EdgeADC

Руководство по администрированию EdgeADC

ВЕРСИЯ ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ

5.0.0

Содержание

Свойства документа

Номер документа:2 .0.3.19.25.12.03

Дата создания документа:19 March 2025

Последнее редактирование документа: 19 March 2025

Автор документа: Джей Савур

Документ Последний раз редактировался:

Документ: EdgeADC - версия 5.0.0

Отказ от документов

Скриншоты и графика в данном руководстве могут незначительно отличаться от вашего продукта из-за различий в выпуске продукта. Edgenexus прилагает все разумные усилия для обеспечения полноты и точности информации в этом документе. Edgenexus не несет ответственности за любые ошибки. Edgenexus внесет изменения и исправления в информацию, содержащуюся в этом документе, в будущих выпусках, когда возникнет такая необходимость.

Авторские права

Товарные знаки

Поддержка Edgenexus

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

Введение

Вы читаете это руководство, потому что собираетесь развернуть Edgenexus EdgeADC и эффективно и экономично сбалансировать нагрузку для серверных приложений.

EdgeADC построен на базе высокозащищенного механизма, который обеспечивает высокую масштабируемость, безопасность, высокую производительность и очень простой в использовании интерфейс управления. Эти факторы гарантируют, что развернутая вами система обеспечит наилучшую стоимость владения.

Цель этого документа

Этот документ написан для того, чтобы вы могли управлять EdgeADC с помощью удобного веб-интерфейса. Функции и их конфигурации описаны подробно, и мы надеемся, что этого будет достаточно, чтобы вы смогли настроить EdgeADC в соответствии с вашими требованиями.

Для кого предназначен этот документ?

Этот документ предназначен для людей, обладающих знаниями в области сетевых технологий, в частности протоколов, приложений и серверов.

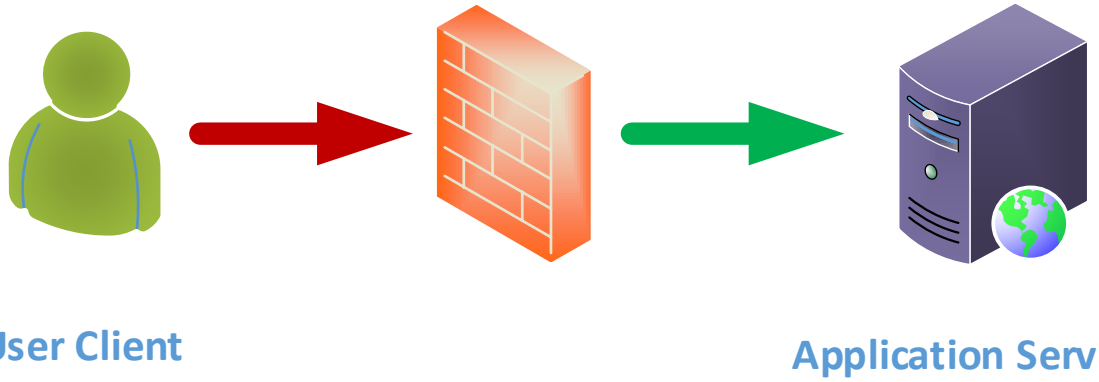
Балансировка нагрузки 101

Что такое балансировщик нагрузки или ADC?

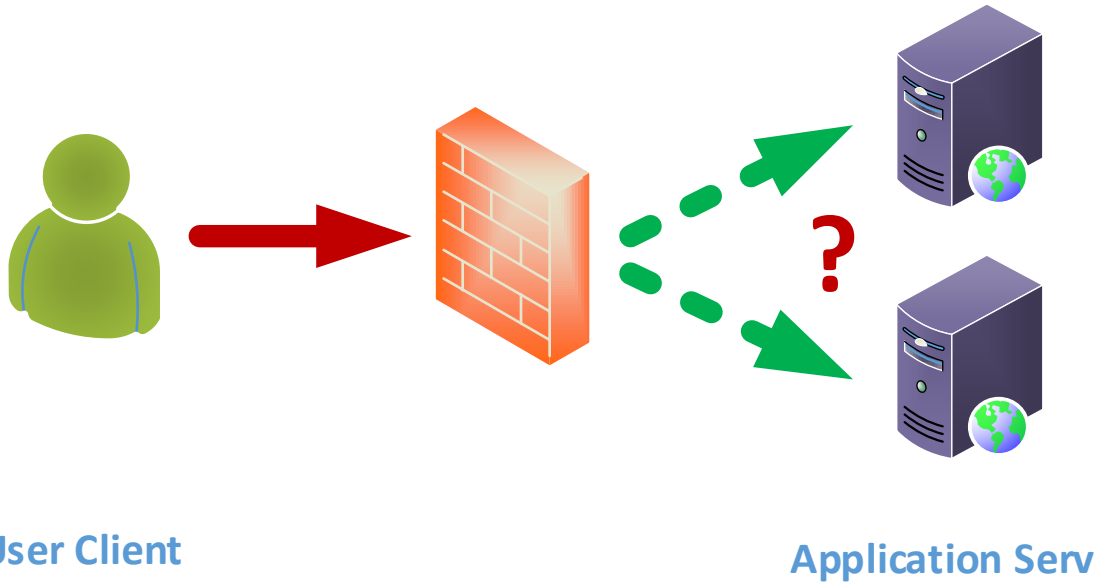
Балансировщики нагрузки претерпели значительную эволюцию и имеют гораздо больше интеллектуальных возможностей, чем раньше. Сегодня их часто называют контроллерами доставки приложений или ADC.

Прежде чем понять, что такое балансировщик нагрузки или ADC, необходимо разобраться в проблемах ИТ-специалиста и пользователя. Итак, давайте рассмотрим пример.

- У компании есть веб-приложение, которое она публикует в Интернете. Приложение размещено на одном веб-сервере, а данные хранятся на отдельном сервере баз данных.



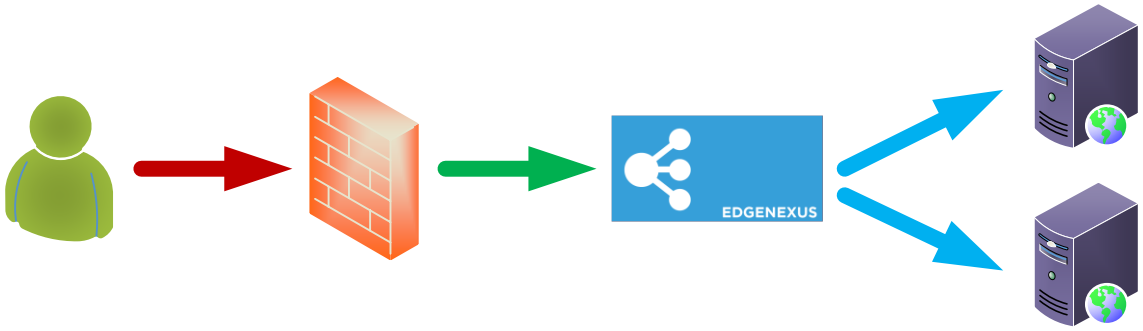
- В качестве примера этот сервер использует IP-адрес 1.2.3.4.
- Количество клиентов, обращающихся к приложению, постоянно растет, и некоторые отмечают, что производительность приложения снижается.
- Анализ работы сервера показывает, что трафик на нем сильно возрос и продолжает расти.
- Поэтому было принято решение добавить еще один сервер для размещения приложения.
- Новый второй сервер использует IP-адрес 1.2.3.5.
- Проблема заключается в том, как направить клиента на новый и текущий сервер, чтобы разделить нагрузку и обеспечить сохранение сеанса пользователя на первом вошедшем в систему сервере.



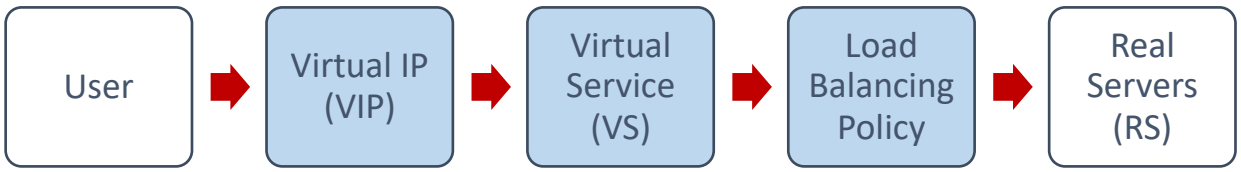
- Ответ - балансировщик нагрузки или ADC.

Теперь решение.

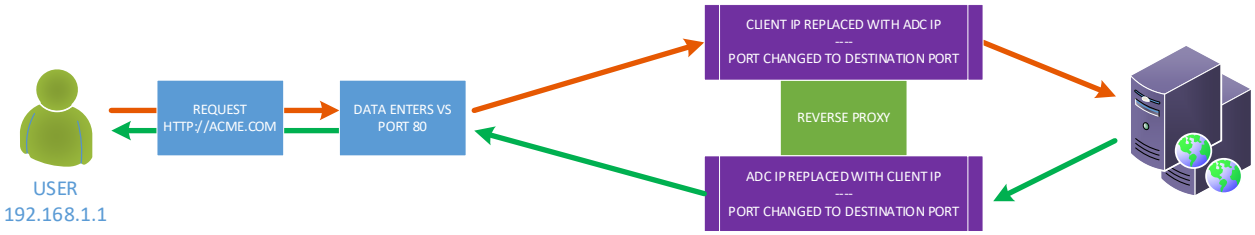
- Мы размещаем ADC перед двумя серверами приложений.



- ADC будет иметь внешний IP-адрес 1.2.3.6, и брандмауэр NAT будет перенаправлять запросы на этот адрес, а не на прежний 1.2.3.4.
- IP-адрес ADC, принимающий запросы, называется VIP, а конфигурация - виртуальной службой.
- ADC получает запросы от пользователей-клиентов и передает их реальным серверам с помощью политик баланса нагрузки, отслеживая работоспособность серверов приложений для обеспечения эффективности.



- ADC балансирует трафик на серверах в зависимости от используемой политики балансировки нагрузки, характера нагрузки и состояния серверов приложений.
- Трафик с серверов будет отправляться обратно клиенту через ADC в обратном направлении.
- Из-за природы обратного прокси сервер и клиент анонимны друг для друга.



- Технология обратного прокси обеспечивает оптимальный уровень безопасности.

VIP-клиенты и виртуальные службы (VS)

VIP - это, по сути, IP-адрес, определенный для использования на EdgeADC и позволяющий пользователям получать доступ к привязанным к нему сервисам. Вот, собственно, и все, что представляет собой VIP. Благодаря тому, как работает EdgeADC, VIP не обязательно должен находиться в той же подсети, что и реальные серверы, и эта методология трансляции сетевых адресов делает технологию очень безопасной для хакеров, пытающихся получить доступ к внутренним серверам.

Примечание: IP-адрес VIP не может быть таким же, как IP-адрес, используемый для IP-адреса управления.

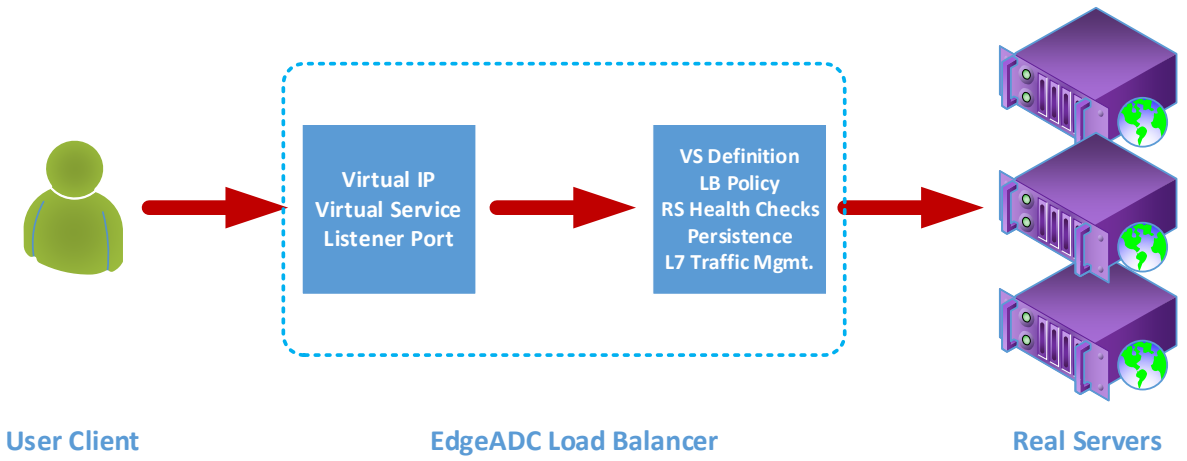
Виртуальные службы составляют основу технологий проксирования и балансировки нагрузки EdgeADC. Виртуальный IP-адрес - это адрес, через который VS рекламируется в сети и во всем мире, прослушивая трафик и запросы от клиентов, желающих использовать приложения, которые он обслуживает.

Когда клиенты попадают на VS, VS будет настроен на выполнение множества действий с трафиком, включая, но не ограничиваясь этим:

- Прокси-соединение клиента
- Выполняются специфические функции, такие как сжатие, ускорение, балансировка нагрузки, проверка трафика и т. д.
- Перенаправление запросов клиента на целевые серверы, определенные в рамках политик балансировки нагрузки виртуальной службы.

Можно считать, что VS - это IP-адрес (VIP), который EdgeADC прослушивает, готовясь к запросам данных. При стандартных конфигурациях TCP или HTTP клиент подключается к VIP, а EdgeADC обрабатывает запрос в соответствии с определением, входящим в VS. После этого EdgeADC отправит трафик на указанные реальные серверы.

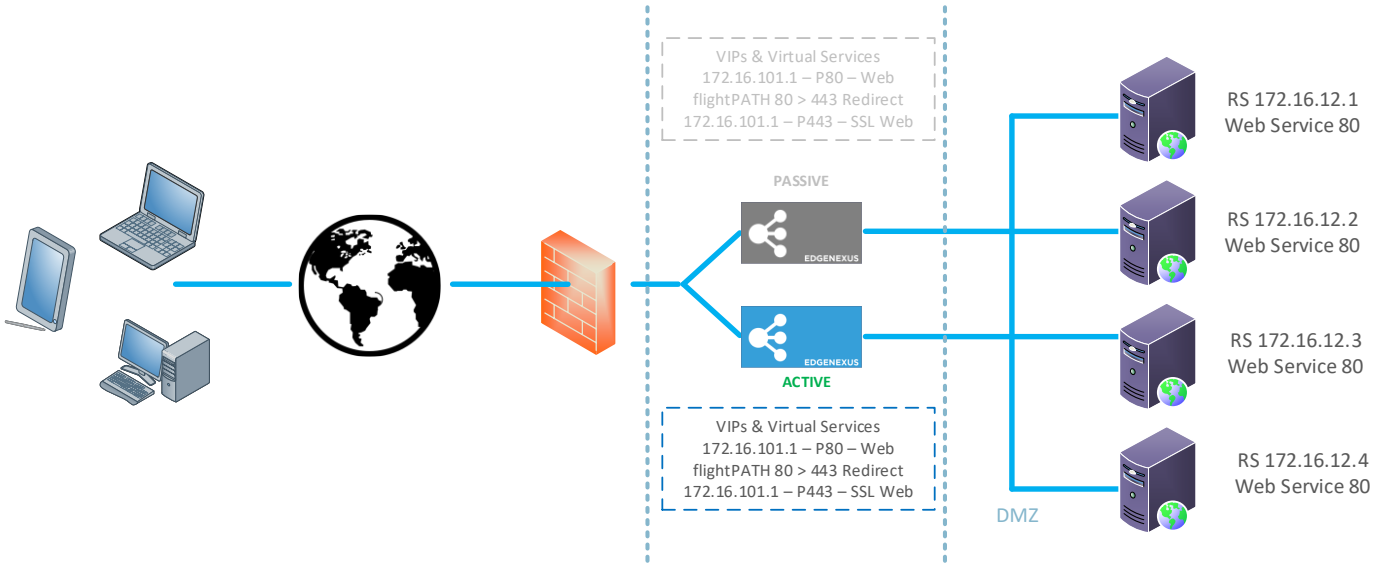
VS получает соединение и данные в типичной конфигурации, а затем завершает или проксирует их с помощью механизма обратного прокси в EdgeADC. Затем EdgeADC открывает новое соединение с реальными серверами и отправляет данные дальше. Когда реальные серверы отвечают на запрос, EdgeADC отправляет ответ клиенту, используя аналогичный обратный путь, что зависит от настроек, заданных в опции Connectivity на вкладке Real Servers Load Balancing.



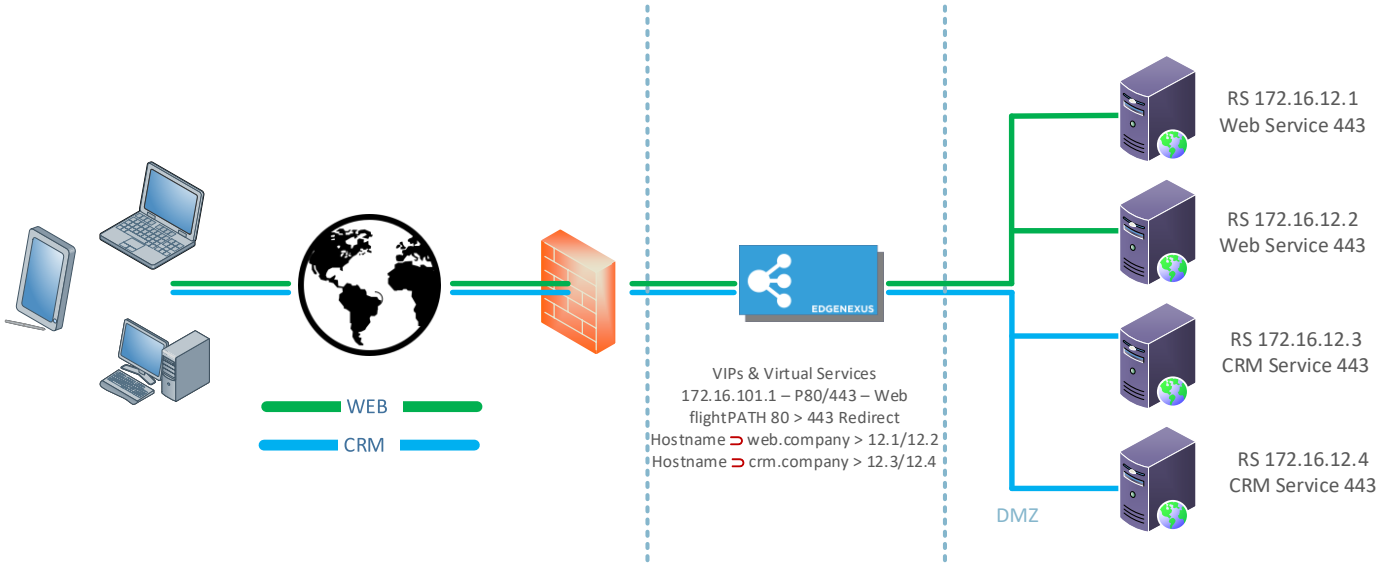
Определение виртуальной службы включает в себя один IP-адрес (VIP) и набор портов, которые служат точками входа для различных служб, использующих различные протоколы.

Например, вам нужно сбалансировать нагрузку ряда веб-серверов для обеспечения устойчивости. Предположим, что доступ к этим системам будет осуществляться по защищенному протоколу HTTPS с помощью https://myweb.company.com.

Если посмотреть на определение такой конфигурации, то она будет состоять из одного VIP с двумя записями, одна для порта 80, а другая для порта 443. К VIP-порту 80 будет прикреплено правило flightPATH, которое принудительно преобразует трафик в HTTPS. Вторая запись для порта 443 будет направлять трафик на Real Servers, определенные под ней. Аналогичным образом, вы можете разместить другие службы под тем же VIP для балансировки нагрузки на почтовые серверы или другие серверы приложений.



В менее функциональных ADC службы, использующие одни и те же порты, нуждаются в разных VIP, но ADC и его система flightPATH позволяют использовать один VIP с несколькими службами, использующими одни и те же порты. Таким образом, вы можете иметь два приложения, доступ к которым осуществляется через 443 с разными именами хостов, используя один VIP. Пример показан ниже.



Системы EdgeADC чрезвычайно гибкие и позволяют создавать очень сложные и функциональные конфигурации.

Что такое тип службы балансировки нагрузки?

Типы сервисов балансировки нагрузки состоят из алгоритмов и методик, используемых для интеллектуального распределения или балансировки нагрузки трафика между пулами серверов. Метод и алгоритм, который ADC делает доступным, зависит от типа сервиса или приложения, используемого на серверах, на которых происходит балансировка нагрузки, а также от состояния сети и используемых серверов. Следует отметить, что тип сервиса балансировки нагрузки, который вы выберете для использования, также зависит от уровня трафика, проходящего через ADC. Так, при низкой пропускной способности или нагрузке можно использовать простые типы служб балансировки нагрузки. Но при более высокой нагрузке может потребоваться выбор более сложных типов, чтобы добиться более эффективного распределения нагрузки на внутренние серверы.

В EdgeADC доступны следующие типы сервисов балансировки нагрузки.

DICOM	LAYER 4 UDP	RPC
FTP	УРОВЕНЬ 4 TCP/UDP	RPC/ADS
HTTP (S)	DNS	RPC/CA/PF
IMAP	POP3	SMTP
LAYER 4 TCP	RDP	GSLB

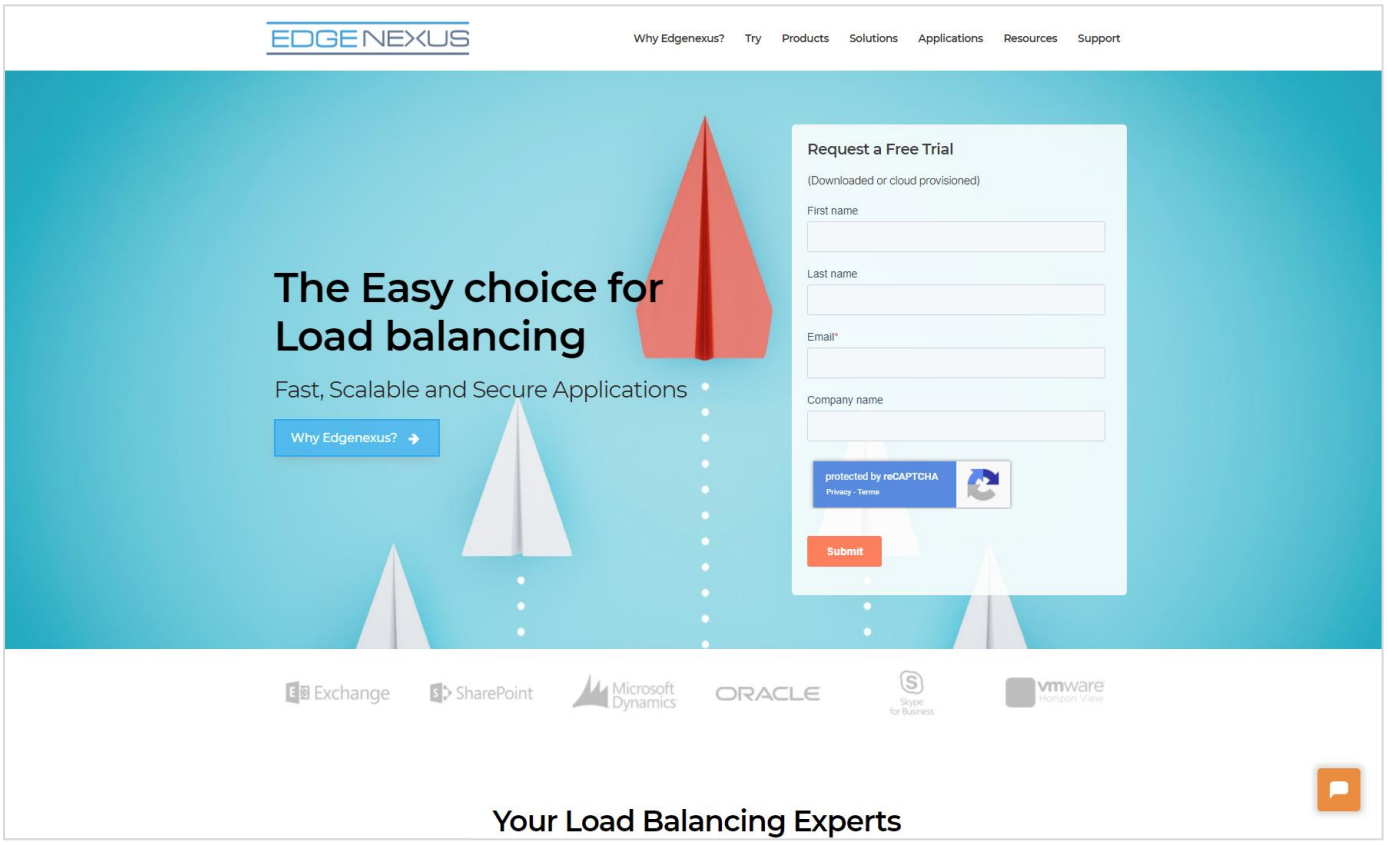
Начало путешествия

Загрузка EdgeADC

Перед установкой первым делом необходимо загрузить EdgeADC, подходящий для вашей среды.

Мы предлагаем редакции для большинства виртуализированных сред и ISO-версии для установки непосредственно на "голое" оборудование.

Первый шаг - заполнить форму оценки на сайте Edgenexus, расположенном по адресу https://www.edgenexus.io/products/load-balancer/free-trial/.



Процесс прост: заполнив и отправив форму, вы попадете на страницу загрузки, где сможете выбрать подходящий образ для вашего окружения.

Редакции EdgeADC доступны для следующих систем виртуализации:

- VMware ESX
- Microsoft Hyper-V
- Citrix XenServer
- Nutanix
- KVM

Вы также можете провести пробное тестирование в облаке с помощью редакций Microsoft Azure или Amazon AWS marketplace.

Если вы решили загрузить программное обеспечение для локальной установки, вы получите EdgeADC со встроенной 14-дневной пробной лицензией. Мы рекомендуем вам обратиться по адресуsales@edgenexus.io и запросить 30-дневный лицензионный ключ со всеми включенными функциями.

Установка

Установка ng EdgeADC

EdgeADC (ADC) доступен для установки на различные платформы, для каждой из которых требуется свой инсталлятор, и они становятся доступны вам после регистрации для загрузки.

Вот различные доступные модели установки.

- VMware ESXi
- KVM
- Citrix Xen
- Nutanix AHV
- Microsoft Hyper-V
- Oracle VM
- Проксмокс (использовать OVA)
- ISO для оборудования BareMetal

Размер виртуальной машины, на которой будет размещен ADC, зависит от сценария использования и пропускной способности данных.

Установка на VMware ESXi

ADC поддерживается 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 распакуйте файл в подходящую директорию на хосте ESXi или в сети SAN.
- В клиенте vSphere выберите File: Deploy OVA/OVF Template (Файл: Развернуть шаблон OVA/OVF).
- Найдите и выберите место, где вы сохранили 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 выберите Power > Power-On.
- После этого ваш VA загрузится, и на консоли появится экран загрузки ADC.

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 виртуальной машине 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 стандартным способом. Он будет работать с VMXNET3

Включение интерфейса VMXNET3 на уже работающем VA

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

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

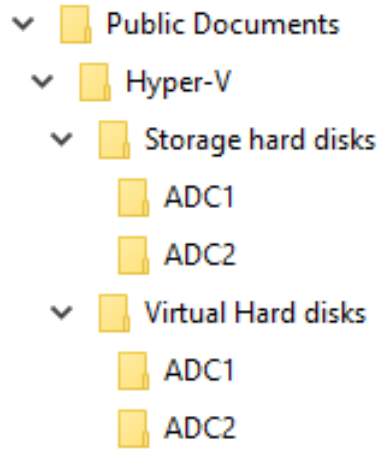
Для продолжения работы обратитесь к разделу **КОНФИГУРАЦИЯ ПЕРВОЙ ЗАГРУЗКИ**.

Установка на Microsoft Hyper-V

Виртуальное устройство Edgenexus ADC Virtual можно легко установить в системе виртуализации Microsoft Hyper-V. В данном руководстве предполагается, что вы правильно указали и настроили систему Hyper-V и системные ресурсы для размещения ADC и его архитектуры балансировки нагрузки.

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

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



- Скопируйте извлеченный файл EdgeADC .vhd в папку "Storage hard disk", созданную выше.
- В клиенте Hyper-V Manager щелкните правой кнопкой мыши на сервере и выберите "Импортировать виртуальную машину".
- Перейдите в папку, содержащую загруженный файл образа ADC VA, извлеченный ранее
- Выберите виртуальную машину - выделите виртуальную машину для импорта и нажмите Далее
- Выберите виртуальную машину - выделите виртуальную машину для импорта и нажмите Далее
- Выберите тип импорта - выберите "**Скопировать виртуальную машину (создать новый уникальный идентификатор)**", нажмите далее
- Выберите папки для файлов виртуальных машин - пункт назначения можно оставить по умолчанию Hyper-V или выбрать другое местоположение
- Найдите Virtual Hard Disks (Виртуальные жесткие диски) - найдите и выберите папку с виртуальными жесткими дисками, созданную выше, и нажмите кнопку Далее
- Выберите папки для хранения виртуальных жестких дисков - перейдите и выберите папку Storage hard disks, созданную ранее, и нажмите кнопку next.
- Убедитесь в правильности данных в окне Завершение работы мастера импорта и нажмите кнопку Готово
- Щелкните правой кнопкой мыши на только что импортированной виртуальной машине **ADC** и выберите Start

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

- Пока ВМ инициализируется, можно щелкнуть правой кнопкой мыши на записи ВМ и выбрать Connect... После этого откроется консоль EdgeADC.

- После того как вы настроите свойства сети, VA перезагрузится и представит вход в консоль VA.

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

Установка на 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 файл **OVA**, затем нажмите **"Открыть далее".**
- В ответ на запрос выберите место создания виртуальной машины.
- Выберите сервер XenServer, который вы хотите установить, и нажмите **"NEXT".**
- В ответ на запрос выберите хранилище (SR) для размещения виртуальных дисков.
- Выберите SR с достаточным пространством и нажмите **"NEXT"**.
- Нанесите на карту виртуальные сетевые интерфейсы. На обоих интерфейсах будет написано Eth0, однако обратите внимание, что нижний интерфейс - Eth1.
- Выберите целевую сеть для каждого интерфейса и нажмите **NEXT.**
- **НЕ** отмечайте пункт "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. Помните, что вы должны назначить статические IP-адреса, если у вас нет работающего DHCP-сервера для передачи данных. Если этого не сделать, при импорте появится сообщение Connecting continuously and failed. Нажмите **"NEXT".**
- Просмотрите всю информацию и проверьте правильность настроек. Нажмите **"Завершить".**
- Ваша ВМ начнет передавать виртуальный диск "ADC" и после завершения будет отображаться под вашим XenServer.
- Теперь в клиенте XenCenter вы сможете увидеть новую виртуальную машину.
  Щелкните правой кнопкой мыши на виртуальной машине и нажмите "**START**".
- После этого загрузится ваша ВМ, и появится экран загрузки ADC.

- После настройки появляется возможность входа в систему VA.

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

Установка на KVM

В следующем разделе показано, как установить EdgeADC на платформу KVM. Платформа KVM, использованная в этом упражнении, работала под управлением операционной системы CentOS v8 с установленными Cockpit и виртуализацией.

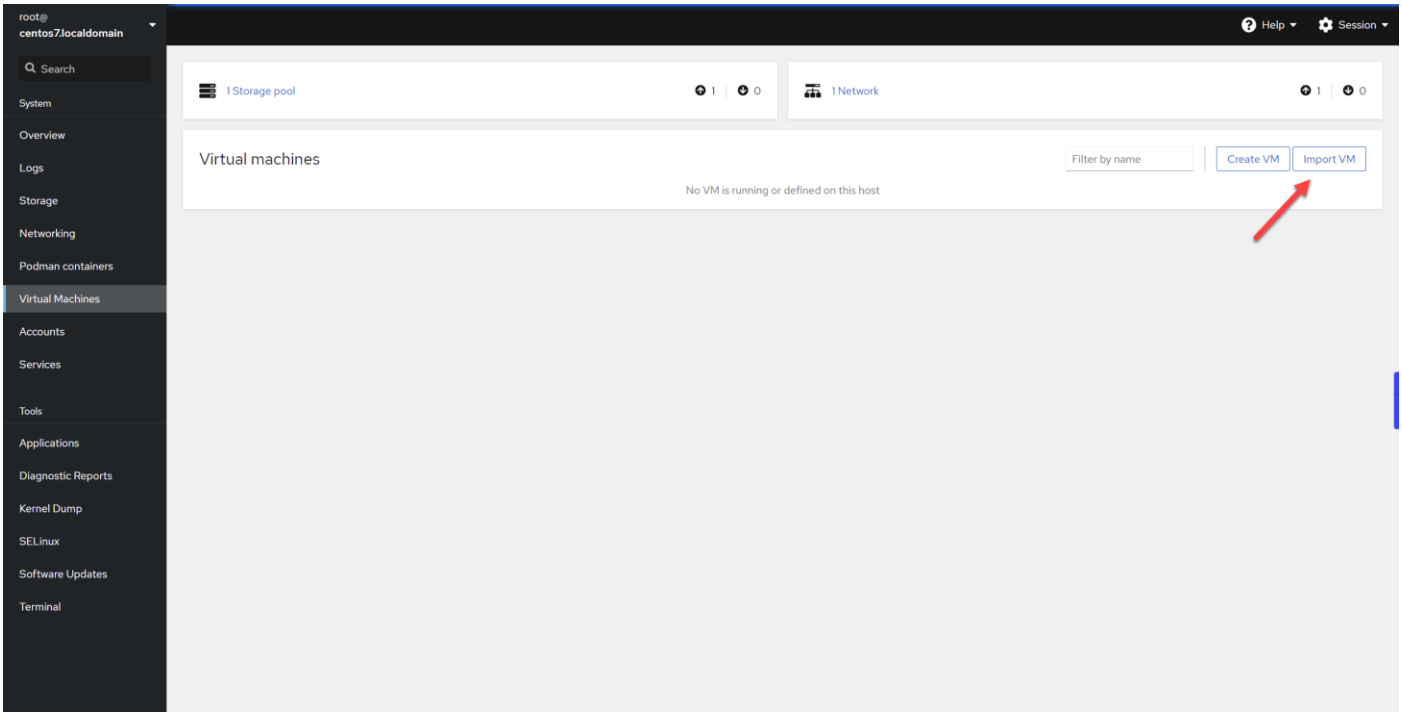
Требования и версии

Это руководство актуально для EdgeADC 4.2.6 и выше.

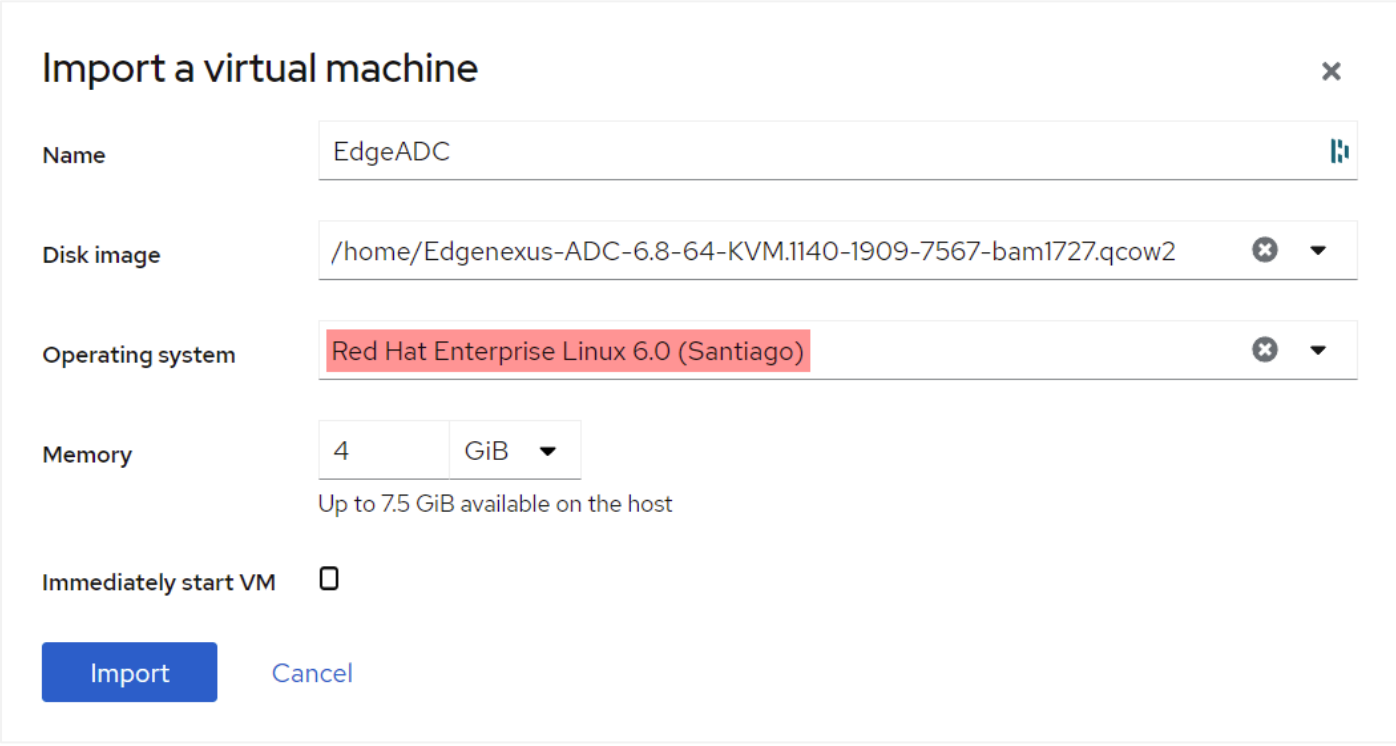
Приведенное ниже руководство не касается установки KVM или его сетевого подключения.

Мы предположили, что вы загрузили виртуальное приложение KVM и сохранили его на хосте в доступном месте.

- Первым шагом будет вход в консоль Cockpit.

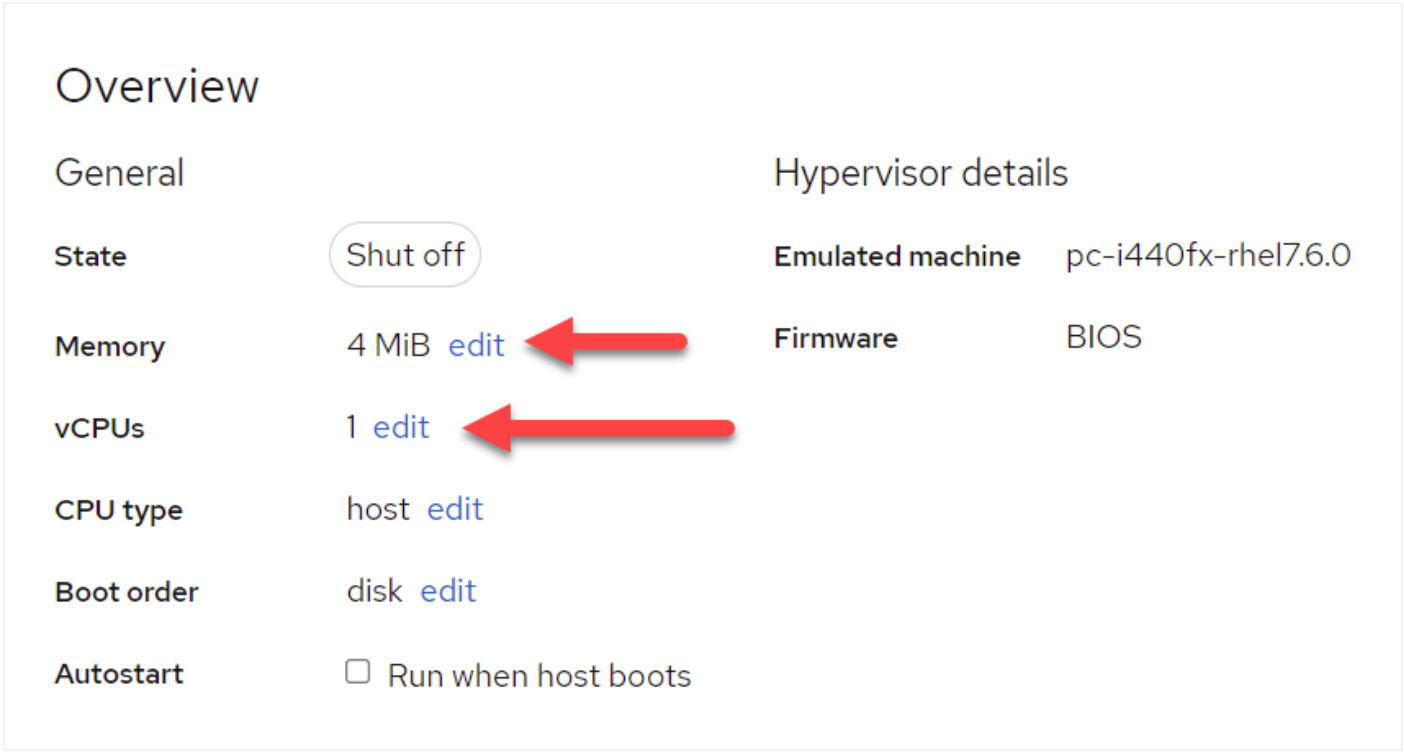


- Нажмите кнопку Импорт виртуальной машины
- В первом диалоговом окне необходимо указать детали для импорта виртуального устройства. Содержание полей показано на рисунке ниже. В качестве ОС необходимо указать Red Hat Enterprise 6.0.

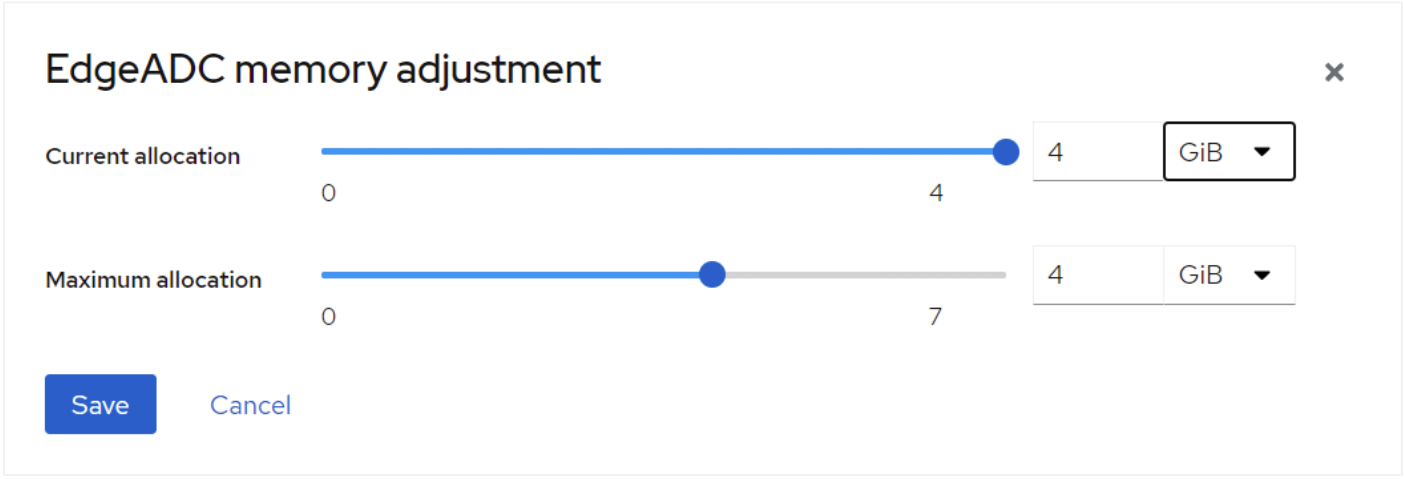


- Убедитесь, что флажок "Immediately Start VM" снят.

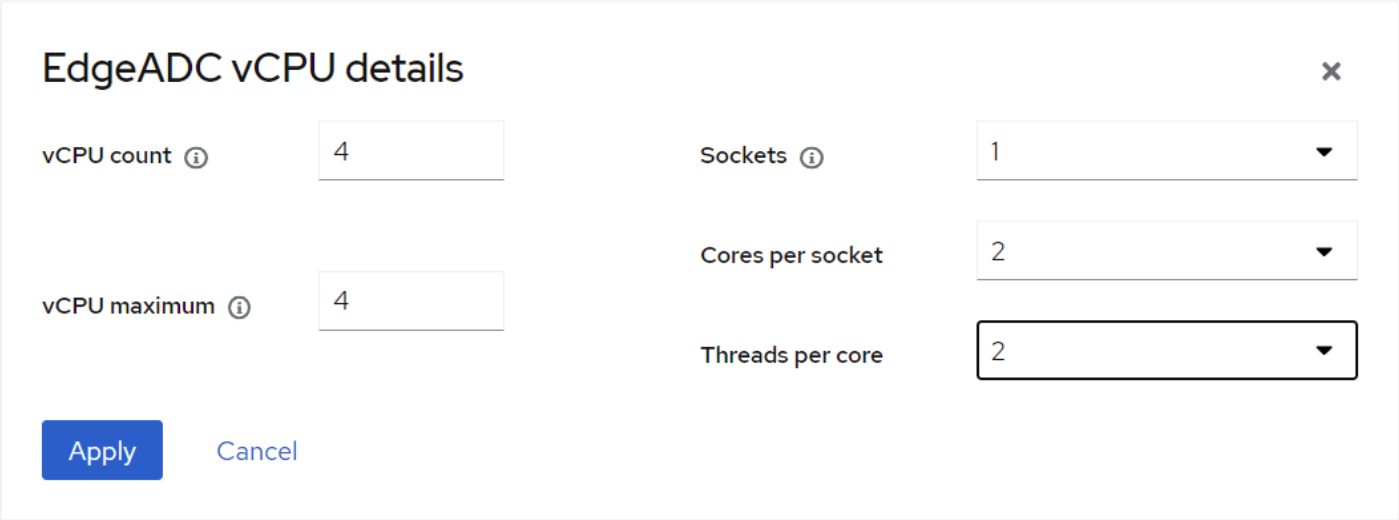
- После того как вы заполнили все данные, нажмите кнопку Импорт.
- На следующем этапе необходимо указать распределение vCPU и памяти, которые вы хотите использовать.



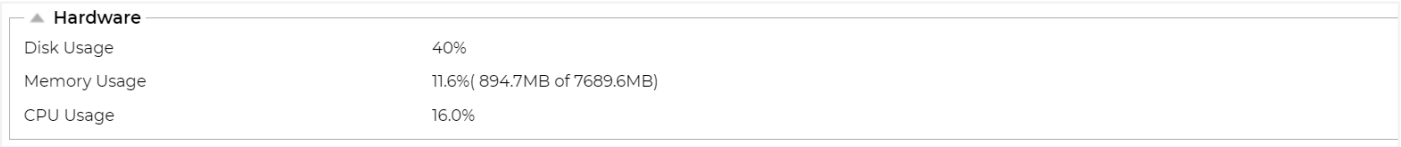
- Чтобы выделить память, вы увидите диалоговое окно, подобное приведенному ниже.



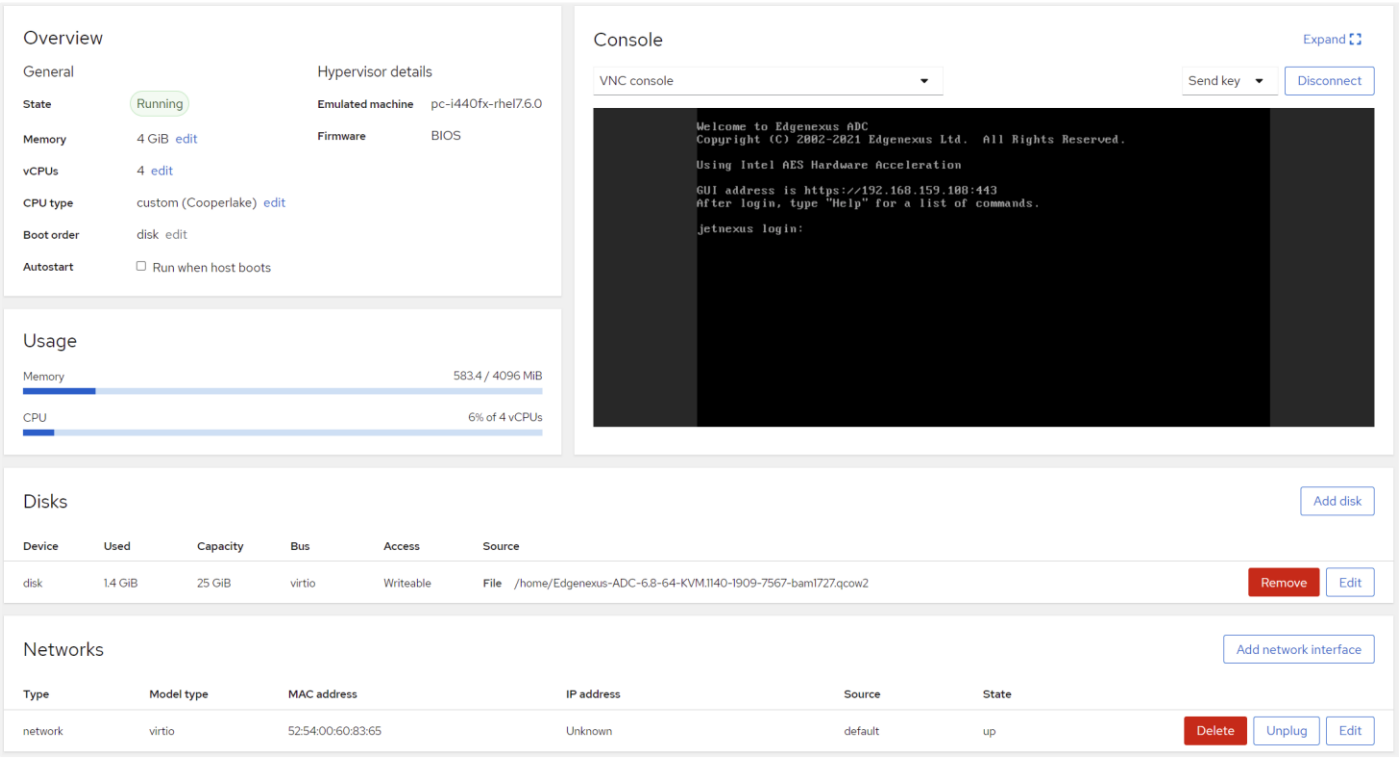
- Чтобы выделить vCPU, вы увидите диалоговое окно, подобное приведенному ниже.



- Приведенные нами варианты являются лишь примерами, но вполне работоспособны, если только вы не используете большую пропускную способность с повторным шифрованием SSL, в этом случае вам нужно будет внести соответствующие изменения, используя раздел Hardware в меню View > Statistics.



- Теперь в KVM установлен рабочий АЦП. Смотрите изображение ниже.



Установка на Nutanix AHV

В следующем разделе показано, как установить EdgeADC на платформу Nutanix AHV.

Требования и версии

Это руководство актуально для EdgeADC 4.2.6 и выше.

Все версии гипервизора Nutanix совместимы, но сертификация проводилась на версии Nutanix 5.10.9.

- Первым шагом будет вход в систему Nutanix Prism Central.

Загрузка изображения EdgeADC

- Перейдите в раздел Виртуальная инфраструктура > Образы
- Нажмите кнопку Добавить изображение
- Выберите файл изображения EdgeADC, который вы загрузили, и нажмите кнопку Открыть, чтобы загрузить изображение.
- Введите название изображения в поле Описание изображения.
- Выберите подходящую категорию
- Выберите изображение и нажмите клавишу со стрелкой вправо.
- Выберите Все изображения и нажмите кнопку Сохранить.

Создание виртуальной машины

- Перейдите в раздел Виртуальная инфраструктура > ВМ
- Нажмите кнопку Создать виртуальную машину
- Введите имя ВМ, количество процессоров и количество ядер, которые вы хотите выделить для ВМ.
- Затем прокрутите диалоговое окно вниз и введите объем памяти, который вы хотите выделить для ВМ. Вы можете начать с 4 ГБ и увеличивать этот объем в зависимости от использования.

Добавление диска

- Затем щелкните ссылку Добавить новый диск.
- Выберите опцию Clone from Image Service в раскрывающемся списке Operation (Операция).
- Выберите добавленное изображение EdgeADC и нажмите кнопку Добавить.
- Выберите диск, который будет загрузочным.

Добавление сетевой карты, сети и родства

- Затем нажмите кнопку Добавить новую сетевую карту. Вам понадобятся две сетевые карты.
- Выберите сеть и нажмите кнопку Добавить
- Нажмите кнопку Установить сродство
- Выберите хосты Nutanix, на которых разрешено запускать ВМ, и нажмите кнопку Save (Сохранить).
- Проверьте сделанные настройки и нажмите кнопку Сохранить

Включение виртуальной машины

- В списке виртуальных машин щелкните имя виртуальной машины, которую вы только что создали.
- Нажмите кнопку включения питания для виртуальной машины
- После включения ВМ нажмите кнопку Launch Console (Запуск консоли).

Настройка сетевого подключения EdgeADC

- Следуйте инструкциям в разделе Первая загрузочная среда.
- Теперь EdgeADC готов к работе, и вы сможете получить доступ к его графическому интерфейсу, используя браузер и IP-адрес управления.

Установка на ProxMox

Установка на ProxMox проста, но требует нескольких дополнительных шагов.

Мы будем использовать версию установки VMWare OVA. Это многоэтапный процесс, требующий знания команд оболочки ProxMox. Однако мы сделали инструкции максимально простыми для

выполнения. Мы предполагаем, что вы уже знакомы с ProxMox, поэтому не будем углубляться в его особенности.

Загрузка OVA в ProxMox

Поскольку мы используем OVA-версию, сначала нам нужно загрузить OVA в ProxMox.

