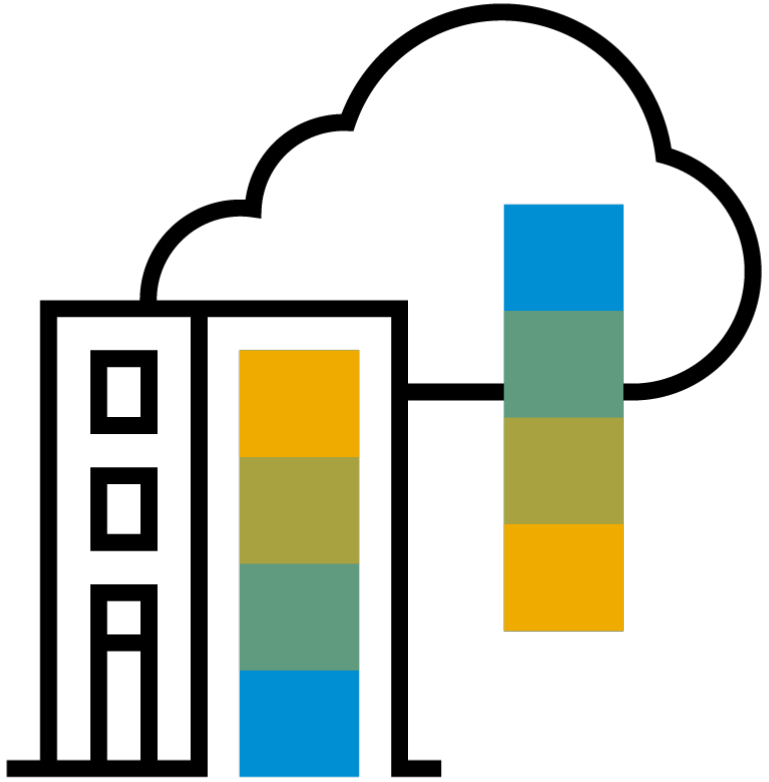
Архитектура, потоки данных и безопасность live-подключения в SAP Analytics Cloud



PUBLIC

THE BEST RUN SAP

Содержание

Что такое live-подключение при использовании SAP Analytics Cloud

Live-подключение на основе технологии CORS

- Потоки данных при работе с live-подключением
- Настройка SAML2
- Хранимые данные в SAP Analytics Cloud
- Другие примеры архитектуры при реализации live-подключения

