CHAPTER 17

デバイスとクレデンシャルの管理

この章では、Cisco NX-OS デバイス、および Cisco Data Center Network Manager for LAN（DCNM-LAN）サーバが各デバイスに対して自己認証するために使用するクレデンシャルの管理方法について説明します。

この章の内容は、次のとおりです。

デバイスとクレデンシャルの概要

ここでは、次の内容について説明します。

デバイス

デバイスとクレデンシャル機能により、デバイスの管理状態を管理できます。管理対象の物理デバイスが仮想デバイス コンテキスト（VDC）をサポートする場合、DCNM-LAN は、各 VDC をデバイスとして表します。複数の VDC を持つ物理デバイス上の単一 VDC の実行コンフィギュレーションおよびステータス情報を取得する必要がある場合は、物理デバイス上のすべての VDC に対してデバイス ディスカバリを実行する代わりに、デバイスとクレデンシャル機能を使用して、変更された VDC を表す単一のデバイスを再検出できます。

クレデンシャル

デバイスとクレデンシャル機能では、管理対象の各デバイスを異なるクレデンシャルで保護する機能をサポートしています。DCNM-LAN では、検出したデバイスごとに一意なクレデンシャルを設定できます。また、デバイスに一意なクレデンシャルを設定しない場合にデフォルトのクレデンシャルを使用することもできます。一部の管理対象デバイスだけが同じクレデンシャルを共有している場合は、一部のデバイスに一意なクレデンシャルを設定し、一部の管理対象デバイスで共有されているクレデンシャルをデフォルトのクレデンシャルとして設定します。

デバイスとクレデンシャル機能は、一意のデバイス クレデンシャル セットを各 DCNM-LAN サーバ ユーザに関連付けます。これにより、管理対象デバイス上のアカウンティング ログに各 DCNM-LAN サーバ ユーザの操作が反映されます。デバイス クレデンシャルが設定されていないユーザとして DCNM-LAN クライアントにログインすると、そのユーザ アカウント用のデバイス クレデンシャルを設定するように DCNM-LAN クライアントから要求されます。

アカウント機能のサポートを重視していない組織でも、DCNM-LAN サーバの各ユーザにはデバイス クレデンシャルを設定する必要があります。その際、各ユーザに指定するクレデンシャルは同じでもかまいません。

デバイスのステータス

デバイスとクレデンシャル機能では、各デバイスのステータスが表示されます。表示されるステータスは次のとおりです。

- Managed（管理対象）：DCNM-LAN はセキュア シェル（SSH）を使用してデバイスに接続して、デバイスの実行コンフィギュレーションを設定し、デバイスからログなどのデータを取得できます。このステータスが表示されるのは、Cisco NX-OS のサポートされているリリースを実行しており、DCNM-LAN によるディスカバリをサポートするように正しく設定されているデバイスだけです。詳細については、「Cisco NX-OS デバイスのディスカバリ準備状態の確認」（P.16-7）を参照してください。
- Unmanaged（管理対象外）：DCNM はデバイスの管理、またはデバイスのステータスの監視を行いません。
- Unreachable（到達不能）：DCNM からデバイス（到達不能になる前に管理対象だったデバイス）に接続できません。このステータスには次の原因が考えられます。
  - ネットワーク障害のため、DCNM-LAN サーバがデバイスにアクセスできない。
  - SSH がデバイス上でディセーブルになっている。
  - デバイス上のすべての端末ラインが使用中である。

VDC のサポート

VDC をサポートするデバイスの場合、DCNM-LAN は、物理デバイス上の各 VDC を個別のデバイスとして扱います。これにより、デバイス上の各 VDC に一意なクレデンシャルを用意できます。また、DCNM-LAN は各 VDC のステータスも個別に追跡します。

デバイスとクレデンシャル機能のライセンス要件

次の表に、この機能のライセンス要件を示します。

製品	ライセンス要件
Cisco DCNM-LAN	デバイスとクレデンシャル機能にライセンスは必要ありません。ライセンス パッケージに含まれていない機能は Cisco DCNM-LAN にバンドルされており、無料で提供されます。Cisco DCNM LAN エンタープライズ ライセンスの取得とインストールの詳細については、『*Cisco DCNM Installation and Licensing Guide, Release 5.x*』を参照してください。

