ロギング サービスの実装

このモジュールでは、ロギング サービスをルータに実装する必要がある新しいタスクと改訂されたタスクを説明します。

Cisco IOS XR ソフトウェアには基本ロギング サービスが用意されています。 ロギング サービスでは、システム ロギング（syslog）メッセージモニタリングおよびトラブルシューティングのロギング情報を収集し、取得したロギング情報のタイプを選択できます。

（注） Cisco IOS XR ソフトウェアでのロギング サービスおよびこのモジュールの一覧で示されているロギング コマンドの詳細については、このモジュールの「関連資料，（32 ページ）」の項を参照してください。

ロギング サービスの実装の機能履歴

リリース	変更箇所
リリース 3.7.2	この機能が導入されました。

ロギング サービスを実装する前提条件

ネットワーク オペレーション センター（NOC）でロギング サービスを実装するには、次の前提条件が必要です。

- 適切なタスク ID を含むタスク グループに関連付けられているユーザ グループに属している必要があります。 このコマンド リファレンスには、各コマンドに必要なタスク ID が含まれます。ユーザ グループの割り当てが原因でコマンドを使用できないと考えられる場合、AAA 管理者に連絡してください。
- syslog サーバ ホストを syslog メッセージの受信先に設定するには、syslog サーバに接続できる必要があります。

ロギング サービスの実装に関する情報

ロギング サービスを実装するには、次の概念を理解する必要があります。

システム ロギング プロセス

デフォルトでは、ルータは syslog メッセージを syslog プロセスに送信するように設定されます。syslog プロセスでは、ロギング バッファ、端末回線、syslog サーバのなどの syslog メッセージの宛先に対するメッセージの分配を制御します。 syslog プロセスはデフォルトでメッセージをコンソール端末にも送信します。

システム ロギング メッセージの形式

デフォルトでは、Cisco IOS XR ソフトウェアの syslog プロセスで生成される syslog メッセージの一般形式は、次のようになります。

node-id : *timestamp* : *process-name* [*pid*] : % *message -group -severity -message -code* : *message-text*

次にサンプルの syslog メッセージを示します。

```
RP/0/RSP0/CPU0:Nov 28 23:56:53.826 : config[65710]: %SYS-5-CONFIG_I : Configured from console
 by console
```

この表では、Cisco IOS XR ソフトウェアの syslog メッセージの一般的な形式を説明します。

表 *1*：一般的な *syslog* メッセージ形式

フィールド	説明
node-id	syslog メッセージの生成元となるノードです。

フィールド	説明
timestamp	*month day HH:MM:SS* 形式のタイム スタンプです。メッセージが生成された日時を示します。 （注） タイム スタンプ形式は、**service timestamps** コマンドを使用して変更できます。タイムスタンプの形式の修正，（19 ページ）の項を参照してください。
process-name	syslog メッセージを生成したプロセスのプロセスです。
[*pid*]	syslog メッセージを生成したプロセスのプロセス ID（pid）です。
%message -group- severity -message -code	syslogメッセージに関連付けられているメッセージ グループ名、重大度、メッセージ コードです。
message-text	syslog メッセージを説明する文字列です。

syslog メッセージの宛先

コンソール端末への syslog メッセージのロギングは、デフォルトでイネーブルです。 コンソール端末へのロギングをディセーブルにするには、グローバル コンフィギュレーション モードで **logging console disable** コマンドを使用します。 コンソールへのロギングを再度イネーブルにするには、グローバル コンフィギュレーション モードで **logging console** コマンドを使用します。

syslog メッセージは、コンソール以外の宛先に送信できます。たとえば、ロギング バッファ、syslog サーバ、コンソール以外の終端回線（vtys など）です。

この表では、syslog の宛先を指定するために使用するコマンドを一覧で示します。

表 *2*：*syslog* の宛先を設定するために使用するコマンド

コマンド	説明
logging buffered	syslog メッセージの宛先としてロギング バッファを指定します。
logging {*hostname* | *ip-address*}	syslog サーバ ホストを syslog メッセージの宛先として指定します。

コマンド	説明
logging monitor	コンソール以外の端末回線を syslog メッセージの宛先として指定します。

logging buffered コマンドでは、ロギング メッセージをロギング バッファにコピーします。 循環バッファであるため、バッファがいっぱいになると、古いメッセージが新しいメッセージで置き換えられます。 バッファに記録された syslog メッセージを表示するには、**show logging** コマンドを使用します。最初に表示されるメッセージは、バッファ内で最も古いメッセージです。 ロギング バッファの現在の内容をクリアするには、**clear logging** コマンドを使用します。 ロギング バッファへのロギングをディセーブルにするには、グローバル コンフィギュレーション モードで **no logging buffered** コマンドを使用します。

logging コマンドは、ロギング メッセージを受信する syslog サーバ ホストを識別します。 このコマンドを何度も発行すると、ロギング メッセージを受信する syslog サーバのリストが作成されます。 指定された IP アドレスやホスト名を持つ syslog サーバを、利用可能な syslog サーバのリストから削除するには、グローバル コンフィギュレーション モードで **no logging** コマンドを使用します。

logging monitor コマンドは、vtys などのコンソール端末以外の端末回線への syslog メッセージのロギングをグローバルにイネーブルにします。 コンソール以外の端末回線へのロギングをディセーブルにするには、グローバル コンフィギュレーション モードで **no logging monitor** コマンドを使用します。

コンソール以外の宛先に syslog メッセージを送信するためのガイドライン

ロギング プロセスでは、syslog メッセージをコンソール端末以外の宛先に送信します。そのプロセスはデフォルトでイネーブルです。 ロギング バッファ、端末回線、syslog サーバへのロギングはイネーブルです。

現在の端末セッションのロギング

logging monitor コマンドは、コンソール端末以外の端末回線への syslog メッセージのロギングをグローバルにイネーブルにします。 **logging monitor** コマンドをイネーブルにしたら、**terminal monitor** コマンドを使用して、端末セッション中に syslog メッセージを表示します。

端末セッション中、syslog メッセージの端末へのロギングをディセーブルにするには、EXEC モードで **terminal monitor disable** コマンドを使用します。 **terminal monitor disable** コマンドは、現在の端末セッションのロギングのみをディセーブルにします。

現在の端末セッションの syslog メッセージのロギングを再度イネーブルにするには、EXEC モードで **terminal monitor** コマンドを使用します。

