CHAPTER 21

スタンドアロン Content Engine とトランザクションのモニタリング

この章では、ローカルで管理される構成（スタンドアロン Content Engine）をモニタリングする方法を説明します。この章の内容は、次のとおりです。

（注） ACNS 5.3.1 ソフトウェアおよびそれ以降のリリースでは、Secure File Transfer Protocol（SFTP）を使用して Content Engine に接続し、ログ ファイルを安全に取得できます。

この章で使用する CLI（コマンドライン インターフェイス）コマンドの構文および使用方法については、『*Cisco ACNS Software Command Reference*』Release 5.5 を参照してください。Content Router、Content Distribution Manager、または Content Distribution Manager に登録されている Content Engine（Content Distribution Manager に登録されていないスタンドアロン Content Engine とは異なる）のモニタリングについては、『*Cisco ACNS Software Configuration Guide for Centrally Managed Deployment*』Release 5.5 を参照してください。

スタンドアロン Content Engine のモニタリング

パフォーマンスを測定して、設定の調整に必要な兆候を見つけたり、Content Engine を追加導入したりするためには、Content Engine をモニタすることが重要です。ここでは、SNMP（簡易ネットワーク管理プロトコル）と ACNS ソフトウェア アラームを使用してスタンドアロン Content Engine をモニタリングする方法を説明します。ACNS 5.2.1 ソフトウェアおよびそれ以降のリリースが実行されているスタンドアロン Content Engine のパフォーマンスをモニタリングするために、複数のツールが用意されています。これらのツールには、Cisco Discovery Protocol（CDP）、SNMP、ACNS ソフトウェア アラームなどがあります。詳しくは、次の項を参照してください。

- CDP によるスタンドアロン Content Engine のモニタリング（p.21-2）
- SNMP によるスタンドアロン Content Engine のモニタリング（p.21-2）
- ACNS ソフトウェア アラームによるスタンドアロン Content Engine のモニタリング（p.21-11）

CDP によるスタンドアロン Content Engine のモニタリング

CDP は、すべての Cisco 製デバイス上で実行されるデバイス ディスカバリ プロトコルです。CDP を使用すると、ネットワーク内の各デバイスは、定期的なメッセージをネットワーク内の他のすべてのデバイスに送信します。これらのデバイスは、他のデバイスから送信される定期的なメッセージを受信して、近隣デバイスについての情報を入手し、近隣デバイスのインターフェイスの状況を判断します。

CDP により、ネットワーク管理アプリケーションは、近隣デバイスのデバイス タイプ、および SNMP エージェント アドレスを確認できます。その後、アプリケーションは、ネットワーク内で SNMP 照会を送信できます。また CiscoWorks2000 は、ブート後に Content Engine から送信される CDP パケットを認識することによって、Content Engine の存在を知ります。

Content Engine 関連のタスクが Content Engine プラットフォームの存在、タイプ、およびバージョンをシステム マネージャに通知するには、Content Engine プラットフォームが CDP をサポートしている必要があります。

次の例では、単一の CLI コマンドによってスタンドアロン Content Engine での CDP の実行をイネーブルにします。

```
ContentEngine(config)# interface FastEthernet 0/0 cdp enable
```

SNMP によるスタンドアロン Content Engine のモニタリング

SNMP は、相互運用可能な標準ベースのプロトコルであり、SNMP エージェントによる Content Engine の外部モニタリングを可能にします。

SNMP 管理ネットワークは、3 つの主要なコンポーネントで構成されています。それらは、管理対象デバイス、エージェント、および管理システムです。

- 管理対象デバイスとは、SNMP エージェントを含む、管理対象ネットワークに置かれるネットワーク ノードです。
- 管理対象デバイスは、管理情報の収集と保存を行い、SNMP を使用して、SNMP を使用する管理システムにこの情報を提供します。管理対象デバイスには、ルータ、アクセス サーバ、スイッチ、ブリッジ、ハブ、コンピュータ ホスト、およびプリンタがあります。
- SNMP エージェントとは、管理対象デバイスに置かれるソフトウェア モジュールです。エージェントは、管理情報をローカルで認識し、SNMP と互換性のある形式にその情報を変換します。SNMP エージェントは、MIB（管理情報ベース）からデータを収集します。MIB は、デバイス パラメータとネットワーク データについての情報のリポジトリです。このエージェントは、トラップまたは特定イベントの通知を、マネージャに送信することもできます。

ACNS 5.x ソフトウェアを実行している各 Content Engine には、Content Engine のデバイス設定およびアクティビティに関する情報収集の役割を担う SNMP エージェントがあります。この SNMP 情報にアクセスするには、SNMP 管理アプリケーションが管理ステーション上に導入済みであることが必要です。この SNMP 管理ステーションは、Content Engine から情報を取得するために、SNMP を使用してデバイス エージェントに SNMP Get 要求を送信することから、SNMP ホストと呼ばれます。

SNMP 管理ステーションとデバイス エージェント（Content Engine 上の SNMP エージェント）は、SNMP を使用して次のような通信を行います。

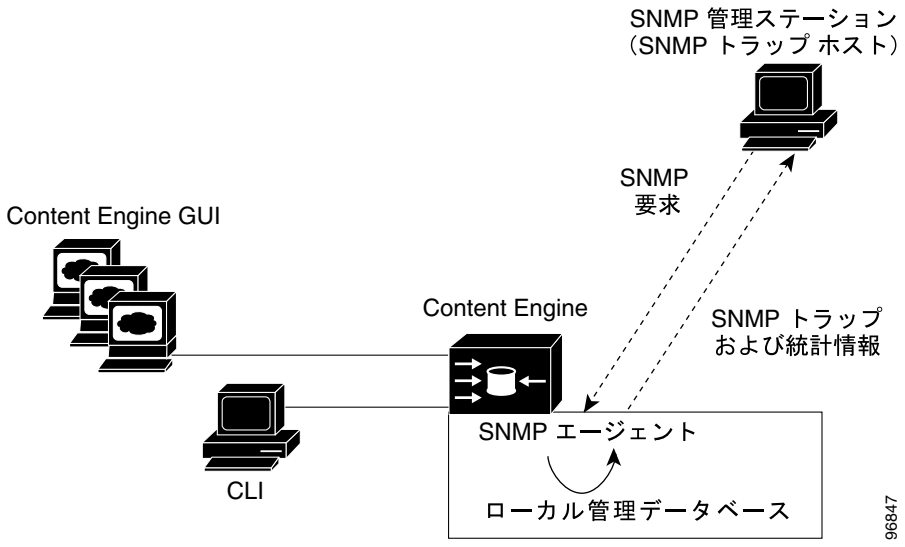
1. SNMP 管理ステーション（SNMP ホスト）は、SNMP を使用して Content Engine から情報を要求します。
2. SNMP 要求の受信後、Content Engine 上のデバイス エージェントは、各デバイス（Content Engine）に関する情報を含むテーブルにアクセスします。このテーブル、すなわちデータベースは、MIB（管理情報ベース）と呼ばれます。

（注）　Content Engine 上の SNMP エージェントは、通常ではない状況下では、SNMP ホストとの通信を開始するのみです。このエージェントは、ホストへ送信する必要のあるトラップが設定されているときに通信を開始します。詳細は、「SNMP トラップを送信するためのスタンドアロン Content Engine の設定」（p.21-8）を参照してください。

3. デバイス エージェントは、MIB 内で指定された情報を特定すると、SNMP を使用してその情報を SNMP 管理ステーションに送信します。

図 21-1 に、Content Engine がスタンドアロンの場合の、SNMP の動作を示します。

図 21-1　スタンドアロン ACNS Content Engine での SNMP コンポーネント



SNMP の各種バージョンの概要

ACNS 5.x ソフトウェアは、次のバージョンの SNMP をサポートします。

- バージョン 1（SNMPv1）：これは、最初に実現された SNMP です。機能の詳細については、RFC 1157 を参照してください。
- バージョン 2（SNMPv2c）：これは、2 番めのリリースの SNMP であり、RFC 1902 に記述されています。データ タイプ、カウンタ サイズ、およびプロトコル オペレーションに機能が追加されました。
- バージョン 3（SNMPv3）：これは、最新バージョンの SNMP であり、RFC 2271 ～ RFC 2275 で定義されています。

SNMP セキュリティ モデルとセキュリティ レベル

SNMPv1 と SNMPv2c には、SNMP パケット トラフィックを機密にするセキュリティ（認証またはプライバシ）メカニズムがありません。その結果、通信回線上のパケットをのぞき見することが可能であり、SNMP コミュニティ ストリングが漏えいする可能性があります。

SNMPv1 と SNMPv2c のセキュリティ上の欠点を補うために、SNMPv3 は、ネットワーク上のパケットの認証と暗号化を行って、Content Engine への安全なアクセスを確保します。ACNS 5.x ソフトウェアの SNMP エージェントは、SNMPv1 と SNMPv2c 以外に、SNMPv3 もサポートしています。

SNMPv3 は、次のセキュリティ機能を備えています。

- メッセージの完全性：伝送中のパケットが何の干渉もされないようにします。
- 認証：メッセージが正当な送信元から発信されたかどうかを判別します。
- 暗号化：パケットの内容を暗号化して、無許可の送信元から見えないようにします。

SNMPv3 は、セキュリティ モデルだけでなく、セキュリティ レベルも備えています。セキュリティ モデルとは、ユーザ、およびそのユーザが属するグループ用に設定された認証プロセスです。セキュリティ レベルとは、セキュリティ モデル内で許容されるセキュリティのレベルです。セキュリティ モデルとセキュリティ レベルを組み合わせると、SNMP パケットの処理時にどのセキュリティ プロセスを使用するかが決まります。セキュリティ モデルは SNMPv1、SNMPv2c、および SNMPv3 の 3 つがあります。

表 21-1 に、セキュリティ モデルとセキュリティ レベルの組み合わせを示します。

表 21-1　SNMP セキュリティ モデルとセキュリティ レベル

モデル	レベル	認証	暗号化	プロセス
v1	noAuthNoPriv	コミュニティ ストリング	なし	ユーザ認証にコミュニティ ストリングの一致を使用する。
v2c	noAuthNoPriv	コミュニティ ストリング	なし	ユーザ認証にコミュニティ ストリングの一致を使用する。
v3	noAuthNoPriv	Username	なし	ユーザ認証にユーザ名の一致を使用する。
v3	AuthNoPriv	Message Digest 5（MD5）または Secure Hash Algorithm（SHA）	なし	Hash-Based Message Authentication Code（HMAC）-MD5、または、HMAC-SHA アルゴリズムに基づいて、認証を行う。
v3	AuthPriv	MD5 または SHA	あり	HMAC-MD5 または HMAC-SHA アルゴリズムに基づいて認証を行う。Cipher Block Chaining（CBC）-DES（DES-56）標準に基づいて、Data Encryption Standard（DES）の 56 ビット暗号化（パケット認証）を行う。

SNMPv3 エージェントは、次のモードで使用できます。

- noAuthNoPriv モード（パケットに対してオンになっているセキュリティ メカニズムがない）

- AuthNoPriv モード（プライバシ アルゴリズム [DES 56] を使用して暗号化する必要がないパケット用）
- AuthPriv モード（暗号化が必要なパケット用。プライバシとしては、パケットに対して認証が実行されることを要求する）

