診断とトラブルシューティング

このセクションでは、システム操作に問題が発生した場合に役立つ情報について説明します。

ネットワーク ユーティリティ

ここでは、ネットワーク ユーティリティ ツールの使用方法について説明します。

- ping：特定のホスト システムが Expressway から接続でき、そのシステムに到達できるようにネットワークが正しく設定されていることを確認できます。
- トレースルート：Expressway から特定の宛先ホスト システムに送信されたネットワーク パケットが取得したルートの詳細を検出することができます。
- Tracepath：Expressway から特定の宛先ホスト システムに送信されたネットワーク パケットが取得したパスを検出することができます。
- DNS ルックアップ：特定のホスト名宛の要求に応答するドメイン名サーバ（DNS サーバ）を確認することができます。
- SRV 接続テスト機能：DNS で特定のサービス レコードをチェックし、返されたレコードへの接続を確認できます。

ping

[Ping] ツール（**[メンテナンス（Maintenance）]** > **[ツール（Tools）]** > **[ネットワーク ユーティリティ（Network utilities）]** > **[Ping]**）を使用して、システムの問題のトラブルシューティングに役立てることができます。

このツールでは、特定のホストシステムに接続できるかと、ネットワークがそのシステムに到達するように正しく設定されているかを確認できます。また、Expressway から宛先ホスト システムへメッセージを送信するためにかかった時間の詳細を報告します。

このツールを使用するには、次の手順を実行します。

1. **[ホスト（Host）]** フィールドに、接続を試みるホスト システムの IP アドレスまたはホスト名を入力します。
2. [Ping] をクリックします。

新しいセクションが表示され、接続試行の結果が示されます。成功すると、次の情報が表示されます。

ホスト	クエリされたホスト システムにより返されたホスト名と IP アドレス。
Response time (ms)	要求を Expressway からホスト システムに送信し、返されるまでにかかった時間（ミリ秒単位）。

トレースルート

[トレースルート（Traceroute）] ツール（**[メンテナンス（Maintenance）]**>**[ツール（Tools）]**>**[ネットワーク ユーティリティ（Network utilities）]**>**[トレースルート（Traceroute）]**）を使用して、システムの問題のトラブルシューティングに役立てることができます。

Expressway から特定の宛先ホスト システムに送信されたネットワーク パケットが取得したルートを検出することができます。パス上の各ノードの詳細、および各ノードが要求に応答するためにかかった時間が報告されます。

このツールを使用するには、次の手順を実行します。

1. **[ホスト（Host）]** フィールドに、パスをトレースするホスト システムの IP アドレスまたはホスト名を入力します。
2. [Traceroute] をクリックします。

トレースの結果を示すバナーがある新しいセクションが表示され、次のようなパス内の各ノードの詳細が示されます。

TTL	（存続時間）。これは、ノードの連番を示す、要求のホップ カウントです。
応答	ノードの IP アドレスと、Expressway から受信した各パケットへの応答にかかった時間（ミリ秒）が表示されます。 *** は、ノードが要求に応答しなかったことを示しています。

Expressway と特定のホスト間で取得するルートは、トレースルート要求ごとに異なる場合があります。

Tracepath

[トレースパス（Tracepath）] ツール（**[メンテナンス（Maintenance）] > [ツール（Tools）] > [ネットワーク ユーティリティ（Network utilities）] > [トレースパス（Tracepath）]**）を使用して、システムの問題のトラブルシューティングに役立てることができます。

Expressway から特定の宛先ホスト システムに送信されたネットワーク パケットが取得したルートを検出することができます。

このツールを使用するには、次の手順を実行します。

1. **[ホスト（Host）]** フィールドに、ルートをトレースするホスト システムの IP アドレスまたはホスト名を入力します。
2. [トレースパス（Tracepath）] をクリックします。

トレースの結果を示したバナーとともに、パスの各ノードの詳細、各ノードが要求に応答するためにかかった時間、および最大伝送ユニット（MTU）を示す新しいセクションが表示されます。

Expressway と特定のホスト間で取得するルートは、トレースパス要求ごとに異なる場合があります。

DNS ルックアップ

[DNS ルックアップ（DNS lookup）] ツール（**[メンテナンス（Maintenance）] > [ツール（Tools）] > [ネットワーク ユーティリティ（Network utilities）] > [DNS ルックアップ（DNS lookup）]**）を使用して、システムの問題のトラブルシューティングに役立てることができます。

指定したホスト名を DNS にクエリし、ルックアップが成功した場合は結果が表示されます。

このツールを使用するには、次の手順を実行します。

1. **[ホスト（Host）]** フィールドに、次のいずれかを入力します。
   - クエリするホストの名前
   - 逆 DNS ルックアップを実行する場合は、IPv4 アドレスまたは IPv6 アドレス
2. **[クエリ タイプ（Query type）]** フィールドで、検索するレコードのタイプを選択します。

