

Configurar o switch com SXP e IBNS 2.0 para redes baseadas em identidade

Contents

[Introdução](#)

[Pré-requisitos](#)

[Componentes Utilizados](#)

[Informações de Apoio](#)

[Visão Geral da Configuração da Política de Controle de Identidade](#)

[Configurar](#)

[Configuração do Switch](#)

[Configuração do ISE](#)

[Passo 1: Criar políticas de autenticação e autorização no ISE](#)

[Passo 2: Configurar um dispositivo SXP no ISE](#)

[Etapa 3: Configure a senha global em ConfiguraçõesSXPS](#)

[Verificar](#)

[Troubleshooting](#)

[Explicação de log](#)

Introdução

Este documento descreve os procedimentos para configurar os Switches Cisco com SXP e IBNS 2.0 para redes baseadas em identidade.

Pré-requisitos

Componentes Utilizados

As informações neste documento são baseadas nestas versões de software e hardware:

- Patch 4 do Identity Services Engine (ISE) versão 3.3
- Switch Cisco Catalyst 3850

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a rede estiver ativa, certifique-se de que você entenda o impacto potencial de qualquer comando.

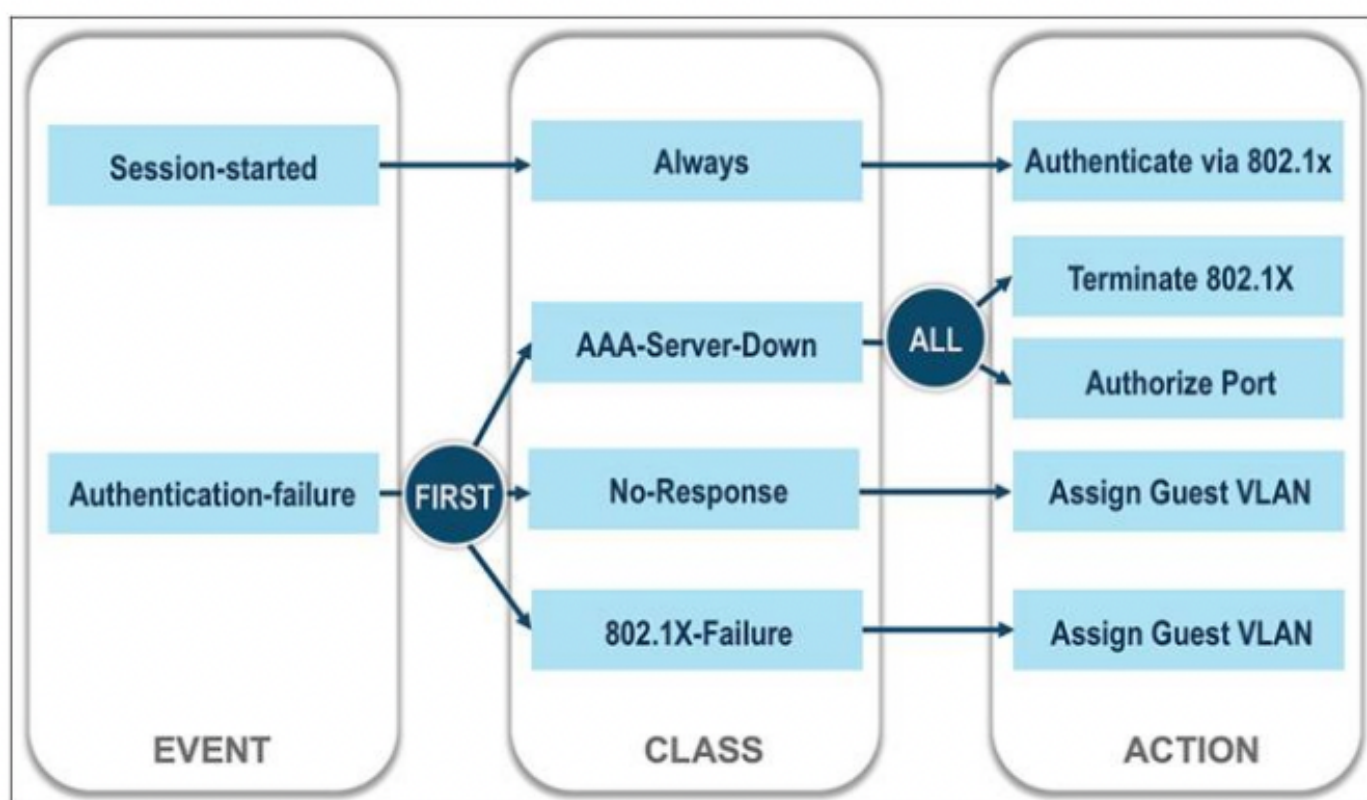
Informações de Apoio

As políticas de controle de identidade definem as ações que o Gerenciador de Sessão de Acesso

executa em resposta a condições específicas e eventos de endpoint. Usando uma linguagem de política consistente, várias ações do sistema, condições e eventos podem ser combinados para formar essas políticas.

As políticas de controle são aplicadas em interfaces e são responsáveis principalmente por gerenciar a autenticação de endpoint e ativar serviços em sessões. Cada política de controle é composta por uma ou mais regras e por uma estratégia de decisão que determina como essas regras são avaliadas.

Uma regra de política de controle inclui uma classe de controle (uma instrução de condição flexível), um evento que dispara a avaliação da condição e uma ou mais ações. Embora os administradores definam quais ações são acionadas por eventos específicos, alguns eventos vêm com ações padrão predefinidas.



Política de Controle de Identidade

Visão Geral da Configuração da Política de Controle de Identidade

As políticas de controle definem o comportamento do sistema usando um evento, uma condição e uma ação. A configuração de uma política de controle envolve três etapas principais:

1. Criar classes de controle:

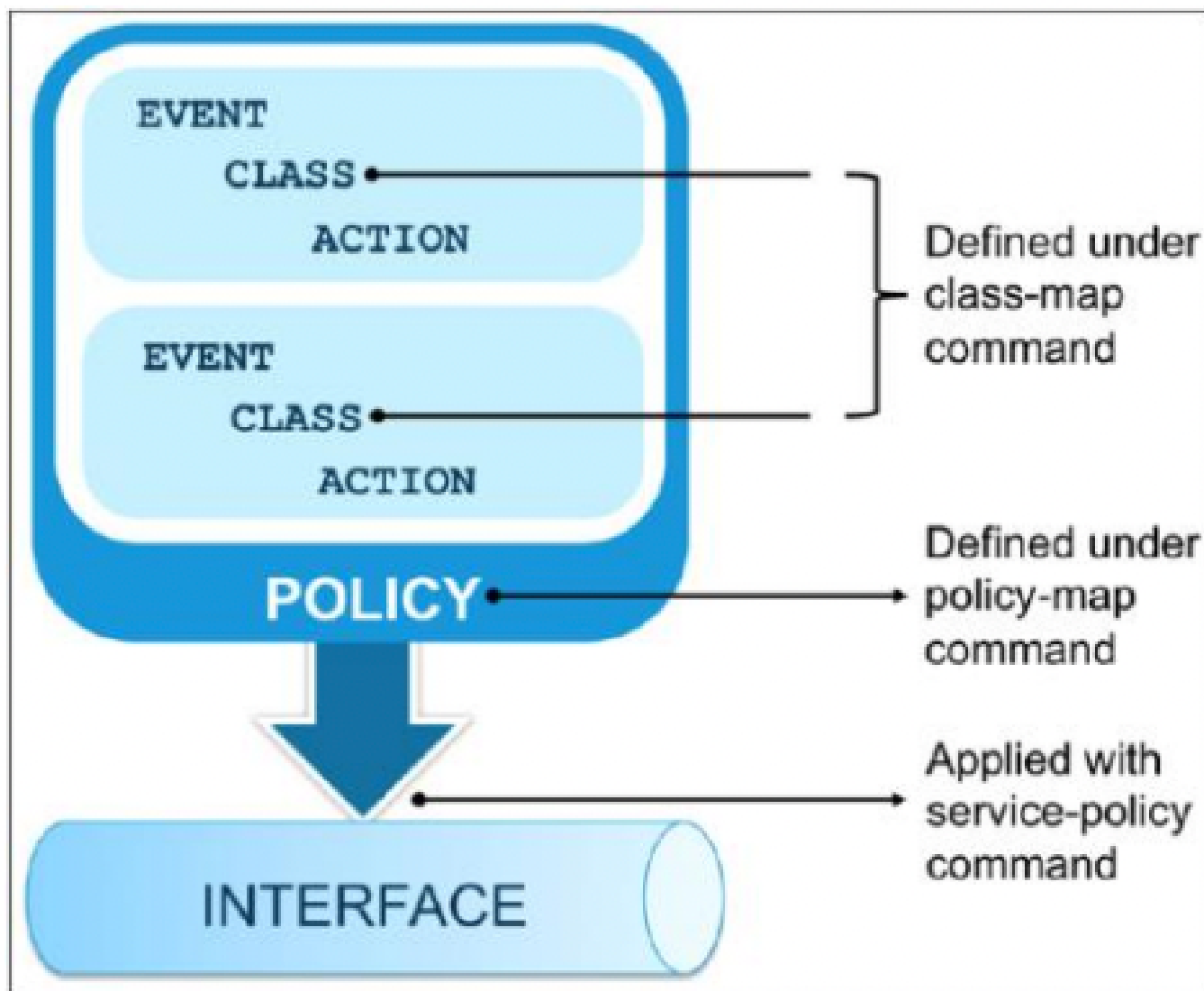
Uma classe de controle define as condições necessárias para ativar uma política de controle. Cada classe pode ter várias condições que são avaliadas como verdadeiro ou falso. Você pode definir se all, any ou none das condições devem ser verdadeiras para que a classe seja considerada verdadeira. Como alternativa, os administradores podem usar uma classe padrão que não tenha condições e sempre seja avaliada como verdadeira.

2. Crie a política de controle:

Uma política de controle contém uma ou mais regras. Cada regra inclui uma classe de controle, um evento que dispara a verificação de condição e uma ou mais ações. As ações são numeradas e executadas em ordem.

