
# トランザクション ログの使用

この章では、トランザクション ログの使用方法について説明します。この章の構成は、次のとおりです。


- トランザクション ログ形式の概要（p.19-2）
- トランザクション ロギングと NTLM 認証（p.19-8）
- ログ ファイル使用上の注意事項（p.19-9）
- Content Distribution Manager GUI によるトランザクション ロギングのイネーブル化（p.19-12）
- WMT トランザクション ロギングの使用（p.19-17）
- リアルタイム トランザクション ロギングの使用（p.19-21）


トランザクション ログを使用すると、管理者は、Content Engine を通過したトラフィックを表示できます。トランザクション ログの一般的なフィールドは、要求が行われた日付と時刻、要求されたURL、それがキャッシュ ヒットであったかキャッシュ ミスであったか、要求のタイプ、転送されたバイト数、および送信元 IP アドレスです。

# トランザクション ログ形式の概要

ACNS 5.x ソフトウェアでは、ユーザは Squid、拡張 Squid、Apache、またはトランザクション ログ用カスタマイズ ログのいずれかの形式を選択できます。

## Squid スタイルのトランザクション ロギング

Squid スタイルのログ形式は、Content Engine のトランザクション ロギングのデフォルト形式です。使用される Squid ログ ファイル形式は、Squid-1.1 *access.log* ファイル形式に関連したネイティブ ログ ファイル形式です。Squid-1.1 ネイティブ ログ ファイル形式の詳細については、次の URL にある Squid 資料『*Frequently Asked Questions*』の「6.6 access.log」を参照してください。

http://www.squid-cache.org/Doc/FAQ/FAQ.html

Squid ログ ファイル形式は、次のとおりです。

time elapsed remotehost code/status bytes method URL rfc931 peerstatus/peerhost type

Squid ログ形式の例は、次のとおりです。

1012429341.115 100 172.16.100.152 TCP_REFRESH_MISS/304 1100 GET
http://www.cisco.com/images/homepage/news.gif - DIRECT/www.cisco.com

## 拡張 Squid ログ形式

拡張 Squid 形式では、Squid スタイルの形式でロギングされるフィールドの他に、ログ ファイル内の各レコードに関連したユーザ名がロギングされ、課金請求に使用されます。この形式では、Squid 形式に関連した RFC フィールドを使用して、認証されたユーザがロギングされます。ユーザ情報を取得できない場合、このフィールドには常に「-」（ダッシュ）が入ります。

拡張 Squid スタイル ログ形式の例は、次のとおりです。

1012429341.115 100 172.16.100.152 TCP_MISS/302 184 GET
http://www.cisco.com/cgi-bin/login myloginname DIRECT/www.cisco.com

## Apache スタイルのトランザクション ロギング

Apache 形式は、World Wide Web Consortium（W3C）ワーキング グループによって規定された Common Log File（CLF; 共通ログ ファイル）形式です。この形式は、多くの業界標準のログ ツールと互換性があります。詳細は、次の URL に示されている W3C Common Log File の Web サイトを参照してください。

http://www.w3.org/Daemon/User/Config/Logging.html

Apache スタイルのログ ファイル形式は、次のとおりです。

remotehost rfc931 authuser date request status bytes

Apache スタイルのログ ファイル形式の例は、次のとおりです。

172.16.100.152 - - [Wed Jan 30 15:26:26 2002]

“GET/http://www.cisco.com/images/homepage/support.gif HTTP/1.0” 200 632

# カスタム形式のトランザクション ロギング

**transaction-logs format custom** コマンドを使用すると、事前定義されたネイティブ Squid 形式、拡張 Squid 形式、あるいは Apache CLF 形式に含まれていない追加フィールドをログ形式ストリングを使用してロギングできます。ログ形式ストリングとは、表 19-1 に一覧表示されているトークンを含み、Apache ログ形式ストリングに似たストリングです。ログ形式ストリングに含むことができるリテラル文字は、ログ ファイルにコピーされます。二重バックスラッシュ（\\）は、リテラル バックスラッシュを表すときに使用され、バックスラッシュのあとに単一引用符（\'）を続けると、リテラル単一引用符を表すときに使用できます。リテラル二重引用符は、ログ形式ストリングの一部として表すことはできません。制御文字 \t と \n は、それぞれタブ文字と改行文字を表すときに使用できます。

表 19-1 に、ログ形式ストリングに受け入れ可能な形式トークンを示します。この表に表示されている形式トークンの「...」部分は、任意の条件です。この形式トークンの部分は %a のように省略することもできます。ある任意の条件が形式トークンに含まれていてその条件が満たされると、表 19-1 の Value カラムに表示されるものはトランザクション ログ出力に含まれます。任意の条件が形式トークンに含まれていても、その条件が満たされない場合、表示されるトランザクション ログ出力はハイフン（-）に置き換えられます。条件の形式は HTTP ステータス コードのリストであり、コードの前に感嘆符（!）が付く場合と付かない場合があります。感嘆符は、そのあとに続くすべてのステータス コードを無効にするために使用します。つまり、! のあとにリストされたステータス コードがどれも、要求の HTTP ステータス コードと一致しない場合に、形式トークンに関連した値がロギングされます。! のあとに表示されたステータス コードのいずれかが、要求の HTTP ステータス コードと一致する場合は、ハイフン（-）がロギングされます。

たとえば、「%400,501{User-Agent}i」は、400 エラーと 501 エラー（Bad Request、Not Implemented）の発生時にだけ User-Agent ヘッダー値をロギングします。一方、「%!200,304,302{Referer}i」は、通常のステータスを戻さなかった要求すべての Referer ヘッダー値をロギングします。

カスタム形式は現在、次の要求ヘッダーをサポートしています。

- User-Agent
- Referer
- Host
- Cookie

カスタム ログ形式ストリングで指定された次の Request、Referer、および User-Agent の各形式トークンの出力は、トランザクション ログ エントリ内で常に二重引用符で囲まれています。

%r

%{Referer}i

%{User-Agent}i

%{Cookie}i 形式トークンは、二重引用符で囲まずに生成されます。これは、Cookie 値自体に二重引用符が含まれているからです。Cookie 値には、属性と値の複数のペアが含まれ、各ペアはスペースで区切られます。カスタム形式ストリングで Cookie 形式のトークンを使用する場合、そのトークンを形式ストリングの最後のフィールドに置くことを推奨します。これにより、Cookie 形式のトークンがトランザクション ログ レポーティング ツールにより簡単に解析できます。別の方法として、形式トークン ストリング「\'%{Cookie}i\'」を使用する場合、Cookie ヘッダーを単一引用符で囲むことができます。

次のコマンドを入力すると、よく知られている Apache Combined Log Format を生成できます。

**transaction-logs format custom "[%{%d}t/%{%b}t/%{%Y}t:%{%H}t:%{%M}t:%{%S}t %{%z}t] %r %s %b %{Referer}i %{User-Agent}i"**

次に示す、Apache Combined Format のトランザクション ログ エントリ例は、上記のカスタム形式ストリングを使用して設定されています。

[11/Jan/2003:02:12:44 -0800] "GET http://www.cisco.com/swa/i/site_tour_link.gif HTTP/1.1" 200 3436 "http://www.cisco.com/" "Mozilla/4.0 (compatible; MSIE 5.5; Windows NT 5.0)"

