システム ロギングの実装

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。

システム ロギング実装の機能履歴

リリース	変更内容
リリース 6.1.2	プラットフォーム自動モニタリング（PAM）ツールは、すべての Cisco IOS XR 64 ビット プラットフォームに導入されました。

システム ロギングの実装

システム ロギング（Syslog）は、システム ログ メッセージの送信に使用される標準アプリケーションです。ログ メッセージは、デバイスの正常性を示すか、発生した問題を指摘します。重大度に応じて通知メッセージを簡素化する場合もあります。IOS XR ルータは、syslog メッセージを syslog プロセスに送信します。デフォルトでは、syslog メッセージはコンソール端末に送信されます。しかし、syslog メッセージは、ロギング バッファ、syslog サーバ、端末回線などのコンソール以外の宛先に送信することができます。

syslog メッセージ形式

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 category -group -severity -message
 -code : message-text
```

次の表は、Cisco IOS XR ソフトウェアでの syslog メッセージの一般形式について説明しています。

表 *1 : syslog* メッセージの形式

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。
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。
process-name	syslog メッセージを生成したプロセスのプロセスです。
size	syslog メッセージを生成したプロセスのプロセス ID（pid）です。
[pid]	syslog メッセージに関連付けられているメッセージ カテゴリ、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 メッセージの重大度

コンソール端末、syslog サーバ、および端末回線などのロギング先の場合、syslog メッセージの重大度を指定することによって、ロギング先に送信されるメッセージの数を制限できます。ただし、ロギングバッファ宛先では、指定された重大度に関係なく、すべての重大度のsyslogメッセージが送信されます。この場合、重大度レベルは、**show logging** コマンドの出力に表示される syslog メッセージを、指定された値以下で制限するだけです。次の表では、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の順に一覧で示します。

表 *2 : syslog* メッセージの重大度

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

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

システム ロギングの設定に関する前提条件

Network Operating Center（NOC）でシステム メッセージのロギングを設定するには、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。

システム ログ機能の設定

必要に応じてシステム ロギングを設定するには、この項のタスクを実行します。

ロギング バッファへのロギングの設定

Syslogメッセージは、ロギングバッファと呼ばれる内部循環バッファを含む複数の宛先に送信できます。logging buffered コマンドを使用して、syslog メッセージをロギング バッファに送信できます。

設定例

次の例に、syslogメッセージをロギングバッファに送信するための設定を示します。ロギングバッファのサイズは3000000バイトに設定されています。ロギングバッファのサイズのデフォルト値は 2097152 バイトです。

```
RP/0/RP0/CPU0:Router# configure
RP/0/RP0/CPU0:Router(config)# logging buffered 3000000
RP/0/RP0/CPU0:Router(config)# commit
```

リモート サーバへのロギングの設定

Syslog メッセージは、ロギング バッファ、syslog サーバ、端末回線などのコンソール以外の宛先に送信することができます。logging コマンドを使用して syslog サーバの IP アドレスまたはホスト名を指定することにより、syslog メッセージを外部の syslog サーバに送信できます。また、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。

次の表に、syslog サーバに送信される syslog メッセージの管理に役立つ、Cisco IOS XR ソフトウェアでサポートされている機能を示します。

表 *3: Syslog* メッセージを管理するための機能

機能	説明
UNIX システム ログ機能	Facility は、ログ メッセージを送信したアプリケーションまたはプロセスを記述するために UNIX が使用する識別子です。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。
ホスト名プレフィックス ロギング	Cisco IOS XR ソフトウェアは、ホスト名の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追加するには、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 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終了するかに関係なく、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、logging source-interface コマンドを使用します。

設定例

次の例に、syslog メッセージを外部の syslog サーバに送信するための設定を示します。IP アドレス 10.3.32.154 は syslog サーバとして設定され、logging trap コマンドは重大度に基づいて syslog サーバに送信される syslog メッセージを制限するために使用されています。

