H3Cスイッチと

Windows Server 2016 NPS認証サーバー統合ガイド

Copyright©2023 New H3C Technologies Co., Ltd. 無断複写・転載を禁じます。

本書のいかなる部分も、New H3C Technologies Co.,Ltd.の事前の書面による同意なしに、いかなる形式または手段によっても、複製または送信することはできません。

New H3C Technologies Co.,Ltd.の商標を除き、本書に記載されているすべての商標は、それぞれの所有者に帰属します。 このドキュメントの情報は、予告なしに変更されることがあります。

内容

序	2
認証方法におけるH3CスイッチとWindows Server 2016 NPSの互換性	2
前提条件	2
例:MAC認証の構成	3
ネットワーク設定	3
使用されるソフトウェアのバージョン	3
例:共有ユーザーカウントを使用したMAC認証の設定	4
設定ファイル	
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	22
スイッチの設定	22
Windows Server 2016 NPSサーバーの構成	
設定の確認	
例:802.1X認証の設定	
ネットワーク構成	
使用されるソフトウェアのバーション	
例:LDAPサーバーを介したローカルボータル認証の設定	28
ネットワーク構成	
使用されるソフトウェアのバージョン	
キ順 ふウのな辺	
設定ファイル	
例:802.1X CHAP認証の設定	
例:802.1X PAP認証の設定	39
例:VLAN割り当てを使用した802.1XまたはMAC認証の設定	42
ネットワーク構成	42
使用されるソフトウェアのバージョン	42
例:VLAN ID割り当てを使用した802.1XまたはMAC認証の設定	42
Windows Server 2016 NPSサーバーの構成	42

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

🌄 リモート デスクトップ接続	-		Х
リモート デスクトップ 接続			
コンピューター(C): 101.0.144.123 ユーザー名: 指定されていません	~		
接続時には資格情報を要求されます。 ③ オプションの表示(Q) 接続(N)		ヘルプ(H)

#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

♥ Windows セキュリティ	×
資格情報を入力してくだ	さい
これらの資格情報は、10.10.11.34	への接続に使用されます。
Administrator	
パスワード	
このアカウントを記憶する	
その他	
ОК	キャンセル

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

📥 サーバー マネージャー		– 🗆 X
 ダッシュ 		俚(M) <mark>ツール(T)</mark> 表示(V) へルプ(H)
	サーバー マネージャーへようこそ	iSCSI イニシエーター Microsoft Azure サービス ODBC Data Sources (32-bit) ODBC データ ソース (64 ビット)
■■ すべてのサーバー ■■ ファイル サービスと記憶域サ ▷	1 このローカル・ 24ックスタート(0)	Windows PowerShell Windows PowerShell (x86) Windows PowerShell ISE
	2 役割と機能	の Windows PowerShell ISE (x86) Windows Server パックアップ
	3 管埋するサ- 最新情報(W) 4 サーバー グル	- / Windows メモリシショア イベント ビューアー ノー コンピューターの管理
	5 このサーバーマ	コンボーネント サービス サービス
	詳細情報(L) <	システム構成 システム情報 ヤキュリティが強化された Windows Defender ファイアウォール
	役割とサーバー グループ	タスク スケジューラ ディスク クリーンアップ ビニィゴのビコニガレ長 声ル
	121日の数:「「リーハーソルーノの数:」「リーハーの占計数:」	「 「マイノルテノランと鉄道化 パフォーマンス モニター リソース モニター
		レジストリ エディター ローカル セキュリティ ポリシー 印刷の管理
		回復ドライブ

#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

🛃 ローカル セキュリティ ポリシー			– 🗆 X
ファイル(F) 操作(A) 表示(V) ヘルプ(H)			
🗢 🔿 🙍 📷 🗙 🗐 🔒 🛛 🗊			
セキュリティの設定 アカウント ポリシー スワードのポリシー スワードのポリシー ローカル ポリシー セキュリティが強化された Windows Defer ホットワーク リスト マネージャー ポリシー 公開キーのポリシー ジリアウェアの制限のポリシー アブリケーション制御ポリシー アリケーション制御ポリシー ま査ポリシーの詳細な構成	 ポリシー ペスワードの長さ パスワードの変更禁止期間 パスワードの有効期間 パスワードの履歴を記録する 暗号化を元に戻せる状態でパスワードを引いたす必要があるパスワ 	セキュリティ 0文字以_ 0日 42日 0回 呆存する 有効 −ド 有効	の設定 E

