EDGE NEXUS

EdgeADC

РУКОВОДСТВО ПО АДМИНИСТРИРОВАНИЮ

Содержание

Свойства документа

Номер документа: 2.0.6.8.21.23.06

Дата создания документа: 30 апреля 2021 года

Последнее редактирование документа: June 8, 2021

Автор документа: Джей Савур

Документ Последний раз редактировался:

Направление документов: EdgeADC - Версия 4.2.7.1890

Отказ от документа

Скриншоты и графика в данном руководстве могут незначительно отличаться от вашего продукта из-за различий в версии выпуска вашего продукта. Компания Edgenexus прилагает все разумные усилия для обеспечения полноты и точности информации в данном документе. 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 товарными знаками или зарегистрированными товарными знаками компании Edgenexus Limited. Все другие торговые марки являются собственностью соответствующих владельцев и признаются.

Поддержка Edgenexus

Если у вас возникли технические вопросы по данному продукту, пожалуйста, обратитесь в службу поддержки по адресу: support@edgenexus.io.

Установка EdgeADC

Продукт EdgeADC (в дальнейшем именуемый 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.

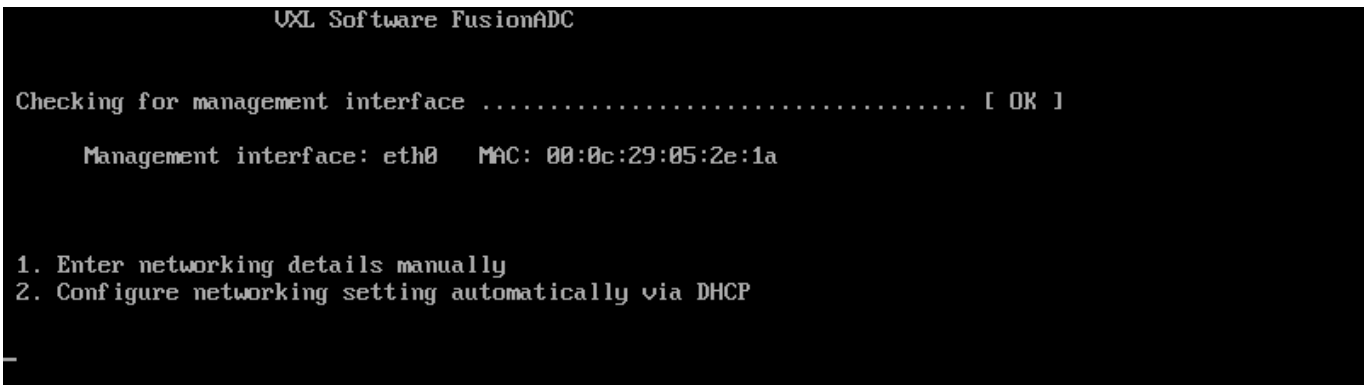
VMware ESXi

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 хосте ESXi или в 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 устройство ADC.
- Выберите хранилище данных с достаточным пространством и нажмите **NEXT**
- Затем вам будет предоставлена информация о продукте; нажмите **NEXT**
- Нажмите кнопку **NEXT.**
- После копирования файлов в хранилище данных можно 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 VA загрузится, и на консоли появится экран загрузки ADC.



Для продолжения работы обратитесь к разделу **КОНФИГУРАЦИЯ ПЕРВОЙ ЗАГРУЗКИ.**

Установка интерфейса VMXNET3

Драйвер VMXnet3 поддерживается, но сначала 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. Остановка ВМ (команда выключения CLI или отключение питания графического интерфейса)
2. Получите MAC-адреса обеих сетевых карт (запомните порядок 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. Перезапуск VA

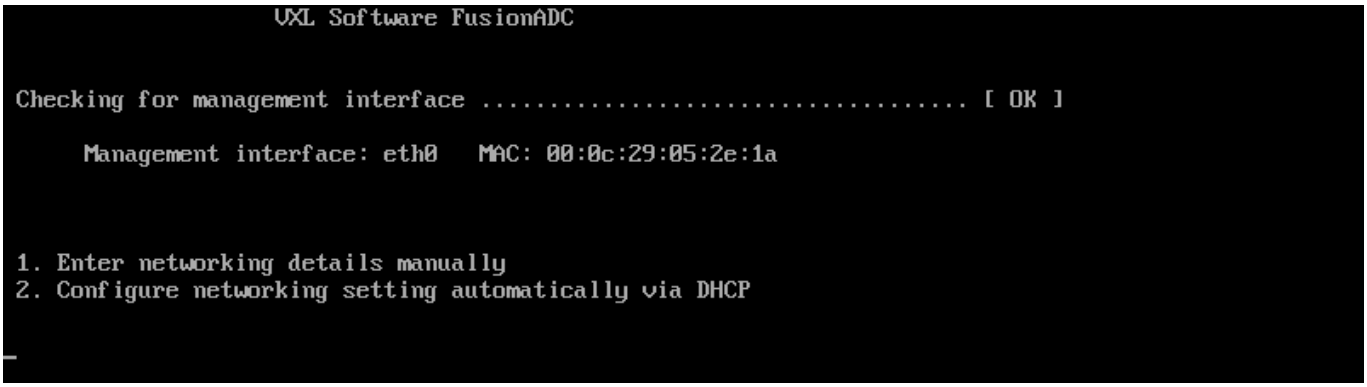
Мы поддерживаем VMware ESXi в качестве производственной платформы. Для ознакомительных целей вы можете использовать VMware Workstation и Player.

Microsoft Hyper-V

Виртуальное устройство ADC совместимо с установкой на сервер Microsoft Hyper-V Server.

- Распакуйте zip-файл Hyper-V ADC VA на локальную машину или сервер.
- Откройте диспетчер Hyper-V Manager.
- В диспетчере Hyper-V Manager щелкните правой кнопкой мыши на сервере и выберите **"Импортировать виртуальную машину".**
- Перейдите в папку, содержащую файлы ADC Hyper-V.
- Нажмите **"Копировать виртуальную машину (создать новый уникальный идентификатор)".**
- Установите флажок **"Дублировать все файлы, чтобы ту же виртуальную машину можно было импортировать снова".**
- Нажмите **"Импорт"**
- Ваша машина импортируется с именем **"ADC ADC VA for Hyper-V".**
- Убедитесь, что вы выбрали правильную сеть на сетевой карте
- Если вы устанавливаете более одного виртуального устройства, вам придется настроить для каждого устройства уникальный MAC-адрес
- Щелкните правой кнопкой мыши на только что созданной виртуальной машине и нажмите **"Подключить".**
- Нажмите зеленую кнопку "Пуск" или щелкните **"ActionStart".**

- Ваш VA загрузится, и появится экран консоли ADC.



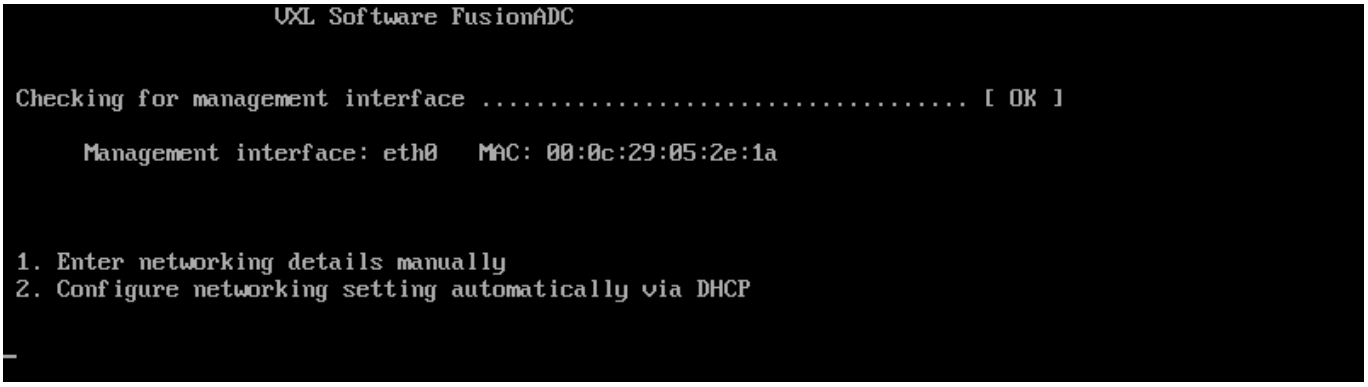
- После настройки сетевых свойств VA перезагрузится и представит вход в консоль VA.

Для продолжения работы обратитесь к разделу **КОНФИГУРАЦИЯ ПЕРВОЙ ЗАГРУЗКИ.**

Citrix XenServer

Виртуальное устройство ADC 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 хранения (SR) для размещения виртуального диска, когда появится соответствующий запрос.
- Выберите SR 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 Network 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, при импорте будет написано Connecting continuously then failed. Нажмите "**NEXT**"
- Просмотрите всю информацию и проверьте правильность настроек. Нажмите "**FINISH".**
- Ваша виртуальная машина 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**".
- После этого загрузится ваша виртуальная машина, и появится экран загрузки ADC.



- После настройки появляется возможность входа в VA.

Для продолжения работы обратитесь к разделу **КОНФИГУРАЦИЯ ПЕРВОЙ ЗАГРУЗКИ.**

Конфигурация первой загрузки

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

Первая загрузка - Сведения о 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, ваш АЦП после тайм-аута свяжется с сервером DHCP, 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 рекомендуем не использовать для работы ADC VA адрес DHCP, если этот IP-адрес не связан с MAC-адресом VA в 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 проверит, не используется ли IP-адрес в настоящее время, и если да, то снова увеличит его и перепроверит.

Изменение IP-адреса управления

Вы можете изменить IP-адрес VA в любое время с помощью команды **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. Смотрите 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 использования в производственных или ознакомительных целях.

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 для использования SSL-сертификата по своему выбору.

Как только браузер достигнет ADC, он покажет 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 настроенную дату и время, установленные в настоящее время	Tue Sept 3 13:00 UTC 2013
по умолчанию			Назначьте заводские настройки по умолчанию для вашего прибора	
выход			Выход из интерфейса командной строки	
помощь			Отображает все допустимые 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
уволиться			Выход из интерфейса командной строки	
перезагрузка			Разорвите все соединения и перезагрузите АЦП АЦП	перезагрузка
перезапустить			Перезапустите виртуальные службы ADC ADC	
маршрут	[пустой]		Просмотр таблицы маршрутизации	маршрут
	добавить	стандартный gw	Добавьте IP-адрес шлюза по умолчанию	route add default gw 192.168.100.254
установить	зеленая сторона		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 параметры глобальной конфигурации	
отключение			Завершите все соединения и отключите питание АЦП АЦП	
статус			Отображает текущую статистику данных	

топ		Просмотр информации о процессе, такой как процессор и память	
viewlog	сообщения	Отображение необработанных сообщений syslog	Просмотр сообщений журнала

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

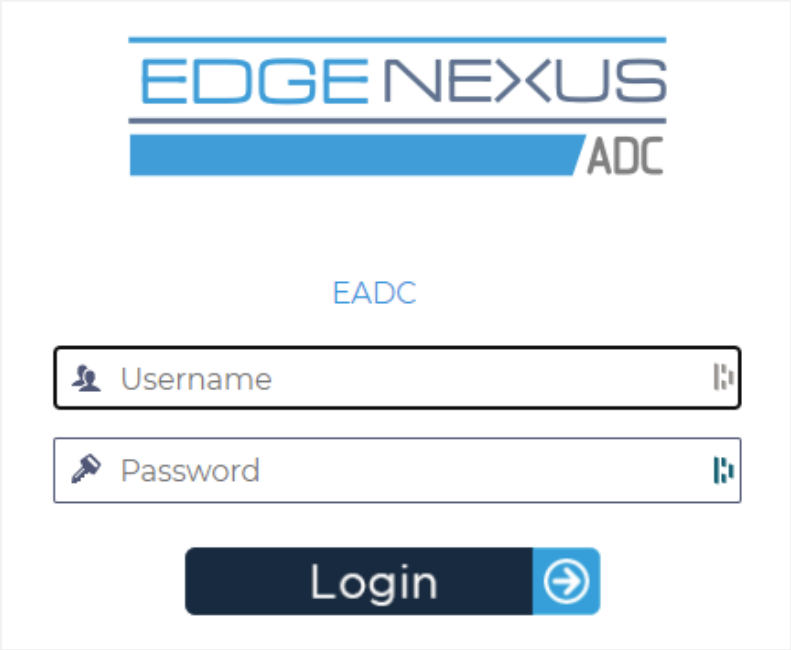
Запуск веб-консоли ADC

Все операции с АЦП (также называемым ADC) 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, как показано ниже, позволяя вам войти в систему как пользователь admin.



Учетные данные для входа по умолчанию

По умолчанию используются следующие учетные данные для входа в систему:

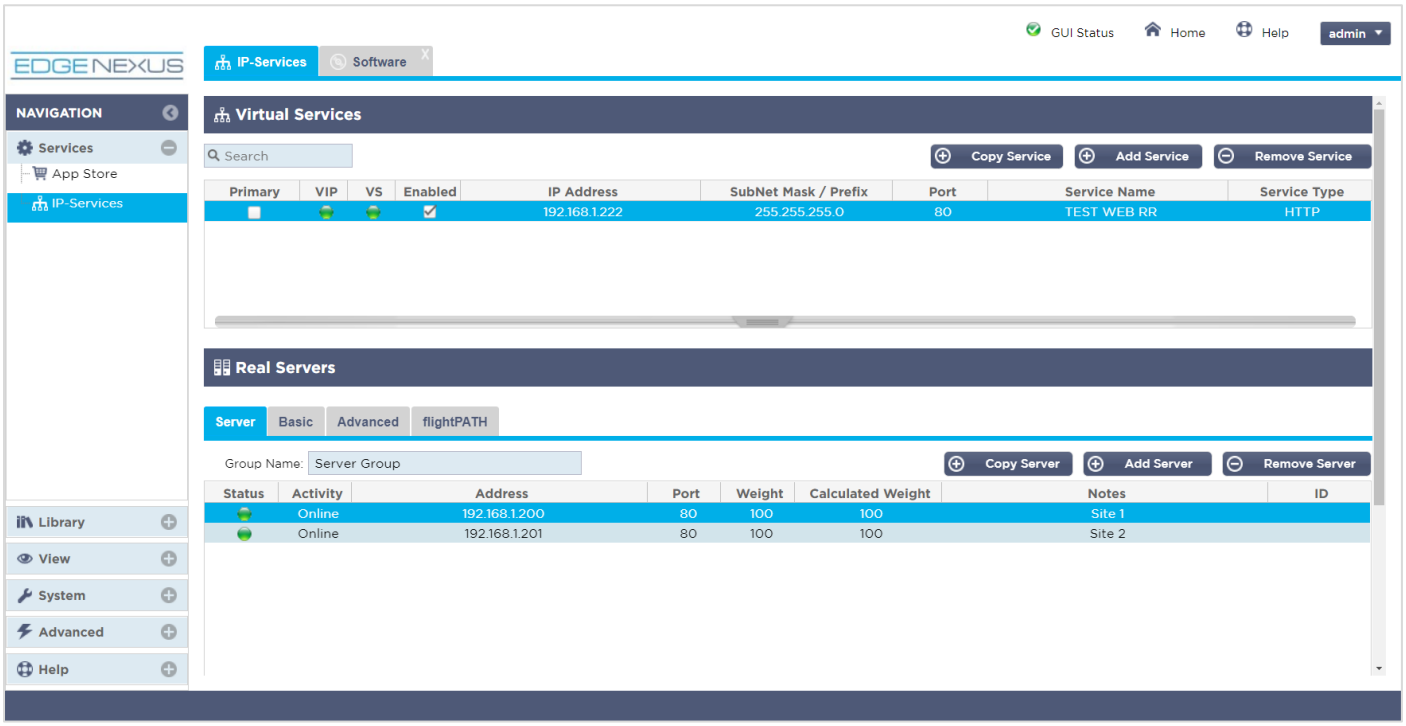
- Имя пользователя: admin
- Пароль: jetnexus

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

После успешного входа в систему отобразится главная приборная панель АЦП.

Главная приборная панель

На рисунке ниже показано, как выглядит главная 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.

Если двигаться слева направо, то сначала идет раздел "Навигация". Раздел Навигация состоит из различных областей внутри ADC. Когда вы нажимаете на определенный выбор в разделе Навигация, в правой части экрана отображается соответствующий раздел. 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 ADC имеет несколько областей. Когда вы нажмете на пункт Услуги, он расширится и покажет доступные варианты.

IP-услуги

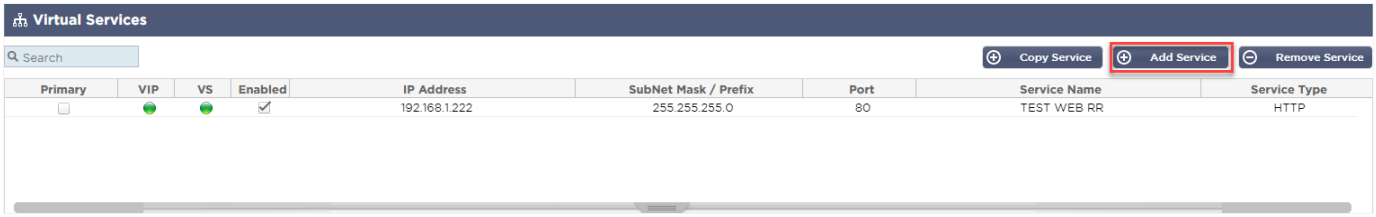
Раздел IP-служб ADC позволяет добавлять, удалять и настраивать различные виртуальные IP-службы, необходимые для конкретного случая использования. Настройки и опции представлены в следующих разделах. Эти разделы находятся в правой части экрана приложения.

Виртуальные услуги

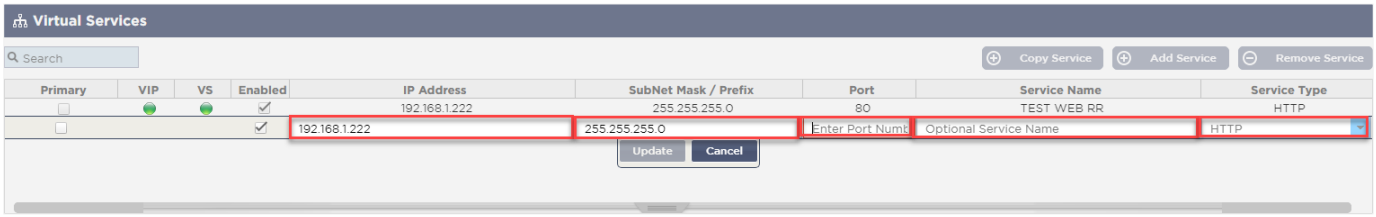
Виртуальная служба объединяет виртуальный IP-адрес (VIP) и порт TCP/UDP, который прослушивает ADC. Трафик, поступающий на IP-адрес виртуальной службы, перенаправляется на один из реальных серверов, связанных с этой службой. IP-адрес виртуальной службы не может совпадать с адресом управления ADC, т.е.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

ADC определяет способ повторного распределения трафика на серверы 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.

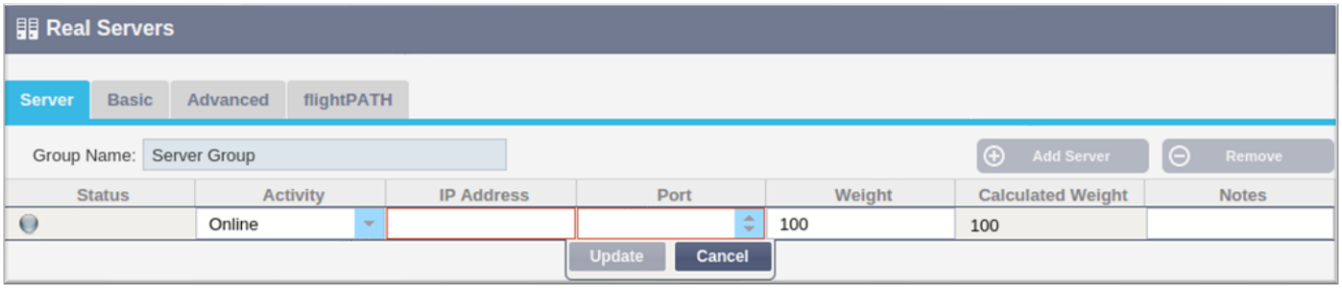


- Затем вы перейдете в режим **редактирования строки.**
- Заполните четыре выделенных поля, чтобы продолжить, а затем нажмите кнопку обновления.

Для перемещения по полям используйте клавишу TAB.

Поле	Описание
IP-адрес	Введите новый виртуальный IP-адрес, который будет целевой точкой входа для доступа к реальному серверу. На этот IP-адрес 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 совпадать со значением реального сервера, если вы используете обратный прокси.
Название услуги	Название услуги - это текстовое представление назначения VIP-клиента. Оно необязательно, но мы рекомендуем указать его для ясности.
Тип услуги	Существует множество различных типов услуг, которые вы можете выбрать. Типы услуг уровня 4 не могут использовать технологию flightPATH.

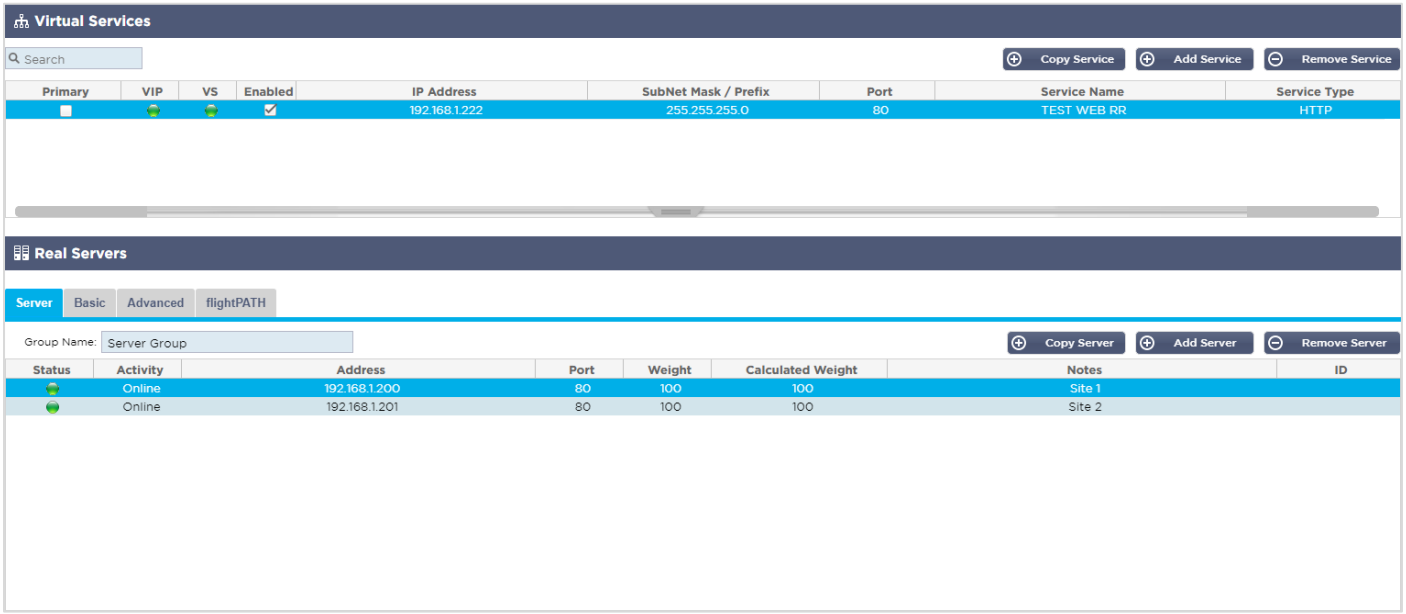
Теперь вы можете нажать кнопку Update, чтобы сохранить этот раздел и автоматически перейти к разделу Real Server, описанному ниже:



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 принимает 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 сервера Real Server. Он должен быть точным и не должен быть адресом DHCP.
Порт	Целевой порт доступа на реальном сервере. При использовании обратного прокси он может отличаться от порта входа, указанного на VIP.
Взвешивание	Эта настройка обычно автоматически конфигурируется АЦП. Вы можете изменить его, если хотите изменить взвешивание приоритетов.

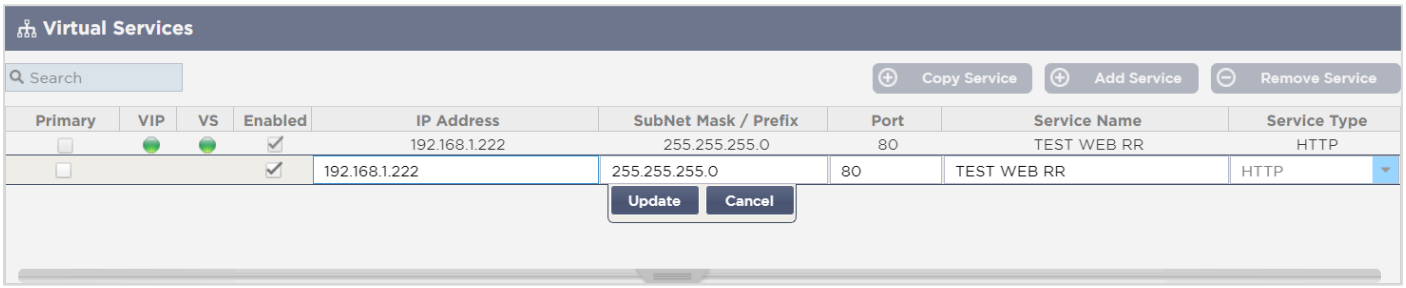
- Нажмите кнопку Обновить или нажмите Enter, чтобы сохранить изменения.
- Индикатор состояния сначала станет серым, а затем зеленым, если проверка состояния сервера прошла успешно. Он загорится красным, если монитор реального сервера не работает.
- Сервер, на котором горит красный индикатор состояния,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

Пример завершенной виртуальной услуги

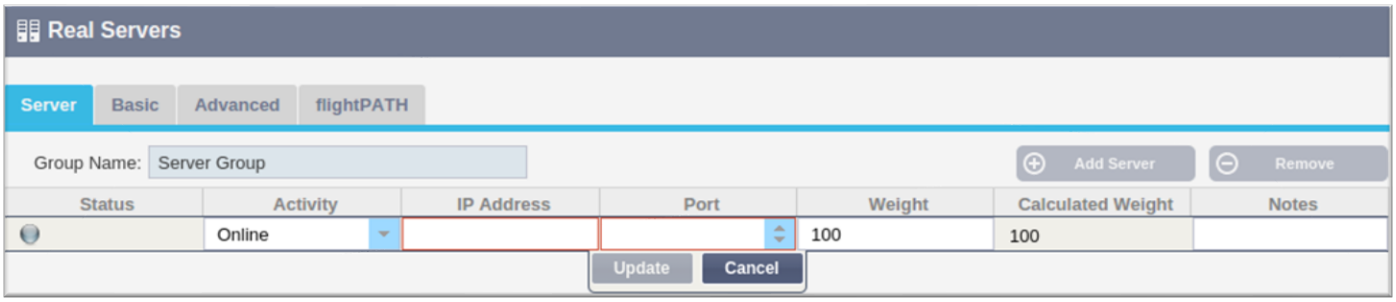


Создание новой виртуальной службы с использованием существующей VIP

- Выделите виртуальную службу, которую вы хотите скопировать
- Нажмите Добавить виртуальную службу, чтобы войти в режим редактирования строки



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

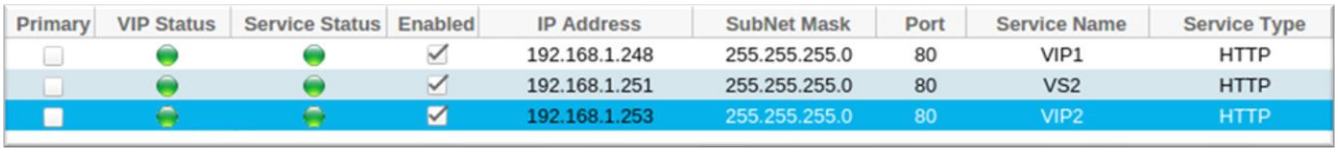


- Оставьте опцию Активность сервера как Online - это означает, что нагрузка будет сбалансирована, если он пройдет стандартный монитор здоровья TCP Connect. Этот параметр можно изменить позже, если потребуется.
- Введите IP-адрес реального сервера
- Введите номер порта для реального сервера
- Введите дополнительное имя для сервера Real Server
- Нажмите Обновить, чтобы сохранить изменения
- Индикатор состояния сначала станет серым, затем зеленым, если проверка 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

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 поле 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

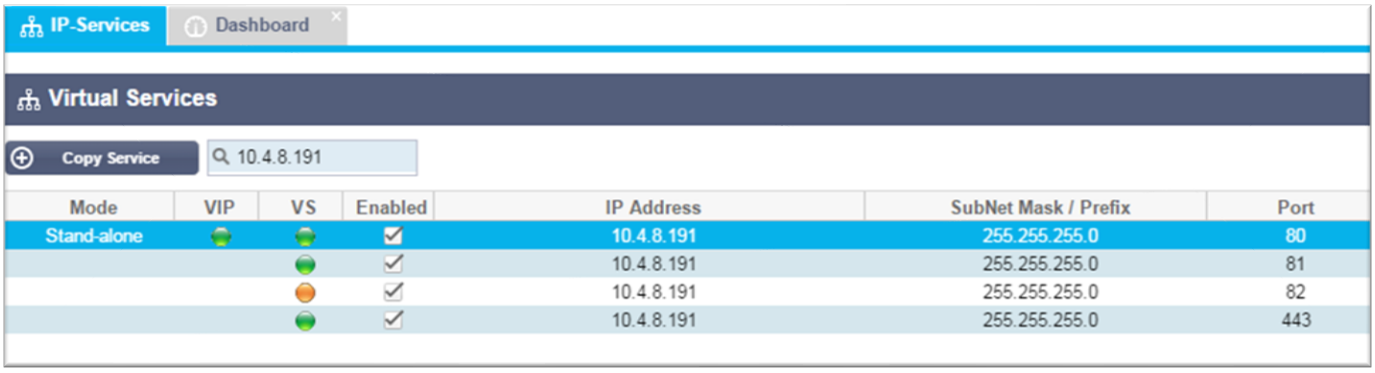
- Кнопка Копировать службу скопирует всю службу, включая все связанные с ней реальные серверы, основные настройки, расширенные настройки и правила flightPATH.
- Выделите услугу, которую вы хотите дублировать, и нажмите Копировать услугу
- Появится редактор строк с мигающим курсором в колонке IP-адрес
- 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 настройки, например, политику балансировки нагрузки, монитор Real Server или удалите правило flightPATH.

Фильтрация отображаемых данных

Поиск определенного термина

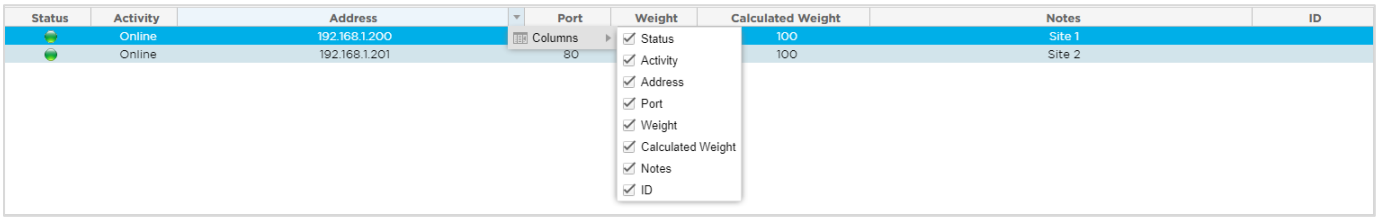
Поле Поиск позволяет искать в таблице по любому значению, например, по октетам IP-адреса или имени службы.



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

Выбор видимости столбцов

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

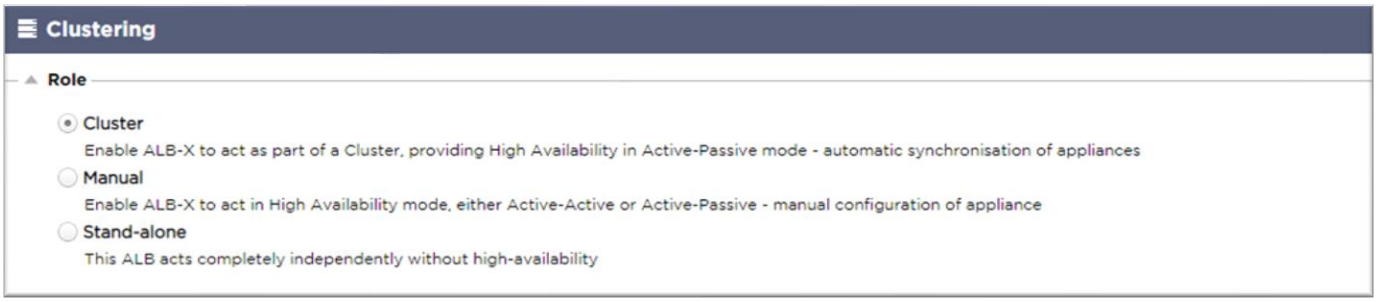


- Наведите курсор мыши на любой из столбцов
- В правой части колонки появится маленькая стрелка.
- Нажатием на флажки можно выбрать столбцы, которые вы хотите видеть на приборной панели.

Понимание колонок виртуальных служб

Основной/режим

В столбце Primary/Mode указывается роль высокой доступности, выбранная 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 столбце Primary/Mode указывается режим, в котором он работает в настоящее время. Если в вашем центре данных есть HA пара устройств ADC, 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 в столбце Primary рядом с каждым уникальным виртуальным IP будет находиться поле, 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 столбце Primary будет указано Stand-alone.