   （逆ルックアップの場合は **[クエリ タイプ（Query type）]** は無視され、自動的に PTR レコードが検索されます）。

（注） 適切な逆引きルックアップを容易にするために、152.50.10.in-addr.arpa（アドレスのサブネットは 10.50.152.0/24）とアドレス内のターゲット DNS サーバの形式にします。これにより、サブネット内のすべての要求がデフォルトサーバではなく、ターゲット DNS サーバに送信されます。

オプション	検索対象
すべて	任意のタイプのレコード
A (IPv4 address)	ホスト名をホストの IPv4 アドレスにマッピングするレコード
AAAA (IPv6 address)	ホスト名をホストの IPv6 アドレスにマッピングするレコード
SRV（サービス）（SRV (services)）	SRV レコード（H.323、SIP、ユニファイドコミュニケーション、および TURN サービスに固有のものを含む。下記参照）。
NAPTR（名前の権限ポインタ）（NAPTR (Name authority pointer)）	ドメイン名を（たとえば URI や他のドメイン名に）上書きするレコード

3. デフォルトでは、システムはシステムのデフォルトのすべての DNS サーバ（**[システム（System）] > [DNS]**）にクエリを送信します。特定のサーバのみを照会するには、**[次の DNS サーバに照合して確認する（Check against the following DNS servers）]** を *[カスタム（Custom）]* に設定し、使用する DNS サーバを選択します。
4. [Lookup] をクリックします。

選択した各**クエリ タイプ**に対して個別の DNS クエリが実行されます。DNS に送信されるクエリに含まれるドメインは、指定された**ホスト**が完全修飾名であるかどうかによって異なります（完全修飾ホスト名には少なくとも 1 つの「「ドット」」が含まれています）。

- 指定された**ホスト**が完全修飾名である場合：
  - DNS に対し、最初に**ホスト**のクエリが実行されます。
  - **ホスト**のルックアップが失敗すると、**Host.<system_domain>** に対する追加のクエリが実行されます（**<system_domain>** は **DNS** ページで設定されている**ドメイン名**）。
- 指定された**ホスト**が完全修飾名でない場合：
  - DNS に対し、最初に **Host.<system_domain>** のクエリが実行されます。
  - **ホスト**のルックアップが失敗すると、次は **Host.<system_domain>** のクエリが実行されます

SRV レコード タイプのルックアップの場合、複数の DNS クエリが実行されます。次の _service._protocol の組み合わせごとに SRV クエリが実行されます。

- _h323ls._udp.<domain>
- _h323rs._udp.<domain>
- _h323cs._tcp.<domain>
- _sips._tcp.<domain>
- _sip._tcp.<domain>
- _sip._udp.<domain>
- _collab-edge._tls
- _cisco-uds._tcp
- _turn._udp.<domain>
- _turn._tcp.<domain>

それぞれの場合、その他すべてのクエリ タイプについて、**ホスト**または**Host.<system_domain>** の <domain> に対して 1 つまたは 2 つのクエリが実行されます。

結果

新しいセクションが表示され、すべてのクエリ結果が示されます。成功すると、次の情報が表示されます。

クエリーのタイプ	Expressway によって送信されたクエリのタイプ。
名前	クエリに対する応答に含まれているホスト名。
TTL	このクエリの結果が Expressway にキャッシュされる時間（秒単位）。
クラス	IN（インターネット）は、応答がインターネットホスト名、サーバ、またはIPアドレスを含む DNS レコードであったことを示します。
タイプ	クエリに対する応答に含まれているレコードタイプ。
応答	この**[名前（Name）]**および**[タイプ（Type）]**のクエリに対する応答として受信したレコードの内容。

転送プロトコル

Expressway は UDP と TCP を使用して DNS 解決を行います。DNS サーバからは、通常、UDP とTCP 応答が送られます。UDP 応答が 512 バイトの UDP メッセージ サイズの制限を超えていると、Expressway は UDP 応答を処理できません。一般に、これが問題になることはありません。Expressway は代わりに TCP 応答を処理できるためです。

ただし、ポート 53 での TCP インバウンドをブロックしている場合、UDP 応答のサイズが 512 バイトを超えていると、Expressway は DNS からの応答を処理できません。この場合、DNS ルックアップ ツールを使用しても結果は表示されず、要求したアドレスを必要とするすべての操作は失敗します。

ただし、ポート 53 での TCP インバウンドをブロックしている場合、UDP 応答のサイズが 512 バイトを超えていると、Expressway は DNS からの応答を処理できません。この場合、DNS ルックアップ ツールを使用しても結果は表示されず、要求したアドレスを必要とするすべての操作は失敗します。