（注） **terminal monitor** コマンドおよび **terminal monitor disable** コマンドはローカルで設定され、端末セッションが終了すると有効ではなくなります。

syslog サーバに送信された syslog メッセージ

syslog サーバに送信された syslog メッセージを管理しやすくするために、Cisco IOS XR ソフトウェアには次の機能が搭載されています。

- UNIX システム ファシリティ
- ホスト名プレフィックス ロギング
- ソース インターフェイス ロギング

UNIX システム ロギング ファシリティ

logging facility コマンドを使用して、syslog メッセージが送信される syslog ファシリティを設定できます。 これらの UNIX システム ファシリティの詳細については、ご使用の UNIX オペレーティング システムのオペレータ マニュアルを参照してください。 syslog の形式は、Berkeley Standard Distribution（BSD）UNIX バージョン 4.3 と互換性があります。

この表では、*type* 引数に指定できるファシリティ タイプ キーワードを説明します。

表 *3*：ロギング ファシリティ タイプのキーワード

ファシリティ タイプのキーワード	説明
auth	認可システムを示します。
cron	cron ファシリティを示します。
daemon	システム デーモンを示します。
kern	カーネルを示します。
local0–7	ローカルで定義されたメッセージ用に予約されています。
lpr	回線プリンタ システムを示します。
mail	メール システムを示します。
news	USENET ニュースを示します。
sys9	システムの使用を示します。

ファシリティ タイプのキーワード	説明
sys10	システムの使用を示します。
sys11	システムの使用を示します。
sys12	システムの使用を示します。
sys13	システムの使用を示します。
sys14	システムの使用を示します。
syslog	システム ログを示します。
user	ユーザ プロセスを示します。
uucp	UNIX から UNIX へのコピー システムを示します。

ホスト名プレフィックス ロギング

syslog サーバに送信されたシステム ロギング メッセージを管理しやすくするために、Cisco IOS XR ソフトウェアではホスト名プレフィックス ロギングをサポートしています。 イネーブルにすると、ホスト名プレフィックス ロギングでは、ルータから syslog サーバに送信される syslog メッセージにホスト名プレフィックスを追加します。 ホスト名プレフィックスを使用して、さまざまなネットワーキング デバイスから特定の syslog サーバに送信されるメッセージを分類することができます。

syslog サーバに送信される syslog メッセージにホスト名プレフィックスを付加するには、グローバル コンフィギュレーション モードで、**logging hostname** コマンドを使用します。

syslog 送信元アドレス ロギング

デフォルトでは、syslog メッセージが syslog サーバに送信されるとき、syslog メッセージにはルータから出るために使用するインターフェイスの IP アドレスが含まれています。 syslog メッセージがどのインターフェイスを使用してルータを出るかにかかわらず、すべての syslog メッセージに同じ IP アドレスを含めるように設定するには、グローバル コンフィギュレーション モードで **logging source-interface** コマンドを使用します。

UNIX syslog デーモンの設定

4.3 BSD UNIX システム上で syslog デーモンを設定するには、/etc/syslog.conf ファイルに次のような行を含めます。

```
local7.debug /usr/adm/logs/cisco.log
```

debugging キーワードでは syslog レベルを指定します。他のキーワードの一般的な説明については、表 7：syslog メッセージの重大度, （10 ページ）を参照してください。 **local7** キーワードでは、使用するロギング ファシリティを指定します。他のキーワードの一般的な説明については、表 3：ロギング ファシリティ タイプのキーワード, （5 ページ）を参照してください。

syslog デーモンは、次のフィールドで指定されたファイルに、このレベルまたはより重大なレベルのメッセージを送信します。 このファイルは、syslog デーモンに書き込み権限がある既存ファイルである必要があります。

ローカル ストレージ デバイスでのロギング メッセージのアーカイブ

syslog メッセージは、ハード ディスクやフラッシュ ディスクなどのローカル ストレージ デバイスのアーカイブに保存することもできます。 メッセージは重大度に基づいて保存できます。アーカイブのサイズ、メッセージが追加される頻度（日次または週次）、アーカイブに保存するメッセージの週合計などの属性を指定できます。

アーカイブ属性の設定

ロギング アーカイブを作成して、ロギング メッセージを収集および保存する方法を指定するには、グローバル コンフィギュレーション モードで **logging archive** コマンドを使用します。 **logging archive** コマンドでは、ロギング アーカイブ サブモードを開始します。このモードでは、syslog をアーカイブするための属性を設定できます。

この表では、ロギング アーカイブ サブモードでアーカイブ属性を指定するために使用されるコマンドを一覧で示します。

表 *4*：*syslog* アーカイブ属性を設定するために使用するコマンド

コマンド	説明
archive-length *weeks*	アーカイブでアーカイブ ログが保持される最長週数を指定します。 保存期間がこの週数を超えるログは、自動的にアーカイブから削除されます。

コマンド	説明
archive-size *size*	ストレージデバイス上にある syslog アーカイブの最大合計サイズを指定します。 このサイズを超過すると、新しいログ用の領域を確保するため、アーカイブ内の最も古いファイルが削除されます。
device {**disk0** | **disk1** | **harddisk**}	syslog がアーカイブされるローカル ストレージ デバイスを指定します。 デフォルトでは、ログは <device>/var/log のディレクトリに作成されます。 デバイスが設定されていない場合は、他のすべてのロギング アーカイブ設定が拒否されます。 フラッシュ ディスクよりもハードディスクの容量の方が大きいため、syslog はハードディスクにアーカイブすることを推奨します。
file-size *size*	アーカイブにある 1 つのログ ファイルの最大ファイル サイズ（メガバイト単位）を指定します。 この制限サイズに達すると、自動的に新しいファイルが作成され、1 つずつ順に大きいシリアル番号が付与されます。
frequency {daily | weekly}	ログが収集される頻度を日次または週次で指定します。
severity *severity*	アーカイブするログ メッセージの最小重大度を指定します。 設定されたこのレベル以上の syslog メッセージがすべてアーカイブされ、これらのレベルより小さいメッセージは除外されます。 詳細については、重大度, （9 ページ）を参照してください。

ストレージ ディレクトリのアーカイブ

デフォルトでは、syslog アーカイブは <device>/var/log のディレクトリに格納されます。 個別のアーカイブ ファイルはアーカイブが作成された年月日に基づいてサブディレクトリに保存されます。 たとえば、2006/02/26 に作成されたアーカイブ ファイルは、次のディレクトリに保存されます。

```
harddisk:/var/log/2006/02/26
```

重大度

宛先に送信される syslog メッセージの重大度を指定して、ロギングの宛先に送信されるメッセージの数を制限できます（重大度の定義は表 7：syslog メッセージの重大度，（10 ページ）を参照）。

