ロギング サポート

Cisco Unified Border Element（SP Edition）は、ログを扱うためのさまざまな機能を提供します。ロギングは、指定した条件下でログが生成されるように設定できます。ログは、オン デマンドでも生成できます。ログから得られる情報は、ネットワークの操作に関する問題の分析やトラブルシューティング、ネットワークの改善に関する領域の特定などに使用できます。

Cisco Unified Border Element（SP Edition）は、以前は Integrated Session Border Controller と呼ばれており、このマニュアルでは通常 Session Border Controller（SBC; セッション ボーダー コントローラ）と呼びます。

本章で使用されているコマンドの詳細な説明については、次の場所にある『*Cisco Unified Border Element (SP Edition) Command Reference: Unified Model*』を参照してください。

http://www.cisco.com/en/US/docs/ios/sbc/command/reference/sbcu_book.html

すべての Cisco IOS コマンドの詳細については、http://tools.cisco.com/Support/CLILookup にある Command Lookup Tool を使用するか、Cisco IOS マスター コマンド リストを参照してください。

ロギング サポートの機能履歴

リリース	変更内容
Cisco IOS XE Release 2.x	syslog 機能は、Cisco IOS XE Release 3.1S 以前のリリースで導入されました。
Cisco IOS XE Release 3.5S	相関 ID を使用してリンクされる特定のコールに関連付けられたすべての相関ログをイネーブルにできるように、コール ログ相関機能が導入されました。 アラーム機能がアラーム ログを処理する新機能を含むように強化されました。

内容

この章の内容は、次のとおりです。

syslog 機能

コンソールに表示されるすべての Cisco Unified Border Element（SP Edition）デバッグ メッセージは、Cisco IOS の syslog に記録されます。ログ サイズ、パーシステンス、リダイレクションを設定するすべての Cisco IOS syslog コマンドが、syslog を管理するために使用できます。

コンソール メッセージに加え、Cisco Unified Border Element（SP Edition）は、独自の内部バッファにログを記録します。これは問題判別ログと呼ばれ、ソフトウェアの強制リロードが行われた場合や、**sbc dump-diagnostics** コマンドを使用した結果として保存されます。問題レポートを作成する場合、問題判別ログ ファイルは問題のレポートの一部として含まれています。

内部ログ レベル

セッション ボーダ コントローラ（SBC）アプリケーションは、コンソールと問題判別ログの詳細の制御に内部ログ レベルを使用します。コンソールおよび問題判別ログ レベルはいずれも個別に変更できますが、問題判別ログ バッファのサイズは制限されており、重要なログが失われる可能性があるため、問題判別ログ レベルを変更することは推奨しません。

デフォルトの SBC 問題判別ログ レベルはコンソールでは 63、バッファでは 60 です。**debug sbc log-level console** コマンド、**debug sbc log-level filter** コマンド、または **debug sbc log-level buffer** コマンドを使用して、デフォルトの SBC 問題判別ログ レベルを変更できます。

ログ レベル	Syslog レベル
90	Fatal
80	Error
70	Unexpected
63	Configuration Error
60	Operational
50	Audit
40	Statistics
30	Verbose Operational
20	Verbose Statistics
10	Internal Diagnostic

syslog 機能のイネーブル化

SBC の syslog 機能をイネーブルにするには、内部ログ レベルを設定し、syslog 固有のロギング コマンドを実行します。次の例では、デフォルトの問題判別ログ レベルが 63（最初の再起動である場合はそれ以上のアクションは不要）を前提としています。

1. 次のコマンドを使用してロギングをイネーブルにします。

```
Router# configure
Router(config)# logging enable
Router(config)# logging standby
```

（注） **logging standby** コマンドにより、アクティブとスタンバイの syslog 設定を同期できます。

2. syslog メッセージの送信先を設定します。場所には、次のいずれかを設定できます。
   - コンソール：logging console <1 ～ 7>

     ```
     Router(config)# logging console severity-level
     ```
   - バッファ：logging buffer <1 ～ 7>

     ```
     Router(config)# logging buffered severity-level
     ```

     （注） ロギング統計情報およびロギング バッファを表示するには、**show logging** コマンドを使用します。ロギング バッファをクリアするには、**clear logging** コマンドを使用します。
   - syslog サーバ：logging trap <1 ～ 7>

     ```
     Router(config)# logging host ip_address [tcp[/port] | udp[/port]]
     Router(config)# logging trap severity-level
     Router(config)# logging device-id {hostname | ipaddress interface_name | string
     text | context-name}
     Router(config)# logging facility number
     ```