SRV 接続テスト機能

SRV 接続テスト機能は、Expressway が所定のドメイン上の特定のサービスに接続できるかどうかをテストするネットワーク ユーティリティです。このツールを使用すると、Cisco Webex ハイブリッド コール サービスやビジネス ツー ビジネス ビデオ コールなどの Expressway ベースのソリューションを設定しながら事前に接続をテストできます。

このツールで接続をテストする際は、クエリする DNS サービス レコード ドメインと、そのドメインでテストするサービス レコード プロトコルを指定します。Expressway は指定されたプロトコルごとに DNS SRV クエリを実行し、DNS から返されたホストへの TCP 接続を試行します。TLS を指定した場合、Expressway は TCP が成功しなければ TLS 接続を試行しません。

Expressway 接続テスト ページに、DNS の応答と接続試行が示されます。接続が失敗した場合は、その理由と併せてその特定の問題を解決するためのアドバイスも表示されます。

接続をトラブルシューティングするには、テストで生成された TCP データを *.pcap* 形式でダウンロードできます。選択的に DNS クエリのダンプ（特定の接続試行）をダウンロードすることも、テスト全体を記録した単一の *.pcap* ファイルを取得することもできます。

このツールを使用するには、次の手順を実行します。

1. **[メンテナンス（Maintenance）]** > **ツール（Tools）]** > **[** > **[ネットワーク ユーティリティ（Network utilities）]** > **[接続テスト（Connectivity Test）]** に移動します。
2. クエリする **[サービス レコード ドメイン（Service Record Domain）]** を入力します（例：`callservice.webex.com`）。
3. テストする **[サービス レコード プロトコル（Service Record Protocols）]** を入力します（例：`_sips._tcp`）。

   複数のプロトコルを指定する場合は、各プロトコルをカンマで区切ります（例：`_sip._tcp,_sips._tcp`）。
4. [実行（Run）] をクリックします。

Expresswayは、サービス、プロトコル、およびドメインの組み合わせで構成されるSRVレコードに対してDNSへクエリを行います。たとえば、`_sip._tcp.callservice.webex.com`と`_sips._tcp.callservice.webex.com`へのクエリなどです。

デフォルトでは、システムはシステムのデフォルトのすべてのDNSサーバ（**[システム（System）] > [DNS]**）にクエリを送信します。

サービス レコードのオプション

導入環境でテストする必要がある、_service._protocolの組み合わせの例を次に示します。

- _h323ls._udp.<domain>
- _h323rs._udp.<domain>
- _h323cs._tcp.<domain>
- _sips._tcp.<domain>
- _sip._tcp.<domain>
- _sip._udp.<domain>
- _collab-edge._tls
- _cisco-uds._tcp
- _turn._udp.<domain>
- _turn._tcp.<domain>
- _cms-web._tls.<domain>
- _sipfederationtls._tcp.<domain>

テスト結果

ページの下部にあるセクションに、クエリ結果と接続テストの結果が示されます。テスト結果には、次の表に記載する情報の一部またはすべてが含まれます。

表 *1 :* 接続テストの結果：*DNS SRV*ルックアップ

結果フィールド	説明
ステージ（Stage）	テストのステージ。クエリに対する応答ごとにステージが1つ、クエリ結果全体に別のステージが1つあります。
サービス レコード（Service Record）	クエリしたレコードセットから検出されたSRVレコード。

結果フィールド	説明
結果（Result）	DNS SRV レコードでマッピングされているホスト（テストが成功した場合）。DNS レコードで定義されている場合、エントリごとのプライオリティ、重み、ポートも示されます。
ヒント（Hint）	このフィールドには、この結果テーブルの値は保持されません。
TCP ダンプ（TCP Dump）	結果全体について、SRV クエリの TCP レコードが含まれる .pcap ファイルをダウンロードすることができます。

表 *2:* 接続テストの結果：*TCP* 接続

結果	説明
ステージ（Stage）	テストのステージ。サービスに対する TCP プロトコルのクエリによって返されたホストごとにテストが 1 回行われます。すべてのテストを集計した結果もあります。
ターゲット（Target）	DNS SRV クエリによって返されたホスト名。
結果（Result）	テストが正常に完了したことを示します。またはテストが失敗した理由が示されます（既知の場合）。
ヒント（Hint）	失敗したテストのトラブルシューティングに利用できるポインタ。
TCP ダンプ（TCP Dump）	特定の接続試行の TCP レコードが含まれる .pcap ファイルをダウンロードすることができます。

