H3Cスイッチと

Windows Server 2016 NPS認証サーバー統合ガイド

内容

序

このドキュメントでは、ユーザークセス認証のためにH3CスイッチをWindows Server 2016 NPSサーバーと統合する例を示します。このドキュメントでは、次の認証および承認機能の例を示します。:

- MAC認証
- 802.1X認証
- ポータル認証
- 許可VLANの割り当て
- 許可ACLの割り当て。
- 承認ユーザープロファイルの割り当て

認証および承認機能のサポートは、デバイスモデルによって異なります。詳細については、スイッチのセキュリティコンフィギュレーションガイドを参照してください。

認証方法におけるH3CスイッチとWindows Server 2016 NPSの互換性

H3Cスイッチ	Windows Server 2016 NPSの場合	互換性
共有ユーザーカウントによるMAC認証	CHAP認証	はい
MACauthenticationwith MACベースのユーザーカウント	CHAP認証	はい
802.1X CHAP認証	CHAP認証	はい
802.1X PAP認証	PAP認証	はい
802.1X EAP認証	EAP-PEAP認証	はい
ローカルポータル+LDAP認証	CHAP認証	はい
認可VLAN	• VLAN ID許可 • VLAN名の許可 • VLANグループ名の許可 • マルチVLAN許可 • Auto VLAN authorization (タグ属性を使用したVLAN許可)	はい
許可ACL	許可スタティックACL	はい
Authorizationユーザープロファイル	Authorizationユーザープロファイル	はい

前提条件

次の情報は、H3Cスイッチに適用されます。例の手順と情報は、スイッチのソフトウェアまたはハードウェアのバージョン、およびWindows Server 2016 NPSサーバーのソフトウェアバージョンによって若干異なる場合があります。

設定例はラボ環境で作成および検証され、すべてのデバイスは工場出荷時のデフォルト設定で起動されました稼働中のネットワークで作業している場合は、すべての構成項目がネットワークに及ぼす潜在的な影響を理解していることを確認してくださいこと

例:MAC認証の構成

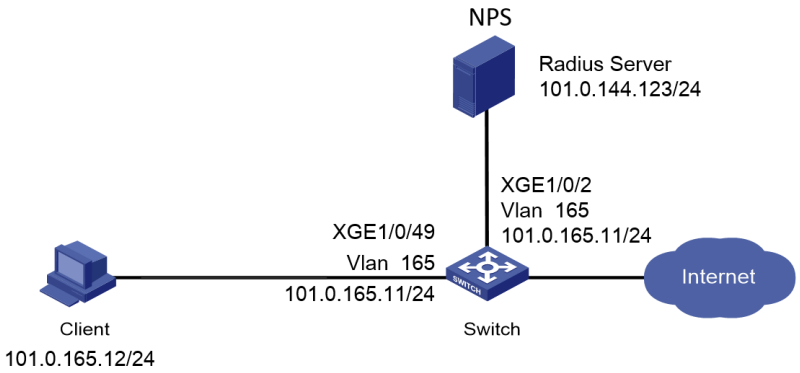
ネットワーク設定

図1に示すように、Windows Server 2016 NPSサーバーと連動してクライアントでMAC認証を実行するようにスイッチを構成しますクライアントは、ネットワークリソースにアクセスするためにMAC認証に合格する必要があります

次のようにスイッチを構成します

- NPSサーバーをRADIUSサーバーとして使用して、クライアントのMAC認証を実行します。
- すべてのMAC認証ユーザーに指定されたユーザー名とパスワードを使用して共有アカウントを作成するか、クライアントのMACアドレスをMAC認証のユーザー名とパスワードとして使用します。

図1 ネットワークダイアグラム



使用されるソフトウェアのバージョン

この設定例は、次のハードウェアおよびソフトウェアバージョンで作成され、検証されています。

ハードウェア	ソフトウェアのバージョン
S5560X-54C-PWR-EIスイッチ	バージョン7.1.070
認証サーバー	Windows Server 2016 NPSの場合

例:共有ユーザーカウントを使用したMAC認証の設定

前提条件

この例では、認証の設定だけを示します。クライアント、スイッチ、およびサーバーが相互に通信するためのネットワーク接続を持っていることを確認します。

スイッチの設定

#RADIUSスキームradius1を作成し、ユーザー認証およびアカウンティング用にNPSサーバーを101.0.144.123に指定し、プレーンテキスト形式で共有キーを**admin**に設定し、RADIUSサーバーに送信されるユーザー名からドメイン名を除外します。

<Switch> system-view

[Switch] radius scheme radius1

[Switch-radius-radius1] primary authentication 101.0.144.123

[Switch-radius-radius1] primary accounting 101.0.144.123

[Switch-radius-radius1] key authentication simple admin

[Switch-radius-radius1] key accounting simple admin

[Switch-radius-radius1] user-name-format without-domain

[Switch-radius-radius1] quit

#MAC認証にCHAPを使用するようにスイッチを設定します。

[Switch] mac-authentication authentication-method chap

#ISPドメインmac-authを作成し、認証、認可、およびアカウンティングのためにRADIUSスキームをISPドメインに適用します。

[Switch] domain mac-auth

[Switch-isp-mac-auth] authentication default radius-scheme radius

[Switch-isp-mac-auth] authorization default radius-scheme radius1

[Switch-isp-mac-auth] accounting default radius-scheme radius1

[Switch-isp-mac-auth] quit

#VLAN 165とVLAN-interface 165を作成し、VLANインターフェイスにIPアドレスを割り当てます。

[Switch] vlan 165

[Switch-vlan165] quit

[Switch] interface Vlan-interface 165

[Switch-Vlan-interface165] ip address 101.0.165.11 255.255.255.0

[Switch-Vlan-interface165] quit

#Ten-GigabitEthernet 1/0/49をVLAN 165に割り当て、Ten-GigabitEthernet 1/0/49でMAC認証をイネーブルにします。

[Switch]interface Ten-GigabitEthernet 1/0/49

[Switch-Ten-GigabitEthernet1/0/49] port access vlan 165

[Switch-Ten-GigabitEthernet1/0/49] mac-authentication

[Switch-Ten-GigabitEthernet1/0/49] quit

#ISPドメインmac-authをデフォルトのISPドメインとして指定します。

[Switch] domain default enable mac-auth

#MAC認証ドメインとしてISPドメインmac-authを指定します。

[Switch] mac-authentication domain mac-auth

#MAC認証用のオフライン検出およびクワイエットタイマーを設定します。

[Switch] mac-authentication timer offline-detect 180

[Switch] mac-authentication timer quiet 180

#MAC認証ユーザーが共有するアカウントのユーザー名**user**とパスワード**123456**をプレーンテキスト形式で指定します。

[Switch] mac-authentication user-name-format fixed account user password simple 123456

#MAC認証をグローバルにイネーブルにします。

[Switch]mac-authentication

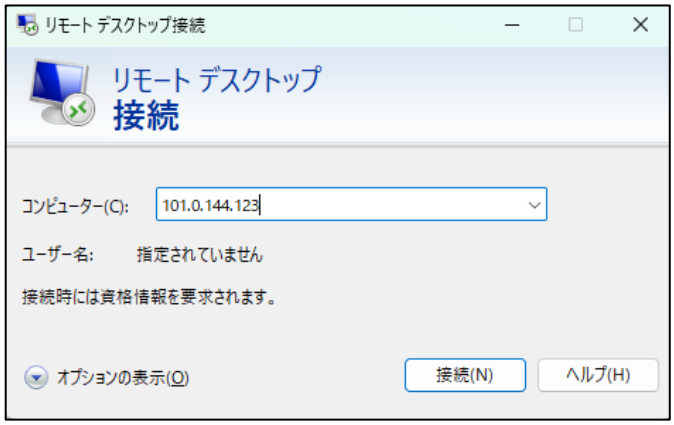
Windows Server 2016 NPSサーバーの構成

1. Windows Server 2016 NPSサーバーにログインします。

   #クライアントの**リモートデスクトップ接続**を開き、**コンピューター**フィールドにNPSサーバーの管理IPアドレスを入力し、**接続**をクリックします。

   この例では、コンピューターのIPアドレスは**101.0.144.123**です。

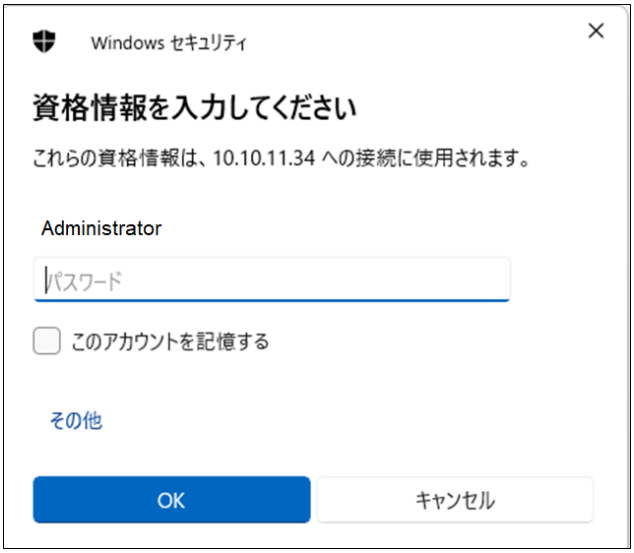
   図2 リモートデスクトップ接続



   #開いたウィンドウで、NPSサーバーにログインするためのユーザー名とパスワードを入力し、**OK**をクリックします。

この例では、ユーザー名は**Administrator**、パスワードは**admin@123456**です。

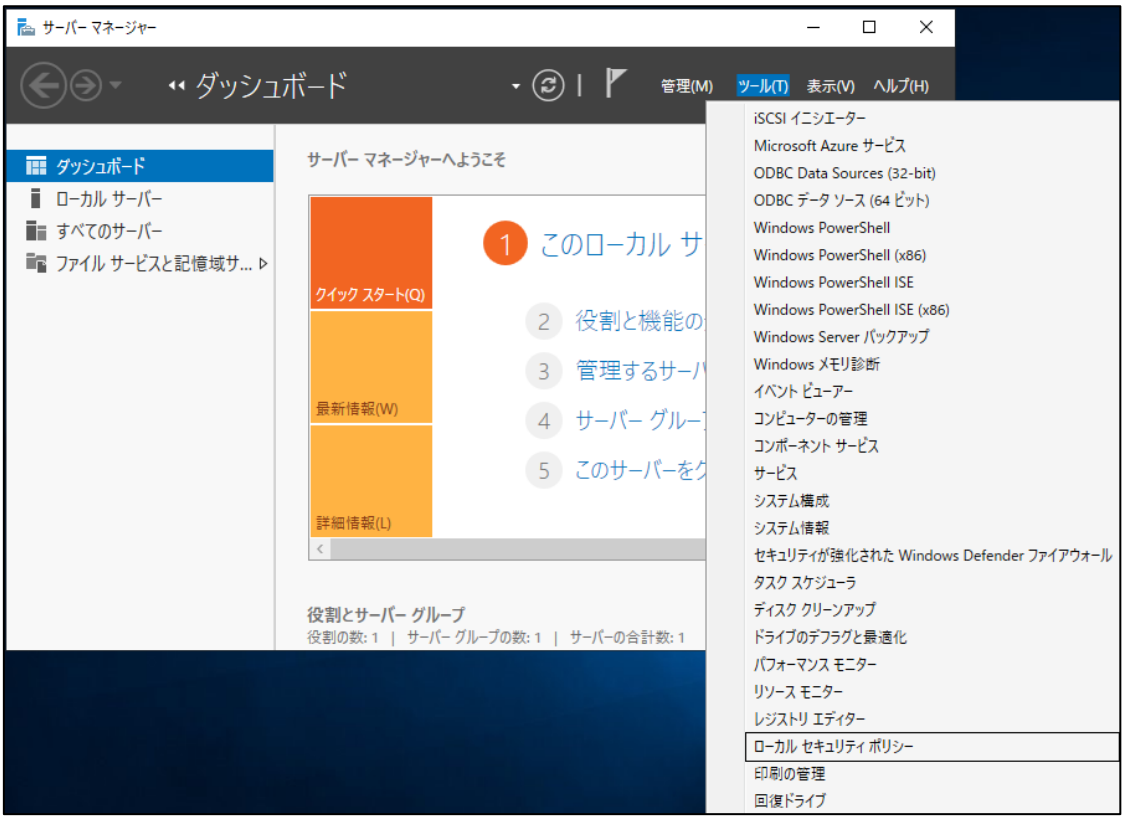
図3 ログインユーザー名とパスワードの入力



2. ローカルセキュリティポリシーを設定します。

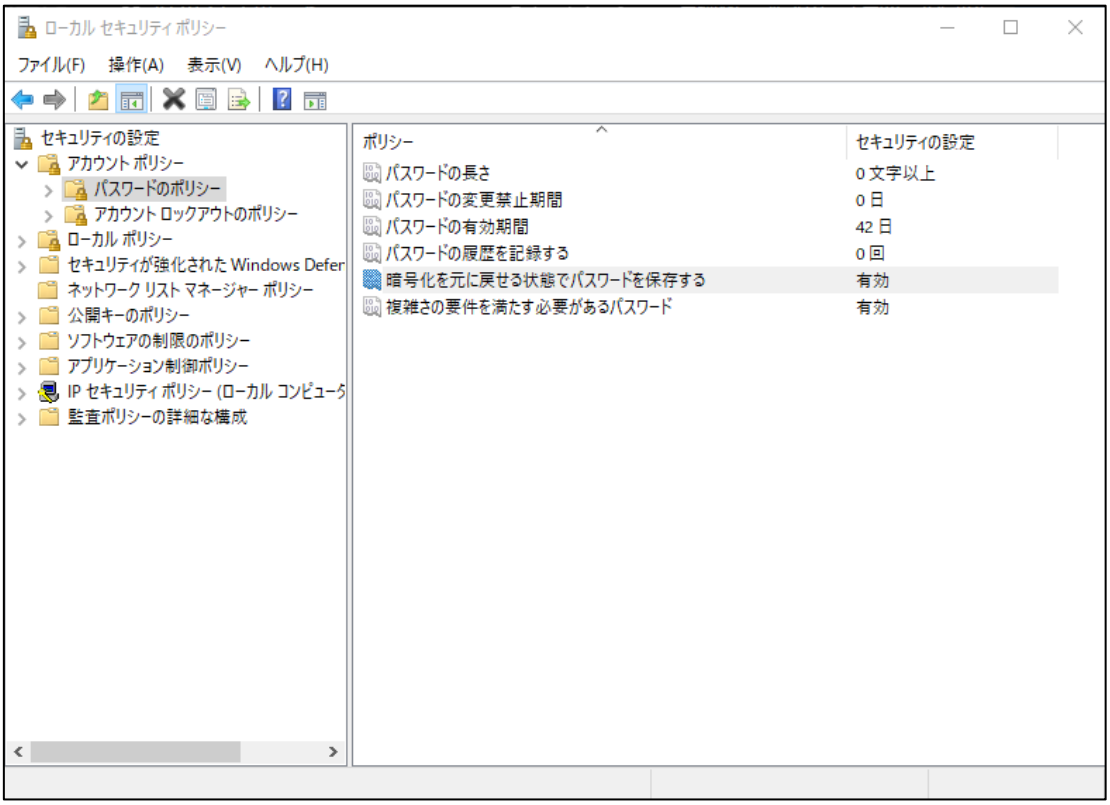
サーバーマネージャーのダッシュボードで、**ツール > ローカルセキュリティポリシー**を選択します。

図4 ローカルセキュリティポリシーの設定



#表示された**ローカルセキュリティポリシー**ウィンドウで、左側のナビゲーションペインの**パスワードのポリシー**を選択します。**複雑さの要件を満たす必要があるパスワード**フィールドでは**無効**に設定し、**暗号化を元に戻せる状態でパスワードを保存する**フィールドでは**有効**に設定します。

