システム ログ

この章では、さまざまなタイプのロギングに関連するパラメータを設定する方法と、その内容を表示する方法について説明します。内容は次のとおりです。

機能の概要と変更履歴

要約データ

該当製品または機能エリア	すべてのレガシー製品
該当プラットフォーム	• ASR 5500 • UGP • VPC-DI • VPC-SI

機能のデフォルト	有効
関連する CDETS ID	21.3：CSCuy65332
このリリースでの関連する変更点：	N/A
関連資料	• *ASR 5500 System Administration Guide* • *Command Line Interface Reference* • *VPC-DI* システム管理ガイド • *VPC-SI System* アドミニストレーション ガイド

マニュアルの変更履歴

（注） リリース 21.2 および N5.5 よりも前に導入された機能の改訂履歴の詳細は示していません。

改訂の詳細	リリース
この標準で定義されている RFC5424 と syslog メッセージングの標準をサポートするため、StarOS 内の syslog クライアントがこのリリースで更新されました。StarOS は、以前の RFC3164 メッセージフォーマットを引き続きサポートします。また、このリリースでは、複数のポートを使用して複数の syslog サーバーの IP アドレスを設定することもできます。 （注） リリース 21.6 では、UDP のみを使用したトランスポート層のメッセージングがサポートされています。このリリースでは、TLS と TCP はサポートされていません。	21.6
管理者がイベント ID またはイベント ID の範囲に対してロギングを完全に無効にした場合、またはロギングのレベルをデフォルトのロギングレベル未満（エラーレベル）に変更した場合に通知を行うため、2 つの新しいクリティカル CLI イベントログと 2 つの新しい SNMP トラップが追加されています。このリリースでは、これらのイベントログとトラップはデフォルトで有効になっており、無効にすることはできません。詳細については、グローバル構成モードのフィルタリング （7 ページ） を参照してください。 この機能の結果として、追加または変更されたコマンドはありません。 **show snmp trap statistics** コマンド出力が拡張され、ロギングイベントが無効になっているか、またはロギングレベルがデフォルトの（エラー）ロギングレベルよりも下に変更された場合に、イベント内に詳細が表示されるようになりました。	21.3

改訂の詳細	リリース
最初の導入。	21.2 よりも前

システムログのタイプ

システムで設定および表示できるログには、次の 5 つのタイプがあります。

重要 すべてのイベントログをすべての製品で設定できるわけではありません。設定可能性は、使用されているハードウェア プラットフォームとライセンスによって異なります。

- **イベント**：イベントロギングを使用して、システムのステータスを判断し、システムで使用されているプロトコルとタスクに関する重要な情報をキャプチャできます。これは、すべてのコンテキスト、セッション、およびプロセスに適用されるグローバル機能です。
- **アクティブ**：アクティブログは、 CLI instance-by-CLI インスタンスベースでオペレータが設定可能です。1 つの CLI インスタンスで管理ユーザーによって設定されたアクティブログは、別の CLI インスタンスの管理ユーザーによって表示することはできません。各アクティブログは、システムに対してグローバルに設定されているものとは独立したフィルタプロパティと表示プロパティを使用して設定できます。イベントが生成されると、アクティブログがリアルタイムで表示されます。
- **トレース**：トレースロギングを使用して、接続されている特定のサブスクライバセッションで発生する可能性のある問題を迅速に分離できます。トレースは、特定のコール ID（callid）番号、IP アドレス、モバイルステーション ID（MSID）番号、またはユーザー名に対して実行できます。
- **モニター**：モニターロギングは、特定のセッションに関連付けられているすべてのアクティビティを記録します。この機能は、特定のサブスクライバのモニタリング機能に関する司法当局の要請を遵守するために使用できます。モニターは、サブスクライバの MSID またはユーザー名に基づいて実行できます。
- **クラッシュ**：クラッシュロギングには、システムソフトウェアのクラッシュに関する有用な情報が保存されています。この情報は、クラッシュの原因を特定するのに役立ちます。

重要 ステートフルファイアウォールと NAT は、ロギングがファイアウォールに対して有効になっている場合に、画面上のさまざまなメッセージのロギングをサポートします。これらのログは、critical、error、warning、および debug などのさまざまなレベルで詳細なメッセージを提供します。ステートフルファイアウォールと NAT 攻撃ログは、攻撃によってドロップされたパケットの送信元 IP アドレス、宛先 IP アドレス、プロトコル、または攻撃タイプに関する情報も提供します。また、システムで設定されている場合は、syslog サーバーにも送信されます。ステートフル ファイアウォールおよび NAT のロギングサポートの詳細については、『*PSF Administration guide*』または『*NAT Administration Guide*』の「*Logging Support*」の章を参照してください。

イベントロギングパラメータの設定

システムは、ユーザー定義のフィルタに基づいてログを生成するように設定できます。フィルタは、システムがモニターするファシリティ（システムタスクまたはプロトコル）と、イベントエントリの生成をトリガーするシビラティ（重大度）レベルを指定します。

イベントログはシステムメモリに保存され、CLI を使用して表示できます。イベントロギング情報を保存する 2 つのメモリバッファがあります。最初のバッファには、アクティブなログ情報が保存されます。2 番目のバッファには、非アクティブなロギング情報が保存されます。非アクティブバッファは一時的なリポジトリとして使用され、データを上書きせずにログを表示できます。ログは、手動による介入によってのみ非アクティブバッファにコピーされます。

各バッファには最大 50,000 のイベントを保存できます。これらのバッファがキャパシティに達すると、最も古い情報が削除され、最新の情報を保存するための領域が確保されます。

ログデータの損失を防ぐために、ネットワーク インターフェイスを介して syslog サーバーにログを送信するようにシステムを設定できます。

重要 TACACS+ アカウンティング（CLI イベントロギング）は、合法的傍受ユーザー（priv レベル 15 および 13）に対して生成されません。

イベントログフィルタの設定

Exec モードおよびグローバル構成モード レベルでイベントログの内容をフィルタリングできます。詳細については、『*Command Line Interface Reference*』を参照してください。

Exec モードのフィルタリング

これらのコマンドを使用すると、グローバル ロギング パラメータを変更することなく、ログに含まれるデータの量を制限できます。

Exec モードのコマンドを介してログをフィルタ処理するには、次の例に従います。

アクティブなフィルタリング

logging active [copy runtime filters] [event-verbosity *event_level* **] [pdu-data** *format* **] [pdu-verbosity** *pdu_level* **]**

注：

- **copy runtime filters** ：ランタイムフィルタをコピーし、そのコピーを使用して現在のロギングセッションをフィルタ処理します。
- **event-verbosity** *event_level*：イベントのロギングで使用する verboseness のレベルを次のいずれかに指定します。
  - *min*：イベントに関する最小限の情報を表示します。情報には、イベント名、ファシリティ、イベント ID、シビラティ（重大度）レベル、日付、および時刻が含まれます。
  - *concise*：イベントに関する詳細情報を表示しますが、システム内にイベントの送信元を提供しません。
  - *full*：イベントが生成されたシステム内の場所を識別する送信元情報など、イベントに関する詳細情報を表示します。
- **pdu-data** *format*：ログに記録された場合のパケットデータユニットの出力形式を次のいずれかに指定します。
  - *none*： RAW 形式（未フォーマット）
  - *hex*：16 進数形式
  - *hex-ascii*：メインフレームのダンプと同様の 16 進数および ASCII
- **pdu-verbosity** *pdu_level*：パケットデータユニットのロギングに使用する verboseness のレベルを 1 ～ 5 の整数で指定します。5 が最も詳細なものです。

「設定の確認と保存」の章の説明に従って、設定を保存します。

インスタンスによるフィルタリングの無効化または有効化

logging filter active facility *facility* **level** *severity_level* **[critical-info | no-critical-info]**

logging filter { disable | enable } facility *facility* **{ all | instance** *instance_number* **}**

注：

- **active**：アクティブプロセスのみにロギングオプションを設定するように指示します。
- **disable**：特定のインスタンスまたはすべてのインスタンスのロギングを無効にします。このキーワードは、aaamgr、hamgr、および sessmgr ファシリティでのみサポートされています。

- **enable**：特定のインスタンスまたはすべてのインスタンスのロギングを有効にします。このキーワードは、aaamgr、hamgr、および sessmgr ファシリティでのみサポートされています。デフォルトでは、aaamgr、hamgr、および sessmgr のすべてのインスタンスに対してロギングが有効になっています。
- **facility** *facility* and **level** *severity_level*：どのシステムファシリティをどのレベルでログに記録するかを決定するロギングフィルタを設定します。詳細については、ファシリティの指定 （10 ページ）とイベントのシビラティ（重大度） （40 ページ）を参照してください。
- **all | instance** *instance_number*：すべてのインスタンス、または aaamgr、hamgr、または sessmgr の特定のインスタンスに対して、ロギングを無効にするか有効にするかを指定します。**show session subsystem facility** *facility* コマンドを実行して、特定のインスタンス番号を識別します。

（注） これらのキーワードは、**disable** および **enable** キーワードでのみサポートされています。

- **level** *severity_level*：次のリストからログに記録される情報のレベルを指定します。このレベルは、最高から最低の順に並べられます。
  - critical ：エラーイベントを表示
  - error：エラーイベントおよびシビラティ（重大度）レベルが高いすべてのイベントを表示
  - warning：警告イベントおよびシビラティ（重大度）レベルが高いすべてのイベントを表示
  - unusual ：異常イベントおよびシビラティ（重大度）レベルが高いすべてのイベントを表示
  - info：情報イベントおよびシビラティ（重大度）レベルが高いすべてのイベントを表示
  - trace：トレースイベントおよびシビラティ（重大度）レベルが高いすべてのイベントを表示
  - debug：すべてのイベントを表示

（注） このキーワードは、**active** キーワードとの組み合わせでのみサポートされています。

- **critical-info**：重要な情報のカテゴリ属性を持つイベントを表示するように指定します。これらのタイプのイベントの例は、システムプロセスとタスクが開始される際のブートアップ時に表示されます。これがデフォルトの設定です。

no-critical-info ：重要な情報のカテゴリ属性を持つイベントを表示しないように指定します。

（注） これらのキーワードは、**active** キーワードとの組み合わせでのみサポートされています。

重要 ファシリティの単一のインスタンスにおけるロギングを有効にするには、まずファシリティのすべてのインスタンスを無効にしてから、（**logging filter disable facility** *facility* **all**）次に特定のインスタンスのロギングを有効にする必要があります（**logging filter enable facility** *facility* **instance** *instance_number*）。デフォルトの動作に復元するには、すべてのインスタンスのロギングを再度有効にする必要があります（**logging filter enable facility** *facility* **all**）。