SNMPv3 を使用すると、ユーザは、データ改ざんの心配をすることなく、SNMP エージェントから管理情報を安全に収集できます。また、Content Engine の設定を変更する SNMP セット パケットなどの機密情報が暗号化されるので、ワイヤ上で内容が流出するのを防止できます。さらに、グループ ベースの管理モデルでは、異なるユーザが、異なるアクセス権限を使用して、同じ SNMP エージェントにアクセスすることも可能です。

サポートされる MIB

ACNS 5.x ソフトウェアの SNMP の実装は、次の MIB をサポートしています。

- MIB-II
- ENTITY-MIB
- HOST-RESOURCES-MIB
- CISCO-CONTENT-ENGINE-MIB
- CISCO-ENTITY-ASSET-MIB
- CISCO-CONFIG-MAN-MIB
- CISCO-CDP-MIB

（注） ACNS 5.2.1 ソフトウェアおよびそれ以降のリリースでは、CISCO-CONTENT-ENGINE-MIB がストリーミング WMT（MMS および MMS-over-HTTP）、RealProxy、および Cisco Streaming Engine の統計情報をサポートします。スタンドアロン Content Engine では、WMT と RealProxy がサポートされます

Cisco Streaming Engine は、Content Distribution Manager に登録された Content Engine でのみサポートされます。Cisco Streaming Engine は、スタンドアロン Content Engine ではサポートされません。ACNS 5.5 ソフトウェアでは、CISCO-CONTENT-ENGINE-MIB は MMS-over-HTTP に対してのみストリーミング WMT をサポートします。

（注） ACNS 5.3.1 ソフトウェア リリースでは、CISCO-CONTENT-ENGINE-MIB が変更され、Windows Media 9 クライアントおよびサーバ（Windows Media 9 Player および Windows Media 9 サーバ）用の WMT RTSP ストリーミングがサポートされるようになりました。

ACNS 5.2.1 ソフトウェアおよびそれ以降のリリースでは、SNMP と Node Health Manager の整合性を保つため、CISCO-CONTENT-ENGINE-MIB に 6 つの汎用アラーム トラップが備わっています。6 つの汎用アラーム トラップのリストについては、表 21-5 を参照してください。

ACNS 5.1.1 ソフトウェアおよびそれ以降のリリースでは、Content Engine 上で SNMP アクセスを制御するために、IP Access Control List（ACL; アクセス制御リスト）を使用できます。IP ACL の詳細な定義については、第 19 章「スタンドアロン Content Engine での IP アクセス制御リストの作成と管理」を参照してください。

スタンドアロン Content Engine への MIB ファイルのダウンロード

次の Cisco FTP サイトから MIB ファイルをダウンロードすることにより、ACNS 5.x ソフトウェアが実行されているスタンドアロン Content Engine でサポートされているすべての MIB を入手できます。

ftp://ftp.cisco.com/pub/mibs/v2

各 MIB で定義されている MIB オブジェクトの説明は、上述の FTP サイトにある MIB ファイルに記載されています。

スタンドアロン Content Engine での SNMP エージェントのイネーブル化

デフォルトでは、スタンドアロン Content Engine 上での SNMP エージェントはディセーブルとなっており、SNMP コミュニティ ストリングは定義されていません。SNMP コミュニティ ストリングは、スタンドアロン Content Engine 上の SNMP エージェントにアクセスする際に、認証用パスワードとして使用されます。認証されるには、スタンドアロン Content Engine に送信されるすべての SNMP メッセージに含まれる Community Name フィールドが、そのスタンドアロン Content Engine 上で定義された SNMP コミュニティ ストリングと一致する必要があります。

SNMP コミュニティ ストリングが Content Engine 上で定義されていると、SNMP エージェントはスタンドアロン Content Engine 上でイネーブルになります。SNMP コミュニティ ストリングを定義し、SNMP エージェントをイネーブルにするには、Content Engine GUI または CLI を使用して、次の手順を実行します。

- Content Engine GUI から、**System > SNMP** の順に選択します。表示される SNMP ウィンドウで、Community フィールドまでスクロールし、SNMP コミュニティ ストリングを入力します。**Update** をクリックします。
- Content Engine CLI で、**snmp-server community** コマンドを使用します。

```
ContentEngine(config)# snmp-server community comaccess
```

SNMPv3 プロトコルを SNMP 要求に使用する場合、次のステップで、SNMP ユーザ アカウントを定義します。SNMP ユーザ アカウントは、SNMP を介したスタンドアロン Content Engine へのアクセスに使用されます。SNMPv 3 ユーザ アカウントをスタンドアロン Content Engine 上に作成する方法の詳細は、「スタンドアロン Content Engine での SNMP ユーザの定義」（p.21-6）を参照してください。

スタンドアロン Content Engine での SNMP ユーザの定義

SNMP ユーザをスタンドアロン Content Engine 上に定義するときには、次の重要な点に留意してください。

- SNMPv3 プロトコルを SNMP 要求に使用する場合、SNMP を介して Content Engine にアクセスできるように、少なくとも 1 つの SNMP v3 ユーザ アカウントをスタンドアロン Content Engine 上に定義する必要があります。
- SNMPv1 または SNMPv2c セキュリティ モデルを使用して定義されたグループは、SNMP ユーザと対応付けないでください。SNMP ユーザはコミュニティ ストリングのみに対応付けます。

SNMPv3 ユーザの定義

Content Engine GUI または CLI のいずれかを使用すると、スタンドアロン Content Engine 上で SNMPv3 ユーザ アカウントを定義できます。

Content Engine GUI を使用してスタンドアロン Content Engine 上に SNMPv3 ユーザ アカウントを設定する手順は、次のとおりです。

ステップ 1　Content Engine GUI から、**System > SNMP** の順に選択します。

SNMPv1 または SNMPv2 設定用の SNMP ウィンドウが表示されます。

ステップ 2　SNMP ウィンドウの一番下までスクロールします。SNMP ウィンドウの一番下で、SNMPv3 Configuration **Click here** リンクをクリックします。

SNMPv3 設定用（SNMPv3 ユーザ アカウントを含む）の SNMP ウィンドウが表示されます。

ステップ 3　SNMPv3 ウィンドウの SNMPV3 User configuration セクションまでスクロールします。SNMPV3 User Configuration フィールドとドロップダウン リストを使用して、新規の SNMPv3 ユーザ アカウントをこの Content Engine に定義します。

a. Name フィールドに、SNMP ユーザの名前を入力します。文字、数字、ダッシュ、およびアンダースコアは使用できますが、ブランクは使用できません。この名前が、Content Engine 上の SNMP エージェントと通信しようとする SNMP ホスト上でのユーザの名前です。

b. Group フィールドに、SNMP ユーザが所属するグループの名前を入力します。

c. Remote SnmpID フィールドに、SNMP ユーザのうちの少なくとも 1 人に対して、リモート SNMP エンティティ（たとえば、SNMP ネットワーク管理ステーション）のグローバルに一意な識別子を入力します。

ヒント　SNMPv3 通知メッセージを送信するには、リモート SNMP ID オプションを持つ SNMPv3 ユーザが少なくとも 1 人、Content Engine 上に設定されている必要があります。SNMP ID は、オクテット ストリング形式で入力します。たとえば、リモート SNMP エンティティの IP アドレスが 192.147.142.129 である場合、オクテット ストリングは 00:00:63:00:00:00:a1:c0:93:8e:81 となります。

d. **Auth-Algorithm** ドロップダウン リストから、SNMP ユーザ認証に使用するアルゴリズムを選択します（**md5**、**sha**、または **no_auth**）。デフォルトでは、認証なしのタイプである **no_auth** が選択されます。

- HMAC-MD5-96 認証レベルの場合は、**md5** を選択します。
- HMAC-SHA-96 認証レベルの場合は、**sha** を選択します。

e. オプションの Auth-Password フィールドに、HMAC MD5 ユーザ認証パスワードを入力します。このフィールドは、**md5** を認証タイプとして選択した場合にのみ、適用されます。

f. オプションの Priv-Password フィールドに、HMAC MD5 ユーザのプライベート パスワードを入力します。このフィールドは、**md5** を認証タイプとして選択した場合にのみ、適用されます。これは、SNMP エージェントがホストからパケットを受信できるようにするストリングです。

ステップ 4　**Update** をクリックして、新規の SNMPv3 ユーザ アカウントを追加します。

作成されたばかりの新規ユーザ アカウントが SNMPv3 ウィンドウに表示されます。

ステップ 5　引き続き、SNMPv3 ユーザ アカウントを追加します。既存の SNMPv3 ユーザ アカウントを削除する場合は、削除しようとするアカウントの横にある **Delete** チェックボックスをクリックします。

ステップ 6　**Update** を再度クリックして、SNMPv3 ユーザ アカウントに対して加えた変更を保存します。

Content Engine CLI を使用してスタンドアロン Content Engine（SNMP サーバ）上に SNMPv3 ユーザ アカウントを定義するには、**snmp-server user** 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。SNMP アクセスを無効にするには、このコマンドの **no** 形式を使用します。

snmp-server user *name group* [**auth** {**md5** *password* [**priv** *password*] | **sha** *password* [**priv** *password*]} | **remote** *octetstring* [**auth** {**md5** *password* [**priv** *password*] | **sha** *password* [**priv** *password*]}]]

表 21-2 に、**snmp-server user** コマンドのパラメータを示します。

表 21-2　snmp-server user 用の CLI コマンド パラメータ

パラメータ	説明
name	SNMP ユーザの名前
group	SNMP ユーザが所属するグループ
auth	（任意）ユーザ認証パラメータを設定する。
md5	HMAC MD5 認証アルゴリズムを設定する。
password	HMAC MD5 ユーザ認証パスワード
priv	（任意）パケット用の認証パラメータを設定する。
password	HMAC MD5 ユーザ プライベート パスワード
sha	HMAC SHA 認証アルゴリズムを設定する。
password	HMAC SHA 認証パスワード
remote	（任意）ユーザが所属するリモート SNMP エンティティのエンジン ID を指定する。
octetstring	エンジン ID オクテット ストリング

次の例では、SNMPv3 ユーザ アカウントが Content Engine で作成されます。この SNMPv3 ユーザは **acme** という名前で、**admin** という名前のグループに属しています。この SNMP ユーザ アカウントは認証パスワードなしで設定されたため、Content Engine 上の SNMP エージェントは、このユーザからの SNMP 要求の認証を実行しません。

```
ContentEngine(config)# snmp-server user acme admin
```

SNMP トラップを送信するためのスタンドアロン Content Engine の設定

Content Engine GUI または CLI のいずれかを使用すると、スタンドアロン Content Engine 上で SNMP トラップの送信を設定できます。

Content Engine GUI から、**System > SNMP** の順に選択します。SNMP ウィンドウが表示されます。SNMP ウィンドウから、次のいずれかを実行します。

- SNMP トラップを特定の SNMP ホストに送信するように Content Engine の SNMPv1 または SNMPv2 のエージェントを設定する場合は、このウィンドウの該当するフィールドに情報を入力し、**UPDATE** をクリックします。