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

📥 サーバー マネージャー			– 🗆 X
	ボード	• @ 🗗	管理(M) ッール(T) 表示(V) ヘルプ(H) 役割と機能の追加
ダッシュボード	サーバー マネージャーへようこそ		役割と機能の削除 サーバーの追加
■ ローカル サーハー ■ すべてのサーバー ■ ファイル サービスと記信博サート		1 このローカ	サーバー グループの作成 サーバー マネージャーのプロパティ
	クイック スタート(Q)	2 役割と機	能の追加
		3 管理する	サーバーの追加
		4 サ−バ− グ	ループの作成
	詳細情報(L) <	5 このサーバ	ーをクフワト サーヒスに接続す 非表示 >
	役割とサーバー グループ 役割の数: 1 サーバー グループ	D数:1 サーバーの合計数	ğ:1 ~

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

🚵 役割と機能の追加ウィザード		<u>111</u> 1		×
インストールの種類	の選択	WIN-H	対象サ- 3UVFNM3	/(- 9Al
開始する前に インストールの種類 サーバーの選訳 サーバーの役割 機能 確認 諸果	インストールの種類を選択します。役割および機能は、実行中の物理コンピューター、仮想コンピュ の仮想ハード ディスク (VHD) にインストールできます。	ーター、ま	たはオフラ スまたは セ	5イン 9€93
	< 前へ(P) 次へ(N) > インストー	JL (1)	キャンセ	ル

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

🏊 役割と機能の追加ウィザード				-		×
対象サーバーの選択				WIN-I	対象サー H3UVFNM3	パー 9AI
開始する前に インストールの種類 サーバーの選択 サーバーの役割 機能 確認	役割と機能をインストールする ● サーバー プールからサーバー ○ 仮想ハード ディスクから選 サーバー プール フィルター:	5サ−バ−または仮想八 -を選択 択	-ド ディスクを選択します。			
結果	名前 MINI LIDLR/ENIADOAL	IP アドレス	オペレーティング システム	2010 01 - 1 - 1		
	1 台のコンビューターが見つか このページには、サーバーマネ- それ以降のリリースの Windo てデータ収集が完了していない	りました -ジャーの [サーバーの過 ws Server を実行して いサーバーは表示されま	加] コマンドを使用して追加された、 いるサーバーが表示されます。オフラ せん。	Windows Serv イン サーバーや、新	er 2012 ま 新たに追加	たは され
		< 前	fへ(P) 次へ(N) >	インストール(I)	キャンセ	JL

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。

≧ 役割と機能の追加ウィザ−ド			-		×
サーバーの役割の選	択		WIN-H	対象サー 3UVFNM3!	/(- 9AI
開始する前に	選択したサーバーにインストールする役割を 1 つ以上選択します。				
インストールの種類	役割	説明			
サ <i>−</i> パ <i>−</i> の選択 サ <i>−</i> パ−の役割 機能 確認 結果	 Active Directory Rights Management サーとス Active Directory ドメイン サービス Active Directory デトウェイト ディレクトリ サービス Active Directory 証明書サービス DHCP サーバー DNS サーバー FAX サーバー Host Guardian サービス Hyper-V Web サーバー (IIS) Windows Server Update Services Windows Kalley センス デバイス正常性場成証明 ネットワークボリシービス センス アイル サービス 記憶域サービス (1/12 個をインストール): ボリューム ライセンス認証サービス リモート デスクトッブ サービス マ 同副とドキュメント サービス 	ネットワーク ポリシー 提供するネットワー/ (NPS) は、ネットワー 護に役立ちます。	-とアクセン クポリシー ークのセキ	ス サービス; - サーバー ュリティの∮	が 呆
	<前へ(P) 次へ(N) >	> インスト-	-ル(I)	キャンセ	μ

