенье	Это имя файла cookie, отправленного сервером.	MS-WSMAN=afYfn1CDqqCDqUD::
Заголовок ответа	Это может быть любой HTTP-заголовок	Referrer, User-Agent, From, Date
Версия ответа	Версия HTTP, отправленная сервером	HTTP/1.0 ИЛИ HTTP/1.1
Источник IP	Это либо IP-адрес источника, IP-адрес прокси-сервера или какой-либо другой агрегированный IP-адрес	ClientIP , Proxy IP, Firewall IP. Можно также использовать несколько IP и подсетей. Вы должны исключить точки, так как они являются RegEX. Пример 10\.1\.2\.3 - 10.1.2.3

Матч	**Описание**	**Пример**
Принять	Типы содержимого, которые допустимы	Принять: текст/plain
Accept-Encoding	Допустимые кодировки	Accept-Encoding: <compress | gzip | deflate | sdch | identity>.
Accept-Language	Приемлемые языки для ответа	Язык приема: en-US
Accept-Ranges	Какие типы диапазонов частичного содержимого поддерживает этот сервер	Accept-Ranges: bytes
Авторизация	Учетные данные для аутентификации по протоколу HTTP	Авторизация: Basic QWxhZGRpbjpvcGVuIHNlc2FtZQ==

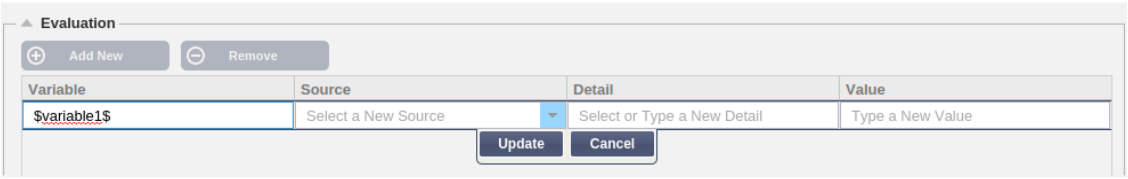
Зарядка -	Содержит информацию о расходах, связанных с применением запрашиваемого метода	
Content-Encoding	Тип кодировки, используемый в данных.	Content-Encoding: gzip
Content-Length	Длина тела ответа в октетах (8-битных байтах)	Content-Length: 348
Content-Type	Тип mime тела запроса (используется с запросами POST и PUT)	Content-Type: application/x-www-form-urlencoded
Печенье	HTTP cookie, ранее отправленный сервером с помощью Set-Cookie (ниже).	Cookie: $Version=1; Skin=new;
Дата	Дата и время, когда было отправлено сообщение	Дата = "Дата" ":" HTTP-дата
ETag	Идентификатор для конкретной версии ресурса, часто дайджест сообщения	ETag: "aed6bdb8e090cd1:0".
С сайта	Адрес электронной почты пользователя, делающего запрос	От: user@example.com
If-Modified-Since	Позволяет возвращать сообщение 304 Not Modified, если содержимое не изменилось	If-Modified-Since: Sat, 29 Oct 1994 19:43:31 GMT
Last-Modified	Дата последнего изменения для запрашиваемого объекта, в формате RFC 2822	Last-Modified: Tue, 15 Nov 1994 12:45:26 GMT
Pragma	Заголовки, специфичные для реализации, могут иметь различные эффекты в любом месте цепочки запрос-ответ.	Pragma: no-cache
Реферрер	Это адрес предыдущей веб-страницы, с которой была получена ссылка на текущую запрашиваемую страницу	Реферер: HTTP://www.edgenexus.io
Сервер	Имя для сервера	Сервер: Apache/2.4.1 (Unix)
Set-Cookie	HTTP-куки	Set-Cookie: UserID=JohnDoe; Max-Age=3600; Version=1
User-Agent	Строка агента пользователя	User-Agent: Mozilla/5.0 (совместимый; MSIE 9.0; Windows NT 6.1; WOW64; Trident/5.0)
Варьировать	Сообщает нижестоящим прокси-серверам, как сопоставить заголовки будущих запросов, чтобы решить, можно ли использовать кэшированный ответ, а не запрашивать новый с исходного сервера.	Vary: User-Agent
X-Powered-By	Указывает технологию (например, ASP.NET, PHP, JBoss), поддерживающую веб-приложение	X-Powered-By: PHP/5.4.0

Проверьте	Описание	Пример
Существовать	Здесь не важны детали условия, только то, что оно существует/не существует	Host - Does - Exist
Начало	Строка начинается со значения	Путь - Does - Start - /secure
Конец	Строка заканчивается значением	Путь - Делает - Конец - .jpg
Содержите	Строка содержит Значение	Заголовок запроса - Принимать - Есть - Содержит - изображение
Равный	Строка равна значению	Host - Does - Equal - www.jetnexus.com
Иметь длину	Строка имеет длину значения	Host - Does - Have Length - 16www.jetnexus.com = TRUEwww.jetnexus.co.uk = FALSE
Соответствие RegEx	Это позволяет Вам ввести полное регулярное выражение, совместимое с Perl	Origin IP - Does - Match Regex - 10\...* | 11\...*

Пример

- В примере есть два условия, и **ОБА** должны быть выполнены, чтобы выполнить действие
- Первое - это проверка того, что запрашиваемый объект является изображением
- Второй - проверка наличия определенного имени хоста

Оценка



Добавление переменной - это интересная функция, которая позволит Вам извлекать данные из запроса и использовать их в Действиях. Например, Вы можете зарегистрировать имя пользователя или отправить электронное письмо, если возникла проблема безопасности.

- Переменная: Она должна начинаться и заканчиваться символом $. Например, $variable1$
- Источник: Выберите из выпадающего списка источник переменной
- Подробно: Выберите из списка, когда это уместно. Если Источник=Заголовок запроса, Деталь может быть User-Agent
- Значение: Введите текст или регулярное выражение для точной настройки переменной.

Встроенные переменные:

- Встроенные переменные уже жестко закодированы, поэтому Вам не нужно создавать для них запись оценки.
- Вы можете использовать любую из перечисленных ниже переменных в своем действии
- Объяснение каждой переменной находится в таблице "Условия" выше
    - Метод = $method$

- Path = $path$
- Querystring = $querystring$
- Sourceip = $sourceip$
- Код ответа (текст также включает "200 OK") = $resp$
- Host = $host$
- Версия = $version$
- Клиентский порт = $clientport$
- Clientip = $clientip$
- Геолокация = $geolocation$"

Пример действия:

- Действие = Перенаправление 302
  - Цель = HTTPs://$host$/404.html
- Действие = Журнал
  - Target = Клиент из $sourceip$:$sourceport$ только что сделал запрос $path$ page

Объяснение:

- Клиент, обращающийся к несуществующей странице, как правило, получает страницу 404 браузера
- В этом случае пользователь перенаправляется на исходное имя хоста, которое он использовал, но неверный путь заменяется на 404.html
- В syslog добавляется запись: "Клиент с 154.3.22.14:3454 только что сделал запрос на страницу wrong.html".

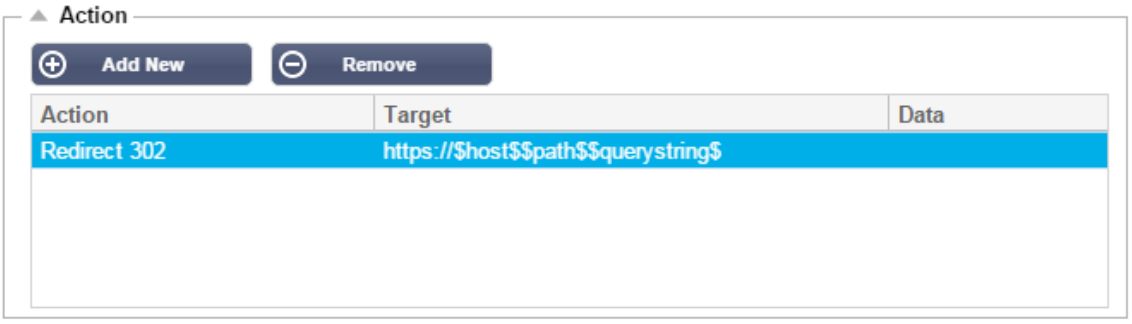
Источник	Описание	Пример
Печенье	Это имя и значение заголовка файла cookie	MS-WSMAN=afYfn1CDqqCDqUD::где имя - MS-WSMAN, а значение - afYfn1CDqqCDqUD::
Хозяин	Это имя хоста, извлеченное из URL-адреса	www.mywebsite.com или 192.168.1.1
Язык	Вот язык, извлеченный из HTTP-заголовка Language	Это условие приведет к появлению выпадающего списка языков.
Метод	Это выпадающий список методов HTTP	Выпадающий список будет включать GET, POST
Путь	Это путь к сайту	/mywebsite/index.html
ПОСТ	Метод запроса POST	Проверка данных, загружаемых на веб-сайт
Пункт запроса	Это имя и значение запроса. Как таковой, он может принимать либо имя запроса, либо значение, также	"Best=jetNEXUS", где соответствие - Best, а значение - edgeNEXUS
Строка запроса	Это вся строка после символа ?	HTTP://server/path/program?query_string
Заголовок запроса	Это может быть любой заголовок, отправленный клиентом	Referrer, User-Agent, From, Date...
Заголовок ответа	Это может быть любой заголовок, отправленный сервером	Referrer, User-Agent, From, Date...
Версия	Это версия HTTP	HTTP/1.0 или HTTP/1.1