Безопасность при использовании CORS

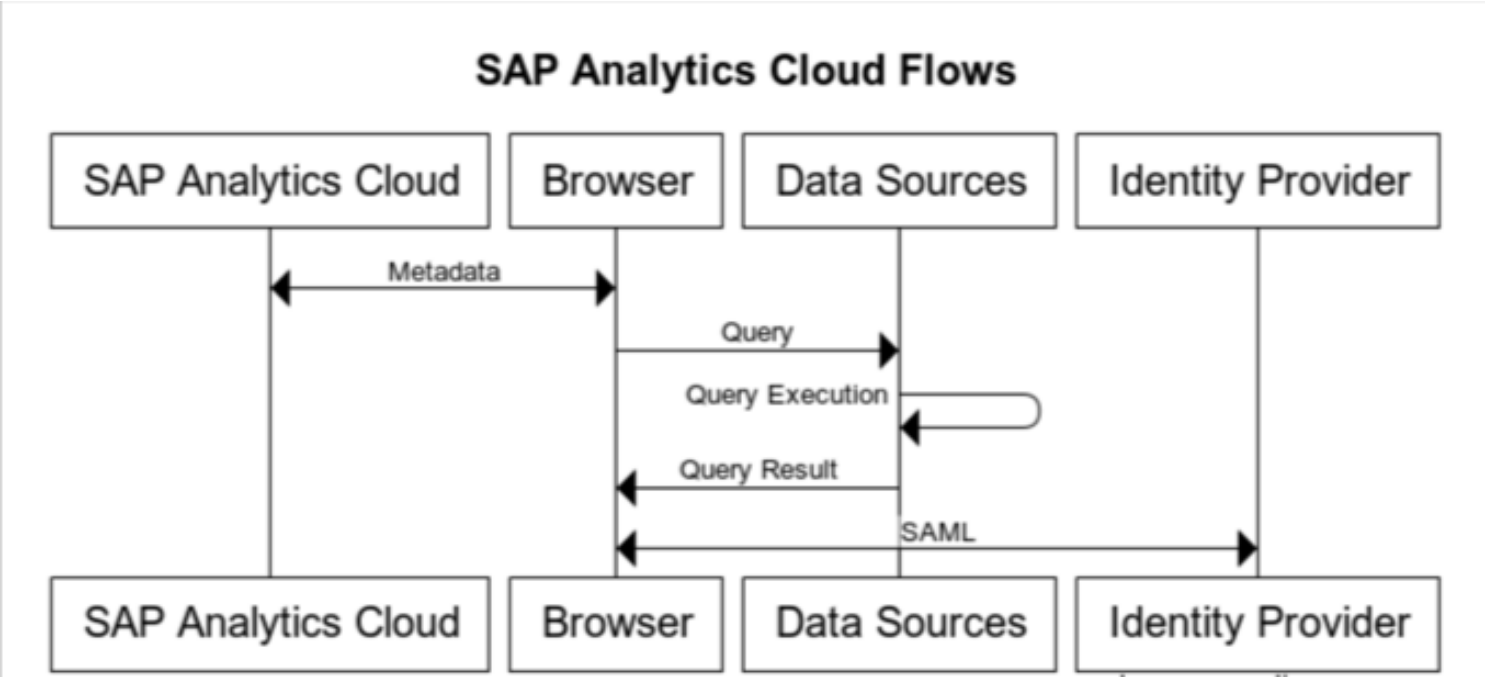
- Сертификаты и протоколы безопасности
- Примеры запросов и ответов CORS
- Прочие рекомендации

Инструкции по настройке CORS

“Live-подключение – это прямое взаимодействие браузера и источника данных”

Взаимодействие браузера с другими серверами

Браузер является центральным компонентом для всех взаимодействий. Запросы создаются браузером через Javascript и выполняются службами запросов в источнике данных следующим образом

