NTP の設定

この章では、Cisco NX-OS デバイスでネットワーク タイム プロトコル（NTP）を設定する方法について説明します。

この章は、次の項で構成されています。

NTP の詳細

ネットワーク タイム プロトコル（NTP）は、分散している一連のタイム サーバとクライアント間で 1 日の時間を同期させ、複数のネットワーク デバイスから受信するシステム ログや時間関連のイベントを相互に関連付けられるようにします。NTP ではトランスポート プロトコルとして、ユーザ データグラム プロトコル（UDP）を使用します。すべての NTP 通信は UTC を使用します。

NTP サーバは通常、タイム サーバに接続されたラジオ クロックやアトミック クロックなどの正規の時刻源から時刻を受信し、ネットワークを介してこの時刻を配信します。NTP はきわめて効率的で、毎分 1 パケット以下で 2 台のマシンを相互に 1 ミリ秒以内に同期します。

NTP ではストラタム（stratum）を使用して、ネットワーク デバイスと正規の時刻源の距離を表します。

- ストラタム 1 のタイム サーバは、信頼できる時刻源に直接接続されます（無線時計や原子時計または GPS 時刻源など）。
- ストラタム 2 の NTP サーバは、ストラタム 1 のタイム サーバから NTP を使用して時刻を受信します。

同期の前に、NTP は複数のネットワーク サービスが報告した時刻を比較し、1 つの時刻が著しく異なる場合は、それが Stratum 1 であっても、同期しません。Cisco NX-OS は、無線時計や原子時計に接続できず、ストラタム 1 サーバとして動作することはできないため、インターネット上で利用できるパブリック NTP サーバを使用することを推奨します。ネットワークがインターネットから切り離されている場合、Cisco NX-OS では、NTP によって時刻が同期されていなくても、NTP で同期されているものとして時刻を設定できます。

（注） NTP ピア関係を作成して、サーバで障害が発生した場合に、ネットワーク デバイスを同期させて、正確な時刻を維持するための時刻提供ホストを指定できます。

デバイス上の時刻は重要な情報であるため、NTP のセキュリティ機能を使用して、不正な時刻を誤って（または悪意を持って）設定できないように保護することを強く推奨します。その方法として、アクセス リストベースの制約方式と暗号化認証方式があります。

NTP アソシエーション

N TP アソシエーションは、次のいずれかになります。

- ピア アソシエーション：デバイスが別のデバイスに同期するか、別のデバイスをそのデバイスに同期させることができます。
- サーバ アソシエーション：デバイスは、サーバに同期します。

設定する必要があるのはアソシエーションの片側だけです。他方のデバイスは自動的にアソシエーションを確立できます。

時間サーバとしての NTP

Cisco NX-OS デバイスでは、時刻を配信するために NTP を使用できます。他のデバイスからタイム サーバとして設定できます。デバイスを正規の NTP サーバとして動作するよう設定し、外部の時刻源と同期していないときでも時刻を配信させることもできます。

クロック マネージャ

クロックはさまざまなプロセス間で共有する必要のあるリソースです。NTP などの複数の時刻同期プロトコルが、システムで稼働している可能性があります。

クロック マネージャを使用して、システム内のさまざまなクロックを制御するプロトコルを指定できます。プロトコルを指定すると、システム クロック更新が開始します。クロック マネージャの設定の詳細については『Cisco Nexus 9000 シリーズ NX-OS 基本設定ガイド』を参照してください。

高可用性

NTP はステートレス リスタートをサポートします。リブート後またはスーパーバイザ スイッチオーバー後に、実行コンフィギュレーションが適用されます。ハイアベイラビリティの詳細については、『Cisco Nexus 9000 シリーズ NX-OS ハイ アベイラビリティおよび冗長性ガイド』を参照してください。

NTP ピアを設定すると、NTP サーバ障害の発生時に冗長性が得られます。

仮想化のサポート

NTP は Virtual Routing and Forwarding（VRF）インスタンスを認識します。NTP サーバおよび NTP ピアに対して特定の VRF を設定していない場合、NTP はデフォルトの VRF を使用します。VRF の詳細については、『Cisco Nexus 9000 シリーズ NX-OS ユニキャスト ルーティング設定ガイド』を参照してください