- Войдите в консоль ProxMox
- Создайте папку под названием OVA_Import.
- Теперь вам нужно использовать SFTP-клиент, например WinSCP (Windows) или CyberDuck (Mac), чтобы передать OVA-файл.
- Когда файл будет передан, вы увидите его в созданной вами папке.
- Введите следующую команду, чтобы извлечь содержимое файла OVA.
- Tar xvf {filename}. См. пример ниже.

```
tar xvf Edgenexus-ADC-6.8-64-OVA.1155-1961-9704-bam2221.ova
```

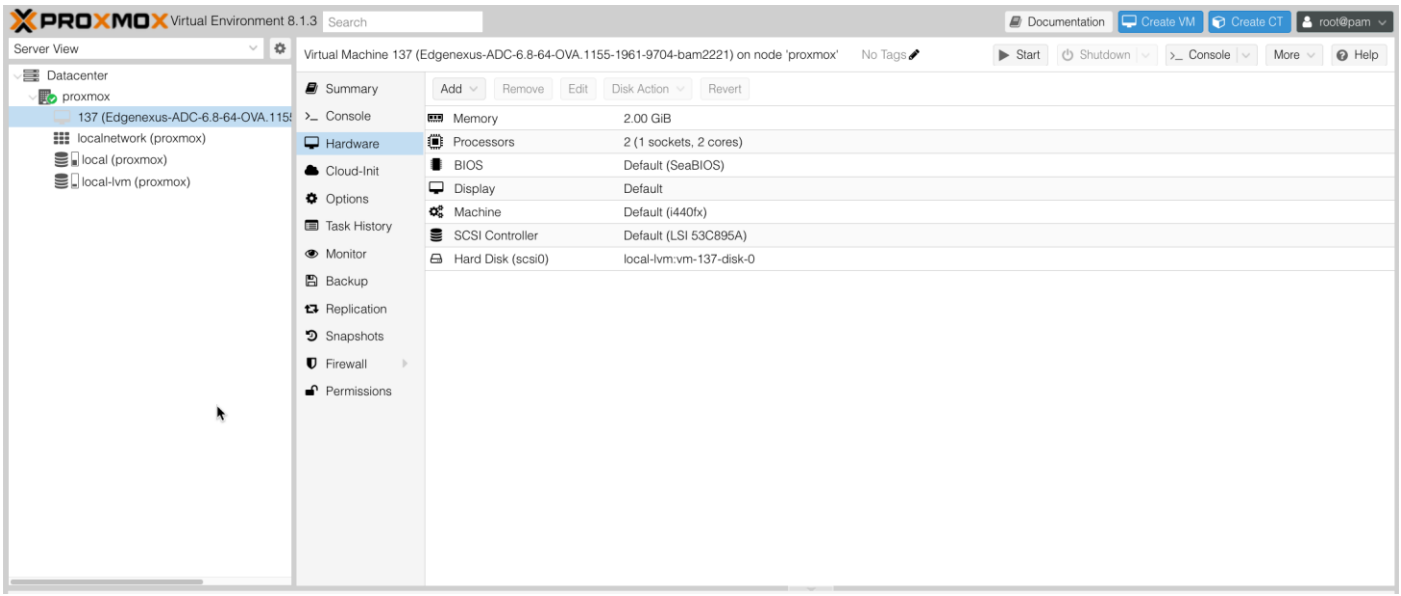
- После извлечения вы должны увидеть что-то вроде приведенного ниже примера.

```
root@proxmox:~/OVA_Import# ls
Edgenexus-ADC-6.8-64-OVA.1155-1961-9704-bam2221.ova
root@proxmox:~/OVA_Import# tar xvf Edgenexus-ADC-6.8-64-OVA.1155-1961-9704-bam2221.ova
Edgenexus-ADC-6.8-64-OVA.1155-1961-9704-bam2221.ovf
Edgenexus-ADC-6.8-64-OVA.1155-1961-9704-bam2221.mf
Edgenexus-ADC-6.8-64-OVA.1155-1961-9704-bam2221-disk1.vmdk
root@proxmox:~/OVA_Import#
```

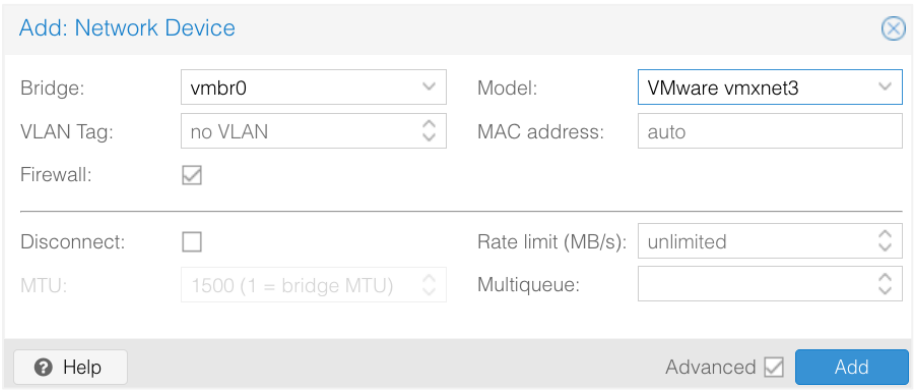
- Имеется три файла. Файлы .ovf и .mf - это конфигурация. .vmdk - виртуальный диск с ADC.
- Следующим шагом будет импорт VMDK в ProxMox и создание виртуальной машины.
- Введите следующую команду, чтобы создать виртуальную машину с помощью файлов конфигурации.

```
qm importovf 137 ./{filename.ovf} local-lvm --format qcow2
```

- В данном примере мы указали ID 100, но для вашей установки он может быть другим, если у вас уже есть виртуальные машины, созданные в ProxMox. Вы можете определить следующий ID, начав процесс создания виртуальных машин в ProxMox, или выбрав число больше 100, которое будет безопасно недоступно.
- Теперь виртуальная машина создана.



- Следующим шагом будет добавление сетевого интерфейса к виртуальной машине.
- Нажмите на Hardware (Оборудование) на правой панели.
- Нажмите кнопку Добавить и выберите сетевой интерфейс.



- Настройте его, как показано на изображении выше. Важно выбрать модель VMware vmxnet3.
- После настройки нажмите кнопку Добавить.
- Вы можете установить дополнительные сетевые адаптеры в зависимости от ваших потребностей.
- Теперь вы можете запустить виртуальную машину и приступить к выполнению инструкций, приведенных в главе "Конфигурация первой загрузки".

Конфигурация первой загрузки

При первой загрузке ADC (также обозначаемый ниже как VA) отображает следующий экран, запрашивающий конфигурацию для производственных операций.

Первая загрузка - сведения о сети вручную

При первой загрузке у вас будет 10 секунд, чтобы прервать автоматическое назначение IP-адресов 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 постоянны, они переживут перезагрузку, и их не нужно будет настраивать заново на VA.

Первая загрузка - DHCP успешно

Если вы не прервете процесс назначения сети, ваш АЦП по истечении времени свяжется с DHCP-сервером, чтобы получить данные о своей сети. Если контакт будет успешным, то вашему аппарату будет присвоена следующая информация.

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

Мы советуем использовать DHCP-адрес для работы ADC только в том случае, если этот IP-адрес постоянно связан с MAC-адресом ADC на DHCP-сервере. При использовании виртуальных устройств мы всегда рекомендуем использовать **фиксированный IP-адрес**. Выполняйте действия, описанные **В РАЗДЕЛЕ ИЗМЕНЕНИЕ IP-АДРЕСА УПРАВЛЕНИЯ** и последующих разделах, пока не завершите настройку сети.

Первая загрузка - DHCP не работает

Если у вас нет DHCP-сервера или соединение не работает, 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 в любой момент изменить IP-адрес VA с помощью команды **set greenside=n.n.n.n.n,** как показано ниже.

```
set greenside={IP-адрес}
```

Изменение маски подсети для eth0

Сетевые интерфейсы используют префикс 'eth'; базовый сетевой адрес называется eth0. Маску подсети или сетевую маску можно изменить с помощью команды **set mask [NIC] [MASK]**. Пример приведен ниже.

```
set mask eth0 {mask}
```

Назначение шлюза по умолчанию

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

```
route add default gw {IP Address}
```

Проверка значения шлюза по умолчанию

Чтобы проверить, правильно ли добавлен шлюз по умолчанию, 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

Для настройки, мониторинга и ввода АЦП в эксплуатацию можно использовать любой интернет-браузер с поддержкой JavaScript.

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

По умолчанию АЦП использует самоподписанный SSL-сертификат. Вы можете изменить АЦП на использование SSL-сертификата по своему усмотрению.

Как только браузер достигнет ADC, появится экран входа в систему. Заводские учетные данные по умолчанию для ADC следующие:

Username: admin / Pwd: jetnexus

Справочная таблица команд

Команда	Параметр1	Параметр2	Описание	Пример
дата			Показывает настроенную дату и время, установленные в данный момент	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	[пусто]		Просмотр конфигурации интерфейса для всех интерфейсов	ifconfig
	eth0		Просмотрите конфигурацию интерфейса только eth0	ifconfig eth0
machineid			Эта команда предоставит идентификатор машины, используемый для лицензирования ADC ADC	EF4-3A35-F79
уйти			Выход из интерфейса командной строки	
перезагрузка			Разорвите все соединения и перезагрузите АЦП АЦП	перезагрузка
перезапустить			Перезапустите виртуальные службы ADC ADC	
маршрут	[пусто]		Просмотр таблицы маршрутизации	маршрут
	добавить	стандартное gw	Добавьте IP-адрес шлюза по умолчанию	route add default gw 192.168.100.254
установить	Гринсайд		Установите IP-адрес управления для ADC	set greenside=192.168.101.1
	маска		Установка маски подсети для интерфейса. Имена интерфейсов: eth0, eth1....	установить маску eth0 255.255.255.0
показать			Отображение параметров глобальной конфигурации	
отключение			Завершите все соединения и отключите питание АЦП АЦП	
статус			Отображение текущей статистики 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.

Веб-консоль

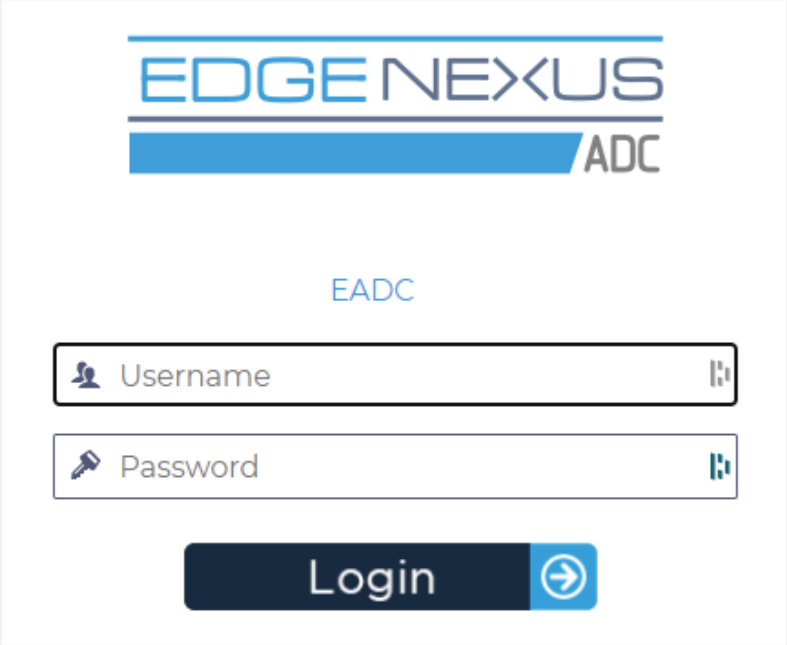
Запуск веб-консоли ADC

Все операции с АЦП настраиваются и выполняются с помощью веб-консоли. Доступ к веб-консоли осуществляется через любой браузер с поддержкой JavaScript.

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

https://adc.company.com

После запуска веб-консоль ADC выглядит так, как показано ниже, позволяя вам войти в систему в качестве пользователя admin.



Учетные данные для входа по умолчанию

По умолчанию используются следующие учетные данные:

Username: admin / Pwd: jetnexus

Вы можете изменить это в любое время с помощью конфигурации пользователя, расположенной *в разделе Система > Пользователи*.

После успешного входа в систему на экране появится главная приборная панель ADC.

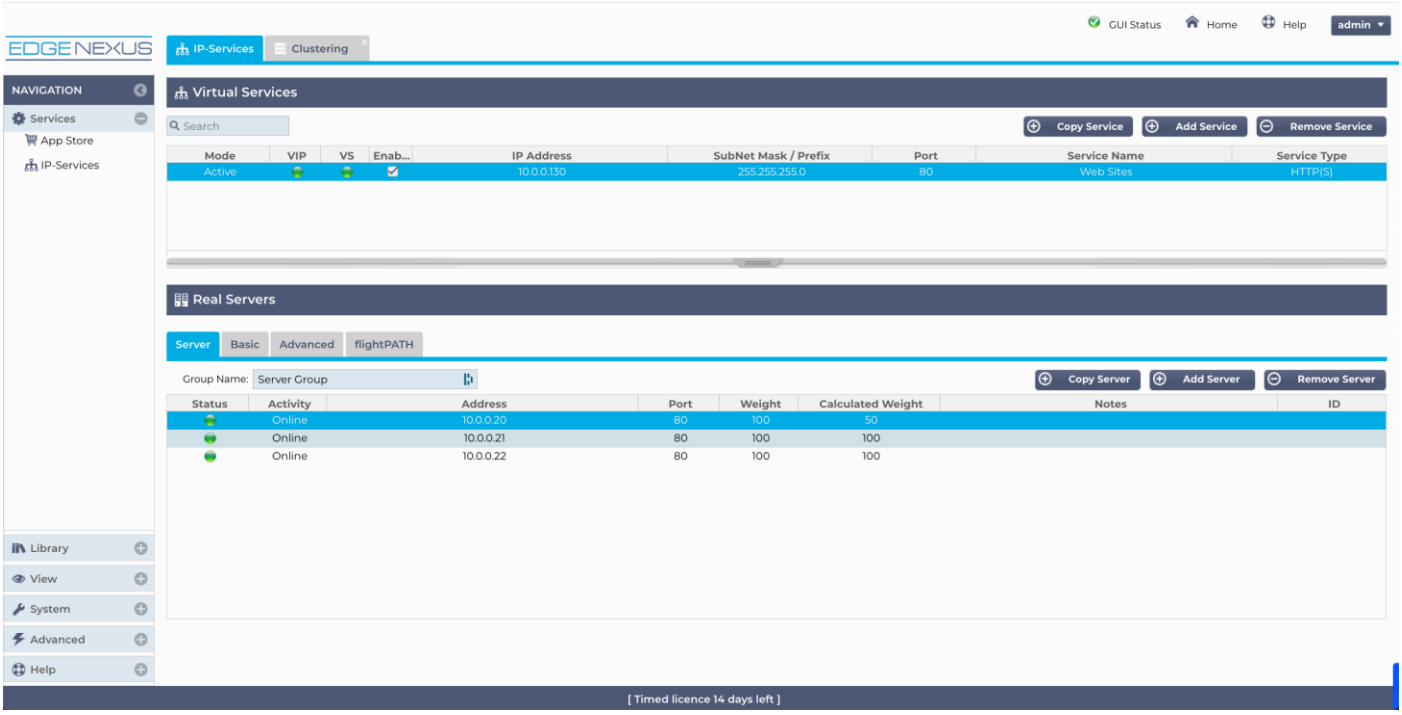
Использование внешней службы аутентификации

Если вы хотите использовать внешнюю службу аутентификации, вы можете сделать это, настроив сервер аутентификации и службу аутентификации.

Информацию об этом можно найти в разделахАутентификация иСлужба аутентификации

Главная приборная панель

На изображении ниже показано, как выглядит главная приборная панель или "домашняя страница" ADC. Время от времени мы можем вносить некоторые изменения в целях улучшения, но все функции останутся.



Раздел "Навигация" в левой части позволяет перемещаться по различным областям функциональных возможностей АЦП. По умолчанию выбран раздел Services (Услуги) и открыт подраздел IP Services (Услуги IP), на что указывает вкладка, расположенная над разделом Virtual Services (Виртуальные услуги). Эта вкладка является фиксированной и отображается всегда.

При нажатии на раздел в навигации этот раздел раскрывается и показывает свое содержимое. При нажатии на опцию в разделе содержимое раздела откроется справа, а сверху будет размещена вкладка, позволяющая быстро переключаться.

Различные разделы навигации подробно описаны в последующих главах.

Услуги

IP-услуги

Раздел IP Services в 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.

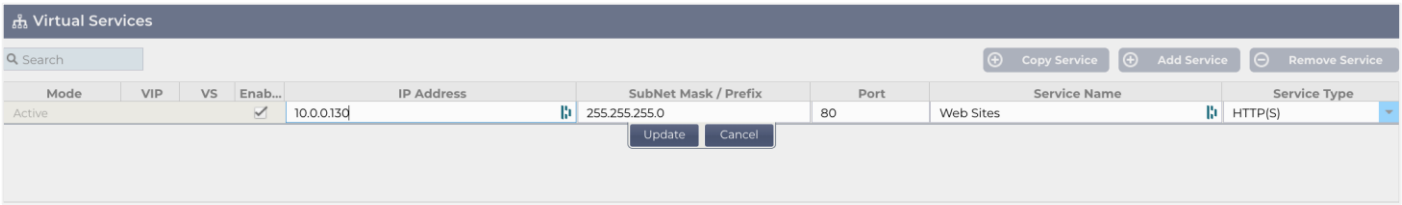
Виртуальные услуги

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

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

Создание новой виртуальной службы с использованием нового VIP-клиента

- Нажмите кнопку Добавить виртуальную службу, как указано выше.



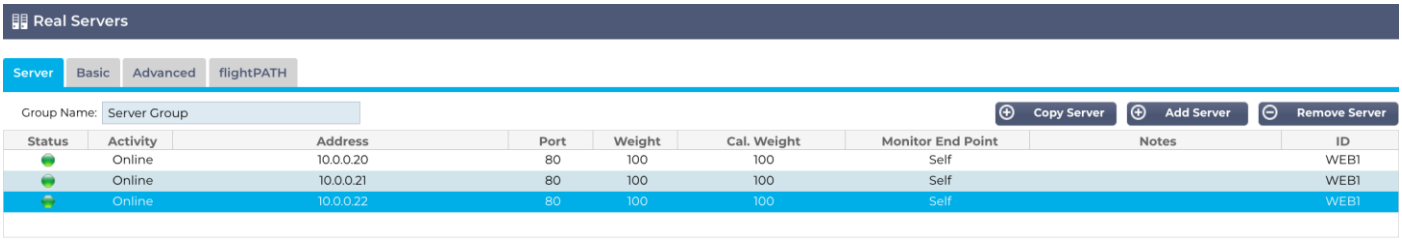
После этого вы перейдете в режим **редактирования строки**.

- 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 в качестве целевой точки 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 с реальным сервером, если вы используете обратный прокси.
Название услуги	Название услуги - это текстовое представление назначения VIP-клиента. Оно необязательно, но мы рекомендуем указать его для ясности. Обратите внимание, что это поле используется для других конкретных целей при использовании GSLB.
Тип услуги	Существует множество различных типов услуг, которые вы можете выбрать. Типы услуг уровня 4 не могут использовать технологию flightPATH.

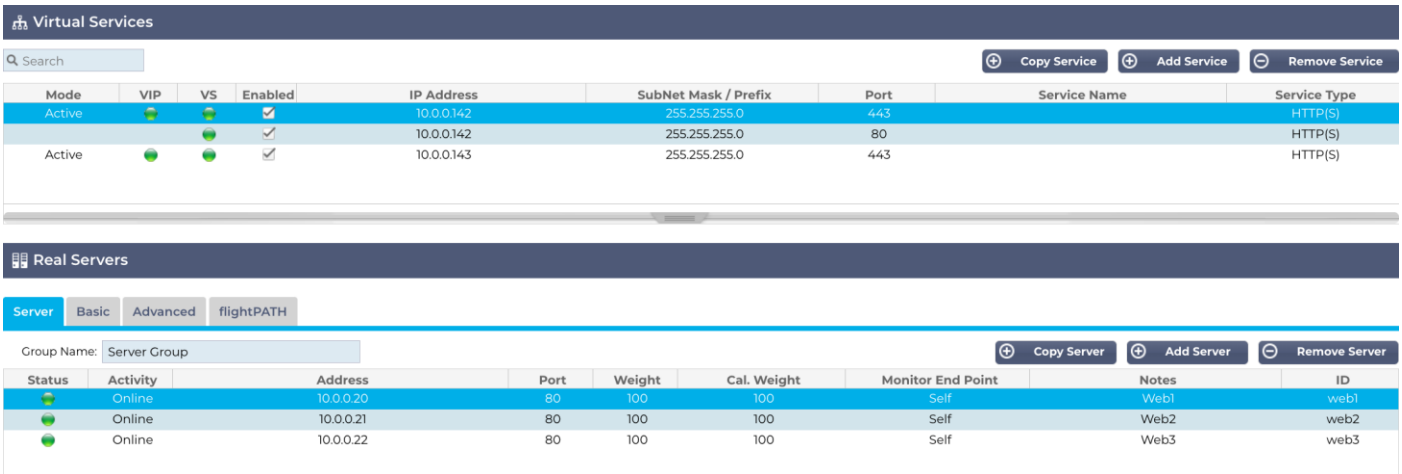
Теперь вы можете нажать кнопку Update, чтобы сохранить этот раздел и автоматически перейти к разделу Real Server, описанному ниже:



Поле	Описание
Деятельность	Поле Activity можно использовать для отображения и изменения состояния 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 дренажа, чтобы можно было промыть постоянство и перевести сервер в автономное состояние, не затрагивая пользователей. Standby - сервер переведен в состояние ожидания
IP-адрес	Это значение - IP-адрес 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 вес приоритета.
Кал. Вес	Если оставить значение Weighting по умолчанию, АЦП будет автоматически рассчитывать весовые коэффициенты на основе времени отклика.
Конечная точка мониторинга	По умолчанию используется значение 'Self'. Однако вы можете изменить его на значение порта или IP-адрес:порт. Это поле используется для мониторинга другой конечной точки и определения того, следует ли передавать трафик виртуальной службе. См.Как использовать Monitor End Point ниже.

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

Пример выполненной виртуальной услуги

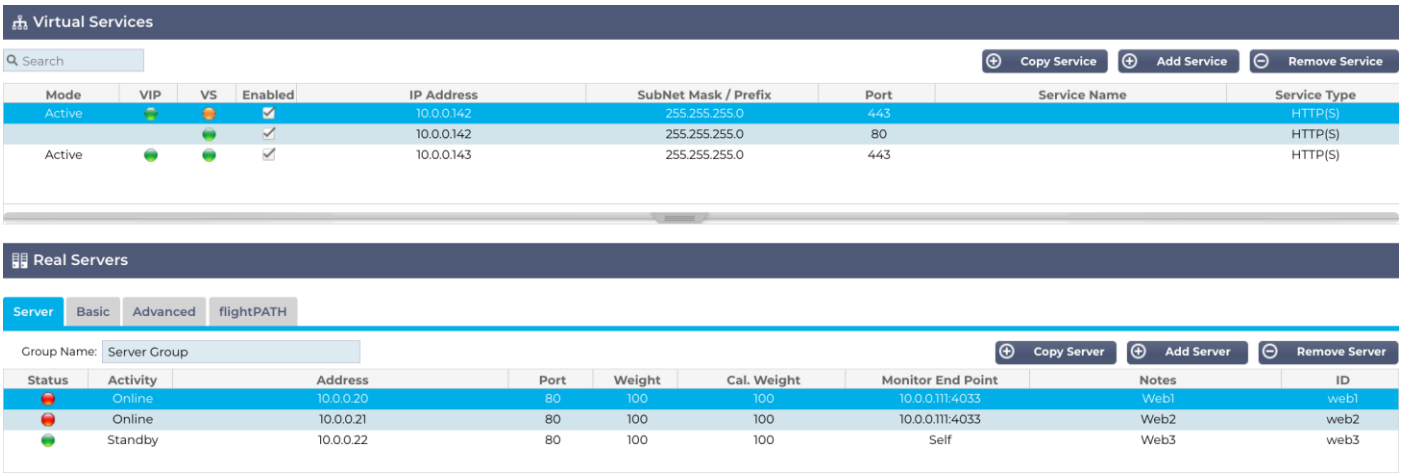


Как использовать Monitor End Point

Пример 1

Рассмотрим пример инфраструктуры, состоящей из двух сбалансированных по нагрузке веб-серверов, которые доставляют веб-приложение конечному пользователю. Веб-приложение подключено к серверу базы данных в задней части. Доступ к серверу базы данных прекращается, но серверы веб-приложения продолжают работать. Пользователи пытаются использовать веб-приложение и получают ошибки.

Решение заключается в использовании Monitor End Point.



- В примере показаны два веб-сервера, 10.0.0.20 и 10.0.0.21, а также третий веб-сервер 10.0.0.22. Сервер 10.0.0.22 был переведен в режим ожидания.
- Два активных веб-сервера были настроены с конечной точкой мониторинга 10.0.0.111:4033, которая является IP-адресом и портом подключения сервера базы данных.
- В случае разрыва соединения с сервером базы данных оба активных сервера перейдут в автономный режим, а резервный сервер перейдет в режим онлайн, обслуживая веб-страницу, которая может сообщить клиенту, что системы находятся на техническом обслуживании.

Пример 2

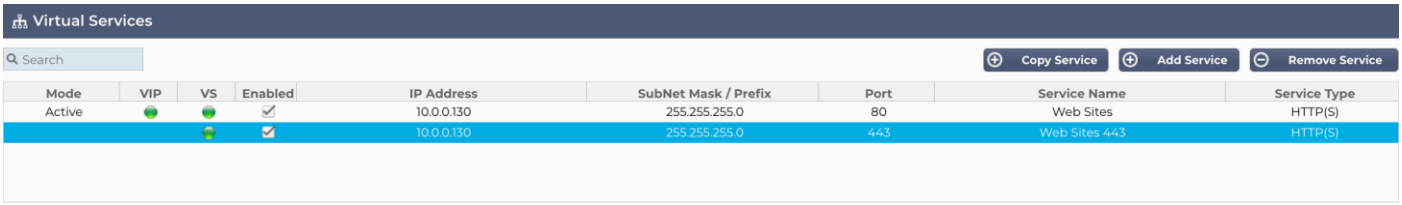
Еще один пример использования Monitor End Point - балансировка нагрузки на серверы с протоколом UDP, например Always-On-VPN. Как вы, возможно, знаете, UDP-порты не поддаются надежному мониторингу, поэтому возникает необходимость в мониторинге TCP-порта.

Использование Monitor End Point позволяет нам сделать именно это. Основной порт, используемый серверами Always-on-VPN, будет 53/udp, но вы будете отслеживать, скажем, 8433/tcp. В этом случае вам просто нужно ввести значение порта в поле Monitor End Point.

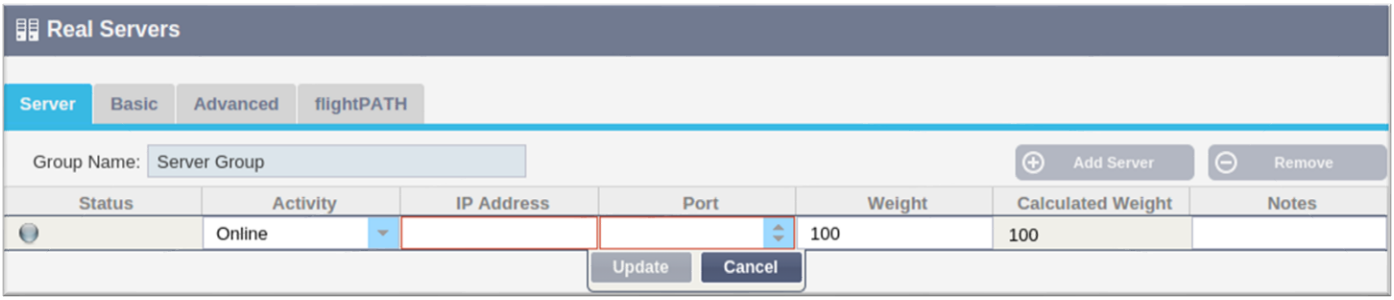
Создание виртуальных служб

Вы также можете создать субвиртуальные службы в случаях, когда вам нужно сбалансировать нагрузку, используя разные порты на одном VIP. Например, к серверам с одним и тем же виртуальным IP может осуществляться доступ по портам 80, 8088 и 443, поэтому для этого необходимо создать субвиртуальные службы.

- Выделите виртуальную службу, которую нужно скопировать.
- Нажмите Добавить виртуальную службу, чтобы перейти в режим редактирования строки.



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

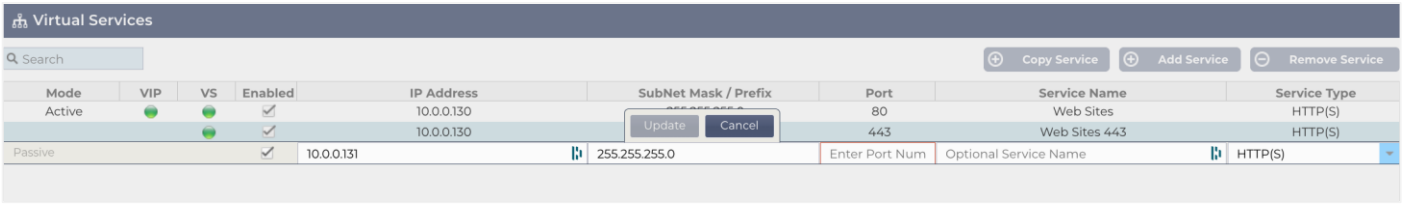


- Оставьте для параметра Активность сервера значение Онлайн - это означает, что нагрузка будет сбалансирована, если он пройдет стандартный мониторинг здоровья TCP Connect. Эту настройку можно изменить позже, если потребуется.
- Введите IP-адрес для сервера Real Server
- Введите номер порта для реального сервера
- Введите дополнительное имя для Real Server в поле Notes. Помните, что это поле примечаний используется для других, специфических целей, например в переменных flightPATH и т. д.
- Нажмите кнопку Обновить, чтобы сохранить изменения.
- Индикатор состояния сначала станет серым, затем зеленым, если монитор реального сервера работает успешно. Если монитор реального сервера не работает, он станет красным.
- 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.
- Щелкните поле IP-адреса для этой службы, чтобы перевести его в редактируемое состояние.



- 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, базовые настройки, расширенные настройки и правила flightPATH
- Выделите службу, которую нужно продублировать, и нажмите кнопку Копировать службу
- Появится редактор строк с мигающим курсором на колонке IP Address
- 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.

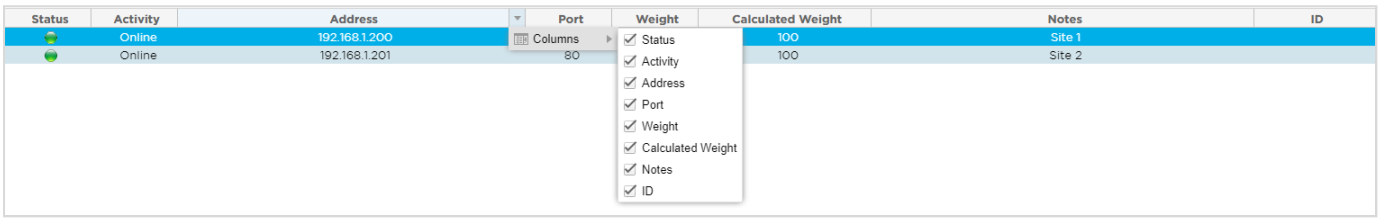
Фильтрация отображаемых данных

Поиск определенного термина

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

Выбор видимости столбцов

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



- Наведите курсор 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 Mode указывается роль высокой доступности, выбранная для текущего VIP. Сведения о режимах см. в разделе Система > Кластеризация>Роли.

Вариант	Описание
Активный	В режиме кластера значение этого поля - Active. Если в вашем центре обработки данных есть пара устройств ADC в режиме HA, одно из них будет отображаться как Active, а другое - как Passive. Если текущее устройство
Пассивный	Если АЦП выступает в качестве вторичного участника кластера, то в столбце "Режим" отображается "Пассивный".
Руководство	Роль Manual позволяет паре ADC работать в режиме Active-Active для разных виртуальных IP-адресов. В этом случае в столбце Primary рядом с каждым уникальным виртуальным IP будет стоять флажок, который можно выбрать 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

В этом столбце отображается информация о состоянии каждой виртуальной службы. Индикаторы выделены цветом и выглядят следующим образом:

LED	Значение
●	Онлайн
●	Failover-Standby. Эта виртуальная служба работает в режиме горячего резерва
●	Указывает на то, что "вторичка" задерживает "первичку".
●	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.
●	В автономном режиме. Серверы содержимого недоступны или не включены серверы содержимого
●	Состояние поиска
●	Не лицензировано или превышено количество лицензированных виртуальных IP-адресов

Включено

По умолчанию для этого параметра установлено значение Включено, и флажок отображается как отмеченный. Виртуальную службу можно отключить, дважды щелкнув по строке, сняв флажок, а затем нажав кнопку Обновить.

IP-адрес

Добавьте свой IPv4-адрес в десятичной точечной системе счисления или IPv6-адрес. Это значение является виртуальным IP-адресом (VIP) для вашей службы. 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. Например, "255.255.255.0". Вы также можете использовать значение подсети, например /24, или для IPv6 добавить свой префикс. Дополнительную информацию об IPv6 можно найти на сайте **HTTPS://EN.WIKIPEDIA.ORG/WIKI/IPV6_ADDRESS**

Порт

Добавьте номер порта, связанного с вашей службой. Порт может быть номером порта TCP или UDP. Например, TCP "80" для веб-трафика и TCP "443" для защищенного веб-трафика. Можно также указать диапазон значений, например 80-87.

В настоящее время невозможно использовать значения, разделенные запятыми, для указания несмежных значений портов.

Название услуги

Добавьте дружественное имя для идентификации вашей службы. Например, "Производственные веб-серверы". Это поле также используется при использовании GSLB.

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

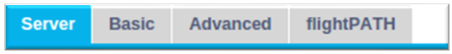
сервисов Layer 4. Службы уровня 4 просто балансируют трафик в соответствии с политикой балансировки нагрузки:

Тип услуги	Порт/протокол	Уровень обслуживания	Комментарий
TCP четвертого уровня	Любой порт TCP	Уровень 4	АЦП не изменяет никакой информации в потоке данных и выполняет стандартную балансировку нагрузки на трафик в соответствии с политикой балансировки нагрузки
Уровень 4 UDP	Любой порт UDP	Уровень 4	Как и в случае с Layer 4 TCP, ADC не изменяет никакой информации в потоке данных и выполняет стандартную балансировку трафика в соответствии с политикой балансировки нагрузки.
Уровень 4 TCP/UDP	Любой порт TCP или UDP	Уровень 4	Это идеальный вариант, если ваш сервис имеет основной протокол, например UDP, но будет возвращаться к TCP. ADC не изменяет никакой информации в потоке данных и выполняет стандартную балансировку нагрузки на трафик в соответствии с политикой балансировки нагрузки
DNS	TCP/UDP	Уровень 4	Используется для балансировки нагрузки на DNS-серверы.
HTTP (S)	Протокол HTTP или HTTPS	Уровень 7	АЦП может взаимодействовать, манипулировать и изменять поток данных с помощью flightPATH.
FTP	Протокол передачи файлов	Уровень 7	Использование раздельных 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 на серверы служб терминалов
RPC	Удаленный вызов процедур	Уровень 4	Используется при балансировке нагрузки на системы с помощью вызовов RPC
RPC/ADS	Exchange 2010 Статический RPC для службы адресной книги	Уровень 4	Используйте при балансировке нагрузки на серверы Exchange
RPC/CA/PF	Exchange 2010 Static RPC для клиентского доступа и общих папок	Уровень 4	Используйте при балансировке нагрузки на серверы Exchange

DICOM	Цифровая визуализация и коммуникации в медицине	Уровень 4	Используется при балансировке нагрузки на серверы, использующие протоколы DICOM

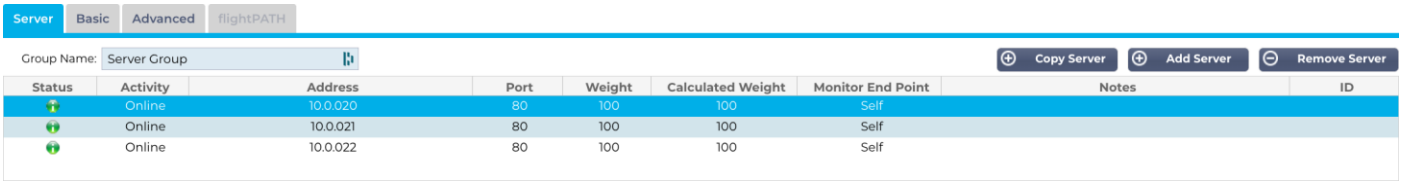
Настоящие серверы

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



Сервер

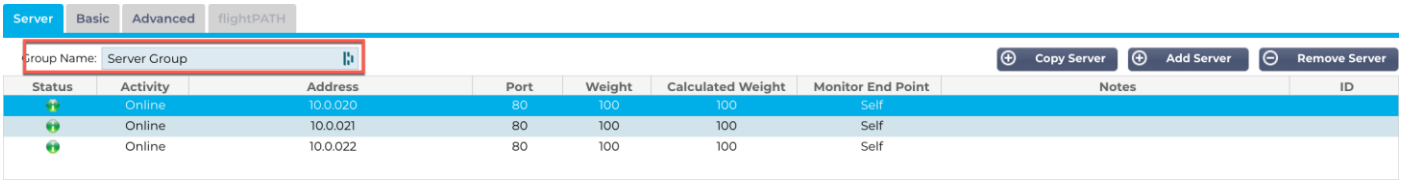
На вкладке Сервер содержатся определения реальных внутренних серверов, сопряженных с выбранной в данный момент виртуальной службой. В раздел "Реальные серверы" необходимо добавить хотя бы один сервер.



Добавить сервер

- Выберите соответствующий VIP, который вы ранее определили.
- Нажмите Добавить сервер
- Появится новая строка с мигающим курсором в колонке IP-адрес
- Введите IPv4-адрес вашего сервера в десятичной системе счисления. Реальный сервер может находиться в той же сети, что и виртуальная служба, в любой непосредственно подключенной локальной сети или в любой сети, к которой может быть проложен маршрут ADC. Пример "10.1.1.1".
- Перейдите в столбец Порт и введите номер порта TCP/UDP для вашего сервера. Номер порта может совпадать с номером порта виртуальной службы или быть другим номером порта для подключения обратного прокси. ADC автоматически переведет порт на этот номер.
- Перейдите в раздел "Примечания", чтобы добавить все необходимые сведения о сервере. Пример: "Веб-сервер IIS 1".

Название группы



После добавления серверов, составляющих набор для балансировки нагрузки, вы также можете указать 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 подключено
●	Состояние выводов
●	Не лицензировано или превышено количество лицензированных серверов Real Servers

Деятельность

Вы можете в любой момент изменить Активность реального сервера 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.
Дренаж	Все реальные серверы, назначенные как Drain, будут продолжать обслуживать существующие соединения, но не будут принимать новые соединения. Индикатор состояния будет мигать зеленым/синим, 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. Поведение слива можно изменить на вкладке "Дополнительные настройки".
Offline	Все реальные серверы, установленные как Offline, будут немедленно переведены в автономный режим и не будут принимать трафик.
В режиме ожидания	Все реальные серверы, установленные в качестве резервных, будут оставаться в автономном режиме до тех пор, пока **ВСЕ** серверы группы Online не пройдут проверку Server Health Monitor. Когда это произойдет, трафик будет приниматься группой Standby в соответствии с политикой балансировки нагрузки. Если один сервер в группе Online пройдет проверку Server Health Monitor, этот сервер Online будет получать весь трафик, а группа Standby перестанет получать трафик.

IP-адрес

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 доступным для редактирования, когда будет указана соответствующая политика балансировки нагрузки.

Вес по умолчанию для Real Server равен 100, а 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 "Наименьшее количество подключений", 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 метод балансировки нагрузки Round Robin, который ротирует запросы через набор серверов с балансировкой нагрузки, изменение весов влияет на то, как часто серверы выбираются в качестве целевых.

Если мы считаем, что политика балансировки нагрузки Fastest использует наименьшее время, необходимое для получения ответа, то регулировка 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.

Конечная точка мониторинга

Эта функция позволяет указать определенные конечные точки для мониторинга и, таким образом, определить состояние здоровья для записи Real Server. Вы можете оставить значение по умолчанию "Self", и тогда функция будет полагаться на мониторы реального сервера, указанные для виртуальной службы. Кроме того, можно указать IP-адрес, порт или IP-адрес:порт, что позволит вам контролировать другую конечную точку в вашей сети. В качестве примера можно привести, например, сервер базы данных, от которого зависят службы.

Примечания

Введите в поле Notes любые примечания, которые помогут описать определяемую запись. Например, "IIS Server1 - London DC". Это поле можно использовать для особых нужд в правилах flightPATH и GSLB.

ID

Эта настройка имеет несколько вариантов использования.

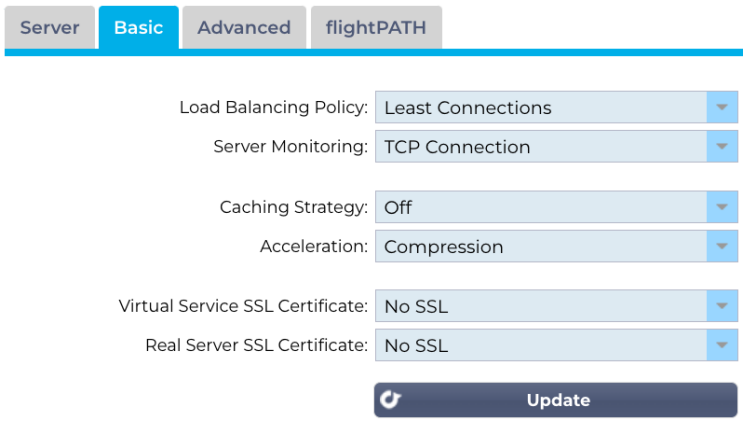
Настойчивость

Это значение можно использовать в сочетании с методом сохранения на основе идентификатора куки. Этот метод очень похож на метод сохранения на основе сессий PHP, но использует новую технику, называемую Cookie ID Based и cookie RegEx h=[^;]+. Метод сохранения на основе идентификатора Cookie будет использовать значение в поле ID для создания Cookie.

Использование flightPATH

Вы также можете использовать значение в этом поле для направления трафика и т. д.

Основные



Политика балансировки нагрузки

В раскрывающемся списке отображаются поддерживаемые в настоящее время политики балансировки нагрузки. Список политик балансировки нагрузки с пояснениями приведен ниже.

Least Connections
Fastest
Persistent Cookie
Round Robin
IP-Bound
IP List Based
Shared IP List Based
Classic ASP Session Cookie
ASP.NET Session Cookie
JSP Session Cookie
JAX-WS Session Cookie
PHP Session Cookie
RDP Cookie Persistence
Cookie ID Based

Вариант	Описание
Наименьшее количество соединений	Балансировщик нагрузки будет отслеживать количество текущих соединений с каждым Real Server. Сервер Real Server с наименьшим количеством соединений получает последующий новый запрос.
Самый быстрый	Политика балансировки нагрузки Fastest автоматически рассчитывает время ответа на все запросы для каждого сервера, сглаженное по времени. В столбце Вычисленный вес содержится автоматически вычисленное значение. Ручной ввод возможен только при использовании этой политики балансировки нагрузки.
Постоянный файл cookie	Уровень 7 Принадлежность/сохранение сеанса Режим балансировки нагрузки на основе списка IP-адресов используется для каждого первого запроса. ADC вставляет cookie в заголовки первого HTTP-ответа. После этого ADC использует клиентский cookie для маршрутизации трафика к одному и тому же внутреннему серверу. Этот файл cookie используется для сохранения трафика, когда клиент должен каждый раз обращаться к одному и тому же внутреннему серверу. Срок действия куки истечет через 2 часа, и соединение будет сбалансировано по

	нагрузке в соответствии с алгоритмом, основанным на списке IP-адресов. Это время истечения настраивается с помощью jetPACK.
Раунд Робин	Round Robin обычно используется в брандмауэрах и базовых балансировщиках нагрузки и является самым простым методом. Каждый реальный сервер получает новый запрос в порядке очереди. Этот метод подходит только в том случае, если вам нужно равномерно распределить нагрузку запросов на серверы; примером могут служить поисковые веб-серверы. Однако если вам нужно сбалансировать нагрузку в зависимости от нагрузки на приложение или сервер, или даже обеспечить использование одного и того же сервера для сеанса, метод Round Robin не подходит.
IP Bound	Layer 3 Session Affinity/Persistence Cookie. В этом режиме IP-адрес клиента служит основой для выбора сервера Real Server, который получит запрос. Это действие обеспечивает постоянство. В этом режиме могут работать протоколы HTTP и Layer 4. Этот метод полезен для внутренних сетей, где топология сети известна, и вы можете быть уверены в отсутствии "суперпрокси" выше по течению. При использовании Layer 4 и прокси-серверов все запросы могут выглядеть так, как будто они поступают от одного клиента, и поэтому нагрузка будет неравномерной. В HTTP информация заголовка (X-Forwarder-For) используется при наличии, чтобы справиться с прокси.
Список IP-адресов	Соединение с сервером 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.
Список общих IP-адресов	Этот тип службы доступен только в том случае, если для параметра Режим подключения установлено значение Прямое возвращение сервера. Он был добавлен в основном для поддержки балансировки нагрузки VMware.
Постоянный файл cookie	Уровень 7 Принадлежность/сохранение сеанса Режим балансировки нагрузки на основе списка IP-адресов используется для каждого первого запроса. ADC вставляет cookie в заголовки первого HTTP-ответа. После этого ADC использует клиентский cookie для маршрутизации трафика к одному и тому же внутреннему серверу. Этот файл cookie используется для сохранения трафика, когда клиент должен каждый раз обращаться к одному и тому же внутреннему серверу. Срок действия куки истечет через 2 часа, и соединение будет сбалансировано по нагрузке в соответствии с алгоритмом, основанным на списке IP-адресов. Это время истечения настраивается с помощью jetPACK.
Классический файл cookie сеанса ASP	Active Server Pages (ASP) - это технология Microsoft, используемая на стороне сервера. При выборе этой опции ADC будет поддерживать постоянство сеанса на одном и том же сервере, если куки ASP обнаружены и находятся в списке известных куки. При обнаружении нового файла cookie ASP нагрузка будет сбалансирована с использованием алгоритма наименьших подключений.
Cookie сеанса ASP.NET	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 будут обнаружены и найдены в списке известных куки. При обнаружении нового файла cookie ASP нагрузка будет сбалансирована с использованием алгоритма наименьших подключений.
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.
JAX-WS Session Cookie	Веб-службы Java (JAX-WS) - это технология Oracle для сервера. При выборе этого режима ADC будет сохранять сеанс на одном и том же сервере, если куки JAX-WS будут обнаружены и найдены в списке известных куки. При

	обнаружении нового файла cookie JAX-WS нагрузка будет сбалансирована с использованием алгоритма наименьших подключений.
Cookie сеанса PHP	Personal Home Page (PHP) - это серверная технология с открытым исходным кодом. При выборе этого режима ADC будет сохранять сеанс на одном и том же сервере при обнаружении куки PHP.
Постоянство файлов cookie 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 соединение с сервером можно поддерживать 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 зашифрованный IP, а ID реального сервера (считывается при загрузке). Значение по умолчанию - CookieIDName="h"; однако если в расширенных настройках виртуального сервера есть значение переопределения, используйте его. **ПРИМЕЧАНИЕ**: Мы перезаписываем выражение cookie выше, чтобы заменить h= новым значением, если это значение установлено. Последнее замечание: 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 несколько предустановленных методов мониторинга реального сервера.

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

Важно выбрать правильный монитор для службы. Например, если Real Server - это RDP-сервер, монитор 200OK не имеет значения. В равной степени выбор TCP Connection и 200OK также не имеет смысла, поскольку для работы 200OK необходимо рабочее TCP-соединение. Если вы не знаете, какой монитор выбрать, то для начала лучше всего выбрать TCP Connection

Вы можете выбрать несколько мониторов, поочередно щелкая 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 на приборной панели появятся события, как показано на рисунке ниже:

Мы видим, что уровень 3 Ping и уровень 4 TCP Connect прошли успешно, если мы посмотрим на верхнюю строку, но уровень 7 200OK потерпел неудачу. Эти результаты мониторинга дают достаточно информации, чтобы указать, что с маршрутизацией все в порядке и на соответствующем порту запущена служба, но веб-сайт не отвечает корректно на запрошенную

страницу. Теперь пришло время взглянуть на веб-сервер и раздел Library > Real Server Monitor (Библиотека > Монитор реального сервера), 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, и 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 корректный эхо-ответ, ADC считает, что сервер Real Server работает, и пропуск трафика к серверу продолжается. Кроме того, служба будет доступна 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, но сервисы 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 нужно проверить, доступен ли на сервере порт службы UDP, 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 терминальным сервером Microsoft.
200 OK	В этом методе инициализируется TCP-соединение с реальным сервером. После успешного соединения АЦП отправляет реальному серверу HTTP-запрос. Ожидается HTTP-ответ и проверяется наличие кода ответа "200 OK". АЦП считает, что реальный сервер работает, если получен код ответа "200 OK". Если ADC не получает код ответа "200 OK" по какой-либо причине, включая таймауты, невозможность подключения и другие причины, ADC отмечает Real Server недоступным. Этот метод мониторинга применим только для типов служб HTTP и ускоренный HTTP. Если для HTTP-сервера используется тип службы уровня 4, его можно использовать, 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 "Ассоциативный запрос" Echoscu. Общение, включающее "Associate Accept" от сервера контента, передачу небольшого количества данных, затем "Release Request" и "Release Response", успешно завершает монитор. Если монитор не завершается успешно, то реальный сервер считается отключенным по какой-либо причине.
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.

Для настройки подробных параметров кэширования обратитесь к странице Настройка кэша. Обратите внимание, что когда кэширование применяется к VIP с типом службы Accelerated "HTTP", сжатые объекты не кэшируются.

Вариант	**Описание**
Хозяин	Кэширование на хост основано на приложении для каждого имени хоста. Для каждого домена/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 виртуальный сервис. Эта опция является специализированной настройкой для использования с несколькими клонами одного сайта.

Ускорение

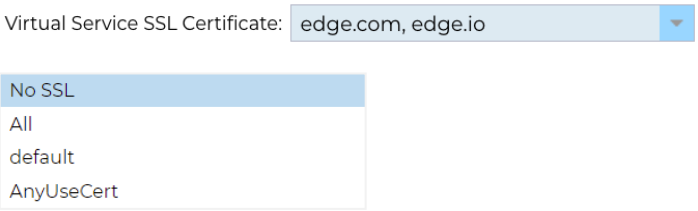
Вариант	**Описание**
С сайта	Отключите сжатие для виртуальной службы
Компрессия	При выборе этого параметра включается сжатие для выбранной виртуальной службы. ADC динамически сжимает поток данных, передаваемый клиенту по запросу. Этот процесс применяется только к объектам, содержащим заголовок content-encoding: gzip. Пример содержимого включает HTML, CSS или JavaScript. Вы также можете исключить определенные типы содержимого с помощью раздела "Глобальные исключения".

Примечание: Если объект кэшируемый, 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 подтверждено.

Сертификат SSL виртуальной службы (шифрование между клиентом и ADC)

По умолчанию установлено значение Нет SSL. Если тип вашей службы - "HTTP", вы можете выбрать сертификат из выпадающего списка, чтобы применить его к виртуальной службе. В этом списке появятся сертификаты, которые были созданы или импортированы.

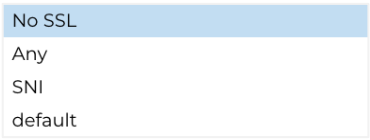
Можно также выделить несколько сертификатов для применения к службе. Эта операция автоматически включит расширение SNI, чтобы разрешить сертификат на основе "Доменного имени", запрошенного клиентом.



Вариант	**Описание**
Нет SSL	Трафик от источника к ADC не шифруется.
Все	Загружает все доступные сертификаты для использования
По умолчанию	Эта опция приводит к применению локально созданного сертификата "По умолчанию" на стороне канала браузера. Используйте этот параметр для проверки SSL, если сертификат не был создан или импортирован.

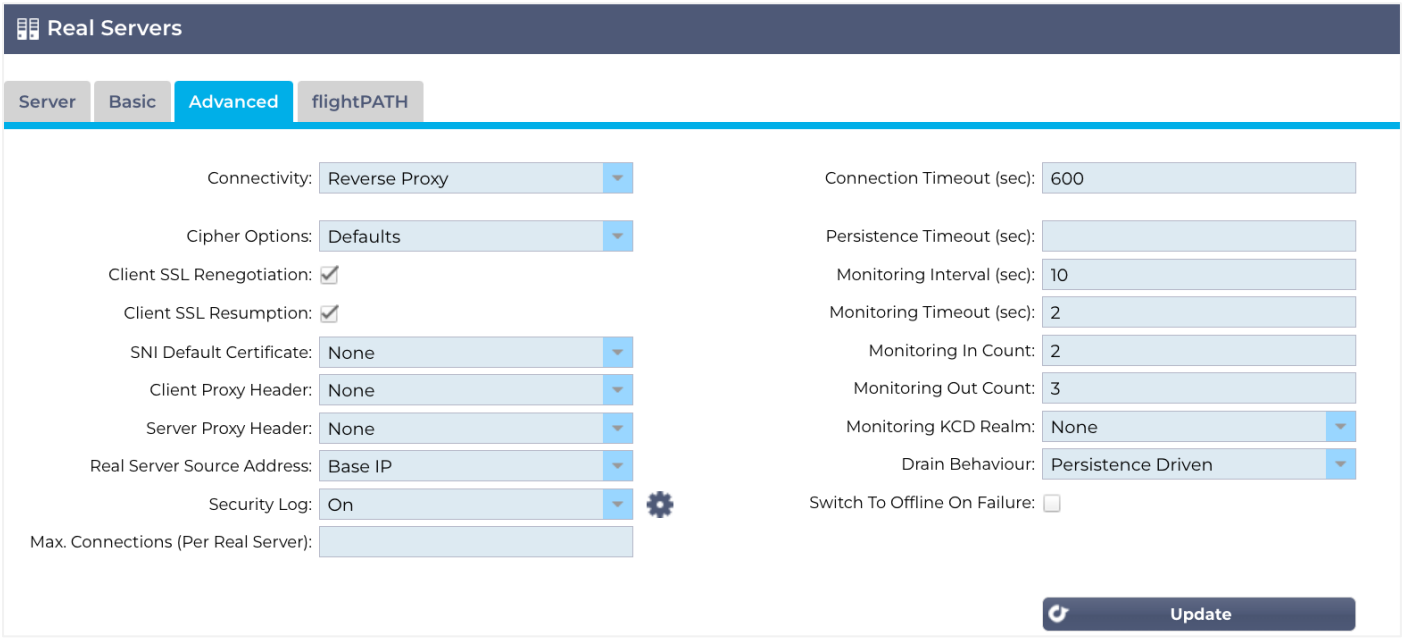
SSL-сертификат реального сервера (шифрование между АЦП и реальным сервером)

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 ADC к Real Server не шифруется. Выбор сертификата на стороне браузера означает, что "No SSL" может быть выбран на стороне клиента для обеспечения так называемой "разгрузки SSL".
Любой	ADC выступает в роли клиента и принимает любой сертификат, представленный Real Server. При выборе этой опции трафик от ADC к реальному серверу шифруется. Используйте параметр "Любой", когда сертификат указан на стороне виртуальной службы, обеспечивая так называемое "SSL Bridging" или "SSL Re-Encryption".
SNI	SNI, или Server Name Indication, - это расширение сетевого протокола TLS, с помощью которого клиент указывает имя хоста, к которому он пытается подключиться, в начале процесса передачи данных . Эта настройка позволяет ADC представлять несколько сертификатов на одном виртуальном IP-адресе и TCP-порту.
По умолчанию	Здесь отображаются все созданные вами самоподписанные сертификаты.

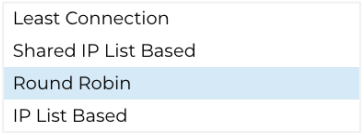
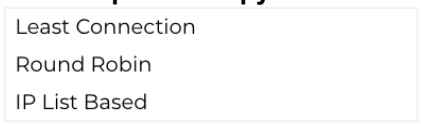
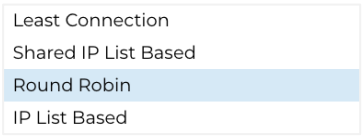
Расширенный



Возможность подключения

Ваша виртуальная служба может быть настроена на различные типы подключения. Пожалуйста, выберите режим подключения, который будет применяться к сервису.