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

📥 サーバー マネージャー			_	- 🗆 X	
 ダッシュ 	_ボード •	· ③ 🗗 🕯	理(M) <mark>ツール(T)</mark> 表	表示(V) ヘルプ(H)	
 <i>望 ダッシュボード</i> □ーカルサーバー ■ すべてのサーバー ? NPAS ■ ファイル サービスと記憶域サ ▷ 	サーバー マネージャーへようこそ クイック スタート(Q) 最新情報(W)	このローカル 2 役割と機能 3 管理するサ 4 サーバーグリ	iSCSI イニュ Microsoft ODBC Dat ODBC プー ササ Windows Windows Windows Windows Windows Windows	シエーター Azure サービス ta Sources (32-bit) - ク ソース (64 ビット) PowerShell PowerShell (x86) PowerShell ISE PowerShell ISE (x86) Server パックアップ メモリ診断 1-アー - の管理	
	詳細情報(L) < 役割とサーバーグループ 役割の数: 2 サーバーグループのま	 す ダイイング 5 このサーバー 5 このサーバー 	レ コンポーネン タービス システム構 システム構 セキュリティ タスクスケジ ディスククリ ネットワーク	パト サービス 成 報 が強化された Window ジューラ リーンアップ 「フラグと最適化 「ポリシー サーバー	rs Defender ファイアウォール
			パフォーマン リソース モロ レジストリコ ローカル セ 印刷の管理 回復ドライ:	ス モニター ニター エディター キュリティ ポリシー 星 ブ	

#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

新しい RADIUS クライアント	×
設定詳細設定	
☑ この RADIUS クライアントを有効にする(E)	
□ 既存のテンプレートを選択する(T):	
✓	
名前とアドレス フレンドリ名(F):	
tolly	
アドレス (IP または DNS)(D):	
101.0.165.11 確認(\/)	
共有シークレット 既存の共有シークレット テンプレートを選択(M):	
なし ~	
共有シークレットを直接入力する場合は [手動] をクリックし、 自動で生成する場合は [生成] をクリックします。ここに指定した共有シークレットを、 RADIUS クライアントの構 成時にも指定する必要があります。 共有シークレットでは大文字と小文字が区別どれ ます。	
 ● 手動(U) ○ 生成(G) 共有シークレット(S): 	
•••••	
共有シークレットの確認入力(0):	
OK キャンセノ	Ψ

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

🔁 サーバー マネージャー	– 🗆 X
 ・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・	<mark>ツール(T)</mark> 表示(V) ヘルプ(H) iSCSL イーシェーター
The set of the	iSCSI イニシエーター Microsoft Azure サービス ODBC Data Sources (32-bit) ODBC $\vec{\tau}$ - タ ソース (64 ビット) Windows PowerShell Windows PowerShell (x86) Windows PowerShell ISE Windows PowerShell ISE Windows Server パックアップ Windows Server パックアップ Vindows Server パックアップ Server Server Se

#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

	- C	ı x
ファイル(F) 操作(A) 表示(V) ヘルプ(H)		
書 コンピューターの管理(ローカル) 名前	操作	
◇ 悩 システムツール 11 システムツール	コンピューターの管理 (ロー	·カル) 🔺
> 図 イベントビューアー 目出 ビマル ITTUE Serve	他の操作	+
> 刻 共有フォルダー ・ 1 サービス C ア J リワーション		
新しいユーザー(N)		
> (N) パワ: 最新の情報に更新(F)		
□ 5 / · · · · · · · · · · · · · · · · · ·		
> 🐌 Windows Server バックア		
置 デイメノの管理 、 ■、サービスとアプリケーション		
< >>		
新しいローカル ユーザー アカウントを作成します。	-	

#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

新しいユーザー N				?	Х
63					
ユーザー名(U):	user				
フル ネーム(F):	user				
説明(D):	user				
パスワード(P):		•••••			
パスワードの確認入け	ታ(C):	•••••			
🗹 ユーザーは次回口	グオン時	こパスワードの変更がぬ	必要(M)		
🗌 ユーザーはパスワー	ドを変更	できない(S)			
□ パスワードを無期	限にする	W)			
□ アカウントを無効(こする(B)				
ヘルプ(H)			作成(E)	閉じる((0)