```
RP/0/RP0/CPU0:Router# configure
RP/0/RP0/CPU0:Router(config)# logging 10.3.32.154
(Optional) RP/0/RP0/CPU0:Router(config)# logging 10.3.32.155 vrf vrfa
RP/0/RP0/CPU0:Router(config)# logging trap warnings
RP/0/RP0/CPU0:Router(config)# logging facility kern (optional)
RP/0/RP0/CPU0:Router(config)# logging hostnameprefix 123.12.35.7 (optional)
```

```
RP/0/RP0/CPU0:Router(config)# logging source-interface HundredGigE 0/0/1/0 (optional)
RP/0/RP0/CPU0:Router(config)# commit
```

関連項目

- ロギング バッファへのロギングの設定 （3 ページ）
- 端末回線へのロギングの設定 （5 ページ）

端末回線へのロギングの設定

デフォルトでは、syslogメッセージはコンソール端末に送信されます。しかし、syslogメッセージは、コンソール以外の端末回線に送信することもできます。logging monitor コマンドを使用して、syslog メッセージをロギング バッファに送信できます。

設定例

次の例に、syslog メッセージをコンソール以外の端末回線に送信するための設定を示します。この例では、重大度レベルが critical に設定されています。terminal monitor コマンドは、ターミナル セッション中に syslog メッセージを表示するように設定されています。デフォルトの重大度は debugging です。

```
RP/0/RP0/CPU0:Router# configure
RP/0/RP0/CPU0:Router(config)# logging monitor critical
RP/0/RP0/CPU0:Router(config)# commit
RP/0/RP0/CPU0:Router# terminal monitor
```

コンソール端末へのロギングの変更

デフォルトでは、syslog メッセージはコンソール端末に送信されます。コンソール端末への syslog メッセージのロギングを変更できます

設定例

次に、コンソール端末への syslog メッセージのロギングを変更する例を示します。

```
RP/0/RP0/CPU0:Router# configure
RP/0/RP0/CPU0:Router(config)# logging console alerts
RP/0/RP0/CPU0:Router(config)# commit
```

タイム スタンプ形式の変更

デフォルトでは、syslog メッセージのタイム スタンプが有効になっています。タイム スタンプは、month day HH:MM:SS の形式で生成され、メッセージが生成された日時を示します。

設定例

次の例では、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を変更する方法を示します。

```
RP/0/RP0/CPU0:Router# configure
RP/0/RP0/CPU0:Router(config)# service timestamps log datetime localtime msec or service
 timestamps log uptime
RP/0/RP0/CPU0:Router(config)# service timestamps debug datetime msec show-timezone or
```

```
service timestamps debug uptime
RP/0/RP0/CPU0:Router(config)# commit
```

重複 syslog メッセージの抑制

特に大規模ネットワークで、重複メッセージが作成されないようにすると、メッセージクラッターを減らし、ログの解釈作業を効率化できます。重複メッセージの抑制機能により、ロギング ヒストリと syslog ファイルの両方で、重複するイベント メッセージを大幅に削減できます。

設定例

次の例に、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示します。

```
RP/0/RP0/CPU0:Router# configure
RP/0/RP0/CPU0:Router(config)# logging suppress duplicates
RP/0/RP0/CPU0:Router(config)# commit
```

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

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。logging archive コマンドを使用して、ロギング アーカイブを作成し、ロギング メッセージの収集および保存方法を指定できます。

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

機能	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。
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。

機能	説明
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** 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。

設定例

次に、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例を示します。

