ISE에서 외부 Syslog 서버 구성

목차

소개

이 문서에서는 ISE에서 외부 Syslog 서버를 구성하는 방법에 대해 설명합니다.

사전 요구 사항

요구 사항

다음 주제에 대한 지식을 보유하고 있으면 유용합니다.

- Identity Services Engine (ISE).
- Syslog 서버

사용되는 구성 요소

이 문서의 정보는 다음 소프트웨어 및 하드웨어 버전을 기반으로 합니다.

- ISE(Identity Services Engine) 3.3 버전.
- Kiwi Syslog 서버 v1.2.1.4

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

.

ISE의 syslog 메시지는 로그 컬렉터에서 수집 및 저장됩니다. 이러한 로그 컬렉터는 MnT가 수집된 로그를 로컬에 저장하도록 모니터링 노드에 할당됩니다.

외부 로그를 수집하려면 외부 syslog 서버를 구성합니다. 이를 타겟이라고 합니다. 로그는 미리 정의된 다양한 범주로 분류됩니다.

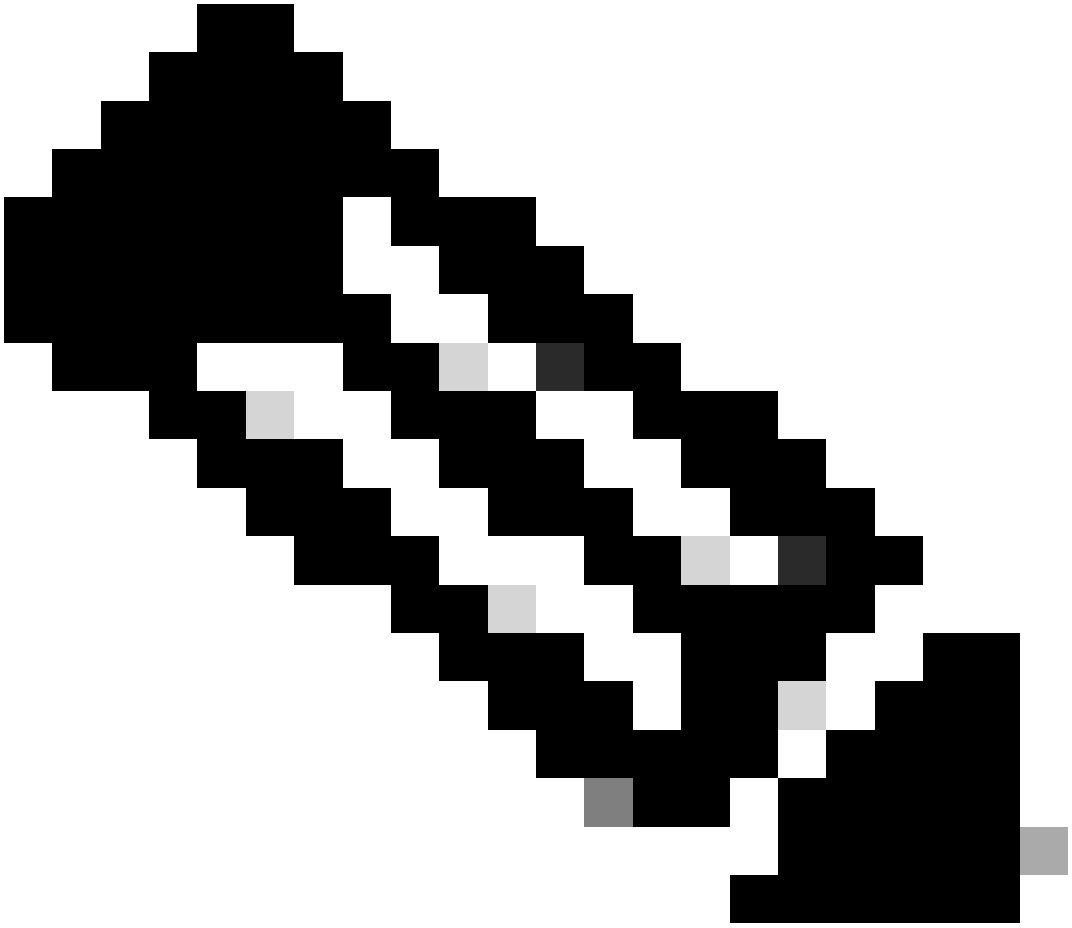
대상, 심각도 수준 등과 관련된 카테고리를 편집하여 로깅 출력을 사용자 지정할 수 있습니다.

설정

웹 인터페이스를 사용하여 시스템 로그 메시지가 전송되는 원격 syslog 서버 대상을 생성할 수 있습니다. 로그 메시지는 syslog 프로토콜 표준에 따라 원격 syslog 서버 대상으로 전송됩니다(RFC-3164 참조).

원격 로깅 대상 구성(UDP Syslog)

Cisco ISE GUI에서 Menu(메뉴)를 클릭하고 Administration(관리)>System(시스템)>Logging(로깅)>Remote Logging Targets(원격 로깅 대상)> Add(추가)를 클릭합니다.



참고: 이 컨피그레이션 예는 Configuring Remote Logging Target(원격 로깅 대상 구성)이라는 스크린샷을 기반으로 합니다.

- 이름을 Remote_Kiwi_Syslog로 지정합니다. 여기서 원격 Syslog 서버의 이름을 입력할 수 있습니다. 이 이름은 설명적인 목적으로 사용됩니다.
- Target Type as UDP Syslog, 이 컨피그레이션 예에서는 UDP Syslog가 사용되고 있지만 Target Type 드롭다운 목록에서 추가 옵션을 구성할 수 있습니다.

UDP Syslog: UDP를 통해 syslog 메시지를 전송하는 데 사용되며, 경량화 및 고속 로깅에 적합합니다.