     （注） **logging device-id** コマンドを使用すると、ログをリモート サーバに送信するときに syslog メッセージをカスタマイズできます。
   - telnet セッション：logging monitor <1 ～ 7>

     ```
     Router(config)# logging monitor severity-level
     Router# terminal monitor
     ```
   - SNMP 管理ステーション：logging history <1 ～ 7>

     ```
     Router(config)# logging history severity-level
     ```
   - スーパーバイザ：logging supervisor <1 ～ 7>

     ```
     Router(config)# logging supervisor severity-level
     ```

3. syslog メッセージ固有の操作を設定：

```
Router(config)# logging message syslog_id [level severity_level]
Router# show logging message
Router# clear logging
```

4. syslog のグローバルな設定：

```
Router(config)# logging queue queue-size
Router# show logging queue
Router(config)# logging timestamp
Router(config)# logging rate-limit {num {interval | level severity_level |
message syslog_id} | unlimited {level severity_level | message syslog_id}}
Router# show logging
```

コール ログ相関

コール ログ相関機能により、相関 ID を使用してリンクされる特定のコールに関連付けられたすべての相関ログをイネーブルにできます。この機能を使用して、特定のコールのログについて、リアルタイム フィルタリングを行うこともできます。各 SIP コール、REGISTER、SUBSCRIBE、または NOTIFY メッセージに、64 ビットの診断コリレータが割り当てられます。

次のパラメータに基づいてフィルタを設定できます。

- ダイヤルまたはダイヤル番号
- Session Initiation Protocol（SIP）Universal Resource Identifier（URI; ユニバーサル リソース識別子）
- リモート シグナリング アドレス
- リモート VPN ID
- 隣接
- VRF

指定したフィルタ タイプと一致するログが、単独の問題判別のトレース ファイルと Inter Process Signal（IPS: プロセス間シグナル）トレース ファイルに保存されます。

相関ログ フィルタをイネーブルにするには、次のコマンドを使用します。

debug sbc *sbc-name* correlation-logs filter *filter-name* **[pdtrc-log-level** *value***]**

相関ログ フィルタをディセーブルにするには、次のコマンドを使用します。

no debug sbc *sbc-name* correlation-logs filter *filter-name*

デバッグ ログ、フィルタ、ログ レベルを表示するには、次のコマンドを使用します。

show debugging

問題判別ログ レベル

debug sbc *sbc-name* **correlation-logs filter** *filter-name* **[pdtrc-log-level** *value***]** コマンドの **pdtrc-log-level** オプションを使用して、フィルタに問題判別レベルを設定できます。問題判別トレース ログ レベルの範囲は 0 ～ 100 です。デフォルトのログ レベルは 60 です。ログ レベル 100 は、ログを 1 つも出力しないことを示し、0 はすべてのログを出力することを示します。

表 1 に、問題判別ログ レベルの一覧を示します。

表 1　　問題判別ログ レベル

問題判別ログ レベル	説明
90	クリティカルなシステム エラー
80	メジャーなシステム エラー
70	マイナーなシステム エラー
63	設定エラー
60	コール エラー
55	コール概要
50	コール詳細
40	コール統計情報
30	処理詳細
20	統計情報詳細
10	内部診断

コール ログ相関機能の例

次の例では、相関ログをフィルタリングするためのさまざまなフィルタを示します。

```
Router# debug sbc test correlation-logs filter ?

    adjacency                 Adjacency, matching calls to or from this adjacency
    dn                        Dialed/dialing number,matching calls to or from this number
    remote-signalling-address Remote signalling address matching to or from this address
    sip-uri                   SIP-URI, matching calls to or from this URI
    vrf                       VRF name
```

次の例では、隣接パラメータに基づく相関ログのフィルタリングを示します。

```
Router# debug sbc test correlation-logs filter adjacency abc
    Debugging filter log-level set to default level 60

Router# show debugging
    SBC correlator filter Adjacency name is abc
    IpsTracing is enabled
```

次の例では、ダイヤル番号パラメータに基づく相関ログのフィルタリングを示します。

```
Router# debug sbc test correlation-logs filter dn aa

    Debugging filter log-level set to default level 60

Router# show debugging

    SBC correlator filter DN is aa
```

```
    IpsTracing is enabled
```