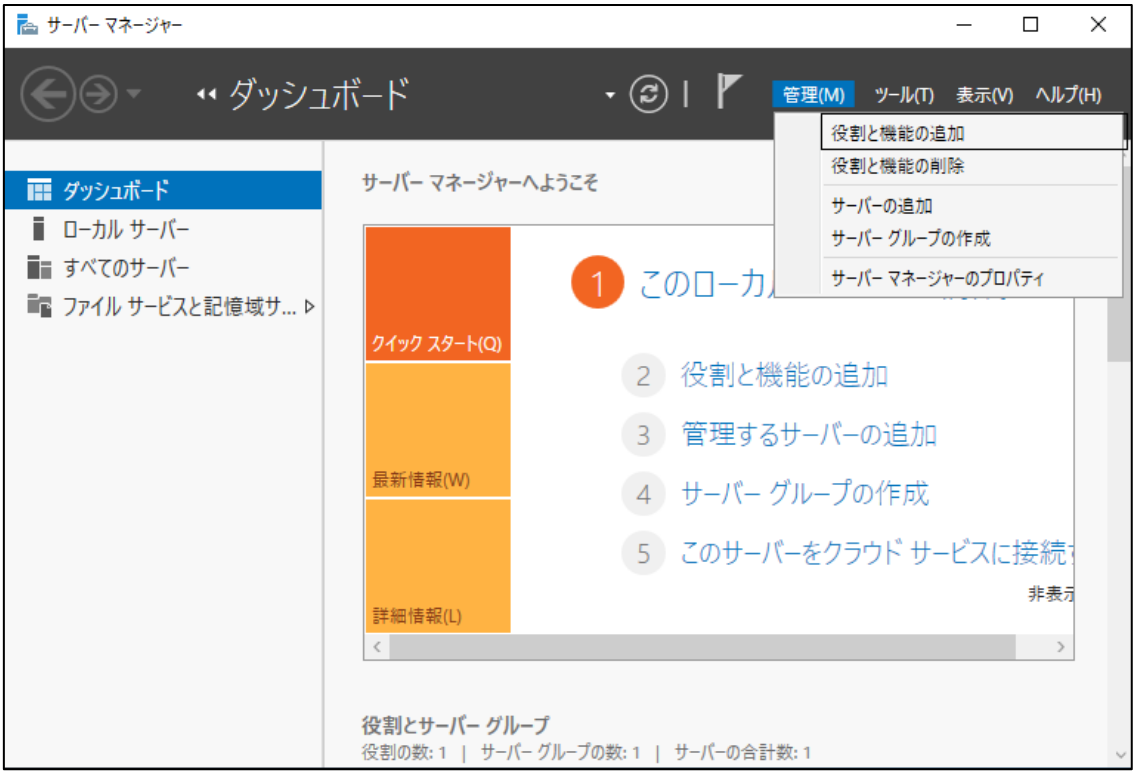
図5 パスワードポリシーの設定



3. 役割と機能を追加する:

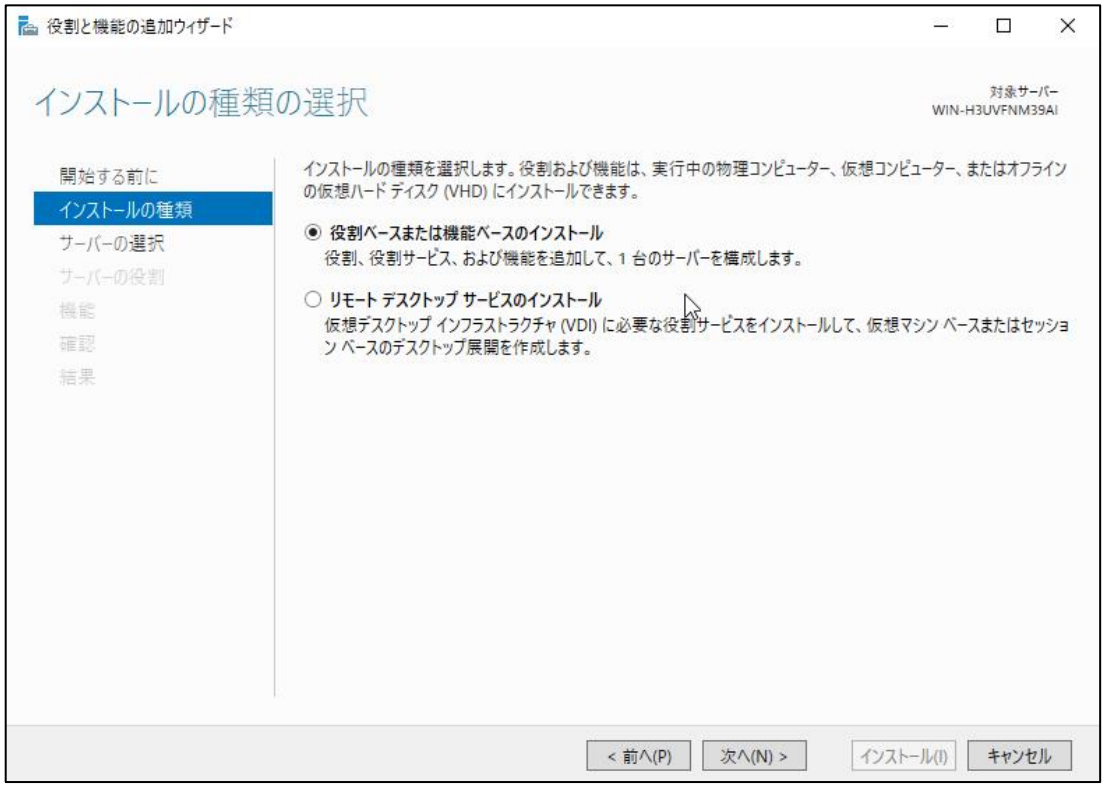
#**サーバーマネージャー**の**ダッシュボード**で、**管理 > 役割と機能の追加**を選択します。

図6 役割と機能の追加



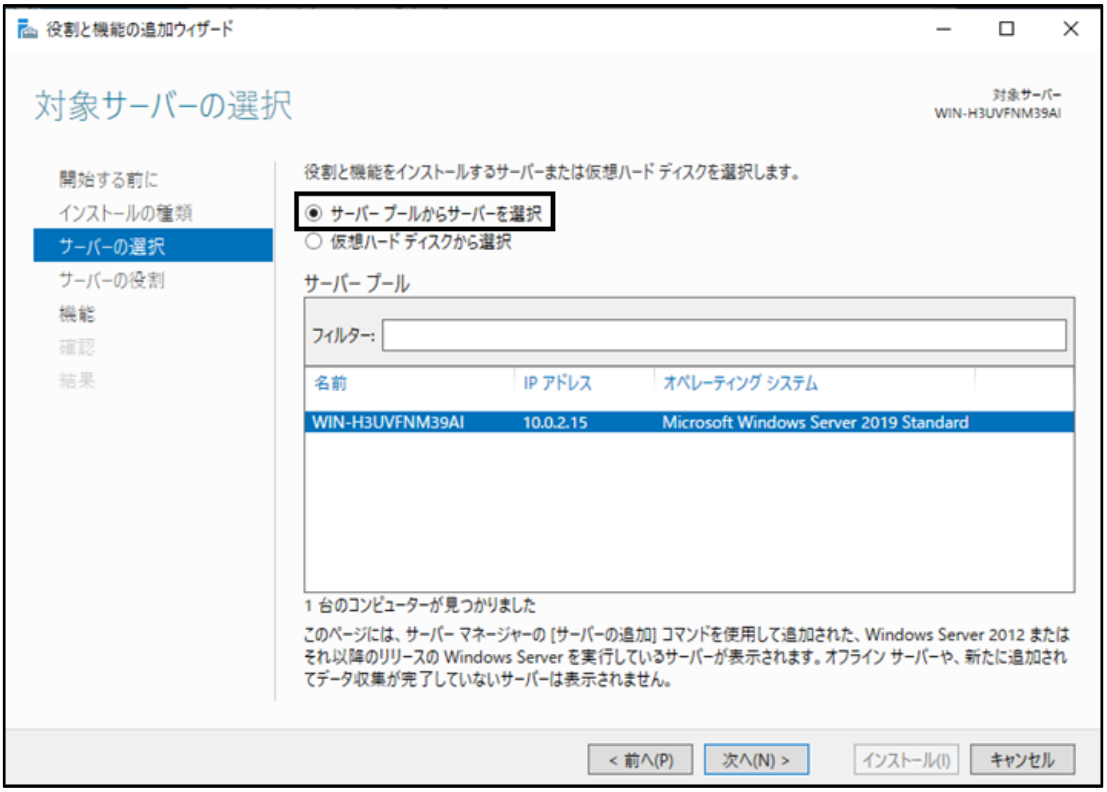
役割と機能の追加Wizardで、左側のナビゲーションウィンドウの**インストールの種類**をクリックし、**役割ベースまたは機能ベースのインストール**をクリックします。

図7 インストールタイプの選択



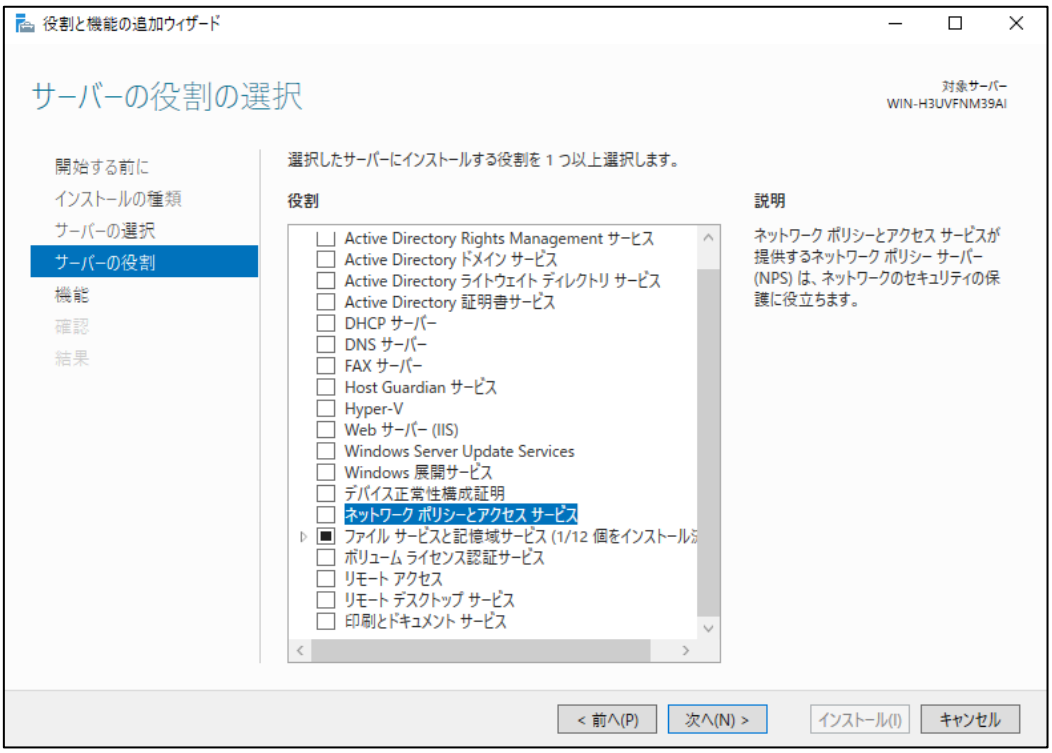
次へをクリックします。**対象サーバーの選択**ウィンドウで、**サーバープールからサーバーを選択**を選択します。ログインしたサーバーがサーバープールの一覧に含まれていることを確認します。

図8 ターゲットサーバーの選択



次へをクリックします。**サーバーの役割**ウィンドウで、**ネットワークポリシーとアクセスサービス**を選択し、**次へ**をクリックします。プロンプトに従ってインストールを完了します。

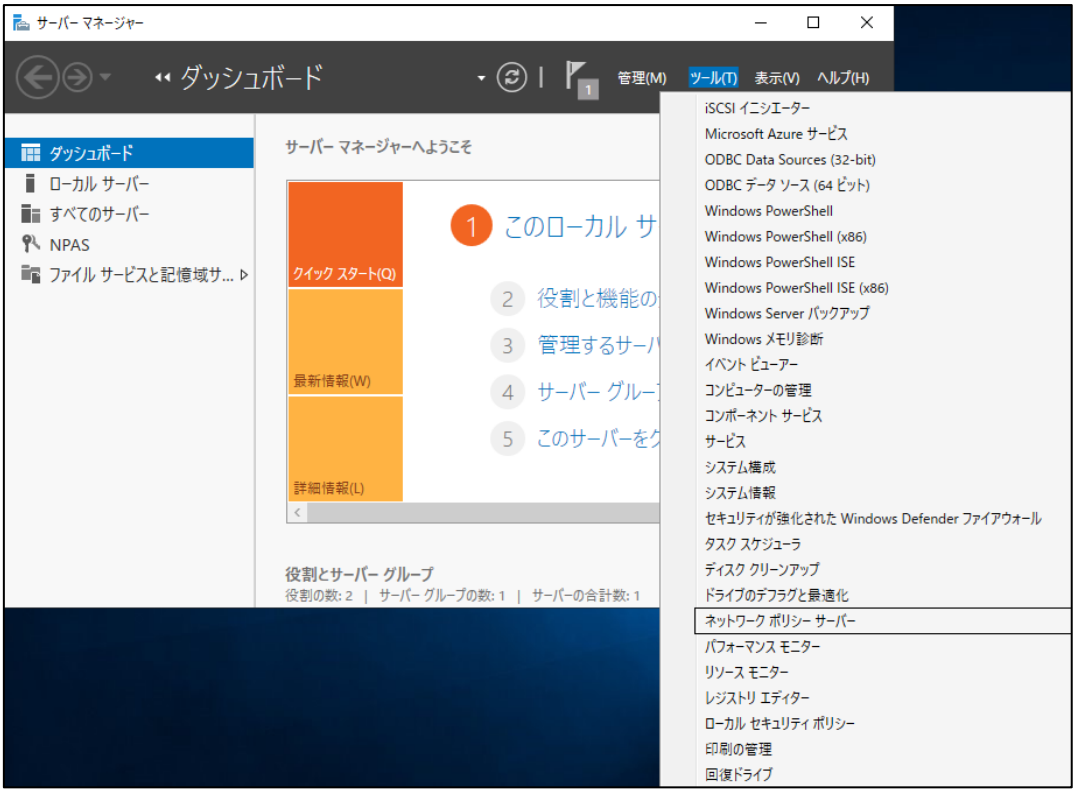
図9 サーバーの役割の選択



4. RADIUSクライアントを設定します。

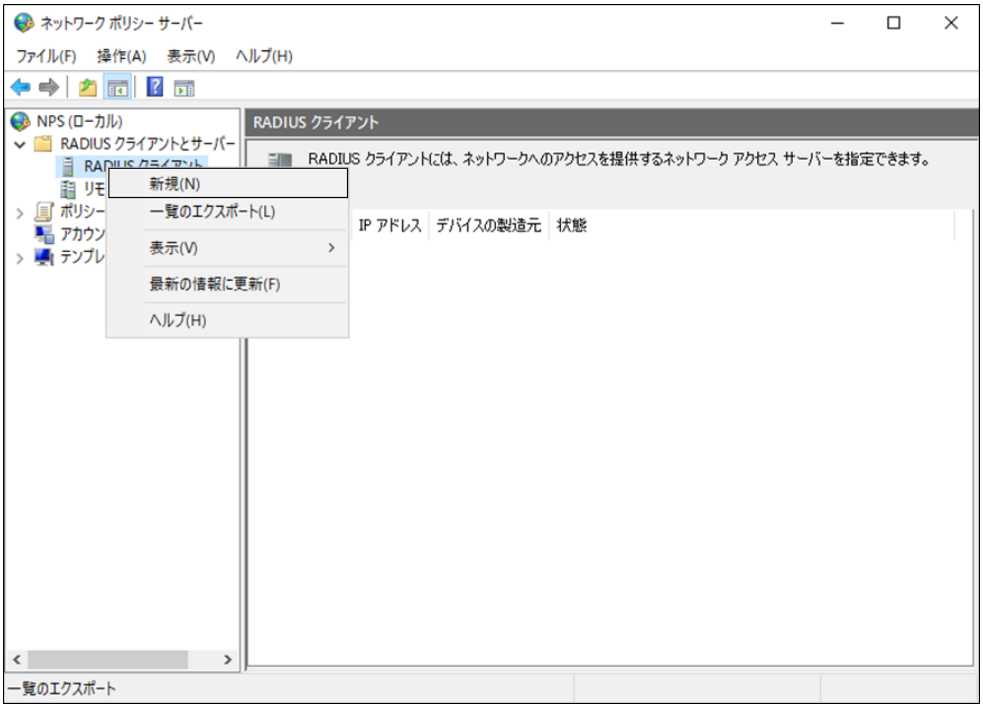
サーバーマネージャーのダッシュボードで、**ツール** > **ネットワークポリシーサーバー**を選択します。

