システムメッセージロギングの設定

この章では、Cisco NX-OS デバイス上でシステム メッセージ ロギングを設定する方法について説明します。

この章は、次の内容で構成されています。

システム メッセージ ロギングの詳細

システムメッセージロギングを使用して宛先を制御し、システムプロセスが生成するメッセージの重大度をフィルタリングできます。端末セッション、ログ ファイル、およびリモート システム上の Syslog サーバへのロギングを設定できます。

システムメッセージのフォーマットおよびデバイスが生成するメッセージの詳細については、『Cisco NX-OS System Messages Reference』を参照してください。

デフォルトでは、デバイスはターミナル セッションにメッセージを出力し、ログ ファイルにシステム メッセージをログ記録します。

次の表に、システムメッセージで使用されている重大度を示します。重大度を設定する場合、システムはそのレベル以下のメッセージを出力します。

Table 1: **システム メッセージの重大度**

レベル	説明
0：緊急	システムが使用不可

レベル	説明
1：アラート	即時処理が必要
2：クリティカル	クリティカル状態
3：エラー	エラー状態
4：警告	警告状態
5：通知	正常だが注意を要する状態
6：情報	単なる情報メッセージ
7：デバッグ	デバッグ実行時にのみ表示

デバイスは重大度 0、1、または 2 のメッセージのうち、最新の 100 メッセージを NVRAM ログに記録します。NVRAM へのロギングは設定できません。

メッセージを生成したファシリティと重大度に基づいて記録するシステム メッセージを設定できます。

Syslogサーバ

syslog サーバは、syslog プロトコルに基づいてシステム メッセージを記録するリモート システム上で動作します。IPv4 または IPv6 の Syslog サーバを最大 8 つ設定できます。

ファブリック内のすべてのスイッチで syslog サーバの同じ設定をサポートするために、Cisco Fabric Services（CFS）を使用して syslog サーバ設定を配布できます。

Note 最初のデバイス初期化時に、メッセージが syslog サーバに送信されるのは、ネットワークの初期化後です。

セキュアな Syslog サーバ

Cisco NX-OS リリース 9.2(1) 以降では、リモート ロギング サーバへのセキュアな TLS トランスポート接続をサポートするように Syslog サーバを設定できます。さらに、相互認証の設定によって NX-OS スイッチ（クライアント）のアイデンティティを強化することができます。NX-OS スイッチの場合、この機能は TLSv1.1 および TLSv1.2 をサポートします。

セキュアな Syslog サーバの機能では、デバイス認証および暗号化を提供するために TCP/TLS トランスポートおよびセキュリティ プロトコルを使用します。この機能を使用すると、（クライアントとして機能している）Cisco NX-OS デバイスが、ロギングにセキュアな接続をサポートする（サーバとして機能している）リモート Syslog サーバに対してセキュアな暗号化されたアウトバウンド接続を確立できるようになります。認証と暗号化により、この機能では、セキュリティ保護されていないネットワーク上でもセキュアな通信を実現できます。

システムメッセージロギングの注意事項および制約事項

システム メッセージ ロギングには次の設定上の注意事項と制約事項があります。

- システム メッセージは、デフォルトでコンソールおよびログ ファイルに記録されます。
- syslog サーバに到達する前に出力されるシステム メッセージ（スーパーバイザ アクティブ メッセージやオンライン メッセージなど）は、syslog サーバに送信できません。
- Cisco では、すべてのプロセスのログ レベルをデフォルトのまま維持することを推奨しています。レベルを上げて高い値に設定すると、お客様向けではないsyslogメッセージが表示される可能性があります。これらのメッセージは、誤ったアラームを生成する可能性があり、通常は TAC による短期的なトラブルシューティングの目的で使用されます。Cisco では、デフォルトよりも上のレベルの syslog メッセージをサポートしていません。
- Syslog の制限により、securePOAP pem ファイル名の文字長は 230 文字に制限されていますが、セキュア POAP は pem ファイル名として 256 文字の長さをサポートしています。
- Cisco NX-OS リリース 9.2(1) 以降では、リモート ロギング サーバへのセキュアな TLS トランスポート接続をサポートするようにSyslogサーバを設定できます。この機能は、TLS v1.1 および TLS v1.2 をサポートします。
- Cisco NX-OS リリース 10.2(4)M 以降、TLS v1.3 が Cisco Nexus 9000 シリーズ プラットフォーム スイッチでサポートされています。
- Cisco NX-OS リリース 10.4(3)F 以降、TLS v1.2 と TLS v1.3 だけが Cisco Nexus 9000 シリーズプラットフォーム スイッチでサポートされています。syslog の TLS v1.1 および TLS v1.0 のサポートは廃止されました。
- セキュアなsyslogサーバがインバンド（非管理）インターフェイスを介して到達できるようにするには、CoPP プロファイルに調整が必要な場合があります。特に、複数のロギング サーバが設定されている場合、および短時間で多数の syslog が生成される場合（ブートアップや設定アプリケーションなど）。
- このガイドラインは、ユーザ定義の永続ロギング ファイルに適用されます。

  syslogコマンド **logging logfile** では、永続的な場所（/logflash/log）と非永続的な場所（/log）の両方でログファイルを設定できます。