#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

ファレル・掛け(A) 表示(V) ヘルブ(H) ● 「「」」」」 ● 「」」 ● 「」」」 ● 「」」 ● 「」」」 ● 「」」 ● 「」」」 ● 「」」 ● 「」」」 ● 「」」 ● 「」」 ● 「」」 ● 「」」 ● 「」」 ● 「」」 ● 「」」 ● ● ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○	🛃 コンピューターの管理		- 🗆 X
 ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ●	ファイル(F) 操作(A) 表示(V) ヘルプ(H	8)	
 ■ 272/2-7-06定理(0-7)/l) ● 272 スパジューラ ● 272 スパジューラ ● 274 スパントビューア- ● 275 スパントビューア- ● 01-7)/1 ユーザー ● 01-7)/1 ユーザー ● 01-7)/1 ユーザー ● 01-7)/1 マーサー ● 01-7)/1 マーサ ● 01-7)/1 マーサー ● 01-7)/1 マーサ ● 01-7)/1 ○ 01-1 (01-7)/1 ○ 01-1 (01-7)/1 ○ 01-1 (01-1)/1 ○ 01-1 (01-1)/1 ○ 01-1 (01-1)/1 ○ 01-1 (01-1)/1 ○ 01-1 (01-1)/1 ○ 01-1 (01-1)/1 ○ 01-1 (01-1)/1 ○ 01-1 (01-1)/1 ○	🗢 🍣 🙋 📰 🗙 🖾 🗟 🗖 🗖	userのプロパティ ? ×	
	■ コンビューターの管理(ローカル)	全般 所属するグルーブ プロファイル 環境 セッション リモート制御 リモートデスクトップ サービスのプロファイル ダイヤルイン リモート アクセス許可 ・ アクセスを許可(W) (* アクセスを許可(W) ・ アクセスを指否(D) (* NPS ネットワーク ポリシーでアクセスを制御(P) 「 発信者番号を確認(V): コールパック オブション ・ - ・ コールパック オブション ・ ・ コールパック レマック(Y): ・ ● 静的 IP アドレスを割り当てる(I) このダイヤルイン接続に対して有効にする IP アドレス(T) このダイヤルイン接続に対して有効にする IP アド 静的 IP アドレス(T) このダイヤルイン接続に対して有効にする IP・トを定 静的 IP・トド(い) 、 OK キャンセル 通用(A) ヘルレブ	 <u> 温</u> -ザ- ▲ 他の操作 ▶ user ▲ 他の操作 ▶

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

コンピューターの管理	(ローカル)	名前		說明	操作	
> (1) 9727 7-1		Access Contro	Assista	このグループのメンバーは、このコンピュー	グループ	•
> 🛃 イベントビュ	1-7-	Backup Opera	s	コンビューター/トメインに完全なアクセス Backup Operators は、パックアップの	他の操作	•
> 図 共有フォルク	9-	Certificate Ser	vice DC	このグループのメンバーは、エンタープライ		
✓ 20 □-カルユー □-カルユー	-サーとクルーフ	Sryptographic	Operat	メンバーは、暗号化操作の実行を許		
■ ユーリー ○ グルーゴ	e	Device Owner	s	このグループのメンバーは、システム全体		
> (1) /(77-5	新しいグルー	·プ(N)	1 Users	メンバーは、このコンピューターで分散 C		
書 デバイス	表示(V)	>	ers	このグループのメンバーは、ローカル コン		
✓ ■記憶域				既定では Users グループのメンバーと…		
> 🚯 Windo	食物の情報	ミに更新(ト)	strators	このクループのメンバーには、Hyper-V		
□ 11×20	一覧のエク、	スホート(L)	uratio	インション・ション ション ション ション ション ション ション ション ション ション		
in the second	へルプ(H)		a Users	このグループのメンバーは、このコンピュー		
		Performance I	Monitor	このグループのメンバーは、ローカルやリ		
		Power Users		Power Users は、後方互換のための		
		Print Operator	rs	ドメイン コントローラーにインストールされ		
		RDS Endpoint	Servers	このグループのサーバーは、仮想マシンを		
		RDS Managen	nent Ser	このクループのサーバーは、リモートテス		
		RUS Remote A	access S	このグループのサーバーは、RemoteAp		
		Remote Mana	dement	このグループのメンバーにはタモートからロ		
		Replicator	gement	ドメイン内のファイル レブリケーションを		
		Storage Replic	a Admi	このグループのメンバーには、記憶域レ		
		System Manag	ged Acc	このグループのメンバーはシステムで管		
		Users Users		ユーザーが、システム全体に及ぶ変更を		

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

新しいグループ			?	×
グループ名(G):	group1			
説明(D):				
所属するメンバー(M):				
追加(A)	削除(R)			
ヘルプ(H)		作成(C)	閉じる(O))

図19 グループへのメンバーの追加

ユーザー の選択	×
オブジェクトの種類の選択(S): ユーザー または ビルトイン セキュリティ プリンシパル	オブジェクトの種類(O)
場所の指定(F): WIN-H3UVFNM39AI	場所(L)
選択するオブジェクト名を入力してください (例)(<u>E</u>): WIN-H3UVFNM39Al¥user	名前の確認(C)
詳細設定(A) OK	キャンセル