  たとえば、Content Engine から、SNMP トラップ メッセージで送信される SNMP トラップ ホストのホスト名または IP アドレスを指定して、SNMP トラップ ホストを定義する必要があります。
- SNMP トラップを特定の SNMP ホストに送信するように Content Engine の SNMPv3 エージェントを設定するには、SNMP ウィンドウの一番下までスクロールします。SNMPv3 Configuration **Click here** リンクをクリックします。SNMPv3 エージェントを Content Engine 上で設定するための SNMP ウィンドウが表示されます。SNMPv3 ウィンドウを使用して、この Content Engine 用に SNMP トラップおよび SNMPv3 ユーザ アカウントを設定します。

SNMPv3 ユーザ アカウントを設定する場合の詳細は、「SNMPv3 ユーザの定義」（p.21-6）を参照してください。SNMP ウィンドウのフィールドに関する詳細は、ウィンドウの一番下の **HELP** ボタンをクリックし、情報を参照してください。

Content Engine CLI を使用して、SNMP トラップを送信するようスタンドアロン Content Engine を設定する場合は、次の重要な点に留意してください。

- SNMP ホストがトラップを受信するには、そのホストに対する **snmp-server enable traps** コマンドおよび **snmp-server host** コマンドの両方を設定する必要があります。さらに、**snmp-server community** コマンドを使用して SNMP を有効にする必要もあります。
- SNMP エージェントは、デフォルトでディセーブルで、コミュニティ ストリングは設定されていません。

Content Engine CLI を使用してスタンドアロン Content Engine 上に SNMPv3 トラップを設定する手順は、次のとおりです。

ステップ 1　**snmp-server group** *name* グローバル コンフィギュレーション コマンドを使用して、セキュリティ モデル グループ（SNMPv1、SNMPv2c、SNMPv3）の中からいずれか 1 つを選択します。

snmp-server group *name* {**v1** [**notify** *name*] [**read** *name*] [**write** *name*] | **v2c** [**notify** *name*] [**read** *name*] [**write** *name*] | **v3** {**auth** [**notify** *name*] [**read** *name*] [**write** *name*] | **noauth** [**notify** *name*] [**read** *name*] [**write** *name*] | **priv** [**notify** *name*] [**read** *name*] [**write** *name*]}}

ここで各パラメータの意味は、次のとおりです。

- *name*　グループの名前
- **v1**　Version 1 セキュリティ モデルを使用するグループを指定する。
- **notify**　（任意）グループの通知ビューを指定する。
- *name*　通知ビューの名前
- **read**　（任意）グループの読み取りビューを指定する。
- *name*　読み取りビューの名前
- **write**　（任意）グループの書き込みビューを指定する。
- *name*　書き込みビューの名前
- **v2c**　Version 2c セキュリティ モデルを使用するグループを指定する。
- **v3**　ユーザ セキュリティ モデル（SNMPv3）を使用するグループを指定する。
- **auth**　AuthNoPriv セキュリティ レベルを使用するグループを指定する。
- **noauth**　noAuthNoPriv セキュリティ レベルを使用するグループを指定する。
- **priv**　AuthPriv セキュリティ レベルを使用するグループを指定する。

ステップ 2　Content Engine 上の SNMP トラップすべてをイネーブルにします。

```
ContentEngine(config)# snmp-server enable traps
```

snmp-server enable traps コマンドを入力しない場合、トラップは送信されません。すべての SNMP トラップまたは SNMP 認証トラップのみをディセーブルにする場合は、このコマンドの **no** 形式を使用します。

ステップ 3　Content Engine からの SNMP トラップをどのホストが受信するかを指定します。

次の例では、コミュニティ ストリング public を使用して、すべての SNMP トラップをホスト 172.31.2.160 に送信するように Content Engine を設定する方法を示しています。

```
ContentEngine(config)# snmp-server host 172.31.2.160 public
```

（注）　SNMP トラップを送信するには、少なくとも 1 つの SNMP トラップ ホストを設定する必要があります。ACNS 5.1 ソフトウェアおよびそれ以前のリリースの場合、設定できる SNMP ホストは最大で 4 つです。ACNS 5.2.1 ソフトウェアおよびそれ以降のリリースでは、Content Engine 上に最大で 8 つの SNMP ホストを設定できます。

ステップ 4　Content Engine 上の SNMP エージェントをイネーブルにし、Content Engine の SNMP エージェントにアクセスする際の認証パスワードとして、コミュニティ ストリングを割り当てます。

次の例では、パスワードとして comaccess を指定する方法を示しています。

```
ContentEngine(config)# snmp-server community comaccess
```

ヒント　Content Engine に送信されるすべての SNMP メッセージでは、メッセージの **Community Name** フィールドとここで定義されたコミュニティ ストリングが、認証のために一致する必要があります。

snmp-server community string グローバル コンフィギュレーション コマンドでは、SNMPv1、SNMPv2c、および SNMPv3 に対するビュー ベースのアクセス制御が行われますが、異なるバージョンへの下位互換性も引き続き維持されます。

ACNS 5.1 ソフトウェア リリースより前の ACNS 5.x ソフトウェアの **snmp-server community string** グローバル コンフィギュレーション コマンドには、SNMP メッセージが MIB オブジェクト上で一連の動作を実行できるようにするための、コミュニティ ストリングを作成するオプションがありませんでした。そのため、**rw** オプションが導入されました。また、旧バージョンの SNMP エージェントは、MIB オブジェクトへの選択的なアクセス制御機能も備えておらず、どの MIB オブジェクトへのアクセスも、SNMP コミュニティ ストリングの認証に基づいて拒否または許可されていました。

ビュー ベースのアクセス制御を導入することにより、MIB サブツリーの一部のみへのアクセスを許可するコミュニティ ストリングを設定できるようになりました。このコマンドの旧バージョンとの下位互換性を維持するために、グループ名が指定されなかった場合は、デフォルトの読み取りグループ、またはデフォルトの書き込みグループ（**rw** オプションがコマンドラインで指定された場合）がコミュニティ ストリングに対応付けられます。これらのデフォルト グループはどちらも、ユーザには非表示であり、コンフィギュレーション ファイルや **show snmp group** EXEC コマンドには表示されませんが、SNMP エージェントの初期化時に作成されます。

スタンドアロン Content Engine での SNMP エージェントのディセーブル化

スタンドアロン Content Engine 上で SNMP エージェントをディセーブルにするには、**no snmp-server** 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。

```
ContentEngine(config)# no snmp-server
```

SNMP エージェントをディセーブルにし、定義済みのコミュニティ ストリングを削除する場合は、**no snmp-server community** 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。

```
ContentEngine(config)# no snmp-server community
```

スタンドアロン Content Engine での SNMP トラップのディセーブル化

スタンドアロン Content Engine 上ですべての SNMP トラップをディセーブルにするには、**no snmp-server enable traps** 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。

```
ContentEngine(config)# no snmp-server enable traps
```

MIB-II SNMP 認証トラップの送信をディセーブルにする場合は、**no snmp-server enable traps snmp authentication** コマンドを入力します。

ACNS ソフトウェア アラームによるスタンドアロン Content Engine のモニタリング

SNMP は、従来より、SNMP トラップ生成によるエラー状態のレポートに使用されてきました。ACNS 5.x では、「SNMP によるスタンドアロン Content Engine のモニタリング」（p.21-2）に説明されているとおり、引き続きこのモニタリング方式が使用されます。

ACNS 5.2.1 ソフトウェアおよびそれ以降のリリースでは、Node Health Manager 機能がサポートされています。Node Health Manager は、重大な問題に注意を促すようにアラームを生成する ACNS アプリケーションをイネーブルにします。Node Health Manager とは、このようなアラームのデータ リポジトリで、Content Engine 上でモニタリングされているアプリケーション、サービス（キャッシュ サービスなど）、リソース（ディスク ドライブなど）の状態データやアラーム情報を収集します。たとえば、この新機能によって、モニタリングされているアプリケーション（HTTP プロキシ キャッシング サービスなど）が、Content Engine 上で正常に動作しているかどうかを調べることができます。これらのアラームは、ACNS ソフトウェア アラームと呼ばれています。

ACNS 5.2.1 ソフトウェアおよびそれ以降のリリースでは、次の Content Engine アプリケーションで ACNS ソフトウェア アラームを生成させることが可能です。

- Node Health Manager（過負荷状態と Node Manager の動作状態に関するアラーム）
- サービス障害発生時用 Node Manager（モニタリングされているアプリケーションの動作状態）
- ディスク障害発生時用 System Monitor（sysmon）

Content Engine によって通知されたアラームは、表 21-3 のように、Content Engine の CLI コマンドを使用して表示できます。通知されたアラームと解除されたアラームすべてについて、SNMP トラップが送信されます。送信される SNMP トラップのタイプは、アラームによって異なります。

（注）　Content Distribution Manager に登録されている Content Engine の場合、Content Distribution Manager に対しても、Node Health Manager によってアラームの通知が送信されます。このトピックの詳細は、『*Cisco ACNS Software Configuration Guide for Centrally Managed Deployments*』Release 5.5 を参照してください。

ACNS 5.2.1 ソフトウェア リリースでは、ACNS ソフトウェア アラーム（問題の原因）の送信元を系統立てて特定できるようにするため、複数の CLI コマンドが追加されました（表 21-3 を参照）。CLI コマンドを使用すると、多数の ACNS ソフトウェア ログを 1 つ 1 つ検索することなく、問題の発生源を特定できます。

表 21-3　Show Alarms CLI コマンドのリスト

CLI コマンド	説明	詳細
show alarm	Content Engine 上で現在通知されているすべての ACNS ソフトウェア アラーム（クリティカル、メジャー、マイナーの各アラーム）のリストを表示する。	「ACNS ソフトウェア アラームに関する情報の表示」（p.21-15）を参照してください。
show alarm critical	Content Engine 上で現在通知されている ACNS ソフトウェア クリティカル アラームのみのリストを表示する。	「ACNS ソフトウェア アラームに関する情報の表示」（p.21-15）を参照してください。
show alarm major	Content Engine 上で現在通知されている ACNS ソフトウェア メジャー アラームのみのリストを表示する。	「ACNS ソフトウェア アラームに関する情報の表示」（p.21-15）を参照してください。
show alarm minor	Content Engine 上で現在通知されている ACNS ソフトウェア マイナー アラームのみのリストを表示する。	「ACNS ソフトウェア アラームに関する情報の表示」（p.21-15）を参照してください。
show alarm detail	現在通知されている ACNS ソフトウェア アラームに関する詳細情報を表示する。	「ACNS ソフトウェア アラームに関する詳細情報の表示」（p.21-15）を参照してください。
show alarms history	Content Engine　上で以前通知され、解除された ACNS ソフトウェア アラームの履歴を表示する。CLI には、以前に通知され、解除されたイベントのうち、最新の 100 アラームのみが記録される。	「ACNS ソフトウェア アラームに関する履歴情報の表示」（p.21-16）を参照してください。
show alarms status	Content Engine 上で現在通知されている ACNS ソフトウェア アラームの数を表示する。過負荷状態のアラームと過負荷設定のアラームも表示される。	「ACNS ソフトウェア アラームに関するステータス情報の表示」（p.21-17）を参照してください。