3. Aplicar a política de controle:

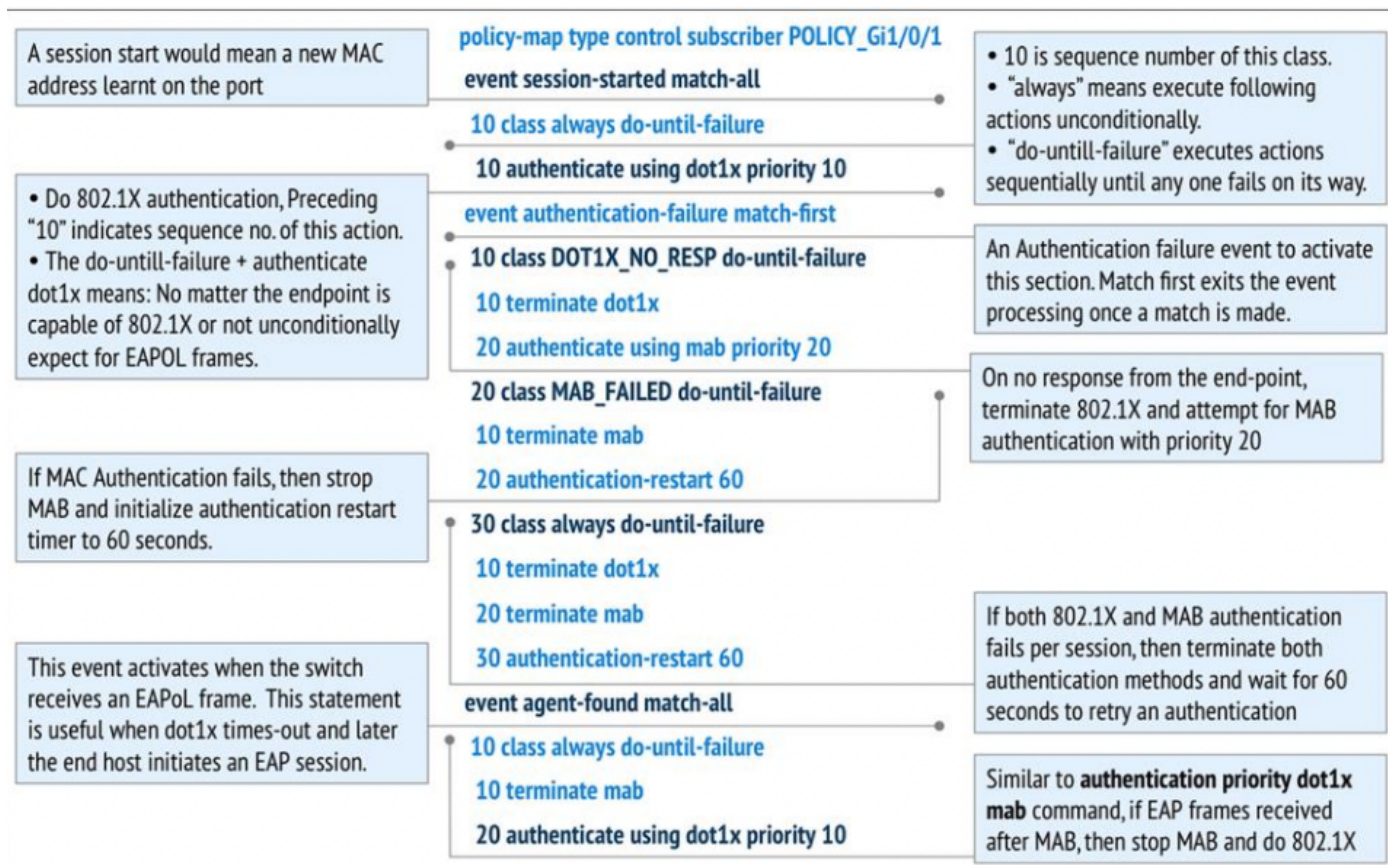
Finalmente, aplique a política de controle a uma interface para ativá-la.



Configuração da Política de Controle de Identidade

O comando `authentication display new-style` converte as configurações herdadas em um novo estilo.

```
switch#authentication display new-style
```



Interpretando a Política de Controle de Identidade

Configurar

Configuração do Switch

WS-C3850-48F-E#show run aaa

!

aaa authentication dot1x default group radius local

aaa authorization network default group radius local

username admin password 0 xxxxxx

!

!

!

!

servidor radius ISE1

address ipv4 10.127.197.xxx auth-port 1812 acct-port 1813

chave pac xxxx@123

!

!

aaa group server radius ISE2

nome do servidor ISE1

!

!

!

!

aaa new-model

aaa session-id common

!

aaa server radius dynamic-author

client 10.127.197.xxx server-key xxxx@123

dot1x system-auth-control

!

