Kerberos в Active Directory

osp.ru/winitpro/2010/11/13006806

11.02.2011 Брайан Десмонд

Хотя использование Kerberos порой напоминает черную магию, это одна из ключевых технологий Active Directory (AD). Большинство настроек Kerberos абстрагировано, и взаимодействовать с протоколом приходится нечасто. Тем не менее Kerberos применяется всякий раз, когда пользователь регистрируется на компьютере, присоединенном к AD, а также при доступе к сетевым ресурсам, таким как общие папки и приложения.

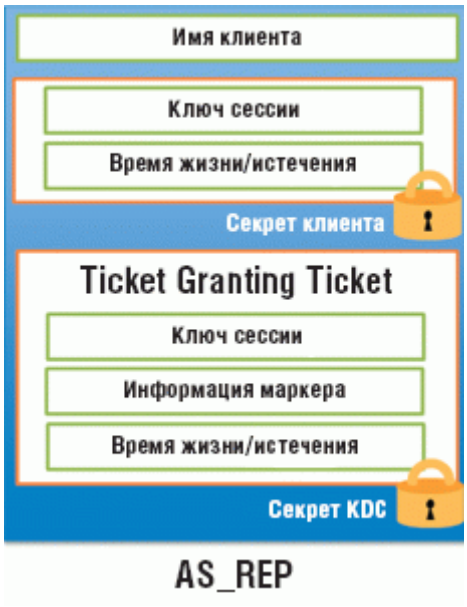
Подробнее

Вместо того чтобы передавать через сеть собственно пароль, Kerberos работает с последовательностью билетов. На высоком уровне это выглядит так: при регистрации пользователя на компьютере формируется серия обменов данными с контроллером домена (DC), и в случае успеха пользователю назначается билет на право получения билетов (TGT). Впоследствии при каждом обращении к службе, такой как общая папка или приложение, TGT используется, чтобы получить билет для доступа к службе или приложению.

Проверка подлинности

Когда компьютер выполняет проверку подлинности при регистрации, в контроллер домена отправляется сообщение AS_REQ или Authentication Service Request. В Kerberos контроллер домена именуется центром распространения ключей Key Distribution Center (KDC). На рисунке 1 показаны важнейшие элементы запроса AS_REQ. Имя клиента представляет собой основное имя пользователя (UPN) или унаследованное имя пользователя (sAMAccountName). Имя службы в этом случае всегда одно и то же, запрос к службе krbtgt в контексте домена или пользователя. Чтобы предотвратить атаки с повторной передачей пакетов, в ходе которой злоумышленник повторно использует сообщение AS_REQ, текущее время шифруется с использованием хеша пароля пользователя. Допустимое расхождение при этом — пять минут. Если зашифрованная отметка времени отличается от текущего времени более чем на пять минут, то запрос отвергается.

Когда KDC получает сообщение AS_REQ, в первую очередь предпринимается попытка расшифровать отметку времени с использованием локальной копии хеша пароля пользователя. Если попытка заканчивается неудачей, клиент получает сообщение об ошибке, и обработка запроса прекращается. Если дешифрация проходит удачно, а значение отметки времени находится в приемлемых пределах, KDC выдает пользователю сообщение AS_REP (Authentication Service Reply) от службы проверки подлинности со встроенным билетом TGT. На рисунке 2 показано содержимое сообщения AS_REP. На данном этапе компьютер пользователя сохраняет в кэше билет TGT и сеансовый ключ на время существования TGT и удаляет пароль пользователя. По умолчанию время существования билетов TGT, сформированных центрами KDC AD, истекает через десять часов.



AS_REP

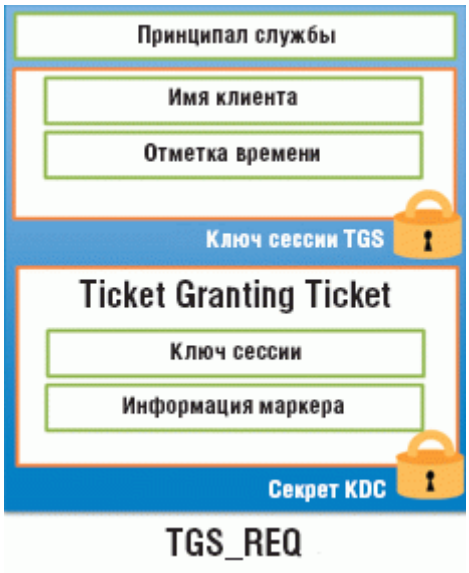
В AD для Kerberos требуется зашифрованная отметка времени в сообщении AS_REQ. Первоначальный обмен известен как предварительная проверка подлинности. В Kerberos в стандартном виде не обязательно шифровать отметки времени; вполне достаточно сообщения AS_REQ, содержащего имя клиента и имя службы. Недостаток такого подхода заключается в уязвимости для атаки методом перебора по словарю, так как каждый запрос, содержащий уникальное имя клиента, будет возвращать ошибку, указывающую, что клиент не обнаружен, или выдаст действительный TGT данному пользователю.