NTP の前提条件

NTP の前提条件は、次のとおりです。

- NTP を設定するには、NTP が動作している 1 つ以上のサーバに接続できなければなりません。

NTP の注意事項と制約事項

NTP に関する設定時の注意事項および制約事項は、次のとおりです。

- NTP サーバ機能はサポートされます。
- デフォルト以外の VRF で名前ベースの NTP サーバ（FQDN）を設定する前に、その特定の VRF で DNS サーバを設定する必要があります。オプションを使用してグローバルコンフィギュレーションモードからDNSサーバを設定する場合、その名前ベースのNTPサーバ設定は実行コンフィギュレーションに追加されません。**use-vrf** この方法を使用して NTP サーバを設定しようとした場合は、コマンドの **no** バージョンを使用して NTP 設定を削除し、その VRF の下に DNS サーバを追加してから、VRF に名前ベースの NTP サーバを追加する必要があります。構成された DNS サーバーは到達可能であり、照会されたときに NTP サーバーの FQDN の正しい IP を返す必要があります。
- 使用するクロックの信頼性が確実な場合（つまり、信頼できる NTP サーバのクライアントである場合）に限り、別のデバイスとの間にピア アソシエーションを設定することを推奨します。
- 単独で設定したピアは、サーバの役割を担いますが、バックアップとして使用する必要があります。サーバが 2 台ある場合、いくつかのデバイスが一方のサーバに接続し、残りの

デバイスが他方のサーバに接続するように設定できます。その後、2 台のサーバ間にピアアソシエーションを設定すると、信頼性の高い NTP 構成になります。

- サーバが 1 台だけの場合は、すべてのデバイスをそのサーバのクライアントとして設定することを推奨します。
- 設定できる NTP エンティティ（サーバおよびピア）は、最大 64 です。
- VRF で NTP を設定する場合は、NTP サーバおよびピアが、設定された VRF を介して相互にアクセスできることを確認します。
- ネットワーク全体の NTP サーバおよび Cisco NX-OS デバイスに、NTP 認証キーを手動で配信します。
- スイッチをエッジ デバイスとして使用して NTP を利用したい場合は、**ntp access-group** コマンドを使用して必要なエッジ デバイスにのみ NTP をフィルタリングすることを推奨します。
- システムに **ntp passive**、**ntp broadcast client**、または **ntp multicast client** コマンドが設定されている場合、対称アクティブの着信パケット、ブロードキャスト パケット、マルチキャスト パケットを NTP が受信する際に、送信者と同期させるための一時的なピア アソシエーションを設定できます。

（注） 上記コマンドのいずれかを有効にする前に必ず **ntp authenticate** bを指定してください。そうしないと、上記のパケット タイプのいずれかを送信する任意のデバイス（悪意のある攻撃者に制御されたデバイスを含む）とデバイスが同期される可能性があります。

- **ntp authenticate** コマンドが指定されている場合、対称アクティブ パケット、ブロードキャスト パケット、マルチキャスト パケットが受信されても、**ntp trusted-key** グローバル コンフィギュレーション コマンドで指定された認証キーの 1 つがパケットで運ばれていない限り、システムとピアの同期は行われません。
- **ntp access-group** コマンドなど他の方法で、デバイスの NTP サービスと非承認ホストとの通信防止の措置が取られている場合を除き、非承認のネットワーク ホストとの同期を避けるには、**ntp passive**、**ntp broadcast client**、**ntp multicast client** コマンドを指定した段階で随時 **ntp authenticate** コマンドを指定する必要があります。
- The **ntp authenticate** コマンドは、**ntp server** および **ntp peer** コンフィギュレーション コマンドで設定されたピア アソシエーションを認証しません。**ntp server** および **ntp peer** アソシエーションを認証するには、**key** キーワードを指定します。
- 1 つの NTP アクセス グループに最大 4 つの IP ACL を設定できます。IPv4 および IPv6 ACL がサポートされています。
- インバンド ポートでパケット フラッディングが発生すると、NTPD による CPU 使用率が 90% を超える可能性があります。NTPD によるこの高い CPU 使用率を克服するには、カ

スタム CoPP ポリシーを使用して、NTP への着信トラフィックをレート制限します。コントロール プレーン ポリシングの詳細については、cisco.com の『Cisco Nexus 9000 Series NX-OS Security Configuration Guide』の関連バージョンの「Configuring Control Plane Policing」の章を参照してください。