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選択します。ホ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

🚳 ネットワーク ポリシー サーバー		_		×
ファイル(F) 操作(A) 表示(V) /	ルプ(H)			
🗢 🄿 🙍 📰 🚺				
● NPS (ローカル)	ネットワーク ポリシー			
 ADJUS クライアントとサーバー ボリシー 接続要求ポリシー 接続要求ポリシー 	ネットワーク ポリシーでは、ネットワークへの接続を許可するユーザーと、これらのユ きる状況と接続できない状況を指定できます。	.ーザーがネットワ	ークに接続て	
Marting 新規(N)	状態 処理順序	アクセスの種類	ソース	
> 🌉 テンプレートの 一覧のエク	スポート(L) 有効 1 イバガンリモート アクセス サーバーへの接続 有効 999998	アクセスを許… アクセスの拒否	指定なし 指定なし	
表示(V)	> バーへの接続 有効 999999	アクセスの拒否	指定なし 指定なし	
最新の情報	に更新(F)			
ヘルプ(H)				
	条件 - 次の条件を満たしている場合:			
	条件 値			
	設定 - 次の設定が適用されます:			_
	設定値			
	<			>

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

新しいネットワーク ポリ	۶- ×
条 题 描述	件の指定 聴要求に対してこのネットワーク ポリシーを評価するかどうかを決定する条件を指定します。少なくとも 1 つの条件が必要 で
条件(C):	条件の選択 ×
条件 	 条件を選択し、「追加」をクリックします。 グルーブ Windows グルーブの条件は、接続ユーザーまたは接続コンピューターが選択されたグルーブのいずれかに所属している必要があることを指定します。 コンピューターグルーブ コンピューターグルーブの条件は、接続するコンピューターが選択したグルーブのいずれかに属している必要があることを指定します。 ユーザーグルーブの条件は、接続オるコンピューターが選択したグルーブのいずれかに属している必要があることを指定します。 目付と時刻の制限 目付と時刻の制限 日付と時刻の制限(は、接続の試行を許可または拒否する日時を指定します。これらの制限は、NPS サーバーのある場
条件の説明	所のタイム ソージに基づいて指定してください。 「追加(D)… キャンセル 「追加(D)… 「編集(E)… 」 『川珍(R) 「 」 「 」 「 」 」 」
	前へ(P) 次へ(N) 完了(F) キャンセル

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

グループの選択	×
オブジェクトの種類の選択(S):	
グループ	オブジェクトの種類(O)
場所の指定(F):	
WIN-H3UVFNM39AI	場所(L)
選択するオブジェクト名を入力してください (例)(E):	
WIN-H3UVFNM39Al¥group1	名前の確認(C)
詳細設定(A)	OK キャンセル

#条件が指定されました。

図24 グルー	プの条件の指定
気いネットワーク	7 ポリシー ×
	条件の指定 接続要求に対してこのネットワーク ポリシーを評価するかどうかを決定する条件を指定します。 少なくとも 1 つの条件が必要 です。
条件(<u>C</u>):	
条件 ^梁 ユーザー	値 ヴループ WIN-H3UVFNM39AI¥group1
条件の説明: ユーザー グルー	ブの条件は、接続ユーザーが選択されたグループのいずれかに所属している必要があることを指定します。 道加(D) 編集(E) 削除(B)
	前へ(P) 次へ(N) 完了(F) キャンセル

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

ペ 新しいネットワーク ポリシー ×	<
アクセス許可の指定 接続要求がこのポリシーに一致する場合に、ネットワーク アクセスを許可するかまたは拒否するかを構成します。	
 アクセスを許可する(A) クライアントの接続試行がこのポリシーの条件に一致する場合、アクセスを許可します。 アクセスを拒否します。 ユーザー ダイヤルイン プロパティ (NPS ポリシーよりも優先される) によってアクセスを判断する(S) クライアントの接続試行がこのポリシーの条件に一致する場合、ユーザー ダイヤルイン プロパティに応じてアクセスを許可または拒否します。 	
前へ(P) 次へ(N) 完了(E) キャンセル	

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

新しいネットワーク ポリシー	Х
認証方法の構成 接続要求がこのポリシーの条件を満たすために必要な認証方法を、1 つ以上指定してください。 EAP 認証には、 EAP の 類を構成する必要があります。)種
EAP の種類は、NPS とクライアントとの間で、表示されている順序でネゴシェートされます。	
EAP の種類(1): 上へ移動(U) 達加(D) 編集(E) 削除(B) ************************************	
前へ(P) 次へ(N) 完了(E) キャンセル	