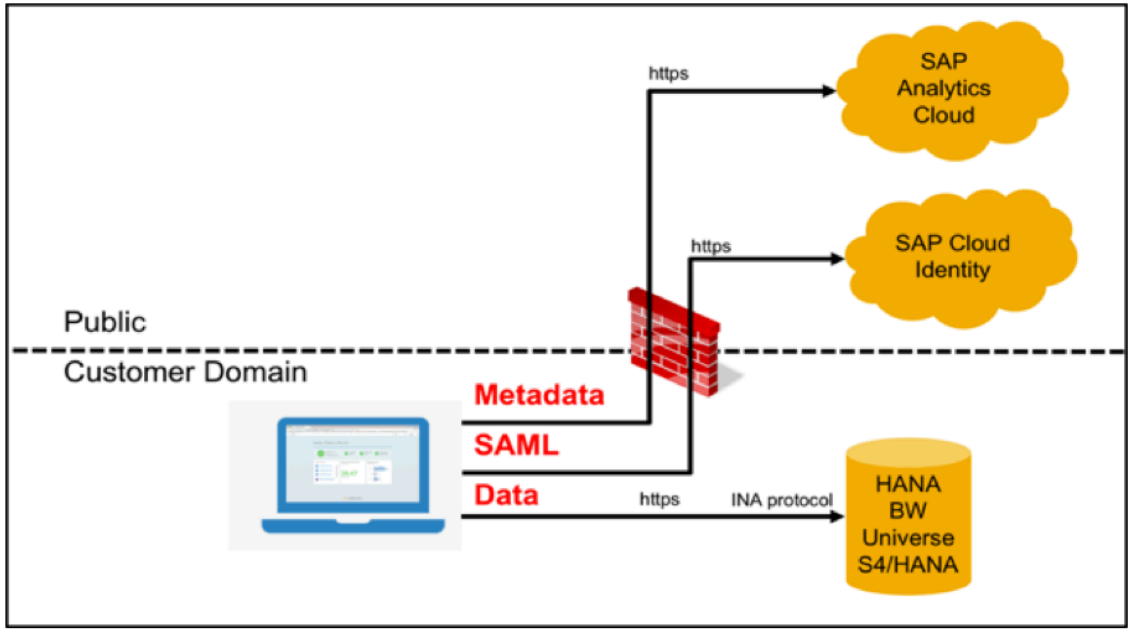


Что такое Live Connection

При использовании Live подключения данные надёжно хранятся в существующем источнике данных, там же выполняются запросы к данным. Результат запроса отправляется обратно в ваш браузер, который отображает вашу отчётность. Браузер взаимодействует напрямую с SAP Analytics Cloud, Identity Provider (доверенный сервер авторизации) и всеми подключёнными источниками данных.

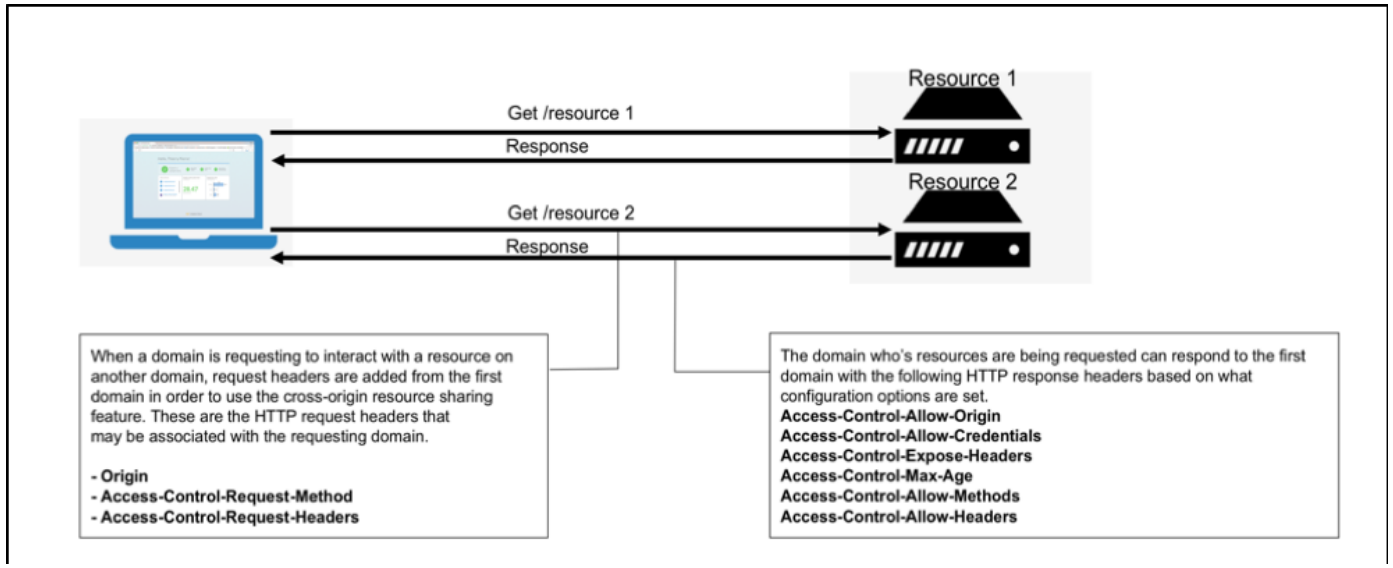
Таким образом, браузер работает с тремя типами соединений:

- Запросы Get / Post из браузера в SAP Analytics Cloud предназначены для метаданных.
- Запросы Get / Post от браузера к серверу авторизации предназначены для SAML 2.
- Запросы Get / Post / Options из браузера в источники данных предназначены для данных.



Live-подключение с использованием CORS

CORS (Cross-origin resource sharing) - это механизм, позволяющий запрашивать ограниченные ресурсы на веб-странице из другого домена за пределами домена, из которого был получен первый ресурс.



В веб-страницу можно свободно встраивать объекты с перекрестным происхождением:

- веб-страницы
- изображения
- таблицы стилей
- скрипты
- iframes
- видео.

Что такое метаданные?

Метаданные, хранимые в SAP Analytics Cloud, полностью зашифрованы.