**表 19-1　カスタム形式のログ形式ストリング値**

| 形式トークン | 値 |
|---|---|
| %...a | 要求側クライアントの IP アドレス |
| %...A | Content Engine の IP アドレス |
| %...B<br>%...b | HTTP ヘッダーを除く送信バイト数 |
| %...c | 応答完了時の接続ステータス<br><br>X = 応答が完了する前に接続が打ち切られました。<br>+ = 応答の送信後、接続は維持可能。<br>ñ = 応答の送信後、接続はクローズされました。 |
| %...f | ファイル名 |
| %...h | リモート ホスト（要求側クライアントの IP アドレスがロギングされます） |
| %...H | 要求プロトコル |
| %...{Foobar}i | Foobar コンテンツ：サーバに送信される要求中のヘッダー行。Foobar の値は User-Agent、Referer、Host、または Cookie のいずれかをヘッダーにできます。 |
| %...l | リモート ログ名。Content Engine 上には実装されていないので、ハイフン（-）がロギングされます。 |
| %...m | 要求方式 |
| %...p | 要求に対してサービスを提供するサーバの正規ポート。Content Engine 上には適用されないので、ハイフン（-）がロギングされます。 |
| %...P | 要求に対してサービスを提供した子のプロセス ID |
| %...q | 照会ストリング（照会ストリングが存在する場合は ? が先頭に付き、存在しなければ空のストリング） |
| %...r | 要求の先頭行 |
| %...s | ステータス。translog コードは、要求に対して常に HTTP 応答コードを戻します。 |
| %...t | 共通ログ時刻形式（または標準英語形式）の時刻 |
| %...{format}t | 表 19-2 で指定された形式トークンによって指定される形式の時刻 |
| %...T | 要求のサービスに要した時間（秒単位、小数部 3 桁の浮動小数点数値） |
| %...u | リモート ユーザ |
| %...U | 要求された URL パス（照会ストリングを含まない） |
| %...v<br>%...V | ホストが要求の中で指定された場合に報告されるホスト要求ヘッダー フィールドの値。ホスト要求ヘッダーにホストが指定されていない場合は、URL に指定されたサーバの IP アドレスが報告されます。 |

表 19-2 に、表 19-1 にリストされている形式トークン %...{format}t の日付と時刻の形式トークンを示します。

**表 19-2　日付と時刻の形式トークン**

| 形式トークン | 値 |
|---|---|
| %a | 曜日名の省略形 |
| %A | 完全な曜日名 |
| %b | 月名の省略形 |
| %B | 完全な月名 |
| %c | 日付と時刻の表示 |
| %C | 2 桁の整数で表す世紀番号（年 /100） |
| %d | 10 進数で表す月の日付（01 ～ 31） |
| %D | %m/%d/%y の指定と同等（米国以外の国では、%d/%m/%y の使用が一般的であることに注意してください。つまり、世界的にはこの形式はあいまいであるため、使用すべきではありません）。 |
| %e | %d と同じように、10 進数で表す月の日付。ただし、日付の前にあるゼロ（0）はスペースに置き換えられます。 |
| %G | 世紀を 10 進数で表す ISO 8601 で規定された年数。ISO の週番号と対応する 4 桁の年数（%V を参照）。この形式と値は %y と同じですが、ISO 週番号が前年または翌年にわたる場合、代わりにその年が使用されます。 |
| %g | %G と同じですが、世紀部分がありません。つまり、2 桁の年数（00 ～ 99）。 |
| %h | %b と同等 |
| %H | 24 時間制の 10 進数の時間（00 ～ 23） |
| %I | 12 時間制の 10 進数の時間（00 ～ 12） |
| %j | 10 進数で表す年の日付（001 ～ 366） |
| %k | 24 時間制の 10 進数の時間（0 ～ 23）。1 桁の場合は、その数字の前が、ブランクになります（%H も参照）。 |
| %l | 12 時間制の 10 進数の時間（1 ～ 12）。1 桁の場合は、その数字の前が、ブランクになります（%I も参照）。 |
| %m | 10 進数で表す月（01 ～ 12） |
| %M | 10 進数で表す分（00 ～ 59） |
| %n | 改行文字 |
| %p | 所定の時間値に応じて、AM または PM 表示。もしくは、現在のロケールに対応するストリング。正午は pm として、真夜中は am として扱います。 |
| %P | %p と同じですが、小文字表記の am または pm 表記。もしくは、現在のロケールに対応するストリング。 |
| %r | a.m. または p.m. 表記の時間。「%I:%M:%S %p」に相当します。 |
| %R | 24 時間表記の時間（%H:%M）。秒数を含むバージョンの場合、下記の %T を参照。 |
| %s | 規定の日時、すなわち、1970-01-01 00:00:00 UTC 以降の秒数 |
| %S | 10 進数で表す秒（00 ～ 61） |
| %t | タブ文字 |
| %T | 24 時間表記の時間（%H:%M:%S） |
| %u | 10 進数で表す曜日（1 ～ 7）、月曜日を 1 とします（%w も参照） |
| %U | 10 進数で表す現行年の週番号（00 ～ 53）。最初の日曜日を、第 1 週（週 01）の最初の日とします（%V と %W も参照）。 |

表 19-2　日付と時刻の形式トークン（続き）

| 形式トークン | 値 |
|---|---|
| %V | ISO 8601：1988 で規定された現在の年の週番号を 10 進数で表します（01 ～ 53）。第 1 週には、現行年の少なくとも 4 日があり、月曜日が週の第 1 日となります（%U と %W も参照）。 |
| %w | 10 進数で表す曜日（0 ～ 6）、日曜日を 0 とします。%u も参照。 |
| %W | 現行年の週番号を 10 進数で表します（00 ～ 53）。最初の月曜日を、第 1 週（週 01）の最初の日とします。 |
| %x | 時刻部分がない日付の表記 |
| %X | 日付部分がない時刻の表記 |
| %y | 世紀部分がない 10 進数で表す年（00 ～ 99） |
| %Y | 世紀部分を含む 10 進数で表す年 |
| %z | GMT からの相対時間としての時間帯。RFC822 準拠の日付の発行が必要（[%a, %d %b  %Y %H:%M:%S %z] を使用）。 |
| %Z | 時間帯、または名前、または略語 |
| %% | リテラル % 文字 |

## W3C カスタマイズ可能なロギング形式

ACNS ソフトウェアでは、柔軟にロギングできるようにするために、Apache の共通ログ形式（CLF）、Squid 形式、および拡張 Squid 形式などの固定形式とは別に、W3C カスタマイズ可能なロギング形式をサポートしています。

W3C カスタマイズ可能なロギング形式は、基本的なトランスログ（トランザクション ログ）トークンを公開する一連の形式トークンをサポートしています。W3C カスタマイズ可能なロギング形式は、HTTP Web サーバの観点から定義された点に限定されていて、特定の Web キャッシュ固有のカスタム オプション（固定 Squid 形式で提供するオプションなど）を提供しません。結果的に、Cisco および Squid のようなカスタマイズされた新たなロギング フィールドをサポートするために、W3C カスタマイズ可能なロギング形式への拡張機能である新たな形式トークンが、ACNS 5.3 ソフトウェア リリースに追加されました。これらの形式トークンは、W3C カスタマイズ可能なトークン セット内からの Squid のようなロギング形式をサポートできます。

ACNS 5.4 ソフトウェアは、次のトランザクション ロギング形式をサポートします。

- W3C 形式でサポートされていない拡張 Squid と等価な内部トークンのサポート
- 設定済みの HTTP 発信プロキシを Squid スタイルの「DEFAULT_PARENT」階層イベントとして扱う階層トークンのサポート

ACNS 5.4 ソフトウェアには、次の W3C カスタマイズ可能なロギング形式用の特殊なトークン シーケンスが含まれます。

%...{}C

「...」は任意です。指定すると、カンマで区切られた条件付き HTTP 応答コードのシーケンスになります。「C」は大文字「C」を表し、拡張されたカスタマイズ可能な動作トークン セットを指定します。このトークン セットに対してトークンがディレクティブにより指定されます。このディレクティブは、2 文字のトークン ディレクティブです。

拡張 Squid 形式からの既存のディレクティブおよび新規ディレクティブのリストについては、表 19-3 を参照してください。ただし、ACNS 5.4 ソフトウェアでサポートされていても、W3C の定義では現在サポートされていません。

**表 19-3　トランスログのトークン ディレクティブ**

| 形式トークン | 値 |
|---|---|
| %...{es}C | Epox（1970 年 1 月 1 日）からの経過秒数として表示される現在の時刻 |
| %...{em}C | Epox（1970 年 1 月 1 日）からの経過ミリ秒数として表示される現在の時刻 |
| %...{te}C | 要求が完了するまでに、経過したミリ秒数 |
| %...{rd}C | Squid のようなキャッシュ ステータス コード ストリング（たとえば、TCP_HIT および TCP_CLIENT_REFRESH_MISS） |
| %..{cs}C | クライアントに送信されるバイト数（プロトコル ヘッダーを含む） |
| %...{rh}C | Content Engine に適用されるときの厳密な Squid スタイルの階層 |
| %...{rH}CE | 拡張 Squid スタイル階層。「%...{rh}C」と同じですが、発信プロキシが明示的に定義されていて、要求を満たすために使用されるときに「DIRECT/origin_server_ip_address」ではなく「DEFAULT_PARENT/proxy_ip_addess」がロギングされる場合を除きます。 |
| %...{rt}C | 定義したプロトコル ヘッダーによって指定される、応答内にあるオブジェクトの Mime-Type |
| %...{ru}C | 追加照会ストリングを含む、要求されている URL |
| %...{as}C | アプリケーション固有の情報。特定の要求処理アプリケーションは、Squid 形式の仕様の一部としてサポートされている特定のストリングをここでロギングする場合があります。たとえば、SmartFilter URL フィルタリングは、このトークン シーケンスが使用されている情報をロギングします。 |