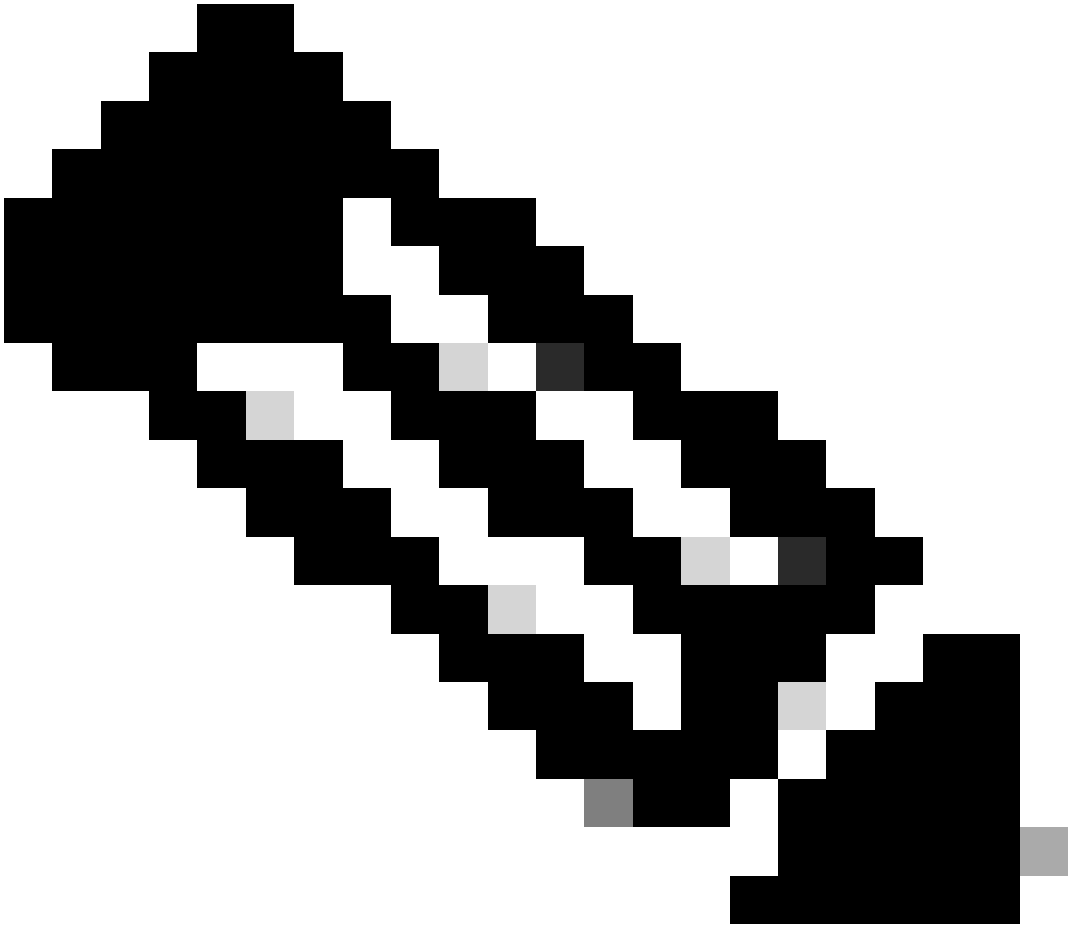
TCP Syslog: TCP를 통해 syslog 메시지를 전송하는 데 사용되며, 오류 확인 및 재전송 기능과 함께 안정성을 제공합니다.

보안 Syslog: TLS 암호화를 사용하여 TCP를 통해 전송되는 syslog 메시지를 참조하여 데이터 무결성과 기밀성을 보장합니다.

- Status as Enabled(상태 활성화)는 Statusdrop(상태) 드롭다운 목록에서 Enabled(활성화됨)를

선택해야 합니다.

- 설명, 선택적으로 새 대상에 대한 간단한 설명을 입력할 수 있습니다.
- 호스트 / IP 주소, 여기서 로그를 저장 하는 대상 서버의 IP 주소 또는 호스트 이름을 입력 합니다. Cisco ISE는 로깅에 대한 IPv4 및 IPv6 형식을 지원 합니다.



참고: FQDN으로 syslog 서버를 구성할 경우 성능에 영향을 주지 않도록 DNS 캐싱을 설정해야 한다는 점을 반드시 언급해야 합니다. DNS 캐싱이 없으면 ISE는 FQDN으로 구성된 원격 로깅 대상에 syslog 패킷을 보내야 할 때마다 DNS 서버를 쿼리합니다. 이는 ISE 성능에 심각한 영향을 미칩니다.

이service cache enable를 해결하려면 구축의 모든 PSN에서 명령을 사용합니다.

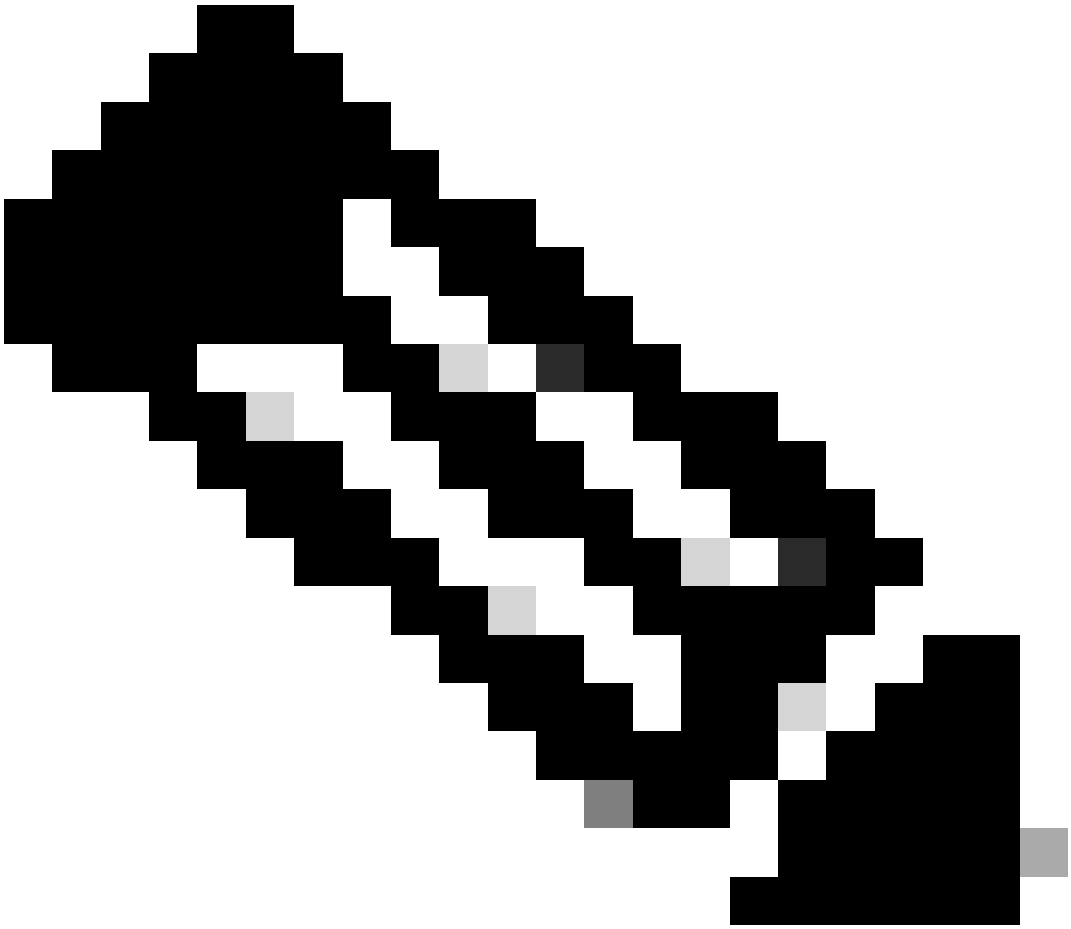
예

```
ise/admin(config)# service cache enable hosts ttl 180
```