Exec モードの **show instance-logging** コマンドを使用して、ファシリティごとに有効にされたインスタンスのインスタンス番号を表示できます。

グローバル構成モードのフィルタリング

Exec モードおよびグローバル構成モード レベルでイベントログの内容をフィルタリングできます。

システムの実行時間イベントロギングパラメータを設定するには、次の例に従います。

```
configure
   logging filter runtime facility facility level report_level
   logging display { event-verbosity | pdu-data | pdu-verbosity }
   end
```

注：

- **facility** *facility* and **level** *severity_level*：どのシステムファシリティをどのレベルでログに記録するかを決定するロギングフィルタを設定します。詳細については、ファシリティの指定 （10 ページ）とイベントのシビラティ（重大度） （40 ページ）を参照してください。
- ログに記録するすべてのファシリティに対して手順を繰り返します。
- オプション：**logging disable eventid** コマンドを追加して、イベント ID の制限を設定します。システムは、特定のイベント ID またはある範囲のイベント ID の送信を制限して、ログに記録されるデータの量が最も有用なレベルとなるよう最小限に抑える機能を提供します。追加のイベント ID またはイベント ID の範囲のロギングを無効にするには、この手順を繰り返します。
- 管理者が上記のコマンド（**logging disable eventid**）を使用してイベント ID またはイベント ID 範囲のイベントロギングを制限すると、システムは重大なイベントログ「cli 30999 critical」と、無効にされた特定のイベント ID またはイベント ID 範囲を持つ SNMP トラップ「1361 (DisabledEventIDs)」を生成します。

このリリースでは、これらのイベントログとトラップはデフォルトで有効になっており、無効にすることはできません。

- 管理者がロギングレベルを下げる（**logging filter runtime facility *facility* level *report_level*** コマンドを使用して、デフォルトレベルである「error」より下にする）と、システムは重大なイベントログ「cli 30998 Critical」と、無効にされた特定のイベント ID またはイベント ID 範囲を持つ SNMP トラップ「1362 (LogLevelChanged)」を生成します。

  このリリースでは、これらのイベントログとトラップはデフォルトで有効になっており、無効にすることはできません。

次の例は、イベントロギングまたはログレベルが変更された場合に生成されるトラップの CLI 出力を示しています。

```
[local]host# show snmp trap statistics
SNMP Notification Statistics:
  ...
Trap Name                           #Gen #Disc  Disable Last Generated
----------------------------------- ----- -----  ------- --------------------
…
DisabledEventIDs                       1     0        0  2017:05:11:15:35:25
LogLevelChanged                        2     0        0  2017:05:11:15:28:03
```

```
[local]host# show snmp trap history
There are x historical trap records (5000 maximum)

Timestamp                Trap Information
-------------------------
```

```
…
Thu May 11 15:28:03 2017 Internal trap notification 1362 (LogLevelChanged) Logging level
 of facility resmgr is changed to critical by user #initial-config# context local privilege
 level Security Administrator ttyname /dev/pts/0 address type IPV4 remote ip address
0.0.0.0
…
Thu May 11 15:35:25 2017 Internal trap notification 1361 (DisabledEventIDs) Event IDs
from 100 to 1000 have been disabled by user adminuser context context privilege level
security administrator ttyname tty address type IPV4 remote ip address 1.2.3.4
…
Mon May 15 10:14:56 2017 Internal trap notification 1362 (LogLevelChanged) Logging level
 of facility sitmain is changed to critical by user staradmin context local privilege
level Security Administrator ttyname /dev/pts/1 address type IPV4 remote ip address
161.44.190.27
```

「設定の確認と保存」の章の説明に従って、設定を保存します。

syslog サーバの設定

syslog アーキテクチャ

システムロギング（syslog）は、StarOS から UDP トランスポート層を介してイベント情報を生成し、一元化されたイベントメッセージコレクタに送信するアーキテクチャです。syslog はクライアント/サーバーアーキテクチャを使用します。

- **syslog クライアント**：StarOS 製品で実行されている一連のプロセスであり、イベントメッセージの送信デバイスとして動作します。

- **syslog サーバー**：StarOS 製品から送信されたイベントメッセージを受信するように設定された外部サーバーです。

StarOS 製品は、受信の確認応答を必要とせずに、syslog プロトコルを使用してイベントメッセージを転送します。システムは、syslog サーバーがメッセージを受信できるかどうかに関係なく、イベントメッセージを転送します。

外部 syslog サーバーへイベントメッセージを送信するようにするシステムの設定

実行時イベントロギングのフィルタで生成された情報は、永続ストレージ用の syslog サーバーに送信できます。

重要 syslog サーバーに送信されるデータは、情報提供のために使用することを目的としています。課金やパフォーマンスのモニタリングなどの機能は、syslog には基づかないようにする必要があります。

重要 システムはコンテキストごとに syslog サーバーを設定する柔軟性を備えていますが、ネットワークトラフィックからのログトラフィックを分離するために、すべてのサーバーをローカルコンテキストで設定することを推奨します。

Syslog サーバーを設定するには、次の例を使用します。

```
configure
  context local
    logging syslog ip_address
    end
```

注：

- *ip_address* は、ネットワーク上のシステムログサーバーの IP アドレスを、IPv4 のドット付き 10 進表記か、または IPv6 のコロンで区切られた 16 進表記で指定します。
- **logging syslog** コマンドでは、いくつかのオプションのキーワードを使用できます。詳細については、『*Command Line Interface Reference*』の「*Context Configuration Mode Commands*」の章を参照してください。
- 追加の syslog サーバーを設定する場合は、必要に応じてこの手順を繰り返します。設定可能な syslog サーバーの数に制限はありません。

詳細については、『*Command Line Interface Reference*』の **logging** コマンドを参照してください。

「設定の確認と保存」の章の説明に従って、設定を保存します。

アクティブログの設定

アクティブログは、CLI instance-by-CLI インスタンスでオペレータが設定可能なイベントログです。1 つの CLI インスタンスで管理ユーザーによって設定されたアクティブログは、別の CLI インスタンスの管理ユーザーには表示されません。各アクティブログは、システムに対してグローバルに設定されているものとは独立したフィルタプロパティと表示プロパティを使用して設定できます。アクティブログは、生成時にリアルタイムで表示されます。

アクティブなログは、デフォルトではアクティブなメモリバッファに書き込まれません。アクティブなログをアクティブなメモリバッファに書き込むには、グローバル構成モードで次のコマンドを実行します。

```
[local]host_name(config)# logging runtime buffer store all-events
```

アクティブなログがアクティブなメモリバッファに書き込まれると、すべての CLI インスタンスのすべてのユーザーが使用できるようになります。

次の例を使用して、グローバル構成モードでアクティブロギングを設定します。

```
[local]host_name(config)# logging filter runtime facility facility level
report_level
```

注：

- どのシステムファシリティをどのレベルでログに記録するかを決定するロギングフィルタを設定します。詳細については、ファシリティの指定 （10 ページ）とイベントのシビラティ（重大度） （40 ページ）を参照してください。
- ログに記録するすべてのファシリティに対して手順を繰り返します。
- オプション：**logging disable eventid** コマンドを追加して、イベント ID の制限を設定します。システムは、特定のイベント ID またはある範囲のイベント ID の送信を制限して、ログに記録されるデータの量が最も有用なレベルとなるよう最小限に抑える機能を提供します。追加のイベント ID またはイベント ID の範囲のロギングを無効にするには、この手順を繰り返します。
- Exec モードの **logging active** コマンドでは、いくつかのキーワードオプションと変数を使用できます。詳細については、『*Command Line Interface Reference*』の「*Exec Mode Commands*」の章を参照してください。

必要なすべての情報が収集されたら、Exec モードで次のコマンドを入力して、アクティブなログの表示を停止できます。

```
no logging active
```

ファシリティの指定

重要 ロギングに使用できる実際のファシリティは、プラットフォームタイプ、StarOS のバージョン、およびインストールされている製品ライセンスによって異なります。

次のファシリティは、イベントデータをロギングするように設定できます。

- **a10**：A10 インターフェイス ファシリティ
- **a11**：A11 インターフェイス ファシリティ
- **a11mgr**：A11 マネージャファシリティ
- **aaa-client**：認証、許可、およびアカウンティング（AAA）クライアントファシリティ
- **aaamgr**：AAA マネージャのロギングファシリティ
- **aaaproxy**：AAA プロキシファシリティ
- **aal2**：ATM アダプテーション レイヤ 2（AAL2）プロトコルのロギング ファシリティ
- **acl-log**：アクセスコントロールリスト（ACL）のロギングファシリティ
- **acsctrl**：アクティブ チャージング サービス（ACS）コントローラファシリティ
- **acsmgr**：ACS マネージャファシリティ
- **afctrl**：ファブリックコントローラファシリティ [ASR 5500 のみ]
- **afmgr**：Fabric Manager のロギングファシリティ [ASR 5500 のみ]
- **alarmctrl**：アラームコントローラファシリティ
- **alcap**：Access Link Control Application Part（ALCAP）プロトコルのロギングファシリティ
- **alcapmgr**：ALCAP マネージャのロギングファシリティ
- **all**：すべてのファシリティ
- **asngwmgr**：アクセス サービス ネットワーク（ASN）ゲートウェイ マネージャ ファシリティ
- **asnpcmgr**：ASN ページング コントローラ マネージャ ファシリティ
- **bfd**：Bidirectional Forwarding Detection（BFD）プロトコル
- **bgp**：ボーダー ゲートウェイ プロトコル（BGP）ファシリティ
- **bindmux**：IPCF BindMux-Demux マネージャのロギングファシリティ
- **bngmgr**：ブロードバンド ネットワーク ゲートウェイ（BNG）Demux マネージャのロギングファシリティ
- **bssap+**：SGSN と MSC/VLR（2.5G および 3G）間のログインインターフェイス用のベース ステーション サブシステム アプリケーション部品+プロトコルファシリティ
- **bssgp**：ベース ステーション サブシステムの GPRS プロトコル ログイン ファシリティは、SGSN と BSS 間の情報の交換を処理します（2.5G のみ）
- **callhome**：Call Home アプリケーションのロギングファシリティ