表 *3 :* 接続テストの結果：*TCP* 接続

結果フィールド	説明
ステージ（Stage）	テストの段階。各ホストに、TLS プロトコルでクエリしたサービスに対するテストを 1 つずつ返します。テストは、ホストでサポートされている各 TLS バージョンを使用して次の順序で実行されます。 • TLS 1.2 • TLS 1.1 • TLS 1 たとえば、ホストは 3 つのすべてのバージョンをサポートしており、TLS 1.1 バージョンを使用して接続が成功した場合、チェックは 2 つのテストを返します。 すべてのテストを集計した結果もあります。 （注） Expressway がホストへの TLS 接続を確立できない場合、そのホストに対する TLS 接続試行は行われません。
ターゲット（Target）	DNS SRV クエリによって返されたホスト名。
結果（Result）	テストが正常に完了したことを示します。またはテストが失敗した理由が示されます（既知の場合）。
ヒント（Hint）	失敗したテストのトラブルシューティングに利用できるポインタ。
TCP ダンプ（TCP Dump）	特定の接続試行の TCP レコードが含まれる .pcap ファイルをダウンロードすることができます。

診断ツール

ここでは、Expressway 診断ツールの使用方法について説明します。

- 診断ロギングの設定
- システム スナップショットの作成

- ネットワーク ログ レベルの設定とサポート ログ レベルの設定の高度なロギング設定ツール
- インシデントレポート

Expressway は SIP 「セッション識別子」をサポートしています。コールのすべてのデバイスがセッション識別子を使用していると仮定すると、このメカニズムは SIP ヘッダーの *[セッション ID（Session-ID）]* フィールドを使用して、コールのトランジット全体を通して一意のコードを維持します。セッション識別子は、Expressway サーバ上の特定のコールを検索して追跡するために使用できるので、複数のコンポーネントにかかわるコールの問題を調査する場合に便利です。セッション識別子のサポートには、インターワーキングされた SIP/H.323 コールの SIP 側、および Microsoft システムとの間のコールが含まれます。セッション識別子は、RFC 7989 で定義されています。

診断ロギングの設定

診断ログ ツール（**[メンテナンス（Maintenance）]** > **[診断（Diagnostics）]** > **[診断ロギング（Diagnostic logging）]**）は、トラブルシューティングに役立つ場合があります。一定期間のシステムアクティビティの診断ログを生成し、それをダウンロードして、シスコのカスタマーサポート担当者に送信できます。ロギングの進行中に *tcpdump* を取得およびダウンロードすることができます。

はじめに

- 一度に生成できる診断ログは 1 つだけです。新しい診断ログを作成すると、以前に作成されたログが置き換えられます。
- Expressway は、関連するシステムアクティビティを継続的にログに記録します。診断ロギング機能は、診断ロギング時間の開始から診断ロギングが停止するまでのアクティビティを抽出し、便利な Web ベースのダウンロード機能を提供します。
- **[再起動/リブート（Restart/Reboot）]**：診断ログのみが収集されます。他のファイルはバンドルから欠落します。
- 診断ログを起動すると、関連するシステムモジュールのログ レベルが自動的に「「デバッグ」」に設定されます。ログを停止するとログレベルが元の値にリセットされるため、結果の詳細ログレベルで設定されたアラームを無視します。
- 診断ロギングは、Web インターフェイスを介して制御されます。CLI オプションはありません。
- tcpdumpオプションを選択すると、ネットワークインターフェイスごとに最大3つのパケットキャプチャファイルが作成され、それぞれの最大サイズは20MBです（つまり、デュアルネットワークインターフェイスを備えた Expressway で、合計サイズが 80 MB の最大4つのファイルを作成できます）。

（注） X14.0 以降、.pcap ファイルの数はネットワークインターフェイスごとに最大 20 個増加し、tcpdump は Web UI を介して連続的に実行できます。ファイルの最大サイズは 20 MB です。

注意 診断ログを有効にすると、システムのパフォーマンスが影響を受ける可能性があります。診断ログは、シスコのカスタマーサポートのアドバイスに基づいて、またはトラフィックの負荷が軽いときにのみ収集する必要があります。

診断ログを生成するプロセス

1. **[Maintenance]** > **[Diagnostics]** > **[Diagnostic logging]** を選択します。
2. （オプション）*[Take tcpdump while logging]*を選択します。診断ログの進行中に tcpdump を使用するには、このオプションを選択できます。tcpdump は、ロギングの完了時に別のファイルとしてダウンロードできます。

（注） ユーザインターフェイスで tcpdump が有効になっている場合、管理者は **IP アドレス**と**ポート**フィルタを提供できます。

管理者が特定のホスト（IPアドレスまたは完全修飾ドメイン名（FQDN））および/またはポートから送信されるパケットを pcap ファイルで確認する場合、tcpdump フィルタが使用されます。管理者は、フィルタリングされたパケットを取得するために識別されるフィールドに値を指定できます。バージョン X14.0 から、tcpdump は LAN ごとに 20 個の pcap ファイルをキャプチャし、すべての pcap ファイルのサイズは 20 MB です。