WS-C3850-48F-E#show run | em POLICY_Gi1/0/45

assinante de controle de tipo de mapa de política POLICY_Gi1/0/45

service-policy type control subscriber POLICY_Gi1/0/45

WS-C3850-48F-E#show run | sec POLICY_Gi1/0/45

assinante de controle de tipo de mapa de política POLICY_Gi1/0/45

event session-started match-all

10 classes sempre do-until-failure

10 autenticar usando dot1x priority 10

event authentication-failure match-first

5 class DOT1X_FAILED do-until-failure

10 terminam dot1x

20 authentication-restart 60

10 class DOT1X_NO_RESP do-until-failure

10 terminam dot1x

20 autenticar usando a prioridade mab 20

20 class MAB_FAILED do-until-failure

10 terminate mab

20 authentication-restart 60

40 classes sempre do-until-failure

10 terminam dot1x

20 terminate mab

30 authentication-restart 60

event agent-found match-all

10 classes sempre do-until-failure

10 terminate mab

20 autenticar usando dot1x priority 10

event authentication-success match-all

10 classes sempre do-until-failure

10 ative o modelo de serviço DEFAULT_LINKSEC_POLICY_MUST_SECURE

service-policy type control subscriber POLICY_Gi1/0/45

WS-C3850-48F-E#show run interface gig1/0/45

Criando configuração...

Configuração atual: 303 bytes

!

interface GigabitEthernet1/0/45

switchport access vlan 503

switchport mode access

access-session host-mode single-host

sessão de acesso fechada

access-session port-control auto

mab

sem aplicação de função cts

dot1x pae authenticator

service-policy type control subscriber POLICY_Gi1/0/45

fim

WS-C3850-48F-E#show run cts

!

lista de autorização de cts ISE2

cts sxp enable

cts sxp connection 10.127.197.xxx password none mode peer speaker hold-time 0 0

cts sxp default source-ip 10.196.138.yyy

senha padrão do cts sxp xxxx@123

Configuração do ISE

Passo 1: Criar políticas de autenticação e autorização no ISE

Authentication Policy(2)

Status	Rule Name	Conditions	Use	Hits	Actions
Search					
	Authentication Rule 1	Network Access-Device IP Address EQUALS 10.196.138.132	All_User_ID_Stores Options	4	
	Default		All_User_ID_Stores Options	0	
> Authorization Policy - Local Exceptions					
> Authorization Policy - Global Exceptions					

Authentication Policy(2)

Status	Rule Name	Conditions	Results	Hits	Actions
			Profiles	Security Groups	
Search					
	Authorization Rule 1	Network_Access_Authentication_Passed	PermitAccess	Select from list	3
	Default		DenyAccess	Select from list	0

Passo 2: Configurar um dispositivo SXP no ISE

Overview

Components

TrustSec Policy

Policy Sets

SXP

Integrations

Troubleshoot

Reports

Settings

SXP Devices

All SXP Mappings

SXP Devices > SXP Connection

Upload from a CSV file

Add Single Device

Input fields marked with an asterisk (*) are required.

Name

switchb1

IP Address*

10.196.138.132

Peer Role*

LISTENER

Connected PSNs*

isesec

SXP Domains*

default

Status*

Enabled

Password Type*

NONE

Password

Passo 3: Configurar a senha global nas configurações do SXP

Identity Services Engine

Work Centers / TrustSec

Bookmarks

Dashboard

Context Visibility

Operations

Policy

Administration

Work Centers

Interactive Features

Overview

Components

TrustSec Policy

Policy Sets

SXP

Integrations

Troubleshoot

Reports

Settings

General TrustSec Settings

TrustSec Matrix Settings

Work Process Settings

SXP Settings

ACI Settings

SXP Settings

☒

Publish SXP bindings on pxGrid

☒

Add Radius and PassiveID mappings into SXP IP SGT mapping table

Global Password

Global Password

This global password will be overridden by the device specific password

Timers

Verificar

Detalhes de WS-C3850-48F-E#show access-session interface gig1/0/45

Interface: GigabitEthernet1/0/45

ID IIF: 0x1A146F96

Endereço MAC: b496.9126.decc

Endereço IPv6: Desconhecido

Endereço IPv4: Desconhecido

Nome de usuário: divya123

Status: Autorizado

Domínio: DADOS

Modo de host operacional: host único

Diretório de controle operacional: ambos

Intervalo de sessão: N/A

ID de sessão comum: 0000000000000000B95163D98

ID da sessão da conta: Desconhecido

Identificador: 0x6f000001

Política atual: POLICY_Gi1/0/45

Diretivas Locais:

Modelo de serviço: DEFAULT_LINKSEC_POLICY_MUST_SECURE (prioridade 150)

Política de segurança: Deve Proteger

Status de segurança: Link não seguro

Políticas de servidor:

Lista de status do método:

Estado do método

Êxito de Autenticação dot1x

WS-C3850-48F-E#

WS-C3850-48F-E(config)#do show cts sxp conn

SXP : Habilitado

Versão mais alta suportada: 4

Senha padrão: Configurado

Cadeia de chaves padrão: não definido

Nome da cadeia de chaves padrão: Não aplicável

IP de origem padrão: 10.196.138.aaaa

Período de abertura de nova tentativa de conexão: 120 seg

Período de reconciliação: 120 seg

O timer de repetição de abertura está em execução

Limite de passagem de Peer-Sequence para exportação: não definido

Limite de passagem de Peer-Sequence para importação: não definido

IP de mesmo nível : 10.127.197.xxx

IP de origem: 10.196.138.aaaa

Status de conexão : Ligado

Versão de conversão : 4

Recurso de conexão : IPv4-IPv6-Sub-rede

Tempo de espera de conexão : 120 segundos

Modo local : Ouvinte do SXP

Conexão inst#: 1

TCP conn fd : 1

Senha TCP conn: nenhum

O temporizador de espera está em execução

Duração desde a última alteração de estado: 0:00:00:22 (dd:hr:mm:seg)

Número total de conexões SXP = 1

0xFF8CBFC090 VRF:, fd: 1, peer ip: 10.127.197.xxx

cdbp:0xFF8CBFC090 <10.127.197.145, 10.196.138.yyy> tableid:0x0

WS-C3850-48F-E(config)#

O relatório de registro ao vivo mostra a marca SGT Convidado aplicado:

Overview		Steps		
Event	5200 Authentication succeeded	Step ID	Description	Latency (ms)
Username	divya123	11001	Received RADIUS Access-Request	
Endpoint Id	B4:96:91:26:DE:CC ⓘ	11017	RADIUS created a new session	0
Endpoint Profile	Intel-Device	15049	Evaluating Policy Group	70
Authentication Policy	New Policy Set 1_copy >> Authentication Rule 1	15008	Evaluating Service Selection Policy	1
Authorization Policy	New Policy Set 1_copy >> Authorization Rule 1	11507	Extracted EAP-Response/Identity	22
Authorization Result	PermitAccess	12500	Prepared EAP-Request proposing EAP-TLS with challenge	2
		12625	Valid EAP-Key-Name attribute received	0
		11006	Returned RADIUS Access-Challenge	0
		11001	Received RADIUS Access-Request	16
		11018	RADIUS is re-using an existing session	0
		12301	Extracted EAP-Response/NAK requesting to use PEAP instead	0
		12300	Prepared EAP-Request proposing PEAP with challenge	0
		12625	Valid EAP-Key-Name attribute received	0
		11006	Returned RADIUS Access-Challenge	0
		11001	Received RADIUS Access-Request	5
		11018	RADIUS is re-using an existing session	0
		12302	Extracted EAP-Response containing PEAP challenge-response and accepting PEAP as negotiated	0
		61025	Open secure connection with TLS peer	1
		12318	Successfully negotiated PEAP version 0	0
		12800	Extracted first TLS record; TLS handshake started	2
		12805	Extracted TLS ClientHello message	1
		12806	Prepared TLS ServerHello message	0
		12807	Prepared TLS Certificate message	0
		12808	Prepared TLS ServerKeyExchange message	18
		12810	Prepared TLS ServerDone message	0
		12305	Prepared EAP-Request with another PEAP challenge	0
		11006	Returned RADIUS Access-Challenge	0
		11001	Received RADIUS Access-Request	4
		11018	RADIUS is re-using an existing session	0
		12304	Extracted EAP-Response containing PEAP challenge-response	1
		12305	Prepared EAP-Request with another PEAP challenge	0
		11006	Returned RADIUS Access-Challenge	0
		11001	Received RADIUS Access-Request	5
		11018	RADIUS is re-using an existing session	0
		12304	Extracted EAP-Response containing PEAP challenge-response	0
		12305	Prepared EAP-Request with another PEAP challenge	0
		11006	Returned RADIUS Access-Challenge	0
		11001	Received RADIUS Access-Request	8
		11018	RADIUS is re-using an existing session	0
		12304	Extracted EAP-Response containing PEAP challenge-response	1
		12318	Successfully negotiated PEAP version 0	0