- **cap**：プリペイドアプリケーション（2.5G および 3G）で使用されるプロコトル用 CAMEL Application Part（CAP）のロギングファシリティ
- **cbsmgr**：セルブロードキャスティング サービス（CBS）のロギングファシリティ [HNBGW]
- **cdf**：チャージング データ ファンクション（CDF）のロギングファシリティ
- **cfctrl**：コンテンツ フィルタリング コントローラのロギングファシリティ
- **cfmgr**: コンテンツ フィルタリング マネージャのロギングファシリティ
- **cgw**：統合アクセスゲートウェイ（CGW）のロギングファシリティ
- **cli**：コマンド ラインインターフェイス（CLI）のロギングファシリティ
- **cmp**：証明書管理プロトコル（IPSec）のロギングファシリティ
- **confdmgr**：ConfD Manager Proclet（netconf）のロギングファシリティ
- **connectedapps**：SecGW ASR 9000 oneP 通信プロトコル
- **connproxy**：コントローラプロキシのロギングファシリティ
- **credit-control**：Credit Control（CC）ファシリティ
- **csp**：カード/スロット/ポート コントローラ ファシリティ
- **css**：コンテンツ サービス セレクション（css）ファシリティ
- **css-sig**：CSS RADIUS シグナリングファシリティ
- **cx-diameter**：Cx Diameter メッセージファシリティ [CSCF <--> HSS]
- **data-mgr**：データ マネージャ フレームワーク のロギングファシリティ
- **dcardctrl**: IPSec のドーターカードコントローラのロギングファシリティ
- **dcardmgr**：IPSec ドーターカードマネージャのロギングファシリティ
- **demuxmgr**：Demux Manager API ファシリティ
- **dgmbmgr**：Diameter Gmb アプリケーション マネージャのロギングファシリティ
- **dhcp**：Dynamic Host Configuration Protocol（DHCP）のロギングファシリティ
- **dhcpv6**：DHCPv6
- **dhost**：分散ホストのロギングファシリティ
- **diabase**：Diabase メッセージファシリティ
- **diactrl**：Diameter Controller Proclet のロギングファシリティ
- **diameter**：Diameter エンドポイントのロギングファシリティ
- **diameter-acct**：Diameter アカウンティング
- **diameter-auth**：Diameter 認証

- **diameter-dns**：Diameter DNS サブシステム
- **diameter-ecs**：ACS Diameter シグナリングファシリティ
- **diameter-engine**：Diameter バージョン 2 エンジンのロギングファシリティ
- **diameter-hdd**：Diameter Horizontal Directional Drilling（HDD）インターフェイスファシリティ
- **diameter-svc**：Diameter サービス
- **diamproxy**：DiamProxy のロギングファシリティ
- **doulosuemgr**：DOULOS（IMS-IPSec）ユーザー機器マネージャ
- **dpath**：IPSec データパスのロギングファシリティ
- **drvctrl**：ドライバコントローラのロギングファシリティ
- **eap-diameter**：Extensible Authentication Protocol（EAP; 拡張可能認証プロトコル）IP セキュリティファシリティ
- **eap-ipsec**: Extensible Authentication Protocol（EAP; 拡張可能認証プロトコル）IPSec ファシリティ
- **eap-sta-s6a-s13-s6b-diameter**：EAP/STA/S6A/S13/S6B Diameter メッセージファシリティ
- **ecs-css**：ACSMGR <-> セッション マネージャ シグナリング インターフェイス ファシリティ
- **egtpc**：eGTP-C のロギングファシリティ
- **egtpmgr**：拡張 GPRS トンネリングプロトコル（eGTP）マネージャのロギングファシリティ
- **egtpu**：eGTP-U のロギングファシリティ
- **embms**：eMBMS ゲートウェイファシリティ
- **embms**：eMBMS ゲートウェイ Demux ファシリティ
- **epdg**：evolved Packet Data（ePDG）ゲートウェイのロギングファシリティ
- **event-notif**：イベント通知インターフェイスのロギングファシリティ
- **evlog**：イベントログファシリティ
- **famgr**：外部エージェントマネージャのロギングファシリティ
- **firewall**：ファイアウォールのロギングファシリティ
- **fng**：フェムト ネットワーク ゲートウェイ（FNG）のロギングファシリティ
- **gbmgr**：SGSN Gb インターフェイス マネージャ ファシリティ
- **gmm**：

  - 2.5 G の場合：GPRS Mobility Management（GMM）レイヤをログに記録します（LLC レイヤの上）
  - 3G の場合：アクセス アプリケーション レイヤ（RANAP レイヤの上）をログに記録します。

- **gprs-app**：GPRS アプリケーションのロギングファシリティ
- **gprs-ns**：GPRS ネットワーク サービス プロトコル（SGSN と BSS の間のレイヤ）のロギングファシリティ
- **gq-rx-tx-diameter**：Gq/Rx/Tx Diameter メッセージファシリティ
- **gss-gcdr**：GTPP ストレージサーバーの GCDR ファシリティ
- **gtpc**：GTP-C プロトコルのロギングファシリティ
- **gtpcmgr**：GTP-C プロトコルマネージャのロギングファシリティ
- **gtpp**：GTP-prime プロトコルのロギングファシリティ
- **gtpu**：GTP-U プロトコルのロギングファシリティ
- **gtpumgr**：GTP-U Demux マネージャ
- **gx-ty-diameter**：Gx/Ty Diameter メッセージファシリティ
- **gy-diameter**：Gy Diameter メッセージファシリティ
- **h248prt**：H.248 ポートマネージャファシリティ
- **hamgr**：ホーム エージェント マネージャのロギングファシリティ
- **hat**：高可用性タスク（HAT）プロセスファシリティ
- **hdctrl**：HD コントローラのロギングファシリティ
- **henbapp**：Home Evolved NodeB（HENB）アプリファシリティ
- **henbgw**：HENB-GW ファシリティ
- **henbgw-pws**：HENB-GW Public Warning System ロギングファシリティ
- **henbgw-sctp-acs**：HENB-GW アクセス Stream Control Transmission Protocol（SCTP）ファシリティ
- **henbgw-sctp-nw**：HENBGW ネットワーク SCTP ファシリティ
- **henbgwdemux**：HENB-GW Demux ファシリティ
- **henbgwmgr**：HENB-GW マネージャファシリティ
- **hnb-gw**：HNB-GW（3G Femto GW）ロギングファシリティ
- **hnbmgr**：HNB-GW Demux マネージャ ロギング ファシリティ

- **hss-peer-service**：ホームサブスクライバサーバー（HSS）ピアサービスファシリティ
- **iftask**：VPC-SI および VPC-DI プラットフォームで使用される内部フォワーダータスク（INTEL DPDK）
- **igmp**：Internet Group Management Protocol（IGMP）
- **ikev2**：インターネット キー エクスチェンジ バージョン 2（IKEv2）
- **ims-authorizatn**：IP マルチメディアサブシステム（IMS）認証サービスファシリティ
- **ims-sh**：Diameter Sh インターフェイスサービスファシリティ
- **imsimgr**：SGSN IMSI マネージャファシリティ
- **imsue**：IMS User Equipment（IMSUE）ファシリティ
- **ip-arp**：IP Address Resolution Protocol（ARP）
- **ip-interface**：IP インターフェイスファシリティ
- **ip-route**：IP ルートファシリティ
- **ipms**：インテリジェント パケット モニタリング システム（IPMS）のロギングファシリティ
- **ipne**: IP Network ENABLER（IPNE）ファシリティ
- **ipsec**：IP セキュリティ ロギング ファシリティ
- **ipsecdemux**：IPSec demux のロギングファシリティ
- **ipsg**：IP サービス ゲートウェイ インターフェイスのロギングファシリティ
- **ipsgmgr**: IP サービス ゲートウェイ ファシリティ
- **ipsp**：IP プール共有プロトコルのロギングファシリティ
- **kvstore**：Key/Value ストア（kvstore）ファシリティ
- **l2tp-control**：レイヤ 2 トンネリングプロトコル（L2TP）コントロールのロギングファシリティ
- **l2tp-data**：L2TP データロギングファシリティ
- **l2tpdemux**: L2TP Demux マネージャのロギングファシリティ
- **l2tpmgr**: L2TP マネージャのロギングファシリティ
- **lagmgr**：Link Aggregation GROUP（LAG）マネージャのログインファシリティ
- **lcs**：ロケーションサービス（LCS）のロギングファシリティ
- **ldap**：ライトウェイト ディレクトリ アクセス プロトコル
- **li**：コマンドの説明については、『*Lawful Intercept Configuration Guide*』を参照してください。

- **linkmgr**：SGSN/BSS SS7 リンクマネージャのロギングファシリティ（2.5G のみ）
- **llc**：論理リンク制御（LLC）プロトコルのロギングファシリティ。SGSN の場合、MS と SGSN の間の論理リンクについて、GMM レイヤと BSSGP レイヤの間にある LLC レイヤをログに記録します。
- **local-policy**：ローカル ポリシー サービス ファシリティ
- **location-service**：ロケーション サービス ファシリティ
- **m3ap**：M3 アプリケーション プロトコル ファシリティ
- **m3ua**：M3UA プロトコル ロギング ファシリティ
- **magmgr**：モバイル アクセス ゲートウェイ マネージャのロギングファシリティ
- **map**：モバイル アプリケーション パート（MAP）プロトコルのロギングファシリティ
- **megadiammgr**：MegaDiameter マネージャ（SLF サービス）のロギングファシリティ
- **mme-app**：モビリティ マネージメント エンティティ（MME）アプリケーションのロギングファシリティ
- **mme-embmsembms**：MME eMBMS ファシリティ
- **mme-misc**：MME その他のロギングファシリティ
- **mmedemux**：MME Demux マネージャのロギングファシリティ
- **mmemgr**：MME マネージャファシリティ
- **mmgr**：マスターマネージャのロギングファシリティ
- **mobile-ip**：モバイル IP プロセス
- **mobile-ip-data**：モバイル IP データファシリティ
- **mobile-ipv6**：モバイル IPv6 のロギングファシリティ
- **mpls**：マルチプロトコル ラベル スイッチング（MPLS）プロトコルのロギングファシリティ
- **mrme**：Multi Radio Mobility Entity（MRME）ロギングファシリティ
- **mseg-app**：Mobile Services Edge Gateway（MSEG）アプリケーション ロギング ファシリティ
- **mseg-gtpc**：MSEG GTP-C アプリケーション ロギング ファシリティ
- **mseg-gtpu**：MSEG GTP-U アプリケーション ロギング ファシリティ
- **msegmgr**：MSEG Demux マネージャ ロギング ファシリティ
- **mtp2**：Message Transfer Part 2（MTP2）サービスのロギングファシリティ
- **mtp3**：Message Transfer Part 3（MTP3）プロトコルのロギングファシリティ