この表は、登録数に応じて、1 つの pcap ファイル（最大 20 MB）と 20 の pcap ファイルを生成するのにかかる平均時間（秒単位）を表しています。

Expressway C：

	20 MB	**400 MB**
5 ユーザ	2	40
20 ユーザ	2	40
2500 ユーザ	10	200

Expressway E：

	20 MB	**400 MB**
5 ユーザ	1	20
20 ユーザ	1	20
2500 ユーザ	2	40

これらの数値は、トラブルシューティングに使用される環境に固有のものです。このパフォーマンステストの実行中に、1 ノードとモバイルおよびリモートアクセス（MRA）ビデオを使用しました。

3. **IP アドレス で tcpdump をフィルタリングする（Filter tcpdump by IP address**）を入力します。
4. **ポートで tcpdump をフィルタリングする（Filter tcpdump by port**） を入力します。範囲は 1 ～ 65536 です。
5. [Start new log] をクリックします。
6. （任意）**マーカー** テキストを入力して、**[マーカーの追加（Add Marker）]** をクリックします。
   - 特定のアクティビティが実行される前にマーカー機能を使用して、ログファイルにコメントテキストを追加することができます。これは、診断ログファイル内の特定

のセクションを識別するのに役立ちます。マーカーテキストには、ログファイルに DEBUG_MARKER タグがあります。

- 診断ログの進行中に、必要に応じた数のマーカーを追加できます。

7. 診断ログにトレースするシステムの問題を再現します。
8. [Stop Logging] をクリックします。
9. [ログの収集（Collect Logs）] をクリックします。
10. ログの収集が完了したら、**[ログのダウンロード（Download log）]** をクリックして、ローカル ファイル システムに診断ログ アーカイブを保存します。

    アーカイブを保存するように促されます（実際の表現はブラウザによって異なります）。

診断ログアーカイブに含まれているファイル

- loggingsnapshot_<*system host name*>_<*timestamp*>.txt： ロギング期間中に実行されたアクティビティに応じたログメッセージが記録されています。
- xconf_dump_<*system host name*>_<*timestamp*>.txt：ロギング開始時のシステム設定に関する情報が記録されています。
- xconf_dump_<*system host name*>_<*timestamp*>.xml：XML 形式の xconfig のより完全なバージョン
- xstat_dump_<*system host name*>_<*timestamp*>.txt：ロギング開始時のシステムのステータスに関する情報が記録されています。
- xconf_dump_<*system host name*>_<*timestamp*>.xml：XML 形式の xstatus のより完全なバージョン
- （該当する場合）eth*n*_diagnostic_logging_tcpdump x_<*system host name*>_<*timestamp*> .pcap：ロギング期間中にキャプチャされたパケットが記録されています。
- ca_<*system host name*>_<*timestamp*>.pem
- server_<*system host name*>_<*timestamp*>.pem

要求された場合は、シスコサポートの担当者にこれらのファイルを送信できます。

⚠

注意 *tcpdump* ファイル には、機密情報が含まれている場合があります。*tcpdump* ファイルは、信頼できる受信者にのみ送信してください。送信前にファイルを暗号化し、アウトオブバンドで復号パスワードを送信することを考慮してください。

コラボレーション ソリューション アナライザー ツールへのリンク

必要に応じて、**解析ログ**を使用してコラボレーションソリューションアナライザのトラブルシューティングツールへのリンクを開きます。

ログを再度ダウンロードするには

ログを再度ダウンロードする場合は、**[ログ収集（Log Collection）]**ボタンを使用することで再度収集できます。ボタンがグレー表示されている場合は、ブラウザのページを更新します。

クラスタ化システム

Expresswayがクラスタの一部である場合、一部のアクティビティは「現在」のピア（現在管理者としてログインしているピア）にのみ適用されます。

- ロギングの開始操作と停止操作は、現在のピアには関係なくクラスタ内のすべてのピアに適用されます。
- *tcpdump* 操作は、現在のピアには関係なくクラスタ内のすべてのピアに適用されます。
- 各クラスタ ピアは独自の統合ログを維持し、そのピアでのみ発生するアクティビティを記録します。
- マーカー テキストは、現在のピアにのみ適用されます。
- 現在ピアからの診断ログのみダウンロードできます。
- 他のピアのログへのマーカの追加、または他のピアからの診断ログのダウンロードを行うには、そのピアに管理者としてログインする必要があります。

デバッグを目的として包括的な情報を収集する場合は、クラスタ内のピアごとに診断ログを抽出することを推奨します。

システム スナップショットの作成

「システム スナップショット（System snapshot）」ページ（**[メンテナンス（Maintenance）]** > **[診断（Diagnostics）]** > **[システムスナップショット（System snapshot）]**）では、診断目的で使用できるファイルを作成できます。これらのファイルは、経験している問題のトラブルシューティングに役立てるため、要求されたときにサポート担当者に送信する必要があります。