Вариант	**Описание**
Обратный прокси-сервер	Обратный прокси - это значение по умолчанию, которое использует сжатие и кэширование при использовании на уровне 7. На уровне 4 обратный прокси работает без кэширования и сжатия. В этом режиме ваш ADC действует как обратный прокси и становится адресом источника, который видят реальные серверы.
Прямое возвращение сервера	Direct Server Return или DSR, также известный как DR - Direct Routing, позволяет серверу, находящемуся 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. **Этот режим можно использовать только с типами служб TCP, UDP и TCP/UDP.** Политики сохранения балансировки нагрузки также ограничены наименьшим количеством соединений, общим списком IP-адресов, круговым обходом и списком IP-адресов.  Использование DSR также требует внесения изменений в Real Server. Обратитесь к разделу Изменения реального сервера.
NAT	По умолчанию ADC использует IP-адрес ADC в качестве IP-адреса источника, а серверы Real Server отправляют ответ обратно в ADC для возврата клиенту. Это хорошо почти во всех обстоятельствах, но есть сценарии, когда реальный сервер должен видеть исходный IP-адрес клиента, а не ADC. Когда применяется режим NAT, ADC получает входящий запрос, а затем отправляет его на реальный сервер после того, как изменит IP-адрес источника на адрес виртуальной службы (VIP-адрес). **Этот режим можно использовать только со следующими политиками балансировки нагрузки:** 
Шлюз	Режим шлюза позволяет направлять весь трафик через ADC, позволяя направлять Real Servers через ADC в другие сети через виртуальные сервисы ADC или аппаратные интерфейсы. Использование устройства в качестве шлюза для серверов Real Servers идеально при работе в многоинтерфейсном режиме. Политики сохранения балансировки нагрузки также ограничены наименьшим количеством соединений, общим списком IP-адресов, круговым обходом и списком IP-адресов.  Этот метод требует, чтобы Real Server установил шлюз по умолчанию на адрес локального интерфейса ADC (eth0, eth1 и т. д.). Обратитесь к разделу "Изменения реального сервера". ***Обратите внимание, что режим шлюза не поддерживает обход отказа в кластерной среде.***

Параметры шифра

Шифры составляют основу криптографии SSL и чрезвычайно важны для успешной и безопасной доставки веб-контента и приложений.

ADC содержит встроенный набор шифров по умолчанию, включающий самые современные и безопасные из доступных для использования.

Бывают случаи, когда пользователь хочет объявить о наличии определенного набора шифров, и ADC позволяет создавать такие шифры с помощью написанных пользователем jetPACKS. Написанные пользователями jetPACKS могут быть импортированы в ADC через Configuration > Software, а затем доступны для выбора с помощью меню Cipher Options.

Варианты шифров индивидуальны для каждого VIP-клиента, обеспечивая высокую гибкость и безопасность.

Дополнительную информацию о параметрах шифра см: *Cipher*

Переговоры клиента SSL

Отметьте этот флажок, если хотите разрешить инициированное клиентом повторное согласование SSL. Чтобы предотвратить возможные DDOS-атаки на уровень SSL, снимите этот флажок.

Возобновление работы SSL клиента

Отметьте этот флажок, если хотите включить возобновление сеансов сервера SSL, добавленных в кэш сеансов. Когда клиент предлагает повторно использовать сессию, сервер попытается использовать ее повторно, если она будет найдена. Если флажок "Возобновление" 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 установлено значение Нет, что приведет к обрыву соединения в случае отсутствия точного совпадения. Выберите любой из установленных сертификатов из выпадающего списка, чтобы представить его в случае, если точное совпадение SSL-сертификата не удастся.

Протокол прокси

Протокол Proxy Protocol разработан для того, чтобы сетевые прокси-серверы могли передавать информацию о клиентском соединении (например, IP-адрес и номер порта) на принимающий сервер. Этот протокол особенно полезен в сценариях, когда необходимо сохранить фактический IP-адрес конечного пользователя при маршрутизации трафика через балансировщик нагрузки или обратный прокси. Он помогает сохранить исходный IP-адрес клиента для ведения журнала, статистики или в целях безопасности, повышая возможность принятия обоснованных решений на основе истинного источника трафика.

Заголовок клиентского прокси-сервера

Заголовок клиентского прокси означает заголовок, добавляемый ADC к запросу клиента и содержащий исходную информацию о соединении (например, IP-адрес и порт клиента). Это очень важно в средах, где ADC выступает в роли прокси, а серверу необходимо знать исходные данные клиента для таких целей, как ведение журнала, оценка безопасности и поддержание специфического для клиента поведения. Заголовок Client Proxy Header гарантирует, что, несмотря на посредническую роль ADC, сервер может точно определить исходные данные соединения клиента и взаимодействовать с ним.

Опции включают:

Вариант	**Описание**
Нет	Если заголовок Proxy отсутствует или не поддерживается в текущем типе сервиса.
Удалить	Удаляет заголовок Proxy из TCP-пакета
Вперед	Передает заголовок Proxy на сервер

Заголовок прокси-сервера

Существует две версии заголовков серверного прокси: Версия 1 и Версия 2.

Вариант	Описание
Версия 1	• Текстовый формат, простой в реализации и отладке. • Предоставляет основную информацию о подключении клиента, включая IP-адрес источника, IP-адрес назначения, порт источника и порт назначения. • Строка протокола добавляется в начало TCP-соединения, что делает его удобочитаемым, но несколько менее эффективным с точки зрения производительности по сравнению с двоичными форматами.
Версия 2	• Двоичный формат, разработанный для повышения производительности и эффективности. • Расширяет информацию, которая может быть передана о соединении, поддерживая дополнительные данные, такие как семейство адресов и специфическая информация о протоколе. • Обеспечивает лучшую совместимость с современными сетевыми протоколами и функциями, включая поддержку IPv6 и транспортных протоколов за пределами TCP.

Параметры заголовка Client Proxy Header и Server Proxy header доступны только для типов служб Layer 4 и Layer 7 HTTP.

Адрес источника реального сервера

Эта настройка работает вместе с обратным прокси и службой Layer 4 TCP, Layer 4 UDP или HTTP(S). Настройка предоставляет три варианта, которые вы можете выбрать.

Вариант	Описание
Базовый IP-адрес (по умолчанию)	В качестве исходного IP-адреса запроса используется eth0 или базовый IP-адрес АЦП.
Виртуальный IP	Используется виртуальный IP-адрес службы.
<IP-адрес>	Позволяет указать IP-адрес, который является частью ADC. Это может быть другой сетевой интерфейс или другой VIP.

Журнал безопасности

Значение "Вкл." установлено по умолчанию и используется для каждого сервиса, позволяя регистрировать информацию об аутентификации в журналах W3C. Нажав на значок Cog, вы перейдете на страницу System > Logging, где можно проверить настройки протоколирования W3C.

Макс. Соединения

Ограничивает количество одновременных подключений Real Server и задается для каждой службы. Например, если вы установите значение 1000 и у вас будет два сервера Real Server, ADC ограничит **каждый** сервер Real Server до 1000 одновременных подключений. 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 числа подключений. То, что вы установите здесь, зависит от ресурсов вашей системы.

Таймаут соединения

По умолчанию таймаут соединения составляет 600 секунд или 10 минут. Этот параметр регулирует время, в течение которого соединение будет прерываться при отсутствии активности. Уменьшите

этот параметр для недолговечного веб-трафика без статических данных, который обычно составляет 90 секунд или меньше. Увеличьте этот параметр для соединений с активным состоянием, таких как RDP, до 7200 секунд (2 часа) или более, в зависимости от вашей инфраструктуры. Пример с таймаутом RDP означает, что если пользователь неактивен в течение 2 часов или менее, соединения останутся открытыми.

Таймаут постоянства

Параметр Persistence Timeout в балансировщиках нагрузки определяет продолжительность сохранения балансировщиком нагрузки информации о сеансе для клиента. Это гарантирует, что последующие запросы от одного и того же клиента будут направлены на один и тот же внутренний сервер, что способствует согласованности сеансов и взаимодействию с учетом состояния. По истечении указанного периода без дальнейшей активности клиента информация о сессии удаляется, и новые запросы могут быть направлены на другой сервер.

Интервал мониторинга

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 таймаута - это время, в течение которого ADC будет ждать ответа сервера на запрос соединения. По умолчанию это значение равно 2 с. Увеличьте это значение для загруженных серверов.

Мониторинг в графе

Значение по умолчанию для этого параметра равно 2. Значение 2 означает, что сервер Real Server должен пройти две успешные проверки работоспособности, прежде чем он будет запущен. Увеличение этого значения повышает вероятность того, что сервер сможет обслуживать трафик, но в зависимости от интервала времени 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 трижды потерпеть неудачу, 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.

Мониторинг KCD Realm

Этот параметр позволяет включить мониторинг Kerberos Constrained Delegation Realm, который вы установили в определениях Kerberos. См. раздел Аутентификация > Kerberos.

Поведение при сливе

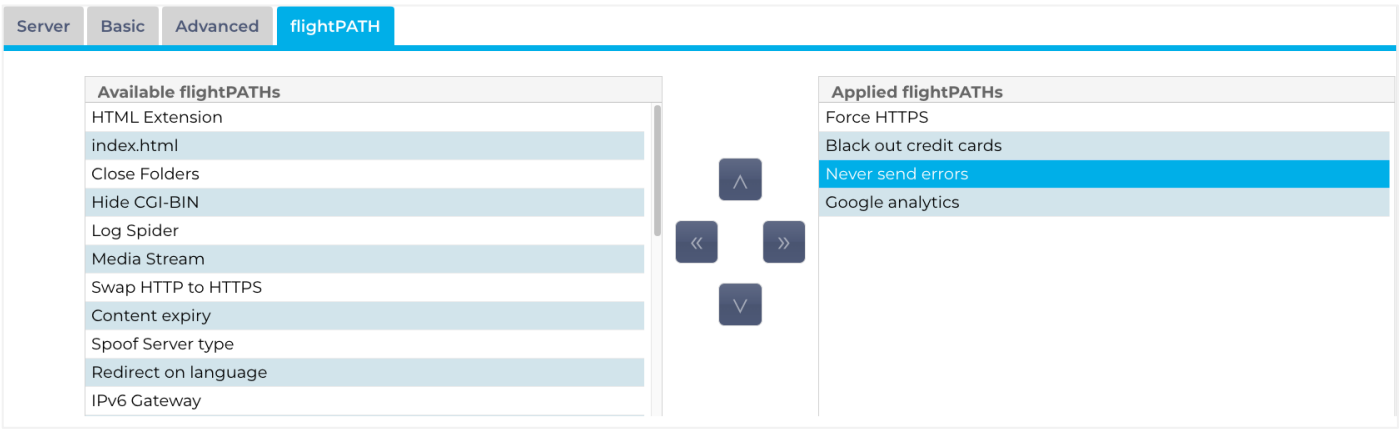
Когда какой-либо реальный сервер переводится в режим Drain, всегда лучше иметь возможность контролировать поведение трафика, отправляемого на него. Меню Drain Behaviour позволяет выбрать поведение трафика для каждой виртуальной службы. Возможны следующие варианты:

Вариант	Описание
Управляемые постоянством	Это выбор по умолчанию. Всякий раз, когда пользователь посещает сессию персистентности, она расширяется. При круглосуточном использовании возможно, что слив никогда не произойдет. Однако если количество соединений с реальным сервером достигает 0, слив завершается, сессии сохранения удаляются, а все посетители заново балансируются при следующем соединении.
Миграция посетителей	Постоянная сессия игнорируется при повторном подключении - (устаревшее поведение до 2022 года) Новые TCP-соединения (независимо от того, являются ли они частью существующей сессии или нет) всегда устанавливаются с реальным сервером в режиме онлайн. Если сессия сохранения была связана с истощающимся реальным сервером, она перезаписывается. Виртуальная служба будет фактически игнорировать постоянство для любых новых соединений, и они будут перераспределены на новый сервер.
Сессии на пенсии	Постоянные сессии не продлеваются. Входящие пользовательские соединения будут назначены на желаемый сервер, но их сессия сохранения не будет продлена. Поэтому по истечении времени сессии персистенции они будут рассматриваться как новые соединения и перемещаться на другой сервер.

Переход в автономный режим при сбое

Если этот флажок установлен, реальные серверы, не прошедшие проверку здоровья, переводятся в автономный режим и могут быть запущены только вручную.

flightPATH



flightPATH - это технология управления трафиком, разработанная компанией Edgenexus и доступная исключительно в 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 нужной цели. Эти особенности делают flightPATH

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

flightPATH доступен только для использования с HTTPS-соединениями, и этот раздел не отображается, если тип виртуального сервиса не HTTP.

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

Примените доступное правило, перетащив его с левой стороны на правую, или выделите правило и нажмите стрелку вправо, чтобы переместить его на правую сторону.

Порядок выполнения важен и начинается с того, что первым выполняется верхнее правило. Чтобы изменить порядок выполнения, выделите правило и перемещайте его вверх и вниз с помощью стрелок.

Важно понимать, что правила flightPATH в этом разделе ADC работают по принципу булева **ИЛИ**, в то время как условия и действия в области определения flightPATH работают по принципу **И.**

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

Добавлять, удалять и редактировать правила flightPATH можно в разделе "Настройка flightPATH" данного руководства.

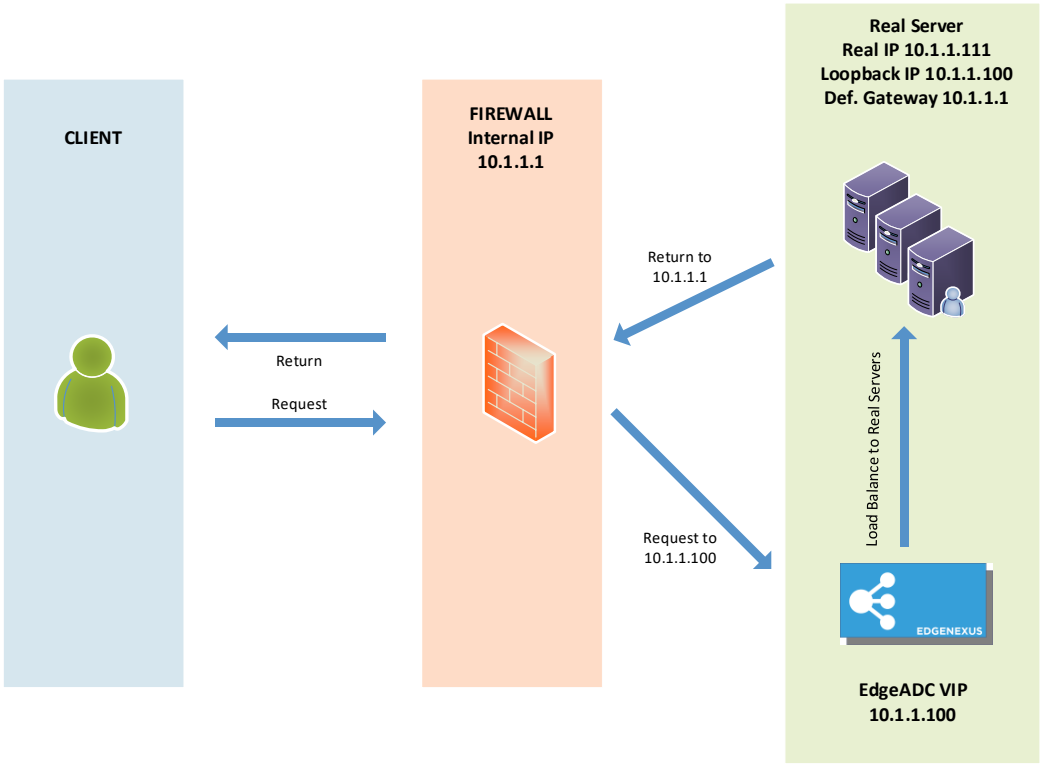
Реальные изменения сервера для прямого возвращения сервера

Direct Server Return или DSR, как его еще называют (DR - Direct Routing в некоторых кругах), позволяет серверу, находящемуся за ADC, отвечать клиенту напрямую, минуя ADC при ответе. DSR подходит только для использования с балансировкой нагрузки на четвертом уровне. Кэширование и сжатие не доступны, если они включены.

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

Как это работает

- Клиент отправляет запрос в EdgeADC VIP.
- Запрос, полученный EdgeADC
- Запрос направляется на серверы контента
- Ответ отправляется непосредственно клиенту без прохождения через EdgeADC



Необходимая конфигурация сервера содержимого

Общие сведения

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

Windows

- Сервер содержимого должен иметь loopback или Alias, настроенный с IP-адресом канала или VIP
    - Метрика сети должна быть 254, чтобы предотвратить ответ на ARP-запросы

- Добавление адаптера обратной связи в Windows Server 2012 - нажмите здесь
- Добавление адаптера обратной связи в Windows Server 2003/2008 - нажмите здесь

- Выполните следующие действия в командной строке для каждого сетевого интерфейса, настроенного на серверах Windows Real Servers

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

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

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

Linux

- Добавьте постоянный интерфейс loopback
- Отредактируйте "/etc/sysconfig/network-scripts".

ifcfg-lo:1
DEVICE=lo:1
IPADDR=x.x.x.x
NETMASK=255.255.255.255
BROADCAST=x.x.x.x
ONBOOT=да

- Отредактируйте файл "/etc/sysctl.conf".

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

- Выполните команду "sysctl - p".

Изменения реального сервера - режим шлюза

Режим шлюза позволяет направлять весь трафик через ADC, что позволяет направлять трафик, исходящий от серверов контента, в другие сети через интерфейсы на устройстве ADC. Использовать устройство в качестве шлюза для серверов контента следует при работе в многоинтерфейсном режиме.

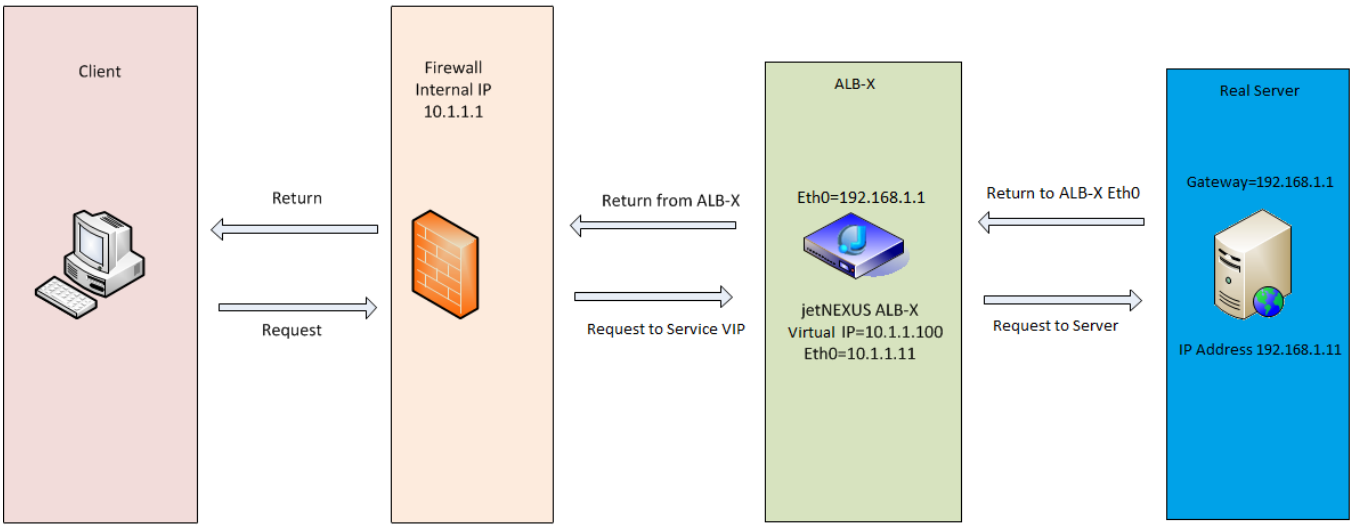
Как это работает

- Клиент отправляет запрос на EdgeADC.
- Запрос получен EdgeADC
- Запрос, отправленный на серверы контента
- Ответ отправлен в EdgeADC
- ADC направляет ответ клиенту

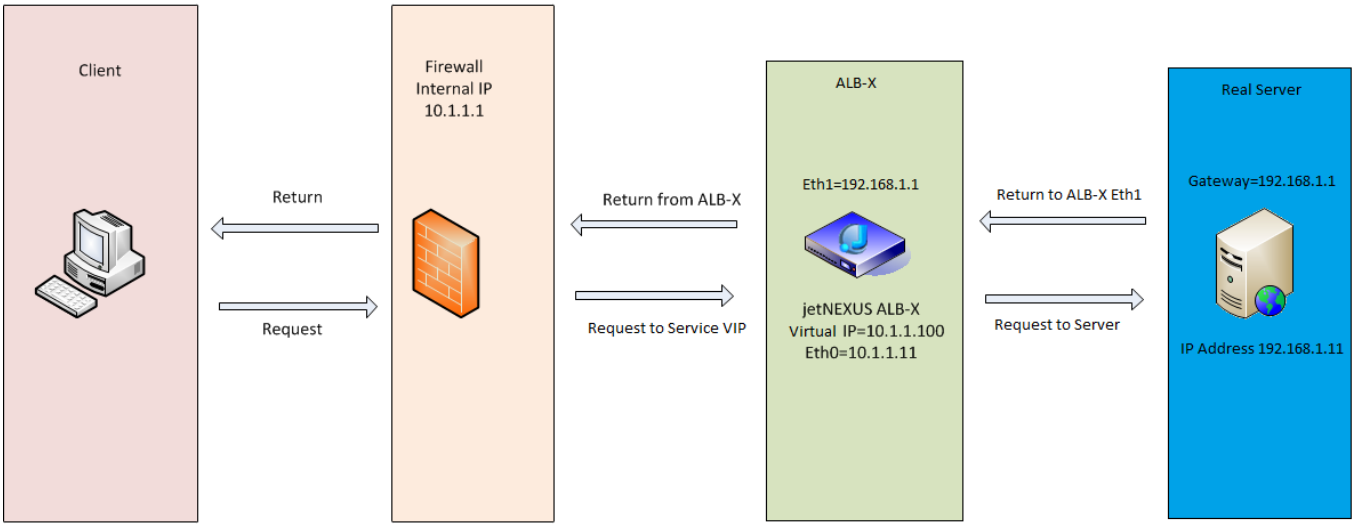
Необходимая конфигурация сервера содержимого

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

Пример с одной рукой



Пример с двумя руками

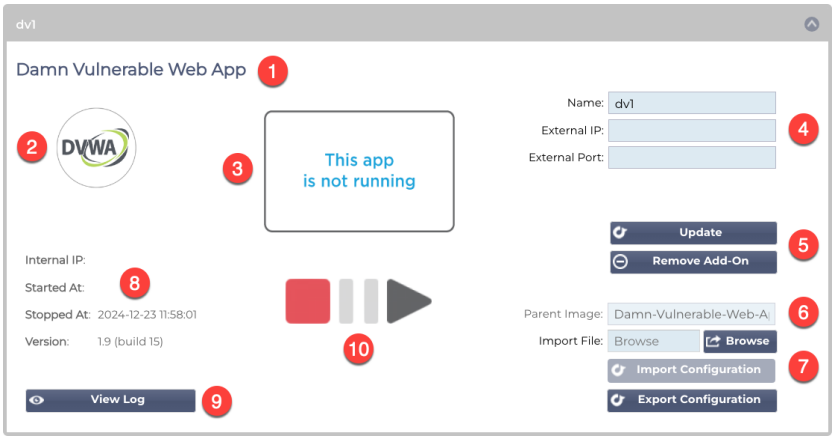


Библиотека

Дополнения

Дополнения - это приложения, которые загружаются в виде контейнеров и работают в изолированном режиме внутри ADC. Примерами дополнений могут быть брандмауэр приложений или даже микроэкземпляр самого ADC.

Приложение развертывается в разделе Add-Ons с помощью страницы Apps, как описано в этом руководстве. После развертывания приложение выглядит следующим образом.



Как видно из приведенного выше изображения, есть несколько элементов, которые выделены.

Артикул	Описание
❶	Название приложения
❷	Иконка приложения
❸	Отображение работы приложения. Если приложение запущено, на экране будет отображаться его миниатюра.
❹	Подробности доступа: **Имя**: Это внутреннее имя, которое вы используете для ссылки на приложение в разделе виртуальных служб. Невозможно ссылаться на приложение, используя его IP-адрес. Только буквенно-цифровое, без пробелов. **Внешний IP**: Это IP-адрес, который вы должны предоставить приложению. Он будет входить в подсеть вашей сети. **Внешний порт**: Это важное поле. Вам нужно будет указать порты, которые будут использоваться для доступа к приложению. Если к приложению обращается внешний трафик, необходимо указать его, используя следующую нотацию: 53/tcp или 53/udp. Кроме того, необходимо указать порт пользовательского интерфейса для приложения. Они указаны во всплывающей подсказке поля для каждого приложения.
❺	Кнопка "Обновить": После заполнения данных, указанных на сайте❸ , нажмите эту кнопку, чтобы подтвердить введенные данные и настроить приложение. Кнопка Remove Add-On используется для удаления приложения из раздела Apps. Чтобы удалить приложение, убедитесь, что все ссылки на него также удалены перед попыткой удаления.
❻	Parent Image - это информационное поле, которое не используется с точки зрения пользователя.
❼	Импорт и экспорт конфигурации важен для сохранения резервной копии настроек. Используйте это для выполнения функции импорта и экспорта.
❽	Сведения о запуске содержат информацию об IP-адресе внутреннего API, времени запуска и остановки, а также номере версии приложения.
❾	Эта кнопка позволяет загрузить и просмотреть журнал. В первую очередь она используется при необходимости открыть тикет в службу поддержки.
❿	Управление приложением осуществляется с помощью этих кнопок. Красная=остановлено, золотая=приготовлено и зеленая=работает.

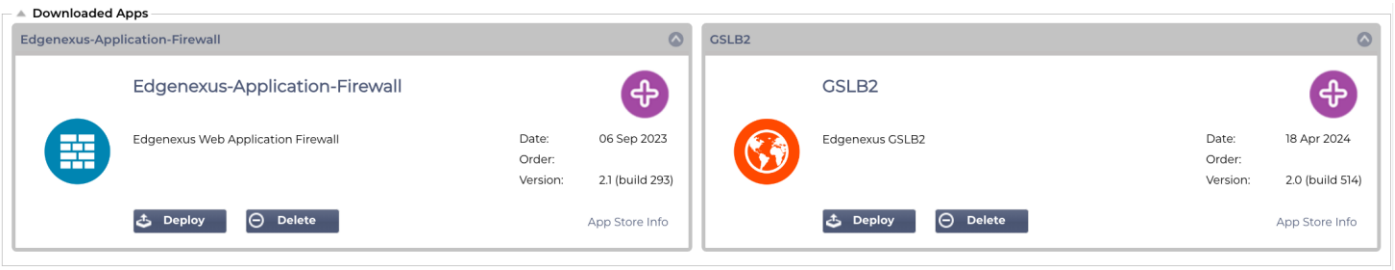
Приложения

Раздел Apps имеет несколько подразделов, в которых хранятся приложения, доступные для использования на ADC. Это фильтр, загруженные приложения и приобретенные приложения.

Фильтр

Фильтр позволяет отфильтровать приложения/инструменты по их типу.

Загруженные приложения

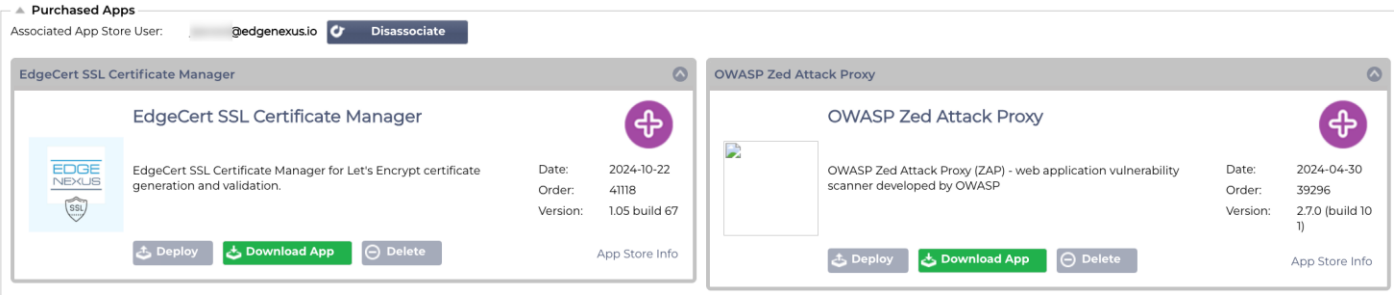


В этом разделе содержатся приложения, которые были загружены на ADC. Вы могли загрузить их на локальный рабочий стол, а затем загрузить на ADC, или загрузить их через встроенный портал App Store.

Каждое приложение оснащено двумя кнопками, а также данными, указывающими на номер версии и дату ее выпуска.

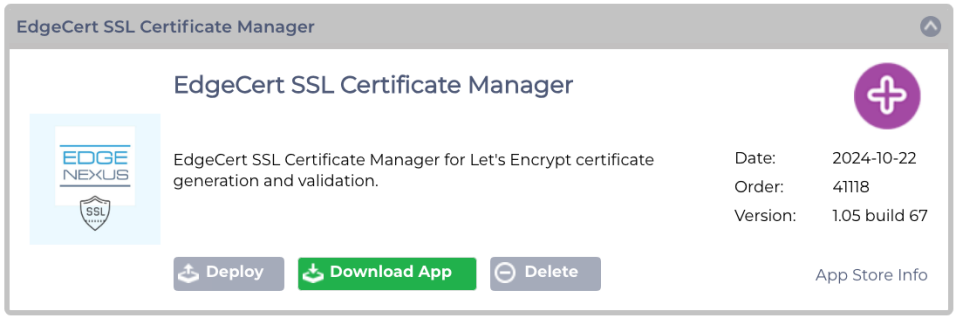
Кнопка Deploy развернет приложение в виде защищенного контейнера, а кнопка Delete удалит приложение из ADC.

Приобретенное приложение



Первое, что вы заметите, - это ассоциированный пользователь App Store и связанная с ним кнопка. Вам нужно будет войти в систему, используя учетные данные App Store, чтобы ADC был связан с App Store. Под ней вы найдете приложения, связанные с вашей учетной записью.

Войдя в App Store, напрямую или через встроенный портал, вы можете приобрести приложения. Они указаны в этом разделе и могут быть загружены в ADC для развертывания.



Каждое приложение имеет несколько кнопок: Развернуть, Загрузить приложение и Удалить. Кроме того, справа есть ссылка App Store Info, которая приведет вас на соответствующую страницу App Store и покажет информацию об аддоне.

Развернуть

В разделе Apps (Приложения) в разделе Add-Ons отображаются приобретенные, загруженные и развернутые приложения. После развертывания приложение появится в разделе "Загруженные".

Скачать приложение

Приложение можно загрузить из App Store, нажав на эту кнопку.

Удалить

Если вы хотите удалить загруженное приложение.

Аутентификация

На странице Библиотека> Аутентификация можно настроить серверы аутентификации и создать правила аутентификации.

Настройка аутентификации - рабочий процесс

Чтобы применить аутентификацию к вашей службе, выполните следующие шаги.

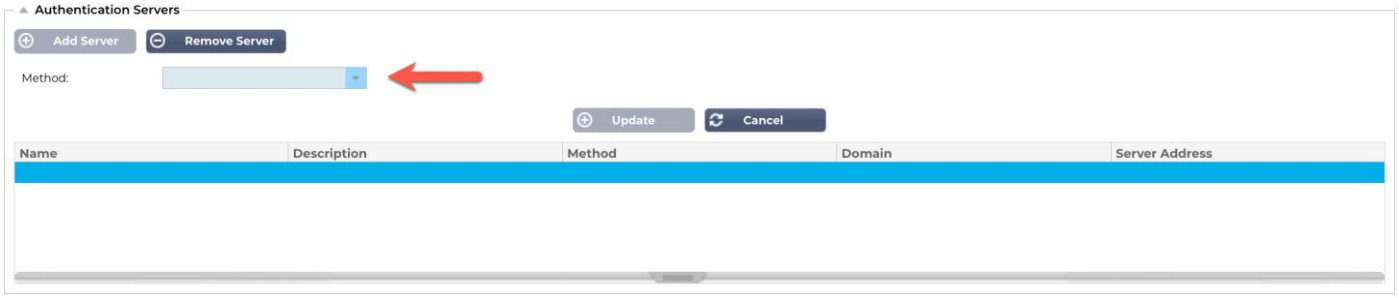
1. Создайте сервер аутентификации.
2. Создайте правило аутентификации, использующее сервер аутентификации.
3. Создайте правило flightPATH, которое использует правило аутентификации.
4. Примените правило flightPATH к службе

Серверы аутентификации

Чтобы настроить рабочий метод аутентификации, сначала нужно создать сервер аутентификации.

На первом этапе необходимо выбрать метод аутентификации.

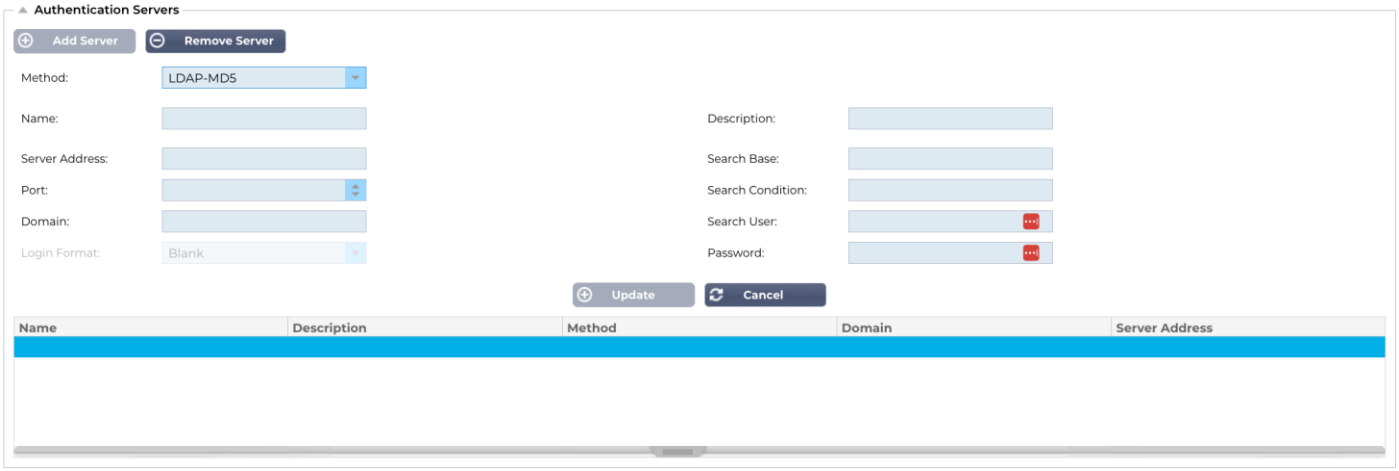
- Нажмите Добавить сервер.
- Выберите метод из выпадающего меню.



Функция Authentication Server является динамической и отображает только те поля, которые необходимы для выбранного вами метода аутентификации.

- Заполните поля точно, чтобы обеспечить правильное подключение к серверам.

Опции для LDAP, LDAP-MD5, LSAPS, LDAPS-MD5, Radius и SAML

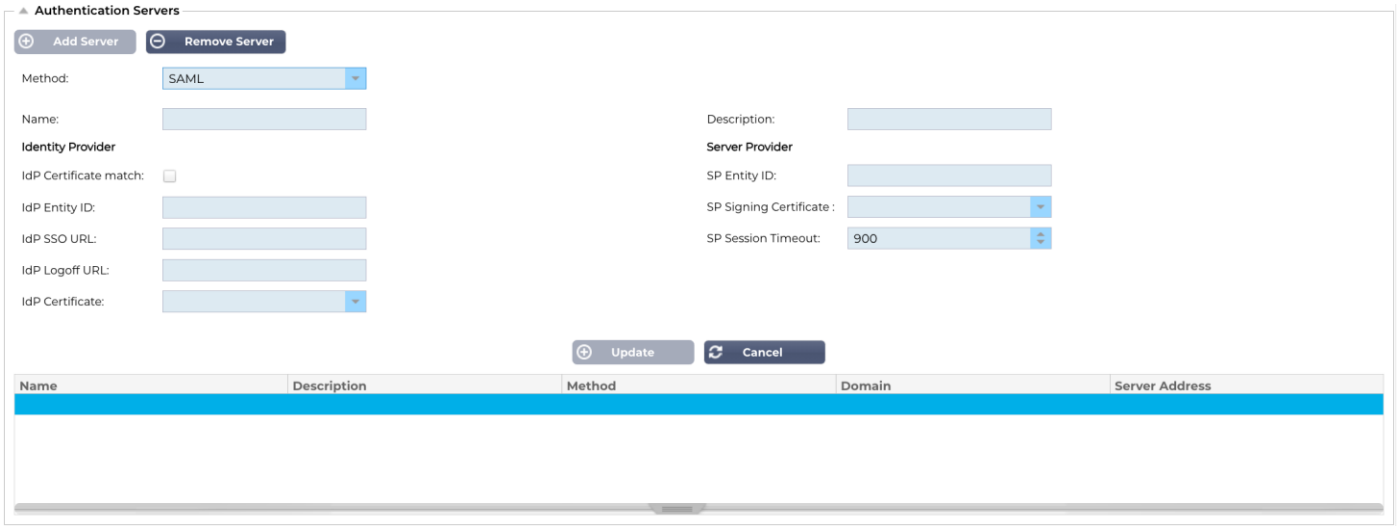


Вариант	Описание
Метод	Выберите метод аутентификации

	LDAP - базовый LDAP с именами пользователей и паролями, отправляемыми открытым текстом на LDAP-сервер. LDAP-MD5 - базовый LDAP с именем пользователя в виде открытого текста и паролем, хэшированным MD5 для повышения безопасности. LDAPS - LDAP через SSL. Отправляет пароль открытым текстом по зашифрованному туннелю между ADC и сервером LDAP. LDAPS-MD5 - LDAP через SSL. Пароль хешируется MD5 для дополнительной безопасности в зашифрованном туннеле между ADC и сервером LDAP.
Имя	Задайте серверу имя для идентификации - это имя будет использоваться во всех правилах.
Адрес сервера	Добавьте IP-адрес или имя хоста сервера аутентификации.
Порт	Для LDAP и LDAPS порты по умолчанию установлены на 389 и 636. Для Radius обычно используется порт 1812. Для SAML порты устанавливаются в ADC.
Домен	Добавьте имя домена для сервера LDAP.
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 полный синтаксис домена и имени пользователя. Пример: *mycompany\jdoe ИЛИ jdoe@mycompany*. Информация о домене, введенная на уровне сервера, игнорируется. Пусто - АЦП примет все, что введет пользователь, и отправит это на сервер аутентификации. Эта опция используется при использовании MD5.
Описание	Добавить описание
База поиска	Это значение является отправной точкой для поиска в базе данных LDAP. Пример *dc=mycompany,dc=local*
Условия поиска	Условия поиска должны соответствовать RFC 4515. Пример: (MemberOf=CN=Phone- VPN,CN=Users,DC=mycompany,DC=local).
Поиск пользователя	Выполните поиск пользователя администратора домена на сервере каталогов.
Пароль	Пароль для пользователя администратора домена.
Мертвое время	Количество времени, по истечении которого неактивный сервер снова помечается как активный

Параметры аутентификации SAML

ВАЖНО: При настройке аутентификации через SAML необходимо создать приложение Enterprise App для Entra ID Authentication. Инструкции по этому вопросу приведены в главеНастройка приложения аутентификации Entra ID в Microsoft Entra

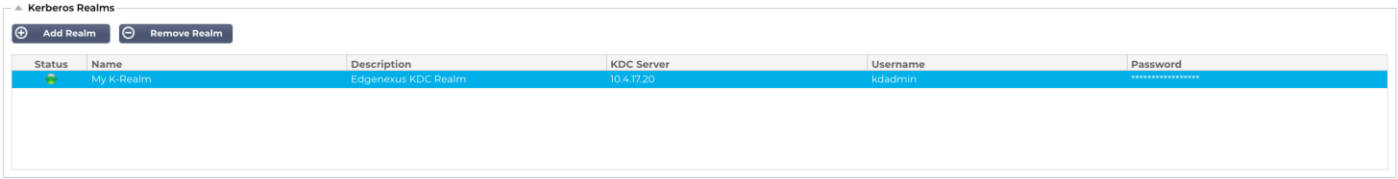


Вариант	Описание
Метод	Выберите метод аутентификации LDAP - базовый LDAP с именами пользователей и паролями, отправляемыми открытым текстом на LDAP-сервер. LDAP-MD5 - базовый LDAP с именем пользователя в виде открытого текста и паролем, хэшированным MD5 для повышения безопасности. LDAPS - LDAP через SSL. Отправляет пароль открытым текстом по зашифрованному туннелю между ADC и сервером LDAP. LDAPS-MD5 - LDAP через SSL. Пароль хешируется MD5 для дополнительной безопасности в зашифрованном туннеле между ADC и сервером LDAP.
Имя	Задайте серверу имя для идентификации - это имя будет использоваться во всех правилах.
Поставщик идентификационных данных	
Соответствие сертификата IdP	IdP Certificate Match - это процесс проверки соответствия цифрового сертификата, используемого поставщиком идентификационных данных (IdP) для подписи утверждений SAML, сертификату, которому доверяет поставщик услуг (SP). Эта проверка гарантирует, что IdP является легитимным и что отправляемые им утверждения являются подлинными и неизменными. SP обычно хранит сертификат IdP в своих метаданных и сравнивает сертификат, встроенный в утверждения SAML, с сохраненным сертификатом, чтобы определить соответствие.
Идентификатор субъекта IdP	SAML IdP Entity ID - это глобально уникальный идентификатор, который служит окончательным адресом провайдера идентификации (IdP) в экосистеме Security Assertion Markup Language (SAML). Этот идентификатор обычно представляет собой URL или URI, который однозначно отличает IdP от других субъектов, участвующих в процессах аутентификации и авторизации на основе SAML. Он играет важную роль в установлении доверия и обеспечении безопасного взаимодействия между IdP, поставщиками услуг (SP) и пользователями.
URL-адрес IdP SSO	IdP SSO URL, сокращение от Single Sign-On URL, - это определенный URL конечной точки, предоставляемый поставщиком идентификационных данных (IdP), который служит шлюзом аутентификации для инициирования сеансов единого входа (SSO). Перенаправляя пользователя на этот URL, IdP предлагает ему пройти аутентификацию, используя свои учетные данные, и после успешной аутентификации перенаправляет его обратно к поставщику услуг (SP) с утверждением, содержащим его идентификационные данные. Это утверждение затем проверяется SP, что позволяет пользователю получить доступ к ресурсам SP без необходимости повторной аутентификации.
URL-адрес выхода из IdP	SAML IdP Log off URL - это специальная конечная точка провайдера идентификации (IdP), которая инициирует и управляет процессом выхода из сеансов единого входа (SSO). Когда пользователь нажимает кнопку выхода из приложения, приложение перенаправляет его на URL-адрес выхода IdP. После этого IdP аннулирует сеанс пользователя на всех доверяющих сторонах, связанных с аутентификацией SSO, и отправляет ответ о выходе обратно в приложение, фактически выводя пользователя из всех подключенных приложений.
Сертификат IdP	Сертификат SAML IdP - это цифровой сертификат X.509, выданный доверенным органом поставщику идентификационных данных (IdP), который участвует в протоколах аутентификации Security Assertion Markup Language (SAML). Этот сертификат служит безопасным средством проверки личности IdP и удостоверения целостности и конфиденциальности сообщений SAML, передаваемых между IdP и поставщиками услуг (SP). Вы можете выбрать сертификат IdP, который будет установлен в ADC, с помощью выпадающего меню.
Описание	Описание для определения.
Поиск пользователя	Выполните поиск пользователя администратора домена.

Пароль	Для указания пароля для пользователя admin.
Поставщик сервера	
Идентификатор субъекта SP	SP Entity ID - это уникальный идентификатор, который служит глобальным адресом для конкретного поставщика услуг (SP) в контексте протокола SAML. Это стандартизированный способ идентификации SP, который обычно представляет собой URL или другой URI, указывающий на метаданные SAML SP, содержащие такую важную информацию, как сертификаты шифрования и конечные точки аутентификации.
Сертификат подписи SP	Сертификат подписи SAML SP - это сертификат X.509, используемый поставщиком услуг (SP) для подписи ответов SAML, обеспечивающий подлинность и целостность сообщений, которыми обмениваются SP и поставщик идентификационных данных (IdP) при аутентификации с помощью единого входа (SSO). SP подписывает ответ с помощью своего закрытого ключа, а IdP проверяет подпись с помощью открытого ключа, связанного с сертификатом, подтверждая личность отправителя и то, что содержимое сообщения не было подделано.
SP Таймаут сеанса	SP Session Timeout - это максимальный срок, в течение которого сеанс аутентификации пользователя считается действительным на стороне поставщика услуг (SP) после успешного единого входа в систему (SSO) через поставщика идентификационных данных (IdP). По истечении указанного времени SP завершает сессию и требует от пользователя повторной аутентификации для получения доступа к защищенным ресурсам. Этот механизм помогает защитить от несанкционированного доступа и гарантирует, что пользовательские сессии не будут простаивать в течение длительного времени.

KDC Realms

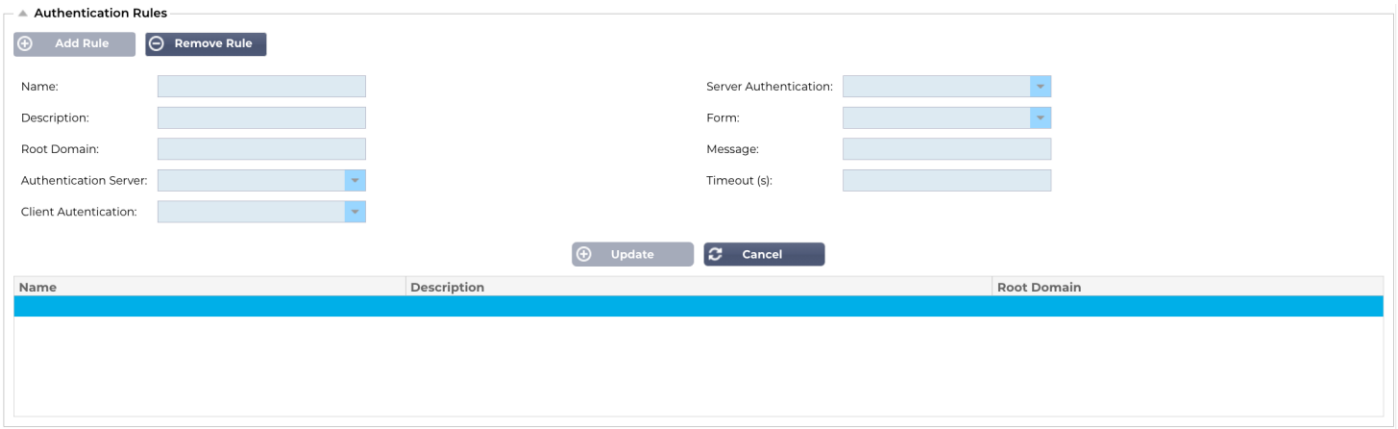
KDC Realms относятся к конфигурациям протокола аутентификации Kerberos, где каждое царство - это, по сути, домен или сеть, работающая под управлением одного центра распределения ключей (Key Distribution Center, KDC). Такая конфигурация определяет группу систем, которые управляются одним главным KDC, что обеспечивает безопасную аутентификацию и механизмы выдачи билетов по всей сети. Области могут быть иерархическими или неиерархическими, с возможностью установления доверительных отношений между ними для безопасной межобластной аутентификации.



Пользовательский интерфейс ADC, как показано на изображении выше, позволяет определить области Kerberos. Эта информация может быть использована в правилах аутентификации.

Правила аутентификации

На следующем этапе необходимо создать правила 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 в систему на всех поддоменах.
Сервер аутентификации	Это выпадающее окно, содержащее настроенные вами серверы.
Аутентификация клиента:	Выберите значение, соответствующее вашим потребностям: Basic (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 подходящее значение. Нет - если на вашем сервере нет никакой 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 подходящее 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 таймаут, по истечении которого пользователь должен будет пройти аутентификацию снова. Обратите внимание, что параметр Timeout действителен только для аутентификации на основе форм.

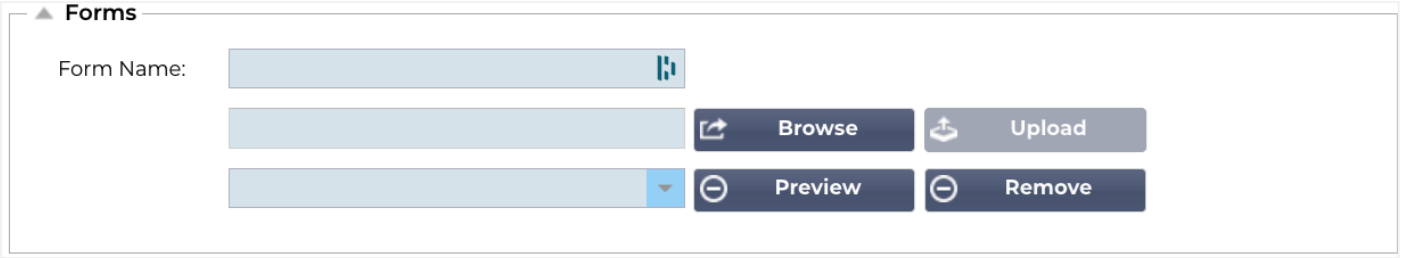
Если вы хотите обеспечить единый вход для пользователей, заполните поле Root Domain (Корневой домен) своим доменом. В данном примере это mycompany.com. Теперь у нас может быть несколько сервисов, которые будут использовать edgenexus.io в качестве корневого домена, и вам нужно будет войти в систему только один раз. Если мы рассмотрим следующие сервисы:

- SharePoint.mycompany.com
- usercentral.mycompany.com
- App Store.mycompany.com

Эти службы могут располагаться на одном VIP-клиенте или быть распределены между 3 VIP-клиентами. Пользователю, впервые зашедшему на usercentral.mycompany.com, будет предложено войти в систему в зависимости от используемого правила аутентификации. Затем этот же

пользователь может подключиться к App Store.mycompany.com и будет автоматически аутентифицирован ADC. Вы можете установить таймаут, который заставит пройти аутентификацию по истечении этого периода бездействия.

Формы



В этом разделе вы сможете загрузить пользовательскую форму.