表 19-3 に一覧表示されているトークンに加え、複数の「%...{xx}C」スタイル トークンを %...{xx}C スタイル内の単一の組み込みトークン シーケンスに凝縮できます。複数のスタイル トークンを単一の組み込みトークン シーケンスに凝縮するには、複数のトークンを {} カッコで囲み、その各トークンの前に「%」記号をつけて指定する必要があります。次に例を示します。

%{rh}C %{rt}C %{as}C

これは、次のように凝縮された組み込みトークン形式でも表現できます。

%{%rh %rt %as}C

コマンドライン構文は、次のように表示された単一のトークンを受け入れます。

%{%rh}C

および

%{rh}C

は、等価な表現です。

組み込みトークン シーケンスの一部ではない文字（たとえば、空白文字など）は、出力ファイル内に文字どおりに繰り返されています。

上記のトークンのセットを使用して、拡張 Squid のような形式の行を W3C カスタマイズ可能なロギング形式仕様の範囲内で設定できます。次に例を示します。

“%{es}C.%{em}C %{te}C %a %{rd}C/%s %{cs}C %m %{ru}C %u %{rh}C %{rt}C %{as}C”

次の例では、Squid の「seconds-since-epoch」タイムスタンプ形式ではなく、ユーザが読み取れるタイムスタンプが使用されていることを指定する拡張 Squid のような形式を示しています。また、設定済みの発信プロキシ（[%...{rH}C] によって指定）がロギングされていることも示しています。

“[%{%d/%b/%Y:%H:%M:%S %z}t] %{te}C %a %{rd}C/%s %{cs}C %m %{ru}C %u %{rH}C %{rt}C %{as}C”

未知またはサポートされていないトランスログ トークンは、ログ ファイル内にトークンを構成する文字としてロギングされています。たとえば、「%{xy}C」はログ ファイルに「xy」とロギングされています。トークン仕様シーケンス外の文字はすべてログ ファイル内部で文字どおりに繰り返されています。

# トランザクション ロギングと NTLM 認証

使用するデバイスが NT LAN Manager（NTLM）認証用に設定されていて、Apache スタイルまたは拡張 Squid スタイルの形式を使用する場合、トランザクション ログの「authenticated username」フィールドに Windows のドメイン名とユーザ名が記録されます。ドメイン名が使用できる場合、ドメイン名とユーザ名の両方が「authenticated username」フィールドに、domain\username の形式で記録されます。username だけが使用できる場合、username だけが「authenticated username」フィールドに記録されます。domainname と username の両方が使用できない場合、「-」（ハイフン）がこのフィールドに記録されます。

# ログ ファイル使用上の注意事項

ここでは、ログ ファイル使用上の注意事項について説明します。

## 作業ログの概要

sysfs がマウントされている場所に応じて、トランザクションは、ローカル ディスク上の作業ログとして次のファイルの 1 つに記録されます。

- /local1/logs/working.log
- /local2/logs/working.log

sysfs がマウントされている場所に応じて、ローカル ディスク上の作業ログとして記録されるログ ファイルは次のとおりです。

- Windows Media Technology（WMT）ログは、ローカル ディスク上の作業ログとして、次のファイルの 1 つに記録されます。
  - /local1/logs/export/working.log
  - /local2/logs/export/working.log
- RealSubscriber ログは、ローカル ディスク上の作業ログとして、次のファイルの 1 つに記録されます。
  - /local1/logs/real-subscriber-logs/working.log
  - /local2/logs/real-subscriber-logs/working.log
- Cisco Streaming Engine ログは、ローカル ディスク上の作業ログとして、次のファイルの 1 つに記録されます。
  - /local1/logs/cisco-streaming-engine/working.log
  - /local2/logs/cisco-streaming-engine/working.log
- RealProxy ログは、ローカル ディスク上の作業ログとして、次のファイルの 1 つに記録されます。
  - /local1/logs/real-proxy/working.log
  - /local2/logs/real-proxy/working.log

## 作業ログのアーカイブ

データをアーカイブ ログに移動して、作業ログをクリアする間隔を指定できます。アーカイブ ログ ファイルは、sysfs がマウントされている場所に応じて、ローカル ディスクの /local1/logs/ ディレクトリまたは /local2/logs/ ディレクトリに置かれます。

複数のアーカイブ ファイルが保存されているので、ファイル名には、ファイルをアーカイブしたときのタイムスタンプが含まれます。また、ファイルは FTP/SFTP サーバにエクスポートできるため、ファイル名には、この Content Engine の IP アドレスも含まれます。

アーカイブ ファイル名は次の形式を使用します。

celog_IPADDRESS_YYYYMMDD_HHMMSS.txt

## トランザクション ログのサニタイズ

トランザクション ログ ファイルのクライアントの IP アドレスおよびユーザ名を隠すことができます。デフォルトでは、トランザクション ログのサニタイズ機能は有効ではありません。サニタイズ機能を有効にすると、トランザクション ログの IP アドレスを 0.0.0.0 に変更することで、クライアントのネットワーク ID を隠します。

## ログ ファイルのエクスポート

キャッシュ ログ ファイルのあと処理を容易にするために、トランザクション ログを外部ホストにエクスポートできます。この機能により、設定可能な間隔で、FTP を使用してログ ファイルを外部ホストに自動的にエクスポートできます。FTP を使用するときのユーザ名とパスワードは設定可能で、ログ ファイルのアップロード先のディレクトリも設定可能です。

ログ ファイルには、自動的に次の形式でファイル名が付けられます。

*<type>_<ipaddr>_yyyymmdd_hhmmss.txt*

ここでファイル名を構成している要素は、次のとおりです。

- *<type>* は、ログ ファイルのタイプを表します。HTTP、HTTPS、FTP などのキャッシュ ログの場合は *celog* です。また、WMT ログの場合は、*mms_export* です。
- *<ipaddr>* は、Content Engine の IP アドレスを表します。
- *yyyymmdd_hhmmss* は、ログをエクスポートするためにアーカイブされたときの日付と時刻を表します。

（注）　WMT ログには、ファイル名に .txt 拡張子がありません。

## 外部 FTP サーバへのトランザクション ログのエクスポート

トランザクション ログを FTP サーバにエクスポートするには、まずトランザクション ログのエクスポートをイネーブルにしてから、FTP または セキュア FTP（SFTP）サーバのパラメータを設定する必要があります。この機能は、最大 4 台の FTP サーバをサポートできます。次の情報が、各ターゲット FTP サーバに必要です。

- サーバの IP アドレス、またはホスト名

  Content Engine は、DNS lookup を行ってホスト名を変換してから、設定にこの IP アドレスを保存します。
- FTP ユーザのログインおよびユーザ パスワード
- 転送されたファイルが書き込まれるディレクトリのパス

  ユーザのログイン用に完全修飾パス、または相対パスを使用します。ユーザは、このディレクトリに対する書き込み権限を所有している必要があります。

また、アーカイブしたログ ファイルを gzip 形式に圧縮してから、外部の FTP サーバにエクスポートすることもできます。圧縮されたファイル名には、.gz 拡張子が付きます。ログ ファイルを圧縮すると、Content Engine と FTP エクスポート サーバ両方で、圧縮していないアーカイブ ファイルに比べて必要なディスク スペースを減らすことができ、またエクスポートするファイルのサイズが小さくなるので、エクスポート時に必要な帯域幅も減らすことができます。

### 外部 FTP サーバからパーマネント エラーを受信後のエクスポートの再開

FTP サーバが Content Engine へパーマネント エラーを返したときは、アーカイブ トランザクション ログは、そのサーバにはエクスポートされません。設定が正しくないサーバに対し、Content Engine のトランザクション ログ エクスポート パラメータを再入力して、このエラー状態をクリアにする必要があります。