- **multicast-proxy**：マルチキャストプロキシのロギングファシリティ
- **nas**：非アクセス階層（NAS）プロトコルのロギングファシリティ [MME 4G]
- **netwstrg**：ネットワーク ストレージ ファシリティ
- **npuctrl**：ネットワーク プロセッサ ユニット制御ファシリティ
- **npumgr**：ネットワーク プロセッサ ユニット マネージャ ファシリティ
- **npumgr-acl**：NPUMGR ACL のロギングファシリティ
- **npumgr-drv**：NPUMGR DRV のロギングファシリティ
- **npumgr-flow**：NPUMGR FLOW のロギングファシリティ
- **npumgr-fwd**：NPUMGR FWD のロギングファシリティ
- **npumgr-init**：NPUMGR INIT のロギングファシリティ
- **npumgr-lc**：NPUMGR LC のロギングファシリティ
- **npumgr-port**：NPUMGR PORT のロギングファシリティ
- **npumgr-recovery**：NPUMGR RECOVERY のロギングファシリティ
- **npumgr-rri**：NPUMGR RRI（リバースルートインジェクション）のロギングファシリティ
- **npumgr-vpn**：NPUMGR VPN のロギングファシリティ
- **ocsp**：オンライン証明書ステータスプロトコル
- **ogw-app**：オフロードゲートウェイ（OGW）アプリケーション ロギング ファシリティ [リリース12.0 以前のバージョンのみ]
- **ogw-gtpc**：OGW GTP-C アプリケーションのロギングファシリティ [リリース12.0 以前のバージョンのみ]
- **ogw-gtpu**：OGW GTP-U アプリケーションのロギングファシリティ [リリース12.0 以前のバージョンのみ]
- **ogwmgr**：OGW Demux マネージャのロギングファシリティ [リリース12.0 以前のバージョンのみ]
- **orbs**：オブジェクト リクエスト ブローカ システムのロギングファシリティ
- **ospf**：OSPF プロトコルのロギングファシリティ
- **ospfv3**：OSPFv3 プロトコルのロギングファシリティ
- **p2p**：ピアツーピアの検出のロギングファシリティ
- **pagingmgr**：PAGINGMGR のロギングファシリティ
- **pccmgr**：Intelligent Policy Control Function（IPCF）Policy Charging and Control（PCC）マネージャライブラリ

- **pdg**：Packet Data Gateway（PDG）ロギングファシリティ
- **pdgdmgr**：Pdg Demux マネージャのロギングファシリティ
- **pdif**: Packet Data Interworking Function（PDIF）のロギングファシリティ
- **pgw**：Packet Data Network Gateway（PGW）ロギングファシリティ
- **phs**：Personal Handyphone System（PHS）
- **phs-control**：Phs X1/X5 および X2/X6 インターフェイスのロギングファシリティ
- **phs-data**：PHS データのロギングファシリティ
- **phs-eapol**：PHS EAP over LAN（EAPOL）ロギングファシリティ
- **phsgwmgr**: PHS ゲートウェイ マネージャ ファシリティ
- **phspcmgr**：PHS ページング コントローラ マネージャ ファシリティ
- **pmm-app**：パケット モビリティ マネージメント（PMM）アプリケーション のロギング ファシリティ
- **ppp**：ポイントツーポイントプロトコル（PPP）リンクとパケットファシリティ
- **pppoe**：PPP over Ethernet のロギングファシリティ
- **proclet-map-frwk**：Proclet マッピングフレームワークのロギングファシリティ
- **push**：VPNMGR CDR プッシュのロギングファシリティ
- **radius-acct**：RADIUS アカウンティング ロギング ファシリティ
- **radius-auth**：RADIUS 認証のロギングファシリティ
- **radius-coa**：RADIUS の認可変更および radius 接続解除
- **ranap**：Radio Access Network Application Part（RANAP）プロトコルの SGSN と RNS（3G）間のファシリティロギング情報フロー
- **rct**：リカバリ制御タスクのロギングファシリティ
- **rdt**：リダイレクトタスクのロギングファシリティ
- **resmgr**：Resource Manager のロギングファシリティ
- **rf-diameter**：Diameter Rf インターフェイス メッセージ ファシリティ
- **rip**：Routing Information Protocol（RIP）のロギングファシリティ [RIP は現時点ではサポートされていません。]
- **rlf**：レート制限機能（RLF）のロギングファシリティ
- **rohc**：Robust Header Compression（RoHC）ファシリティ
- **rsvp**：予約プロトコルのロギングファシリティ

- **rua**：RANAP ユーザーアダプテーション（RUA）[3G フェムト GW メッセージ] のロギングファシリティ
- **s102**：S102 プロトコルのロギングファシリティ
- **s102mgr**：S102Mgr のロギングファシリティ
- **s1ap**：S1 アプリケーションプロトコル（S1AP）プロトコルのロギングファシリティ
- **sabp**：Service Area Broadcast Protocol（SABP）のロギングファシリティ
- **saegw**：System Architecture Evolution（SAE）ゲートウェイファシリティ
- **sbc**：SBc プロトコルのロギングファシリティ
- **sccp**：Signalling Connection Control Part（SCCP）プロトコルのロギング（RANAP と TCAP レイヤ間のコネクション型メッセージ）。
- **sct**：共有設定タスクのロギングファシリティ
- **sctp**：Stream Control Transmission Protocol（SCTP）プロトコルのロギングファシリティ
- **sef_ecs**：Severely Errored Frames（SEF）API 印刷ファシリティ
- **sess-gr**：SM GR ファシリティ
- **sessctrl**：セッションコントローラのロギングファシリティ
- **sessmgr**：セッションマネージャのロギングファシリティ
- **sesstrc**：セッショントレースのロギングファシリティ
- **sft**：スイッチファブリックタスクのロギングファシリティ
- **sgs**：SG インターフェイスプロトコルのロギングファシリティ
- **sgsn-app**：SGSN-APP がさまざまな SGSN の「グルー」インターフェイスをロギング（たとえば、PMM、MAP、GPRS FSM、SMS など）。
- **sgsn-failures**：SGSN コールの失敗（接続/アクティブ化の拒否) のロギングファシリティ（2.5G）
- **sgsn-gtpc**：SGSN と GGSN 間の制御メッセージをロギングする SGSN GTP-C プロトコル
- **sgsn-gtpu**：ユーザーデータメッセージをロギングする SGSN GTP-U プロトコル
- **sgsn-mbms-bearer**：SGSN マルチメディアブロードキャスト/マルチキャストサービス（MBMS）ベアラー APP（SMGR）のロギングファシリティ
- **sgsn-misc**：スタックマネージャが、レイヤ間のバインディングと削除をロギングするために使用する
- **sgsn-system**：SGSN システムコンポーネントのロギングファシリティ（使用頻度が低い）
- **sgsn-test**：SGSN テストのロギングファシリティ（使用頻度の低い）

- **sgtpcmgr**：SGTPC および GGSN を介した SGSN GTP-C Manager のロギング情報の交換
- **sgw**：サービング ゲートウェイ ファシリティ
- **sh-diameter**：Sh Diameter メッセージファシリティ
- **sitmain**：システム初期化タスクのメインロギングファシリティ
- [**slmgr.vbs**]：スマート ライセンシング マネージャのロギングファシリティ
- **sls**：サービスレベル仕様（SLS）プロトコルのロギングファシリティ
- **sm-app**：SM プロトコルのロギングファシリティ
- **sms**: ショートメッセージサービス（SMS）による MS と SMSC の間のメッセージのロギング
- **sndcp**：Sub Network Dependent Convergence Protocol（SNDCP）のロギングファシリティ
- **snmp**：SNMP のロギングファシリティ
- **sprmgr**：IPCF Subscriber Policy Register（SPR）マネージャのロギングファシリティ
- **srdb**：スタティック評価データベース
- **srp**: サービス冗長性プロトコル（SRP）のロギングファシリティ
- **sscfnni**：Service-Specific Coordination Function for Signaling at the Network Node Interface（SSCF-NNI）のロギングファシリティ
- **sscop**：Service-Specific Connection-Oriented Protocol（SSCOP）のロギングファシリティ
- **ssh-ipsec**：Secure SHELL（SSH）IP セキュリティのロギングファシリティ
- **ssl**：Secure Socket Layer（SSL）メッセージのロギングファシリティ
- **stat**：統計情報のロギングファシリティ
- **supserv**：補足サービスのロギングファシリティ [H.323]
- **system**：システムのロギングファシリティ
- **tacacsplus**：TACACS+ プロトコル ロギング ファシリティ
- **tcap**：TCAP プロトコルのロギングファシリティ
- **testctrl**：テストコントローラのロギングファシリティ
- **testmgr**：テストマネージャのロギングファシリティ
- **threshold**：しきい値のロギングファシリティ
- **ttg**：Tunnel Termination Gateway（TTG）のロギングファシリティ
- **tucl**：TCP/UDP コンバージェンスレイヤ（TUCL）のロギングファシリティ
- **udr**：ユーザーデータレコード（UDR）ファシリティ（Charging サービスで使用）

- **user-data**：ユーザーデータのロギングファシリティ
- **user-l3tunnel**：ユーザーレイヤ 3 トンネルのロギングファシリティ
- **usertcp-stack**：ユーザー TCP スタック
- **vim**：Voice インスタントメッセージ（VIM）のロギングファシリティ
- **vinfo**：VINFO のロギングファシリティ
- **vmgctrl**：仮想メディアゲートウェイ（VMG）コントローラファシリティ
- **vmgctrl**：VMG コンテンツ マネージャ ファシリティ
- **vpn**：仮想プライベートネットワークのロギングファシリティ
- **vpp**：Vector Packet Processing（VPP）のロギングファシリティ
- **wimax-data**：WiMAX データ
- **wimax-r6**：WiMAX R6
- **wsg**：ワイヤレス セキュリティ ゲートウェイ（ASR 9000 セキュリティゲートウェイ）
- **x2gw-app**：X2GW（X2 プロキシゲートウェイ、eNodeB）アプリケーションのロギング ファシリティ
- **x2gw-demux**：X2GW demux タスクのロギングファシリティ

トレースロギングの設定

トレースロギングは、現在アクティブな特定のセッションの問題を迅速に解決するのに役立ちます。これらは、Exec モードで **logging filter** コマンドを使用して設定されたグローバル イベントログフィルタに依存しない修飾子に基づいて生成される一時的なフィルタです。ただし、イベントログと同様に、ログによって生成される情報は、アクティブなメモリバッファに保存されます。

選択したコールに関連付けられているすべてのデバッグレベルイベントが保存されます。

重要 トレースログは、セッションの処理に影響します。デバッグ目的でのみ実装する必要があります。

Exec モードでトレースログを設定するには、次の例を使用します。

```
[local]host_name# logging trace { callid call_id | ipaddr ip_address | msid
ms_id | username username }
```

必要なすべての情報が収集されたら、次のコマンドを入力して、トレースログを削除できます。

```
[local]host_name# no logging trace { callid call_id | ipaddr ip_address | msid
 ms_id | username username }
```

モニターログの設定

モニターロギングは、特定のサブスクライバのすべてのセッションに関連付けられているすべてのアクティビティを記録します。この機能は、特定のサブスクライバのモニタリング機能に関する司法当局の要請を遵守している場合に使用できます。