Как создать пользовательскую форму

Хотя базовая форма, которую предоставляет ADC, достаточна для большинства целей, бывают случаи, когда компании хотят представить пользователю свою собственную личность. Вы можете создать свою собственную форму, которая будет предлагаться 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 понятной формы

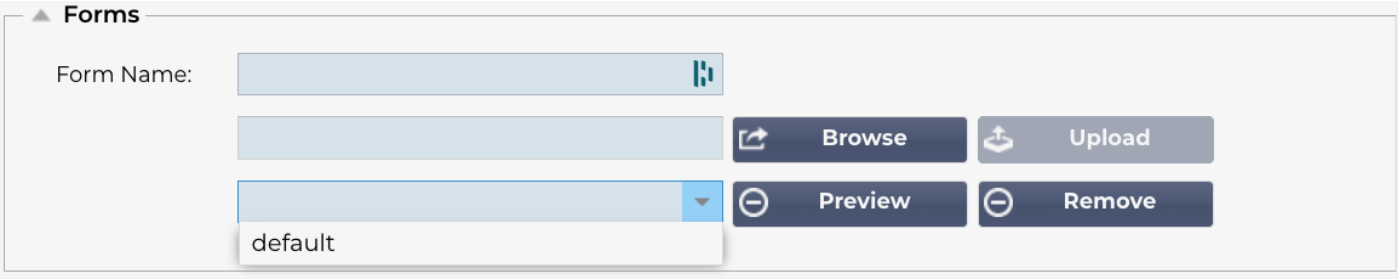
```
<HTML>
<HEAD>
<TITLE>ПРИМЕР ФОРМЫ АВТОРИЗАЦИИ</TITLE>.
</HEAD>
<BODY>
%JNMESSAGE%<br>
<form name="loginform" action="%JNURL%" method="post"> USER: <input type="text" name="JNUSER" size="20" value=""></br>.
PASS: <input type="password" name="JNPASS" size="20" value=""></br>
<input type="submit" name="submit"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

Добавление пользовательской формы

Создав пользовательскую форму, вы можете добавить ее в раздел "Формы".

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

Предварительный просмотр пользовательской формы



Чтобы просмотреть только что загруженную пользовательскую форму, выделите ее и нажмите кнопку Preview. Вы также можете использовать этот раздел для удаления форм, которые больше не нужны

Примечание: При использовании продуктов для фильтрации файлов cookie, таких как AdGuard, вы можете получить сообщение об ошибке 404. Чтобы избежать этого, внесите IP-адрес ADC в белый список.

Кэш

ADC способен кэшировать данные во внутренней памяти и улучшать работу веб-служб. Настройки, управляющие этой функциональностью, приведены в этом разделе.

Глобальные настройки кэша

Максимальный размер кэша (МБ)

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

Желаемый размер кэша (МБ)

Это значение обозначает оптимальный объем 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, которого кэш должен пытаться достичь при каждой автоматической или ручной проверке размера кэша. Промежуток между максимальным и желаемым размером кэша существует для того, чтобы учесть поступление и перекрытие нового содержимого между периодическими проверками размера кэша для удаления просроченного содержимого. И снова, возможно, будет более эффективным принять значение по умолчанию (30 МБ) и периодически проверять размер кэша в разделе "Монитор -> Статистика" для определения подходящего размера.

Время кэширования по умолчанию (Д/ЧЧ:ММ)

Введенное здесь значение представляет собой срок хранения содержимого без явного срока действия. Время кэширования по умолчанию - это период, в течение которого хранится содержимое без директивы "не хранить" или явного времени истечения срока действия в заголовке трафика.

Запись в поле имеет вид "D/HH:MM" - таким образом, запись "1/01:01" (по умолчанию 1/00:00) означает, что для хранения ADC 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 HTTP-ответов:

- 200 - стандартный ответ для успешных HTTP-запросов
- 203 - Заголовки не являются окончательными, а получены из локальной или сторонней копии

- 301 - Запрашиваемому ресурсу был присвоен новый постоянный URL-адрес
- 304 - Не изменен с момента последнего запроса и вместо него следует использовать локально кэшированную копию
- 410 - Ресурс больше не доступен на сервере, и адрес пересылки неизвестен

Это поле следует редактировать с осторожностью, поскольку наиболее распространенные коды ответов, которые можно кэшировать, уже перечислены.

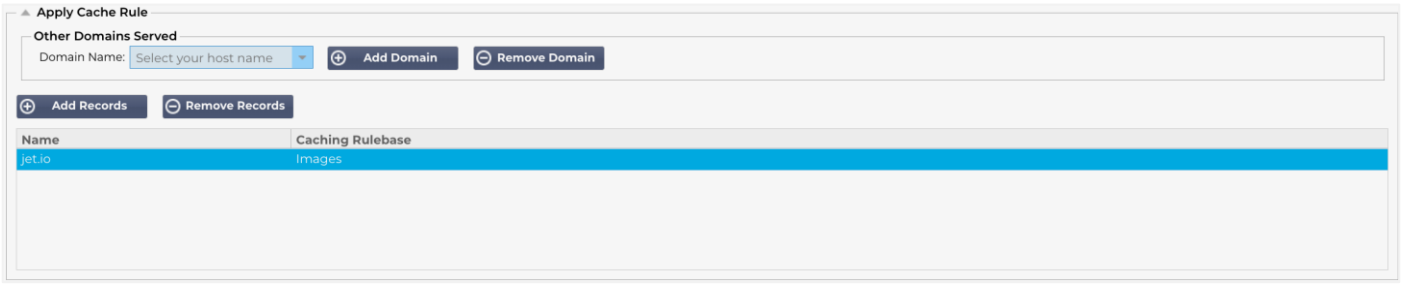
Таймер проверки кэша (Д/ЧЧ:ММ)

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.

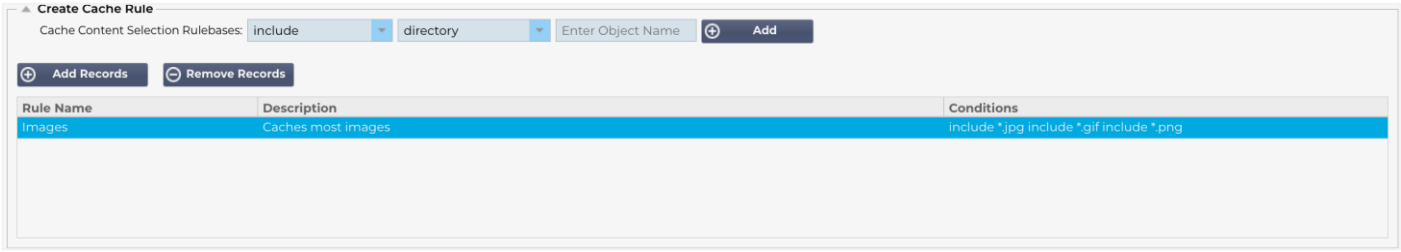
Применить правило кэширования



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 десятичной системе счисления. Пример www.mycompany.com или 192.168.3.1:80.
- Щелкните по стрелке выпадающего списка и выберите свой домен из списка
- Список будет заполнен до тех пор, пока трафик проходит через виртуальную службу и к ней применяется стратегия кэширования
- Выберите правило кэширования, дважды щелкнув на столбце Caching Rulebase и выбрав его из списка

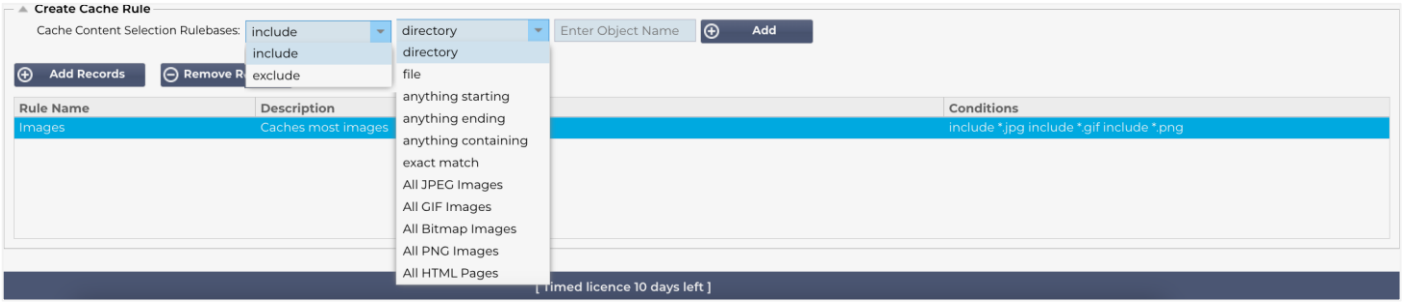
Создание правила кэширования



Этот раздел позволяет создать несколько различных правил кэширования, которые затем можно применить к домену:

- Нажмите кнопку Добавить записи и дайте 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 критерий отбора, например, 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 правила будут отображаться в одной строке до тех пор, пока вы не нажмете на поле "Условия", после чего они будут отображаться в отдельной строке.

flightPATH

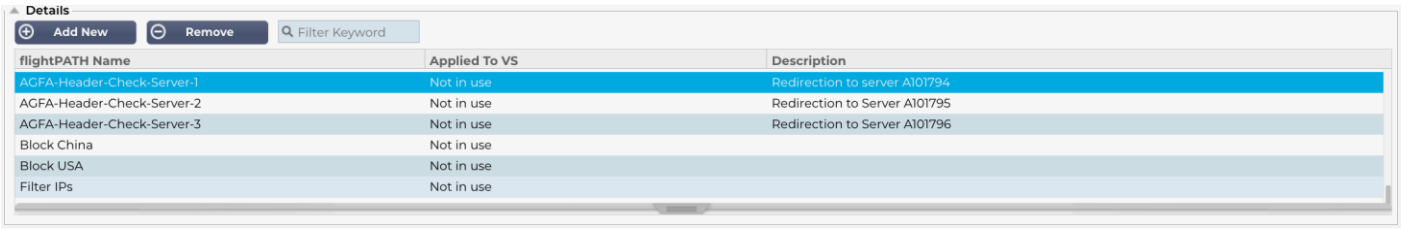
flightPATH - это технология управления трафиком, встроенная в ADC, которая позволяет проверять HTTP- и HTTPS-трафик в режиме реального времени и выполнять действия в зависимости от условий.

Чтобы использовать правила flightPATH, они должны быть применены к виртуальной службе с помощью вкладки flightPATH в разделе Real Servers.

Правило траектории полета состоит из четырех элементов:

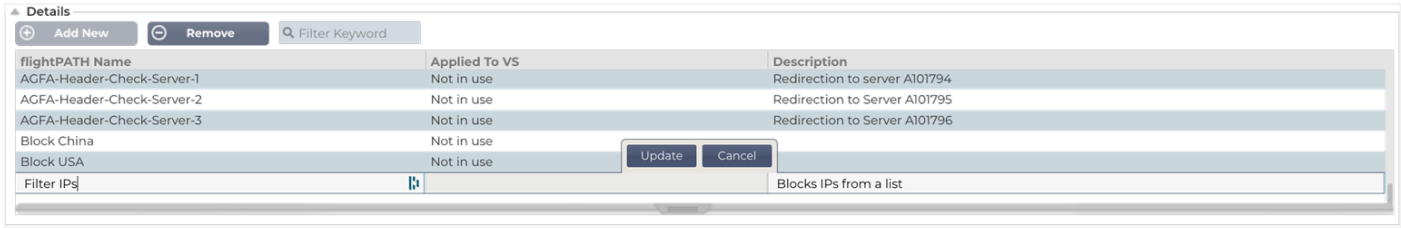
1. Details, где вы определяете имя flightPATH и службу, к которой он прикреплен.
2. Условие(я), которое(ые) может быть определено(ы), чтобы вызвать срабатывание правила.
3. Оценка, позволяющая определять переменные, которые можно использовать в действиях.
4. Действия, которые используются для управления 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



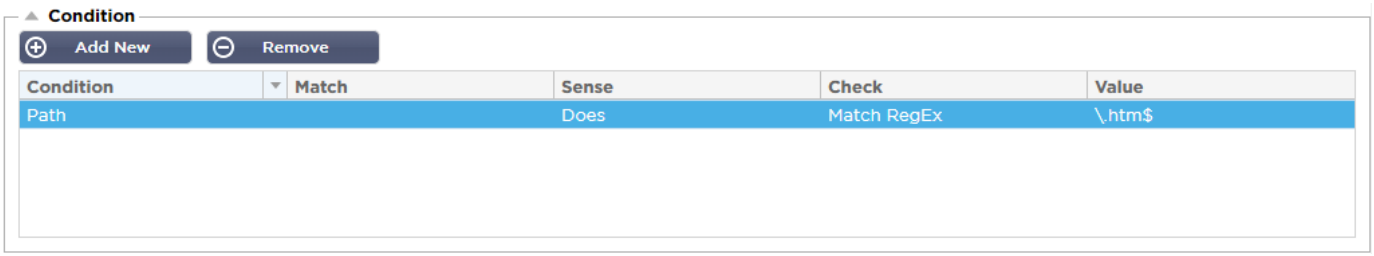
Поле	Описание
Имя FlightPATH	Это поле предназначено для имени правила flightPATH. Имя, которое вы здесь указываете, появляется в других частях ADC и на него ссылаются.
Применяется к VS	Этот столбец доступен только для чтения и показывает VIP, к которому применяется правило flightPATH.
Описание	Значение,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

Шаги по добавлению правила flightPATH

1. Сначала нажмите кнопку Добавить новый, расположенную в разделе Подробности.
2. Введите имя для правила. Пример Auth2
3. Введите описание вашего правила
4. Когда правило будет применено к службе, вы увидите, как в столбце "Применить к" автоматически заполняется значение IP-адреса и порта.
5. Не забудьте нажать кнопку "Обновить", чтобы сохранить изменения, а если вы ошиблись, просто нажмите "Отменить", чтобы вернуться к предыдущему состоянию.

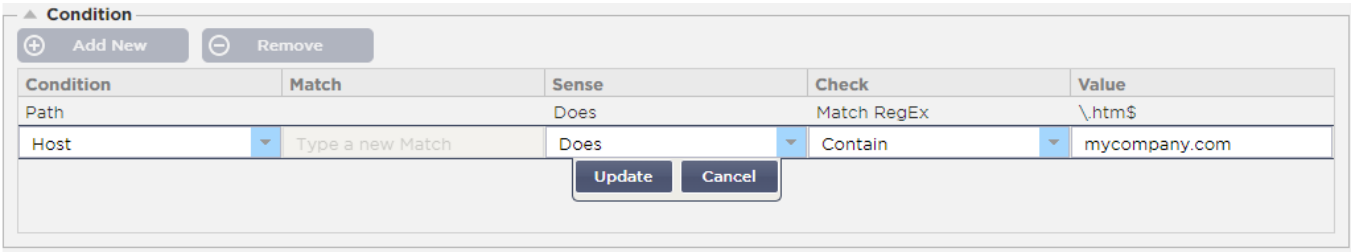
Состояние

Правило flightPATH может содержать любое количество условий. Условия работают по принципу **AND** и позволяют задать условие, при котором срабатывает действие. Если вы хотите использовать условие **OR**, создайте дополнительные правила flightPATH и примените их 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



Сначала нужно выбрать значение в столбце Условие.

Мы предусмотрели несколько условий в выпадающем списке, которые охватывают все возможные сценарии. Когда будут добавлены новые условия, они будут доступны через обновления Jetpack.

Доступны следующие варианты:

СОДЕРЖАНИЕ	ОПИСАНИЕ	ПРИМЕР
<form>	HTML-формы используются для передачи данных на сервер	Пример "форма не имеет длины 0"
Местоположение ГЕО	Сравнивает IP-адрес источника с кодами стран ISO 3166.	Местонахождение ГЕО равно GB, ИЛИ Местонахождение ГЕО равно Germany
Хозяин	Хост, извлеченный из URL-адреса	www.mywebsite.com или 192.168.1.1
Язык	Язык, извлекаемый из HTTP-заголовка language	Это условие приведет к появлению выпадающего списка языков
Метод	Выпадающий список методов HTTP	Выпадающий список, включающий GET, POST и т.д.
Происхождение IP	Если восходящий прокси поддерживает X-Forwarded-for (XFF), он будет использовать истинный адрес Origin.	IP-адрес клиента. Он также может использовать несколько IP-адресов или подсетей. 10\.1\.2\.* - это подсеть 10.1.2.0 /24 10\.1\.2\.3|10\.1\.2\.4 Используйте | для нескольких IP-адресов
Путь	Путь к сайту	/mywebsite/index.asp
ПОСТ	Метод запроса POST	Проверка данных, загружаемых на веб-сайт

Запрос	Имя и значение запроса, может принимать либо имя запроса, либо значение.	"Best=jetNEXUS", где совпадение - 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	Заданная пользователем строка в теле ответа	Сервер вверх
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 объединенный IP-адрес	IP-адрес клиента, IP-адрес прокси-сервера, IP-адрес брандмауэра. Можно также использовать несколько IP и подсетей. Точки необходимо экранировать, так как они являются RegEX. Пример 10\.1\.2\.3 - это 10.1.2.3

Матч

Поле Match может быть выпадающим или текстовым и определяется в зависимости от значения в поле Condition. Например, если условие установлено на Host, поле Match недоступно. Если условие установлено на <form>, поле Match отображается как текстовое поле, а если условие - POST, поле Match представляется как выпадающий список, содержащий соответствующие значения.

Доступны следующие варианты:

МАТЧ	**ОПИСАНИЕ**	**ПРИМЕР**
Принять	Типы содержимого, которые допустимы	Принять: text/plain
Accept-Encoding	Допустимые кодировки	Accept-Encoding: <compress | gzip | deflate | sdch | identity>.
Accept-Language	Приемлемые языки для ответа	Язык приема: en-US
Диапазоны приема	Какие типы диапазонов частичного содержимого поддерживает этот сервер	Диапазон приема: байты
Авторизация	Учетные данные для аутентификации по протоколу HTTP	Авторизация: Basic QWxhZGRpbjpvcGVuIHNlc2FtZQ==
Заряжайся	Содержит информацию о расходах на применение запрашиваемого метода	
Content-Encoding	Тип используемой кодировки	Content-Encoding: gzip
Content-Length	Длина тела ответа в октетах (8-битных байтах)	Content-Length: 348

Content-Type	Тип mime тела запроса (используется для запросов 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 создания сообщения	Дата = "Дата" ":" HTTP-дата
ETag	Идентификатор для конкретной версии ресурса, часто это дайджест сообщения.	ETag: "aed6bdb8e090cd1:0".
С сайта	Адрес электронной почты пользователя, сделавшего 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 велась 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)
Vary	Указывает нижестоящим прокси-серверам, как сопоставить заголовки будущих запросов, чтобы решить можно ли использовать кэшированный ответ, а не запрашивать новый с оригинального сервера	Vary: User-Agent
X-Powered-By	Указание технологии (например, ASP.NET, PHP, JBoss), поддерживающей веб-приложение	X-Powered-By: PHP/5.4.0

Чувство

Поле Sense представляет собой выпадающее булево поле и 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

ПРОВЕРИТЬ	ОПИСАНИЕ	ПРИМЕР
Существовать	Здесь не важны детали условия, важно лишь то, что оно существует/не существует	Хост> Существует >
Начало	Строка начинается со значения	Путь> Начинается> Начинается /secure>

Конец	Строка заканчивается значением	Путь> заканчивается> - .jpg
Содержите	Строка содержит значение	Заголовок запроса> Принять> Содержит ли> изображение>
Равный	Строка равна значению	Хозяин> Равняется ли >> www.edgenexus.io
Длина	Строка имеет длину, равную значению	Хост> Имеет ли> длину> 16 www.edgenexus.io = TRUE www.edgenexus.com = FALSE
Соответствие RegEx	Позволяет ввести полное регулярное выражение, совместимое с Perl.	IP-адрес происхождения> Соответствует ли> Regex
Список матчей	Позволяет сопоставить значение со списком значений. Это полезно, когда нужно сопоставить, например, определенные IP-адреса. Значения разделяются запятыми (,) или точками (|).	IP-адрес источника> Does > Match List > 10.10.10.1, 10.10.10.2, 10.10.10.3 и т. д.
Превышение длины	Позволяет проверить, не превышает ли значение указанную длину.	Путь > Есть > Превысить длину > 200

Шаги для добавления условия

Добавить новое условие flightPATH очень просто. Пример показан выше.

1. Нажмите кнопку Добавить новый в области Условие.
2. Выберите условие в раскрывающемся окне. В качестве примера возьмем Host. Вы также можете ввести текст в поле, и ADC отобразит значение в выпадающем списке.
3. Выберите смысл. Например, Does
4. Выберите флажок. Например, "Содержать
5. Выберите значение. Например, mycompany.com

В приведенном выше примере показано, что есть два условия, которые оба должны быть TRUE, чтобы правило было выполнено

- Первая проверка заключается в том, что запрашиваемый объект является изображением
- Второй проверяет, является ли хост в URL адресе www.imagepool.com.

Оценка

Возможность добавления определяемых переменных - это очень интересная возможность. Другие АЦП предлагают такую возможность с помощью сценариев или командной строки, что не является идеальным вариантом для любого пользователя. EdgeADC позволяет определять 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".

- $sourceip$ - IP-адрес источника запроса
- $sourceport$ - Порт источника, который был использован
- $clientip$ - IP-адрес клиента
- $clientport$ - Порт, используемый клиентом
- $host$ - хост, указанный в запросе
- $method$ - Используемый метод: GET, POST и т. д.
- $path$ - путь, указанный в запросе
- $querystring$ - Строка запроса, используемая в запросе
- $version$ - Версия HTTP-запроса в REQUEST (в настоящее время разрешены только 1 и 1.1).
- $resp$ - Ответ от сервера. например, 200OK, 404 и т. д.
- $geolocation$ - ГЕО-положение, из которого был отправлен запрос.

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

Объяснение:

- Клиент, обращающийся к несуществующей странице, обычно получает в браузере страницу 404 Error.
- Вместо этого пользователь перенаправляется на исходное имя хоста, которое он использовал, но неверный путь заменяется на 404.html.
- В Syslog добавляется запись: "Клиент с адреса 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 в URL, чтобы отразить URL, введенный пользователем.

- Нажмите Добавить новый

- Выберите Переписать путь в раскрывающемся меню Действие
- В поле Target введите $path$/myimages
- Нажмите кнопку Обновить

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

Действие	Описание	Пример
Cookie запроса на добавление	Добавьте куки запроса, подробно описанные в разделе "Цель", со значением в разделе "Данные".	Target= Cookie Data= MS-WSMAN=afYfn1CDqqCDqCVii
Добавить заголовок запроса	Добавьте заголовок запроса типа Target со значением в секции Data	Target= Accept Data= image/png
Добавить Cookie для ответа	Добавьте куки-файлы ответа, подробно описанные в разделе "Цель", со значением в разделе "Данные".	Target= Cookie Data= MS-WSMAN=afYfn1CDqqCDqCVii
Добавить заголовок ответа	Добавьте заголовок запроса, подробный в разделе Target, со значением в разделе Data	Target= Cache-Control Data= max-age=8888888
Кузов Заменить все	Найдите тело ответа и замените все экземпляры	Цель= http:// (строка поиска) Данные= https:// (строка замены)
Замена корпуса в первую очередь	Выполните поиск в теле ответа и замените только первый экземпляр	Цель= http:// (строка поиска) Данные= https:// (строка замены)
Замена корпуса Последняя	Выполните поиск в теле ответа и замените только последний экземпляр	Цель= http:// (строка поиска) Данные= https:// (строка замены)
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" Data= N/A
Журнал событий	Это приведет к регистрации события в системном журнале	Target= "flightPATH зарегистрировал это в syslog" Data= N/A
Перенаправление 301	Это приведет к постоянному перенаправлению	Цель= http://www.edgenexus.io Данные= N/A

Перенаправление 302	Это приведет к временному перенаправлению	Цель= http://www.edgenexus.io Данные= N/A
Удалить куки запроса	Удалите cookie запроса, подробно описанные в разделе "Цель	Target= Cookie Data= MS-WSMAN=afYfn1CDqqCDqCVii
Удалить заголовок запроса	Удалите заголовок запроса, подробно описанный в разделе Цель	Цель=Сервер Данные=H/A
Удалить ответ	Удалите куки-файлы ответа, подробно описанные в разделе "Цель".	Target=jnAccel
Удалить ответ	Удалите заголовок ответа, подробно описанный в разделе Заголовок цели	Target= Etag Data= N/A
Заменить cookie запроса	Замените cookie запроса, указанные в разделе "Цель", на значение в разделе "Данные".	Target= Cookie Data= MS-WSMAN=afYfn1CDqqCDqCVii
Замена заголовка запроса	Замените заголовок запроса в цели значением Data	Target= Connection Data= keep-alive
Заменить	Замените cookie ответа, указанные в разделе Target, значением из раздела Data Cookie	Target=jnAccel=afYfn1CDqqCDqCVii Date=MSWSMAN=afYfn1CDqqCDqCVii
Заменить ответ	Замените заголовок ответа, указанный в разделе Target, на значение в разделе Data Header.	Цель = Данные сервера = Удержано в целях безопасности
Перезапись пути	Это позволит вам перенаправить запрос на новый URL, основываясь на условии	Target= /test/path/index.html$querystring$ Data= N/A
Используйте безопасный сервер	Выберите, какой безопасный сервер или виртуальную службу использовать	Target=192.168.101:443 Data=N/A
Используйте	Выберите, какой сервер или виртуальную службу использовать	Цель= 192.168.101:80 Данные= N/A

Зашифровать cookie	Это позволит зашифровать файлы cookie в формате 3DES, а затем закодировать их в base64	Target= Введите имя cookie, которое будет зашифровано, вы можете использовать * в качестве подстановочного символа в конце Data= Введите ключевую фразу для шифрования.

Сценарий правил flightPATH

У клиента есть сайт электронной коммерции, и у него возникли проблемы с блокировкой файлов cookie последними версиями браузеров.

Заказчик отслеживает проблемы и обнаруживает, что основная причина заключается в отсутствии "безопасной" и "односайтовой" маркировки для соответствующих файлов cookie.

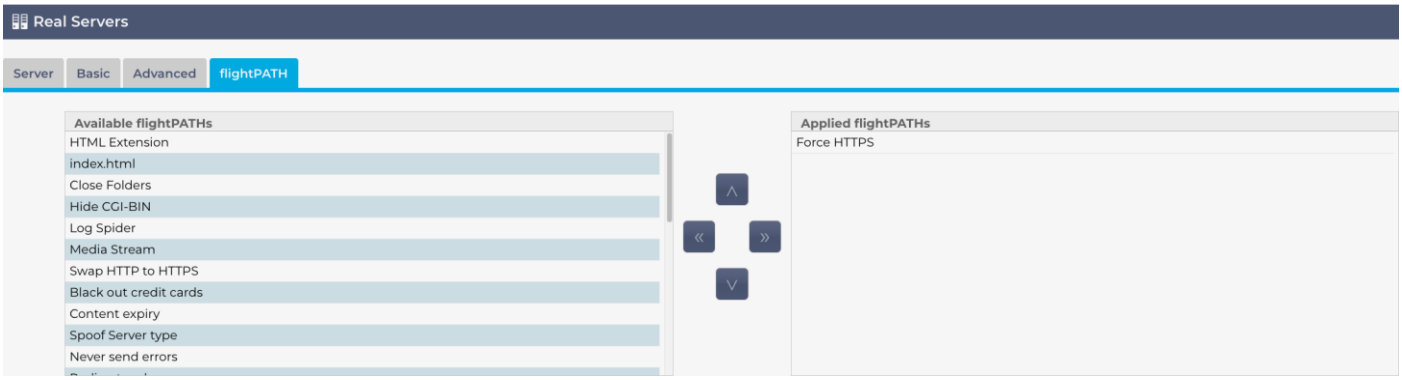
Давайте посмотрим, чем может помочь flightPATH.

- У нас есть cookie с именем 'wp_woocommerce_session_97929973749972642'.
- Имя cookie - 'wp_woocommerce_session_' со случайным уникальным значением ID '97929973749972642', сгенерированным системой электронной коммерции.
- Теги "same-site" и "secure" кажутся пустыми, следовательно, cookie блокируется новыми ограничениями безопасности браузера.
- Чтобы этого не произошло, мы можем создать следующие правила flightPATH.
- **flightPATH Правило для идентификатора сеанса**
  - **Состояние**:
    Оставьте пустым
  - **Оценка**:
    Переменная = $переменная_1$
    Источник = Cookie ответа
    Деталь = wp_woocommerce_session_*
  - Действие
    Действие = Заменить cookie ответа
    Цель = wp_woocommerce_session_*
    Данные = $variable_1$
- **Правило flightPATH для тегов**
  - **Условие:**
    Условие = Cookie ответа
    Соответствие = woocommerce_cart_hash
    Чувствовать = Есть
    Проверка = Существует
    Значение = Оставить пустым
  - **Оценка:**
    Переменная = $переменная_2$
    Источник = Cookie ответа
    Деталь = woocommerce_cart_hash
    Значение = Оставить пустым
  - **Действие:**
    Действие = Заменить cookie ответа
    Цель = woocommerce_cart_hash
    Данные = $variable_2$,SameSite=None,Secure

Теперь примените правила к виртуальным службам, которым они необходимы.

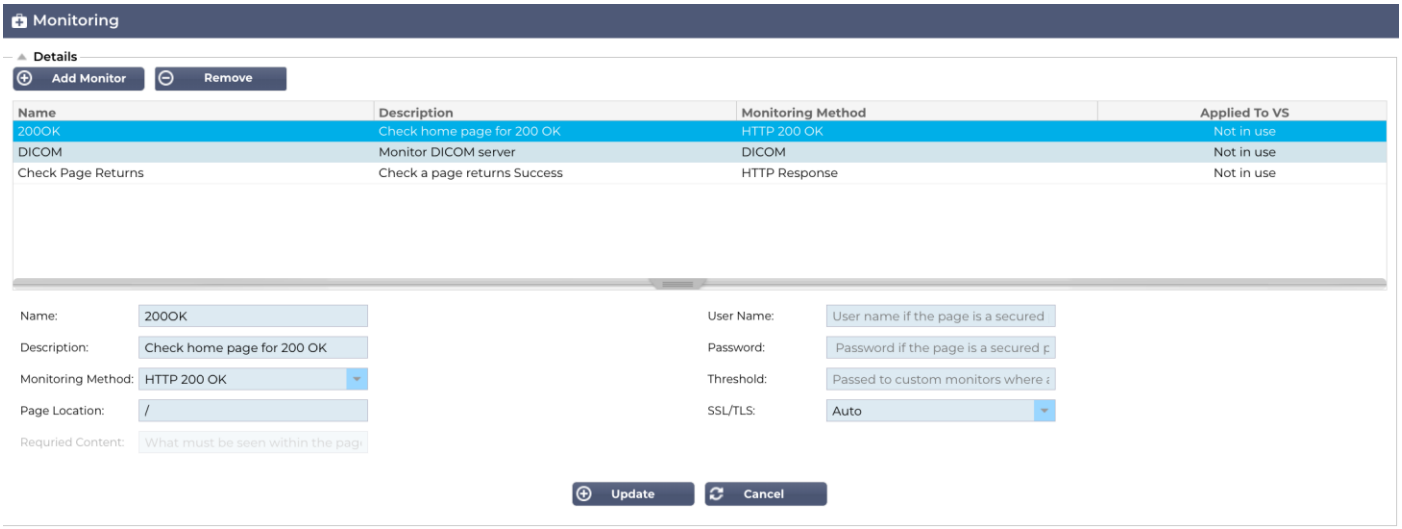
Применение правила flightPATH

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



- Перейдите в раздел "Службы" > "IP-службы" и выберите VIP, которому нужно 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



Мониторинг реальных серверов важен в сценарии балансировки нагрузки для обнаружения и реагирования на проблемы с серверами, обеспечения сбалансированного распределения нагрузки, оптимизации использования ресурсов, определения приоритетности критически важных сервисов, а также выявления и устранения уязвимостей программного обеспечения.

Страница Library> Real Server Monitors позволяет добавлять, просматривать и редактировать пользовательский мониторинг. Это "проверки здоровья" сервера уровня 7, которые выбираются из поля Server Monitoring на вкладке Basic определяемой вами виртуальной службы.

Типы мониторов реального сервера

Существует несколько мониторов Real Server Monitors, которые описаны в таблице ниже. Разумеется, вы можете написать дополнительные мониторы с помощью PERL.

Метод мониторинга	Описание	Пример
HTTP 200 OK	Устанавливается TCP-соединение с реальным сервером. После установления соединения на реальный сервер отправляется короткий HTTP-запрос. Когда ответ получен, он проверяется на наличие строки '200 OK'. Если она присутствует, сервер считается работоспособным. Обратите внимание, что при использовании этого монитора загружается вся страница с содержимым. 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".	**Запрос** GET / HTTP/1.1 Хост: 192.168.159.200 Принять: */* Язык приема: en-gb User-Agent: Edgenexus-ADC/4.0 Соединение: Keep-Alive Cache-Control: no-cache **Ответ** HTTP/1.1 200 OK Content-Type: text/html Last-Modified: Wed, 31 Jan 2018 15:08:18 GMT Диапазон приема: байты ETag: "0dd3253a59ad31:0". Сервер: Microsoft-IIS/10.0 Дата: Tue, 13 Jul 2021 15:55:47 GMT Content-Length: 1364 <!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Strict//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-strict.dtd">. <html xmlns="http://www.w3.org/1999/xhtml">

		<head> <meta http-equiv="Content-Type" content="text/html; charset=iso-8859-1" /> <title>jetNEXUS</title> <style type="text/css"> <!-- тело { цвет:#FFFFFF; ... </body> </html>
HTTP 200 Head	Создается TCP-соединение с сервером Real Server, в поле PATH которого указывается местоположение для проверки. Головная часть ответа извлекается с сервера, а содержимое отбрасывается. Ответ проверяется на наличие 200 OK. Если он присутствует, сервер считается работоспособным. Обратите внимание, что при использовании этого монитора извлекается только головная часть. 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".	**Запрос** HEAD / HTTP/1.1 Хост: 192.168.159.200 Принять: */* Язык приема: en-gb User-Agent: Edgenexus-ADC/4.0 Соединение: Keep-Alive Cache-Control: no-cache **Ответ** HTTP/1.1 200 OK Content-Length: 1364 Content-Type: text/html Last-Modified: Wed, 31 Jan 2018 15:08:18 GMT Диапазон приема: байты ETag: "0dd3253a59ad31:0". Сервер: Microsoft-IIS/10.0 Дата: Tue, 13 Jul 2021 15:49:19 GMT
Параметры HTTP 200	С сервером Real Server устанавливается TCP-соединение и выполняется запрос Options. Опции возвращаются и проверяются на содержание 200 OK. Если содержимое 200 OK найдено, значит, сервер считается доступным.	**Запрос** ПАРАМЕТРЫ / HTTP/1.1 Хост: 192.168.159.200 Принять: */* Язык приема: en-gb User-Agent: Edgenexus-ADC/4.0 Соединение: Keep-Alive Cache-Control: no-cache **Ответ** HTTP/1.1 200 OK Разрешить: OPTIONS, TRACE, GET, HEAD, POST Сервер: Microsoft-IIS/10.0 Публичные: ОПЦИИ, ОТСЛЕДИТЬ, ПОЛУЧИТЬ, ГОЛОВА, ПОСТ Дата: Tue, 13 Jul 2021 16:23:39 GMT Content-Length: 0
Головка HTTP	Монитор HTTP Head позволяет проверить наличие определенного значения в части Head HTTP-потока. Мы можем ввести Path и Required Response в соответствующие поля, а затем проверить наличие этого значения в ответе. Если значение Required Response будет найдено в Head, считается, что сервер работает и доступен. Мы также можем использовать это на специально защищенных страницах, где требуется имя пользователя и пароль. Таким образом, результат работы монитора можно считать точным.	**Запрос** HEAD /ispagethere.htm HTTP/1.1 Хост: 192.168.159.200 Принять: */* Язык приема: en-gb User-Agent: Edgenexus-ADC/4.0 Соединение: Keep-Alive Cache-Control: no-cache **Ответ** HTTP/1.1 200 OK Content-Length: 1364 Content-Type: text/html Last-Modified: Wed, 31 Jan 2018 15:08:18 GMT

	Например, если предоставить **файл /ispagethere.html** и значения **200 OK** в полях Path и Required Response, то будет получен успешный результат, если сервер работает, страница доступна и отвечает на запрос. 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".	Диапазон приема: байты ETag: "0dd3253a59ad31:0". Сервер: Microsoft-IIS/10.0 Дата: Wed, 14 Jul 2021 08:28:18 GMT
Параметры HTTP	Монитор HTTP Options позволяет проверить наличие определенного значения в возвращаемых данных Options. Мы вводим Path и Required Response в соответствующие поля, а затем проверяем ответ. Если в данных Options найден требуемый ответ, значит, сервер доступен и работает. Значениями Required Response могут быть любые из следующих: OPTIONS, TRACE, GET, HEAD и POST. Например, если указать **/ispagethere.html** и значения **GET** в полях Path и Required Response, результат будет успешным, если сервер работает, страница доступна и отвечает на запрос. 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".	**Запрос** OPTIONS /ispagethere.htm HTTP/1.1 Хост: 192.168.159.200 Принять: */* Язык приема: en-gb User-Agent: Edgenexus-ADC/4.0 Соединение: Keep-Alive Cache-Control: no-cache **Ответ** HTTP/1.1 200 OK Разрешить: OPTIONS, TRACE, GET, HEAD, POST Сервер: Microsoft-IIS/10.0 Публичные: ОПЦИИ, ТРАССИРОВКА, ПОЛУЧИТЬ, ГОЛОВА, ПОСТ Дата: Wed, 14 Jul 2021 09:47:27 GMT Content-Length: 0
HTTP-ответ	С сервером Real Server устанавливается соединение и HTTP-запрос/ответ и проверяется, как описано в предыдущих примерах. 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. Например, в примере, показанном справа, мы указали **/ispagethere.htm** в качестве пути и **Microsoft-IIS** в качестве требуемого ответа. Если текст найден, считается, что сервер Real Server работает. Этот метод мониторинга можно использовать только для типов служб HTTP и Accelerated HTTP. Однако если для HTTP-сервера используется тип службы уровня 4, он все	**Запрос** GET /ispagethere.htm HTTP/1.1 Хост: 192.168.159.200 Принять: */* Язык приема: en-gb User-Agent: Edgenexus-ADC/4.0 Соединение: Keep-Alive Cache-Control: no-cache **Ответ** HTTP/1.1 200 OK Content-Type: text/html Last-Modified: Wed, 31 Jan 2018 15:08:18 GMT Диапазон приема: байты ETag: "0dd3253a59ad31:0". Сервер: Microsoft-IIS/10.0 Дата: Wed, 14 Jul 2021 10:07:13 GMT Content-Length: 1364 <!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Strict//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-strict.dtd">.

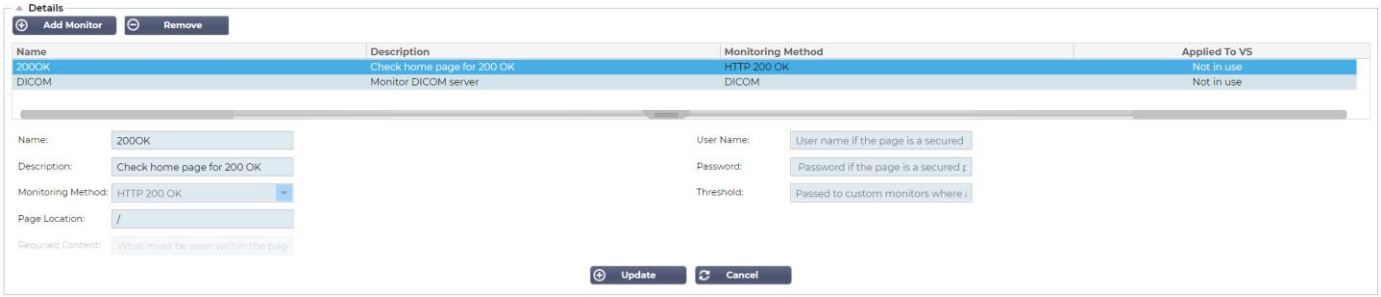
	равно может быть использован, если SSL не используется на реальном сервере или обрабатывается соответствующим образом с помощью "Content SSL".	<html xmlns="http://www.w3.org/1999/xhtml"> <head> <meta http-equiv="Content-Type" content="text/html; charset=iso-8859-1" /> <title>jetNEXUS</title> <style type="text/css"> <!-- тело { цвет:#FFFFFF; ...
Многопортовый монитор TCP	Этот метод похож на описанный выше, за исключением того, что вы можете использовать несколько разных 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 Требуемое содержание: 135,59534,59535
TCP вне диапазона	Метод TCP Out of Band похож на TCP Connect, за исключением того, что вы можете указать порт, который хотите отслеживать, в столбце требуемого содержимого. Этот порт обычно не совпадает с портом трафика и используется, когда вы хотите связать службы вместе	Имя: TCP Out of Band Описание: Мониторинг внеполосного/трафика порта Расположение страницы: N/A Необходимое содержание: 555
DICOM	Мы отправляем DICOM-эхо, используя значение "Source Calling" AE Title в столбце требуемого содержимого. Вы также можете задать значение AE Title "Destination Called" в разделе Notes каждого сервера. Столбец Notes можно найти в разделе IP Services--Виртуальные службы - Страница сервера.	Название: DICOM Описание: Проверка работоспособности L7 для службы DICOM Метод мониторинга: DICOM Расположение страницы: N/A Необходимое содержание: Значение AET
LDAPS	Эта новая проверка работоспособности используется для проверки работоспособности и ответа сервера LDAP/AD.	Имя: LDAPS Описание: Проверка работоспособности сервера LDAP/AD Ниже приведены параметры использования: **Имя пользователя**: cn=username,cn=users,dc=domainname, dc=local **Пароль**: DomainUserPassword **Содержание**: 200OK
SNMP v2	Этот метод мониторинга позволяет проверить состояние доступности сервера с помощью ответа SNMP MIB сервера. Значение Require Response должно содержать имя сообщества.	
Проверка DNS-сервера	При балансировке нагрузки на DNS-серверы полезно проверить, отвечает ли сервер на DNS-запросы. Монитор можно использовать следующим образом: • Поле Path используется для FQDN, который вы запрашиваете. Например, если вы хотите запросить www.edgenexus.io, введите это в поле Path. • Если оставить это значение пустым, то монитор будет использовать для выполнения запроса поиск по умолчанию. • Поле Required Response можно оставить пустым, и монитор будет считать, что любой ответ считается правильным. В противном случае в поле Required Response следует ввести ожидаемый IP-адрес. Например, это может быть 101.10.10.100. Если запрос вернет это значение, монитор отметит успех; в противном случае он отметит неудачу.	

	Успешный результат означает, что DNS-сервер, на который вы перераспределяете нагрузку, работает.

Страница Real Server Monitors состоит из трех разделов.

Подробности

Раздел "Сведения" используется для добавления новых мониторов и удаления ненужных. Вы также можете отредактировать существующий монитор, дважды щелкнув на нем.



Имя

Название монитора по вашему выбору.

Описание

Текстовое описание для этого монитора, и мы рекомендуем сделать его как можно более подробным.

Метод мониторинга

Выберите метод мониторинга из раскрывающегося списка. Доступны следующие варианты:

- HTTP 200 OK
- HTTP 200 Head
- Параметры HTTP 200
- Головка HTTP
- Параметры HTTP
- HTTP-ответ
- Многопортовый монитор TCP
- TCP вне диапазона
- DICOM
- SNMP v2
- Проверка DNS-сервера
- LDAPS

Расположение страницы

URL Расположение страницы для HTTP-монитора. Это значение может быть относительной ссылкой, например /folder1/folder2/page1.html. Также можно использовать абсолютную ссылку, где веб-сайт привязан к имени хоста.

Обязательное содержание

Это значение содержит любой контент, который монитор должен обнаружить и использовать. Представленное здесь значение будет меняться в зависимости от выбранного метода мониторинга.

Применяется к VS

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

Пользователь

Некоторые пользовательские мониторы могут использовать это значение вместе с полем пароля для входа на сервер 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 пороговое значение, например уровень процессора.

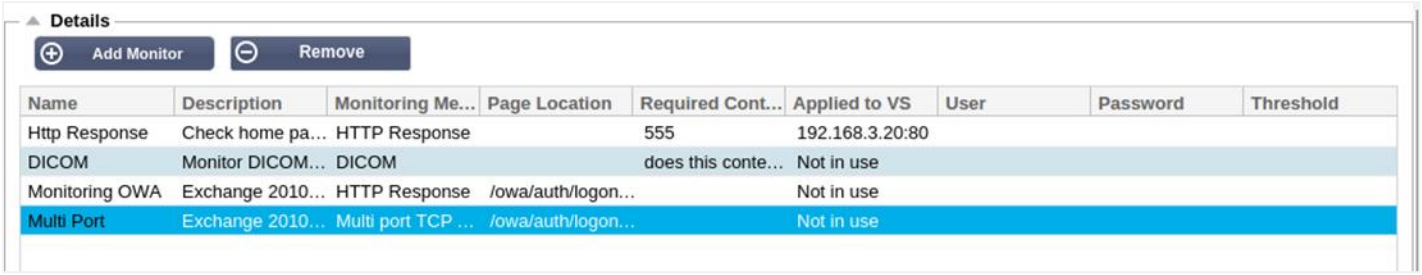
ПРИМЕЧАНИЕ: Убедитесь, что ответ, полученный от сервера приложений, не является ответом "Chunked".

SSL/TLS

В этом поле можно указать, использовать или не использовать SSL. Настройки могут быть следующими:

- Вкл.
- Выключить - отключение SSL
- Авто - останется в текущем состоянии

Примеры монитора реального сервера



Монитор загрузки

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

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

- Дайте монитору имя, чтобы его можно было идентифицировать в списке "Метод мониторинга".
- Найдите файл .pl
- Нажмите кнопку Загрузить новый монитор
- Ваш файл будет загружен в нужное место и станет виден как новый метод мониторинга.

Индивидуальные мониторы

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

- Нажмите на раскрывающееся окно
- Выберите имя пользовательского монитора
- Нажмите кнопку 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 на Perl.

Команда #Monitor-Name: - это имя, используемое для Perl-скрипта, хранящегося на ADC. Если вы не включите эту строку, то ваш скрипт не будет найден!

Следующие пункты являются обязательными:

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

Сценарии Perl выполняются в среде CHROOTED. Они часто вызывают другие приложения, такие как WGET или CURL. Иногда их нужно обновить для определенных функций, например SNI.

Динамические ценности

- my $host = $_[0]; ### IP или имя хоста (берется из данных RS или OOB, если используется)
- my $port = $_[1]; ### Порт хоста (берется из данных RS или OOB, если используется)
- my $content = $_[2]; ### Требуемое содержимое из настроек монитора (то, что должно быть видно в ответе)
- my $notes = $_[3]; ### заметки из данных RS в IP Services (используйте это для уникальной настройки каждого монитора RS)
- my $page = $_[4]; ### расположение страницы в настройках монитора
- my $user = $_[5]; ### имя пользователя из настроек монитора
- my $password = $_[6]; ### пароль из настроек монитора
- my $threshold = $_[7]; ### параметр порога из настроек монитора
- my $rsaddr = $_[8]; ### IP-адрес RS (отличается от _[0] в случае внеполосного мониторинга)
- my $rsport = $_[9]; ### RS-порт (отличается от _[1], если речь идет о внеполосном мониторинге)

- my $timeout = $_[10]; ### мониторинг таймаута контакта в секундах из IP Services > Real Server > Advanced > Monitoring Timeout

Индивидуальные проверки здоровья имеют два результата

- Успешно
  Возвращаемое значение 1
  Печать сообщения об успехе в Syslog
  Отметить реальный сервер в режиме онлайн (при условии совпадения IN COUNT)
- Неудачный
  Возвращаемое значение 2
  Печать сообщения о неудаче в Syslog
  Пометить реальный сервер как автономный (при условии совпадения OUT Count)

Пример пользовательского монитора здоровья

```
#Monitor-Name HTTPS_SNI
использовать строго:
предупреждения об использовании;
# Имя монитора, как указано выше, отображается в раскрывающемся списке Доступные проверки здоровья
# В этот скрипт передается 6 значений (см. ниже)
# Сценарий вернет следующие значения
# 1 - тест пройден 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":
}
else {
        $resolve = "$notes:$host";
}
if ($user && $password) {
        $auth = "-u $user:$password :
}
my @lines = 'curl -s -i -retry 1 -max-time 1 -k -H "Host:$notes --resolve $resolve $auth HTTPs://${notes}${page} 2>&1';
if(join(""@lines)=~/$content/)
        {
        print "HTTPs://$notes}${page} ищет - $content - Health check successful.\n";
```

```
        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

Использование RegEx - Все регулярные выражения должны использовать синтаксис операторов, совместимый с Perl.

SSL-сертификаты

Для успешного использования балансировки 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, проверить, управлять им, а затем снова зашифровать перед отправкой на целевой сервер.

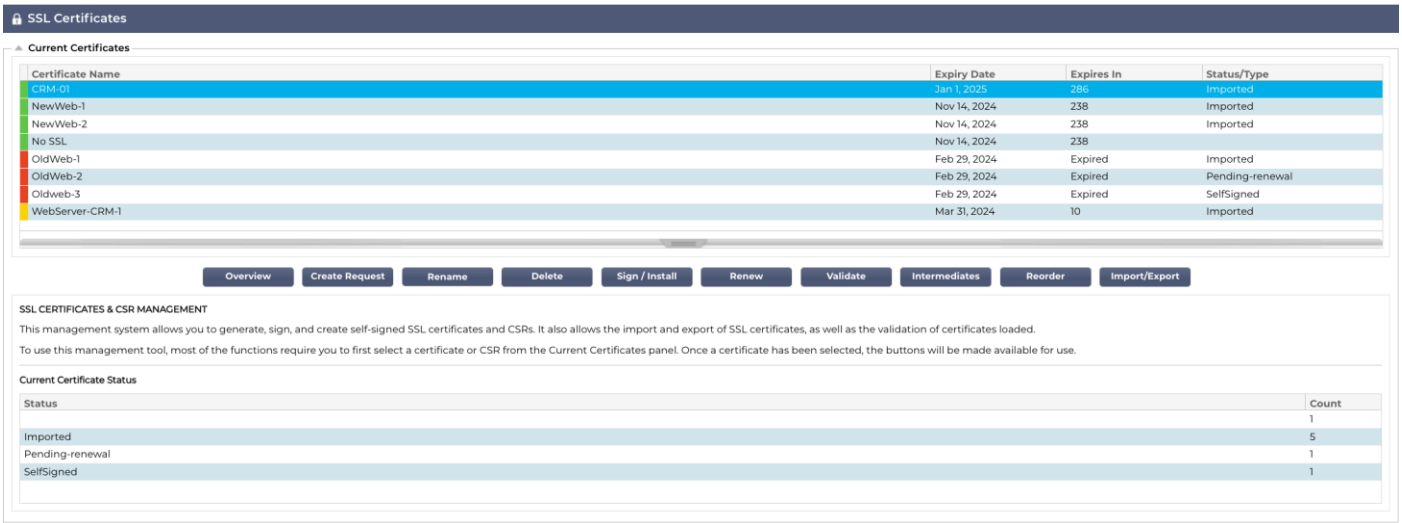
Сертификаты SSL могут варьироваться от самоподписанных сертификатов, которые может генерировать ADC, до традиционных сертификатов (с подстановочным знаком), доступных у надежных поставщиков. Также можно использовать сертификаты с доменной подписью, которые генерируются из Active Directory.

Что ADC делает с сертификатом SSL?

ADC может выполнять правила управления трафиком (flightPATH) в зависимости от того, что содержат данные. Это управление не может быть выполнено для данных, зашифрованных по протоколу SSL. Когда ADC нужно проверить данные, сначала их нужно расшифровать, а для этого ему необходим 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 сервер Real Server.

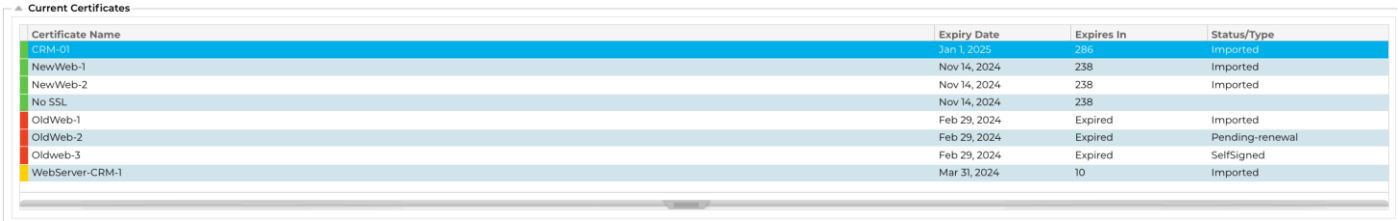
Диспетчер конфигурации SSL

В последующих версиях 196X реализован новый, более простой метод настройки и управления SSL-сертификатами и запросами сертификатов.



В диспетчере конфигурации SSL есть три основных раздела.

Область листинга сертификатов



В верхней части менеджера отображаются SSL-сертификаты, которые доступны для использования или ожидают активации от доверенного центра.

Сертификаты отображаются в виде четырех колонок, в которых указаны имя сертификата, дата истечения срока действия, Expires In (количество дней до истечения срока действия) и статус/тип сертификата.

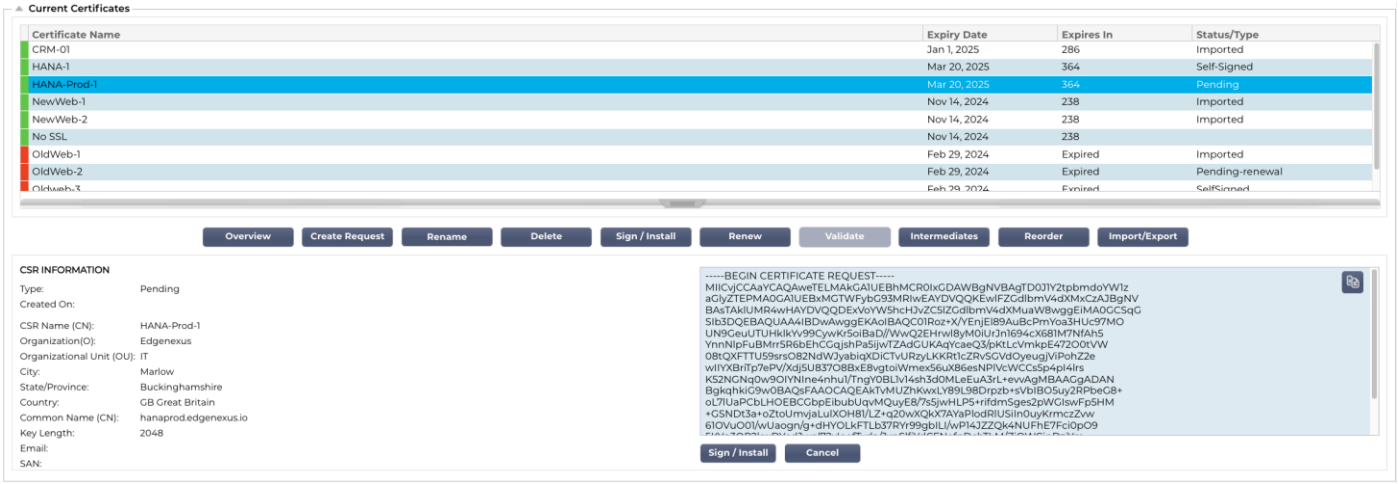
Цветовые коды

Как вы можете видеть, в каждой строке показан сертификат вместе с цветовым кодированным блоком. Ниже приведена таблица, в которой показаны различные блоки с цветовой кодировкой и их значение.

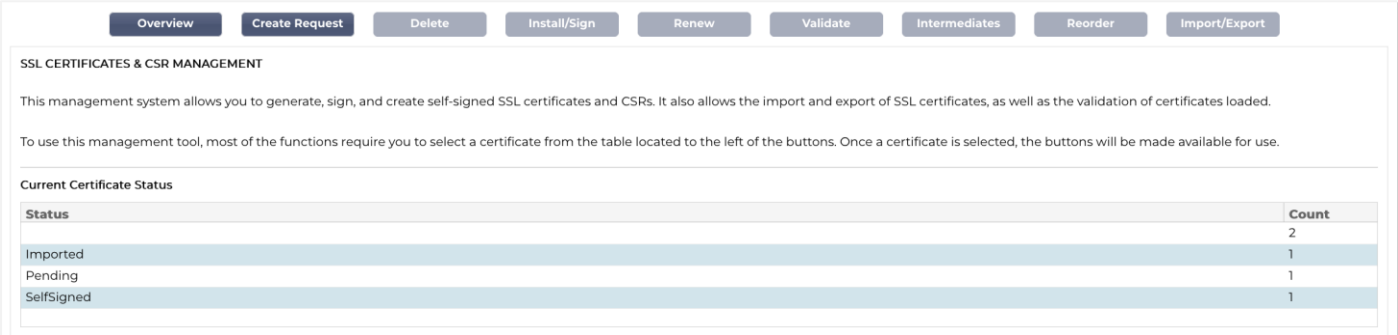
Цветовой код	Значение
	Сертификат является действующим и до истечения срока его действия остается более 60 дней
	Срок действия сертификата истекает менее чем через 30 дней
	Срок действия сертификата составляет от 30 до 60 дней
	Срок действия сертификата истекает, осталось <1 день
	Срок действия сертификата истек

Отображение информации о сертификате/CSR

При нажатии на сертификат или CSR информация о нем отображается на нижней панели. См. изображение ниже.

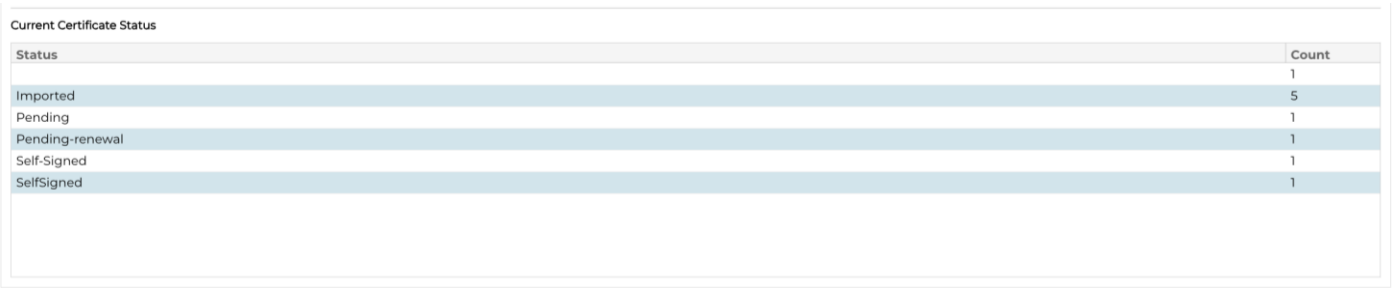


Кнопки действий и области конфигурации



Есть несколько кнопок действий, которые доступны и вступают в игру, когда сертификат выбран в Листинге.

Обзор



Кнопка "Обзор" отображает общую ситуацию по сертификатам в нижней части. В отличие от других действий, кнопка "Обзор" является независимой и не требует выбора сертификата.

Создать запрос

Если вы хотите создать самоподписанный сертификат или CSR, вам нужно нажать на кнопку Create Request. Откроется общая панель ввода, в которой можно указать все необходимые данные.

Имя сертификата AD (CN)

Это описательное поле, которое используется для отображения имени сертификата в ADC. Запись в поле должна быть алфавитно-цифровой без пробелов.

Организация (O)

В этом поле указывается название организации, которая будет использовать сертификат.

Организационное подразделение (OU)

Обычно используется для указания отдела или организационной единицы, но это необязательное поле.

Город/местность

Как следует из названия, пользователи обычно указывают, где находится организация.

Штат/провинция

Укажите в этом поле штат, округ или провинцию.

Страна

Это обязательное поле, которое необходимо заполнить, выбрав страну, в которой будет использоваться сертификат. Пожалуйста, убедитесь, что предоставленная здесь информация является точной.

Общее название (FQDN)

Это очень важное поле, которое используется для указания полного доменного имени (FQDN) сервера (серверов), который должен быть защищен с помощью сертификата. Это может быть что-то вроде www.edgenexus.io, или **edgenexus.io**, или даже подстановочный знак ***.edgenexus.io**. Вы также можете использовать IP-адрес, если хотите привязать к нему сертификат.