パーマネント エラー（Permanent Negative Completion Reply、RFC 959）は、サーバに対する FTP コマンドが受け入れられず、それに対するアクションが取られなかったときに発生します。パーマネント エラーは、無効なユーザのログイン、無効なユーザ パスワード、十分なアクセス権限のないディレクトリや、存在しないディレクトリへのアクセス試行が原因で発生します。

# 外部 SFTP サーバへのトランザクション ログのエクスポート

Secure File Transfer Protocol（SFTP; セキュア ファイル転送プロトコル）サーバへトランザクション ログをエクスポートすることもできます。まず、この機能をイネーブルにしてから、SFTP サーバのパラメータを設定する必要があります。次の情報が、各ターゲット SFTP サーバに必要です。

- SFTP サーバの IP アドレス、またはホスト名

  Content Engine は、DNS lookup を行ってホスト名を変換してから、設定にこの IP アドレスを保存します。
- SFTP ユーザのログインおよびユーザ パスワード
- 転送されたファイルが書き込まれるディレクトリのパス

  ユーザのログイン用に完全修飾パス、または相対パスを使用します。ユーザは、このディレクトリに対する書き込み権限を所有している必要があります。

## 非管理者ユーザの SFTP アクセス

ACNS 5.3.5 ソフトウェア リリースでは、Content Engine 上の SFTP サーバは、非管理者ユーザ（すなわち、ゼロ以外の UID を持ったユーザ）が SFTP を使用して Content Engine にアクセスできるように拡張されました。ACNS 5.3.5 ソフトウェア リリースでは、この新機能をイネーブルまたはディセーブルにする **sshd allow-non-admin-users** および **no sshd allow-non-admin-users** グローバル コンフィギュレーション コマンドが追加されました。デフォルトでは、この機能は Content Engine 上でディセーブルとなっており、非管理者ユーザは SFTP を使用して Content Engine にアクセスできません。この機能をイネーブルにするには、Content Engine で **sshd allow-non-admin-users** コマンドを入力します。この機能をイネーブルにしたあとで Content Engine で **no sshd allow-non-admin-users** コマンドを入力すると再度ディセーブルにできます。

この機能がイネーブルになると、**show running-config** EXEC コマンドの出力には、Content Engine 上で この機能がイネーブルであることが表示されます。

# Content Distribution Manager GUI によるトランザクション ロギングのイネーブル化

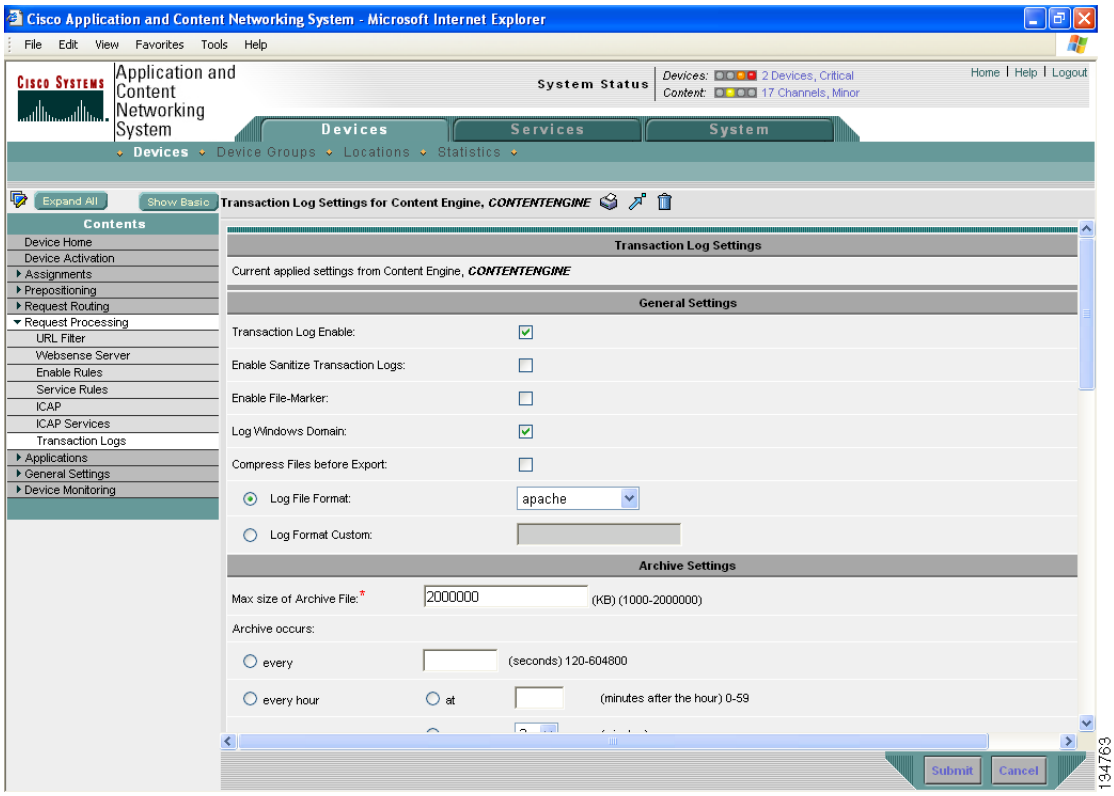
トランザクション ロギングをイネーブルにする手順は、次のとおりです。

**ステップ 1**　Content Distribution Manager GUI から、**Devices > Devices** の順に選択します。

**ステップ 2**　設定する Content Engine の名前の横にある **Edit** アイコンをクリックします。Contents ペインが左側に表示されます。

Contents ペインから、**Request Processing > Transaction Logs** の順に選択します。Transaction Logs settings ウィンドウが表示されます（図 19-1 を参照）。表 19-4 では、このウィンドウ内のフィールドについて説明し、対応する CLI グローバル コンフィギュレーション コマンドを示します。

**図 19-1　Transaction Log Settings ウィンドウ ― 一般設定**




**ステップ 3**　使用しているデバイス上でトランザクション ロギングをアクティブにするには、General Settings という項目の下にある **Transaction Log Enable** チェックボックスにチェックマークを付けます。

**ステップ 4**　クライアントの IP アドレスとユーザ名を隠すには、**Enable Sanitize Transaction Logs** チェックボックスにチェックマークを付けます。

**ステップ 5**　トランザクション　ログにファイルの開始位置と終了位置を示すマーカーを追加するには、**Enable File-Marker** チェックボックスにチェックマークを付けます。

**ステップ 6**　トランザクション ログの「authenticated username」フィールドに Windows ドメイン名とユーザ名を記録するには、**Log Windows Domain** チェックボックスにチェックマークを付けます。

（注）　このオプションが機能するのは、使用しているデバイスが NT LAN Manager（NTLM）認証用に設定されていて、Apache スタイル、または拡張 Squid スタイルのトランザクション ログ形式を使用している場合です。

**ステップ 7**　アーカイブされたログ ファイルを gzip 形式に圧縮してから外部 FTP サーバにエクスポートできるようにするには、**Compress Files before Export** チェックボックスにチェックマークを付けます。