いくつかのタイプのスナップショット ファイルを作成できます。

- **ステータススナップショット**：システムの現在の設定とステータス設定が含まれています。
- **ログスナップショット**：ログファイル（イベントログ、設定ログ、ネットワークログなど）情報が含まれます。
- **完全なスナップショット**：すべてのシステム情報の完全なダウンロードが含まれています。このスナップショット ファイルの準備の完了には数分かかる場合があり、スナップショットの進行中にシステム パフォーマンスが低下する可能性があります。

システム スナップショットファイルを作成するには、次の手順に従います。

1. スナップショットファイルのダウンロードを開始するには、いずれかのスナップショットボタンをクリックします。通常、サポート担当者が、どのタイプのスナップショットファイルが必要であるかを示します。
   - スナップショット作成プロセスが開始されます。このプロセスはバックグラウンドで動作します。必要に応じてスナップショットページから離れ、後で戻ってきて生成されたスナップショット ファイルをダウンロードすることができます。
   - スナップショット ファイルが作成されると、**[スナップショットのダウンロード（Download snapshot）]** ボタンが表示されます。
2. [スナップショットのダウンロード（Download snapshot）] をクリックします。ポップアップ ウィンドウが表示され、ファイルを保存するよう指示されます（実際の表現は、ブラウザによって異なります）。サポート担当者に簡単にファイルを送信できる場所を選択します。

ネットワーク ログ レベルの設定

「ネットワークログの設定（Network Log configuration）」ページ（**[メンテナンス（Maintenance）] > [診断（Diagnostics）] > [詳細設定（Advanced）] > [ネットワークログの設定（Network Log configuration）]**）を使用して、ネットワークログメッセージモジュールの範囲のログレベルを設定します。

⚠

注意 ログ レベルを変更すると、システムのパフォーマンスに影響を与える可能性があります。シスコ カスタマー サポートのアドバイスがあった場合にのみ、ログ レベルを変更してください。

ログ レベルを変更するには、次の手順を実行します。

1. ログ レベルを変更するモジュールの**名前**をクリックします。
2. ドロップダウン リストから必要な**レベル**を選択します。
   - ログ レベルの *[*致命的（*Fatal*）*]* は冗長性が最も低く、*[*トレース（*Trace*）*]* は冗長性が最も高いレベルです。
   - 各メッセージのカテゴリには、デフォルトで *[*情報（*Info*）*]* のログ レベルが設定されます。
3. [保存（Save）] をクリックします。

サポート ログ レベルの設定

[サポートログの設定（Support Log configuration）] ページ（**[メンテナンス（Maintenance）] > [診断（Diagnostics）** > **[詳細設定（Advanced）] > [サポート ログの設定（Support Log**

configuration）]）を使用して、サポートログメッセージモジュールの範囲にログレベルを設定します。

⚠

注意 ログ レベルを変更すると、システムのパフォーマンスに影響を与える可能性があります。シスコ カスタマー サポートのアドバイスがあった場合にのみ、ログ レベルを変更してください。

ログ レベルを変更するには、次の手順を実行します。

1. ログ レベルを変更するモジュールの**名前**をクリックします。
2. ドロップダウン リストから必要な**レベル**を選択します。
   - ログ レベルの *[*致命的（*Fatal*）*]* は冗長性が最も低く、*[*トレース（*Trace*）*]* は冗長性が最も高いレベルです。
   - 各メッセージのカテゴリには、デフォルトで *[*情報（*Info*）*]* のログ レベルが設定されます。
3. [保存（Save）] をクリックします。

インシデントレポート

Expressway のインシデント レポート機能は、アプリケーションの障害などの重要なシステム問題に関する情報を自動的に保存します。ここでは、インシデントレポートを表示する方法について説明します。

また、手動または自動でインシデントレポートをシスコのカスタマーサポートに送信する方法も説明されています。これらのレポートに含まれている情報をシスコのカスタマーサポートによる障害の原因の診断に使用できます。このプロセス中に収集されたすべての情報は社外秘として扱われ、問題を診断して解決する目的のみにシスコの担当者が使用します。

インシデント レポートに関する注意：プライバシー保護された個人データ

シスコに対するレポートにプライバシー保護された個人データが含まれることは決してありません。

プライバシー保護された個人データは、将来、過去、および既存の顧客、従業員、およびその他のすべての個人または団体に関する個人情報が含まれている、顧客が何らかの方法で情報源から受け取るか導出する個人または団体に関するすべての情報を意味します。プライバシー保護された個人データには、名前、住所、電話番号、電子アドレス、社会保障番号、クレジットカード番号、顧客の機密ネットワーク情報（47 U.S.C. § 222 で定義されている内容、およびその施行規則）、IP アドレスまたはその他のハンドセット ID、アカウント情報、信用情報、人