この表では、syslog メッセージの重大度を制御するコマンドを一覧で示します。

表 *5*：*syslog* メッセージの重大度を制御するために使用するコマンド

コマンド	説明
logging buffered [*severity*]	ロギング バッファに送信する syslog メッセージを重大度に基づいて制限します。
logging console [*severity*]	コンソール端末に送信する syslog メッセージを重大度に基づいて制限します。
logging monitor [*severity*]	端末回線に送信する syslog メッセージを重大度に基づいて制限します。
logging trap [*severity*]	syslog サーバに送信する syslog メッセージを重大度に基づいて制限します。
severity *severity*	syslog アーカイブに送信する syslog メッセージを重大度に基づいて制限します。

logging buffered、**logging console**、**logging monitor**、**logging traps** コマンドでは、指定した重大度番号以下の syslog メッセージがそれぞれの宛先に送信されないように制限します。この番号は *severity* 引数で指定します。

（注） 重大度の番号が小さい syslog メッセージは、より重要なイベントであることを示します。 重大度の定義については、表 7：syslog メッセージの重大度，（10 ページ）を参照してください。

ロギング ヒストリ表

snmp-server enable traps syslog コマンドで、簡易ネットワーク管理プロトコル（SNMP）ネットワーク管理ステーション（NMS）に送信するように syslog メッセージ トラップをイネーブルにしている場合、ルータの履歴テーブルに送信および保存されるメッセージのレベルを変更できます。また履歴テーブルに保存されるメッセージ数も変更できます。

SNMP トラップは宛先への到達が保証されていないため、メッセージは履歴テーブルに格納されます。デフォルトでは、syslog トラップがイネーブルでない場合でも、レベル警告および上記（表 7：syslog メッセージの重大度, （10 ページ） を参照）の 1 つのメッセージが履歴テーブルに保存されます。

この表では、ロギング ヒストリ表の重大度と表のサイズのデフォルトを変更するために使用されるコマンドを一覧で示します。

表 *6*：ロギング ヒストリ表のコマンド

コマンド	説明
logging history *severity*	履歴ファイルに保存されて SNMP サーバに送信される syslog メッセージのデフォルトの重大度を変更します。
logging history size *number*	履歴テーブルに保存できる syslog メッセージの数を変更します。

（注） 表 7：syslog メッセージの重大度, （10 ページ） に、level キーワードおよび重大度を示します。 SNMP を使用する場合、重大度の値は +1 を使用します。 たとえば、**emergency** は 0 ではなく 1 になり、**critical** は 2 ではなく 3 になります。

Syslog メッセージの重大度の定義

この表では、 *severity* 引数に指定できる重大度キーワードおよび対応する UNIX syslog 定義を、最も重大度の高いレベルから低いレベルに順番に一覧で示します。

表 *7*：*syslog* メッセージの重大度

重大度のキーワード	レベル	説明	syslog 定義
emergencies	0	システムが使用不可	LOG_EMERG
alerts	1	即時処理が必要	LOG_ALERT
critical	2	クリティカルな状態	LOG_CRIT
errors	3	エラー状態	LOG_ERR
warnings	4	警告状態	LOG_WARNING

重大度のキーワード	レベル	説明	syslog 定義
notifications	5	正常だが注意を要する状態	LOG_NOTICE
informational	6	情報メッセージだけ	LOG_INFO
debugging	7	デバッグ メッセージ	LOG_DEBUG

syslog 重大度コマンドのデフォルト

この表では、*severity* 引数をサポートするコマンドのデフォルトの重大度設定を一覧で示します。

表 *8*：重大度コマンドのデフォルト

コマンド	デフォルトの重大度キーワード	レベル
logging buffered	debugging	7
logging console	informational	6
logging history	warnings	4
logging monitor	debugging	7
logging trap	informational	6

ロギング サービスの実装方法

ここでは、次の手順について説明します。

システム ロギング メッセージ宛先の設定

このタスクでは、コンソール端末以外の宛先へのロギングを設定する方法を説明します。

概念の情報については、syslog メッセージの宛先, （3 ページ）の項を参照してください。

手順の概要

1. **configure**
2. **logging buffered** [*size* | *severity*]
3. **logging monitor** [*severity*]
4. 次のいずれかのコマンドを使用してください。
   - **end**
   - **commit**
5. **terminal monitor**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**configure** 例： `RP/0/RSP0/CPU0:router# configure`	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	**logging buffered** [*size*	*severity*] 例： `RP/0/RSP0/CPU0:router(config)# logging buffered severity warnings`	ロギング バッファを syslog メッセージの宛先として指定し、ロギング バッファのサイズを設定し、ロギング バッファに送信される syslog メッセージを重大度に基づいて制限します。 • *size* 引数のデフォルト値は 4096 バイトです。 • *severity* 引数のデフォルト値は **debugging** です。 • *severity* 引数のキーワード オプションは、**emergencies**、**alerts**、**critical**、**errors**、**warnings**、**notifications**、**informational**、**debugging** です。 • デフォルトでは、*severity* 引数の重大度や *size* 引数のバッファ サイズを指定せずにこのコマンドを入力すると、重大度が **debugging** に、バッファ サイズが 4096 バイトに設定されます。
ステップ 3	**logging monitor** [*severity*] 例： `RP/0/RSP0/CPU0:router(config)# logging monitor critical`	コンソール端末以外の端末回線を syslog メッセージの宛先として指定し、端末回線に送信されるメッセージの数を重大度に基づいて制限します。 • *severity* 引数のキーワード オプションは、**emergencies**、**alerts**、**critical**、**errors**、**warnings**、**notifications**、**informational**、**debugging** です。 • デフォルトでは、*severity* 引数の重大度を指定せずにこのコマンドを入力すると、重大度は**debugging** に設定されます。

	コマンドまたはアクション	目的

ステップ 4	次のいずれかのコマンドを使用してください。
	• **end**
	• **commit**
	
	例：
	`RP/0/RSP0/CPU0:router(config)# end`
	または
	`RP/0/RSP0/CPU0:router(config)# commit`
		設定変更を保存します。
		• **end** コマンドを実行すると、変更をコミットするように要求されます。
		`Uncommitted changes found, commit them before exiting(yes/no/cancel)? [cancel]:`
		◦ yes と入力すると、実行コンフィギュレーション ファイルに変更が保存され、コンフィギュレーション セッションが終了して、ルータが EXEC モードに戻ります。
		◦ no と入力すると、コンフィギュレーションセッションが終了して、ルータが EXEC モードに戻ります。変更はコミットされません。
		◦ cancel と入力すると、現在のコンフィギュレーション セッションが継続します。コンフィギュレーションセッションは終了せず、設定変更もコミットされません。
		• 実行コンフィギュレーション ファイルに設定変更を保存し、コンフィギュレーションセッションを継続するには、**commit** コマンドを使用します。