VIP

Эта колонка обеспечивает визуальную обратную связь о состоянии каждой виртуальной службы. Индикаторы имеют следующую цветовую кодировку:

LED	**Значение**
●	Онлайн
●	Failover-Standby. Эта виртуальная служба находится 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 серверы содержимого не включены
●	Состояние поиска
●	Не лицензировано или превышено количество лицензированных виртуальных IP-адресов

Включено

По умолчанию эта опция включена, и флажок отображается как установленный. Виртуальную службу можно отключить, 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 системе счисления. Пример "255.255.255.0". Или для IPv6 добавьте свой префикс. Для получения дополнительной информации об IPv6 см. **HTTPS://EN.WIKIPEDIA.ORG/WIKI/IPV6_ADDRESS**

Порт

Добавьте номер порта, связанный с вашей услугой. Порт может быть номером порта TCP или UDP. 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

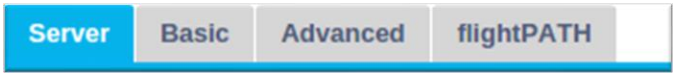
Обратите внимание, что при использовании всех типов сервисов "Layer 4" ADC не будет взаимодействовать или изменять поток данных, поэтому flightPATH недоступен при использовании сервисов Layer 4. Службы уровня 4 просто балансируют трафик в соответствии с политикой балансировки нагрузки:

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 трафика в соответствии с политикой балансировки нагрузки
Уровень 4 UDP	Любой порт UDP	Уровень 4	Как и в случае с TCP уровня 4, 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
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	Используется при балансировке нагрузки на почтовые серверы
POP3	Протокол почтового отделения	Уровень 4	Используется при балансировке нагрузки на почтовые серверы
IMAP	Протокол доступа к интернет-сообщениям	Уровень 4	Используется 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	Используется при балансировке нагрузки на системы, использующие 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	Используется при балансировке нагрузки серверов, использующих протоколы DICOM

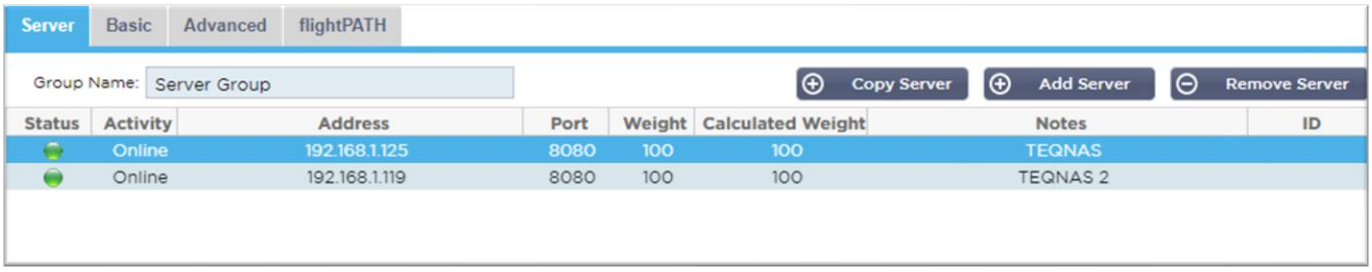
Настоящие серверы

В разделе Real Servers приборной панели есть несколько вкладок: Server, Basic, Advanced и flightPATH.



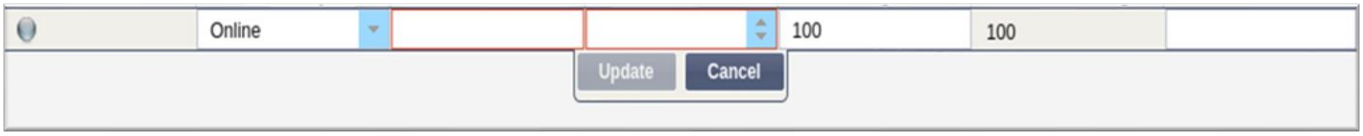
Сервер

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



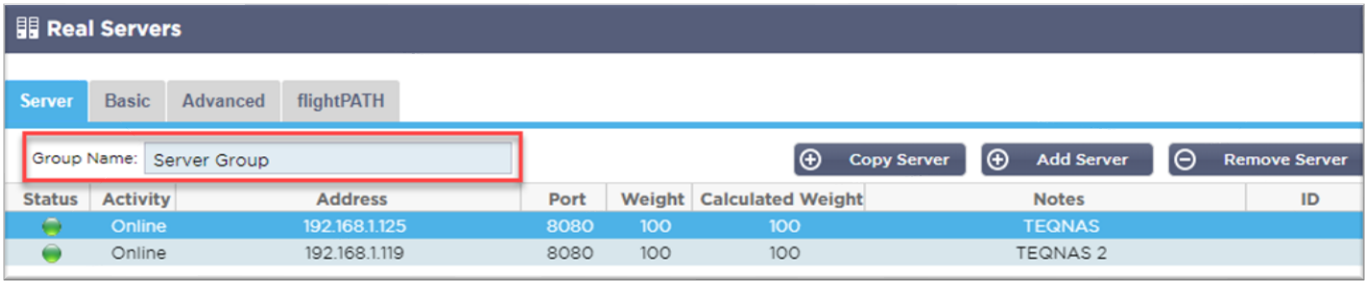
Добавить сервер

- Выберите соответствующий VIP, который вы определили ранее.
- 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 к столбцу 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 в раздел Notes (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 Update.

Индикаторы состояния реального сервера

Состояние реального сервера можно определить по светлому цвету в столбце "Состояние". См. ниже:

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

Деятельность

Вы можете изменить Активность реального сервера в любое время с помощью выпадающего меню. Для этого дважды щелкните по строке Real Server, 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 Drain, будут продолжать обслуживать существующие соединения, но не будут принимать новые соединения. Индикатор состояния будет мигать зеленым/синим цветом, пока идет процесс слива. После естественного закрытия существующих соединений 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 получит весь трафик, а группа Standby перестанет получать трафик.

IP-адрес

В этом поле указывается 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

Этот столбец станет редактируемым, когда будет указана соответствующая политика балансировки нагрузки.

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

Пример для трех серверов может выглядеть следующим образом:

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

Если учесть, что политика балансировки нагрузки установлена на Least Connections, а общее количество клиентских подключений составляет 200;

- 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.

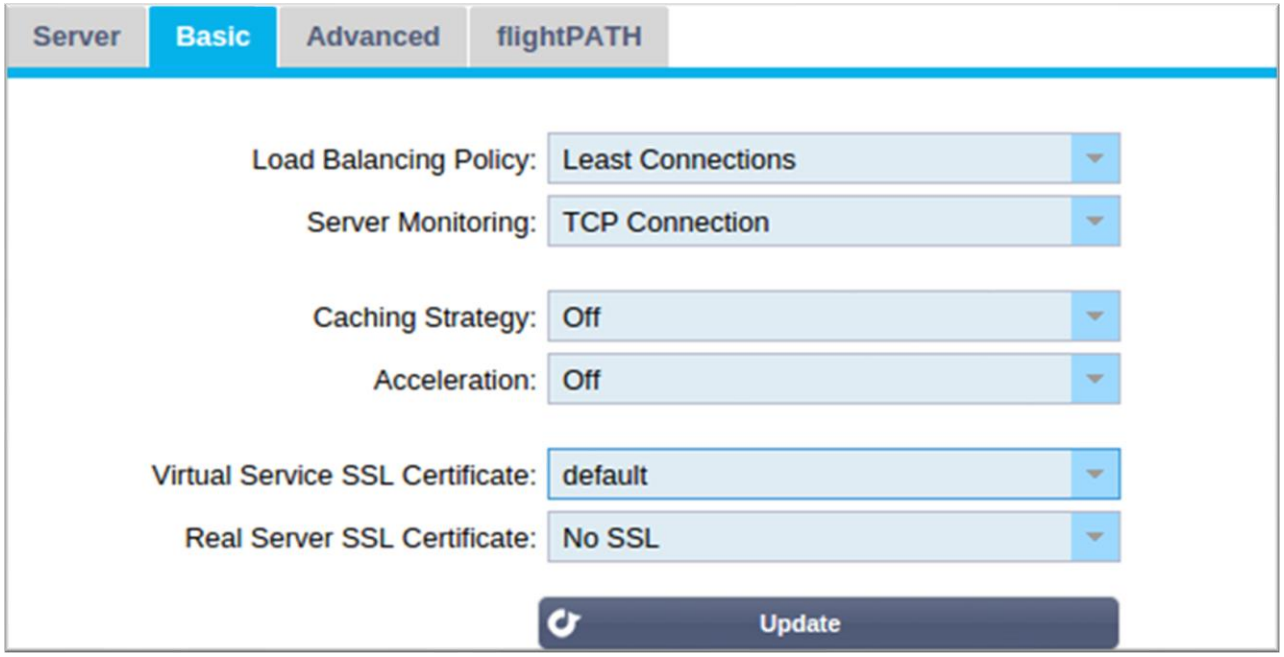
Расчетный вес

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

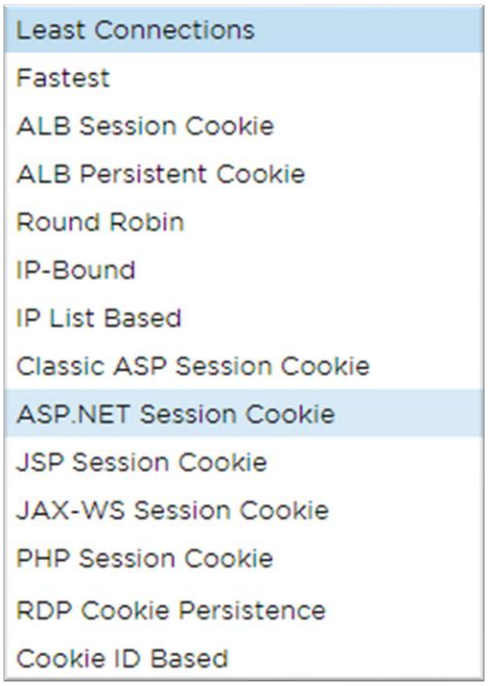
Введите в поле Notes любые особые заметки, полезные для описания определяемой записи. Пример "IIS Server1 - London DC".

Основной



Политика балансировки нагрузки

В раскрывающемся списке отображаются поддерживаемые в настоящее время политики балансировки нагрузки, доступные для использования. Список политик балансировки нагрузки 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. В столбце Рассчитанный вес содержится автоматически рассчитанное значение. Ручной ввод возможен только при использовании этой политики балансировки нагрузки.

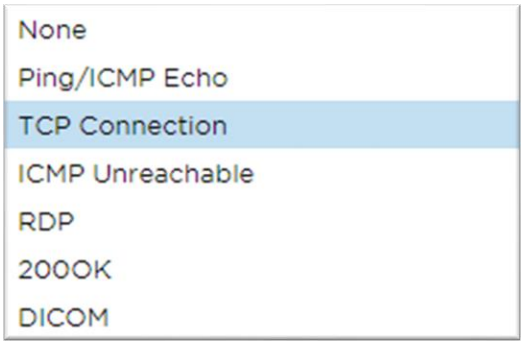
Раунд Робин	Round Robin обычно используется в брандмауэрах и базовых балансировщиках нагрузки и является самым простым методом. Каждый реальный сервер получает новый запрос по порядку. Этот метод подходит только тогда, когда вам нужно равномерно распределить нагрузку запросов на серверы; примером могут 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 является основой для выбора сервера Real Server, который получит запрос. Это действие обеспечивает постоянство. HTTP и протоколы четвертого уровня могут использовать этот режим. Этот метод полезен для внутренних сетей, где топология сети известна, и вы можете быть уверены, что нет "суперпрокси" 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 уровня 3 - 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.
Layer 7 Session Affinity/Persistence - ALB Session Cookie	Этот режим является наиболее популярным методом сохранения балансировки нагрузки HTTP. В этом режиме ADC использует балансировку нагрузки на основе списка IP 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.
Layer 7 Session Affinity/Persistence - ALB Persistent Cookie	Режим балансировки нагрузки на основе списка IP используется для каждого первого запроса. ADC 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 сохранения информации, когда клиент должен каждый раз обращаться к одному и тому же внутреннему серверу. Срок действия cookie истекает через 2 часа, и соединение будет сбалансировано по нагрузке в соответствии с алгоритмом, основанным на списке IP-адресов. Это время истечения срока действия настраивается с помощью jetPACK.
Куки сеанса - Классический куки сеанса ASP	Active Server Pages (ASP) - это технология Microsoft на стороне сервера. При выборе этой опции ADC будет поддерживать постоянство сеанса на том же сервере, если куки ASP будут

	обнаружены и найдены в списке известных куки. При обнаружении нового файла cookie ASP нагрузка будет сбалансирована с использованием алгоритма наименьших подключений.
Cookie сеанса - ASP.NET Cookie сеанса	Этот режим применяется к **ASP.net.** При выборе этого режима ADC будет поддерживать постоянство сеанса на одном и том же сервере, если куки ASP.NET обнаружены и находятся в его списке известных куки. При обнаружении нового файла cookie ASP нагрузка будет сбалансирована с использованием алгоритма наименьших подключений.
Cookie сеанса - Cookie сеанса 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 файла cookie JSP нагрузка на него будет сбалансирована с использованием алгоритма наименьших подключений.
Cookie сессии - JAX-WS Cookie сессии	Веб-службы Java (JAX-WS) - это технология Oracle для сервера. При выборе этого режима ADC будет поддерживать постоянство сеанса на одном и том же сервере, если куки JAX-WS обнаружены и находятся в его списке известных куки. При обнаружении нового файла cookie 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 ADC будет поддерживать постоянство сеанса 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. Это означает, что метод аналогичен методу CookieListBased, но использует другое имя cookie и хранит уникальное значение cookie, не скремблированный IP, а ID 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 выражение cookie выше, 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 знаете, какой монитор выбрать, то для начала подойдет стандартный TCP Connection.

Вы можете выбрать несколько мониторов, щелкая по очереди 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, если установить мониторы Ping/ICMP Echo, TCP Connection и 200OK, то в Dashboard Events появятся события, как показано на рисунке ниже:

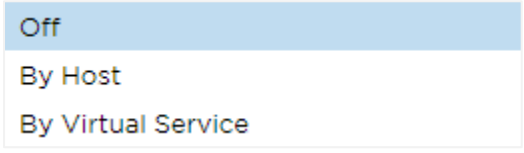
Мы видим, что Layer 3 Ping и Layer 4 TCP Connect прошли успешно, если посмотреть на верхнюю строку, но Layer 7 200OK потерпел неудачу. Эти результаты мониторинга дают достаточно информации, чтобы показать, что с маршрутизацией все в порядке и есть служба, запущенная на соответствующем порту, но веб-сайт 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 ADC отправляет 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 сервиса.
TCP-соединение	В этом режиме устанавливается TCP-соединение с реальным сервером и немедленно разрывается без отправки каких-либо данных. Если соединение успешно установлено, ADC 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-соединений.
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. HTTP-ответ ожидается и проверяется на наличие кода ответа "200 OK". Если код ответа "200 OK" получен, АЦП считает, что реальный сервер работает. Если ADC не получает код ответа "200 OK" по какой-либо причине, включая тайм-ауты, невозможность подключения и другие причины, ADC отмечает Real Server как недоступный. Этот метод мониторинга применим только для типов служб HTTP и ускоренного HTTP. Если для HTTP-сервера используется тип службы уровня 4, 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 при подключении к Real Server выполняется "Associate Request" от Echoscu. Общение, включающее "Associate Accept" от сервера содержимого, передачу небольшого количества данных, затем "Release Request", затем "Release Response", успешно завершает монитор. Если по какой-либо причине монитор не завершается успешно, то Реальный сервер считается отключенным.
Определяется пользователем	В списке появится любой монитор, настроенный в разделе Мониторинг реального сервера.

Стратегия кэширования

По умолчанию стратегия кэширования отключена и установлена как Off. Если тип вашего сервиса - HTTP, то вы можете применить два типа стратегии кэширования.



Обратитесь к странице Configure Cache для настройки подробных параметров кэширования. Обратите внимание, что когда кэширование применяется к VIP с типом сервиса Accelerated "HTTP", сжатые объекты не кэшируются.

Вариант	Описание
Хозяин	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.
Виртуальная служба	При выборе этой опции доступно кэширование для каждой виртуальной службы. 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	При выборе этого параметра включается 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 содержимого с помощью раздела Глобальные исключения.

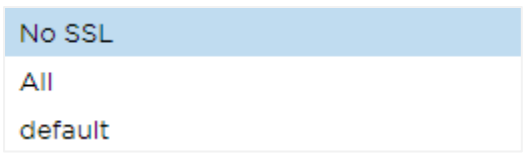
Примечание: Если объект является кэшируемым, ADC будет хранить сжатую версию и обслуживать ее статически (из памяти) до тех пор, пока срок действия содержимого не истечет и оно не будет повторно проверено.

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

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.

Указание 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 порту TCP.

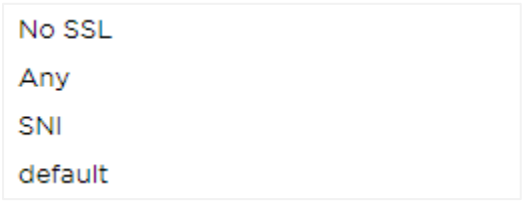


Вариант	Описание
Нет SSL	Трафик от источника к АЦП не шифруется.

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.
Импортированные пользователем SSL-сертификаты	Здесь отображаются все сертификаты, которые вы импортировали в ADC.

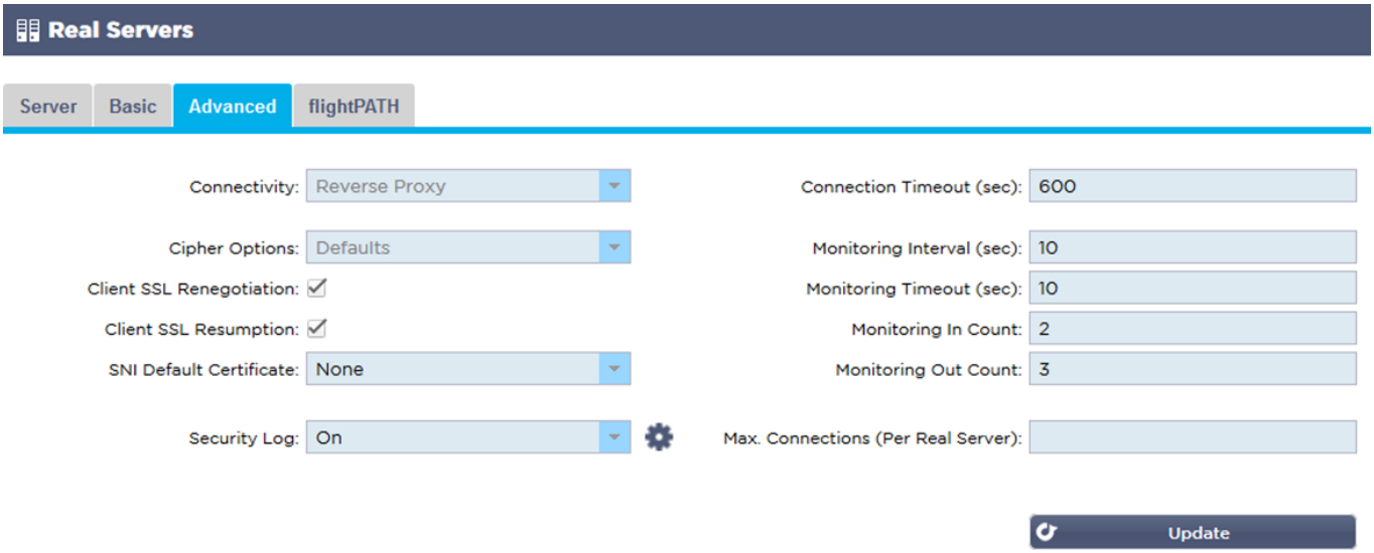
SSL-сертификат реального сервера (шифрование между АЦП и реальным сервером)

По умолчанию для этого параметра установлено значение No SSL. Если ваш сервер требует зашифрованного соединения, это значение должно быть любым другим, кроме No SSL. В этом списке появятся сертификаты, которые были созданы или импортированы.



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 выступает в роли клиента и принимает любой сертификат, представленный Real Server. Трафик от АЦП к реальному серверу шифруется при выборе этой опции. Используйте опцию "Любой", когда сертификат указан на стороне виртуальной службы, обеспечивая так называемое "SSL Bridging" или "SSL Re-Encryption".
SNI	ADC выступает в роли клиента и принимает любой сертификат, представленный Real Server. Трафик от АЦП к реальному серверу шифруется, если выбран этот параметр. Используйте опцию "Любой", если сертификат указан на стороне виртуальной службы, обеспечивая так называемое "SSL Bridging" или "SSL Re-Encryption". Выберите эту опцию, чтобы включить SNI на стороне сервера.
Импортированные пользователем SSL-сертификаты	Здесь отображаются все сертификаты, которые вы импортировали в ADC.

Расширенный



Связь

Ваша виртуальная услуга может быть настроена на четыре различных типа подключения. Пожалуйста, выберите режим подключения, который будет применяться к услуге.

Вариант	**Описание**
Обратный прокси-сервер	Reverse Proxy - значение по умолчанию, работает на Layer7 со сжатием и кэшированием. И на уровне Layer4 без кэширования и сжатия. В этом режиме ваш ADC действует как обратный прокси и становится адресом источника, который видят реальные серверы.
Прямое возвращение 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 направлять весь трафик через ADC, позволяя направлять трафик от Real Servers 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, поскольку нет поддержки постоянства, кроме как на основе списка IP. Этот метод требует, чтобы Real Server установил свой шлюз по умолчанию на локальный адрес интерфейса (eth0, eth1 и т.д.) ADC. Обратитесь к разделу Изменения реального сервера.

Параметры шифра

Вы можете установить шифры на уровне каждой службы, и это актуально только для служб 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 службы. Преимуществом этого является то, что вы можете создать несколько служб с различными уровнями безопасности. Имейте в виду, что старые клиенты несовместимы 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 уровень SSL, сняв флажок.

Возобновление SSL клиента

Установите этот флажок, если вы хотите включить возобновление SSL сеансов сервера, добавленных в кэш сеансов. Когда клиент предлагает повторное использование сессии, сервер попытается повторно использовать сессию, если она будет найдена. Если флажок Resumption не установлен, кэширование сеансов для клиента или сервера не происходит.

Сертификат SNI 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 удалось.

Журнал безопасности

'On' - это значение по умолчанию, которое используется для каждой службы и позволяет службе регистрировать информацию об аутентификации в журналах W3C. Нажав на значок Cog, вы перейдете на страницу System > Logging, где можно 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 этот параметр для недолговечного веб-трафика без статических данных, который обычно составляет 90 секунд или меньше. Увеличьте этот показатель для соединений с 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.

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

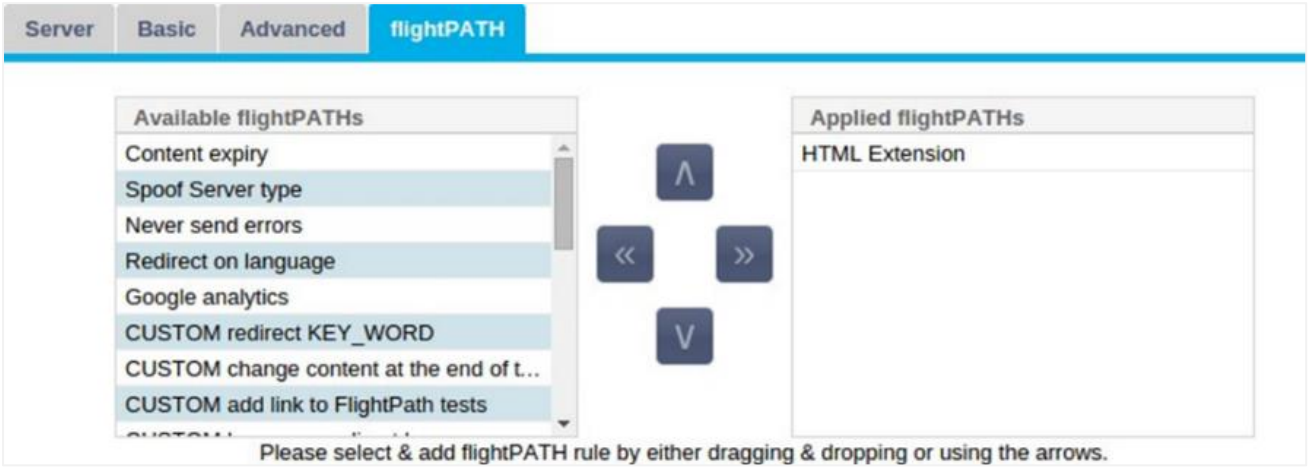
Счетчик выходов мониторинга

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.

Макс. Соединения

Ограничивает количество одновременных соединений Real Server и устанавливается для каждой службы. Например, если вы настроите значение 1000 и у вас два Real Server, ADC ограничит **каждый** 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 подключений. 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 отображается, 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, которое выполняется 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 "Настройка flightPATH" данного руководства.

Библиотека

Дополнения

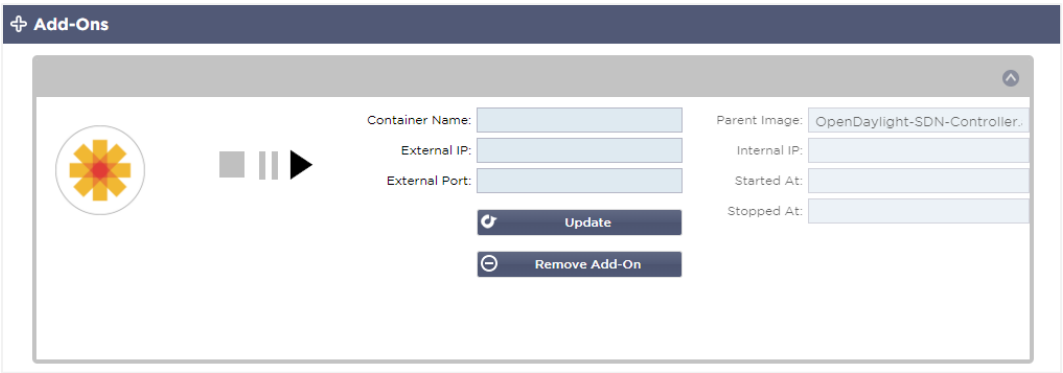
Дополнения - это контейнеры на базе Docker, которые могут работать в изолированном режиме внутри ADC. Примерами дополнений могут быть брандмауэр приложений или даже микроэкземпляр самого ADC.

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 перейти в раздел "Приложения", загрузить и установить приложение.

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



Приобретение дополнения

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

Перейдите на страницу Библиотека > Приложения на приборной панели ADC.

Здесь вы можете выбрать приложение, которое хотите загрузить и затем установить.

Если вы делаете это с приборной панели ADC, выберите только 1 элемент. У вас может быть несколько наборов 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 "Приобретенные приложения" вашего ADC, и вы сможете их загрузить.

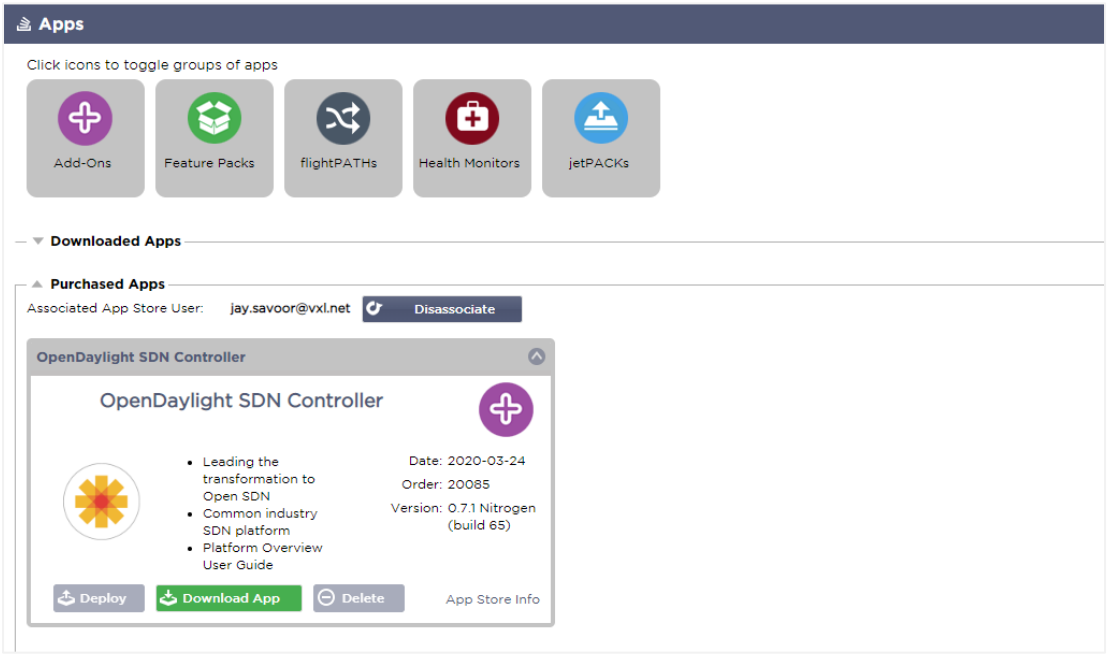
Приложения ассоциируются с принадлежащими вам и зарегистрированными ADC.

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:

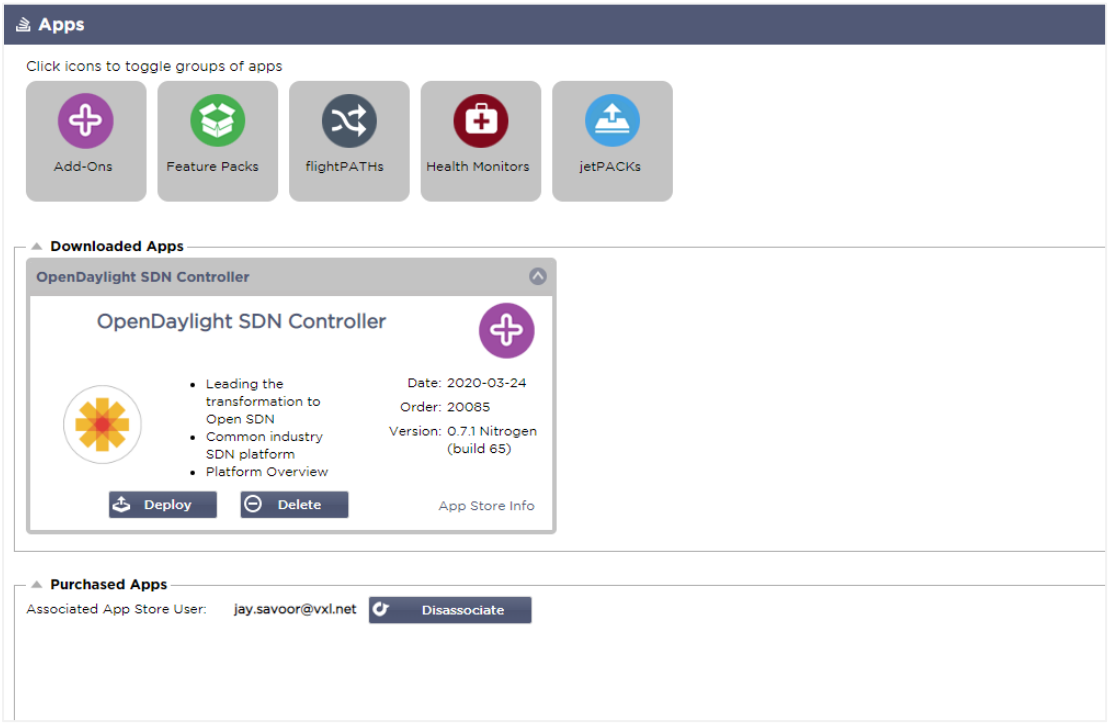
- Дополнения: **HTTPS://APPSTORE.EDGENEXUS.IO/PRODUCT-CATEGORY/ADD-ONS/**
- Мониторы здоровья: **HTTPS://APPSTORE.EDGENEXUS.IO/PRODUCT-CATEGORY/SERVER-HEALTH-MONITORS/**
- jetPACKS: **HTTPS://APPSTORE.EDGENEXUS.IO/PRODUCT-CATEGORY/JETPACKS/**

- Feature Packs: 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 Downloaded Apps и развернуто на ADC с помощью кнопки Deploy. Этот процесс занимает некоторое время в зависимости от ресурсов, доступных для ADC. После развертывания приложение появится в разделе "Загруженные приложения".



Аутентификация

Страница Library > Authentication 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.

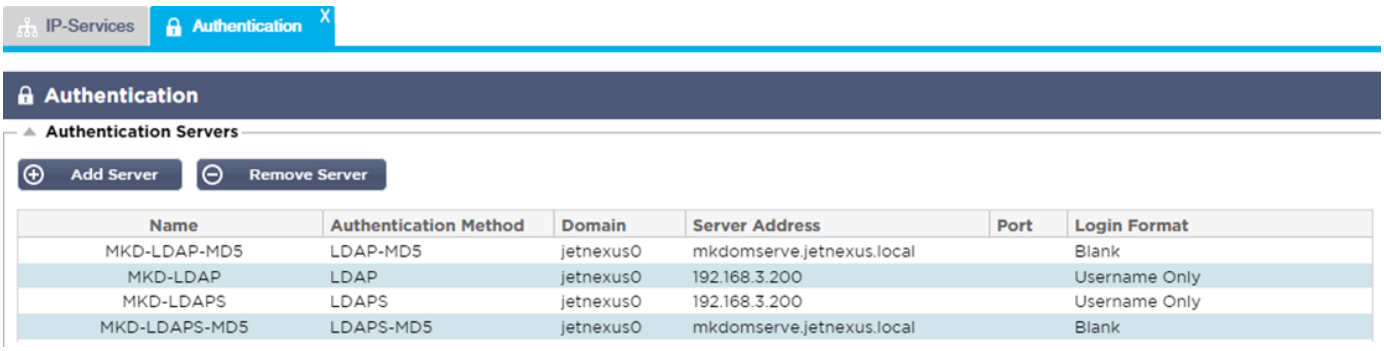
Настройка аутентификации - рабочий процесс

Чтобы применить аутентификацию к вашей службе, выполните, как минимум, следующие шаги.

1. Создайте сервер аутентификации.
2. Создайте правило аутентификации, которое использует сервер аутентификации.
3. Создайте правило flightPATH, которое использует правило аутентификации.
4. Применить правило flightPATH к службе

Серверы аутентификации

Чтобы настроить работающий метод аутентификации, мы должны сначала настроить сервер аутентификации.



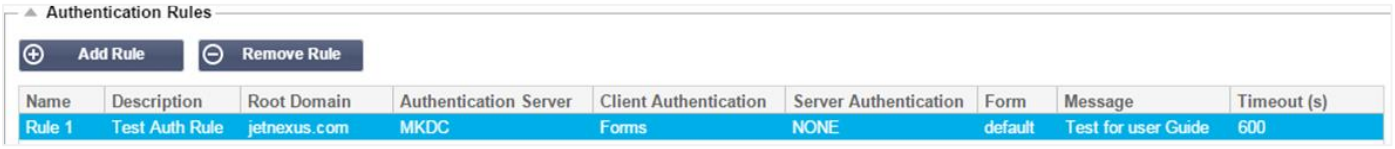
- Нажмите кнопку Добавить сервер.
- Это действие приведет к созданию пустой строки, готовой к заполнению.

Вариант	**Описание**
Имя	Дайте вашему серверу имя для 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, хэшированным MD5 для повышения безопасности. LDAPS - LDAP через SSL. Отправляет пароль открытым текстом в зашифрованном туннеле между АЦП и сервером LDAP. LDAPS-MD5 - LDAP через SSL. Пароль хешируется MD5 для дополнительной безопасности в зашифрованном туннеле между АЦП и сервером LDAP.
Домен	Добавьте имя домена 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 нужный вам формат входа. Имя пользователя - при выборе этого формата 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. Этот параметр используется при использовании MD5.
Пассфраза	Эта опция не используется в данной версии.
Мертвое время	Не используется в данной версии

Правила аутентификации

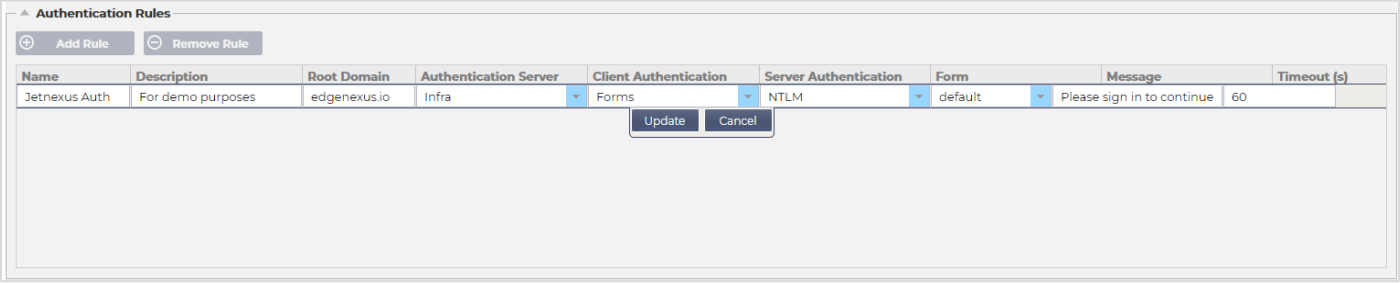
Следующим этапом является создание правил аутентификации для использования с определением сервера.