（注） 推奨されるレート制限は、ポリシー **CIR** フィールドの場合は 1000 kbps、**BC** フィールドの場合は 64,000 バイトです。

- Cisco NX-OS リリース 10.1(1) 以降、Cisco Nexus 9000 スイッチはストラタム 14 および 15 と同期しません。
- Cisco NX-OS リリース 10.3(3)F 以降、RFC 8573 標準に沿って、NTP セキュリティは、認証キーのタイプ 6 暗号化サポートとともに AES128CMAC 認証メカニズムによって強化されています。次の注意事項と制限事項が適用されます。
  - この機能には、パスワードをタイプ 0、タイプ 7、またはタイプ 6 として設定するオプションがあります。
  - 構成できる一意のキーの最大数は 1024 で、範囲は 1 ～ 65535 です。
  - タイプ 6 認証を機能させるには、**feature password encryption aes** とともに、構成する新しいタイプ 6 キーを生成するために使用したものと同じプライマリ（マスター）キーをデバイスに構成します。
  - **encryption re-encrypt obfuscated** コマンドを使用して再暗号化を適用すると、タイプ 6 以外のすべての NTP パスワードがタイプ 6 に再暗号化されます。
  - コマンドは、NTP に設定されているすべてのタイプ 6 パスワードを削除します。**encryption delete type6**
  - **encryption decrypt type6** コマンドは、既存の構成済みのタイプ 6 パスワードを復号化します。
  - AES128CMAC/タイプ 6 でサポートされるバージョンから非 AES128CMAC/タイプ 6 でサポートされるバージョンに ISSD を実行するには、タイプ 6 キーの設定を解除してから ISSD を実行します。
  - プログラム（restconf/Netconf など）でキーチェーンを構成する場合は、encryptType と keyString を指定することをお勧めします。指定しない場合、キー チェーン インフラは、欠落しているプロパティのすでに使用可能な（またはデフォルトの）値を使用して keyString を構成します。
  - 欠落しているプロパティを構成する必要がある場合は、両方のピア ルータで同じ手順を実行する必要があります。

NTP のデフォルト設定

次の表に、NTP パラメータのデフォルト設定を示します。

パラメータ	デフォルト
NTP	イネーブル
NTP 認証	ディセーブル
NTP アクセス	イネーブル
NTP ロギング	無効化

NTP の設定

（注） この機能の Cisco NX-OS コマンドは、Cisco IOS のコマンドとは異なる場合があるので注意してください。

NTP の有効化または無効化

NTP をイネーブルまたはディセーブルにできます。NTP はデフォルトでイネーブルです。

手順の概要

1. **configure terminal**
2. [**no**] **feature ntp**
3. （任意） **copy running-config startup-config**

手順の詳細

手順

	コマンドまたはアクション	目的

ステップ 1	**configure terminal**
	例：
	`switch# configure terminal`
	`switch(config)#`
		グローバル構成モードを開始します。

ステップ 2	[**no**] **feature ntp** 例：	NTP を有効または無効にします。

	コマンドまたはアクション	目的
	`switch(config)# feature ntp`	
ステップ 3	（任意） **copy running-config startup-config** 例： `switch(config)# copy running-config startup-config`	実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

正規の NTP サーバとしてのデバイスの設定

デバイスを正規の NTP サーバとして動作するよう設定し、既存のタイム サーバと同期していないときでも時刻を配信させることができます。

手順の概要

1. **configure terminal**
2. [**no**] **ntp master** [*stratum*]
3. （任意） **show running-config ntp**
4. （任意） **copy running-config startup-config**

手順の詳細

手順

	コマンドまたはアクション	目的

ステップ 1	**configure terminal**
	例：
	`switch# configure terminal`
	`switch(config)#`
		グローバル コンフィギュレーション モードを開始します

ステップ 2	[**no**] **ntp master** [*stratum*] 例： `switch(config)# ntp master`	正規の NTP サーバとしてデバイスを設定します。 NTP クライアントがこれらの時間を同期するのと別の階層レベルを指定できます。指定できる範囲は 1 ～ 15 です。
ステップ 3	（任意） **show running-config ntp** 例： `switch(config)# show running-config ntp`	NTP コンフィギュレーションを表示します。
ステップ 4	（任意） **copy running-config startup-config** 例： `switch(config)# copy running-config startup-config`	実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

