クレデンシャル管理

LAN クレデンシャル管理

デバイス設定の変更中、Cisco Nexusダッシュボード ファブリック コントローラ はユーザーから提供されたデバイスのログイン情報を使用します。ただし、LAN スイッチのログイン情報が指定されていない場合、Nexusダッシュボード ファブリック コントローラ により **[設定（Settings）] > [LAN ログイン情報（LAN Credentials Management）]** ページを開いて LAN ログイン情報を設定するように求められます。

Cisco Nexusダッシュボード ファブリック コントローラ は、次の 2 つのログイン情報のセットを使用して LAN デバイスに接続します。

- **ディスカバリ ログイン情報**：Cisco Nexusダッシュボード ファブリック コントローラ は、デバイスのディスカバリおよび定期的なポーリング中にこれらのログイン情報を使用します。

  NDFC は、SSH および SNMPv3 でディスカバリ クレデンシャルを使用して、スイッチからハードウェアまたはソフトウェアインベントリを検出しました。したがって、これらはディスカバリ クレデンシャルと呼ばれます。スイッチごとに 1 つのインベントリを検出できます。これらは読み取り専用であり、スイッチ上で設定を変更することはできません。

- **構成変更ログイン情報**：ユーザーがデバイス構成を変更する機能を使用しようとすると、Cisco Nexusダッシュボード ファブリック コントローラ はこれらのログイン情報を使用します。

LAN クレデンシャル：LAN クレデンシャルで書き込みオプションを使用して、スイッチの設定を変更できます。1 つのスイッチで、ユーザーごとに 1 つのログイン情報が許可されます。ユーザーロールは、SSH 接続を介してスイッチに設定をプッシュするための書き込みオプションを使用するために NDFC にアクセスする必要があります。

NX-OS スイッチで作成されたユーザーロールの場合、SNMPv3 ユーザーは同じパスワードで作成されます。SSH および SNMPv3 のログイン情報がログイン情報の検出に一致することを確認します。SNMP 認証が失敗した場合、ログイン情報の検出はエラーメッセージの表示を停

止します。SNMP 認証は成功したが SSH 認証が失敗した場合、ログイン情報は続行されますが、スイッチのステータスに SSH エラーの警告が表示されます。

NX-OS スイッチで作成されたユーザーロールが AAA 認証を使用する場合、SNMPv3 ユーザーは作成されません。コントローラは、この AAA 認証を使用して NDFC 内のスイッチを検出またはインポートすることにより、ローカル SNMPv3 ユーザーがスイッチ上に作成されていないことを検出します。したがって、スイッチ上で exec コマンドを実行して、スイッチ上に同じパスワードを持つ SNMPv3 ユーザーを作成します。作成された SNMPv3 ユーザーロールは一時的なものです。ユーザーロールが期限切れになると、NDFC からのスイッチの継続的な検出により、SNMPv3 ユーザーが作成されます。

LAN ログイン情報管理では、構成変更ログイン情報を指定できます。LAN スイッチの設定を変更する前に、スイッチの LAN クレデンシャルを入力する必要があります。ログイン情報を提供しない場合、構成変更アクションは拒否されます。

これらの機能は、LAN ログイン情報機能からデバイス書き込みログイン情報を取得します。

- アップグレード（ISSU）
- メンテナンス モード（GIR）
- パッチ（SMU）
- テンプレートの展開
- POAP-Write erase reload、Rollback
- インターフェイスの作成/削除/設定
- VLAN の作成/削除/設定
- VPC ウィザード

デバイスが最初に検出されたかどうかに関係なく、構成変更のログイン情報を指定する必要があります。これは 1 回限りの操作です。ログイン情報が設定されると、ログイン情報は構成変更操作に使用されます。

Default Credentials

デフォルトのログイン情報は、ユーザーがアクセスできるすべてのデバイスに接続するために使用されます。次の [デバイス（Devices）] で各デバイスのログイン情報を指定することで、デフォルトのログイン情報を上書きできます。

Cisco Nexusダッシュボード ファブリック コントローラ は、まず、デバイスの個々のスイッチ ログイン情報を使用しようとします。[デバイス（Devices）] のログイン情報（ユーザー名/パスワード）列が空の場合、デフォルトのログイン情報が使用されます。

スイッチテーブル

デバイス テーブルには、ユーザーがアクセスできるすべての LAN スイッチがリストされます。デフォルトのログイン情報を上書きするスイッチ ログイン情報を個別に指定できます。ほとんどの場合、デフォルトのログイン情報のみを入力する必要があります。