Поле	**Описание**
Имя	Добавьте подходящее имя для правила аутентификации.
Описание	Добавьте подходящее описание.
Корневой домен	Этот параметр следует оставить пустым, если вам не нужен единый вход на поддоменах.
Сервер аутентификации	Это выпадающее поле, содержащее настроенные вами серверы.
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 можно добавить сообщение. Вы можете выбрать форму, которую вы загрузили, используя раздел ниже.
Аутентификация сервера	Выберите соответствующее значение. None - если ваш сервер не имеет никакой существующей аутентификации, выберите этот параметр. Этот параметр 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 - При выборе этой опции АЦП будет использовать свою встроенную форму.

	Пользовательская - вы можете добавить разработанную вами форму и выбрать ее здесь.
Сообщение	Добавьте личное сообщение в форму.
Тайм-аут	Добавьте в правило тайм-аут, по истечении которого пользователь должен будет повторно пройти аутентификацию. Обратите внимание, что параметр Timeout действует только для аутентификации на основе форм.

Единый вход



Если вы хотите обеспечить единый вход для пользователей, заполните колонку Корневой домен своим доменом. В данном примере мы использовали edgenexus.io. Теперь у нас может быть 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 предложением войти в систему в зависимости от используемого правила аутентификации. Затем этот же пользователь может подключиться к appstore. mycompany.com и будет автоматически аутентифицирован ADC. Вы можете установить тайм-аут, который будет принудительно аутентифицировать пользователя по истечении этого периода бездействия.

Формы

В этом разделе вы сможете загрузить пользовательскую форму.

Как создать пользовательскую форму

Хотя базовая форма, предоставляемая 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"

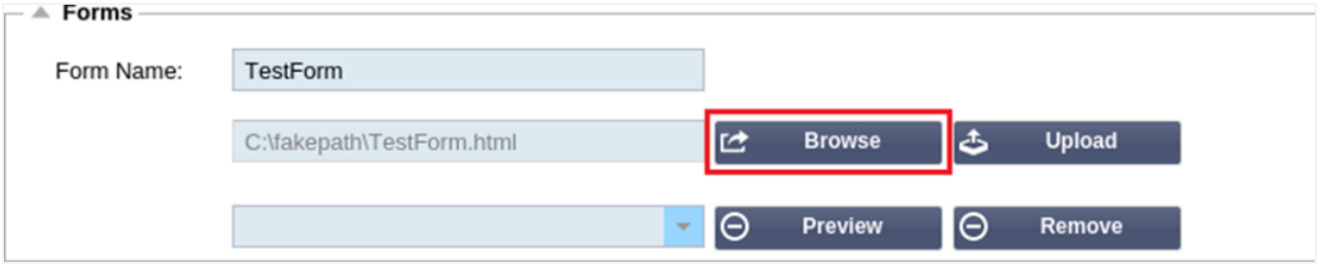
Пароль:	name="JNPASS"
Необязательное сообщение1:	%JNMESSAGE%
Необязательное сообщение2:	%JNAUTHMESSAGE%
Изображения	Если вы хотите добавить изображение, то, пожалуйста, добавьте его в строке с использованием кодировки Base64.

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

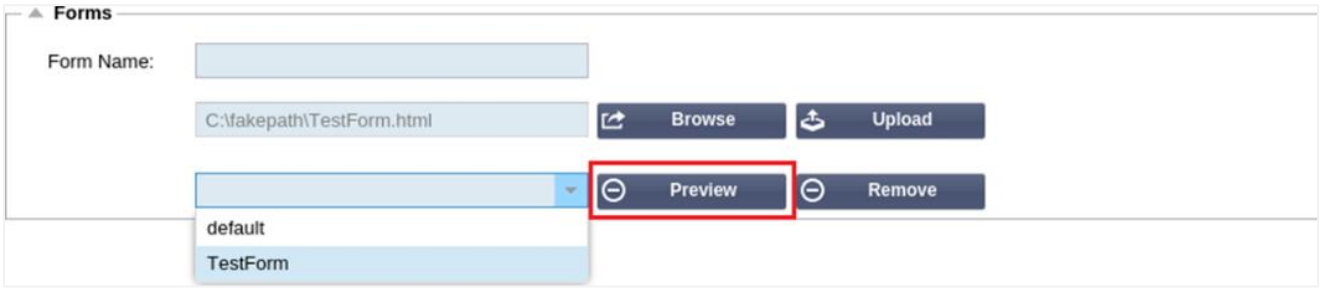
После создания пользовательской формы вы можете добавить ее с помощью раздела Формы.



1. Выберите имя для вашей формы
2. Поиск формы на местном уровне
3. Нажмите Загрузить

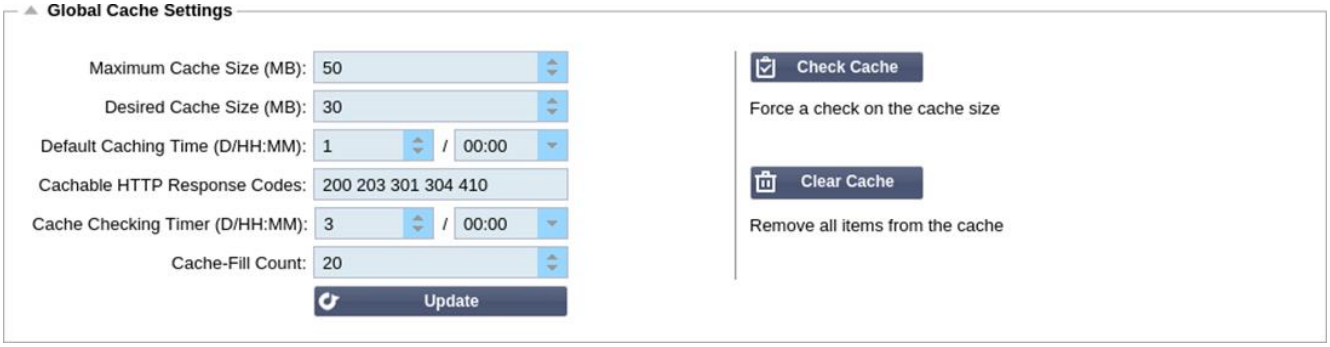
Предварительный просмотр вашей пользовательской формы

Чтобы просмотреть пользовательскую форму, которую вы только что загрузили, выделите ее и нажмите 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 функцией, 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 неизменности кэша после перезапуска, 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 - это оптимальный размер, который кэш должен пытаться достичь при каждой автоматической или ручной проверке размера кэша. Промежуток между максимальным и желаемым размером кэша существует для того, чтобы обеспечить 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 содержимого без явного срока действия. Время кэширования по умолчанию - это период, в течение которого хранится содержимое 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 для хранения АЦП будет хранить содержимое в течение одного дня, "01:00" - одного часа, а "00:01" - одной минуты.

Кэшируемые коды ответов HTTP

Одним из наборов кэшированных данных являются ответы HTTP. Кэшируются следующие коды ответов HTTP:

- 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, 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.

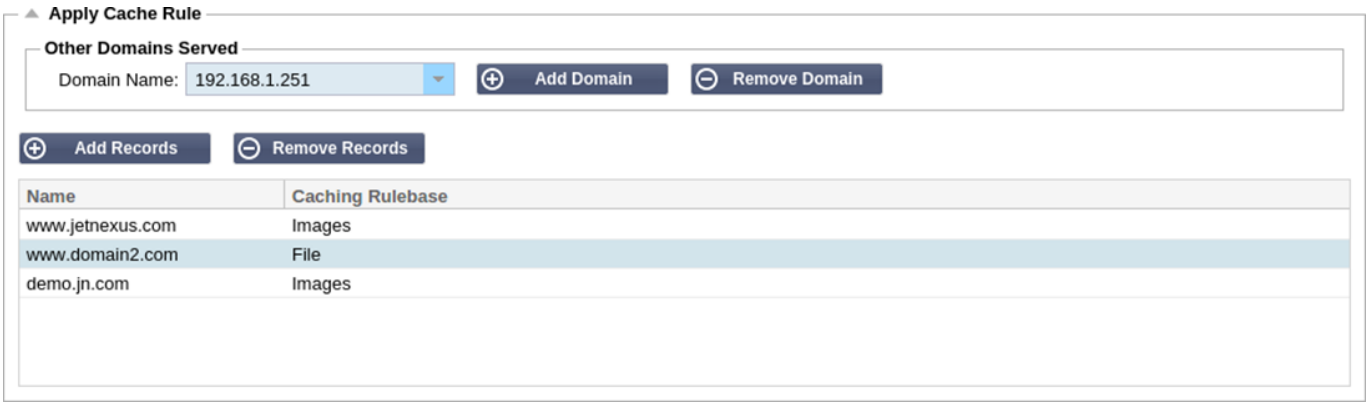
Время проверки кэша (Д/ЧЧ:ММ)

Эта настройка определяет интервал времени между операциями обрезки кэша.

Подсчет заполнения кэш-памяти

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

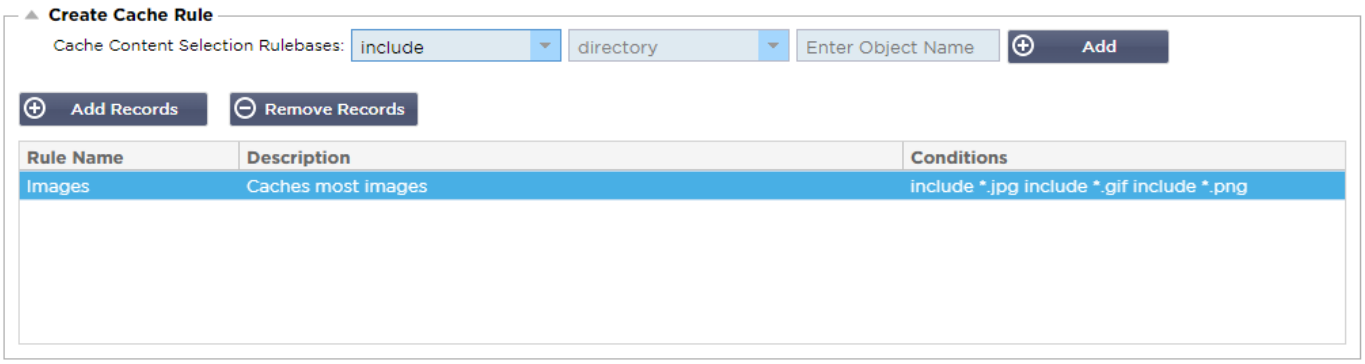
Применить правило кэширования



Этот раздел позволяет 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
- Нажмите на выпадающую стрелку 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 правило кэширования, дважды щелкнув на столбце Caching Rulebase и выбрав из списка

Создание правила кэширования



Этот раздел позволяет 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 условия вручную или воспользоваться кнопкой 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 теперь в условия добавлено 'include *.jpg'.
- Вы можете добавить больше условий. Если вы решили сделать это вручную, вам нужно добавить каждое условие на НОВУЮ строку. Обратите внимание, что ваши правила будут отображаться на одной строке, пока вы не щелкните в поле Условия, после чего они будут отображаться на отдельной строке.

flightPATH

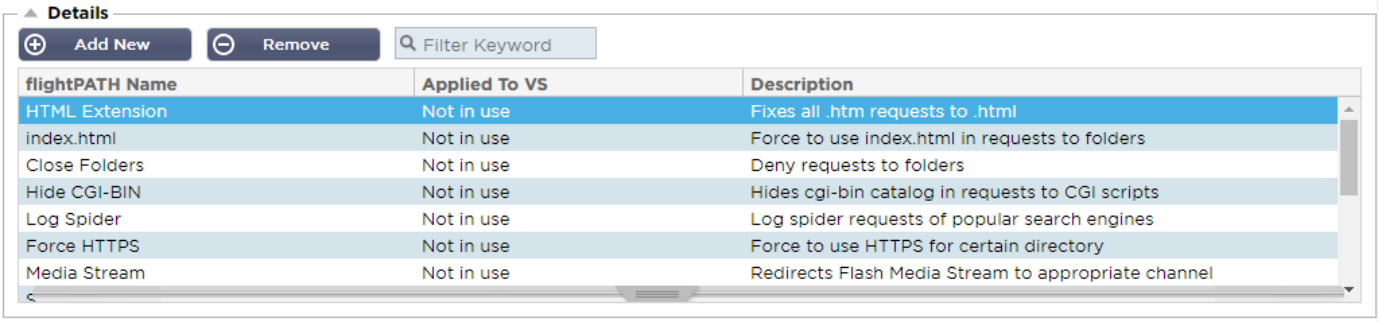
flightPATH - это технология управления трафиком, встроенная в ADC. flightPATH позволяет проверять трафик HTTP и HTTPS в режиме реального времени и выполнять действия в зависимости от условий.

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

Правило траектории полета состоит из четырех элементов:

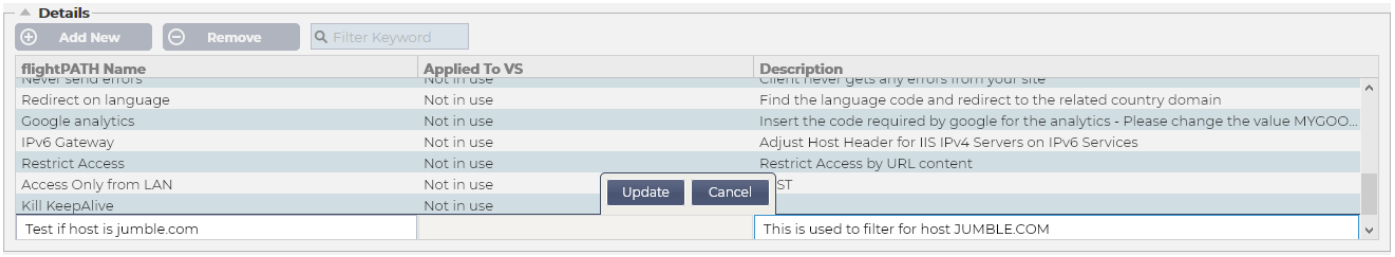
1. Details, где вы определяете имя flightPATH и службу, к которой он прикреплен.
2. Условие(я), которое может быть определено, чтобы вызвать срабатывание правила.
3. Оценка, позволяющая определять переменные, которые могут быть использованы в рамках Действий
4. Действия, которые используются для управления тем, что должно произойти при выполнении условий

Подробности



В разделе подробностей отображаются доступные правила flightPATH. В этом разделе можно добавлять новые правила flightPATH и удалять определенные.

Добавление нового правила flightPATH



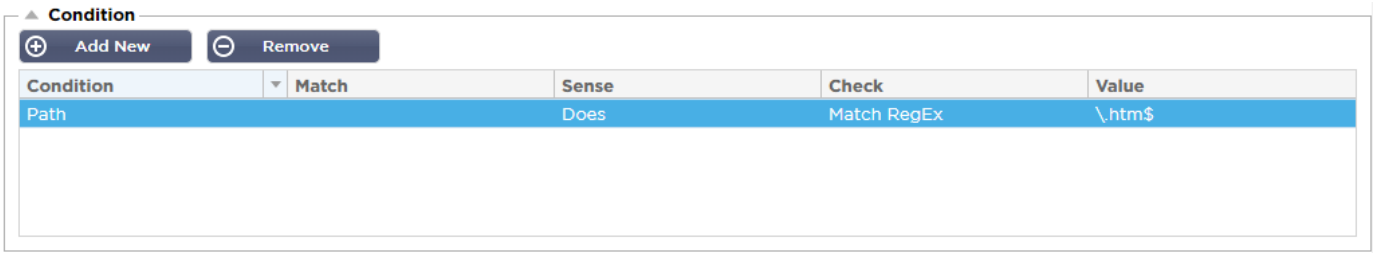
Поле	Описание
Имя FlightPATH	Это поле предназначено для имени правила flightPATH. Имя, которое вы здесь указываете, появляется в других частях ADC и на него ссылаются.
Применяется к VS	Этот столбец доступен только для чтения и показывает VIP, к которому применяется правило flightPATH.
Описание	Значение,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

Шаги для добавления правила flightPATH

1. Сначала нажмите кнопку Добавить новый, расположенную в разделе Подробности.
2. Введите имя для вашего правила. Пример Auth2
3. Введите описание вашего правила
4. После применения правила к службе вы увидите, как в колонке Applied To автоматически заполняются IP-адрес и значение порта.
5. Не забудьте нажать кнопку "Обновить", чтобы сохранить изменения, а если вы ошиблись, просто нажмите кнопку "Отменить", чтобы вернуться к предыдущему состоянию.

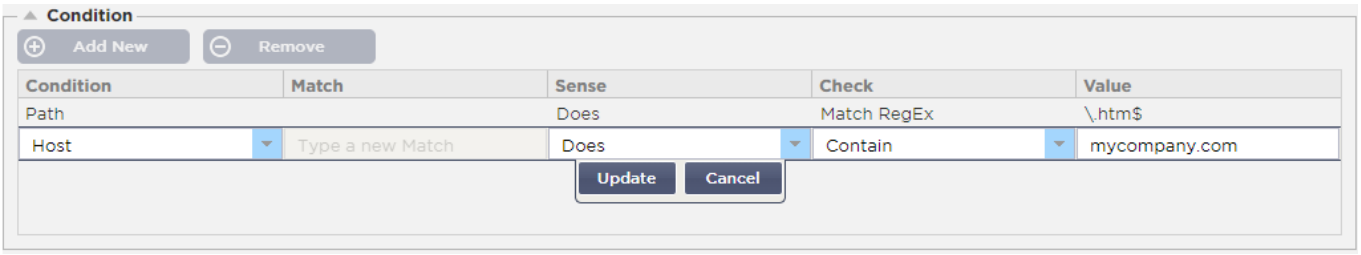
Состояние

Правило flightPATH может содержать любое количество условий. Условия работают по принципу AND, позволяя 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:

ПОДРОБНЕЕ	ОПИСАНИЕ	ПРИМЕР
<форма>	HTML-формы используются для передачи данных на сервер	Пример "форма не имеет длины 0".
Местонахождение ГЭП	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 извлекается из HTTP-заголовка language	Это условие приведет к появлению выпадающего списка со списком языков
Метод	Выпадающий список методов HTTP	Выпадающий список, включающий GET, POST и т.д.
IP-адрес происхождения	Если восходящий прокси поддерживает X-Forwarded-for (XFF), он будет использовать истинный адрес происхождения.	IP-адрес клиента. Он также может использовать несколько IP-адресов 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 веб-сайту	/mywebsite/index.asp
ПОСТ	Метод запроса POST	Проверка данных, загружаемых на веб-сайт
Запрос	Имя и значение запроса, может	"Best=jetNEXUS", где соответствие -

	принимать либо имя запроса, либо также значение	Best, а значение - edgeNEXUS
Строка запроса	Вся строка запроса после символа ?	
Запрос куки	Имя файла cookie, запрашиваемого клиентом	MS-WSMAN=afYfn1CDqqCDqUD::
Заголовок запроса	Любой заголовок HTTP	Referrer, User-Agent, From, Date
Версия для запросов	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 или другой агрегированный IP-адрес	ClientIP , Proxy IP, Firewall IP. Можно также использовать несколько IP и подсетей. Точки необходимо экранировать, так как они являются RegEX. Пример 10\.1\.2\.3 - 10.1.2.3

Матч

Поле Match может быть выпадающим или текстовым значением 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 представляется 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 данный сервер	Диапазон приема: байты
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-куки, ранее отправленные сервером с помощью Set-Cookie (см. ниже).	Cookie: $Version=1; Skin=new;
Дата	Дата и время получения сообщения	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 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

Чувства

Поле Sense - это выпадающее булево поле, которое содержит варианты Does или Doesn't.

Проверьте

Поле Проверка позволяет установить контрольные значения для условия.

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

ПРОВЕРЬТЕ	ОПИСАНИЕ	ПРИМЕР
Существовать	Здесь не важна детальность условия, только то, что оно существует/не существует	Хозяин - существует
Начало	Строка начинается со значения	Путь - Does - Start - /secure
Конец	Строка заканчивается значением	Путь - Делает - Конец - .jpg
Содержать	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 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 новый в области Условие.
2. Выберите условие из выпадающего списка. В качестве примера возьмем Host. Вы также можете ввести текст в поле, и ADC отобразит значение в выпадающем списке.
3. Выберите чувство. Например, Does
4. Выберите проверку. Например, Contain
5. Выберите значение. Например, mycompany.com

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

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

Оценка

Возможность добавления определяемых переменных - это очень важная возможность. Обычные АЦП предлагают эту возможность с помощью сценариев или опций 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 - выбор значений из выпадающего списка или ручной ввод.
- Значение - значение, которое хранит переменная, может быть буквенно-цифровым значением или RegEx для тонкой настройки.

Встроенные переменные:

Встроенные переменные уже жестко закодированы, поэтому вам не нужно создавать для них запись оценки.

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, как правило, 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.

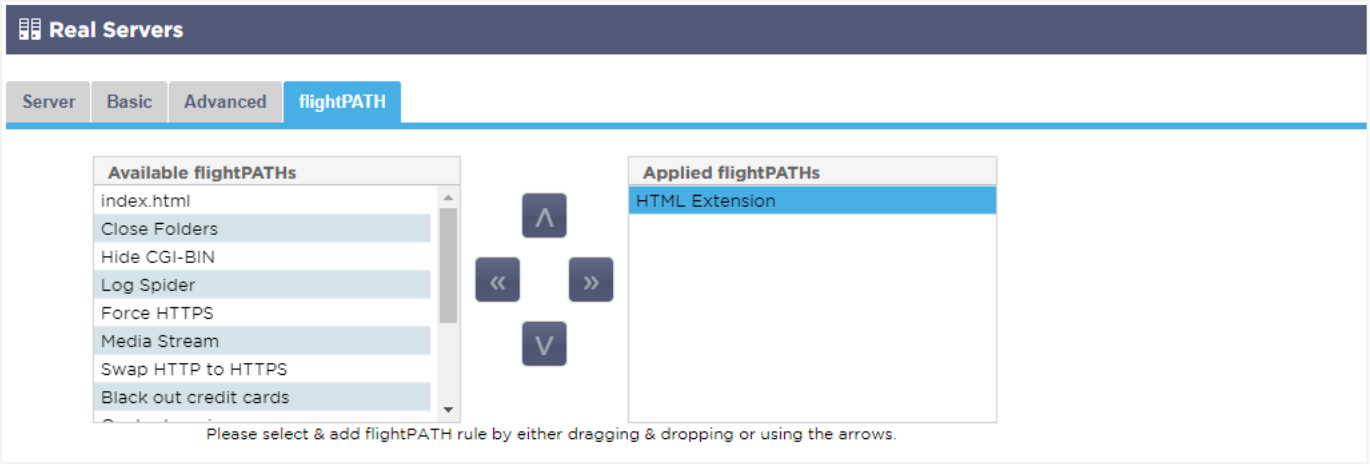
В этом примере мы хотим переписать часть пути URL, чтобы отразить URL, набранный пользователем.

- Нажмите Добавить новый
- Выберите Rewrite Path в раскрывающемся меню Action
- В поле Target введите $path$/myimages
- Нажмите Обновить

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

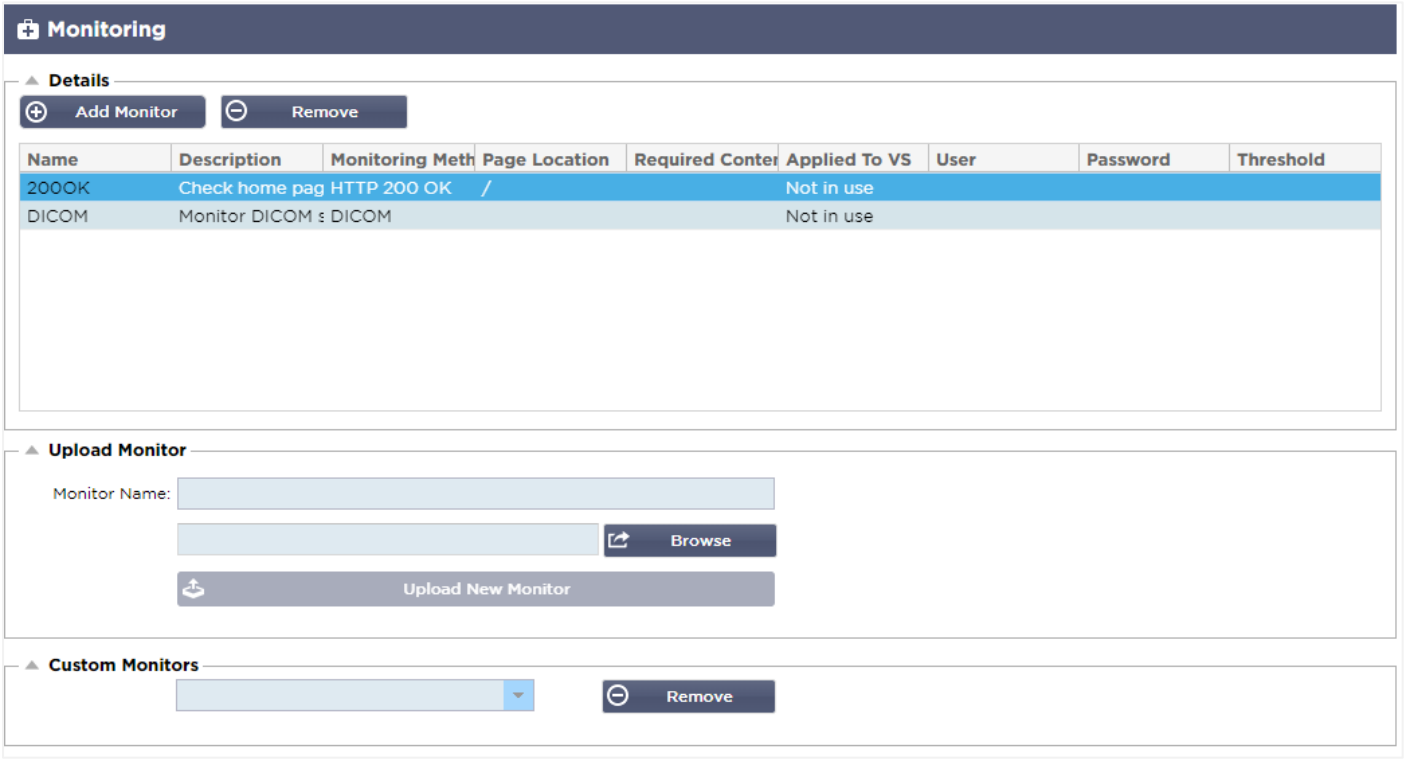
Применение правила flightPATH

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 можно 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



При настройке балансировки нагрузки полезно отслеживать состояние реальных серверов и работающих на них приложений. Например, в веб-серверах можно настроить специальную страницу, которую можно использовать для мониторинга состояния, или воспользоваться одной из других систем мониторинга, имеющихся в ADC.

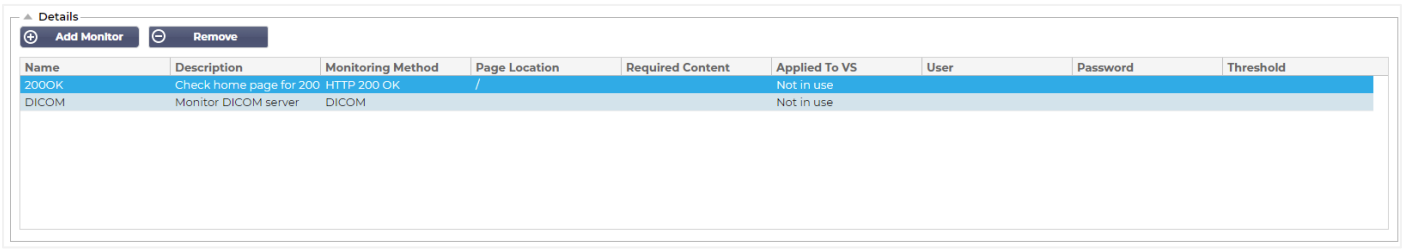
Страница Library > Real Server Monitors позволяет добавлять, просматривать и редактировать пользовательский мониторинг. Это "Проверки здоровья" сервера уровня 7, которые выбираются из поля Мониторинг сервера на вкладке Основные для определенной вами виртуальной службы.

Страница "Мониторы реального сервера" состоит из трех разделов.

- 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 по нему.



Имя

Имя по вашему выбору для вашего монитора.

Описание

Текстовое описание для этого Монитора, и мы рекомендуем сделать его максимально описательным.

Метод мониторинга

Выберите метод мониторинга из раскрывающегося 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 можно использовать только для типов служб HTTP и Accelerated HTTP. Однако, если для HTTP-сервера используется тип службы уровня 4, его все равно можно использовать, если SSL не используется на реальном сервере или обрабатывается соответствующим образом с помощью средства "Content SSL".	Имя: 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: N/A
HTTP-ответ	К реальному серверу устанавливается соединение и HTTP-запрос/ответ, который 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 полным заголовком, частью заголовка, строкой из части страницы или просто одним словом. Если текст найден, считается, что Real Server работает. Этот метод	Имя: 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

	мониторинга можно использовать только для типов служб HTTP и Accelerated HTTP. Однако, если для HTTP-сервера используется тип службы уровня 4, 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 содержимого. Вы также можете установить значение AE Title "Destination Called" в разделе Notes каждого сервера. Вы можете найти столбец Notes в IP Services-. -Виртуальные службы - Страница сервера.	Имя: DICOM Описание: Проверка работоспособности 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 хотите отслеживать, в колонке требуемого содержимого. Этот порт обычно не совпадает с портом трафика и используется, когда вы хотите связать службы вместе	Имя: 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 вы можете использовать несколько различных портов. Монитор считается успешным только в том случае, если все порты, указанные в разделе требуемого содержимого, отвечают правильно.	Название: Многопортовый монитор Описание: Мониторинг нескольких 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, например /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 в Real Server.

Пароль

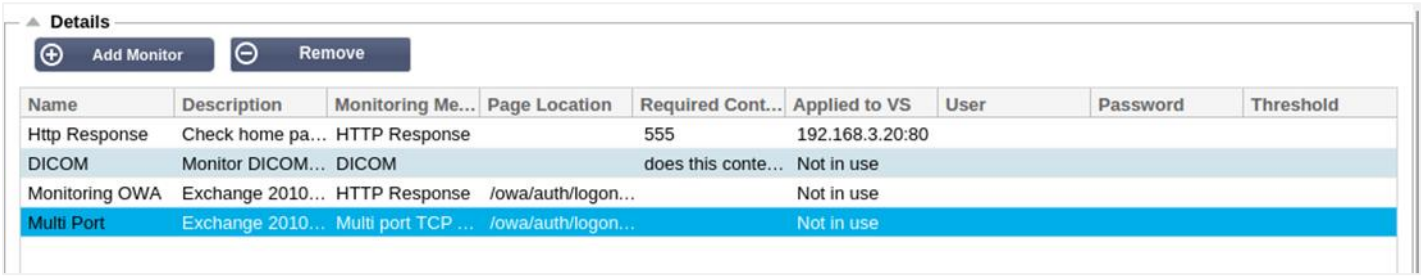
Некоторые пользовательские мониторы могут использовать это значение вместе с полем User для входа в Real Server.

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 можно просмотреть загруженные пользовательские мониторы и удалить их, если они больше не нужны.

- Нажмите на выпадающее поле
- Выберите имя пользовательского монитора
- Нажмите Удалить
- Ваш пользовательский монитор больше не будет отображаться 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 можно использовать в сценарии Perl.

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
- использовать строго;
- предупреждение об использовании;

Сценарии 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 содержимое" 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

Индивидуальные медицинские осмотры имеют два результата

- Успешный
  Возвращаемое значение 1Печатать
  сообщение об успехе в SyslogМаркировка
  реального сервера в режиме онлайн (при условии совпадения IN COUNT)
- Unsuccessful
  Возвращаемое значение 2Печатать

сообщение о неудаче в SyslogПометить
реальный сервер как автономный (при условии совпадения OUT Count).