• **포트** as **514**, 이 컨피그레이션 예에서 Kiwi Syslog 서버는 UDP syslog 메시지의 기본 포트인 포트 **514**에서 수신 대기합니다. 그러나 사용자는 이 포트 번호를 1~65535 사이의 값으로 변경할 수 있습니다. 원하는 포트가 방화벽에 의해 차단되고 있지 않은지 확인하십시오.

• **Facility Code** as **LOCAL6**, 드롭다운 목록에서 로깅에 사용해야 하는 syslog 기능 코드를 선택할 수 있습니다. 유효한 옵션은 Local0~Local7입니다.

• **Maximum Length** as **1024(최대 길이**: 1024). 여기서 원격 로그 대상 메시지의 최대 길이를 입력할 수 있습니다. 최대 길이는 기본적으로 ISE 3.3 버전인 **1024**로 설정되며, 값은 200~1024바이트입니다.



참고: 잘린 메시지를 원격 로깅 대상으로 전송하지 않으려면 Maximum Length(최대 길이)를 8192로 수정할 수 있습니다.

- **Include Alarms For this Target,** 이 컨피그레이션 예에서는 **Include Alarms For this Target**을 단순하게 유지하기 위해 이 컨피그레이션 예에서 Include Alarms For this Target을 선택하지 않습니다. 그러나 이 확인란을 선택하면 경보 메시지도 원격 서버로 전송됩니다.

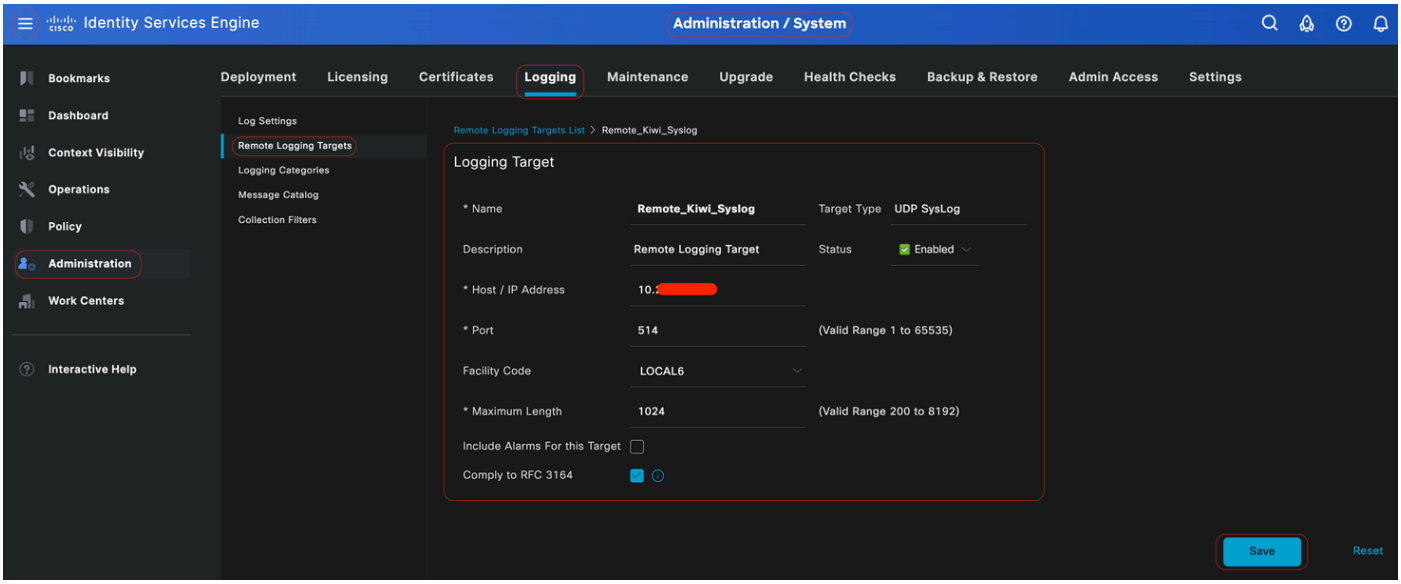
- **Compare RFC 3164**(RFC **3164 준수**)가 선택된 경우 이 확인란을 선택하면 백슬래시(\)를 사용하더라도 원격 서버로 전송되는 syslog 메시지의 구분 기호(, ; { } \ \)가 이스케이프되지 않습니다.

-

컨피그레이션이 완료되면 Save(저장)를 **클릭합니다**.

-

저장하면 시스템에 다음 경고가 표시됩니다. 서버에 **대한 비보안(TCP/UDP) 연결을 만들도록 선택했습니다. 계속하시겠습니까?Yes(예)**를 클릭합니다.



원격 대상 구성

로깅 범주에서 원격 대상 구성

Cisco ISE는 syslog 타겟으로 감사 가능 이벤트를 전송합니다. 원격 로깅 대상을 구성한 후에는 **원격** 로깅 대상을 의도된 범주에 매핑하여 감사 가능한 이벤트를 전달해야 합니다.