ステップ 5	**terminal monitor** 例： `RP/0/RSP0/CPU0:router# terminal monitor`	現在の端末セッションにおける syslog メッセージの表示をイネーブルにします。 （注） 現在の端末の syslog メッセージのロギングは、**terminal monitor disable** コマンドでディセーブルにできます。 • 現在のセッションのメッセージのロギングが **terminal monitor disable** コマンドでディセーブルにされている場合、現在のセッションの syslog メッセージの表示を再度イネーブルにするには、このコマンドを使用します。 （注） このコマンドは EXEC モード コマンドであるため、ローカルで設定され、現在のセッションが終了するとイネーブルではなくなります。

リモート サーバへのロギングの設定

このタスクでは、リモート syslog サーバへのロギングを設定する方法を説明します。

はじめる前に

syslog サーバ ホストを syslog メッセージの受信先に設定するには、syslog サーバに接続できる必要があります。

手順の概要

1. configure
2. **logging** {*ip-address* | *hostname*}
3. **logging trap** [*severity*]
4. **logging facility** [*type*]
5. **logging hostnameprefix** *hostname*
6. **logging source-interface** *type interface-path-id*
7. 次のいずれかのコマンドを使用してください。
   - **end**
   - **commit**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	configure 例： `RP/0/RSP0/CPU0:router#`	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	**logging** {*ip-address* | *hostname*} 例： `RP/0/RSP0/CPU0:router(config)# logging 10.3.32.154`	syslog サーバ ホストを syslog メッセージの宛先として指定します。 • このコマンドを何度も発行すると、ロギング メッセージを受信する syslog サーバのリストが作成されます。
ステップ 3	**logging trap** [*severity*] 例： `RP/0/RSP0/CPU0:router(config)#`	syslog サーバに送信する syslog メッセージを重大度に基づいて制限します。 • デフォルトでは、*severity* 引数の重大度を指定せずにこのコマンドを入力すると、重大度は **informational** に設定されます。
ステップ 4	**logging facility** [*type*] 例： `RP/0/RSP0/CPU0:router(config)# logging facility kern`	（任意）syslog ファシリティを設定します。 • デフォルトでは、*type* 引数にファシリティ タイプを指定せずにこのコマンドを入力すると、ファシリティは **local-7** に設定されます。

	コマンドまたはアクション	目的
ステップ 5	**logging hostnameprefix** *hostname* 例： `RP/0/RSP0/CPU0:router(config)#`	（任意）ルータから syslog サーバに送信される syslog メッセージにホスト名プレフィックスを追加します。 ヒント　ホスト名プレフィックス ロギングは、syslog サーバで受信される syslog メッセージを並べ替えるときに便利です。
ステップ 6	**logging source-interface** *type interface-path-id* 例： `RP/0/RSP0/CPU0:router(config)#`	（任意）syslog 送信元アドレスを設定します。 • デフォルトでは、syslog サーバに送信された syslog メッセージには、ルータから出るために使用するインターフェイスの IP アドレスが含まれています。 • syslog メッセージがどのインターフェイスを使用してルータを出るかにかかわらず、ルータから送信されるすべての syslog メッセージに同じ IP アドレスが含まれるように設定するには、このコマンドを使用します。

ステップ 7	次のいずれかのコマンドを使用してください。
	
	• **end**
	
	• **commit**
	
	例：
	
	`RP/0/RSP0/CPU0:router(config)# end`
	または
	
	`RP/0/RSP0/CPU0:router(config)# commit`
		設定変更を保存します。
		
		• **end** コマンドを実行すると、変更をコミットするように要求されます。
		
		`Uncommitted changes found, commit them before exiting(yes/no/cancel)? [cancel]:`
		
		◦ yes と入力すると、実行コンフィギュレーション ファイルに変更が保存され、コンフィギュレーション セッションが終了して、ルータが EXEC モードに戻ります。
		
		◦ no と入力すると、コンフィギュレーション セッションが終了して、ルータが EXEC モードに戻ります。変更はコミットされません。
		
		◦ cancel と入力すると、現在のコンフィギュレーション セッションが継続します。コンフィギュレーション セッションは終了せず、設定変更もコミットされません。
		
		• 実行コンフィギュレーション ファイルに設定変更を保存し、コンフィギュレーション セッションを継続するには、**commit** コマンドを使用します。

ロギング ヒストリ表の設定

このタスクでは、ロギング ヒストリ表を設定する方法を説明します。

概念の情報については、重大度, （9 ページ）の項を参照してください。

はじめる前に

SNMP NMS へのメッセージのロギングは、**snmp-server enable traps syslog** コマンドでイネーブルにします。 SNMP の詳細については、関連資料, （32 ページ）の項を参照してください。

手順の概要

1. **configure**
2. **logging history** *severity*
3. **logging history size** *number*
4. 次のいずれかのコマンドを使用してください。
   - **end**
   - **commit**
5. **show logging history**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**configure** 例： `RP/0/RSP0/CPU0:router# configure`	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	**logging history** *severity* 例： `RP/0/RSP0/CPU0:router(config)# logging history errors`	履歴ファイルに保存されて SNMP サーバに送信される syslog メッセージのデフォルトの重大度を変更します。 • デフォルトでは、重大度が **warnings** 以下の syslog メッセージが履歴ファイルに格納され、SNMP サーバに送信されます。
ステップ 3	**logging history size** *number* 例： `RP/0/RSP0/CPU0:router(config)# logging history size 200`	履歴テーブルに保存できる syslog メッセージの数を変更します。 • デフォルトでは、1 つの syslog メッセージが履歴テーブルに格納されます。 （注） 履歴テーブルが一杯になると（メッセージの数がこのコマンドで指定した最大数に達すると）、新しいメッセージを保存できるよう、最も古いメッセージがテーブルから削除されます。

	コマンドまたはアクション	目的

ステップ 4	次のいずれかのコマンドを使用してください。
	• **end**
	• **commit**
	
	例：
	`RP/0/RSP0/CPU0:router(config)# end`
	または
	`RP/0/RSP0/CPU0:router(config)# commit`
		設定変更を保存します。
		• **end** コマンドを実行すると、変更をコミットするように要求されます。
		`Uncommitted changes found, commit them before exiting(yes/no/cancel)? [cancel]:`
		◦ yes と入力すると、実行コンフィギュレーション ファイルに変更が保存され、コンフィギュレーションセッションが終了して、ルータが EXEC モードに戻ります。
		◦ no と入力すると、コンフィギュレーションセッションが終了して、ルータが EXEC モードに戻ります。変更はコミットされません。
		◦ cancel と入力すると、現在のコンフィギュレーション セッションが継続します。コンフィギュレーションセッションは終了せず、設定変更もコミットされません。
		• 実行コンフィギュレーション ファイルに設定変更を保存し、コンフィギュレーションセッションを継続するには、**commit** コマンドを使用します。