図10 ネットワークポリシーサーバー設定ウィンドウを開く



#左側のナビゲーションペインで、**RADIUS クライアントとサーバー** > **RADIUS クライアント**の順に選択します。**RADIUS クライアント**を右クリックし、**新規**を選択してRADIUSクライアントを作成します。

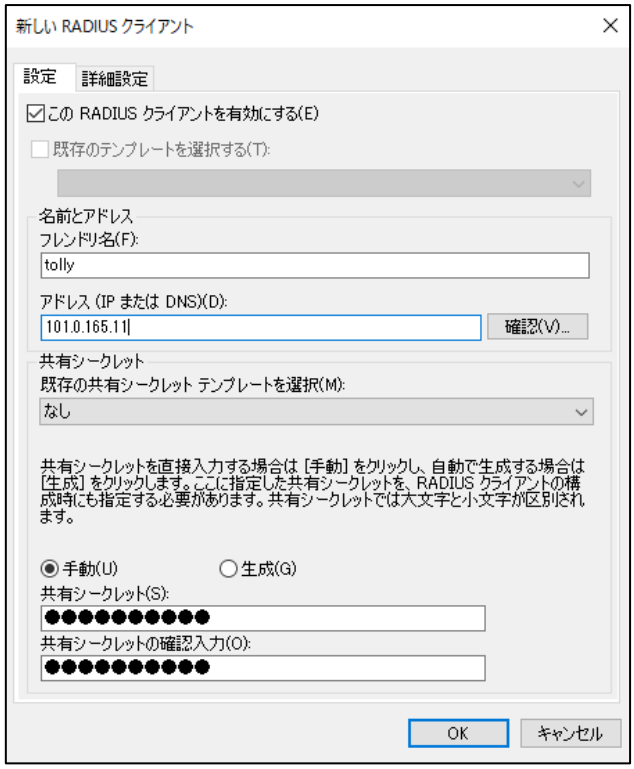
図11 RADIUSクライアントの作成



#開いたウィンドウで、RADIUSクライアントのフレンドリ名、アドレス、および共有秘密を指定します。共有秘密が、スイッチのプライマリ認証およびアカウンティングサーバーに設定されている共

有キーと同じであることを確認します。

図12 RADIUSクライアントの設定

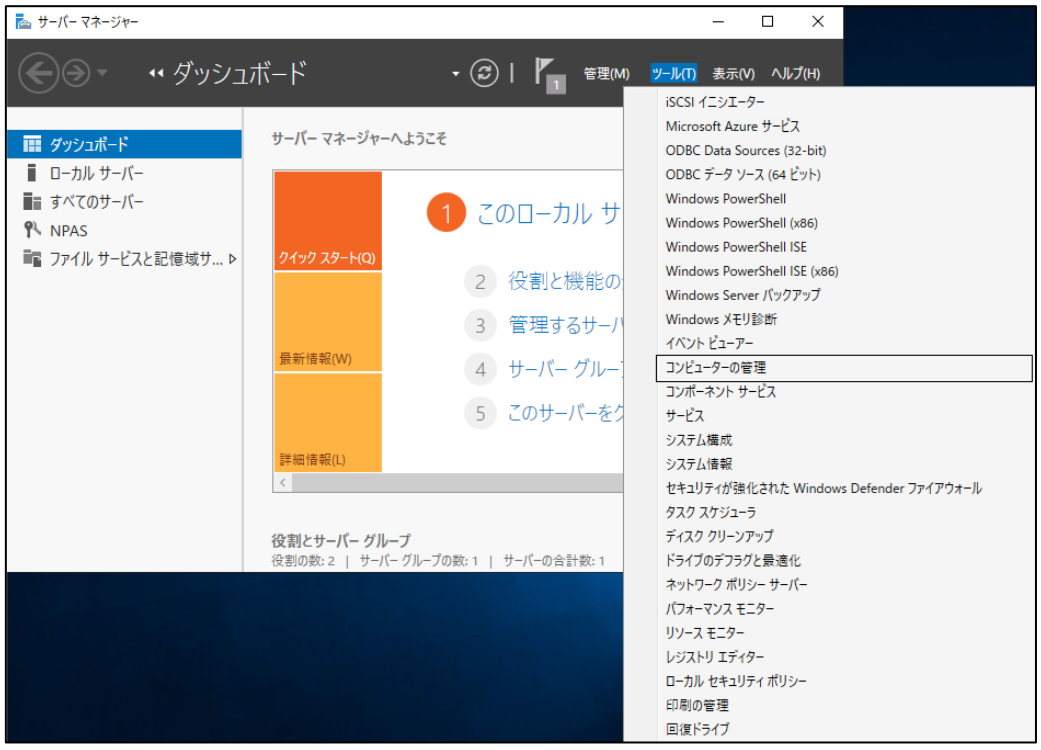


OKをクリックします。

5. ユーザーを追加する:

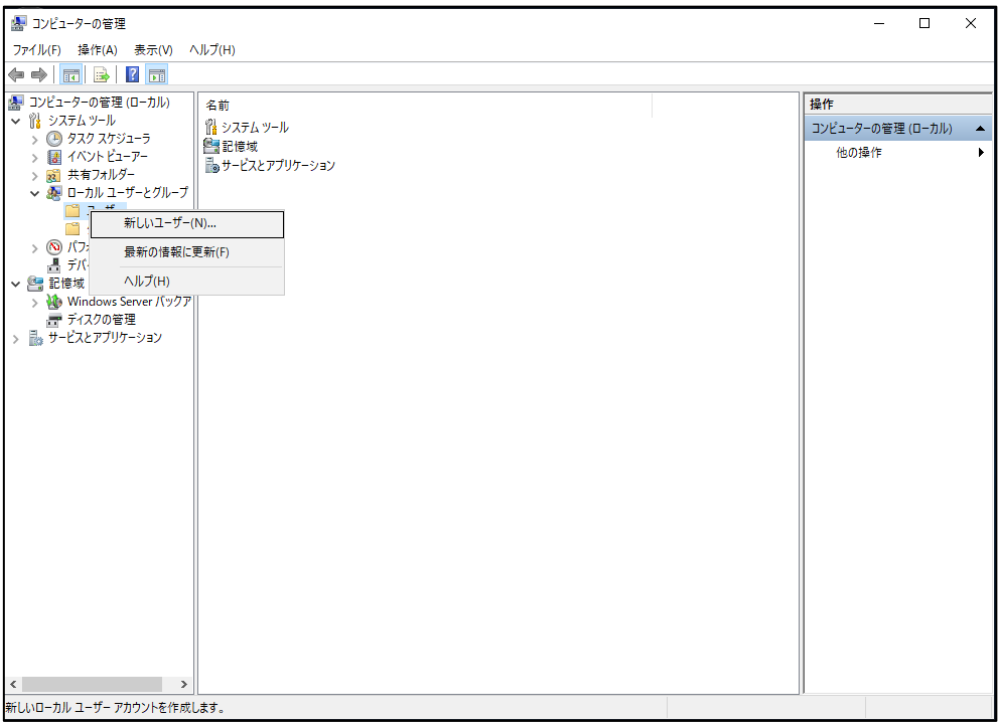
#サーバーマネージャーのダッシュボードで、**ツール > コンピューターの管理**を選択します。

図13 コンピューターの管理設定ウィンドウを開く



#左側のナビゲーションペインで、**ローカルユーザーとグループ > ユーザー**を選択します。**ユーザー**を右クリックし、**新しいユーザー...**を選択して新しいユーザーを作成します。

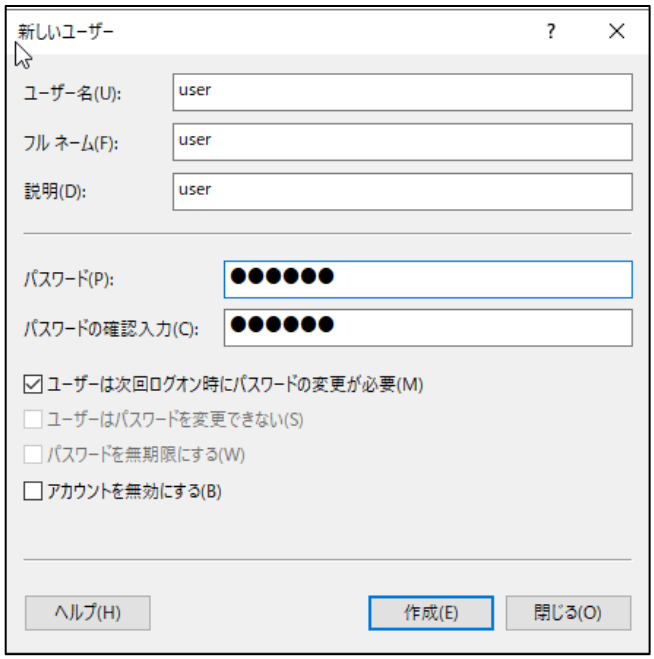
図14 新しいユーザーの追加



#ユーザーを作成します。ユーザーのユーザー名とパスワードが、スイッチ上のMAC認証ユーザー用に設定された共有アカウントのユーザー名とパスワードと同じであることを確認します。

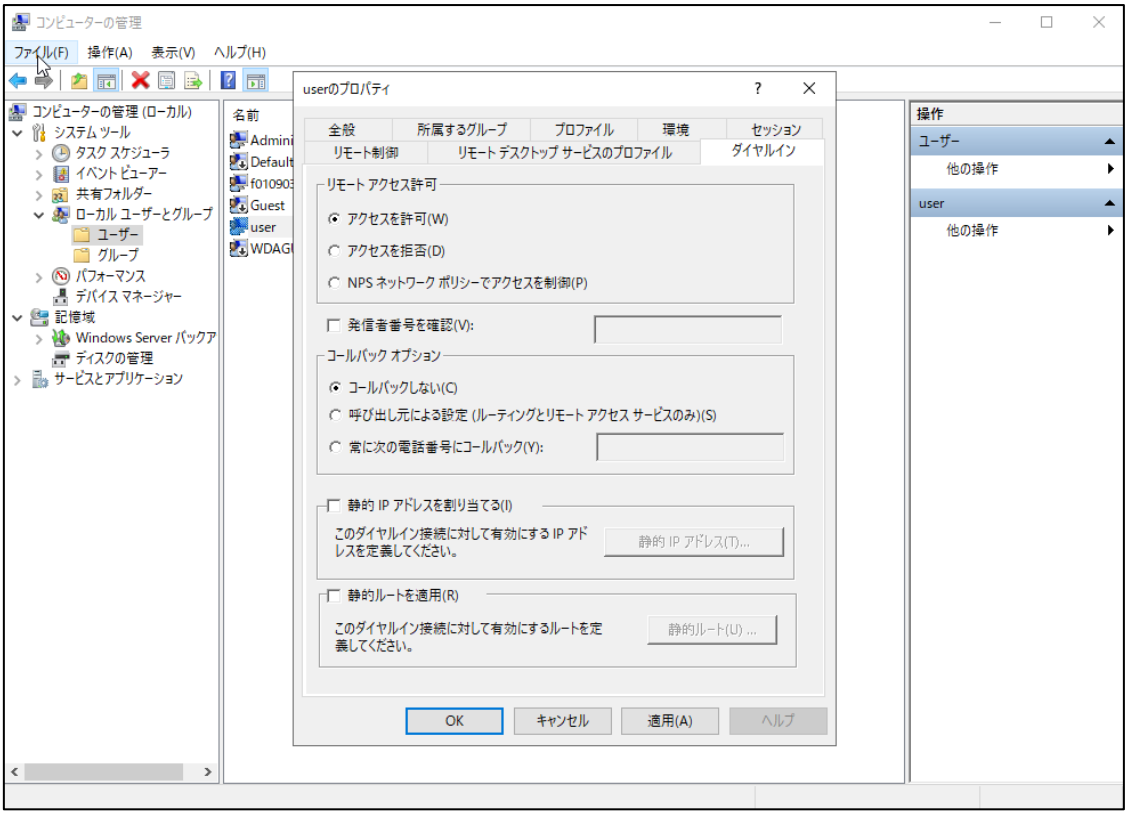
この例では、ユーザー名は**user**、パスワードは**123456**です。

図15 新しいユーザーの設定



#ユーザーリストで、**ユーザー**を選択して右クリックし、**プロパティ**を選択します。開いたウィンドウで、**ダイヤルイン**タブをクリックし、**リモートアクセス許可**領域の**アクセスを許可**を選択して、**OK**をクリックします。

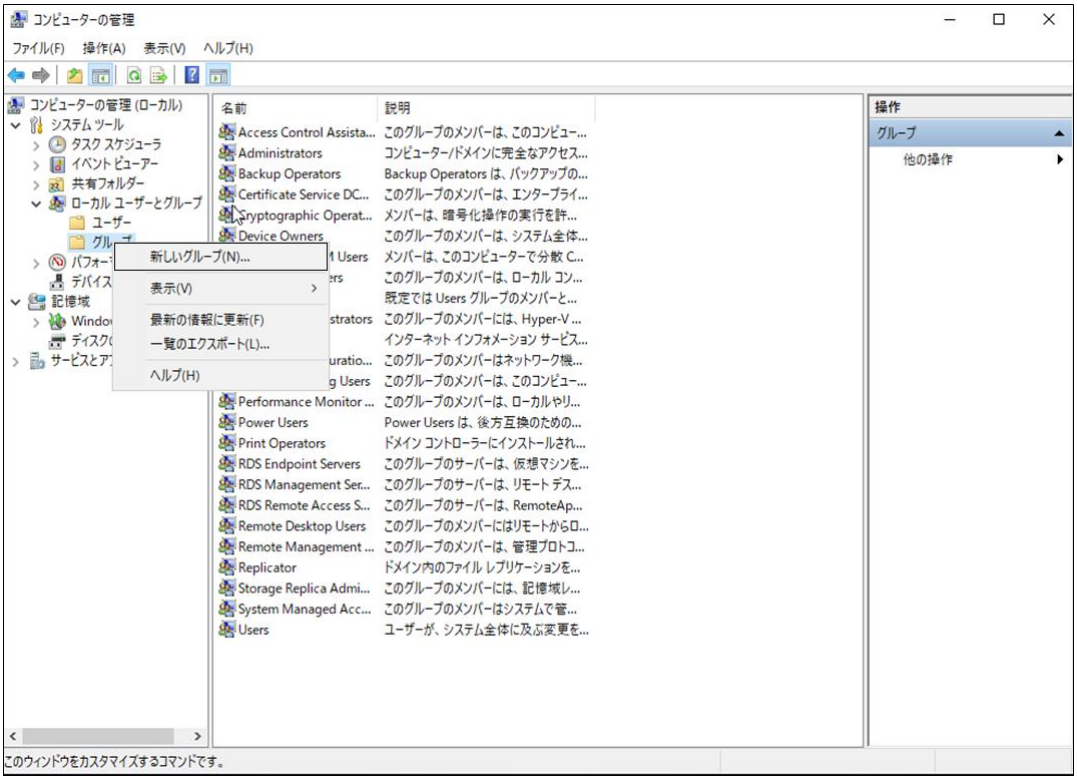
図16 ユーザーのネットワークアクセス権限の設定



6. グループを追加する:

#左側のナビゲーションペインで、[ローカルユーザーとグループ]>[グループ]を選択します。[グループ]を右クリックします。
「新規グループ.」を選択して新しいグループを作成します。

図17 新しいグループの作成



開いたウィンドウで、グループ名を入力し、**追加**を選択し、グループにメンバーを追加して**作成**をクリックします。

この例では、グループ名は**group1**で、メンバーユーザーがグループに追加されます。

図18 グループの作成

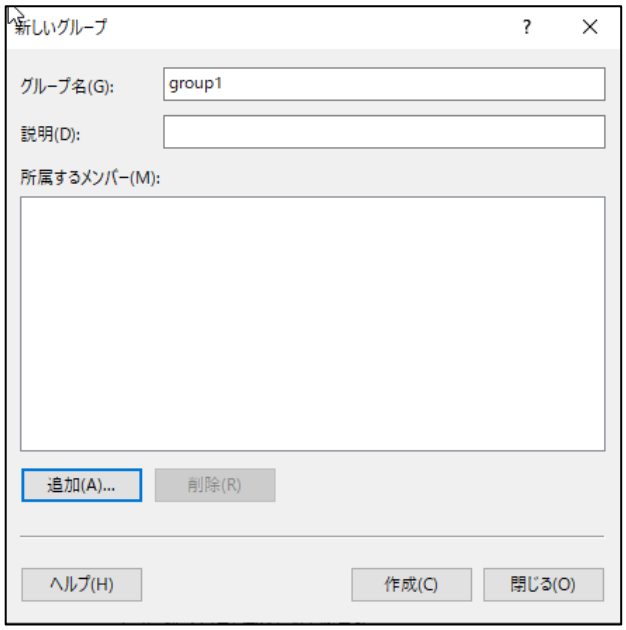
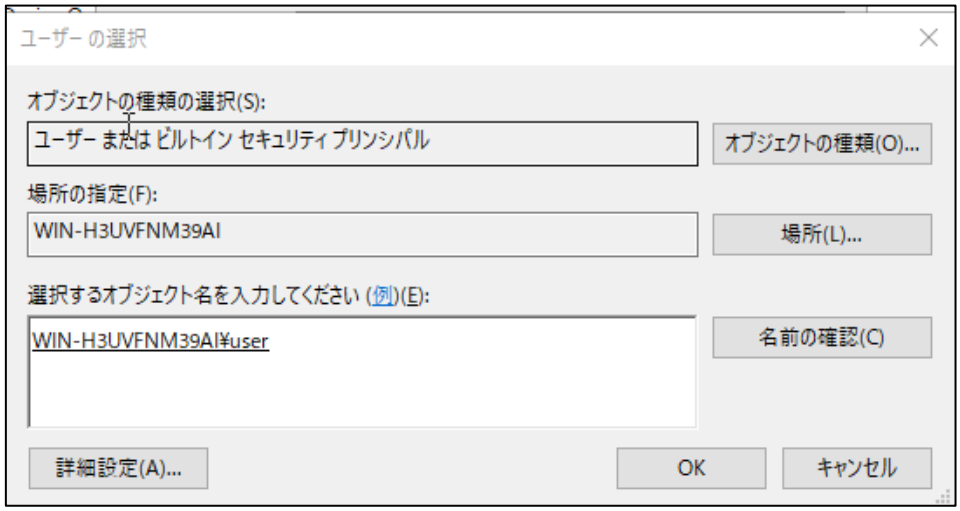


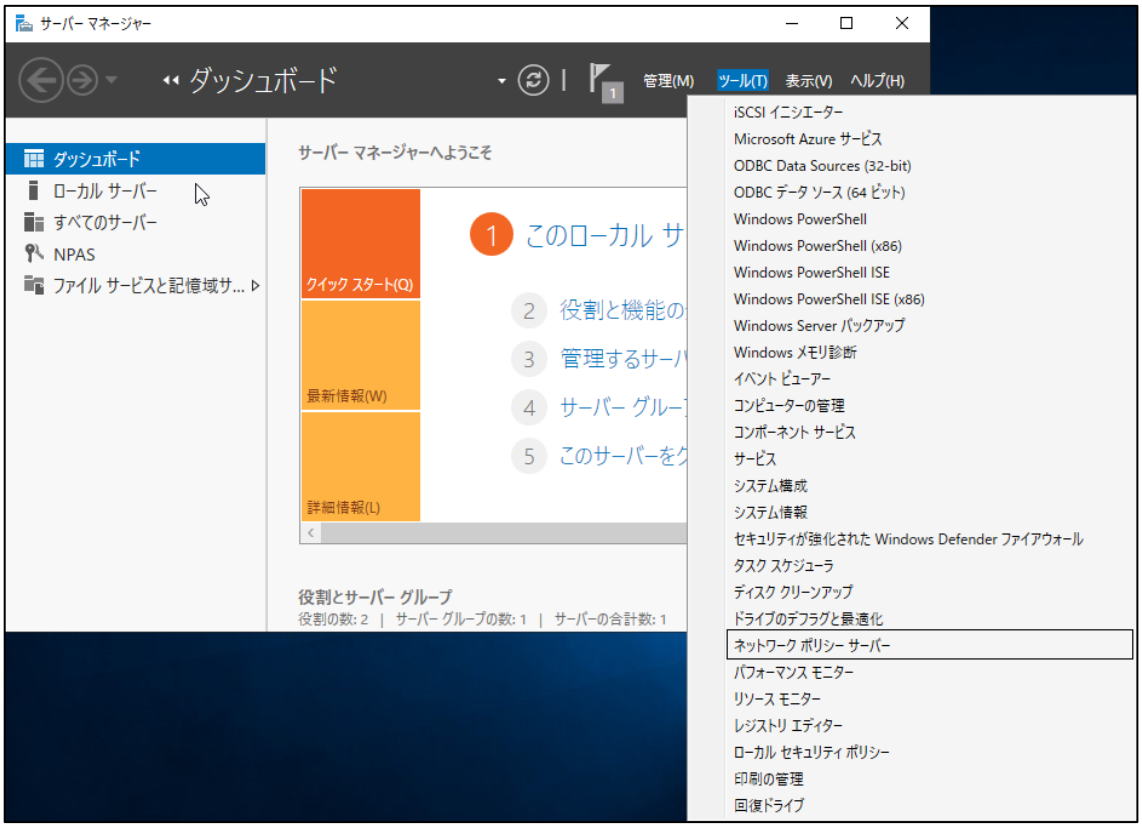
図19 グループへのメンバーの追加



7. ポリシーを追加します。

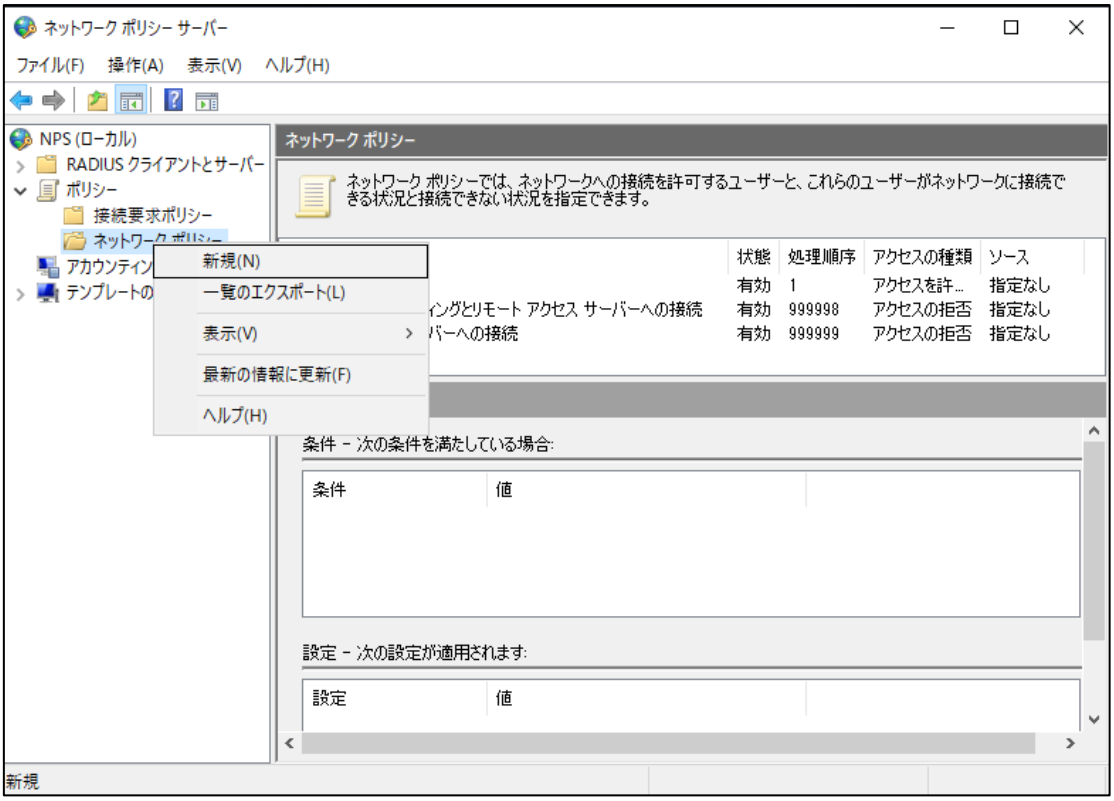
サーバーマネージャーの**ダッシュボード**で、**ツール** > **ネットワークポリシーサーバー**を選択します。

図20 ネットワークポリシーサーバー設定ウィンドウを開く



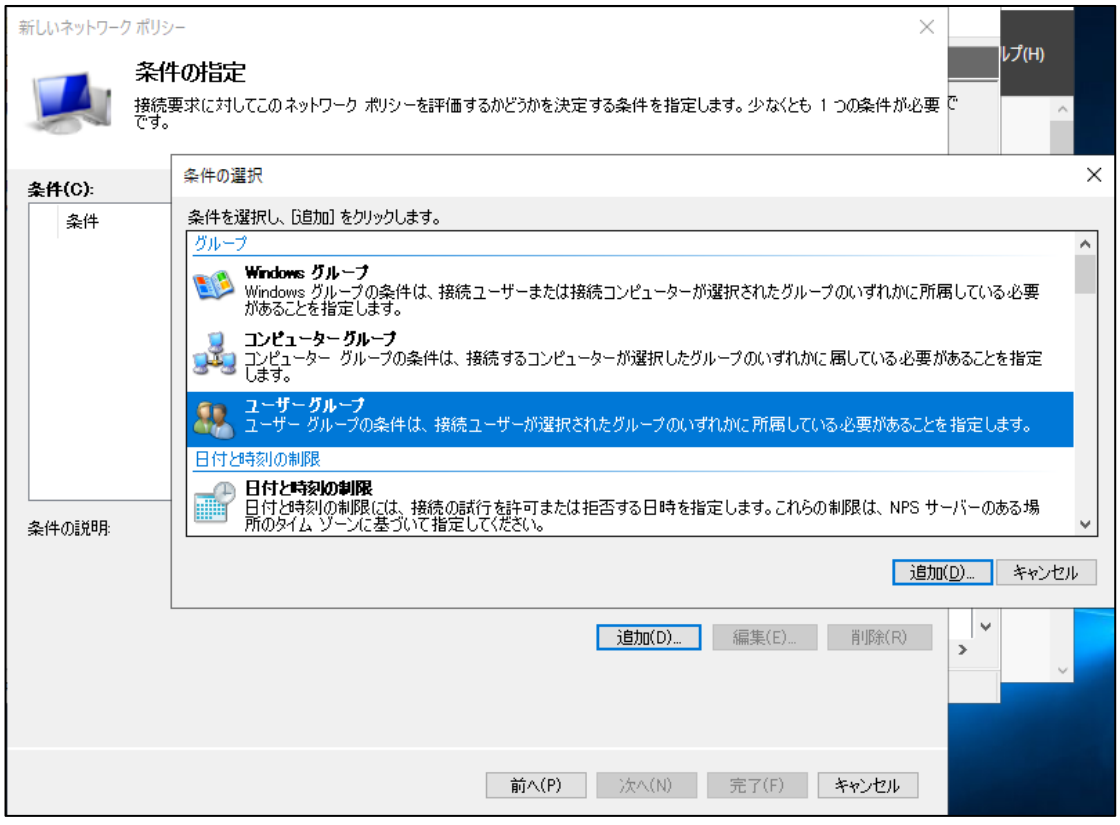
#左側のナビゲーションペインで、**ポリシー** > **ネットワークポリシー**を選択します。**ネットワークポリシーを右クリックします。新規**を選択して新しいネットワークポリシーを作成します。

図21 新しいネットワークポリシーの作成



追加をクリックして、ネットワークポリシーのユーザーグループを追加します。開いたウィンドウで**ユーザーグループ**を選択し、**追加**をクリックします。

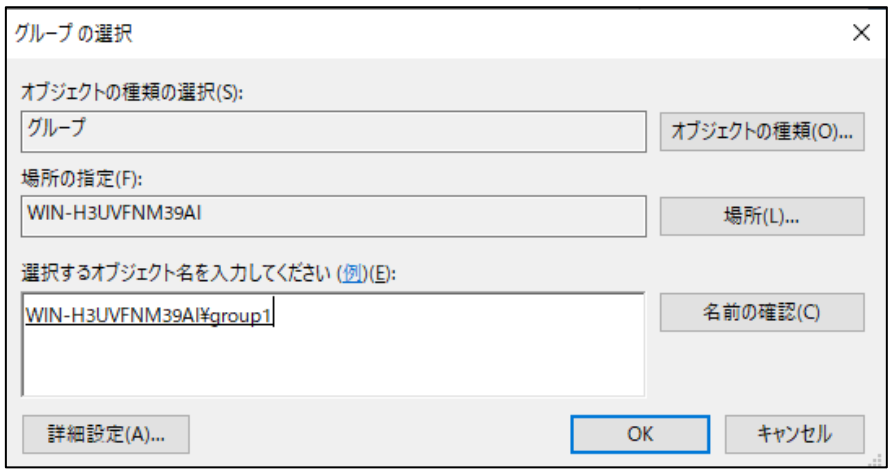
図22 ユーザーグループの追加



ユーザーグループウィンドウで、**選択するオブジェクト名を入力してください(例)(E)**フィールドにグループ名を入力し、**名前の確認**をクリックします。関連するフルグループ名が表示されたら、**OK**をクリックします。