  デフォルトのログファイルには「messages」という名前が付けられ、バックアップ ファイル（存在する場合）とともに、**delete /log/** または **delete logflash:/log/** コマンドでもこのファイルは messages.1、messages.2、messages.3、messages.4 を削除できません。

  カスタム名のログファイル（**logging logfile** *file-name severity*）を設定するためのプロビジョニングがありますが、このカスタム名のファイルは削除操作によって削除できます。この場合、syslog ロギングは機能しません。

  たとえば、カスタム名のログ ファイルが設定され、同じファイルが削除操作によって削除されます。これは意図的な削除操作であるため、syslogメッセージをカスタム ログファイルに記録するには、コマンド **logging logfile** *file-name severity* を使用してカスタム ログファ

イルを再設定する必要があります。この設定が実行されるまで、syslog ロギングは実行できません。

- 通常、syslog にはローカル タイム ゾーンが表示されます。ただし、NGINX などの一部のコンポーネントでは、ログが UTC タイム ゾーンで表示されます。
- Cisco NX-OS リリース 10.3(4a)M 以降では、syslog プロトコル RFC 5424 を有効にする既存の **logging rfc-strict 5424** コマンド（オプション）が、次のように新しいキーワード（**full**）を追加することで拡張されています。

  logging rfc-strict 5424 full

  このキーワードを追加すると、Syslog プロトコルの RFC 5424 標準に完全に準拠します。ただし、`[APP-NAME] [PROCID] [MSG-ID] [STRUCTRED-DATA]` フィールドに値が使用できない場合、nil 値はダッシュ（-）で示されます。
- Cisco NX-OS リリース 10.5（3）以降では、syslog プロトコル RFC 5424 を有効にする既存の **logging rfc-strict 5424** コマンド（オプション）が、次のように新しいキーワード（**utc**）を追加することで拡張されています。

  logging rfc-strict 5424 utc

  このキーワードを追加すると、UTC 時刻フォーマット付きの Syslog プロトコルの RFC 5424 標準を有効にします。

  次のコマンドを使用して、Syslog プロトコルの RFC 5424 標準に UTC 時間形式で完全に準拠することもできます： **logging rfc-strict 5424 utc full**。

システム メッセージ ロギングのデフォルト設定

次の表に、システム メッセージ ロギング パラメータのデフォルト設定を示します。

Table 2: **デフォルトのシステム メッセージ ロギング パラメータ**

パラメータ	デフォルト
コンソール ロギング	重大度 2 でイネーブル
モニタ ロギング	重大度 5 でイネーブル
ログ ファイル ロギング	重大度 5 のメッセージ ロギングがイネーブル
モジュール ロギング	重大度 5 でイネーブル
ファシリティ ロギング	イネーブル
タイムスタンプ単位	秒
Syslog サーバ ロギング	ディセーブル
Syslog サーバ設定の配布	無効化

システムメッセージロギングの設定

（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。

ターミナル セッションへのシステム メッセージ ロギングの設定

重大度に基づいて、コンソール、Telnet、および SSH セッションにメッセージを記録するようにデバイスを設定できます。

デフォルトでは、ターミナル セッションでロギングはイネーブルです。

Note コンソールのボー レートが 9600 ボー（デフォルト）の場合、現在の Critical（デフォルト）ロギング レベルが維持されます。コンソール ロギング レベルを変更しようとすると、必ずエラー メッセージが生成されます。ロギング レベルを上げる（Critical よりも上に）には、コンソールのボー レートを 38400 ボーに変更する必要があります。

SUMMARY STEPS

1. **terminal monitor**
2. **configure terminal**
3. [**no**] **logging console** [*severity-level*]
4. (Optional) **show logging console**
5. [**no**] **logging monitor** [*severity-level*]
6. (Optional) **show logging monitor**
7. [**no**] **logging message interface type ethernet description**
8. (Optional) **copy running-config startup-config**

DETAILED STEPS

Procedure

	Command or Action	Purpose
ステップ 1	**terminal monitor** **Example:** `switch# terminal monitor`	デバイスがコンソールにメッセージを記録できるようにします。
ステップ 2	**configure terminal** **Example:**	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

	Command or Action	Purpose
	`switch# configure terminal` `switch(config)#`	
ステップ 3	[**no**] **logging console** [*severity-level*] **Example:** `switch(config)# logging console 3`	指定された重大度とそれより上位の重大度のメッセージをコンソールセッションに記録するように、デバイスを設定します。小さい値は、より高い重大度を示します。重大度は 0 ～ 7 の範囲です。 • 0：緊急 • 1：アラート • 2：クリティカル • 3：エラー • 4：警告 • 5：通知 • 6：情報 • 7：デバッグ 重大度が指定されていない場合、デフォルトの 2 が使用されます。**no** オプションは、メッセージをコンソールにログするデバイスの機能をディセーブルにします。
ステップ 4	(Optional) **show logging console** **Example:** `switch(config)# show logging console`	コンソール ロギング設定を表示します。
ステップ 5	[**no**] **logging monitor** [*severity-level*] **Example:** `switch(config)# logging monitor 3`	デバイスが指定された重大度とそれより上位の重大度のメッセージをモニタに記録できるようにします。小さい値は、より高い重大度を示します。重大度は 0 ～ 7 の範囲です。 • 0：緊急 • 1：アラート • 2：クリティカル • 3：エラー • 4：警告 • 5：通知 • 6：情報

