NTP の設定

この章は、次の内容で構成されています。

NTP の概要

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。

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。

CFS を使用した NTP の配信

Cisco Fabric Services（CFS）は、ローカル NTP コンフィギュレーションをネットワーク内のすべてのシスコデバイスに配信します。デバイス上でCFSをイネーブルにすると、NTPコンフィギュレーションが起動された場合には常に、ネットワーク全体のロックが NTP に適用されます。NTPコンフィギュレーションを変更した後で、これらの変更を破棄することもコミットすることもできます。いずれの場合でも、CFS のロックはこのときに NTP アプリケーションから解放されます。

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。

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。

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。

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 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 は、クロック プロトコルが NTP に設定されている場合に動作します。PTP と NTP を同時に構成することはサポートされていません。
- 別のデバイスとの間にピア アソシエーションを設定できるのは、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 サーバーのクライアントである場合）に限られます。
- 単独で設定したピアは、サーバー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。
- サーバーが 1 台だけの場合は、すべてのデバイスをそのサーバーのクライアントとして設定する必要があります。
- 設定できる NTP エンティティ（サーバーおよびピア）は、最大 64 です。
- NTP に対して CFS がディセーブルになっていると、その NTP からコンフィギュレーションは配信されず、ネットワーク内の他のデバイスからの配信も受け取られません。
- NTP に対して CFS 配信をイネーブルにしても、commit コマンドを入力するまで、NTP コンフィギュレーション コマンドのエントリは NTP コンフィギュレーションに対してネットワークをロックします。ロック中は、ネットワーク内の（ロックを保持しているデバイス以外の）すべてのデバイスは NTP コンフィギュレーションを変更できません。
- CFS を使用して NTP をディセーブルにする場合、ネットワーク内のすべてのデバイスは、NTP に対して使用するよう設定したものと同じ VRF を持っている必要があります。
- VRF で NTP を設定する場合は、NTP サーバーおよびピアが、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 サーバーおよび Cisco NX-OS デバイスに、NTP 認証キーを手動で配信する必要があります。

デフォルト設定

表 *1:* デフォルトの *NTP* パラメータ

パラメータ	デフォルト
NTP 認証	無効
NTP アクセス	有効
NTP ロギング	無効

NTP の設定

NTP サーバーおよびピアの構成

NTP サーバーおよびピアを設定できます。

始める前に

NTP サーバとそのピアの IP アドレスまたは DNS 名がわかっていることを確認します。

CFS を使用して他のデバイスに NTP コンフィギュレーションを配信する場合は、次を完了している必要があります。

- CFS 配信の有効化。
- CFS for NTP の有効化。

手順の概要

1. switch# **configure terminal**
2. switch(config)# [**no**] **ntp server** {*ip-address* | *ipv6-address* | *dns-name*} [**key** *key-id*] [**maxpoll** *max-poll*] [**minpoll** *min-poll*] [**prefer**] [**use-vrf** *vrf-name*]
3. switch(config)# [**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） switch(config)# **show ntp peers**
5. （任意） switch(config)# **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	switch# **configure terminal**	グローバル構成モードを開始します。
ステップ 2	switch(config)# [**no**] **ntp server** {*ip-address* | *ipv6-address* | *dns-name*} [**key** *key-id*] [**maxpoll** *max-poll*] [**minpoll** *min-poll*] [**prefer**] [**use-vrf** *vrf-name*]	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）。 これをデバイスの優先 NTP サーバーにするには、**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 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** 引数として、default、management、または 32 文字までの任意の英数字の文字列を使用できます（大文字と小文字は区別されます）。 （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	switch(config)# [**no**] **ntp peer** {*ip-address* | *ipv6-address* | *dns-name*} [**key** *key-id*] [**maxpoll** *max-poll*] [**minpoll** *min-poll*] [**prefer**] [**use-vrf** *vrf-name*]	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、

	コマンドまたはアクション	目的
		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）。 これをデバイスの優先 NTP サーバーにするには、**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 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** 引数として、default、management、または 32 文字までの任意の英数字の文字列を使用できます（大文字と小文字は区別されます）。
ステップ 4	（任意） 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。
ステップ 5	（任意） switch(config)# **copy running-config startup-config**	リブートおよびリスタート時に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て、変更を継続的に保存します。