NTP サーバおよびピアの設定

NTP サーバおよびピアを設定できます。

始める前に

使用している NTP サーバと、そのピアの IP アドレスまたはドメイン ネーム システム（DNS）名がわかっていることを確認します。

手順の概要

1. **configure terminal**
2. [**no**] **ntp server** {*ip-address* | *ipv6-address* | *dns-name*} [**key** *key-id*] [**maxpoll** *max-poll*] [**minpoll** *min-poll*] [**prefer**] [**use-vrf** *vrf-name*]
3. [**no**] **ntp peer** {*ip-address* | *ipv6-address* | *dns-name*} [**key** *key-id*] [**maxpoll** *max-poll*] [**minpoll** *min-poll*] [**prefer**] [**use-vrf** *vrf-name*]
4. （任意） **show ntp peers**
5. （任意） **copy running-config startup-config**

手順の詳細

手順

	コマンドまたはアクション	目的

ステップ 1	**configure terminal**
	例：
	`switch# configure terminal`
	`switch(config)#`
		グローバル コンフィギュレーション モードを開始します

ステップ 2	[**no**] **ntp server** {*ip-address* | *ipv6-address* | *dns-name*} [**key** *key-id*] [**maxpoll** *max-poll*] [**minpoll** *min-poll*] [**prefer**] [**use-vrf** *vrf-name*] 例： `switch(config)# ntp server 192.0.2.10`	1 つのサーバと 1 つのサーバ アソシエーションを形成します。 NTP サーバとの通信で使用するキーを設定するには、**key** キーワードを使用します。*key-id* 引数の範囲は 1 ～ 65535 です。 サーバをポーリングする最大および最小の間隔を設定するには、 **maxpoll** および **minpoll** キーワードを使用します。 *max-poll* および *min-poll* 引数の範囲は4ー16（2の累乗として設定されます。つまり、実質的に16ー65536秒）で、デフォルト値はそれぞれ 6 と 4 です（*maxpoll* デフォルト = 64秒、*minpoll* デフォルト= 16秒）。 このサーバをデバイスの優先 NTP サーバにするには、 **prefer** キーワードを使用します。

	コマンドまたはアクション	目的
		指定された VRF を介して通信するように NTP サーバを設定するには、**use-vrf** キーワードを使用します。*vrf-name* 引数には、**default**、**management**、または大文字と小文字が区別される最大 32 文字の任意の英数字文字列を指定できます。 （注） NTP サーバとの通信で使用するキーを設定する場合は、そのキーが、デバイス上の信頼できるキーとして存在していることを確認してください。
ステップ 3	[**no**] **ntp peer** {*ip-address* | *ipv6-address* | *dns-name*} [**key** *key-id*] [**maxpoll** *max-poll*] [**minpoll** *min-poll*] [**prefer**] [**use-vrf** *vrf-name*] 例： `switch(config)# ntp peer 2001:0db8::4101`	1 つのピアと 1 つのピア アソシエーションを形成します。複数のピア アソシエーションを指定できます。 NTP ピアとの通信で使用するキーを設定するには、**key** キーワードを使用します。*key-id* 引数の範囲は 1 ～ 65535 です。 サーバをポーリングする最大および最小の間隔を設定するには、**maxpoll** および **minpoll** キーワードを使用します。*max-poll* および *min-poll* 引数の範囲は4ー16（2の累乗として設定されます。つまり、実質的に 16ー131072 秒）で、デフォルト値はそれぞれ 6 と 4 です（*maxpoll* デフォルト＝64秒、*minpoll* デフォルト= 16秒）。 デバイスに対して対象の NTP ピアを優先にするには、**prefer** キーワードを使用します。 指定された VRF を介して通信するように NTP ピアを設定するには、**use-vrf** キーワードを使用します。*vrf-name* 引数には、**default**、**management**、または大文字と小文字が区別される最大 32 文字の任意の英数字文字列を指定できます。
ステップ 4	（任意） **show ntp peers** 例： `switch(config)# show ntp peers`	設定されたサーバおよびピアを表示します。 （注） ドメイン名が解決されるのは、DNS サーバが設定されている場合だけです。 DNS/ネームサーバが IPv4 と IPv6 の両方を解決する場合、NX-OS では IPv6 アドレスが優先されます。
ステップ 5	（任意） **copy running-config startup-config** 例：	実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

	コマンドまたはアクション	目的
	`switch(config)# copy running-config startup-config`	

NTP 認証の設定

ローカル ロックを同期させる時刻源を認証するようデバイスを設定できます。NTP 認証をイネーブルにすると、**ntp trusted-key** コマンドによって指定されたいずれかの認証キーを時刻源が保持している場合のみ、デバイスはその時刻源と同期します。デバイスは、認証チェックに失敗したすべてのパケットをドロップし、それらのパケットでローカルクロックがアップデートされないようにします。NTP 認証はデフォルトでディセーブルになっています。