	Command or Action	Purpose
		• 7：デバッグ 設定は Telnet および SSH セッションに適用されます。 重大度が指定されていない場合、デフォルトの 2 が使用されます。**no** オプションは、メッセージを Telnet および SSH セッションにログするデバイスの機能をディセーブルにします。
ステップ 6	(Optional) **show logging monitor** **Example:** `switch(config)# show logging monitor`	モニタ ロギング設定を表示します。
ステップ 7	[**no**] **logging message interface type ethernet description** **Example:** `switch(config)# logging message interface type ethernet description`	システム メッセージ ログ内で、物理的なイーサネット インターフェイスおよびサブインターフェイスに対して説明を追加できるようにします。この説明は、インターフェイスで設定された説明と同じものです。 **no** オプションは、物理イーサネット インターフェイスのシステム メッセージ ログ内のインターフェイス説明の印刷をディセーブルにします。
ステップ 8	(Optional) **copy running-config startup-config** **Example:** `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。

Syslog メッセージの送信元 ID の設定

リモート syslog サーバに送信される syslog メッセージにホスト名、IP アドレス、またはテキスト文字列を付加するように Cisco NX-OS を設定できます。

手順の概要

1. **configure terminal**
2. **logging origin-id** {**hostname** | **ip** *ip-address* | **string** *text-string*}
3. （任意） **show logging origin-id**
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	必須: **logging origin-id** {**hostname** | **ip** *ip-address* | **string** *text-string*} 例： `switch(config)# logging origin-id string n9k-switch-abc`	リモート syslog サーバに送信される syslog メッセージに追加するホスト名、IPアドレス、またはテキスト文字列を指定します。
ステップ 3	（任意） **show logging origin-id** 例： `switch(config)# show logging origin-id` `Logging origin_id : enabled (string: n9k-switch-abc)`	リモート syslog サーバに送信される syslog メッセージに付加される、設定済みのホスト名、IP アドレス、またはテキスト文字列を表示します。
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。

ファイルへのシステム メッセージの記録

システム メッセージをファイルに記録するようにデバイスを設定できます。デフォルトでは、システム メッセージは /logflash/log/*logfilename* に記録されます。

手順の概要

1. **configure terminal**
2. [**no**] **logging logfile** *logfile-name severity-level* [**persistent threshold** *percent* | **size** *bytes*]
3. **logging event** {**link-status** | **trunk-status**} {**enable** | **default**}
4. （任意） **show logging info**
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**] **logging logfile** *logfile-name severity-level* [**persistent threshold** *percent* | **size** *bytes*] 例： `switch(config)# logging logfile my_log 6` `switch(config)# logging logfile my_log 6 persistent threshold 90`	非永続的または永続的なログファイルパラメータを設定します。 *logfile-name*：システム メッセージの保存に使用するログ ファイルの名前を設定します。デフォルトのファイル名は「message」です。 severity-level：ログに記録する最小の重大度レベルを設定します。小さい値は、より高い重大度を示します。デフォルトは 5 です。範囲は 0 ー 7 です。 • 0：緊急 • 1：アラート • 2：クリティカル • 3：エラー • 4：警告 • 5：通知 • 6：情報 • 7：デバッグ **persistent threshold** *percent*：オプションで、永続ログ ファイルのしきい値パーセンテージを設定します。範囲は 0 ～ 99 です。 （注） **persistent threshold** を 0（ゼロ）に設定すると、永続しきい値機能が無効になり、しきい値 syslog は生成されません。 *percent* は、永続ファイルのパーセントしきい値サイズを設定します。しきい値サイズに達すると、アラート通知メッセージがログに記録されます。永続ログファイルの使用率が 100% に達すると、システ

