

PassiveID 세션에 보안 그룹 태그를 할당하도록 ISE 3.2 구성

목차

[소개](#)

[사전 요구 사항](#)

[요구 사항](#)

[사용되는 구성 요소](#)

[배경 정보](#)

[구성](#)

[순서도](#)

[설정](#)

[다음을 확인합니다.](#)

[ISE 확인](#)

[PxGrid 가입자 확인](#)

[TrustSec SXP 피어 확인](#)

[문제 해결](#)

[ISE에서 디버깅 활성화](#)

[로그 조각](#)

소개

이 문서에서는 ISE 3.2의 권한 부여 정책을 통해 수동 ID 세션에 SGT(Security Group Tag)를 구성하고 할당하는 방법을 설명합니다.

사전 요구 사항

요구 사항

다음 주제에 대한 지식을 보유하고 있으면 유용합니다.

- Cisco ISE 3.2
- 패시브 ID, TrustSec 및 PxGrid

사용되는 구성 요소

이 문서의 정보는 다음 소프트웨어 및 하드웨어 버전을 기반으로 합니다.

- Cisco ISE 3.2
- FMC 7.0.1
- 16.12.1을 실행하는 WS-C3850-24P

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

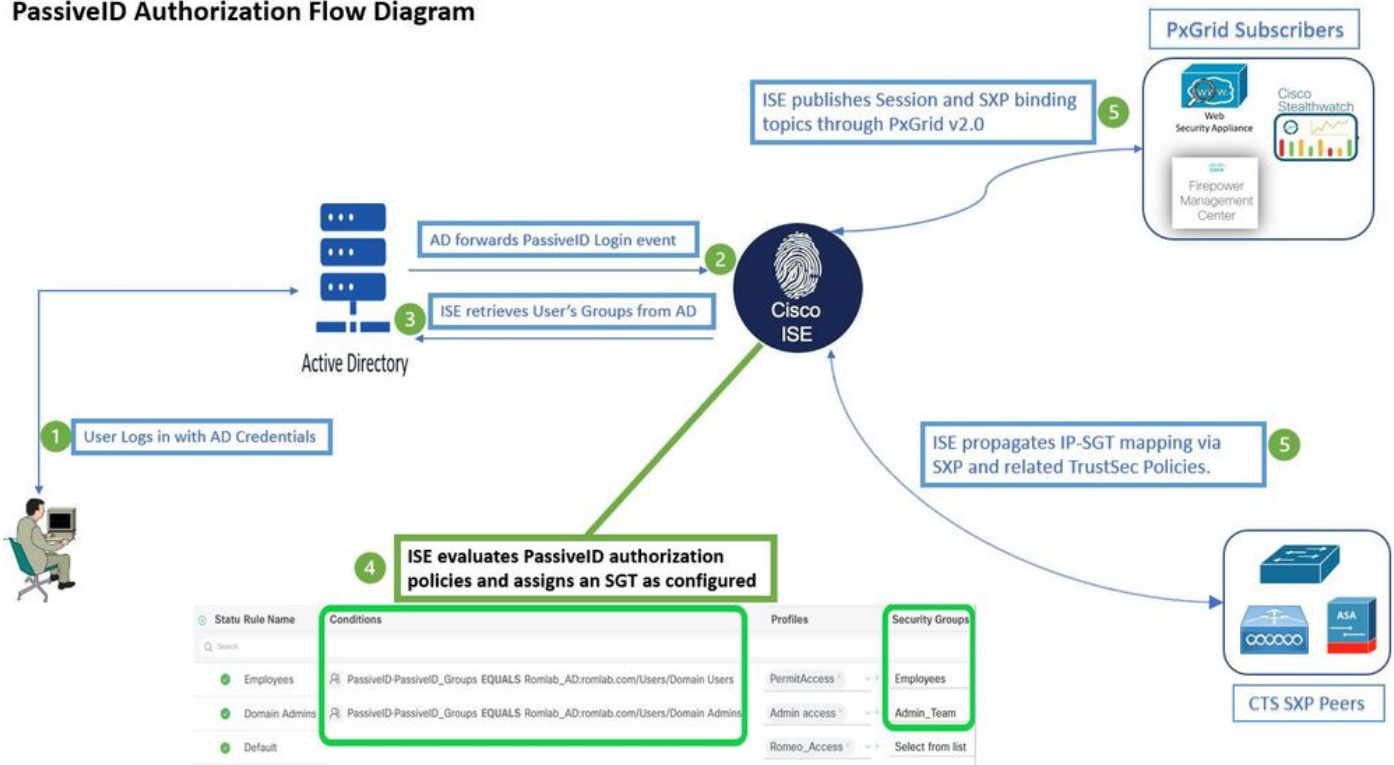
Cisco ISE(Identity Services Engine) 3.2는 이 기능을 지원하는 최소 버전입니다. 이 문서에서는 PassiveID, PxGrid 및 SXP 컨피그레이션을 다루지 않습니다. 관련 정보는 Admin [Guide를 참조하십시오](#).