デバイスとクレデンシャル機能を管理するための前提条件

デバイスとクレデンシャル機能でデバイス ディスカバリを実行するには、次の前提条件を満たしている必要があります。

- DCNM-LAN サーバが検出対象のデバイスに接続できること。
- Cisco NX-OS デバイスが、Cisco NX-OS のサポートされているリリースを実行していること。Cisco NX-OS のサポートされているリリースの詳細については、『*Cisco DCNM Release Notes, Release 5.x*』を参照してください。
- Cisco NX-OS デバイスが、デバイス ディスカバリを正常に完了するために必要な最小構成を備えていること。詳細については、「Cisco NX-OS デバイスのディスカバリ準備状態の確認」（P.16-7）を参照してください。

デバイスとクレデンシャル機能の注意事項と制約事項

デバイスとクレデンシャル機能における設定上の注意事項と制約事項は次のとおりです。

- デバイスとクレデンシャル機能を使用したデバイス ディスカバリでは、CDP ベースのネイバー ディスカバリはサポートされていません。CDP ベースのディスカバリを使用する方法については、「デバイス ディスカバリの管理」（P.16-1）を参照してください。
- デフォルトのクレデンシャルやデバイス固有のクレデンシャルを変更する場合は慎重に行ってください。クレデンシャルが間違っていると、DCNM-LAN がデバイスを管理できなくなります。

デバイスとクレデンシャル機能の設定

ここでは、次の内容について説明します。

- 「デバイスの一意なクレデンシャルの消去」（P.17-9）

デバイスの追加

デバイスを追加できます。デバイスを追加した後、デバイスを検出できます。詳細については、「デバイスの検出」（P.17-4）を参照してください。

はじめる前に

デバイスの IPv4 アドレスを確認します。

DCNM-LAN がデフォルトのデバイス クレデンシャルを使用しているデバイスと通信できるかどうか、または DCNM-LAN にデバイスを追加するとき一意なデバイス クレデンシャルを追加する必要があるかどうかを確認します。

手順の詳細

ステップ 1　[Feature Selector] ペインで、[DCNM Server Administration] > [Devices and Credentials] の順に選択します。

[Contents] ペインの [Devices] 領域に検出済みのデバイスが表示されます。

ステップ 2　メニュー バーで、[Actions] > [New Device] の順に選択します。

[Contents] ペインの [Devices] 領域に空白行が表示されます。

ステップ 3　新規デバイスの [IP Address] 列に、DCNM-LAN がそのデバイスに接続するときに使用する必要のある IPv4 アドレスを入力します。

ステップ 4　Enter を押します。

ステップ 5　（任意）一意なデバイス クレデンシャルを追加する必要がある場合は、[User Credentials] 列で、追加したデバイスのエントリをダブルクリックし、下矢印ボタンをクリックして、一意なデバイス クレデンシャルを設定します。

ステップ 6　メニュー バーで、[File] > [Deploy] の順に選択して、変更内容を DCNM-LAN サーバに適用します。

新規デバイスのステータスは「Unmanaged」です。

デバイスの検出

デバイスを検出できます。

管理対象外のデバイスを検出すると、ステータスが「Managed」に変わります。検出中、DCNM-LAN はデバイスの実行コンフィギュレーションを取得します。

デバイスを再検出すると、DCNM-LAN が取得するコンフィギュレーション データで、デバイスの既存のコンフィギュレーション データが置換されます。DCNM-LAN が保持しているデバイスのコンフィギュレーション データが正しくない場合は（たとえば、デバイス管理者がコマンドライン インターフェイスを使用して実行コンフィギュレーションを変更した場合など）、この手順を使用して、DCNM-LAN が保持しているデバイスのコンフィギュレーション データを更新できます。