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

常规 详细信	ŧ.						1
网络策略服务	器已向某个用户授予	币访问权限。				^	
用户:	10.	WINL 1DD01//41 ELID					
女王	10: 5%-	WIN-IDP9IK4L50P\user					
*** つ	≕ ಗ್ರ.	WIN-1D00K/USUD					
完全的	%* 艮定的帐户名称:	WIN-1DP9IK4L5UP\user					
nter also beix \ 1 (00° 4/7)							
各户病计异机。	ID.						
又土 能白?	1D: Σ¥≂.	NOLL SID					
	317. 昆宁的能白乞狗·						
被调题	我们的"百姓"	00-E0-24-50-40-2B					
调用如	alana (1997) alana (1997)	A0-36-9F-8B-63-4C					-
NAS:							+
NAS	IPv4 地址:	101.0.165.11					
NAS	IPv6 地址:	-					
NAS	标识符:	tolly					
NAS	端口类型:	以太网					
NAS	靖口:	16785508					
」 日志名称(M):	安全						
来源(S):	Microsoft W	/indows securi 记录时间(D);	2022/11/2 15:26:07				
事件 ID(F):	6272	任备举别(Y);	网络策略服务器				
级别们	信自	关键字(K)·	审核成功				
用户(U):	新辞	计算机(R):	WIN-1DP9IK4I 5UP				
握作代码(O):	信息						
更多信息(I):	事件日志联核	几帮助					
复制(P)						关	闭(C)

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 macauthentication 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 macauthentication 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。

🌆 コンピューターの管理					- C	ı x		
ファイル(F) 操作(A) 表示(V)	ファイル(F) 操作(A) 表示(V) ヘルブ(H)							
🗢 🔿 🖄 📰 🙆 🛃 👔								
🌆 コンピューターの管理 (ローカル)	名前	フル ネーム	説明		操作			
◇ 🎁 システムツール	Administrator		コンピューター/ドメインの管理用 (ビルト		ユーザー			
> 🕑 ダスク スケシューフ	DefaultAcco		システムで管理されるユーザー アカウン		他の操作	•		
ション ジョン・ション ジョン・ション ジョン・ション ジョン・ション・ション ひょうしょう しょうしょう ひょうしょう ひょう ひょうしょう ひょう ひょう ひょう ひょう ひょう ひょう ひょう ひょう ひょう ひ	f010903ef7e0	f010903ef7e0	my ap					
∽ 🌆 ローカル ユーザーとグループ	🛃 Guest		コンピューター/ドメインへのゲスト アクセ					
☐ 7-#f-	l Ser user	user	user Windows Defender Application G					
新しいユーサー	(N)		windows belender Application G					
> (M) パパ 表示(V)	>							
✓ 営 記憶域 最新の情報に	:更新(F)							
> 🐏 Win ―覧のエクスオ	ポート(L)							
■ デイス ■ サービス AILプ(H)								
> 10 9-EXC - 002(0)								
深切した商日の人間プをまテします					1			
選択した項目のハルノを救示します。								

図28 新しいユーザーの追加

図29新しいユーザーの設定

奈仁 いつし折し		2	\sim
		:	^
ユーザー名(U):	c8e265355de0		
フル ネーム(F):	c8e265355de0		
説明(D):	c8e265355de0		
パスワード(P):	•••••		
パスワードの確認入	.カ(C):		
□ ユーザーは次回	ログオン時にパスワードの変更が必要(M)		
□ ユーザーはパスワ	ラードを変更できない(S)		
□ パスワードを無其	月限にする(W)		
□ アカウントを無効	かにする(B)		
ヘルプ(H)	作成(E)	閉じる((D)

図30 グループの作成



図31 グループ名の入力

新しいグループ			?	×
グループ名(G):	group2			
説明(D):				
所属するメンバー(M)	:			
追加(A)	削除(R)			
ヘルプ(H)		作成(C)	閉じる(C))

