

NTLM과 LDAP 인증의 차이점은 무엇입니까?

목차

- [질문](#)
- [환경](#)
- [클라이언트 경험](#)
- [기본](#)
- [NTLM\(SSP\)](#)
- [보안](#)
- [기본](#)
- [NTLM\(SSP\)](#)

질문

NTLM과 LDAP 인증의 차이점은 무엇입니까?

환경

Cisco WSA(Web Security Appliance), 모든 버전의 AsyncOS

WSA와의 인증은 다음과 같은 가능성을 통해 분류할 수 있습니다.

클라이언트 > WSA	WSA > 인증 서 버	인증 서버 유형
기본 인증	LDAP 인증	LDAP 서버
기본 인증	LDAP 인증	LDAP를 사용하는 Active Directory 서 버
기본 인증	NTLM 기본 인증	Active Directory 서버(NTLM Basic)
NTLM 인증	NTLMSSP 인증	Active Directory 서버(NTLMSSP)

참고:NTLMSSP는 일반적으로 NTLM이라고 합니다.

기본 인증과 NTLM 인증의 중요한 차이점은 다음과 같습니다.

클라이언트 경험

기본

클라이언트는 항상 자격 증명을 묻는 메시지가 표시됩니다.자격 증명을 입력한 후에는 일반적으로

브라우저에서 제공된 자격 증명을 기억하기 위한 확인란을 제공합니다.브라우저가 닫힐 때마다 클라이언트가 다시 프롬프트를 표시하거나 이전에 기억된 자격 증명을 다시 보냅니다.

참고:NTLM Basic은 클라이언트의 기본 인증을 사용하므로 동일한 속성을 갖습니다.

NTLM(SSP)

- 클라이언트는 Windows 로그인 자격 증명을 사용하여 투명하게 인증합니다.
- 클라이언트가 자격 증명을 요청하는 유일한 경우는 Windows 자격 증명에 처음 실패할 경우(클라이언트가 인증에 사용된 도메인이 아니라 컴퓨터에 로컬로 로그인된 경우 이 경우) 또는 클라이언트가 WSA를 신뢰하지 않는 경우입니다.

보안

기본

자격 증명은 일반 텍스트를 사용하여 비보안 상태로 전송됩니다.클라이언트와 WSA 간의 간단한 패킷 캡처는 사용자의 사용자 이름과 비밀번호를 표시합니다.

NTLM(SSP)

자격 증명은 3방향 핸드셰이크(다이제스트 스타일 인증)를 통해 안전하게 전송됩니다. 비밀번호는 전선에서 전송되지 않습니다.

NTLM 프로세스는 다음과 같이 표시됩니다.

1. 클라이언트가 NTLM 협상 패킷을 전송합니다.이는 클라이언트가 NTLM 인증을 수행할 것임을 WSA에 알려줍니다.
2. WSA는 클라이언트에 NTLM Challenge 문자열을 전송합니다.
3. 클라이언트는 비밀번호를 기반으로 알고리즘을 사용하여 문제를 수정하고 챌린지 응답을 WSA에 전송합니다.
4. 그런 다음 AD 서버는 챌린지 문자열을 적절하게 수정했는지 여부에 따라 클라이언트가 올바른 비밀번호를 사용하고 있는지 확인합니다.