モニターは、サブスクライバのMSIDまたはユーザー名に基づいて実行できます。また、司法当局によって規定された限定期間にのみ使用することを目的としています。したがって、必要なモニタリング期間の直後に終了する必要があります。

この項では、モニターログを有効または無効にする手順について説明します。

モニターログの有効化

モニターログのターゲットを設定するには、次の例を使用します。

```
configure
  logging monitor { ip_addr | ipv6_addr | msid id | username name }
  end
```

モニターログの追加のターゲットを設定するには、この手順を繰り返します。

モニターログの無効化

モニターログを無効にするには、次の例を使用します。

```
configure
  no logging monitor { ip_addr | ipv6_addr | msid id | username name }
  end
```

ロギング設定と統計情報の表示

ロギング設定と統計情報を確認するには、Exec モードで次のコマンドを入力します。

```
[local]host_name# show logging [ active | verbose ]
```

キーワードを指定しなかった場合は、グローバルフィルタ設定が表示され、有効になっている他のタイプのロギングに関する情報も表示されます。

次の表に、**verbose** キーワードを使用したときに表示される統計情報の説明を示します。

表 *1:* ロギング設定コマンドと統計情報コマンド

フィールド	説明
General Logging Statistics	

フィールド	説明
Total events received	システムによって生成されたイベントの合計数が表示されます。
Number of applications receiving events	イベントを受信しているアプリケーションの数が表示されます。
Logging Source Statistics	
Event sequence ids by process	生成されたイベントがあるシステムプロセスのリストと、生成されたイベントの参照識別番号が表示されます。
Msg backlog stat with total cnt	生成されたイベントの合計数と比較してログに記録されたイベントメッセージの数が表示されます。
LS L2 filter drop rate	ロギングソース（LS）のレイヤ2（L2）イベントのドロップのパーセンテージが表示されます。
Abnormal Log Source Statistics	異常なロギングソース（LS）の統計情報が表示されます（存在する場合）。
Runtime Logging Buffer Statistics	
Active buffer	現在アクティブなメモリバッファに記録されているイベントの数と、バッファ内の最も古いエントリと最新のエントリのタイムスタンプが表示されます。
Inactive buffer	非アクティブなメモリバッファに現在ログインしているイベント数が表示されます。

CLI を使用したイベントログの表示

システムによって生成されるイベントログは、次のいずれかの方法で表示できます。

- **syslog サーバーから、次のようにします。**システムが syslog サーバーにログを送信するように設定されている場合、ログは syslog サーバーで直接表示できます。
- **システム CLI から、次のようにします。**システムのメモリバッファに保存されているログは、CLI から直接表示できます。
- **コンソールポートから、次のようにします。**デフォルトでは、CLI セッションがアクティブになっていない場合、システムはコンソールインターフェイスを介して端末にイベントを自動的に表示します。

この項では、CLI を使用してイベントログを表示する手順を説明します。これらの手順は、Exec モードのルートプロンプトを使用していることが前提になります。

手順

ステップ 1 アクティブなログメモリバッファを非アクティブなログメモリバッファにコピーします。

アクティブなログメモリバッファが非アクティブなログメモリバッファにコピーされると、非アクティブなログメモリバッファ内の既存の情報が削除されます。

アクティブと非アクティブの両方のイベントログメモリバッファは、Exec モードの CLI を使用して表示できます。ただし、データが上書きされないようにするために、非アクティブなログを表示することをお勧めします。アクティブなログバッファからの情報は、次のコマンドを入力して非アクティブなログバッファにコピーできます。

```
[local]host_name# logs checkpoint
```

ステップ 2 次のコマンドを入力してログを表示します。

```
[local]host_name# show logs
```

show logs コマンドでは、いくつかのオプションのキーワードや変数を使用できます。詳細については、『*Command Line Interface Reference*』にある「*Exec Mode Show Commands*」の章を参照してください。

クラッシュログの設定と表示

ソフトウェアのクラッシュが発生した場合は、クラッシュの原因を特定するのに役立つ情報をシステムが保存します。この情報はシステムメモリ内で維持することも、ネットワークサーバーに転送して保存することもできます。

システムでは、次の 2 種類のログを生成することができます。

- **クラッシュログ**：クラッシュログには、ソフトウェアクラッシュに関するあらゆる情報が記録されます（完全なコアダンプ）。サイズが原因で、システムメモリに保存することはできません。したがって、ログを保存できるローカルデバイスか、またはネットワークサーバーを指定する Universal Resource Locator（URL）を使用して設定されている場合にのみ、これらのログが生成されます。
- **クラッシュログの要約**：クラッシュイベントレコードは、ソフトウェアクラッシュが発生したときに自動的に生成され、管理カード上のフラッシュメモリに保存されます。クラッシュログの要約には、関連付けられたダンプファイルとともに、クラッシュイベントのレコードのリストが含まれています。このログは、CLI コマンドを使用してイベントレコードとダンプファイルを表示します。

クラッシュロギングのアーキテクチャ

クラッシュログは、クラッシュイベント情報の永続的なリポジトリです。各イベントには番号が付けられており、CPU（minicore）、NPU、またはカーネルクラッシュに関連するテキストが含まれます。ログに記録されたイベントは、固定長レコードに記録され、/flash/crashlog2. に保存されます。

クラッシュが発生するたびに、次のクラッシュ情報が保存されます。

1. イベントレコードは、/flash/crashlog2 ファイル（クラッシュログ）に保存されます。

2. 関連する minicore、NPU、またはカーネルダンプファイルは、/flash/crsh2 ディレクトリに保存されます。
3. 完全なコアダンプは、ユーザーが設定したディレクトリに保存されます。

重要 crashlog2 ファイルは、関連する minicore、NPU、およびカーネルダンプとともに、冗長管理カード（SMC、MIO/UMIO）間で自動的に同期されます。フルコアダンプは、管理カード間で同期されません。

次の動作は、クラッシュロギングプロセスに適用されます。

- クラッシュイベントがアクティブな管理カードに到着すると、イベントレコードは、/flash/crsh2 の minicore、NPU、またはカーネルダンプファイルとともに crashlog2 ファイルに保存されます。クラッシュイベントとダンプファイルも、スタンバイ管理カード上の同じ場所に自動的に保存されます。
- クラッシュログエントリが CLI コマンドを使用して削除されると、アクティブとスタンバイの両方の管理カードで削除されます。
- 管理カードを追加または交換すると、アクティブカードとスタンバイカードによってクラッシュログとダンプファイルが自動的に同期されます。
- クラッシュイベントが受信され、クラッシュログファイルがいっぱいになると、クラッシュログ内の最も古いエントリと関連するダンプファイルが、両方の管理カードの最新の到着イベントとダンプファイルに置き換えられます。最大 120 のクラッシュイベントの情報を、管理カードに保存できます。
- クラッシュイベントが重複すると、既存のレコードのヒット数が変更され、古いクラッシュレコードで新しいレコードが更新されます。カウントに追加すると、イベントが最初に発生したときにタイムスタンプが使用されます。

ソフトウェアクラッシュログ接続先の設定

システムは、ソフトウェアのクラッシュログ情報を次のいずれかの場所に保存するように設定できます。

- ASR 5000 上：
  - **コンパクトフラッシュ™**：SMC に取り付けられています（要約されたクラッシュログおよび関連するダンプファイルのみ）。
  - **PCMCIA フラッシュカード**：SMC の PCMCIA1 スロットに取り付けられています。
- ASR 5500 上：
  - **フラッシュメモリ**：アクティブな MIO/UMIO に取り付けられています（要約されたクラッシュログおよび関連するダンプファイルのみ）。

- **USB メモリスティック**：アクティブな MIO/UMIO の USB スロットに取り付けられています。

- VPC 上
  - **フラッシュメモリ**：仮想マシンからアクセス可能です。
  - **USB メモリスティック**：プラットフォームの USB スロットに取り付けられています（USB スロットはハイパーバイザを介して有効になっています）。

- **ネットワークサーバー**：システムが Trivial File Transfer Protocol（TFTP）、File Transfer Protocol（FTP）、Secure File Transfer Protocol（SFTP）、または Hypertext Transfer Protocol（HTTP）を使用してアクセスできるネットワーク上のワークステーションまたはサーバーです。これは、複数のシステムが同じ設定を必要とする大規模なネットワークの展開に推奨されます。

重要 FTP はサポートされていません。

クラッシュログファイル（完全なコアダンプ）は、指定された場所で発生すると一意の名前で書き込まれます。名前の形式は、*crash-card-cpu-time-core* です。*Card* はカードスロット、*cpu* はカード上の CPU の数、*time* は 16 進表記の Portable Operating System Interface（POSIX）のタイムスタンプです。

次の例を使用して、グローバル構成モードでソフトウェアのクラッシュログの接続先を設定します。

```
configure
  crash enable [ encrypted ] url crash_url
  end
```

注：

- このコマンドの詳細については、『*Command Line Interface Reference*』の「*Global Configuration Mode Commands*」の章を参照してください。
- 追加のソフトウェアのクラッシュログの接続先を設定するには、この手順を繰り返します。設定可能な接続先の数に制限はありません。

「設定の確認と保存」の章の説明に従って、設定を保存します。

CLI を使用して要約されたクラッシュログ情報の表示

管理カード（**/flash/crashlog2**）上のフラッシュメモリに一連のイベントレコードとして保存されている要約されたクラッシュ情報を表示できます。各クラッシュイベントレコードには、表示可能な（minicore、NPU、またはカーネル）関連のダンプファイル **(/flash/crsh2)** があります。

システムで発生したソフトウェアクラッシュイベントを表示するには、この項の手順に従ってください。これらの手順は、Exec モードのルートプロンプトを使用していることが前提になります。

手順

ステップ 1 次の Exec モードコマンドを入力して、ソフトウェアクラッシュイベントのリストを表示します。

`[local]host_name#` **show crash { all | list | number** *crash_num* **}**

注：

- **Show crash list** を実行して、特定のクラッシュイベントの番号を取得します。
- **Show crash number** *crash_num* を実行して、ターゲットクラッシュイベントの出力を表示します。