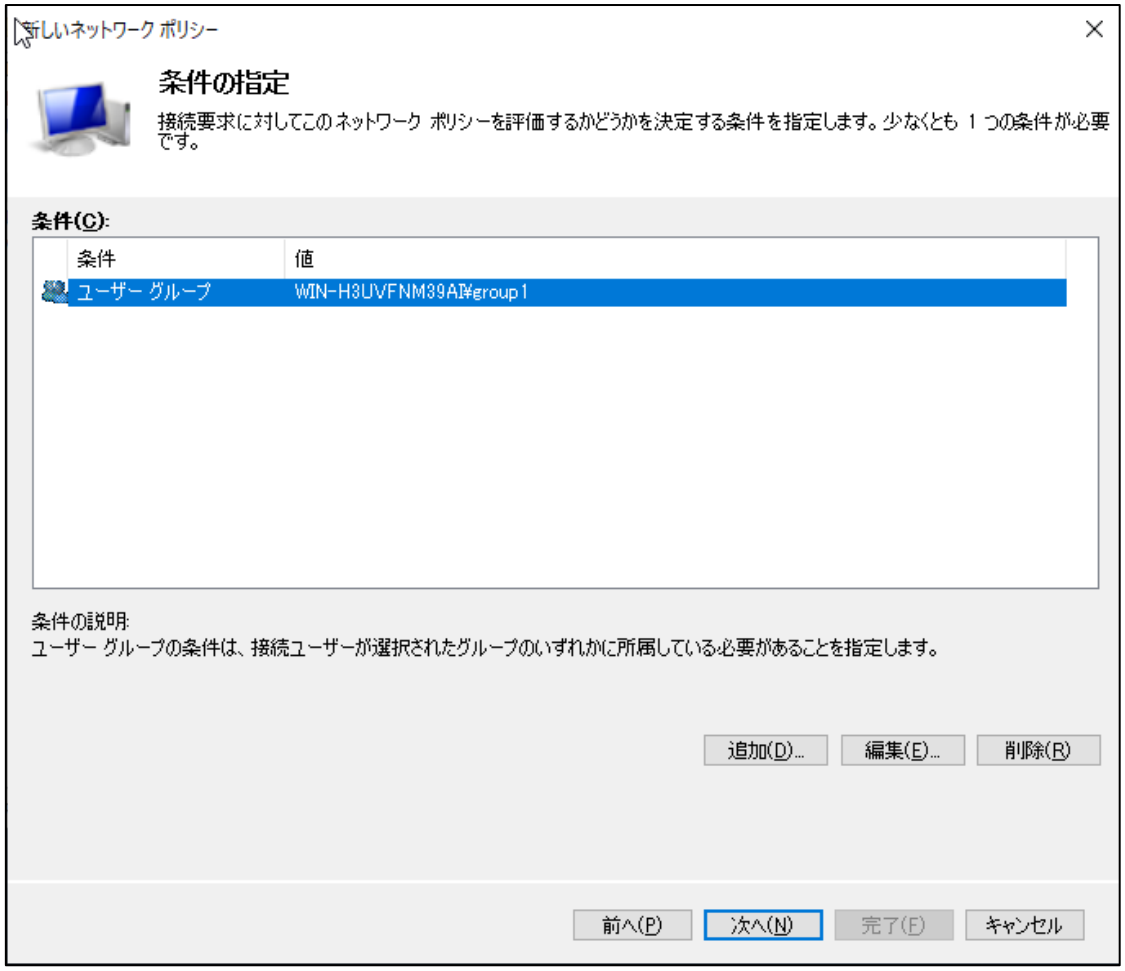
この例では、グループ名は**group1**で、関連付けられたフルグループ名は**WIN-H3UVFNM39AI\group1**。

図23 グループの設定



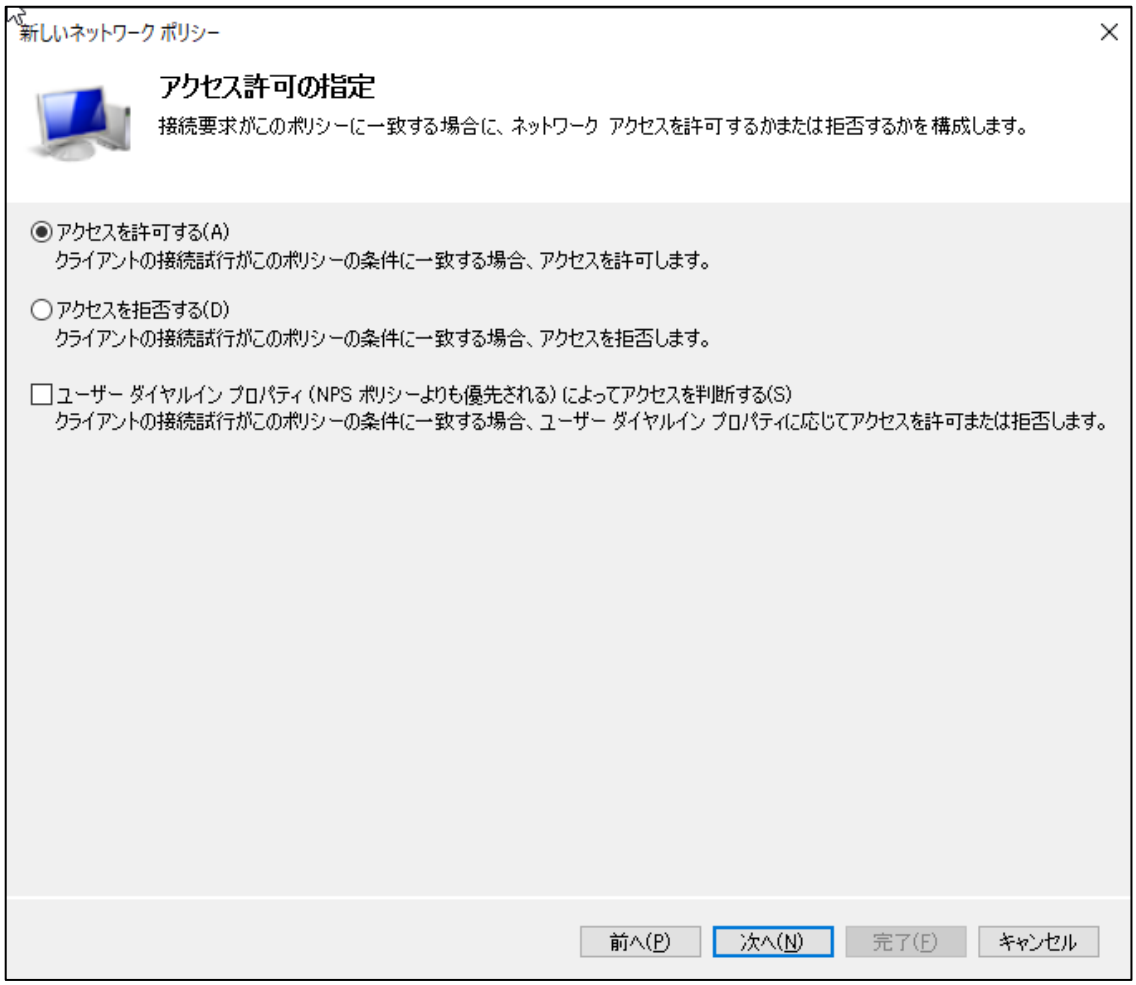
条件が指定されました。

図24 グループの条件の指定



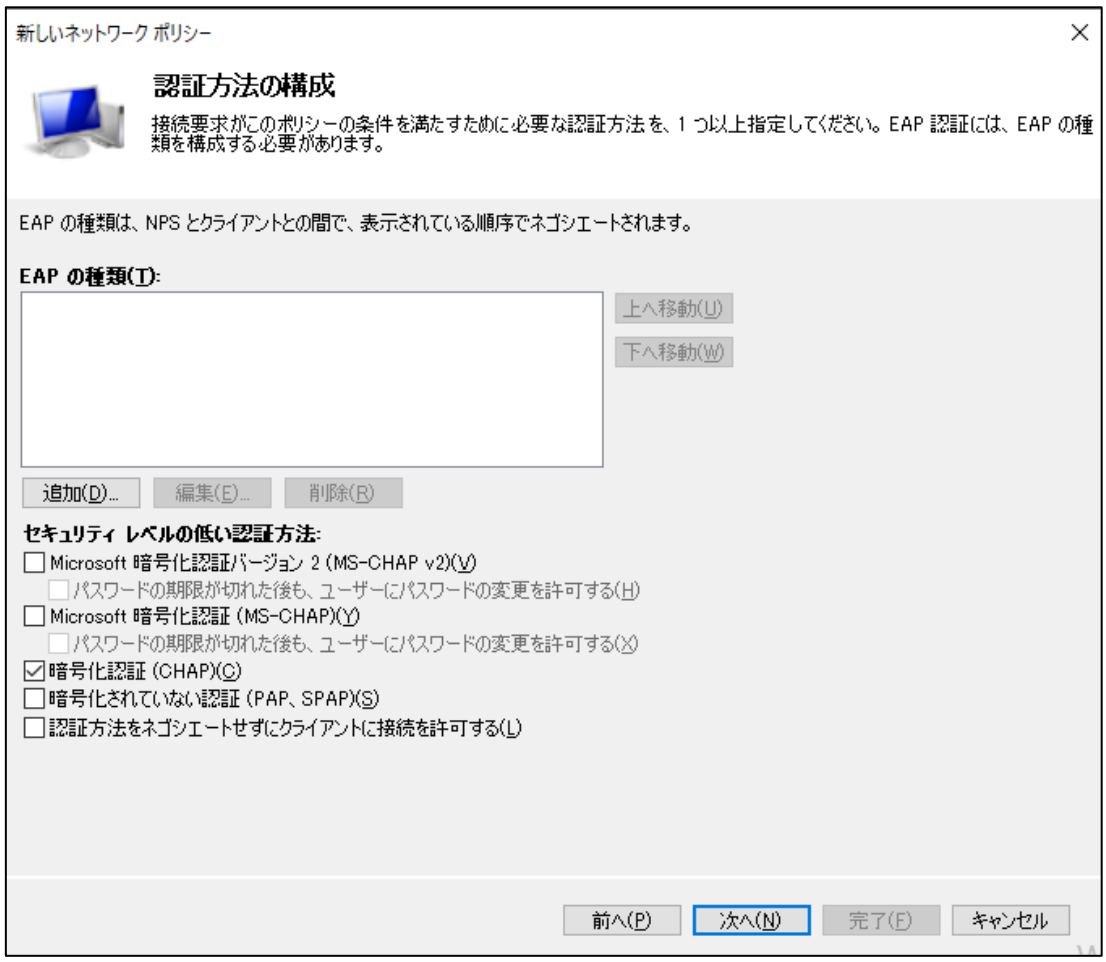
次へをクリックし、**アクセス許可の指定**を**アクセスを許可する**に指定し、**次へ**をクリックします。

図25 アクセス権の指定



認証方法の構成タブに置いて、認証方法として**暗号化認証(CHAP)**を指定し**次へ**をクリックして設定を完了します。

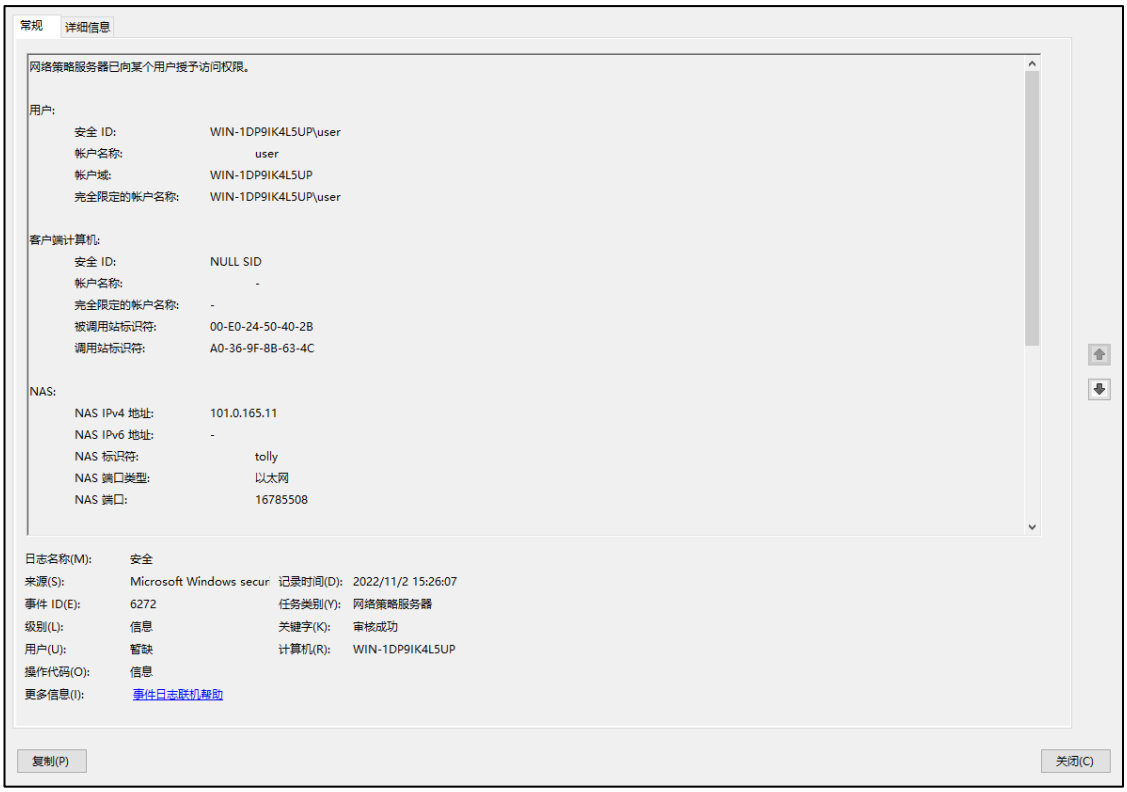
図26 認証方式の指定



設定の確認

1. クライアントで、NPSサーバーにpingを実行して、MAC認証を通過してオンラインになることができることを確認します(詳細は省略)。
2. NPSサーバーで、オンラインユーザーに関する情報を表示します。

図27 ユーザーのオンライン情報の表示



3. オンラインMAC認証ユーザーに関する情報を表示するには、スイッチ上でdisplay mac-authentication connectionコマンドを使用します。

<Switch> display mac-authentication connection

Total connections: 1

Slot ID: 1

User MAC address: a036-9f8b-634c

Access interface: Ten-GigabitEthernet1/0/2

Username: user

User access state: Successful

Authentication domain: mac-

auth IPv4 address:

101.0.165.12

IPv4 address source: User

packet Initial VLAN: 165

Authorization untagged VLAN: N/A

Authorization tagged VLAN: N/A

Authorization VSI: N/A

Authorization microsegment ID:

N/A Authorization ACL

number/name: N/A Authorization

dynamic ACL name: N/A

Authorization user profile: N/A

Authorization CAR: N/A

Authorization URL: N/A

Authorization IPv6 URL: N/A

Authorization temporary redirect: Disabled

Start accounting: Successful

Real-time accounting-update failures: 0

Termination action: Default

Session timeout period: N/A

Offline detection: 300 sec (command-configured)

Online from: 2013/01/08 02:47:40

Online duration: 0h 26m 8s

Port-down keep online: Disabled (offline)

The output shows that the user using the shared account **user** has passed MAC authentication and come online.