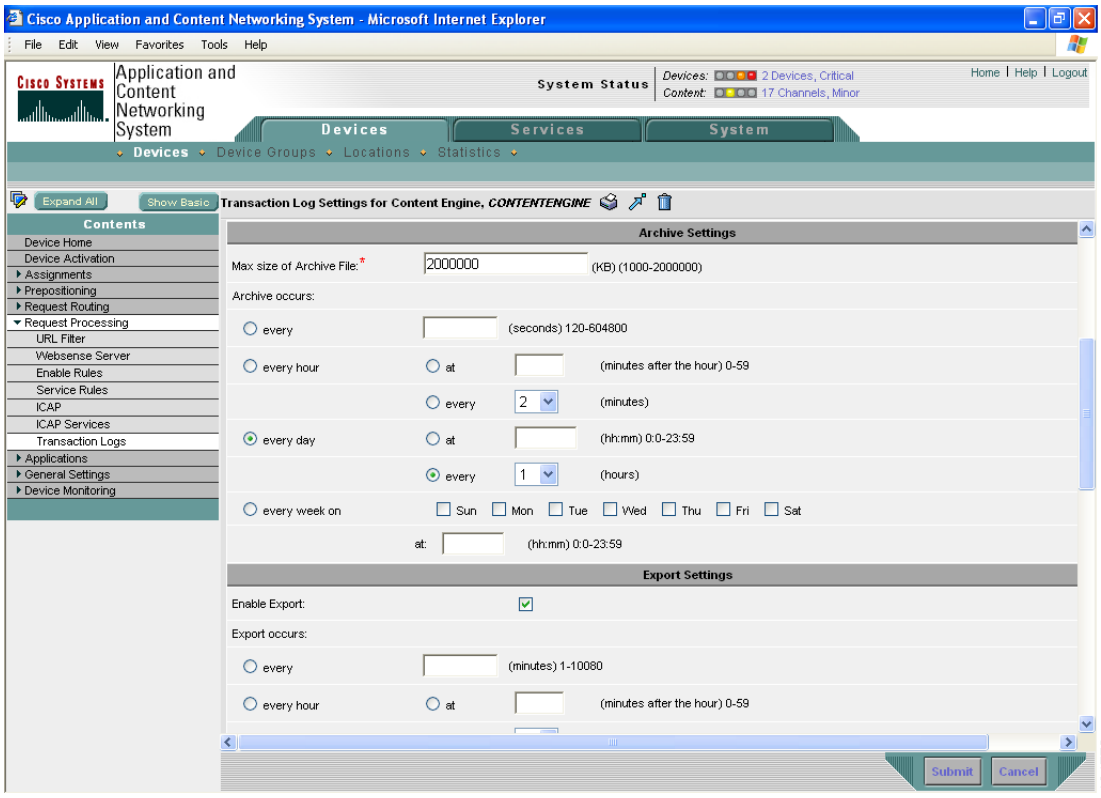
**ステップ 8**　ログ ファイル形式を選択するには、**Log File Format** オプション ボタンをクリックし、ドロップダウン リストからログ ファイル形式を選択します。**apache**、**extended-squid**、または **squid** のいずれかを選択します。

別の方法として、トランザクション ログ用にカスタム形式を使用する場合は、**Log Format Custom** オプション ボタンをクリックしてから、用意されているフィールドにカスタム形式ストリングを入力します（「カスタム形式のトランザクション ロギング」[p.19-3] を参照）。

**ステップ 9**　Archive Settings という項目（図 19-2 を参照）の下の Max Size of Archive File フィールドに、アーカイブ ファイルの最大サイズの値をキロバイト単位で指定します。表 19-4 では、このウィンドウ内のフィールドについて説明し、対応する CLI グローバル コンフィギュレーション コマンドを示します。

この値は、ローカル ディスク上で保持されているアーカイブ ファイルの最大サイズです。

**図 19-2　Transaction Log Settings ウィンドウ — アーカイブ設定**



**ステップ 10** データをアーカイブ ログに移動して作業ログをクリアする間隔をスケジュールに組み込むには、**Archive occurs** セクションで指定されるオプションの中からタイム オプションを選択します。

**ステップ 11** この設定を保存するには、**Submit** をクリックします。

**表 19-4　トランザクション ログの一般設定およびアーカイブ設定**

| GUI パラメータ | 機能 | CLI コマンド |
|---|---|---|
| **General Settings**<br>Transaction Log Enable | Content Engine 上のトランザクション ロギングをイネーブルにします。 | **transaction-logs enable** |
| Enable Sanitize Transaction Logs | クライアントの IP アドレスとユーザ名を隠します。 | **transaction-logs sanitize** |
| Enable File-Marker | トランザクション ログにマーカーを追加して、ファイルの開始位置と終了位置を示します。 | **transaction-logs file-marker** |
| Log Windows Domain | Windows ドメイン名とユーザ名をトランザクション ログの「authenticated username」フィールドに記録します。 | **transaction-logs log-windows-domain** |
| Compress Files before Export | アーカイブしたログ ファイルを外部の FTP サーバにエクスポートする前に、gzip 形式への圧縮をイネーブルにします。 | **transaction-logs export compress** |
| Log File Format | ログ ファイル形式を設定します（**apache**、**extended-squid**、または **squid**）。 | **transaction-logs format** {**squid** \| **extended-squid** \| **apache**} |
| Log Format Custom | カスタム ログ ファイル形式を設定します。 | **transaction-logs format custom** *string* |
| **Archive Settings**<br>Max Size of Archive File | ローカル ディスクに保持するアーカイブ ファイルの最大サイズ（キロバイト単位） | **transaction-logs archive max-file-size** *kilobytes* |
| Archive occurs every（interval） | データをアーカイブ ログに移動することによって作業ログがクリアされる間隔 | **transaction-logs archive interval** {*seconds* \| **every-week** [**on** *weekdays* **at** *hour:minute*] \| **every-day** {**at** *hour:minute* \| **every** *hours*} \| **every-hour** {**at** *minute* \| **every** *minutes*}} |

FTP サーバへのエクスポートをイネーブルにする手順は、次のとおりです。

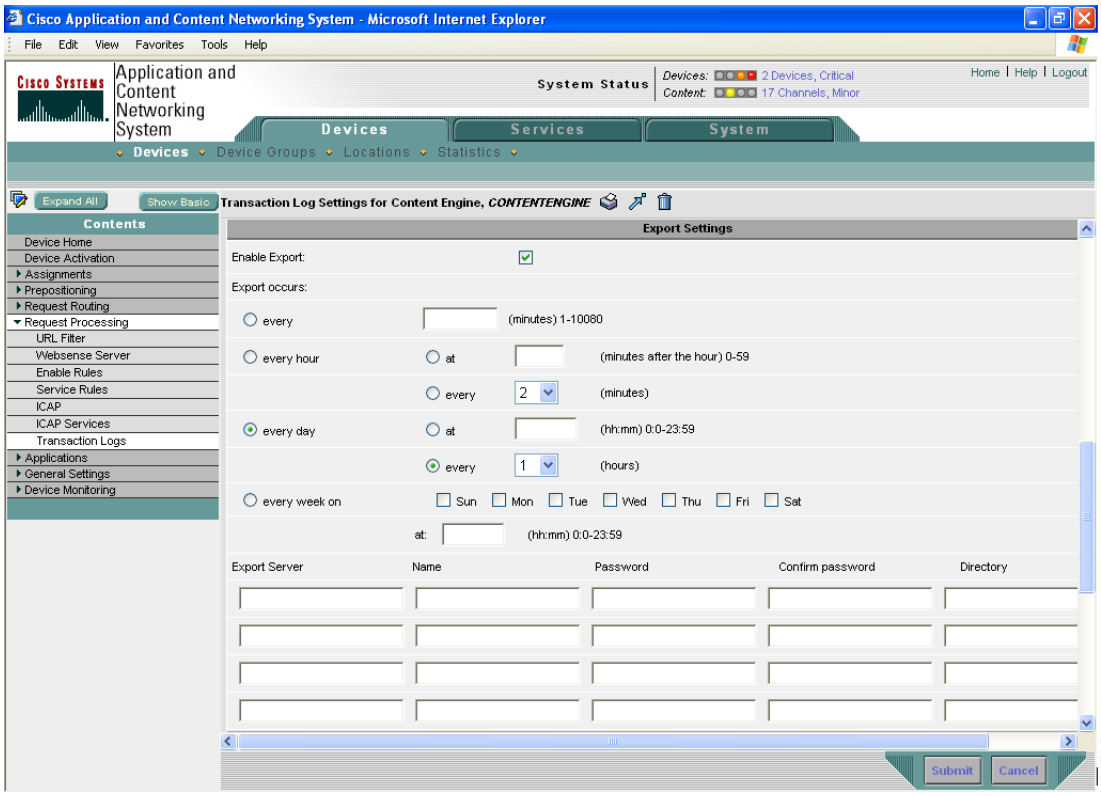
**ステップ 1**　Content Distribution Manager GUI から、**Devices > Devices** の順に選択します。

**ステップ 2**　設定する Content Engine の名前の横にある **Edit** アイコンをクリックします。Contents ペインが左側に表示されます。

**ステップ 3**　Contents ペインから、**Request Processing > Transaction Logs** の順に選択します。Transaction Logs settings ウィンドウが表示されます

**ステップ 4**　Export Settings とうい項目の下の **Enable Export** チェックボックスにチェックマークを付けます(図 19-3 を参照)。表 19-5 では、このウィンドウ内のフィールドについて説明し、対応する CLI グローバル コンフィギュレーション コマンドを示します。