	コマンドまたはアクション	目的
		ムは別の syslog メッセージ通知を送信します。既存のログ ファイルのバックアップファイルが作成され、設定されたしきい値のパーセンテージが適用される、新しいログ ファイルへの書き込みが開始されます。最大で、新しい方から合計 5 つのバックアップファイルが保持されます。5ファイルを超えると、システムは最も古いものからファイルを削除します。 （注） 永続的ロギングは、システム対応の機能です。ログ ファイルは /logflash/log/[filename] にあります。 次の show コマンドの出力は、永続ログ ファイル機能をサポートしています。 • **show logging info** • **show logging** 出力には、永続ログについての次のような情報が含まれます。 `Logging logflash: enabled (Severity: notifications)(threshold percentage: 99)` `Logging logfile: enabled` `Name - messages: Severity - notifications Size - 4194304` **size** *bytes*：オプションとして、最大ファイル サイズを指定します。範囲は4096 ー 4194304 バイトです。
ステップ 3	**logging event** {**link-status** | **trunk-status**} {**enable** | **default**} 例： `switch(config)# logging event link-status default`	インターフェイス イベントをロギングします。 • **link-status**：すべての UP/DOWN メッセージおよびCHANGEメッセージをログに記録します。 • **trunk-status**：すべてのトランク ステータス メッセージをロギングします。 • **enable**：ポート レベルのコンフィギュレーションを上書きしてロギングをイネーブルにするよう、指定します。 • **default**：ロギングが明示的に設定されてないインターフェイスで、デフォルトのロギング設定を使用するよう、指定します。
ステップ 4	（任意） **show logging info** 例：	ロギング設定を表示します。

	コマンドまたはアクション	目的
	`switch(config)# show logging info`	
ステップ 5	（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。

モジュールおよびファシリティ メッセージのロギングの設定

モジュールおよびファシリティに基づいて記録するメッセージの重大度およびタイムスタンプの単位を設定できます。

SUMMARY STEPS

1. **configure terminal**
2. [**no**] **logging module** [*severity-level*]
3. (Optional) **show logging module**
4. [**no**] **logging level** *facility severity-level*
5. (Optional) **show logging level** [*facility*]
6. (Optional) [**no**] **logging level** *ethpm*
7. [**no**] **logging timestamp** {**microseconds** |**milliseconds** |**seconds**}
8. (Optional) **show logging timestamp**
9. (Optional) **copy running-config startup-config**

DETAILED STEPS

Procedure

	Command or Action	Purpose
ステップ 1	**configure terminal** **Example:** `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**] **logging module** [*severity-level*] **Example:** `switch(config)# logging module 3`	指定された重大度またはそれ以上の重大度であるモジュール ログ メッセージをイネーブルにします。重大度は 0 ～ 7 の範囲です。 • 0：緊急 • 1：アラート • 2：クリティカル • 3：エラー

	Command or Action	Purpose
		• 4：警告 • 5：通知 • 6：情報 • 7：デバッグ 重大度が指定されていない場合、デフォルトの 5 が使用されます。**no** オプションを使用すると、モジュール ログ メッセージがディセーブルになります。
ステップ 3	(Optional) **show logging module** **Example:** `switch(config)# show logging module`	モジュール ロギング設定を表示します。
ステップ 4	[**no**] **logging level** *facility severity-level* **Example:** `switch(config)# logging level aaa 2`	指定された重大度またはそれ以上の重大度である指定のファシリティからのロギング メッセージをイネーブルにします。重大度は 0 ～ 7 の範囲です。 • 0：緊急 • 1：アラート • 2：クリティカル • 3：エラー • 4：警告 • 5：通知 • 6：情報 • 7：デバッグ 同じ重大度をすべてのファシリティに適用するには、**all** ファシリティを使用します。デフォルト値については、**show logging level** コマンドを参照してください。 **no** オプションを使用すると、指定されたファシリティのロギング重大度がデフォルトのレベルにリセットされます。ファシリティおよび重大度を指定しなかった場合、すべてのファシリティがそれぞれのデフォルト重大度にリセットされます。
ステップ 5	(Optional) **show logging level** [*facility*] **Example:**	ファシリティごとに、ロギング レベル設定およびシステムのデフォルト レベルを表示します。ファシリ

	Command or Action	Purpose
	`switch(config)# show logging level aaa`	ティを指定しなかった場合は、すべてのファシリティのレベルが表示されます。 **Note** 実行構成での authpriv のロギング レベルは、10.4(3)F より前のリリースでは authpri として表示され、リリース 10.4(3)F からは authpriv として表示されます。
ステップ 6	(Optional) [**no**] **logging level** *ethpm* **Example:** **switch(config)# logging level ethpm ?** <0-7> 0-emerg;1-alert;2-crit;3-err;4-warn;5-notif;6-inform;7-debug link-down Configure logging level for link down syslog messages link-up Configure logging level for link up syslog messages **switch(config)#logging level ethpm link-down ?** error ERRORS notif NOTICE **(config)# logging level ethpm link-down error ?** <CR> **(config)# logging level ethpm link-down notif ?** <CR> **switch(config)#logging level ethpm link-up ?** error ERRORS notif NOTICE **(config)# logging level ethpm link-up error ?** <CR> **(config)# logging level ethpm link-up notif ?** <CR>	レベル 3 のイーサネット ポート マネージャ リンクアップ/リンクダウン syslog メッセージのロギングを有効にします。 **no** オプションを使用すると、イーサネット ポート マネージャの syslog メッセージにデフォルトのロギング レベルが使用されます。
ステップ 7	[**no**] **logging timestamp** {**microseconds** |**milliseconds** |**seconds**} **Example:** `switch(config)# logging timestamp milliseconds`	ロギング タイムスタンプ単位を設定します。デフォルトでは、単位は秒です。 **Note** このコマンドは、スイッチ内で保持されているログに適用されます。また、外部のロギング サーバには適用されません。
ステップ 8	(Optional) **show logging timestamp** **Example:** `switch(config)# show logging timestamp`	設定されたロギング タイムスタンプ単位を表示します。