図32 グループへのメンバーの追加

新しいグループ		?	\times			他の操作
グループ名(G):	group2					
説明(D):						
所属するメンバ-	(M):					
	ユーザー の選択					×
	オブジェクトの種類の選択(S):					
	ユーザー または ビルトイン セキュリティ プリンシパル				オブジ	ジェクトの種類(O)
	場所の指定(F):					
	WIN-H3UVFNM39AI					場所(L)
	選択するオブジェクト名を入力してください (<u>例)(E)</u> :					
追加(A)	WIN-H3UVFNM39AI¥c8e265355de0				4	名前の確認(C)
ヘルプ(H)	詳細設定(A)			OK	:	キャンセル

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

푝	┣件 6272	, Microsoft	: Windows secur	ity auditing.			
	常规	详细信息					
_							
	网络第	節略服务器已	向某个用户授予	访问权限。			
	用户:						
		安全 ID:		WIN-5RKO	EVTVVAD\001	094000005	
		帐户名称	:	001	094000005		
		帐户域:		WIN-5RKO	EVTVVAD		
		完全限定	的帐户名称:	WIN-5RKO	EVTVVAD\001	094000005	
	客户端	\计算机:					
		安全 ID:		NULL SID			
		帐户名称	:	-			
		完全限定	的帐户名称:	-			
	1	· · · · · · · · · · · · · · · · · · ·	±=>=10%*.	00 50 34 50	40.34		
	日志名	称(M):	安全				
	来 源(S)):	Microsoft Wi	ndows securi	记录时间(D):	2022/9/5 17:38:00	
	事件 II	D(E):	6272		任务类别(Y):	网络策略服务器	
	级别(L)):	信息		关键字(K):	审核成功	
	用户(U):	暂缺		计算机(R):	WIN-5RKOEVTVVAD	

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 macauthentication 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。

図34 ネットワークダイアグラム

- 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。
 - NPS Radius Server 101.0.144.123/24 XGE1/0/2 Vlan 165 101.0.165.11/24 Vlan 165 101.0.165.11/24 Liternet Switch