ISE 3.1 이전 버전에서는 SGT(Security Group Tag)를 Radius 세션 또는 Active Authentication(예: 802.1x 및 MAB)에만 할당할 수 있습니다. ISE 3.2에서는 ISE(Identity Services Engine)가 AD DC(Active Directory 도메인 컨트롤러) WMI 또는 AD 에이전트 같은 공급자로부터 사용자 로그인 이벤트를 수신할 때 사용자 AD(Active Directory) 그룹 멤버십에 따라 SGT(Security Group Tag)를 PassiveID 세션에 할당하도록 PassiveID 세션에 대한 권한 부여 정책을 구성할 수 있습니다. firepower PassiveID에 대한 IP-SGT 매핑 및 AD 그룹 세부 정보는 SXP(SGT Exchange Protocol)를 통해 TrustSec 도메인 및/또는 pxGrid(Platform Exchange Grid) 가입자(예: Cisco FMC(Domain Management Center) 및 Cisco Secure Network Analytics(Stealthwatch)에 게시할 수 있습니다.

구성

순서도

PassiveID Authorization Flow Diagram

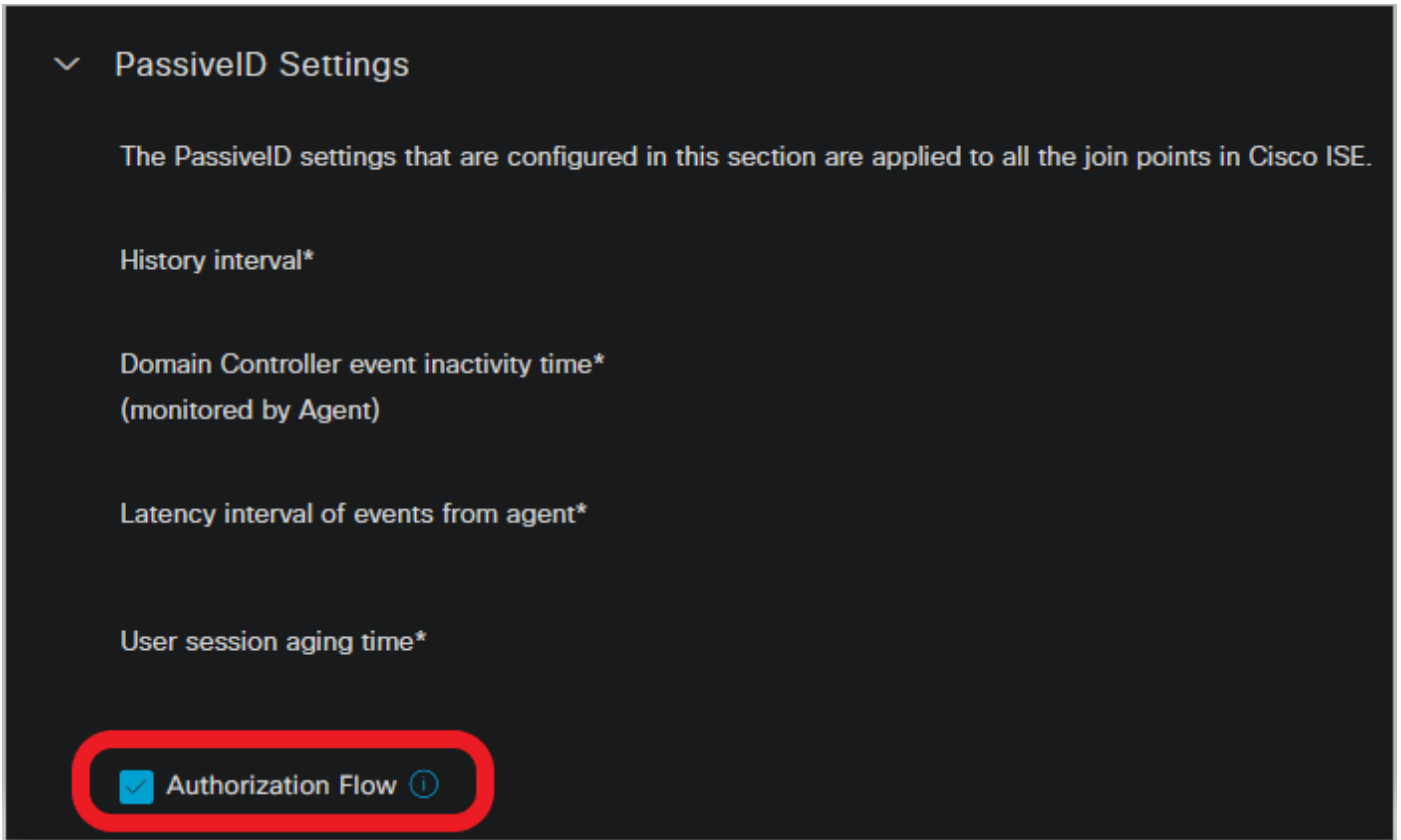


순서도

설정

인증 흐름을 활성화 합니다.

탐색 Active Directory > Advanced Settings > PassivelD Settings Cisco의 Authorization Flow passivelD 로그인 사용자에 대한 권한 부여 정책을 구성하려면 확인란을 선택합니다. 이 옵션은 기본적으로 비활성화되어 있습니다.

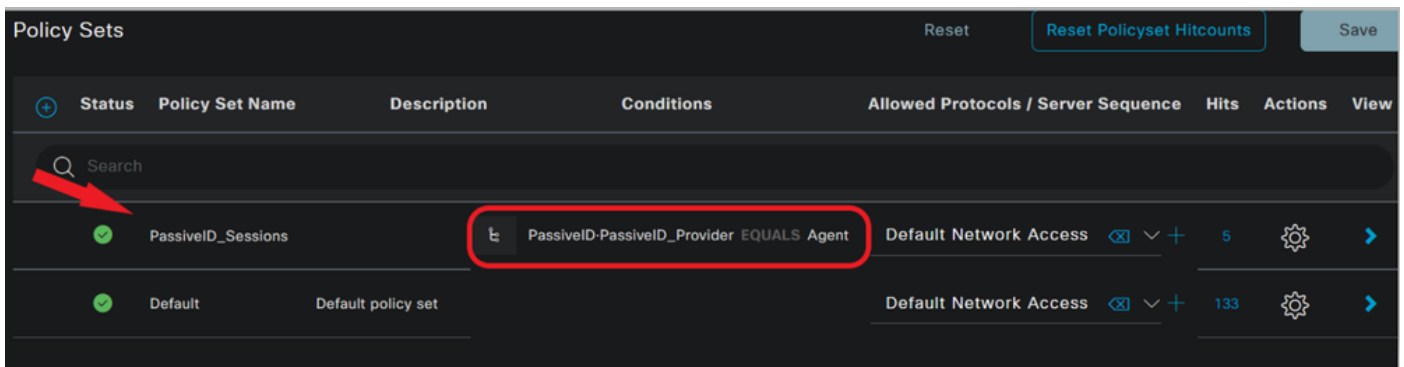


권한 부여 흐름 활성화

 참고: 이 기능이 작동하려면 구축에서 PassivelD, PxGrid 및 SXP 서비스를 실행해야 합니다. 아래에서 이를 확인할 수 있습니다. Administration > System > Deployment .

정책 집합 구성:

1. PassivelD에 대한 별도의 정책 집합을 생성합니다(권장).
2. 조건의 경우 특성을 사용합니다 PassiveID·PassiveID_Provider 제공 기관 유형을 선택합니다.



정책 집합

3. 1단계에서 생성한 정책 집합에 대한 권한 부여 규칙을 구성합니다.