口統計学的情報、および単独または他のデータとの組み合わせで特定の個人に固有の情報を提供できるその他の情報が、制限なく含まれます。

プライバシー保護された個人データは、レポートを自動的に送信するように Expressway が設定されている場合もシスコに送信されないことを確認してください。

このような情報の漏洩を防ぐことができない場合は、自動設定機能は使用しないでください。代わりに、「インシデント レポートの詳細」ページのデータをコピーしてテキスト ファイルに貼り付けます。その後、シスコのカスタマー サポートにファイルを転送する前に、機密情報を削除できます。

インシデント レポートは、常にローカルに保存され、「インシデント レポートの表示」ページで表示できます。

自動インシデント レポートの有効化

自動インシデント レポートを有効にする前に、インシデント レポートに関する注意：プライバシー保護された個人データをお読みください。

インシデント レポートをシスコ カスタマー サポートに自動的に送信するように Expressway を設定するには、次の手順を実行します。

1. **[メンテナンス（Maintenance）]**>**[診断（Diagnostics）]**>**[インシデントレポート（Incident reporting）]**>**[設定（Configuration）]** に移動します。
2. **[インシデント レポート送信モード（Incident reports sending mode）]** を *[オン（On）]* に設定します。
3. エラー レポートの送信先の Web サーバの **[インシデント レポートの URL（Incident reports URL）]** を指定します。デフォルトは `https://cc-reports.cisco.com/submitapplicationerror/` です。
4. オプション。シスコのカスタマー サポートがエラー レポートのフォローアップに使用できる **[連絡先の電子メールアドレス（Contact email address）]** を指定します。
5. オプション。インシデント サーバへの接続に使用する **[プロキシ サーバ（Proxy server）]** を指定します。（http|https）://address:port/ という形式を使用してください（例：`http://www.example.com:3128/`）。
6. **[コアダンプの作成（Create core dumps）]** が *[オン（On）]* に設定されていることを確認します。これは、役立つ診断情報が提供されるため、推奨される設定です。

（注） **[インシデント レポート送信モード（Incident reports sending mode）]** が *[オフ（Off）]* に設定されている場合、インシデントはどの URL にも送信されませんが、ローカルに保存され、**[インシデントの詳細（Incident detail）]** ページからインシデント レポートの表示できます。

インシデント レポートを手動で送信

インシデント レポートをシスコに手動で送信するかどうかを決定する前に、インシデント レポートに関する注意：プライバシー保護された個人データをお読みください。

インシデント レポートをシスコのカスタマー サポートに手動で送信するには、次の手順を実行します。

1. **[メンテナンス（Maintenance）]** > **[診断（Diagnostics）]** > **[インシデント レポート（Incident reporting）]** > **[表示（View）]** に移動します。
2. 送信するインシデントをクリックします。**「インシデントの詳細（Incident detail）」** ページが表示されます。
3. ページの下部にスクロールし、[インシデント レポートのダウンロード（Download incident report）] をクリックします。オプションで、ファイルを保存できます。
4. ファイルをシスコ カスタマー サポートに転送できる場所に保存します。

レポートからの機密情報の削除

ダウンロードしたインシデント レポートは Base64 でエンコードされており、そのファイル内の情報について意味のある表示や編集を行うことはできません。

シスコに送信する前にレポートを編集する必要がある場合は（たとえば、機密情報と考えられるものを削除する必要がある場合）、**「インシデントの詳細（Incident detail）」** ページの情報をコピーしてテキスト ファイルに貼り付け、そのファイル内の情報 を編集してからシスコに送信する必要があります。

インシデント レポートの表示

「インシデント ビュー（Incident view）」 ページ（**[メンテナンス（Maintenance）]** > **[診断（Diagnostics）]** > **[インシデント レポート（Incident reporting）]** > **[表示（View）]**）には、Expressway が最後にアップグレードされてから発生したすべてのインシデント レポートのリストが表示されます。各インシデントに対するレポートが生成され、これらのレポートに含まれている情報をシスコのカスタマー サポートによる障害の原因の診断に使用できます。

各レポートについて、以下の情報が表示されます。

フィールド	説明
時刻	インシデントが発生した日時。
バージョン	インシデントが発生したときに実行していた Expressway ソフトウェアのバージョン。
ビルド	インシデントが発生したときに実行していた Expressway ソフトウェア バージョンの内部ビルド番号。

フィールド	説明
状態（State）	インシデントの現在の状態。 *[保留中（Pending）]*：インシデントがローカルに保存されたが送信されていないことを示します。 *[Sent]*：インシデントの詳細が [インシデント レポート] ページで指定された URL に送信されたことを示します。