結果として得られる出力は、すべてのプラットフォームで同じとは限りません。

同様のクラッシュイベントに関する情報は、このコマンドの出力では抑制されます。

ステップ 2 特定のクラッシュイベントに関連付けられているダンプファイルを表示します。

ダンプファイルに含まれる情報は、ソフトウェアがクラッシュする原因となっている内部または外部の要因を特定して診断するのに役に立ちます。

- クラッシュ #：クラッシュイベントをログに記録するときに StarOS によって割り当てられた一意の番号
- SW バージョン：StarOS ビルドリリース形式：RR.n(bbbbb)
- 同様のクラッシュカウント：類似したクラッシュの数
- 最初のクラッシュ時刻：YYYY-MMM-DD+hh:mm:ss の形式で最初のクラッシュが発生したときのタイムスタンプ
- 失敗メッセージ：イベントメッセージのテキスト
- 関数：コード識別子
- プロセス：クラッシュが発生した場所（カード、CPU、PID など）
- クラッシュ時間：クラッシュが発生したときのタイムスタンプ（YYYY-MMM-DD+hh:mm:ss タイムゾーン）
- 最近の errno：最新のエラー番号のテキスト。
- スタック：メモリスタック情報
- ラストバウンス：クラッシュ前に受信したメッセージングに関する情報
- レジスタ：メモリレジスタの内容
- 現在の着信メッセージ：現在の着信メッセージの 16 進情報
- アドレス マップ
- 最近のヒープアクティビティ（最も古いもの）
- 最近のイベント（最も古いもの）
- プロファイルの深さ

各クラッシュログエントリの情報内容は、クラッシュのタイプと StarOS リリースによって異なります。

過剰なイベントロギングの削減

イベントロギング（evlogd）は、StarOS ファシリティによって送信されたイベントメッセージをキャプチャする共有メディアです。1 つまたは複数のファシリティが継続的に大量のイベントメッセージを送信し続けると、残りの通常に動作している機能が影響を受けます。このシナリオでは、特にログを生成するファシリティの数が増えるにつれて、システムパフォーマンスが低下していきます。

イベントメッセージロギングのレートコントロールは、ログの送信元パスで処理されます。基本的に、カウンタは秒ごとに 0 に設定され、evlogd に送信されたログイベントごとに増分します。1 秒未満でカウンタがしきい値に達すると、イベントは送信され、キューに入るか、または（evlogd メッセンジャキューがいっぱいの場合は）ドロップされます。

メッセージロギングのレートに対するこのコマンドで設定された上限しきい値を超過するファシリティがあり、同じ状態が長時間続く場合、StarOS は SNMP トラップまたはアラームを介してユーザーに通知します。

新しい threshold コマンドを使用すると、ユーザーはファシリティイベントキューを満杯とするパーセンテージを指定できます。このしきい値を超えると、問題のあるファシリティを指定する SNMP トラップとアラームが生成されます。

このコマンドに関連付けられている SNMP トラップの形式は次のとおりです。

- **ThreshLSLogsVolume**

```
<timestamp> Internal trap notification <trap_id> (ThreshLSLogsVolume) threshold
<upper_percent>%
measured value <actual_percent>% for facility <facility_name> instance <instance_id>
```

- **ThreshClearLSLogsVolume**

```
<timestamp> Internal trap notification <trap_id> (ThreshClearLSLogsVolume) threshold
 <upper_percent>%
measured value <actual_percent>% for facility <facility_name> instance <instance_id>
```

ポーリング間隔内にトリガー条件が発生した場合は、そのポーリング間隔が終了するまではアラートやアラームは生成されません。

両方のトラップを有効または抑制するには、グローバル構成モードの **snmp trap** コマンドを使用します。

ログソースのしきい値の設定

ログソースのしきい値の設定と実装に関連する 3 つのグローバル構成モードコマンドがあります。

1. **threshold ls-logs-volume**：トラップやアラームをそれぞれ生成およびクリアするための上限および下限しきい値のパラメータを設定します。
2. **threshold poll ls-logs-volume interval**：このしきい値のポーリング間隔を設定します。

3. **threshold monitoring ls-logs-volume** : このしきい値のモニタリングをオンまたはオフにします。

Syslog サーバーを設定するには、次の例を使用します。

```
configure
  [ default ] threshold ls-logs-volume upper_percent [ clear lower_percent ]
  [ default ] threshold poll ls-logs-volume interval duration
  [ no ] threshold monitoring ls-logs-volume
 end
```

注：

- *upper_percent* と *lower_percent* は、0 ～ 100 の整数として表わされます。*upper_percent* のデフォルト値は 90% です。*lower_percent* が指定されていない場合、デフォルトのクリア値は *upper_percent* です。
- **threshold poll ls-logs-volume interval** はポーリング間隔を秒単位で設定します。デフォルトの間隔は 300 秒（5 分）です。
- **threshold monitoring ls-logs-volume** はこの機能を有効または無効にします。

このしきい値の設定を確認するには、Exec モードの **show threshold** コマンドを実行します。

「設定の確認と保存」の章の説明に従って、設定を保存します。

ログのチェックポインティング

チェックポインティングは、ログに記録されたデータが以前に表示されたものか、マークされたものかを識別します。チェックポインティングを使用すると、最後のチェックポイント以降のログ情報のみを表示できます。

個々のログには、アクティブログに最大 50,000 のイベントが含まれている場合があります。ログのチェックポイントを実行すると、最大 50,000 のイベントが非アクティブなログファイルに記録されます。これにより合計で最大 100,000 イベントとなり、これらはログに記録された各ファシリティで使用できます。

Exec モードの logs checkpoint コマンドを使用してログデータのチェックポインティングを実行し、特別なアクティビティが発生する前にログの内容を既知のポイントに設定します。また、このコマンドを定期メンテナンスの一環として含めて、ログデータを管理することもできます。

ログのチェックポインティングでは、現在のログデータを非アクティブなログに移動します。最後にチェックポインティングされたデータが、非アクティブログに保持されます。後続のログのチェックポインティングによって、以前にチェックポインティングされた非アクティブなログデータがクリアされ、新たにチェックポインティングされたデータに置き換えられます。チェックポインティングされたログデータは表示できません。

重要 ログファイルがいっぱいになるのを防ぐために、ログのチェックポインティングを定期的に実行する必要があります。50,000 のイベントが記録されたログは、新しいイベントがログに記録されると、最も古いイベントを最初に破棄します。

重要 インスペクタレベルの管理ユーザーは、このコマンドを実行できません。

ログファイルの保存

ログファイルは、URL で指定されたローカルまたはリモートの場所にあるファイルに保存できます。ログファイルを保存するには、次の Exec モードコマンドを使用します。

save logs { *url* } **[active] [inactive] [callid** *call_id* **] [event-verbosity** *evt_verboseness* **] [facility** *facility* **] [level** *severity_level* **] [pdu-data** *pdu_format* **] [pdu-verbosity** *pdu_verboseness* **] [since** *from_date_time* **[until** *to_date_time* **]] [| { grep** *grep_options* **| more }]**

save logs コマンドの詳細については、『*Command Line Interface Reference*』の「*Exec Mode Commands*」の章を参照してください。

イベント ID の概要

重要 イベント ID の使用は、プラットフォームのタイプとプラットフォームで実行されているライセンスによって異なります。

識別番号（ID）は、システムでロギングが有効になっている場合に発生するイベントを参照するために使用されます。前述したように、ログはファシリティごとに収集されます。各ファシリティには、次の表に示すように、独自の範囲のイベント ID があります。

表 *2:* システムファシリティとイベント *ID* の範囲

ファシリティ	説明	イベント ID の範
a10	A10 プロトコルファシリティ	28000 ～ 28999
a11	A11 プロトコルファシリティ	29000 ～ 29999
a11mgr	A11 マネージャファシリティ	9000 ～ 9999
aaa-client	AAA クライアントファシリティ	6000 ～ 6999
aaamgr	AAA マネージャファシリティ	36000 ～ 36999

ファシリティ	説明	イベント ID
aaaproxy	AAA プロキシファシリティ	64000 ～ 649
aal2	AAL2 プロトコルファシリティ	173200 ～ 17
acl-log	IP アクセスコントロールリスト（ACL）ファシリティ	21000 ～ 219
acsctrl	アクティブ チャージング サービス コントローラ（ACSCtrl）ファシリティ	90000 ～ 909
acsmgr	アクティブ チャージング サービス マネージャ（ACSMgr）ファシリティ	91000 ～ 919
afctrl	Ares ファブリックコントローラ（ASR 5500 のみ）	186000 ～ 18
afmgr	Ares Fabric Manager（ASR 5500 のみ）	187000 ～ 18
alarmctrl	アラーム コントローラ ファシリティ	65000 ～ 659
alcap	Access Link Control Application Part（ALCAP）プロトコルファシリティ	160900 ～ 16
alcapmgr	ALCAP マネージャファシリティ	160500 ～ 16
asf	ASF ファシリティ	73000 ～ 739
asfprt	ASFPRT ファシリティ	59000 ～ 599
asngwmgr	アクセス サービス ネットワーク（ASN）ゲートウェイ マネージャ ファシリティ	100000 ～ 10
asnpcmgr	ASNページング/ロケーション レジストリ マネージャ ファシリティ	100500 ～ 10
bcmcs	ブロードキャスト/マルチキャストサービス（BCMCS）ファシリティ	109000 ～ 10
bfd	Bidirectional Forwarding Detection（BFD）プロトコルファシリティ	170500 ～ 17
bgp	ボーダー ゲートウェイ プロトコル（BGP）ファシリティ	85000 ～ 859
bindmux	BindMux マネージャ ファシリティ [インテリジェントポリシー制御機能（IPCF）]	158200 ～ 15
bngmgr	ブロードバンドネットワーク ゲートウェイ（BNG）マネージャファシリティ	182000 ～ 18
bssap	Base Station System Application Part+（BSSAP+）サービスファシリティ	131000 ～ 13
bssgp	Base Station System GPRS Protocol（BSSGP）ファシリティ	115050 ～ 11
callhome	Call Home ファシリティ	173600 ～ 17
cap	CAMEL Application Part（CAP）ファシリティ	87900 ～ 880
chatconf	CHATCONF ファシリティ	74000 ～ 749

