Windows Serverを使用したCatalyst Centerでの 外部認証の設定

内容
<u>はじめに</u>
前提条件
<u>要件</u>
<u>使用するコンポーネント</u>
<u>設定</u>
管理者ロールポリシー
<u>オブザーバロールポリシー。</u>
外部認証の有効化

はじめに

このドキュメントでは、Windows Serverのネットワークポリシーサーバ(NPS)をRADIUSとして 使用して、Cisco DNA Center(DNA Center)で外部認証を設定する方法について説明します。

前提条件

要件

次の項目に関する基礎知識

- ・ Cisco DNA Centerのユーザとロール
- Windows Serverネットワークポリシーサーバ、RADIUSおよびActive Directory

使用するコンポーネント

- Cisco DNA Center 2.3.5.x
- ドメインコントローラ、DNSサーバ、NPS、およびActive Directoryとして機能する Microsoft Windows Serverバージョン2019

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このド キュメントで使用するすべてのデバイスは、クリアな(デフォルト)設定で作業を開始していま す。本稼働中のネットワークでは、各コマンドによって起こる可能性がある影響を十分確認して ください。



注:Cisco Technical Assistance Center(TAC)は、Microsoft Windows Serverに対するテク ニカルサポートを提供しません。 Microsoft Windows Serverの設定に関する問題が発生し た場合は、Microsoftサポートにテクニカルサポートを要請してください。

設定

管理者ロールポリシー

1. WindowsのStartメニューをクリックして、NPSを検索します。次に、Network Policy Serverを選択します。



Network Policy Server

Desktop app



Windowsネットワークポリシーサービス

- 3. OKを2回クリックします。
- 4. RADIUS Clients and Serversを展開し、RADIUS Clientsを右クリックして、Newを選択します。



```
RADIUSクライアントの追加
```

5. フレンドリ名、Cisco DNA Center管理IPアドレス、および共有秘密を入力します(これは 後で使用できます)。

Settings Advanced	
Enable this RADIUS client	
Select an existing template:	
	\sim
Name and Address	
Friendly name:	
DNAC	
Address (IP or DNS):	
10.88.244.160	Verfy
Shared Secret	
Select an existing Shared Secrets template:	
None	~
To manually type a shared secret, click Manual. To automatically gene secret, click Generate. You must configure the RADIUS client with the secret entered here. Shared secrets are case-sensitive. Generate Shared secret:	rate a shared same shared
To manually type a shared secret, click Manual. To automatically gene secret, click Generate. You must configure the RADIUS client with the secret entered here. Shared secrets are case-sensitive. Manual Generate Shared secret:	rate a shared same shared
To manually type a shared secret, click Manual. To automatically gene secret, click Generate. You must configure the RADIUS client with the secret entered here. Shared secrets are case-sensitive. Manual Generate Shared secret: Confirm shared secret:	rate a shared same shared
To manually type a shared secret, click Manual. To automatically gene secret, click Generate. You must configure the RADIUS client with the secret entered here. Shared secrets are case-sensitive.	rate a shared same shared
To manually type a shared secret, click Manual. To automatically gene secret, click Generate. You must configure the RADIUS client with the secret entered here. Shared secrets are case-sensitive.	rate a shared same shared

Radiusクライアントの設定

- 6. OKをクリックして保存します。
- 7. Policiesを展開して、Network Policiesを右クリックし、Newを選択します。



8. ルールのポリシー名を入力し、Nextをクリックします。

New Network Policy

	Specify Network Policy Name and Connection Type You can specify a name for your network policy and the type of connections to which the policy is applied.
Policy name	r.
DNAC-Admin-	Policy
Network conne Select the type type or Vendor select Unspec	ection method e of network access server that sends the connection request to NPS. You can select either the network access server r specific, but neither is required. If your network access server is an 802.1X authenticating switch or wireless access point, afied.
Type of net	twork access server:
Unspecific	ed v
Vendor spe	eofic:
	Previous Next Finish Cancel

ポリシー名

o

9. 特定のドメイングループを許可するには、次の2つの条件を追加してNextをクリックします

- ユーザグループ:Cisco DNA Centerで管理者ロールを持つことができるドメイングループを追加します(この例では、Sup_Ad_NPSグループを使用)。
- ・ ClientIPv4Address:Cisco DNA Center管理IPアドレスを追加します。

en menter energ	
Specify the o	Conditions conditions that determine whether this network policy is evaluated for a connection request. A mini tion is required.
Conditions:	
Condition	Value
🚇 User Groups	DNAWEST\Sup_Ad_NPS
🕎 Clent IPv4 Address	10.88.244.160
Condition description:	
Condition description: The Client IP Address conditio	on specifies the IP address of the RADIUS client that forwarded the connection request to NPS.
Condition description: The Client IP Address conditio	on specifies the IP address of the RADIUS client that forwarded the connection request to NPS.
Condition description: The Client IP Address conditio	on specifies the IP address of the RADIUS client that forwarded the connection request to NPS.
andition description: The Client IP Address conditio	on specifies the IP address of the RADIUS client that forwarded the connection request to NPS. Add Edt
andition description: The Client IP Address conditio	on specifies the IP address of the RADIUS client that forwarded the connection request to NPS. Add Edt Remove
andition description: The Client IP Address conditio	on specifies the IP address of the RADIUS client that forwarded the connection request to NPS. Add Edt Remove
andition description: The Client IP Address conditio	on specifies the IP address of the RADIUS client that forwarded the connection request to NPS. Add Edt Remove