	Command or Action	Purpose
ステップ 9	(Optional) **copy running-config startup-config** **Example:** `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。

RFC 5424 に準拠したロギング syslog の構成

コマンドは、次の方法で変更できます：

- [*no*] **logging rfc-strict 5424**
- **show logging rfc-strict 5424**

手順の概要

1. `switch(config)#`[*no*] logging rfc-strict 5424
2. `switch(config)#` **logging rfc-strict 5424**
3. `switch(config)#`show logging rfc-strict 5424

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*] logging rfc-strict 5424	（オプション）コマンドを無効にするか、またはそのデフォルトに設定します
ステップ 2	`switch(config)#` **logging rfc-strict 5424**	メッセージ ロギング ファシリティを変更し、メッセージが準拠する必要のある RFC を設定します。
ステップ 3	`switch(config)#`show logging rfc-strict 5424	RFC 5424 に準拠する syslog を表示します

syslog サーバの設定

Note シスコは、管理仮想ルーティングおよび転送（VRF）インスタンスを使用するサーバとして、syslog サーバを設定することを推奨します。VRF の詳細情報については、『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。

システム メッセージを記録する、リモート システムを参照する syslog サーバーを最大で 8 台設定できます。

Note Cisco NX-OS リリース 10.3(2)F までは、ユーザーが特定のデフォルト値を入力すると、logging server コマンドの実行中の構成にそれらのデフォルト値がランダムまたは一貫性なく表示されていました。ただし、Cisco NX-OS リリース 10.3(2)F 以降では、実行中の構成には常にデフォルト以外の値のみが表示されます。

たとえば、以前のリリースで、特定のユーザー入力に対し、実行中の構成が `logging server 1.1.1.1 port 514 facility local7 use-vrf default` という値を表示していたような場合、Cisco NX-OS リリース 10.3(2)F 以降では、同じ入力に対し、実行中の構成は `logging server 1.1.1.1` という値のみを表示します。デフォルト ポート、デフォルト ファシリティ（local7）、デフォルト VRF などのデフォルト値が実行中の構成で表示されないことに注意してください。

SUMMARY STEPS

1. **configure terminal**
2. [**no**] **logging server** *host* [*severity-level* [**use-vrf** *vrf-name*]]
3. **logging source-interface loopback** *virtual-interface*
4. (Optional) **show logging server**
5. (Optional) **copy running-config startup-config**

DETAILED STEPS

Procedure

	Command or Action	Purpose
ステップ 1	**configure terminal** **Example:** `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**] **logging server** *host* [*severity-level* [**use-vrf** *vrf-name*]] **Example:** `switch(config)# logging server 192.0.2.253` **Example:** `switch(config)# logging server 2001::3 5 use-vrf red`	指定されたホスト名、IPv4 または IPv6 アドレスで Syslog サーバーを構成します。**use-vrf** キーワードを使用すると、メッセージ ロギングを VRF の特定の Syslog サーバーに限定できます。 **use-vrf** *vrf-name* キーワードは、VRF 名のデフォルトまたは管理値を示します。デフォルト VRF は、デフォルトで管理 VRF です。ただし、**show-running** コマンドはデフォルトの VRF をリストしません。重大度は 0 ～ 7 の範囲です。 • 0：緊急 • 1：アラート • 2：クリティカル

	Command or Action	Purpose
		• 3：エラー • 4：警告 • 5：通知 • 6：情報 • 7：デバッグ デフォルトの発信ファシリティは local7 です。 **no** オプションは、指定したホストのロギング サーバを削除します。 この最初の例では、ファシリティ local 7 のすべてのメッセージを転送します。2 番目の例では、重大度が 5 以下のメッセージを、VRF red の指定された IPv6 アドレスに転送します。 **Note** このコマンドを構成すると、次のいずれかのサーバー ステータスが表示されます。 • **[構成済み（Configured）]**：正常に構成されました。 • **[エラーは見つかりませんでした（No errors found）]**：syslog がリモート syslog サーバーに正常に送信された場合、このステータスが表示されます。 • **[一時的に到達不能（Temporarily unreachable）]**：送信に問題がある場合、このステータスが表示されます。ただし、内部では、システムは送信の問題を探査しています。しばらくして問題が解決すると、ステータスは [エラーが見つかりませんでした（No errors found）] に変わります。
ステップ 3	Required: **logging source-interface loopback** *virtual-interface* **Example:** `switch(config)# logging source-interface loopback 5`	リモート Syslog サーバの送信元インターフェイスをイネーブルにします。 *virtual-interface* 引数の範囲は 0 ～ 1023 です。
ステップ 4	(Optional) **show logging server** **Example:** `switch(config)# show logging server`	Syslog サーバ設定を表示します。