（注）　スタンドアロン Content Engine では、ACNS ソフトウェア アラームに関する情報は、Content Engine CLI を介した場合だけでなく、SNMP を介した場合でも利用可能です。スタンドアロン Content Engine 上でこのアラーム情報にアクセス可能な CLI コマンドのリストについては、表 21-3 を参照してください。

アラームの重大度

ACNS ソフトウェア アラームには、3 つのレベルがあります（表 21-4 を参照）。

表 21-4　ACNS ソフトウェア アラームのアラーム重大度のレベル

アラーム レベル	説明
Critical	Content Engine を介した既存のトラフィックに影響を及ぼすアラームで、致命的な状態とみなされる（Content Engine は回復不能で、トラフィック処理を継続できない）。
Major	主要サービス（キャッシュ サービスなど）に障害が発生しているか、ダウンしている状態を示すアラーム。このサービスを回復させるための処置が早急に必要とされる。ただし、他のノード コンポーネントは正常に動作しており、既存サービスへの影響は最小限であると考えられる。
Minor	サービスには影響を及ぼさない状態（Non-service Affecting 状態）を示すアラーム。ただし、深刻な障害の発生を防ぐため、修正処置が必要とされる。

show alarms history EXEC コマンドによる出力には、ACNS ソフトウェア アラームの重大度が含まれます。

```
ContentEngine# show alarms history

    Op Sev Alarm ID             Module/Submodule     Instance
    -- --- -------------------- -------------------- --------------------
  1 C  Mi  servicedead          nodemgr              mediacache
  2 C  Mi  servicedead          nodemgr              cache
  3 R  Mi  servicedead          nodemgr              mediacache
  4 R  Mi  servicedead          nodemgr              cache
  5 C  Mi  servicedead          nodemgr              rpc_httpd
  6 R  Mi  servicedead          nodemgr              rpc_httpd
  7 C  Mi  servicedead          nodemgr              rpc_httpd
  8 R  Mi  servicedead          nodemgr              rpc_httpd
  9 C  Mi  servicedead          nodemgr              mediacache
 10 C  Mi  servicedead          nodemgr              cache
 11 R  Mi  servicedead          nodemgr              mediacache
 12 R  Mi  servicedead          nodemgr              cache
 13 C  Mi  servicedead          nodemgr              cache
 14 C  Mi  servicedead          nodemgr              mediacache
 15 C  Mi  servicedead          nodemgr              rtspg
 16 R  Mi  servicedead          nodemgr              cache
 17 R  Mi  servicedead          nodemgr              mediacache
 18 R  Mi  servicedead          nodemgr              rtspg


Op - Operation: R-Raised, C-Cleared
Sev - Severity: Cr-Critical, Ma-Major, Mi-Minor
```

過負荷アラーム

ACNS 5.2.1 ソフトウェアおよびそれ以降のリリースでは、Content Engine は、Node Health Manager からのアラームの着信比率をトラッキングできます。一定時間あたりのアラームの着信量が High-Water Mark（HWM; 最高水準点）を超えた場合、Content Engine はアラーム過負荷状態になります。スタンドアロン Content Engine がアラーム過負荷状態になった場合、次の状況が発生します。

- 以降の通知アラームと解除アラームに対する SNMP トラップが、一時停止します。通知アラームと解除アラームに対し、それぞれ過負荷アラームのトラップが送信されます。ただし、通知アラームの過負荷アラームと解除アラームの過負荷アラームの間に発生するアラーム操作に関するトラップは、一時停止します。
- 過負荷アラームの通知と解除の送信はブロックされません。
- アラームの着信比率が Low-Water Mark（LWM; 最低水準点）より小さい率まで減少した場合、Content Engine の状態はアラーム過負荷状態のままになります。

アプリケーションの動作状態の確認

Node Manager により、Content Engine 上で生成されるアプリケーション（HTTP キャッシュ アプリケーション、WMT ストリーミング アプリケーション、RTSP ゲートウェイ [RTSPG] ストリーミング アプリケーションなど）の動作状態がトラッキングされます。Node Manager によって、生成されたアプリケーションの終了が検出された場合、アラームが生成されます。Node Manager がアプリケーションからキープアライブ信号を受信しなくなると、アプリケーションに障害が発生したとみなされます。

アプリケーションに障害が発生した際は、Node Manager によってサービス障害アラームが生成され、状態がレポートされます。次に、サービスが再起動されます。サービスの実行が短時間（通常は 10 秒間）確認されると、サービス障害アラームは解除されます。

再起動後にもアプリケーションに障害が発生した場合は、サービス障害アラームの通知が継続され、Node Manager によってサービスの再起動が試行されます。再起動は、通常、Node Manager によって最大 10 回まで行われます。その後、Node Manager により該当サービスについてサービス無効アラームが通知されると、「サービス障害」アラームが解除され、サービス再起動の試行は停止します。

サービスを再起動するためには、該当機能の設定を解除し、設定し直す必要があります（たとえば、NTP サービスの場合、**no ntp server** *hostname* | *IP address* グローバル コンフィギュレーション コマンドを入力して NTP サービスの設定を解除し、**ntp server** *hostname* | *IP address* グローバル コンフィギュレーション コマンドを使用して NTP サービスを再設定します）。

スタンドアロン Content Engine での SNMP アラーム トラップの設定

Content Engine では、特定のアラーム状態に対して SNMP トラップを生成させるように設定することができます。スタンドアロン Content Engine では、次の状態に基づいて、SNMP アラーム トラップの生成を設定できます。

- アラームの重大度（クリティカル、メジャー、マイナー）
- アクション（アラーム通知と解除）

ACNS 5.2.1 ソフトウェア リリースでは、CISCO-CONTENT-ENGINE-MIB（CCE MIB）に次の 6 つの汎用アラーム トラップが追加されました表 21-5 を参照してください。

表 21-5　汎用アラーム トラップ

アラーム トラップの名前	重大度	アクション	アラーム トラップをイネーブルにする CLI コマンド
cceAlarmCriticalRaised	Critical	通知	**snmp-server enable traps alarm raise-critical**
cceAlarmCriticalCleared	Critical	解除	**snmp-server enable traps alarm clear-critical**
cceAlarmMajorRaised	Major	通知	**snmp-server enable traps alarm raise-major**
cceAlarmMajorCleared	Major	解除	**snmp-server enable traps alarm clear-major**
cceAlarmMinorRaised	Minor	通知	**snmp-server enable traps alarm raise-minor**
cceAlarmMinorCleared	Minor	解除	**snmp-server enable traps alarm clear-minor**

（注）　これら 6 つの汎用アラーム トラップは、デフォルトでディセーブルです。

この 6 つの汎用アラーム トラップにより、SNMP と Node Health Manager の間の整合性が保たれます。6 つの汎用アラーム トラップは、それぞれ Content Engine CLI を使用してイネーブルまたはディセーブルにできます。ACNS 5.2.1 ソフトウェアおよびそれ以降のリリースでは、**snmp-server enable traps** グローバル コンフィギュレーション コマンドに **alarm** オプションが含まれています。

```
ContentEngine(config)# snmp-server enable traps alarm ?
  clear-critical  Enable clear-critical alarm trap
  clear-major     Enable clear-major alarm trap
  clear-minor     Enable clear-minor alarm trap
  raise-critical  Enable raise-critical alarm trap
  raise-major     Enable raise-major alarm trap
  raise-minor     Enable raise-minor alarm trap
```

次の例では、クリティカル アラームが解除された場合に SNMP トラップが生成されるように、Content Engine（SNMP サーバ）を設定しています。

```
ContentEngine(config)# snmp-server enable traps alarm clear-critical
```

ACNS ソフトウェア アラームに関する情報の表示

スタンドアロン Content Engine 上で現在通知されているすべてのクリティカル、メジャー、マイナーの各アラームに関する情報を表示する場合は、**show alarm** EXEC コマンドを入力します。Content Engine 上で現在通知されているアラームがない場合は、「None」と表示されます。次に出力例を示します。

```
ContentEngine# show alarm

Critical Alarms:
----------------
None

Major Alarms:
-------------
None

Minor Alarms:
-------------
None
```

また、次に示すとおり、Content Engine 上で現在通知されている ACNS ソフトウェア アラームのうち、指定したレベルの情報のみを表示することもできます。

- クリティカル アラームに関する情報のみを表示するには、**show alarm critical** EXEC コマンドを入力します。
- メジャー アラームに関する情報のみを表示するには、**show alarm major** EXEC コマンドを入力します。
- マイナー アラームに関する情報のみを表示するには、**show alarm minor** EXEC コマンドを入力します。

（注） アラームのさまざまな重大度（クリティカル、メジャー、マイナー）に関する詳細は、表 21-4 を参照してください。

ACNS ソフトウェア アラームに関する詳細情報の表示

現在通知されている SNMP アラームの詳細を表示する場合は、**show alarm detail** EXEC コマンドを入力します。このコマンドを使用すると、特定のアラームについてより詳しい情報を確認できます。

ACNS ソフトウェア アラームに関する履歴情報の表示

スタンドアロン Content Engine 上で以前通知され、解除された ACNS ソフトウェア アラームの履歴を表示する場合は、**show alarms history** EXEC コマンドを入力します。

```
ContentEngine# show alarms history

    Op Sev Alarm ID             Module/Submodule     Instance
    -- --- -------------------- -------------------- --------------------
  1 C  Mi  servicedead          nodemgr              mediacache
  2 C  Mi  servicedead          nodemgr              cache
  3 R  Mi  servicedead          nodemgr              mediacache
  4 R  Mi  servicedead          nodemgr              cache
  5 C  Mi  servicedead          nodemgr              rpc_httpd
  6 R  Mi  servicedead          nodemgr              rpc_httpd
  7 C  Mi  servicedead          nodemgr              rpc_httpd
  8 R  Mi  servicedead          nodemgr              rpc_httpd
  9 C  Mi  servicedead          nodemgr              mediacache
 10 C  Mi  servicedead          nodemgr              cache
 11 R  Mi  servicedead          nodemgr              mediacache
 12 R  Mi  servicedead          nodemgr              cache
 13 C  Mi  servicedead          nodemgr              cache
 14 C  Mi  servicedead          nodemgr              mediacache
 15 C  Mi  servicedead          nodemgr              rtspg
 16 R  Mi  servicedead          nodemgr              cache
 17 R  Mi  servicedead          nodemgr              mediacache
 18 R  Mi  servicedead          nodemgr              rtspg


Op - Operation: R-Raised, C-Cleared
Sev - Severity: Cr-Critical, Ma-Major, Mi-Minor
```

アラームに関するより詳細な情報を表示する場合は、**show alarms history detail support** EXEC コマンドを入力します。

```
Content Engine# show alarms history detail support
     Op Sev Alarm ID             Module/Submodule     Instance
     -- --- -------------------- -------------------- --------------------
   1 C  Mi  servicedead          nodemgr              rtspg
     Jul  2 18:22:04.577 UTC, Processing Error Alarm, #000001, 2000:330004
     nodemgr: The rtspg service has died.

     /alm/min/nodemgr/-service_name-/servicedead:

         -service name- service has died.

     Explanation:
         The node manager found the specified service to be dead.
         Attempts will be made to restart this service.

     Action:
         Examine the syslog for messages relating to cause of service
          death. The alarm will be cleared if the service stays
         alive  and does not restart in a short while.


   2 R  Mi  servicedead          nodemgr              rtspg
     Jul  2 18:21:54.231 UTC, Processing Error Alarm, #000001, 2000:330004
     nodemgr: The rtspg service has died.

     /alm/min/nodemgr/-service_name-/servicedead:

         -service name- service has died.

     Explanation:
         The node manager found the specified service to be dead.
         Attempts will be made to restart this service.

     Action:
         Examine the syslog for messages relating to cause of service
          death. The alarm will be cleared if the service stays
         alive  and does not restart in a short while.

Op - Operation: R-Raised, C-Cleared
Sev - Severity: Cr-Critical, Ma-Major, Mi-Minor
```