ステップ 5	**show logging history** 例： `RP/0/RSP0/CPU0:router# show logging history`	（任意）syslog 履歴テーブルの状態についての情報を表示します。

コンソール端末およびロギング バッファへのロギングの修正

このタスクでは、コンソール端末およびロギング バッファのロギングの設定を変更する方法を説明します。

（注） デフォルトでは、ロギングはイネーブルです。

手順の概要

1. **configure**
2. **logging buffered** [*size* | *severity*]
3. **logging console** [*severity*]
4. 次のいずれかのコマンドを使用してください。
   - **end**
   - **commit**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**configure** 例： `RP/0/RSP0/CPU0:router# configure`	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	**logging buffered** [*size*	*severity*] 例： `RP/0/RSP0/CPU0:router(config)# logging buffered size 60000`	ロギング バッファを syslog メッセージの宛先として指定し、ロギング バッファのサイズを設定し、ロギング バッファに送信される syslog メッセージを重大度に基づいて制限します。 • *size* 引数のデフォルトは 4096 バイトです。 • *severity* 引数のデフォルトは **debugging** です。 • *severity* 引数のキーワード オプションは、**emergencies**、**alerts**、**critical**、**errors**、**warnings**、**notifications**、**informational**、**debugging** です。 • デフォルトでは、*severity* 引数の重大度や *size* 引数のバッファ サイズを指定せずにこのコマンドを入力すると、重大度が **debugging** に、バッファ サイズが 4096 バイトに設定されます。
ステップ 3	**logging console** [*severity*] 例： `RP/0/RSP0/CPU0:router(config)# logging console alerts`	コンソール端末に送信するメッセージを重大度に基づいて制限します。 • デフォルトでは、syslog メッセージは **informational** の重大度でコンソール端末のログに記録されます。 • *severity* 引数のキーワード オプションは、**emergencies**、**alerts**、**critical**、**errors**、**warnings**、**notifications**、**informational**、**debugging** です。 • *severity* 引数の重大度を指定せずにこのコマンドを入力すると、重大度は **informational** に設定されます。

	コマンドまたはアクション	目的
		（注） **logging console disable** コマンドでコンソール端末へのロギングがディセーブルにされている場合に、ロギングを再度イネーブルにするには、このコマンドを使用します。

ステップ 4	次のいずれかのコマンドを使用してください。
	• **end**
	• **commit**
	例：
	`RP/0/RSP0/CPU0:router(config)# end`
	または
	`RP/0/RSP0/CPU0:router(config)# commit`
		設定変更を保存します。
		• **end** コマンドを実行すると、変更をコミットするように要求されます。
		`Uncommitted changes found, commit them before exiting(yes/no/cancel)? [cancel]:`
		◦ yes と入力すると、実行コンフィギュレーション ファイルに変更が保存され、コンフィギュレーション セッションが終了して、ルータが EXEC モードに戻ります。
		◦ no と入力すると、コンフィギュレーションセッションが終了して、ルータが EXEC モードに戻ります。変更はコミットされません。
		◦ cancel と入力すると、現在のコンフィギュレーション セッションが継続します。コンフィギュレーションセッションは終了せず、設定変更もコミットされません。
		• 実行コンフィギュレーションファイルに設定変更を保存し、コンフィギュレーションセッションを継続するには、**commit** コマンドを使用します。

タイムス タンプの形式の修正

このタスクでは、syslog メッセージおよびデバッグ メッセージのタイム スタンプ形式を変更する方法を説明します。

手順の概要

1. **configure**
2. 次のいずれかを実行します。
   - **service timestamps log datetime** [**localtime**] [**msec**] [**show-timezone**]
   - **service timestamps log uptime**
3. 次のいずれかを実行します。
   - **service timestamps debug datetime** [**localtime**] [**msec**] [**show-timezone**]
   - **service timestamps debug uptime**
4. 次のいずれかのコマンドを使用してください。
   - **end**
   - **commit**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**configure** 例： `RP/0/RSP0/CPU0:router# configure`	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	次のいずれかを実行します。
	• **service timestamps log datetime** [**localtime**] [**msec**] [**show-timezone**]
	• **service timestamps log uptime**
	
	例：
	`RP/0/RSP0/CPU0:router(config)# service timestamps log datetime localtime msec`
	または
	`RP/0/RSP0/CPU0:router(config)# service timestamps log uptime`
		syslog メッセージのタイム スタンプ形式を変更します。
		• デフォルトでは、タイム スタンプはイネーブルです。 デフォルトのタイム スタンプ形式は month day HH:MM:SS です。
		• **service timestamps log datetime** コマンドを発行すると、日時のタイム スタンプが付くように syslog メッセージが設定されます。
		◦ 任意で **localtime** キーワードを指定すると、タイム スタンプにローカル タイムゾーンが含まれます。
		◦ 任意で **msec** キーワードを指定すると、タイム スタンプにミリ秒が含まれます。
		◦ 任意で **show-timezone** キーワードを指定すると、タイム スタンプにタイムゾーン情報が含まれます。
		• **service timestamps log uptime** コマンドを発行すると、ルータが最後にリブートされたときから経過した時間のタイム スタンプが付くように syslog メッセージが設定されます。

	コマンドまたはアクション	目的
		◦**service timestamps log uptime** コマンドでは、タイム スタンプを HHHH:MM:SS に設定します。これはルータが最後にリブートされたときからの時間を示します。

ステップ 3	次のいずれかを実行します。
	• **service timestamps debug datetime** [**localtime**] [**msec**] [**show-timezone**]
	• **service timestamps debug uptime**
	例：
	`RP/0/RSP0/CPU0:router(config)# service timestamps debug datetime msec show-timezone`
	または
	`RP/0/RSP0/CPU0:router(config)# service timestamps debug uptime`
		デバッグ メッセージのタイム スタンプ形式を変更します。
		• デフォルトでは、タイム スタンプはイネーブルです。 デフォルトのタイム スタンプ形式は month day HH:MM:SS です。
		• **service timestamps log datetime** コマンドを発行すると、日時のタイム スタンプが付くようにデバッグ メッセージが設定されます。
		◦任意で **localtime** キーワードを指定すると、タイム スタンプにローカル タイムゾーンが含まれます。
		◦任意で **msec** キーワードを指定すると、タイム スタンプにミリ秒が含まれます。
		◦任意で **show-timezone** キーワードを指定すると、タイム スタンプにタイムゾーン情報が含まれます。
		• **service timestamps log uptime** コマンドを発行すると、ネットワーク デバイスが最後にリブートされたときから経過した時間のタイム スタンプが付くようにデバッグ メッセージが設定されます。
		ヒント キーワードや引数を指定せずに **service timestamps** コマンドを入力すると、**service timestamps debug uptime** コマンドと同じように機能します。