出力は、共有アカウントユーザーを使用しているユーザーがMAC認証に合格し、オンラインになったことを示しています。

設定ファイル

```
#
 mac-authentication
 mac-authentication domain mac-auth
 mac-authentication user-name-format fixed account user password cipher
      $c$3$2HmbYwuGcvFCwTALdWqK5AzOvn2w5SY=
 mac-authentication authentication-method chap
#
 domain mac-auth
  authentication lan-access radius-scheme radius1
  accounting lan-access radius-scheme radius1
#
radius scheme radius1
 primary authentication 101.0.144.123
 primary accounting 101.0.144.123
 key authentication cipher
 $c$3$9jjl0lp5VA/WXEw065ZIT7j4AIN88XTF key accounting
 cipher $c$3$fk1zm9nf2IFMdk+I7hGsyBcsAwqLobi7
 user-name-format without-domain
#
interface Ten-GigabitEthernet1/0/2
 port link-mode bridge
 port access vlan 165
 mac-authentication
```

例:MACベースのユーザーアカウントを使用したMAC認証の設定

重要:

MACベースのユーザーアカウントを使用したMAC認証では、スイッチはユーザーからのパケット内の送信元MACアドレスを、MAC認証用のユーザー名およびパスワードとして使用します。

スイッチの設定

「例:共有ユーザーアカウントを使用したMAC認証の設定」の説明に従ってスイッチを設定します。ただし、**mac-authentication user-name-format fixed**はaccountコマンドを**undo mac-authentication user-name-format**コマンドとともに使用して、デフォルトのユーザアカウントポリシーを復元します。

[Switch] undo mac-authentication user-name-format

Windows Server 2016 NPSサーバーの構成

「例:共有ユーザーアカウントを使用したMAC認証の構成」の説明に従ってNPSサーバーを構成します。ただし、ユーザーをサーバーに追加するときに、MAC認証ユーザーのMACアドレスにユーザー名とパスワードを設定する必要があります。

#サーバーマネージャーのダッシュボードで、**ツール > コンピューターの管理 > ローカルユーザーとグループ**を選択します。次に、新しいユーザーを追加し、次のようにグループを構成します。

図28 新しいユーザーの追加

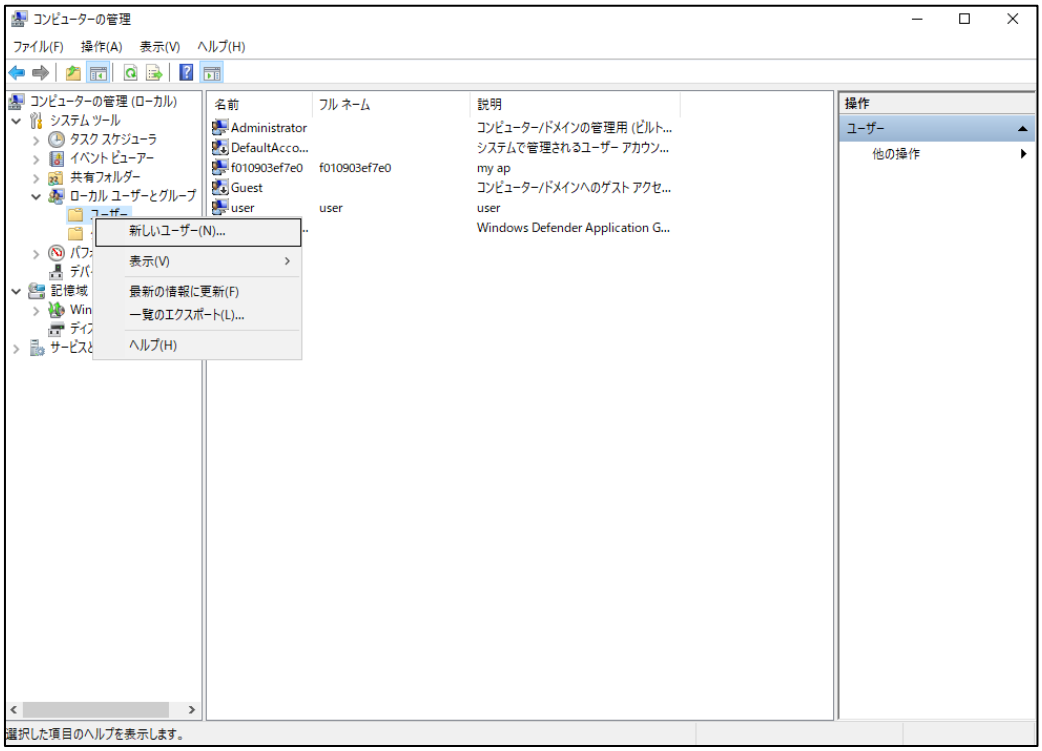


図29 新しいユーザーの設定

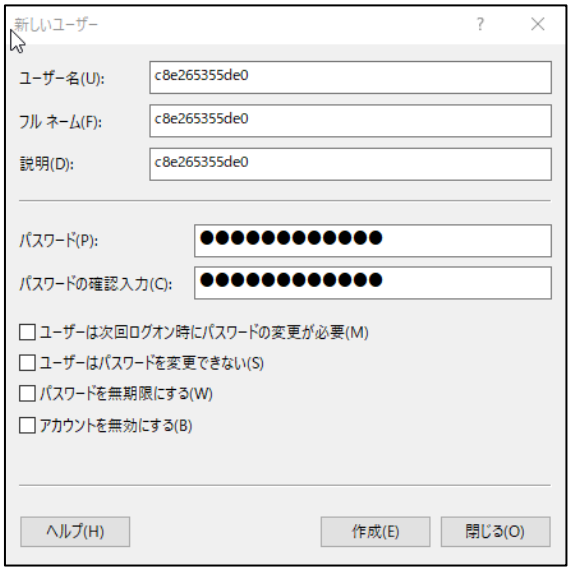


図30 グループの作成

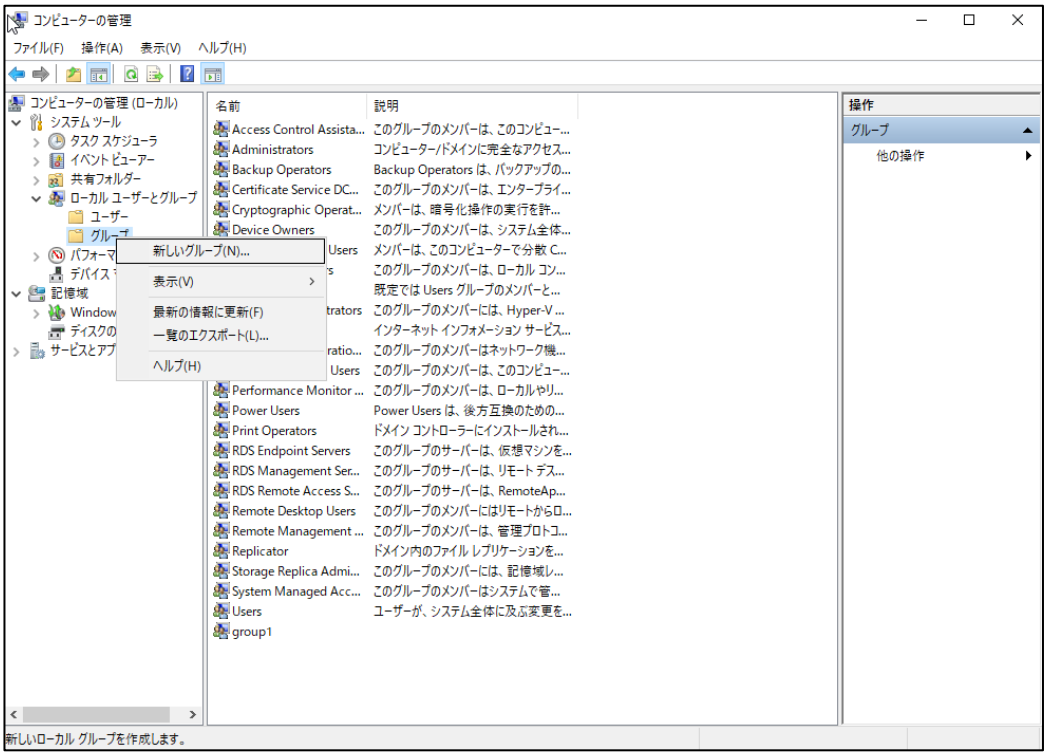


図31 グループ名の入力

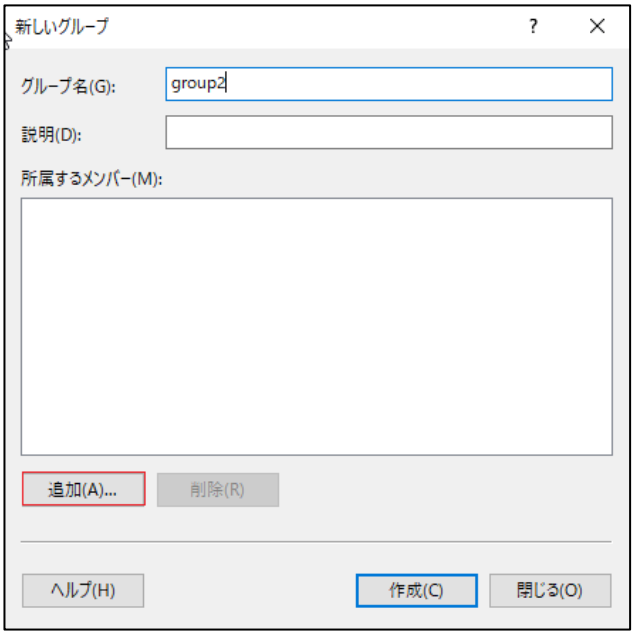
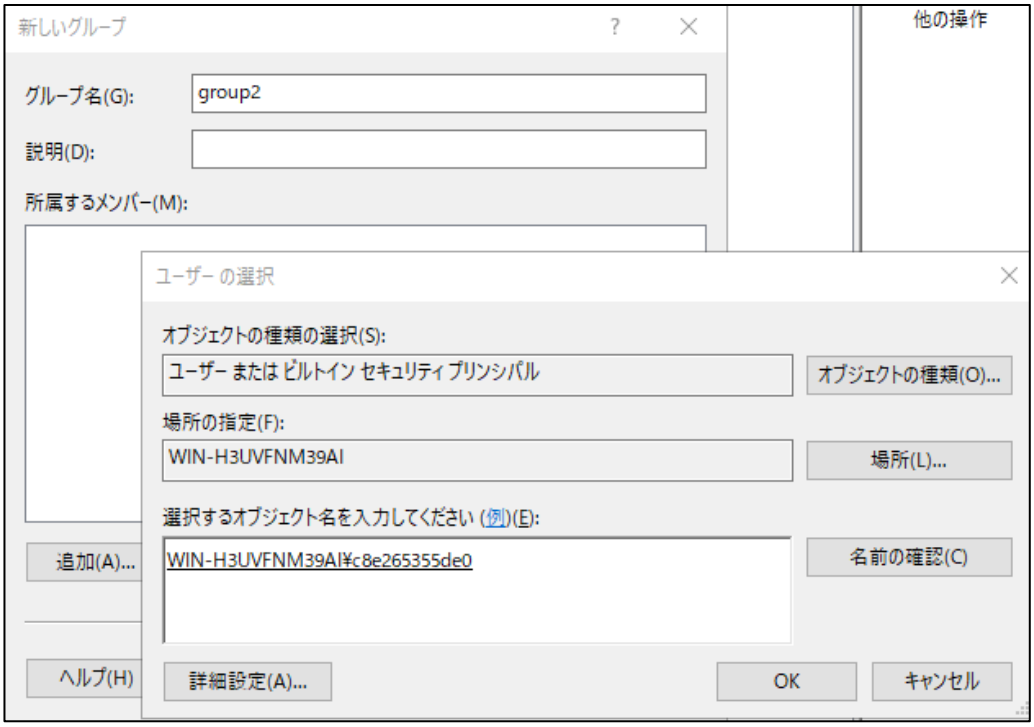


図32 グループへのメンバーの追加



設定の確認

1. クライアントで、NPSサーバーにpingを実行して、MAC認証を通過してオンラインになることができることを確認します(詳細は省略)。
2. NPSサーバーで、オンラインユーザーに関する情報を表示します。

   図33 ユーザーのオンライン情報の表示

3. オンラインMAC認証ユーザーに関する情報を表示するには、スイッチ上でdisplay mac-authentication connectionコマンドを使用します。

   [Switch] display mac-authentication connection

   Total connections: 1

   Slot ID: 1

   User MAC address: c8e2-6535-5de0

   Access interface: Ten-GigabitEthernet1/0/2

   Username: c8e265355de0

   User access state: Successful

   Authentication domain: mac-

   auth IPv4 address:

   101.0.165.12

   IPv4 address source: User

   packet Initial VLAN: 165

   Authorization untagged VLAN: N/A

   Authorization tagged VLAN: N/A

   Authorization VSI: N/A

   Authorization microsegment ID:

   N/A Authorization ACL

   number/name: N/A Authorization

dynamic ACL name: N/A
Authorization user profile: N/A
Authorization CAR: N/A
Authorization URL: N/A
Authorization IPv6 URL: N/A
Authorization temporary redirect: Disabled
Start accounting: Successful
Real-time accounting-update failures: 0
Termination action: Default
Session timeout period: N/A
Offline detection: 300 sec (command-configured)
Online from: 2013/01/08 05:10:17 Online duration: 0h 0m 16s
Port-down keep online: Disabled (offline)
The output shows that the user has passed MAC authentication and come online.

設定ファイル

```
mac-authentication
mac-authentication domain mac-auth
mac-authentication user-name-format mac-address without-hyphen
uppercase mac-authentication authentication-method chap
#
domain mac-auth
 authentication lan-access radius-scheme radius1
 authorization lan-access radius-scheme radius1
 accounting lan-access radius-scheme radius1
#
radius scheme radius1
 primary authentication 101.0.144.123
 primary accounting 101.0.144.123
 key authentication cipher $c$3$9jjl0lp5VA/WXEw065ZIT7j4AIN88XTF key accounting
  cipher $c$3$fk1zm9nf2IFMdk+I7hGsyBcsAwqLobi7
  user-name-format without-domain
#
interface Ten-GigabitEthernet1/0/2
 port link-mode bridge
 port access vlan 165
 mac-authentication
```

例:802.1X認証の設定

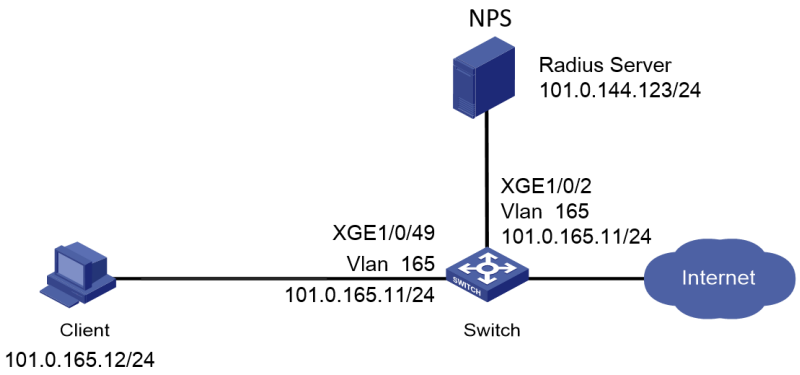
ネットワーク構成

図34に示すように、Windows Server 2016 NPSサーバーと連携してクライアントの802.1X認証を実行するようにスイッチを構成します。クライアントがネットワークリソースにアクセスするには、802.1X認証を通過する必要があります。

スイッチを次のように設定します。

- NPSサーバーをRADIUSサーバーとして使用して、クライアントの802.1X認証を実行します。
- 802.1X認証には、PAP、CHAP、または証明書認証(EAP-PEAPなど)を使用します。
-

図34 ネットワークダイアグラム



使用されるソフトウェアのバージョン

この設定例は、次のハードウェアおよびソフトウェアバージョンで作成され、検証されています。

ハードウェア	ソフトウェアのバージョン
S5560X-54C-PWR-EIスイッチ	バージョン7.1.070
認証サーバー	Windows Server 2016 NPSの場合

例:LDAPサーバーを介したローカルポータル認証の設定

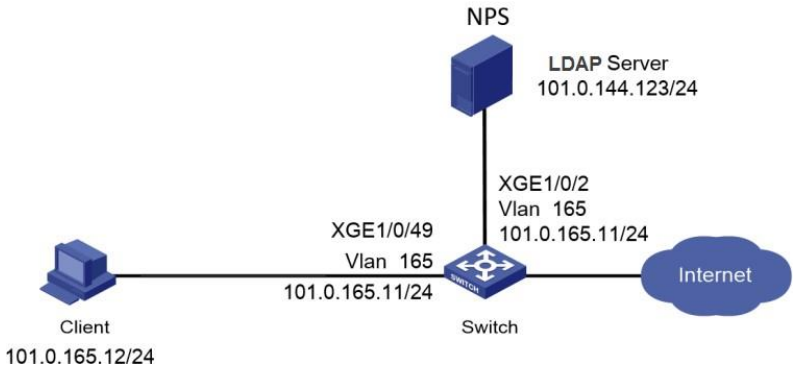
ネットワーク構成

図35に示すように、Windows Server 2016 NPSサーバーと連携してクライアントのポータル認証を実行するようにスイッチを構成します。クライアントがネットワークリソースにアクセスするには、ポータル認証を通過する必要があります。

スイッチを次のように設定します。

- NPSサーバーをLDAPサーバーおよびポータル認証サーバーとして使用して、クライアントのポータル認証を実行します。
- 直接ポータル認証を使用します。

図35 ネットワークダイアグラム



使用されるソフトウェアのバージョン

この設定例は、次のハードウェアおよびソフトウェアバージョンで作成され、検証されています。

ハードウェア	ソフトウェアのバージョン
S5560X-54C-PWR-EIスイッチ	バージョン7.1.070
認証サーバー	Windows Server 2016 NPSの場合