Деталь	Описание	Пример
Принять	Типы содержимого, которые допустимы	Принять: текст/plain
Accept-Encoding	Допустимые кодировки	Accept-Encoding: <compress | gzip | deflate | sdch | identity>.
Accept-Language	Приемлемые языки для ответа	Язык приема: en-US
Accept-Ranges	Какие типы диапазонов частичного содержимого поддерживает этот сервер	Accept-Ranges: bytes
Авторизация	Учетные данные для аутентификации по протоколу HTTP	Авторизация: Basic QWxhZGRpbjpvcGVuIHNlc2FtZQ==
Зарядка -	Содержит информацию о расходах, связанных с применением запрашиваемого метода	
Content-Encoding	Тип кодировки, используемый в данных.	Content-Encoding: gzip
Content-Length	Длина тела ответа в октетах (8-битных байтах)	Content-Length: 348
Content-Type	Тип mime тела запроса (используется с запросами POST и PUT)	Content-Type: application/x-www-form-urlencoded
Печенье	HTTP cookie, ранее отправленный сервером с помощью Set-Cookie (см. ниже)	Cookie: $Version=1; Skin=new;
Дата	Дата и время, в которое было отправлено сообщение	Дата = "Дата" ":" HTTP-дата
ETag	Идентификатор для конкретной версии ресурса, часто дайджест сообщения	ETag: "aed6bdb8e090cd1:0".
С сайта	Адрес электронной почты пользователя, делающего запрос	От: user@example.com
If-Modified-Since	Позволяет возвращать сообщение 304 Not Modified, если содержимое не изменилось	If-Modified-Since: Sat, 29 Oct 1994 19:43:31 GMT
Last-Modified	Дата последнего изменения для запрашиваемого объекта, в формате RFC 2822	Last-Modified: Tue, 15 Nov 1994 12:45:26 GMT
Pragma	Специфические для реализации заголовки, которые могут иметь различные эффекты в любой точке цепочки запрос-ответ.	Pragma: no-cache
Реферрер	Это адрес предыдущей веб-страницы, с которой была получена ссылка на текущую запрашиваемую страницу	Реферер: HTTP://www.edgenexus.io
Сервер	Имя для сервера	Сервер: Apache/2.4.1 (Unix)
Set-Cookie	HTTP-куки	Set-Cookie: UserID=JohnDoe; Max-Age=3600; Version=1

User-Agent	Строка агента пользователя	User-Agent: Mozilla/5.0 (совместимый; MSIE 9.0; Windows NT 6.1; WOW64; Trident/5.0)
Варьировать	Сообщает прокси-серверам, как сопоставить заголовки будущих запросов, чтобы решить, можно ли использовать кэшированный ответ вместо того, чтобы запрашивать новый ответ у исходного сервера.	Vary: User-Agent
X-Powered-By	Указывает технологию (например, ASP.NET, PHP, JBoss), поддерживающую веб-приложение	X-Powered-By: PHP/5.4.0

Действие

Действие - это задача или задачи, которые включаются после выполнения условия или условий.



Действие

Дважды щелкните на колонке Действие, чтобы просмотреть выпадающий список.

Цель

Дважды щелкните на колонке Цель, чтобы просмотреть выпадающий список. Список будет меняться в зависимости от действия.

Вы также можете набирать текст вручную с помощью некоторых действий.

Данные

Дважды щелкните на колонке "Данные", чтобы вручную добавить данные, которые Вы хотите добавить или заменить.

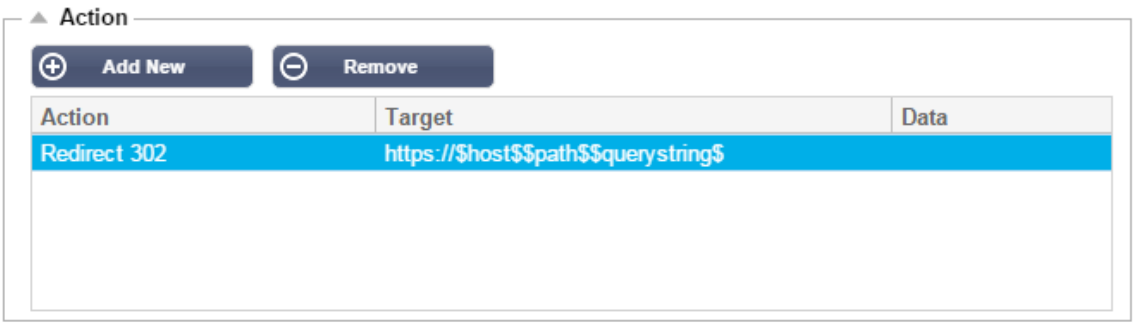
Список всех действий подробно описан ниже:

Действие	**Описание**	**Пример**
Cookie для добавления запроса	Добавьте cookie запроса, подробно описанные в разделе "Цель", со значением в разделе "Данные	Target= Cookie Данные= MS-WSMAN=afYfn1CDqqCDqCVii

Добавить заголовок запроса	Добавьте заголовок запроса типа Target со значением в секции Data	Цель = Принять Data= image/png
Добавить ответную печенье	Добавьте ответный Cookie, подробно описанный в разделе Цель, со значением в разделе Данные	Target= Cookie Данные= MS-WSMAN=afYfn1CDqqCDqCVii
Добавить заголовок ответа	Добавьте заголовок запроса, подробный в разделе Цель, со значением в разделе Данные	Target= Cache-Control Данные= max-age=8888888
Кузов Заменить все	Найдите тело ответа и замените все экземпляры	Target= HTTP:// (Строка поиска) Data= HTTPs:// (Заменяемая строка)
Замена тела в первую очередь	Найдите тело ответа и замените только первый экземпляр	Target= HTTP:// (Строка поиска) Data= HTTPs:// (Заменяемая строка)
Замена корпуса Последняя	Выполните поиск в теле ответа и замените только последний экземпляр	Target= HTTP:// (Строка поиска) Data= HTTPs:// (Заменяемая строка)
Капля	Это приведет к разрыву соединения	Цель = Н/Д Данные= Н/Д
Электронная почта	Отправит письмо на адрес, настроенный в Email Events. Вы можете использовать переменную в качестве адреса или сообщения	Target= "flightPATH отправил сообщение об этом событии" Данные= Н/Д
Событие в журнале	Это приведет к регистрации события в Системном журнале	Target= "flightPATH зарегистрировал это в syslog" Данные= Н/Д
Перенаправление 301	Это приведет к постоянному перенаправлению	Target= HTTP://www.edgenexus.ioData= N/A
Перенаправление 302	Это создаст временное перенаправление	Target= HTTP://www.edgenexus.ioData= N/A
Удалить Cookie запроса	Удалите cookie запроса, подробно описанные в разделе Цель	Target= Cookie Данные= MS-WSMAN=afYfn1CDqqCDqCVii
Удалить заголовок запроса	Удалите заголовок запроса, подробно описанный в разделе Цель	Target=ServerData=N/A
Удаление Cookie с ответами	Удалите ответные cookie, подробно описанные в разделе "Цель	Target=jnAccel
Удалить заголовок ответа	Удалите заголовок ответа, подробно описанный в разделе "Цель	Target= Etag Данные= Н/Д
Заменить Cookie запроса	Замените cookie запроса, указанные в разделе "Цель", значением в разделе "Данные".	Target= Cookie Данные= MS-WSMAN=afYfn1CDqqCDqCVii

Заменить заголовок запроса	Замените заголовок запроса в Цели значением данных	Цель = Соединение Data= keep-alive
Заменить Cookie ответа	Замените cookie-файл ответа, указанный в разделе "Цель", на значение в разделе "Данные".	Target=jnAccel=afYfn1CDqqCDqCViiDate=MS-WSMAN=afYfn1CDqqCDqCVii
Заменить заголовок ответа	Замените заголовок ответа, подробно описанный в разделе Target, на значение в разделе Data	Цель= Сервер Данные = Удержано в целях безопасности
Путь перезаписи	Это позволит Вам перенаправить запрос на новый URL, основываясь на условии	Target= /test/path/index.html$querystring$ Данные= Н/Д
Используйте безопасный сервер	Выберите, какой безопасный сервер или виртуальную службу использовать	Target=192.168.101: 443Data=N/A
Используйте сервер	Выберите, какой сервер или виртуальную службу использовать	Target= 192.168.101:80Data= N/A
Зашифровать Cookie	Это приведет к 3DES-шифрованию файлов cookie, а затем к их кодированию base64	Target= Введите имя cookie, которое будет зашифровано, Вы можете использовать * в качестве подстановочного знака в концеData= Введите парольную фразу для шифрования

Пример:



Приведенное ниже действие создаст временное перенаправление браузера на защищенный виртуальный сервис HTTPS. Оно будет использовать те же имя хоста, путь и строку запроса, что и запрос.

Общее применение

Брандмауэр и безопасность приложений

- Блокировать нежелательные IP-адреса
- Принуждение пользователя к HTTPS для определенного (или всего) контента
- Блокировать или перенаправлять пауков
- Предотвращение и предупреждение межсайтового скриптинга
- Предотвращение и предупреждение SQL-инъекций
- Скрыть внутреннюю структуру каталогов

- Перезапись файлов cookie
- Защищенный каталог для определенных пользователей

Особенности

- Перенаправление пользователей на основе пути
- Обеспечьте единую регистрацию в нескольких системах
- Сегментировать пользователей на основе ID пользователя или Cookie
- Добавьте заголовки для разгрузки SSL
- Определение языка
- Переписать запрос пользователя
- Исправьте неработающие URL-адреса
- Ведение журнала и оповещение по электронной почте о 404 кодах ответа
- Предотвращение доступа к каталогу/просмотра
- Отправляйте паукам различный контент

Предварительно разработанные правила

Расширение HTML

Изменяет все запросы .htm на .html

Состояние:

- Условие = Путь
- Чувствовать = Делать
- Проверка = Соответствие RegEx
- Значение = \.htm$

Оценка:

- Пустой

Действия:

- Действие = Переписать путь
- Цель = $path$l

Index.html

Принудительное использование index.html в запросах к папкам.