	Command or Action	Purpose
ステップ 5	(Optional) **copy running-config startup-config** **Example:** `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。

セキュアな Syslog サーバの設定

手順の概要

1. **configure terminal**
2. [**no**] **logging server** *host* [*severity-level* [**port** *port-number*][**secure**[**trustpoint client-identity** *trustpoint-name*]][**use-vrf** *vrf-name*]]
3. （任意） **logging source-interface** *interface name*
4. （任意） **show logging server**
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**] **logging server** *host* [*severity-level* [**port** *port-number*][**secure**[**trustpoint client-identity** *trustpoint-name*]][**use-vrf** *vrf-name*]] 例： `switch(config)# logging server 192.0.2.253 secure` 例： `switch(config)# logging server 2001::3 5 secure trustpoint client-identity myCA use-vrf red`	指定されたホスト名、あるいは IPv4 または IPv6 アドレスで Syslog サーバを設定します。必要に応じて、CA によって署名されるクライアント アイデンティティ証明書をインストールし、trustpoint client-identity オプションを使用することで相互認証を適用できます。 セキュアな TLS 接続のデフォルト宛先ポートは 6514 です。
ステップ 3	（任意） **logging source-interface** *interface name* 例： `switch(config)# logging source-interface lo0`	リモート Syslog サーバの送信元インターフェイスをイネーブルにします。
ステップ 4	（任意） **show logging server** 例：	Syslog サーバ設定を表示します。secure オプションを設定する場合、出力のエントリにトランスポート

	コマンドまたはアクション	目的
	`switch(config)# show logging server`	情報が含まれるようになります。デフォルトでは、secure オプションが設定されていない場合、トランスポートは UDP です。
ステップ 5	（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。

セキュアな Syslog サーバーの構成 - OCSP の non-strict モード

Cisco NX-OS リリース 9.3(8) では、OCSP レスポンダがダウンしている場合、または OCSP 署名の問題がある場合、OCSP は strict モードで動作するため、SSL 接続は失敗します。したがって、Cisco NX-OS リリース 9.3(9) 以降、strict モードを有効または無効にできる次の新しいコマンドが導入されました。

[**no**] **logging secure ocsp strict**

（注） デフォルトでは、strict-mode が有効になっています。non-strict モードを有効にするには、このコマンドの no 形式を使用します。

CA 証明書の設定

セキュアな Syslog 機能のサポートには、トラストポイントの設定によってリモート サーバを認証する必要があります。

手順の概要

1. **configure terminal**
2. [**no**] **crypto ca trustpoint** *trustpoint-name*
3. **crypto ca authenticate** *trustpoint-name*
4. （任意） **show crypto ca certificate**
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**] **crypto ca trustpoint** *trustpoint-name* 例： `switch(config)# crypto ca trustpoint winca` `switch(config-trustpoint)#`	トラストポイントを設定します。 （注） トラストポイントの設定の前に ip domain-name を設定する必要があります。
ステップ 3	必須: **crypto ca authenticate** *trustpoint-name* 例： `switch(config-trustpoint)# crypto ca authenticate winca`	トラストポイントの CA 証明書を設定します。
ステップ 4	（任意） **show crypto ca certificate** 例： `switch(config)# show crypto ca certificates`	設定されている証明書/チェーンと、関連付けられているトラストポイントを表示します。
ステップ 5	（任意） **copy running-config startup-config** 例： `switch(config)# copy running-config startup-config`	デバイスのリロード後にトラストポイントが持続されるように、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ます。

CA 証明書の登録

NX-OS スイッチ（クライアント）が識別するようリモートサーバによって要求される相互認証では、ピア認証が必須であるため、これは証明書をスイッチに登録するための追加設定です。

手順の概要

1. **configure terminal**
2. **crypto key generate rsa label** *key name* **exportable modules 2048**
3. [**no**] **crypto ca trustpoint** *trustpoint-name*
4. **rsakeypair** *key-name*
5. **crypto ca trustpoint** *trustpoint-name*
6. [**no**] **crypto ca enroll** *trustpoint-name*
7. **crypto ca import** *trustpoint-name* **certificate**