Как показано на рисунке 2, сообщение AS_REP содержит два блока зашифрованных данных. Первый шифруется с применением хеша пароля пользователя и содержит сеансовый ключ и отметку времени окончания существования билета. Сеансовый ключ используется для шифрования будущих соединений с центром KDC. Второй компонент, билет TGT, шифруется с помощью секрета KDC. Секрет KDC в реализации Kerberos в AD хранится как пароль учетной записи пользователя krbtgt, существующей в каждом домене AD. Учетная запись krbtgt создается, когда назначается первый DC в домене; этой учетной записи принадлежит решающая роль в функционировании домена.

Получение билета службы

В Kerberos любой объект, к которому требуется получить доступ, называется службой. К службам относятся серверы файлов и печати, серверы базы данных и внутренние веб-приложения. Для доступа к службе пользователь предоставляет билет службы. Первый шаг — определить имя участника службы service principal name (SPN), к которой нужно получить доступ. Задача формирования SPN возлагается на компьютер или приложение пользователя.

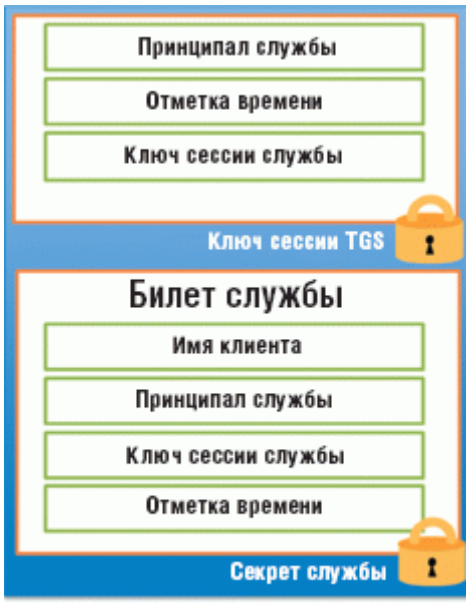
В случае с сервером файлов с именем srv01.contoso.com, SPN службы файлов будет cifs/srv01.contoso.com. Аналогично для веб-приложения на сайте web01.contoso.com имя SPN может быть http/web01.contoso.com. Типичная проблема, с которой сталкиваются администраторы AD, — дублирование имен SPN, при котором более одного пользователя или компьютера в каталоге имеют одно и то же имя SPN, зарегистрированное в атрибуте servicePrincipalName. В этом случае центру KDC неизвестно, как отвечать на запрос билета службы, так как существует несколько служб с одним именем.



TGS_REQ

Если взглянуть на атрибут servicePrincipalName в AD, можно заметить, что ни одно из двух упомянутых образцовых имен SPN не определено ни в одной учетной записи компьютера в AD. Чтобы уменьшить количество дублированных данных, сохраненных в каталоге, AD обеспечивает сопоставление на уровне леса стандартных имен SPN для каждой учетной записи компьютеров в каталоге. Буквально десятки встроенных имен SPN применяются к каждому компьютеру, определенному в атрибуте. Данные хранятся в атрибуте spnMappings объекта Directory Service в разделе Configuration (=Directory Service, CN=Windows NT, CN=Services, CN=Configuration); этот атрибут сопоставляет службу HOST объекта со множеством других служб, среди которых службы CIFS и HTTP. Если нужно определить конкретную службу для каждой системы в лесу, не составляет труда изменить этот атрибут, чтобы добавить службу к списку заранее определенных служб.