Условие: это условие является общим условием, которое будет соответствовать большинству объектов

- Условие = Хозяин
- Чувствовать = Делать
- Проверка = Существование

Оценка:

- Пустой

Действия:

- Действие = Перенаправление 302
- Цель = HTTP://$host$$path$index.html$querystring$

Закрыть папки

Отказывать в запросах на папки.

Условие: это условие является общим условием, которое будет соответствовать большинству объектов

- Состояние = об этом нужно как следует подумать
- Чувство =
- Проверка =

Оценка:

- Пустой

Действия:

- Действие =
- Цель =

Спрячьте CGI-BBIN:

Скрывает каталог cgi-bin в запросах к CGI-скриптам.

Условие: это условие является общим условием, которое будет соответствовать большинству объектов

- Условие = Хозяин
- Чувствовать = Делать
- Проверка = Соответствие RegEX
- Значение = \.cgi$

Оценка:

- Пустой

Действия:

- Действие = Переписать путь
- Цель = /cgi-bin$path$

Бревно-паук

Ведите журнал запросов пауков популярных поисковых систем.

Условие: это условие является общим условием, которое будет соответствовать большинству объектов

- Условие = Заголовок запроса
- Соответствие = User-Agent
- Чувствовать = Делать
- Проверка = Соответствие RegEX
- Значение = Googlebot|Slurp|bingbot|ia_archiver

Оценка:

- Переменная = $crawler$
- Источник = Заголовок запроса
- Деталь = User-Agent

Действия:

- Действие = Зарегистрировать событие
- Цель = [$crawler$] $host$$path$$$querystring$

Принудительное использование HTTPS

Принудительно использовать HTTPS для определенной директории. В этом случае, если клиент обращается к чему-либо, содержащему каталог /secure/, то он будет перенаправлен на HTTPs версию запрашиваемого URL.

Состояние:

- Условие = Путь
- Чувствовать = Делать
- Проверять = Содержать
- Значение = /secure/

Оценка:

- Пустой

Действия:

- Действие = Перенаправление 302
- Цель = HTTPs://$host$$path$$querystring$

Медиапоток:

Перенаправляет Flash Media Stream на соответствующую службу.

Состояние:

- Условие = Путь
- Чувствовать = Делать
- Проверка = Конец
- Значение = .flv

Оценка:

- Пустой

Действия:

- Действие = Перенаправление 302
- Цель = HTTP://$host$:8080/$path$

Замена HTTP на HTTPS

Измените любой жестко закодированный HTTP:// на HTTPS://

Состояние:

- Условие = Код ответа
- Чувствовать = Делать
- Проверка = Равно
- Значение = 200 OK

Оценка:

- Пустой

Действия:

- Действие = Тело Заменить все
- Цель = HTTP://
- Данные = HTTPs://

Заглушите кредитные карты

Проверьте, нет ли в ответе кредитных карт, и если таковая найдена, удалите ее.

Состояние:

- Условие = Код ответа
- Чувствовать = Делать
- Проверка = Равно
- Значение = 200 OK

Оценка:

- Пустой

Действия:

- Действие = Тело Заменить все
- Target = [0-9]+[0-9]+[0-9]+[0-9]+-[0-9]+[0-9]+[0-9]+[0-9]+-[0-9]+[0-9]+[0-9]+[0-9]+-[0-9]+[0-9]+[0-9]+[0-9]+
- Данные = xxxx-xxx-xxx-xxx-xxx

Срок годности контента

Добавьте на страницу разумный срок годности контента, чтобы уменьшить количество запросов и 304.

Условие: это общее условие. Рекомендуется сосредоточить это условие на Ваших

- Условие = Код ответа
- Чувствовать = Делать
- Проверка = Равно
- Значение = 200 OK

Оценка:

- Пустой

Действия:

- Действие = Добавить заголовок ответа
- Цель = Cache-Control
- Данные = max-age=3600

Тип поддельного сервера

Получите тип сервера и измените его на какой-либо другой.

Условие: это общее условие. Рекомендуется сосредоточить это условие на Ваших

- Условие = Код ответа

- Чувствовать = Делать
- Проверка = Равно
- Значение = 200 OK

Оценка:

- Пустой

Действия:

- Действие = Заменить заголовок ответа
- Цель = Сервер
- Данные = Секрет

Никогда не отправляйте ошибки

Клиент никогда не получает никаких ошибок с Вашего сайта.

Состояние

- Условие = Код ответа
- Чувствовать = Делать
- Проверять = Содержать
- Значение = 404

Оценка

- Пустой

Действие

- Действие = Перенаправление 302
- Цель = HTTP//$host$/

Перенаправление на язык

Найдите код языка и перенаправьте на домен соответствующей страны.

Состояние

- Условие = Язык
- Чувствовать = Делать
- Проверять = Содержать
- Значение = Немецкий (Стандарт)

Оценка

- Переменная = $host_template$
- Источник = Хозяин
- Значение = .*\.

Действие

- Действие = Перенаправление 302
- Цель = HTTP//$host_template$de$path$$querystring$

Google Analytics

Вставьте код, требуемый Google для аналитики - Пожалуйста, измените значение MYGOOGLECODE на Ваш Google UA ID.

Состояние

- Условие = Код ответа
- Чувствовать = Делать
- Проверка = Равно
- Значение = 200 OK

Оценка

- пустой

Действие

- Действие = Тело Заменить Последнее
- Цель = </body>
- Data = <scripttype= 'text/javascript'> var _gaq = _gaq || []; _gaq.push(['_setAccount', 'MY GOOGLE CODE']); _gaq.push(['_trackPageview']); (function() { var ga = document.createElement('script'); ga.type = 'text/javascript'; ga.async = true; ga.src = ('HTTPs' == document.location.protocol ?'HTTPs//ssl' 'HTTP//www') + '.google-analytics.com/ga.js'; var s = document.getElementsByTagName('script')[0];s.parentNode.insertBefore(ga, s); })(); </script> </body>

Шлюз IPv6

Настройка заголовка Host для серверов IIS IPv4 на службах IPv6. Серверы IIS IPv4 не любят видеть IPV6 адрес в запросе клиента хоста, поэтому данное правило заменяет его общим именем.

Состояние

- пустой

Оценка

- пустой

Действие

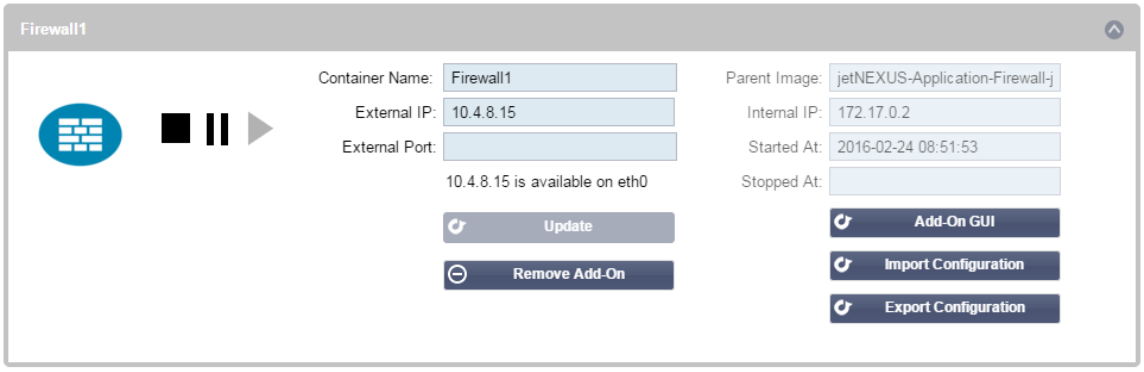
- Действие = Заменить заголовок запроса
- Цель = Хозяин
- Данные =ipv4.host.header

Брандмауэр веб-приложений (edgeWAF)

Брандмауэр веб-приложений (WAF) предоставляется по запросу и лицензируется на ежегодной платной основе. Установка WAF производится с помощью встроенного раздела Apps в ADC.

Запуск WAF

Работающий в контейнере Docker Container, WAF требует установки некоторых сетевых параметров перед запуском.

