상담원 문제 해결 도구를 사용하여 Windows 상담원 문제 해결

목차

소개

이 문서에서는 기본 제공 에이전트 문제 해결 도구 PowerShell 스크립트를 사용하여 일반적인 Windows 에이전트 문제를 해결하는 방법에 대해 설명합니다.

사전 요구 사항

요구 사항

이 문서에 대한 특정 요건이 없습니다.

사용되는 구성 요소

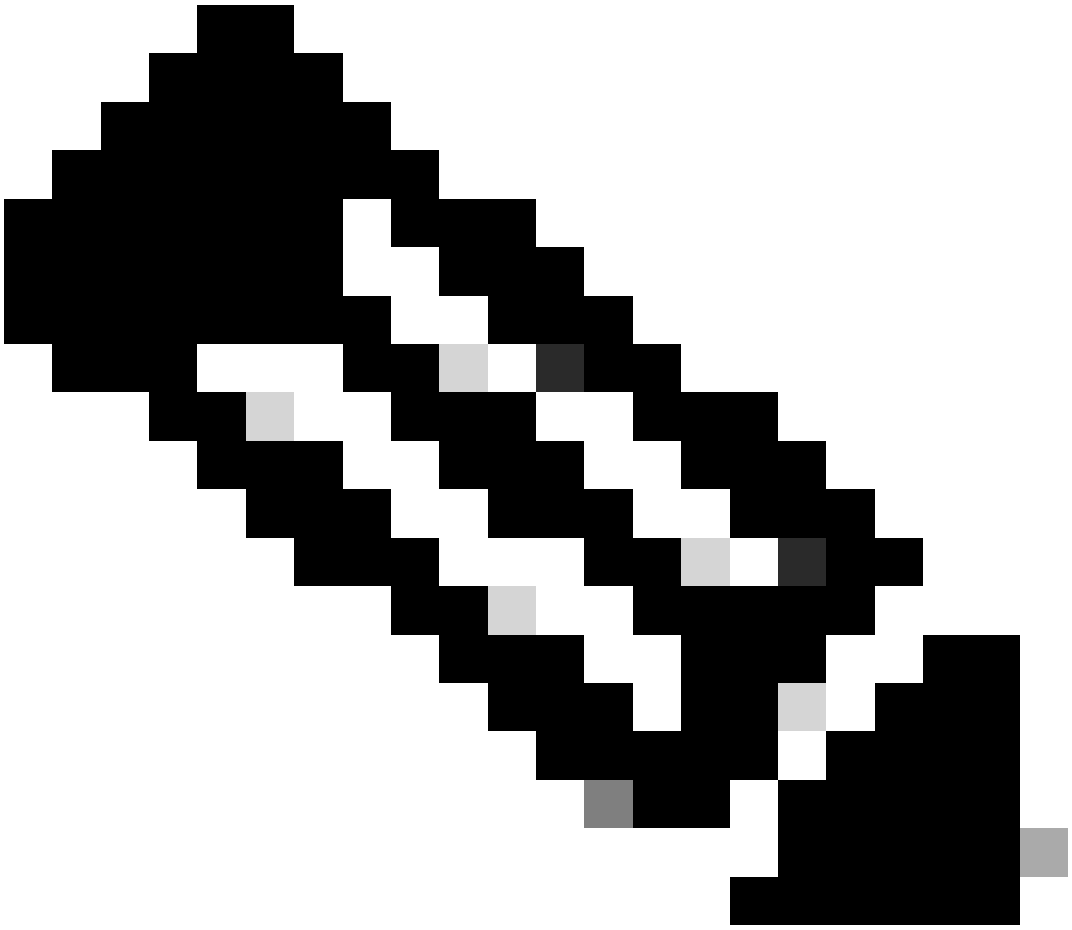
이 문서의 정보는 다음 소프트웨어 및 하드웨어 버전을 기반으로 합니다.

- PowerShell 버전 4.0

이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다. 이 문서에 사용된 모든 디바이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다. 현재 네트워크가 작동 중인 경우 모든 명령의 잠재적인 영향을 미리 숙지하시기 바랍니다.