**図 19-3　Transaction Log Settings ウィンドウ — エクスポート設定**




**ステップ 5**　表示されたタイム オプションを使用して、データを FTP サーバに移動して作業ログをクリアする間隔を指定します。

**ステップ 6**　Export Server フィールドに、FTP サーバの IP アドレスまたはホスト名の情報を入力します。

**(注)**　FTP エクスポート機能は、最大 4 台の サーバをサポートできます。各サーバに対して、それぞれ有効なユーザ名、パスワード、ディレクトリを設定する必要があります。

**ステップ 7**　Name フィールドに、ユーザ ID を入力します。

**ステップ 8**　Password フィールドおよび Confirm Password フィールドに、ステップ 7 で指定したユーザのパスワードを入力します。

**ステップ 9**　Directory フィールドに、トランザクション ログを含める作業ディレクトリの名前を入力します。

**(注)**　Name フィールドに指定するユーザは、指定のディレクトリへの書き込み権限を持っている必要があります。

**ステップ 10** 選択されたサーバが セキュア FTP サーバの場合、**SFTP** チェックボックスにチェックマークを付けます。

**ステップ 11** この設定を保存するには、**Submit** をクリックします。

**表 19-5　トランザクション ログ エクスポート設定**

| GUI パラメータ | 機能 | CLI コマンド |
|---|---|---|
| Enable Export | 外部 FTP サーバへのトランザクション ログ エクスポートをイネーブルにします。 | **transaction-logs export enable** |
| Export occurs（interval） | データを FTP または SFTP サーバに移動することによって作業ログがクリアされる間隔 | **transaction-logs export interval** {*minutes* \| **every-week** [**on** *weekdays* **at** *hour:minute*] \| **every-day** {**at** *hour:minute* \| **every** *hours*} \| **every-hour**{**at** *minute* \| **every** *minutes*}} |
| Export Server | FTP サーバの IP アドレスまたはホスト名 | **transaction-logs export ftp-server** {*hostname* \| *servipaddrs*} *login passw directory* |
| Name | ユーザの名前 | |
| Password | ユーザのパスワード | |
| Confirm Password | ユーザのパスワードを確認します。 | |
| Directory | トランザクション ログを含む作業ディレクトリ名 | |
| SFTP | セキュア FTP サーバを設定します。 | **transaction-logs export sftp-server** {*hostname* \| *servipaddrs*} *login passw directory* |

# WMT トランザクション ロギングの使用

企業によっては、ストリーミング メディアは収入源なので、しっかりと動きを把握する必要があります。これらの企業は顧客に対してオンデマンド コンテンツとライブ放送のストリーミング配信を提供して顧客に課金するので、ある特定の顧客が視聴したコンテンツ、コンテンツを視聴している時間、視聴品質を、ログに記録された情報に頼って追跡するしかありません。したがって、トランザクション ロギングの正確さと信頼性は、これらの企業にとって非常に重要です。

Windows Media Services 9 シリーズは、Windows Media Services バージョン 4.1 と比較して、より安定したロギング モデルです。5.4 ソフトウェアは Windows Media Services 9 ロギングに対応しています。

（注）　ACNS ソフトウェア（リリース 5.1 以前）でサポートされていたのは、標準の Windows Media Services バージョン 4.1 および拡張 Windows Media Services バージョン 4.1 のロギング形式だけでした。

ACNS 5.4 ソフトウェアでは、次のロギング形式が WMT トランザクション ロギングでサポートされています。

- 標準 Windows Media Services バージョン 4.1
- 拡張 Windows Media Services バージョン 4.1
- 標準 Windows Media Services バージョン 9.0
- 拡張 Windows Media Services バージョン 9.0

ロギング形式の拡張バージョンには、Content Engine 固有の追加フィールドが含まれます（たとえば、CE-action フィールドはキャッシュ ヒットまたはキャッシュ ミスを指定し、CE-bytes フィールドは Content Engine から送信されたバイト数を指定します）。

WMT ストリーミング用の Content Engine のトランザクション ロギング形式は、Windows Media Service と W3C 準拠のログ形式と整合性が保たれています。ログ行はクライアントがアクセスしたストリームごとに書き込まれます。ログのロケーションを設定することはできません。FTP を使用して、これらのログをエクスポートできます。トランザクション ロギングがイネーブルになっていると、デーモンが /local1/logs/export に WMT トランザクション用の *working.log* ファイルを別個に作成します。

トランザクション ログ内のすべてのクライアント情報は、デフォルトではオリジン サーバへ送信されます。

## Windows Media Services 9 が受け入れるログ形式

Windows Media Player は次のプロトコルを使用して、Windows Media サーバと接続します。

- Windows Media Player バージョン 9.0 より前の Windows Media Player は、HTTP/1.0 または MMS プロトコルを使用します。
- Windows Media Player バージョン 9.0 は、HTTP/1.1 および RTSP を使用します。

Windows Media Player のバージョンによって、ログはテキスト、バイナリ、または Extensible Markup Language（XML）などの異なる形式で送信されます。表 19-6 に、Windows Media Services 9 が受け入れるログ形式を示します。

表 19-6　Windows Media Services 9 ログ形式

| プロトコル | プレーヤーおよびディストリビュータ | ログ タイプ |
|---|---|---|
| HTTP/1.0 | Windows Media Player バージョン 9.0 よりも前。<br>Content Engine（キャッシングとプロキシ サーバ）は Windows Media Services バージョン 9.0 を実行し、Windows Media Services 4.1 を実行している WMT サーバからストリーミングを行います。 | W3C 標準スペース区切りテキスト ログ |
| MMS | Windows Media Player バージョン 9.0 よりも前 | バイナリ構造のログ |
| HTTP/1.1 | Windows Media Player バージョン 9.0<br>配信サーバは Windows Media Services 9.0 を実行します。<br>Content Engine（キャッシングとプロキシ サーバ）は Windows Media Services 9.0 を実行します。 | XML 構造のログ |
| RTSP | Windows Media Player バージョン 9.0<br>配信サーバは Windows Media Services 9.0 を実行します。<br>Content Engine（キャッシングとプロキシ サーバ）は Windows Media Services 9.0 を実行します。 | XML 構造のログ |

（注）　ACNS 5.4 ソフトウェアは、MMS-over-HTTP 用の XML ロギングをサポートします。Windows Media Player から Content Engine（Windows Media サーバ）に送られた XML ログ ファイルは解析され、Content Engine 上に保管されている通常の WMT トランザクション ログに保存されます。ACNS ソフトウェアでは現在、MMS-over-RTSP（Windows Media Services 9 経由の RTSP）はサポートされて*いません。*