始める前に

この手順で指定する予定の認証キーによって、NTP サーバが設定されていることを確認します。

手順の概要

1. **configure terminal**
2. [**no**] **ntp authentication-key** *number* {**md5** | **aes128cmac**} *password string encryption-type*
3. **ntp server** *ip-address* **key** *key-id*
4. （任意） **show ntp authentication-keys**
5. [**no**] **ntp trusted-key** *number*
6. （任意） **show ntp trusted-keys**
7. [**no**] **ntp authenticate**
8. （任意） **show ntp authentication-status**
9. （任意） **copy running-config startup-config**

手順の詳細

手順

	コマンドまたはアクション	目的

ステップ 1	**configure terminal**
	例：
	`switch# configure terminal`
	`switch(config)#`
		グローバル コンフィギュレーション モードを開始します。

ステップ 2	[**no**] **ntp authentication-key** *number* {**md5** | **aes128cmac**} *password string encryption-type* 例：	認証キーを定義します。認証キーの範囲は1～65535です。 デバイスが時刻源と同期するのは、時刻源がこれらの認証キーのいずれかを持ち、**ntp trusted-key** *number*

	コマンドまたはアクション	目的

	`switch(config)# ntp authentication-key 42 md5 aNiceKey`
	`switch(config)# ntp authentication-key 21 md5 JDYk3pp/Fuv0zWyVSRhS6EDERSSsp1uA7s57dvdsx g74ndf02lEI9dF6WX6Z78/5R8qPmSRRrDUDtCcUlZ XDUrf0ErodS3ikPQA= 6`
	`switch(config)# ntp authentication-key 12 aes128cmac JDYkzj4NojJdSkQPvBhFvAO9xCSVwj2iRGvShNSg ER4JwMBMtUEibfqkscgZ4+/iTdDmeCRW9SGWLxKb 3Xk5g8pz4bR7Iu1a7QA= 6`
		コマンドによってキー番号が指定されている場合だけです。
		md5 または aes128cmac 認証方式を選択できます。
		ユーザーが同じプライマリ（**マスター**）キーから生成されたタイプ 6 キーを使用している場合、ユーザーが**機能パスワード暗号化 aes** を有効にするまで、デバイスは時刻源に同期しません。
		タイプ 0 およびタイプ 7 の暗号化タイプの場合、最大長は 32 文字です。リリース 10.3(3)F までは、15 文字（英数字）でした。タイプ 6 暗号化タイプの場合、最大文字数は 128 文字です。

ステップ 3	**ntp server** *ip-address* **key** *key-id* **例**： `switch(config)# ntp server 192.0.2.1 key 1001`	1 つのサーバと 1 つのサーバ アソシエーションを形成します。 NTP サーバとの通信で使用するキーを設定するには、**key** キーワードを使用します。*key-id* 引数の範囲は 1 ～ 65535 です。 認証を必須とする場合は、**key** キーワードを使用する必要があります。**ntp server** または **ntp peer** コマンドで **key** キーワードを指定しない場合、認証なしでの動作が続けられます。
ステップ 4	（任意） **show ntp authentication-keys** **例**： `switch(config)# show ntp authentication-keys`	設定済みの NTP 認証キーを表示します。
ステップ 5	[**no**] **ntp trusted-key** *number* **例**： `switch(config)# ntp trusted-key 42`	1 つ以上のキー（ステップ 2 で定義されているもの）を指定します。デバイスを時刻源と同期させるには、未設定のリモート シンメトリック、ブロードキャスト、およびマルチキャストの時刻源を NTP パケット内に入力する必要があります。trusted key の範囲は 1 ～ 65535 です。 このコマンドにより、デバイスが、信頼されていない時刻源と誤って同期する、ということが防止されます。
ステップ 6	（任意） **show ntp trusted-keys** **例**： `switch(config)# show ntp trusted-keys`	設定済みの NTP の信頼されているキーを表示します。