Они обрабатываются в самом браузере с помощью javascript для целей отображения в отчётах.

Отдельные объекты отчётов хранят необходимую информацию для формирования запроса и построения данного отчёта.

Пример:

ID	Name	Phone Number	Salary
1	Alex Bean	555-324-2342	$80,000
2	Corey Foo	777-234-2318	$100,000

Названия аналитик (но не сами данные в этих колонках) хранятся в SAP analytics Cloud;
Метаданными являются:
“ID”, “Name”, “Phone Number”, “Salary”
Данными являются:
1, Alex Bean, 555-324-2342, $80,000
2, Corey Foo, 777-234-2318, $100,000

Таблица 1. Объекты, хранимые в SAP Analytics Cloud

• Название подключения Браузер использует эту информацию для установления прямого подключения к источникам данных (HANA, BW, S4/HANA, Universe)	Имя соединения, его описание, сервер источника данных и порт, предпочтительный язык. Пользователь и пароль не сохраняются в описании соединения SAC. По этой причине мы рекомендуем использовать SAML2 Single Sign-On с источниками данных, чтобы избежать ввода имени пользователя и пароля при запуске журнала с live-подключением.
• Название модели На основе определения соединения модель определяет запрос к вашему источнику данных на основе метаданных источника данных.	Связь с используемым объектом источника данных (имя BEX-запроса / Calculation View / BOE Universe) • Названия полей (показатели и аналитики) • Свойства показателей: типы, масштабирование, десятичные знаки, типы агрегации, формулы, единицы и валюты, особые агрегации. • Название аналитики/измерения и тип иерархии. • Значения фильтров для запроса источников данных (фильтры страниц и фильтры объектов, например, в графике). Никакие данные или значения измерений из источников данных не хранятся в SAC для live-соединения, кроме выбранных элементов для объектов (фильтров объектов) и фильтров страниц, используемых в запросе, если таковые имеются.
• Название истории: на основе моделей история определяет вашу панель управления.	Связь отдельных моделей, название истории (журнала/дашборда), макет (структура отчёта), форматирование, названия страниц внутри истории, ссылка на используемые RSS-каналы, ссылка на встроенные HTML страницы, изображения для отчётов, правила условного форматирования, связанный анализ (связь нескольких объектов для управления единым поведением), типы диаграмм, положения диаграммы в шаблоне, конкретные параметры диаграммы (цвет и стиль, комментарий , определение дисперсии, определение опорной линии, верхний параметр N, сортировка параметров, все параметры в зависимости от типа диаграммы), значения фильтра, формулы, значения используемых переменных и т.д. Никакие данные или значения измерений из источников данных не хранятся в SAC для live-соединения, кроме значений фильтра, если они есть.

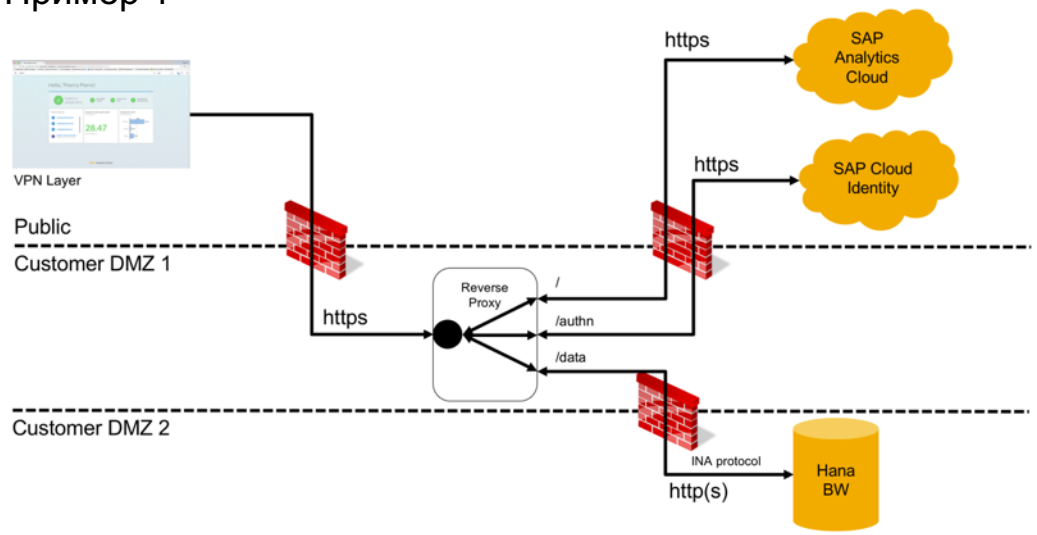
Потоки данных (примеры)