## WMT トランザクション ロギングの設定

WMT トランザクション ロギングを設定する手順は、次のとおりです。

**ステップ 1**　Content Engine の Transaction Logs Settings ウィンドウに進みます。

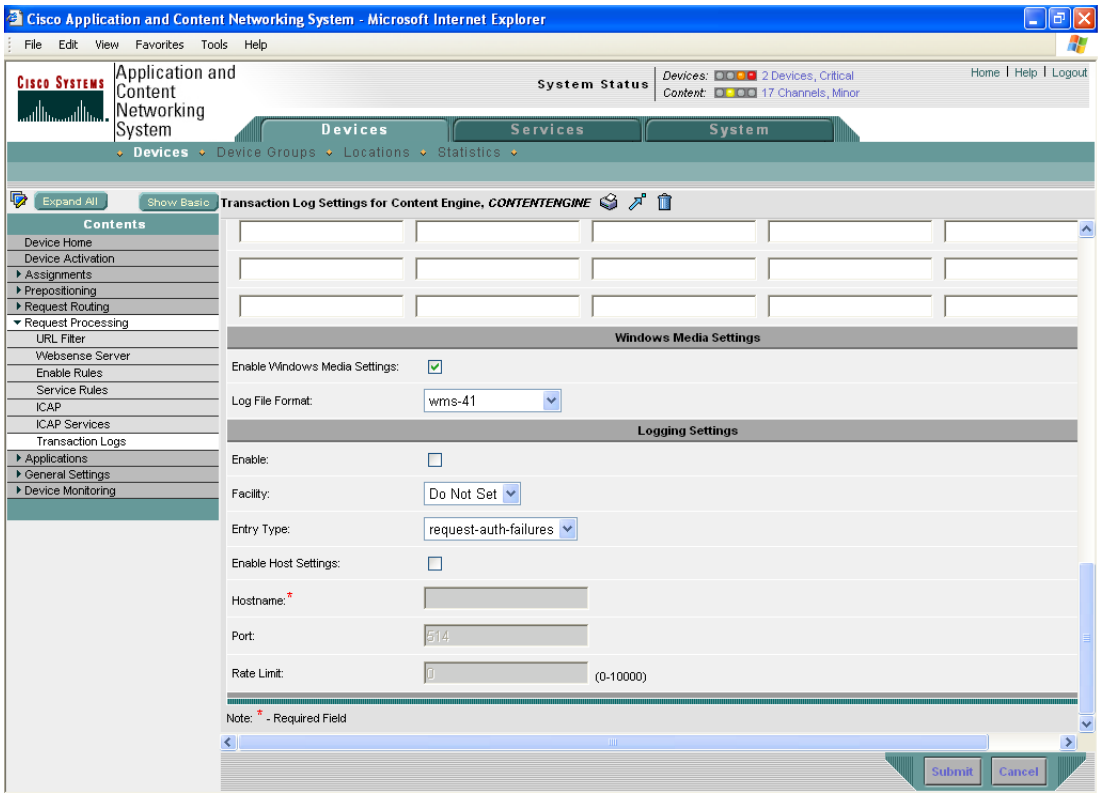
a. Content Distribution Manager GUI から、**Devices > Devices** の順に選択します。

b. 設定する Content Engine の名前の横にある **Edit** アイコンをクリックします。Contents ペインが左側に表示されます。

c. Contents ペインから、**Request Processing > Transaction Logs** の順に選択します。Transaction Logs Settings ウィンドウが表示されます（図 19-1 を参照）。

**ステップ 2**　WMT ストリーミング セッションのトランザクション ログを生成するには、WMT Settings という項目（図 19-4 を参照）の下で、**Enable WMT Settings** チェックボックスにチェックマークを付けます。

図 19-4　Transaction Log Settings ウィンドウ — WMT とロギング設定




**ステップ 3**　**Log File Format** ドロップダウン リストから WMT トランザクション ログ用のロギング形式を選択します。表 19-7 に、ドロップダウン リストのオプションを示します。

表 19-7　WMT ログ ファイル形式のオプション

| ログ形式 | 説明 |
|---|---|
| extended | トランザクション ログ用 WMT 拡張設定を指定します。WMT トランザクション ログで、ユーザ名ロギングをイネーブルにします。 |
| wms-41 | WMT をセットして、拡張 Windows Media Services 4.1 形式でトランザクション ログを生成します。<br><br>このオプションを使用すると、Content Engine は標準 Windows Media Services 4.1 形式を使用してトランザクション ログを生成します。Content Engine には、トランザクション ログに次の 3 つの追加フィールドが含まれます。<br><br>• CE_action（キャッシュ ヒットまたはキャッシュ ミス）<br>• CE-bytes（1 回のキャッシュ ヒットに対して Content Engine から送信されたバイト数）<br>• username（NTLM、Negotiate、Digest、基本認証が使われる場合の WMT 要求のユーザ名） |

表 19-7　WMT ログ ファイル形式のオプション（続き）

| ログ形式 | 説明 |
|---|---|
| wms-90 | WMT をセットして、拡張 Windows Media Services 9 形式でトランザクション ログを生成します。<br><br>このオプションを使用すると、Content Engine は標準 Windows Media Services 9 形式を使用してトランザクション ログを生成します。Content Engine には、トランザクション ログに次の 3 つの追加フィールドが含まれます。<br><br>• CE_action（キャッシュ ヒットまたはキャッシュ ミス）<br>• CE-bytes（1 回のキャッシュ ヒットに対して Content Engine から送信されたバイト数）<br>• username（NTLM、Negotiate、Digest、基本認証が使われる場合の WMT 要求のユーザ名） |
| wms-41 | WMT をセットして、標準 Windows Media Services 4.1 形式でトランザクション ログを生成します。 |
| wms-90 | WMT をセットして、標準 Windows Media Services 9 形式でトランザクション ログを生成します。 |

CLI から WMT トランザクション ロギングを設定するには、次のグローバル コンフィギュレーション コマンドを使用します。

**wmt transaction-logs format** {**extended** {**wms-41** | **wms-90**} | **wms-41** | **wms-90**}

# リアルタイム トランザクション ロギングの使用

認証エラーなどの特定のエラーをトランザクション ログでリアルタイムにモニタできます。HTTP トランザクション ログ メッセージをリモート Syslog サーバに送信することによって、リアルタイムでリモート Syslog サーバをモニタでき、HTTP 要求の認証失敗を確認できます。このリアルタイム トランザクション ログ機能を使用すると、リアルタイムで HTTP 要求認証エラーなどの特定のエラーのトランザクション ログをモニタできます。ローカル ファイル システムへの既存のトランザクション ロギングは変更されないままです。

このリアルタイムでのモニタを行うために、UDP を転送プロトコルとして使用して、トランザクション ログ メッセージをリモート Syslog サーバに送信するように Content Engine を設定する必要があります。UDP は信頼性の低い転送プロトコルであるため、リモート Syslog ホストに対する転送メッセージは信頼できません。そこで、リモート Syslog サーバで受信する Syslog メッセージをモニタする必要があります。トランザクション ロギング モジュールがリモート Syslog サーバへメッセージを送信する速度を制限できます。Syslog メッセージの形式は、Syslog ログ メッセージのペイロードとして、トランザクション ログ メッセージと一緒に、標準 Syslog ログ メッセージ形式の中にあります。

リモート Syslog サーバへのリアルタイム トランザクション ロギングは、トランザクション ログ エントリとしてメッセージ ペイロードと一緒に標準 Syslog ログ メッセージ形式を使用します。新しい Syslog エラー ID が、このタイプのリアルタイム トランザクション ログ メッセージ用に定義されています。Content Engine を設定して、1 台のリモート Syslog ホストへトランザクション ログ メッセージをリアルタイムで送信できます。リモート Syslog ホストへのトランザクション ログ エントリのメッセージ形式は、トランザクション ログ ファイル形式と同じで、Cisco 標準 Syslog ヘッダー情報の先頭に追加されます。

トランザクション ロギング モジュール（Content Engine）からリモート Syslog ホストへ送信されたリアルタイム Syslog メッセージの形式の例を次に示します。

*fac-pri* Apr 22 20:10:46 ce-host cache:%CE-TRNSLG-6-460012:*translog formatted msg*

このメッセージ内のフィールドは、次のとおりです。

- *fac-pri* は、ファシリティ パラメータ、および 32 ビットの 10 進数値 0 から 1023（0x0000 および 0x03FF）として（標準 Syslog 形式として）符号化されたトランザクション ログ メッセージのプライオリティを示します。最下位 3 ビットはプライオリティ（0 - 7）を、次の下位 7 ビットはファシリティ（0 - 127）を示します。

  リアルタイム トランザクション ログ メッセージがリモート Syslog ホストにロギングされる場合、このトランザクション ロギング モジュールが使用するファシリティ パラメータは「user」です。トランザクション ロギングに異なるファシリティ パラメータを設定しないかぎり、同じファシリティがリモート Syslog ホストに送信されます。Priority フィールドは、リアルタイム トランザクション ログ メッセージに対して常に LOG_INFO に設定されています。

  上記の例で、*fac-pri* のデフォルト値は 14（0x000E）であり、この場合 facility = user（LOG_USER [1]）および priority = LOG_INFO（6）です。
- メッセージ内の次のフィールドは日付で、上記の例のような形式です。
- *ce-host* は、メッセージを送信している Content Engine のホスト名、または IP です。
- *cache* はメッセージを送信している Content Engine 上のプロセス名です。
- %CE-TRNSLG-6-460012 は、リアルタイム トランザクション ログ メッセージの Content Engine 上の Cisco 標準形式 Syslog ヘッダーです。この識別子は、プライオリティ レベル 6 で、情報のメッセージを示します。