- 각 규칙에 대한 조건을 생성하고 AD 그룹, 사용자 이름 또는 둘 모두를 기반으로 PassiveID 사전을 사용합니다.
- 각 규칙에 대해 보안 그룹 태그를 지정하고 컨피그레이션을 저장합니다.

The screenshot shows the 'Authorization Policy (3)' configuration page in Cisco ISE. The table below summarizes the visible data:

Status	Rule Name	Conditions	Profiles	Security Groups	Hits	Actions
●	Employees	PassiveID:PassiveID_Groups EQUALS Lfc_AD:Lfc.lab/Users /Domain Users	PermitAccess ×	Employees	3	⊗ ↓ + ⚙
●	Domain Admins	PassiveID:PassiveID_Groups EQUALS Lfc_AD:Lfc.lab/Users /Domain Admins	Admin access ×	Admin_Team	2	⊗ ↓ + ⚙
●	Default		DenyAccess ×	Select from list	0	⊗ ↓ + ⚙

권한 부여 정책

참고: 인증 정책은 이 흐름에서 사용되지 않으므로 관련이 없습니다.

참고: PassiveID_Username, PassiveID_Groups, 또는 PassiveID_Provider 특성을 사용하여 권한 부여 규칙을 생성합니다.

4. 다음으로 이동 Work Centers > TrustSec > Settings > SXP Settings 를 활성화하려면 Publish SXP bindings on pxGrid 및 Add RADIUS and PassiveID Mappings into SXP IP SGT Mapping Table PassiveID 매핑을 PxGrid 가입자와 공유하고 이를 ISE의 SXP 매핑 테이블에 포함합니다.

The screenshot shows the 'SXP Settings' page in Cisco ISE. The following table summarizes the configuration options shown:

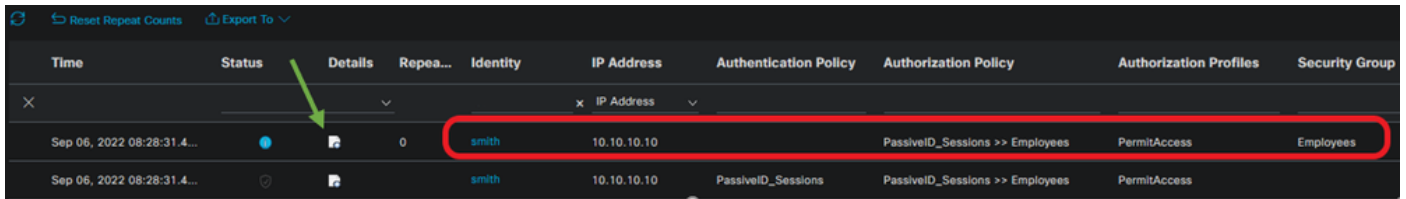
Option	Status
Publish SXP bindings on pxGrid	Checked
Add Radius and PassiveID mappings into SXP IP SGT mapping table	Checked

다음을 확인합니다.

구성이 올바르게 작동하는지 확인하려면 이 섹션을 활용하십시오.

ISE 확인

AD DC(Active Directory 도메인 컨트롤러) WMI 또는 AD 에이전트와 같은 공급자에서 사용자 로그인 이벤트를 ISE로 전송했으면 라이브 로그를 확인합니다. 탐색 **Operations > Radius > Live Logs**.



Time	Status	Details	Repea...	Identity	IP Address	Authentication Policy	Authorization Policy	Authorization Profiles	Security Group
Sep 06, 2022 08:28:31.4...	●	📄	0	smith	10.10.10.10	PassiveID_Sessions	PassiveID_Sessions >> Employees	PermitAccess	Employees
Sep 06, 2022 08:28:31.4...	○	📄		smith	10.10.10.10	PassiveID_Sessions	PassiveID_Sessions >> Employees	PermitAccess	

Radius 라이브 로그

Details(세부사항) 열에서 돋보기 아이콘을 클릭하여 여기에 표시된 대로 사용자(이 예에서는 smith(Domain Users))에 대한 세부 보고서를 봅니다.