（注）　デバイスを検出しても、そのデバイスの実行コンフィギュレーションは影響を受けません。

はじめる前に

一意のデバイス クレデンシャルを使用してデバイス エントリを設定していること、または DCNM-LAN がデフォルトのデバイス クレデンシャルを使用してデバイスに接続できることを確認してください。詳細については、「デフォルトのデバイス クレデンシャルの設定」（P.17-6）を参照してください。

手順の詳細

ステップ 1　[Feature Selector] ペインで、[DCNM Server Administration] > [Devices and Credentials] の順に選択します。

[Contents] ペインの [Devices] 領域に検出済みのデバイスが表示されます。

ステップ 2　検出するデバイスをクリックします。

ステップ 3　メニュー バーで、[Actions] > [Discover] の順に選択します。

デバイス ディスカバリが開始されます。デバイスのステータスが「Discovering（検出中）」に変わります。

ステップ 4　ステータスが「Managed」に変わるまで待ちます。

通常は、5 分未満でデバイス ディスカバリが行われます。ステータスが「Managed」に変わったら、DCNM-LAN を使用してデバイスを設定できます。

変更内容を保存する必要はありません。

デバイスの非管理対象化

デバイスのステータスを「Unmanaged」にすることができます。

はじめる前に

ステータスを変更するデバイスを正しく選択していることを確認してください。DCNM-LAN は管理対象外デバイスの実行コンフィギュレーションを制御できません。

手順の詳細

ステップ 1　[Feature Selector] ペインで、[DCNM Server Administration] > [Devices and Credentials] の順に選択します。

[Contents] ペインの [Devices] 領域に検出済みのデバイスが表示されます。

ステップ 2　ステータスを「Unmanaged」に変更するデバイスをクリックします。

ステップ 3　メニュー バーで、[Actions] > [Unmanage] の順に選択します。

少し経つと、デバイスのステータスが「Unmanaged」に変わります。

変更内容を保存する必要はありません。

デバイスの削除

デバイスを削除できます。デバイスを削除すると、そのデバイスに関するすべてのコンフィギュレーション データが DCNM-LAN から削除されます。

DCNM-LAN で管理するつもりのないデバイスは削除することを検討する必要があります。また、VDC をサポートするデバイスのネットワーク管理者がデバイスのコマンドライン インターフェイスを使用して VDC を削除する場合は、その VDC を表しているデバイスを DCNM-LAN から削除する必要があります。

（注）　デバイスを削除しても、そのデバイスの実行コンフィギュレーションは影響を受けません。

はじめる前に

削除対象のデバイスを正しく選択していることを確認します。

手順の詳細

ステップ 1　[Feature Selector] ペインで、[DCNM Server Administration] > [Devices and Credentials] の順に選択します。

[Contents] ペインの [Devices] 領域に検出済みのデバイスが表示されます。

ステップ 2　削除するデバイスをクリックします。

ステップ 3　メニュー バーで、[Actions] > [Delete] の順に選択します。

[Devices] 領域からデバイスが消去されます。

変更内容を保存する必要はありません。

デフォルトのデバイス クレデンシャルの設定

デフォルトのクレデンシャルを設定できます。デフォルトのクレデンシャルは、検出された Cisco NX-OS デバイスに対して接続するとき、DCNM-LAN がデバイスに対して自身を認証するために使用します。DCNM-LAN は、一意なデバイス クレデンシャルが設定されていない検出済みの各デバイスと通信するとき、デフォルトのデバイス クレデンシャルを使用します。

（注）　デバイス クレデンシャルは、DCNM-LAN サーバのユーザごとに一意です。

はじめる前に

デフォルトのデバイス クレデンシャルの内容を確認します。DCNM-LAN がデフォルトのクレデンシャルを使用して通信するすべての Cisco NX-OS デバイスには、DCNM-LAN に設定するデフォルトのクレデンシャルと同じユーザ名とパスワードが設定されたネットワーク管理者アカウントを定義しておく必要があります。