Пример пользовательского монитора здоровья

```
#Monitor-Name HTTPS_SNI
использовать 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 $auth        =;
if ($port)
{
        $resolve = "$notes:$port:$host":
}
иначе {
        $resolve = "$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 - $content - Health check successful.\n";
        возврат(1);
        }
else
        {
        print "HTTPs://${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.

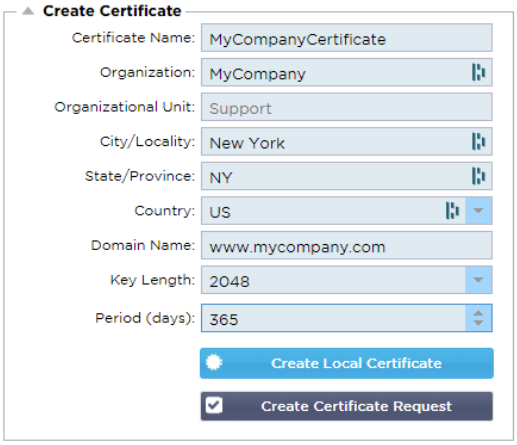
Что делает ADC с SSL-сертификатом?

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 ADC может использовать глобально доверенный сертификат SSL, он может генерировать самоподписанный сертификат SSL. Самоподписанный SSL-сертификат идеально подходит для внутренних требований балансировки нагрузки. Однако ваши ИТ-политики могут потребовать наличия доверенного сертификата или сертификата ЦС домена.

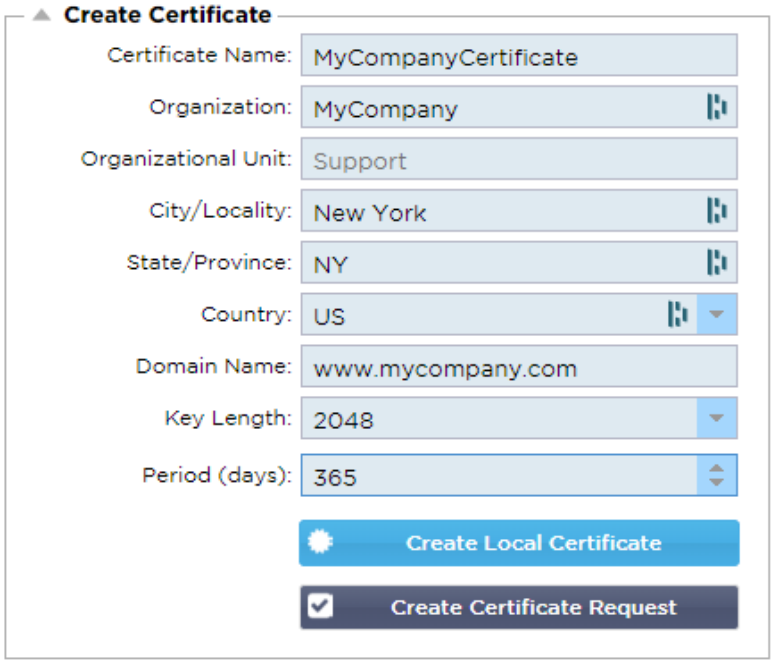
Как создать локальный SSL-сертификат



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

Создание запроса на сертификат (CSR)

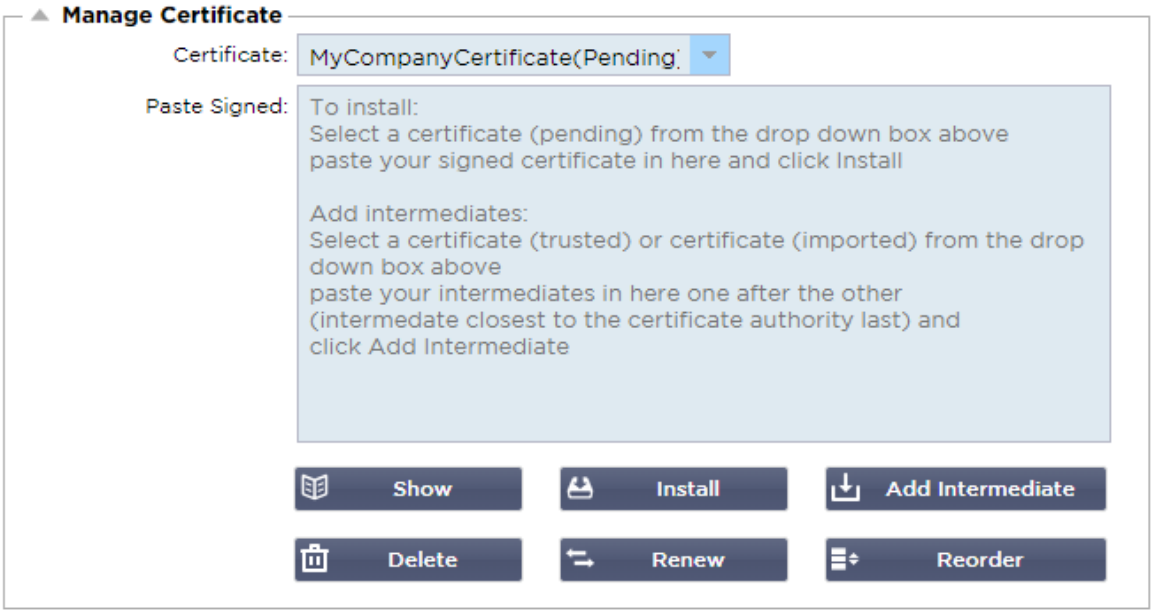
Когда вам нужно получить глобально доверенный SSL от внешнего провайдера, вам нужно будет создать CSR для генерации SSL-сертификата.



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

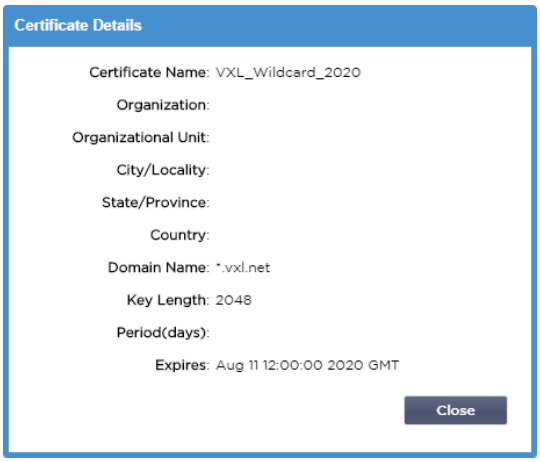
Вам нужно будет вырезать и вставить содержимое в ТЕКСТОВЫЙ файл и назвать его с расширением CSR, например, *mycert.csr*. Этот файл CSR нужно будет предоставить в центр сертификации для создания SSL-сертификата.

Управление сертификатом



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

Показать

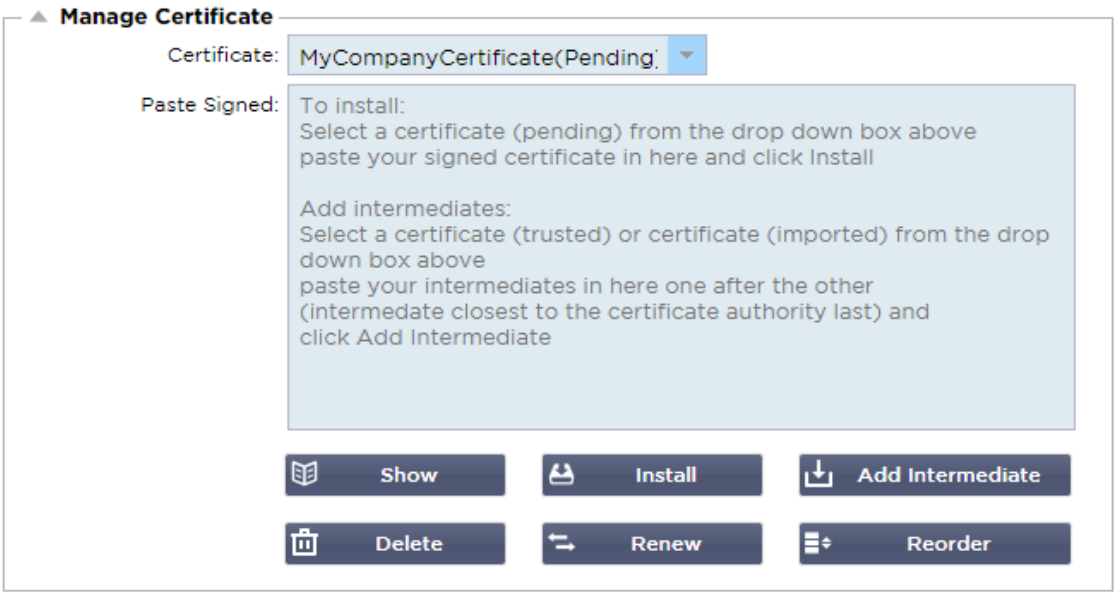


Бывают случаи, когда вы хотите просмотреть детали установленного SSL-сертификата.

- Выберите сертификат из выпадающего меню
- Нажмите на кнопку Показать
- Во всплывающем окне, показанном ниже, будут представлены сведения о сертификате.

Установка сертификата

После получения сертификата от доверенного центра сертификации необходимо сопоставить его со сгенерированным CSR и установить его в ADC.



- Выберите сертификат, который вы создали в описанных выше шагах. Для элемента строки будет установлен статус (Pending). В примере MyCompanyCertificate показан на изображении выше.
- Откройте файл сертификата в текстовом редакторе
- Копирование всего содержимого файла в буфер обмена
- Вставьте содержимое подписанного SSL-сертификата, полученного от доверенного центра, в поле с надписью Paste Signed.
- Вы также можете вставить промежуточные элементы ниже этого, соблюдая правильный порядок:
    1. (TOP) Подписанный вами 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, поскольку они существуют на клиентских машинах.
       (ADC также содержит корневой пучок для повторного шифрования, когда он выступает в качестве клиента Real Server)
- Нажмите кнопку Установить
- После установки сертификата вы должны увидеть статус (Trusted) рядом с вашим сертификатом.

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

Добавить посредника

В некоторых случаях требуется добавлять промежуточные сертификаты отдельно. Например, вы могли импортировать сертификат, не содержащий 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 Delete. После удаления сертификат будет полностью удален из ADC, и его необходимо будет заменить, а затем снова применить к виртуальным службам, если это потребуется.

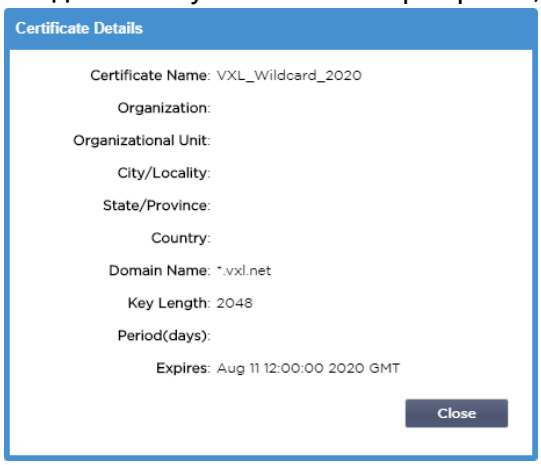
Примечание: Перед удалением сертификата убедитесь, что он не прикреплен к рабочему VIP-клиенту.

Продлить сертификат

Кнопка Renew позволяет получить новый запрос на подпись 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 можно было получить новый сертификат

- Когда вы получите новый сертификат, выполните действия, 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, будут представлены сведения 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 раскрывающихся 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 Импорт.
- Теперь ваш сертификат будет находиться в соответствующих выпадающих меню SSL в ADC.

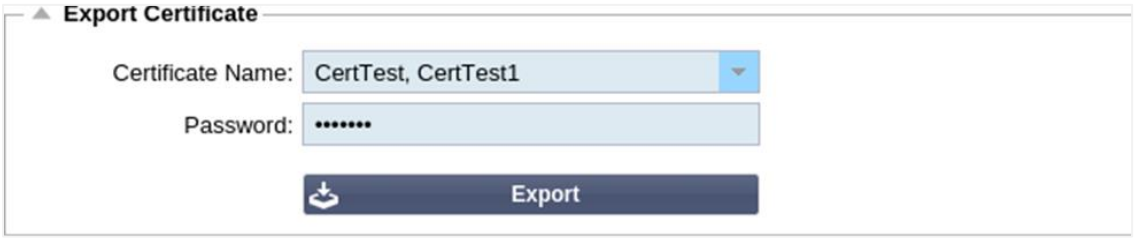
Импорт нескольких сертификатов

Этот раздел позволяет 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, экспортировав несколько сертификатов
- Введите пароль, который вы использовали для создания файла JNBK
- Нажмите 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. Для этого в АЦП предусмотрена соответствующая возможность.



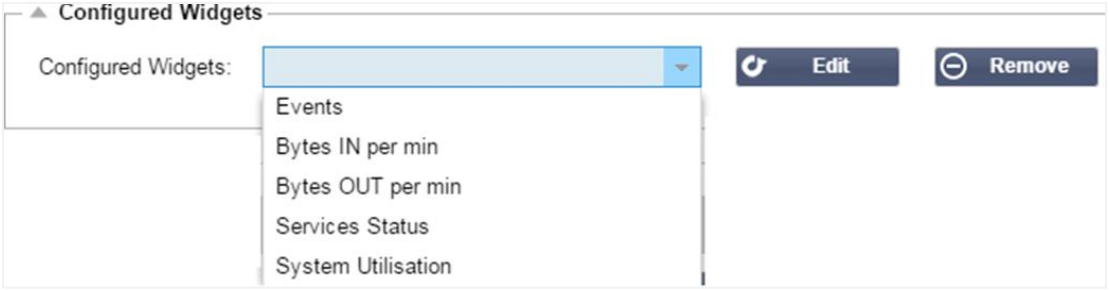
- Щелкните сертификат или сертификаты, которые вы хотите установить. Вы можете выбрать опцию Все, чтобы выбрать все перечисленные сертификаты.
- Введите пароль для защиты экспортируемого файла. Пароль должен состоять не менее чем из шести символов. Можно использовать буквы, цифры и некоторые символы.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

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

Виджеты

На странице Библиотека > Виджеты можно настроить различные легкие визуальные компоненты, отображаемые на пользовательской приборной панели.

Настроенные виджеты

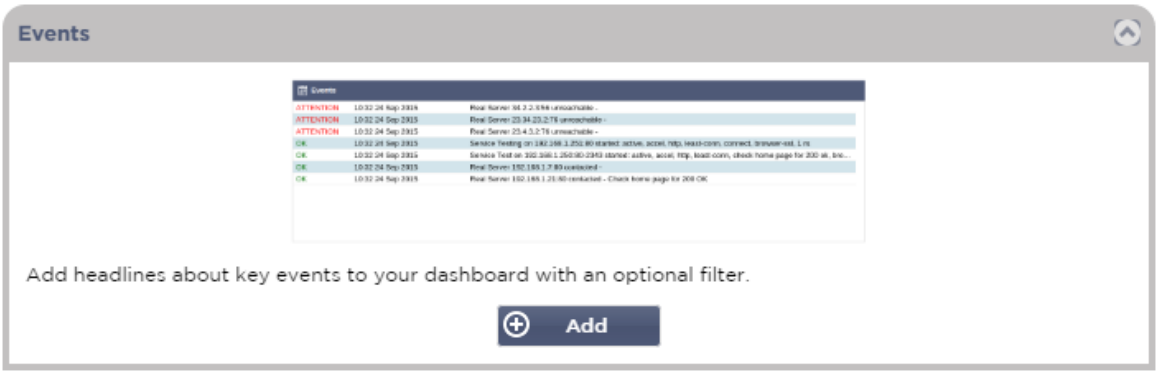


Раздел Настроенные виджеты позволяет просматривать, редактировать или удалять любые виджеты, созданные в разделе доступных виджетов.

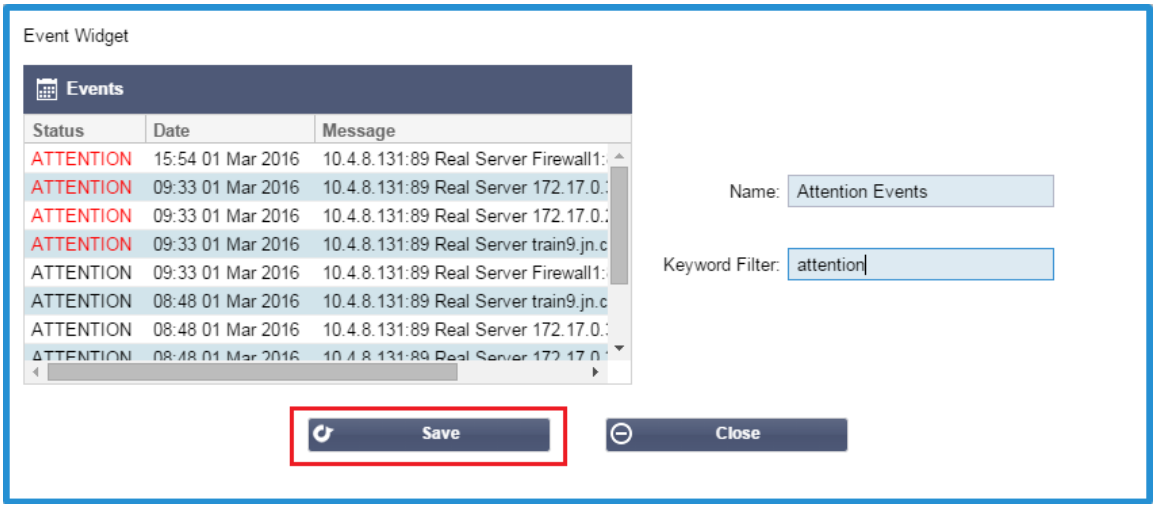
Доступные виджеты

В ADC предусмотрено пять различных виджетов, которые можно настроить в соответствии с вашими требованиями.

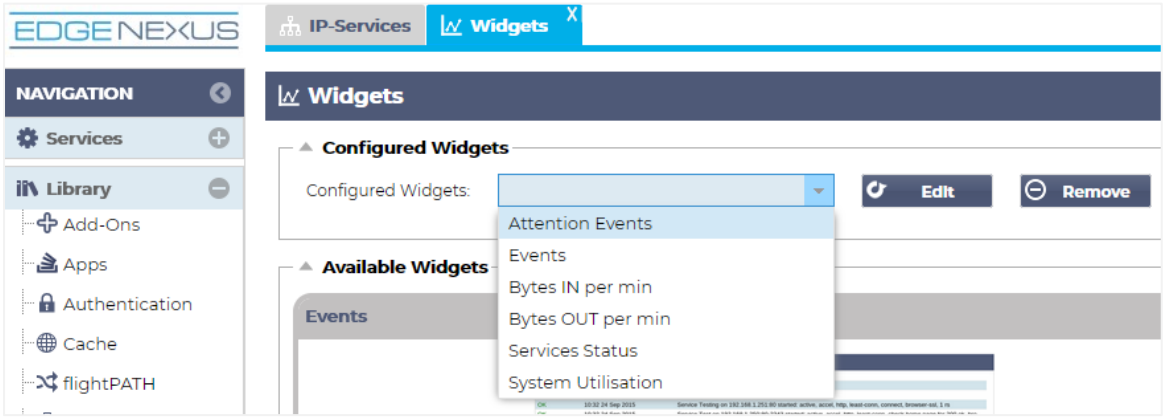
Виджет событий



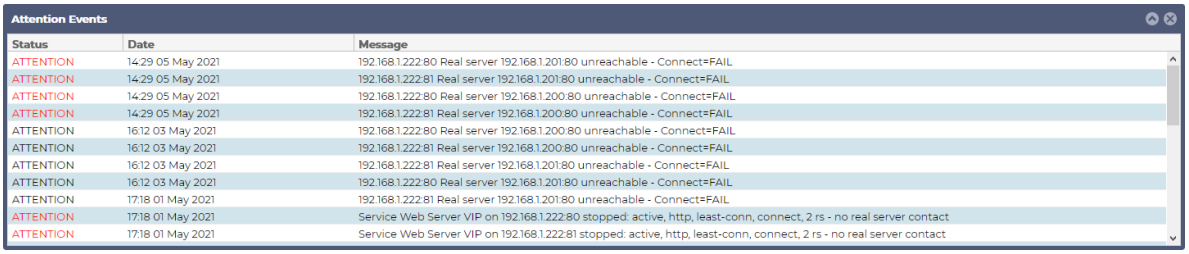
- Чтобы добавить событие в виджет "События", нажмите кнопку Добавить.
- Укажите название для вашего события. В нашем примере в качестве названия события мы добавили Attention Events.
- Добавьте фильтр ключевых слов. Мы также добавили значение фильтра Внимание



- Нажмите Сохранить, затем Закрыть
- Теперь вы увидите дополнительный виджет под названием Attention Events в выпадающем списке Configured Widgets.

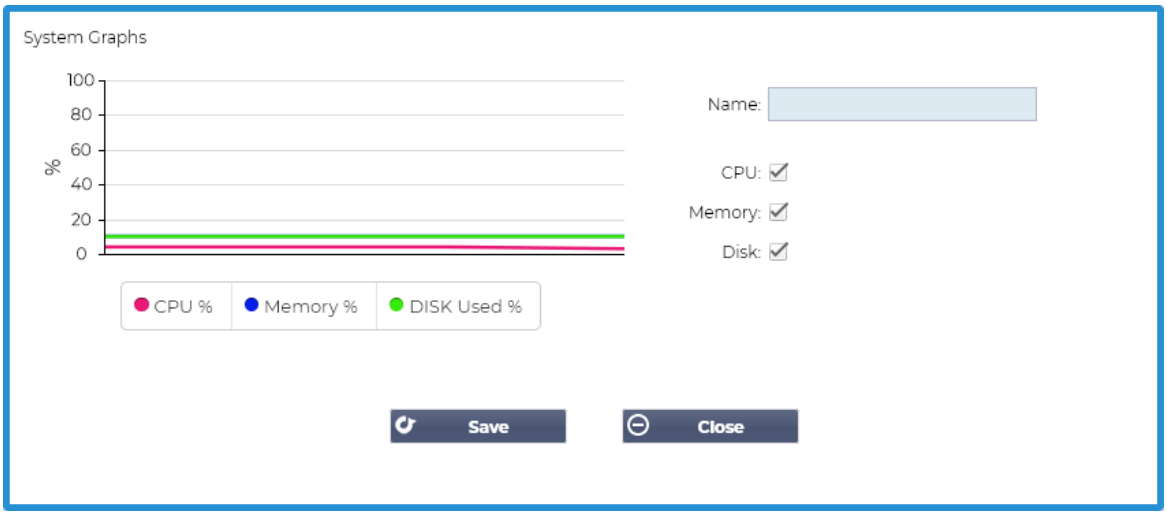


- Вы можете видеть, что теперь мы добавили этот виджет в раздел View > Dashboard.
- Выберите виджет "События внимания", чтобы отобразить его на приборной панели. См. ниже.



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

Виджет системных графиков

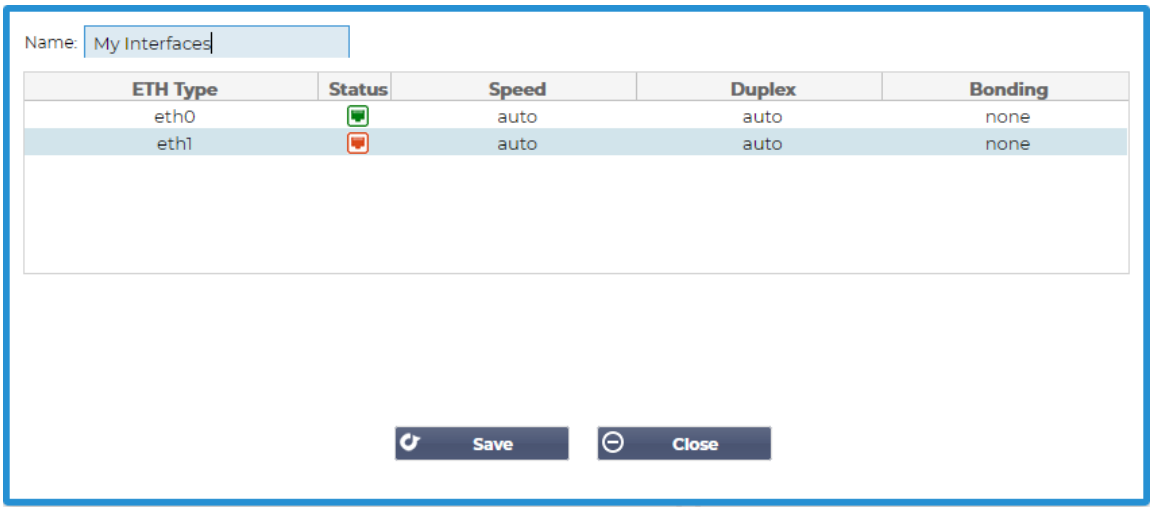


В АЦП имеется настраиваемый виджет System Graph. Нажав кнопку Добавить на виджете, вы можете добавить следующие графики мониторинга для отображения.

- ПРОЦЕССОР
- ПАМЯТЬ
- ДИСК

После добавления они будут доступны по отдельности в меню виджетов приборной панели.

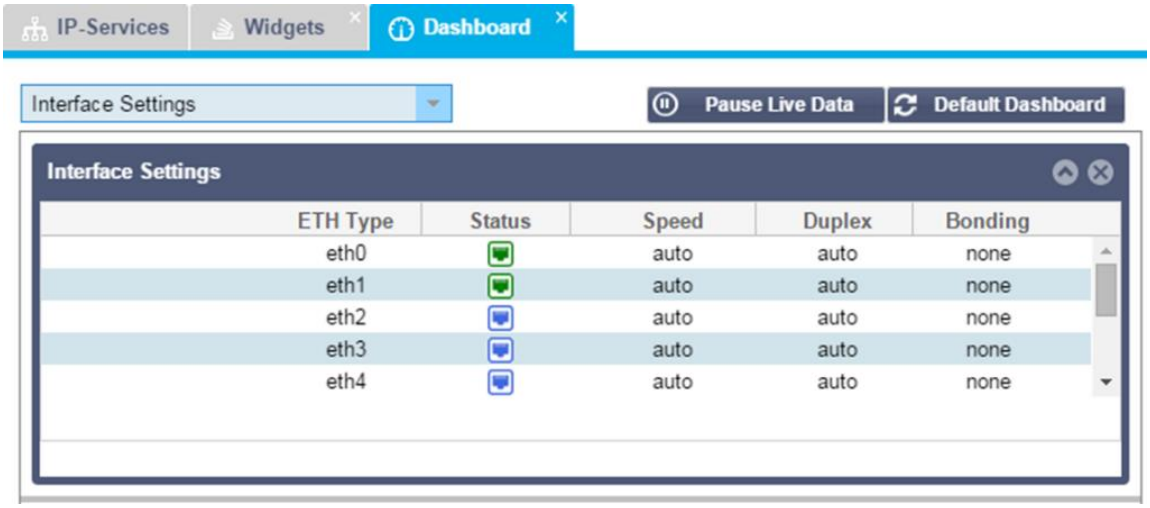
Виджет интерфейса



Виджет Interface позволяет отображать 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.

После завершения нажмите кнопку Сохранить, а затем кнопку Закрыть.

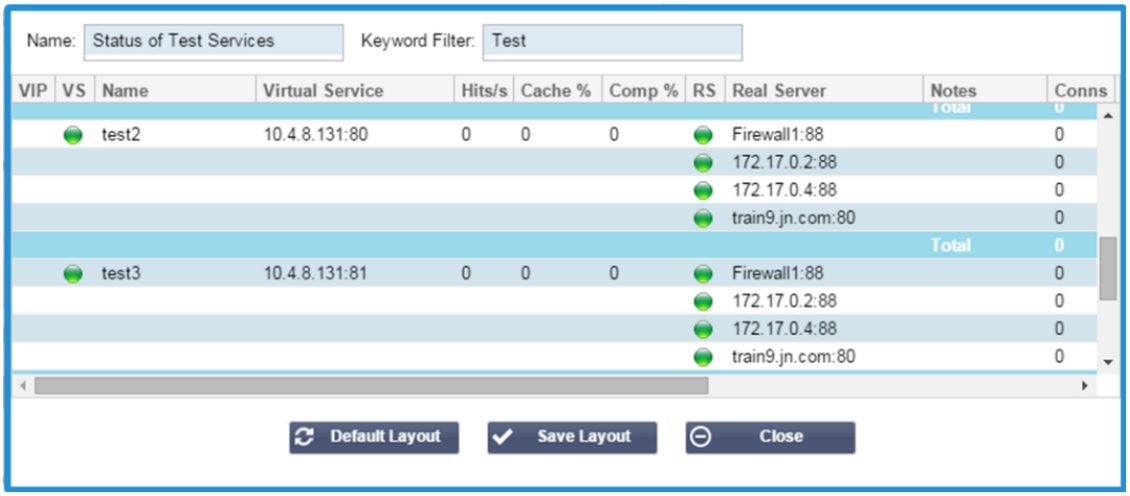
Выберите виджет, который вы только что настроили, из выпадающего меню виджета на панели инструментов. Вы увидите экран, как показано на рисунке ниже.



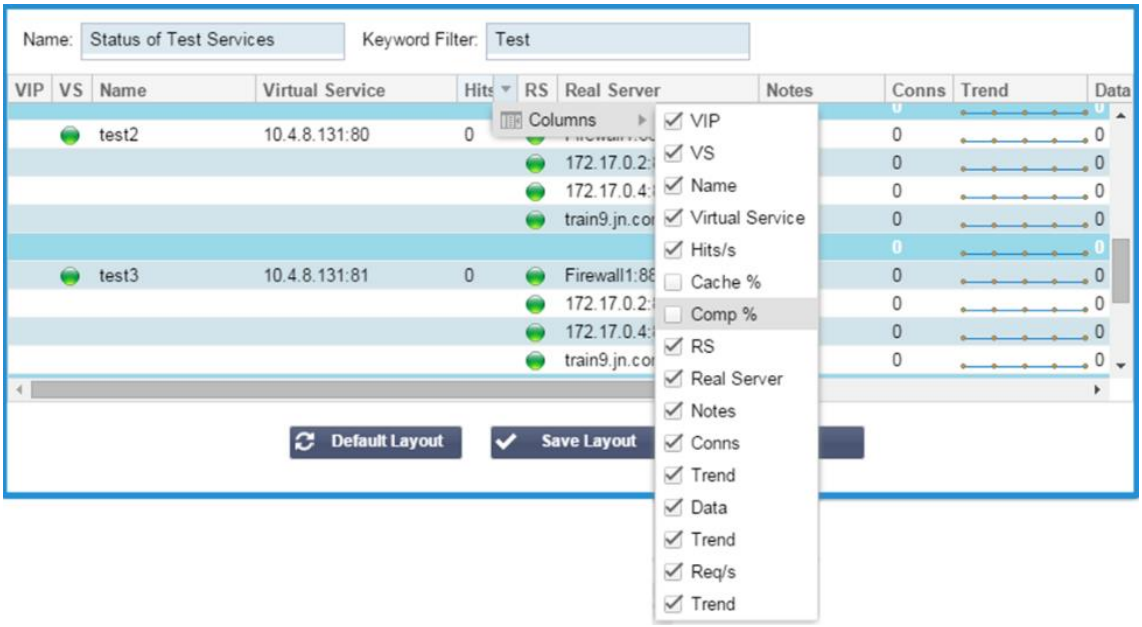
Виджет состояния

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

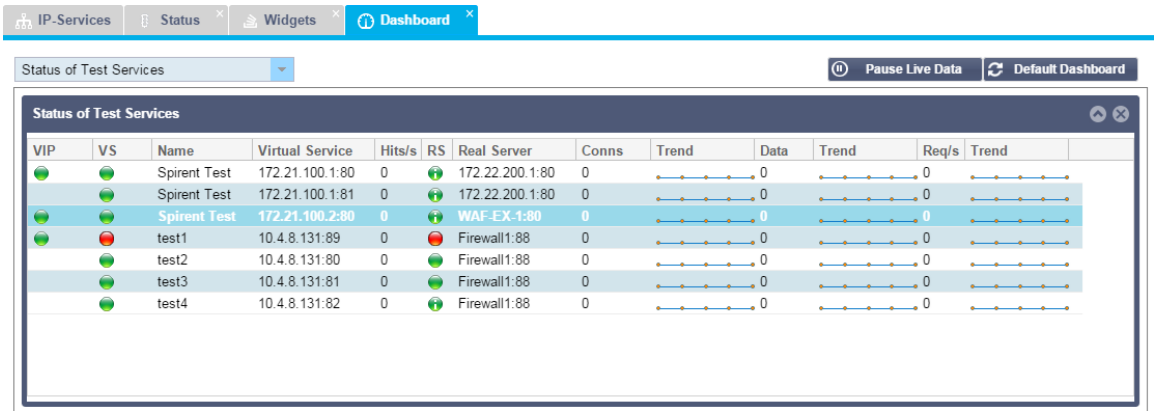
- Нажмите Добавить.



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

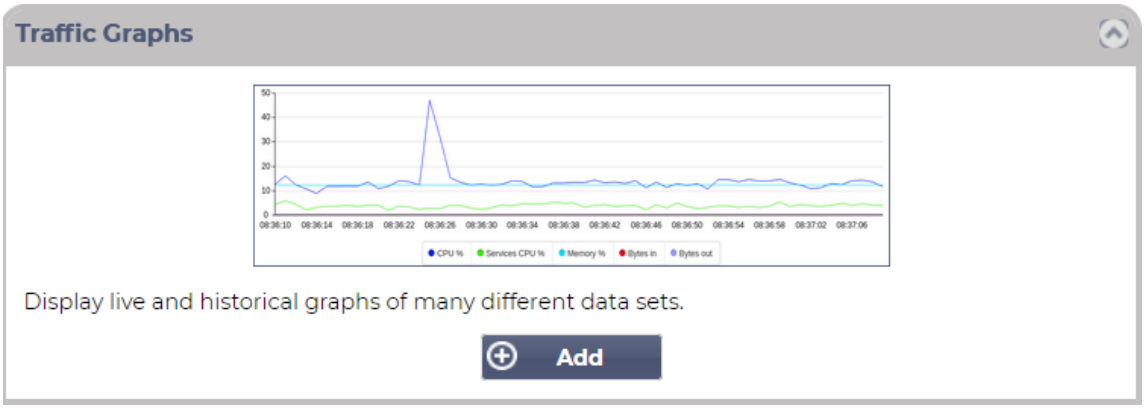


- Как только вы будете удовлетворены, нажмите Сохранить, а затем Закрыть.
- Выбранный виджет Status будет доступен в разделе Dashboard.



Виджет графики трафика

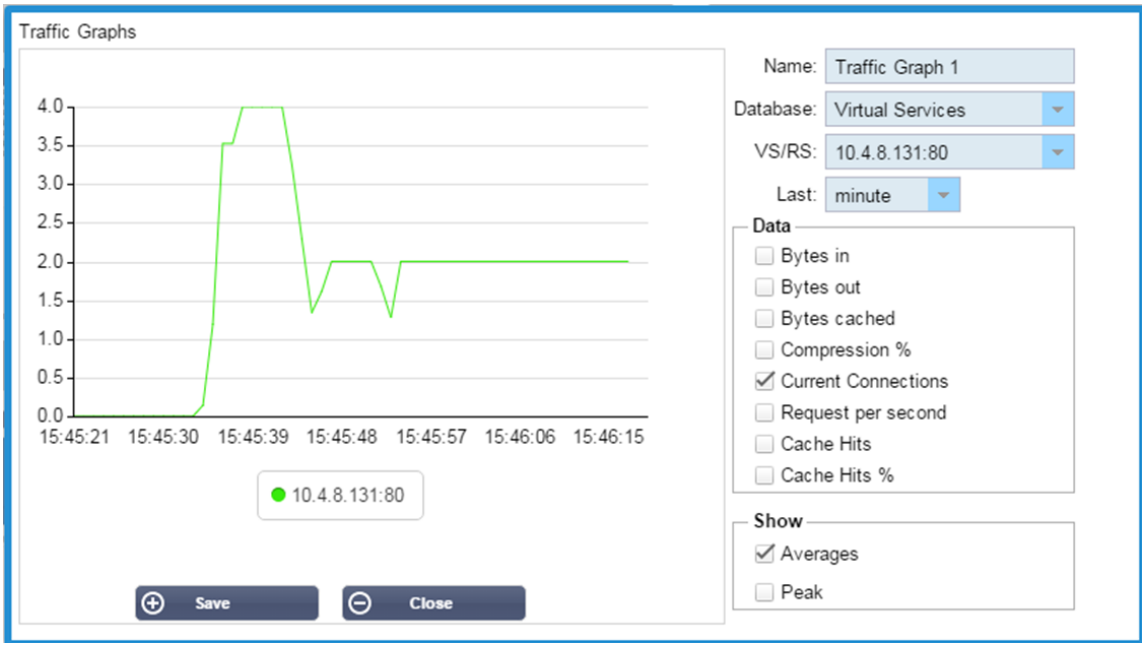
Этот виджет может быть настроен на отображение текущих и исторических данных трафика по виртуальным службам и реальным серверам. Кроме того, вы можете просмотреть общие текущие и исторические данные по глобальному трафику



- Нажмите кнопку Добавить
- Назовите свой виджет.
- Выберите базу данных среди виртуальных служб, реальных серверов или системы.

- Если вы выбрали Virtual Services, 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 базы данных
    - База данных виртуальных служб
    - Байты в
    - Вывод байтов
    - Кэшированные байты
    - Сжатие %
    - Текущие соединения
    - Запросы в секунду
    - Хиты кэша
    - Хиты кэша %
- Настоящие серверы
    - Байты в
    - Вывод байтов
    - Текущие соединения
    - Запрос в секунду
    - Время отклика
- Система
    - CPU %
    - Услуги ЦП
    - Память %
    - Свободный диск %
    - Байты в
    - Вывод байтов
- Выбор отображения средних или пиковых значений
- После выбора всех параметров нажмите Сохранить и закрыть

Пример графика трафика



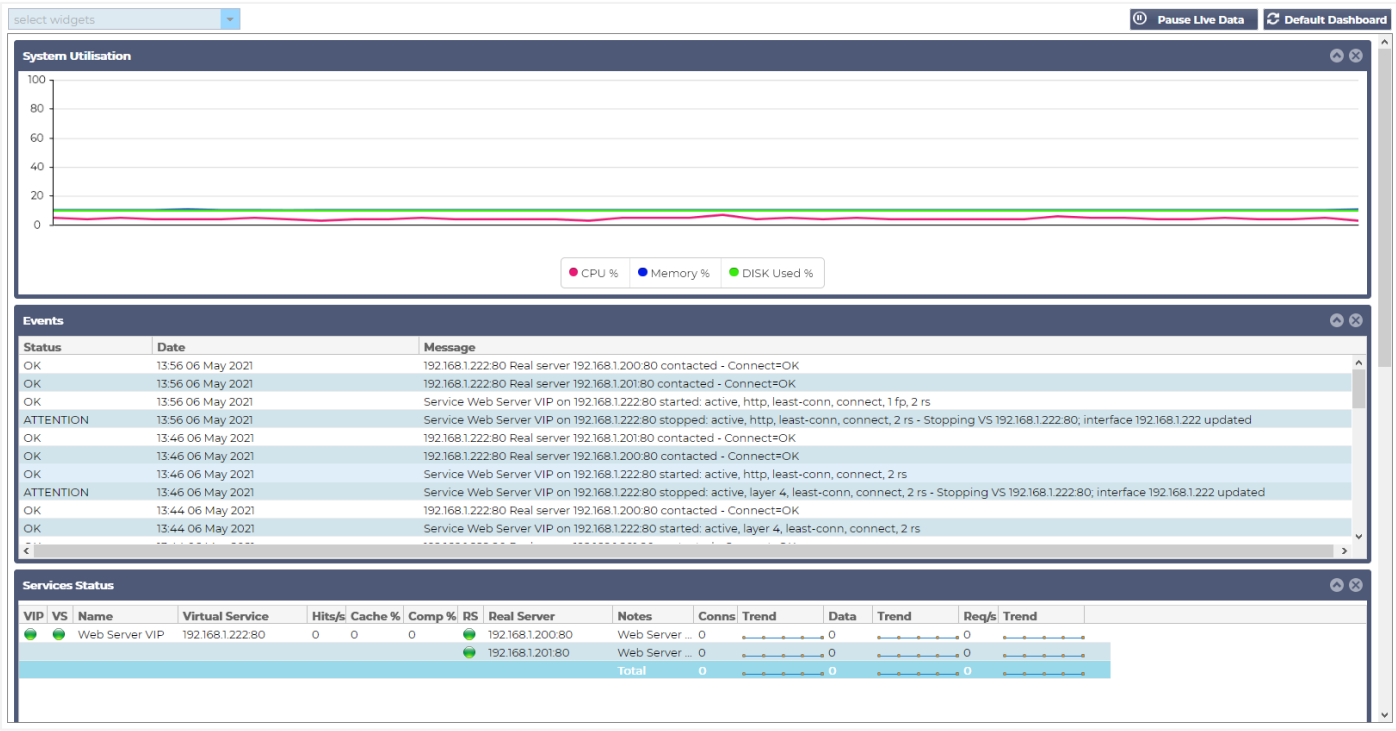
Теперь вы можете добавить свой виджет Traffic Graph в меню View > Dashboard.

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, позволяющую сделать это простым и понятным способом.

Приборная панель доступна с помощью сегмента Вид на панели навигатора. При ее выборе отображается несколько виджетов по умолчанию, а также можно выбрать любые настроенные виджеты, которые вы определили.



Использование приборной панели

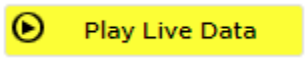
В Dashboard U есть четыре элемента: меню виджетов, кнопка паузы/воспроизведения и кнопка Default Dashboard.

Меню виджетов

Меню "Виджеты", расположенное в верхней левой части приборной панели, позволяет 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 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. После приостановки кнопка переходит в состояние "Воспроизвести данные в реальном времени".



По окончании просто нажмите кнопку Play Live Data (Воспроизвести данные в реальном времени), чтобы возобновить сбор данных и обновить приборную панель.

Кнопка приборной панели по умолчанию

Может возникнуть ситуация, когда вы захотите вернуть макет приборной панели 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

Изменить размер виджета можно очень просто. Нажмите и удерживайте строку заголовка виджета и перетащите его в левую или правую часть области Dashboard. Вы увидите пунктирный прямоугольник, который представляет собой новый размер виджета. Переместите 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 прямоугольник, расположенный 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, его можно перетащить, 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 History (История), выбираемая в навигаторе, позволяет администратору изучить исторические показатели работы ADC. Исторические представления могут быть созданы для виртуальных служб, реальных серверов и системы.

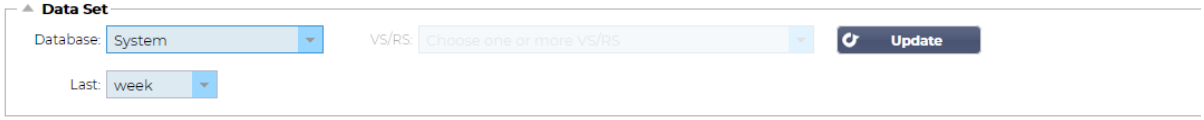
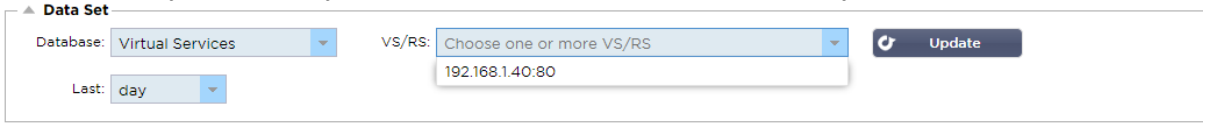
Это также позволит вам увидеть балансировку нагрузки в действии и поможет выявить любые ошибки или закономерности, требующие изучения. Обратите внимание, что для использования этой функции необходимо включить ведение журнала в System > History.

Просмотр графических данных

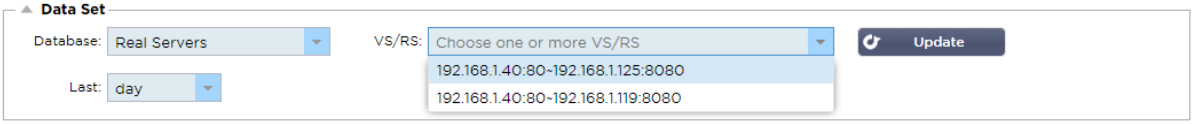
Набор данных

Чтобы просмотреть исторические данные в графическом формате, 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 Last, - это минута, час, день, неделя, месяц и год.

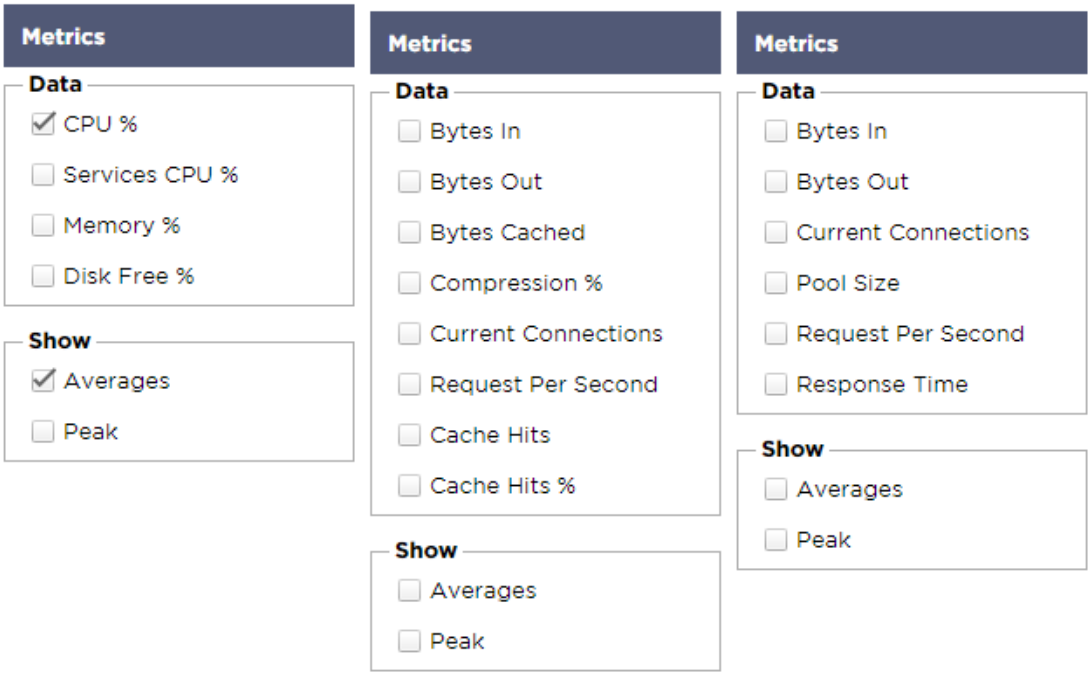
База данных	Описание
Система	Выбрав эту базу данных, вы сможете просмотреть данные о процессоре, памяти и дисковом пространстве с течением времени 
Виртуальные услуги	Выбрав эту базу данных, вы сможете выбрать все виртуальные службы в базе данных с того момента, когда вы начали регистрировать данные.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

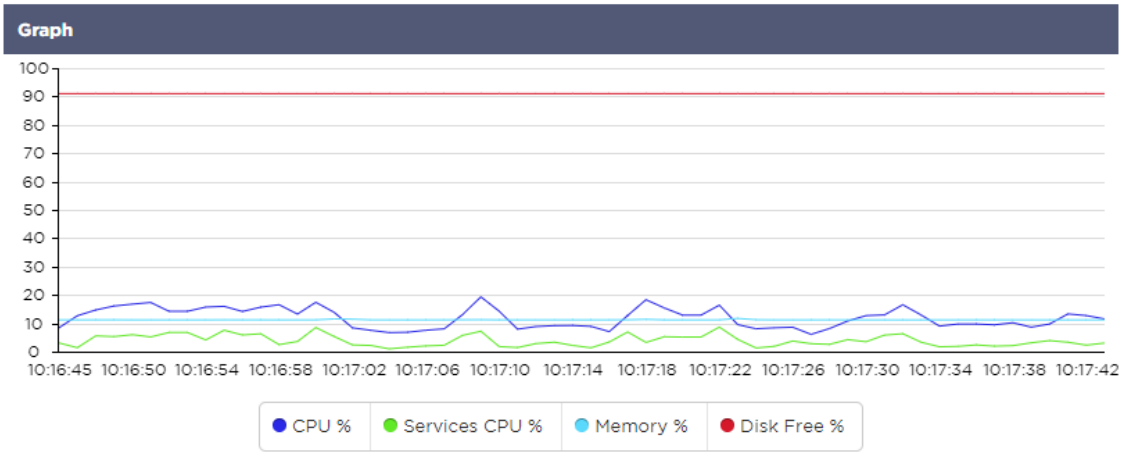


Метрика

После выбора набора данных, который вы будете использовать, пришло время выбрать метрики, которые вы хотите отобразить. На рисунке ниже показаны метрики, доступные для выбора администратором: эти параметры соответствуют системам, виртуальным службам и реальным серверам (слева направо).



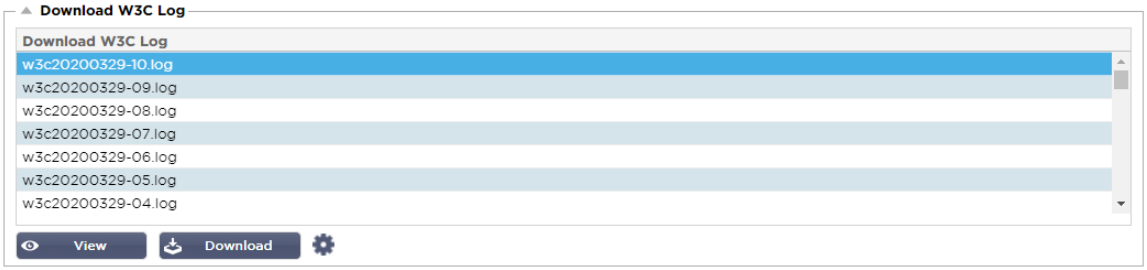
Образец графика



Журналы

Страница Журналы в разделе Вид позволяет просматривать и загружать журналы W3C и Системы. Страница состоит из двух разделов, как показано 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 исходный адрес 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 загрузить его.

Просмотр кнопки

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

Кнопка загрузки

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

Значок шестеренки

Нажав на этот значок, вы перейдете в раздел W3C Log Settings, расположенный в System > Logging. Мы подробно обсудим это в разделе "Ведение журнала" данного руководства.

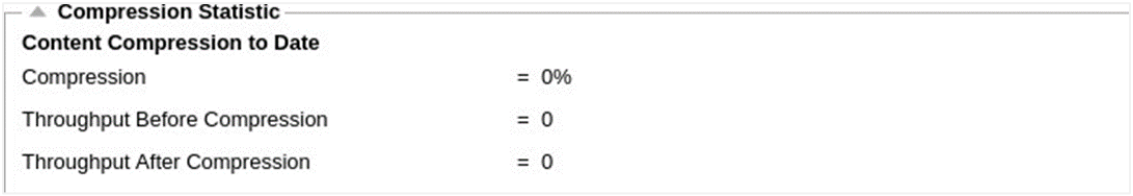
Статистика

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

Компрессия

Вся цель ADC заключается в отслеживании данных и направлении 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 ADC; эти данные предоставляются панелью Сжатие в Статистике.

Сжатие контента на сегодняшний день

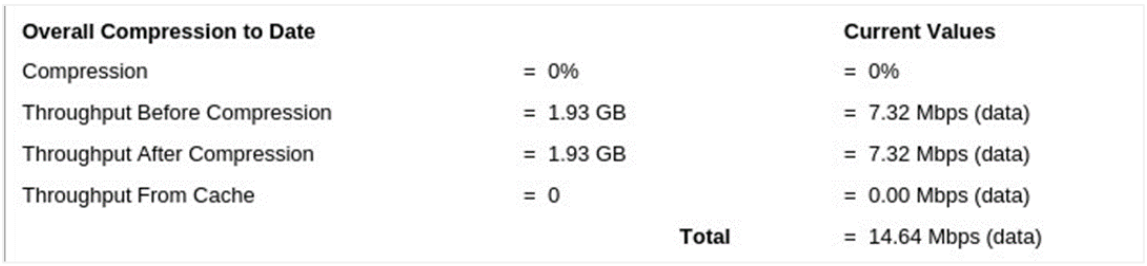


Compression Statistic

Content Compression to Date	
Compression	= 0%
Throughput Before Compression	= 0
Throughput After Compression	= 0

Данные, приведенные в этом разделе, отражают уровень сжатия, достигнутый АЦП для сжимаемого содержимого. 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)

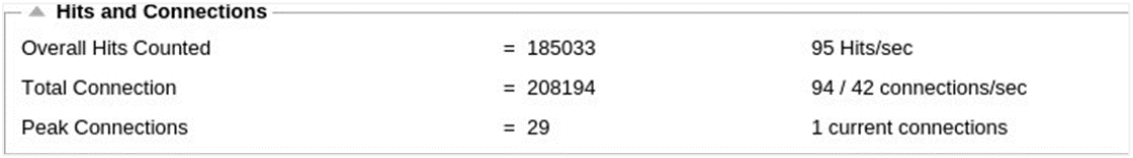
Значения, представленные в этом разделе, сообщают о степени сжатия, достигнутой ADC для всего содержимого. Типичный процент для этого зависит от того, сколько предварительно сжатых изображений содержится в ваших услугах. Чем больше количество изображений, тем меньше будет общий процент сжатия.