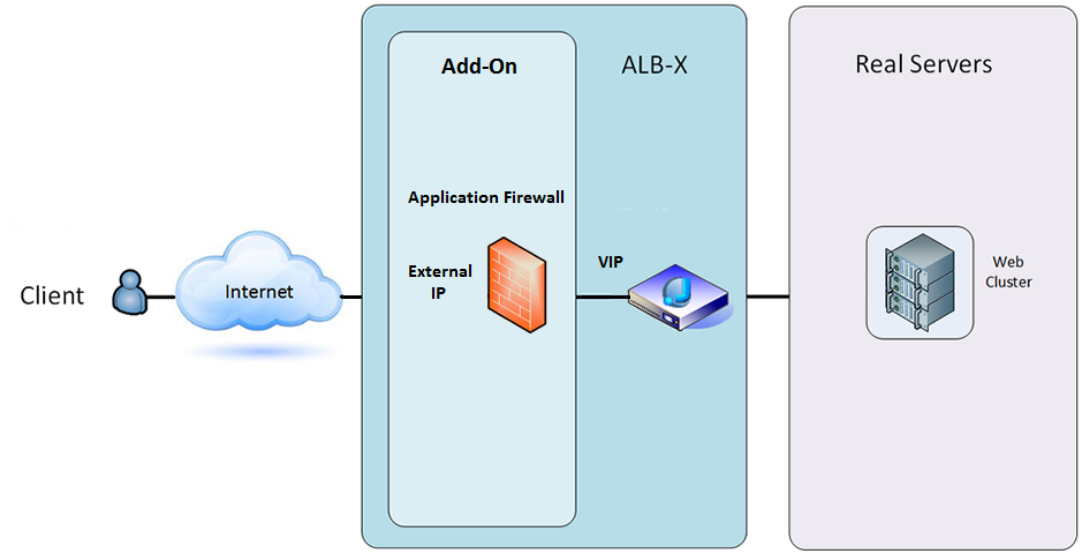


Вариант	Описание
Остановитесь	Она будет серой, пока не будет запущен экземпляр Add-On. Нажмите эту кнопку, чтобы остановить экземпляр Docker.
Пауза	Эта кнопка приостановит работу Дополнения.
Играть	Это запустит Дополнение с текущими настройками.
Название контейнера	Дайте своему контейнеру имя, чтобы идентифицировать его среди других контейнеров. Оно должно быть уникальным. При желании Вы можете использовать это имя в качестве имени для реального сервера, и оно будет автоматически разрешаться во внутренний IP-адрес экземпляра
Внешний IP	Здесь Вы можете установить внешний IP для доступа к Вашей надстройке. Это может быть доступ к графическому интерфейсу надстройки, а также к службе, которая работает через надстройку. В случае надстройки Firewall это IP-адрес Вашего HTTP-сервиса. Брандмауэр может быть настроен на доступ к серверу или ALB-X VIP, который содержит несколько серверов для балансировки нагрузки.
Внешний порт	Если Вы оставите это поле пустым, то все порты будут перенаправлены в Ваш брандмауэр. Чтобы ограничить это, просто добавьте список портов, разделенных запятыми. Пример 80, 443, 88. Обратите внимание, что адрес GUI брандмауэра будет **HTTP//[Внешний IP]88/waf.** Поэтому либо оставьте параметр Внешний порт пустым, либо добавьте порт 88 для доступа к графическому интерфейсу, если Вы ограничиваете список портов.
Обновление	Вы можете обновить настройки Дополнительного модуля только после его остановки. После остановки Вашего экземпляра Вы можете изменить имя контейнера, настройки внешнего IP и внешнего порта.
Удалить дополнение	Полностью удалит Дополнение со страницы Дополнения. Вам нужно будет перейти на страницу Library-Apps, чтобы снова развернуть Дополнение.
Образ родителя	Указывает образ Docker, из которого собрана надстройка. Может существовать несколько версий брандмауэра или другого типа дополнений, поэтому это

	поможет отличить их друг от друга. Этот раздел предназначен только для информационных целей и поэтому выделен серым цветом.
Внутренний IP	Docker автоматически создает внутренний IP-адрес и, следовательно, его нельзя редактировать. Если Вы остановите экземпляр Docker и перезапустите его, будет выдан новый внутренний IP-адрес. Именно по этой причине Вам следует либо использовать внешний IP-адрес для Вашей службы, либо использовать имя контейнера для реального адреса сервера Вашей службы.
Начато в	Здесь будет указана дата и время запуска Дополнения. Пример 2016-02-16 155721
Остановился на	Здесь будет указана дата и время, когда дополнение было остановлено. Пример 2016-02-24 095839

Пример архитектуры

WAF с использованием внешнего IP-адреса

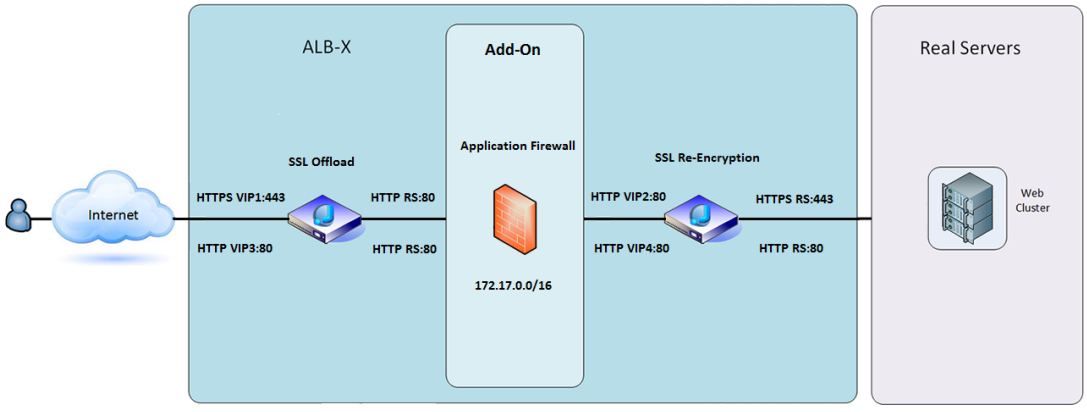


В этой архитектуре для Вашего сервиса можно использовать только HTTP, поскольку брандмауэр не может проверять HTTPS-трафик.

Брандмауэр должен быть настроен на передачу трафика на ALB-X VIP.

ALB-X VIP, в свою очередь, будет настроен для балансировки нагрузки трафика на Ваш веб-кластер.

WAF, использующий внутренний IP-адрес



В этой архитектуре Вы можете указать HTTP и HTTPS.

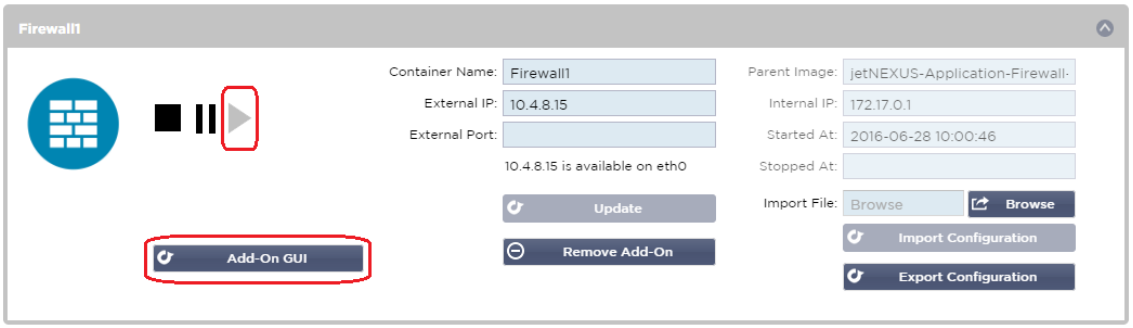
HTTPS может быть сквозным, когда шифруются соединения от Клиента к ALB-X и от ALB-X к реальным серверам.

Трафик от ALB-X до внутреннего IP-адреса брандмауэра должен быть незашифрованным, чтобы его можно было проверить.

После того, как трафик прошел через брандмауэр, он направляется на другой VIP, который может либо повторно зашифровать трафик и распределить нагрузку на безопасные серверы, либо просто распределить нагрузку на незащищенные серверы по HTTP.

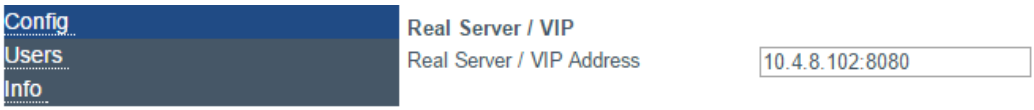
Доступ к Вашему дополнению WAF

- Заполните данные для Вашего брандмауэра
- Вы можете ограничить порты только теми, которые Вам нужны, или оставить это поле пустым, чтобы разрешить все порты.
- Нажмите кнопку Воспроизведение
- Появится кнопка Add-On GUI

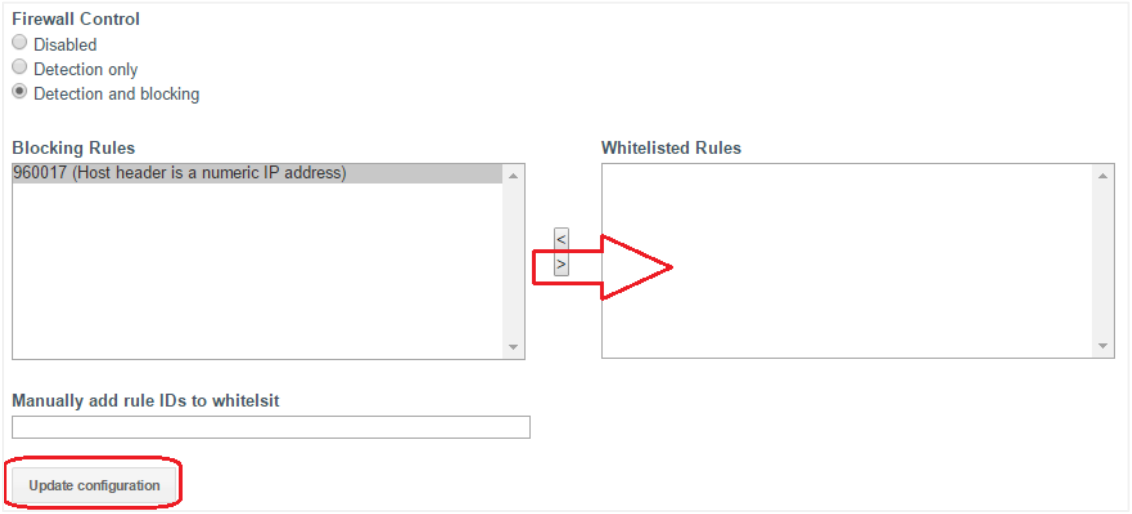


- Нажмите на эту кнопку, и откроется браузер на HTTP://[внешний IP]:88/waf
- В данном примере это будет HTTP://10.4.8.15:88/waf
- Перед Вами откроется диалог входа в систему.
- Введите учетные данные для Вашего ADC.
- После успешного входа в систему перед Вами откроется главная страница WAF.