Source Timestamp	2025-06-23 14:01:01.632
Received Timestamp	2025-06-23 14:01:01.632
Policy Server	isec
Event	5200 Authentication succeeded
Username	divya123
User Type	User
Endpoint Id	B4:96:91:26:DE:CC
Calling Station Id	B4-96-91-26-DE-CC
Endpoint Profile	Intel-Device
Authentication Identity Store	Internal Users
Identity Group	Profled
Audit Session Id	0000000000000000B95163D98

Endpoint Profile	Intel-Device
Authentication Identity Store	Internal Users
Identity Group	Profled
Audit Session Id	0000000000000000B95163D98
Authentication Method	dot1x
Authentication Protocol	PEAP (EAP-MSCHAPv2)
Service Type	Framed
Network Device	switchb
NAS IPv4 Address	10.196.138.132
NAS Port Id	GigabitEthernet1/0/45
NAS Port Type	Ethernet
Authorization Profile	PermitAccess
Security Group	Guests
Response Time	222 milliseconds

Troubleshooting

Ative esta depuração no switch para solucionar problemas do dot1x:

- debug dot1x all

Explicação de log

dot1x-packet:EAPOL pak rx - Ver: Tipo 0x1: 0x1 >>>> Pacote EAPoL recebido pelo switch
dot1x-packet: comprimento: 0x0000

dot1x-ev:[b496.9126.decc, cliente Gig1/0/45] detectado, evento de início de sessão de envio para b496.9126.decc >>>> cliente dot1x detectado

dot1x-ev:[b496.9126.decc, Gig1/0/45] Autenticação Dot1x iniciada para 0x26000007

(b496.9126.decc)>>>> dot1x iniciada

%AUTHMGR-5-START: Iniciando 'dot1x' para cliente (b496.9126.decc) na Interface Gig1/0/45
AuditSessionID 0A6A258E0000003500C9CFC3

dot1x-sm:[b496.9126.decc, Gig1/0/45] Posting !EAP_RESTART on Client 0x26000007 />>>>
Solicitando que o cliente reinicie o Processo EAP

dot1x-sm:[b496.9126.decc, Gig1/0/45] Postando RX_REQ no Cliente 0x26000007 >>>>
aguardando o pacote EAPoL do cliente

dot1x-sm:[b496.9126.decc, Gig1/0/45] Postando AUTH_START para 0x26000007 >>>> Iniciando
processo de autenticação

dot1x-ev:[b496.9126.decc, Gig1/0/45] Enviando pacote EAPOL >>>> Solicitação de identidade

dot1x-packet:EAPOL pak Tx - Ver: Tipo 0x3: 0x0

dot1x-packet: comprimento: 0x0005

dot1x-packet:código EAP: id 0x1: Comprimento 0x1: 0x0005

dot1x-packet: digite: 0x1

dot1x-packet:[b496.9126.decc, Gig1/0/45] pacote EAPOL enviado ao cliente 0x26000007