次の例では、リモート シグナリング アドレス パラメータに基づく相関ログのフィルタリングを示します。

```
Router# debug sbc test correlation-logs filter remote-signalling-address ipv4 192.0.2.1

    Debugging filter log-level set to default level 60

Router# show debugging

    SBC buffer log-level is 0
    SBC correlator
    Filter Remote signalling-address ipv4 address is 192.0.2.1
    IpsTracing is enabled
    SBC correlator
    Filter DN is abc
    Pd loglevel is 70
    IpsTracing is enabled
```

次の例では、SIP URI パラメータに基づく相関ログのフィルタリングを示します。

```
Router# debug sbc test correlation-logs filter sip-uri ccc
    Debugging filter log-level set to default level 60

Router# show debugging

    SBC correlator filter Adjacency name is abc
    IpsTracing is enabled
    SBC correlator filter Remote signalling-address ipv4 address is 192.0.2.1
    IpsTracing is enabled
    SBC correlator filter SIP-URI is ccc
    IpsTracing is enabled
    SBC correlator filter DN is aa
    IpsTracing is enabled
```

次の例では、VRF パラメータに基づく相関ログのフィルタリングを示します。

```
Router# debug sbc test correlation-logs filter vrf new ipv4 rsa 192.0.2.1 pdtrc-log-level
70

    Debugging filter log-level set to default level 60

Router# show debugging

    SBC correlator Filter Remote signalling-address ipv4 address is 192.0.2.1
    SBC correlator Filter VRF is new with Vpn(id) = 3
    Pd loglevel is 70
    IpsTracing is enabled
    SBC correlator Filter SIP-URI is 9.0.0.0
    Pd loglevel is 0
    IpsTracing is enabled
```

アラーム ログ

SBC の動作に関するさまざまなタイプのイベントのアラームを生成するように SBC を設定できます。また、システムの機能を監視し、調整に使用できるデバッグ情報を記録するように SBC を設定できます。アラームに基づいて、SBC がビジネス要件に従って動作を続行するための是正措置、予防処置を実行できます。長時間にわたって、SBC によって生成されたアラームを監視し、この情報を分析することも重要です。この要件に対応するため、アラーム ログを生成、表示、保存するように SBC を設定できます。アラーム ログに表示された情報は、相互運用性の問題や不正な設定など、一般的な問題の

解決に役立ちます。これらのログは、専門のサポート スタッフが、エスカレーションや調査が必要となる可能性のある問題を特定するためにも使用できます。ログ情報を使用して、システム全体の効率を改善できます。

（注） すべてのアラーム ログ情報はルート プロセッサのフェールオーバー後に失われます。

アラーム ログを設定するには、次のコマンドのいずれかを組み合わせて使用します。

- アラーム ログを生成する必要があるアラーム タイプを指定するデバッグには、**debug sbc alarm-filter** コマンドを使用します。
- アラームをログに記録する出力モードとアラームの重大度を指定するには、**debug sbc alarm-log-level** コマンドを使用します。
- ログ ファイルの書き込みを行っている間に、アラーム ログの保存に使用されるバッファの空き領域が不足することがあります。また、今後の参照できるようにアラーム ログを保存したいと考えることもあります。バッファからファイル システムへのアラーム ログ ファイルの定期的な移動を設定するには、**sbc periodic-dump-alarms** コマンドを使用します。
- バッファから、指定のファイル システムまたはルータに設定されているデフォルトのファイル システムにアラーム ログを移動するには、**sbc dump-alarms** コマンドを使用します。

アラーム ログの設定

ここでは、アラーム ログの設定に使用できるコマンドについて説明します。ここで説明するコマンドの使用が必須ではないことに注意してください。アラーム ログを設定するには、次のコマンドのいずれかを組み合わせて使用します。