8. （任意） **show crypto ca certificates**
9. **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	必須: **crypto key generate rsa label** *key name* **exportable modules 2048** 例： `switch(config-trustpoint)# crypto key generate rsa label myKey exportable modulus 2048`	RSA キーペアを設定します。デフォルトでは、Cisco NX-OS ソフトウェアは 1024 ビットの RSA キーを作成します。
ステップ 3	[**no**] **crypto ca trustpoint** *trustpoint-name* 例： `switch(config)# crypto ca trustpoint myCA` `switch(config-trustpoint)#`	トラストポイントを設定します。 （注） トラストポイントの設定の前に ip domain-name を設定する必要があります。
ステップ 4	必須: **rsakeypair** *key-name* 例： `switch(config-trustpoint)# rsakeypair myKey`	トラストポイント CA に生成されたキーペアを関連付けます。
ステップ 5	**crypto ca trustpoint** *trustpoint-name* 例： `switch(config)# crypto ca authenticate myCA`	トラストポイントの CA 証明書を設定します。
ステップ 6	[**no**] **crypto ca enroll** *trustpoint-name* 例： `switch(config)# crypto ca enroll myCA`	CA に登録するスイッチのアイデンティティ証明書を生成します。
ステップ 7	**crypto ca import** *trustpoint-name* **certificate** 例： `switch(config-trustpoint)# crypto ca import myCA certificate`	CA によって署名されたアイデンティティ証明書をスイッチにインポートします。
ステップ 8	（任意） **show crypto ca certificates** 例： `switch# show crypto ca certificates`	設定されている証明書またはチェーンと、関連付けられているトラストポイントを表示します。

	コマンドまたはアクション	目的
ステップ 9	必須: **copy running-config startup-config** 例： `switch# 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。

UNIX または Linux システムでの syslog サーバの設定

/etc/syslog.conf ファイルに次の行を追加して、UNIX または Linux システム上に syslog サーバを設定できます。

facility.level <five tab characters> *action*

次の表に、設定可能な syslog フィールドを示します。

表 *3 : syslog.conf* の *syslog* フィールド

フィールド	説明
Facility	メッセージの作成者。auth、authpriv、cron、daemon、kern、lpr、mail、mark、news、syslog、user、local0 ～ local7 です。アスタリスク（*）を使用するとすべてを指定します。これらのファシリティ指定により、発信元に基づいてメッセージの宛先を制御できます。 （注） ローカル ファシリティを使用する前に設定をチェックします。
Level	メッセージを記録する最小重大度。debug、info、notice、warning、err、crit、alert、emerg です。アスタリスク（*）を使用するとすべてを指定します。none を使用するとファシリティをディセーブルにできます。
Action	メッセージの宛先。ファイル名、前に @ 記号を加えたホスト名、ユーザをカンマで区切ったリスト、またはすべてのログイン ユーザを表すアスタリスク（*）を使用できます。

手順の概要

1. /etc/syslog.conf ファイルに次の行を追加して、ファイル /var/log/myfile.log に local7 ファシリティのデバッグ メッセージを記録します。
2. シェル プロンプトで次のコマンドを入力して、ログ ファイルを作成します。

3. 次のコマンドを入力して、システム メッセージ ロギング デーモンが myfile.log をチェックして、新しい変更を取得するようにします。

手順の詳細

手順

ステップ 1 /etc/syslog.conf ファイルに次の行を追加して、ファイル /var/log/myfile.log に local7 ファシリティのデバッグ メッセージを記録します。

例：

```
debug.local7 var/log/myfile.log
```

ステップ 2 シェル プロンプトで次のコマンドを入力して、ログ ファイルを作成します。

例：

```
$ touch /var/log/myfile.log
$ chmod 666 /var/log/myfile.log
```

ステップ 3 次のコマンドを入力して、システム メッセージ ロギング デーモンが myfile.log をチェックして、新しい変更を取得するようにします。

例：

```
$ kill -HUP ~cat /etc/syslog.pid~
```

ログ ファイルの表示およびクリア

ログ ファイルおよび NVRAM のメッセージを表示したり消去したりできます。

SUMMARY STEPS

1. **show logging last** *number-lines*
2. **show logging logfile duration** *hh:mm:ss*
3. **show logging logfile last-index**
4. **show logging logfile** [**start-time** *yyyy mmm dd hh:mm:ss*] [**end-time** *yyyy mmm dd hh:mm:ss*]
5. **show logging logfile** [**start-seqn** *number*] [**end-seqn** *number*]
6. **show logging nvram** [**last** *number-lines*]
7. **clear logging logfile** [**persistent**]
8. **clear logging nvram**

DETAILED STEPS

Procedure

	Command or Action	Purpose
ステップ 1	Required: **show logging last** *number-lines* **Example:** `switch# show logging last 40`	ロギング ファイルの最終行番号を表示します。最終行番号には 1 ～ 9999 を指定できます。
ステップ 2	**show logging logfile duration** *hh:mm:ss* **Example:** `switch# show logging logfile duration 15:10:0`	入力された時間内のタイム スタンプを持つログ ファイルのメッセージを表示します。
ステップ 3	**show logging logfile last-index** **Example:** `switch# show logging logfile last-index`	ログファイルの最後のメッセージのシーケンス番号を表示します。
ステップ 4	**show logging logfile** [**start-time** *yyyy mmm dd hh:mm:ss*] [**end-time** *yyyy mmm dd hh:mm:ss*] **Example:** `switch# show logging logfile start-time 2013 oct 1 15:10:0`	入力されたスパン内にタイム スタンプがあるログ ファイルのメッセージを表示します。終了時間を入力しないと、現在の時間が使用されます。月の時間フィールドには 3 文字を、年と日の時間フィールドには数値を入力します。
ステップ 5	**show logging logfile** [**start-seqn** *number*] [**end-seqn** *number*] **Example:** `switch# show logging logfile start-seqn 100 end-seqn 400`	シーケンス番号の範囲内である、発生したメッセージを表示します。終了シーケンス番号を指定しなかった場合は、ログ ファイルの、開始番号から最後のメッセージまでのメッセージが表示されます。
ステップ 6	**show logging nvram** [**last** *number-lines*] **Example:** `switch# show logging nvram last 10`	NVRAM のメッセージを表示します。表示される行数を制限するには、表示する最終行番号を入力できます。最終行番号には 1 ～ 100 を指定できます。
ステップ 7	**clear logging logfile** [**persistent**] **Example:** `switch# clear logging logfile`	ログ ファイルの内容をクリアします。 **persistent**：永続的な場所から、ログファイルの内容をクリアします。
ステップ 8	**clear logging nvram** **Example:** `switch# clear logging nvram`	NVRAM の記録されたメッセージをクリアします。