Overview

Event	5236 Authorize-Only succeeded
Username	smith
Endpoint Id	10.10.10.10
Endpoint Profile	
Authentication Policy	PassiveID_Sessions
Authorization Policy	PassiveID_Sessions >> Employees
Authorization Result	PermitAccess

Authentication Details

Source Timestamp	2022-09-06 20:28:31.393
Received Timestamp	2022-09-06 20:28:31.393
Policy Server	ise-3-2
Event	5236 Authorize-Only succeeded
Username	smith
Endpoint Id	10.10.10.10
Calling Station Id	10.10.10.10
IPv4 Address	10.10.10.10
Authorization Profile	PermitAccess


Other Attributes

ConfigVersionId	108
AuthorizationPolicyMatched_	Employees
ISEPolicySetName	PassiveID_Sessions
AD-User-Resolved-Identities	smith@Lfc.lab
AD-User-Resolved-DNs	CN=smith,CN=Users,DC=Lfc,DC=lab
AD-User-DNS-Domain	Lfc.lab
AD-Groups-Names	Lfc.lab/Builtin/Administrators
AD-Groups-Names	Lfc.lab/Builtin/Remote Desktop Users
AD-Groups-Names	Lfc.lab/Builtin/Remote Management Users
AD-Groups-Names	Lfc.lab/Builtin/Users
AD-Groups-Names	Lfc.lab/Users/Denied RODC Password Replication Group
AD-Groups-Names	Lfc.lab/Users/Domain Test
AD-Groups-Names	Lfc.lab/Users/NAD Admins
AD-Groups-Names	Lfc.lab/Users/Domain Users
AD-User-NetBios-Name	Lfc
AD-User-SamAccount-Name	smith
AD-User-Qualified-Name	smith@Lfc.lab
AuthorizationSGTName	Employees
ProviderIpAddress	10.10.10.132
SessionId	cf0d2acd-0d3d-413b-b2fb-6860df3f0d84
provider	Agent
UseCase	PassiveIDAuthZOnly

Steps

15041	Evaluating Identity Policy
15013	Selected Identity Source - All_AD_Join_Points
24432	Looking up user in Active Directory - All_AD_Join_Points
24325	Resolving identity - Lfc\smith
24313	Search for matching accounts at join point - Lfc.lab
24315	Single matching account found in domain - Lfc.lab
24323	Identity resolution detected single matching account
24355	LDAP fetch succeeded - Lfc.lab
24416	User's Groups retrieval from Active Directory succeeded - All_AD_Join_Points
22037	Authentication Passed
90506	Running Authorize Only Flow for Passive ID - Provider Agent
15049	Evaluating Policy Group
15008	Evaluating Service Selection Policy
15036	Evaluating Authorization Policy
90500	New Identity Mapping
5236	Authorize-Only succeeded

수동 ID	수동태	추적	passiveid-*.log
PxGrid	pxgrid	추적	pxgrid-server.log
SXP	sxp	디버그	sxp.log

 참고: 트러블슈팅이 완료되면 디버그를 재설정하고 관련 노드를 선택한 다음 **Reset to Default**.

로그 조각

1. ISE는 공급자로부터 로그인 이벤트를 수신합니다.

Passiveid-*.log 파일:

```

2022-09-06 20:28:31,309 DEBUG [Grizzly-worker(27)][[]] com.cisco.idc.agent-probe- Received login event.
Identity Mapping.probe = Agent , dc-host = /10.10.10.132 , Identity Mapping.server = ise-3-2 , event-operation-
type = ADD ,

2022-09-06 20:28:31,309 DEBUG [Grizzly-worker(27)][[]] com.cisco.idc.agent-probe- Validating incoming logging
event...

2022-09-06 20:28:31,309 DEBUG [Grizzly-worker(27)][[]] com.cisco.idc.agent-probe- Building login event to be
published to session directory.
2022-09-06 20:28:31,309 DEBUG [Grizzly-worker(27)][[]] com.cisco.idc.agent-probe- retrieving user's additional
information from Active Directory.

2022-09-06 20:28:31,326 DEBUG [Grizzly-worker(26)][[]] com.cisco.idc.agent-probe- Forwarded login event to
session directory. Identity Mapping.id-src-first-port = -1 , Identity Mapping.dc-domainname = Lfc.lab , Identity
Mapping.id-src-port-start = -1 , Identity Mapping.probe = Agent , Identity Mapping.id-src-port-end = -1 , Identity
Mapping.event-user-name = smith , Identity Mapping.dc-host = /10.10.10.132 , Identity Mapping.agentId = ,
Identity Mapping.server = ise-3-2 , Identity Mapping.event-ip-address = 10.10.10.10 ,