ファシリティ	説明	イベント ID の範
cli	CLI（コマンドラインインターフェイス）のロギングファシリティ	30000 ～ 30999
connproxy	接続プロキシファシリティ	190000 ～ 19099
crdt-ctl	クレジット制御ファシリティ	127000 ～ 12799
csg	Closed Subscriber Groups（CSG）ファシリティ	188000 ～ 18899
csg-acl	CSG アクセスコントロールリスト（ACL）ファシリティ	189000 ～ 18999
csp	カード/スロット/ポート（CSP）ファシリティ	7000 ～ 7999
css	コンテンツ ステアリング サービス（CSS）ファシリティ [ESC]	77000 ～ 77499
css-sig	コンテンツ サービス セレクション（CSS）RADIUS シグナリング ファシリティ	77500 ～ 77599
cx-diameter	Cx Diameter メッセージファシリティ	92840 ～ 92849
dcardctrl	ドーターカードコントローラファシリティ	62000 ～ 62999
dcardmgr	ドーターカード マネージャ ファシリティ	57000 ～ 57999
demuxmgr	Demux マネージャファシリティ	110000 ～ 11099
dgmbmgr	Diameter Gmb（DGMB）アプリケーションマネージャ ファシリティ	126000 - 126999
dhcp	DHCP ファシリティ	53000 ～ 53999
dhcpv6	DHCPv6 プロトコルファシリティ	123000 ～ 12399
dhost	分散型ホストマネージャファシリティ	83000 ~ 83999
diameter	Diameter エンドポイントファシリティ	92000 ～ 92599
diabase	Diabase メッセージファシリティ	92800 ～ 92809
diameter-acct	Diameter アカウンティング プロトコル ファシリティ	112000 ～ 11299
diameter-auth	Diameter 認証プロトコルファシリティ	111000 ～ 11199
diameter-dns	Diameter DNS サブシステムファシリティ	92600 ～ 92699
diameter-ecs	ECS Diameter シグナリングファシリティ	81990 ～ 81999
diameter-hdd	Diameter Horizontal Directional Drilling（HDD）インターフェイス ファシリティ	92700-92799
diameter-svc	Diameter サービスファシリティ	121200 ～ 12199
diamproxy	Diameter プロキシファシリティ	119000 ～ 11999
dpath	IPSec ファシリティのデータパス	54000 ～ 54999
drvctrl	ドライバ コントローラ ファシリティ	39000 ～ 39999

ファシリティ	説明	イベント ID
ds3mgr	DS3 および DS3/E ラインカード マネージャ ファシリティ（NPU マネージャ コントローラ ファシリティの一部）	40000 ～ 409
eap-diameter	Extensible Authentication Protocol（EAP; 拡張可能認証プロトコル）Diameter ファシリティ	92870 ～ 928
eap-ipsec	EAP IPSec ファシリティ	118000 ～ 118
ecs-css	ACS セッション マネージャ（ACSMgr）シグナリング インターフェイス ファシリティ	97000 ～ 970
edr	イベント データ レコード（EDR）ファシリティ	80000 ～ 809
egtpc	eGTP-C ファシリティ	141000 ～ 14
egtpmgr	eGTP マネージャ ファシリティ	143000 ～ 14
egtpu	eGTP-U ファシリティ	142000 ～ 14
epdg	Evolved Packet Data Gateway（ePDG）ファシリティ	178000 ～ 17
evlog	イベント ログ ファシリティ	2000 ～ 2999
famgr	外部エージェント（FA）マネージャ ファシリティ	33000 ～ 339
ファイアウォール	ファイアウォール機能	96000 ～ 969
fng	フェムト ネットワーク ゲートウェイ（FNG）ファシリティ	149000 ～ 14
gbrmgr	Gb-Manager ファシリティ	201900 ～ 20
gcdr	GGSN 課金データ レコード（G-CDR）ファシリティ	66000 ～ 669
gmm	GPRS Mobility Management（GMM）ファシリティ	88100 ～ 882
gprs-app	General Packet Radio Service（GPRS）アプリケーション ファシリティ	115100 ～ 11
gprs-ns	GPRS-NS プロトコル ファシリティ	115000 ～ 11
gq-rx-tx-diameter	Gq/Rx/Tx Diameter メッセージ ファシリティ	92830 ～ 928
gss-gcdr	GTPP ストレージ サーバーの GCDR ファシリティ	98000 ～ 980
gtpc	GTPC プロトコル ファシリティ	47000 ～ 479
gtpcmgr	GTPC シグナリング デマルチプレクサ マネージャ ファシリティ	46000 ～ 469
gtpp	GTP-PRIME プロトコル ファシリティ	52000 ～ 529
gtpu	GTPU プロトコル ファシリティ	45000 ～ 459
gtpumgr	GTPU マネージャ ファシリティ	157200 ～ 15
gx-ty-diameter	Gx/Ty Diameter メッセージ ファシリティ	92820 ～ 928
gy-diameter	Gy Diameter メッセージ ファシリティ	92810 ～ 928

ファシリティ	説明	イベント ID の範
h248prt	H.248 プロトコルファシリティ	42000 - 42999
hamgr	ホームエージェント（HA）マネージャファシリティ	34000 ～ 34999
hat	高可用性タスク（HAT）ファシリティ	3000 ～ 3999
hdctrl	ハードディスク（HD）コントローラファシリティ	132000 ～ 13299
hddshare	HDD 共有ファシリティ	184000 ～ 18499
henb-gw	Home eNodeB-GW ファシリティ	195000 ～ 19599
henbapp	Home eNodeB アプリケーションファシリティ	196000 ～ 19699
henbgwdemux	Home eNodeB-GW Demux ファシリティ	194000 ～ 19499
henbgwmgr	Home eNodeB-GW マネージャファシリティ	193000、193999
hnb-gw	Home NodeB（HNB）ゲートウェイファシリティ	151000 ～ 15199
hnbmgr	HNB マネージャファシリティ	158000 ～ 15819
hss-peer-service	ホーム サブスクライバ サーバー（HSS）ファシリティ [MME]	138000 ～ 13899
igmp	Internet Group Management Protocol（IGMP）	113000 ～ 11399
ikev2	IKEv2 ファシリティ	122000 ～ 12299
ims-authorizatn	IMS 承認サービス ライブラリ ファシリティ	98100 ～ 98999
ims-sh	IMS SH ライブラリファシリティ	124000 ～ 12499
imsimgr	International Mobile Subscriber Identity（IMSI）マネージャファシリティ	114000 ～ 11499
imsue	IMS User Equipment（IMSUE）ファシリティ	144000 ～ 14599
ip-arp	IP Address Resolution Protocol（ARP）ファシリティ	19000 ～ 19999
ip-interface	IP インターフェイスファシリティ	18000 ～ 18999
ip-route	IP ルートファシリティ	20000 ～ 20999
ipms	インテリジェント パケット モニタリング システム（IPMS）ファシリティ	134000 ～ 13499
ipne	IP Network ENABLER（IPNE）ファシリティ	192000 ～ 19299
ipsec	IPSec プロトコルファシリティ	55000 ～ 56998
ipsg	IP サービスゲートウェイ（IPSG）ファシリティ	128000 ～ 12899
ipsgmgr	IPSG マネージャ（IPSGMgr）ファシリティ	99000 ～ 99999
ipsp	IP プール共有プロトコル（IPSP）ファシリティ	68000 ～ 68999
kvstore	Key/Value ストア（kvstore）ファシリティ	125000 ～ 12599

ファシリティ	説明	イベント ID
l2tp-control	L2TP Control PDU Protocol ファシリティ	50000 ～ 509
l2tp-data	L2TP Data PDU Protocol ファシリティ	49000 ～ 499
l2tpdemux	L2TP Demux ファシリティ	63000 ～ 639
l2tpmgr	L2TP マネージャファシリティ	48000 ～ 489
lagmgr	Link Aggregation GROUP（LAG）マネージャファシリティ	179000 ～ 17
ldap	Lightweight Directory Access Protocol（LDAP）リクエストファシリティ	160000 ～ 16
li	合法的傍受（LI）ログファシリティ	69000 ～ 699
linkmgr	リンク マネージャ ファシリティ	89500 ～ 899
llc	論理リンク制御（LLC）レイヤファシリティ（GPRS）	115700 ～ 11
local-policy	ローカルポリシー設定ファシリティ	161400 ～ 16
m3ap	M3 アプリケーション プロトコル（M3AP）ファシリティ	211500 ～ 21
m3ua	MTP レベル 3（M3UA）プロトコルファシリティ [SIGTRAN]	87500 ～ 876
magmgr	モバイル アクセス ゲートウェイ（MAG）マネージャファシリティ	137500 ～ 13
map	モバイル アプリケーション パート（MAP）プロトコルファシリティ [SS7]	87100 ～ 872
megadiammgr	MegaDiameter マネージャファシリティ	121000 ～ 12
mme-app	モビリティマネージメントエンティティ（MME）アプリケーションファシリティ	147000 ～ 14
mme-embms	MME evolved Multimedia Broadcast Multicast Service（eMBMS）ファシリティ	212000 ～ 21
mme-misc	MME その他のファシリティ	155800 ～ 15
mmedemux	MME Demux マネージャファシリティ	154000 ～ 15
mmemgr	MME マネージャファシリティ	137000 ～ 13
mmgr	マスターマネージャ（MMGR）ファシリティ	86000 ～ 863
mobile-ip	モバイル IP（MIP）プロトコルファシリティ	26000 ～ 269
mobile-ip-data	MIP トンネルデータファシリティ	27000 ～ 279
mobile-ipv6	モバイル IPv6 ファシリティ	129000 ～ 12
mpls	マルチ プロトコル ラベル スイッチング（MPLS）ファシリティ	163500 ～ 16

ファシリティ	説明	イベント ID の範
mseg-app	Mobile Services Edge Gateway（MSEG）アプリケーション ファシリティ 本リリースではサポートされていません。	172300 ～ 17299
mseg-gtpc	MSEG GTPC アプリケーション ファシリティ 本リリースではサポートされていません。	172000 ～ 17219
mseg-gtpu	MSEG GTPU アプリケーション ファシリティ 本リリースではサポートされていません。	172200 ～ 17229
msegmgr	MSEG マネージャファシリティ 本リリースではサポートされていません。	171000 ～ 17199
mtp2	Message Transfer Part 2（MTP2）サービスファシリティ [SS7]	116900 ～ 11699
mtp3	Message Transfer Part 3（MTP3）サービスファシリティ [SS7]	115600 ～ 11569
multicast-proxy	マルチキャスト プロキシ ファシリティ	94000 ～ 94999
nas	ネットワーク アクセス シグナリング（NAS）ファシリティ	153000 ～ 15399
netwstrg	ネットワーク ストレージ ファシリティ	78000 ～ 78999
npuctrl	ネットワーク処理ユニット（NPU）制御ファシリティ	16000 ～ 16999
npudrv	NPU ドライバファシリティ	191000 ～ 19199
npumgr	NPU マネージャ（NPUMGR）ファシリティ	17000 ～ 17999
npumgr-acl	NPUMGR ACL ファシリティ	169000 ～ 16999
npumgr-drv	NPUMGR ドライバファシリティ	185000 ～ 18599
npumgr-flow	NPUMGR フローファシリティ	167000 ～ 16799
npumgr-fwd	NPUMGR 転送ファシリティ	168000 ～ 16899
npumgr-init	NPUMGR 初期化ファシリティ	164000 ～ 16499
npumgr-lc	NPUMGR LC ファシリティ	180000 ～ 18099
npumgr-port	NPUMGR ポートファシリティ	166000 ～ 16699
npumgr-recovery	NPUMGR リカバリファシリティ	165000 ～ 16599
npumgr-vpn	NPUMGR VPN ファシリティ	181000 ～ 18199
npusim	NPUSIM ファシリティ	176000 ～ 17699
ntfy-intf	イベント通知インターフェイス ファシリティ	170000 ～ 17049
orbs	orbs：オブジェク リクエスト ブローカ（ORB）システムファシリティ	15000 ～ 15999