- На главной странице отображается графический обзор событий, т.е. действий по фильтрации, выполняемых Брандмауэром приложений.
- Графики, скорее всего, будут пустыми, когда Вы впервые откроете страницу, поскольку не будет попыток доступа через брандмауэр.
- Вы можете настроить IP-адрес или доменное имя сайта, на который Вы хотите направить трафик после того, как брандмауэр отфильтрует его.
- Это можно изменить в разделе Управление > Конфигурация



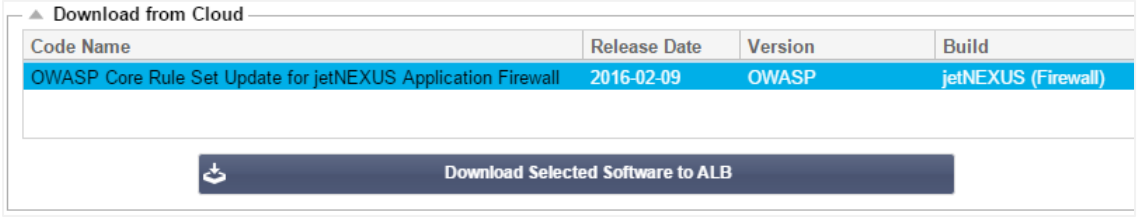
- Брандмауэр проверит трафик и затем отправит его на IP-адрес реального сервера или VIP-адрес, указанный здесь. Вы также можете ввести порт вместе с IP-адресом. Если Вы введете IP-адрес сам по себе, порт будет считаться портом 80. Нажмите кнопку "Обновить конфигурацию", чтобы сохранить новые настройки.
- Когда брандмауэр блокирует ресурс приложения, правило, блокирующее трафик, появится в списке Blocking Rules на странице Whitelist.
- Чтобы брандмауэр не блокировал ресурс действующего приложения, переместите правило блокировки в раздел "Правила белого списка".



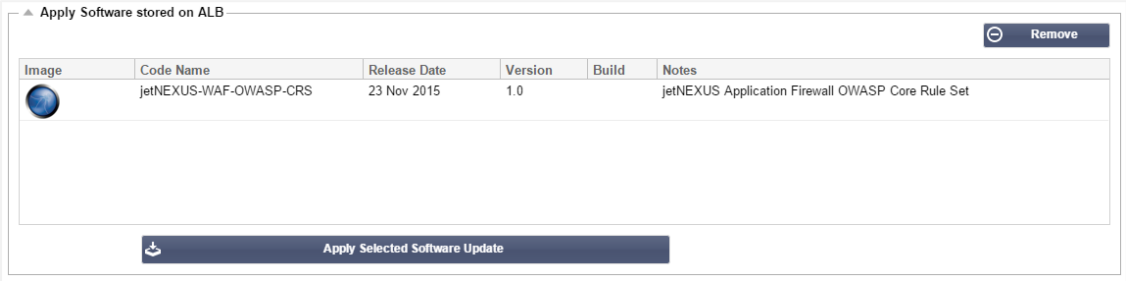
- Нажмите Update Configuration, когда Вы перенесли все правила из раздела Blocking в раздел Whitelist.

Обновление правил

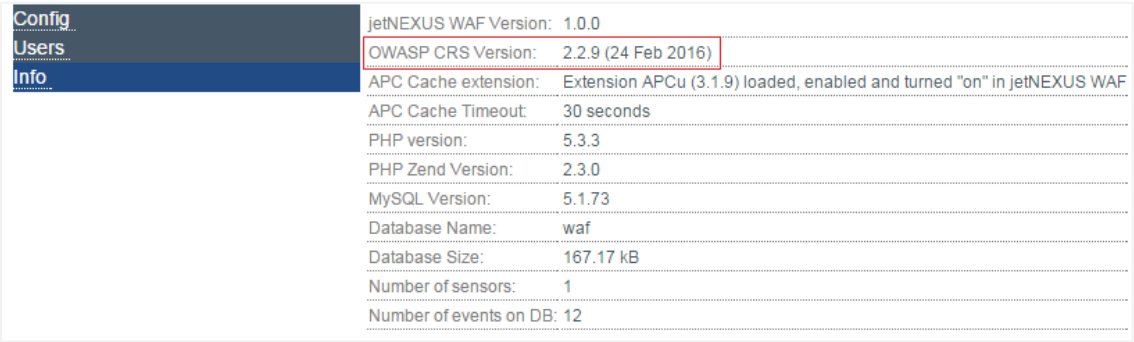
- Правила брандмауэра приложений можно обновить, зайдя в раздел Дополнительно - Программное обеспечение
- Нажмите кнопку Обновить для просмотра доступного программного обеспечения в разделе Подробности обновления программного обеспечения
- Теперь отображается дополнительное поле под названием Загрузить из облака
- Проверьте, имеется ли набор основных правил OWASP.



- Если это так, Вы можете выделить и нажать Загрузить выбранное программное обеспечение в ALB-X
- Это действие затем загрузит смарт-файл в прикладное программное обеспечение, хранящееся на ALB



- Выделите jetNEXUS-WAF-OWASP-CRS и нажмите Применить Выбранное обновление ПО и нажмите Применить
- Брандмауэр автоматически обнаружит обновленный набор правил, загрузит и применит его.
- Идентификаторы правил "белого списка" будут сохранены. Однако новые правила могут начать блокировать действительные ресурсы приложения.
- В этом случае проверьте список правил блокировки на странице "Белый список".
- Вы также можете проверить раздел "Информация об управлении" в графическом интерфейсе брандмауэра на наличие версии OWASP CRS



Глобальная балансировка нагрузки сервера (edgeGSLB)

Введение

Глобальная балансировка нагрузки серверов (GSLB) - это термин, используемый для описания методов распределения сетевого трафика по Интернету. GSLB отличается от балансировки нагрузки серверов (SLB) или балансировки нагрузки приложений (ALB), поскольку обычно используется для распределения трафика между несколькими центрами обработки данных, тогда как традиционные ADC/SLB используются для распределения трафика в пределах одного центра обработки данных.

GSLB обычно используется в следующих ситуациях:

Устойчивость и аварийное восстановление

У Вас есть несколько центров обработки данных, и Вы хотите запустить их в активно-пассивной ситуации, чтобы в случае отказа одного центра обработки данных трафик направлялся в другой.

Балансировка нагрузки и геолокация

Вы хотите распределить трафик между центрами обработки данных в ситуации Active-Active на основе определенных критериев, таких как производительность центра обработки данных, возможности центра обработки данных, проверка состояния центра обработки данных, физическое местоположение клиента (чтобы Вы могли отправить его в ближайший центр обработки данных) и т.д.

Коммерческие соображения

Убедитесь, что пользователи из определенных географических мест направляются в определенные центры обработки данных. Обеспечить, чтобы другим пользователям предоставлялся (или блокировался) различный контент, в зависимости от нескольких критериев, таких как страна, в которой находится клиент, ресурс, который он запрашивает, язык и т.д.

Обзор системы доменных имен

GSLB может быть сложным; поэтому стоит потратить время на то, чтобы понять, как работает загадочная система сервера доменных имен (DNS).

DNS состоит из трех ключевых компонентов:

- DNS resolver, т.е. Клиент: resolver отвечает за инициирование запросов, которые в конечном итоге приводят к полному разрешению требуемого ресурса.
- Сервер имен: это сервер имен, к которому клиент первоначально подключается для выполнения разрешения DNS.
- Авторитетные серверы имен: Включите серверы имен домена верхнего уровня (TLD) и корневые серверы имен.

Типичная транзакция DNS описана ниже:

- Пользователь вводит 'example.com' в веб-браузере, запрос отправляется в Интернет и принимается рекурсивным резольвером DNS.
- Затем резольвер запрашивает корневой сервер имен DNS (.).

- Затем корневой сервер отвечает резольверу адресом DNS-сервера домена верхнего уровня (TLD) (например, .com или .net), который хранит информацию для своих доменов. При поиске example.com наш запрос направлен на ДВУ .com.
- Затем преобразователь запрашивает ДВУ .com.
- Затем сервер TLD отвечает IP-адресом сервера имен домена example.com.
- Наконец, рекурсивный преобразователь посылает запрос серверу имен домена.
- Затем IP-адрес, например, example.com, возвращается резольверу от сервера имен.
- Затем DNS-резольвер отвечает веб-браузеру IP-адресом первоначально запрошенного домена.
- После того, как восемь этапов поиска DNS вернули IP-адрес, например, example.com, браузер может запросить веб-страницу:
- Браузер делает HTTP-запрос на IP-адрес.
- Сервер на этом IP возвращает веб-страницу для отображения в браузере.

Этот процесс может быть еще более сложным:

Кэширование

Серверы преобразования имен кэшируют ответы и могут отправлять один и тот же ответ многим клиентам. Резолверы на стороне клиента и приложения могут иметь различные политики кэширования.