システム メッセージ ロギングの設定確認

システム メッセージ ロギングの設定情報を表示するには、次の作業のいずれかを行います。

コマンド	目的
show logging console	コンソール ロギング設定を表示します。
show logging info	ロギング設定を表示します。
show logging last *number-lines*	ログ ファイルの末尾から指定行数を表示します。
show logging level [*facility*]	ファシリティ ロギング重大度設定を表示します。
show logging logfile duration *hh:mm:ss*	入力された時間内のタイム スタンプを持つログ ファイルのメッセージを表示します。
show logging logfile last-index	ログファイルの最後のメッセージのシーケンス番号を表示します。
show logging logfile [**start-time** *yyyy mmm dd hh:mm:ss*] [**end-time** *yyyy mmm dd hh:mm:ss*]	開始日時と終了日時に基づいてログファイルのメッセージを表示します。
show logging logfile [**start-seqn** *number*] [**end-seqn** *number*]	シーケンス番号の範囲内である、発生したメッセージを表示します。終了シーケンス番号を指定しなかった場合は、ログ ファイルの、開始番号から最後のメッセージまでのメッセージが表示されます。
show logging module	モジュール ロギング設定を表示します。
show logging monitor	モニタ ロギング設定を表示します。
show logging nvram [**last** *number-lines*]	NVRAM ログのメッセージを表示します。
show logging server	Syslog サーバ設定を表示します。
show logging timestamp	ロギング タイムスタンプ単位設定を表示します。

繰り返されるシステム ロギング メッセージ

システム プロセスはロギング メッセージを生成します。生成される重大度レベルを制御するために使用されるフィルタによっては、多数のメッセージが生成され、その多くが繰り返されます。

ロギング メッセージの量を管理するスクリプトの開発を容易にし、**show logging log** コマンドの出力の「フラッディング」から繰り返されるメッセージを排除するために、繰り返されるメッセージをロギングする次の方法が使用されます。

以前の方法では、同じメッセージが繰り返された場合、デフォルトでは、メッセージ内でメッセージが再発生した回数が示されていました。

```
2019 Mar 11 13:42:44 Cisco-customer %PTP-2-PTP_INCORRECT_PACKET_ON_SLAVE:
Incorrect delay response packet received on slave interface Eth1/48 by
```

```
2c:5a:0f:ff:fe:51:e9:9f. Source Port Identity is 08:00:11:ff:fe:22:3e:4e. Requesting
Port
Identity is 00:1c:73:ff:ff:ee:f6:e5
2019 Mar 11 13:43:15 Cisco-customer last message repeated 242 times
```

新しいメソッドは、繰り返しメッセージの最後に繰り返し回数を追加するだけです。

```
2019 Mar 11 13:42:44 Cisco-customer %PTP-2-PTP_INCORRECT_PACKET_ON_SLAVE:
Incorrect delay response packet received on slave interface Eth1/48 by
2c:5a:0f:ff:fe:51:e9:9f. Source Port Identity is 08:00:11:ff:fe:22:3e:4e. Requesting
Port
Identity is 00:1c:73:ff:ff:ee:f6:e5

2019 Mar 11 13:43:15 Cisco-customer %PTP-2-PTP_INCORRECT_PACKET_ON_SLAVE:
Incorrect delay response packet received on slave interface Eth1/48 by
2c:5a:0f:ff:fe:51:e9:9f. Source Port Identity is 08:00:11:ff:fe:22:3e:4e. Requesting
Port
Identity is 00:1c:73:ff:ff:ee:f6:e5 (message repeated 242 times)
```

システム メッセージ ロギングの設定例

システム メッセージ ロギングのコンフィギュレーション例を示します。

```
configure terminal
 logging console 3
 logging monitor 3
 logging logfile my_log 6
 logging module 3
 logging level aaa 2
 logging timestamp milliseconds
 logging server 172.28.254.253
 logging server 172.28.254.254 5 facility local3
 copy running-config startup-config
```

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
システム メッセージ	『*Cisco NX-OS System Messages Reference*』

関連資料

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。