dot1x-ev:[Gig1/0/45] pkt recebido saddr =b496.9126.decc , daddr = 0180.c200.0003, tipo éter-pae
= 888e.0100.000a

dot1x-packet:EAPOL pak rx - Ver: Tipo 0x1: 0x0 // Resposta de identidade

dot1x-packet: comprimento: 0x000A

dot1x-sm:[b496.9126.decc, Gig1/0/45] Postando EAPOL_EAP para 0x26000007 >>>> Pacote
EAPoL (Resposta EAP) recebido, preparando solicitação para o servidor

dot1x-sm:[b496.9126.decc, Gig1/0/45] Postando EAP_REQ para 0x26000007 >>>> Resposta do
servidor recebida, Solicitação EAP está sendo preparada

dot1x-ev:[b496.9126.decc, Gig1/0/45] Enviando pacote EAPOL

dot1x-packet:EAPOL pak Tx - Ver: Tipo 0x3: 0x0

dot1x-packet: comprimento: 0x0006

dot1x-packet:código EAP: id 0x1: Comprimento 0xE5: 0x0006

dot1x-packet: digite: 0xD

dot1x-packet:[b496.9126.decc, Gig1/0/45] pacote EAPOL enviado ao cliente 0x26000007 >>>>
solicitação EAP enviada

dot1x-ev:[Gig1/0/45] pkt recebido saddr =b496.9126.decc , daddr = 0180.c200.0003, tipo ether-
pae = 888e.0100.0006 //Resposta EAP recebida

dot1x-packet:EAPOL pak rx - Ver: Tipo 0x1: 0x0

dot1x-packet: comprimento: 0x0006

||

||

||

|| Aqui muitos eventos EAPOL-EAP e EAP_REQ ocorrem porque muitas informações são

trocadas entre o switch e o cliente

|| Se os eventos posteriores a este não se seguirem, então os temporizadores e as informações enviadas até agora precisam ser verificados

||

||

||

dot1x-packet:[b496.9126.decc, Gig1/0/45] Recebeu um Êxito de EAP >>>> Êxito de EAP recebido do Servidor

dot1x-sm:[b496.9126.decc, Gig1/0/45] Posting EAP_SUCCESS for 0x26000007 >>>> Posting EAP Success event

dot1x-sm:[b496.9126.decc,Gig1/0/45] Posting AUTH_SUCCESS on Client 0x26000007 >>>> Posting Authentication success

%DOT1X-5-SUCCESS: Autenticação bem-sucedida para cliente (b496.9126.decc) na Interface Gig1/0/45 AuditSessionID 0A6A258E0000003500C9CFC3

dot1x-packet:[b496.9126.decc, Gig1/0/45] Dados da chave EAP detectados ao adicionar à lista de atributos >>>> Dados adicionais da chave detectados enviados pelo servidor

%AUTHMGR-5-SUCCESS: Autorização bem-sucedida para cliente (b496.9126.decc) na Interface Gig1/0/45 AuditSessionID 0A6A258E0000003500C9CFC3

dot1x-ev:[b496.9126.decc, Gig1/0/45] Recebeu Êxito de Autorização para o cliente 0x26000007 (b496.9126.decc) >>>> Êxito de Autorização

dot1x-ev:[b496.9126.decc, Gig1/0/45] Enviando pacote EAPOL >>>> Enviando sucesso EAP ao cliente

dot1x-packet:EAPOL pak Tx - Ver: Tipo 0x3: 0x0

dot1x-packet: comprimento: 0x0004

dot1x-packet:código EAP: id 0x3: Comprimento 0xED: 0x0004

dot1x-packet:[b496.9126.decc, Gig1/0/45] pacote EAPOL enviado ao cliente 0x26000007

Sobre esta tradução

A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês ([link fornecido](#)) seja sempre consultado.