Примечание: Для тестирования мы остановим и отключим DNS-клиент Windows в разделе служб Вашей операционной системы. Имена DNS будут продолжать разрешаться; однако, он не будет кэшировать результаты или регистрировать имя компьютера. Ваш системный администратор должен решить, является ли это лучшим вариантом для Вашей среды, поскольку это может повлиять на другие службы.

Время жить

Разрешающий сервер имен может игнорировать Time To Live (TTL), т.е. время кэширования ответа.

Обзор GSLB

GSLB основан на DNS и использует очень похожий механизм, описанный выше.

ADC может изменить ответ на основании нескольких факторов, описанных далее в руководстве. ADC использует мониторы, проверяющие доступность удаленных ресурсов, обращаясь к самому ресурсу. Однако, чтобы применить любую логику, система должна сначала получить DNS-запрос.

Это возможно в нескольких вариантах. Первая - когда GSLB выступает в качестве авторитетного сервера имен.

Второй вариант является наиболее распространенной реализацией и похож на конфигурацию авторитарного сервера имен, но использует поддомен. Основной авторитетный DNS-сервер не заменяется GSLB, но делегирует поддомен для разрешения. Либо прямое делегирование имен, либо использование CNAME позволяет Вам контролировать, что обрабатывается, а что нет GSLB. В этом случае Вам не нужно направлять весь DNS-трафик на GSLB для систем, которым не требуется GSLB.

Резервирование обеспечивается таким образом, что если один сервер имен (GSLB) выходит из строя, то удаленный сервер имен автоматически отправляет другой запрос на другой GSLB, предотвращая падение сайта.

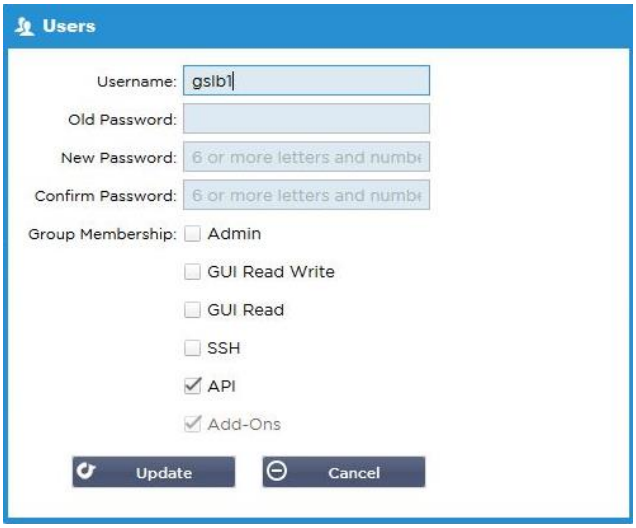
Конфигурация GSLB

После загрузки GSLB Add-On, пожалуйста, разверните его, посетив страницу Library > Apps в графическом интерфейсе ADC GUI и нажав кнопку "Deploy", как показано ниже.

После установки, пожалуйста, настройте детали GSLB Add-On, включая имя контейнера, внешний IP и внешние порты на странице Library > Add-Ons графического интерфейса ADC, как показано на рисунке ниже.

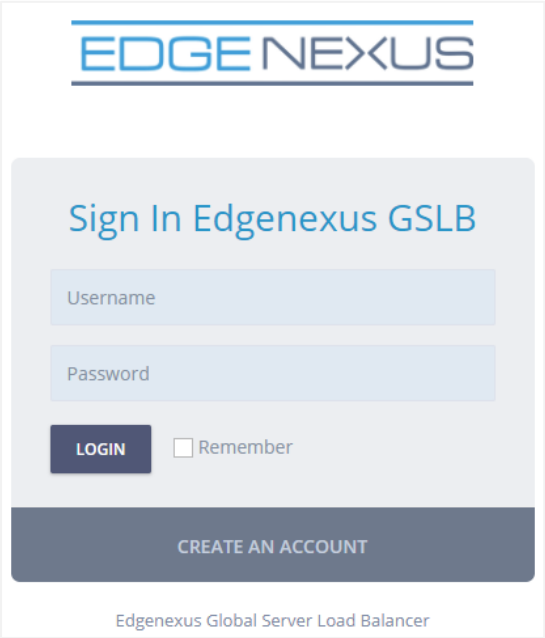
- Имя контейнера - это уникальное имя запущенного экземпляра Add-On, размещенного в ADC, оно используется для различения нескольких Add-On одного типа.
- Внешний IP - это IP в Вашей сети, который будет назначен GSLB.
- Вы должны настроить GSLB на внешний IP-адрес, если Вы хотите принимать решения на основе GEO, так как это позволит GSLB видеть реальный IP-адрес клиента.
- Внешние порты - это список TCP и UDP портов GSLB, к которым можно получить доступ из других сетевых узлов.
- Пожалуйста, поставьте "53/UDP, 53/TCP, 9393/TCP" в поле ввода Внешние порты, чтобы разрешить DNS (53/UDP, 53/TCP) и связь edgeNEXUS GSLB GUI (9393/TCP).
- После настройки деталей Дополнения, пожалуйста, нажмите кнопку Обновить.
- Запустите GSLB Add-On, нажав на кнопку Run.

- Следующий шаг - позволить edgeNEXUS GSLB Add-On считывать и изменять конфигурацию АЦП.
- Посетите страницу Система > Пользователи в графическом интерфейсе ADC GUI и отредактируйте пользователя с тем же именем, что и GSLB Add-On, который Вы развернули, как показано на рисунке ниже.
- Отредактируйте пользователя "gslb1" и отметьте API, затем нажмите Обновить - в более поздних версиях программного обеспечения галочка может быть уже установлена по умолчанию.



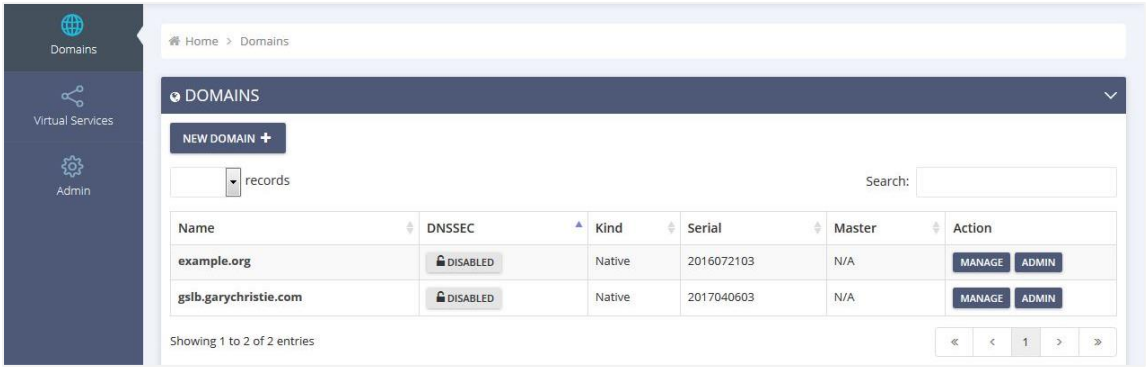
- Следующий шаг необходим только в том случае, если Вы настраиваете GSLB в целях тестирования или оценки и не хотите изменять данные зон DNS в Интернете.
- В этом случае, пожалуйста, проинструктируйте ADC использовать GSLB Add-On в качестве основного сервера разрешения DNS, изменив "DNS Server 1" на странице System > Network графического интерфейса ADC, как показано на рисунке ниже.
- DNS-сервер 2 может быть настроен, как правило, на Ваш локальный DNS-сервер или на сервер в интернете, например, Google 8.8.8.8.

- Теперь самое время войти в GSLB GUI.
- Пожалуйста, перейдите на страницу Library > Add-Ons в графическом интерфейсе ADC GUI и нажмите кнопку Add-On GUI.
- При нажатии откроется новая вкладка браузера, на которой будет представлена страница входа в GSLB GUI, как показано ниже.

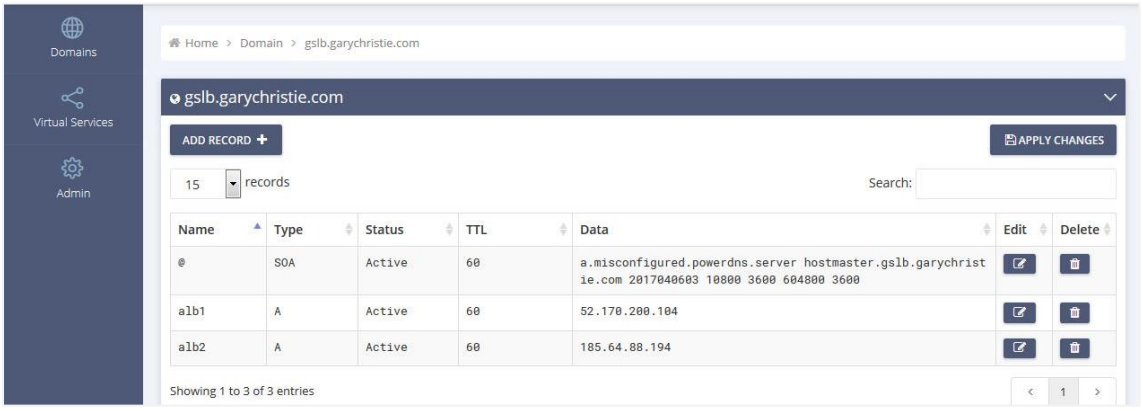


- Имя пользователя по умолчанию - admin, а пароль по умолчанию - jetnexus. Пожалуйста, не забудьте изменить пароль на странице Администратор > Мой профиль в графическом интерфейсе GSLB.
- Следующим шагом в последовательности настройки является создание зоны DNS в сервере имен PowerDNS, который является частью GSLB, делая его либо авторитетным сервером имен для зоны "example.org", либо зоной поддомена, такой как поддомен "geo.example.org", упомянутый в разделе "Обзор GSLB на основе DNS" выше.
- Для получения подробной информации о конфигурации зоны DNS обратитесь к **ДОКУМЕНТАЦИИ ПО POWERDNS NAMESERVER**. Пример зоны показан на рисунке 6.