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, проходящих в АЦП и из него. Единица измерения будет меняться по мере роста размера от кбит/с до Мбит/с и Гбит/с.

Удары и связи



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. Что означают хиты и соединения?

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

Общее количество подсчитанных хитов

Цифры в этом разделе показывают накопленное количество некэшированных просмотров с момента последнего сброса. В правой части рисунка показано текущее количество обращений в секунду.

Всего подключений

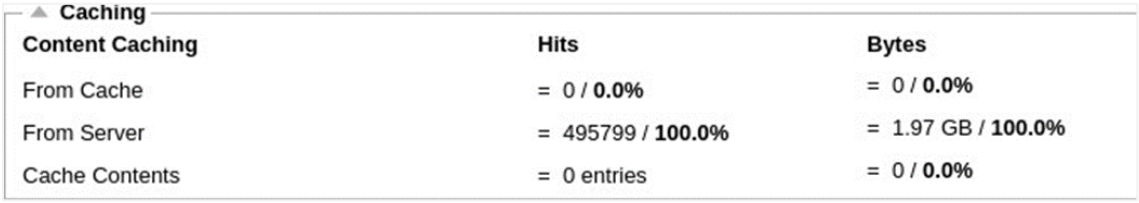
Значение Total Connections представляет собой суммарное количество TCP-соединений с момента последнего сброса. Цифра во втором столбце указывает на количество TCP-соединений, совершаемых в секунду с АЦП. Цифра в правом столбце - это количество TCP-соединений в секунду, выполненных с реальными серверами. 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 приводится 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 указывается 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.

Оборудование

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

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 ADC в настоящее время. Естественно, что этот показатель может колебаться.

Статус

На странице View > Status отображается 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 находится в режиме горячего резервирования
●	Указывает на то, что "пассив" задерживает "актив".
●	Не в сети. Реальные серверы недоступны, или не включены реальные серверы
●	Состояние поиска
●	Не лицензировано или превышено количество лицензированных виртуальных IP-адресов

Колонка состояния VS

Статус	Описание
●	Онлайн
●	Failover-Standby. Эта виртуальная служба находится в режиме горячего резервирования
●	Указывает на то, что "пассив" задерживает "актив".
●	Служба требует внимания. Этот индикатор состояния может быть результатом того, что реальный сервер не прошел мониторинг состояния 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 не включены реальные серверы
●	Состояние поиска
●	Не лицензировано или превышено количество лицензированных виртуальных IP-адресов

Цвет индикатора указывает на состояние виртуальной службы.

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 ADC.

Состояние 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 подключен
●	Состояние поиска
●	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 увидеть балансировку нагрузки в действии. Очень полезно для проверки правильности работы политики балансировки нагрузки.

Данные

Значение в этой колонке показывает объем 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 получить доступ и управлять всеми общесистемными аспектами АЦП.

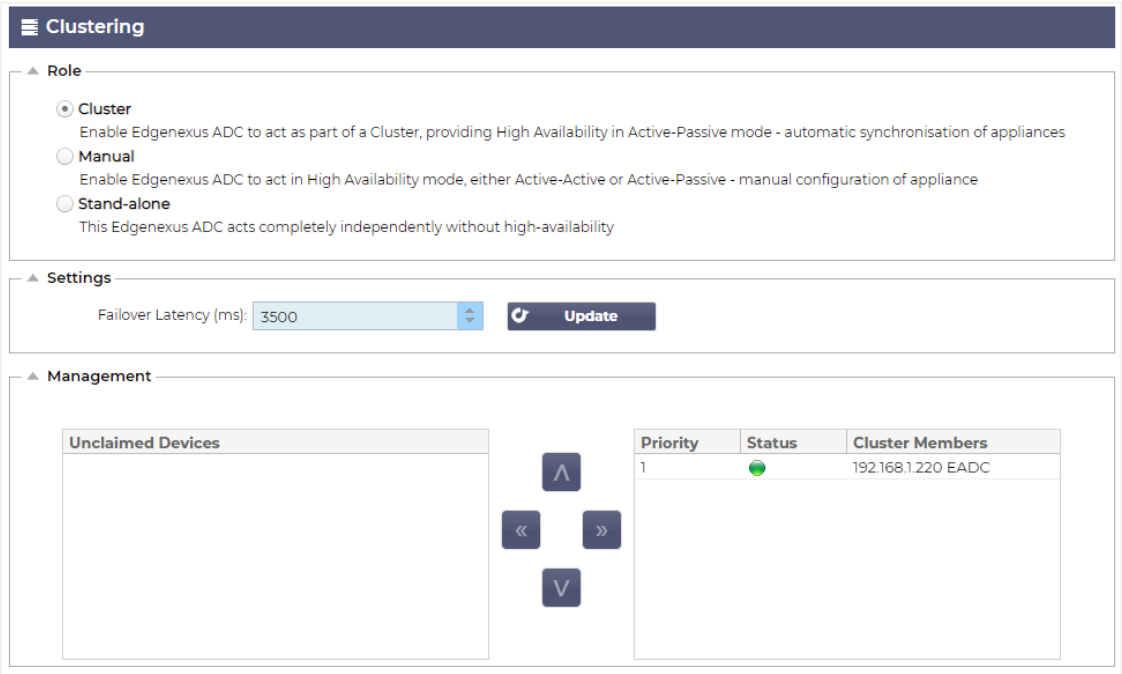
Кластеризация

ADC можно использовать как одиночное автономное устройство, и он будет отлично работать в этом качестве. Однако, если учесть, что назначение ADC - балансировка нагрузки на множество серверов, необходимость кластеризации самого ADC становится очевидной. Легко настраиваемый пользовательский интерфейс ADC делает конфигурацию системы кластеризации простой.

Страница Система > Кластеризация - это место, где вы будете настраивать высокую доступность устройств ADC. Этот раздел состоит из нескольких частей.

Важное замечание

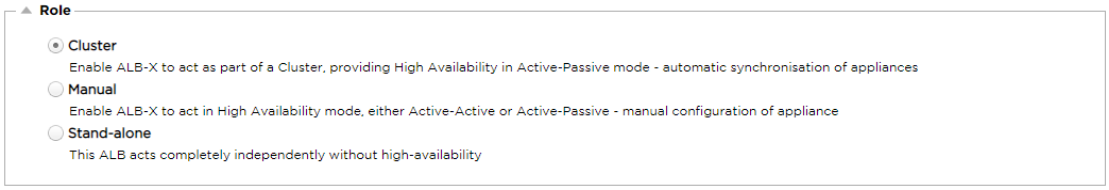
- Для поддержания высокой доступности сердцебиения не требуется выделенный кабель между парой АЦП.
- Сердцебиение происходит в той же сети, что и виртуальная служба, требующая обеспечения высокой доступности.
- Между устройствами ADC не происходит обхода отказа.
- Когда высокая доступность включена на двух или более ADC, каждый блок будет транслировать через UDP виртуальные службы, которые он настроен предоставлять.
- При отказоустойчивости высокой доступности используется одноадресный обмен сообщениями и Gratuitous ARP для информирования новых коммутаторов Active load balancer.



Роль

При настройке ADC на высокую доступность доступны три роли кластера.

Кластер



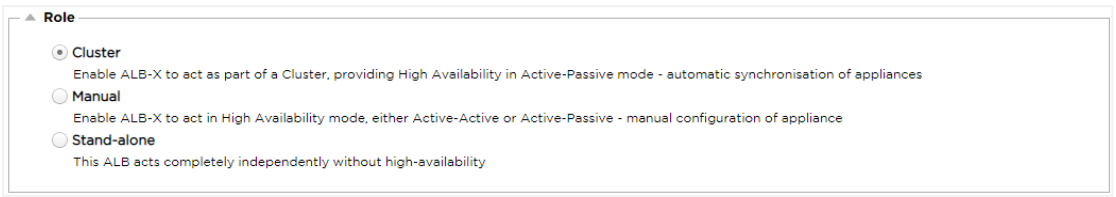
- По умолчанию новый ADC включается с ролью Cluster. В этой роли каждый член кластера будет иметь одинаковую "рабочую конфигурацию", и поэтому только один АЦП в кластере будет активным в любой момент времени.
- Рабочая конфигурация" означает все параметры конфигурации, за исключением элементов, которые должны быть уникальными, таких как IP-адрес управления, имя ALB, 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, а все остальные ADC являются пассивными членами.
- Вы можете редактировать любой ADC в кластере, и изменения будут синхронизированы со всеми членами кластера.
- При удалении ADC из кластера все виртуальные службы будут удалены из этого ADC.
- Вы не можете удалить последний член кластера в Невостребованные устройства. Чтобы удалить последний член кластера, измените роль на Manual или Stand-alone.
- Следующие объекты не синхронизируются:
    - Раздел "Дата и время вручную" - (синхронизируется раздел NTP)
    - Задержка обхода отказа (мс)
    - Раздел "Оборудование
    - Раздел "Приборы
    - Раздел сети

Отказ владельца кластера

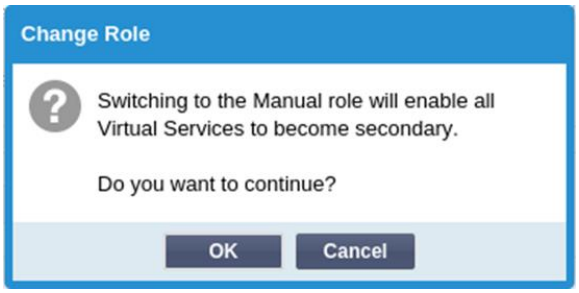
- Когда владелец кластера выходит из строя, один из оставшихся членов автоматически берет на себя его обязанности и продолжает балансировать нагрузку трафика.
- Когда владелец кластера вернется, он возобновит балансировку нагрузки и возьмет на себя роль владельца.
- Предположим, что владелец вышел из 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 отредактируете 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

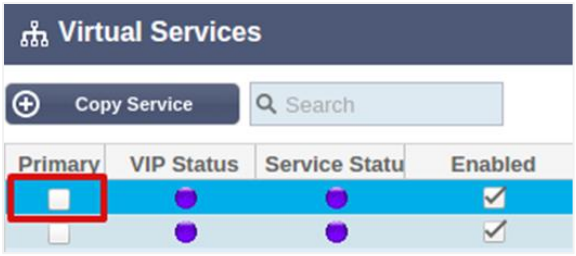
- Если вы хотите изменить роль с Cluster на Manual, нажмите радиокнопку рядом с опцией роли Manual.



- После нажатия радиокнопки вы увидите следующее сообщение:



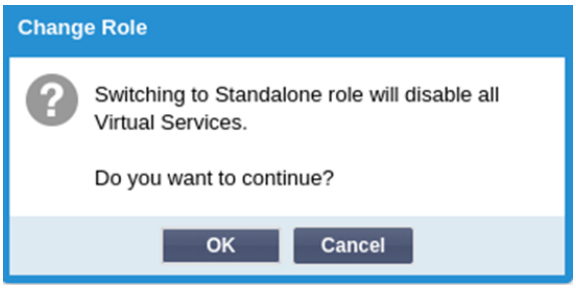
- Нажмите кнопку OK
- Проверьте раздел Виртуальные службы. Вы увидите, что в столбце Primary теперь не установлен флажок.



- 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 кластера на автономный

- Если вы хотите изменить роль с кластерной на автономную, нажмите на радиокнопку рядом с опцией Standalone.
- На экране появится следующее сообщение:



- Нажмите OK, чтобы изменить роли.
- Проверьте свои виртуальные службы. Вы увидите, что столбец Primary изменил название на Stand-alone.
- Вы также увидите, что все виртуальные службы отключены (не отмечены) в целях 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 каждом блоке с помощью графического интерфейса, 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 основном столбце (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 оба столбца Primary отмечены, то происходит процесс выборов, и наименьший MAC-адрес становится активным.
    - Если оба флажка сняты, то происходит тот же процесс выборов. Кроме того, если оба флажка сняты, то автоматического возврата к исходному активному АЦП не происходит.

Самостоятельная роль

ADC в роли автономного не будет взаимодействовать с другими ADC относительно своих служб, 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 сети возникнет конфликт.

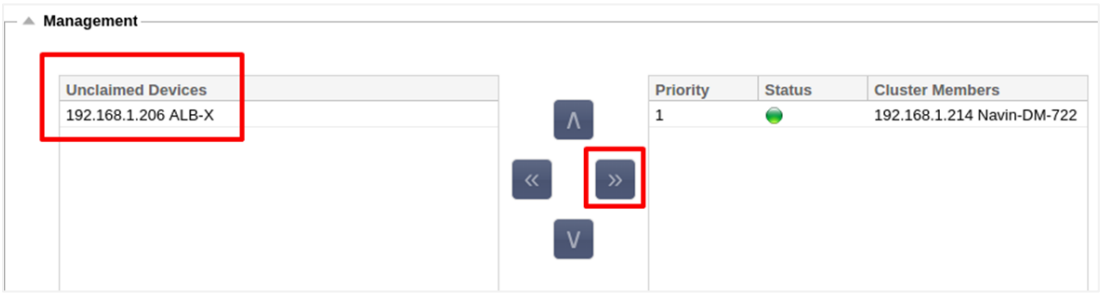
Настройки

В разделе "Настройки" вы можете установить задержку обхода отказа 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.

Управление

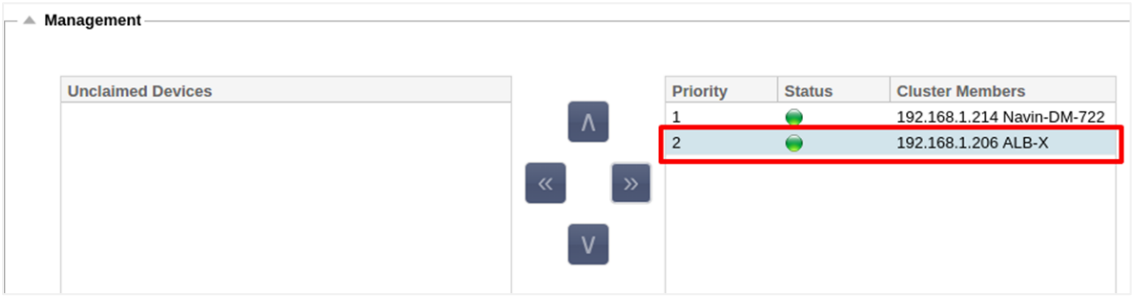
В этом разделе можно добавлять и удалять членов кластера, а также изменять приоритет АЦП в кластере. Раздел состоит из двух панелей и набора клавиш со стрелками между ними. Область слева - это Невостребованные устройства, а самая правая область - это сам кластер.



Добавление АЦП в кластер

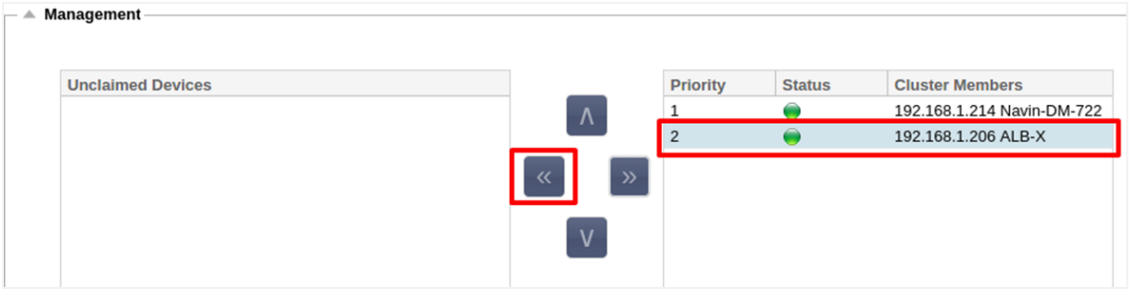
- Перед добавлением ADC в кластер необходимо убедиться, что всем устройствам ADC присвоены уникальные имена в разделе Система > Сеть.
- Вы должны увидеть ADC как Приоритет 1 с зеленым статусом и его имя в колонке Члены кластера в разделе управления. Этот ADC является основным устройством по умолчанию.
- 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 включить ADC в кластер.
- Теперь ваш ADC должен отображаться как Приоритет 2 в списке членов кластера.



Удаление члена кластера

- Выделите член кластера, который вы хотите удалить из кластера.
- Нажмите кнопку со стрелкой влево.

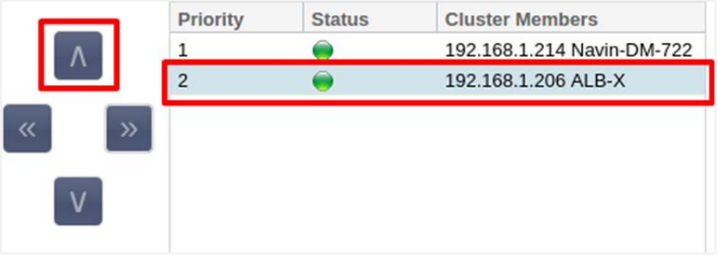


- Вам будет представлен запрос на подтверждение.
- Нажмите OK для подтверждения.
- Ваш ADC будет удален и отображен в разделе "Невостребованные устройства".

Изменение приоритета АЦП

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

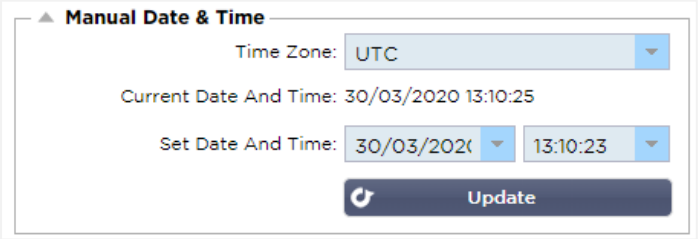
- ADC в верхней части списка Cluster Members имеет приоритет 1 и является активным ADC для всех виртуальных служб.
- ADC, который является вторым в списке, получает приоритет 2 и является пассивным ADC для всех виртуальных служб.
- Чтобы изменить, какой АЦП является активным, просто выделите АЦП и нажмите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



Дата и время

Раздел даты и времени 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, установленное 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, например, в Лондоне, выберите Европа/Лондон, чтобы установить свое местоположение.

Если после вышеуказанных изменений дата и время все еще неправильные, пожалуйста, измените дату вручную

Установите дату и время

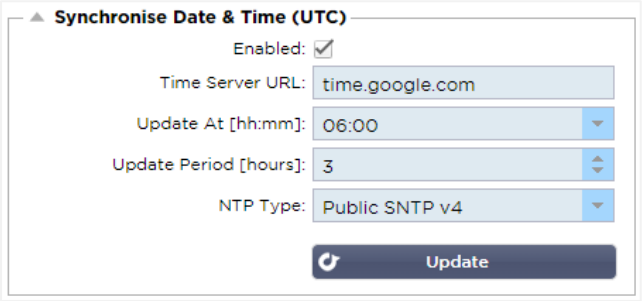
Эта настройка представляет собой фактическую дату и время.

- 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 правильного ввода нажмите Обновить, чтобы подать заявку.
- После этого вы увидите новые дату и время, выделенные жирным шрифтом.

Синхронизация даты и времени (UTC)

Вы можете использовать серверы NTP 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 расположен в глобальной сети Интернет, рекомендуется использовать FQDN.

Обновление в [чч:мм]

Выберите запланированное время, в которое ADC должен синхронизироваться с сервером NTP.

Период обновления [часы]:

Выберите частоту синхронизации.

Тип NTP:

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

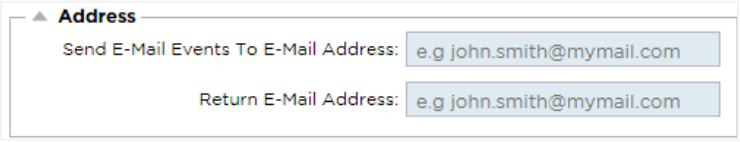
Примечание: Обратите внимание, что синхронизация осуществляется только по UTC. Если вы хотите установить местное время, это можно сделать только вручную. Это ограничение будет изменено в последующих версиях, чтобы включить возможность выбора часового пояса.

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 настроить подключение к серверу электронной почты и отправку уведомлений системным администраторам. Страница организована в следующие разделы.

Адрес



Отправить на электронную почту События на адреса электронной почты

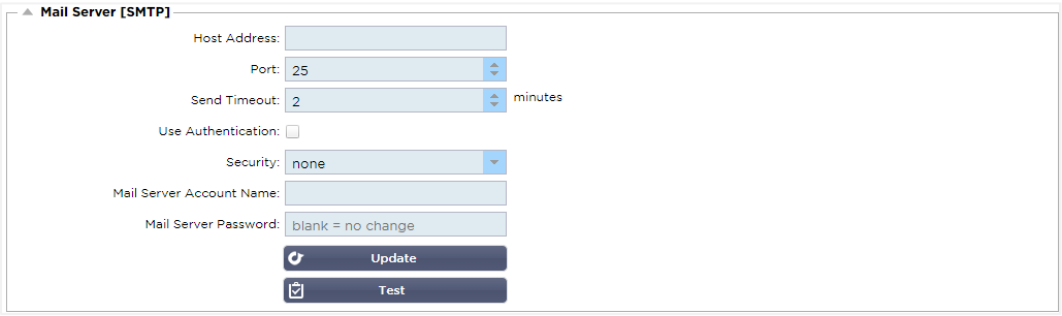
Добавьте действительный адрес электронной почты, на который будут отправляться оповещения, уведомления и события. Пример support@domain.com.

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 необходимо добавить данные SMTP-сервера, который будет использоваться для отправки электронных писем. 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.

Использовать аутентификацию

Поставьте галочку, если ваш SMTP-сервер требует аутентификации.

Безопасность

- Нет
- По умолчанию установлено значение "нет".
- SSL - Используйте этот параметр, если ваш SMTP-сервер требует аутентификации по протоколу Secure Sockets Layer.
- TLS - Используйте этот параметр, если ваш SMTP-сервер требует аутентификации Transport Layer Security.

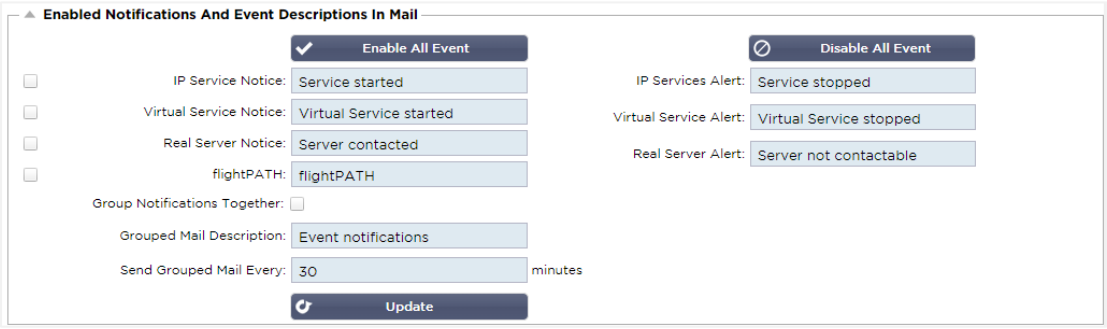
Имя учетной записи основного сервера

Добавьте имя пользователя, необходимое для аутентификации.

Пароль почтового сервера

Добавьте пароль, необходимый для аутентификации.

Уведомления и оповещения



Существует несколько типов уведомлений о событиях, которые ADC будет отправлять лицам, настроенным на их получение. Вы можете отметить и включить уведомления и оповещения, которые должны рассылаться. Уведомления возникают при обращении к реальным серверам или запуске каналов. Оповещения возникают, когда с серверами Real Servers 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 реальный сервер и порт подключены или не могут связаться, ADC отправит уведомление реальному серверу.

flightPATH

Это уведомление представляет собой электронное письмо, отправляемое при выполнении какого-либо условия, и в нем настроено действие, предписывающее 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.

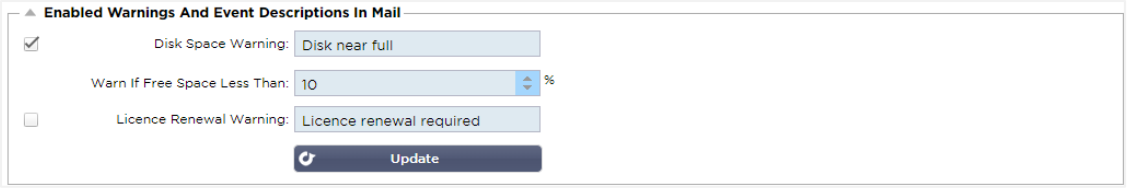
Описание групповой почты

Укажите соответствующую тему для группового уведомления по электронной почте.

Интервал групповой отправки

Задайте время ожидания 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. При достижении этого значения вам будет отправлено электронное письмо.

Истечение срока действия лицензии

Этот параметр позволяет включить или отключить предупреждение об истечении срока действия лицензии, отправляемое по электронной почте системному администратору. При достижении этого значения вам будет отправлено электронное письмо.

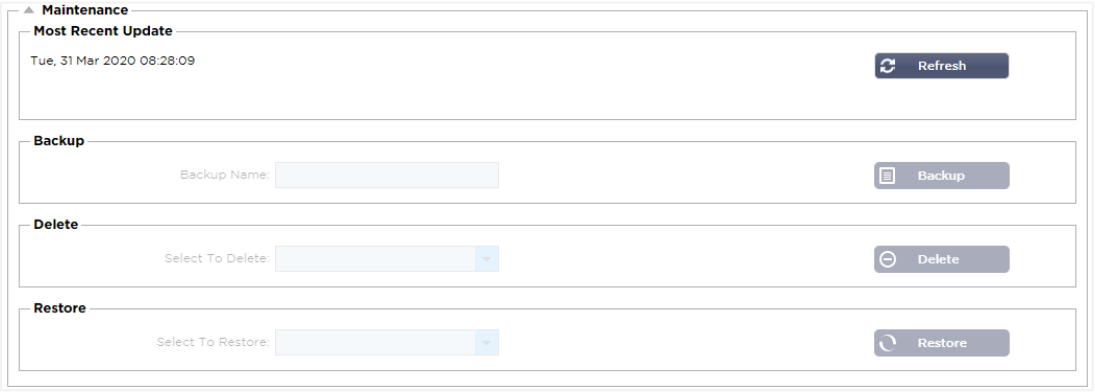
История системы

В разделе Система находится опция История системы, позволяющая получать исторические данные для таких элементов, как процессор, 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 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. Снимите флажок Enabled в разделе Collect Data и нажмите Update, чтобы разрешить ведение исторических журналов.