ACNS ソフトウェア アラームに関するステータス情報の表示

Content Engine 上で現在通知されているすべてのアラームの数を表示するには、**show alarms status** EXEC コマンドを入力します。次の出力例は、現在通知されている ACNS ソフトウェア アラームの数を示しています。表示には、過負荷アラーム設定に関する情報（Content Engine 上で現在過負荷検出がイネーブルにされているかディセーブルにされているかなど）も含まれます。

```
ContentEngine# show alarms status

Critical Alarms :          0
Major Alarms    :          0
Minor Alarms    :          0

Overall Alarm Status : None
Device is NOT in alarm overload state.
Device enters alarm overload state @   10 alarms/sec.
Device exits alarm overload state  @    1 alarms/sec.
Overload detection is DISABLED.
```

スタンドアロン Content Engine でのクリティカル ディスク ドライブのモニタリング

Content Engine が適切に動作するためには、次のようなクリティカル ディスク ドライブが必要です。

- 「disk00」と呼ばれる 1 台めのディスク ドライブ
- 1 つめの sysfs（システム ファイル システム）パーティションが含まれるディスク ドライブ

  sysfs パーティションは、トランザクション ログ、システム ログ（Syslog）、内部デバッグ ログを含むログ ファイルを保存するために使用されます。Content Engine 上のイメージ ファイルや設定ファイルの保存にも使用できます。

（注）　*クリティカル ドライブ*という用語は、disk00 または 1 つめの sysfs パーティションが含まれるディスク ドライブのいずれかとして定義されています。Content Engine のモデルよって、クリティカル ドライブの状況も異なります。たとえば、より小規模な、ディスク ドライブが 1 台の Content Engine では、クリティカル ディスク ドライブは 1 台のみです。より高性能な、複数のディスク ドライブがある Content Engine では、Content Engine 上にクリティカル ディスク ドライブが複数ある場合もあります。

Content Engine がブートされた際のシステム起動時にクリティカル ディスク ドライブが検出されなかった場合、Content Engine 上の ACNS システムはサービス低下状態で実行されることになります。クリティカル ディスク ドライブの 1 台で実行時に障害が発生した場合、アプリケーションが正常に機能しない、動作を一時的に中断または停止する、あるいは ACNS システム自体が動作を一時的に中断または停止する可能性があります。したがって、Content Engine 上のクリティカル ディスク ドライブをモニタリングし、ディスク ドライブ エラーが通知されるようにすることが非常に重要です。

ACNS システムでは、ディスク デバイス エラーは、次のいずれかのイベントとして定義されています。

- Linux カーネルによって検出された Small Computer Systems Interface（SCSI）または Integrated Drive Electronics（IDE）デバイス エラー
- アプリケーションによるディスク デバイス アクセス（open（2）、read（2）、write（2）などのシステム コール）で、EIO エラー コードの障害が発生した場合
- 起動時に検出されたディスク デバイスに、実行時にアクセスできない場合

ACNS 5.2.1 ソフトウェアおよびそれ以降のリリースでは、Content Engine ディスク ドライブをモニタリングできます。ディスク ステータスは、フラッシュ（不揮発性ストレージ）に記録されます。Content Engine のディスク ドライブにエラーが発生した際、sysfs パーティションが動作可能な場合にはメッセージがシステム ログに書き込まれ、Content Engine 上に SNMP が設定されている場合には SNMP トラップが生成されます。

Content Engine 上では、クリティカル ディスク ドライブの状態のトラッキングに加えて、ディスク デバイス エラー処理スレショルドも設定できます。ディスク デバイス エラーの数が指定されたスレショルドに到達した場合、該当するディスク デバイスは自動的に不良とマークされます。ACNS システムでは、不良ディスク デバイスの使用がただちに中止されるわけではありません。不良ディスク ドライブの使用は、次の再起動後に停止されます。

指定されたスレッシュホールドを超えた場合、Content Engine では、このイベントが記録されるか、再起動が実行されます。自動リロード機能がイネーブルの場合にスレッシュホールドを超えると、ACNS システムによって Content Engine が自動的に再起動されます。このスレッシュホールドを指定する場合の詳細は、「ディスク エラー処理スレッシュホールドの指定」（p.21-19）を参照してください。

（注）　**disk drive mark** EXEC コマンドを使用すると、ディスク ドライブに手動で不良または正常とマークできます。詳細は、「Content Engine ディスク ドライブに対する手動でのマークとマークの解除」（p.21-19）を参照してください。

ACNS 5.2.1 ソフトウェア リリースでは、SCSI ドライブの不良（ただし不使用）セクタの再配置がサポートされるようになりました。ACNS 5.3.1 ソフトウェアおよびそれ以降のリリースでは、この機能が IDE および Serial Advanced Technology Attachment（SATA）ドライブにまで拡張されました。このトピックに関する詳細は、『*Cisco ACNS Software Upgrade and Maintenance Guide*』Release 5.x を参照してください。

ディスク エラー処理スレッシュホールドの指定

ACNS 5.2.1 ソフトウェアおよびそれ以降のリリースでは、ディスク エラー処理スレッシュホールドを設定できます。このスレッシュホールドは、ディスク ドライブが不良とマークされるまでに検出されるディスク エラーの数を決定します。デフォルトでは、このスレッシュホールドは 10 に設定されています。

デフォルトのスレッシュホールドを変更する場合は、**disk error-handling threshold** 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。有効値は 0 ～ 100 です。ディスク ドライブが不良とマークされないようにする場合は、0 と指定します。

次の例では、ディスク ドライブが自動的に不良とマークされるまでに、指定されたディスク ドライブ（disk00 など）に対して 5 回のディスク ドライブ エラーが許容されます。

```
ContentEngine(config)# disk error-handling threshold 5
```

不良ディスク ドライブがクリティカル ディスク ドライブで、自動リロード機能（**disk error-handling reload** コマンド）がイネーブルの場合、ACNS ソフトウェアによってディスク ドライブが不良とマークされ、Content Engine は自動的にリロードされます。Content Engine のリロード後、Syslog メッセージと SNMP トラップが生成されます。

Content Engine の自動リロード機能は、デフォルトでディセーブルです。自動リロード機能をイネーブルにする場合は、**disk error-handling reload** 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。

```
ContentEngine(config)# disk error-handling reload
```

自動リロード機能をディセーブルにする場合は、**no disk error-handling reload** 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。

```
ContentEngine(config)# no disk error-handling reload
```

Content Engine ディスク ドライブに対する手動でのマークとマークの解除

Content Engine 上のディスク ドライブは、次のような方法を使用して手動でマークを解除するまで、Not used の状態になります。

- ディスクの状態をリセットするには、スタンドアロン Content Engine 上で、次のいずれかの **disk add** EXEC コマンドを使用します。これらの **disk add** コマンドのいずれかを使用すると、ディスクの Not used 状態がリセットされます。

  disk add *diskname* [**sysfs** {**remaining** | *disk-space*}] [cfs {**remaining** | *disk-space*}] | [mediafs {**remaining** | *disk-space*}]

- 手動で 1 つまたはすべてのディスク ドライブを正常（使用中）または不良（リロード後不使用）とマークするには、**disk mark** EXEC コマンドを使用します。

次の例では、disk03 を bad（不良）とマークし、Content Engine をリロード後に disk03 から bad のマークを解除し、再び使用できるようにする方法を示しています。

ステップ 1　disk03 を bad とマークします。

```
Content Engine# disk mark ?
      WORD  Disk name (e.g. disk00, disk01,..)
Content Engine# disk mark disk03 ?
      bad   Mark as bad disk drive, don't use it
      good  Mark as good disk drive
Content Engine# disk mark disk03 bad
    disk03 is marked as bad.
    It will be not used after reload.
```

ステップ 2　disk03 は、Content Engine の起動後にマークされたため、「*」がマークされていることを確認します。

```
Content Engine# show disks details
(*) Disk drive won't be used after reload.
......
disk03: Normal        (h00 c00 i03 l00 - Int DAS)        70001MB( 68.4GB) (*)
    FREE:                    70001MB( 68.4GB)
......
```

disk03 は Normal（現在使用中）と表示されていることに注意してください。

ステップ 3　**reload** EXEC コマンドを入力して、Content Engine をリロードします。次のプロンプトが表示されたら、**Enter** キーを押して、リロードを実行します。

```
Content Engine# reload
Proceed with reload?[confirm]
......
```

Content Engine のリロード後、bad（不良）とマークされた disk03 は使用不可となります。

ステップ 4　disk03 が Not used とマークされていることを確認します。

```
Content Engine# show disks details
(*) Disk drive won't be used after reload.
......
disk03: Not used (*)
......
```

disk03 は、Content Engine の再起動後に不良であると検出されたため、Not used (*) と表示されています。

ステップ 5　disk03 のマークを手動で bad から good に変更します。

```
Content Engine# disk mark disk03 good
disk03 is marked as good.
It will be used after reload.
```

ステップ 6　disk03 が Not used とマークされていることを確認します。

```
Content Engine# show disks details
......
disk03: Not used
......
```

SMART によるディスクの状態のプロアクティブなモニタリング

ACNS 5.3.1 ソフトウェアおよびそれ以降のリリースでは、Self Monitoring, Analysis, and Reporting Technology（SMART）により、ディスクの状態をプロアクティブにモニタリングできます。SMART は、ハード ドライブ診断情報と、近い将来発生する可能性のあるディスク障害についての情報を提供します。

SMART は多くのディスク ベンダーによってサポートされており、ディスク状態の識別に使用される標準的な方式です。SMART 属性には、動作や環境の状態に関する情報を ACNS ソフトウェアに提供する読み取り専用の属性（時間ごとの仕事率や、ロードとアンロードの回数など）がいくつかあり、この情報から、近い将来発生するディスク障害を読み取れることがあります。

