jwt续签为什么要使用双token(accesstoken,refreshtoken)

作者：微信公众号：【架构师老卢】 10-26 16:2 28

概述：使用Refresh Token和Access Token来进行JWT续签是一种安全和灵活的方法，旨在提高系统的安全性并降低一些潜在风险。这种模式通常被用于更复杂的身份验证和授权方案中，例如OAuth 2.0。以下是详细解释Refresh Token和Access Token的作用和目的： **Access Token（访问令牌）：** **作用和目的**：Access Token是用于访问受保护资源的令牌。它包含了用户的身份信息和权限信息，并用于验证用户是否有权访问某些资源。Access Token通常具有短暂的有效期，以减小被滥用的风险。 **短暂性**：Access Token通常只有较短的有效期（例如，15分钟），这是为了减小在Access Token被窃取或滥用时造成的风险。 **轻量级**：Access Token的大小通常较小，以便在每个请求中传递，而不会增加显著的网络开销。 **Refresh Token（刷新令牌）：** **作用和目的**：Refresh Token是用于刷新Access Token的特殊令牌。它通常具有更长的有效期，用于续签Access Token，而不需要用户重新登录。 **长期有效**：Refresh Token通常比Access Token具有更长的有效期（例如，30天），因为它通常只用于请求新的Access Token。 **敏感性**：Refresh Token通常比Access Token更敏感，因为它可以用来获取新的Access Token。因此，它需要在存储和传输过程中进行额外的安全保护。 **使用Refresh Token和Access Token的流程**： 用户登录成功后，服务器颁发一个Access Token和一个Refresh Token。 用户使用Access Token来访问受保护的资源，直到Access Token过期。 当Access Token过期时，用户可以使用Refresh Token来请求一个新的Access Token，而不需要重新登录。 Refresh Token只能用一次来获取新的Access Token，这提供了额外的安全性。 如果Refresh Token过期或被滥用，用户需要重新登录以获取新的Refresh Token。 **优势和目的**： **安全性**：Refresh Token通常具有更长的有效期，但是在获取新的Access Token时需要一定的安全验证。这提供了更好的安全性，因为Access Token的泄漏风险较小。 **用户体验**：使用Refresh Token可以实现无感知的续签，提高了用户体验，因为用户不需要频繁地重新登录。 **灵活性**：Refresh Token模式适用于一些特殊场景，如OAuth 2.0授权服务器，允许客户端持续访问资源，同时保持安全性。 使用Refresh Token和Access Token的模式可以提高应用程序的安全性，同时提供更好的用户体验，尤其是在需要长时间授权或需要频繁续签Access Token时。然而，这种模式也需要额外的安全措施，以确保Refresh Token的安全性。

风险。 **短暂性**：Access Token通常只

使用Refresh Token和Access Token来进行JWT续签是一种安全和灵活的方法，旨在提高系统的安全性并降低一些潜在风险。这种模式通常被用于更复杂的身份验证和授权方案中，例如OAuth 2.0。以下是详细解释Refresh Token和Access Token的作用和目的：

Access Token（访问令牌）：

作用和目的：Access Token是用于访问受保护资源的令牌。它包含了用户的身份信息和权限信息，并用于验证用户是否有权访问某些资源。Access Token通常具有短暂的有效期，以减小被滥用的风险。

短暂性：Access Token通常只有较短的有效期（例如，15分钟），这是为了减小在Access Token被窃取或滥用时造成的风险。

轻量级：Access Token的大小通常较小，以便在每个请求中传递，而不会增加显著的网络开销。

Refresh Token（刷新令牌）：

作用和目的：Refresh Token是用于刷新Access Token的特殊令牌。它通常具有更长的有效期，用于续签Access Token，而不需要用户重新登录。

长期有效：Refresh Token通常比Access Token具有更长的有效期（例如，30天），因为它通常只用于请求新的Access Token。

敏感性：Refresh Token通常比Access Token更敏感，因为它可以用来获取新的Access Token。因此，它需要在存储和传输过程中进行额外的安全保护。

使用Refresh Token和Access Token的流程：

用户登录成功后，服务器颁发一个Access Token和一个Refresh Token。

用户使用Access Token来访问受保护的资源，直到Access Token过期。

当Access Token过期时，用户可以使用Refresh Token来请求一个新的Access Token，而不需要重新登录。

Refresh Token只能用一次来获取新的Access Token，这提供了额外的安全性。

如果Refresh Token过期或被滥用，用户需要重新登录以获取新的Refresh Token。

优势和目的：

安全性：Refresh Token通常具有更长的有效期，但是在获取新的Access Token时需要一定的安全验证。这提供了更好的安全性，因为Access Token的泄漏风险较小。

用户体验：使用Refresh Token可以实现无感知的续签，提高了用户体验，因为用户不需要频繁地重新登录。

灵活性：Refresh Token模式适用于一些特殊场景，如OAuth 2.0授权服务器，允许客户端持续访问资源，同时保持安全性。

使用Refresh Token和Access Token的模式可以提高应用程序的安全性，同时提供更好的用户体验，尤其是在需要长时间授权或需要频繁续签Access Token时。然而，这种模式也需要额外的安全措施，以确保Refresh Token的安全性。