배경 정보

상담원 문제 해결 도구 스크립트에는 상담원의 전반적인 상태, 상담원 등록과 관련된 알려진 문제, 상담원 업그레이드와 관련된 알려진 문제를 확인하고 전체 적용 상태를 확인하며 추가 분석을 위해 로그를 수집할 수 있는 몇 가지 옵션이 있습니다.



> 참고: 상담원 문제 해결 도구는 버전 3.9부터 상담원과 함께 패키지로 제공됩니다. 3.9 이전 버전의 경우 기본적으로 포함되지 않습니다. 3.9 이전 버전을 사용하는 경우 3.9 에이전트가 설치된 Windows 시스템에서 스크립트를 복사하여 (C:\Program Files\Cisco Tetration)에 붙여 넣어 문제 해결 도구를 사용할 수 있습니다.

스크립트 실행 단계

상담원 문제 해결 도구 스크립트를 실행하려면 다음 단계를 수행하십시오.

1. 관리자로 PowerShell을 엽니다.

2. CSW 설치 디렉토리로 이동합니다(기본 위치: C:\ Program Files \Cisco Tetration)을 참조하십시오.

3. 다음 명령을 사용하여 스크립트를 실행합니다.

.\AgentTroubleshootTool.psl

이 에이전트 문제 해결 도구 스크립트에서 사용할 수 있는 매개 변수 목록

상담원 문제 해결 도구에는 상담원의 여러 가지 문제를 해결할 수 있는 몇 가지 옵션이 있습니다. 사용 가능한 옵션은 다음과 같습니다.

-agentHealth: 에이전트 상태 보고서 실행
-agent등록: 에이전트 등록에서 문제 확인
-agentUpgrade: 에이전트 업그레이드에 문제가 있는지 확인
-시행상태: 시행 관련 문제 확인
-collectLogs: 디버깅을 위해 로그 수집
-collectDebugLogs: loglevel:5가 활성화된 로그를 수집합니다. 여기에는 -collectLogs 매개 변수를 사용하여 수집한 로그도 포함됩니다
모두: -collectDebugLogs를 제외한 모든 매개 변수 실행

이러한 옵션을 사용하려면 적절한 매개 변수를 사용하여 스크립트를 실행하면 됩니다.
예를 들어 에이전트의 상태를 확인하려면 -agentHealth 매개 변수를 사용하여 스크립트를 실행합니다.

.\AgentTroubleshootingTool.ps1 -agentHealth

매개 변수 세부 정보 -agentHealth

-agentHealth 매개 변수에서 다음 항목을 확인합니다.

1. 서비스 TetSensor 및 TetEnforcer가 실행 중입니다.
2. 센서 ID가 유효함
3. PATH 변수에 'C:\ Windows\System32'이 포함됨
4. 상담원이 ETW 또는 NPCAP를 사용 중입니다. OS가 2008R2이면 NPCAP Health를 확인하는 것입니다.

컬렉터/EFE 및 WSS와의 백엔드 연결이 좋습니다.

다음은 -agentHealth를 사용하여 스크립트를 실행할 때의 스크립트 출력 예입니다 매개변수

.\AgentTroubleshootingTool.ps1 -agentHealth

```
PS C:\Program Files\Cisco Tetration> .\AgentTroubleshootingTool.ps1 -agentHealth
***Running Checks for Agent Health at 08/07/2023 13:55:01***
Service status is Good!
Sensor ID is Valid
PATH variable contains 'C:\Windows\System32'
Agent is using ETW for packet capture.
Backend connectivity to Collectors/EFE's and WSS is Good
!!!Agent Health is Good!!!
```

매개 변수 세부 정보 -agentRegistration

-agentRegistration 매개 변수 아래에서 다음 항목을 확인합니다.

1. -agentHealth 매개 변수를 사용하여 수집된 보고서를 포함합니다.
2. 등록 오류는 오류 코드(예: 401/403 등)를 기반으로 합니다.

에이전트를 실수로 UI에서 삭제한 경우 클러스터에 다시 등록하는 옵션도 있습니다.

다음은 -agentRegistration을 사용하여 스크립트를 실행할 때 표시되는 스크립트 출력의 예입니다 매개변수.