（注）　強力なパスワードを使用することをお勧めします。強力なパスワードの一般的なガイドラインとしては、パスワードの長さを 8 文字以上にすることや、少なくとも 1 つの文字、数字、および記号を使用することなどが挙げられます。たとえば、Re1Ax@h0m3 というパスワードは 10 文字で、1 つの記号と 3 つの数字に加えて大文字と小文字が使用されています。

手順の詳細

ステップ 1　[Feature Selector] ペインで、[DCNM Server Administration] > [Devices and Credentials] の順に選択します。

[Contents] ペイン内の [Devices] 領域の上の [Default Credentials] 領域に、検出済みのデバイスの一覧が表示されます。

ステップ 2　[User Name] フィールドに、デフォルトのクレデンシャルのユーザ名を入力します。有効なユーザ名は 1 ～ 32 文字です。数字、記号、文字（大文字小文字を区別）を使用できます。

（注）　Cisco NX-OS では、最大 28 文字のユーザ名をサポートしています。

ステップ 3　[Password] フィールドの右側にある下矢印ボタンをクリックします。

ステップ 4　[Password] フィールドと [Confirm Password] フィールドに、デフォルトのクレデンシャルのパスワードを入力します。数字、記号、文字（大文字小文字を区別）を使用できます。

（注）　Cisco NX-OS では、最大 64 文字のパスワードをサポートしています。

ステップ 5　[OK] をクリックします。

ステップ 6　メニュー バーで、[File] > [Deploy] の順に選択して、変更内容を DCNM-LAN サーバに適用します。

デフォルトのデバイス クレデンシャルの消去

デフォルトのデバイス クレデンシャルを消去できます。

（注）　デフォルトのデバイス クレデンシャルを消去すると、各管理対象デバイスに一意なクレデンシャルを設定していない限り、DCNM-LAN は検出済みのデバイスに接続できなくなります。

はじめる前に

デフォルトのデバイス クレデンシャルなしで DCNM-LAN を使用する場合は、次の手順を実行する前に、検出済みの各デバイスに一意なデバイス クレデンシャルが設定されていることを確認する必要があります。詳細については、「デバイスの一意なクレデンシャルの設定」（P.17-8）を参照してください。

手順の詳細

ステップ 1　[Feature Selector] ペインで、[DCNM Server Administration] > [Devices and Credentials] の順に選択します。

[Contents] ペイン内の [Devices] 領域の上の [Default Credentials] 領域に、検出済みのデバイスの一覧が表示されます。

ステップ 2　[Default Credentials] 領域で、[Clear] をクリックします。

[User Name] フィールドと [Password] フィールドが消去されます。

ステップ 3　メニュー バーで、[File] > [Deploy] の順に選択して、変更内容を DCNM-LAN サーバに適用します。

デバイスの一意なクレデンシャルの設定

検出済みのデバイスに一意なクレデンシャルを設定できます。検出済みのデバイスに一意なクレデンシャルが存在する場合、DCNM-LAN は、デフォルトのデバイス クレデンシャルではなく一意なクレデンシャルを使用してそのデバイスに接続します。

（注）　デバイス クレデンシャルは、DCNM-LAN サーバのユーザごとに一意です。

はじめる前に

検出済みのデバイスに設定されているネットワーク管理者用ユーザ アカウントのユーザ名とパスワードを確認します。

（注）　強力なパスワードを使用することをお勧めします。強力なパスワードの一般的なガイドラインとしては、パスワードの長さを 8 文字以上にすることや、少なくとも 1 つの文字、数字、および記号を使用することなどが挙げられます。たとえば、Re1Ax@h0m3 というパスワードは 10 文字で、1 つの記号と 3 つの数字に加えて大文字と小文字が使用されています。

手順の詳細

ステップ 1　[Feature Selector] ペインで、[DCNM Server Administration] > [Devices and Credentials] の順に選択します。

[Contents] ペインの [Devices] 領域に検出済みのデバイスが表示されます。

ステップ 2　デバイスの [User Credentials] 列で、入力値をダブルクリックして、下矢印ボタンをクリックします。

ステップ 3　[User Name] フィールドに、ユーザ名を入力します。有効なユーザ名は 1 ～ 32 文字です。数字、記号、文字（大文字小文字を区別）を使用できます。