На рисунке 3 показано содержимое сообщения TGS_REQ (Ticket Granting Service Request), которое KDC получает от клиента, если тот пытается обратиться к службе. Первый фрагмент информации — имя SPN службы, для которой клиент запрашивает билет. Имя клиента и отметка времени зашифрованы с помощью сеансового ключа, полученного клиентом в переданном ранее сообщении AS_REP. Эта информация повторно используется для предотвращения атак, в ходе которых злоумышленник повторно задействует сообщение запроса. Также прилагается экземпляр билета TGT, ранее полученного клиентом.



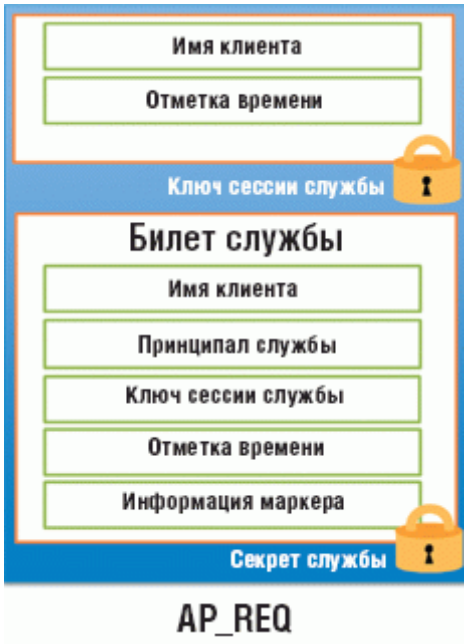
TGS_REP

Если KDC получает сообщение TGS_REQ и указан один элемент для SPN, отметка времени находится в допустимом диапазоне и билет TGT действителен (не просрочен), то клиенту предоставляется билет службы как часть сообщения TGS_REP (рисунок 4). Сообщение TGS_REP содержит все данные, необходимые клиенту для доступа к службе.

С помощью секрета службы (например, пароля учетной записи компьютера или учетной записи службы) шифруется билет службы, который клиент кэширует и использует всегда, когда необходим доступ к службе. Так же как у билетов TGT, время, в течение которого разрешено повторно использовать билеты службы, ограничено (десять часов по умолчанию в реализации Kerberos в AD). Имея билет службы, клиент может запросить доступ к ней.

Доступ к службам

После того как клиент получает билет службы, приложение, обращающееся к службе, может предъявить этот билет службе и запросить доступ. Механика предъявления билета службы не так стандартизована, как получение билета, из-за различий, свойственных приложениям. В случае со службой HTTP билет службы встраивается в заголовки запроса HTTP.



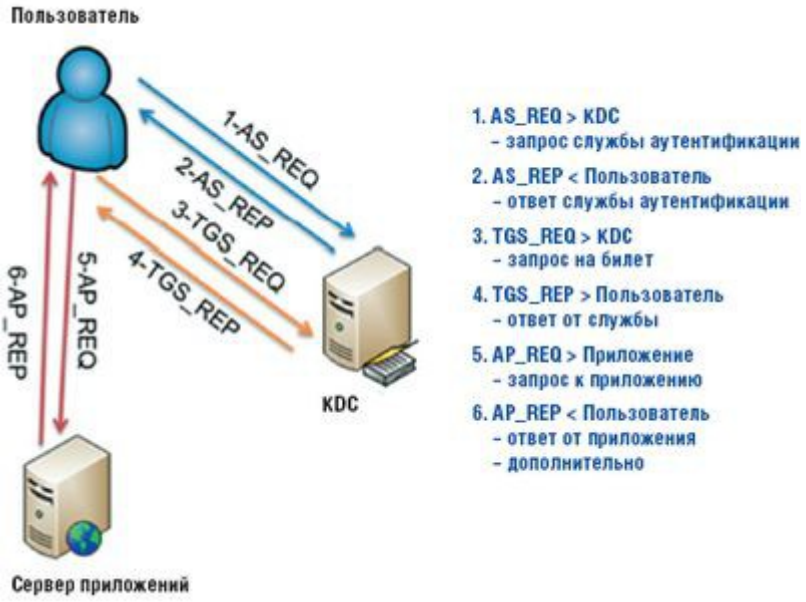
Билет службы предъявляется приложению в форме сообщения AP_REQ Kerberos, как показано на рисунке 5. Служба дешифрует билет службы и получает сеансовый ключ, который можно использовать для дешифрации полей отметки времени и имени клиента, которые в свою очередь используются для проверки подлинности билета службы. Даже если служба принимает билет службы, на данном этапе клиент просто прошел проверку в службе. Выполнить задачу авторизации службе предстоит на основе информации о клиенте.