手順の概要

1. **debug sbc** *sbc-name* **alarm-filter** *alarm-type*
2. **debug sbc** *sbc-name* **alarm-log-level [buffer | console]** *severity-level*
3. **sbc periodic-dump-alarms {dump-location** *file-system* **[time-period** *time-period***] | time-period** *time-period***}**
4. **sbc dump-alarms [***file-system***]**
5. **show debugging**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**debug sbc** *sbc-name* **alarm-filter** *alarm-type* **例：** `Router# debug sbc MySbc alarm-filter audit-congestion`	アラーム ログを生成する必要のあるアラーム タイプを設定します。 • *sbc-name*：SBC の名前。 • *アラーム タイプ*: 次のいずれかのアラームです。 – **audit-congestion**：監査輻輳をコールします。 – **blacklist-alert**：ブラックリスト アラートです。 – **blacklist-event**：ブラックリスト イベントです。 – **h248**：H248 接続に失敗しました。 – **handled-exception**：例外を処理しました。 – **routing-component**：ルーティング コンポーネントがアクティブに設定されていません。 – **routing-config**：ルーティングの設定がアクティブに設定されていません。 – **routing-invalid**：無効なルーティング設定です。 – **sip-congestion**：SIP 輻輳が検出されました。 – **sip-peer**：SIP ピアを使用できません。 – **vqm**：Voice Quality Metrics（VQM; 音声品質メトリック）のしきい値を超えました。
ステップ 2	**debug sbc** *sbc-name* **alarm-log-level [buffer | console]** *severity-level* **例：** `Router(config)# debug sbc MySbc alarm-log-level console 40`	アラームをログに記録する出力モードとアラームの重大度を設定します。 • *sbc-name*：SBC の名前。 • **buffer**：アラーム ログをバッファに保存する必要があることを指定します。 **（注）** ファイル システムで作成される 1 つのログ ファイルのサイズが 2 MB を超えることはできません。特定のログ ファイルのサイズが 2 MB に達すると、新しいファイルが作成され、ロギング出力は新しいファイルに保存されます。 • **console**：ログの出力をコンソールに表示する必要があることを指定します。 • *severity-level*：ログが生成されるアラームの重大度です。範囲は 0 ～ 100 です。バッファに保存されているアラーム ログのデフォルトは 40 です。コンソールに表示されるアラーム ログのデフォルトは 80 です。ロギングをディセーブルにするには、値を 100 に設定します。値を 0 に設定すると、アラーム重大度のすべてのレベルについて、ログが生成されます。

コマンドまたはアクション	目的
ステップ 3 **sbc periodic-dump-alarms {dump-location** *file-system* **[time-period** *time-period***] | time-period** *time-period***}** **例：** `Router(config-sbc)# sbc periodic-dump-alarms dump-location bootflash: time-period 120`	バッファからファイル システムへのアラーム ログ ファイルの定期的な移動を設定します。 • **dump-location**：ファイル システムで、アラーム ログを保存する場所を指定します。 • *file-system*：アラーム ログの移動先とするファイル システムの名前を指定します。たとえば、*file-system* は、次のいずれかになります。 – **bootflash:** – **flash:** – **fpd:** – **ftp:** – **http:** – **https:** – **obfl:** – **pram:** – **rcp:** – **scp:** – **tftp:** • **time-period** *time-period*：ログを移動する間隔を指定します。範囲は 0 ～ 1440 です。デフォルトは 60 です。 **（注）** このコマンドの **no** 形式を使用すると、ログを移動する間隔は 0 に設定され、ログの定期的な移動はディセーブルになります。

	コマンドまたはアクション	目的
ステップ 4	**sbc dump-alarms** [*file-system*] **例：** `Router(config-sbc-sbe-cacpolicy)# sbc dump-alarms bootflash:`	バッファから、指定のファイル システムまたはルータに設定されているデフォルトのファイル システムにアラーム ログを移動します。 • *file-system*：アラーム ログの移動先とするファイル システムの名前を指定します。たとえば、*file-system* は、次のいずれかになります。 – **bootflash:** – **flash:** – **fpd:** – **ftp:** – **http:** – **https:** – **obfl:** – **pram:** – **rcp:** – **scp:** – **tftp:**
ステップ 5	**show debugging** **例：** `Router# show debugging`	ルータに対してイネーブルになっているデバッグのタイプに関する情報を表示します。 このコマンドの出力には、**debug sbc alarm-filter** コマンドおよび **debug sbc alarm-log-level** コマンドを実行して作成されるデバッグ設定が含まれます。

show debugging コマンドの次の出力例は、**debug sbc alarm-filter** コマンドおよび **debug sbc alarm-log-level** コマンドを実行して作成されるデバッグの設定例を示します。この例では、これらのデバッグ コマンドを使用して、重大度が 60 以上であるアラームについて監査輻輳を呼び出すためにログを生成し、120 分間隔で指定のファイル システムにログを移動する必要があることを指定しています。

```
Router# show debugging

SBC:
  SBC buffer alarm-log-level : 60
  SBC alarm filter 1 : AUDIT CONGESTION
  SBC alarm periodic dump time : 120 min
```