Длина ключа

Используется для указания длины ключа шифрования для сертификата SSL.

Период (дни)

Срок действия сертификата в днях. По истечении этого срока сертификат становится нерабочим.

Электронная почта

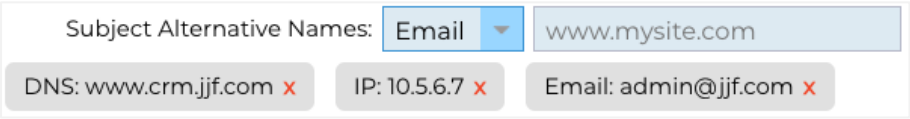
Это административный идентификатор электронной почты, используемый для сертификата.

Альтернативные названия предметов (SAN)

Subject Alternative Name (SAN) - это расширение SSL-сертификатов, позволяющее защищать несколько доменных имен в рамках одного сертификата. Эта функция особенно полезна для защиты веб-сайтов с несколькими поддоменами или различными доменными именами, позволяя использовать более рациональный и экономически эффективный подход к управлению SSL. Благодаря использованию SAN один SSL-сертификат может охватывать множество доменных имен и поддоменов, устраняя необходимость в отдельных сертификатах для каждого веб-адреса, тем самым упрощая процесс защиты веб-коммуникаций и обеспечивая шифрование данных в различных доменах.

Это поле состоит из двух элементов: выпадающего списка, позволяющего выбрать тип SAN, и текстового поля для указания значения.

EdgeADC имеет следующие доступные для использования SAN: DNS, IP-адрес, адрес электронной почты и URI. Вы можете выбрать и указать несколько SAN для сертификата или CSR.



Указанные SAN можно удалить, нажав на красный **x**, расположенный в каждом значении SAN.

- **DNS** - поле DNS Subject Alternate Name (SAN) позволяет указать дополнительные доменные имена, для которых действителен сертификат. В отличие от поля Common Name (CN), которое позволяет указать только один домен, поле SAN может включать несколько доменных имен, обеспечивая гибкость и масштабируемость при управлении сертификатами. Это особенно полезно для организаций, предоставляющих множество услуг в различных доменах и поддоменах, так как позволяет обеспечить безопасность связи для всех этих подразделений с помощью одного сертификата SSL/TLS, упрощая администрирование и повышая безопасность.
- **IP-адрес** - альтернативное имя IP-субъекта (SAN) позволяет включать IP-адреса наряду с доменными именами в качестве объектов, защищаемых сертификатом. Эта функция очень важна для защиты прямого доступа к службам через IP-адреса, обеспечивая возможность установления зашифрованных соединений при обращении к серверу не через его доменное имя, а непосредственно через IP-адрес. Применяя IP SAN, организации могут повысить безопасность своей сети, обеспечивая шифрование SSL/TLS как для доменных, так и для IP-соединений, что делает их универсальными для сред, в которых доменные имена могут не использоваться или быть предпочтительными для доступа к внутренним ресурсам или конкретным службам.
- **Email Address (Адрес электронной почты)** - параметр Email Address Subject Alternative Name (SAN) позволяет указать дополнительные адреса электронной почты, которые будут связаны с сертификатом, помимо основного домена или организации, для которой он был выпущен. Это позволяет сертификату подтвердить личность издателя для нескольких адресов электронной почты, а не только для одного домена или общего имени (CN). Это особенно полезно в сценариях, где требуется безопасная связь по электронной почте для различных адресов электронной почты одной и той же организации или подразделения, обеспечивая аутентификацию зашифрованных сообщений электронной почты и привязку к личности эмитента, подтвержденной сертификатом. Таким образом, Email Address SAN является ключевой функцией для повышения безопасности и надежности почтовых сообщений в зашифрованной среде.
- **URI** - URI (Uniform Resource Identifier) SAN используется для указания дополнительных идентификаторов, представленных в виде URI для одной сущности, защищенной сертификатом. В отличие от традиционных записей SAN, которые обычно включают доменные имена (DNS-имена) или IP-адреса, URI SAN позволяет сертификату связать сущность с определенными URI, такими как URL-адрес определенного ресурса или конечной точки службы. Это обеспечивает более гибкую и точную идентификацию, позволяя устанавливать защищенные соединения с конкретными ресурсами или службами в домене, а не только защищать сам домен, что повышает детализацию и область применения сертификатов SSL/TLS.

После правильного заполнения вы можете создать запрос на подписание сертификата (CSR) и отправить его на подписание в центр сертификации или создать самоподписанный сертификат для немедленного использования.

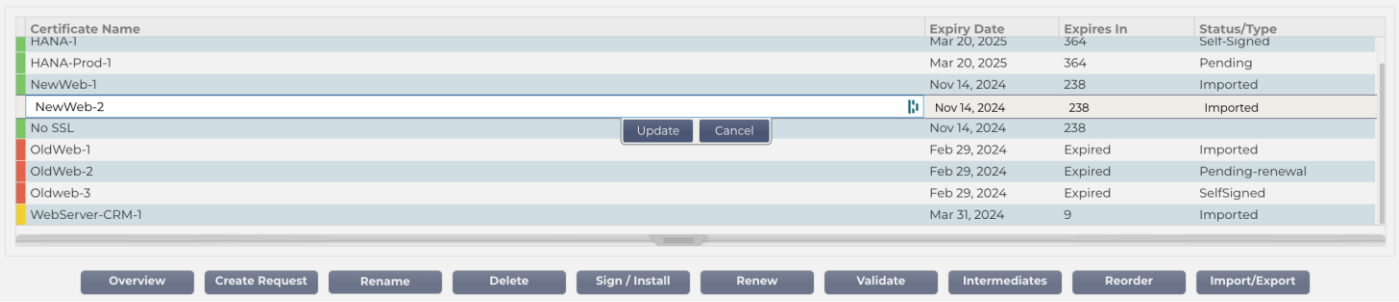
Кнопка "Отмена" отменит весь запрос, а кнопка "Сброс" сбросит все поля.

Переименовать

Кнопка Rename (Переименовать) позволяет переименовать сертификаты, которые не используются в виртуальных службах.

Чтобы воспользоваться этой функцией:

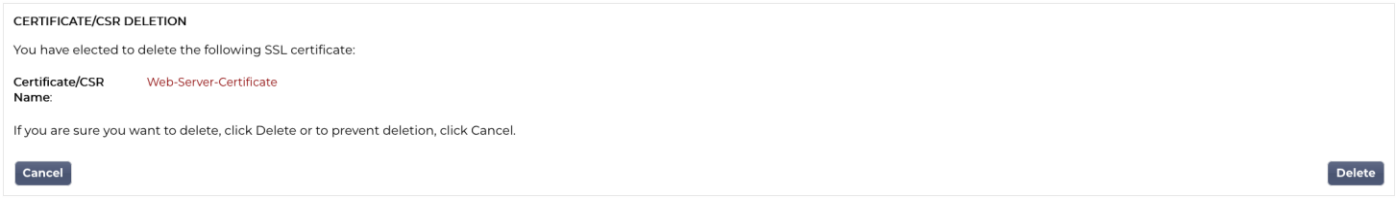
- Выделите сертификат, который нужно переименовать, и нажмите на кнопку Rename (Переименовать).
- Строка сертификата изменится, и вы сможете изменить его название.



- После этого нажмите кнопку Обновить.
- Вы также можете дважды щелкнуть на сертификате, чтобы переименовать его.

Удалить

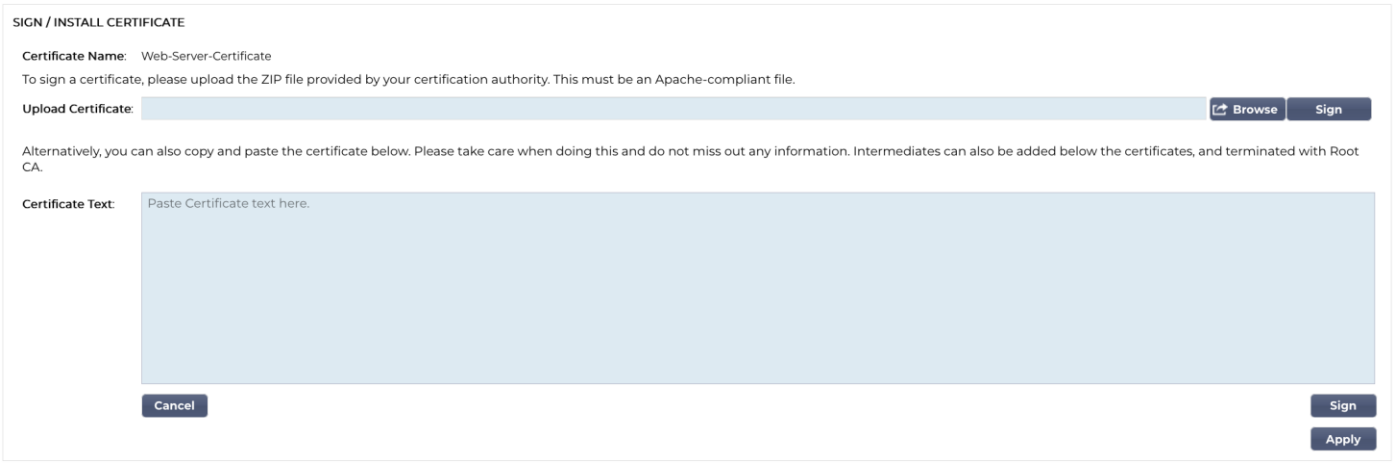
Кнопка Удалить будет доступна только при выборе сертификата. При нажатии на нее отображается следующее содержимое



В нижней панели отобразится запрос на удаление, а также имя сертификата, для которого было запрошено удаление.

Нажмите кнопку Удалить в правой нижней части панели, чтобы продолжить удаление.

Установка/подписание



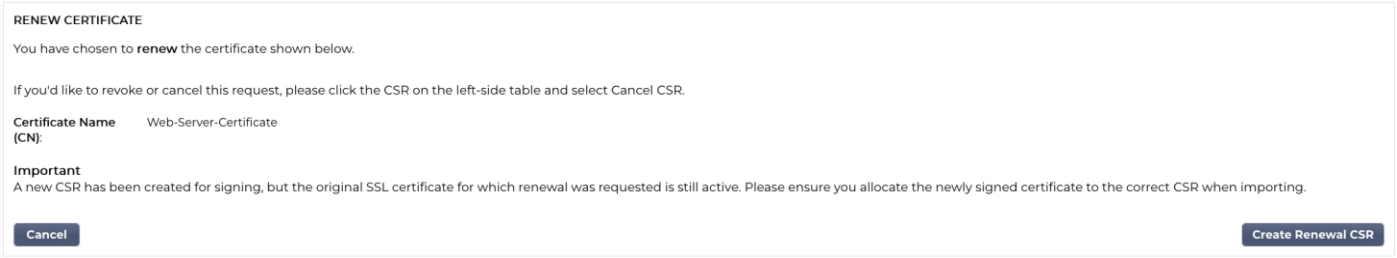
Когда вы создаете CSR и хотите, чтобы запрос был подписан центром сертификации (ЦС), вы отправляете CSR в ЦС. В ответ ЦС отправит подписанный сертификат вместе с файлом закрытого ключа и всеми промежуточными данными, необходимыми для правильной работы сертификата.

Они могут прислать вам ZIP-файл, содержащий все необходимые элементы, который можно загрузить с помощью верхней части правой панели.

Кроме того, вы можете создать набор сертификатов в текстовом редакторе и вставить его содержимое в поле Certificate Text (Текст сертификата) в нижней части панели.

После использования любого из этих способов нажмите кнопку Подписать, а затем кнопку Применить. Теперь подписанный сертификат будет отображаться в левой панели.

Обновить



Когда срок действия сертификата истекает, кнопка Продлить позволяет продлить и обновить сертификат. Существует два типа продления.

Самоподписанные сертификаты

Самоподписанные сертификаты, в отличие от доверенных, не могут быть обновлены с помощью CSR. Вместо этого самоподписанный сертификат обновляется путем представления новой конфигурации с использованием существующих данных. Пользователю разрешается указать новое имя сертификата и новое значение срока его действия.

После этого новый самоподписанный сертификат будет создан и сохранен в хранилище сертификатов. После этого администратор должен убедиться, что виртуальные службы, использующие сертификат, своевременно перенастроены.

Доверенные подписанные сертификаты

Когда речь идет о сертификатах, которым доверяют и которые подписаны центром сертификации, принято использовать CSR.

Когда вы нажмете на сертификат с истекающим сроком действия в верхней панели и нажмете кнопку Обновить, вам будет представлен новый CSR с текущими данными сертификата. Затем этот CSR можно загрузить и передать в центр сертификации для подписания, после чего подписанный сертификат можно установить.

У сертификата, который вы попросили продлить, появится новый статус - Renewing. После установки подписанного сертификата вам будет предложено присвоить сертификату новое имя. Оно будет отображаться как "Доверенный". Оригинальный сертификат будет сохранен, и все службы, использующие его, должны быть настроены на использование нового сертификата как можно скорее.

Подтвердить сертификат

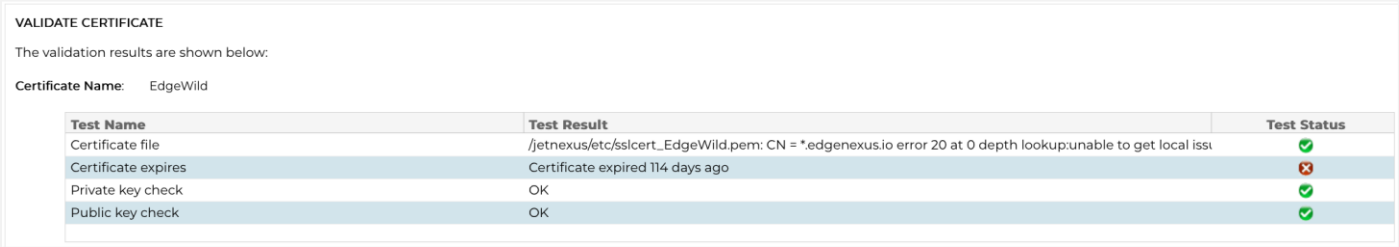
SSL-сертификат состоит из нескольких частей, и очень важно, чтобы эти части не только присутствовали, но и находились в правильном порядке. Ниже перечислены причины, по которым необходимо проверять SSL-сертификаты, полученные от сторонних организаций.

- **Аутентификация**: Проверка подлинности гарантирует, что сертификат получен от доверенного органа и удостоверяет личность веб-сайта или сервера. Это помогает предотвратить атаки типа "человек посередине", когда злоумышленник может перехватить обмен данными между клиентом и сервером.
- **Целостность**: Проверка сертификата SSL позволяет убедиться в том, что он не был подделан или изменен. Это очень важно для поддержания целостности защищенного соединения.
- **Проверка цепочки доверия**: Сертификаты SSL выпускаются центрами сертификации (ЦС). Проверка сертификата включает в себя проверку того, что он привязан к доверенному корневому ЦС. Этот процесс гарантирует, что сертификат является легитимным и ему можно доверять.
- **Статус отзыва**: Во время проверки также важно проверить, не был ли SSL-сертификат отозван центром сертификации, выдавшим его. Сертификат может быть отозван, если он был выдан ошибочно, закрытый ключ сайта был скомпрометирован или сайт больше не нуждается в сертификате. Импорт отозванного сертификата может привести к уязвимостям в системе безопасности.

- **Проверка срока действия**: SSL-сертификаты действительны в течение определенного периода. Проверка сертификата при импорте включает в себя проверку срока его действия, чтобы убедиться, что он все еще действителен. Использование сертификата с истекшим сроком действия может привести к уязвимостям и заставить браузеры или клиентов отклонить безопасное соединение.
- **Конфигурация и совместимость**: Проверка гарантирует, что конфигурация сертификата совместима с политикой безопасности клиента и техническими требованиями сервера или приложения. Сюда входит проверка используемых алгоритмов, назначения сертификата и других технических деталей.
- **Соответствие нормам**: В некоторых отраслях нормативные акты могут требовать подтверждения сертификатов SSL для обеспечения безопасной работы с конфиденциальной информацией. Это особенно важно в таких отраслях, как финансы, здравоохранение и электронная коммерция.

Система управления SSL ADC позволяет проверять импортированный сертификат SSL.

- Выберите импортированный сертификат SSL.
- Нажмите кнопку Проверить.
- Результаты можно увидеть на нижней панели, как показано на изображении ниже.



Добавление посредников

Как уже говорилось, SSL-сертификаты состоят из нескольких частей, одна из которых - промежуточные сертификаты, составляющие цепочку.

Менеджер SSL Manager в ADC позволяет добавить все недостающие промежуточные сертификаты.

- Щелкните на SSL, к которому вы хотите добавить промежуточный сертификат.
- Нажмите кнопку "Посредники".
- Появится панель, как на рисунке ниже.

- Вставьте содержимое промежуточного сертификата.
- Нажмите кнопку Применить.

Возможно, вам потребуется изменить порядок промежуточных сертификатов, чтобы SSL-сертификат проверялся правильно. Это делается с помощью кнопки Reorder.

Повторный заказ

Чтобы сертификат SSL работал правильно, он должен быть расположен в правильном порядке.

Золотое правило заключается в том, что сертификат отправителя должен быть первым, а последний корневой сертификат - последним в цепочке. В общем случае это выглядит примерно так, как показано ниже:

```
Первоначальный эмитент > Промежуточный 1 > Окончательный корень.
```

Final Root - это доверенный корневой сертификат, предоставленный центром сертификации.

В некоторых случаях имеется несколько промежуточных сертификатов, которые также должны быть размещены в правильном положении. По сути, каждый следующий сертификат должен подтверждать предыдущий. В итоге это может выглядеть следующим образом.

```
Первоначальный эмитент > Промежуточный 1 > Окончательный корень
```

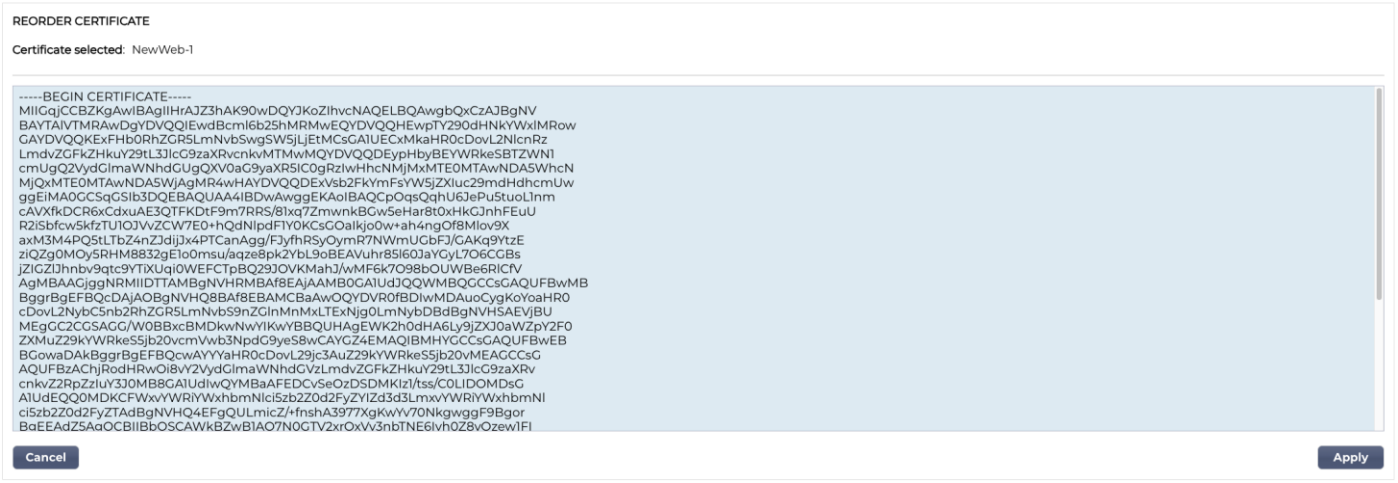
Когда вы импортируете, скажем, промежуточный продукт 2, он может оказаться в конце цепочки, что приведет к отказу в сертификации. Следовательно, необходимо изменить порядок и поместить промежуточный продукт 2 в правильное положение (показано красным).

Таким образом, окончательный вариант будет выглядеть так:

```
Оригинальный эмитент > Промежуточный 1 > Промежуточный 2 >  Окончательный корень
```

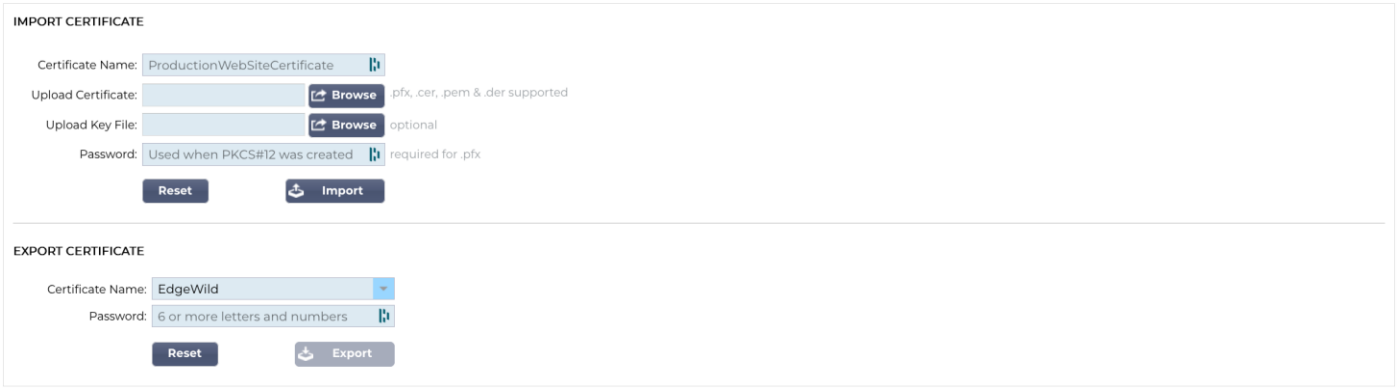
```
----- НАЧАЛО СЕРТИФИКАТА-----
MIIFKTCCBBGgAwIBAgISA/UUyBjJ71fucZuvpiLsdfsdfsdfd
...
hoFWWJt3/SeBKn+ci03RRvZsdfdsfsdfw=
-----END CERTIFICATE-----
----- НАЧАЛО СЕРТИФИКАТА-----
MIIFFjCCAv6gAwIBAgIRAJErCErPDBinsdfsfsdfsdfsfsdfsd
....
nLRbwHqsdqD7hHwg==
-----END CERTIFICATE-----
----- НАЧАЛО СЕРТИФИКАТА-----
MIIFYDCCBsdfSDFSDFVSDVzfsdffvqdsfgsT664ScbvsfGDGSDV
...
Dfvp7OOGAN6dEOM4+SDFSDZET+DFGDFQSD45Bddfghqsqf6Bsff
-----END CERTIFICATE-----
----- НАЧАЛО СЕРТИФИКАТА-----
MIIFYDCCBsdfSDFSDFVSDVzfsdffvqdsfgsT664ScbvsfGDGSDV
...
Dfvp7OOGAN6dEOM4+SDFSDZET+DFGDFQSD45Bddfghqsqf6Bsff
-----END CERTIFICATE-----
```

После выбора сертификата и нажатия кнопки Reorder раздел Reorder выглядит так, как показано на рисунке ниже.



Чтобы изменить порядок разделов сертификата, вы можете скопировать текст в поле, отредактировать и изменить порядок содержимого в текстовом редакторе, а затем вставить его обратно, чтобы заменить существующее содержимое. После этого нажмите кнопку Применить.

Импорт/экспорт



Когда вы получаете сертификат от поставщика SSL-сертификатов, он поставляется в виде ZIP-файла или набора файлов. Они содержат SSL-сертификат, файл ключа и корневой ca, а также все промежуточные файлы

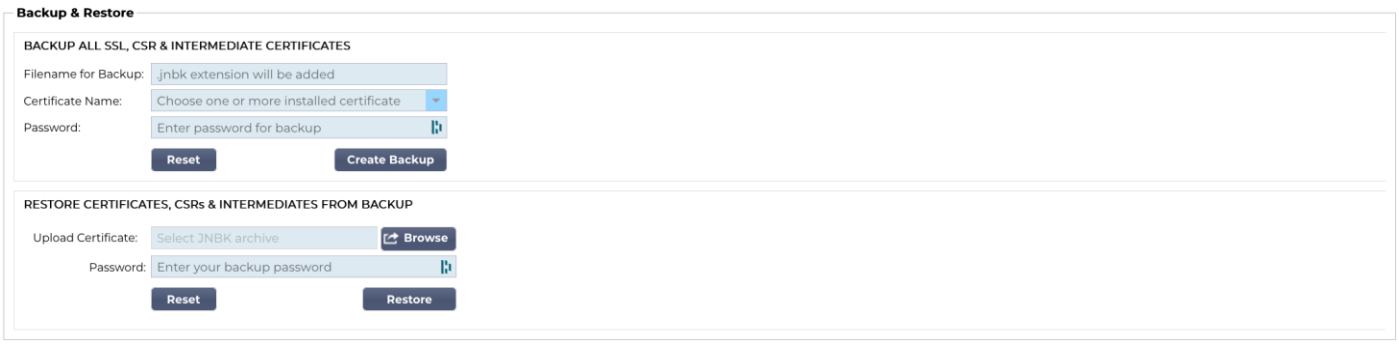
Вам нужно будет импортировать их в ADC, и поэтому мы предоставили метод их импорта.

Существует несколько форматов сертификатов SSL, таких как CER, DER, PEM и PFX. Некоторые форматы требуют добавления файла KEY в процедуру импорта. Файлы PFX требуют ввода пароля для импорта сертификата PFX.

Мы также предусмотрели возможность экспорта сертификата из ADC, если это необходимо. При экспорте файл будет иметь формат PFX, поэтому для его создания требуется пароль.

Резервное копирование и восстановление

Резервное копирование



Чтобы создать резервную копию сертификатов в хранилище сертификатов ADC:

- Добавьте имя файла, который будет использоваться для резервного копирования.
- С помощью раскрывающегося меню выберите один сертификат или ВСЕ для резервного копирования всех сертификатов.
- Добавить пароль
- Нажмите кнопку Создать резервную копию.
- Созданный файл - это файл JNBK, который зашифрован.

ВАЖНО

Резервное копирование будет работать только с импортированными сертификатами Trusted.

Восстановить

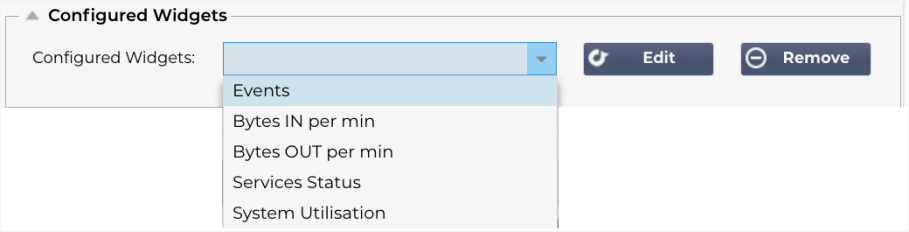
Чтобы восстановить резервную копию, воспользуйтесь нижней частью раздела "Резервное копирование и восстановление".

- Перейдите к файлу резервной копии и найдите его.
- Введите пароль.
- Нажмите кнопку Восстановить.
- Сертификаты из файла резервной копии будут восстановлены.

Виджеты

Страница "Библиотека > Виджеты" позволяет настроить различные легкие визуальные компоненты, отображаемые на пользовательской приборной панели.

Настроенные виджеты

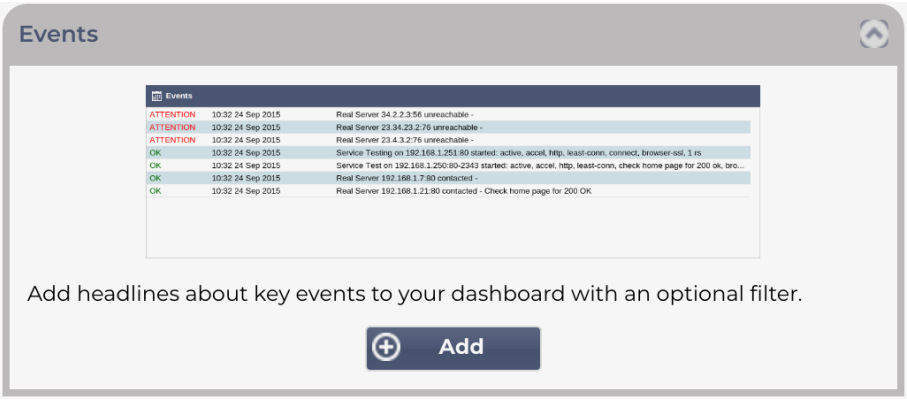


Раздел "Настроенные виджеты" позволяет просматривать, редактировать или удалять любые виджеты, созданные в разделе "Доступные виджеты".

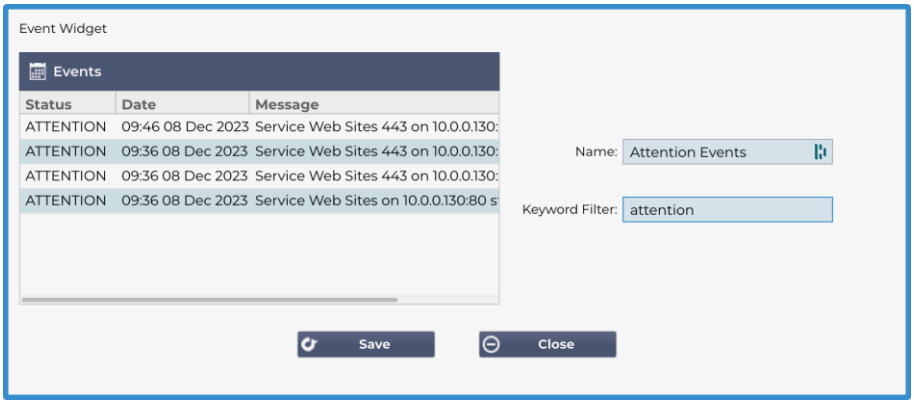
Доступные виджеты

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

Виджет событий

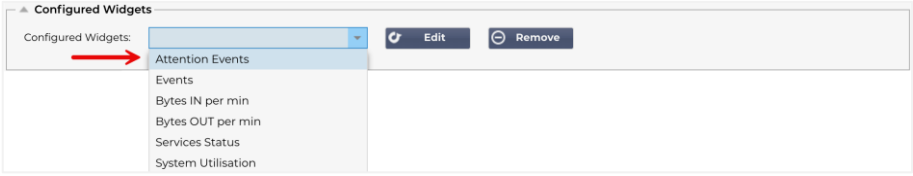


- Чтобы добавить событие в виджет "События", нажмите кнопку "Добавить".
- Укажите название мероприятия. В нашем примере мы добавили Attention Events в качестве названия события.
- Добавьте фильтр по ключевым словам. Мы также добавили значение фильтра Attention



- Нажмите Сохранить, затем Закрыть

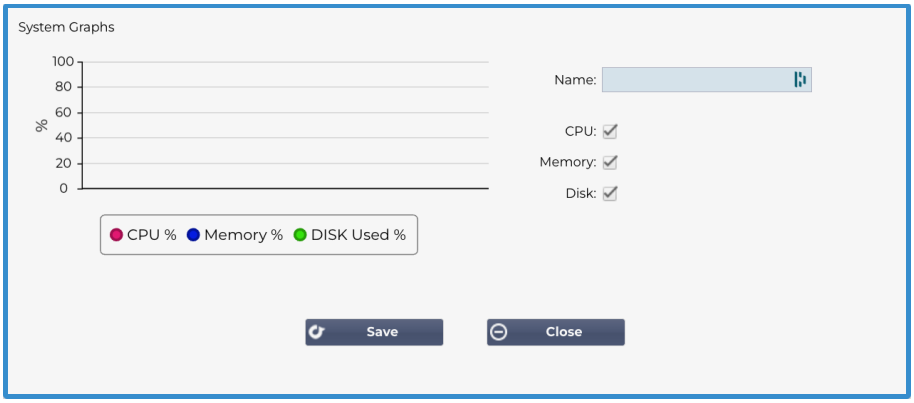
- Теперь вы увидите дополнительный виджет под названием Attention Events в раскрывающемся списке Configured Widgets.



- Вы можете видеть, что теперь мы добавили этот виджет в раздел View > Dashboard.
- Выберите виджет "Внимание, события", 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

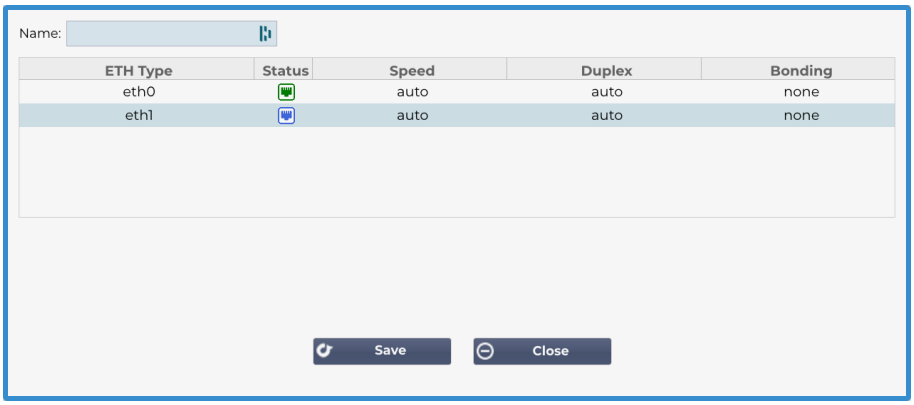


В АЦП имеется настраиваемый виджет "Системный график". Нажав кнопку Добавить на виджете, вы можете добавить следующие графики мониторинга для отображения.

- ПРОЦЕССОР
- ПАМЯТЬ
- ДИСК

После добавления они будут по отдельности доступны в меню виджетов Dashboard.

Виджет интерфейса



Виджет Interface позволяет отображать данные для выбранного сетевого интерфейса, например ETH0, ETH1 и так далее. Количество доступных для добавления интерфейсов зависит от того, сколько сетевых интерфейсов вы определили для виртуального устройства или выделили в аппаратном устройстве.

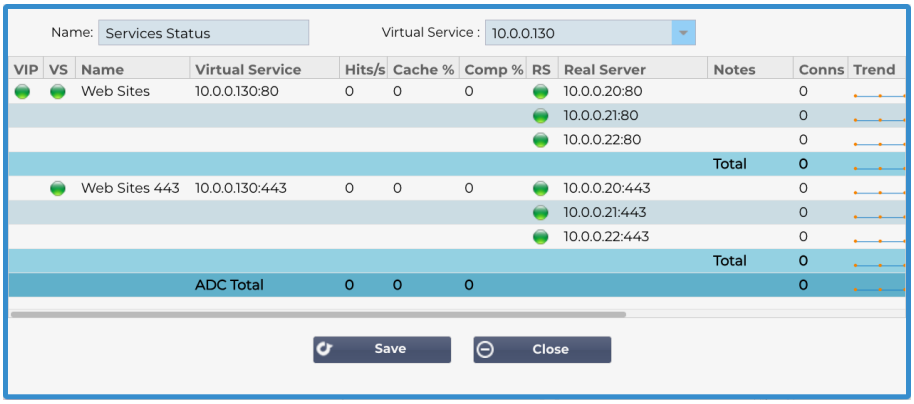
После завершения нажмите кнопку Сохранить, а затем кнопку Закрыть.

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

Виджет состояния

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

- Нажмите кнопку Добавить.



- Введите имя службы, которую вы хотите контролировать.
- Вы также можете выбрать столбцы, которые хотите отобразить в виджете, нажав на заголовок столбца.
- Когда вы будете удовлетворены, нажмите кнопку Сохранить, а затем Закрыть.
- Выбранный виджет Status будет доступен в разделе Dashboard.

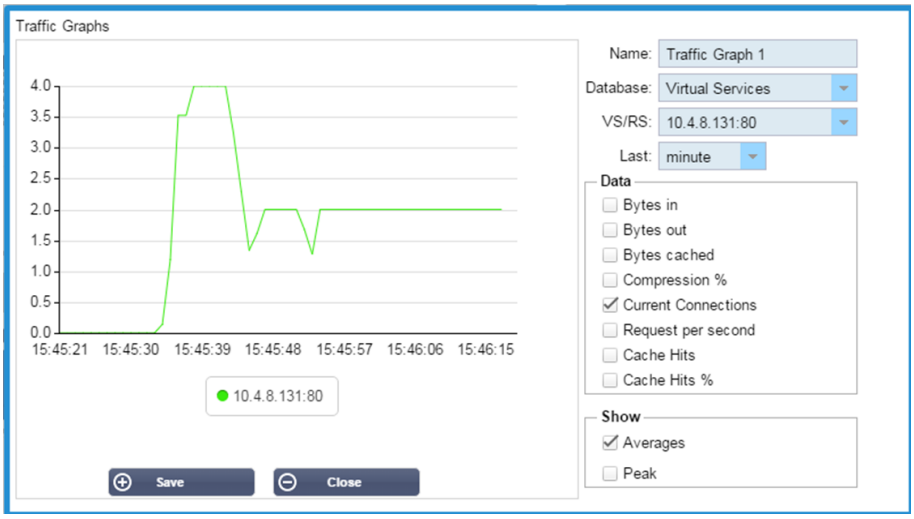
Виджет графики трафика

Этот виджет можно настроить на отображение текущих и исторических данных о трафике для виртуальных служб и реальных серверов. Кроме того, можно просмотреть общие текущие и исторические данные по глобальному трафику

- Нажмите кнопку Добавить
- Назовите свой виджет.
- Выберите базу данных из списка Виртуальные службы, Реальные серверы или Система.
- 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
    - Выдача байтов
    - Кэшированные байты
    - Сжатие %
    - Текущие соединения
    - Запросы в секунду
    - Хиты кэша
    - Хиты кэша %
- Настоящие серверы
    - Байты в
    - Выдача байтов
    - Текущие соединения
    - Запрос в секунду
    - Время отклика
- Система
    - % ПРОЦЕССОРА
    - Услуги центрального процессора
    - Память %
    - Свободный диск %
    - Байты в

- Выдача байтов
- Выбор отображения средних или пиковых значений
- Выбрав все параметры, нажмите кнопку Сохранить и закрыть.

Пример графика трафика



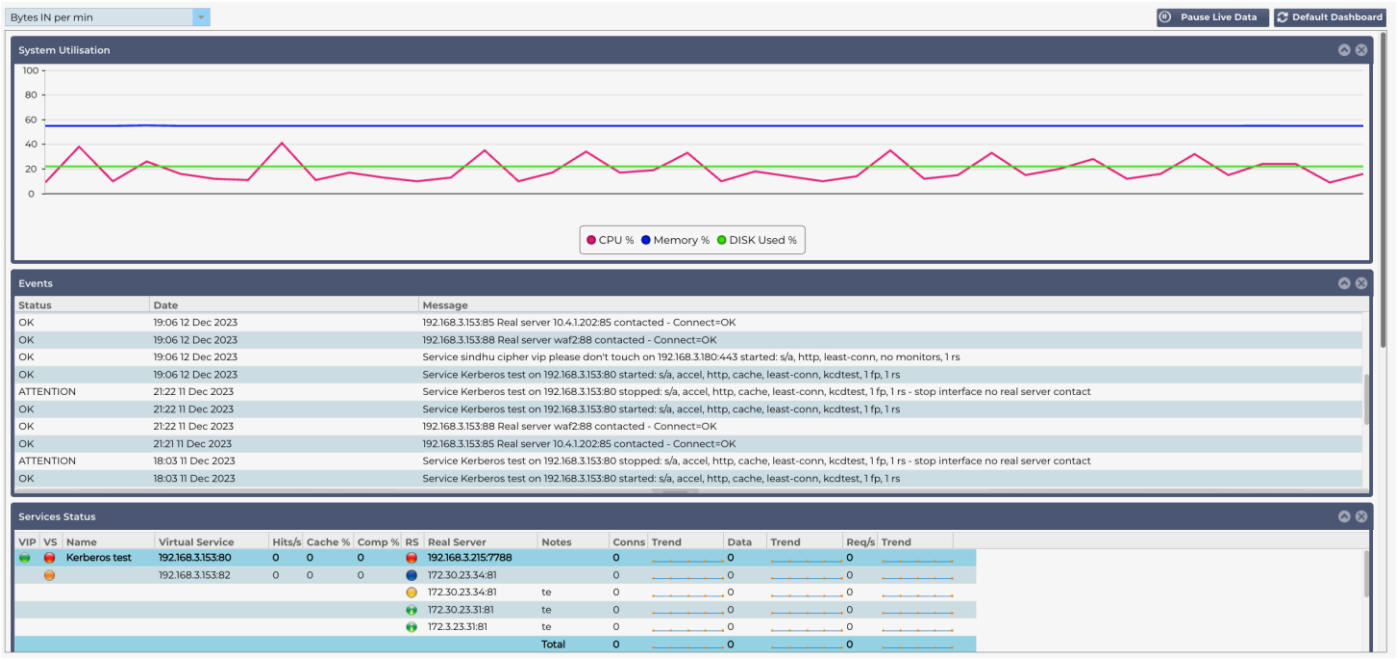
Теперь вы можете добавить свой виджет Traffic Graph в панель View> Dashboard.

Посмотреть

Приборная панель

Как и во всех интерфейсах управления ИТ-системами, часто возникает необходимость просмотреть показатели производительности и данные, которые обрабатывает ADC. Мы предоставляем настраиваемую приборную панель, с помощью которой вы сможете легко и удобно это сделать.

Панель Dashboard доступна с помощью сегмента View на панели навигатора. При выборе он показывает несколько виджетов по умолчанию и позволяет 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 выбирать и добавлять любые стандартные или пользовательские виджеты, которые вы определили. Чтобы воспользоваться этим меню, выберите виджет из выпадающего списка.

Кнопка приостановки данных в реальном времени

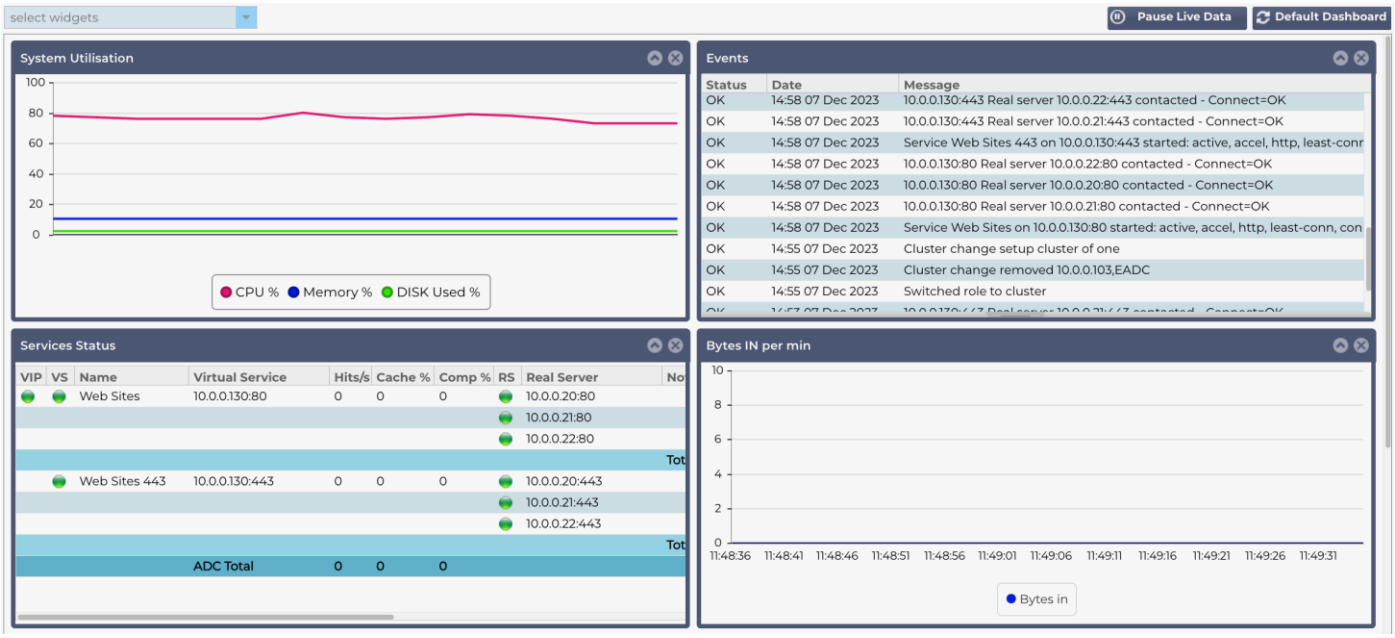
Эта кнопка позволяет выбрать, должен ли ADC обновлять приборную панель в режиме реального времени. После приостановки ни один виджет приборной панели не будет обновляться, что позволит вам изучать содержимое в свое удовольствие. После приостановки кнопка переходит в состояние Play Live Data.

По окончании просто нажмите кнопку Play Live Data, чтобы возобновить сбор данных и обновить приборную панель.

Кнопка приборной панели по умолчанию

Может случиться так, что вы захотите сбросить настройки 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, обозначающий 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 любой момент, щелкнув по строке заголовка виджета. Это действие свернет виджет и отобразит только строку заголовка.

Перемещение порядка виджетов

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

Удаление виджета

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

История

Опция History (История), выбираемая в навигаторе, позволяет администратору изучить исторические показатели работы ADC. Исторические представления могут быть созданы для виртуальных служб, реальных серверов и системы.

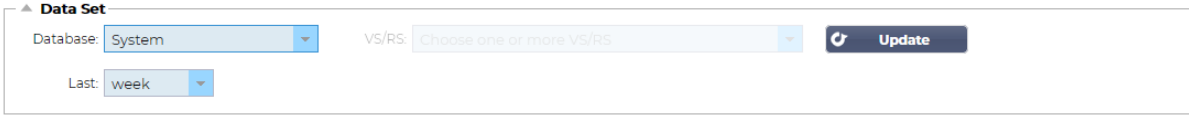
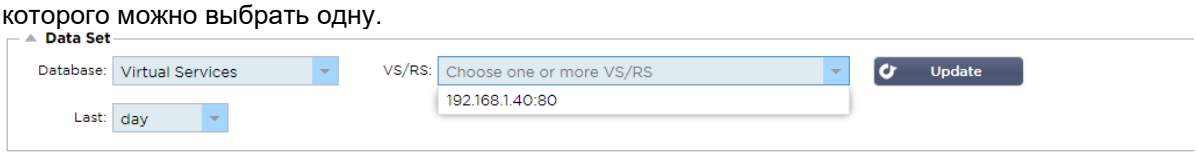
Это также позволяет увидеть балансировку нагрузки в действии и выявить любые ошибки или закономерности, требующие изучения. Обратите внимание, что для использования этой функции необходимо включить ведение исторического журнала в разделе Система > История.

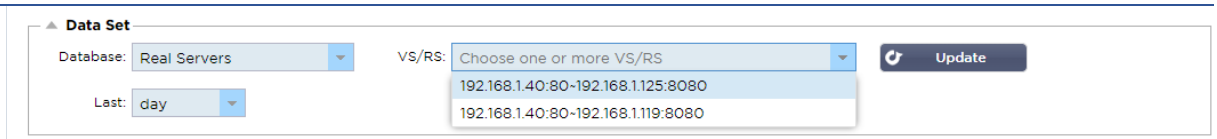
Просмотр графических данных

Набор данных

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

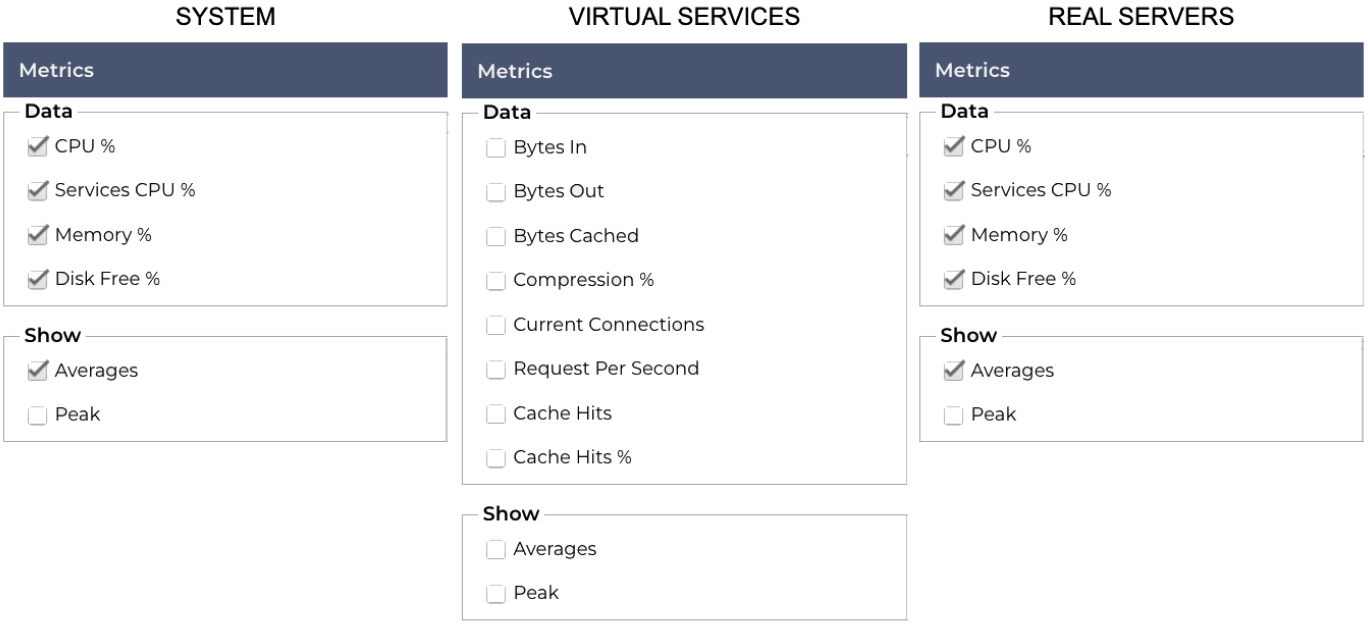
Сначала нужно выбрать базу данных и период, относящийся к информации, которую вы хотите просмотреть. В раскрывающемся списке Last можно выбрать следующие периоды: минута, час, день, неделя, месяц и год.

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. Появится список виртуальных служб, из которого можно выбрать одну. 
Реальные услуги	Выбрав эту базу данных, вы сможете выбрать все Real Servers в базе данных с момента начала регистрации данных. Появится список реальных серверов, из которого можно выбрать один.

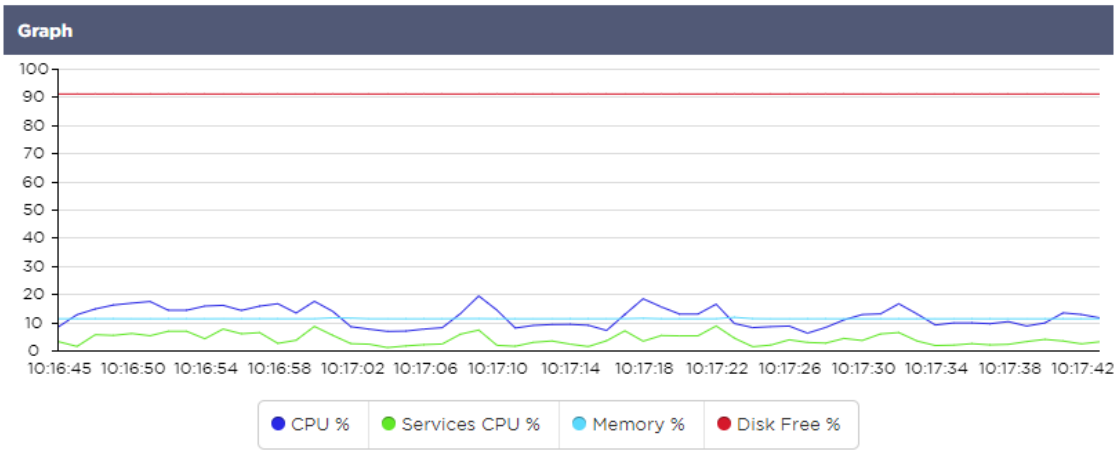


Метрики

После того как вы выбрали набор данных, который 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).



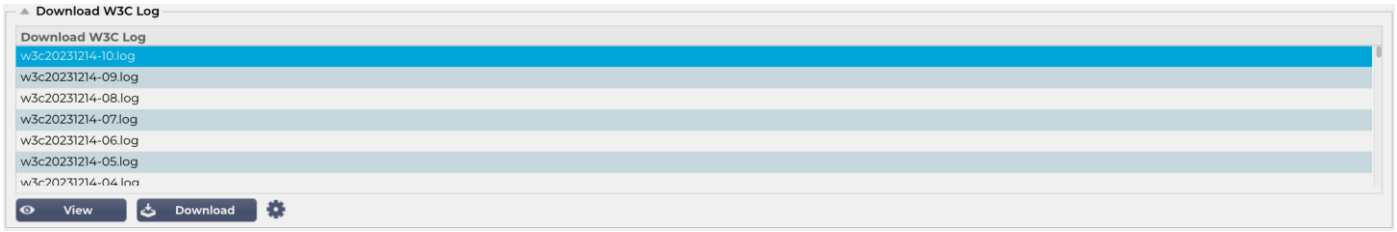
Образец графика



Журналы

Страница Logs в разделе View позволяет просматривать и загружать журналы W3C и System. Страница состоит из двух разделов, как показано ниже.

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 IP-адрес источника, версию HTTP, тип браузера, страницу, на которую ссылается пользователь, и временную метку. Журналы W3C могут быть очень большими в зависимости от объема данных и категории регистрируемой информации.

В разделе W3C вы можете выбрать нужный вам журнал, а затем просмотреть или скачать его.

Просмотр кнопки

Кнопка View (Просмотр) позволяет просмотреть выбранный журнал в окне текстового редактора, например Notepad.

Скачать кнопку

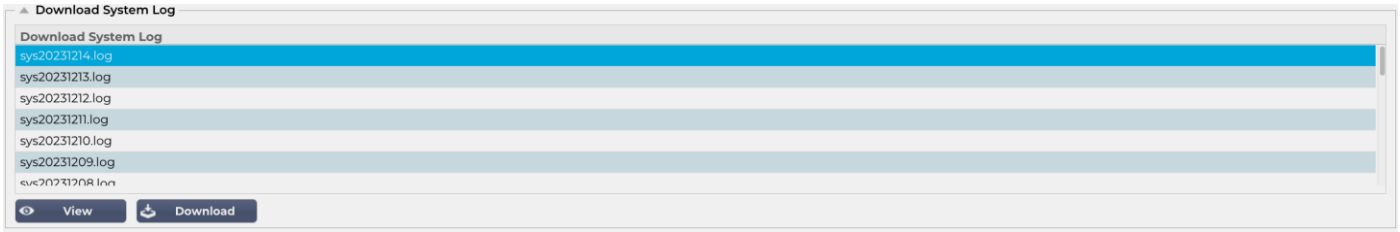
Эта кнопка позволяет загрузить журнал в локальное хранилище для последующего просмотра.

Значок шестеренки

Щелкнув на этом значке, вы перейдете в раздел настроек журнала W3C, расположенный в разделе Система > Ведение журнала. Мы подробно обсудим это в разделе "Ведение журнала".

Системный журнал

Системный журнал очень важен для отладки или изучения того, что происходило с ADC. Он предназначен для достаточно опытных сотрудников ИТ-отдела.