В билет службы также обычно входят данные, известные как сертификат атрибута привилегий Privilege Attribute Certificate (PAC). На рисунке 5 сертификат PAC именуется информацией маркера Token Information. Это та же информация маркера, которую KDC включает в билет TGT пользователя (рисунок 2). Сертификат PAC составлен из такой информации, как идентификатор безопасности (SID) пользователя, сведения о членстве в группе и правах безопасности/привилегиях пользователя. Когда пользователь предъявляет билет TGT в центр KDC, чтобы запросить билет службы, KDC копирует информацию маркера из TGT и вставляет в поле PAC билета службы. Служба использует эту информацию, чтобы подготовить маркер доступа для пользователя и проверить авторизацию пользователя, обычно на основе членства в группе.

Допускается передача дополнительного сообщения Kerberos, известного как AP_REP или Application Reply, после того как пользователь предъявляет билет службы в сообщении AP_REQ, показанном на рисунке 5. Сообщение Application Reply — необязательное; как правило, приложение не отправляет такое сообщение, если не происходит ошибки. Пример ситуации, когда формируется сообщение AP_REP: клиент запрашивает (в сообщении AP_REQ) у службы подтверждение подлинности через процесс, известный как обоюдная проверка подлинности.

Обзор процесса

На рисунке 6 показана схема потока сообщений, когда пользователь решает обратиться к службе на сервере приложений. Пользователь регистрируется на своей рабочей станции, которая выдает последовательность сообщений AS_REQ и AS_REP в центр KDC, откуда пользователь получает билет TGT, если учетные данные верны. Затем TGT пользователя кэшируется в памяти, и каждый раз, когда пользователю нужно получить доступ к службе (например, к серверу файлов, серверу печати, веб-приложению), пользователь предъявляет TGT центру KDC и запрашивает билет службы для службы. Пользователь получает билет службы и предъявляет его приложению, чтобы запросить доступ.



Если используются контроллеры домена только для чтения (RODC), поток сообщений немного отличается от показанного на рисунке 6, в зависимости от политик репликации паролей и места кэширования паролей. Следует иметь в виду, что центру KDC требуется доступ к секретам службы и пользователя или компьютера, чтобы издавать билеты службы или билеты TGT соответственно. По умолчанию RODC не кэширует пароли, поэтому у него нет доступа к необходимым секретам.

Если RODC получает запрос для TGT или билета службы, который контроллер не может выполнить (из-за некэшированного пароля), запрос передается доступному для записи контроллеру домена, обладающему необходимыми секретами для

шифрования ответа. Доступный для записи DC отправляет ответ в RODC, который в свою очередь передает его клиенту. Если RODC располагает кэшированным паролем для пользователя или службы, к которой пользователь хочет получить доступ, то RODC просто выдает билет TGT и/или службы таким же способом, как показано на рисунке 6.

Если вернуться к рисунку 2, можно увидеть, что билет TGT пользователя зашифрован с помощью секрета KDC. Этот секрет — пароль для учетной записи krbtgt, которая имеется во всех доменах AD. Учитывая положения, заложенные в основу RODC (то есть его уязвимость по умолчанию), было бы потенциально опасно хранить в RODC пароль доменной учетной записи krbtgt. Если RODC будет скомпрометирован, взломщик сможет самостоятельно издавать билеты TGT. В целях снижения риска каждый RODC располагает собственной учетной записью krbtgt и никогда не осведомлен о паролях учетных записей домена или другого RODC. Доступные для записи контроллеры домена имеют доступ к паролям всех учетных записей krbtgt, поэтому они могут расшифровать билеты TGT, изданные любым RODC в домене.

Прозрачная проверка подлинности

Kerberos почти прозрачен для администраторов AD. В отличие от многих схем проверки подлинности, в Kerberos никогда не требуется передавать пароли через сеть, как и нет необходимости хранить пароль пользователя в памяти после начального процесса регистрации. Благодаря этим преимуществам существенно снижается уязвимость, свойственная другим протоколам проверки подлинности.

Брайан Десмонд (brian@briandesmond.com) — старший консультант компании Moran Technology Consulting (Чикаго). Имеет сертификат Directory Services MVP. Автор книги «Active Directory», ведет блог www.briandesmond.com