SMART のサポートは、ベンダーによって異なります。各ディスク ベンダーがサポートする SMART の属性セットは異なります。次の出力例では、**show disk SMART-info** EXEC コマンドを 2 つの異なる Content Engine（Content Engine A と Content Engine B）に入力しています。これらの 2 つの Content Engine には、それぞれ異なるベンダーが製造したハード ディスクが備えられています。

```
ContentEngineA# show disks SMART-info
=== disk00 ===
Device: IBM      IC35L036UCD210-0 Version: S5BS
Serial number:         22222222
Device type: disk
Transport protocol: Fibre channel (FCP-2)
Local Time is: Sun Jan  2 03:14:16 2005 Etc
Device supports SMART and is Enabled
Temperature Warning Disabled or Not Supported
SMART Health Status: OK

=== disk01 ===
disk01: Not present

ContentEngineB# show disk SMART-info
Disk 01:
========
Device Model:     HITACHI_DK23BA-20
Serial Number:    111111
Firmware Version: 00E0A0D2
SMART support is: Available - device has SMART capability.
SMART support is: Enabled
SMART overall-health self-assessment test result: PASSED
Vendor Specific SMART Attributes with Thresholds:
ID# ATTRIBUTE_NAME          FLAG     VALUE WORST THRESH TYPE      WHEN_FAILED RAW_VALUE
  1 Raw_Read_Error_Rate     0x000d   100   083   050    Pre-fail     -       677
  3 Spin_Up_Time            0x0007   100   100   050    Pre-fail     -       0
  4 Start_Stop_Count        0x0032   100   100   050    Old_age      -       249
  5 Reallocated_Sector_Ct   0x0033   099   099   010    Pre-fail     -       30
  <cr>
```

さらに詳細な情報を表示するには、**show disk SMART-info details** EXEC コマンドを入力します。**show disk SMART-info** コマンドおよび **show disk SMART-info details** コマンドの出力は、ディスク ベンダーとドライブ技術の種類（IDE、SCSI、および SATA ディスク ドライブ）によって異なります。

SMART 属性はベンダーによって異なりますが、SMART 属性の多くには共通の解釈方法があります。各 SMART 属性には、正規化された現在の値とスレッシュホールド値があります。現在の値がスレッシュホールド値を超えると、そのディスクは障害があるとみなされます。ACNS ソフトウェアは、SMART 属性をモニタリングし、Syslog メッセージ、SNMP トラップ、およびアラームにより、近い将来に発生する障害を報告します。

ACNS 5.3.1 ソフトウェアおよびそれ以降のリリースでは、**show tech-support** EXEC コマンドからの出力にも SMART 情報が含まれています。

スタンドアロン Content Engine によるシステム ロギング

システム ログ ファイル（Syslog）専用のパラメータを設定する場合は、システム ロギング機能を使用します。このファイルには、認証エントリ、特権レベル、および管理に関する詳細情報が保存されています。システム ロギングは、内部では常にイネーブルになっています。システム ログ ファイルは、システム ファイル システム（sysfs）パーティションに /local1/syslog.txt として置かれます。

スタンドアロン Content Engine 上では、システム ロギングは、デフォルトでイネーブルになっています。表 21-6 に、システム ロギングのデフォルト設定を示します。

表 21-6　システム ロギングのデフォルト設定

設定	デフォルト設定
コンソール用メッセージのプライオリティ	warning
ログ ファイル用メッセージのプライオリティ	debug
ログ ファイル	/local1/var/log/syslog.txt
ログ ファイル リサイクル サイズ	0,000,000 バイト

Content Engine GUI または CLI を使用すると、スタンドアロン Content Engine が各種レベルのイベント メッセージをディスク、コンソール、またはリモート Syslog ホストに送信するように設定できます。デフォルト Syslog 設定の変更方法の詳細については、「スタンドアロン Content Engine でのシステム ロギングの設定」（p.21-23）を参照してください。

ACNS 5.3.1 ソフトウェアおよびそれ以降のリリースでは、プロキシ モードのネイティブ FTP がサポートされます。ACNS 5.3.1 ソフトウェアおよびそれ以降のリリースでは、プロキシ モードのネイティブ FTP に対する Syslog メッセージがサポートされます。次に、プロキシ モードのネイティブ FTP サポートに関する Sysylog メッセージの例を示します。

```
CE-FTP_PROXY-3-252009:   Failed to configure FTP Proxy-mode listener on port
                    '[port]'.

Explanation:        Could not start proxy-mode listener for FTP control
                    connection for the specified port.  The port is temporarily
                    in an un-bindable state, or is in use by some other
                    application.

Action:             Check whether the port has been configured for use by a
                    different application.  If not, retry the ftp-native
                    incoming proxy command after 2 minutes.  If this error
                    repeats frequently, contact Cisco TAC.
```

ACNS 5.1.x ソフトウェアおよびそれ以前のリリースでは、不良セクタにアクセスするたびに、ディスク障害 Syslog メッセージが生成されます。ACNS 5.2.1 ソフトウェア リリースでは、IDE ディスク上の単一の不良セクタに対する複数の Syslog メッセージをフィルタリングするサポートが追加されました。ACNS 5.3.1 ソフトウェアおよびそれ以降のリリースでは、SCSI ディスク および SATA ディスク上の単一の不良セクタに対して複数の syslog メッセージをフィルタリングできます。

ACNS 5.3.1 ソフトウェアおよびそれ以降のリリースでは、**show disk failed-sectors** EXEC コマンドを入力すると、Content Engine ディスク上の不良セクタのリストを表示できます。

```
ContentEngine# show disk failed-sectors
    List of failed sectors on disk00
    --------------------------------
    89923
    9232112
   List of failed sectors on disk01
    --------------------------------
    <None>
```

特定のディスク ドライブだけについて不良セクタのリストを表示するには、**show disk failed-sectors** コマンドの入力時にディスク名を指定します。次の例は、disk01 の不良セクタのリストを表示する方法を示しています。

```
ContentEngine# show disk failed-sectors disk01
```

ディスク障害がある場合は、ACNS 5.3.1 ソフトウェアおよびそれ以降のリリースを実行している Content Engine にログインする際に、障害を通知するメッセージが出力されます。

システム ロギングの現在の設定の表示

スタンドアロン Content Engine 上で現在の Syslog ホスト設定を表示する場合は、**show logging** EXEC コマンドを入力します。

```
ContentEngine# show logging
Syslog to host is enabled.
Priority for host logging to 1.2.1.1:514 is set to: warning
Syslog to console is disabled
Priority for console logging is set to:  warning
Syslog to disk is enabled
Priority for disk logging is set to:  notice
Filename for disk logging is set to:  /local1/syslog.txt
Syslog facility is set to syslog
Syslog disk file recycle size is set to 10000000
```

スタンドアロン Content Engine でのシステム ロギングの設定

Content Engine GUI または CLI のいずれかを使用すると、スタンドアロン Content Engine にシステム ロギングを設定できます。設定の際に、Content Engine がさまざまなレベルのメッセージをディスク、コンソール、または最大 4 つのリモート Syslog ホストに送信するかどうかを指定します。

Content Engine GUI から、**System > Syslog** の順に選択します。表示された Syslog ウィンドウを使用して、Content Engine のシステム ロギングを設定します。Syslog ウィンドウの使用方法に関する詳細は、ウィンドウの **Help** ボタンをクリックし、コンテキスト ヘルプにアクセスしてください。

Content Engine CLI から、**logging** グローバル コンフィギュレーション コマンドを使用して、該当する Syslog 用のパラメータを設定します。

```
ContentEngine(config)# logging ?
  console   Log to console
  disk      Store log in a file
  facility  Facility parameter when log to host
  host      Log to host (maximum of 4 hosts)
```

Content Engine CLI を使用して、スタンドアロン Content Engine にシステム ロギングを設定する方法の詳細については、次の項を参照してください。

- Syslog プライオリティ レベルの RealProxy エラー コードへのマッピング（p.21-27）
- Syslog プライオリティ レベルの RealProxy エラー コードへのマッピング（p.21-27）
- リモート Syslog ホストに対するシステム ロギングの設定（p.21-25）

コンソールに対するシステム ロギングの設定

システム ロギングは、各種レベルのメッセージ（プライオリティ レベル）をコンソールに送信するように設定することができます。コンソールに対してシステム ロギングを設定し、コンソールに送信する各種レベルのメッセージを指定するには、**logging console priority** 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。

logging console {**enable** | **priority** *loglevel* }

表 21-7 に、このコマンドのパラメータを示します。

表 21-7　logging console CLI コマンドのパラメータ

パラメータ	説明
console	コンソールに対してシステム ロギングを設定
enable	コンソールに対するシステム ロギングをイネーブルにする。
priority	コンソールに対して送信されるメッセージのプライオリティ レベルを設定
loglevel	次のキーワードのいずれかを使用
• **alert**	ただちに処置を講じることが必要。プライオリティ 1
• **critical**	ただちに処置を講じることが必要。プライオリティ 2
• **debug**	デバッグ メッセージプライオリティ 7
• **emergency**	システムは使用不能。プライオリティ 0
• **error**	エラー状態プライオリティ 3
• **information**	情報メッセージ。プライオリティ 6
• **notice**	正常だが注意すべき状態プライオリティ 5
• **warning**	警告状態。プライオリティ 4

（注）　Content Engine からリモート ホストへの Syslog メッセージは、ポート 514 ではなくポート 10000 から発信されます。

次の例では、**type-tail** EXEC コマンドを使用して syslog.txt ファイルの最後の数行を表示しています。このコマンドは、指定されたテキスト ファイルの最後の数行のみを表示します。

```
ContentEngine# type-tail syslog.txt
Jan 18 17:50:03 ContentEngine Host[3766]: authentication failure; (uid=0) ->
aaHH for content_engine_config service
Jan 18 17:50:05 ContentEngine login[3766]: Failed login session from 172.16.1.1
for user aaHH:  Authentication service cannot retrieve authentication info.
Jan 18 18:39:05 ContentEngine Host[6787]: set privilege level to `0'
Jan 18 18:39:05 ContentEngine login: user login on 1 from 172.16.66.148
```

ディスクに対するシステム ロギングの設定

システム ロギングは、各種レベルのメッセージ（プライオリティ レベル）をディスクに送信するように設定することができます。ディスクに対してシステム ロギングを設定し、ディスクに送信する各種レベルのメッセージを指定するには、**logging disk priority** 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。

logging disk {**enable** | **filename** *filename* | **priority** *loglevel* | **recycle** *size*}

表 21-8 に、このコマンドのパラメータを示します。

表 21-8　logging disk CLI コマンドのパラメータ

パラメータ	説明
disk	ディスク ファイルに対してシステム ロギングを設定
enable	ディスク ファイルに対するシステム ロギングをイネーブルにする。
filename	Syslog ファイルの名前を設定する。
filename	Syslog ファイルの名前を指定する。
priority	Syslog ファイルに対して送信されるメッセージのプライオリティ レベルを設定
loglevel	次のキーワードのいずれかを使用
• **alert**	ただちに処置を講じることが必要。プライオリティ 1
• **critical**	ただちに処置を講じることが必要。プライオリティ 2
• **debug**	デバッグ メッセージプライオリティ 7
• **emergency**	システムは使用不能。プライオリティ 0
• **error**	エラー状態プライオリティ 3
• **information**	情報メッセージ。プライオリティ 6
• **notice**	正常だが注意すべき状態プライオリティ 5
• **warning**	警告状態。プライオリティ 4
recycle	ファイルがリサイクル サイズを超えた場合に、syslog.txt（ログ ファイル）を上書きする。
size	Syslog ファイルのサイズ（バイト単位、1000000 ～ 50000000）

リモート Syslog ホストに対するシステム ロギングの設定

ACNS 5.1 ソフトウェアでは、リモート Syslog ホスト 1 つのみに対するロギングがサポートされており、スタンドアロン Content Engine に対するリモート Syslog ホストを 1 つ設定する場合に、次の 2 つのコマンドが使用されていました。

```
ContentEngine(config)# logging host hostname
ContentEngine(config)# logging priority priority
```