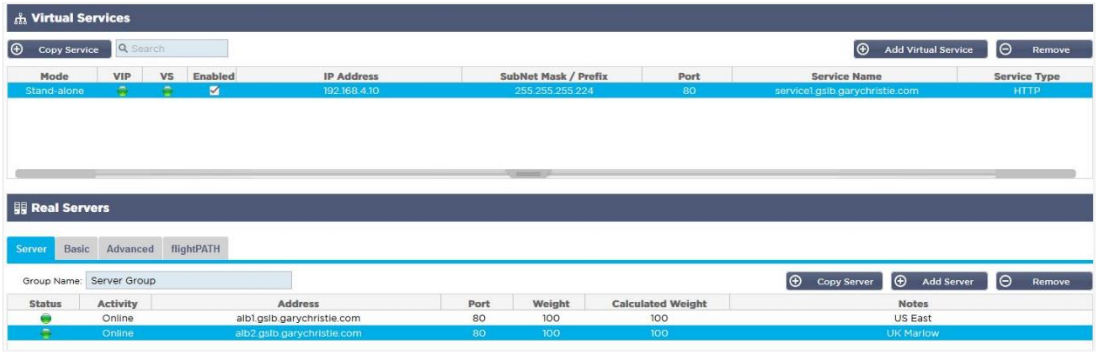
* edgeNEXUS GSLB GUI основан на проекте с открытым исходным кодом PowerDNS-Admin.



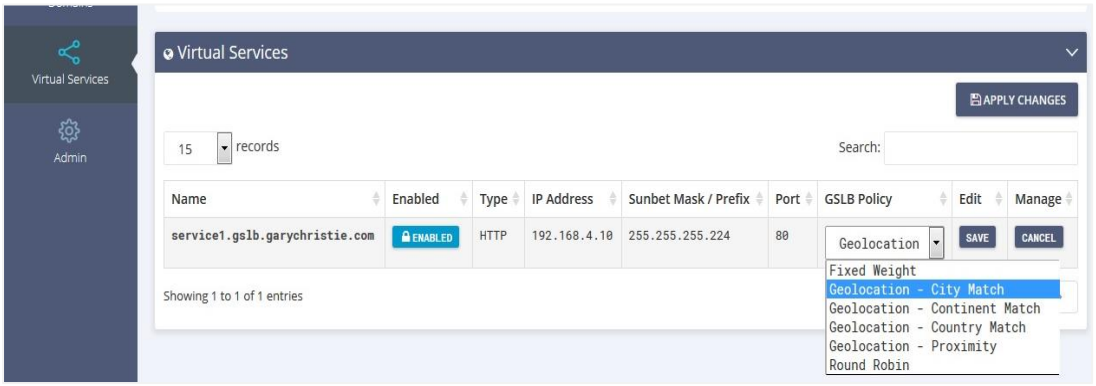
- После создания зоны DNS, пожалуйста, нажмите кнопку Manage и добавьте имена хостов в домен, как показано на рисунке ниже.
- После редактирования существующих записей в графическом интерфейсе GSLB, пожалуйста, нажмите кнопку Сохранить.
- После завершения создания записей имен хостов, пожалуйста, нажмите кнопку Применить изменения. Если Вы не нажмете кнопку Применить, а затем измените страницу, Вы потеряете свои изменения.
- Ниже мы создали записи, которые являются записями адресов IPv4.
- Пожалуйста, убедитесь, что Вы создали запись для всех записей, которые Вы хотите разрешить, включая записи AAAA для адресов IPv6.



- Теперь давайте вернемся к графическому интерфейсу ADC и определим виртуальную службу, соответствующую только что созданной зоне DNS.



- Виртуальная служба будет использоваться для проверки здоровья серверов в домене GSLB.
- GSLB использует механизм проверки работоспособности ADC, включая пользовательские мониторы. Его можно использовать с любым из типов услуг, поддерживаемых ADC.
- Перейдите на страницу Services > IP-Services графического интерфейса ADC и создайте виртуальную службу, как показано на рисунке ниже.
- Обязательно настройте Имя службы на правильное доменное имя, которое Вы хотите использовать в GSLB. GSLB прочитает это через API и автоматически заполнит раздел Виртуальные службы в графическом интерфейсе GSLB.
- Пожалуйста, добавьте все серверы в домене GSLB в разделе Real Servers вышеуказанного изображения.
- Вы можете указать серверы либо по их доменным именам, либо по IP-адресам.
- Если Вы укажете доменные имена, то будут использоваться записи, созданные на Вашей GSLB.
- Вы можете выбрать различные методы и параметры мониторинга здоровья сервера на вкладках Basic и Advanced.
- Вы можете установить активность некоторых серверов в режим ожидания для сценария Active-Passive.
- В этом случае, если сервер "Online" не прошел проверку работоспособности, а есть здоровый резервный сервер, Edgenexus EdgeGSLB преобразует доменное имя в адрес резервного сервера.
- Обратитесь к разделу **ВИРТУАЛЬНЫЕ СЛУЖБЫ** для получения подробной информации о настройке виртуальных служб.
- Теперь давайте перейдем к графическому интерфейсу GSLB.
- Перейдите на страницу Виртуальные службы и выберите политику GSLB для домена API, полученную из раздела Виртуальные службы ADC.
- Это показано на рисунке ниже.



- GSLB поддерживает следующие политики:

Политика	Описание

Фиксированный вес	GSLB выбирает сервер с наибольшим весом (вес сервера может быть назначен пользователем). В случае, если несколько серверов имеют наибольший вес, GSLB выберет один из этих серверов случайным образом.
Взвешенная круговая тренировка	Выбирайте серверы один за другим, подряд. Серверы с большим весом выбираются чаще, чем серверы с меньшим весом.
Геолокация	Близость - выбирайте сервер, который расположен ближе всего к местоположению клиента, используя данные географической широты и долготы. Серверы в той же стране, что и клиент, являются предпочтительными, даже если они более удалены, чем серверы в соседних странах.
Геолокация	Соответствие городу - выберите сервер в том же городе, что и клиент. Если в городе клиента нет сервера, выберите сервер в стране клиента. Если в стране клиента нет сервера, выберите сервер на том же континенте. Если это невозможно, выберите сервер, который расположен ближе всего к местоположению клиента, используя данные географической широты и долготы.
Геолокация	Соответствие стране - выбор сервера в той же стране, что и клиент. Если нет сервера в той же стране, попробуйте сервер на том же континенте, затем попробуйте ближайший.
Геолокация	Соответствие континенту - выберите сервер на том же континенте, что и клиент. Если нет сервера на том же континенте, попробуйте выбрать ближайший.

- После того, как Вы выбрали политику GSLB, не забудьте нажать кнопку Применить изменения.
- Теперь Вы можете просмотреть и скорректировать детали виртуальной услуги, нажав на кнопку Manage (Управление).
- В результате откроется страница, показанная ниже.
- Если Вы выбрали одну из политик на основе веса, Вам может понадобиться настроить веса GSLB сервера.
- Если Вы выбрали одну из политик GSLB на основе геолокации, Вам может понадобиться указать географические данные для серверов.
- Если Вы не укажете никаких географических данных для серверов, GSLB будет использовать данные, предоставленные **БАЗОЙ ДАННЫХ MAXMIND'S GEOLITE2**.
- Вы также можете изменить имя сервера, порт и активность на этой странице.
- Эти изменения будут синхронизированы с АЦП, когда Вы нажмете кнопку "Применить изменения".