```
RP/0/RP0/CPU0:Router# configure
RP/0/RP0/CPU0:Router(config)# logging archive
RP/0/RP0/CPU0:Router(config-logging-arch)# device disk1
RP/0/RP0/CPU0:Router(config-logging-arch)# frequency weekly
RP/0/RP0/CPU0:Router(config-logging-arch)# severity warnings
RP/0/RP0/CPU0:Router(config-logging-arch)# archive-length 6
RP/0/RP0/CPU0:Router(config-logging-arch)# archive-size 50
RP/0/RP0/CPU0:Router(config-logging-arch)# file-size 10
RP/0/RP0/CPU0:Router(config)# commit
```

プラットフォーム自動モニタリング

プラットフォーム自動モニタリング（PAM）は、プロセス クラッシュ、メモリ リーク、CPU ホッグ、トレースバック、syslog、ディスク使用率などの問題をモニタするために Cisco IOS XR ソフトウェア イメージ に統合されたシステム モニタリング ツールです。PAM はすべての Cisco IOS XR 64 ビット プラットフォームでデフォルトで有効になっています。PAM ツールは、これらのシステムの問題を検出すると、問題のトラブルシューティングに必要なデータを

収集し、問題を示すSyslogメッセージを生成します。自動収集されたトラブルシューティング情報は、harddisk:/cisco_support/ または /misc/disk1/cisco_support/ ディレクトリに個別のファイルとして保存されます。

PAM イベント

PAM は、プロセスのクラッシュ、トレースバック、潜在的なメモリ リーク、CPU ホッグ、またはフル ファイル システムを検出すると、自動的にログを収集し、これらのログ（該当する場合はコア ファイルとともに）を *.tgz* ファイルとして harddisk:/cisco_support/ または /misc/disk1/cisco_support/ ディレクトリに保存します。また、PAM は重大度が warning の syslog メッセージを生成し、それぞれの問題について言及します。

.tgz ファイルの形式は *PAM-<platform>-<PAM event>-<node-name>-<PAM process>-<YYYYMMDD>-<checksum>.tgz* です。たとえば、*PAM--crash-xr_0_RP0_CPU0-ipv4_rib-2016Aug16-210405.tgz* は、PAM がプロセスのクラッシュを検出した場合に収集されるファイルです。

PAM は、コア ファイルがデフォルトのアーカイブ フォルダ（harddisk:/ または /misc/disk1/）に保存されていることを前提としているため、コアアーカイブの場所を変更したり（例外ファイルパスを設定することによって）、PAM がイベントを検出した後に生成されたコア ファイルを削除したりしないでください。従わない場合、PAM はプロセスのクラッシュを検出しません。また、一度報告した後は、PAM は同じノード内の同じプロセスにおける同じ問題を再度報告しません。

ログの収集中に使用されるコマンドのリストについては、「PAM ツールによって収集されるファイル （12 ページ）」を参照してください。

以下の項では、PAM の主なイベントについて説明します。

クラッシュのモニタリング

PAMは、すべてのノードのプロセスクラッシュをリアルタイムでモニタします。以下は、PAMがプロセスのクラッシュを検出したときに生成されるサンプル syslog です。

```
RP/0/RP0/CPU0:Aug 16 21:04:06.442 : logger[69324]: %OS-SYSLOG-4-LOG_WARNING : PAM detected
 crash for ipv4_rib on 0_RP0_CPU0.
All necessary files for debug have been collected and saved at
0/RP0/CPU0 : harddisk:/cisco_support/PAM--crash-xr_0_RP0_CPU0-ipv4_rib-2016Aug16-210405.tgz

Please copy tgz file out of the router and send to Cisco support. This tgz file will be
 removed after 14 days.)
```

トレースバックのモニタリング

PAM は、すべてのノードのトレースバックをリアルタイムでモニタします。以下は、PAM がトレースバックを検出したときに生成されるサンプル syslog です。

```
RP/0/RP0/CPU0:Aug 16 21:42:42.320 : logger[66139]: %OS-SYSLOG-4-LOG_WARNING : PAM detected
 traceback for ipv4_rib on 0_RP0_CPU0.
All necessary files for debug have been collected and saved at
0/RP0/CPU0 :
```

```
harddisk:/cisco_support/PAM--traceback-xr_0_RP0_CPU0-ipv4_rib-2016Aug16-214242.tgz
Please copy tgz file out of the router and send to Cisco support. This tgz file will be
 removed after 14 days.)
```

メモリ使用率モニタリング

PAM は、すべてのノードのプロセス メモリ使用率をモニタします。PAM は、メモリ使用率の傾向をモニタし、収集されたデータに独自のアルゴリズムを適用することによって、潜在的なメモリ リークを検出します。デフォルトでは、すべてのノードで最大出力を 30 分間隔で定期的に収集します。

以下は、PAM が潜在的なメモリ リークを検出したときに生成されるサンプル syslog です。