Как упоминалось ранее, данные не отправляются и не хранятся в клиенте SAP Analytics Cloud. Данные остаются в вашем бэк-энде. Данные не реплицируются в SAP Analytics Cloud.

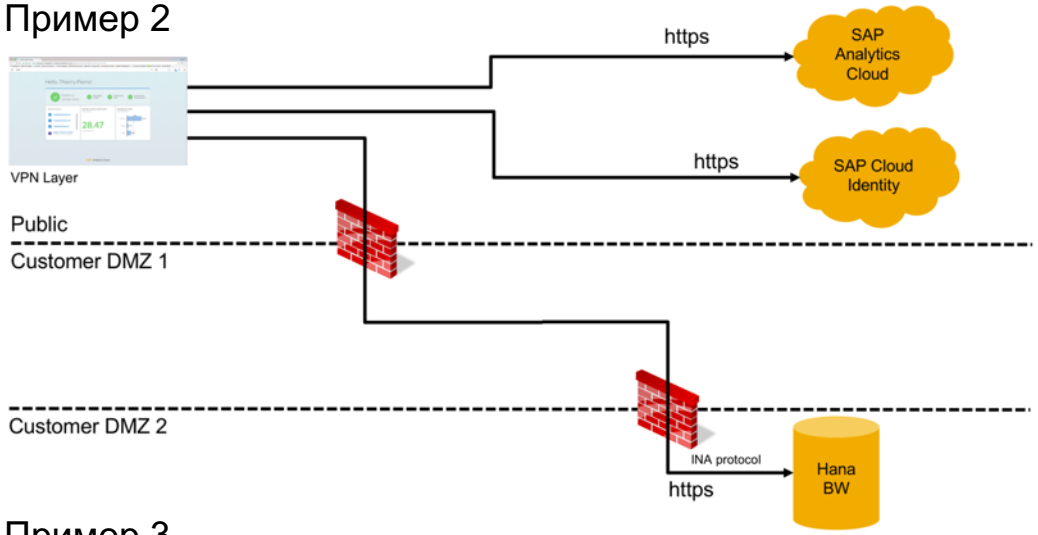
Если браузер осуществляет подключение из-за пределов защищенного домена клиента, поддерживаются стандартные механизмы безопасности (VPN, брандмауэр, балансировщик нагрузки, прокси и т.д.)

Далее приведены некоторые примеры клиентов, которые получают доступ к источнику данных из внешних сетей.