	コマンドまたはアクション	目的
ステップ 7	[**no**] **ntp authenticate** 例： `switch(config)# ntp authenticate`	ntp passive、ntp broadcast client、および ntp multicast で認証を有効または無効にします。NTP 認証はデフォルトでディセーブルになっています。
ステップ 8	（任意） **show ntp authentication-status** 例： `switch(config)# show ntp authentication-status`	NTP 認証の状況を表示します。
ステップ 9	（任意） **copy running-config startup-config** 例： `switch(config)# copy running-config startup-config`	実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

NTP アクセス制限の設定

アクセス グループを使用して、NTP サービスへのアクセスを制御できます。具体的には、デバイスで許可する要求のタイプ、およびデバイスが応答を受け取るサーバを指定できます。

アクセス グループを設定しない場合は、すべてのデバイスに NTP アクセス権が付与されます。何らかのアクセス グループを設定した場合は、ソース IP アドレスがアクセス リストの基準をパスしたリモート デバイスに対してだけ、NTP アクセス権が付与されます。

- **match-all** キーワードがない場合、パケットは permit が見つかるまでアクセス グループに対して（以下に示す順で）評価されます。permit が検出されない場合、パケットはドロップされます。
- **match-all** キーワードがある場合、パケットはすべてのアクセス グループに対して（以下に示す順で）評価され、最後に成功した評価（ACL が設定されている最後のアクセス グループ）に基づいてアクションが実行されます。
- peer：クライアント、対称アクティブ、対称パッシブ、サービス、コントロール、およびプライベート パケット（すべてのタイプ）を処理
- serve：クライアント、コントロール、およびプライベート パケットを処理
- serve-only：クライアント パケットだけを処理
- query-only：コントロールおよびプライベート パケットだけを処理

アクセス グループは次の順で評価されます：

1. peer（すべてのパケット タイプ）
2. serve（クライアント、コントロール、およびプライベート パケット）
3. serve-only（クライアント パケット）または query-only（コントロールおよびプライベート パケット）

serve-only または query-only の ACL 処理は、NTP パケット タイプによって異なります。

手順の概要

1. **configure terminal**
2. [**no**] **ntp access-group match-all** | {{**peer** | **serve** | **serve-only** | **query-only** }*access-list-name*}
3. （任意） **show ntp access-groups**
4. （任意） **copy running-config startup-config**

手順の詳細

手順

	コマンドまたはアクション	目的

ステップ 1	**configure terminal**
	例：
	`switch# configure terminal`
	`switch(config)#`
		グローバル コンフィギュレーション モードを開始します

ステップ 2	[**no**] **ntp access-group match-all** | {{**peer** | **serve** | **serve-only** | **query-only** }*access-list-name*}
	例：
	`switch(config)# ntp access-group match-all`
	`switch(config)# ntp access-group peer peer-acl`
	`switch(config)# ntp access-group serve serve-acl`
		NTP のアクセスを制御し、基本の IP アクセス リストを適用するためのアクセス グループを作成または削除します。
		設定ピアの遅延 ACL 1ルールに NTP が一致する場合、ACL 処理は停止し、次のアクセス グループ オプションへと継続しません。
		• **peer** キーワードは、デバイスが時刻要求と NTP 制御クエリーを受信し、アクセス リストで指定されているサーバと同期するようにします。
		• **serve** キーワードは、アクセス リストに指定されているサーバからの時刻要求と NTP 制御クエリーをデバイスが受信できるようにしますが、指定されたサーバとは同期しないようにします。
		• **serve-only** キーワードは、デバイスがアクセス リストで指定されたサーバからの時刻要求だけを受信するようにします。
		• **query-only** キーワードは、デバイスがアクセス リストで指定されたサーバからの NTP 制御クエリーのみを受信するようにします。
		• **match-all** キーワードを使用すると、アクセス グループ オプションが、制限の最も緩いものから最も厳しいもの、peer、serve、serve-only、

	コマンドまたはアクション	目的
		query-only の順序でスキャンされるようにできます。着信パケットが peer アクセス グループの ACL に一致しない場合、パケットは serve アクセス グループに送信され、処理されます。パケットが serve アクセス グループの ACL に一致しない場合、serve-only アクセス グループに送られ、これが継続されます。 （注） **match-all** キーワードは、Cisco NX-OS リリース 7.0(3)I6(1) 以降で利用可能なもので、Cisco Nexus 9000 シリーズ スイッチと、Cisco Nexus 3164Q、31128PQ、3232C、および 3264Q スイッチでサポートされています。 • *access-list-name* 変数は、NTP アクセスグループの名前です。名前は、特殊文字を含む、最大 64 文字の英数字ストリングで指定できます。
ステップ 3	（任意） **show ntp access-groups** 例： `switch(config)# show ntp access-groups`	NTP アクセス グループのコンフィギュレーションを表示します。
ステップ 4	（任意） **copy running-config startup-config** 例： `switch(config)# copy running-config startup-config`	実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