그러면 로깅 대상이 이러한 각 로깅 범주에 매핑될 수 있습니다. 이러한 로그 범주의 이벤트 로그는 PSN 노드에서만 생성되며, 해당 노드에서 활성화된 서비스에 따라 관련 로그를 원격 Syslog 서버로 전송하도록 구성할 수 있습니다.

- **AAA 감사**
- **AAA 진단**
- **어카운팅**
- **외부 MDM**
- **수동 ID**
- **상태 및 클라이언트 프로비저닝 감사**
- **상태 및 클라이언트 프로비저닝 진단**
- **프로파일러**

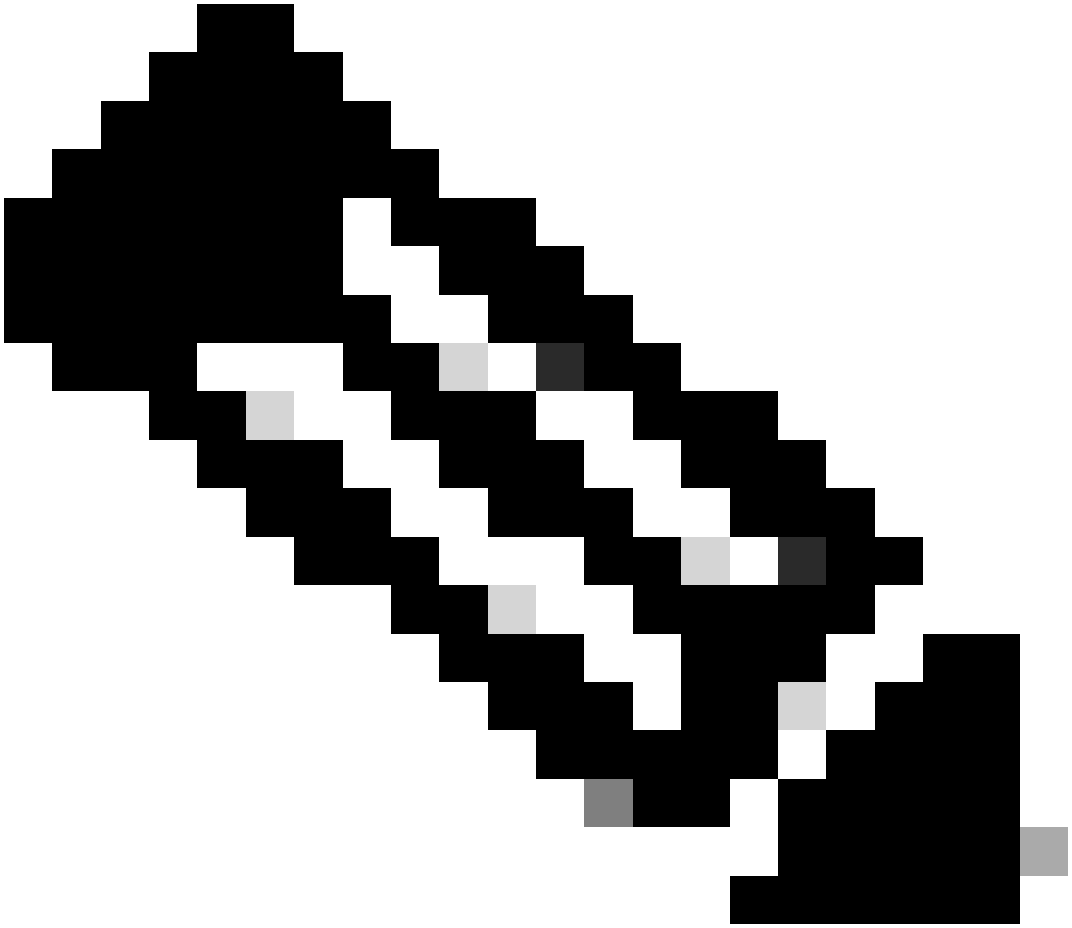
이러한 로그 범주의 이벤트 로그는 구축의 모든 노드에서 생성되며 관련 로그를 원격 Syslog 서버로 전송하도록 구성할 수 있습니다.

- **관리 및 운영 감사**
-

시스템 진단

- **시스템 통계**

이 컨피그레이션 예에서는 4개의 로깅 범주, 즉 **통과한 인증**, **실패한 시도** 및 **Radius 계정 관리**와 ISE 관리자 로깅 트래픽에 대한 이 범주의 인증 트래픽 로그를 보낼 3개의 로깅 범주 아래에 원격 대상을 구성합니다.



참고: **이 컨피그레이션 예는 Configuring Remote Logging Target(원격 로깅 대상 구성)이라는 스크린샷을 기반으로 합니다.**

Cisco ISE GUI에서 Menuicon()을 클릭하고 **Administration(관리)>System(시스템)>Logging(로깅)>Logging Categories(로깅 범주)**를 선택한 다음 필수 범주(Passed Authentications(통과한 인증), Failed Attempts(실패한 시도) 및 Radius Accounting(Radius 계정 관리))를 클릭합니다.

1단계-Log Severity Level(심각도 수준 기록**):** 이벤트 메시지는 심각도 수준과 연결되어 있으므로 관리자가 메시지를 필터링하고 우선 순위를 지정할 수 있습니다. 필요에 따라 로그 심각도 레벨을 선택합니다. 일부 로깅 범주의 경우 이 값은 기본적으로 설정되며 편집할 수 없습니다. 일부 로깅 범주의 경우 드롭다운 목록에서 다음 심각도 수준 중 하나를 선택할 수 있습니다.

- **치명적**: 긴급 수준 이 레벨은 Cisco ISE를 사용할 수 없으며 필요한 조치를 즉시 취해야 함을 의미합니다.
- **ERROR**: 이 레벨은 심각한 오류 상태를 나타냅니다.
- **WARN**: 이 레벨은 정상이지만 심각한 상태를 나타냅니다. 이는 여러 로깅 범주에 대해 설정된 기본 레벨입니다.
- **INFO**: 이 레벨은 정보 메시지를 나타냅니다.

-

DEBUG: 이 레벨은 진단 버그 메시지를 나타냅니다.