（注）　Cisco NX-OS では、最大 28 文字のユーザ名をサポートしています。

ステップ 4　[Password] フィールドと [Confirm Password] フィールドに、パスワードを入力します。数字、記号、文字（大文字小文字を区別）を使用できます。

（注）　Cisco NX-OS では、最大 64 文字のパスワードをサポートしています。

ステップ 5　[OK] をクリックします。

ステップ 6　メニュー バーで、[File] > [Deploy] の順に選択して、変更内容を DCNM-LAN サーバに適用します。

デバイスの一意なクレデンシャルの消去

検出済みデバイスの一意なクレデンシャルを消去できます。

（注）　検出済みデバイスの一意なクレデンシャルを消去すると、DCNM-LAN はデフォルトのクレデンシャルを使用してデバイスに接続するようになります。

はじめる前に

一意なデバイス クレデンシャルなしで DCNM-LAN を運用する場合は、次の手順を実行する前に、DCNM-LAN にデフォルトのデバイス クレデンシャルが設定されていることを確認する必要があります。詳細については、「デフォルトのデバイス クレデンシャルの設定」（P.17-6）を参照してください。

手順の詳細

ステップ 1　[Feature Selector] ペインで、[DCNM Server Administration] > [Devices and Credentials] の順に選択します。

[Contents] ペインの [Devices] 領域に検出済みのデバイスが表示されます。

ステップ 2　デバイスの [User Credentials] 列で、入力値をダブルクリックして、下矢印ボタンをクリックします。

ステップ 3　[User Name] フィールドのテキストをすべて削除します。

ステップ 4　[Password] フィールドのテキストをすべて削除します。

ステップ 5　[Confirm Password] フィールドのテキストをすべて削除します。

ステップ 6　[OK] をクリックします。

ステップ 7　メニュー バーで、[File] > [Deploy] の順に選択して、変更内容を DCNM-LAN サーバに適用します。

デバイス クレデンシャルとステータスの表示

デバイスのステータス、およびデバイスにクレデンシャルが設定されているかどうかを表示するには、[Feature Selector] ペインで、[DCNM Server Administration] > [Devices and Credentials] の順に選択します。

[Contents] ペインの [Default Credentials] 領域に、デフォルトのクレデンシャルが表示されます。クレデンシャルとステータスなど、デバイスに関する情報は、[Contents] ペインの [Devices] 領域に表示されます。

[Reason] フィールドに、デバイスのステータスを解説する簡単なメッセージが表示されます。次の表に、メッセージによって示される問題の解決方法に関する情報を示します。

理由	解決方法
Success	該当なし。DCNM-LAN がデバイスを管理しています。
Authentication failure（認証失敗）	デバイスのクレデンシャルが正しいことを確認します。DCNM-LAN がデバイスに到達可能であることを確認します。
Unsupported platform（サポート対象外のプラットフォーム）	デバイスがサポートされているプラットフォームであること、そのプラットフォームでサポートされているリリースの Cisco NX-OS を実行していることを確認します。サポートされているプラットフォームおよび Cisco NX-OS リリースの詳細については、『*Cisco DCNM Release Notes, Release 5.x*』を参照してください。
Device sync up failure（デバイスの同期化失敗）	Cisco Nexus 7000 シリーズ デバイス用。アカウント機能およびシステム メッセージのログ メッセージの連番の形式が適切ではありません。デバイス上のログ ファイルを消去し、デバイスを再検出します。
Unmanaged manually（手動による非管理対象化）	DCNM-LAN ユーザがデバイスのステータスを「Unmanaged」に変更しました。デバイスを再検出します。
Error when executing database query（データベース クエリー実行時のエラー）	デバイスを再検出します。エラーが再度発生する場合は、DCNM-LAN データベースをクリーンアップします。データベースのクリーンアップの詳細については、第 29 章「Cisco DCNM-LAN データベースのメンテナンス」を参照してください。
Auto synchronization for device is disabled by user（ユーザによるデバイスの自動同期化のディセーブル化）	デバイスを再検出します。
Logging levels required by DCNM-LAN are not configured on the device（DCNM-LAN に必要なログ レベルがデバイスに設定されていない）	デバイスを再検出します。詳細については、「ログ レベル自動設定のサポート」（P.16-4）を参照してください。
Error in SSH connection（SSH 接続のエラー）	デバイスで SSH がイネーブルになっていること、SSH が適切に機能していることを確認します。デバイスを再検出します。
Unreachable（到達不能）	デバイスの正しい IP アドレスを指定していることを確認します。DCNM-LAN がデバイスにアクセスできることを確認します。デバイスを再検出します。
Discovery failed because server node stopped/crashed（サーバ ノードの停止またはクラッシュによるディスカバリの失敗）	デバイスを再検出します。
Syslog messages logging disabled on device（デバイスでの Syslog メッセージ ロギングのディセーブル化）	デバイスを再検出します。