NTP ソース IP アドレスの設定

NTP は、NTP パケットが送信されたインターフェイスのアドレスに基づいて、すべての NTP パケットにソース IP アドレスを設定します。特定のソース IP アドレスを使用するよう NTP を設定できます。

手順の概要

1. **configure terminal**
2. [**no**] **ntp source** *ip-address*
3. （任意） **copy running-config startup-config**

手順の詳細

手順

	コマンドまたはアクション	目的

ステップ 1	**configure terminal**
	例：
	`switch# configure terminal`
	`switch(config)#`
		グローバル コンフィギュレーション モードを開始します

ステップ 2	[**no**] **ntp source** *ip-address* 例： `switch(config)# ntp source 192.0.2.1`	すべての NTP パケットにソース IP アドレスを設定します。*ip-address* には IPv4 または IPv6 形式を使用できます。
ステップ 3	（任意） **copy running-config startup-config** 例： `switch(config)# copy running-config startup-config`	実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

NTP ソース インターフェイスの設定

特定のインターフェイスを使用するよう NTP を設定できます。

手順の概要

1. **configure terminal**
2. [**no**] **ntp source-interface** *interface*
3. （任意） **copy running-config startup-config**

手順の詳細

手順

	コマンドまたはアクション	目的

ステップ 1	**configure terminal**
	例：
	`switch# configure terminal`
	`switch(config)#`
		グローバル コンフィギュレーション モードを開始します。

ステップ 2	[**no**] **ntp source-interface** *interface* 例： `switch(config)# ntp source-interface ethernet 2/1`	すべての NTP パケットに対してソース インターフェイスを設定します。サポートされているインターフェイスのリストを表示するには、**?** キーワードを使用します。

	コマンドまたはアクション	目的
ステップ 3	（任意） **copy running-config startup-config** 例： `switch(config)# copy running-config startup-config`	実行コンフィギュレーションを、スタートアップコンフィギュレーションにコピーします。

NTP ロギングの設定

重要な NTP イベントでシステム ログを生成するよう、NTP ロギングを設定できます。NTP ロギングはデフォルトでディセーブルになっています。

手順の概要

1. **configure terminal**
2. [**no**] **ntp logging**
3. （任意） **show ntp logging-status**
4. （任意） **copy running-config startup-config**

手順の詳細

手順

	コマンドまたはアクション	目的

ステップ 1	**configure terminal**
	例：
	`switch# configure terminal`
	`switch(config)#`
		グローバル構成モードを開始します。

ステップ 2	[**no**] **ntp logging** 例： `switch(config)# ntp logging`	重要な NTP イベントでシステム ログを生成することをイネーブルまたはディセーブルにします。NTP ロギングはデフォルトでディセーブルになっています。
ステップ 3	（任意） **show ntp logging-status** 例： `switch(config)# show ntp logging-status`	NTP ロギングのコンフィギュレーション状況を表示します。
ステップ 4	（任意） **copy running-config startup-config** 例： `switch(config)# copy running-config startup-config`	実行コンフィギュレーションを、スタートアップコンフィギュレーションにコピーします。

NTP の設定確認

NTP 設定を表示するには、次のタスクのうちのいずれかを実行します。

コマンド	目的
show ntp access-groups	NTP アクセス グループのコンフィギュレーションを表示します。
show ntp authentication-keys	設定済みの NTP 認証キーを表示します。
show ntp authentication-status	NTP 認証の状況を表示します。
show ntp logging-status	NTP のロギング状況を表示します。
show ntp peer-status	すべての NTP サーバおよびピアのステータスを表示します。
show ntp peers	すべての NTP ピアを表示します。
show ntp rts-update	RTS アップデートの状況を表示します。
ntp ソースを表示する	設定済みの NTP ソース IP アドレスを表示します。
show ntp source-interface	設定済みの NTP ソース インターフェイスを表示します。
show ntp statistics {**io** | **local** | **memory** | **peer** {**ipaddr** {*ipv4-addr* | *ipv6-addr*} | **name** *peer-name*}}	NTP 統計情報を表示します。
show ntp trusted-keys	設定済みの NTP の信頼されているキーを表示します。
show running-config ntp	NTP 情報を表示します。