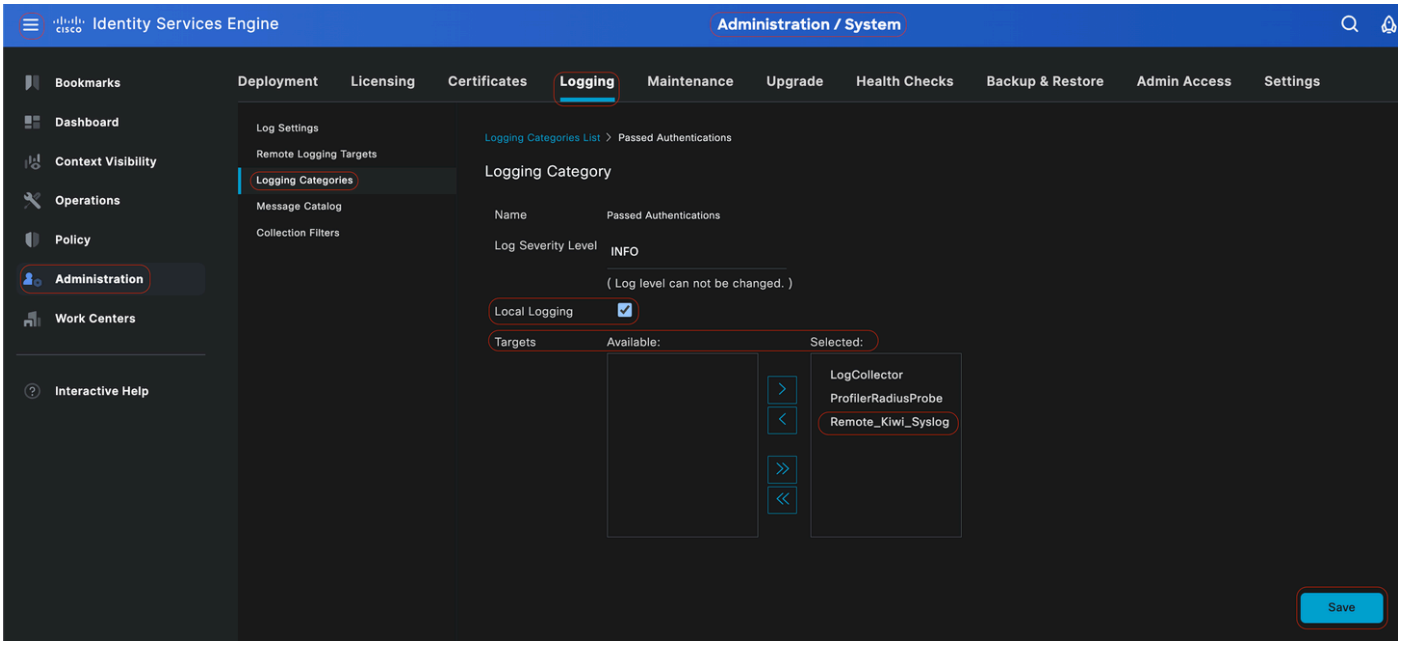
2단계 - 로컬 로깅: 이 확인란을 선택하면 로컬 로그 생성이 활성화됩니다. 즉, PSN에 의해 생성된 로그는 로그를 생성하는 특정 PSN에도 저장됩니다. 기본 컨피그레이션을 유지하는 것이 좋습니다

3단계- 대상: 이 영역에서는 왼쪽 및 오른쪽 화살표 아이콘을 사용하여 Availableselected영역과 Availabletable영역 간에 대상을 전송하여 로깅 범주의 대상을 선택할 수 있습니다.

Availablearea에는 로컬(사전 정의) 및 외부(사용자 정의)의 기존 로깅 대상이 포함됩니다.

처음에 비어 있는 Selectedarea에는 카테고리에 대해 선택된 대상이 표시됩니다.

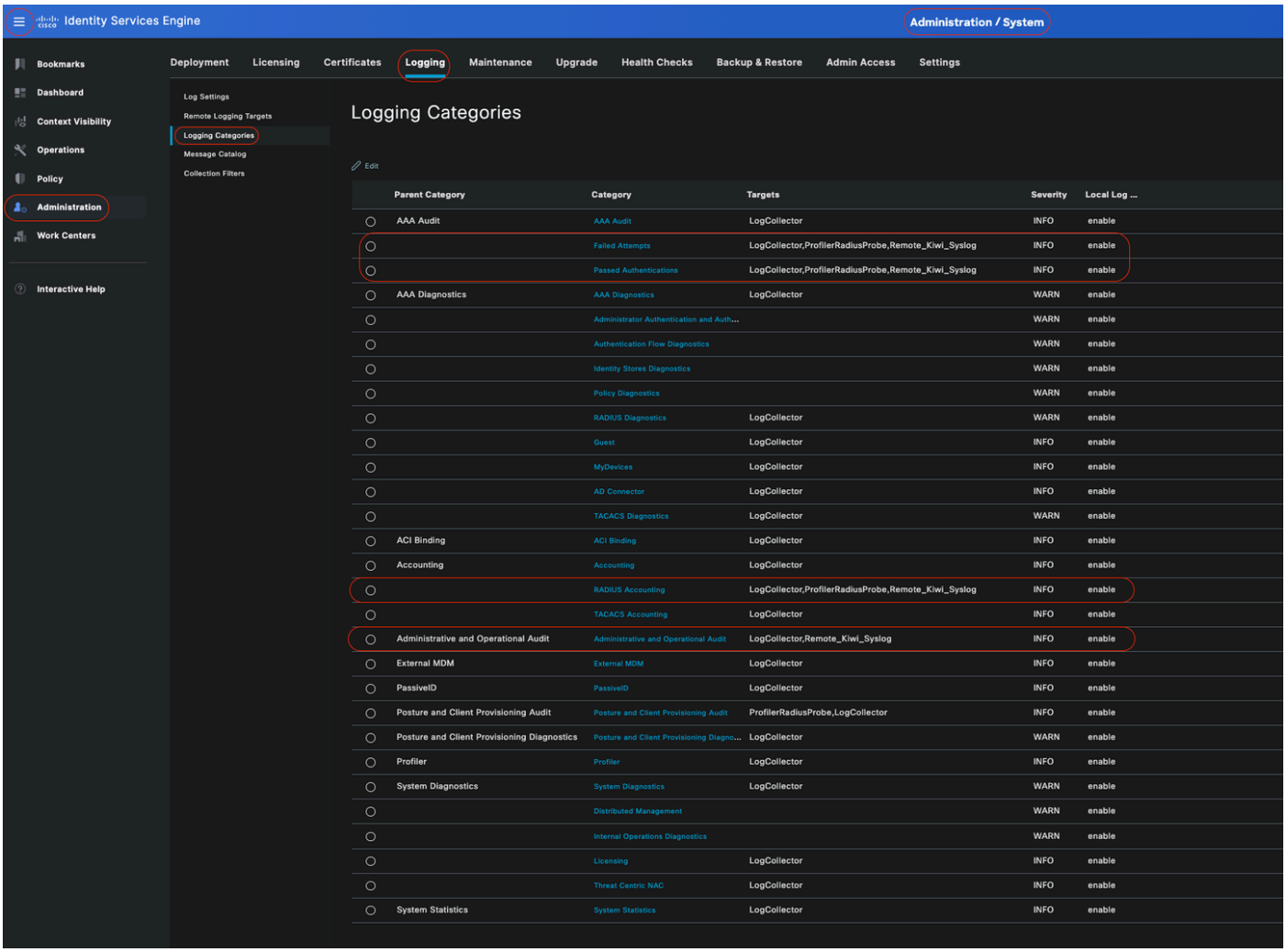
4단계 - 1단계에서 3단계까지 반복하여 Failed Attempts(실패한 시도) 및 Radius Accounting(RADIUS 어카운팅) 범주 아래에 Remote Target(원격 대상)**을** 추가합니다.