.\AgentTroubleshootingTool.ps1 -agentRegistration

```
PS C:\Program Files\Cisco Tetration> .\AgentTroubleshootingTool.ps1 -agentRegistration
***Checking For Agent Registration Issues at 08/07/2023 14:02:47***
Service status is Good!
Sensor ID is Valid
PATH variable contains 'C:\Windows\System32'
Agent is using ETW for packet capture.
Backend connectivity to Collectors/EFE's and WSS is Good
!!!Agent Health is Good!!!
!!!No issues found with Agent Registration!!!
```

매개 변수 세부 정보 -agentUpgrade

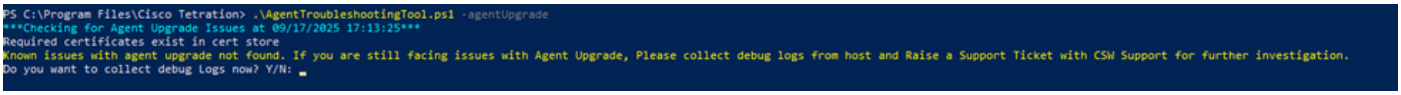
-agentUpgrade 매개 변수 아래에서 다음 사항을 확인합니다.

1. 필요한 인증서는 저장소에서 사용할 수 있습니다.
2. MSI 캐시는 C: \ Windows \Installer 폴더.

알려진 문제가 발견되지 않았지만 에이전트 업그레이드가 계속 실패하는 경우 추가 트러블슈팅을 위해 디버그 로그를 수집하는 옵션을 제공합니다.

다음은 -agentUpgrade를 실행할 때의 스크립트 출력 예입니다 매개변수

.\AgentTroubleshootingTool.ps1 -agentUpgrade



매개 변수 세부 정보 -enforcementHealth

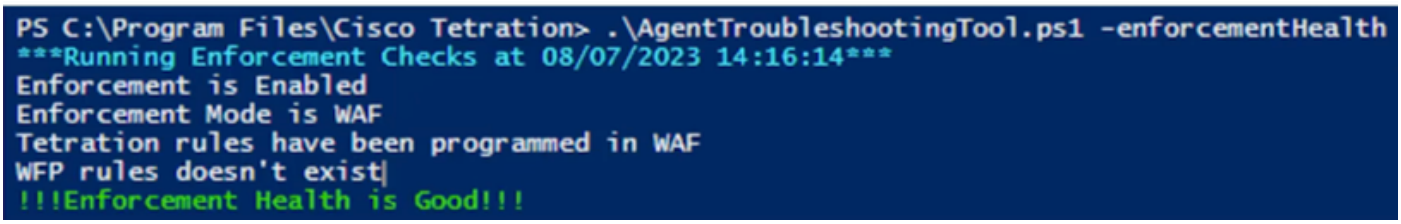
-enforcementHealth 매개 변수에서 다음 항목을 확인합니다.

1. 시행이 활성화되었거나 비활성화되었습니다.
2. 사용할 수 있습니다.
3. CSW 규칙이 WAF로 프로그래밍되었거나 WFP 필터가 프로그래밍되었습니다.
4. CSW WFP 필터가 없습니다(모드가 WAF인 경우).
5. CSW WAF 규칙이 없습니다(WFP 모드인 경우).

4단계와 5단계는 시행 모드가 전환된 경우의 문제를 파악하는 것입니다.

다음은 -enforcementHealth를 사용하여 스크립트를 실행할 때의 스크립트 출력 예입니다 매개변수.

.\AgentTroubleshootingTool.ps1 -enforceHealth



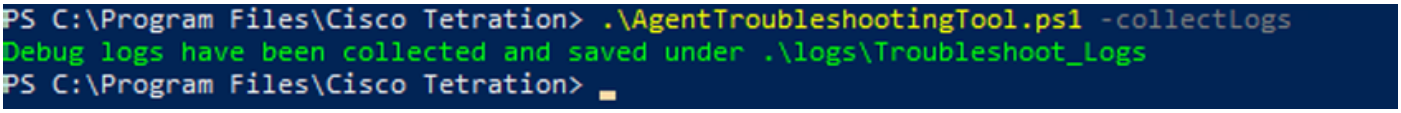
매개 변수 세부 정보 -collectLogs

스크립트는 -collectLogs 매개 변수를 사용하여 실행할 때 디버깅을 위해 로그를 수집합니다.

수집된 로그는 C:\ Program Files \Cisco Tetration\logs\logs\Troubleshoot_Logs 경로에 저장할 수 있습니다.