Просмотр кнопки

Кнопка View (Просмотр) позволяет просмотреть выбранный журнал в окне текстового редактора, например Notepad.

Скачать кнопку

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

Статистика

Раздел статистики ADC - это часто используемая область для системных администраторов, которые хотят убедиться, что производительность ADC соответствует их ожиданиям.

Компрессия

Задача ADC - отслеживать данные и направлять их на серверы Real Servers, настроенные на их получение. Функция сжатия данных предусмотрена в ADC для повышения производительности ADC. В некоторых случаях администраторы захотят протестировать и проверить информацию о сжатии данных ADC; эти данные предоставляются панелью Compression в Statistics.

Сжатие контента на сегодняшний день

Content Compression To Date	
Compression	0%
Throughput Before Compression	0
Throughput After Compression	0

Данные, приведенные в этом разделе, отражают степень сжатия, достигнутую АЦП на сжимаемом содержимом. Значение 60-80 % является типичным.

Общая компрессия на сегодняшний день

Overall Compression To Date			Current Values
Compression	0%		0%
Throughput Before Compression	0		0.00 Mbps (data)
Throughput After Compression	0		0.00 Mbps (data)
Throughput From Cache	0		0.00 Mbps (data)
		Total	0.00 Mbps (data)

Значения, представленные в этом разделе, показывают, насколько сильно ADC сжал все содержимое. Типичный процент зависит от того, сколько предварительно сжатых изображений содержится в ваших сервисах. Чем больше количество изображений, тем меньше будет общий процент сжатия.

Общий ввод/вывод

Total Input	345.9 MB	Input/s	12.7 kbps
Total Output	296.8 MB	Output/s	25.7 kbps

Показатели общего ввода/вывода представляют собой количество необработанных данных, проходящих через АЦП и выходящих из него. Единица измерения меняется по мере роста размера от кбит/с до Мбит/с и Гбит/с.

Хиты и связи

Content Caching	Hits	Bytes
From Cache	0 / -	0 / -
From Server	0 / -	0 / -
Cache Contents	0 entries	0 / 0.0%

Раздел "Хиты и соединения" содержит общую статистику хитов и транзакций, прошедших через ADC. Что же означают хиты и соединения?

- Хит определяется как транзакция уровня 7. Обычно используется для веб-серверов и представляет собой GET-запрос на объект, например изображение.
- Соединение определяется как TCP-соединение 4-го уровня. Через одно TCP-соединение может проходить множество транзакций.

Общее количество подсчитанных хитов

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

Всего соединений

Значение Total Connections представляет собой суммарное количество TCP-соединений с момента последнего сброса. Цифра во втором столбце указывает на количество TCP-соединений, выполняемых в секунду с ADC. Цифра в правом столбце - это количество TCP-соединений в секунду, выполненных с реальными серверами. Пример 6/8 соединений/сек. В приведенном примере мы имеем 6 TCP-соединений в секунду с виртуальной службой и 6 TCP-соединений в секунду с реальными серверами.

Пиковые соединения

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

Кэширование

Как вы помните, ADC 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.

Content Caching	Hits	Bytes
From Cache	0 / -	0 / -
From Server	0 / -	0 / -
Cache Contents	0 entries	0 / 0.0%

Из кэша

Хиты: В первом столбце указано общее количество транзакций, обслуживаемых из кэша ADC с момента последнего сброса. Также приводится процентное соотношение от общего числа транзакций.

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

От сервера

Хиты: В столбце 1 указано общее количество транзакций, обслуживаемых с реальных серверов с момента последнего сброса. Также приводится процентное соотношение от общего числа 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.

Буфер приложений

Buffer Type	Connections Used/Free	Memory Used/Free	Average Buffer Fill Size
Low	0/5k(0%)	0/655MB(0%)	0
Medium	0/5k(0%)	0/30MB(0%)	0
High	0/10k(0%)	0/20MB(0%)	0

Использование буферов приложений в ADC помогает оптимизировать производительность, повысить пропускную способность и обеспечить надежный и эффективный поток данных между клиентами и серверами. Размеры буферов, политики обработки и другие параметры оптимизируются ADC для точной настройки нагрузки в соответствии с конкретными требованиями приложений и инфраструктуры.

В EdgeADC мы делаем всю работу за вас и автоматически настраиваем параметры буфера в зависимости от потребностей.

Постоянство сеанса

Total current sessions	0
% used (of max)	0
New sessions this min	0
Revalidations this min	0
Expired sessions this min	0

Раздел Session Persistence содержит информацию о нескольких параметрах.

Всего текущих сеансов

Это показывает, сколько сеансов персистенции находится в процессе - обновляется каждую минуту

% Использовано (от макс.)

Это показывает, сколько места используется для информации о сеансе.

Новый сеанс в эту минуту

Это показывает, сколько новых сеансов персистентности было добавлено в течение последней минуты.

Переоценить этот мин

Это показывает, в течение последней минуты, сколько существующих сеансов персистентности было повторно подтверждено большим количеством трафика

Просроченные сеансы в эту минуту

Это показывает, сколько сеансов персистенции истекло за последнюю минуту из-за отсутствия трафика в течение таймаута.

Оборудование

Независимо от того, используете ли вы ADC в виртуальной среде или в аппаратном обеспечении, в этом разделе вы найдете ценную информацию о производительности устройства.

Disk Usage	2%
Memory Usage	10.1%(185.4MB of 1832.7MB)
CPU Usage	76.0%

Использование диска

Значение, указанное в столбце 2, представляет собой процент используемого в данный момент дискового пространства и включает информацию о файлах журнала и кэш-данных, которые периодически сохраняются на хранилище.

Использование памяти

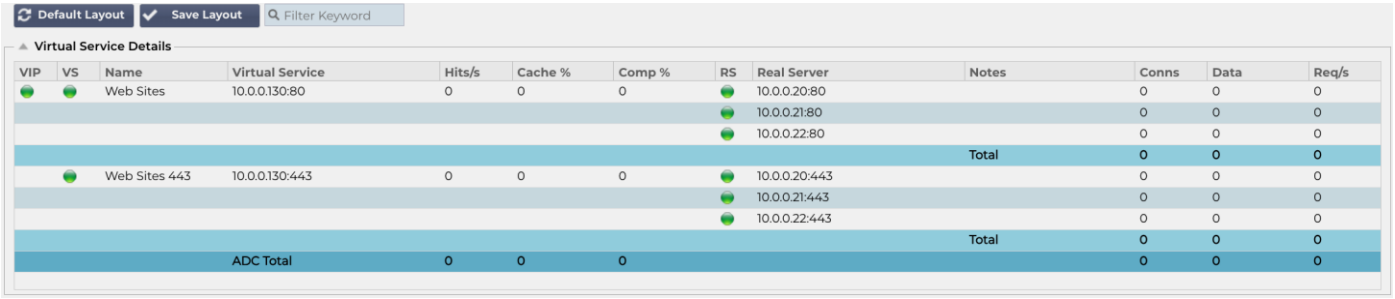
Во втором столбце указан процент памяти, используемой в данный момент. Более значимое число в скобках - это общий объем памяти, выделенный для АЦП. Рекомендуется выделять АЦП не менее 2 ГБ оперативной памяти.

Использование процессора

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

Статус

На странице Вид > Статус 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

VIP-колонна

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

Статус	Описание
●	Онлайн
●	Failover-Standby. Эта виртуальная служба работает в режиме горячего резерва
●	Указывает на то, что "пассив" задерживает "актив".
●	В автономном режиме. Реальные серверы недоступны, или не включены реальные серверы
●	Состояние поиска
●	Не лицензировано или превышено количество лицензированных виртуальных IP-адресов

Колонка состояния VS

Цвет индикатора указывает на состояние виртуальной службы.

Статус	Описание
●	Онлайн
●	Failover-Standby. Эта виртуальная служба работает в режиме горячего резерва
●	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 режим Offline. Трафик будет продолжать идти, но с уменьшенной мощностью реального сервера.
●	В автономном режиме. Реальные серверы недоступны, или не включены реальные серверы
●	Состояние поиска
●	Не лицензировано или превышено количество лицензированных виртуальных IP-адресов

Имя

Имя виртуальной службы

Виртуальная служба (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%

Приведенная здесь цифра представляет собой процент объектов, которые были обслужены из RAM-кэша ADC.

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 подключено
●	Состояние поиска
●	Не лицензировано или превышено количество лицензированных виртуальных IP-адресов

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 соединений с каждым сервером Real Server позволяет увидеть балансировку нагрузки в действии. Это очень полезно для проверки правильности работы политики балансировки нагрузки.

Данные

Значение в этом столбце показывает объем данных, отправляемых на каждый сервер Real Server.

Req/Sec (запросы в секунду)

Количество запросов в секунду, отправляемых на каждый сервер Real Server.

Система

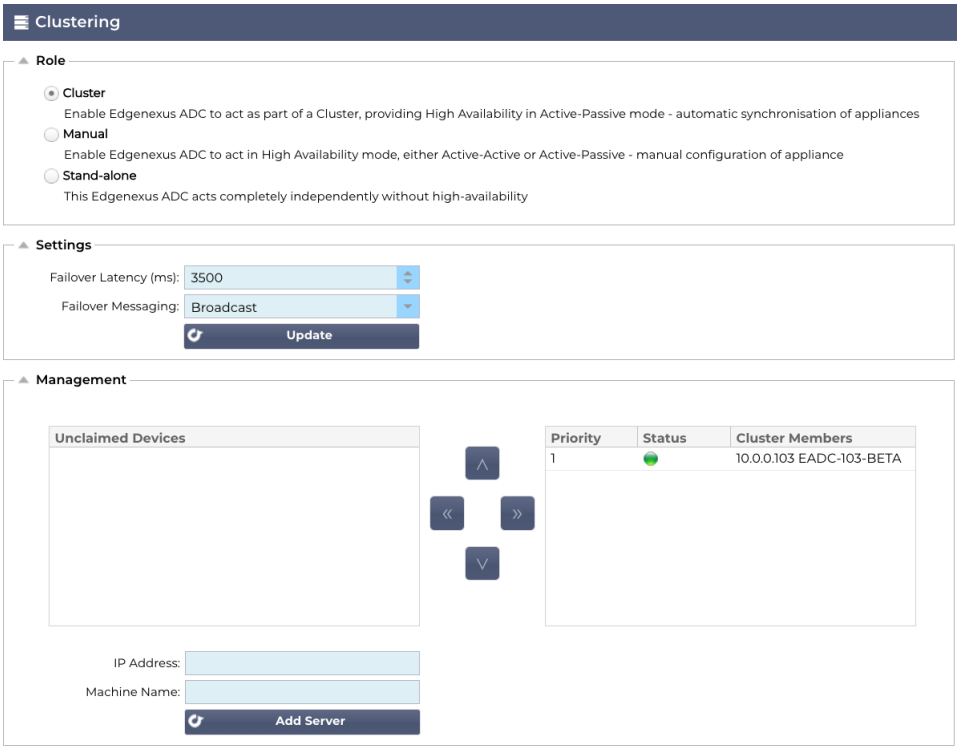
Кластеризация

ADC можно использовать как одиночное автономное устройство, и он будет отлично работать в этом качестве. Однако если учесть, что назначение ADC - балансировать нагрузку серверов, необходимость кластеризации самого ADC становится очевидной. Удобный пользовательский интерфейс ADC делает настройку системы кластеризации простой и понятной.

На странице Система > Кластеризация настраивается высокая доступность устройств ADC. Этот раздел состоит из нескольких разделов.

Важное замечание

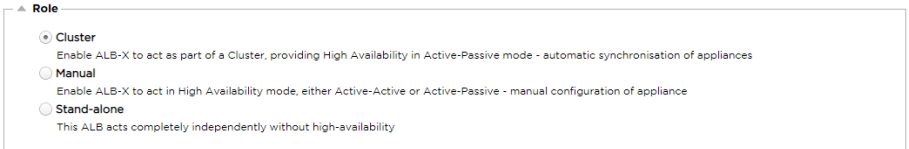
- Для поддержания высокой доступности сердцебиения не требуется выделенный кабель между парами АЦП.
- Сердцебиение происходит в той же сети, что и виртуальная служба, для которой требуется обеспечить высокую доступность.
- Переключение между устройствами ADC не происходит.
- Когда высокая доступность включена на двух или более ADC, каждый блок будет транслировать через UDP виртуальные службы, которые он настроен предоставлять.
- При отказоустойчивом восстановлении высокой доступности используются одноадресные сообщения и Gratuitous ARP для информирования новых коммутаторов Active load balancer.



Роль

При настройке ADC на высокую доступность доступны три роли кластера.

Кластер



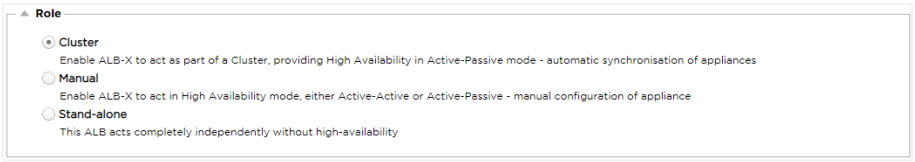
- По умолчанию новый ADC включается с ролью Cluster. В этой роли каждый член кластера будет иметь одинаковую "рабочую конфигурацию", и, таким образом, только один ADC в кластере будет активен в любой момент времени.
- Рабочая конфигурация" означает все параметры конфигурации, за исключением элементов, которые должны быть уникальными, таких как IP-адрес управления, имя ALB, сетевые настройки, детали интерфейса и так далее.
- ADC с приоритетом 1 (самая верхняя позиция) в окне Cluster Members является владельцем кластера и активным балансировщиком нагрузки, а все остальные ADC - 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 последнего участника кластера в раздел Невостребованные устройства. Чтобы удалить последнего участника, измените роль на Manual или Stand-alone.
- Следующие объекты не синхронизируются:
    - Ручная секция даты и времени - (секция NTP синхронизирована)
    - Задержка обхода отказа (мс)
    - Раздел "Оборудование
    - Раздел "Приборы
    - Раздел сети

Отказ владельца кластера

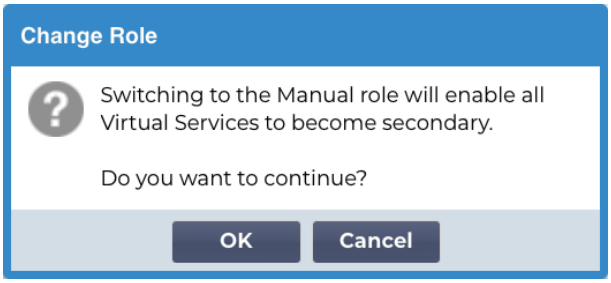
- Если владелец кластера выходит из строя, один из оставшихся участников автоматически берет на себя его функции и продолжает балансировать нагрузку.
- Когда владелец кластера вернется, он возобновит балансировку нагрузки и возьмет на себя роль владельца.
- Предположим, что владелец вышел из строя, и балансировку нагрузки взял на себя участник. 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 его владелец не работает, отредактированный член автоматически перейдет на место владельца без потери трафика

Изменение роли с роли кластера на роль руководства

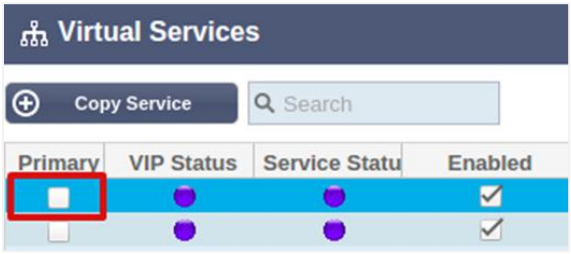
- Если вы хотите изменить роль с "Кластер" на "Вручную", нажмите радиокнопку рядом с опцией роли "Вручную".



- После нажатия на радиокнопку вы увидите следующее сообщение:



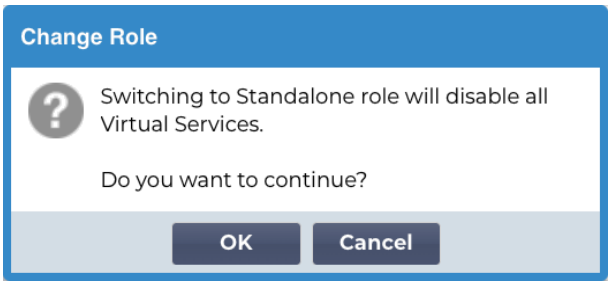
- Нажмите кнопку OK
- Проверьте раздел Виртуальные службы. Вы увидите, что в столбце Primary теперь не установлен флажок.



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

Изменение роли с кластерной на автономную

- Если вы хотите изменить роль с кластерной на автономную, нажмите на радиокнопку рядом с опцией "Автономная".
- Вам будет предложено следующее сообщение:



- Нажмите OK, чтобы изменить роли.
- Проверьте виртуальные службы. Вы увидите, что столбец Primary изменил название на Stand-alone
- Вы также увидите, что все виртуальные службы отключены (сняты галочки) по соображениям безопасности.
- Убедившись, что ни один другой ADC в той же сети не имеет дубликатов виртуальных служб, можно 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 необходимо реплицировать вручную на каждом блоке через графический интерфейс, либо при большом количестве изменений можно создать jetPACK с одного ADC и отправить его на другой.

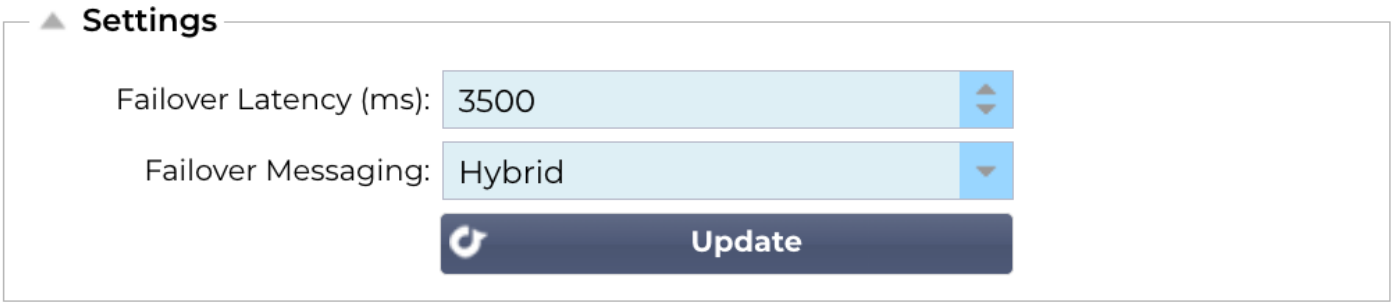
- Чтобы сделать виртуальный IP-адрес "Активным", установите флажок в основном столбце (страница IP Services).
- Чтобы сделать виртуальный IP-адрес "Пассивным", оставьте флажок пустым в основной колонке (страница IP Services).
- В случае, если активная служба переходит в пассивную:
    - Если оба столбца Primary отмечены, то происходит процесс выборов, и наименьший MAC-адрес становится активным.
    - Если оба флажка сняты, происходит тот же процесс выборов. Кроме того, если оба флажка сняты, автоматический возврат к исходному активному ADC не происходит.

Самостоятельная роль

ADC в роли автономного не будет взаимодействовать с другими ADC относительно своих служб, поэтому все виртуальные службы будут оставаться в зеленом статусе и подключенными. Вы

должны убедиться, что все виртуальные службы имеют уникальные IP-адреса, иначе в вашей сети возникнет конфликт.

Настройки

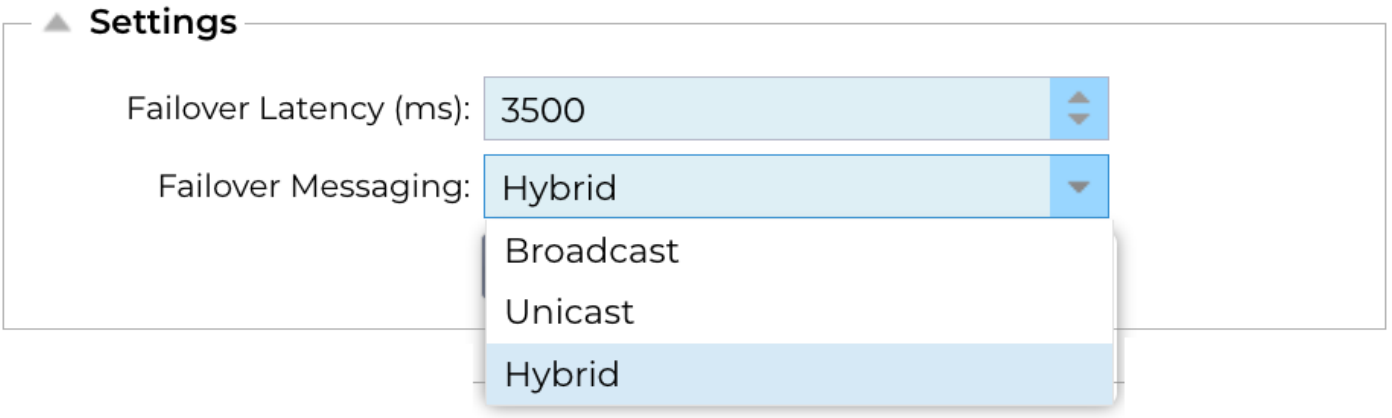


Задержка обхода отказа (мс)

Вы можете установить значение Failover Latency в миллисекундах. Это время, в течение которого 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 до 20000 мс. Если при меньшей задержке наблюдается нестабильность в кластере, следует увеличить это значение.

Обмен сообщениями при отказе

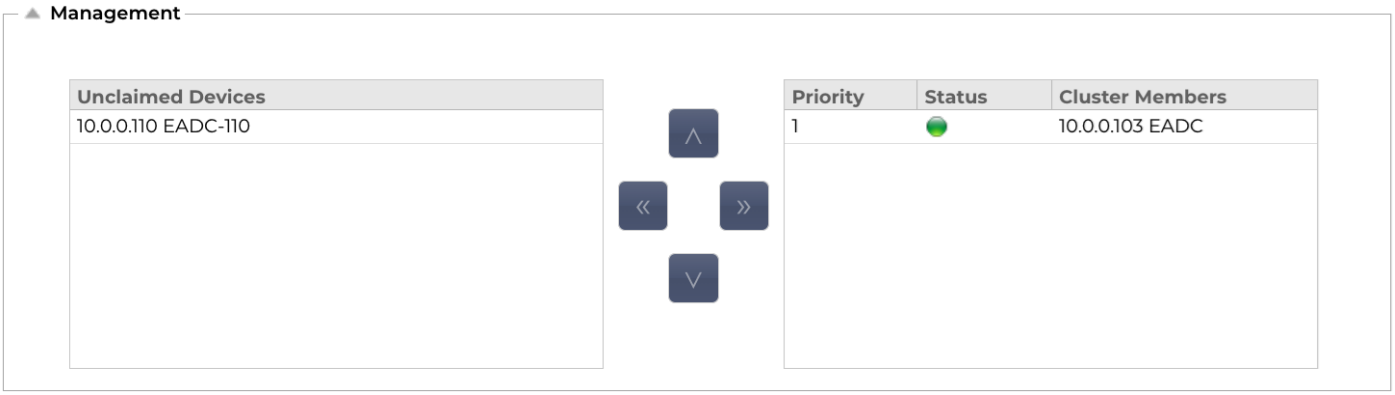


По умолчанию ADC использует широковещательную передачу для обмена сообщениями при обходе отказа. Однако некоторые сети блокируют широковещание, поэтому мы предусмотрели Unicast и Hybrid, сочетание Unicast и Broadcast.

При работе в режиме Broadcast по умолчанию невостребованные устройства будут автоматически занесены в список, а широковещательные сообщения будут использоваться для обхода отказа. При работе в гибридном режиме невостребованные устройства будут по-прежнему рекламироваться по широковещательной рассылке, но связь при обходе отказа будет осуществляться по одноадресной рассылке. В режиме Unicast широковещание не будет осуществляться, и вам может потребоваться вручную указать членов кластера.

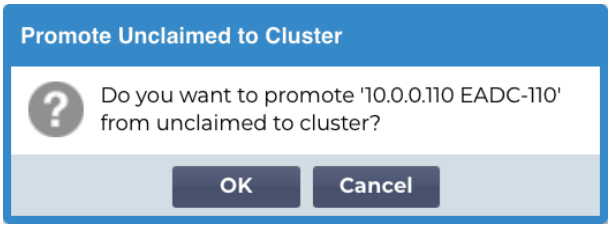
Управление

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

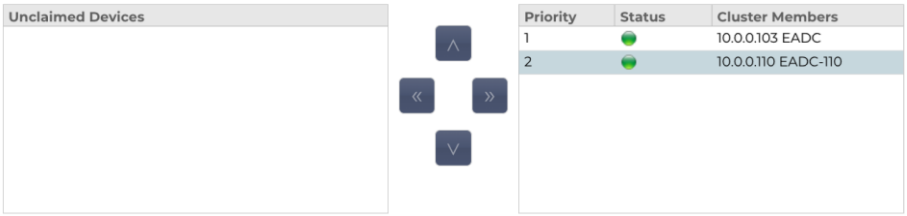


Добавление АЦП в кластер

- Перед добавлением ADC в кластер необходимо убедиться, что всем устройствам ADC присвоено уникальное имя в разделе Система > Сеть.
- Вы должны увидеть ADC в качестве приоритета 1 с зеленым статусом и его имя в столбце Cluster Members в разделе управления. Этот ADC является основным устройством по умолчанию.
- Все остальные доступные ADC будут отображаться в окне Unclaimed Devices (Невостребованные устройства) в разделе управления. Невостребованное устройство - это ADC, назначенный в роли кластера, но не имеющий настроенных виртуальных служб.
- Выделите АЦП в окне Невостребованные устройства и нажмите кнопку со стрелкой вправо.
- Теперь вы увидите следующее сообщение:

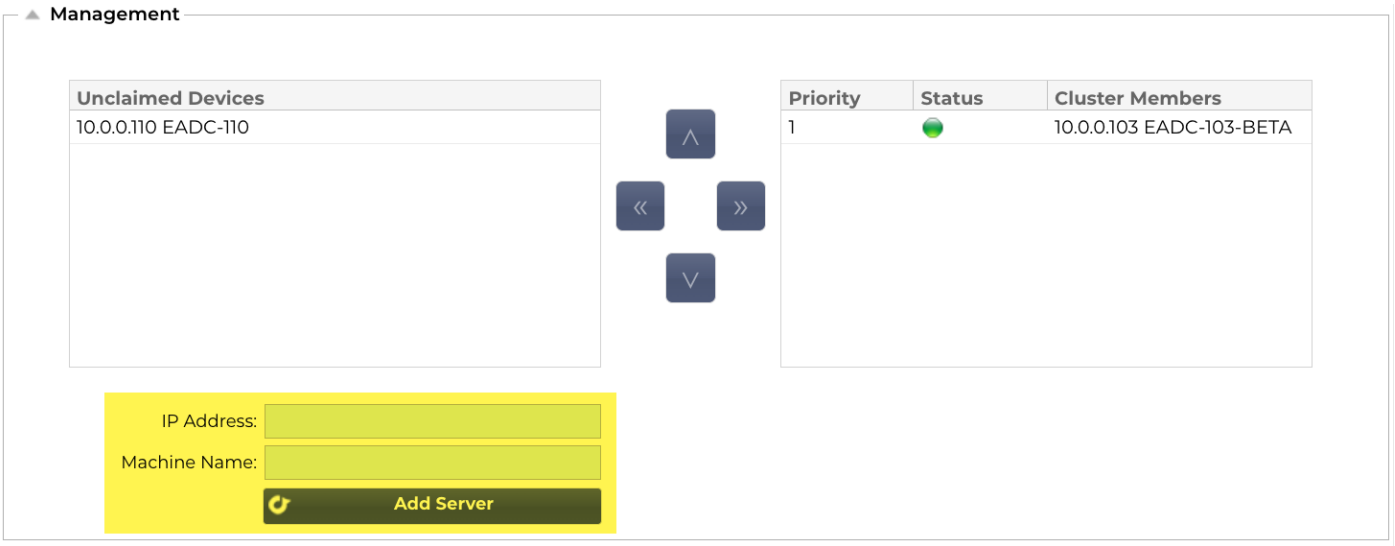


- Нажмите OK, чтобы включить ADC в кластер.
- Теперь ваш ADC должен отображаться как приоритет 2 в списке членов кластера.



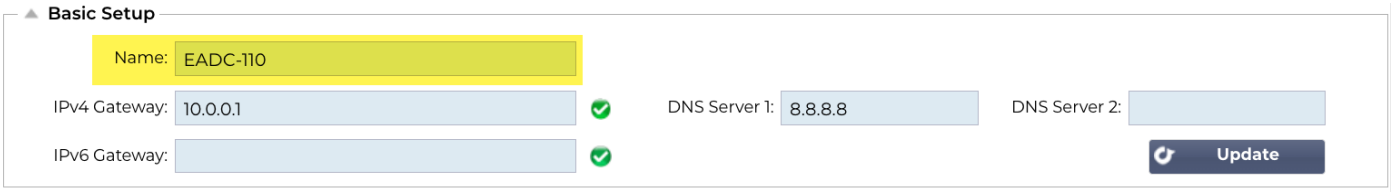
Ручное добавление АЦП в кластер

В системах, где Broadcast заблокирован, для добавления ADC в кластер необходимо выбрать Unicast или Hybrid режим.



Чтобы вручную добавить АЦП в кластер:

1. Укажите его IP-адрес
2. Укажите имя машины - оно доступно в разделе Система > Сеть.



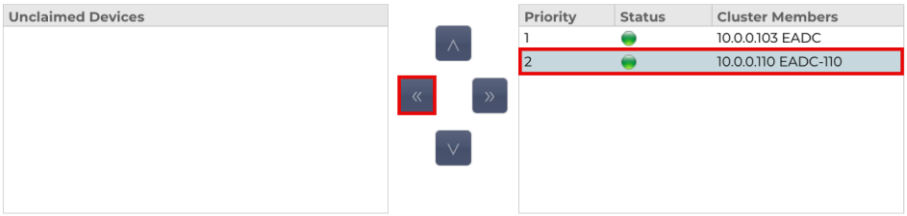
3. Нажмите Добавить сервер

После этого АЦП будет добавлен в кластер.

Если ADC, который вы пытаетесь добавить, уже находится в кластере, вы получите сообщение об ошибке.

Удаление члена кластера

- Выделите участника кластера, которого вы хотите удалить из кластера.
- Нажмите кнопку со стрелкой влево.



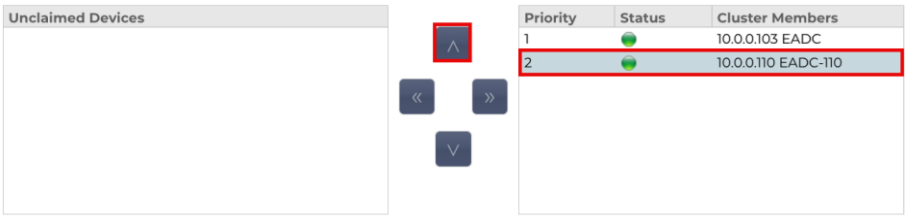
- Вы получите запрос на подтверждение.
- Нажмите OK для подтверждения.
- Ваш ADC будет удален и отображен в разделе "Невостребованные устройства".

Изменение приоритета АЦП

Бывают случаи, когда необходимо изменить приоритет ADC в списке участников.

- ADC, находящийся в верхней части списка Cluster Members, получает приоритет 1 и является активным ADC для всех виртуальных служб.
- ADC, который находится вторым в списке, получает приоритет 2 и является пассивным ADC для всех виртуальных служб.

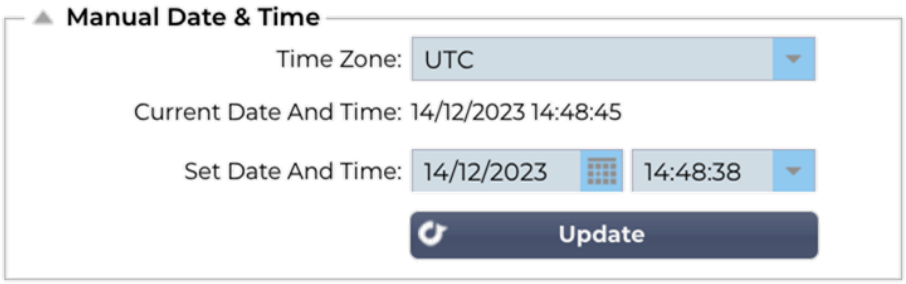
- Чтобы изменить активный АЦП, просто выделите его и нажмите стрелку вверх, пока он не окажется в верхней части списка.



Дата и время

Раздел "Дата и время" позволяет настроить 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 SSL-шифрованием.

Дата и время вручную



Часовой пояс

Значение, заданное в этом поле, представляет собой часовой пояс, в котором находится АЦП.

- Щелкните на выпадающем поле Часовой пояс 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 по-прежнему неверны, пожалуйста, измените дату вручную

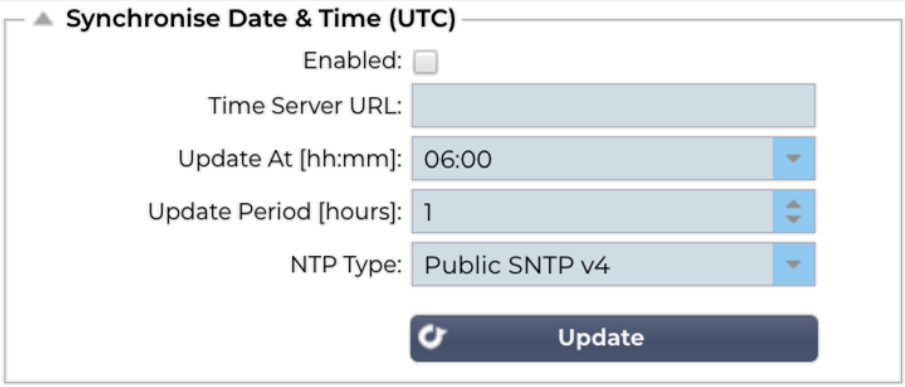
Установите дату и время

Эта настройка представляет собой фактическую дату и время.

- Выберите нужную дату из первого выпадающего списка или,
  в качестве альтернативы можно 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 кнопку Обновить, чтобы применить.
- 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-адрес сервера времени

Введите действительный IP-адрес или полное доменное имя (FQDN) для сервера NTP. Если сервер находится 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 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 Гринвичу. Если вы хотите установить местное время, это можно сделать только вручную. Это ограничение будет изменено в последующих версиях, чтобы включить возможность выбора часового пояса.

События по электронной почте

ADC - это критически важное устройство, и, как и любая другая система, оно оснащено возможностью информировать системного администратора о любых проблемах, которые могут потребовать внимания.

Страница Система > События электронной почты позволяет настроить подключение к серверу электронной почты и отправлять уведомления системным администраторам. Страница состоит из следующих разделов.

Адрес

Отправить по электронной почте События по адресам электронной почты

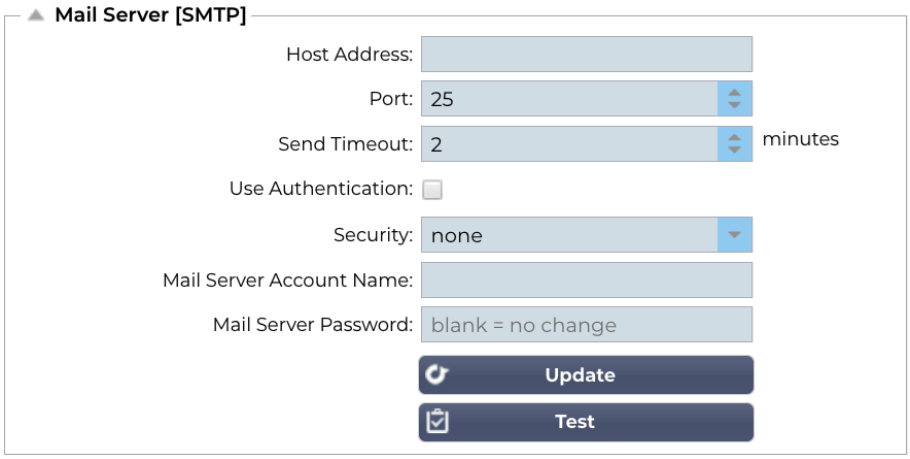
Добавьте действительный адрес электронной почты, на который будут отправляться оповещения, уведомления и события. Примерsupport@domain.com . Можно также добавить несколько адресов электронной почты, используя разделитель-запятую.

Обратный адрес электронной почты:

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

Почтовый сервер (SMTP)

В этом разделе необходимо добавить данные SMTP-сервера, который будет использоваться для отправки писем. Убедитесь, что адрес электронной почты, который вы используете для отправки, авторизован для этого.



Адрес хоста

Добавьте FQDN или 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 для SMTP. По умолчанию установлено значение 2 минуты.

Используйте аутентификацию

Установите флажок, 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 главного 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 реальными серверами невозможно связаться или каналы перестают работать.

IP-служба Уведомление

Уведомление IP-службы проинформирует вас о том, что какой-либо виртуальный IP-адрес находится в сети или перестал работать. Это действие выполняется для всех виртуальных служб, принадлежащих VIP.

Виртуальная служба Уведомление

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

Реальный сервер Уведомление

Когда реальный сервер и порт подключены или не доступны для связи, ADC отправляет уведомление реальному серверу.

flightPATH

Это уведомление отправляется по электронной почте, когда выполняется условие, и в нем настроено действие, указывающее ADC на отправку события по электронной почте.

Групповые уведомления Вместе

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

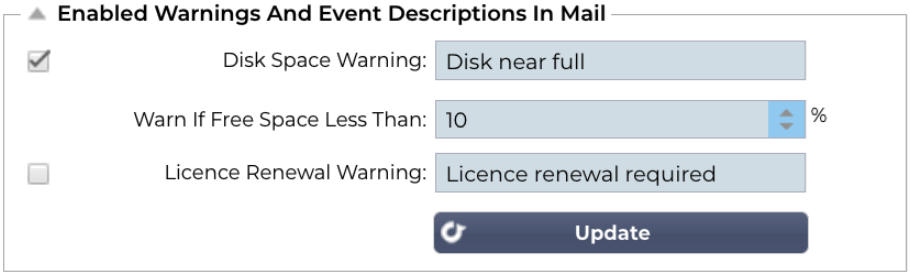
Групповая почта Описание

Укажите соответствующую тему для группового уведомления по электронной почте.

Интервал групповой отправки

Укажите время ожидания перед отправкой группового уведомления по электронной почте. Минимальное время составляет 2 минуты. По умолчанию установлено значение 30 минут.

Включены предупреждения и описания событий в почте



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

Дисковое пространство

Установите процент свободного дискового пространства, при превышении которого будет отправлено предупреждение. При достижении этого значения вам будет отправлено электронное письмо.

Предупреждение, если свободное пространство меньше

Здесь можно задать процентное значение, чтобы ADC мог отправить предупреждение по электронной почте, если объем дискового пространства упадет ниже этого порога.

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

В разделе "Система" находится опция "История системы", позволяющая получать исторические данные по таким элементам, как процессор, память, количество запросов в секунду и другие характеристики. После включения этой опции вы можете просмотреть результаты в графическом виде на странице Вид > История. На этой странице также можно создать резервную копию или восстановить файлы истории на локальном ADC.

Сбор данных

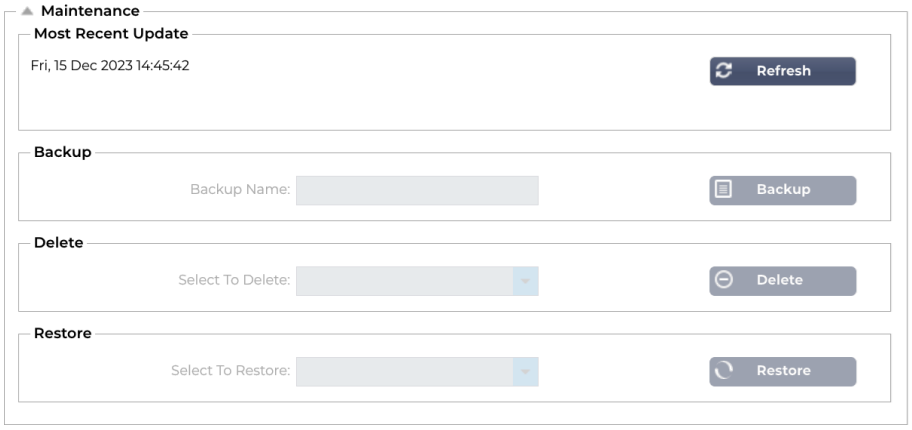
Включить

Чтобы разрешить сбор данных, поставьте галочку.

Собирайте данные каждый

Затем установите временной интервал, через который АЦП будет собирать данные. Это значение времени может находиться в диапазоне 1-60 секунд.

Техническое обслуживание



Последнее обновление

Показывает, когда были собраны последние исторические данные с АЦП.

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.

АЦП на базе HP Enterprise

Этот раздел функций действителен только для ADC, установленных на серверах HPE ProLiant bare metal и использующих ILO.

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 кнопку 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 ADC выдается либо по одной из следующих моделей, что зависит от параметров покупки и типа клиента.

Тип лицензии	Описание
Вечный	Вы, заказчик, имеете право использовать ADC и другое программное обеспечение в течение всего срока службы. 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 основе или с оплатой по факту. 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 на основе тарифа за одного VIP, который оплачивается ежегодно.

Подробности лицензии

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

Идентификатор лицензии

Идентификатор лицензии напрямую связан с идентификатором машины и другими сведениями, относящимися к приобретенному вами устройству ADC. Эта информация очень важна и требуется, когда вы хотите получить обновления и другие элементы из App Store.

Идентификатор машины

Идентификатор машины генерируется с использованием IP-адреса eth0 устройства ADC. Если вы измените IP-адрес устройства ADC, лицензия больше не будет действительна. Вам придется обратиться в службу поддержки за помощью. Мы рекомендуем использовать фиксированные IP-адреса устройств ADC с инструкциями для ИТ-персонала не менять их. Техническая поддержка доступна путем создания тикета на сайте https://www.edgenexus.io/support.

Примечание: Запрещается изменять IP-адрес устройств ADC. Если вы работаете в виртуализированной среде, то исправьте MAC ID и используйте статический IP-адрес.

Выдано

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

Контактное лицо

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

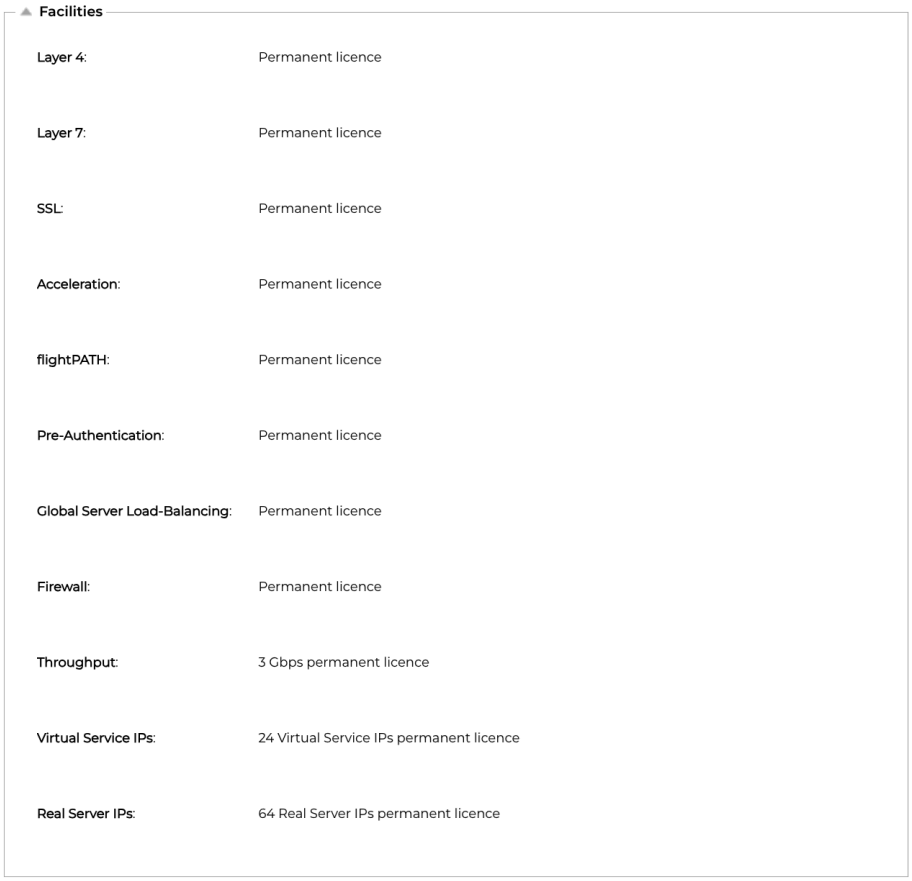
Дата выпуска d

Дата, когда была выдана лицензия.

Имя

Это значение показывает описательное имя устройства ADC Appliance, которое вы указали в разделе Система > Сеть.

Удобства



В разделе "Средства" представлена информация о том, какие функции 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.

Установите лицензию e

- 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 "Вставить лицензию".
- Вы также можете загрузить его в ADC, если копирование/вставка не является для вас подходящим вариантом.
- После этого нажмите кнопку "Обновить".
- Теперь лицензия установлена.

Информация о лицензионной службе

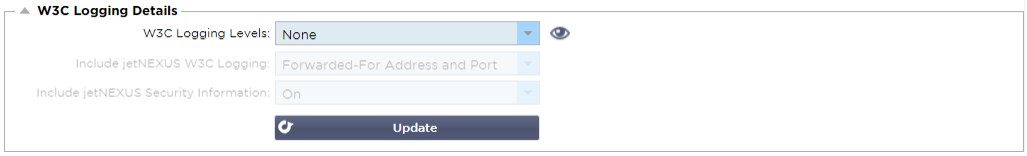
При нажатии на кнопку Информация об обслуживании лицензии отображается вся информация о лицензии. Эту функцию можно использовать для отправки сведений сотрудникам службы поддержки.

Ведение журнала

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

Подробности ведения журнала W3C

Включение регистрации W3C приведет к тому, что ADC начнет записывать журнал, 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 Консорциумом Всемирной паутины (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 сервиса предоставляемые данные различаются.

В таблице выше описаны уровни протоколирования для W3C HTTP.

Значение	Описание
Нет	Журналирование W3C отключено.
Краткое описание	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. в кратком описании полей 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	В этот формат вносится самая разная информация, касающаяся сотрудников отдела развития и поддержки. 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 FTP.

Значение	Описание
Краткое описание	#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

Включите ведение журнала W3C

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

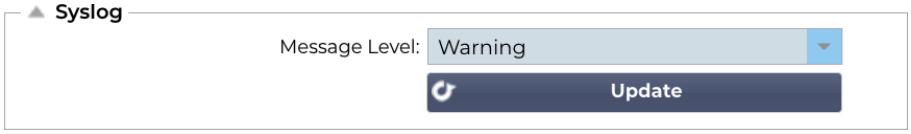
Значение	Описание
Сетевой адрес и порт клиента	Значение, показанное здесь, отображает фактический IP-адрес клиента вместе с портом.
Сетевой адрес клиента	Этот параметр включает и показывает только фактический IP-адрес клиента.
Адрес и порт переадресации	Эта опция показывает информацию, содержащуюся в заголовке XFF, включая адрес и порт.
Адрес для пересылки	Эта опция показывает информацию, содержащуюся в заголовке XFF, включая только адрес.

Включите информацию о безопасности

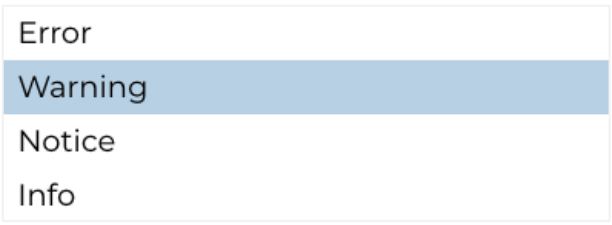
Это меню состоит из двух пунктов:

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.
С сайта	Это отключит возможность регистрировать имя пользователя в журнале W3C на глобальном уровне.

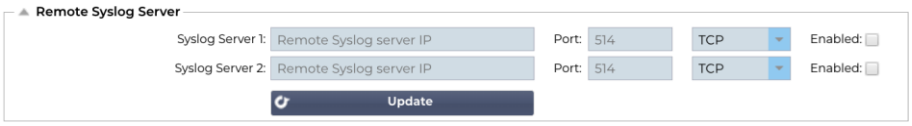
Сервер Syslog



В этом разделе можно задать уровень регистрации сообщений на сервере SYSLOG. Доступны следующие опции.



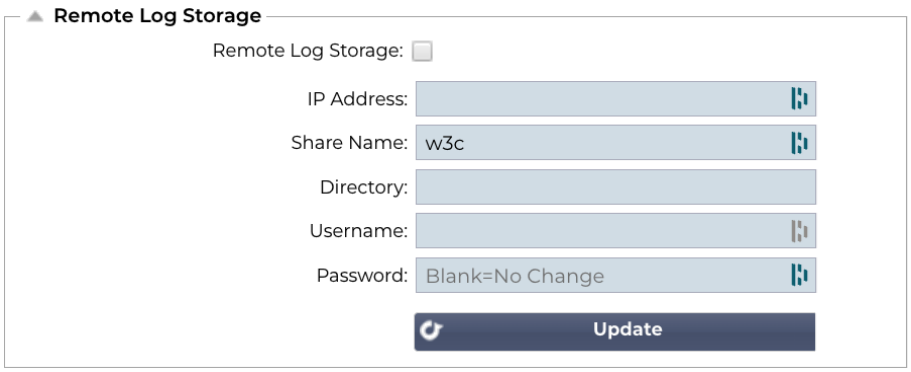
Удаленный сервер Syslog



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

- Добавьте IP-адрес вашего сервера Syslog.
- Добавьте порт
- Выберите, что вы хотите использовать: TCP или UDP.
- Установите флажок Включено, чтобы начать регистрацию
- Нажмите кнопку 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 удаленный сервер до тех пор, пока файл не будет завершен и сжат. Поскольку журналы пишутся каждый час, это может занять до двух часов в устройстве на виртуальной машине и до пяти часов в аппаратном устройстве.

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

Краткое описание поля

Состояние	**Описание**
Дата	Не локализовано = всегда ГГГГ-ММ-ДД (GMT/UTC)
Время	Не локализовано = HH:MM:SS или HH:MM:SS.ZZZ (GMT/UTC) * Примечание - к сожалению, это имеет два формата (Сайт

	не имеет .ZZZ миллисекунд)
x-mil	Только формат сайта = миллисекунда временной метки
c-ip	IP-адрес клиента, насколько это возможно из сети или заголовка X-Forwarded-For
c-port	Порт клиента, который можно определить из сети или заголовка X-Forwarded-For
cs-username	Поле запроса имени пользователя клиента
s-ip	Порт прослушивания ALB
s-port	ALB's listening VIP
x-xff	Значение заголовка X-Forwarded-For
x-xffcustom	Значение заголовка запроса типа X-Forwarded-For с конфигурацией-именем
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 формате brief используется это имя для cs-метода
cs-uri-stem	Путь к запрашиваемому ресурсу * кроме формата Brief
cs-uri-query	Запрос на запрашиваемый ресурс * за исключением формата Brief
ури	* краткий формат регистрирует комбинированный путь и строку запроса
sc-status	Код ответа HTTP
cs(User-Agent)	Строка User-Agent браузера (отправляется клиентом)
реферер	Ссылающаяся страница (как отправлено клиентом)
x-c-версия	HTTP-версия запроса клиента
x-r-версия	Содержимое - 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
время, затраченное на	Сколько времени занял сервер Real Server в секундах
x-trip-times new pcon	миллисекунда с момента подключения до появления сообщения в "списке новичков" миллисекунда с момента подключения до установки соединения с сервером Real Server
acon	миллисекунда с момента подключения до завершения установки соединения с сервером Real Server
rcon	миллисекунда с момента подключения до установления соединения с реальным сервером
rqf	миллисекунда с момента подключения до получения первого байта запроса от клиента
rql	миллисекунда с момента подключения до получения последнего байта запроса от клиента
tqf	миллисекунда с момента подключения до отправки первого байта запроса на Real Server
tql	миллисекунда с момента подключения до отправки последнего байта запроса на Real Server

pcф	миллисекунда с момента подключения до получения первого байта ответа от сервера Real Server
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 с момента подключения до отключения (обе стороны - последняя отключилась)
журнал	миллисекунда с момента подключения к этой записи журнала, за которой 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) соединения
x-compress-action	Как проводилось 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 журнала

Эта функция позволяет очистить файлы журналов с ADC. В раскрывающемся меню можно выбрать тип журнала, который необходимо удалить, а затем нажать кнопку Очистить.

Сеть

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

ВАЖНО

Управление виртуальными сетевыми интерфейсами в виртуальной среде

При развертывании виртуальных машин в виртуализированной среде ESXi сетевые интерфейсы (например, eth0, eth1) автоматически создаются и сопоставляются с сетевыми адаптерами конфигурации хоста (например, Network Adapter 1, Network Adapter 2). Однако эти сопоставления могут не всегда совпадать из-за правил операционной системы, которые привязывают интерфейсы к определенным MAC-адресам. В этом разделе описаны шаги по управлению сетевыми интерфейсами на хосте для предотвращения сбоев в работе служб, когда пользователь не может получить доступ к ВМ.

Основные соображения

1. **Постоянство MAC-адресов**:
   a. Операционная система назначает имена интерфейсов (например, eth0, eth1) на основе правил, которые связывают имя с определенным MAC-адресом.
   b. Удаление и повторное создание сетевого интерфейса виртуальной машины без повторного использования исходного MAC-адреса может привести к несогласованной или нефункциональной сетевой конфигурации.
2. **Внутренние отображения в ADC (EdgeOS)**:
   a. Виртуальные сетевые интерфейсы автоматически распознаются ADC (контроллером доставки приложений) и отображаются внутри сети.
   b. Удаление сетевого интерфейса с узла виртуальной машины может оставить в ADC устаревшие сопоставления, что может привести к нарушению доступа к управлению или сетевым службам.

Рекомендуемые шаги для конфигурации хоста

1. **Перед извлечением сетевой карты**:
   a. Запишите MAC-адрес интерфейса, который вы собираетесь удалить. Его можно посмотреть в настройках виртуальной машины на хосте ESXi.
2. **При добавлении сменной сетевой карты**:
   a. Присвойте новому сетевому адаптеру ранее записанный MAC-адрес, чтобы сопоставление интерфейсов ВМ оставалось неизменным.
3. **Предотвращение случайного удаления критически важных сетевых карт**:
   a. Определите, какие сетевые карты сопоставлены с критическими интерфейсами ADC (например, ETH0 (Greenside) для доступа к управлению). Не удаляйте эти сетевые карты без крайней необходимости.
4. **Проверьте согласованность MAC-адресов**:
   a. Убедитесь, что MAC-адреса, назначенные сетевым интерфейсам ВМ, соответствуют ожидаемой конфигурации в ADC. Используйте инструменты хоста ESXi для подтверждения этого сопоставления.
5. **Координация действий с администраторами виртуальных машин**:
   a. Если необходимо внести изменения, которые могут повлиять на внутреннюю конфигурацию ВМ, сообщите об этом администраторам ВМ, чтобы они подготовились к возможным сбоям и обеспечили сохранение правильного сопоставления.