```
RP/0/RP0/CPU0:Aug 17 05:13:32.684 : logger[67772]: %OS-SYSLOG-4-LOG_WARNING : PAM detected
 significant memory increase
(from 13.00MB at 2016/Aug/16/20:42:41 to 28.00MB at 2016/Aug/17/04:12:55) for
pam_memory_leaker on 0_RP0_CPU0.
All necessary files for debug have been collected and saved at
0/RP0/CPU0 :
harddisk:/cisco_support/PAM--memory_leak-xr_0_RP0_CPU0-pam_memory_leaker-2016Aug17-051332.tgz

(Please copy tgz file out of the router and send to Cisco support. This tgz file will
be removed after 14 days.)
```

CPU モニタリング

PAM は、すべてのノードの CPU 使用率を 30 分間隔で定期的にモニタします。PAM は、次のシナリオのいずれかで CPU ホッグを報告します。

- プロセスが常に多くの CPU を消費する場合（つまり、しきい値の 90% を超える場合）
- CPU 使用率の高い状態が 60 分よりも長く続く場合

以下は、PAM が CPU ホッグを検出したときに生成されるサンプル syslog です。

```
RP/0/RP0/CPU0:Aug 16 00:56:00.819 : logger[68245]: %OS-SYSLOG-4-LOG_WARNING : PAM detected
 CPU hog for cpu_hogger on 0_RP0_CPU0.
All necessary files for debug have been collected and saved at 0/RP0/CPU0 :
harddisk:/cisco_support/PAM--cpu_hog-xr_0_RP0_CPU0-cpu_hogger-2016Aug16-005600.tgz
(Please copy tgz file out of the router and send to Cisco support. This tgz file will
be removed after 14 days.)
RP/0/RP0/CPU0:Jun 21 15:33:54.517 : logger[69042]: %OS-SYSLOG-1-LOG_ALERT : PAM detected
 ifmgr is hogging CPU on 0_RP0_CPU0!
```

ファイル システム モニタリング

PAM は、すべてのノードのディスク使用率を 30 分間隔で定期的にモニタします。以下は、PAM がシステム ファイルがいっぱいであることを検出したときに生成されるサンプル syslog です。

```
RP/0/RP0/CPU0:Jun 20 13:59:04.986 : logger[66125]: %OS-SYSLOG-4-LOG_WARNING : PAM detected
 /misc/config is full on 0_1_CPU0
(please clean up to avoid any fault caused by this). All necessary files for debug have
```

```
 been collected and saved at
0/RP0/CPU0 : harddisk:/cisco_support/PAM--disk_usage-xr_0_1_CPU0-2016Jun20-135904.tgz
(Please copy tgz file out of the router and send to Cisco support. This tgz file will
be removed after 14 days.)
```

PAM の無効化と再有効化

PAM ツールは、monitor_cpu.pl、monitor_crash.pl、monitor_show_show_logging.pl の 3 つのモニタリング プロセスで構成されています。

PAM を無効化または再度有効化する前に、次のオプションを使用して、PAM がルータにインストールされているかどうかを確認します。

- Cisco IOS XR コマンドライン インターフェイスから：

```
Router# show processes pam_manager location all
Tue Jun 14 17:58:42.791 UTC
node:      node0_RP0_CPU0
                  Job Id: 317
                     PID: 14070
         Executable path:
/opt/cisco/XR/packages/iosxr-infra.rp-6.1.1.17I/bin/pam_manager
              Instance #: 1
              Version ID: 00.00.0000
                 Respawn: ON
           Respawn count: 4
            Last started: Mon Jun 13 23:08:43 2016
           Process state: Run
           Package state: Normal
                    core: MAINMEM
                Max. core: 0
                   Level: 999
               Placement: None
             startup_path:
/opt/cisco/XR/packages/iosxr-infra.rp-6.1.1.17I/startup/pam_manager.startup
                   Ready: 0.166s
        Process cpu time: 0.200 user, 0.310 kernel, 0.510 total
JID    TID  Stack  pri  state        NAME             rt_pri
317    14070    0K 20 Sleeping     pam_manager         0
317    14071    0K 20 Sleeping     lwm_debug_threa     0
317    14076    0K 20 Sleeping     pam_manager         0
317    14077    0K 20 Sleeping     lwm_service_thr     0
317    14078    0K 20 Sleeping     qsm_service_thr     0
317    14080    0K 20 Sleeping     pam_manager         0
```

- ルータ シェル プロンプトから：