ACNS 5.2.1 ソフトウェア リリースおよびそれ以降のリリースでは、各種のレベルのイベント メッセージを最大で 4 つのリモート Syslog ホストへ送信するように、Content Engine を設定できます。この変更の反映には、ACNS 5.1.x ソフトウェアの **logging host priority** *priority* グローバル コンフィギュレーション コマンドは推奨されなくなり、**logging host hostname** グローバル コンフィギュレーション コマンドが次のように拡張されました。

```
ContentEngine(config)# [no] logging host hostname [priority priority-code | port port
|rate-limit limit]
```

ここで各パラメータの意味は、次のとおりです。

- *hostname* は、リモート Syslog ホストのホスト名か IP アドレスです。

  最大で 4 つまでのリモート Syslog ホストを指定します。複数の Syslog ホストを指定する場合は、複数のコマンドラインを使用し、1 つのコマンドにつき 1 つのホストを指定します（ACNS 5.1.x ソフトウェアおよびそれ以前のリリースでは、1 つのリモート Syslog ホストにメッセージを送信するようにしか Content Engine を設定できませんでした）。

- *priority-code* は、指定されたリモート Syslog ホストに送信されるメッセージの重大度です。

  デフォルトの priority-code は warning（レベル 4）です。各 Syslog ホストでは、それぞれ、異なるレベルのイベント メッセージを受信できます。次に、異なるプライオリティ コードを示します。

```
ContentEngine(config)# logging host 1.2.3.4 priority ?
   alert        (1) Immediate action needed
   critical     (2) Critical conditions
   debug        (7) Debugging messages
   emergency    (0) System is unusable
   error        (3) Error conditions
   information  (6) Informational messages
   notice       (5) Normal but significant conditions
   warning      (4) Warning conditions
```

（注） 複数の Syslog ホストに同じ種類のメッセージを送信することも可能で、この場合、Content Engine 上に複数の Syslog ホストを設定し、設定されたそれぞれの Syslog ホストに同じプライオリティ コードを割り当てます（たとえば、Sylog ホスト 1、Sylog ホスト 2、Syslog ホスト 3 のそれぞれに、レベル 2 のプライオリティ コード critical を割り当てます）。

- *port* は、Content Engine によってメッセージが送信されるリモート Syslog ホストの宛先ポートです。

  デフォルトのポートは 514 です（ACNS 5.2.1 ソフトウェア リリースより前のリリースでは、デフォルト ポートは変更できませんでした。Syslog メッセージは、指定された Syslog ホストのポート 514 に対してのみ送信されました）。

- *rate-limit* は、リモート Syslog ホストへの送信が許可される 1 秒あたりのメッセージ数です。

  帯域幅や他のリソースの消費を制限するため、リモート Syslog ホストへの一定時間あたりのメッセージ送信量は制限できます。この制限を超えた場合、指定されたリモート Syslog ホストではメッセージが受信されません。デフォルトでは制限がないので、すべての Syslog メッセージが、設定されたすべての Syslog ホストに対して送信されます。一定時間あたりの送信量を超えた場合、CLI EXEC shell login に対して、「message of the day」（motd）が出力されます。

Content Engine がさまざまなレベルの Syslog メッセージを最大で 4 つの外部 Syslog ホストに送信するように設定する場合は、**logging host** 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。次の例では、IP アドレスが 172.31.2.160 のリモート Syslog ホストにプライオリティ コード error（レベル 3）のメッセージを送信するよう、Content Engine を設定しています。

```
ContentEngine(config)# logging host 172.31.2.160 priority error
```

Syslog プライオリティ レベルの RealProxy エラー コードへのマッピング

RealProxy は、エラー メッセージを生成し、RealProxy ログ ファイルに書き込みます。これらのエラー メッセージは、ACNS ソフトウェアにより取り込まれ、システム ログ ファイルに渡されます。表 21-9 に、RealProxy エラー コードと Syslog プライオリティ レベルとの対応を示します。

表 21-9　RealProxy エラー レベルと Syslog プライオリティ レベルとのマッピング

RealProxy エラー コード	RealProxy の状態	RealProxy での意味	Syslog プライオリティ レベル
0	Panic	システム障害を起こす可能性があるエラー。RealProxy は、問題の解決に必要な処置を講じます。	プライオリティ 0：LOG_EMERG Emergency。システムは使用不能
1	Severe	問題を防止するため、ただちにユーザの介入が必要なエラー	プライオリティ 1：LOG_ALERT Alert。ただちに処置を講じることが必要
2	Critical	問題を解決するためにユーザの介入が必要な場合があるエラー	プライオリティ 2：LOG_CRI Critical。クリティカルな状態
3	General	通常のシステム稼働には重大な問題を引き起こさないエラー	プライオリティ 3：LOG_ERR Error。エラー状態
4	Warning	システムには問題を引き起こさないが、注意が必要な状態であることを警告	プライオリティ 4：LOG_WARNING Warning。警告状態
5	Notice	システムには問題を引き起こさないが、注意すべき状態であることを通知	プライオリティ 5：LOG_NOTICE Notice。正常だが注意すべき状態
6	Informational	情報提供のみが目的のメッセージ	プライオリティ 6：LOG_INFO Information。情報メッセージ
7	Debug	プログラムのデバッグ時のみに使用される情報	プライオリティ 7：LOG_DEBUG Debug。デバッグ メッセージ

CiscoWorks2000 の使用

CiscoWorks2000 は、ほとんどのシスコ製デバイスの管理に使用される一連の管理アプリケーションを提供するシスコ製品です。Content Engine は、いっさい変更することなく、次に示すように CiscoWorks2000 と相互運用できます。

- CiscoWorks2000 では、「Generic SNMP」デバイスの下に Content Engine を表示できます。
- CiscoWorks2000 インベントリ モジュールでは、Content Engine が、デバイス名、システム名、説明（ソフトウェア バージョンなど）、アップタイム、およびネットワーク インターフェイス情報とともに表示されます。
- CiscoWorks2000 Syslog モジュールでは、Content Engine の Syslog を解釈できます。
- CiscoWorks2000 アベイラビリティ モジュールでは、Content Engine をトラッキングできます。

Content Engine GUI か CLI のいずれかを使用して、CiscoWorks2000 に準拠した形式での Syslog メッセージの生成をイネーブル、またはディセーブルにできます。たとえば、「スタンドアロン Content Engine でのシステム ロギングの設定」（p.21-23）に説明されているように、Content Engine CLI で **logging host hostname** グローバル コンフィギュレーション コマンドを使用すると、CiscoWorks2000 をリモート Syslog ホストとして設定できます。

スタンドアロン Content Engine でのトランザクションのモニタリング

Content Engine の管理者は、一般的に、Content Engine 上で行われた要求のタイプや要求によってもたらされた結果に注目します。たとえば、ストリーミング メディアが会社の収入源である場合、その会社では、どのお客様がどのコンテンツにアクセスしたかや、ユーザがどれくらいの時間コンテンツを見たか、また、その表示時の品質などをトラッキングする手段が必要になります。これらの会社では、オンデマンド コンテンツやライブ ブロードキャストの配信について課金する必要があるため、コンテンツ アクセス サービスに関するお客様への請求については、記録された情報に基づいて行う必要があります。

Content Engine から配信された要求を記録するソフトウェアのログは、*トランザクション ログ*と呼ばれます。トランザクション ログに記録される一般的なフィールドは、クライアント要求の日付と時刻、要求された URL、キャッシュ ヒットまたはキャッシュ ミス、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 ログは、通常、次のような目的で使用されます。

- 問題の特定と解決
- 負荷のモニタリング
- 課金請求
- 統計分析
- セキュリティ上の問題分析
- コスト分析とプロビジョニング

ACNS 5.2.1 ソフトウェアおよびそれ以降のリリースでは、Windows Media Services 9 ロギングがサポートされています。Windows Media Services 9 シリーズでは、Windows Media Services Version 4.1 よりもより強固なロギング モデルが提供されています。

定義された形式での記録が可能です（Squid、拡張 Squid、Apache の各形式や、カスタム トランザクション ログ形式を使用して、ログにフィールドを追加することも可能）。トランザクション ログの内容は、FTP を使用して定期的に外部サーバにエクスポートできます。また、ログ ローテーション ポリシーを設定することもできます。

（注）　ACNS 5.3.1 ソフトウェアおよびそれ以降のリリースでは、SFTP を使用して、トランザクション ログの内容を外部サーバにエクスポートすることもできます。

ACNS 5.x ソフトウェアが実行されているスタンドアロン Content Engine では、レポートの目的で、すべてのエラーとアクセス アクティビティを記録できます。ACNS 5.x ソフトウェアでは、Content Engine 上の各コンテンツ サービス モジュール（HTTP モジュール、WMT サーバ、FTP プロキシ プロセス、TFTP サーバなど）によって、サービスされた要求のログが記録されます。たとえば、次のタイプの要求が記録されます。

- HTTP 要求
- HTTPS 要求
- FTP 要求
- WMT 要求
- RTSP ストリーミング要求
- TFTP 要求

（注）　*トランザクション*という用語は、Web リソースにおいてクライアントによって実行され、正常終了または異常終了した要求を指します。

RTSP の場合、Windows Media Player の Play メニューから **Repeat** オプションを選択すると、メディア ファイルが連続的にループ再生され、ファイルの再生ごとにトランザクション ログに余分なエントリが記録されます。ほとんどの場合、この現象はプレーヤーの動作が原因で WMT RTSPU プロトコルで発生します。

特定プロトコルの統計情報の表示

コンテンツ転送の各プロトコルには、それぞれ、個々のプロトコルの統計情報を表示するための **show** *protocol-name* **statistics** EXEC コマンドがあります。たとえば、**show statistics http** EXEC コマンドを使用すると、Content Engine によって処理された HTTP 要求に関する重要な統計情報を表示することが可能です。

```
ContentEngine# show statistics http ?
  cluster      Display healing mode statistics
  ims          Display If-Modified-Since statistics
  miss-reason  Display miss/revalide/no-store reason statistics
  monitor      Display http monitor statistics
  object       Display object statistics
  performance  Display performance statistics
  proxy        Display proxy mode statistics
  requests     Display request statistics
  savings      Display savings statistics
  usage        Display usage statistics
```

表 21-10 に、**show** *protocol-name* **statistics** EXEC コマンドを示します。このコマンドの詳細については、『*Cisco ACNS Software Command Reference*』Release 5.5 を参照してください。

表 21-10　show protocol-name statistics EXEC コマンド

コマンド	説明
show statistics https [**error** | **requests**]	Content Engine の HTTPS 統計情報を表示する。
show statistics http {**cluster** | **ims** | **miss-reason** | **monitor** | **object** | **performance** | **proxy outgoing** | **requests** | **savings** | **usage**}	Content Engine の HTTP 統計情報を表示する。
show statistics ftp-over-http	Content Engine の FTP 統計情報を表示する。FTP-over-HTTP 要求の統計情報が含まれます。
show statistics ftp-native	Content Engine の FTP ネイティブ統計情報を表示する。FTP ネイティブ要求についての統計情報（GET 要求に対する FTP ネイティブ エラーなど）が含まれます。
show statistics rtsp {**proxy media-real** {**requests** | **savings**}} {**all** | **bw-usage** | **performance** | **requests**}	Content Engine の RealMedia 要求の統計情報を表示する。
show statistics wmt {**all** | **bytes** [**incoming** | **outgoing**] | **errors** | **multicast** | **requests** | **rule** | **savings** | **streamstat** | **urlfilter** | **usage**}	Content Engine の WMT 要求の統計情報を表示する。