의도한 범주에 원격 대상 매핑

5단계- 원격 대상이 필수 범주에 속하는지 확인합니다.방금 추가한 원격 대상을 볼 수 있어야 합니다.

이 스크린샷에서는 원격 대상 Remote_Kiwi_**Syslog가** 필수 **범주**에 매핑된 것을 볼 수 있습니다.



범주 확인

범주 이해

이벤트가 발생할 때 메시지가 생성됩니다. 커널, 메일, 사용자 레벨 등과 같은 여러 기능에서 생성되는 이벤트 메시지의 유형은 서로 다릅니다.

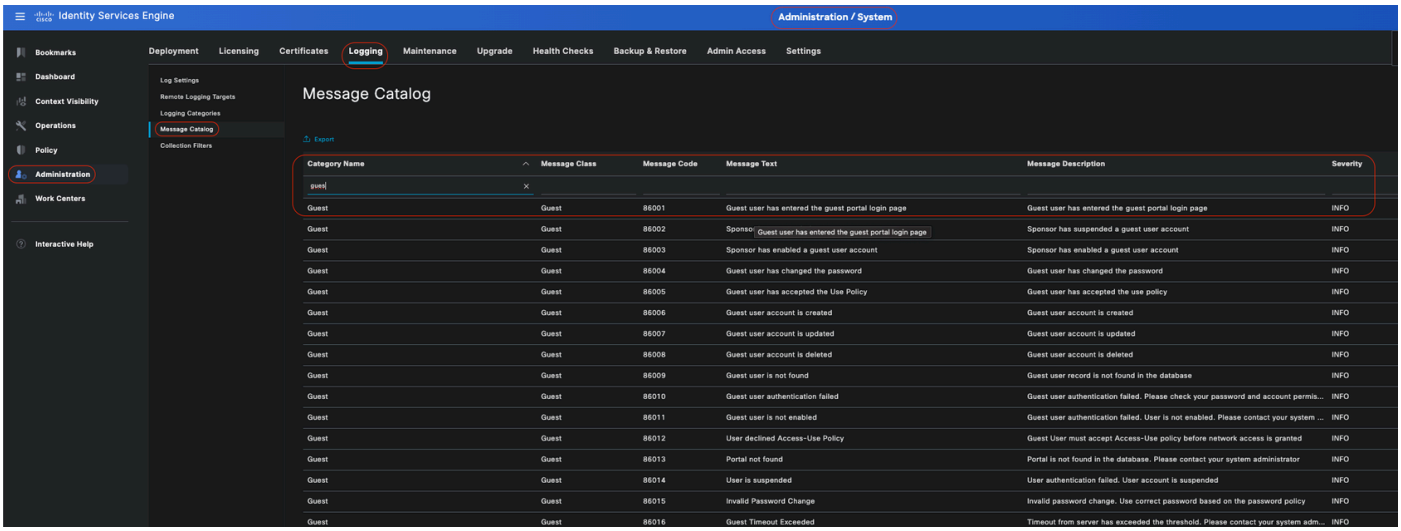
이러한 오류는 메시지 카탈로그 내에서 범주화되며 이러한 이벤트는 범주별로 계층적으로 구성됩니다.

이러한 범주에는 하나 이상의 범주를 포함하는 상위 범주가 있습니다.

상위 범주	카테고리
AAA 감사	AAA 감사 실패한 시도 인증 통과
AAA 진단	AAA 진단 관리자 인증 및 권한 부여

	인증 흐름 진단 ID 저장소 진단 정책 진단 Radius 진단 게스트
어카운팅	어카운팅 Radius 계정 관리
관리 및 운영 감사	관리 및 운영 감사
상태 및 클라이언트 프로비저닝 감사	상태 및 클라이언트 프로비저닝 감사
상태 및 클라이언트 프로비저닝 진단	상태 및 클라이언트 프로비저닝 진단
프로파일러	프로파일러
시스템 진단	시스템 진단 분산 관리 내부 운영 진단
시스템 통계	시스템 통계

이 스크린샷에서는 Guest가 Message Class(**메시지 클래스)**이고 Guest Category(게스트 범주)로 분류되어 있음을 **확인할** 수 **있습니다** . 이 게스트 범주에는 **AAA** Diagnostics라는 상위 범주가 **있습니다**.



메시지 카탈로그

확인 및 문제 해결

원격 로깅 대상에 대해 TCP 덤프를 가져오는 것은 로그 이벤트가 전송되는지 여부를 확인하는 가장 빠른 트러블슈팅 및 확인 단계입니다.