[Nexusダッシュボードファブリック コントローラデバイスのLANログイン情報（LAN Credentials for the Devices）] テーブルには、次のフィールドがあります。

フィールド	説明
[デバイス名（Device Name）]	スイッチの名前が表示されます。
IP アドレス	スイッチの IP アドレスを指定します。
ログイン情報	デフォルトまたはスイッチ固有のカスタムクレデンシャルを使用するかどうかを指定します。
Username	Nexusダッシュボード ファブリック コントローラ がログインに使用するユーザー名を指定します。
ファブリック	スイッチが属するファブリックを表示します。

次の表では、**[アクション（Actions）]** メニューのドロップダウンリストで、**[LAN クレデンシャル管理（SAN Credentials Management）]**に表示されるアクション項目について説明します。

アクション項目	説明
編集	デバイス名を選択し、**[編集（Edit）]** をクリックして、ユーザー名とパスワードを指定します。ローカルまたはカスタムの特定のログイン情報を編集できます
クリア	デバイス名を選択し、**[クリア（Clear）]**をクリックします。 確認ウィンドウが表示されたら、**[はい（Yes）]**をクリックして、NDFC サーバーからスイッチのログイン情報を消去します。
検証	デバイス名を選択し、**[検証（Validate）]**をクリックします。 操作が成功したか失敗したかを示す確認メッセージが表示されます。

ロボットのログイン情報

デフォルトのログイン情報を指定すると、ロボット機能を有効にできます。これにより、ロボットフラグが有効になります。

ロボットのロールは、DCNMの以前のロールに似ています。ロボットのユーザーロールは、スイッチとデバイスのアカウンティングに役立ちます。一般ユーザーアカウントを使用して、NDFC で行われたすべての変更を追跡できます。NDFC で、アウトオブバンド変更と呼ばれるデバイスの変更に影響を与える、ユーザーロールが変更された場合。これらの変更は、一般ユーザーアカウントによる変更としてデバイスに記録されます。したがって、アウトオブバン

ド変更とデバイスで行われた変更を追跡して区別できます。この一般ユーザーアカウントは、デバイスに記録された変更に対するロボットユーザーロールと呼ばれます。

たとえば、NDFC の network-admin を持つユーザーロールは、スイッチの設定をプッシュするためにLANデバイスのログイン情報を入力するアクセス権を持っています。このユーザーロールは、LAN クレデンシャルの作成中にロボットフラグをチェックできます。

LANクレデンシャルに指定されたユーザー名は、デバイスに記録された変更に表示されます。NDFC の LAN クレデンシャルのユーザー名がコントローラとして変更され、ロボットフラグをチェックすると、デバイスのクレデンシャルがデフォルトからロボットに変更されます。このユーザーロールは、NDFCのスイッチの設定をプッシュします。これらの変更は、ユーザーロールの network-admin によって行われた変更としてファブリック展開の履歴タブに記録されますが、スイッチのアカウントログオンはコントローラとして表示されます。したがって、適切なユーザーロールの詳細が NDFC とデバイスに記録されます。

NDFCでは、ロボットのユーザーロールは、すべてのファブリックとデバイスの管理者ロールと見なされます。デフォルトまたはログイン情報がファブリックに設定されていない場合、ロボットのユーザーロールを使用できます（異なるデバイスに設定されている場合）。書き込みアクセス権を持つ他のユーザーロールがNDFCにログインする場合、ロボットのユーザーロールが設定されているため、このユーザーロールはログイン情報を更新するように求められません。ログイン情報は、個々のスイッチ、ロボット、デフォルトのログイン情報の順に設定されます

LANクレデンシャル管理のホームページでは、顧客のログイン情報が設定されていない限り、デバイス設定を変更する際に、デフォルトのログイン情報またはロボットのログイン情報を選択できます。

ログイン情報を設定するには、次の手順を実行します。

1. 必要な **[デバイス名（Device 名）]** を選択し、**[設定（set）]** をクリックします。

   [ログイン情報の設定（Set Credentials）] ウィンドウが表示されます。

2. 適切な詳細を入力します。**[ロボット（Robot）]** チェックボックスをオンにして、ロボットのログイン情報を設定します。

   適切なロールを選択して、デバイスクレデンシャルを追加せずに設定をデバイスにプッシュできます。

必要な **[デバイス名（Device Name）]** を選択し、**[クリア（Clear）]** をクリックします。確認メッセージが表示されたら、**[はい（Yes）]**をクリックしてデフォルトのデバイスクレデンシャルをクリアします。

翻訳について
このドキュメントは、米国シスコ発行ドキュメントの参考和訳です。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動/変更されている場合がありますことをご了承ください。あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。