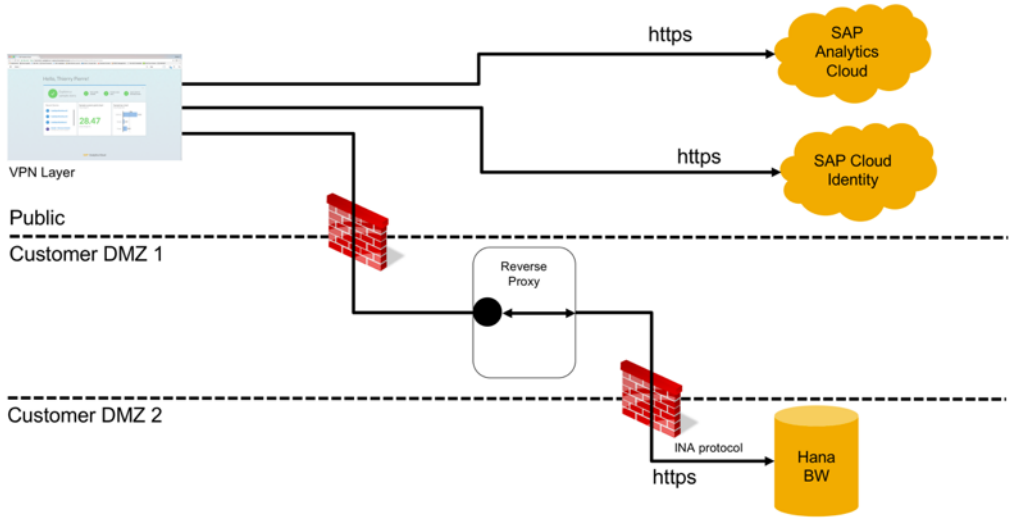
Пример 1



Пример 2



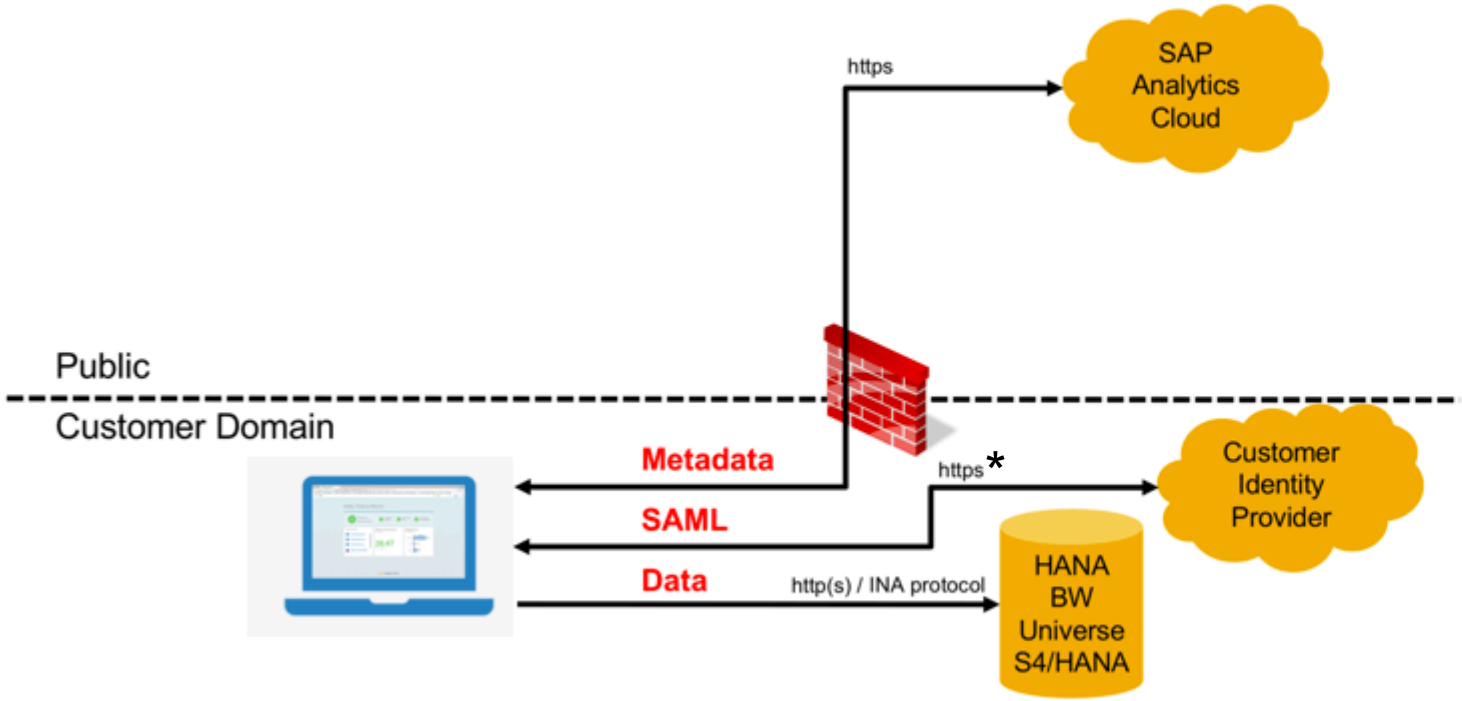
Пример 3



Авторизация по SAML2

По умолчанию для любого сервера SAP Analytics Cloud предоставляется провайдер идентичности на основе SAP Cloud Identity. Это публичный сервис, предоставляемый через общедоступный интернет.