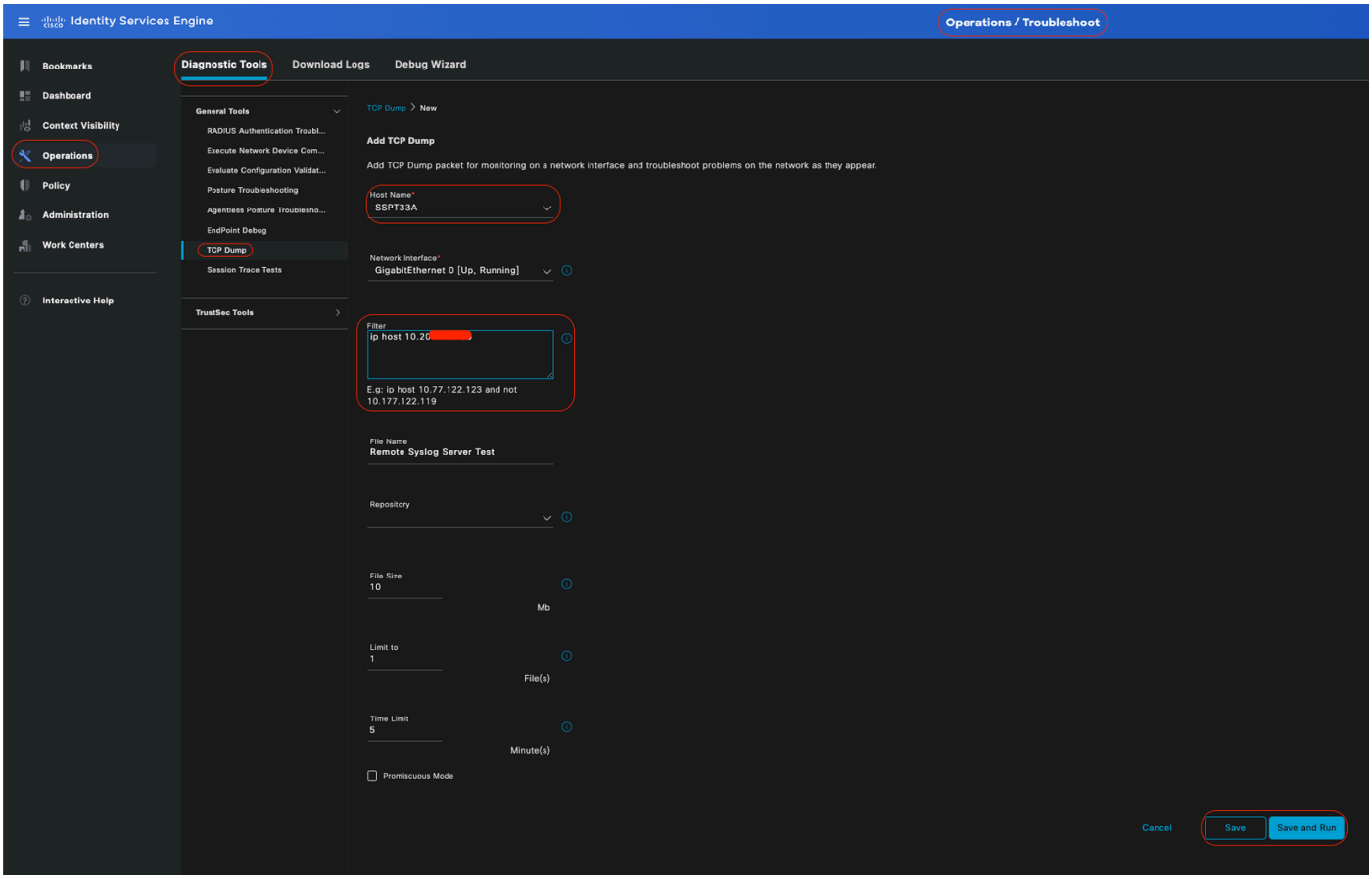
PSN에서 로그 메시지를 생성하고 이러한 메시지를 원격 타겟으로 전송하므로 사용자를 인증하는 PSN에서 캡처를 가져와야 합니다

Cisco ISE GUI에서 Menuicon (

)을 클릭하고 **Operations(운영)**> Troubleshoot(문제 해결)**>TCP Dump(TCP 덤프)**> Click on Add(추가)를 **클릭합니다.**

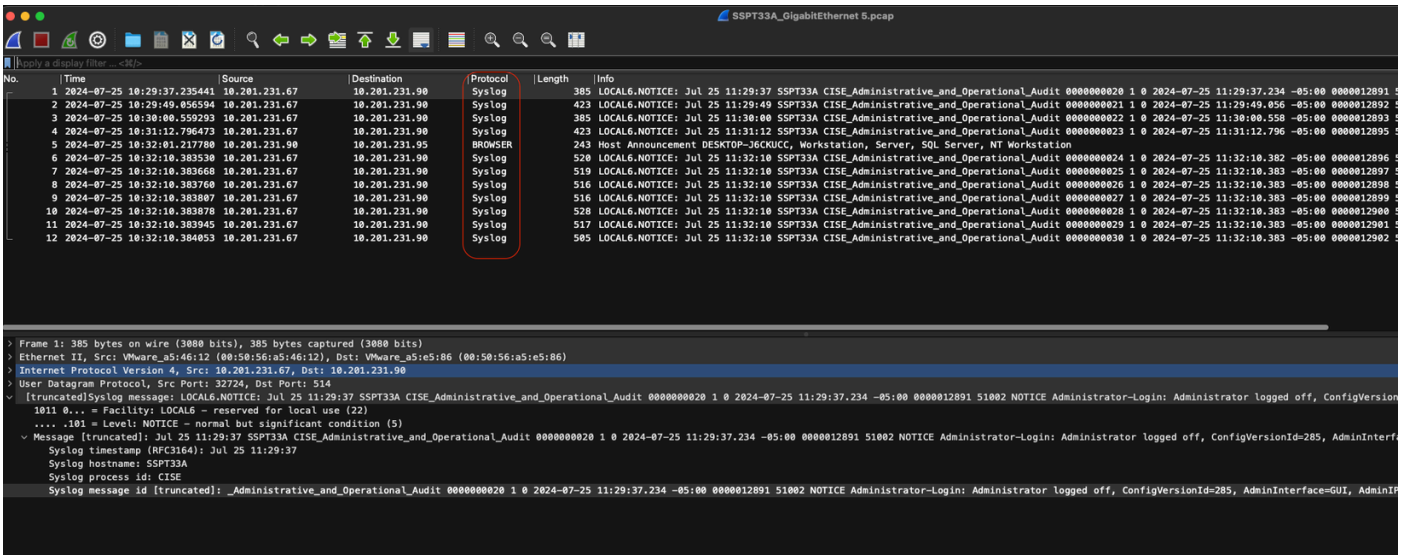
- 트래픽을 필터링하고 ip host <remote_target_IP_addresses> filter 필드를 추가해야 합니다.