（注） Content Engine システムの Syslog メッセージは、トランザクション ロギング用に設定されたリモート Syslog ホストとの通信エラーを報告します。これらの Syslog メッセージは、エラー メッセージの範囲内（%CE-TRNSLG-6-460013 ～ %CE-TRNSLG-3-460016）にあります。最後のエラー メッセージ（%CE-TRNSLG-3-460016）は、「6」（情報レベル メッセージ用）ではなくレベル「3」（エラー レベル メッセージ用）を示していることに注意してください。情報レベル メッセージは、レート制限のためメッセージを廃棄した場合に報告され、廃棄されたメッセージの数が報告されます。これらの Syslog メッセージの詳細については、『*ACNS Syslog Error Book*』を参照してください。

- *translog formatted msg* は、トランザクション ログ ファイル内に表示されるトランザクション ログ メッセージです。

（注） リアルタイム Syslog メッセージの合計長は、1024 文字です。実際のトランザクション ログ エントリがこの制限を超えると、切り捨てられます。

トランザクション ログにユーザ名とドメイン名を含めるには、**Log Windows Domain** のチェックボックスにチェックマークをつけるか、または **transaction-logs log-windows-domain** グローバル コンフィギュレーション コマンドを使用します。

リモート Syslog サーバは、このメッセージをファイルにロギングします。このメッセージ形式は、次のように表示されます。

Apr 22 20:10:46 ce-host cache:%CE-TRNSLG-6-460012:*translog formatted msg*

この場合 ce-host は、リモート Syslog サーバへリアルタイム トランザクション ログ メッセージを送信した Content Engine のホスト名です。

トランザクション ログ用のホストの設定は、リアルタイム トランザクション ログ用メッセージのプライオリティ レベルを指定する必要がない点を除いて、Syslog メッセージ用の設定と同じです。すべてのメッセージはプライオリティレベル 6（LOG_INFO）に関連付けられます。プライオリティレベルに基づいてメッセージをフィルタリングする必要はありません。

## リアルタイム トランザクション ロギングの設定

リアルタイム トランザクション ロギングを設定する手順は、次のとおりです。

**ステップ 1**　Content Engine の Transaction Logs Settings ウィンドウに進みます。

a. Content Distribution Manager GUI から、**Devices > Devices** の順に選択します。

b. 設定する Content Engine の名前の横にある **Edit** アイコンをクリックします。Contents ペインが左側に表示されます。

c. Contents ペインから、**Request Processing > Transaction Logs** の順に選択します。Transaction Logs settings ウィンドウが表示されます（図 19-1 を参照）。

**ステップ 2**　リアルタイム トランザクション ロギングをイネーブルにするには、Logging Settings セクション（図 19-4 を参照）の下で、**Enable** チェックボックスにチェックマークを付けます。チェックボックスにチェックマークを付けず、リアルタイム トランザクション ロギングを一時的にディセーブルにしても、トランザクション ログ用ロギング ホスト設定は保持できます。この新しいロギングオプションは、キャッシュの HTTP トランザクション ログ エントリにのみ適用されます。リアルタイム トランザクション ロギング機能は、デフォルトではディセーブルです。

（注）　**Enable** チェックボックスにチェックマークを付ける前に、General settings セクションの **Transaction Log Enable** チェックボックスにチェックマークを付ける必要があります。そうしないと、Content Engine 全体のトランザクション ロギングをイネーブルにしないかぎり、2 番めの設定は適用されません。

**ステップ 3**　Facility ドロップダウン リストから、適切なトランザクション ログ ファシリティを選択します。

このドロップダウン リストは *Do not set* の初期値に設定されています。この設定は、Syslog ホストに送信されるファシリティが、Syslog メッセージを送信しているローカル ホスト上のファシリティであることを示しています。たとえば、リアルタイム トランザクション ログ メッセージを送信するトランザクション ロギング モジュールの場合、ファシリティは、「ユーザ」ファシリティです。

**ステップ 4**　Entry Type ドロップダウン リストから、Content Engine からリモート Syslog ホストへロギングするトランザクション タイプを選択します。**request-auth-failures** を選択すると、HTTP 要求の認証失敗に関連するトランザクションのみをリモート Syslog ホストへ送信します。**all** を選択すると、すべてのトランザクション メッセージをリモート Syslog ホストへ送信します。「リモート Syslog ホストへロギングするときのトランザクション ログ エントリ タイプの指定」（p.19-24）を参照してください。

**ステップ 5**　トランザクション ログ ファイルのリモート Syslog ホストへの送信をイネーブルにするには、**Enable Host Settings** チェックボックスにチェックマークを付けます。

**ステップ 6**　Hostname フィールドに、トランザクション ログを送信する必要があるリモート Syslog サーバのホスト名、または IP アドレスを入力します。デフォルトでは、リモート Syslog サーバは指定されていません。

**ステップ 7**　Port フィールドで、Content Engine がメッセージを送信する必要があるリモート Syslog ホストの宛先ポートを指定します。デフォルト ポート番号は 514 です。このポートはシステム ロギングでよく知られているポートです。

**ステップ 8**　Rate Limit フィールドで、1 秒間にリモート Syslog ホストへ送信を許可されるメッセージの数を指定します。帯域幅および他のリソース使用量を制限するには、リモート Syslog ホストへのメッセージのレートを制限します。この制限を超えた場合は、指定したリモート Syslog ホストはメッセージを廃棄します。デフォルトではレート制限はありません（レート制限は 0 に設定されています）。また、デフォルトでは、すべての Syslog メッセージはすべての設定済み Syslog ホストに送信されます。範囲は 1 秒間に 1 ～ 10,000 メッセージです。

**ステップ 9**　この設定を保存するには、**Submit** をクリックします。

デフォルトまたはデバイス グループの設定を適用したあとに、保存する必要のある変更内容が保留されている場合、「Click Submit to Save」というメッセージが現在の設定の横に赤で表示されます。また、**Reset** をクリックすると、以前の設定に戻すこともできます。**Reset** ボタンが表示されるのは、デフォルトまたはグループ設定値を適用して現在のデバイス設定値を変更したにもかかわらず、まだそれらを更新していない場合だけです。

変更した設定を保存せずにこのウィンドウから離れようとすると、変更内容の保存を求める警告ダイアログボックスが表示されます。このダイアログボックスは、Internet Explorer のブラウザを使用中にのみ表示されます。

---

## リモート Syslog ホストへロギングするときのトランザクション ログ エントリ タイプの指定

Content Engine は、HTTP 要求の認証失敗に関連付けられているトランザクションのみを送信するように、または、すべてのトランザクションを送信するように設定できます。

一般的に、組織が興味をもつのはセキュリティ目的による HTTP 要求の認証失敗のみです。これらの認証失敗のタイプをリアルタイムでモニタすることで、組織は、どのエンド ユーザが Content Engine を経由した認証に失敗したかを識別できます。

認証サーバに接続しようとしたエンド ユーザに関連付けられている認証失敗トランザクションのみがロギングされます。認証サーバに接続したトランザクションからの応答を待っている「保留中」トランザクションは、ロギングされません。この方法により、どのユーザが Content Engine での認証に失敗したかを判別するときに必要な情報を得ることができ、Syslog ホストへのトラフィックを最小限にします。どのユーザが認証に失敗したかを追跡するには、拡張 Squid スタイル形式、またはカスタム形式トークン %u 付きのカスタム ログ形式のいずれかを設定することによって、ユーザ名をロギングするトランザクション ログ形式を設定する必要があります。トランザクション ログの形式指定の詳細については、「トランザクション ログ形式の概要」（p.19-2）および「カスタム形式のトランザクション ロギング」（p.19-3）を参照してください。

**Enable** チェックボックスにチェックマークを付けて（または **transaction-logs logging enable** グローバル コンフィギュレーション コマンドを指定して）リアルタイム トランザクション ロギングをイネーブルにする場合、HTTP 要求の認証失敗に関するロギングだけがデフォルトです。このデフォルトを変更してすべてのトランザクションをロギングする場合、Entry Type ドロップダウン リストから **all** を選択します（または Content Engine で **transaction-log logging entry-type all** グローバル コンフィギュレーション コマンドを入力します）。ただし、すべてのトランザクションをロギングすると、Syslog ホストが着信トラフィックを処理できない場合に、UDP の速度が大幅に落ちることがあります。