ポリシーの条件

10. Access Grantedを選択し、Nextをクリックします。

New Network	Policy ×
	Specify Access Permission Configure whether you want to grant network access or deny network access if the connection request matches this policy.
 Access gra Grant acces Access der Deny acces 	nted ss if client connection attempts match the conditions of this policy. nied ss if client connection attempts match the conditions of this policy.
Access is d Grant or der	letermined by User Dial-in properties (which override NPS policy) ny access according to user dial-in properties if client connection attempts match the conditions of this policy.
	Previous Next Finish Cancel

使用アクセス権の付与

11. Unencrypted authentication (PAP, SPAP)のみを選択します。

1

Configure Authentication Methods
Configure one or more authentication methods required for the connection request to match this policy. For EAP authentication, you must configure an EAP type.

EAP Types:	Move Up Move Down
Add Edt Remove Less secure authentication methods: Morosoft Encrypted Authentication version 2 (MS-CHAP-v/2) User can change password after it has expired Microsoft Encrypted Authentication (MS-CHAP) User can change password after it has expired How clients to connect without negotiating an authentication methods Allow clients to connect without negotiating an authentication methods	ethod.
	Previous Next Finish Cancel

Unencrypted authenticationを選択します

12. デフォルト値が使用されるため、Nextを選択します。



Configure Constraints

Constraints are additional parameters of the network policy that are required to match the connection request. If a constraint is not matched by the connection request, NPS automatically rejects the request. Constraints are optional; if you do not want to configure constraints, click Next.

Configure the constraints for this network policy. If all constraints are not matched by the connection request, network access is denied.

Constraints:	
Constraints	Specify the maximum time in minutes that the server can remain idle before the connection
😼 Ide Tineout	is disconnected
Session Timeout	Disconnect after the maximum idle time
Called Station ID	
Day and time restrictions	· •
T NAS Port Type	
	1
	Previous Next Finish Cancel

Configure Constraintウィンドウ

13. 標準属性を削除:

Ì	New Network Policy	×
	Configure Settings NPS applies settings to the connection request if all of the network policy matched.	conditions and constraints for the policy an
	Configure the settings for this network policy. If conditions and constraints match the connection request and the policy grants access, settin Settings:	igs are applied.
1	RADIUS Attributes Standard Image: Standard Image: Standard Image: Vendor Specific Routing and Remote Access Image: Mublick and Bandwidth Allocation Protocol (BAP) Image: IP Filters Image: Enception Image: IP Setting:	ct a RADIUS standard attribute, and is not sent to RADIUS clients. See utes.
1.	Add Edt Remove	
	s c Previous N	ext Finish Cancel

14. RADIUS Attributesで、Vendor Specificを選択し、Addをクリックし、Ciscoをベンダーとし て選択し、Addをクリックします。

使用する属性の定義

To add an attribute to the settings, select the attribute, and then click Add. To add a Vendor Specific attribute that is not listed, select Custom, and then click Add. Vendor: Cisco Attributes: Name Vendor Cisco-AV-Pair Cisco Description: Specifies the Cisco AV Pair VSA. Add Oracle	Add Vendor Specific Attribute		
Attributes: Attributes: Oisco-AV-Pair Oisco Description: Specifies the Oisco AV Pair VSA. Add Oose	To add an attribu To add a Vendor Vendor	te to the settings, select the attribute, and then click Add. Specific attribute that is not listed, select Custom, and then click Add.	
Atributes: Name Vendor Cisco-AV-Pair Cisco Description: Specifies the Cisco AV Pair VSA. Add Close	Cisco	\sim	
Name Vendor Cisco-AV-Pair Cisco Description: Specifies the Cisco AV Pair VSA. Add Close	Attributes:		
Specifies the Cisco AV Pair VSA. Add Close	Name Cisco-AV-Pair	Vendor Cisco	
	Specifies the Cis	co AV Pair VSA. Add Close	

```
Cisco AVペアの追加
```

15. Addをクリックし、Role=SUPER-ADMIN-ROLEと入力して、OKを2回クリックします。

New Network Policy

	Configure S	ettings
	NPS applies setting matched.	is to the connection request if all of the network policy conditions and constraints for the policy a
Configure the s If conditions an	ettings for this network nd constraints match th	: policy. re connection request and the policy grants access, settings are applied.
Settings:		
RADIUS AL	tributes	To send additional attributes to RADIUS clients, select a Vendor Specific attribute, and
🚳 Standar	d	then click Edit. If you do not configure an attribute, it is not sent to RADIUS clients. See
Vendor	Specific	your HAUTUS client documentation for required attributes.
Routing an Access	dRemote	Million datas
Bandwid	: and dth Allocation	New Yorks Mar
Protoco	(BAP)	Name Vencor Value
🍸 IP Filter	8	Cisco-AV-Par Cisco Hole+SUPER-ADMIN-HOLE
🔒 Encrypti	ion	
IP Sette	0.00	
99		
		Add Edit Remove
		Previous Next Exists Cancel
		THE THE CONTRACT