- PSN 처리 인증에서 캡처를 가져와야 합니다.



TCP 덤프

이 스크린샷에서는 ISE가 ISE 관리자 로깅 트래픽에 대한 Syslog 메시지를 전송하는 방법을 볼 수 있습니다.


SSPT33A_GigabitEthernet 5.pcap
Apply a display filter ... <⌘/>
No. Time Source Destination Protocol Length Info
1 2024-07-25 10:29:37.235441 10.201.231.67 10.201.231.90 Syslog 385 LOCAL6.NOTICE: Jul 25 11:29:37 SSPT33A CISE_Administrative_and_Operational_Audit 0000000020 1 0 2024-07-25 11:29:37.234 -05:00 0000012891
2 2024-07-25 10:29:49.056594 10.201.231.67 10.201.231.90 Syslog 423 LOCAL6.NOTICE: Jul 25 11:29:49 SSPT33A CISE_Administrative_and_Operational_Audit 0000000021 1 0 2024-07-25 11:29:49.056 -05:00 0000012892
3 2024-07-25 10:30:00.559293 10.201.231.67 10.201.231.90 Syslog 385 LOCAL6.NOTICE: Jul 25 11:30:00 SSPT33A CISE_Administrative_and_Operational_Audit 0000000022 1 0 2024-07-25 11:30:00.558 -05:00 0000012893
4 2024-07-25 10:31:12.796473 10.201.231.67 10.201.231.90 Syslog 423 LOCAL6.NOTICE: Jul 25 11:31:12 SSPT33A CISE_Administrative_and_Operational_Audit 0000000023 1 0 2024-07-25 11:31:12.796 -05:00 0000012895
5 2024-07-25 10:32:01.217780 10.201.231.90 10.201.231.95 BROWSER 243 Host Announcement DESKTOP-J6CKUCC, Workstation, Server, SQL Server, NT Workstation
6 2024-07-25 10:32:10.383530 10.201.231.67 10.201.231.90 Syslog 520 LOCAL6.NOTICE: Jul 25 11:32:10 SSPT33A CISE_Administrative_and_Operational_Audit 0000000024 1 0 2024-07-25 11:32:10.382 -05:00 0000012896
7 2024-07-25 10:32:10.383668 10.201.231.67 10.201.231.90 Syslog 519 LOCAL6.NOTICE: Jul 25 11:32:10 SSPT33A CISE_Administrative_and_Operational_Audit 0000000025 1 0 2024-07-25 11:32:10.383 -05:00 0000012897
8 2024-07-25 10:32:10.383760 10.201.231.67 10.201.231.90 Syslog 516 LOCAL6.NOTICE: Jul 25 11:32:10 SSPT33A CISE_Administrative_and_Operational_Audit 0000000026 1 0 2024-07-25 11:32:10.383 -05:00 0000012898
9 2024-07-25 10:32:10.383807 10.201.231.67 10.201.231.90 Syslog 516 LOCAL6.NOTICE: Jul 25 11:32:10 SSPT33A CISE_Administrative_and_Operational_Audit 0000000027 1 0 2024-07-25 11:32:10.383 -05:00 0000012899
10 2024-07-25 10:32:10.383878 10.201.231.67 10.201.231.90 Syslog 528 LOCAL6.NOTICE: Jul 25 11:32:10 SSPT33A CISE_Administrative_and_Operational_Audit 0000000028 1 0 2024-07-25 11:32:10.383 -05:00 0000012900
11 2024-07-25 10:32:10.383945 10.201.231.67 10.201.231.90 Syslog 517 LOCAL6.NOTICE: Jul 25 11:32:10 SSPT33A CISE_Administrative_and_Operational_Audit 0000000029 1 0 2024-07-25 11:32:10.383 -05:00 0000012901
12 2024-07-25 10:32:10.384053 10.201.231.67 10.201.231.90 Syslog 505 LOCAL6.NOTICE: Jul 25 11:32:10 SSPT33A CISE_Administrative_and_Operational_Audit 0000000030 1 0 2024-07-25 11:32:10.383 -05:00 0000012902
Frame 1: 385 bytes on wire (3080 bits), 385 bytes captured (3080 bits)
Ethernet II, Src: VMware_a5:46:12 (00:50:56:a5:46:12), Dst: VMware_a5:e5:86 (00:50:56:a5:e5:86)
Internet Protocol Version 4, Src: 10.201.231.67, Dst: 10.201.231.90
User Datagram Protocol, Src Port: 32724, Dst Port: 514
[truncated]Syslog message: LOCAL6.NOTICE: Jul 25 11:29:37 SSPT33A CISE_Administrative_and_Operational_Audit 0000000020 1 0 2024-07-25 11:29:37.234 -05:00 0000012891 51002 NOTICE Administrator-Login: Administrator logged off, ConfigVersion
1011 0... = Facility: LOCAL6 - reserved for local use (22)
.... .101 = Level: NOTICE - normal but significant condition (5)
Message [truncated]: Jul 25 11:29:37 SSPT33A CISE_Administrative_and_Operational_Audit 0000000020 1 0 2024-07-25 11:29:37.234 -05:00 0000012891 51002 NOTICE Administrator-Login: Administrator logged off, ConfigVersionId=285, AdminInterf
Syslog timestamp (RFC3164): Jul 25 11:29:37
Syslog hostname: SSPT33A
Syslog process id: CISE
Syslog message id [truncated]: _Administrative_and_Operational_Audit 0000000020 1 0 2024-07-25 11:29:37.234 -05:00 0000012891 51002 NOTICE Administrator-Login: Administrator logged off, ConfigVersionId=285, AdminInterface=GUI, AdminIP

Syslog 트래픽

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.