Резервное копирование

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

Удалить

Выберите файл резервной копии из раскрывающегося 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

Лицензия на использование АЦП выдается либо по 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 необходимости приобретения поддержки 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" с ежегодной оплатой.

Лицензия Подробнее

Каждая лицензия содержит конкретные сведения, относящиеся к лицу или организации, приобретающей ее.

Идентификатор лицензии

Этот идентификатор лицензии напрямую связан с идентификатором машины и другими сведениями, относящимися к вашей покупке 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 устройств ADC. Если вы работаете в виртуализированной среде, то 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.

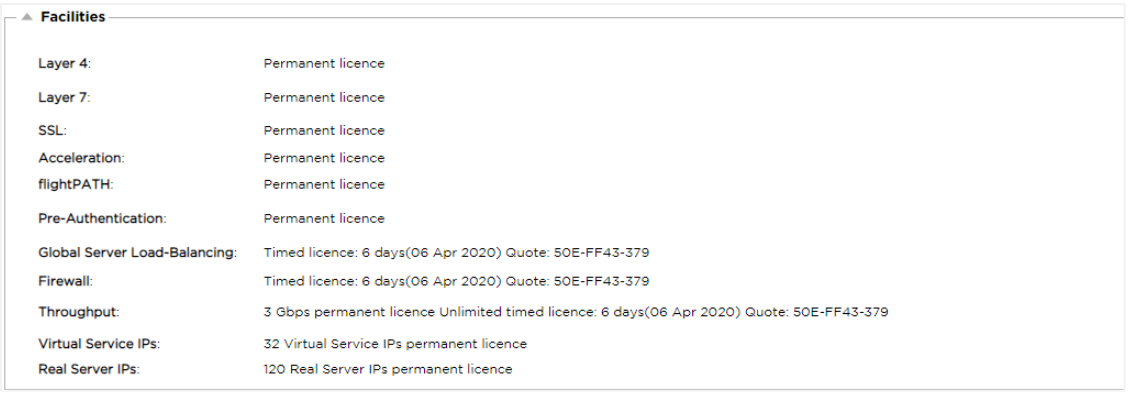
Проблемы с датами

Дата выдачи лицензии

Имя

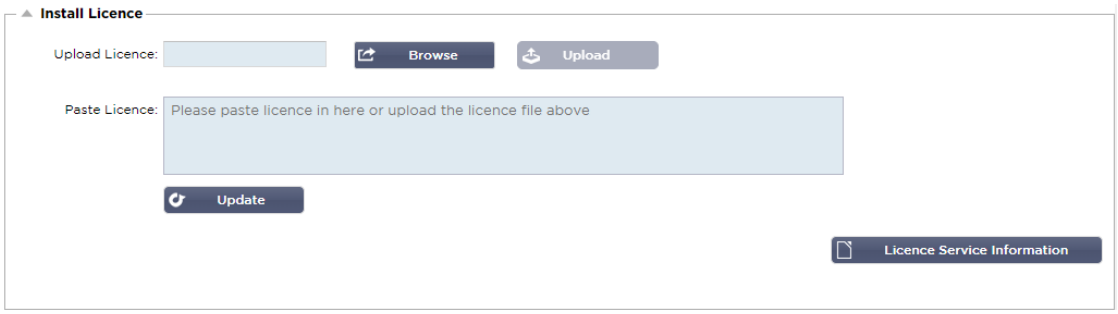
Это значение показывает описательное имя для устройства ADC Appliance, которое вы предоставили.

Удобства



В разделе "Средства" содержится информация 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 лицензии.

Установить лицензии



- Установка новой лицензии очень проста. Когда вы получите новую или запасную лицензию от Edgenexus, 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.
- После этого, пожалуйста, нажмите кнопку обновления
- Теперь лицензия установлена.

Информация о лицензионной службе

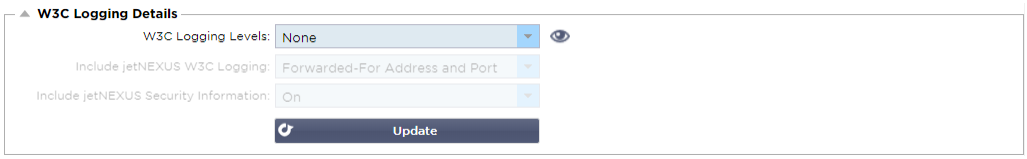
При нажатии кнопки Информация об обслуживании лицензии отобразится вся информация о лицензии. Эту функцию можно использовать для отправки сведений сотрудникам службы поддержки.

Ведение журнала

Страница System > Logging позволяет установить уровни протоколирования 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 IP-адрес источника, версию HTTP, тип браузера, ссылающуюся страницу и отметку времени. Формат был разработан World Wide Web Consortium (W3C), организацией, которая продвигает стандарты для развития Сети. Файл представляет собой текст в формате ASCII с колонками, разделенными пробелами. В файле есть строки комментариев, начинающиеся с символа #. Одна из этих строк комментариев - это строка с указанием полей (с именами 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.

Значение	Описание
Нет	Регистрация W3C отключена.
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. Информацию о значении полей см. ниже. 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 значении полей см. ниже. Здесь представлены 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 HTTP.

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

В таблице ниже описаны уровни протоколирования для W3C FTP.

Включить протоколирование W3C

Этот параметр позволяет установить, какая информация об АЦП должна быть включена в журналы W3C.

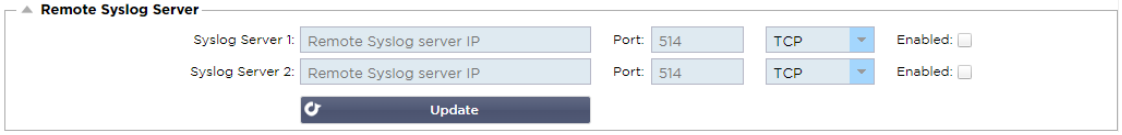
Значение	Описание
Сетевой адрес и порт клиента	Значение, показанное здесь, отображает фактический IP-адрес клиента вместе с портом.
Сетевой адрес клиента	Этот параметр будет включать и показывать только фактический IP-адрес клиента.
Адрес и порт для переадресации	Эта опция покажет детали, содержащиеся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

Включить информацию о безопасности

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.

Это меню состоит из двух опций:

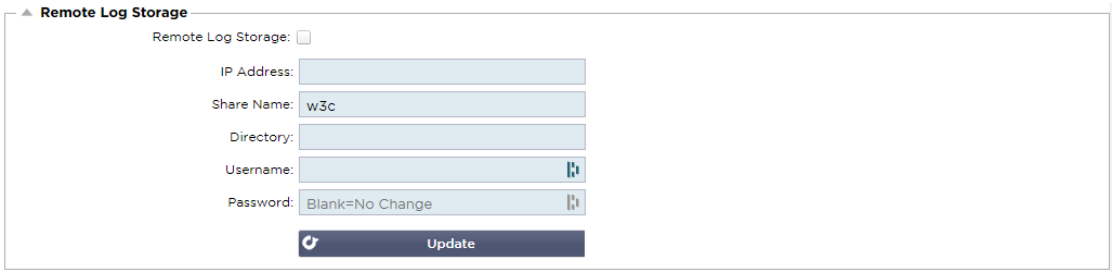
Удаленный сервер Syslog



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

- Добавьте IP-адрес вашего сервера Syslog
- Добавить порт
- Выберите TCP или UDP
- Поставьте галочку
- Нажмите Обновить

Удаленное хранение журналов



Все журналы W3C сохраняются в сжатом виде на ADC каждый час. Самые старые файлы будут удалены, когда на диске останется 30% свободного места. 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 виртуальной машины и до пяти часов в аппаратном устройстве.

Мы включим кнопку тестирования в будущие выпуски, чтобы обеспечить обратную связь, чтобы

Col1	Col2
Удаленное хранение журналов	Поставьте галочку, чтобы включить удаленное хранение журналов
IP-адрес	Укажите IP-адрес вашего сервера SMB. 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

убедиться, что ваши настройки верны.

Краткое описание месторождения

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, как можно лучше определить из сети или заголовка X-Forwarded-For
cs-username	Поле запроса имени пользователя клиента
s-ip	Порт прослушивания ALB
s-port	ALB прослушивание 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
ури	* краткий формат регистрирует комбинированный путь и запрос-строку
sc-status	Код ответа HTTP
cs(User-Agent)	Строка User-Agent браузера (отправленная 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
рсф	миллисекунда с момента подключения до получения первого байта ответа от реального сервера
rsl	миллисекунда с момента подключения до получения последнего байта ответа от сервера Real Server
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 привело к закрытию (или сохранению открытого) соединения
x-compress-action	Как осуществлялось или предотвращалось сжатие
x-sc(Content-Type)	Content-Type ответа
x-cache-action	Как реагировало или предотвращалось кэширование
x-finish	Триггер, вызвавший эту строку журнала

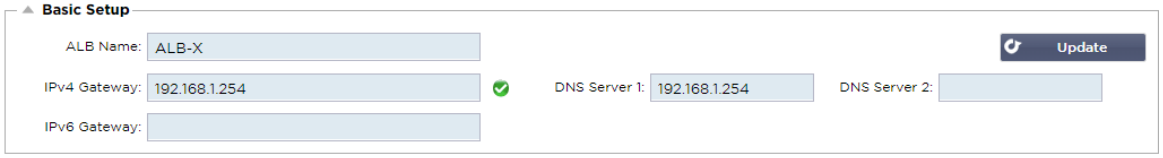
Очистить файлы журналов

Эта функция позволяет очистить файлы журналов с АЦП. В выпадающем меню можно выбрать тип журнала, который вы хотите удалить, а затем нажать кнопку Очистить.

Сеть

Раздел Network в библиотеке позволяет настроить сетевые интерфейсы АЦП и их поведение.

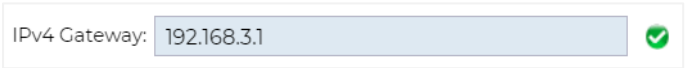
Базовая настройка



Название АЛБ

Укажите имя для 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 в нижней части страницы и белую галочку в зеленом круге рядом с IP-адресом.

Шлюз IPv6

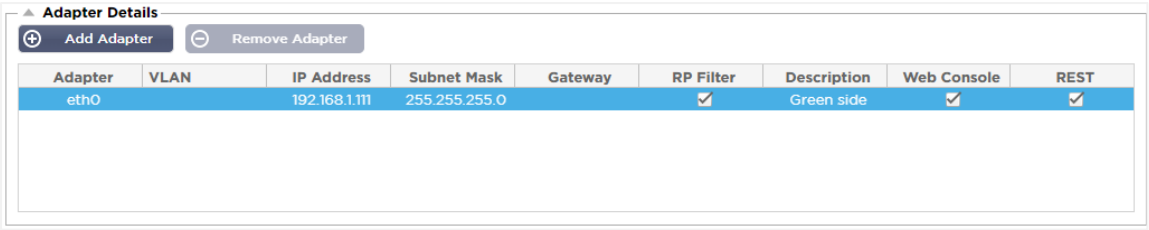
Укажите адрес шлюза IPv6. Этот адрес должен находиться в той же подсети, что и существующий адаптер. Если вы неправильно добавили шлюз, вы увидите белый крестик в красном круге. Когда вы добавите правильный шлюз, вы увидите зеленый баннер успеха в нижней части страницы и белую галочку в зеленом круге 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 отображаются сетевые интерфейсы, установленные в устройстве ADC. Вы можете добавлять и удалять адаптеры по мере необходимости.

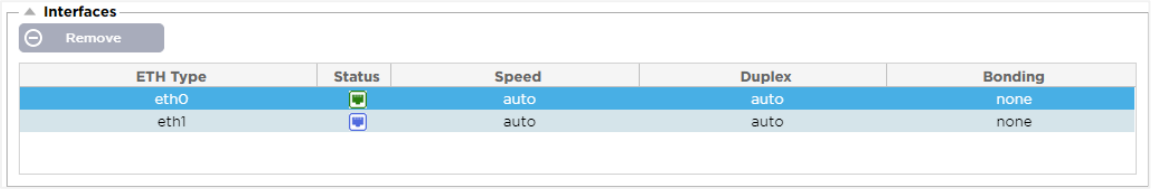


Колонка	Описание
Адаптер	В этом столбце отображаются физические адаптеры, установленные на вашем устройстве. Выберите адаптер из списка доступных адаптеров, щелкнув по нему - двойной щелчок переведет строку списка в режим редактирования.
VLAN	Дважды щелкните, чтобы добавить идентификатор VLAN для адаптера. 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 интерфейсу. Это должно быть 32-битное число IPv4 в четверичной 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	Добавить шлюз для интерфейса. После добавления этого параметра ADC настроит 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 общедоступного интерфейса. Примечание: АЦП автоматически присвоит первому интерфейсу имя Green Side, второму - Red Side, третьему - Side 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 интерфейс в качестве адреса управления для веб-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 получить доступ к веб-консоли после изменения. 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" панели "Сеть" позволяет настроить определенные элементы, относящиеся к сетевому интерфейсу. Вы также можете удалить сетевой интерфейс из списка, нажав кнопку Remove (Удалить). Если вы используете виртуальное устройство, 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 для автосогласования 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 Auto (по умолчанию), Full-Duplex и Half-Duplex.
Связывание	Вы можете выбрать один из определенных вами типов связывания. Более подробную информацию см. в разделе "Связывание".



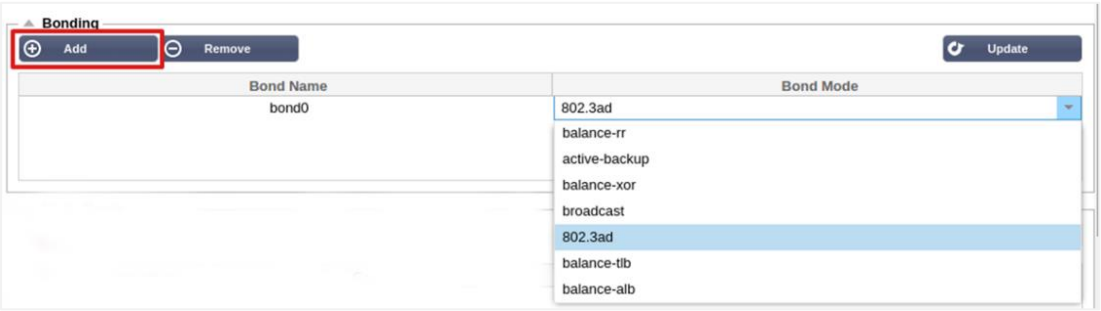
Связывание

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 и 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 можно определить режим работы и параметры мониторинга соединения. Существует семь различных режимов, каждый из которых обеспечивает определенные характеристики балансировки нагрузки и отказоустойчивости. Они показаны на рисунке ниже.

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

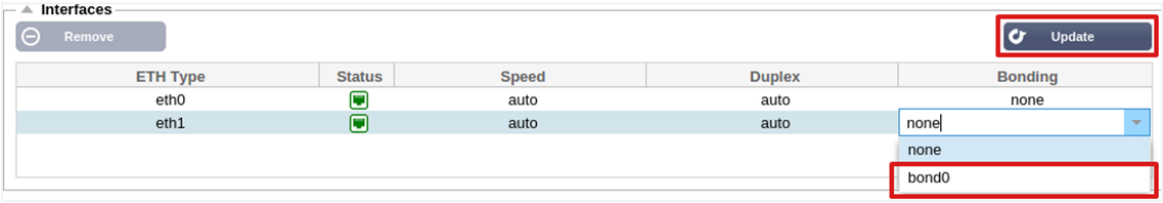


Создание профиля связывания

- Нажмите на кнопку Добавить, чтобы добавить новую облигацию
- Укажите имя для конфигурации связывания
- Выберите режим склеивания, который 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 самостоятельным интерфейсом управления.



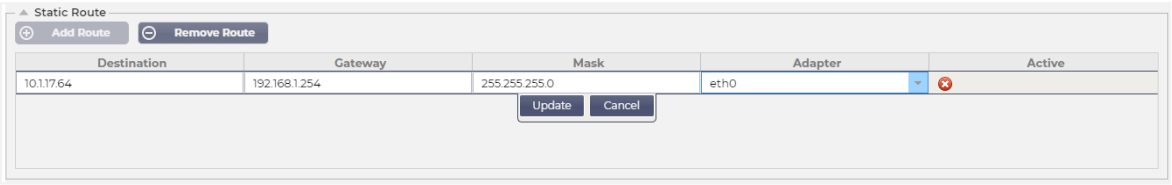
Режимы скрепления

Режим скрепления	Описание
баланс-рр:	Пакеты последовательно передаются/принимаются через каждый интерфейс по очереди.
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.
вещание:	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:	Адаптивный режим объединения каналов с балансировкой нагрузки при передаче: Обеспечивает объединение каналов, не требующее специальной поддержки коммутатора. Исходящий трафик распределяется в соответствии с текущей нагрузкой (вычисляемой 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.
баланс-альб:	Адаптивный режим балансировки нагрузки: также включает balance-tlb плюс балансировку принимаемой нагрузки (rlb) для трафика IPV4 и не требует специальной поддержки коммутатора. Балансировка нагрузки приема достигается путем ARP переговоров. Драйвер бондинга перехватывает ARP-ответы, отправляемые локальной системой, и перезаписывает аппаратный адрес источника уникальным аппаратным адресом одного из ведомых устройств в бондинге, таким образом, что разные пиры 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 Static Routes.



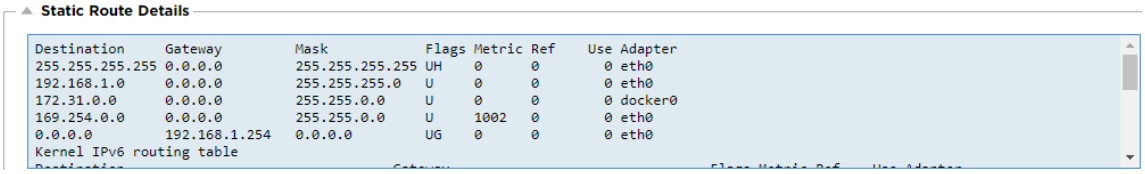
Добавление статического маршрута

- Нажмите кнопку Добавить маршрут
- Заполните поле, используя в качестве руководства данные, приведенные в таблице ниже.
- После завершения нажмите кнопку Обновить.

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 системе счисления. 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 означает, что шлюз недоступен 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

Отметьте этот флажок, чтобы включить настройку Server Nagle. Server Nagle - это средство повышения эффективности сетей TCP/IP за счет уменьшения количества пакетов, которые необходимо отправить 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

Установите флажок, чтобы включить настройку Client Nagle. Как указано 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 выглядит следующим образом.

В обычных условиях входящие запросы направляются на VIP, который видит IP-адрес источника запроса. 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 будет виден IP-адрес, указанный в правиле SNAT. SNAT можно использовать в режимах балансировки нагрузки 4-го и 7-го уровней.

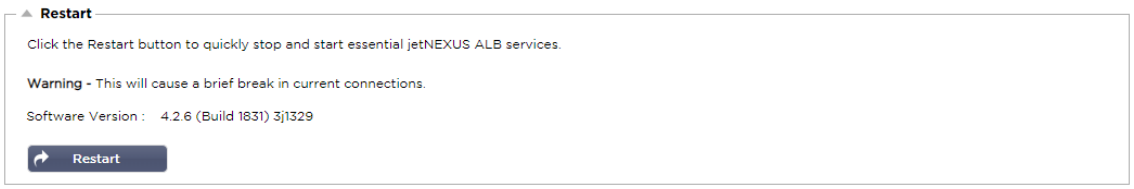
Поле	Описание
Источник IP	IP-адрес источника является необязательным, он может быть либо сетевым IP-адресом (с /mask), либо обычным IP-адресом. Маска может быть либо сетевой маской, либо обычным числом, указывающим количество единиц в левой части сетевой маски. Таким образом, маска /24 эквивалентна 255.255.255.0.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

Мощность

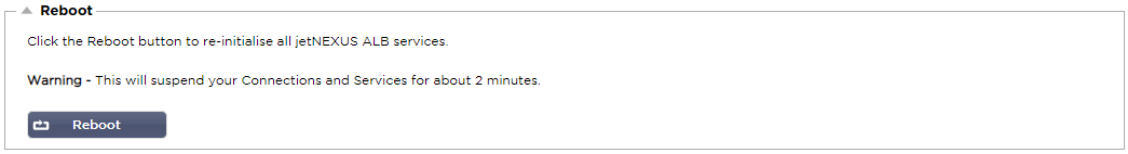
Эта функция системы АЦП также позволяет выполнять несколько задач, связанных с питанием АЦП.

Перезапустить



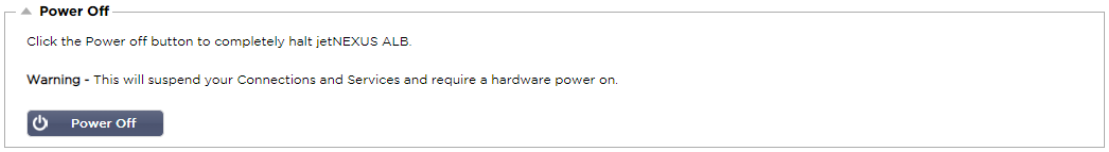
Эта настройка инициирует глобальный перезапуск всех Служб и, соответственно, разрывает все активные в данный момент соединения. Все Службы автоматически возобновят работу через некоторое время, но время будет зависеть от количества настроенных Служб. Появится всплывающее окно с запросом подтверждения перезапуска.

Перезагрузка



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

Выключение питания



Нажатие кнопки Power Off (Выключить) выключит АЦП. Если это аппаратное устройство, для его повторного включения потребуется физический доступ к устройству. Появится всплывающее окно с запросом подтверждения действия выключения.

Безопасность

Этот раздел позволяет 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.

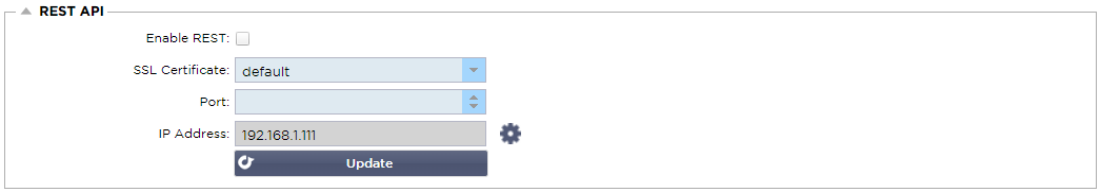
Веб-консоль

SSL-сертификат Выберите сертификат из раскрывающегося списка. Выбранный сертификат будет использоваться для защиты 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, представляет собой интерфейс 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	Отметьте этот флажок, 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 отобразится IP-адрес, к которому привязана служба REST. Вы можете щелкнуть ссылку Cog для доступа к странице Network (Сеть), чтобы изменить, на каком адаптере включена служба REST.
Зубчатое звено	Нажав на эту ссылку, вы перейдете на страницу Network, где можно настроить адаптер для REST.

Документация для REST API

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

Примечание: Если вы получите ошибки на странице Swagger, это связано с проблемой поддержки строк запроса.
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>"}'.
```