Можно выбрать своего собственного провайдера идентичности в вашем собственном домене. Провайдер идентичности должен поддерживать протокол SAML2 Identity Federation.



* Использование HTTPS с публичным действительным сертификатом SSL является обязательным.

Использование HTTPS и SSL

Целью SSL/TLS является обеспечение конфиденциальности и целостности данных между браузером, SAP Analytics Cloud, Identity Provider и источниками данных. Соединение является частным, поскольку для шифрования передаваемых данных используется симметричная криптография. Ключи для этого симметричного шифрования генерируются уникально для каждого соединения и основаны на «общем секрете», согласованном в начале сессии.

Используя протокол HTTP SSL/TLS, вы предотвращаете компрометацию данных, метаданных или подтверждений SAML, с помощью защищённого туннеля.

Таблица 2. CORS

Взаимодействие между		Протокол	Объект
Браузер	SAP Analytics Cloud	Только https (SSL сертификат поставляется SAP)	Метаданные
Браузер	Источник данных	Только https (SSL сертификат обеспечивает клиент*)	Запрос / Результаты запроса
Браузер	Identity Provider	Только https (SSL сертификат обеспечивает клиент** или SAP***)	Статусы SAML2

* Настоятельно рекомендуется использование сертификата SSL, выпущенного доверенным центром сертификации, для источника данных.

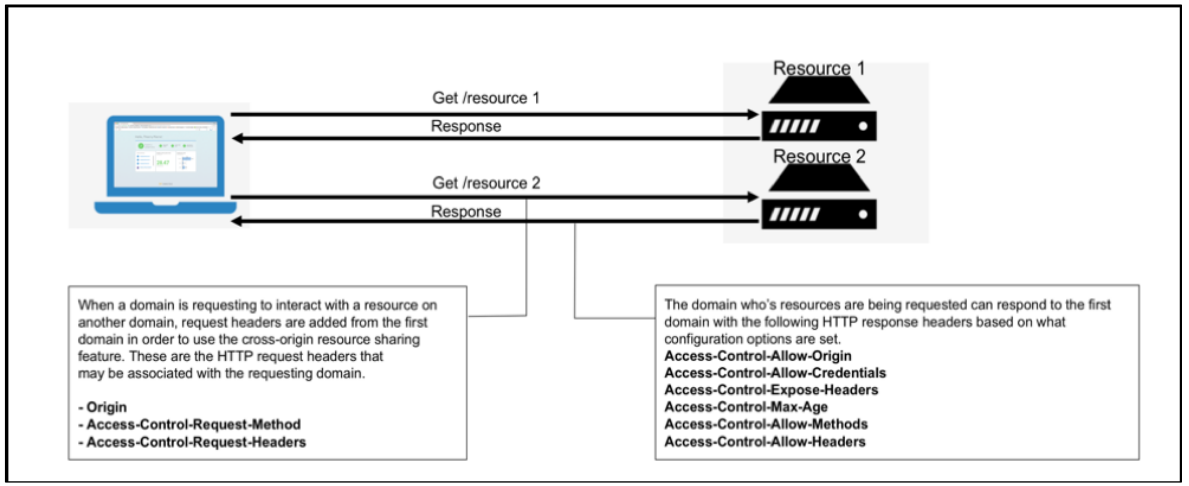
** Настоятельно рекомендуется использование сертификата SSL, выпущенного доверенным центром сертификации, для сервера Identity Provider.

*** При использовании SAP Cloud Identity.

Безопасность при использовании CORS (1 / 3)

Политика «единого происхождения» является важной концепцией в безопасности веб-приложений. Согласно этой политике веб-браузер разрешает сценариям, содержащимся на первой веб-странице, доступ к данным на второй веб-странице, но только в том случае, если обе веб-страницы имеют одинаковое происхождение. Это критический механизм безопасности для изоляции потенциально вредоносных документов.

Если вы хотите безопасно настроить CORS в своём источнике данных (HANA, BW, BOE), вам нужно указать список допустимых ресурсов (Origin), которым разрешено получение данных через CORS (опция Access-Control-Allow-Origin). Это даёт возможность идентифицировать, какой конкретный URI (например, SAP Analytics Cloud) может получить доступ к ресурсам. Затем ваш источник данных будет проверять наличие этого URL в списке.