Cisco AVペア属性が追加されました

16. Closeを選択してからNextを選択します。

17. ポリシー設定を確認し、Finishを選択して保存します。

Completing New Network Policy

You have successfully created the following network policy:

DNAC-Admin-Policy

ļ	Policy conditions:	
	Condition	Value
l	User Groups	DNAWEST\Sup_Ad_NPS
l	Client IPv4 Address	10.88.244.160

Policy settings:

Condition	Value
Authentication Method	Encryption authentication (CHAP)
Access Pemission	Grant Access
Ignore User Dial-In Properties	False
Cisco-AV-Pair	Role=SUPER-ADMIN-ROLE

To close this wizard, click Finish.				
	Previous	Next	Rnish	Cancel

ポリシーの概要

オブザーバロールポリシー。

- 1. WindowsのStartメニューをクリックして、NPSを検索します。次に、Network Policy Serverを選択します。
- 2. 左側のナビゲーションパネルで、NPS (ローカル)オプションを右クリックし、Register server in Active Directoryを選択します。
- 3. OKを2回クリックします。
- 4. RADIUS Clients and Serversを展開して、RADIUS Clientsを右クリックし、Newを選択します。
- 5. フレンドリ名、Cisco DNA Center管理IPアドレス、および共有秘密を入力します(これは 後で使用できます)。
- 6. OKをクリックして保存します。

×

- 7. Policiesを展開して、Network Policiesを右クリックし、Newを選択します。
- 8. ルールのポリシー名を入力し、Nextをクリックします。
- 9. 特定のドメイングループを許可するには、次の2つの条件を追加してNextを選択します。
 - User Group:Cisco DNA Centerでオブザーバロールを割り当てるために、ドメイング ループを追加します(この例ではObserver NPSグループを使用)。
 - ・ ClientIPv4Address:Cisco DNA Center管理IPを追加します。
- 10. Access Grantedを選択してからNextを選択します。
- 11. Unencrypted authentication (PAP, SPAP)だけを選択します。
- 12. デフォルト値が使用されるため、Nextを選択します。
- 13. Standard属性を削除します。
- 14. RADIUS Attributesで、Vendor Specificを選択し、Addをクリックし、ベンダーとして Ciscoを選択し、Addをクリックします。
- 15. Addを選択し、ROLE=OBSERVER-ROLEと入力して、OKを2回押します。
- 16. Close、Nextの順に選択します。
- 17. ポリシー設定を確認し、Finishを選択して保存します。

外部認証の有効化

1. WebブラウザでCisco DNA Centerのグラフィカルユーザインターフェイス(GUI)を開き、 admin特権アカウントを使用してログインします。

	and the second
cisco	
Cisco DNA Center	
The bridge to possible	
Username	
Password	
Log In	

Cisco DNA Centerログインページ

2. Menu > System > Setting > Authentication and Policy Serversの順に移動し、Add > AAAの 順に選択します。

Authentication and Policy Servers

Use this form to specify the servers that authenticate Cisco DNA Center users. Cisco Identity Services Engine (ISE) servers can also supply policy and user information.

9	⊕ Add ∧	1 Export	
	AAA	1	Protocol
	ISE	4.189	RADIUS_TACACS

Windows Serverの追加

3. Windows ServerのIPアドレスと前の手順で使用した共有秘密を入力し、Saveをクリックします。

Add AAA server

Server IP Address*

10.88.244.148

Shared Secret*

SHOW

 \times



Advanced Settings

Cancel



Windows Serverの値

4. Windows ServerのステータスがActiveであることを確認します。

10.88.244.148	RADIUS	AAA	ACTIVE	

Windows Serverの概要

5. Menu > System > Users & Roles > External Authenticationの順に移動し、AAAサーバを選択 します。

AAA Server(s)

Primary AAA Server

IP Address

10.88.244.148

Shared Secret

Info

View Advanced Settings

Update

AAAサーバとしてのWindowsサーバ

6. AAA属性としてCisco-AVPairと入力し、Updateをクリックします。



7. Enable External Userチェックボックスをクリックして、外部認証を有効にします。



確認

Cisco DNA Centerのグラフィカルユーザインターフェイス(GUI)をWebブラウザで開き、 Windowsサーバで設定した外部ユーザでログインして、外部認証を使用して正常にログインでき ることを確認できます。



Cisco DNA Centerログインページ

翻訳について

シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人に よる翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっ ても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性につ いて法的責任を負いません。原典である英語版(リンクからアクセス可能)もあわせて参照する ことを推奨します。