例

NTP サーバおよびピアを設定する例を示します。

```
switch# config t
Enter configuration commands, one per line. End with CNTL/Z.
switch(config)# ntp server 192.0.2.10 key 10 use-vrf Red
switch(config)# ntp peer 2001:0db8::4101 prefer use-vrf Red
switch(config)# show ntp peers
-------------------------------------------------
Peer IP Address Serv/Peer
-------------------------------------------------
2001:0db8::4101 Peer (configured)
192.0.2.10 Server (configured)
switch(config)# copy running-config startup-config
[########################################] 100%
switch(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 認証を有効にすると、**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ソースが保持している場合のみ、デバイスはその時刻ソースと同期します。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. switch# **configure terminal**
2. switch(config)# [**no**] **ntp authentication-key** *number* **md5** *md5-string*
3. （任意） switch(config)# **show ntp authentication-keys**
4. switch(config)# [**no**]**ntp trusted-key** *number*
5. （任意） switch(config)# **show ntp trusted-keys**
6. switch(config)# [**no**] **ntp authenticate**
7. （任意） switch(config)# **show ntp authentication-status**
8. （任意） switch(config)# **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	switch# **configure terminal**	グローバル構成モードを開始します。
ステップ 2	switch(config)# [**no**] **ntp authentication-key** *number* **md5** *md5-string*	認証キーを定義します。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* コマンドによってキー番号が指定されている場合だけです。
ステップ 3	（任意） 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 4	switch(config)# [**no**]**ntp trusted-key** *number*	1 つ以上のキーを指定します。デバイスが時刻ソースと同期するために、時刻ソースはこのキーを NTP パケット内に提供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 5	（任意） 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。
ステップ 6	switch(config)# [**no**] **ntp authenticate**	NTP 認証機能をイネーブルまたはディセーブルにします。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 7	（任意） switch(config)# **show ntp authentication-status**	NTP 認証の状況を表示します。

	コマンドまたはアクション	目的
ステップ 8	（任意） switch(config)# **copy running-config startup-config**	リブートおよびリスタート時に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て、変更を継続的に保存します。

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設定する例を示します。

```
switch# config t
Enter configuration commands, one per line. End with CNTL/Z.
switch(config)# ntp authentication-key 42 md5 aNiceKey
switch(config)# ntp trusted-key 42
switch(config)# ntp authenticate
switch(config)# copy running-config startup-config
[########################################] 100%
switch(config)#
```

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。

手順の概要

1. switch# **configure terminal**
2. switch(config)# [**no**] **ntp access-group** {**peer** | **serve** | **serve-only** | **query-only**} *access-list-name*
3. （任意） switch(config)# **show ntp access-groups**
4. （任意） switch(config)# **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	switch# **configure terminal**	グローバル構成モードを開始します。
ステップ 2	switch(config)# [**no**] **ntp access-group** {**peer**	**serve**	**serve-only**	**query-only**} *access-list-name*	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。

	コマンドまたはアクション	目的
		アクセス グループのオプションは、次の順序で制限の緩いものから厳しいものへとスキャンされます。ただし、ピアに設定された拒否 ACL ルールに NTP が一致した場合、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。
ステップ 3	（任意） 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） switch(config)# **copy running-config startup-config**	リブートおよびリスタート時に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て、変更を継続的に保存します。

例

次に、アクセス グループ「accesslist1」からピアと同期できるようデバイスを構成する例を示します。

```
switch# config t
switch(config)# ntp access-group peer accesslist1
switch(config)# show ntp access-groups
Access List Type
----------------------------
accesslist1 Peer
switch(config)# copy running-config startup-config
[########################################] 100%
switch(config)#
```

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。

NTP ソース IP アドレスを設定するには、グローバル コンフィギュレーション モードで次のコマンドを使用します。

手順の概要

1. switch(config)# [**no**] **ntp source** *ip-address*

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	switch(config)# [**no**] **ntp source** *ip-address*	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。

例

次に、NTP をソース IP アドレスに構成する例を示します。