다음은 -collectLogs를 사용하여 스크립트를 실행할 때의 스크립트 출력 예입니다 매개변수.

.\AgentTroubleshootingTool.ps1 -collectLogs



매개 변수 세부 정보 -collectDebugLogs

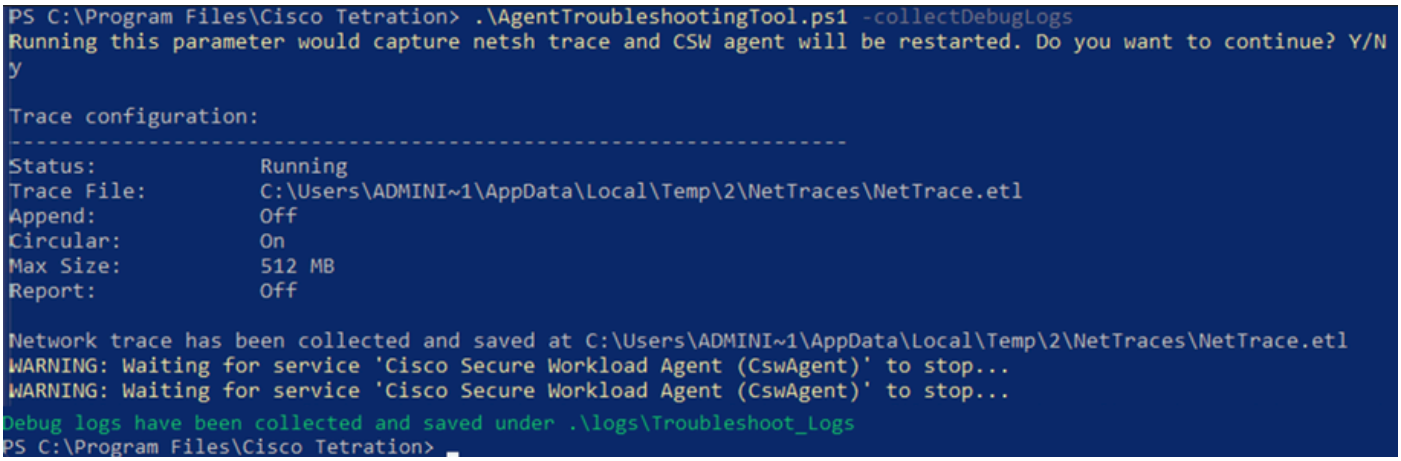
스크립트는 -collectDebugLogs 매개 변수를 실행할 때 디버깅을 위해 loglevel:5가 활성화된 로그를