- вернётся

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

- Валидность
  - GUID действителен в течение 24 часов

Сведения о лицензии

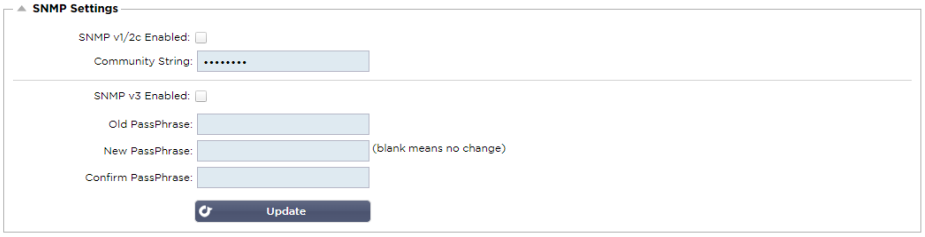
- Команда

```
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	Установите флажок, чтобы включить MIB V1/V2C. SNMP v1 соответствует RFC-1157. SNMP V2c соответствует RFC-1901-1908.
SNMP v3	Установите флажок, 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 включении 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 через SNMP, определяется базой управленческой информации (MIB). MIB описывают структуру данных управления и используют иерархические идентификаторы объектов (OID). Каждый OID может быть прочитан с помощью приложения управления SNMP.

Загрузка MIB

MIB можно загрузить **ЗДЕСЬ.**

ИДЕНТИФИКАТОР 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)

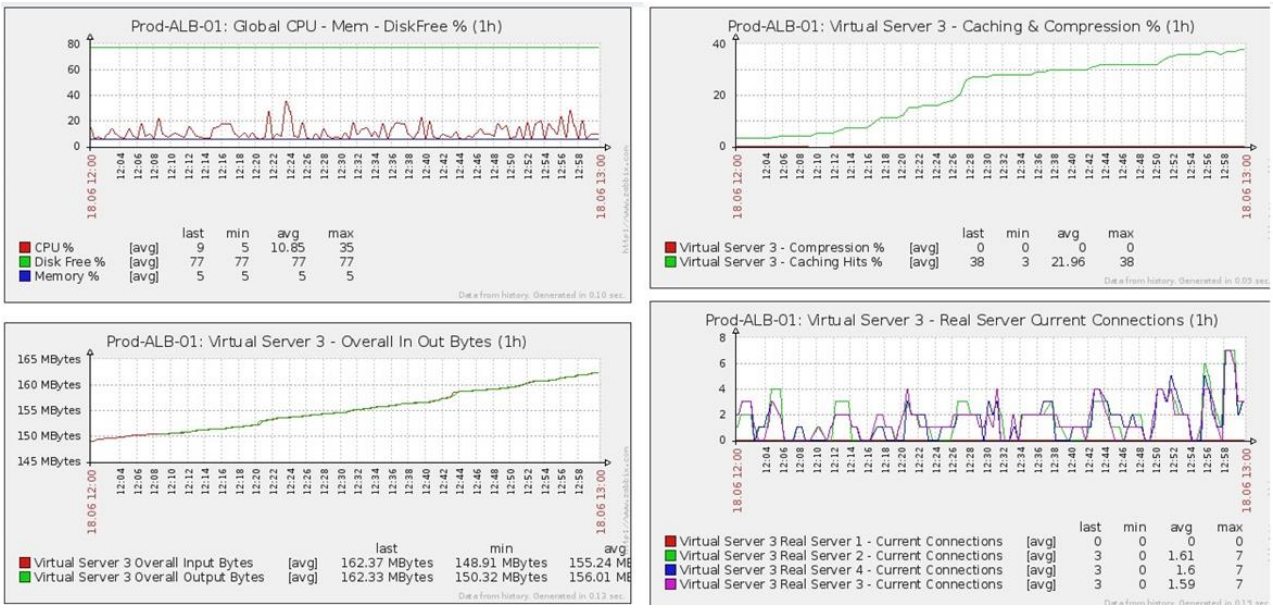
.9 **jetnexusMemoryPercent** (1.3.6.1.4.1.38370.1.1.9.0)
.10 **jetnexusCurrentConnections** (1.3.6.1.4.1.38370.1.1.10.0)

.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 ADC - 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.



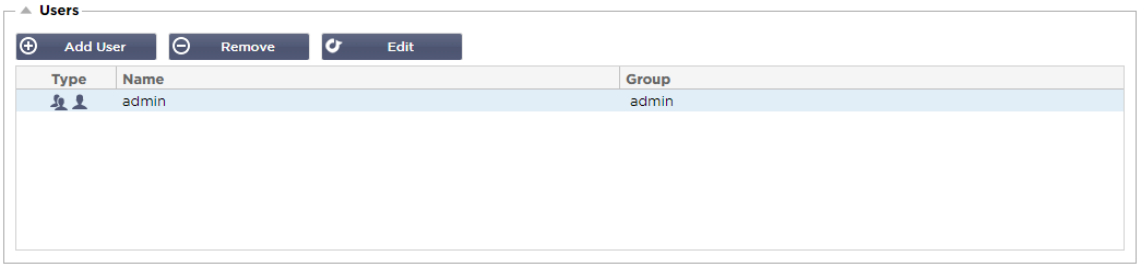
Пользователи и журналы аудита

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

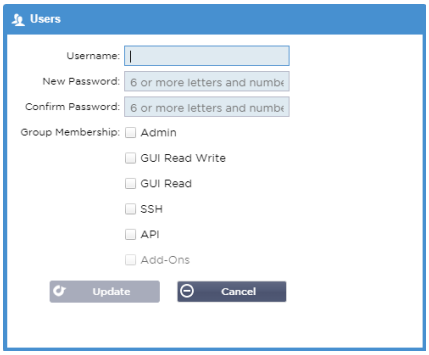
Существует пользователь по умолчанию под именем **admin**, которого вы используете при первой настройке ADC. Пароль по умолчанию для admin - **jetnexus**.

Пользователи

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



Добавить пользователя



Нажмите кнопку Добавить пользователя, показанную на изображении выше, чтобы вызвать диалоговое окно Добавить 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 прописными и строчными • Можно использовать цифры • Символы не допускаются
Пароль	Введите **надежный** пароль, соответствующий приведенным ниже требованиям • Минимальное количество символов 6 • Максимальное количество символов 32 • Должны использовать как минимум 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 этой группы 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 дает доступ к командной строке, которая имеет 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. В целях 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
Все 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 действителен

Удаление пользователя

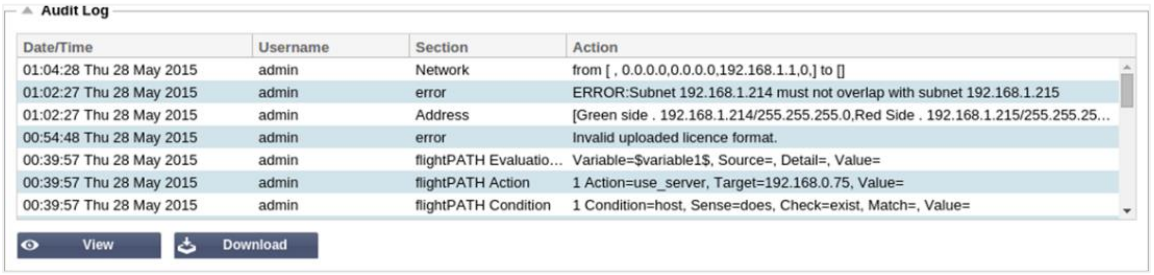
- Выделите существующего пользователя
- Нажмите Удалить
- Вы не сможете удалить пользователя, который в настоящее время входит в систему
- Вы не сможете удалить последнего локального пользователя в группе администраторов
- Вы не сможете удалить последнего оставшегося пользователя кластера в группе администраторов
- Вы не сможете удалить пользователя admin в целях 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, установив соответствующие флажки и обновив их.
- Вы также можете изменить пароль пользователя, если у вас есть права администратора

Журнал аудита

ADC регистрирует изменения, внесенные в конфигурацию ADC 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. Модуль Configuration можно использовать как для загрузки, так и для выгрузки конфигурации.

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

Файл конфигурации - это, по сути, текстовый файл, и поэтому он может быть отредактирован вами с помощью текстового редактора, например, 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 любым текстовым редактором, например, Notepad++.

Загрузка конфигурации

- Вы можете загрузить сохраненный файл конфигурации, найдя сохраненный файл .conf.
- Нажмите кнопку "Загрузить конфигурацию или Jetpack".
- АЦП загрузит и применит конфигурацию, а затем обновит браузер. Если браузер не обновится автоматически, нажмите кнопку обновить браузер.
- После завершения вы будете перенаправлены на страницу Dashboard.

Загрузить jetPACK

- JetPACK - это набор обновлений конфигурации к существующей конфигурации.
- JetPACK может быть как небольшой, например, изменение значения TCP Timeout, так и полная конфигурация 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 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 сбое реального сервера. Установка этого значения на ноль предотвращает 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, изящно завершать сеансы, чтобы их можно было перевести в автономный режим для обслуживания.

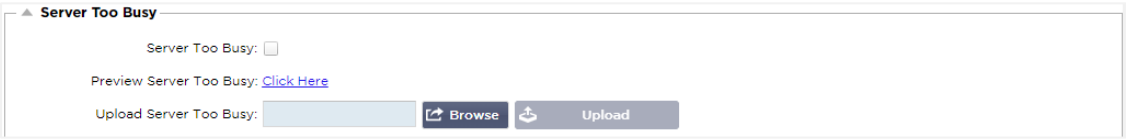
SSL

Этот глобальный параметр позволяет изменять библиотеку SSL по мере необходимости. По умолчанию криптографическая библиотека SSL, используемая ADC, принадлежит OpenSSL. Если вы хотите использовать другую криптографическую библиотеку, это можно изменить здесь.

Протокол

Раздел Протокол используется для настройки многих дополнительных параметров протокола HTTP.

Сервер слишком занят



Предположим, вы ограничили максимальное количество подключений к вашим реальным серверам; вы можете выбрать отображение дружественной веб-страницы после достижения этого предела.

- Создайте простую веб-страницу со своим сообщением. Вы можете включить внешние ссылки на объекты на других веб-серверах и сайтах. В качестве альтернативы, если вы хотите иметь изображения на вашей веб-странице, используйте встроенные изображения в кодировке base64
- Найдите файл HTM(L) вашей недавно созданной веб-страницы.
- Нажмите 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 определения 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 ADC, в заголовок Forwarded-For.
Добавить адрес	Этот выбор добавит IP-адрес устройства или клиента, подключенного к ADC, в заголовок Forwarded-For.
Заменить 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 указать имя, присвоенное заголовку Forwarded-For. Обычно это "X-Forwarded-For", но для некоторых сред оно может быть изменено.

Расширенная журнализация для IIS - Пользовательская журнализация

Информацию X-Forwarded-For можно получить, установив приложение IIS Advanced logging 64-bit. После загрузки создайте пользовательское поле регистрации под названием X-Forwarded-For с указанными 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:

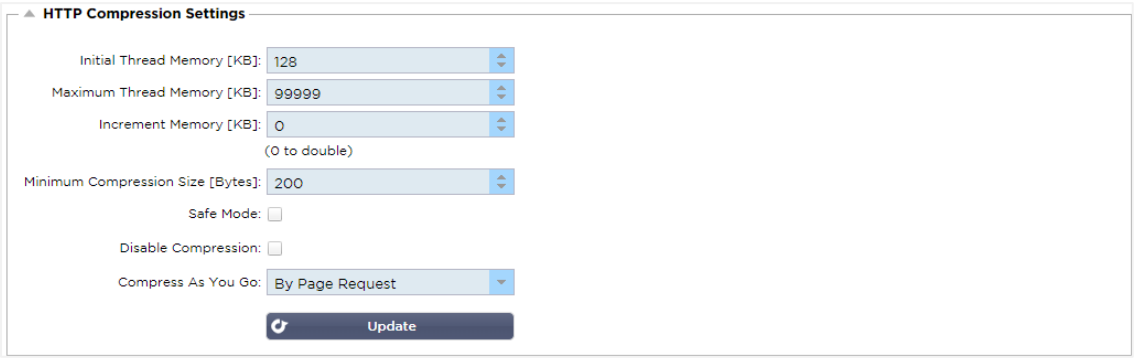
Тип	Значение
LogFormat:	"%h %l %u %t \"%r\" %>s %b \"%{Referer}i\" \"%{User-Agent}i\"" комбинированный
LogFormat:	"%{X-Forwarded-For}i %l %u %t \"%r\" %>s %b \"%{Referer}i\" \"%{User-Agent}i\"" proxy SetEnvIf X- Forwarded-For "^.*\..*\..*\..*\..*" forwarded
CustomLog:	"logs/access_log" combined env=!forwarded
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.
- В строке 2 поле %h (удаленный хост) заменяется значением (значениями), взятым из заголовка X-Forwarded-For, а имя этого шаблона файла журнала устанавливается 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.
- Также 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 возможности Apache по ведению журналов с поворотом (piped), но мы предполагаем, что почти все ее используют.

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

Настройки сжатия HTTP

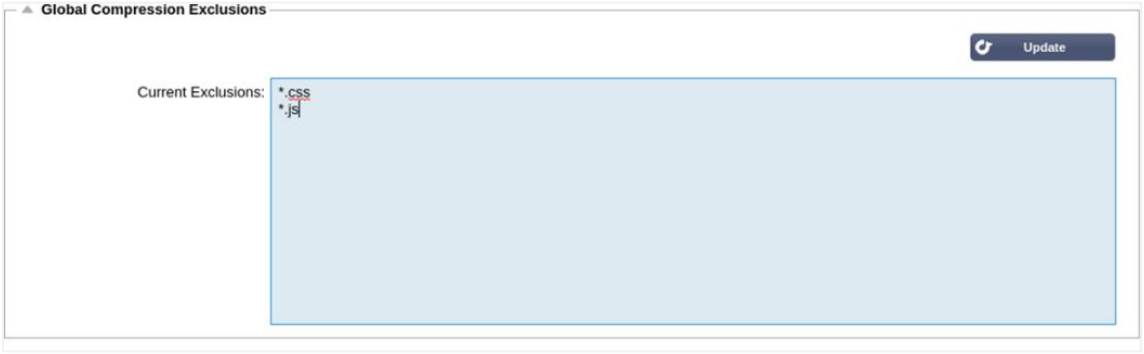


Сжатие является функцией ускорения и включается для каждой службы на странице IP-служб.

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

Вариант	**Описание**
Начальная память потока [KB]	Это значение - объем памяти, который может первоначально выделить ADC под каждый запрос. Для наиболее эффективной работы это значение должно быть установлено на величину, чуть превышающую самый большой несжатый HTML-файл, который могут отправить веб-серверы.
Максимальная память потока [KB]	Это значение - максимальный объем памяти, который АЦП выделит на один запрос. Для обеспечения максимальной производительности ADC 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 задает объем памяти, добавляемый к начальному распределению памяти потоков, когда требуется больше памяти. Значение по умолчанию равно нулю. Это означает, что ADC удвоит выделение памяти, когда данные превысят текущее выделение (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 одинаковый 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 приращение значительного размера (например, ответы размером от 2 Мб до 10 Мб, более эффективным будет начальное значение 1 Мб с приращением 1 Мб).
Минимальный размер сжатия [байты]	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 заключается в том, что хотя ADC знает, какие отдельные браузеры могут обрабатывать сжатое содержимое, некоторые другие прокси-серверы, даже если они заявляют о своей совместимости с HTTP/1.1, не могут корректно передавать сжатые таблицы стилей и JavaScript. Если возникают проблемы с таблицами стилей или JavaScript через прокси-сервер, используйте эту опцию, чтобы отключить сжатие этих типов. Однако это уменьшит общую степень сжатия содержимого.
Отключить сжатие	Поставьте галочку, чтобы запретить ADC сжимать любой ответ.
Компресс по мере выполнения	ON - Используйте Compress as You Go на этой странице. При этом каждый блок данных, полученных от сервера, сжимается в дискретный фрагмент, 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



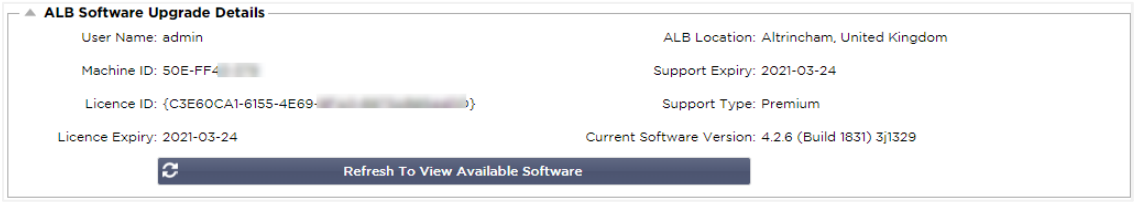
Все страницы с добавленным расширением в списке исключений не будут сжиматься.

- Введите имя индивидуального файла.
- Нажмите кнопку обновить.
- Если вы хотите добавить тип файла, просто введите "*.css", чтобы исключить все каскадные таблицы стилей.
- Каждый файл или тип файла должен быть добавлен с новой строки.

Программное обеспечение

Раздел "Программное обеспечение" позволяет обновить конфигурацию и микропрограмму вашего АЦП.

Сведения об обновлении программного обеспечения



Информация в этом разделе будет заполнена, если у вас есть рабочее подключение к Интернету. Если ваш браузер не имеет 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

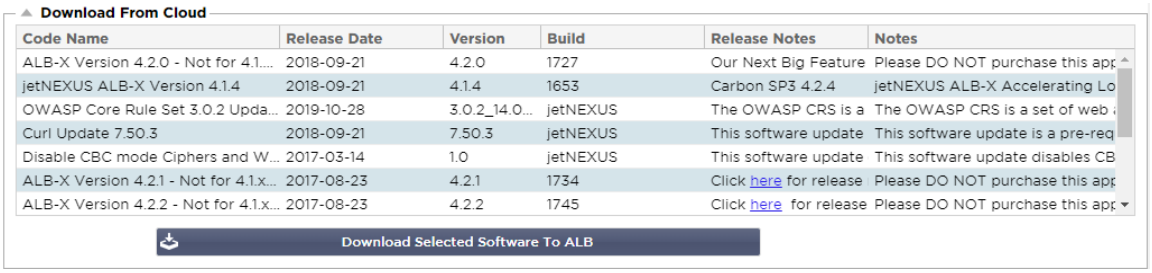
В разделе "Загрузить из облака", показанном ниже, будет отображаться информация об обновлениях, доступных вам в рамках вашего плана поддержки. Вам следует обратить внимание на Тип поддержки и Срок действия поддержки.

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

Загрузить из облака



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

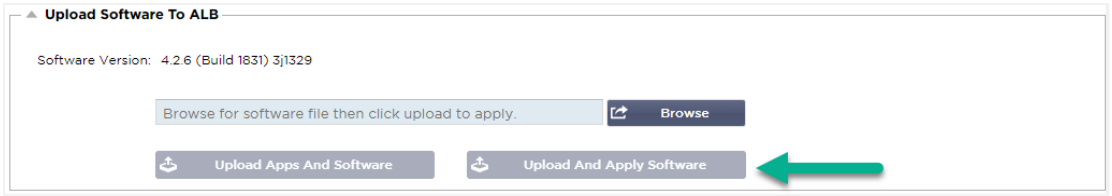
- Выделите интересующую вас строку и нажмите кнопку "Загрузить выбранное программное обеспечение в ALB. " кнопку
- При нажатии выбранное программное обеспечение загрузится на ваш ALB, которое можно применить в разделе "Применить программное обеспечение, хранящееся на ALB" ниже.

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

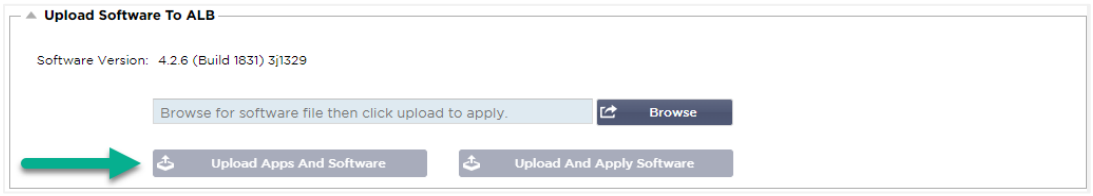
Загрузка приложений



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

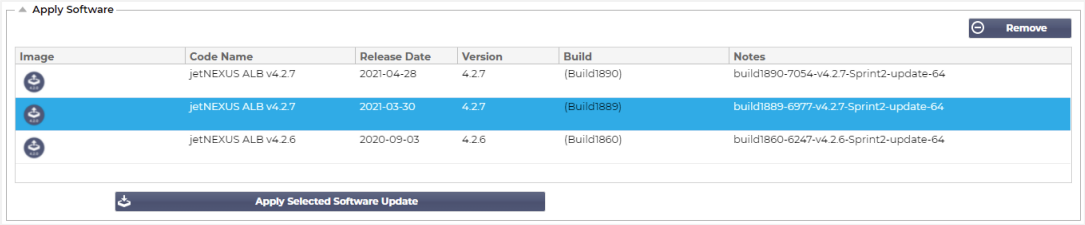
- Существует пять типов приложений
  - <имя приложения>flightpath.alb
  - <имя приложения>.monitor.alb
  - <имя приложения>.jetpack.alb
  - <имя приложения>.addons.alb
  - <имя приложения>.featurepack.alb
- После загрузки каждое приложение можно найти в разделе Библиотека> Приложения.
- Затем вы должны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

Программное обеспечение



- Если вы хотите загрузить программное обеспечение без его применения, воспользуйтесь выделенной кнопкой.
- 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.

Применить 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, имейте в виду, что оно будет загружено, а затем перезагружено ALB для применения.
- Если применяемое обновление является обновлением сигнатуры OWASP, оно будет применено автоматически без перезагрузки.

Устранение неполадок

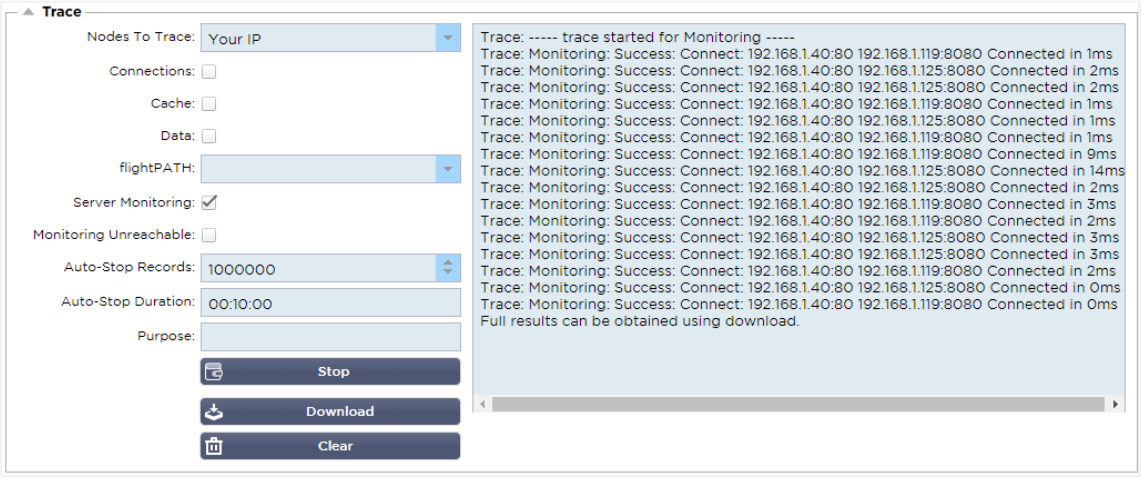
Всегда есть проблемы, которые требуют поиска неисправностей для выявления первопричины и решения. Данный раздел позволяет это сделать.

Файлы поддержки

Если у вас возникла проблема с ADC и вам необходимо открыть заявку на поддержку, 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
- Поднять 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



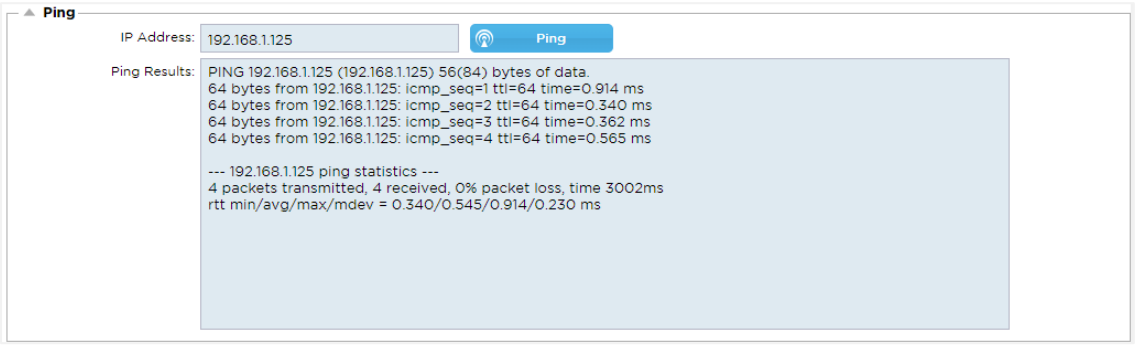
Раздел "Трассировка" позволяет изучить информацию, позволяющую отладить проблему. Предоставляемая информация зависит от опций, которые вы выбираете из выпадающих и отмеченных галочками полей.

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	При установке этого флажка будет отображаться информация о кэшированных объектах.
Данные	Когда этот флажок установлен, в него будут включены необработанные байты данных, обрабатываемые АЦП на входе и выходе.
flightPATH	Меню flightPATH позволяет 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 недоступности	Этот флажок аналогичен вышеуказанному, за исключением того, что он будет показывать только сбойные мониторы и, таким образом, действует как фильтр только для этих сообщений.
Записи автостопа	Значение по умолчанию составляет 1 000 000 записей, после чего функция Trace автоматически останавливается. Это мера предосторожности, чтобы предотвратить случайное включение функции Trace и влияние на работу АЦП.
Продолжительность автостопа	По умолчанию установлено время 10 минут, после чего функция Trace автоматически останавливается. Это мера предосторожности для предотвращения случайного оставления

	функции Trace включенной и влияния на работу АЦП.
Начало	Нажмите, чтобы вручную запустить средство трассировки.
Остановить	Нажмите, чтобы вручную остановить объект Trace 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. Вы можете загрузить Trace.log, чтобы просмотреть всю информацию, собранную во время различных трасс в тот день. По сути, это 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	Очистка журнала 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. После нажатия кнопки "Ping" может потребоваться подождать несколько секунд для получения результата.

Если вы настроили DNS-сервер, то можно ввести полное доменное имя. Настроить DNS-сервер можно в разделе **DNS Server 1 & DNS Server 2**. После нажатия кнопки "Ping" может потребоваться подождать несколько секунд для получения результата.

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".

- Поднять тикет на портале поддержки, подробная информация о котором приведена в конце данного документа.
- Обязательно подробно опишите проблему и прикрепите файл к билету.
- Вы также можете просмотреть содержимое с помощью Wireshark

Вариант	Описание
Адаптер	Выберите свой адаптер из выпадающего списка, обычно 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. Обычное время составляет 15 секунд для сайтов с высокой посещаемостью. Графический интерфейс пользователя 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.

Что такое jetPACK

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

Загрузка пакета jetPACK

- Каждый из представленных ниже jetPACK 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 с помощью Notepad++.
- Нажмите на ссылку jetPACK ниже и сохраните ссылку как файл jetPACK-VIP-Application.txt в выбранном вами месте

Microsoft Exchange

Приложение	Ссылка на скачивание	Что он делает?	Что входит в комплект?
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, 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, 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 виртуальной службы: 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 наименьшего количества CPU. Можно добавить несколько проверок состояния VIP, чтобы проверить работоспособность каждой из отдельных служб.	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 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	Передний край	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-сервисы

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 - разгрузка SSL	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 ввод пароля 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,** 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 - добавляет возможность выбора "Сильных шифров" из списка опций шифров:
    - Шифр = ALL:RC4+RSA:+RC4:+HIGH:!DES-CBC3-SHA:!SSLv2:!ADH:!EXP:!ADHexport:!MD5

- Anti-Beast - добавляет возможность выбрать "Anti Beast" из списка опций шифра:
  - Шифр = ECDHE-RSA-AES128-SHA256:AES128-GCM-SHA256:RC4:HIGH:!MD5:!aNULL:!EDH
- No SSLv3 - добавляет 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 - Добавляет 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 - Добавляет возможность выбора "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 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 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
- Загрузка новой конфигурации или jetPACK
- Искать jetPACK
- Нажмите Загрузить
- Как только экран браузера станет белым, нажмите кнопку 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-то приложения и хотите использовать ее для нескольких других коробок независимо друг от друга.

- Начните с копирования текущей конфигурации из существующего 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".
- Сохранить 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.

Секция 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 подробности 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]
```

В этом разделе содержатся 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="Принудительно использовать 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].
Подробно=
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 можно использовать в области действий.
Действие	Поведение после срабатывания правила.

Что может сделать flightPATH?

flightPATH можно использовать для изменения входящего и исходящего содержимого HTTP(s) 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).

Более подробную информацию о RegEx можно найти на этом полезном сайте https://www.regexbuddy.com/regex.html.

Кроме того, в области **действий** можно создавать и использовать пользовательские переменные, что дает множество различных возможностей.

Состояние

Состояние	Описание	Пример
<форма>	HTML-формы используются для передачи данных на сервер	Пример "форма не имеет длины 0".
Местонахождение ГЭП	Это сравнивает IP-адрес источника 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 со списком языков
Метод	Это выпадающий список методов HTTP	Это выпадающий список, который включает GET, POST и т.д.
Происхождение IP	Если восходящий прокси	IP-адрес клиента. Можно также

	поддерживает X-Forwarded-for (XFF), он будет использовать истинный адрес происхождения.	использовать несколько IP-адресов 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	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 куки	Это имя файла cookie, запрашиваемого клиентом	MS-WSMAN=afYfn1CDqqCDqUD::
Заголовок запроса	Это может быть любой HTTP-заголовок	Referrer, User-Agent, From, Date
Версия для запросов	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 другой агрегированный IP-адрес	ClientIP , Proxy IP, Firewall IP. Можно также использовать несколько IP и подсетей. Точки следует исключить, 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 данный	Диапазон приема: байты

	сервер	
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, используемой 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-куки, ранее отправленные сервером с помощью Set-Cookie (см. ниже).	Cookie: $Version=1; Skin=new;
Дата	Дата и время получения сообщения	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 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 нижестоящим прокси-серверам, как сопоставить заголовки будущих запросов, чтобы решить, можно ли использовать кэшированный ответ вместо того, чтобы запрашивать новый	Vary: User-Agent

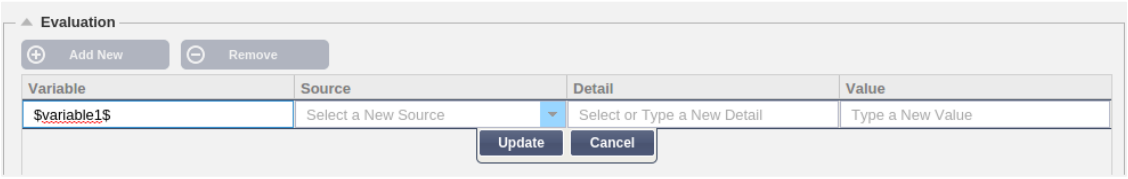
	ответ у исходного сервера.	
X-Powered-By	Указывает технологию (например, ASP.NET, PHP, JBoss), поддерживающую веб-приложение	X-Powered-By: PHP/5.4.0

Проверьте	**Описание**	**Пример**
Существовать	Здесь не важна детальность условия, только то, что оно существует/не существует	Хозяин - существует
Начало	Строка начинается со значения	Путь - Does - Start - /secure
Конец	Строка заканчивается значением	Путь - Делает - Конец - .jpg
Содержать	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 для выполнения действия
- Первое - 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, если это необходимо. Если Source=Request Header, то Details 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 оценочную запись.
- В своем действии вы можете использовать любую из перечисленных ниже переменных
- 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, обычно 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

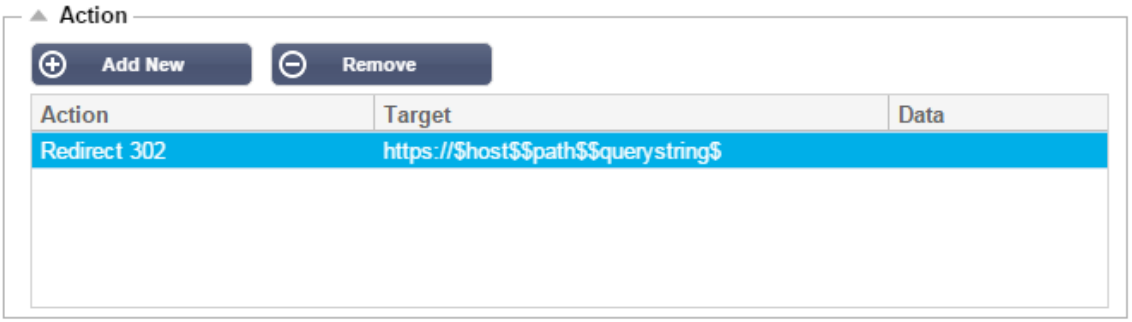
Элемент запроса	Это имя и значение запроса. Как таковой он может принимать либо имя запроса, либо значение.	"Best=jetNEXUS", где соответствие - Best, а значение - edgeNEXUS
Строка запроса	Это вся строка после символа ?	HTTP://server/path/program?query_string
Заголовок запроса	Это может быть любой заголовок, 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 данный сервер	Диапазон приема: байты
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, используемой 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-куки, ранее отправленные 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	If-Modified-Since: Sat, 29 Oct 1994 19:43:31 GMT

	изменилось	
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	Указывает 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

Действие

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



Действие

Дважды щелкните по столбцу Действие для просмотра выпадающего списка.

Цель

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

Вы также можете набирать текст вручную с помощью некоторых действий.

Данные

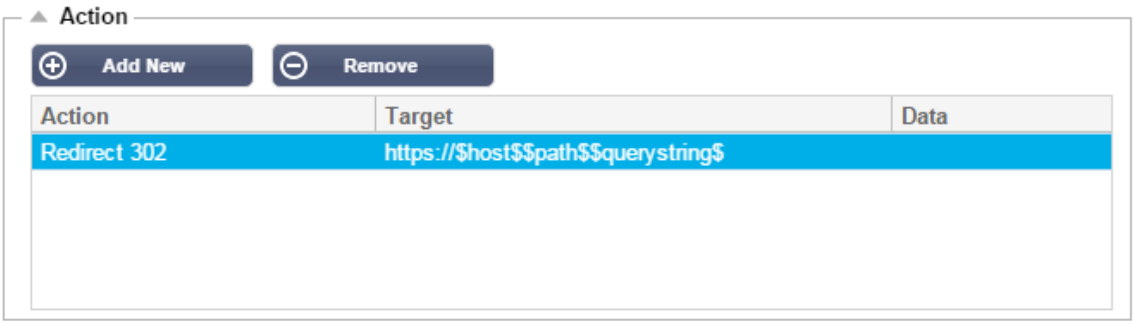
Дважды щелкните по столбцу "Данные", чтобы вручную добавить данные, которые вы хотите добавить или заменить.

Список всех действий подробно описан ниже:

Действие	**Описание**	**Пример**
Cookie для добавления запроса	Добавьте файл cookie запроса, подробно описанный в разделе Target, со значением в разделе Data	Цель = Печенье Данные= MS-WSMAN=afYfn1CDqqCDqCVii
Добавить заголовок запроса	Добавьте заголовок запроса типа Target со значением в разделе Data	Цель = Принять Data= image/png
Добавить ответный файл cookie	Добавьте куки-файлы ответа, подробно описанные в разделе "Цель", со значением в разделе "Данные".	Цель = Печенье Данные= MS-WSMAN=afYfn1CDqqCDqCVii
Добавить заголовок ответа	Добавьте заголовок запроса, подробный в разделе Target, со значением в разделе Data	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 кузова в первую очередь	Поиск тела ответа и замена только первого экземпляра	Target= HTTP:// (Строка поиска) Data= HTTPs:// (Заменяемая строка)
Замена корпуса Последняя	Поиск тела ответа и замена только последнего экземпляра	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. В качестве адреса или сообщения можно использовать переменную	target="flightPATH отправил сообщение об этом событии" Данные = Н/Д
Событие журнала	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 приведет к временному перенаправлению	Target= HTTP://www.edgenexus.ioData= N/A
Удалить файл	Удалить cookie запроса, подробно	Цель = Печенье

cookie с запросом	описанные в разделе "Цель	Данные= MS-WSMAN=afYfn1CDqqCDqCVii
Удалить заголовок запроса	Удалите заголовок запроса, подробно описанный в разделе "Цель	Target=ServerData=N/A
Удалить куки-файл ответа	Удаление ответных cookie-файлов, подробно описанных в разделе "Цель	Target=jnAccel
Удалить заголовок ответа	Удалите заголовок ответа, подробно описанный в разделе "Цель	Target= Etag Данные = Н/Д
Заменить файл cookie запроса	Замените cookie запроса, указанные в разделе "Цель", на значение в разделе "Данные".	Цель = Печенье Данные= MS-WSMAN=afYfn1CDqqCDqCVii
Заменить заголовок запроса	Замените заголовок запроса в Цели значением данных	Цель = Соединение Data= keep-alive
Заменить ответный файл cookie	Замените cookie-файл ответа, указанный в разделе Target, на значение в разделе Data	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
Использовать сервер	Выберите, какой сервер или виртуальную службу использовать	Цель= 192.168.101:80Данные= N/A
Зашифровать куки	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 защищенную виртуальную службу HTTPS. Оно будет использовать те же имя хоста, путь и строку запроса, что и запрос.

Общее использование

Брандмауэр и безопасность приложений

- Блокировка нежелательных IP-адресов
- Принуждение пользователя к HTTPS для определенного (или всего) содержимого
- Блокировать или перенаправлять пауков
- Предотвращение и предупреждение межсайтовых сценариев
- Предотвращение и предупреждение SQL-инъекций
- Скрыть внутреннюю структуру каталогов
- Перезапись файлов cookie
- Защищенный каталог для определенных пользователей

Характеристики

- Перенаправление пользователей на основе пути
- Обеспечение единой регистрации в нескольких системах
- Сегментировать пользователей на основе идентификатора пользователя или Cookie
- Добавьте заголовки для разгрузки SSL
- Определение языка
- Переписать запрос пользователя
- Исправьте неработающие URL-адреса
- Регистрация 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
- Чувствует = Делает
- Проверка = Соответствие RegEx
- Значение = \.htm$

Оценка:

- Пустой

Действия:

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

Index.html

Принудительное использование index.html в запросах к папкам.

Условие: это условие является общим условием, которое подходит для большинства объектов

- Условие = Хозяин
- Чувствует = Делает
- 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 подходит для большинства 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 подходит для большинства объектов

- Условие = Хозяин
- Чувствует = Делает
- Проверка = Соответствие RegEX
- Значение = \.cgi$

Оценка:

- Пустой

Действия:

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

Бревно-паук

Журнал запросов пауков популярных поисковых систем.

Условие: это условие является общим условием, которое подходит для большинства объектов

- Условие = Заголовок запроса
- Соответствие = User-Agent
- Чувствует = Делает
- 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 определенного каталога. В этом случае, если клиент обращается к чему-либо, содержащему каталог /secure/, то он будет перенаправлен на HTTPs версию запрашиваемого URL.

Состояние:

- Условие = Путь
- Чувствует = Делает
- 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
- Чувствует = Делает
- Проверка = Конец
- Значение = .flv

Оценка:

- Пустой

Действия:

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

Замена HTTP на HTTPS

Измените любой жесткий код HTTP:// на HTTPS://.

Состояние:

- Условие = Код ответа
- Чувствует = Делает
- 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
- Чувствует = Делает
- 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

Истечение срока действия 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
- Чувствует = Делает
- 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 другой.