ステップ 4	次のいずれかのコマンドを使用してください。
	• **end**
	• **commit**
	例：
	`RP/0/RSP0/CPU0:router(config)# end`
	または
	`RP/0/RSP0/CPU0:router(config)# commit`
		設定変更を保存します。
		• **end** コマンドを実行すると、変更をコミットするように要求されます。
		`Uncommitted changes found, commit them before exiting(yes/no/cancel)? [cancel]:`
		◦yes と入力すると、実行コンフィギュレーション ファイルに変更が保存され、コンフィギュレーション セッションが終了して、ルータが EXEC モードに戻ります。
		◦no と入力すると、コンフィギュレーション セッションが終了して、ルータが EXEC モードに戻ります。変更はコミットされません。

	コマンドまたはアクション	目的
		◦ cancel と入力すると、現在のコンフィギュレーション セッションが継続します。コンフィギュレーション セッションは終了せず、設定変更もコミットされません。 • 実行コンフィギュレーション ファイルに設定変更を保存し、コンフィギュレーション セッションを継続するには、**commit** コマンドを使用します。

タイム スタンプのディセーブル化

このタスクでは、syslog メッセージにタイム スタンプが含まれないようにする方法を説明します。

手順の概要

1. **configure**
2. 次のいずれかを実行します。
   - **service timestamps disable**
   - **no service timestamps** [**debug** | **log**] [**datetime** [**localtime**] [**msec**] [**show-timezone**]] | **uptime**]
3. 次のいずれかのコマンドを使用してください。
   - **end**
   - **commit**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**configure** 例： `RP/0/RSP0/CPU0:router# configure`	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	次のいずれかを実行します。	syslog メッセージにタイム スタンプが含まれないようにします。

	コマンドまたはアクション	目的
	• **service timestamps disable** • **no service timestamps** [**debug** | **log**] [**datetime** [**localtime**] [**msec**] [**show-timezone**]] | **uptime**]	（注） どちらのコマンドでも syslog メッセージのタイム スタンプをディセーブルにできますが、**service timestamps disable** コマンドを指定すると、設定にコマンドが保存されます。**service timestamps** コマンドの **no** 形式を指定すると、設定からコマンドが削除されます。

ステップ 3	次のいずれかのコマンドを使用してください。
	• **end**
	• **commit**
	例：
	`RP/0/RSP0/CPU0:router(config)# end`
	または
	`RP/0/RSP0/CPU0:router(config)# commit`
		設定変更を保存します。
		• **end** コマンドを実行すると、変更をコミットするように要求されます。
		`Uncommitted changes found, commit them before exiting(yes/no/cancel)? [cancel]:`
		◦ yes と入力すると、実行コンフィギュレーション ファイルに変更が保存され、コンフィギュレーションセッションが終了して、ルータが EXEC モードに戻ります。
		◦ no と入力すると、コンフィギュレーションセッションが終了して、ルータが EXEC モードに戻ります。変更はコミットされません。
		◦ cancel と入力すると、現在のコンフィギュレーション セッションが継続します。コンフィギュレーションセッションは終了せず、設定変更もコミットされません。
		• 実行コンフィギュレーション ファイルに設定変更を保存し、コンフィギュレーションセッションを継続するには、**commit** コマンドを使用します。

重複 syslog メッセージの抑制

このタスクでは、重複する syslog メッセージが連続してロギングされないようにする方法を説明します。

手順の概要

1. **configure**
2. **logging suppress duplicates**
3. 次のいずれかのコマンドを使用してください。
   - **end**
   - **commit**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**configure** 例： `RP/0/RSP0/CPU0:router# configure`	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	**logging suppress duplicates** 例： `RP/0/RSP0/CPU0:router(config)# logging suppress duplicates`	重複する syslog メッセージが連続してロギングされないようにします。 **注意** デバッグ セッション中にこのコマンドがイネーブルの場合、切り離して解決しようとしている問題に関する重要な情報を見落とす可能性があります。こうした場合は、このコマンドをディセーブルにすることを検討してください。

ステップ 3	次のいずれかのコマンドを使用してください。
	• **end**
	• **commit**
	
	例：
	`RP/0/RSP0/CPU0:router(config)# end`
	または
	`RP/0/RSP0/CPU0:router(config)# commit`
		設定変更を保存します。
		• **end** コマンドを実行すると、変更をコミットするように要求されます。
		`Uncommitted changes found, commit them before exiting(yes/no/cancel)? [cancel]:`
		◦ yes と入力すると、実行コンフィギュレーション ファイルに変更が保存され、コンフィギュレーション セッションが終了して、ルータが EXEC モードに戻ります。
		◦ no と入力すると、コンフィギュレーション セッションが終了して、ルータが EXEC モードに戻ります。変更はコミットされません。
		◦ cancel と入力すると、現在のコンフィギュレーション セッションが継続します。コンフィギュレーション セッションは終了せず、設定変更もコミットされません。

	コマンドまたはアクション	目的
		• 実行コンフィギュレーション ファイルに設定変更を保存し、コンフィギュレーション セッションを継続するには、**commit** コマンドを使用します。

リンクステータス syslog メッセージのロギングのディセーブル化

このタスクでは、論理リンクおよび物理リンクのりんくすてーたす syslog メッセージのロギングをディセーブルにする方法を説明します。

リンクステータス メッセージのロギングをイネーブルにした場合、ルータで大量のリンクステータス（アップダウン）のシステム ロギング メッセージが生成される場合があります。 リンクステータス syslog メッセージのロギングをディセーブルにすると、ログに記録されるメッセージの数を減らすことができます。

手順の概要

1. **configure**
2. **logging events link-status disable**
3. 次のいずれかのコマンドを使用してください。
   - **end**
   - **commit**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**configure** 例： `RP/0/RSP0/CPU0:router# configure`	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	**logging events link-status disable** 例： `RP/0/RSP0/CPU0:router(config)# logging events link-status disable`	ソフトウェア（論理）リンクおよび物理リンクのリンクステータス syslog メッセージのロギングをディセーブルにします。 • 物理リンクでは、リンクステータス syslog メッセージのロギングはデフォルトでイネーブルです。