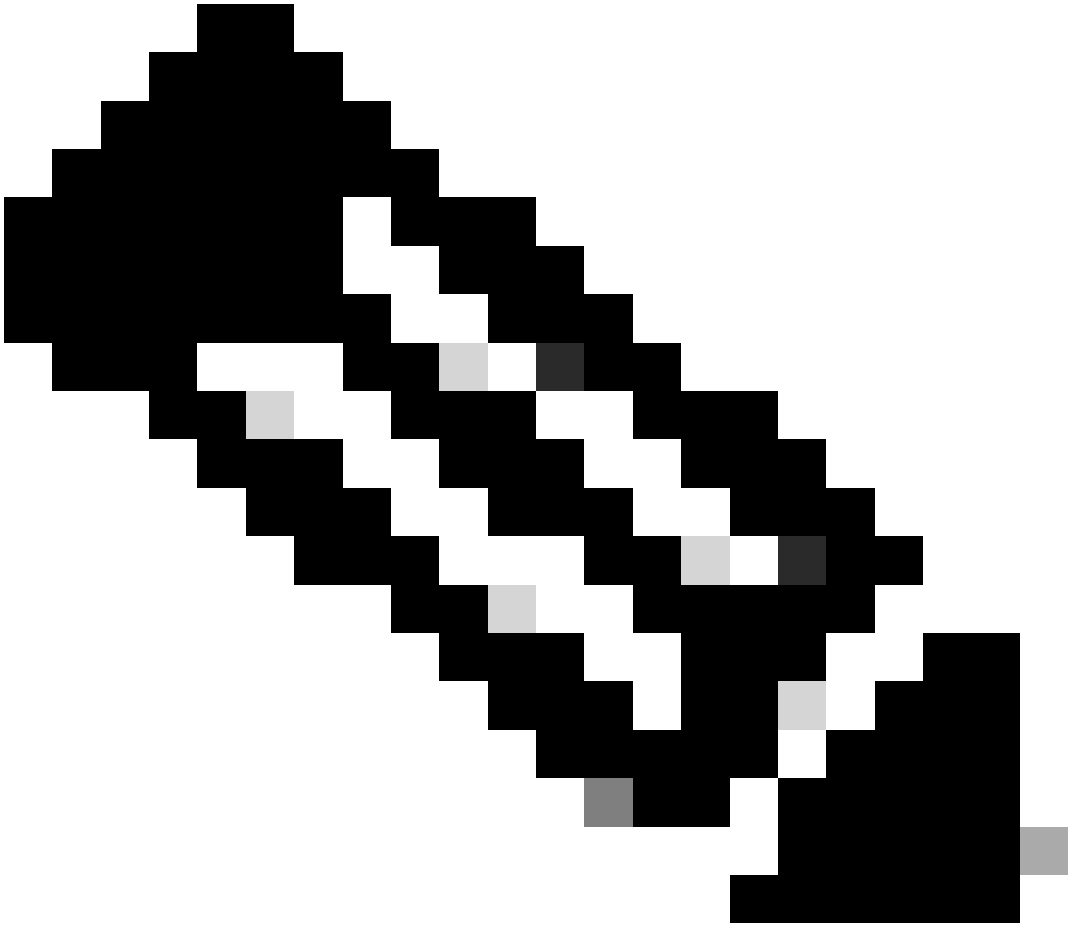
수집합니다.

이 매개 변수를 사용하여 스크립트를 실행하면 netsh 추적이 캡처되고 CSW 에이전트를 다시 시작할 수 있습니다.
수집된 로그는 C:\ Program Files \Cisco Tetration\logs\logs\Troubleshoot_Logs 경로에 저장할 수 있습니다.

다음은 -collectDebugLogs를 사용하여 스크립트를 실행할 때의 스크립트 출력 예입니다 매개변수.

.\AgentTroubleshootingTool.ps1 -collectDebugLogs





참고: 상담원 문제 해결 도구는 빨간색으로 오류를 표시하고 노란색으로 경고를 표시합니다. 상담원 문제 해결 도구에서 플래그가 지정된 일반적인 문제를 해결할 수 없는 경우, 상담원 문제 해결 도구를 사용하여 디버그 로그를 수집하고 보안 워크로드 상담원 로그 번들을 생성한 다음 Cisco TAC에 문의하십시오.

Secure Workload Agent 로그 번들 생성

로그 번들을 수집하려면 Secure Workload 에이전트가 활성 상태여야 합니다.