特定のインシデント レポートに含まれている情報を表示するには、レポートの [Time] をクリックします。「インシデント レポートの詳細」ページが表示され、画面上にレポートを表示するか、またはシスコのカスタマー サポートに手動で転送するために XML ファイルとしてダウンロードすることができます。

インシデント レポートの詳細

「インシデントの詳細（Incident detail）」ページ（**[メンテナンス（Maintenance）] > [診断（Diagnostics）] > [インシデントレポート（Incident reporting）] > [表示（View）]**、次にレポートの **[時間（Time）]** をクリック）には、特定のインシデントレポートに含まれている情報が表示されます。

[インシデント レポート送信モード（Incident reports sending mode）]（[メンテナンス（Maintenance）] > [診断（Diagnostics）] > [インシデント レポート（Incident reporting）] > [設定（Configuration）] を使用）が有効になっている場合、これは外部 Web サービスに送信される情報です。また、これは、[Download incident report] をクリックした場合に Base64 でエンコードされた XML ファイルとしてダウンロードされる情報と同じです。

レポートに含まれている情報は、次のとおりです。

フィールド	説明
時刻	インシデントが発生した日時。
バージョン	インシデントが発生したときに実行していた Expressway ソフトウェアのバージョン。
ビルド	インシデントが発生したときに実行していた Expressway ソフトウェア バージョンの内部ビルド番号。
名前（Name）	ソフトウェアの名前。
System	システム名（設定されている場合）、または IP アドレス。
シリアル番号（Serial number）	ハードウェアのシリアル番号。

フィールド	説明
プロセス ID（Process ID）	インシデントが発生したときに Expressway アプリケーションに設定されていたプロセス ID。
リリース	これが（開発ビルドではなく）リリース ビルドであるかどうかを示す true/false フラグ。
ユーザ名（Username）	このソフトウェアを構築した担当者の名前。リリース ビルドの場合は空白です。
スタック（Stack）	インシデントの原因となった実行スレッドのトレース。
デバッグ情報（Debug information）	すべてのスレッドのアプリケーション コール スタックの完全なトレースおよびレジスタの値。

注意 各コール スタックについて、デバッグ情報には機密情報が含まれている可能性がある変数の内容が含まれています（たとえば、エイリアス値や IP アドレスなど）。ご使用の導入環境で、この情報に特定の個人に固有の情報が含まれている可能性がある場合は、自動インシデント レポートを有効にするかどうかを決定する前に、プライバシー保護された個人データに関するインシデント レポートに関する注意：プライバシー保護された個人データをお読みください。

開発者リソース

Expressway には、シスコのサポート チームと開発チームのみが使用するための機能がいくつか含まれています。シスコのサポート担当者のアドバイスと監視の上で行う場合を除き、これらのページにはアクセスしないでください。

注意 これらのページの機能を誤って使用すると、システムの動作が不安定になったり、パフォーマンス上の問題が発生したり、システム設定が永続的に破損したりする可能性があります。

以下の機能があります。

- デバッグおよびシステム管理ツール
- [Experimental] メニュー

デバッグおよびシステム管理ツール

注意 これらの機能は、シスコのサポート担当者のアドバイスがない限り、お客様は使用できません。これらの機能を誤って使用すると、システムの動作が不安定になったり、パフォーマンス上の問題が発生したり、システム設定が永続的に破損したりする可能性があります。

Expresswayには、デバックとシステム管理用の数多くのツールが搭載されています。管理者はこれらのツールを使用して、設定データへのアクセスや変更、ネットワーク トラフィックへのアクセスなど、ライブ システム上で発生していることを詳細に検査することができます。

これらのツールにアクセスする方法は、次のとおりです。

1. SSH セッションを開始します。
2. 必要に応じて、admin または root としてログインします。
3. シスコのサポート担当者によって指示された手順に従ってください。

[Experimental] メニュー

Expressway Webインターフェイスには、お客様が使用するためのものではないページが数多く含まれています。これらのページは、シスコのサポートおよび開発チームのみが使用するために存在しています。シスコのサポート担当者のアドバイスと監視の上で行う場合を除き、これらのページにはアクセスしないでください。

注意 これらのページの機能を誤って使用すると、システムの動作が不安定になったり、パフォーマンス上の問題が発生したり、システム設定が永続的に破損したりする可能性があります。

これらのページにアクセスする方法は、次のとおりです。

1. `https://<Expressway のホスト名または IP アドレス>/setaccess` に移動します。

   [アクセスの設定（Set access）] ページが表示されます。
2. [アクセスパスワード（Access password）] フィールドに、`qwertsys` と入力します。
3. [アクセスの有効化（Enable access）] をクリックします。

既存のメニュー項目の右側に、新しい**[Experimental]** という最上位メニューが表示されます。