В целях безопасности не рекомендуется использовать «*» для определения разрешённых URL

Безопасность при использовании CORS (2 / 3)

SAP Analytics Cloud отправляет предварительный запрос, чтобы запросить авторизацию у серверной части для метода **GET** следующим образом.

Request

```
Accept: */*
Accept-Encoding: gzip, deflate, br
Accept-Language: en-GB,en;q=0.9,en-US;q=0.8,fr;q=0.7
Access-Control-Request-Headers: authorization
Access-Control-Request-Method: GET
Connection: keep-alive
Host: hxehost.hxe:4390
Origin: https://mytenant.eu1.sapbusinessobjects.cloud
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_13_3) AppleWebKit/537.36
(KHTML, like Gecko) Chrome/65.0.3325.162 Safari/537.36
```

Если сервер найдет Origin URL в списке авторизованных доменов, ответ будет следующим

Response

```
access-control-allow-credentials: true
access-control-allow-headers: accept, authorization, content-type, x-
csrf-token, x-request-with, x-sap-cid
access-control-allow-methods: GET, HEAD, OPTIONS, POST
access-control-allow-origin:
https://mytenant.eu1.sapbusinessobjects.cloud
access-control-max-age: 3600
content-length: 0
content-type: text/html
vary: Origin
```

В этом примере разрешено запросить методы **GET**, **HEAD**, **OPTIONS** и **POST** из действительного источника в ближайшие 3600 секунд.
Access-Control-Max-Age указывает, что ответ действителен в течение 3600 секунд, после чего должен быть выдан новый запрос. Параметр acc**ess-control-max-age** можно изменить в настройках вашего сервера.

Можно заметить, что источник данных возвращает параметр **x-csrf-token**. Это означает, что источники данных предотвращают **CSRF** (подделка межсайтовых запросов) - тип атаки, когда злоумышленник отправляет вредоносные запросы с веб-сайта, который пользователь посещает, на другой сайт, где аутентифицируется жертва. Предотвращение этой атаки основано на сохранении дополнительного случайного ключа безопасности (токена) во время сеанса пользователя (с cookie) и предоставлении его при каждой операции изменения (**PUT**, **POST**, **DELETE**). Если предоставленный токен неверен, источник данных отвечает кодом возврата **HTTP 403** («Запрещено»).

Безопасность при использовании CORS (3 / 3)

Некоторые рекомендации по внедрению CORS

- Использование HTTPS обязательно с действительным сертификатом, выпущенным авторизованным центром. SAP Analytics Cloud не принимает HTTP для CORS;
- Не используйте подстановочный знак (“*”), когда вы определяете список действительных источников в вашем источнике;
- Избегайте использования нескольких доменов;
- Строго используйте рекомендуемые опции Access-Control-Allow-Headers и Access-Control-Expose-Headers;
- Если вы хотите получить доступ к источникам данных из-за пределов вашего защищённого домена, используйте VPN или любые другие механизмы безопасности.

Инструкции по настройке CORS

Для настройки CORS в SAP HANA, BW, S4/HANA и Universe, обратитесь к документации:

Data Source	Documentation
HANA	https://help.sap.com/doc/00f68c2e08b941f081002fd3691d86a7/release/ru-RU/58c890e1c89d41e69b2cec31bac2d95f.html
BW	https://help.sap.com/doc/00f68c2e08b941f081002fd3691d86a7/release/ru-RU/2f61936f350b423ca6b813da1d5a102f.html
Universe	https://help.sap.com/doc/00f68c2e08b941f081002fd3691d86a7/release/ru-RU/036122ceccb34d85a5f2e542bdf9814a.html
S4/HANA	https://help.sap.com/doc/00f68c2e08b941f081002fd3691d86a7/release/ru-RU/c1cbf644b0a1434fbb4ea072a0562286.html

Thank you.

При подготовке данного материала использованы материалы
https://wiki.scn.sap.com/wiki/display/BOC/SAP+Analytics+Cloud+-+Live+Connection+and+security