表示される各フィールドの詳細については、「デバイスとクレデンシャル機能の各フィールドの説明」（P.17-11）を参照してください。

デバイスとクレデンシャル機能の各フィールドの説明

ここでは、デバイスとクレデンシャルの次の各フィールドについて説明します。

- 「デバイスとクレデンシャルの [Contents] ペイン」（P.17-11）

デバイスとクレデンシャルの [Contents] ペイン

表 17-1　デバイスとクレデンシャルの [Contents] ペイン

フィールド	説明
Default Credentials	
User Name	DCNM-LAN サーバが検出または管理しているデバイスへのアクセスに使用する Cisco NX-OS デバイス ユーザ アカウントの名前。デバイス上でこのユーザ アカウントに、network-admin ロールまたは vdc-admin ロールが割り当てられている必要があります。デフォルトでは、このフィールドは空白です。 **（注）** [Default Credentials] セクションの情報は、[Devices] 領域の [User Credentials] フィールド内の情報によって上書きされます。
Password	[User Name] フィールドに、指定した Cisco NX-OS デバイス ユーザ アカウントのパスワード。デフォルトでは、このフィールドは空白です。
Devices	
IP Address	*表示のみ*。Cisco NX-OS デバイスの IPv4 アドレス。
Name	*表示のみ*。Cisco NX-OS デバイスの名前。
User Credentials	DCNM-LAN が Cisco NX-OS デバイスに接続するときに使用する Cisco NX-OS ユーザ アカウント。 **（注）** このフィールドを設定すると、DCNM-LAN は、デバイスに接続するとき、指定したユーザ アカウントを使用します。このフィールドが空白の場合、DCNM-LAN は、[Default Credentials] 領域に指定されたユーザ アカウントを使用します。デフォルトでは、このフィールドは空白です。
Status	*表示のみ*。DCNM-LAN サーバがデバイスに対して接続および設定できるかどうかを示します。有効な値は、次のとおりです。 • [Managed]：DCNM-LAN サーバはデバイスを設定できます。 • [Unmanaged]：DCNM-LAN サーバはデバイスを設定できません。 • [Unreachable]：DCNM-LAN サーバはデバイスに到達できません。
Reason	*表示のみ*。デバイスのステータスに関する簡単な説明が表示されます。詳細については、「デバイス クレデンシャルとステータスの表示」（P.17-9）を参照してください。

デバイスとクレデンシャル機能のその他の関連資料

デバイスとクレデンシャル機能に関する追加情報については、次のセクションを参照してください。

- 「関連資料」（P.17-12）

- 「標準」（P.17-12）

関連資料

関連項目	参照先
Cisco NX-OS XML 管理インターフェイス	『*Cisco NX-OS XML Interface User Guide*』

標準

標準	タイトル
Secure Shell（SSH; セキュア シェル）上の NETCONF プロトコル	RFC 4742

デバイスとクレデンシャル機能の履歴

表 17-2 は、この機能のリリースの履歴です。

表 17-2　デバイスとクレデンシャル機能の履歴

機能名	リリース	機能情報
[Reason] フィールド	5.0(2)	デバイスとクレデンシャル機能に [Reason] フィールドが追加されました。