ファシリティ	説明	イベント ID
ospf	Open Shortest Path First（OSPF）プロトコルファシリティ	38000 ～ 389
ospfv3	OSPFv3 プロトコルファシリティ [IPv6]	150000 ～ 15
p2p	ピアツーピア（P2P）ファシリティ	146000 ～ 14
pccmgr	Policy Charging and Control（PCC）マネージャファシリティ	159000 ～ 15
pdg	Packet Data Gateway（PDG）ファシリティ	152010 ～ 15
pdgdmgr	PDG TCP Demux Manager（pdgdmgr）ファシリティ（顧客固有のファシリティ）	162400 ～ 16
pdif	Packet Data Interworking Function（PDIF）ファシリティ	120000 ～ 12
pgw	Packet Data Network Gateway（PGW）ファシリティ	139000 ～ 13
phs	Personal Handyphone System（PHS）ファシリティ	177000 ～ 17
phs-control	PHS X1/X5 および X2/X6 インターフェイスファシリティ	136000 ～ 13
phs-data	PHS データファシリティ	136900 ～ 13
phs-eapol	PHS EAP over LAN（EAPOL）ファシリティ	136980 ～ 13
phsgwmgr	PHS ゲートウェイ マネージャ ファシリティ	135000 ～ 13
phspcmgr	PHS ページング コントローラ マネージャ ファシリティ	135500 ～ 13
pmm-app	パケット モビリティ マネージメント（PMM）アプリケーション ファシリティ [SGSN]	89200 ～ 894
ppp	Point-To-Point Protocol（PPP）ファシリティ	25000 ～ 259
pppoe	Point-to-Point Protocol over Ethernet（PPPoE）ファシリティ	183000 ～ 18
ptt	PTT ファシリティ	76000 ～ 769
push	PUSH（VPNMgr CDR Push）ファシリティ	133000 ～ 13
radius-acct	RADIUS アカウンティング プロトコル ファシリティ	24000 ～ 249
radius-auth	RADIUS 認証プロトコルファシリティ	23000 ～ 239
radius-coa	RADIUS 許可の変更（CoA）と接続解除ファシリティ	70000 ～ 709
ranap	Radio Access Network Application Part（RANAP）ファシリティ	87700 ～ 878
rct	リカバリ制御タスク（RCT）ファシリティ	13000 ～ 139
rdt	リダイレクタタスク（RDT）ファシリティ	67000 ～ 679
resmgr	Resource Manager (RM) ファシリティ	14000 ～ 149
rf-diameter	Rf Diameter メッセージファシリティ	92860 ～ 928
rip	Routing Information Protocol（RIP）ファシリティ	35000 ～ 359

ファシリティ	説明	イベント ID の範
rohc	Robust Header Compression（ROHC）プロトコルファシリティ	103000 ～ 10399
rsvp	RSVP プロトコルファシリティ	93000 ～ 93999
rua	RANAP User Adaptation（RUA）プロトコルファシリティ	152000 ～ 15200
s1ap	S1 アプリケーション プロトコル（S1AP）ファシリティ	155200 ～ 15579
saegw	System Architecture Evolution ゲートウェイファシリティ	191000 ～ 19199
sccp	Signalling Connection Control Part（SCCP）プロトコルファシリティ [SS7]	86700 ～ 86899
sct	共有設定タスク（SCT）ファシリティ	32000 ～ 32099
sctp	Stream Control Transmission Protocol（SCTP）プロトコルファシリティ	87300 ～ 87499
sess-gr	SESS-GR ファシリティ	77600 ～ 77999
sessctrl	セッション コントローラ ファシリティ	8000 ～ 8999
sessmgr	セッション マネージャ ファシリティ	10000 ～ 12999
sesstrc	セッション トレース ファシリティ	155000 ～ 15519
sft	スイッチファブリックタスク（SFT）ファシリティ	58000 ～ 58999
sgs	SG インターフェイスプロトコルファシリティ [MME]	173000 ～ 17319
sgsn-app	SGSN アプリケーション インターフェイス ファシリティ	115900 ～ 11599
sgsn-failures	SGSN コール失敗ファシリティ	89100 ～ 89199
sgsn-gtpc	SGSN GTP-C プロトコルファシリティ	116000 ～ 11659
sgsn-gtpu	SGSN GTP-U プロトコルファシリティ	86900 ～ 87099
sgsn-mbms-bearer	SGSN MBMS ベアラーアプリケーション（SMGR）ファシリティ	116600 ～ 11679
sgsn-misc	SGSN その他のファシリティ	88800 ～ 89099
sgsn-system	SGSN システム コンポーネント ファシリティ	86400 ～ 86499
sgsn-test	SGSN テストファシリティ	88700 ～ 88799
sgsn2	SGSN2 ファシリティ	114000 ～ 11799
sgtpcmgr	SGSN GTP-C（SGTPC）マネージャファシリティ	117000 ～ 11799
sgw	サービングゲートウェイ（SGW）ファシリティ	140000 ～ 14099
sh-diameter	Sh Diameter メッセージファシリティ	92850 ～ 92859
sipcdprt	SIPCDPRT ファシリティ	95000 ～ 95999
sitmain	システム開始タスク（SIT）メインファシリティ	4000 ～ 4999

ファシリティ	説明	イベント ID
sm-app	ショート メッセージ サービス（SMS）ファシリティ	88300 ～ 884
sms	SMS サービスファシリティ	116800 ～ 11
sndcp	Sub Network Dependent Convergence Protocol（SNDCP）ファシリティ	115800 ～ 11
snmp	Simple Network Management Protocol（SNMP）ファシリティ	22000 ～ 229
sprmgr	Subscriber Policy Register（SPR）マネージャファシリティ	159500 ～ 15
srdb	スタティック評価データベースファシリティ	102000 ～ 10
srp	サービス冗長性プロトコル（SRP）ファシリティ	84000 ～ 849
sscfnni	SSCFNNI プロトコルファシリティ [ATM]	115500 ～ 11
sscop	SSCOP Protocol ファシリティ [ATM]	115400 ～ 11
ssh-ipsec	SSH IP セキュリティファシリティ	56999 ～ 569
ssl	SSL ファシリティ（顧客固有のファシリティ）	156200 ～ 15
stat	統計情報ファシリティ	31000 ～ 319
system	システムファシリティ	1000 ～ 1999
tacacs+	TACACS+ プロトコルファシリティ	37000 ～ 379
taclcp	TACLCP ファシリティ	44000 ～ 449
tcap	Transaction Capabilities Application Part（TCAP）プロトコルのロギングファシリティ [SS7]	86500 ～ 866
testctrl	テスト コントローラ ファシリティ	174000 ～ 17
testmgr	テスト マネージャ ファシリティ	175000 ～ 17
threshold	しきい値ファシリティ	61000 ～ 619
ttg	Tunnel Termination Gateway（TTG）ファシリティ	130000 ～ 13
tucl	TCP/UDP コンバージェンスレイヤ（TUCL）ファシリティ [SS7]	88500 ～ 886
udr	ユーザーデータレコード（UDR）ファシリティ	79000 ～ 799
user-data	ユーザーデータファシリティ	51000 ～ 519
user-l3tunnel	ユーザー L3 トンネルファシリティ	75000 ～ 759
usertcp-stack	ユーザー TCP スタックファシリティ	173300 ～ 17
vim	ボイス インスタント メッセージ（VIM）ファシリティ	60000、6099
vinfo	VINFO ファシリティ	82000、8299
vmgctrl	仮想メディアゲートウェイ（VMG）コントローラファシリティ	41000、4199
vmgctxmgr	VMG コンテキスト マネージャ ファシリティ	43000、4399

ファシリティ	説明	イベント ID の範
vpn	バーチャル プライベート ネットワーク（VPN）ファシリティ	5000 ～ 5999
wimax-data	WiMAX データファシリティ	104900 ～ 10499
wimax-r6	WiMAX R6 プロトコル（シグナリング）ファシリティ	104000 ～ 10489

イベントのシビラティ（重大度）

システムにより、ロギングが有効になっている場合に表示される情報のレベルを柔軟に設定できます。次のレベルがサポートされます。

- **クリティカル**：システムまたはシステムのコンポーネントの機能を停止させる重大なエラーが発生したことをログに記録します。これが最高のシビラティ（重大度）レベルです。
- **エラー**：システムまたはシステムのコンポーネントの動作を低下させるエラーが発生したことをログに記録します。このレベルは、シビラティ（重大度）レベルが高いイベントもログに記録します。
- **警告**：潜在的な問題を示す可能性があるイベントをログに記録します。このレベルは、シビラティ（重大度）レベルが高いイベントもログに記録します。
- **異常**：きわめて異常であり、調査する必要がある可能性のあるイベントをログに記録します。このレベルは、シビラティ（重大度）レベルが高いイベントもログに記録します。
- **情報**：シビラティ（重大度）がより高い情報イベントおよびイベントをログに記録します。
- **トレース**：トレースに役立つイベントやより高いシビラティ（重大度）を持つイベントをログに記録します。
- **デバッグ**：シビラティ（重大度）に関係なく、すべてのイベントをログに記録します。

上記のレベルはそれぞれ、イベント ID の「シビラティ（重大度）」レベルに対応します。したがって、「シビラティ（重大度）」レベルがロギングレベルと等しいイベント ID のみが表示されます。

ログ出力のイベント ID 情報の概要

この項では、ロギングが有効になっておりときに表示されるイベント情報について説明します。

次に、ログに記録されたイベントの出力例を示します。

```
2011-Dec-11+5:18:41.993 [cli 30005 info] [8/0/609 cli:8000609 _commands_cli.c:1290]
[software internal system] CLI session ended for Security Administrator admin on device
 /dev/pts/2
```

次の表で、出力例に含まれている要素について説明します。

表 *3:* イベント要素の説明

要素	説明
2011-Dec-11+5:18:41.993	イベントが生成された日時を示す日付/タイムスタンプ
[cli 30005 info]	以下を含むイベントに関する情報 • イベントが属している機能 • イベント ID • イベントのシビラティ（重大度） この例では、イベントはCLIファシリティに属しており ID は 3005、シビラティ（重大度）は「info」です。
[8/0/609 cli:8000609 _commands_cli.c:1290]	特定の CLI インスタンスに関する情報。
[software internal system]	イベントの発生原因がシステムの動作であることを示しいます。
CLI session ended for Security Administrator admin on device /dev/pts/2	イベントの詳細。イベントの詳細には、イベントの発生固有の変数が含まれている場合と含まれない場合があります。

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。