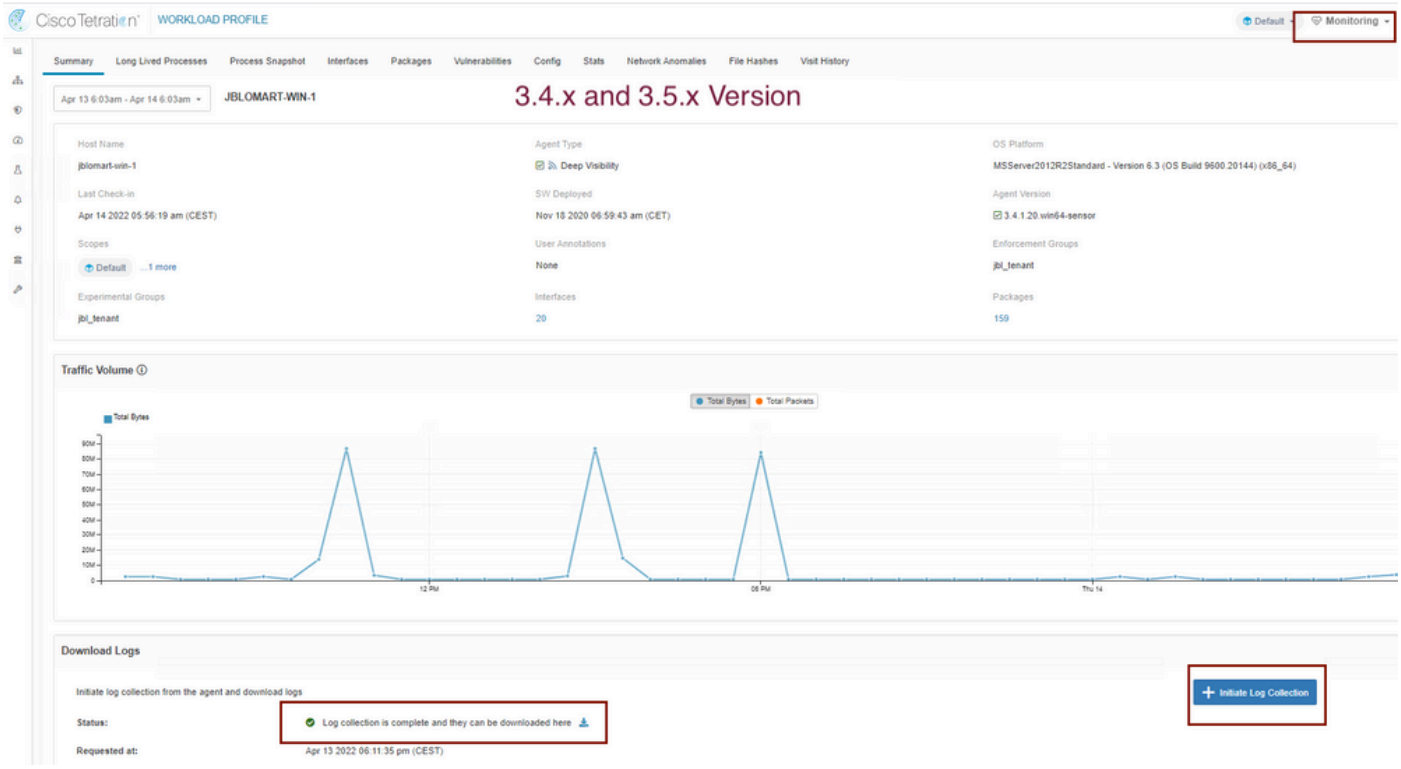
- 3.6.x 버전의 경우 왼쪽 탐색 패널로 이동하여 Manage(관리) > Agent(에이전트)를 선택하고 Agent List(에이전트 목록)를 클릭합니다.
- 3.4.x 및 3.5.x 버전의 경우 오른쪽 상단 드롭다운 메뉴에서 Monitoring(모니터링)으로 이동하고 Agent List(상담원 목록)를 선택합니다.

필터 옵션을 사용하여 에이전트를 검색하고 에이전트를 누릅니다. 에이전트의 작업 로드 프로파일

로 이동합니다. 여기서는 에이전트 컨피그레이션에 대한 세부 정보를 확인할 수 있습니다.
상태 등입니다.

작업 로드 프로필 페이지(3.6.x)의 왼쪽 탐색 패널에서 로그 다운로드(3.4.x 및 3.5.x에서 요약 탭 팔로우)를 선택합니다. Tetration Agent에서 로그 수집을 시작하려면 Initiate Log Collection을 클릭합니다. 로그 수집을 완료하는 데 시간이 걸릴 수 있습니다. 로그 수집이 완료되면 Download hereoption을 클릭하여 로그를 다운로드합니다. 아래로 스크롤하여 케이스 번호에 파일을 업로드할 수 있는 옵션을 가져옵니다.

이 이미지를 참조하여 3.4.x 및 3.5.x 버전에서 실행되는 에이전트에 대한 보안 작업 로드 에이전트 로그 번들을 생성합니다.



3.6.x 버전부터 Secure Workload Agent Log Bundle을 생성하려면 이 이미지를 참조하십시오 

이 번역에 관하여

Cisco는 전 세계 사용자에게 다양한 언어로 지원 콘텐츠를 제공하기 위해 기계 번역 기술과 수작업 번역을 병행하여 이 문서를 번역했습니다. 아무리 품질이 높은 기계 번역이라도 전문 번역가의 번역 결과물만큼 정확하지는 않습니다. Cisco Systems, Inc.는 이 같은 번역에 대해 어떠한 책임도 지지 않으며 항상 원본 영문 문서(링크 제공됨)를 참조할 것을 권장합니다.