Примерный сценарий

1. **Первоначальная настройка**:
   a. ADC VM имеет две сетевые карты: NIC1 (MAC: 00:11:22:33:44:55) и NIC2 (MAC: 00:11:22:33:44:66).
2. **Действия**: Удалите сетевую карту NIC1 и добавьте новую сетевую карту (NIC3).

   a. Присвойте оригинальный MAC-адрес (00:11:22:33:44:55) сетевой карте NIC3 во время создания на хосте ESXi.
3. **Предотвращение воздействия**:
   a. Благодаря повторному использованию оригинального MAC-адреса внутренние сопоставления ADC (например, ETH0) остаются неизменными, что позволяет избежать нарушения доступа к управлению или сетевым службам.

При управлении сетевыми интерфейсами в виртуализированной среде очень важно поддерживать согласованность в назначении MAC-адресов. Если доступ к виртуальной машине недоступен, необходимо выполнить все необходимые действия на стороне хоста, чтобы обеспечить бесперебойную работу и предотвратить перебои в обслуживании. Всегда координируйте свои действия с соответствующими администраторами, чтобы эффективно устранить возможные последствия.

Избегание частых перемещений vMotion для критически важных устройств

vMotion - это мощная функция VMware, которая обеспечивает живую миграцию виртуальных машин (ВМ) между узлами ESXi без простоя. Однако, хотя vMotion очень полезна для поддержания гибкости и доступности инфраструктуры, не рекомендуется часто перемещать критически важные устройства, такие как балансировщики нагрузки, особенно если они активно управляют большим количеством соединений.

Могут существовать и другие подобные технологии, предоставляемые другими производителями, но в данном разделе мы будем работать на базе VMware.

Почему не рекомендуется частое перемещение vMotion

1. **Срывы сеансов**:
   a. Балансировщики нагрузки управляют активными сеансами между клиентами и внутренними серверами. Во время операции vMotion происходит кратковременная реинициализация состояния сети, что может привести к нарушению этих сеансов.
   b. Нарушение связи может привести к обрыву соединения, что потребует от клиентов восстановления сеансов, что может ухудшить качество работы пользователей.
2. **Задержка и потеря пакетов**:
   a. Процесс миграции виртуальной машины включает в себя временную паузу и синхронизацию ее памяти и состояния. Для устройств, обрабатывающих трафик в реальном времени, такая пауза может привести к задержке или даже потере пакетов.
   b. Приложения, рассчитывающие на низкую задержку откликов, могут столкнуться со снижением производительности или таймаутами.
3. **Повышение эффективности использования ресурсов**:
   a. vMotion требует ресурсов процессора, памяти и пропускной способности сети для синхронизации данных между исходным и конечным узлами.
   b. Частые миграции могут создавать нагрузку на ресурсы инфраструктуры и потенциально влиять на другие виртуальные машины и службы, размещенные в той же среде.
4. **Влияние на конфигурации высокой доступности**:
   a. В средах с конфигурациями высокой доступности (HA) частые перемещения vMotion могут конфликтовать с механизмами обхода отказа, что приводит к неожиданному поведению или задержкам в действиях по обходу отказа.
5. **Операционная сложность**:
   a. Постоянное перемещение критически важных виртуальных машин повышает сложность сетевых конфигураций, включая сопоставление виртуальных локальных сетей и правила брандмауэра, что может привести к ошибкам в настройках.

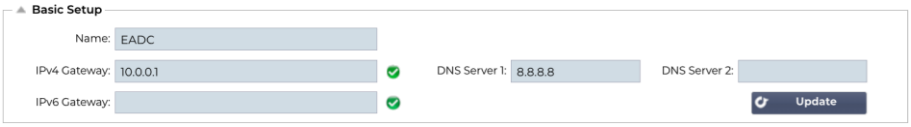
Рекомендации по управлению критически важными приборами

1. **Планирование операций vMotion во время обслуживания Windows**:
   a. Планируйте миграции в периоды низкого трафика, чтобы минимизировать воздействие на активные сеансы.

2. **Реализуйте кластеризацию балансировщика нагрузки**:
    a. Используйте кластеры или конфигурации высокой доступности для балансировщиков нагрузки, чтобы обеспечить избыточность. Это позволит беспрепятственно перенаправлять трафик на другой узел во время операций vMotion.
3. **Мониторинг ресурсов инфраструктуры**:
    a. Перед началом vMotion убедитесь в наличии достаточного количества процессора, памяти и пропускной способности сети, чтобы предотвратить нехватку ресурсов.
4. **Сведите к минимуму частоту миграций**:
    a. Ограничьте vMotion критически важных устройств сценариями, в которых это абсолютно необходимо, например, для обслуживания хоста или восстановления после сбоя.
5. **Тестирование перед производством**:
    a. Протестируйте операции vMotion в среде staging, чтобы понять их влияние на активные сеансы и убедиться, что конфигурации оптимизированы.

Хотя vMotion - бесценный инструмент для управления ВМ, его следует использовать с осторожностью для критически важных устройств, таких как балансировщики нагрузки. Частые миграции могут нарушить работу служб, увеличить задержки и нагрузку на ресурсы. Тщательно планируя операции vMotion и используя такие стратегии, как кластеризация и планирование обслуживания, вы сможете обеспечить надежное предоставление услуг и свести к минимуму риск сбоев.

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 внизу страницы и белую галочку в зеленом круге рядом с IP-адресом.

Шлюз IPv6

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

DNS-сервер 1 и DNS-сервер 2

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

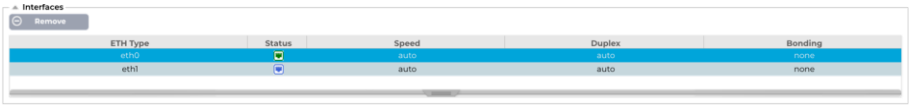
Адаптер Подробнее

В этом разделе панели "Сеть" показаны 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 для одного интерфейса. 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 четверичной десятичной системе счисления. Пример 255.255.255.0
Шлюз	Добавьте шлюз для интерфейса. При его добавлении 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 столбец, а затем установите флажок, чтобы назначить этот интерфейс в качестве адреса управления для веб-консоли графического интерфейса пользователя. Пожалуйста, будьте очень внимательны при изменении интерфейса, на котором будет прослушиваться Web Console. Вам нужно будет настроить правильную маршрутизацию или находиться в той же подсети, что и новый интерфейс, чтобы попасть на веб-консоль 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" на панели "Сеть" позволяет настраивать определенные элементы, относящиеся к сетевому интерфейсу. Вы также можете удалить сетевой интерфейс из списка, нажав кнопку Remove. При использовании виртуального устройства интерфейсы, которые вы видите здесь, ограничены базовым фреймворком виртуализации.



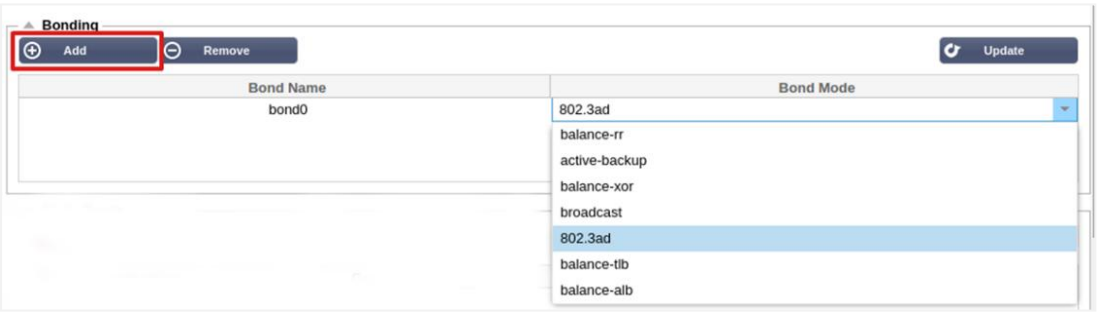
Колонка	Описание
Тип ETH	Это значение указывает на внутреннюю ссылку ОС на сетевой интерфейс. Это поле не может быть настроено. Значения начинаются с ETH0 и далее по порядку в зависимости от количества сетевых интерфейсов.
Статус	Эта графическая индикация показывает текущее состояние сетевого интерфейса. 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 скорость сети 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. Дополнительные сведения см. в разделе "Связывание".

Связывание

Для обозначения объединения сетевых интерфейсов используется множество названий: Port Trunking, Channel Bonding, Link Aggregation, NIC teaming и другие. Связывание объединяет или агрегирует несколько сетевых подключений в единый интерфейс со связью каналов. Связывание позволяет двум или более сетевым интерфейсам действовать как единое целое, увеличивать пропускную способность и обеспечивать резервирование или обход отказа.

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 связанного 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.



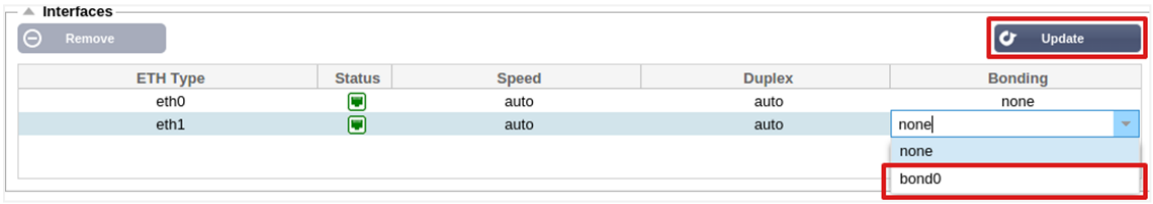
Создание профиля Bonding

- 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.

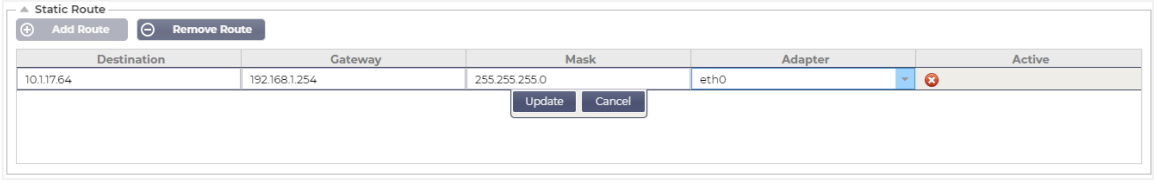


Режимы скрепления

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 - резервным. Этот вторичный интерфейс становится активным только в случае сбоя активного соединения на первом интерфейсе.
баланс иксор:	Передача на основе MAC-адреса источника, XOR'ированного 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 активного агрегатора в соответствии со спецификацией 802.3ad.
баланс - тлб:	Адаптивный режим объединения каналов с балансировкой нагрузки на передачу: Обеспечивает связывание каналов, не требующее специальной поддержки коммутатора. Исходящий трафик распределяется в соответствии с текущей нагрузкой (вычисленной относительно скорости) на каждого ведомого. Текущий ведомый получает входящий трафик. Если принимающий ведомый выходит из строя, другой ведомый принимает MAC-адрес вышедшего из строя принимающего ведомого.
баланс - алб:	Режим адаптивной балансировки нагрузки: также включает balance-tlb плюс балансировку нагрузки при приеме (rlb) для трафика IPV4 и не требует специальной поддержки коммутатора. Балансировка нагрузки на прием достигается путем ARP-переговоров. Драйвер бондинга перехватывает ARP-ответы, отправляемые локальной системой, и переписывает аппаратный адрес источника уникальным аппаратным адресом одного из ведомых в бондинге, так что разные пиры используют разные аппаратные адреса для сервера.

Статический маршрут

Бывают случаи, когда необходимо создать статические маршруты для определенных подсетей в сети. ADC предоставляет вам возможность сделать это с помощью модуля Static Routes.



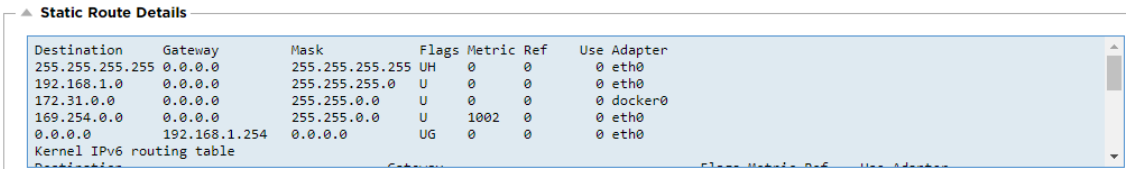
Добавление статического маршрута

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

Поле	Описание
Пункт назначения	Введите адрес сети назначения в десятичной точечной системе счисления. Пример 123.123.123.5
Шлюз	Введите IPv4-адрес шлюза в десятичной точечной системе счисления. 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	Зеленый флажок 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 представлена информация обо всех маршрутах, настроенных на ADC.



Дополнительные настройки сети

Что такое Нагл?

Алгоритм Нагла, также известный как алгоритм TCP No Delay, - это техника, используемая в сетевых коммуникациях для уменьшения количества повторно передаваемых пакетов из-за неупорядоченных данных. Он работает за счет задержки отправки небольших пакетов, если не было получено подтверждение на предыдущие пакеты. Это помогает гарантировать, что данные поступают в правильном порядке, и снижает нагрузку на сеть.

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 пересылать по сети. Эта настройка применяется к серверной стороне транзакции. Следует внимательно относиться к настройкам сервера, поскольку Nagle и отложенный ACK могут сильно повлиять на производительность.

Клиент Нагл

Установите флажок, чтобы включить настройку Client Nagle. Как указано выше, но применяется к транзакции на стороне клиента.

SNAT

SNAT расшифровывается как Source Network Address Translation (трансляция сетевых адресов источника), и разные производители имеют небольшие различия в реализации SNAT. Простое объяснение SNAT для EdgeADC выглядит следующим образом.

При обычных обстоятельствах входящие запросы направляются на VIP, который видит IP-адрес источника запроса. Так, например, если конечная точка браузера имеет IP-адрес 81.71.61.51, это будет видно VIP-клиенту.

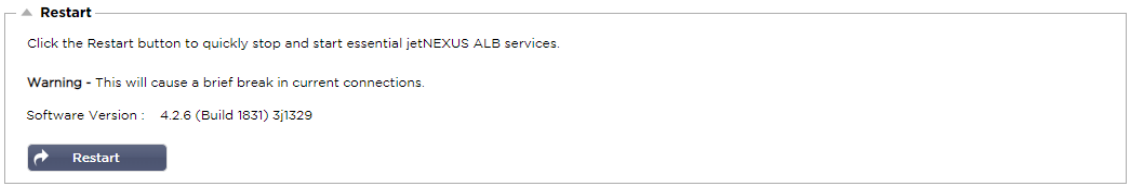
Когда SNAT действует, исходный IP-адрес источника запроса будет скрыт от VIP, и вместо него будет виден IP-адрес, указанный в правиле SNAT. Таким образом, SNAT можно использовать в режимах балансировки нагрузки на уровнях 4 и 7.

Поле	Описание
Источник IP	IP-адрес источника является необязательным и может быть либо сетевым IP-адресом (с /mask), либо обычным IP-адресом. Маска может быть как сетевой маской, так и обычным числом, указывающим количество единиц в левой части сетевой маски. Так, маска /24 эквивалентна 255.255.255.0.
IP-адрес назначения	IP-адрес назначения является необязательным и может быть либо сетевым IP-адресом (с /mask), либо обычным IP-адресом. Маска может быть как сетевой маской, так и обычным числом, указывающим количество единиц в левой части сетевой маски. Так, маска /24 эквивалентна 255.255.255.0.
Порт-источник	Порт источника необязателен, он может быть одним числом, в этом случае он указывает только этот порт, или он может включать двоеточие, которое указывает диапазон портов. Примеры: 80 или 5900:5905.
Порт назначения	Порт назначения необязателен, он может быть одним числом, в этом случае он указывает только этот порт, или может включать двоеточие, которое указывает диапазон портов. Примеры: 80 или 5900:5905.
Протокол	Вы можете выбрать, использовать SNAT для одного протокола или для всех протоколов. Мы советуем быть конкретными, чтобы быть более точными.
SNAT - IP	SNAT to IP - это обязательный IP-адрес или диапазон IP-адресов. Примеры: 10.0.0.1 или 10.0.0.1-10.0.0.3.
SNAT в порт	SNAT to Port является необязательным, он может быть одним числом, в этом случае он указывает только этот порт, или может включать тире, что указывает диапазон портов. Примеры: 80 или 5900-5905.
Примечания	Используйте это имя, чтобы напомнить себе, зачем существуют правила. Это также полезно для отладки в Syslog.

Мощность

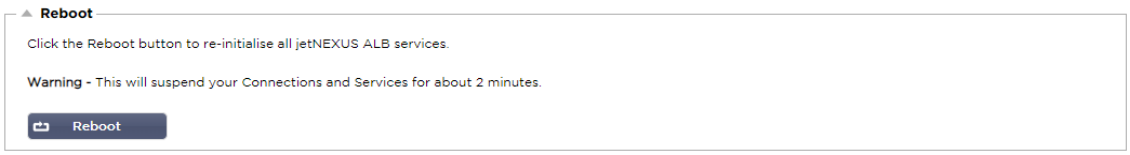
Эта функция системы АЦП также позволяет выполнять несколько задач, связанных с питанием АЦП.

Перезапустите



Эта настройка инициирует глобальный перезапуск всех Служб и, соответственно, разрыв всех активных в данный момент соединений. Все Службы автоматически возобновят работу через некоторое время, но время зависит от количества настроенных Служб. Появится всплывающее окно с запросом на подтверждение действия перезапуска.

Перезагрузка



Нажатие на кнопку Reboot (Перезагрузка) приведет к циклу питания АЦП и автоматически вернет его в активное состояние. Появится всплывающее окно с запросом на подтверждение действия перезагрузки.

Выключение питания

Нажатие на кнопку Power Off (Выключить) выключит ADC. Если это аппаратное устройство, то для его включения потребуется физический доступ к нему. Появится всплывающее окно с запросом на подтверждение действия выключения.

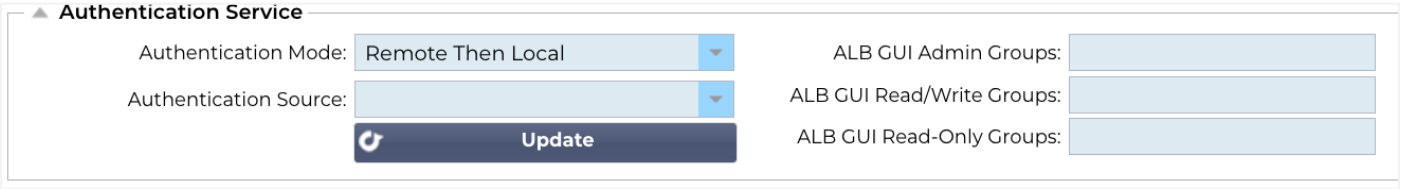
Безопасность

В этом разделе можно изменить пароль веб-консоли, а также включить или отключить доступ к Secure Shell. Здесь также можно включить возможность REST API.

SSH

Вариант	Описание
Удаленное подключение Secure Shell	Поставьте галочку, если вы хотите получить доступ к АЦП с помощью SSH. Для этого отлично подходит программа "Putty".

Служба аутентификации



В большинстве организаций существует требование, что доступ к интерфейсу управления ADC должен осуществляться через собственные службы аутентификации компании.

Для таких сценариев мы предусмотрели функцию Authentication Service, описанную здесь. Эта функция работает с локальными службами каталогов, а также с внешними службами, такими как SAML.

Вариант	Описание
Режим аутентификации	Только локально: Это режим по умолчанию, который использует локальную базу данных внутри ADC, например, для пользователя admin. Удаленный, затем Локальный: ADC попытается проверить пользователя на удаленном сервере аутентификации, указанном в поле Источник аутентификации. Если это не удастся, то в качестве источника проверки будет использоваться локальная база данных.
Источник аутентификации	В этом раскрывающемся меню можно выбрать один из серверов аутентификации, заданных в разделе Библиотека > Аутентификация.
Группы администраторов графического интерфейса ALB	Укажите разрешенные группы администраторов.
Группы чтения/записи графического интерфейса ALB	Укажите разрешенные группы чтения/записи
Группы, доступные только для чтения в графическом интерфейсе ALB	Укажите группы, разрешенные для чтения.

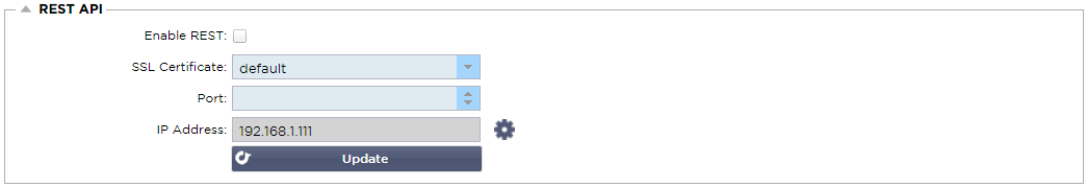
Веб-консоль

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

Вариант	**Описание**
Безопасный порт	По умолчанию для веб-консоли используется порт TCP 443. Если вы хотите использовать другой порт в целях безопасности, вы можете изменить его здесь.

REST API

REST API, также известный как RESTful API, - это 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 ученым-компьютерщиком Роем Филдингом.



Вариант	Описание
Включить REST	Установите этот флажок, чтобы включить доступ с помощью REST API. Обратите внимание, что вам также придется настроить, на каком адаптере будет 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	Задайте порт для службы REST. Желательно использовать порт, отличный от 443.
IP-адрес	Здесь отобразится IP-адрес, к которому привязана служба REST. Вы можете нажать на ссылку Cog, чтобы перейти на страницу Сеть и изменить, на каком адаптере включена служба REST.
Когтеточка	Щелкнув по этой ссылке, 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 тем, что у них есть проблемы с поддержкой строк запросов.
Прокрутите страницу с ошибками, 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 '{"<имя пользователя реста>":"<пароль>"}'
```

- вернётся

```
{ "Loginstatus": "OK", "Username": "<rest username>", "GUID": "<guid>"}
```

- Валидность
  - GUID действителен в течение 24 часов

Детали лицензии

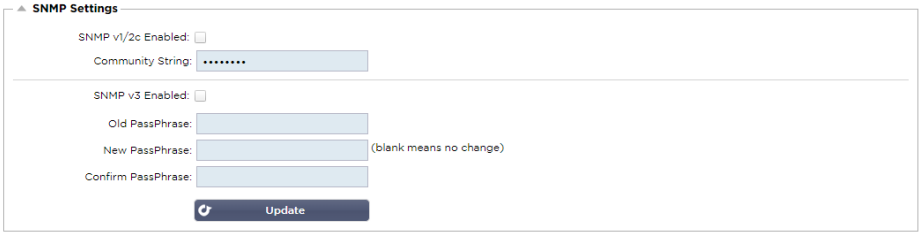
- Команда

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

SNMP

Раздел SNMP позволяет настроить 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 MIB V3. 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, доступная только для чтения, установленная на агенте и используемая менеджером для получения информации SNMP. По умолчанию используется строка сообщества jetnexus
PassPhrase	Это пароль, необходимый при включении SNMP v3; он должен состоять не менее чем из 8 символов и содержать только буквы Aa-Zz и цифры 0-9. По умолчанию используется парольная фраза **jetnexus**

SNMP MIB

Информация, доступная для просмотра по протоколу SNMP, определяется базой управленческой информации (MIB). MIB описывает структуру данных управления и использует 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
```

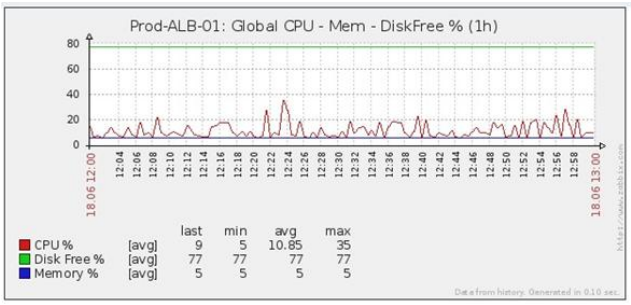
Наши идентификаторы

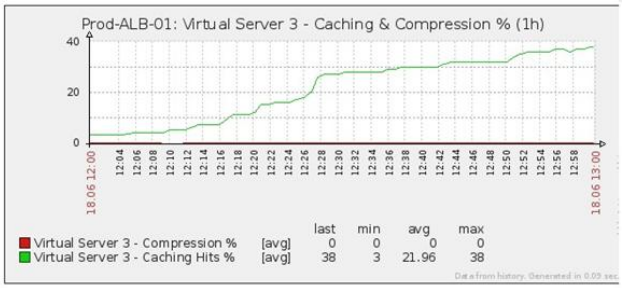
```
.38370 jetnexusMIB
      .1 jetnexusData   (1.3.6.1.4.1.38370.1)
            .1 jetnexusGlobal (1.3.6.1.4.1.38370.1.1)
            .2 jetnexusVirtualServices   (1.3.6.1.4.1.38370.1.2)
            .3 jetnexusServers   (1.3.6.1.4.1.38370.1.3)
                  .1 jetnexusGlobal   (1.3.6.1.4.1.38370.1.1)
                        .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)
```

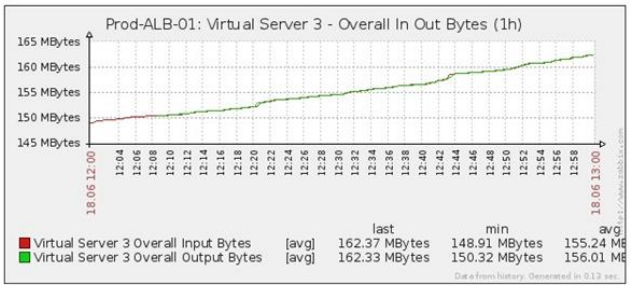
```
        .4 jetnexusCompressedOutputBytes (1.3.6.1.4.1.38370.1.1.4.0)
        .5 jetnexusVersionInfo (1.3.6.1.4.1.38370.1.1.5.0)
        .6 jetnexusTotalClientConnections (1.3.6.1.4.1.38370.1.1.6.0)
        .7 jetnexusCpuPercent (1.3.6.1.4.1.38370.1.1.7.0)
        .8 jetnexusDiskFreePercent (1.3.6.1.4.1.38370.1.1.8.0)
        .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)
```

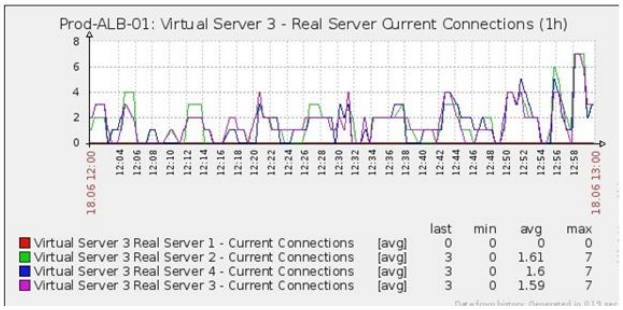
Исторические графики

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


Prod-ALB-01: Global CPU - Mem - DiskFree % (1h)
80
60
40
20
0
18.06 12:00
18.06 13:00
last min avg max
CPU % [avg] 9 5 10.85 35
Disk Free % [avg] 77 77 77 77
Memory % [avg] 5 5 5 5


Prod-ALB-01: Virtual Server 3 - Caching & Compression % (1h)
40
20
0
18.06 12:00
18.06 13:00
last min avg max
Virtual Server 3 - Compression % [avg] 0 0 0 0
Virtual Server 3 - Caching Hits % [avg] 38 3 21.96 38


Prod-ALB-01: Virtual Server 3 - Overall In Out Bytes (1h)
165 MBytes
160 MBytes
155 MBytes
150 MBytes
145 MBytes
18.06 12:00
18.06 13:00
last min avg
Virtual Server 3 Overall Input Bytes [avg] 162.37 MBytes 148.91 MBytes 155.24 MB
Virtual Server 3 Overall Output Bytes [avg] 162.33 MBytes 150.32 MBytes 156.01 MB


Prod-ALB-01: Virtual Server 3 - Real Server Current Connections (1h)
8
6
4
2
0
18.06 12:00
18.06 13:00
last min avg max
Virtual Server 3 Real Server 1 - Current Connections [avg] 0 0 0 0
Virtual Server 3 Real Server 2 - Current Connections [avg] 3 0 1.61 7
Virtual Server 3 Real Server 4 - Current Connections [avg] 3 0 1.6 7
Virtual Server 3 Real Server 3 - Current Connections [avg] 3 0 1.59 7

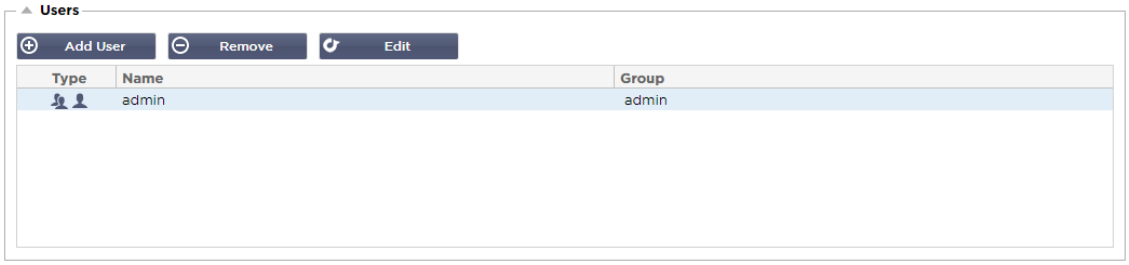
Пользователи и журналы аудита

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

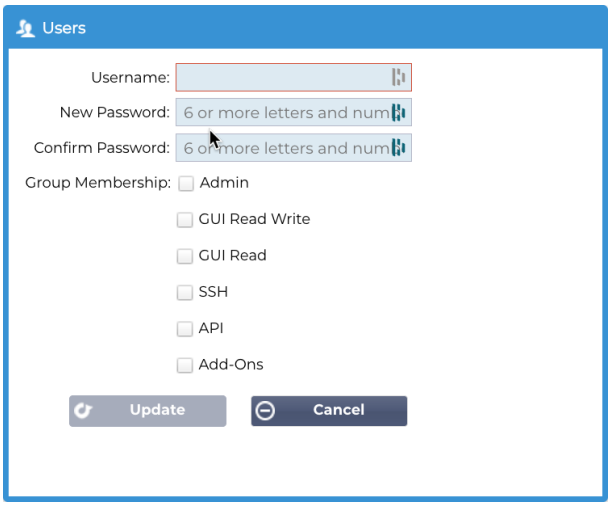
При первой настройке ADC используется пользователь по умолчанию под именем **admin**. Пароль по умолчанию для admin - **jetnexus**.

Пользователи

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



Добавить пользователя



Нажмите кнопку Добавить пользователя, показанную на рисунке выше, чтобы открыть диалог добавления пользователя.

Параметр	Описание/использование
Имя пользователя	Введите имя пользователя по своему выбору. Имя пользователя должно соответствовать следующим требованиям: • Минимальное количество символов 1 • Максимальное количество символов 32 • Буквы могут быть 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 • Необходимо использовать хотя бы комбинацию букв и цифр. • Буквы могут быть прописными или строчными. • Символы разрешены, за исключением тех, что приведены в примере ниже **£**, **%**, &, **<** , **>**
Подтвердите пароль	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 этой группы могут получить доступ к графическому интерфейсу и вносить изменения через него. • GUI Read - Пользователи этой группы могут получить доступ к графическому интерфейсу только для просмотра информации. Изменения не могут быть внесены. • SSH - пользователи этой группы могут получить доступ к ADC 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 • Add-On - Разрешение на доступ к конфигурациям Add-On.

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 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 между всеми ADC в кластере Любое изменение пользователя кластера отразится на всех членах 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. Для пользователя будет действовать последний настроенный пароль.

Удаление пользователя

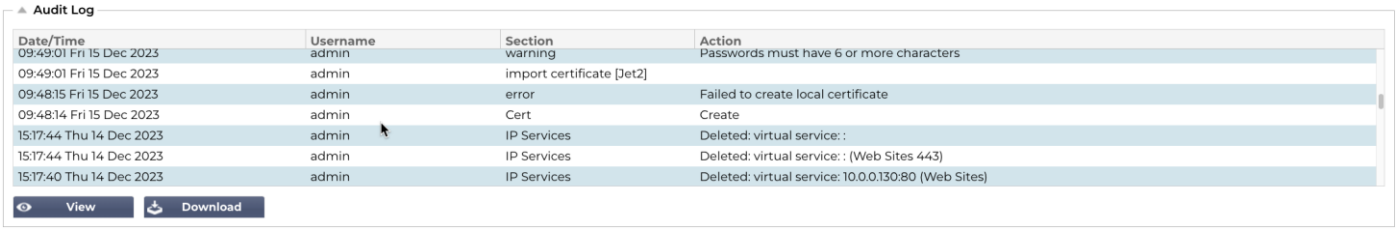
- Выделите существующего пользователя.
- Нажмите кнопку Удалить.
- Вы не сможете удалить пользователя, который в данный момент входит в систему.
- Вы не сможете удалить последнего локального пользователя в группе администраторов.
- Вы не сможете удалить последнего оставшегося пользователя кластера в 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 кнопку Редактировать
- Вы можете изменить членство пользователя в группе, отметив соответствующие поля и обновив их.
- Вы также можете изменить пароль пользователя, если у вас есть права администратора.

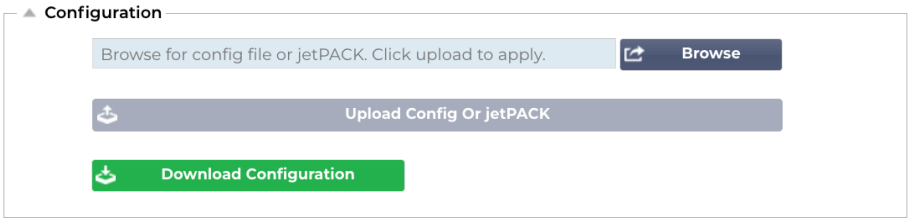
Журнал аудита

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



Расширенный

Конфигурация



Лучше всего загружать и сохранять конфигурацию АЦП после того, как он полностью настроен и работает так, как нужно. 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, который можно редактировать с помощью текстового редактора, такого как Notepad++, Nano или VI. После редактирования файл конфигурации может быть загружен в АЦП.

ВНИМАНИЕ:

Редактирование файла конфигурации EdgeADC предназначено только для квалифицированных специалистов. Если вы решите самостоятельно отредактировать конфигурационный файл и возникнут технические проблемы, служба технической поддержки Edgenexus больше не сможет поддерживать продукт.

Загрузка конфигурации

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

Загрузка конфигурации

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

Критически важно: Не пытайтесь копировать конфигурацию с одного ADC на другой без предварительной консультации со службой поддержки Edgenexus. Это может привести к невозможности восстановления вашего АЦП.

Загрузите пакет JetPACK

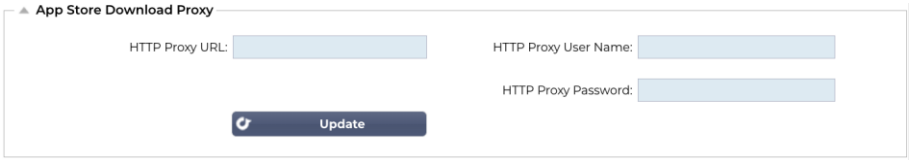
- JetPACK - это набор обновлений существующей конфигурации.
- JetPACK может включать в себя как изменение значения тайм-аута TCP, так и полную конфигурацию для конкретного приложения, например Microsoft Exchange или Microsoft Lync.
    - Вы можете получить JetPACK на портале поддержки, указанном в конце данного руководства.
- Найдите файл jetPACK.txt.
- Нажмите кнопку Загрузить.
- После загрузки браузер автоматически обновится.
- 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.

App Store Download Proxy



Защищенные сети обычно не дают доступа к Интернету, если только данные не отправляются через прокси-серверы организации. EdgeADC является устройством периметра и должен иметь доступ к серверам Edgenexus, чтобы убедиться в достоверности поддержки, а также получить доступ к App Store для загрузки обновлений и приложений.

URL-адрес HTTP-прокси

Это поле используется для указания имени хоста или IP-адреса вашего прокси-сервера.

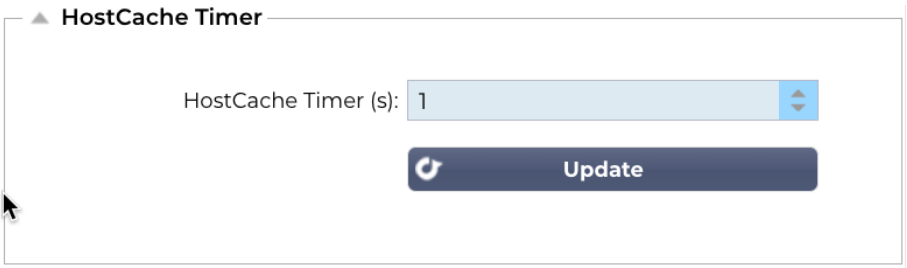
Имя пользователя HTTP-прокси

Введите имя пользователя, используемое для авторизации устройств и пользователей, использующих прокси-сервер.

Пароль HTTP-прокси

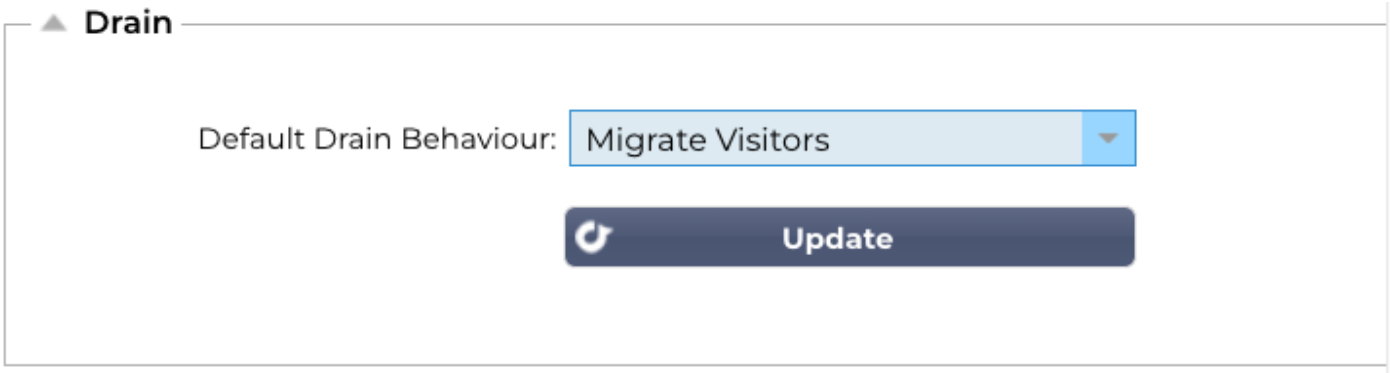
Имя пользователя, указанное в поле HTTP Proxy Username, будет защищенным. В этом поле необходимо ввести соответствующий пароль.

Таймер кэша хоста



Host Cache Timer - это параметр, который сохраняет IP-адрес реального сервера в течение определенного периода времени, когда вместо IP-адреса используется доменное имя. Кэш стирается при отказе реального сервера. Установка этого значения в ноль предотвратит очистку кэша. Максимального значения для этого параметра не существует.

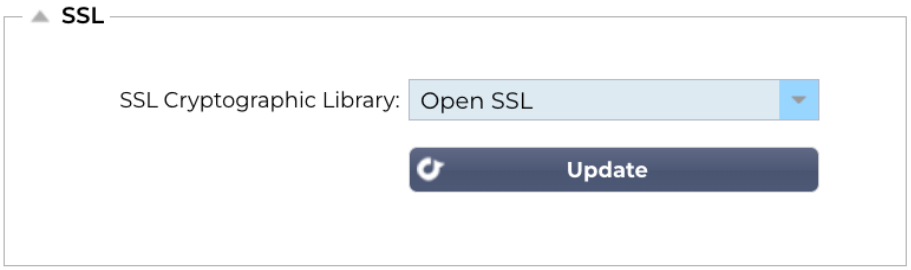
Дренаж



Когда какой-либо реальный сервер переводится в режим Drain, всегда лучше иметь возможность контролировать поведение трафика, отправляемого на него. Меню Drain Behaviour позволяет выбрать поведение трафика для каждой виртуальной службы. Возможны следующие варианты:

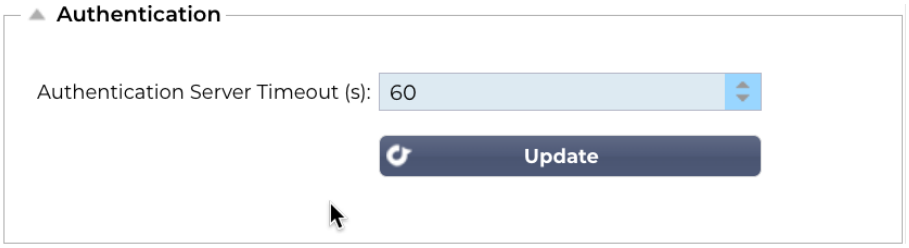
Вариант	**Описание**
Управляемые постоянством	Это выбор по умолчанию. Всякий раз, когда пользователь посещает сессию персистентности, она расширяется. При круглосуточном использовании возможно, что слив никогда не произойдет. Однако если количество соединений с реальным сервером достигает 0, слив завершается, сессии сохранения удаляются, а все посетители заново балансируются при следующем соединении.
Миграция посетителей	Постоянная сессия игнорируется при повторном подключении - (устаревшее поведение до 2022 года) Новые TCP-соединения (независимо от того, являются ли они частью существующей сессии или нет) всегда устанавливаются с реальным сервером в режиме онлайн. Если сессия сохранения была связана с истощающимся реальным сервером, она перезаписывается. Виртуальная служба будет фактически игнорировать постоянство для любых новых соединений, и они будут перераспределены на новый сервер.
Сессии на пенсии	Постоянные сеансы не продлеваются. Входящие пользовательские соединения будут назначены на нужный сервер, но их сессия сохранения не будет продлена. Поэтому по истечении времени сессии персистентности они будут рассматриваться как новое соединение и перемещаться на другой сервер.

SSL



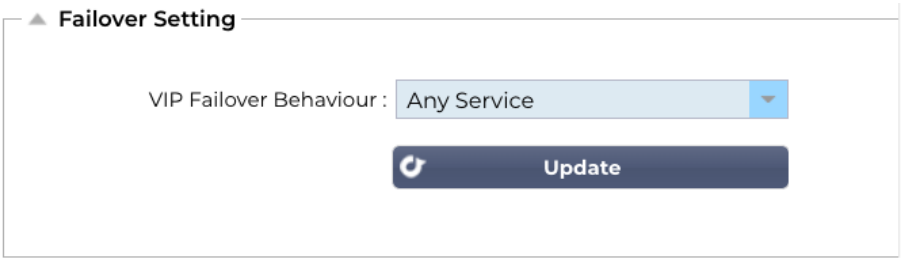
Эта глобальная настройка позволяет изменять библиотеку SSL по мере необходимости. По умолчанию криптографическая библиотека SSL, используемая ADC, принадлежит OpenSSL. Если вы хотите использовать другую криптобиблиотеку, это можно изменить здесь.

Аутентификация



Это значение задает тайм-аут для аутентификации, по истечении которого попытка аутентификации будет считаться неудачной.

Настройка обхода отказа



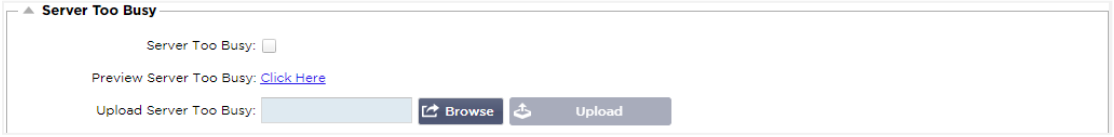
При создании кластерного набора ADC теперь есть два способа указать, как виртуальная служба будет переходить в режим отказа.

Вариант	Описание
Любая услуга	При выборе этой опции отказ любой службы в VIP приведет к тому, что весь VIP с его виртуальными службами будет передан партнеру по кластеру. Например, у вас может быть VIP 10.0.100.101 с виртуальными службами, каждая из которых использует порты 443, 8080, 4399, 2020 и т. д. Если какая-либо из этих подслужб выйдет из строя, произойдет отказ всей VIP.
Все услуги	При выборе этой опции, если одна или несколько подуслуг выйдут из строя, VIP останется на текущем участнике кластера. VIP перейдет к партнеру по кластеру только в том случае, если **все** Службы выйдут из строя. Это удобно, когда вы хотите отключить одну конкретную службу, но не хотите, чтобы VIP-служба отказала.

Протокол

Раздел "Протокол" используется для настройки множества дополнительных параметров протокола HTTP.

Сервер слишком занят



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

- Создайте простую веб-страницу со своим сообщением. Вы можете включить внешние ссылки на объекты на других веб-серверах и сайтах. Если вы хотите разместить на веб-странице изображения, используйте встроенные изображения в кодировке base64.
- Найдите только что созданный файл HTM(L) веб-страницы.
- Нажмите кнопку Загрузить
- Если вы хотите предварительно просмотреть страницу, вы можете сделать это с помощью ссылки Click Here.

Направлено для

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

Направленный выход

Вариант	**Описание**
С сайта	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, к заголовку Forwarded-For.
Замените адрес и порт	Этот выбор заменит значение заголовка Forwarded-For на IP-адрес и порт устройства или клиента, подключенного к ADC.
Заменить адрес	Этот выбор заменит значение заголовка Forwarded-For на IP-адрес устройства или клиента, подключенного к ADC.

Переданный заголовок

В этом поле можно указать имя, присвоенное заголовку Forwarded-For. Обычно это "X-Forwarded-For", но в некоторых средах оно может быть изменено.

Advanced Logging for IIS - Custom Logging

Информацию X-Forwarded-For можно получить, установив приложение IIS Advanced logging 64-bit. После загрузки создайте пользовательское поле ведения журнала под названием X-Forwarded-For с настройками, приведенными ниже.

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

Вам нужно 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:

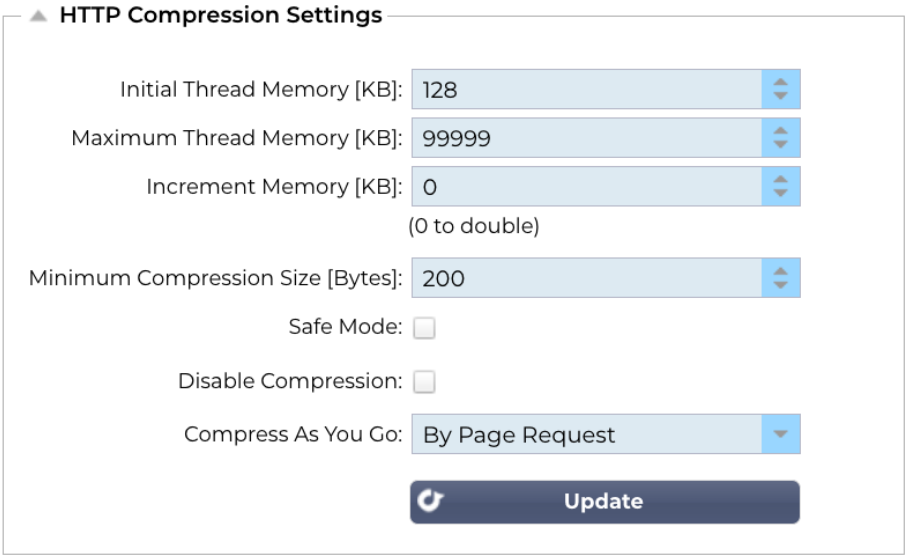
Тип	Значение
LogFormat:	"%h %l %u %t \"%r\" %>s %b \"%{Referer}i\" \"%{User-Agent}i\" комбинированный
LogFormat:	"%{X-Forwarded-For}i %l %u %t \"%r\" %>s %b \"%{Referer}i\" \"%{User-Agent}i\"" proxy SetEnvIf X- Forwarded-For "^.*\..*\..*\..*\..*" forwarded
CustomLog:	"logs/access_log" combined env=!forwarded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

Этот формат использует встроенную в Apache поддержку 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 переменной окружения "forwarded", которая содержит свободное регулярное выражение, соответствующее IP-адресу, что в данном случае вполне нормально, поскольку нас больше волнует, присутствует ли IP-адрес в заголовке X-Forwarded-For.
- Кроме того, строку 3 можно прочитать 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 удобства чтения в строках 4 и 5 не используется функция протоколирования Apache rotate logs (piped), но мы предполагаем, что почти все ее используют.

Эти изменения приведут к тому, что для каждого запроса будет регистрироваться IP-адрес.

Настройки сжатия HTTP



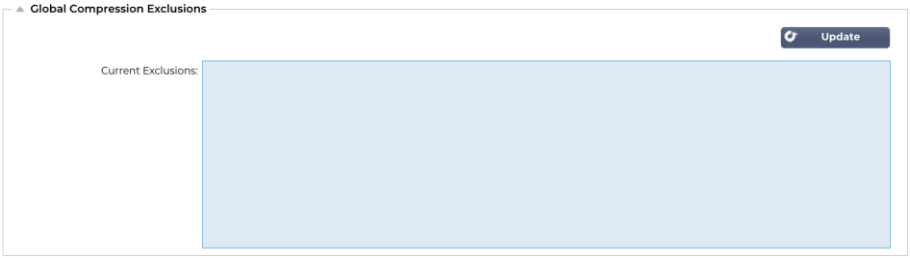
Сжатие является функцией ускорения и включается для каждой службы на странице IP-служб.

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

Вариант	**Описание**
Начальная память потока [КБ]	Это значение - объем памяти, который может быть первоначально выделен для каждого запроса, полученного ADC. Для наиболее эффективной работы это значение должно быть установлено на уровне, превышающем самый большой несжатый HTML-файл, который могут отправить веб-серверы.
Максимальная память потока [КБ]	Это значение - максимальный объем памяти, который ADC 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, ADC запишет его на диск и сожмет данные там.
Увеличение памяти [КБ]	Это значение задает объем памяти, добавляемый к начальному распределению памяти потоков, если требуется больше. По умолчанию значение равно нулю. Это означает, что ADC удвоит объем выделенной памяти, когда данные превысят текущий объем (например, 128 Кб, затем 256 Кб, затем 512 Кб и т. д.), вплоть 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 в 1 Мб).
Минимальный размер сжатия [Байт]	Это значение - размер в байтах, при котором АЦП не будет пытаться сжимать данные. Это полезно, так как 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 ADC не применял сжатие к таблицам стилей и JavaScript. Причина в том, что, хотя ADC знает, какие браузеры могут обрабатывать сжатое содержимое, некоторые другие прокси-серверы, даже если они заявляют, что соответствуют HTTP/1.1, не могут корректно передавать сжатые таблицы стилей и JavaScript. Если возникают проблемы с

	передачей таблиц стилей или JavaScript через прокси-сервер, используйте эту опцию, чтобы отключить сжатие этих типов. Однако это уменьшит общую степень сжатия содержимого.
Отключить сжатие	Установите этот флажок, чтобы запретить ADC сжимать любой ответ.
Сжимайте по мере выполнения	ON - использовать Compress as You Go на этой странице. При этом каждый блок данных, полученных от сервера, сжимается в отдельный кусок, который можно полностью декомпрессировать. OFF - Не использовать Compress As You Go на этой странице. По запросу страницы - использовать Compress as You Go по запросу страницы.

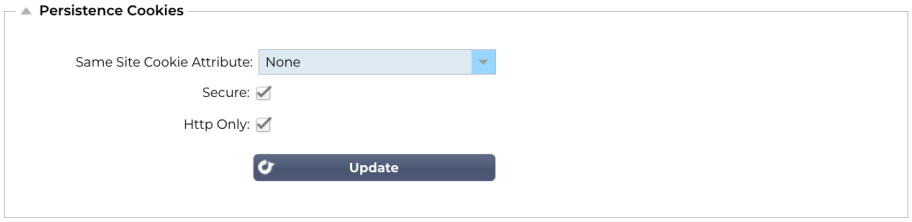
Исключения глобального сжатия



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

- Введите индивидуальное имя 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 в новую строку.

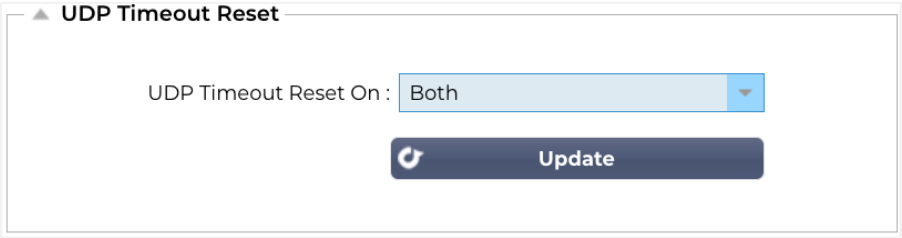
Постоянные файлы cookie



Этот параметр позволяет указать, как будут обрабатываться куки-файлы постоянства.

Поле	Описание
Тот же сайт Атрибут Кука	**Нет**: Все файлы cookie доступны для скриптов **Небрежно**: Предотвращает доступ к файлам cookie на разных сайтах, но они сохраняются, чтобы стать доступными и передаваться на сайт-владелец при его посещении. **Строгий**: не позволяет получить доступ или сохранить любой файл cookie для другого сайта **Выключено**: возврат к поведению браузера по умолчанию
Безопасный	Этот флажок, если он установлен, применяет постоянство к безопасному трафику
Только HTTP	Если флажок установлен, это позволяет использовать постоянные куки только для HTTP-трафика

Сброс таймаута UDP



Сброс таймаута UDP - это механизм, используемый в сетевых коммуникациях, при котором перезапускается таймаут, относящийся к сеансу UDP (User Datagram Protocol). Сброс помогает сохранить сессию активной, обеспечивая непрерывный поток данных без прерывания.

Вариант	Описание
Оба	Сброс таймаута UDP на сервере и клиенте.
Сервер	Сброс таймаута UDP на сервере.
Клиент	Сброс таймаута UDP на клиенте.

Программное обеспечение

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

Подробности обновления программного обеспечения

Информация в этом разделе будет заполнена, если у вас есть работающее подключение к Интернету. Если в вашем браузере нет соединения с Интернетом, этот раздел будет пустым. После подключения вы получите баннер с сообщением ниже.

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

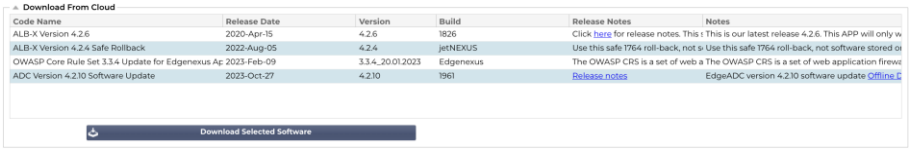
В разделе "Загрузка из облака", показанном ниже, появится информация об обновлениях, доступных для вас в рамках плана поддержки. Обратите внимание на тип поддержки и дату окончания поддержки.

Примечание: Для просмотра информации, доступной в Edgenexus Cloud, мы используем интернет-соединение вашего браузера. Вы сможете загружать обновления программного обеспечения только в том случае, если ADC имеет подключение к Интернету.

Чтобы проверить это:

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

Скачать из облака



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

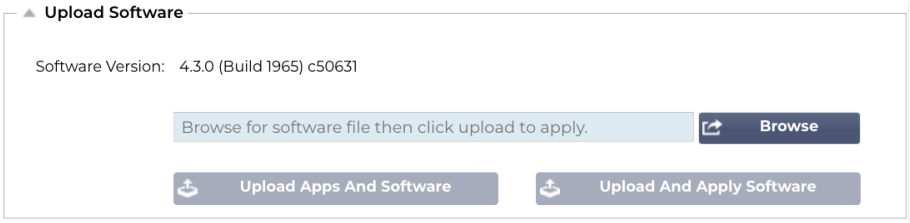
- Выделите интересующую вас строку и нажмите кнопку "Загрузить выбранное программное обеспечение в ALB".
- Выбранное программное обеспечение будет загружено на ваш ALB после щелчка, и его можно применить в разделе "Применить программное обеспечение, хранящееся на ALB" ниже.