```
switch(config)# ntp source 192.0.2.1
```

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。

NTP ソース インターフェイスを設定するには、グローバル コンフィギュレーション モードで次のコマンドを使用します。

手順の概要

1. switch(config)# [**no**] **ntp source-interface** *interface*

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	switch(config)# [**no**] **ntp source-interface** *interface*	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。

例

次に、NTP を特定のインターフェイスに構成する例を示します。

```
switch(config)# ntp source-interface
ethernet 2/1
```

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. switch# **configure terminal**
2. switch(config)# [**no**] **ntp logging**
3. （任意） switch(config)# **show ntp logging-status**
4. （任意） switch(config)# **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	switch# **configure terminal**	グローバル構成モードを開始します。
ステップ 2	switch(config)# [**no**] **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） 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。

	コマンドまたはアクション	目的
ステップ 4	（任意） switch(config)# **copy running-config startup-config**	リブートおよびリスタート時に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て、変更を継続的に保存します。

例

次に、重要な NTP イベントによってシステム ログを生成するよう、NTP ロギングをイネーブルにする例を示します。

```
switch# config t
switch(config)# ntp logging
switch(config)# copy running-config startup-config
[########################################] 100%
switch(config)#
```

NTP 用の CFS 配信のイネーブル化

NTP コンフィギュレーションを他の CFS 対応デバイスに配信するために、NTP 用の CFS 配信をイネーブルにできます。

始める前に

デバイスの CFS 配信をイネーブルにしていることを確認します。

手順の概要

1. switch# **configure terminal**
2. switch(config)# [**no**] **ntp distribute**
3. （任意） switch(config)# **show ntp status**
4. （任意） switch(config)# **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	switch# **configure terminal**	グローバル構成モードを開始します。
ステップ 2	switch(config)# [**no**] **ntp distribute**	CFS を介して配信される NTP コンフィギュレーションのアップデートをデバイスが受信することを、イネーブルまたはディセーブルにします。
ステップ 3	（任意） switch(config)# **show ntp status**	NTP CFS の配信状況を表示します。

	コマンドまたはアクション	目的
ステップ 4	（任意） switch(config)# **copy running-config startup-config**	リブートおよびリスタート時に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て、変更を継続的に保存します。

例

次に、NTP のための CFS 配信をイネーブルにする例を示します。

```
switch# config t
Enter configuration commands, one per
line. End with CNTL/Z.
switch(config)# ntp distribute
switch(config)# copy running-config
startup-config
```

NTP 構成変更のコミット

NTP コンフィギュレーションの変更をコミットすると、保留データベースのコンフィギュレーション変更によって有効なデータベースが上書きされ、ネットワーク内のすべてのデバイスが同じコンフィギュレーションを受け取ります。

手順の概要

1. switch# **configure terminal**
2. switch(config)# **ntp commit**

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	switch# **configure terminal**	グローバル構成モードを開始します。
ステップ 2	switch(config)# **ntp commit**	ネットワーク内のすべての Cisco NX-OS デバイスに NTP コンフィギュレーションの変更を配信し、CFS ロックを解放します。このコマンドは、保留データベースに対して行われた変更によって、有効なデータベースを上書きします。

例

次に、NTP 構成の変更をコミットする例を示します。

```
switch(config)# ntp commit
```

NTP 設定変更の廃棄

コンフィギュレーション変更の後で、これらの変更をコミットせずに、破棄するよう選択することもできます。変更を破棄すると、Cisco NX-OS によって保留データベースの変更が削除され、CFS ロックが解放されます。

NTP コンフィギュレーションの変更を破棄するには、グローバル コンフィギュレーション モードで次のコマンドを使用します。

手順の概要

1. switch(config)# **ntp abort**

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	switch(config)# **ntp abort**	保留データベースで NTP コンフィギュレーションの変更を破棄して、CFS ロックを解放します。このコマンドは、NTP コンフィギュレーションを起動したデバイスで使用します。

例

次の例は、NTP の構成変更を破棄する方法を示しています。