NTP セッションをクリアするには、**clear ntp session** コマンドを使用します。

NTP 統計情報を消去するには、**clear ntp statistics** コマンドを使用します。

NTP の設定例

次に、NTP パケット内で認証キー 42 を提示している時刻源とだけ同期するようデバイスを構成する md5 の例を示します。

```
switch# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
switch(config)# ntp authentication-key 42 md5 aNiceKey
switch(config)# ntp server 192.0.2.105 key 42
switch(config)# ntp trusted-key 42
switch(config)# ntp authenticate
switch(config)# copy running-config startup-config
```

```
[########################################] 100%
switch(config)#
```

次に、NTP パケット内で認証キー 12 を提示している時刻源とだけ同期するようデバイスを構成する aes128cmac の例を示します。

```
switch# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
switch(config)# ntp authentication-key 12 aes128cmac password 0/6/7
switch(config)# ntp server 192.0.2.105 key 12
switch(config)# ntp trusted-key 12
switch(config)# ntp authenticate
switch(config)# copy running-config startup-config
[########################################] 100%
switch(config)#
```

次に、以下の制約事項のある NTP アクセス グループの設定の例を示します。

- peer の制約事項は、「peer-acl」というアクセス リストの条件を満たす IP アドレスに適用されます。
- serve の制約事項は、「serve-acl」というアクセス リストの条件を満たす IP アドレスに適用されます。
- serve-only の制約事項は、「serve-only-acl」というアクセス リストの条件を満たす IP アドレスに適用されます。
- query-only の制約事項は、「query-only-acl」というアクセス リストの条件を満たす IP アドレスに適用されます。

```
switch# configure terminal
switch(config)# ntp peer 10.1.1.1
switch(config)# ntp peer 10.2.2.2
switch(config)# ntp peer 10.3.3.3
switch(config)# ntp peer 10.4.4.4
switch(config)# ntp peer 10.5.5.5
switch(config)# ntp peer 10.6.6.6
switch(config)# ntp peer 10.7.7.7
switch(config)# ntp peer 10.8.8.8
switch(config)# ntp access-group peer peer-acl
switch(config)# ntp access-group serve serve-acl
switch(config)# ntp access-group serve-only serve-only-acl
switch(config)# ntp access-group query-only query-only-acl
switch(config)# ip access-list peer-acl
switch(config-acl)# 10 permit ip host 10.1.1.1 any
switch(config-acl)# 20 permit ip host 10.8.8.8 any
switch(config)# ip access-list serve-acl
switch(config-acl)# 10 permit ip host 10.4.4.4 any
switch(config-acl)# 20 permit ip host 10.5.5.5 any
switch(config)# ip access-list serve-only-acl
switch(config-acl)# 10 permit ip host 10.6.6.6 any
switch(config-acl)# 20 permit ip host 10.7.7.7 any
switch(config)# ip access-list query-only-acl
switch(config-acl)# 10 permit ip host 10.2.2.2 any
switch(config-acl)# 20 permit ip host 10.3.3.3 any
```

（注） 単一の ACL グループのみが適用される場合、他の ACL カテゴリに関連するすべてのパケットは拒否され、設定された ACL グループに関連するパケットのみが処理されます。これについては、以下のシナリオで説明します。

- serve ACL が設定されている場合、クライアント、コントロール、およびプライベート パケットのみが処理され、他のすべてのパケットは拒否されます。
- serve-only ACL が設定されている場合、クライアント パケットのみが処理され、他のすべてのパケットは拒否されます。

複数の ACL が設定されている場合、以下のシナリオで説明されている処理の順序に従います。

- serve と serve-only の両方が、match-all が構成されていない同じ IP アドレスに対して構成されていて、IP が serve-acl で許可され、serve-only で拒否されている場合、クライアント、コントロール、プライベート パケットはその IP に対して許可されます。

その他の参考資料

関連資料

関連項目	マニュアル タイトル
クロック マネージャ	『Cisco Nexus 9000 Series NX-OS Fundamentals Configuration Guide』

MIB

MIB	MIB のリンク
NTP に関連する MIB	サポートされている MIB を検索およびダウンロ 次の URL にアクセスしてください。 https://cisco.github.io/cisco-mibs/supportlists/nexus9 Nexus9000MIBSupportList.html

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。