```

Passiveid-*.log 파일

2. ISE는 구성된 권한 부여 정책에 따라 SGT를 할당하고 PassiveID 사용자에게 대한 IP-SGT 매핑을 PxGrid 가입자 및 SXP 피어에 게시합니다.

sxp.log 파일:


```
2022-09-06 20:28:31,587 DEBUG [sxp-service-http-96443] cisco.ise.sxp.rest.SxpGlueRestAPI:27 - Adding session binding tag=4, ip=10.10.10.10, vns=[], vpns=[null] nasIp=10.10.10.132
```

```
2022-09-06 20:28:31,587 DEBUG [sxp-service-http-96443] cisco.ise.sxp.rest.SxpGlueRestAPI:23 - session binding created for ip address : 10.10.10.10/32
```

```
2022-09-06 20:28:31,613 DEBUG [SxpNotification] cisco.cpm.sxp.engine.SxpEngine:23 - Adding 1 session bindings
```

```
2022-09-06 20:28:31,613 DEBUG [SxpNotificationSerializer-Thread] cisco.cpm.sxp.engine.SxpEngine:42 - Adding session binding RestSxpLocalBinding(tag=4, groupName=null, ipAddress=10.10.10.10/32, nasIp=10.10.10.132, sessionId=cf0d2acd-0d3d-413b-b2fb-6860df3f0d84, peerSequence=null, sxpBindingOpType=ADD, sessionExpiryTimelnMillis=-1, apic=false, routable=true, vns=[DEFAULT_VN]) to VPNs [default]
```

sxp.log 파일

pxgrid-server.log 파일:

```
2022-09-06 20:28:31,693 TRACE [Grizzly(1)][[]] cpm.pxgrid.ws.client.WsEndpoint -:::-- Send. session=[id=b0df936b-bfab-435f-80e6-aa836aa3b24c,client=~ise-fanout-ise-3-2,server=wss://ise-3-2.Lfc.lab:8910/pxgrid/ise/pubsub] frame=[command=SEND,headers=[content-length=1859, destination=/topic/distributed, from=~ise-fanout-ise-3-2, via=~ise-fanout-ise-3-2],content-len=1859] content=MESSAGE
```

```
content-length:1/30
```

```
destination:/topic/com.cisco.ise.session
```

```
message-id:616
```

```
subscription:2
```

```
via::~ise-fanout-ise-3-2
```

```
{"sessions":[{"timestamp":"2022:09:06T20:28:31.41105:00","state":"AUTHENTICATED","userName":"smith","callingStationId":"10.10.10.10","auditSessionId":"ddda40ec-e557-4457-81db-a36af7b7d4ec",
```

```
"ipAddresses":["10.10.10.10"],"nasIpAddress":"10.10.10.132" "ctsSecurityGroup":"Employees" "adNormalizedUser":"smith", "adUserDomainName":"Lfc.lab", "adUserNetBiosName":"Lfc", "adUserResolvedIdentities":"smith@Lfc.lab", "selectedAuthzProfiles":["PermitAccess"]}], "sequence":13}
```

```
2022-09-06 20:28:31,673 TRACE [Grizzly(1)][[]] cpm.pxgrid.ws.client.WsEndpoint -:::-- Send. session=[id=b0df936b-bfab-435f-80e6-aa836aa3b24c,client=~ise-fanout-ise-3-2,server=wss://ise-3-2.Lfc.lab:8910/pxgrid/ise/pubsub] frame=[command=SEND,headers=[content-length=308, destination=/topic/distributed, from=~ise-fanout-ise-3-2, via::~ise-fanout-ise-3-2],content-len=308] content=MESSAGE
```

```
content-length:176
```

```
destination:/topic/com.cisco.ise.sxp.binding
```

```
message-id:612
```

```
subscription:2
```

```
via::~ise-fanout-ise-3-2
```

```
{"operation":"CREATE","binding":{"ipPrefix":"10.10.10.10/32","tag":4, source":"10.10.10.132",
```

```
"peerSequence":["10.10.10.135,10.10.10.132"],"vpn":"default"},"sequence":17}
```

pxgrid-server.log 파일

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.