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

- Условие = Код ответа
- Чувствует = Делает
- 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
- Чувствует = Делает
- 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
- Чувствует = Делает
- 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
- Чувствует = Делает
- 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

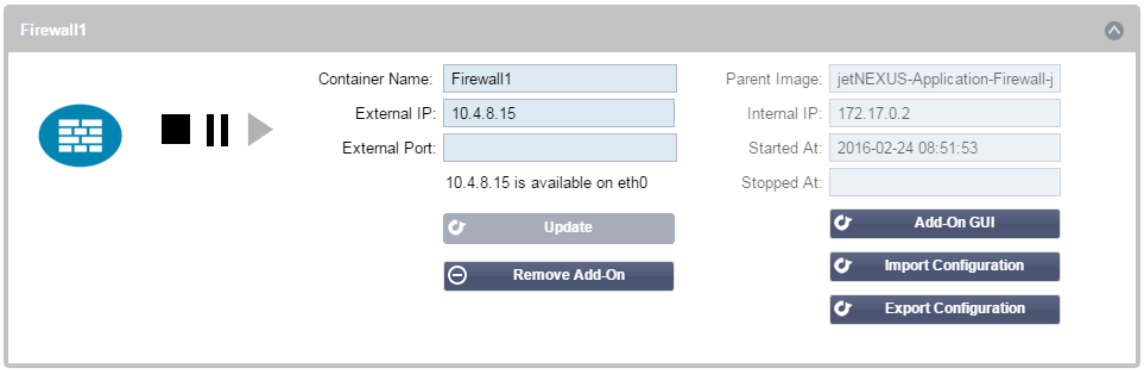
- Действие = Заменить заголовок запроса
- Цель = Хозяин
- Данные =ipv4.host.header

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.

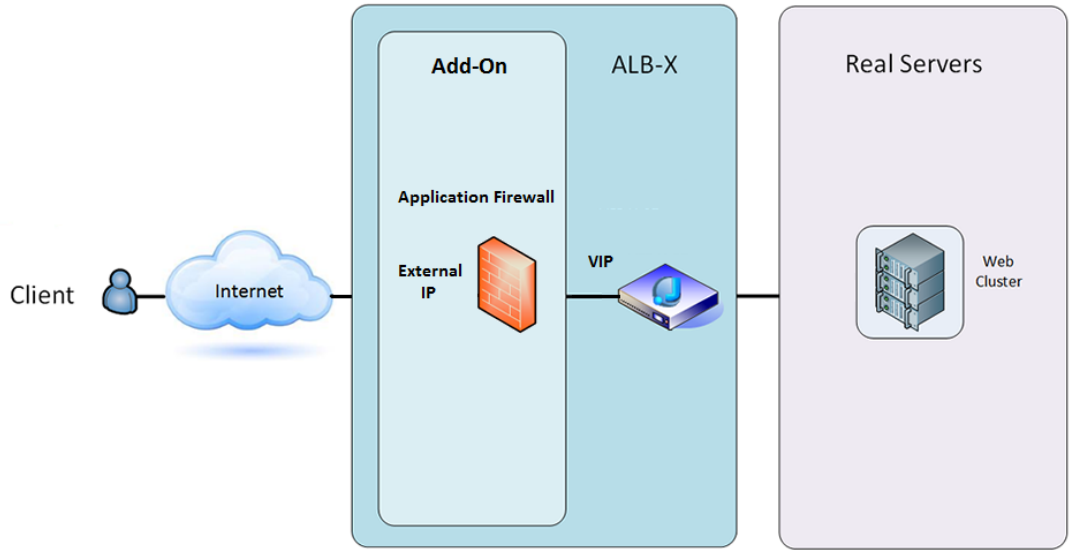


Вариант	Описание
Остановить	Она будет серой, пока не будет запущен экземпляр Add-On. Нажмите эту кнопку, чтобы остановить экземпляр Docker.
Пауза	Эта кнопка приостанавливает работу надстройки.
Играть	Это приведет к запуску надстройки с текущими настройками.
Название контейнера	Дайте своему контейнеру имя, чтобы идентифицировать его среди других контейнеров. Оно должно быть уникальным. Вы можете использовать его в качестве имени для реального сервера, если хотите, и оно будет автоматически разрешаться во внутренний IP-адрес экземпляра.
Внешний IP	Здесь вы можете задать внешний IP-адрес для доступа к вашей надстройке. Это может быть доступ к графическому интерфейсу надстройки, а также к службе, которая работает через надстройку. В случае с Firewall Add-On это IP-адрес вашей службы HTTP. 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 на ваш брандмауэр. Чтобы ограничить его, 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 External Port пустым, либо добавьте порт 88 для доступа к GUI, если вы ограничиваете список портов.
Обновление	Вы можете обновить настройки надстройки только после ее остановки. После остановки экземпляра вы можете изменить имя контейнера, внешний IP и внешний порт.
Удалить надстройку	Полностью удалит дополнение со страницы Дополнения. Вам нужно будет перейти на страницу Library-Apps, чтобы снова развернуть дополнение.
Родительский	Указывает образ Docker, из которого собрана надстройка. Может

образ	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, поэтому его нельзя редактировать. Если вы остановите экземпляр Docker и перезапустите его, будет выдан новый внутренний IP-адрес. По этой причине вы должны либо использовать внешний IP-адрес для вашей службы, либо использовать имя контейнера для реального адреса сервера вашей службы.
Начал в	Здесь будет указана дата и время запуска дополнения. Пример 2016-02-16 155721
Остановился на	Здесь будет указана дата и время остановки надстройки. Пример 2016-02-24 095839

Пример архитектуры

WAF с использованием внешнего IP-адреса

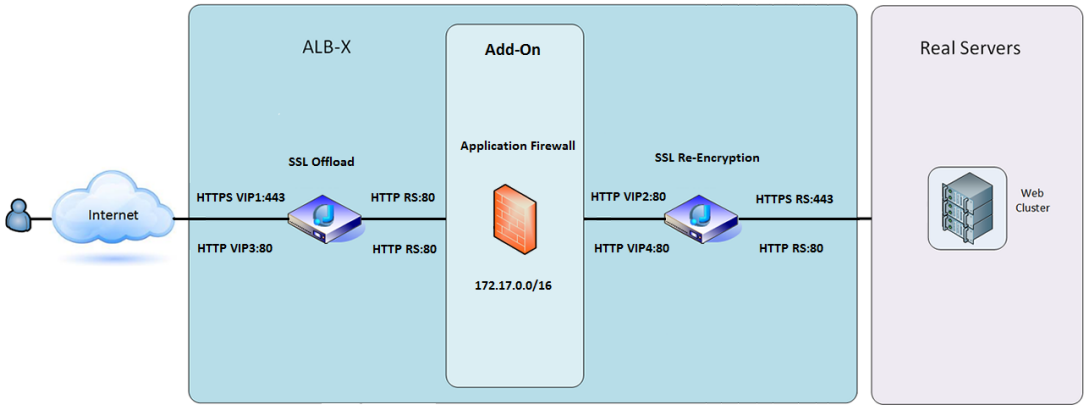


В этой архитектуре для вашего сервиса можно использовать только HTTP, поскольку брандмауэр не может проверять HTTPS-трафик.

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

ALB-X VIP, в свою очередь, будет настроен на балансировку нагрузки трафика для вашего веб-кластера.

WAF использует внутренний IP-адрес



В этой архитектуре можно указать HTTP и HTTPS.

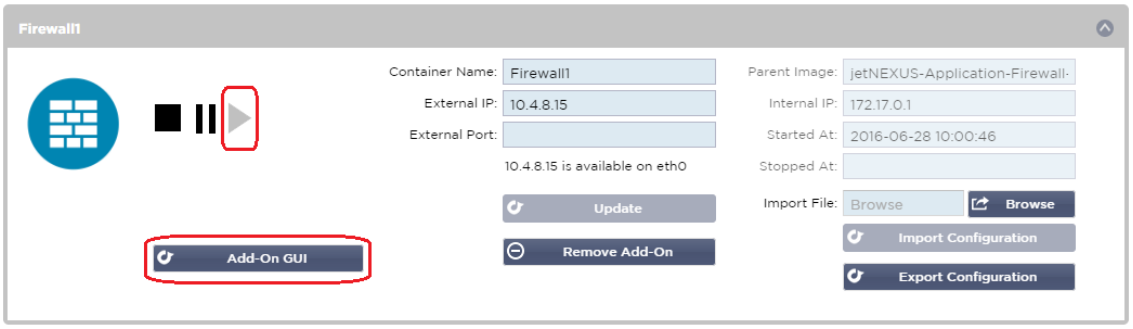
HTTPS может быть сквозным, когда шифруются соединения от клиента к ALB-X и от ALB-X к реальным серверам.

Трафик с ALB-X на внутренний IP-адрес брандмауэра должен быть незашифрованным, чтобы его можно было проверить.

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

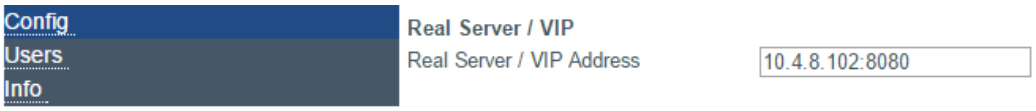
Доступ к вашему дополнению WAF

- Заполните данные для вашего брандмауэра
- Вы можете ограничить порты только тем, что вам нужно, или оставить его пустым, чтобы разрешить все порты.
- Нажмите кнопку Воспроизведение
- Появится кнопка графического интерфейса дополнений

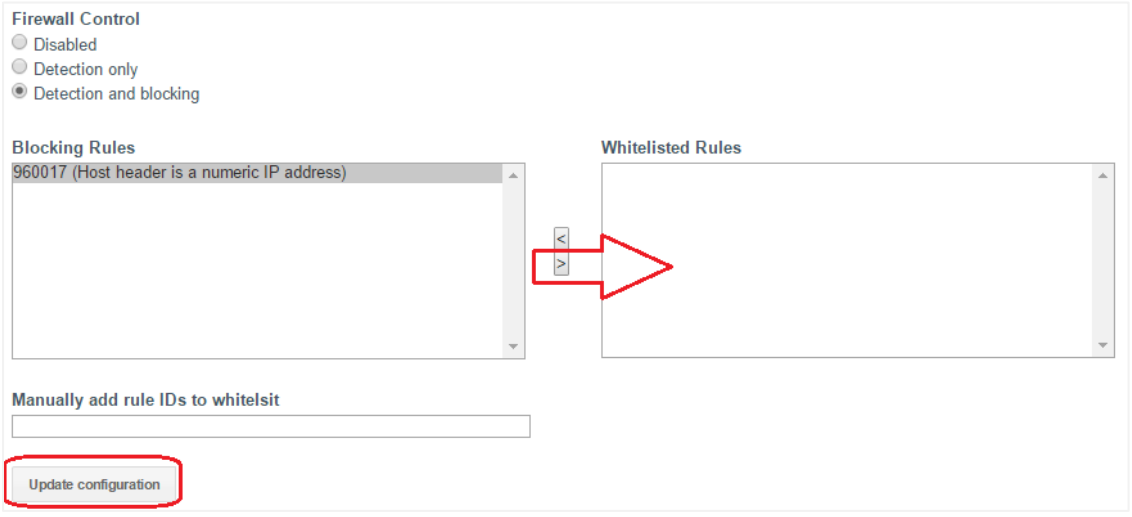


- Нажмите на эту кнопку, и откроется браузер на HTTP://[внешний IP]:88/waf
- В данном примере это будет HTTP://10.4.8.15:88/waf
- Перед вами появится диалоговое окно входа в систему.
- Введите учетные данные для вашего ADC.
- После успешного входа в систему перед вами откроется главная страница WAF.

- На главной странице отображается графический обзор событий, т.е. действий по фильтрации, выполняемых брандмауэром приложений.
- При первом открытии страницы графики, скорее всего, будут пустыми, так как не будет попыток доступа через брандмауэр.
- Вы можете настроить IP-адрес или доменное имя веб-сайта, на который будет отправляться трафик после фильтрации брандмауэром.
- Это можно изменить в разделе Управление > Конфигурация



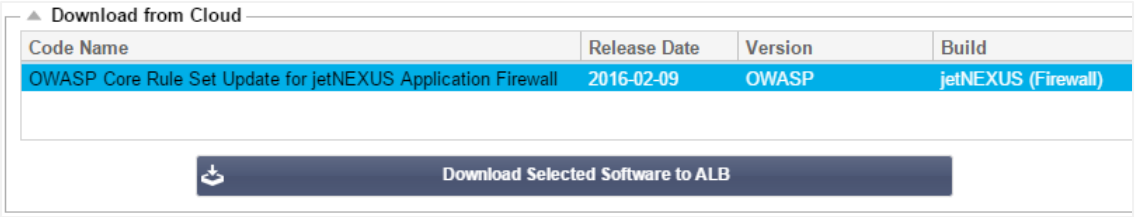
- Брандмауэр проверит трафик и затем отправит его на реальный IP-адрес сервера или VIP-адрес, указанный здесь. Вы также можете ввести порт вместе с IP-адресом. Если вы введете IP-адрес сам по себе, порт будет считаться портом 80. Нажмите кнопку "Обновить конфигурацию", чтобы сохранить новые настройки.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



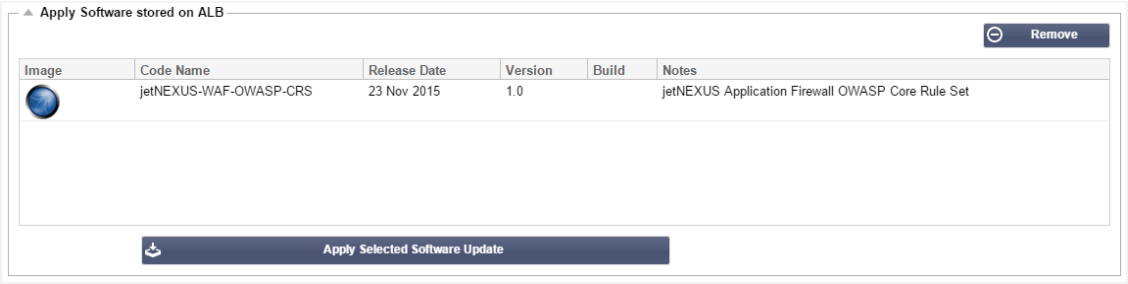
- Нажмите кнопку Обновить конфигурацию, когда вы перенесете все правила из раздела Блокировка в раздел Белый список.

Обновление правил

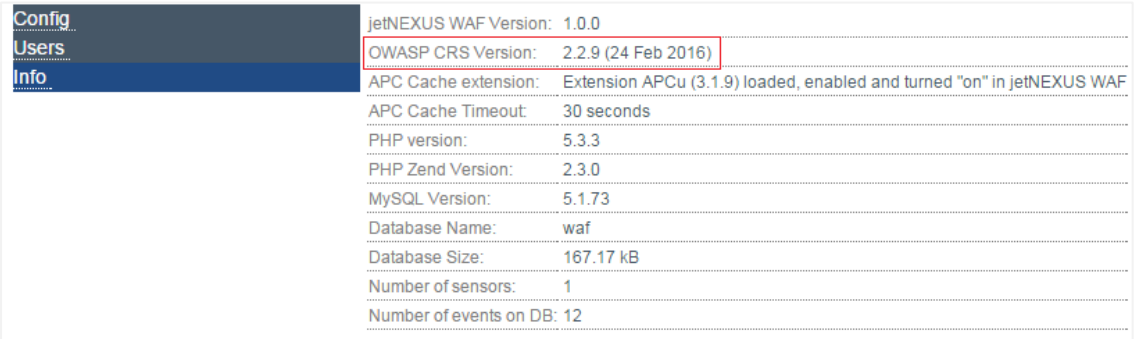
- Правила брандмауэра приложений можно обновить, зайдя в раздел Дополнительно - Программное обеспечение
- Нажмите кнопку Обновить для просмотра доступного программного обеспечения в разделе Сведения об обновлении программного обеспечения
- Теперь отображается дополнительное поле под названием Загрузить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



- Если это так, вы можете выделить и нажать Загрузить выбранное программное обеспечение в ALB-X
- В результате этого действия смарт-файл будет загружен 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, включенных в белый список, 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 версию OWASP CRS в разделе "Информация об управлении" в графическом интерфейсе брандмауэра.



Глобальная балансировка нагрузки сервера (edgeGSLB)

Введение

Глобальная балансировка нагрузки серверов (GSLB) - это термин, используемый для описания методов распределения сетевого трафика в Интернете. GSLB отличается от балансировки нагрузки серверов (SLB) или балансировки нагрузки приложений (ALB), поскольку обычно используется для распределения трафика между несколькими центрами обработки данных, в то время 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 использовать их в ситуации Active-Passive, 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 точек 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 сложной; 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.
- Nameserver: это сервер имен, к которому изначально подключается клиент для выполнения разрешения DNS.
- Авторитетные серверы имен: Включают серверы имен домена верхнего уровня (TLD) и корневые серверы имен.

Типичная транзакция DNS описана ниже:

- Пользователь набирает в веб-браузере 'example.com', запрос отправляется в Интернет и принимается рекурсивным резольвером DNS.
- Затем преобразователь 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 на преобразователь с сервера имен.
- Затем DNS-резольвер отвечает веб-браузеру IP-адресом первоначально запрошенного домена.
- После того как восемь этапов поиска DNS вернут 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 останавливаем и отключаем DNS-клиент Windows в разделе служб 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 время жизни (TTL), т.е. время кэширования ответа.

Обзор GSLB

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

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

Это возможно в нескольких вариантах. В первом случае 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 тем самым падение веб-сайта.

Конфигурация GSLB

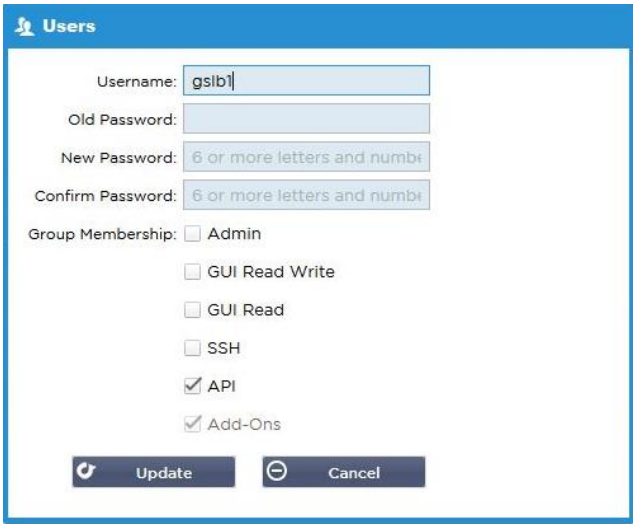
После загрузки GSLB Add-On, пожалуйста, разверните его, посетив страницу Library > Apps в графическом интерфейсе ADC и нажав кнопку "Deploy", как показано ниже.

После установки, пожалуйста, настройте данные 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 просматривать реальный IP-адрес клиента.
- Внешние порты - это список TCP и UDP портов GSLB, к которым можно получить доступ с 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 надстройки нажмите кнопку Обновить.
- Запустите GSLB Add-On, нажав кнопку Run.

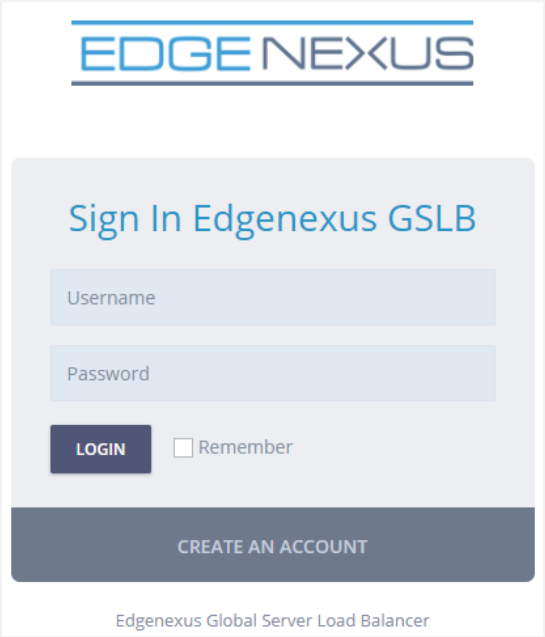
- Следующим шагом будет разрешение edgeNEXUS GSLB Add-On на чтение и изменение конфигурации АЦП.
- Посетите страницу System > Users (Система > Пользователи) графического интерфейса ADC GUI и отредактируйте пользователя с тем же именем, что и GSLB Add-On, который вы развернули, как показано на рисунке ниже.

- Отредактируйте пользователя "gslb1" и отметьте API, затем нажмите Обновить - в более поздних версиях программного обеспечения галочка может быть уже установлена по умолчанию.



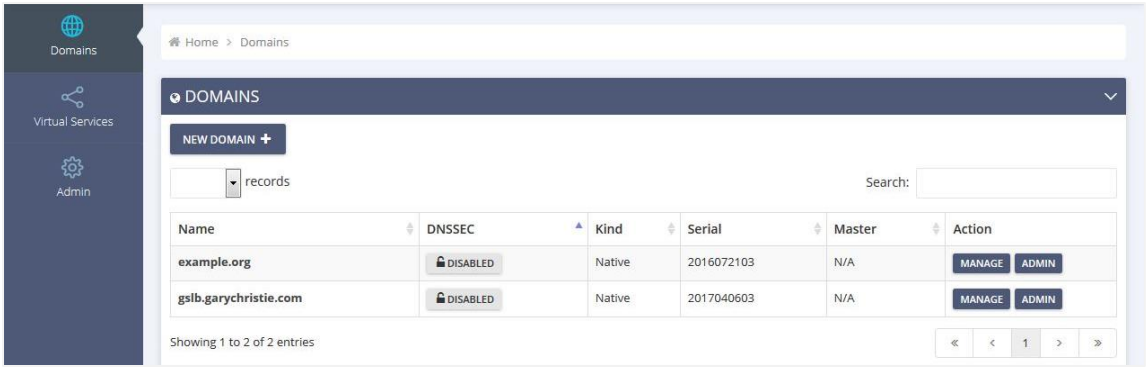
- Следующий шаг необходим только в том случае, если вы настраиваете GSLB для тестирования или оценки и не хотите изменять данные зон DNS в Интернете.
- В этом случае, пожалуйста, проинструктируйте ADC использовать GSLB Add-On в качестве основного сервера разрешения DNS, изменив "DNS Server 1" на странице 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.

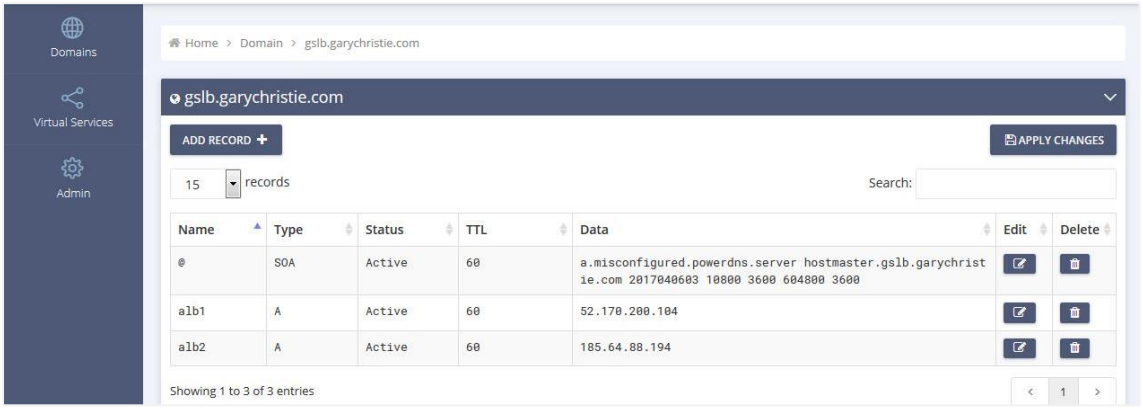


- Имя пользователя по умолчанию - admin, а пароль по умолчанию - jetnexus. Пожалуйста, не забудьте изменить пароль на странице Администратор > Мой профиль в графическом интерфейсе GSLB.
- Следующим шагом в последовательности настройки является создание зоны DNS в сервере имен PowerDNS, который является 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 POWERDNS NAMESERVER**. Пример зоны показан на рисунке 6.

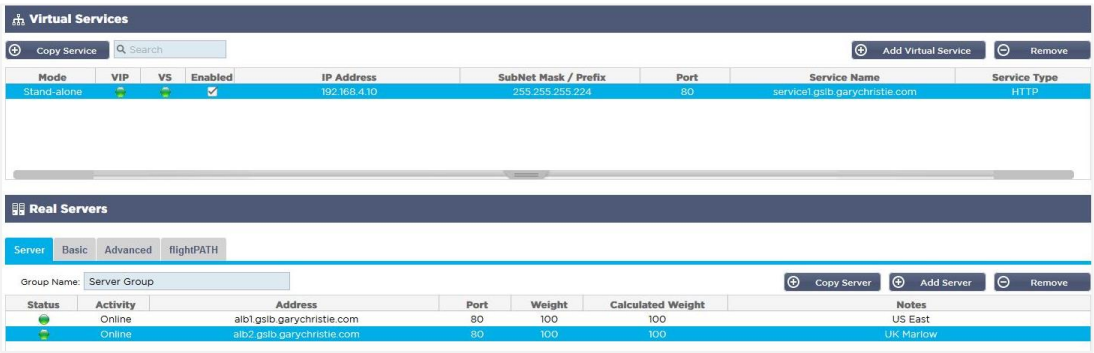
* edgeNEXUS GSLB GUI основан на проекте с открытым исходным кодом PowerDNS-Admin.



- После создания зоны DNS нажмите кнопку Manage (Управление) и добавьте имена хостов в домен, как показано на рисунке ниже.
- После редактирования существующих записей в графическом интерфейсе GSLB нажмите кнопку Сохранить.
- После завершения создания записей имен хостов 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.

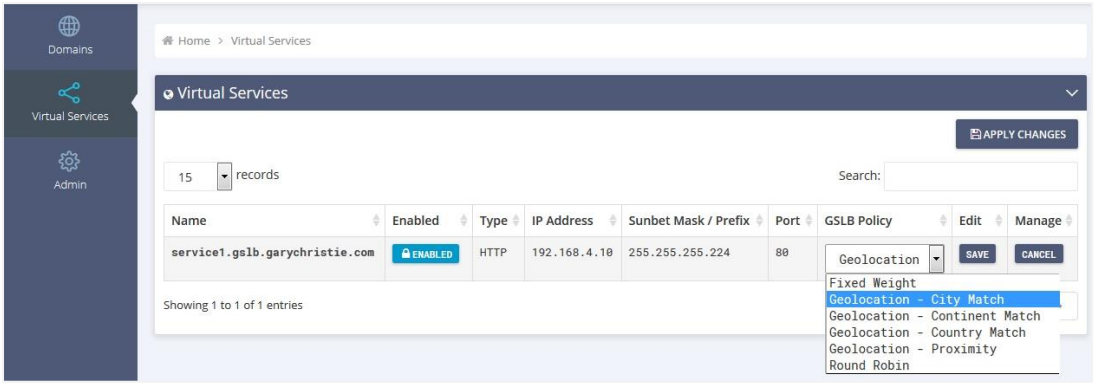


- Теперь давайте вернемся к графическому интерфейсу ADC и определим виртуальную службу, соответствующую только что созданной зоне DNS.



- Виртуальная служба будет использоваться для проверки работоспособности серверов в домене GSLB.
- GSLB использует механизм проверки работоспособности ADC, включая пользовательские мониторы. Его можно использовать с любым из типов служб, 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 Virtual Services в графическом интерфейсе GSLB.
- Добавьте все серверы в домене GSLB в раздел Real Servers на изображении выше.
- 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 состояния 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.
- Подробную информацию о настройке **ВИРТУАЛЬНЫХ СЛУЖБ** см. в разделе **ВИРТУАЛЬНЫЕ СЛУЖБЫ.**
- Теперь 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.



- ГСЛБ 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 выбирает один из них случайным образом.
Взвешенная круговая тренировка	Выбирайте серверы по одному, подряд. Серверы с большим весом выбираются чаще, чем серверы с меньшим весом.
Геолокация	Близость - выбор сервера, 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	City match - выбор сервера 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	Country match - 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	Совпадение континентов - выбор сервера на том же континенте, что и клиент. Если нет сервера на том же континенте, выберите ближайший.

- После того как вы выбрали политику GSLB, не забудьте нажать кнопку Применить изменения.
- Теперь вы можете просмотреть и настроить детали виртуальной услуги, нажав 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, предоставляемые **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".

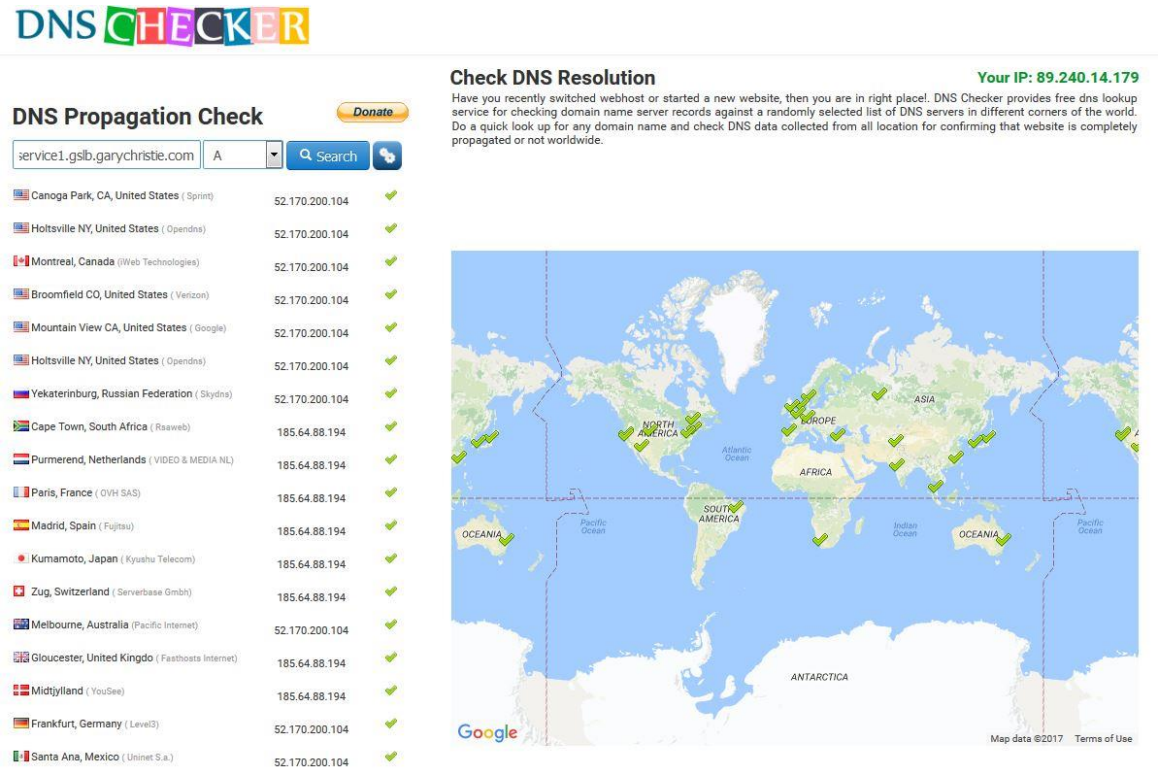
- Отличный способ проверить, какие ответы GSLB будет отправлять клиентам, - использовать NSLOOKUP.
- Если вы используете Windows, команда приведена ниже.

  NSLOOKUP service1.gslb.garychristie.com 192.168.4.10

- Где service1.gslb.garychristie.com - доменное имя, которое вы хотите разрешить.
- Где 192.168.4.10 - внешний IP-адрес вашего GSLB.
- Чтобы проверить, какой IP-адрес будет выдаваться в интернете, можно воспользоваться DNS-сервером 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.
- Пример результатов смотрите ниже.



Пользовательские местоположения

Частные сети

GSLB также можно настроить на использование пользовательских местоположений, чтобы 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 для внутренних частных адресов, соответствующих RFC 1918 для адресов IPv4 и RFC 4193 для адресов IPv6, такой базы данных не существует.

Обратитесь к странице Википедии, объясняющей частную адресацию
HTTPS://EN.WIKIPEDIA.ORG/WIKI/PRIVATE_NETWORK

Как это работает

Обычно идея использования нашей GSLB для внутренних сетей заключается в том, чтобы пользователи с определенных адресов получали разные ответы для службы в зависимости от того, в какой сети они находятся. Итак, рассмотрим два центра обработки данных, Северный и Южный, предоставляющие услугу под названием north.service1.gslb.com и south.service1.gslb.com, соответственно. Когда пользователь из северного центра данных запрашивает GSLB, мы хотим, чтобы GSLB ответил IP-адресом, связанным с north.service1.gslb.com, при условии, что служба работает правильно. В противном случае, если пользователь из южного центра данных обращается к GSLB, мы хотим, чтобы GSLB ответила 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 центра обработки данных
- Назначьте различные частные сети на эти места
- Назначьте каждую услугу на соответствующее место

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. В этом упражнении мы будем считать, что IP-адреса службы и клиента находятся в одной частной сети.
  - 10.1.1.0/24
- Добавить код континента
  - ЕС
- Добавьте код страны
  - ВЕЛИКОБРИТАНИЯ
- Добавить город
  - Энфилд
- Добавить широту - получено из Google
  - 51.6523

- Добавьте долготу - полученную 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
- Добавить код континента
    - ЕС
- Добавьте код страны
    - ВЕЛИКОБРИТАНИЯ
- Добавить город
    - Кройдон
- Добавить широту - получено из Google
    - 51.3762
- Добавьте долготу - полученную из google
    - 0.0982

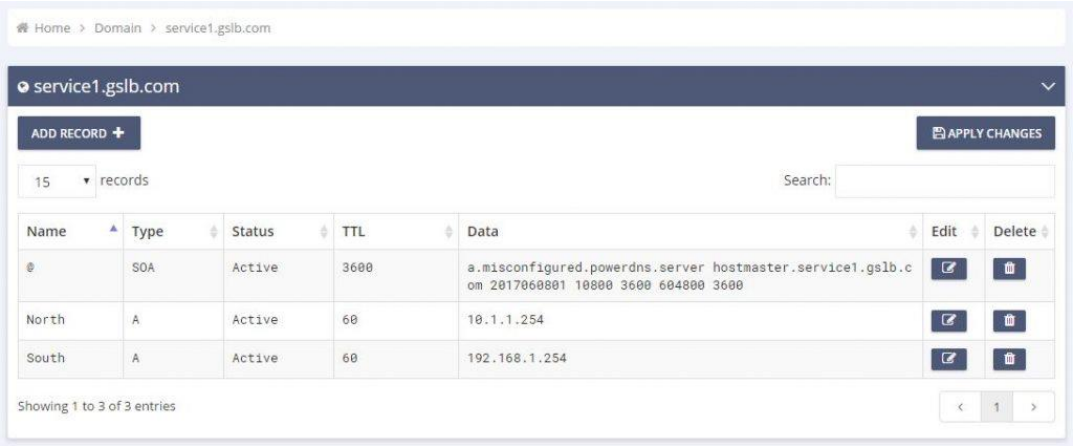
Обратите внимание, пожалуйста, используйте правильный код, который можно получить **ЗДЕСЬ**

Добавить запись A для north.service1.gslb.com

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

Добавить запись A для south.service1.gslb.com

- Нажмите на домен service1.gslb.com
- Нажмите Добавить запись
- Добавить имя
  - Юг
- Тип
  - A
- Статус
  - Активный
- TTL
  - 1 минута
- IP-адрес
  - 192.168.1.254 (Обратите внимание, что эта сеть находится в той же сети, что и местоположение Croydon)



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, так как 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 действующий контракт на поддержку и обслуживание edgeADC, edgeWAF или edgeGSLB.

Чтобы подать заявку в службу поддержки, посетите сайт:

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