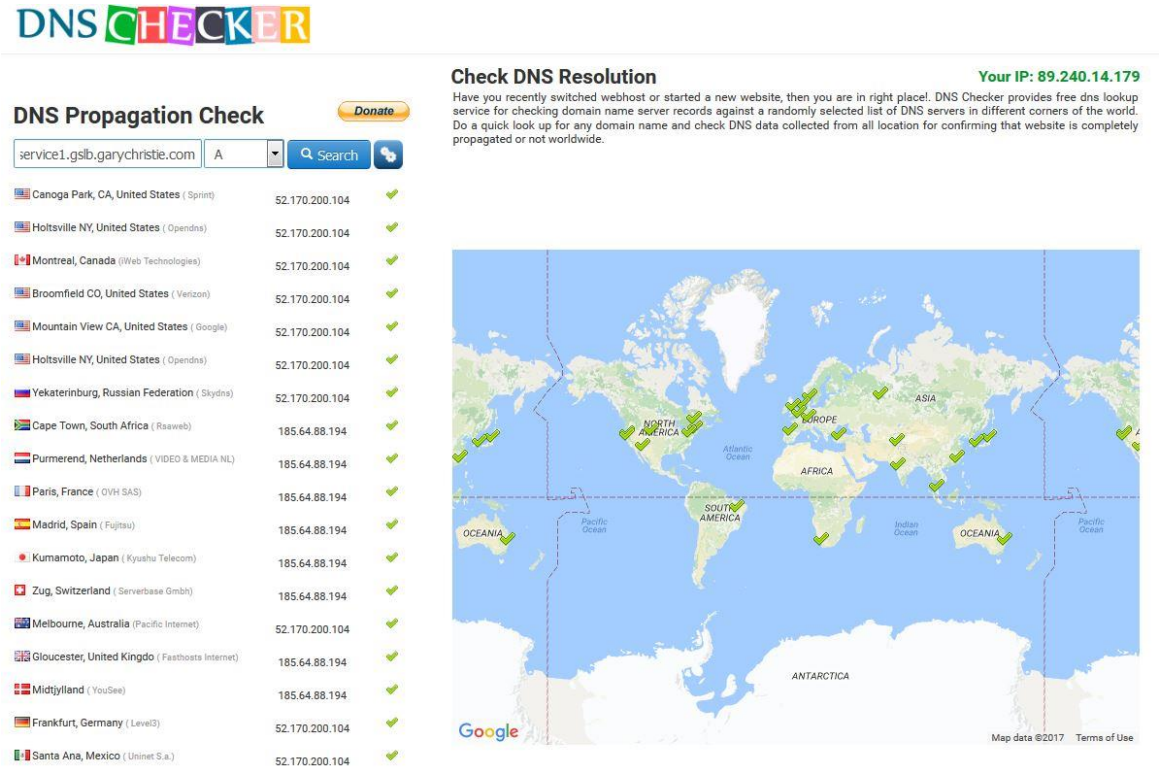
- Отличный способ проверить, какие ответы GSLB отправит обратно клиентам, - это использовать NSLOOKUP.
- Если Вы используете Windows, команда приведена ниже.

```
NSLOOKUP service1.gslb.garychristie.com 192.168.4.10
```

- Где service1.gslb.garychristie.com - это доменное имя, которое Вы хотите разрешить.
- Где 192.168.4.10 - это внешний IP-адрес Вашего GSLB.
- Чтобы проверить, какой IP-адрес будет выдаваться в интернете, Вы можете использовать DNS-сервер google 8.8.8.8.

```
Nslookup service1.gslb.garychristie.com 8.8.8.8.
```

- В качестве альтернативы Вы можете использовать что-то вроде HTTPs://dnschecker.org. Пример HTTPs://dnschecker.org/#A/service1.gslb.garychristie.com.
- Смотрите ниже пример результатов.



Пользовательские местоположения

Частные сети

GSLB также может быть настроен на использование пользовательских местоположений, чтобы Вы могли использовать его во внутренних "частных" сетях. В приведенном выше сценарии GSLB определяет местоположение клиента путем перекрестного сопоставления публичного IP-адреса клиента с базой данных для определения его местоположения. Он также определяет местоположение IP-адреса службы по той же базе данных, и если политика балансировки нагрузки установлена на политику GEO, он вернет ближайший IP-адрес. Этот метод отлично работает с публичными IP-адресами, но нет такой базы данных для внутренних частных адресов, которые соответствуют RFC 1918 для IPv4-адресов и RFC 4193 для IPv6-адресов.

См. страницу Википедии, объясняющую частную адресацию
HTTPS://EN.WIKIPEDIA.ORG/WIKI/PRIVATE_NETWORK

Как это работает

Обычно идея использования GSLB для внутренних сетей заключается в том, чтобы пользователи с определенных адресов получали разные ответы на услугу в зависимости от того, в какой сети они находятся. Итак, рассмотрим два дата-центра, Северный и Южный, предоставляющие услугу под названием north.service1.gslb.com и south.service1.gslb.com, соответственно. Когда пользователь из северного дата-центра запрашивает GSLB, мы хотим, чтобы GSLB ответил IP-адресом, связанным с north.service1.gslb.com, при условии, что сервис работает правильно. Или же, если пользователь из южного центра данных обращается к GSLB, мы хотим, чтобы GSLB ответил IP-адресом, связанным с south.service1.gslb.com, при условии, что сервис работает правильно.

Итак, что нам нужно сделать, чтобы реализовать вышеописанный сценарий?

- Нам необходимо иметь как минимум два пользовательских местоположения, по одному для каждого дата-центра
- Назначьте различные частные сети на эти места
- Назначьте каждую услугу соответствующему месту

Как настроить этот вид на GSLB?

Добавить местоположение для Северного центра обработки данных

- Нажмите на Custom Locations (Пользовательские местоположения) с левой стороны
- Нажмите Добавить местоположение
- Имя
  - Север
- Добавьте частный IP-адрес и маску подсети для Вашей Северной сети. Для этого упражнения мы предположим, что IP-адреса службы и клиента находятся в одной частной сети
  - 10.1.1.0/24
- Добавьте код континента
  - ЕС
- Добавьте код страны
  - ВЕЛИКОБРИТАНИЯ
- Добавить город
  - Энфилд
- Добавить широту - получено из Google
  - 51.6523
- Добавьте долготу - получено из google
  - 0.0807

Обратите внимание, пожалуйста, используйте правильный код, который можно получить здесь

Добавить местоположение для Южного центра обработки данных

- Нажмите на Custom Locations (Пользовательские местоположения) с левой стороны
- Нажмите Добавить местоположение
- Имя
  - Юг
- Добавьте частный IP-адрес и маску подсети для Вашей Южной сети. В этом упражнении мы будем считать, что IP-адреса службы и клиента находятся в одной частной сети.
  - 192.168.1.0/24
- Добавьте код континента
  - ЕС
- Добавьте код страны
  - ВЕЛИКОБРИТАНИЯ
- Добавить город

    - Кройдон
- Добавить широту - получено из Google
    - 51.3762
- Добавьте долготу - получено из google
    - 0.0982

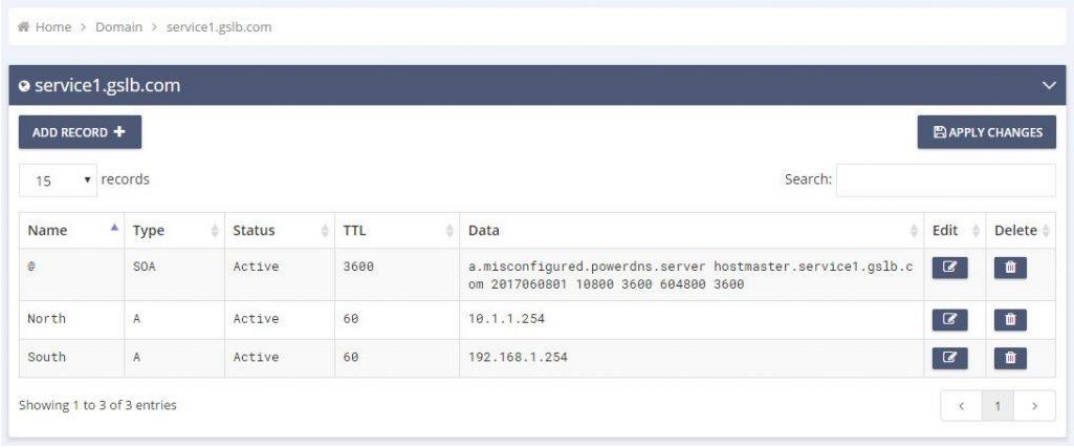
Обратите внимание, пожалуйста, используйте правильный код, который можно получить **ЗДЕСЬ**

Добавьте запись A для north.service1.gslb.com

- Щелкните на домене service1.gslb.com
- Нажмите кнопку Добавить запись
- Добавить имя
    - Север
- Тип
    - A
- Статус
    - Активный
- TTL
    - 1 мин.
- IP-адрес
    - 10.1.1.254 (Обратите внимание, что он находится в той же сети, что и местоположение Enfield)

Добавьте запись A для south.service1.gslb.com

- Щелкните на домене service1.gslb.com
- Нажмите кнопку Добавить запись
- Добавить имя
    - Юг
- Тип
    - A
- Статус
    - Активный
- TTL
    - 1 мин.
- IP-адрес
    - 192.168.1.254 (Обратите внимание, что это находится в той же сети, что и местоположение Кройдон)



Транспортный поток

Пример 1 - Клиент в северном дата-центре

- Клиент IP 10.1.1.23 запрашивает GSLB для service1.gslb.com
- GSLB ищет IP-адрес 10.1.1.23 и сопоставляет его с Custom Location Enfield 10.1.1.0/24
- GSLB просматривает свои записи A для service1.gslb.com и сопоставляет north.service1.gslb.com, поскольку он также находится в сети 10.1.1.0/24
- GSLB отвечает на 10.1.1.23 с IP-адресом 10.1.1.254 для service1.gslb.com

Пример 2 - Клиент в южном дата-центре

- Клиентский IP 192.168.1.23 запрашивает GSLB для service1.gslb.com
- GSLB ищет IP-адрес 192.168.1.23 и сопоставляет его с Custom Location Croydon 192.168.1.0/24
- GSLB просматривает свои записи A для service1.gslb.com и сопоставляет south.service1.gslb.com, поскольку он также находится в сети 192.168.1.0/24
- GSLB отвечает на 192.168.1.23 с IP-адресом 192.168.1.254 для service1.gslb.com

Техническая поддержка

Мы предоставляем техническую поддержку всем нашим пользователям в соответствии со стандартными условиями обслуживания компании.

Мы обеспечим всю поддержку через службу технической поддержки, если у Вас есть активный контракт на поддержку и обслуживание edgeADC, edgeWAF или edgeGSLB.

Чтобы подать заявку в службу поддержки, пожалуйста, посетите сайт:

https://www.edgenexus.io/support/