	コマンドまたはアクション	目的
		• 論理リンクと物理リンクの両方で、リンクステータス syslog メッセージをイネーブルにするには、**logging events link-status software-interfaces** コマンドを使用します。 • リンクステータス syslog メッセージを物理リンクでのみイネーブルするには、**no logging events link-status** コマンドを使用します。

ステップ 3	次のいずれかのコマンドを使用してください。
	• **end**
	• **commit**
	
	例：
	`RP/0/RSP0/CPU0:router(config)# end`
	または
	`RP/0/RSP0/CPU0:router(config)# commit`
		設定変更を保存します。
		• **end** コマンドを実行すると、変更をコミットするように要求されます。
		`Uncommitted changes found, commit them before exiting(yes/no/cancel)? [cancel]:`
		◦ yes と入力すると、実行コンフィギュレーション ファイルに変更が保存され、コンフィギュレーション セッションが終了して、ルータが EXEC モードに戻ります。
		◦ no と入力すると、コンフィギュレーション セッションが終了して、ルータが EXEC モードに戻ります。変更はコミットされません。
		◦ cancel と入力すると、現在のコンフィギュレーションセッションが継続します。コンフィギュレーションセッションは終了せず、設定変更もコミットされません。
		• 実行コンフィギュレーション ファイルに設定変更を保存し、コンフィギュレーション セッションを継続するには、**commit** コマンドを使用します。

システム ロギング メッセージの表示

このタスクでは、ロギング バッファに保存されている syslog メッセージを表示する方法を説明します。

（注） コマンドは、任意の順番で入力できます。

手順の概要

1. **show logging**
2. **show logging location** *node-id*
3. **show logging process** *name*
4. **show logging string** *string*
5. **show logging start** *month day hh*:*mm*:*ss*
6. **show logging end** *month day hh*:*mm*:*ss*

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**show logging** 例： `RP/0/RSP0/CPU0:router# show logging`	ロギング バッファに保存されているすべての syslog メッセージを表示します。
ステップ 2	**show logging location** *node-id* 例： `RP/0/RSP0/CPU0:router# show logging location 0/1/CPU0`	指定されたノードからの syslog メッセージを表示します。
ステップ 3	**show logging process** *name* 例： `RP/0/RSP0/CPU0:router# show logging process init`	指定したプロセスに関連する syslog メッセージを表示します。
ステップ 4	**show logging string** *string* 例： `RP/0/RSP0/CPU0:router# show logging string install`	指定したストリングを含む syslog メッセージを表示します。
ステップ 5	**show logging start** *month day hh*:*mm*:*ss* 例： `RP/0/RSP0/CPU0:router# show logging start december 1 10:30:00`	指定した日時以降に生成されたロギング バッファ内の syslog メッセージを表示します。
ステップ 6	**show logging end** *month day hh*:*mm*:*ss* 例： `RP/0/RSP0/CPU0:router# show logging end december 2 22:16:00`	指定した日時以前に生成されたロギング バッファ内の syslog メッセージを表示します。

ローカルストレージデバイスへのシステムロギングメッセージのアーカイブ

このタスクでは、ローカル ストレージデバイス上のアーカイブに syslog メッセージを保存する方法を説明します。

はじめる前に

（注） ローカル ストレージ デバイスには、アーカイブ ファイルを格納するために利用できる十分な領域が必要です。フラッシュ ディスクよりもハードディスクの容量の方が大きいため、syslog はハードディスクにアーカイブすることを推奨します。

手順の概要

1. configure
2. **logging archive**
3. **device** {**disk0** | **disk1** | **harddisk**}
4. **frequency** {**daily** | **weekly**}
5. **severity** *severity*
6. **archive-length** *weeks*
7. **archive-size** *size*
8. **file-size** *size*
9. 次のいずれかのコマンドを使用してください。
   - **end**
   - **commit**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	configure 例： `RP/0/RSP0/CPU0:router# configure`	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	**logging archive** 例： `RP/0/RSP0/CPU0:router(config)# logging archive`	ロギング アーカイブ コンフィギュレーション モードを開始します。

	コマンドまたはアクション	目的
ステップ 3	**device** {**disk0** | **disk1** | **harddisk**} 例： `RP/0/RSP0/CPU0:router(config-logging-arch)# device disk1`	syslog のロギングに使用するデバイスを指定します。 • この手順は必須です。デバイスが設定されていない場合は、他のすべてのロギング アーカイブ設定が拒否されます。 • フラッシュ ディスクよりもハードディスクの容量の方が大きいため、syslog はハードディスクにアーカイブすることを推奨します。 • デフォルトでは、ログは <device>/var/log のディレクトリに作成されます
ステップ 4	**frequency** {**daily** | **weekly**} 例： `RP/0/RSP0/CPU0:router(config-logging-arch)# frequency weekly`	（任意）ログを収集する頻度を日次または週次で指定します。デフォルトでは、ログは毎日収集されます。
ステップ 5	**severity** *severity* 例： `RP/0/RSP0/CPU0:router(config-logging-arch)# severity warnings`	（任意）アーカイブするログ メッセージの最小重大度を指定します。 設定されたこのレベル以上の syslog メッセージがすべてアーカイブされ、これらのレベルより小さいメッセージは除外されます。 重大度は次のとおりです。 • emergencies • alerts • critical • errors • warnings • notifications • informational • debugging 詳細については、Syslog メッセージの重大度の定義, （10 ページ）の項を参照してください。
ステップ 6	**archive-length** *weeks* 例： `RP/0/RSP0/CPU0:router(config-logging-arch)# archive-length 6`	（任意）アーカイブでアーカイブ ログが保持される最長週数を指定します。 保存期間がこの週数を超えるログは、自動的にアーカイブから削除されます。 デフォルトでは、アーカイブ ログは 4 週間保存されます。

	コマンドまたはアクション	目的
ステップ 7	**archive-size** *size* 例： `RP/0/RSP0/CPU0:router(config-logging-arch)# archive-size 50`	（任意）ストレージデバイス上にある syslog アーカイブの最大合計サイズを指定します。このサイズを超過すると、新しいログ用の領域を確保するため、アーカイブ内の最も古いファイルが削除されます。 デフォルトのアーカイブ サイズは 20 MB です。
ステップ 8	**file-size** *size* 例： `RP/0/RSP0/CPU0:router(config-logging-arch)# file-size 10`	（任意）アーカイブにある 1 つのログ ファイルの最大ファイル サイズ（メガバイト単位）を指定します。この制限サイズに達すると、自動的に新しいファイルが作成され、1 つずつ順に大きいシリアル番号が付与されます。 デフォルトでは、最大ファイルサイズは 1 メガバイトです。