Примечание: Если у АДЦ нет прямого доступа в Интернет, вы получите ошибку, как показано ниже:

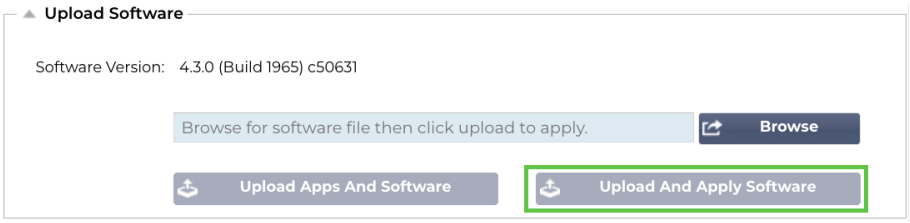
Ошибка загрузки, ALB не может получить доступ к ADC Cloud Services для файла build1734-3236-v4.2.1-Sprint2-update-64.software.alb

Если ваша сеть защищена прокси-сервером, см.App Store Download Proxy

Программное обеспечение для загрузки



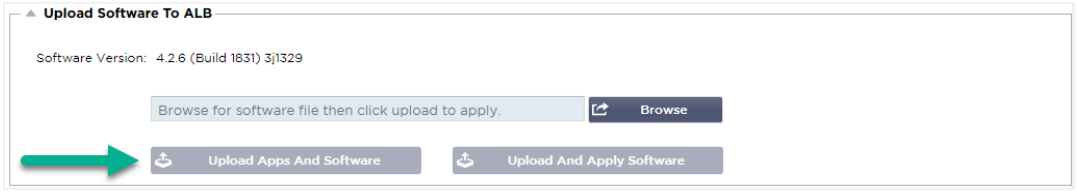
Загрузка приложений



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

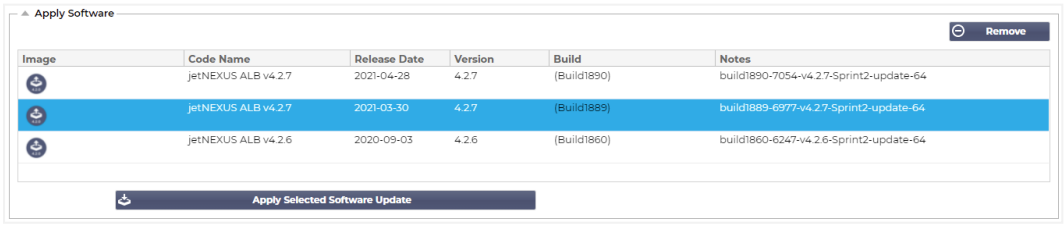
- Существует пять типов приложений
  - <Имя приложения>flightpath.alb
  - <Имя приложения>.monitor.alb
  - <имя приложения>.jetpack.alb
  - <имя приложения>.addons.alb
  - <имя приложения>.featurepack.alb
- После загрузки каждое приложение можно найти в разделе Библиотека>Приложения.
- Затем необходимо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

Программное обеспечение / Обновления прошивки



- 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 АЛБ", откуда вы сможете применить его в удобное для вас время.

Применение программного обеспечения, хранящегося на ADC



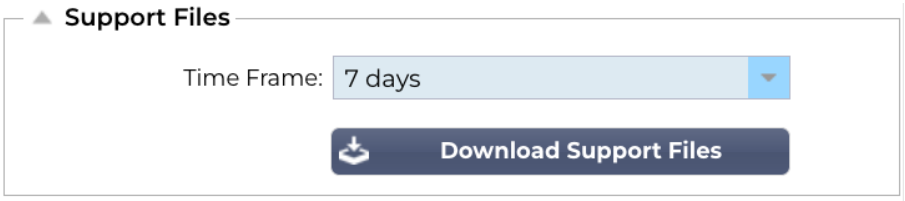
В этом разделе отображаются все файлы программного обеспечения, хранящиеся на ALB и доступные для развертывания. В список будут включены обновленные сигнатуры брандмауэра веб-приложений (WAF).

- 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 сигнатурным обновлением OWASP, оно будет применено автоматически без перезагрузки.

Устранение неполадок

Всегда есть проблемы, которые требуют поиска причин и решений. Данный раздел позволяет это сделать.

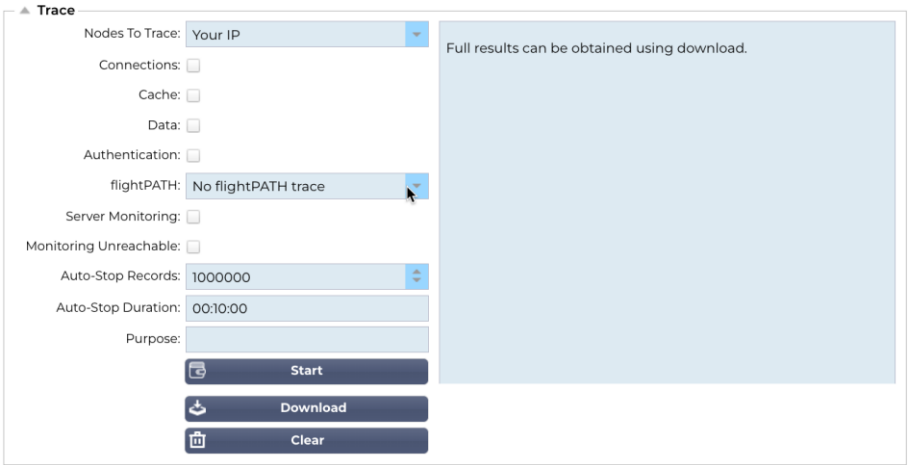
Файлы поддержки



Если у вас возникла проблема с ADC и необходимо открыть тикет поддержки, служба технической поддержки часто запрашивает несколько различных файлов с устройства ADC. Теперь эти файлы объединены в один файл .dat, который можно загрузить в этом разделе.

- Выберите временной интервал из выпадающего списка: На выбор предлагаются 3, 7, 14 и все дни.
- Нажмите "Загрузить файлы поддержки".
- Будет загружен файл в формате Support-jetNEXUS-yyymmddhh-NAME.dat
- Отправьте заявку в службу поддержки на портале поддержки, подробная информация о котором приведена в конце этого документа.
- Убедитесь, что вы подробно описали проблему и прикрепили файл .dat к тикету.

След



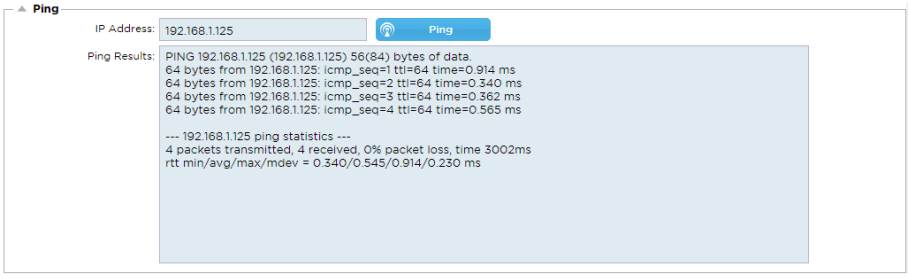
В разделе "Трассировка" можно просмотреть информацию, позволяющую отладить проблему. Предоставляемая информация зависит от опций, которые вы выбираете в раскрывающихся списках и флажках.

Вариант	**Описание**
Узлы для трассировки	**Ваш IP**: Это отфильтрует вывод, чтобы использовать IP-адрес, с которого вы получаете доступ к графическому интерфейсу (обратите внимание, не выбирайте эту опцию для мониторинга, так как мониторинг будет использовать адрес интерфейса ADC). **Все IP**: Фильтр применяться не будет. Следует отметить, что при загруженном блоке это негативно скажется на производительности.

Соединения	При установке этого флажка будет отображаться информация о соединениях на стороне клиента и сервера.
Кэш	При установке этого флажка будет отображаться информация о кэшированных объектах.
Данные	Если этот флажок установлен, в список будут включены байты необработанных данных, обрабатываемые АЦП при входе и выходе.
flightPATH	Меню flightPATH позволяет выбрать конкретное правило flightPATH для мониторинга или Все правила flightPATH.
Мониторинг сервера	При установке этого флажка будут показаны мониторы состояния сервера, активные на ADC, и соответствующие результаты.
Мониторинг недоступности	При выборе этой опции поведение очень похоже на мониторинг сервера, за исключением того, что он показывает только неудачные мониторы и действует как фильтр только для этих сообщений.
Записи автостопа	Значение по умолчанию - 1 000 000 записей, после чего трассировка автоматически прекращается. Эта настройка является мерой предосторожности, чтобы предотвратить случайное включение функции Trace и ее негативное влияние на работу АЦП.
Продолжительность автоостановки	По умолчанию установлено время 10 минут, по истечении которого функция Trace автоматически прекращается. Эта функция является мерой предосторожности для предотвращения случайного оставления функции Trace включенной и влияния на работу АЦП.
Начало	Нажмите эту кнопку, чтобы запустить средство трассировки вручную.
Остановить	Нажмите, чтобы вручную остановить средство трассировки до того, как будет достигнута автоматическая запись или время.
Скачать	Несмотря на то, что вы можете видеть программу просмотра в реальном времени с правой стороны, информация может отображаться слишком быстро. Вместо этого вы можете загрузить журнал Trace.log, чтобы просмотреть всю информацию, собранную во время различных трасс в тот день. Эта функция представляет собой отфильтрованный список информации о трассировке. Если вы хотите просмотреть информацию о трассировке за предыдущие дни, вы можете загрузить Syslog за этот день, но фильтровать придется вручную.
Очистить	Очистка журнала трассировки

Пинг

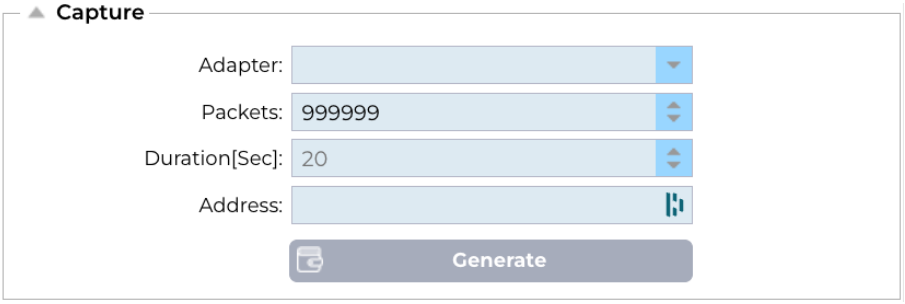
Вы можете проверить сетевое подключение к серверам и другим сетевым объектам в вашей инфраструктуре с помощью инструмента Ping.



Введите IP-адрес узла, который вы хотите проверить, например, шлюз по умолчанию, используя десятичную систему счисления, или адрес IPv6. После нажатия кнопки "Ping" вам, возможно, придется подождать несколько секунд, чтобы получить результат.

Если вы настроили DNS-сервер, то можете ввести полное доменное имя. Настроить DNS-сервер можно в разделе **DNS Server 1 & DNS Server 2**. После нажатия кнопки "Ping" вам, возможно, придется подождать несколько секунд, чтобы получить результат.

Захват



Чтобы захватить сетевой трафик, следуйте простым инструкциям, приведенным ниже.

- Заполните параметры в форме
- Нажмите кнопку Создать
- После запуска захвата в вашем браузере появится окно с вопросом, куда сохранить файл. Он будет иметь формат "jetNEXUS.cap.gz".
- Отправьте заявку в службу поддержки на портале поддержки, подробная информация о котором приведена в конце этого документа.
- Убедитесь, что вы подробно описали проблему и прикрепили файл к тикету.
- Вы также можете просмотреть содержимое с помощью Wireshark

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

Чтобы сохранить производительность, мы ограничили размер загружаемого файла 10 МБ. Если вы обнаружите, что этого недостаточно для получения всех необходимых данных, мы можем увеличить эту цифру.

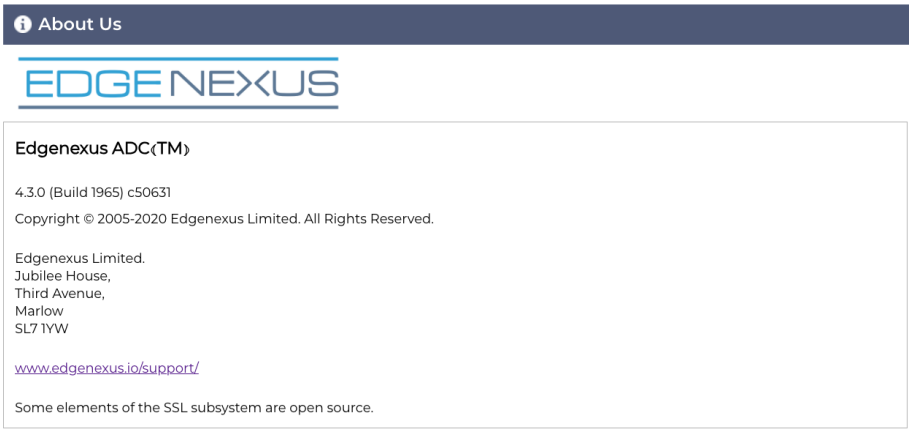
Примечание: Это повлияет на производительность живых сайтов. Чтобы увеличить доступный размер захвата, примените глобальную настройку jetPACK для увеличения размера захвата.

Помощь

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

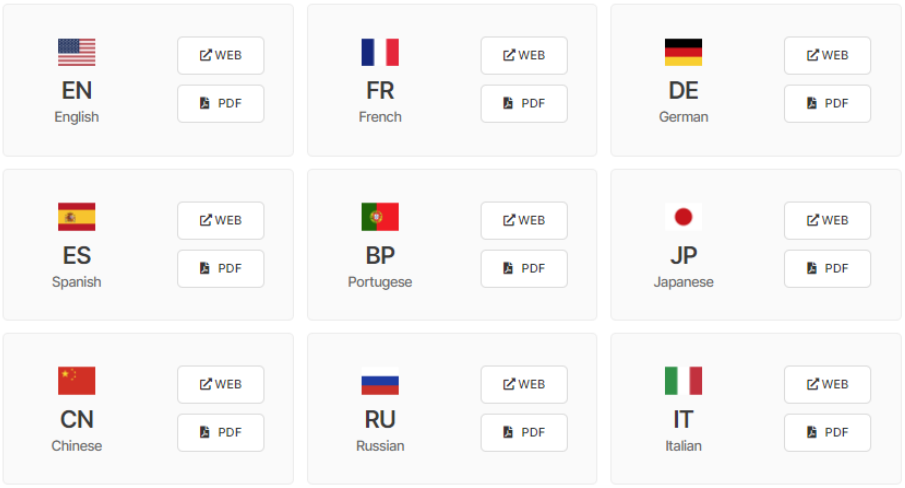
О нас

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



Ссылка

Опция Reference открывает веб-страницу с руководствами пользователя и другими полезными документами. Веб-страницу также можно найти с помощью https://www.edgenexus.io/documentation.



Если вы не нашли то, что искали, обратитесь по адресу .support@edgenexus.io

JetPACKs

Edgenexus jetPACK s

Пакеты jetPACK - это уникальный метод мгновенной настройки ADC для конкретных приложений. Эти простые в использовании шаблоны поставляются предварительно сконфигурированными и полностью настроенными со всеми специфическими для конкретного приложения параметрами, которые необходимы для оптимального предоставления услуг с помощью вашего ADC. Некоторые из jetPACK используют flightPATH для управления трафиком, и для работы этого элемента необходимо иметь лицензию flightPATH. Чтобы узнать, есть ли у вас лицензия на flightPATH, обратитесь к странице **Лицензии**.

Загрузка пакета jetPACK

- Каждый jetPACK, представленный ниже, был создан с уникальным виртуальным IP-адресом, содержащимся в названии jetPACK. Например, первый jetPACK ниже имеет виртуальный IP-адрес 1.1.1.1
- Вы можете либо загрузить этот jetPACK как есть и изменить IP-адрес в графическом интерфейсе, либо отредактировать jetPACK с помощью текстового редактора, например 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 HTTP-службы 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. Виртуальный IP-адрес службы: 1.1.1.1 Порты виртуальных служб: 80, 443, 135, 59534, 59535 Реальные серверы: 127.1.1.1 127.2.2.2 flightPATH: Добавляет перенаправление с HTTP на HTTPS
	jetPACK-1.1.1.2-Exchange-2010-SMTP-RP	То же самое, что и выше, но добавляется служба SMTP на порт 25 в режиме обратного прокси. SMTP-сервер будет видеть адрес интерфейса ALB-X в качестве IP-адреса источника.	Глобальные настройки: Тайм-аут обслуживания 2 часа Мониторы: Монитор уровня 7 для веб-приложения Outlook. Внеполосный монитор уровня 4 для службы клиентского доступа Виртуальный IP-адрес службы: 1.1.1.1 Порты виртуальных служб: 80, 443, 135, 59534, 59535, 25 (обратный прокси)

			Реальные серверы: 127.1.1.1 127.2.2.2 flightPATH: Добавляет перенаправление с HTTP на HTTPS
	jetPACK-1.1.1.3-Exchange-2010-SMTP-DSR	То же самое, что и выше, за исключением того, что этот jetPACK настроит службу SMTP на использование прямого возврата сервера. Этот jetPACK необходим, если ваш SMTP-сервер должен видеть фактический IP-адрес клиента.	Глобальные настройки: Тайм-аут обслуживания 2 часа Мониторы: Монитор уровня 7 для веб-приложения Outlook. Внеполосный монитор уровня 4 для службы клиентского доступа Виртуальный IP-адрес службы: 1.1.1.1 Порты виртуального сервиса: 80, 443, 135, 59534, 59535, 25 (прямой возврат сервера) Реальные серверы: 127.1.1.1 127.2.2.2 flightPATH: Добавляет перенаправление с HTTP на HTTPs
Exchange 2013	jetPACK-2.2.2.1-Exchange-2013-Low-Resource	Эта настройка добавляет 1 VIP и две службы для HTTP и HTTPS трафика и требует меньше всего CPU. Можно добавить несколько проверок состояния VIP, чтобы убедиться, что каждая из отдельных служб находится в рабочем состоянии.	Глобальные настройки: Мониторы: Монитор уровня 7 для OWA, EWS, OA, EAS, ECP, OAB и ADS Виртуальный IP-адрес 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, следовательно, использует больше ресурсов, чем выше. Вы должны настроить каждый сервис как отдельную DNS-запись Пример owa.edgenexus.com, ews.edgenexus.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 Виртуальный сервисный IP: 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 Виртуальный IP-адрес 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	Передняя часть	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	Выгрузка SSL	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

Выгрузка SSL	
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 безопасный порт GUI с 27376 на 443. HTTPs://x.x.x.x
- GUI Timeout 1 day - графический интерфейс 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 **безвозмездных ARP**, чтобы помочь коммутаторам во время перехода.
- Размер захвата 16 МБ - по умолчанию размер захвата составляет 2 МБ. Это значение увеличит размер до 16 МБ.

Cipher s и Cipher jetPACKs

В стандартную комплектацию EdgeADC входят лучшие шифры. Эти шифры соединены с соответствующими протоколами TLS, что упрощает работу пользователей.

Мы предоставили набор дополнительных шифров, которые вы можете использовать, если они вам понадобятся.

Сильные шифры

Добавляет возможность выбрать "Сильные шифры" из списка опций шифров:

```
ALL:RC4+RSA:+RC4:+HIGH:!DES-CBC3-SHA:!SSLv2:!ADH:!EXP:!ADHexport:!MD5
```

Антизверь

Добавляет возможность выбрать "Антизверь" из списка опций шифра:

```
ECDHE-RSA-AES128-SHA256:AES128-GCM-SHA256:RC4:HIGH:!MD5:!aNULL:!EDH
```

Нет SSLv3

Добавляет возможность выбрать "No SSLv3" в списке Cipher Options:

```
ECDHE-RSA-AES128-SHA256:AES128-GCM-SHA256:HIGH:!MD5:!aNULL:!EDH:!RC4
```

Нет SSLv3 нет TLSv1 нет RC4

Добавляет возможность выбрать "No-TLSv1 No-SSLv3 No-RC4" из списка Cipher Options:

```
ECDHE-RSA-AES128-SHA256:AES128-GCM-SHA256:HIGH:!MD5:!aNULL:!EDH:!RC4
```

NO_TLSv1.1

Добавляет возможность выбрать "NO_TLSv1.1" из списка Cipher Options:

```
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
```

Включить шифры TLS-1.0-1.1

В сборке 4.2.10 и далее поддержка Cipher для протоколов TLS1.0 и TLS 1.1 была упразднена. Однако некоторые клиенты продолжают использовать эти старые, устаревшие протоколы для своих внутренних серверов. Нижеприведенный Cipher добавляет возможность включить TLS v1.0 и TLS v1.1.

```
AES128-SHA:AES256-SHA:DES-CBC-SHA:DES-CBC3-SHA:EXP-DES-CBC-SHA:RC4-SHA:RC4-MD5:DHE-RSA-AES128-SHA:DHE-RSA-AES256-
SHA:EDH-RSA-DES-CBC-SHA:EDH-RSA-DES-CBC3-SHA:EXP-EDH-RSA-DES-CBC-SHA:EXP-RC2-CBC-MD5:AES128-SHA256:AES256-
SHA256:DHE-RSA-AES128-SHA256:DHE-RSA-AES256-SHA256:AES128-GCM-SHA256:AES256-GCM-SHA384:DHE-RSA-AES128-GCM-
SHA256:DHE-RSA-AES256-GCM-SHA384:DHE-DSS-AES128-SHA256:DHE-DSS-AES256-SHA256:DHE-DSS-AES128-GCM-SHA256:DHE-DSS-
AES256-GCM-SHA384:AES:ALL:!aNULL:!ADH:!eNULL:!LOW:!EXP:RC4+RSA:+HIGH:+MEDIUM
```

Пример шифра jetPACK

Шифры импортируются в ADC с помощью jetPACK. jetPACK - это простой текстовый файл, содержащий параметры, которые распознает ADC. В примере ниже показан jetPACK, использующий шифр Enable TLS-1.0-1.1.

```
#!update

[jetnexusdaemon-cipher-TLS1-0-TLS-1-1]

Cipher="AES128-SHA:AES256-SHA:DES-CBC-SHA:DES-CBC3-SHA:EXP-DES-CBC-SHA:RC4-SHA:RC4-MD5:DHE-RSA-AES128-SHA:DHE-RSA-
AES256-SHA:EDH-RSA-DES-CBC-SHA:EDH-RSA-DES-CBC3-SHA:EXP-EDH-RSA-DES-CBC-SHA:EXP-RC2-CBC-MD5:AES128-SHA256:AES256-
SHA256:DHE-RSA-AES128-SHA256:DHE-RSA-AES256-SHA256:AES128-GCM-SHA256:AES256-GCM-SHA384:DHE-RSA-AES128-GCM-
```

```
SHA256:DHE-RSA-AES256-GCM-SHA384:DHE-DSS-AES128-SHA256:DHE-DSS-AES256-SHA256:DHE-DSS-AES128-GCM-SHA256:DHE-DSS-AES256-GCM-SHA384:AES:ALL:!aNULL:!ADH:!eNULL:!LOW:!EXP:RC4+RSA:+HIGH:+MEDIUM"

Cipher1=""

Cipher2=""

CipherOptions="-NO_TLSv1.0 -NO_TLSv1.1 -NO_TLSv1.2 -NO_TLSv1"

Description=" TLS v1.0 - v1.1 Enabled"
```

- X-Content-Type-Options - добавьте этот заголовок, если он не существует, и установите для него значение "nosniff" - это предотвратит автоматический "MIME-снайпинг" браузера.
- X-Frame-Options - добавьте этот заголовок, если он не существует, и установите 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 в значение "max-age=31536000 ; includeSubdomains" - это 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 и не используйте jetPACK с одним и тем же виртуальным IP-адресом. Это действие приведет к дублированию IP-адреса в конфигурации. Если вы сделали это по ошибке, вы можете изменить это в графическом интерфейсе.

- Перейдите в раздел Дополнительно > Обновить программное обеспечение
- Раздел конфигурации
- Загрузка новой конфигурации или jetPACK
- Обзор для jetPACK
- Нажмите кнопку Загрузить
- Когда экран браузера станет белым, нажмите кнопку обновления и дождитесь появления страницы Dashboard.

Создание пакета jetPACK

Одна из замечательных особенностей jetPACK - возможность 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".
- Сохраните после завершения

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

Ниже перечислены разделы, которые рекомендуется редактировать/копировать.

Раздел 0:

```
#!jetpack
```

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

Раздел1:

```
[jetnexusdaemon].
```

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

Примеры:

```
ConnectionTimeout=600000
```

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

```
ContentServerCustomTimer=20000
```

Этот пример - задержка в миллисекундах между проверками работоспособности 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 изменение необходимо для обратного прокси Lync 2010/2013.

Раздел 2:

```
[jetnexusdaemon-Csm-Rules]
```

В этом разделе содержатся пользовательские правила мониторинга сервера, которые обычно настраиваются с веб-консоли.

Пример:

```
[jetnexusdaemon-Csm-Rules-0]
Content="Сервер поднят"
Desc="Монитор 1″
Метод="CheckResponse"
Name="Проверка здоровья - работает ли сервер"
Url="HTTP://demo.jetneus.com/healthcheck/healthcheck.html"
```

Раздел 3:

```
[jetnexusdaemon-LocalInterface]
```

В этом разделе содержатся все сведения из 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=">,""Безопасная группа"",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 теми, что были применены к интерфейсу. В примере выше мы видим, что правило flightPATH "6" было применено к каналу, включая это в качестве примера ниже.

Пример:

```
[jetnexusdaemon-Path-6]
Desc="Принудительное использование HTTPS для определенного каталога"
Name="Gary - Force HTTPS"
[jetnexusdaemon-Path-6-Condition-1]
Check="contain"
Условие="путь"
Соответствие=
```

```
Sense="делает"
Значение="/secure/"
[jetnexusdaemon-Path-6-Evaluate-1].
Подробно=
Источник="host"
Значение=
Переменная="$host$"[jetnexusdaemon-Path-6-Function-1]
Action="redirect"
Target="HTTPs://$host$$path$$querystring$"
Значение=
```

flightPATH

Введение в flightPATH

Что такое flightPATH?

flightPATH - это интеллектуальный механизм правил, разработанный компанией Edgenexus для манипулирования и маршрутизации HTTP и HTTPS трафика. Он очень настраиваемый, очень мощный и при этом очень простой в использовании.

Хотя некоторые компоненты flightPATH являются IP-объектами, например Source IP, flightPATH можно применить только к типу службы уровня 7, равному HTTP(s). Если вы выберете любой другой тип службы, то вкладка flightPATH в IP Services будет пустой.

Что может сделать flightPATH?

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

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

Более подробную информацию о RegEx можно найти на этом полезном сайте

Кроме того, в разделе "Оценка" можно создавать пользовательские переменные и использовать их в области "Действия", что открывает множество различных возможностей.

Правило flightPATH состоит из трех компонентов:

Вариант	Описание
Подробности	Используется для добавления или удаления flightPATH и перечисления доступных.
Состояние	Задайте несколько критериев для запуска правила flightPATH.
Оценка	Позволяет использовать переменные, которые можно применять в области действий.
Действие	Поведение после срабатывания правила.

Состояние

В этом разделе вы можете указать пять отдельных параметров, которые применяются к условию. Ниже приводится описание каждого параметра и пример.

Состояние	Описание	Пример
<form>	HTML-формы используются для передачи данных на сервер	Пример "форма не имеет длины 0"
Местоположение ГЕО	При этом IP-адрес источника сравнивается с кодом страны ISO 3166.	Местоположение ГЕО равно GB ИЛИ Местоположение ГЕО равно Germany
Хозяин	Это хост, извлеченный 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	Это выпадающий список, включающий GET, POST и т.д.

Происхождение IP	Если восходящий прокси поддерживает X-Forwarded-for (XFF), он будет использовать истинный адрес Origin.	IP-адрес клиента. Можно также использовать несколько IP-адресов или подсетей. 10\.1\.2\.* - это подсеть 10.1.2.0 /24 10\.1\.2\.3|10\.1\.2\.4 Используйте | для нескольких IP-адресов
Путь	Это путь к веб-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=edgeNEXUS", где совпадение - Best, а значение - edgeNEXUS
Строка запроса	Вся строка запроса после символа ?	
Запросить Cookie	Это имя cookie, запрашиваемого клиентом.	MS-WSMAN=afYfn1CDqqCDqUD::
Заголовок запроса	Это может быть любой HTTP-заголовок	Referrer, User-Agent, From, Date
Версия для запросов	Это HTTP-версия	HTTP/1.0 ИЛИ HTTP/1.1
Орган реагирования	Заданная пользователем строка в теле ответа	Сервер вверх
Код ответа	Код HTTP для ответа	200 OK, 304 Not Modified
Ответное печенье	Это имя файла cookie, отправляемого 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 объединенный IP-адрес	Клиент IP, IP прокси, IP брандмауэра. Можно также использовать несколько IP-адресов и подсетей. Вы необходимо экранировать точки, так как они являются RegEX. Пример 10\.1\.2\.3 - это 10.1.2.3

Матч

Параметр Match зависит от контекста и значения параметра Condition.

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

Заряжайся	Содержит информацию о расходах на применение 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 для запросов 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 создания сообщения	Дата = "Дата" ":" HTTP-дата
ETag	Идентификатор для конкретной версии ресурса, часто это дайджест сообщения.	ETag: "aed6bdb8e090cd1:0".
С сайта	Адрес электронной почты пользователя, сделавшего 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 оказывать различное влияние в любой точке цепочки "запрос - ответ".	Pragma: no-cache
Реферрер	Это адрес предыдущей веб-страницы, с которой велась 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)
Vary	Указывает нижестоящим прокси-серверам, как сопоставить заголовки будущих запросов, чтобы решить можно ли использовать кэшированный ответ, а не запрашивать новый с оригинального сервера	Vary: User-Agent
X-Powered-By	Указывает технологию (например, ASP.NET, PHP, JBoss), поддерживающую веб-приложение	X-Powered-By: PHP/5.4.0

Проверьте

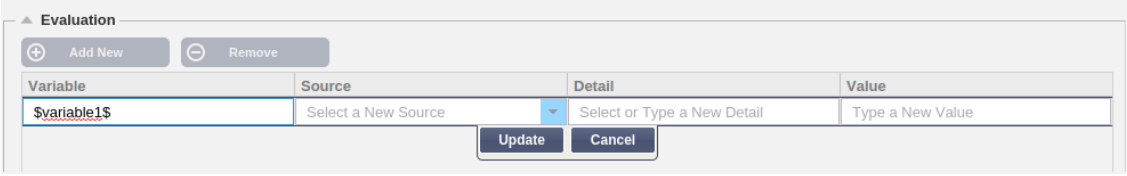
Проверьте	Описание	Пример
Существовать	Здесь не важны детали условия, важно лишь то, что оно существует/не существует	Хост> Существует >
Начало	Строка начинается со значения	Путь> Начинается> Начинается /secure>
Конец	Строка заканчивается значением	Путь> Начало> Конец> .jpg

Содержите	Строка содержит значение	Заголовок запроса> Принять> Содержит ли> изображение>
Равный	Строка равна значению	Хозяин> Равняется ли > > www.edgenexus.io
Длина	Строка имеет длину, равную значению	Хост> Имеет ли> длину> 16 www.edgenexus.io = TRUE www.edgenexus.com = FALSE
Превышение длины	Проверьте, что значение превышает/не превышает заданную длину.	Путь > Делает > Превысить длину - 10
Соответствие RegEx	Это позволяет ввести полное регулярное выражение, совместимое с Perl	IP-адрес происхождения> Соответствует ли> Regex> 10\..* | 11\..*
Список матчей	Позволяет предоставить список значений, разграниченных PIPE (|), по которым можно выполнить проверку.	IP-адрес источника > Есть > Список соответствия > 10.0.0.1 | 10.0.0.100 | 192.178.28.32

Пример

- В примере есть два условия, и **ОБА** должны быть выполнены, чтобы выполнить действие
- Первая проверка заключается в том, что запрашиваемый объект является изображением
- Второй - проверка конкретного имени хоста

Оценка



Добавление переменной - 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 возникли проблемы с безопасностью.

- Переменная: Она должна начинаться и заканчиваться символом $. Например, $variable1$
- Источник: Выберите из раскрывающегося 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 запись оценки.
- Вы можете использовать в своем действии 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") = $resp$
- Хост = $host$
- Версия = $version$
- Клиентский порт = $clientport$
- Клиент = $clientip$
- Геолокация = $geolocation$"

Пример действия:

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

Объяснение:

- Клиент, обратившийся к несуществующей странице, обычно получает в браузере страницу 404.
- 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 адреса 154.3.22.14:3454 только что выполнил запрос на страницу wrong.html".

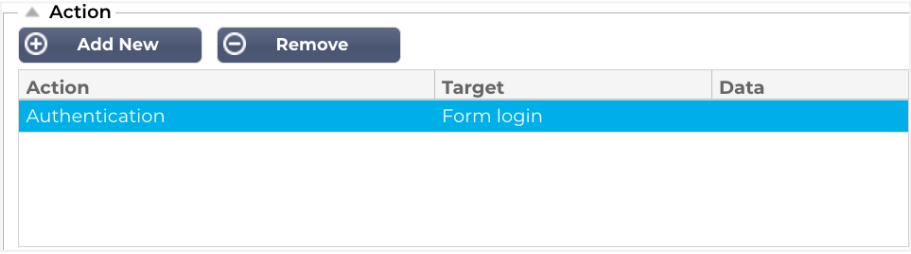
Источник	Описание	Пример
Печенье	Это имя и значение заголовка cookie.	MS-WSMAN=afYfn1CDqqCDqUD::где имя - MS-WSMAN, а значение - afYfn1CDqqCDqUD::
Хозяин	Это имя хоста, извлеченное из URL-адреса	www.mywebsite.com или 192.168.1.1
Язык	Вот язык, извлеченный из HTTP-заголовка Language	Это условие приведет к появлению выпадающего списка языков.
Метод	Это выпадающий список методов HTTP	В раскрывающемся списке будут указаны GET, POST
Путь	Это путь к веб-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 совпадение - 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 HTTP-версия	HTTP/1.0 или HTTP/1.1

Деталь	Описание	Пример
Принять	Типы содержимого, которые допустимы	Принять: text/plain
Accept-Encoding	Допустимые кодировки	Accept-Encoding: <compress | gzip | deflate | sdch | identity>.

Accept-Language	Приемлемые языки для ответа	Язык приема: en-US
Диапазоны приема	Какие типы диапазонов частичного содержимого поддерживает этот сервер	Диапазон приема: байты
Авторизация	Учетные данные для аутентификации по протоколу HTTP	Авторизация: Basic QWxhZGRpbjpvcGVuIHNlc2FtZQ==
Заряжайся	Содержит информацию о расходах на применение 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 для запросов 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, когда сообщение было отправлено	Дата = "Дата" ":" HTTP-дата
ETag	Идентификатор для конкретной версии ресурса, часто это дайджест сообщения.	ETag: "aed6bdb8e090cd1:0".
С сайта	Адрес электронной почты пользователя, сделавшего запрос	От: user@example.com
If-Modified-Since	Позволяет возвращать сообщение 304 Not Modified, если содержимое не изменилось.	If-Modified-Since: Sat, 29 Oct 1994 19:43:31 GMT
Last-Modified	Дата последнего изменения для запрашиваемого объекта в формате RFC 2822	Last-Modified: Tue, 15 Nov 1994 12:45:26 GMT
Pragma	Специфические для реализации заголовки, которые могут иметь различные эффекты в любой точке цепочки "запрос-ответ".	Pragma: no-cache
Реферрер	Это адрес предыдущей веб-страницы, с которой велась 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)
Vary	Сообщает нижестоящим прокси-серверам, как сопоставить заголовки будущих запросов, чтобы решить можно ли использовать кэшированный ответ, а не запрашивать новый с оригинального сервера	Vary: User-Agent
X-Powered-By	Указание технологии (например, ASP.NET, PHP, JBoss), поддерживающей 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, чтобы просмотреть выпадающий список.

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

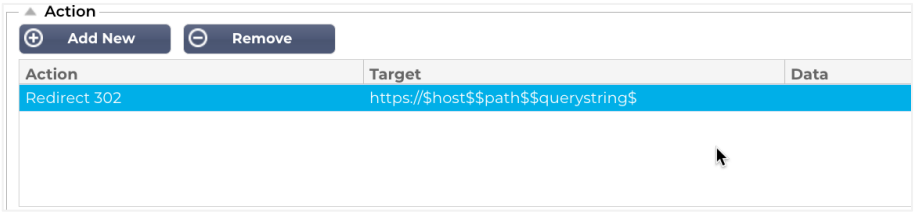
Дважды щелкните на столбце "Данные", чтобы вручную добавить данные, которые вы хотите добавить или заменить.

Список всех действий приведен ниже:

Действие	Описание	Пример
Cookie запроса на добавление	Добавьте куки запроса, подробно описанные в разделе "Цель", со значением в разделе "Данные".	Target= Cookie Данные= MS-WSMAN=afYfn1CDqqCDqCVii
Добавить заголовок запроса	Добавьте заголовок запроса типа Target со значением в секции Data	Цель = Принять Data= image/png
Добавить Cookie для ответа	Добавьте куки-файлы ответа, подробно описанные в разделе "Цель", со значением в разделе "Данные".	Target= Cookie 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:// (Заменяющая строка)
Замена корпуса в первую очередь	Выполните поиск в теле ответа и замените только первый экземпляр	Target= HTTP:// (строка поиска) Data= HTTPs:// (Заменяющая строка)
Замена корпуса Последняя	Выполните поиск в теле ответа и замените только последний экземпляр	Target= HTTP:// (строка поиска) Data= HTTPs:// (Заменяющая строка)
Капля	Это приведет к разрыву соединения	Цель = N/A Данные = N/A
Электронная почта	Отправит письмо на адрес, настроенный в Email Events. В	Target="flightPATH отправил сообщение об этом событии"

	качестве адреса или сообщения можно использовать переменную	Данные = N/A
Журнал событий	Это приведет к регистрации события в системном журнале	Target="flightPATH зарегистрировал это в syslog". Данные = N/A
Перенаправление 301	Это приведет к постоянному перенаправлению	Цель= HTTP://www.edgenexus.io Данные= N/A
Перенаправление 302	Это приведет к временному перенаправлению	Цель= HTTP://www.edgenexus.io Данные= N/A
Удалить куки запроса	Удалите cookie запроса, подробно описанные в разделе "Цель	Target= Cookie Данные= MS-WSMAN=afYfn1CDqqCDqCVii
Удалить заголовок запроса	Удалите заголовок запроса, подробно описанный в разделе Цель	Цель=Сервер Данные=N/A
Удаление cookie-файла ответа	Удалите куки-файлы, указанные в разделе "Цель".	Target=jnAccel
Удалить заголовок ответа	Удалите заголовок ответа, подробно описанный в разделе "Цель	Target= Etag Данные = N/A
Заменить cookie запроса	Замените cookie запроса, указанные в разделе "Цель", на значение в разделе "Данные".	Target= Cookie Данные= MS-WSMAN=afYfn1CDqqCDqCVii
Замена заголовка запроса	Замените заголовок запроса в цели значением Data	Цель = Соединение Data= keep-alive
Заменить cookie ответа	Замените cookie-файл ответа, указанный в разделе Target, на значение в разделе Data	Target=jnAccel=afYfn1CDqqCDqCVii Date=MS-WSMAN=afYfn1CDqqCDqCVii
Заменить заголовок ответа	Замените заголовок ответа, указанный в разделе Target, на значение в разделе Data	Цель= Сервер Данные = Удержано в целях безопасности
Перезапись пути	Это позволит вам перенаправить запрос на новый URL, основываясь на условии	Target= /test/path/index.html$querystring$ Данные = N/A
Используйте безопасный сервер	Выберите, какой безопасный сервер или виртуальную службу использовать	Target=192.168.101:443 Данные=N/A
Используйте сервер	Выберите, какой сервер или виртуальную службу использовать	Цель= 192.168.101:80 Данные= N/A
Зашифровать cookie	Это позволит зашифровать файлы cookie в формате 3DES, а затем закодировать их в base64	Target= Введите имя cookie, которое будет зашифровано, в конце можно использовать символ * в качестве подстановочного знака. Данные= 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

- Блокируйте нежелательные IP-адреса
- Принуждение пользователя к использованию HTTPS для определенного (или всего) содержимого
- Блокируйте или перенаправляйте 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
- Обеспечьте единую регистрацию в нескольких системах
- Сегментируйте 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 кодах ответа 404
- Предотвращение доступа к каталогу/просмотра
- Отправляйте паукам различный контент

Готовые правила

Расширение HTML

Изменяет все запросы .htm на .html

Состояние:

- Условие = Путь
- Чувствовать = делать
- Check = Match RegEx
- Значение = \.htm$

Оценка:

- Пустой

Действие:

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

Index.html

Принудительно используйте index.html в запросах к папкам.

Условие: это общее условие, которое подходит для большинства объектов

- Условие = Хозяин
- Чувствовать = делать
- Проверка = Существовать

Оценка:

- Пустой

Действие:

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

Закрыть папки

Отказывать в запросах на папки.

Условие: это общее условие, которое подходит для большинства объектов

- Состояние = над этим нужно хорошенько подумать
- Чувство =
- Проверка =

Оценка:

- Бланк

Действие:

- Действие =
- Цель =

Спрячьте CGI-BBIN:

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

Условие: это общее условие, которое подходит для большинства объектов

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

Оценка:

- Бланк

Действие:

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

Бревно-паук

Журнал запросов пауков популярных поисковых систем.

Условие: это общее условие, которое подходит для большинства объектов

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

Оценка:

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

Действие:

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

Принудительное использование HTTPS

Принудительное использование HTTPS для определенной директории. В этом случае, если клиент обращается к чему-либо, содержащему директорию /secure/, он будет перенаправлен на HTTPs-версию запрашиваемого URL.

Состояние:

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

Оценка:

- Бланк

Действие:

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

Медиапоток:

Перенаправляет Flash Media Stream на соответствующую службу.

Состояние:

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

Оценка:

- Бланк

Действие:

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

Замена HTTP на HTTPS

Измените все жесткие коды HTTP:// на HTTPS://.

Состояние:

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

Оценка:

- Бланк

Действие:

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

Забудьте о кредитных картах

Проверьте, нет ли в ответе кредитных карт, и если одна из них найдена, удалите ее.

Состояние:

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

Оценка:

- Бланк

Действие:

- 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

Срок действия содержимого

Добавьте на страницу разумную дату истечения срока действия контента, чтобы уменьшить количество запросов и 304.

Состояние: это общее состояние. Рекомендуется сосредоточить это условие на вашем

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

Оценка:

- Бланк

Действие:

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

Тип поддельного сервера

Получите тип сервера и измените его на другой.

Состояние: это общее состояние. Рекомендуется сосредоточить это условие на вашем

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

Оценка:

- Пустой

Действие:

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

Никогда не отправляйте ошибки

Клиент никогда не получает никаких ошибок с вашего сайта.

Состояние

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

Оценка

- Пустой

Действие

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

Перенаправление на язык

Найдите код языка и перенаправьте на домен соответствующей страны.

Состояние

- Условие = Язык
- Чувствовать = делать
- Проверять = Содержать
- Значение = Немецкий (стандарт)

Оценка

- Переменная = $host_template$
- Источник = Хозяин

- Значение = .*\.

Действие

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

Google Analytics

Вставьте код, требуемый Google для аналитики - пожалуйста, измените значение MYGOOGLECODE на ваш Google UA ID.

Состояние

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

Оценка

- пустой

Действие

- Действие = Заменить тело последним
- Цель = </body>
- Данные = <script type='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 в службах IPv6. Серверы IIS IPv4 не любят видеть IPV6-адрес в клиентском запросе хоста, поэтому это правило заменяет его общим именем.

Состояние

- пустой

Оценка

- пустой

Действие

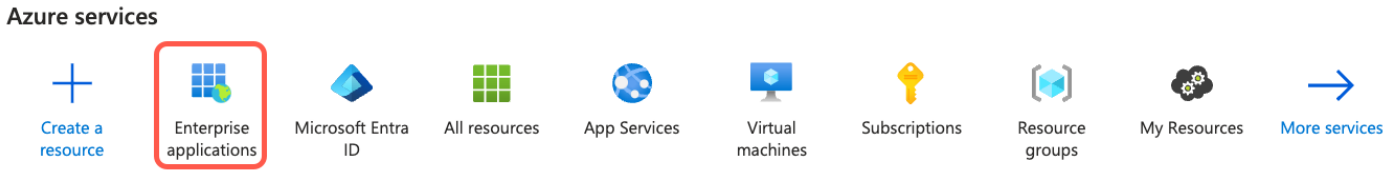
- Действие = Заменить заголовок запроса
- Цель = Хозяин
- Данные =ipv4.host.header

SAML и Entra ID

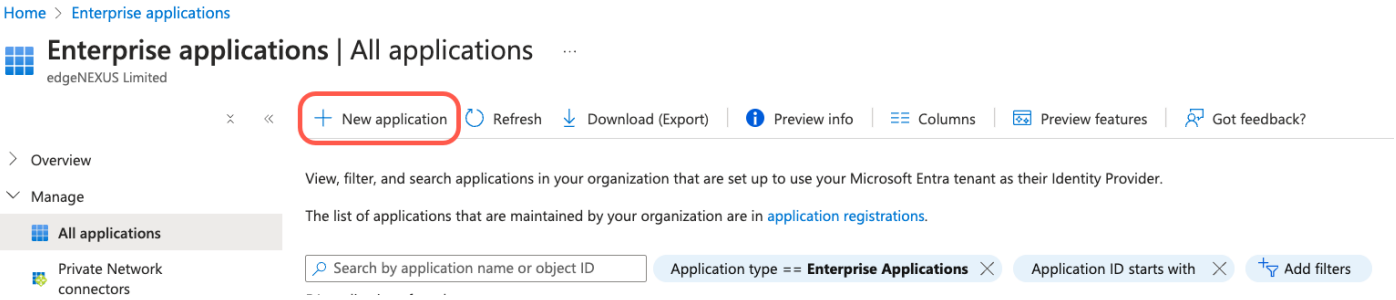
Настройка приложения аутентификации Entra ID в Microsoft Entra

Чтобы аутентификация SAML работала успешно, необходимо настроить корпоративное приложение на портале Microsoft Entra Admin. Это простая задача, которая позволяет создать сертификат подписи, необходимый для запросов и маркеров аутентификации SAML, а также конфигурационные XML-данные.

Для этого сначала нужно войти в Microsoft Entra Portal (https://portal.azure.com) и убедиться, что вы находитесь на странице Azure Services, где в верхней части страницы вы найдете список значков (см. ниже).

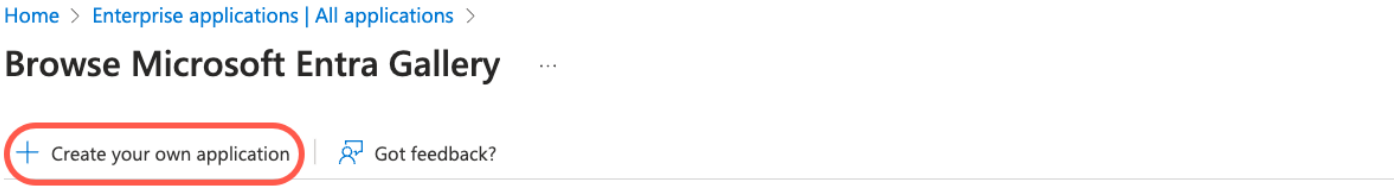


- Щелкните на Приложения для предприятий. Если вы не видите Enterprise Applications в списке значков, вы можете ввести название в строке поиска вверху. Вы увидите страницу, как показано ниже.

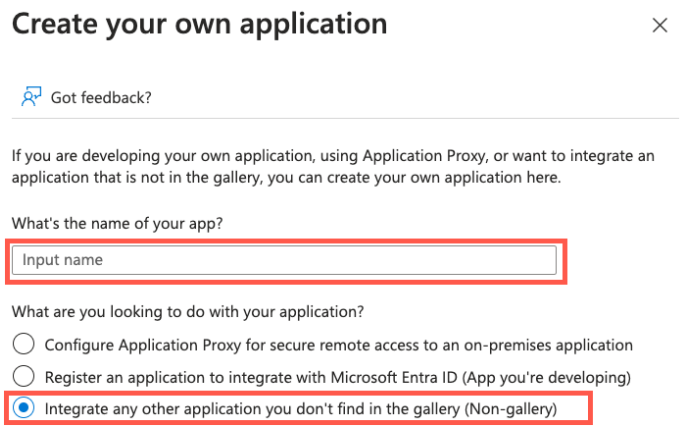


Нажмите на *Новое приложение*

На следующей странице нажмите на кнопку *Создать собственное приложение*.

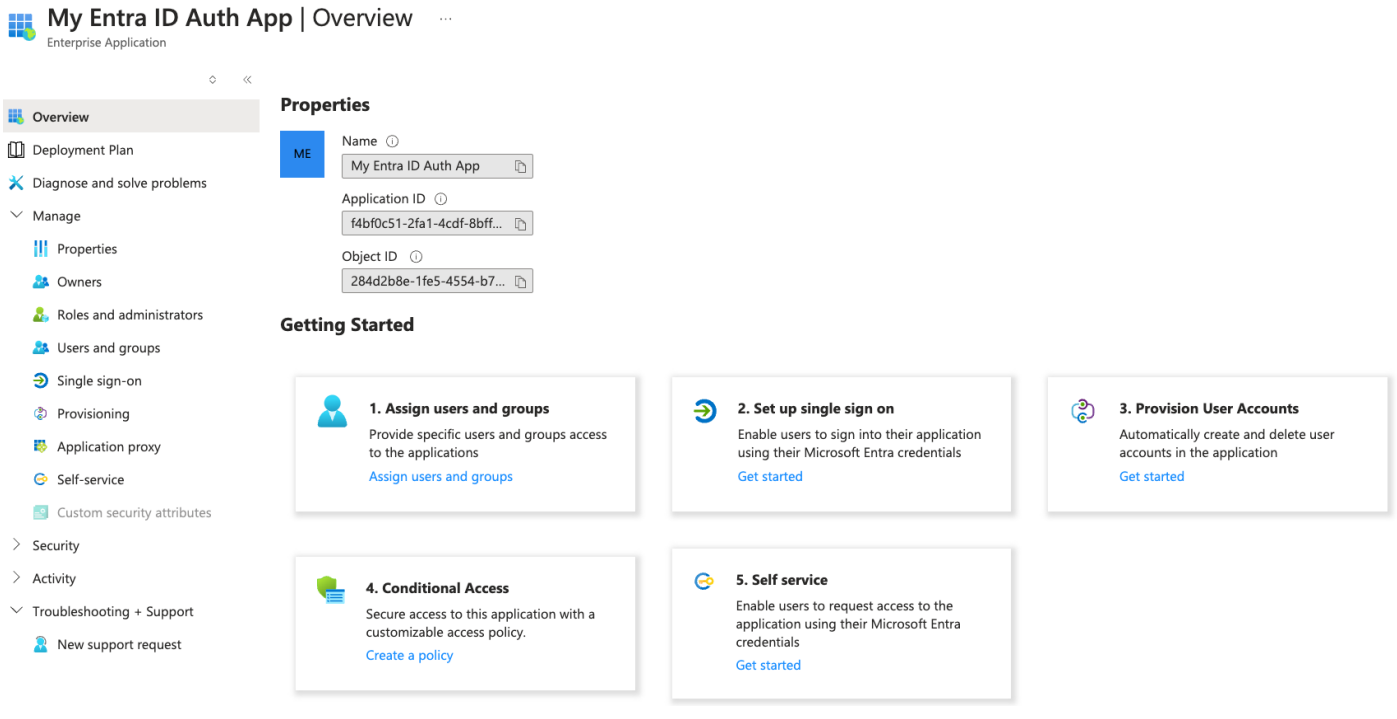


- В правой части страницы откроется раздел "*Создать собственное приложение*".

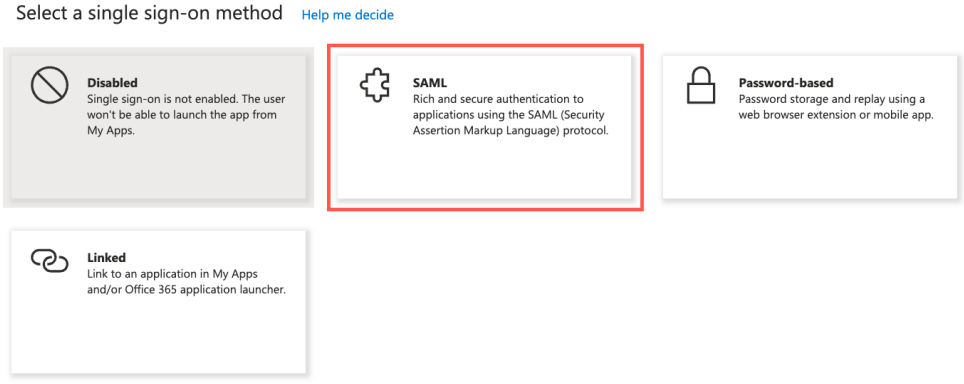


- Укажите название приложения, например, "My Entra ID Auth App". Вы можете выбрать любое имя по своему усмотрению.
- Нажмите на радиокнопку *Интегрировать любое другое приложение, которого нет в галерее (Non-gallery).*
- Нажмите кнопку *Создать*.

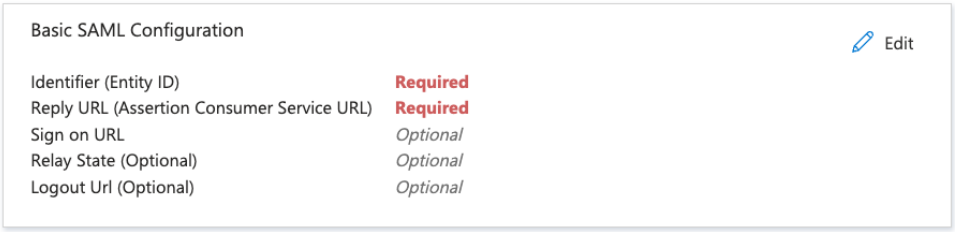
Теперь перед вами откроется страница, похожая на приведенную ниже.



- Нажмите на опцию "Единый вход", расположенную на левой панели навигации.
- Установите флажок SAML



- Теперь вы увидите страницу, содержащую раздел Basic SAML Configuration.



- В области Basic SAML Configuration заполните:
  - Идентификатор (ID субъекта)
  - URL ответа (URL службы потребителей утверждений)
  - URL-адрес для входа в систему
  - URL-адрес выхода из системы (необязательно)
- Сохраните конфигурацию и протестируйте приложение.

Для получения более подробных инструкций вы можете обратиться к документации Enable single sign-on for an enterprise application на сайте Microsoft.

Техническая поддержка

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

Мы предоставляем техническую поддержку, если у вас есть действующий контракт на поддержку и обслуживание EdgeADC, EdgeWAF или EdgeGSLB.

Чтобы отправить заявку в службу поддержки, посетите сайт:

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