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] Idap server ccc

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

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

[Switch-Idap-server-ccc] ip 101.0.144.124

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

[Switch-Idap-server-ccc] quit

#LDAPスキームIdap1を作成し、LDAP認証サーバーをcccとして指定します。

[Switch] Idap scheme Idap1

[Switch-Idap-Idap1] authentication-server ccc

[Switch-Idap-Idap1] 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

 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	ージ
---------------	----

Usemane user
Leg In Leg In Copyright 2: 2004 2022 None 10C Technologies Co., 186AB righty reserved.

```
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

事件 4624	, Microsoft	Windows secur	ity auditing.		
常规	详细信息				
已成功	登录帐户。				
使用者					
	安全 ID:	NULL S	SID		
	帐户名称:		-		
	帐户域:	-			
	登录 ID:	0x0			
登录信	息:				
	登录类型:		3		
	受限制的智	理员模式:	-		
	虚拟帐户:		否		
	提升的令牌	₽ :	是		
日志名和	弥(M):	安全			
来源(S):	:	Microsoft Wi	ndows securi	记录时间(D):	2022/9/6 19:00:23
事件 ID	(E):	4624		任务类别(Y):	登录
级别(L):	:	信息		关键字(K):	审核成功
用户(U)	:	暂缺		计算机(R):	WIN-NT2QI8KLNCM.test.com
操作代码	爯(O):	信息			
更多信息	킢(I):	事件日志联机	<u>帮助</u>		
			_		

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 Idap

authentication portal Idap-scheme Idap

authorization portal none

accounting portal none

#

Idap scheme Idap

authentication-server Idap

#

Idap server Idap

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

En iNode智能客户端	* - ×
802.1X连接	
用户名 user	
连接	
Portal 连接	~
・我	的场景 》
0	≣ % o

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

常规 详细信息				-		
NAS 第 NAS 第	(口类型: (口:	以 ま 167	大网 785508		^	
RADIUS 客户端	:					
香户)焉. 客户)端	及好名称: IP 地址:	tolly 101	.0.165.11			
身份验证详细信	e :					
连接演	求策略名称:	所有用户使用	Windows B	份验证		
网络策	略名称:	802.1x				
身份验	证提供程序:	Wir	ndows			-
身份验	证服务器:	WIN-RS0C6	TAF7VG			4
身份验	证类型:	MD5-CHAP				14
EAP 类	型:	-				
帐户会	话标识符:	3030303030	030303430313	03332323338323130303030303066333038303030303030393933		
日志记	灵结果:	将证	3帐信息写入本	地日志文件。		
」 日志名称(M):	安全					
来源(S):	Microsoft 1	Windows secur	记录时间(D):	2022/9/1 11:06:05		
事件 ID(E):	6272		任务类别(Y):	网络策略服务器		
级别(L):	信息		关键字(K):	审核成功		
用户(U):	智缺		计算机(R):	WIN-RS0C6TAF7VG		
懂作代码(O):	信息					
	事件日志联	机帮助				

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 portmethod 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-nameformat 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

Н3Сのプロパティ		\times
概要 条件 制約 設定		
このネットワーク ポリシーの制約を構成します。 すべての制約が接続要求に一致しない場合、 制約(S):	ネットワーク アクセスは拒否されます。 指定した方法で認証されたクライアントにのみアクセスを許可します。 EAP の種類は、NPS とクライアントとの間で、表示されている順序でネゴシェートされます。 EAP の種類(T): 止へ移動(U) 下へ移動(U) 遠加(D) 編集(E) 削除(R) セキュリティ レベンルの低い認証正方法: Microsoft 暗号化認証下イジョン 2 (MS-CHAP v2)(V) パスワードの規範が切れた後も、ユーザーにパスワードの変更を許可する(H) Microsoft 暗号化認証[(MS-CHAP)(Y) パスワードの規範が切れた後も、ユーザーにパスワードの変更を許可する(X) □ 暗号化認証[(CHAP)(O) ② 暗号化認証[(CHAP)(O) ② 暗号化認証[(PAP、SPAP)(P) □ 認証方法をネゴシエートせずにクライアントに接続を許可する(L)	
	OK キャンセル 適用(A)

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

常规 详细信息				
NAS 🕸	10类型:	以太网		^
NAS 竣	₩ □:	16785508		
RADIUS 客户端	:			
客户端	友好名称:	tolly		
客户端	IP 地址:	101.0.165.11		
身份验证详细信	息:			
连接请	求策略名称:	所有用户使用 Windows 身份	۵Œ	
网络策	略名称:	802.1x		
身份验	证提供程序:	Windows		-
身份验	证服务 <mark>器</mark> :	WIN-RS0C6TAF7VG		1
身份验	证 类型 :	PAP		1
EAP 类	型:	-		La
帐户会	话标识符:	3030303030303034303130	332323136343730303030303066323038303030303030393933	
日志记	录结 果 :	将记帐信息写入本地]志文件。	
I 日志名称(M):	安全			
来源(S):	Microsoft	Windows secur 记录时间(D): 2	322/9/1 10:44:31	
事件 ID(E):	6272	任务类别(Y):	絡策略服务器	
级别(L):	信息	关键字(K): i	i核成功	
用户(U):	暂缺	计算机(R): \	/IN-RS0C6TAF7VG	
操作代码(O):	信息			
更多信息(I):	事件日志联	机帮助		

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 Om 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 portmethod 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

安全 事	件数: 971				
(練字	日期和时	ia	来源	事件ID	千名类别
↓ 审核…	2022/9/5	5 18:52:57	Micro	6272	网络策略服务器
审核	2022/9/5	5 18:52:57	Micro	4634	主销
审核	2022/9/5	5 18:52:57	Micro	4624	送录
审核	2022/9/5	5 18:52:57	Micro	4648	登录
【审核	2022/9/5	18:52:57	Micro	4776	毛据验证
▲ 审核	2022/9/5	5 18:44:19	Micro	5059	具他系统事件
件 6272,	, Microsof	Et Windows secu	urity auditing.		
常规	送细信自				
网络策	略服务器日	日向某个用户授予	予访问权限。		
用户:					
	安全 ID:	:	WIN-5RKO	EVTVVAD	001094000005
	帐户名和	尔:	001	10940000	15
	帐户域:		WIN-5RKO	EVTVVAD	
	完全限点	韵帐户名称;	WIN-5RKO	EVTVVAD'	.001094000005
客户端	计算机;				
	安全 ID		NULL SID		
	帐户名和	* :	-		
	完全限分	计 计 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1	2		
日主名和	≋(M)·	安全			
本酒(C).		Missesse W	Vindanus and	1330+16	D), 2022/0/5 19-52-5
不成(3); 声(+ 1D		6272	vinuows secur	に次町回	0. EXAMPLE 2
#14 ID	():	0272		1135突别	(1): 网络束暗服务器
级别(L):		1言思		天键子(K	: 审核成切
用户(U)	:	暫缺		计算机(R	WIN-5RKOEVTV

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 username-format without-domain

#