手順

前提条件

この例では、認証の設定だけを示します。クライアント、スイッチ、およびサーバーが相互に通信するためのネットワーク接続を持っていることを確認します。

スイッチの設定

#HTTPベースのローカルポータルWebサービスを作成し、そのビューを入力します。リスニングTCPポート番号を2331に指定します。

<Switch> system-view

[Switch] portal local-web-server http tcp-port 2331

[Switch-portal-local-websvr-http] quit

#ポータルWebサーバー**newpt**のURLを**http://101.0.165.11:2331/portal**として構成します。

[Switch] portal web-server newpt

[Switch-portal-websvr-newpt] url http://101.0.165.11:2331/portal

[Switch-portal-websvr-newpt] quit

#LDAPサーバーcccを作成し、管理者DN、ユーザー検索のベースDN、LDAP認証サーバーのIPアドレス、および管理者パスワードを設定します。

[Switch] ldap server ccc

[Switch-ldap-server-ccc] login-dn cn=administrator,cn=users,dc=test,dc=com

[Switch-ldap-server-ccc] search-base-dn dc=test,dc=com

[Switch-ldap-server-ccc] ip 101.0.144.124

[Switch-ldap-server-ccc] login-password cipher 123456

[Switch-ldap-server-ccc] quit

#LDAPスキーム**ldap1**を作成し、LDAP認証サーバーをcccとして指定します。

[Switch] ldap scheme ldap1

[Switch-ldap-ldap1] authentication-server ccc

[Switch-ldap-ldap1] quit

#VLAN 165とVLAN-interface 165を作成し、VLANインターフェイスにIPアドレスを割り当てます。VLAN-interface 165にポータルWebサーバー**newpt**を指定します。

[Switch] vlan 165

[Switch-vlan165] quit

[Switch] interface Vlan-interface 165

[Switch-Vlan-interface165] ip address 101.0.165.11 255.255.255.0

[Switch-Vlan-interface165] portal apply web-server newpt

[Switch-Vlan-interface165] quit

#Ten-GigabitEthernet 1/0/47およびTen-GigabitEthernet 1/0/2をVLAN 165に割り当てます。

[Switch] interface Ten-GigabitEthernet 1/0/47

[Switch-Ten-GigabitEthernet1/0/47] port access vlan 165

[Switch-Ten-GigabitEthernet1/0/47] quit

[Switch] interface Ten-GigabitEthernet 1/0/2

[Switch-Ten-GigabitEthernet1/0/2] port access vlan 165

[Switch-Ten-GigabitEthernet1/0/2] quit

#ISPドメイン**domain1**を作成し、ISPドメイン内のポータルユーザーに対して、認証方法をLDAPに、認可およびアカウンティング方法をnoneに設定します。

[switch] domain domain1

[switch-isp-domain1] authentication portal ldap-scheme ldap1

[switch-isp-domain1] authorization portal none

[switch-isp-domain1] accounting portal none

[switch-isp-domain1] quit

#ISPドメイン**domain1**をデフォルトのISPドメインとして指定します。

[Switch] domain default enable domain1

#VLANインターフェイス165で直接ポータル認証をイネーブルにします。

[Switch] interface Vlan-interface 165

[Switch-Vlan-interface165] portal enable method direct

[Switch-Vlan-interface165] quit

注:

ユーザーは、直接ポータル認証またはサブネット間ポータル認証を使用してオンラインになることができます。サブネット間ポータル認証を実行するには、スイッチ上でportal enable method directコマンドをportal enable method layer3コマンドに置き換えます。サーバーおよびクライアントの設定を変更する必要はありません。

Windows Server 2016 NPSサーバーの構成

「Windows Server 2016 NPSサーバーの構成」の説明に従って、NPSサーバーを構成します。

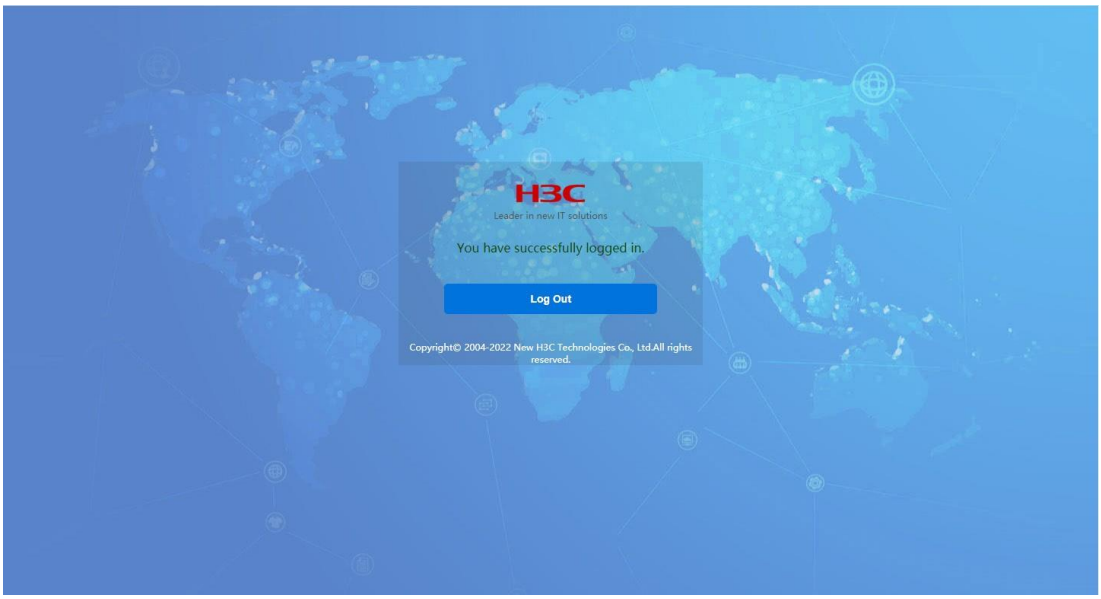
設定の確認

1. クライアントでWebブラウザを開き、アドレス・バーにポータル認証IP(101.0.165.11)を入力して、Enterキーを押します。開いたログインページで、ユーザー名とパスワードを入力します。

   ログインをクリックします。正常にログインできることを確認します。

   図36 Webログインページ

図37 正常なログイン



2. NPSサーバーで、オンラインユーザーに関する情報を表示します。

図38 ユーザーのオンライン情報の表示

3. スイッチ上で、display portal userコマンドを使用して、ポータルユーザーに関する情報を表示します。

<Switch> display portal user all

Total portal users: 1

Username: user

Portal server:

State: Online

VPN instance: N/A

MAC IP VLAN Interface

a036-9f8b-634c 101.0.165.12 165 Vlan-interface165

Authorization information:

DHCP IP pool: N/A

User profile: N/A

Session group profile: N/A

ACL number: N/A

Inbound CAR: N/A

Outbound CAR: N/A

The output shows that the user has passed portal authentication and come online.

出力は、ユーザーがポータル認証に合格し、オンラインになったことを示しています。

設定ファイル

```
interface Vlan-interface165
  ip address 101.0.165.11 255.255.255.0
  portal enable method direct
  portal apply web-server newpt
#
domain ldap
  authentication portal ldap-scheme ldap
  authorization portal none
  accounting portal none
#
ldap scheme ldap
  authentication-server ldap
#
ldap server ldap
  login-dn cn=administrator,cn=users,dc=test,dc=com
  search-base-dn dc=test,dc=com
  ip 101.0.144.124
  login-password cipher $c$3$MU1UdAnLgSFni5hERPL15CYR7NsHW6RkErhr3bQuNA==
#
portal web-server newpt
  url http://101.0.165.11:2331/portal
#
```

```
portal local-web-server http
   default-logon-page en.zip
   tcp-port 2331
  #
```

例:802.1X CHAP認証の設定

前提条件

この例では、認証の設定だけを示します。クライアント、スイッチ、およびサーバーが相互に通信するためのネットワーク接続を持っていることを確認します。

スイッチの設定

#RADIUSスキームradius1を作成し、ユーザー認証およびアカウンティング用にNPSサーバーを101.0.144.123に指定し、プレーンテキスト形式で共有キーをadminに設定し、RADIUSサーバーに送信されるユーザー名からドメイン名を除外します。

<Switch> system-view

[Switch] radius scheme radius1

[Switch-radius-radius1] primary authentication 101.0.144.123

[Switch-radius-radius1] primary accounting 101.0.144.123

[Switch-radius-radius1] key authentication simple admin

[Switch-radius-radius1] key accounting simple admin

[Switch-radius-radius1] user-name-format without-

domain [Switch-radius-radius1] quit

#認証方式を指定します。この例では、EAP終端を実行し、CHAPを使用してRADIUSサーバーと通信するようにスイッチを設定します。

[Switch] dot1x authentication-method CHAP

#ISPドメインdomain1を作成し、認証、認可、およびアカウンティングのためにRADIUSスキームをISPドメインに適用します。

[Switch] domain domain1

[Switch-isp-domain1] authentication default radius-scheme radius1

[Switch-isp-domain1] authorization lan-access radius-scheme radius1

[Switch-isp-domain1] accounting lan-access radius-scheme radius1

[Switch-isp-domain1] quit

#VLAN 165とVLAN-interface 165を作成し、VLANインターフェイスにIPアドレスを割り当てます。

[Switch] vlan 165

[Switch-vlan165]

quit

[Switch] interface Vlan-interface 165

[Switch-Vlan-interface165] ip address 101.0.165.11 255.255.255.0

[Switch-Vlan-interface165] quit

#Ten-GigabitEthernet 1/0/49をVLAN 165に割り当てます。

[Switch]interface Ten-GigabitEthernet 1/0/49

[Switch-Ten-GigabitEthernet1/0/49] port access vlan 165

#Ten-GigabitEthernet 1/0/49で802.1Xをイネーブルにし、ISPドメインdomain1を必須ドメインとして指定します。

[Switch-Ten-GigabitEthernet1/0/49] dot1x

[Switch-Ten-GigabitEthernet1/0/49] dot1x mandatory-domain domain1

#Ten-GigabitEthernet 1/0/49でポートベースのアクセスコントロールをイネーブルにします。

[Switch-Ten-GigabitEthernet1/0/49] dot1x port-method portbased [Switch-Ten-GigabitEthernet1/0/49] quit

#Ten-GigabitEthernet 1/0/2をVLAN 165に割り当てます。

[Switch] interface Ten-GigabitEthernet 1/0/2

[Switch-Ten-GigabitEthernet1/0/2] port access vlan 165

[Switch-Ten-GigabitEthernet1/0/2] quit

#ISPドメインdomain1をデフォルトのISPドメインとして指定します。

[Switch] domain default enable domain1

#802.1Xをグローバルにイネーブルにします。

[Switch] dot1x

Windows Server 2016 NPSサーバーの構成

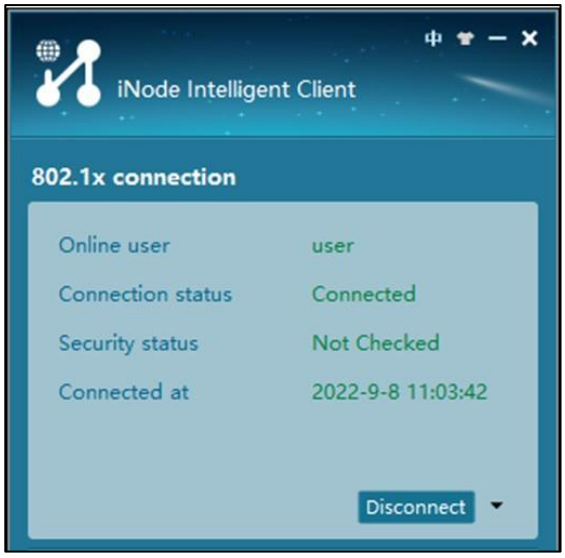
「例:共有ユーザーアカウントを使用したMAC認証の構成」の説明に従って、NPSサーバーを構成します。

設定の確認

1. ユーザー名とパスワードを入力した後、iNodeクライアントを使用して、802.1X認証をパスしてオンラインになることを確認します。

図39 iNodeクライアントを介したアクセス

図40 成功した802.1X接続



2. NPSサーバーで、オンラインユーザーに関する情報を表示します。

図41 ユーザーアクセス情報の表示

3. オンライン802.1X認証ユーザーに関する情報を表示するには、スイッチ上でdisplay dot1x connectionコマンドを使用します。

[Switch] display dot1x connection

Total connections: 1

Slot ID: 1

User MAC address: a036-9f8b-634c

Access interface: Ten-GigabitEthernet1/0/2

Username: user

User access state: Successful

Authentication domain: domain1

EAP packet identifier: 2
Authentication method: CHAP
AAA authentication method: RADIUS
Initial VLAN: 165
Authorization untagged VLAN: N/A
Authorization tagged VLAN list:
N/A Authorization VSI: N/A
Authorization microsegment ID:
N/A Authorization ACL
number/name: N/A Authorization
dynamic ACL name: N/A
Authorization user profile: N/A
Authorization CAR: N/A
Authorization URL: N/A
Authorization IPv6 URL: N/A
Authorization temporary redirect: Disabled
Start accounting: Successful
Real-time accounting-update failures: 0
Termination action: Default
Session timeout period: N/A
Online from: 2013/01/03
08:22:24 Online duration: 0h
0m 35s
The output shows that the user
has passed 802.1X CHAP
authentication and come online.

この出力は、ユーザーが802.1X CHAP認証に合格し、オンラインになったことを示しています。

設定ファイル

```
#
 dot1x
#
interface Ten-GigabitEthernet1/0/2
 port link-mode bridge
 port link-type hybrid
 port hybrid vlan 1 100 165
 untagged port hybrid pvid vlan 165
undo dot1x handshake
 dot1x mandatory-domain
 domain1 undo dot1x
```

```
 multicast-trigger dot1x port-
 method portbased
#
domain domain1
 authentication lan-access radius-scheme radius1
 authorization lan-access radius-scheme radius1
 accounting lan-access radius-scheme radius1
#
radius scheme radius1
 primary authentication 101.0.144.123
 primary accounting 101.0.144.123
 key authentication cipher
 $c$3$9jjl0lp5VA/WXEw065ZIT7j4AIN88XTF key accounting
 cipher $c$3$fk1zm9nf2IFMdk+I7hGsyBcsAwqLobi7 user-name-
 format without-domain
#
```

例:802.1X PAP認証の設定

スイッチの設定

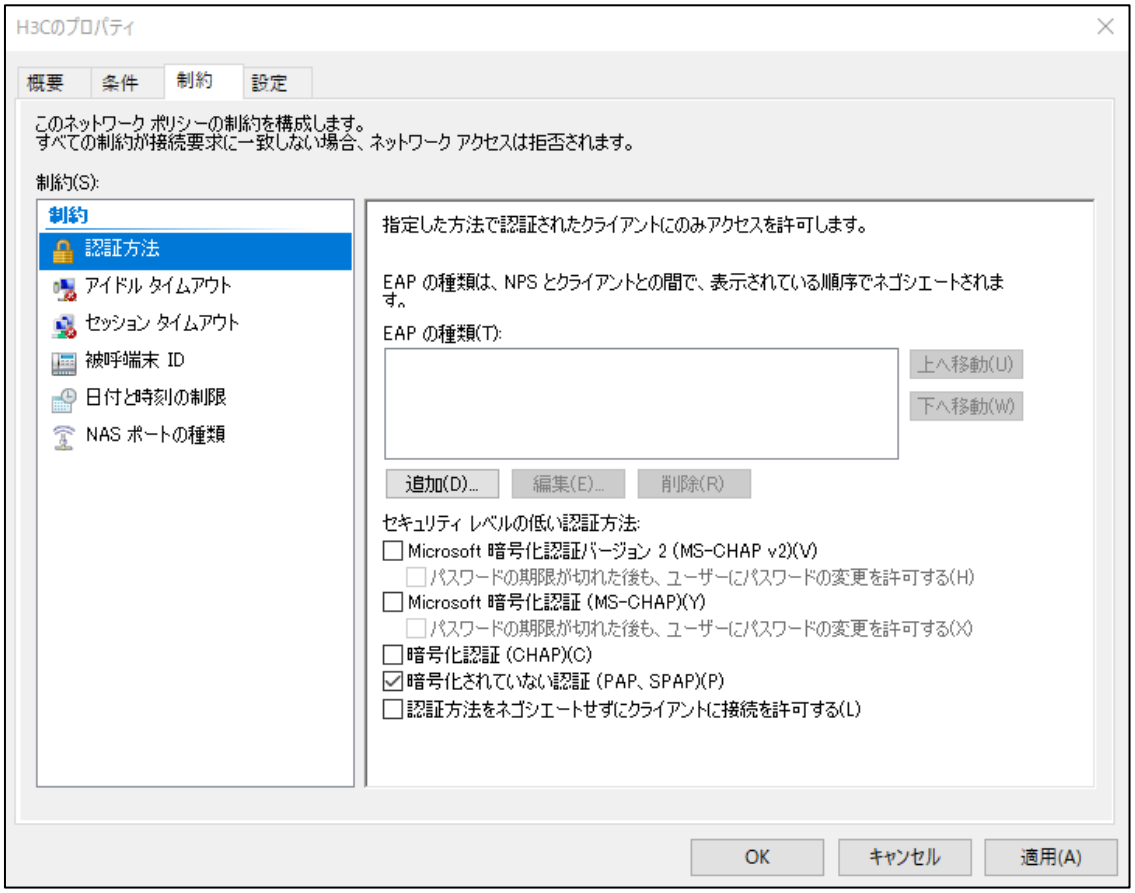
「スイッチの設定」の説明に従ってスイッチを設定します。ただし、次のように認証方式をPAPに設定する必要があります。