```
Router# run ps auxw|egrep perl
Tue Jun 14 18:00:25.514 UTC
root     14324  0.0  0.2  84676 34556 ?  S Jun13   0:40 /usr/bin/perl
/pkg/opt/cisco/pam//monitor_cpu.pl
root     14414  0.0  0.1  65404 14620 ?  S Jun13   0:00 /usr/bin/perl
/pkg/opt/cisco/pam//monitor_crash.pl
```

PAM の無効化

PAM エージェントをシャットダウンするには、XR EXEC モードから次のコマンドを実行します。

ローカル RP の場合：

```
Router# process shutdown pam_manager
```

すべての RP の場合：

```
Router# process shutdown pam_manager location all
```

PAM の再有効化

pam_manager は必須プロセスではないため、手動で無効にした場合は自動的に再起動されません（システム リロードの場合を除く）。PAM エージェントを再起動するには、XR EXEC モードから次のコマンドを実行します。

ローカル RP の場合：

```
Router# process start pam_manager
```

すべての RP の場合：

```
Router# process start pam_manager location all
```

（注） すべてのロケーションで PAM を開始するには、**process start pam_manager** コマンドの **location all** オプションを使用して、すべてのノードで *pam_manager* プロセスを再起動する必要があります。

PAM でのデータ アーカイブ

任意の時点で、PAM は 200 MB を超えるハードディスクのスペースを占有しません。200 MB より多く必要な場合、PAM は古いファイルをアーカイブし、ログを自動的にローテーションします。

PAM は、CPU またはメモリ使用量（**top -b -n1** コマンドを使用）を定期的に 30 分間隔で収集します。ファイルは、<node name>.log というファイル名で harddisk:/cisco_support/ ディレクトリに保存されます（例：harddisk:/cisco_support/xr-0_RP0_CPU0.log）。ファイル サイズが 15MB の制限を超えると、ファイルは .tgz ファイルにアーカイブ（圧縮）され、最大 2 回ローテーションされます（つまり、.tgz ファイルは 2 つしか保持されません）。.tgz ファイルの最大ローテーション数は 3 です。また、ノードがリロードされると、古いファイル（ASCII データ）がアーカイブされ、ローテーションされます。たとえば、RP0 がリロードされると、xr-0_RP0_CPU0.log がアーカイブされます。

PAM によって生成されたコア ファイルは手動で削除しないでください。コア ファイルには、*<process name>_pid.by_user.<yyyymmdd>-<hhmmss>.<node>.<checksum>.core.gz* と名前が付けられます。

PAM ツールによって収集されるファイル

次の表は、さまざまな PAM イベントと、各イベントに対し PAM によって収集される各コマンドとファイルを示しています。

シスコ テクニカル サポートでサービス リクエスト（SR）を発行するときに、個々の *.tgz* ファイルを添付できます。

イベント名	PAM によって収集されるコマンドおよびファイル
プロセスのクラッシュ	• **show install active** • **show platform** • **show version** • コア（gz）ファイル • core.txt ファイル
プロセスのトレースバック	• **show dll** • **show install active** • **show logging** • **show platform** • **show version**
メモリ リーク	• **show install active** • **show platform** • **show version** • コア（gz）ファイル • 実行中のダンプコア • 連続メモリ使用量のスナップショット
ロギング イベントの表示	• **show install active** • **show logging** • **show platform** • **show version** • コア（gz）ファイル • core.txt ファイル

イベント名	PAM によって収集されるコマンドおよびファイル
CPU ホッグ	• **follow process** • **pstack** • **show dll** • **show install active** • **show platform** • **show version** • **top -H** • コア（gz）ファイル • CPU 使用率のスナップショット
ディスク使用量	• **show install active** • **show platform** • **show version** • コンソール ログ • コア（gz）ファイル • ディスク使用率のスナップショット