```
switch(config)# ntp abort
```

CFS セッション ロックの解放

NTP コンフィギュレーションを実行したが、変更をコミットまたは破棄してロックを解放し忘れた場合は、自分で、または他の管理者がネットワーク内の任意のデバイスからロックを解放できます。また、この操作では、保留データベースの変更が破棄されます。

任意のデバイスからセッション ロックを解放し、保留データベースの変更を破棄するには、グローバル コンフィギュレーション モードで次のコマンドを使用します。

手順の概要

1. switch(config)# **clear ntp session**

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	switch(config)# **clear ntp session**	保留データベースでNTPコンフィギュレーションの変更を破棄して、CFS ロックを解放します。

例

次の例は、CFS セッション ロックを解放する方法を示しています。

```
switch(config)# clear ntp session
```

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。

clear ntp session コマンドを使用して、NTP セッションをクリアします。

clear ntp statistics コマンドを使用して、NTP 統計情報をクリアします。

手順の概要

1. **show ntp access-groups**
2. **show ntp authentication-keys**
3. **show ntp authentication-status**
4. **show ntp logging-status**
5. **show ntp peer-status**
6. **show ntp peers**
7. **show ntp pending**
8. **show ntp pending-diff**
9. **show ntp rts-update**
10. **show ntp session status**
11. **show ntp source**
12. **show ntp source-interface**
13. **show ntp statistics** {**io** | **local** | **memory** | **peer** {**ipaddr** {*ipv4-addr* | *ipv6-addr*} | **name** *peer-name*}}
14. **show ntp status**
15. **show ntp trusted-keys**
16. **show running-config ntp**

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	**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 2	**show ntp authentication-keys**	設定済みの NTP 認証キーを表示します。
ステップ 3	**show ntp authentication-status**	NTP 認証の状況を表示します。
ステップ 4	**show ntp logging-status**	NTP のロギング状況を表示します。
ステップ 5	**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。
ステップ 6	**show ntp peers**	すべての NTP ピアを表示します。
ステップ 7	**show ntp pending**	NTP 用の一時 CFS データベースを表示します。
ステップ 8	**show ntp pending-diff**	保留 CFS データベースと現行の NTP コンフィギュレーションの差異を表示します。
ステップ 9	**show ntp rts-update**	RTS アップデートの状況を表示します。
ステップ 10	**show ntp session status**	NTP CFS 配信セッションの情報を表示します。
ステップ 11	**show ntp source**	設定済みの NTP ソース IP アドレスを表示します。
ステップ 12	**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。
ステップ 13	**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。
ステップ 14	**show ntp status**	NTP CFS の配信状況を表示します。
ステップ 15	**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。
ステップ 16	**show running-config ntp**	NTP 情報を表示します。

NTP の設定例

次に、NTP サーバおよびピアを設定し、NTP 認証をイネーブルにして、NTP ロギングをイネーブルにした後で、その設定をスタートアップに保存し、リブートとリスタートを通して保存されるようにする例を示します。

```
switch# config terminal
Enter configuration commands, one per line. End with CNTL/Z.
switch(config)# ntp server 192.0.2.105 key 42
switch(config)# ntp peer 2001:0db8::4101
switch(config)# show ntp peers
-------------------------------------------------
     Peer IP Address            Serv/Peer
-------------------------------------------------
     2001:db8::4101          Peer (configured)
     192.0.2.105           Server (configured)
switch(config)# ntp authentication-key 42 md5 aNiceKey
switch(config)# show ntp authentication-keys
-----------------------------
  Auth key        MD5 String
-----------------------------
     42           aNicekey
switch(config)# ntp trusted-key 42
switch(config)# show ntp trusted-keys
Trusted Keys:
42
switch(config)# ntp authenticate
switch(config)# show ntp authentication-status
Authentication enabled.
switch(config)# ntp logging
switch(config)# show ntp logging
NTP logging enabled.
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# config 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
```

NTP の関連資料

関連項目	マニュアル タイトル
NTP CLI コマンド	*Cisco Nexus 3548* スイッチ *NX-OS* システム管理コマンド リファレンス ガイド

NTP 機能の履歴

この表には、機能の追加や変更によるリリースの更新内容のみが記載されています。

機能名	リリース	機能情報
NTP	5.0(3)A1(1)	この機能が導入されました。

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。