ステップ 9	次のいずれかのコマンドを使用してください。
	• **end**
	• **commit**
	
	例：
	`RP/0/RSP0/CPU0:router(config)# end`
	または
	`RP/0/RSP0/CPU0:router(config)# commit`
		設定変更を保存します。
		• **end** コマンドを実行すると、変更をコミットするように要求されます。
		`Uncommitted changes found, commit them before exiting(yes/no/cancel)? [cancel]:`
		◦ yes と入力すると、実行コンフィギュレーション ファイルに変更が保存され、コンフィギュレーション セッションが終了して、ルータが EXEC モードに戻ります。
		◦ no と入力すると、コンフィギュレーション セッションが終了して、ルータが EXEC モードに戻ります。変更はコミットされません。
		◦ cancel と入力すると、現在のコンフィギュレーション セッションが継続します。コンフィギュレーション セッションは終了せず、設定変更もコミットされません。
		• 実行コンフィギュレーション ファイルに設定変更を保存し、コンフィギュレーションセッションを継続するには、**commit** コマンドを使用します。

ロギング サービスを実装するための設定例

ここでは、次の設定例について説明します。

コンソール端末およびロギング バッファへのロギングの設定：例

次の例では、ロギング バッファへのロギングがイネーブルであり、コンソール端末に送信される syslog メッセージの重大度は **critical** 重大度以下の syslog メッセージに制限され、ロギング バッファのサイズが 60,000 バイトに設定されているロギングの設定を示します。

```
!
logging console critical
logging buffered 60000
!
```

syslog メッセージの宛先の設定：例

次の例では、ロギングがコンソール端末以外の宛先に設定されているロギングの設定を示します。この設定は次のようになります。

- コンソール端末以外の宛先に対するロギングはイネーブル。
- **warnings** 重大度以下の syslog メッセージは syslog サーバ ホストに送信される。
- **critical** 重大度より低い syslog メッセージは端末回線に送信される。
- ロギング バッファのサイズは 60,000 バイトに設定される。
- IP アドレス 172.19.72.224 の syslog サーバ ホストが syslog メッセージの受信先として設定される。

```
!
logging trap warnings
logging monitor critical
logging buffered 60000
logging 172.19.72.224
!
```

ロギング ヒストリ表の設定：例

次の例では、ロギング ヒストリ表のサイズが 200 エントリであり、ロギング ヒストリ表に送信される syslog メッセージの重大度が **errors** の重大度のメッセージに制限されているロギングの設定を示します。

```
logging history size 200
logging history errors
```

タイム スタンプの修正：例

次の例では、month date HH:MM:SS タイムゾーンの形式に従うようにタイム スタンプが設定されているタイム スタンプの設定を示します。

```
service timestamps log datetime show-timezone
```

次の例では、HH:MM:SS ミリ秒のタイムゾーンの形式に従うようにタイム スタンプが設定されているタイム スタンプの設定を示します。

```
service timestamps log datetime msec show-timezone
```

ロギング アーカイブの設定：例

次の例では、ロギング アーカイブを設定する方法とアーカイブ属性を定義する方法を示します。

```
RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# logging archive
RP/0/RSP0/CPU0:router(config-logging-arch)# device disk1
RP/0/RSP0/CPU0:router(config-logging-arch)# frequency weekly
RP/0/RSP0/CPU0:router(config-logging-arch)# severity warnings
RP/0/RSP0/CPU0:router(config-logging-arch)# archive-length 6
RP/0/RSP0/CPU0:router(config-logging-arch)# archive-size 50
RP/0/RSP0/CPU0:router(config-logging-arch)# file-size 10
```

次の作業

アラーム ログ相関を設定するには、*Cisco ASR 9000 Series Aggregation Services Router System Monitoring Configuration Guide*の「アラームおよびアラーム ログ相関の実装とモニタリング」モジュールを参照してください。

その他の参考資料

次の項では、Cisco IOS XR ソフトウェアへのロギング サービスの実装に関連する参考資料を紹介します。

関連資料

関連項目	参照先
ロギング サービス コマンド リファレンス	*Cisco ASR 9000 Series Aggregation Services Router System Monitoring Command Reference*の「*Logging Services Commands*」モジュール

関連項目	参照先
オンボード障害ロギング（OBFL）コンフィギュレーション	*Cisco ASR 9000 Series Aggregation Services Router System Monitoring Configuration Guide*の「オンボード障害ロギング コマンド」モジュール
オンボード障害ロギング（OBFL）コマンド	*Cisco ASR 9000 Series Aggregation Services Router System Monitoring Command Reference*の「*Onboard Failure Logging Commands*」モジュール
アラームおよびロギング相関コマンド	*Cisco ASR 9000 Series Aggregation Services Router System Monitoring Command Reference*の「*Alarm Management and Logging Correlation Commands*」モジュール
アラームおよびロギング相関コンフィギュレーションおよびモニタリング タスク	*Cisco ASR 9000 Series Aggregation Services Router System Monitoring Configuration Guide*の「アラームおよびアラーム ログ相関の実装とモニタリング」モジュール
SNMP コマンド	*Cisco ASR 9000 Series Aggregation Services Router System Monitoring Command Reference*の「*SNMP Commands*」モジュール
SNMP の設定作業	*Cisco ASR 9000 Series Aggregation Services Router System Monitoring Configuration Guide*の「*Implementing SNMP*」モジュール
Cisco IOS XR スタートアップ参考資料	*Cisco ASR 9000 Series Aggregation Services Router Getting Started Guide*
ユーザ グループとタスク ID に関する情報	*Cisco ASR 9000 Series Aggregation Services Router System Security Command Reference*の「*Configuring AAA Services*」モジュール

標準

標準	タイトル
この機能でサポートされる新規の標準または変更された標準はありません。また、既存の標準のサポートは変更されていません。	—

MIB

MIB	MIB のリンク
—	Cisco IOS XR ソフトウェアを使用して MIB を検索およびダウンロードするには、http://cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml にある Cisco MIB Locator を使用し、[Cisco Access Products] メニューからプラットフォームを選択します。

RFC

RFC	タイトル
この機能によりサポートされた新規 RFC または改訂 RFC はありません。また、この機能による既存RFCのサポートに変更はありません。	—

シスコのテクニカル サポート

説明	リンク
シスコのテクニカルサポートWebサイトには、数千ページに及ぶ検索可能な技術情報があります。製品、テクノロジー、ソリューション、技術的なヒント、およびツールへのリンクもあります。 Cisco.com に登録済みのユーザは、このページから詳細情報にアクセスできます。	http://www.cisco.com/en/US/support/index.html