[Switch] dot1x authentication-method PAP

Windows Server 2016 NPSサーバーの構成

「Windows Server 2016 NPSサーバーの構成」の説明に従って、NPSサーバーを構成します。ただし、ネットワークポリシーの認証方法として、暗号化されていない認証(PAP、SPAP)を指定する必要があります。

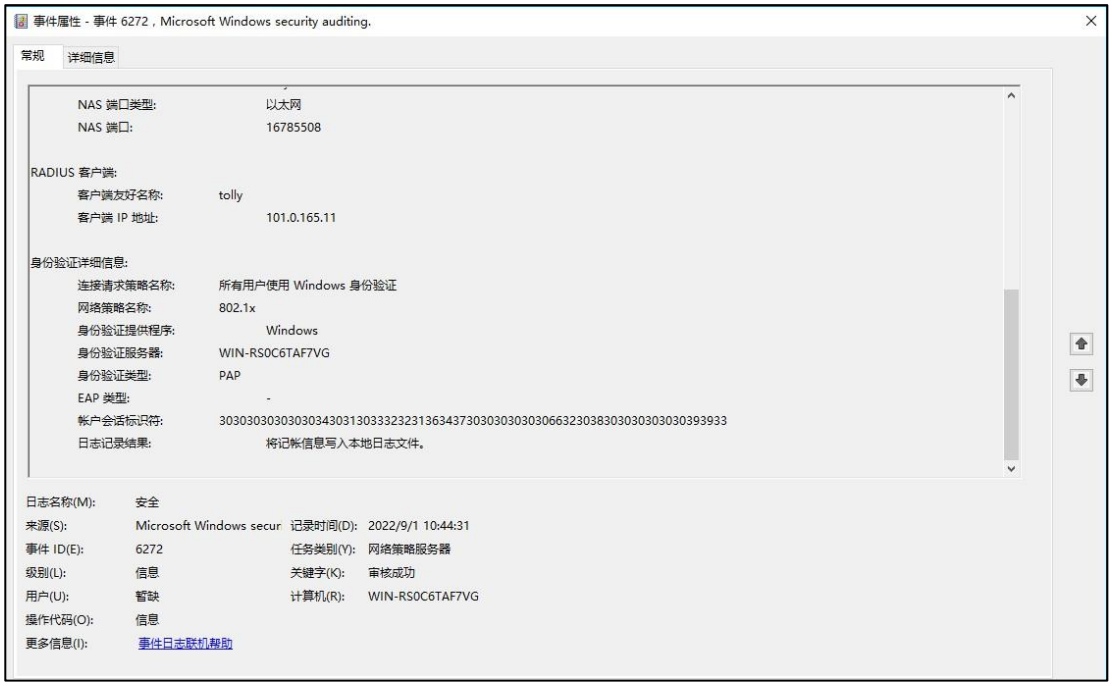
図42 認証方式の指定



設定の確認

1. ユーザー名とパスワードを入力した後、iNodeクライアントを使用して、802.1X認証をパスしてオンラインになることを確認します(詳細は表示されません)。
2. NPSサーバーで、オンラインユーザーに関する情報を表示します。

図43 ユーザーアクセス情報の表示



3. オンライン802.1X認証ユーザーに関する情報を表示するには、スイッチ上でdisplay dot1x connectionコマンドを使用します。

[Switch] display dot1x connection

Total connections: 1

Slot ID: 1

User MAC address: a036-9f8b-634c

Access interface: Ten-GigabitEthernet1/0/2

Username: user

User access state: Successful

Authentication domain: domain1

EAP packet identifier: 2

Authentication method: PAP

AAA authentication method: RADIUS

Initial VLAN: 165

Authorization untagged VLAN: N/A

Authorization tagged VLAN list:

N/A Authorization VSI: N/A

Authorization microsegment ID:

N/A Authorization ACL

number/name: N/A Authorization

dynamic ACL name: N/A

Authorization user profile: N/A

Authorization CAR: N/A

Authorization URL: N/A

Authorization IPv6 URL: N/A

Authorization temporary redirect: Disabled

Start accounting: Successful

Real-time accounting-update failures: 0

Termination action: Default

Session timeout period: N/A

Online from: 2013/01/03

08:25:51 Online duration: 0h

0m 8s

The output shows that the user has passed 802.1X PAP authentication and come online.

設定ファイル

```
#
 dot1x
dot1x authentication-method
pap #
interface Ten-GigabitEthernet1/0/2
 port link-mode bridge
 port link-type hybrid
 port hybrid vlan 1 100 165
 untagged port hybrid pvid vlan 165
undo dot1x handshake
 dot1x mandatory-domain
 domain1 undo dot1x
 multicast-trigger dot1x port-
 method portbased
#
domain domain1
 authentication lan-access radius-scheme radius1
 authorization lan-access radius-scheme radius1
 accounting lan-access radius-scheme radius1
#
radius scheme radius1
 primary authentication 101.0.144.123
 primary accounting 101.0.144.123
 key authentication cipher
 $c$3$9jjl0lp5VA/WXEw065ZIT7j4AIN88XTF key accounting
 cipher $c$3$fk1zm9nf2IFMdk+I7hGsyBcsAwqLobi7 user-name-
 format without-domain

#
```

例:VLAN割り当てを使用した802.1XまたはMAC認証の設定

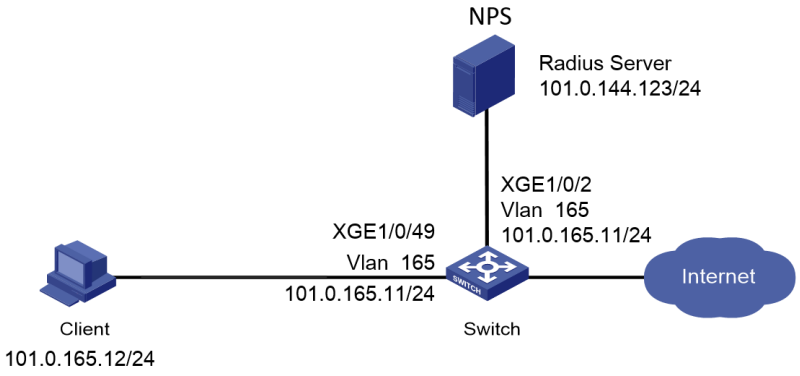
ネットワーク構成

図44に示すように、Windows Server 2016 NPSサーバーと連携してクライアントの802.1XまたはMAC認証を実行するようにスイッチを構成します。クライアントがネットワークリソースにアクセスするには、802.1XまたはMAC認証を通過する必要があります。

スイッチを次のように設定します。

- NPSサーバーをRADIUSサーバーとして使用し、クライアントに対して802.1XまたはMAC認証を実行します。
- クライアントが802.1XまたはMAC認証を通過した後で、クライアントに承認VLANを割り当てるようにNPSサーバーを構成します。初期VLANは144です。

図44 ネットワークダイアグラム



使用されるソフトウェアのバージョン

この設定例は、次のハードウェアおよびソフトウェアバージョンで作成され、検証されています。

ハードウェア	ソフトウェアのバージョン
S5560X-54C-PWR-EIスイッチ	バージョン7.1.070
認証サーバー	Windows Server 2016 NPSの場合

例:VLAN ID割り当てを使用した802.1XまたはMAC認証の設定

スイッチの設定

MAC認証ユーザーの場合は、「スイッチの設定」の説明に従ってスイッチを設定します。

802.1X認証ユーザーの場合は、「スイッチの設定」の説明に従ってスイッチを設定します。

Windows Server 2016 NPSサーバーの構成

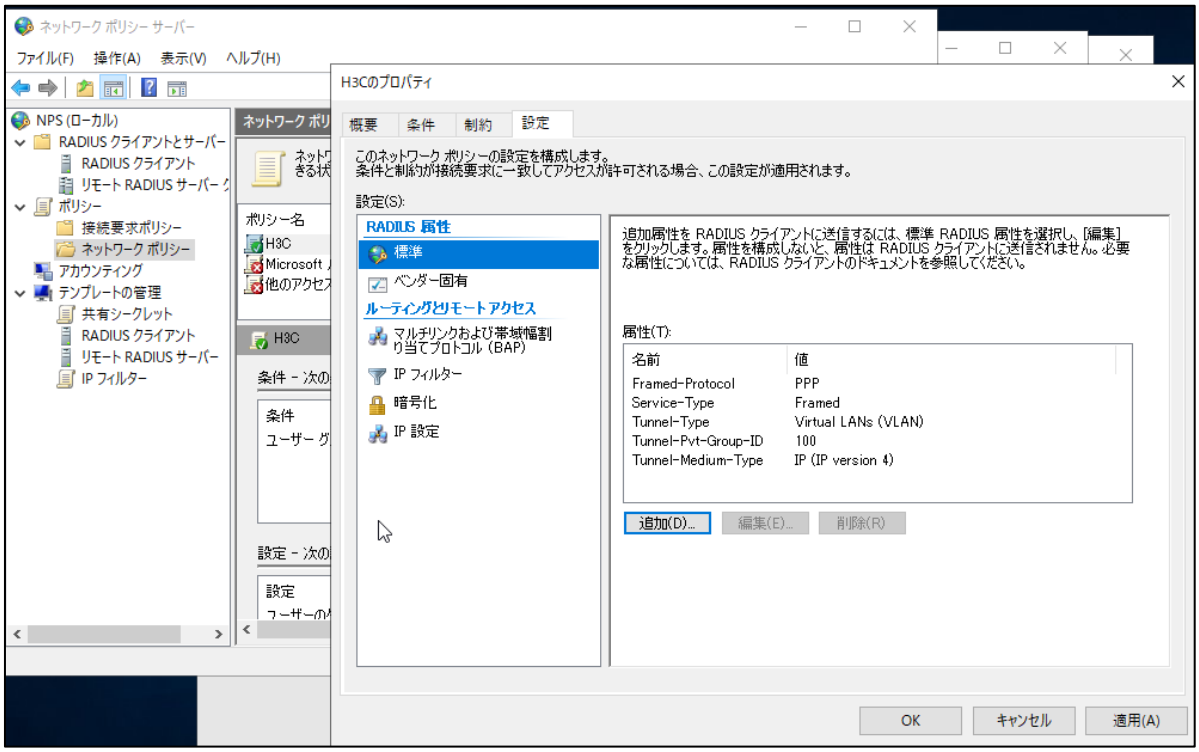
基本設定を構成します。

- 「Windows Server 2016 NPSサーバーの構成」の説明に従って、MAC認証ユーザー用にNPSサーバーを構成します。
- 「Windows Server 802.1 NPSサーバーの構成」の説明に従って、2016 Xユーザー用にNPSサーバーを構成します。

VLAN割り当ての場合は、ネットワークポリシーの**設定**タブでRADIUSアトリビュートを次のように編集する必要があります。

- Tunnel-Medium-Typeアトリビュートを追加してトンネルメディアタイプを指定し、アトリビュートの値を802(すべての802メディアとイーサネット標準フォーマットを含む)に設定します。
- Tunnel-Pvt-Group-IDアトリビュートを追加して、割り当てるグループVLAN IDを指定し、アトリビュートの値を設定します。この例では、100が使用されています。
- Tunnel-Typeアトリビュートを追加して、使用するトンネリングプロトコルを指定し、アトリビュートの値をVirtual LAN(VLAN)に設定します。

図45 ネットワークポリシーのRADIUS属性の指定



設定の確認

1. NPSサーバーで、オンラインユーザーに関する情報を表示します。

図46 ユーザーのオンライン情報の表示

2. スイッチで、802.1XまたはMAC認証ユーザーに、指定された認可VLAN IDが正しく割り当てられていることを確認します。

#オンライン802.1X認証ユーザーに関する情報を表示するには、display dot1x connectionコマンドを使用します。

<Switch> display dot1x connection

Total connections: 1

Slot ID: 1

User MAC address: a036-9f8b-634c

Access interface: Ten-GigabitEthernet1/0/2

Username: user

User access state: Successful

Authentication domain: domain1

EAP packet identifier: 2

Authentication method: CHAP

AAA authentication method: RADIUS

Initial VLAN: 165

Authorization untagged VLAN: 100

Authorization tagged VLAN list:

N/A Authorization VSI: N/A

Authorization microsegment ID:

N/A Authorization ACL

number/name: N/A Authorization

dynamic ACL name: N/A

Authorization user profile: N/A

Authorization CAR: N/A

Authorization URL: N/A

Authorization IPv6 URL: N/A

Authorization temporary redirect: Disabled

Start accounting: Successful

Real-time accounting-update failures: 0

Termination action: Default

Session timeout period: N/A

Online from: 2013/01/08

06:52:03 Online duration: 0h

0m 14s

#オンラインMAC認証ユーザーに関する情報を表示するには、display mac-authentication connectionコマンドを使用します。

[Switch]display mac-authentication connection

Total connections: 1

Slot ID: 1

User MAC address: 0010-9400-0005

Access interface: Ten-GigabitEthernet1/0/2

Username: 001094000005

User access state: Successful

Authentication domain: domain1

IPv4 address: 192.85.1.2

IPv4 address source: User

packet Initial VLAN: 165

Authorization untagged VLAN: 100

Authorization tagged VLAN: N/A

Authorization VSI: N/A

Authorization microsegment ID:

N/A Authorization ACL

number/name: N/A Authorization

dynamic ACL name: N/A

Authorization user profile: N/A

Authorization CAR: N/A

Authorization URL: N/A

Authorization IPv6 URL: N/A

Authorization temporary redirect: Disabled

Start accounting: Successful

Real-time accounting-update failures: 0
Termination action: Default
Session timeout period: N/A
Offline detection: 300 sec (command-configured)
Online from: 2013/01/08 06:25:15
Online duration: 0h 0m 8s
Port-down keep online: Disabled (offline)

この出力は、VLAN 100がユーザーに正常に割り当てられたことを示しています。

設定ファイル

次に、802.1X認証の例を示します。

```
#
 dot1x
#
interface Ten-GigabitEthernet1/0/2
 port link-mode bridge
 port link-type hybrid
 port hybrid vlan 1 100 165
 untagged port hybrid pvid vlan
 165
undo dot1x handshake
 dot1x mandatory-domain
 domain1 undo dot1x
 multicast-trigger dot1x
 port-method portbased
#
domain domain1
 authentication lan-access radius-scheme radius1
 authorization lan-access radius-scheme radius1
 accounting lan-access radius-scheme radius1
#
radius scheme radius1
 primary authentication 101.0.144.123
 primary accounting 101.0.144.123
 key authentication cipher
 $c$3$9jjl0lp5VA/WXEw065ZIT7j4AIN88XTF key accounting
 cipher $c$3$fk1zm9nf2IFMdk+I7hGsyBcsAwqLobi7 user-
 name-format without-domain
#
```