（注）　ACNS 5.3.1 ソフトウェア リリースでは、**show statistics ftp** EXEC コマンドは **show statistics ftp-over-http** および **show statistics ftp-native** EXEC コマンドに置き換えられました。ACNS 5.3.1 ソフトウェア リリースでは、**clear statistics ftp** EXEC コマンドは **clear statistics ftp-over-http** コマンドおよび **clear statistics ftp-native** EXEC コマンドに置き換えられました。

次の例では、モニタリング対象の特定の URL（http://www.abccorp.com など）の HTTP モニタリング統計情報を表示する方法を示しています。

```
ContentEngine# show statistics http monitor
HTTP Monitor URL statistics
---------------------------

Monitor URL                              = http://www.abccorp.com
Total requests                           = 2547
Failed requests                          = 3
Requests above acceptable delay          = 1
Minimum response time                    = 0.072 seconds
Maximum response time                    = 120.281 seconds
```

次の例では、Content Engine によってサービスされた HTTPS 要求に関するモニタリング統計情報を表示する方法を示しています。

```
ContentEngine# show statistics https requests

                            HTTPS Statistics
                                                Total                % of Total
                           ---------------------------------------------------
          Total connections: 1328-
         Tunneled (CONNECT):                        0                      0.0
            Tunneled (wccp):                        0                      0.0
             SSL terminated:                        0                      0.0
          Connection errors:                        0                      0.0
                Total bytes: 8013157-
  Bytes received from client:                  1602824                   20.0
        Bytes sent to client:                 6410333                   80.0
  Bytes received from server:                        0                      0.0
```

次の例では、正常終了または異常終了した発信プロキシ要求のモニタリング統計情報を表示する方法を示しています。

```
ContentEngine# show statistics http proxy outgoing
                    HTTP Outgoing Proxy Statistics

                  IP      PORT    ATTEMPTS    FAILURES
-----------------------------------------------------------------------
             10.10.10.10    1      49026      49026
```

次の例では、Content Engine によって受信された HTTP 要求に関する統計情報を表示する方法を示しています。

```
ContentEngine# show statistics http requests
                            Statistics - Requests
                                          Total             % of Requests
                           -------------------------------------------------
     Total Received Requests:              525979748                        -
               Forced Reloads:                 501468                      0.1
                Client Errors:                  81834                      0.0
                Server Errors:                 149808                      0.0
          URL Blocked (Reset):              514998075                     97.9
                  URL Blocked:                      0                      0.0
       Sent to Outgoing Proxy:                      0                      0.0
Failures from Outgoing Proxy:                       0                      0.0
Excluded from Outgoing Proxy:                       0                      0.0
              ICP Client Hits:                      0                      0.0
              ICP Server Hits:                      0                      0.0
                If-Range Hits:                     32                      0.0
            HTTP 0.9 Requests:                    677                      0.0
            HTTP 1.0 Requests:              524097101                     99.6
            HTTP 1.1 Requests:                1881966                      0.4
         HTTP Unknown Requests:                      4                      0.0
             Non HTTP Requests:                      0                      0.0
           Non HTTP Responses:                    1380                      0.0
       Chunked HTTP Responses:                 1631953                      0.3
         Http Miss Due To DNS:                   31050                      0.0
      Http Deletes Due To DNS:                   12914                      0.0
  Objects cached for min ttl:                   575986                      0.1
```

次の例は、**show statistics http performance** EXEC コマンドの出力例です。このコマンド出力では、Content Engine によってサービスされた HTTP 要求のパフォーマンスに関する統計情報が表示されます。

```
ContentEngine# show statistics http performance
                              Statistics - Performance
                            Avg          Min             Max            Last
                   ------------------------------------------------------------
Requests / Second:          -            -             677               3
   Bytes / Second:          -            -         5995814           81801
Seconds / Request:      0.067        0.000       15453.547           1.499
    Seconds / Hit:      0.308        0.000         979.442           0.158
   Seconds / Miss:      0.066        0.000       15453.547           1.572
                   ------------------------------------------------------------
      Object Size:                   150.2 Avg
                                       0 Min
                                 718732317 Max
                                   21386.0 Last
```

次の例は、**show statistics http savings** EXEC コマンドの出力例です。このコマンドでは、Content Engine がオリジン Web サーバからコンテンツを受信するかわりに、ローカル HTTP キャッシュ（キャッシュ ヒット）から HTTP 要求を処理することで発生する節約に関する統計情報が表示されます。

```
ContentEngine# show statistics http savings
                         Statistics - Savings
                        Requests                          Bytes
          ------------------------------------------------------------
  Total:               525980242                     79047534484
   Hits:                 1966223                     19865155481
   Miss:               524014019                     59182379003
Savings:                    0.4 %                          25.1 %
```

次の例は、**show statistics rtsp proxy media-real requests** EXEC コマンドの出力例です。このコマンド出力では、Content Engine によってサービスされた RTSP 要求の RealMedia キャッシングに関する統計情報が表示されます。

```
ContentEngine# show statistics rtsp proxy media-real requests
                  Media Cache Statistics - Requests
                                              Total              % of Requests
                                    ---------------------------------------------
     Total Received Requests:                     0                          -
            Demand Cache Hit:                     0                        0.0
           Demand Cache Miss:                     0                        0.0
         Demand Pass-Through:                     0                        0.0
                  Live Split:                     0                        0.0
            Live Pass-Through:                    0                        0.0
```

次の例は、**show statistics rtsp proxy media-real savings** EXEC コマンドの出力例です。このコマンド出力例では、コンテンツをオリジン ストリーミング サーバから複数回受信するかわりにローカル キャッシュからサービスしたことで生じた、RealMedia コンテンツに関するメディア キャッシュのヒットおよびミスの数と、節約の量が表示されます。

```
ContentEngine# show statistics rtsp proxy media-real savings
              Media Cache Statistics - Savings
                          Requests                          Bytes
          ------------------------------------------------------------
Total:                 525980242                     79047534484
   Hits:                 1966223                       19865155481
   Miss:               524014019                       59182379003
Savings:                    0.4 %                           25.1 %
```

ACNS ソフトウェア トランザクション ログの使用

スタンドアロン Content Engine（キャッシングおよびストリーミング エンジン）の管理者は、一般に、Content Engine 上で行われた要求のタイプや要求によってもたらされた結果に注目します。たとえば、ストリーミング メディアが会社の収入源である場合、その会社では、どのお客様がどのコンテンツにアクセスしたかや、ユーザがどれくらいの時間コンテンツを見たか、また、その表示時の品質などをトラッキングする手段が必要になります。これらの会社では、オンデマンド コンテンツやライブ ブロードキャストの配信について課金する必要があるため、コンテンツ アクセス サービスに関するお客様への請求については、記録された情報に基づいて行う必要があります。

ACNS 5.x ソフトウェアが実行されているスタンドアロン Content Engine では、すべてのエラーとアクセス アクティビティを記録できます。ACNS 5.x ソフトウェア リリースでは、Content Engine 上の各コンテンツ サービス モジュール（HTTP モジュール、WMT サーバ、FTP プロキシ プロセス、TFTP サーバなど）によって、サービスされた要求のログが記録されます。これらのログは、トランザクション ログと呼ばれています。

通常トランザクション ログに記録される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、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 ログは、通常、次のような目的で使用されます。

- 問題の特定と解決
- 負荷のモニタリング
- 課金請求
- 統計分析
- セキュリティ上の問題分析
- コスト分析とプロビジョニング

トランザクション ログの生成、格納、管理において高い信頼性を確保することは、課金、コスト分析、プロビジョニングにとって非常に重要です。

Content Engine 上の translog モジュールは、トランザクション ロギングを処理し、次の 4 つの主要ロギング形式をサポートしています。

- Apache Common Log File（CLF）形式
- Squid
- 拡張 Squid
- World Wide Web Consortium（W3C）カスタマイズ可能なログ形式

Apache CLF および Squid 形式は、それらを派生したオリジナル アプリケーションに対応する固定形式です。Content Engine は、W3C のカスタマイズ可能なログ形式で定義されている形式（表 21-12 を参照）の大部分をサポートしています。

Windows Media Services 9 シリーズでは、Windows Media Services Version 4.1 よりもより強固なロギング モデルが提供されています。ACNS 5.2.1 ソフトウェアおよびそれ以降のリリースでは、Windows Media Services 9 ロギングがサポートされています。

定義された形式での記録が可能です（Squid、拡張 Squid、Apache の各形式や、カスタム トランザクション ログ形式を使用して、ログにフィールドを追加することも可能）。トランザクション ログの内容は、FTP を使用して外部サーバにエクスポートできます（ACNS 5.3.1 ソフトウェアおよびそれ以降のリリースでは、SFTP を使用して、トランザクション ログの内容を外部サーバにエクスポートすることもできます）。また、ログ ローテーション ポリシーを設定することもできます。

（注）　同時にアクティブにできるログ形式は 1 形式のみです。Content Engine GUI からトランザクション ロギングをイネーブルにした場合は、Squid ログ形式が使用されます。

ACNS 5.2.1 ソフトウェアおよびそれ以降のリリースでは、トランザクション ログ機能が追加され、他のデバイスへのリアルタイム トランザクション ログ機能が実行できるようになりました。リモート Syslog サーバに対して HTTP トランザクション ログ メッセージを送信するよう、Content Engine を設定することが可能です。これによって、HTTP トランザクションの認証エラーのモニタリングをリアルタイムに行うことができます。詳細は、「HTTP 要求認証エラーのリアルタイムでのモニタリング」（p.21-50）を参照してください。

トランザクション ロギングは、ACNS ソフトウェアが実行されている Content Engine 上では、デフォルトでディセーブルになっています。トランザクション ロギングを Content Engine 上でイネーブルにするには、Content Engine GUI または CLI のいずれかを使用できます。

Content Engine GUI からトランザクション ロギングをイネーブルにした場合は、次の出力例のように、Squid ログ形式が使用されます。

```
ContentEngine(config)# transaction-logs ?
  archive             Configure archive parameters
  enable              Enable transaction log feature
  export              Configure file export parameters
  file-marker         Add entries to translog indicating the file begin and end
  format              log file format (default squid)
  log-windows-domain  Log Windows domain with authenticated username if
                      available
  sanitize            Mask end user identities in log file
```

表 21-11 に、スタンドアロン Content Engine でのトランザクション ロギングのデフォルト設定を示します。

表 21-11　スタンドアロン Content Engine でのトランザクション ロギングのデフォルト設定

オプション	デフォルト設定	詳細
アーカイブ	ディセーブル	「作業ログのアーカイブ」（p.21-48）を参照してください。
トランザクション ロギング	ディセーブル	「トランザクション ロギングのイネーブル化」（p.21-35）を参照してください。
エクスポート時の圧縮	ディセーブル	「トランザクション ログ ファイルのエクスポート」（p.21-45）を参照してください。
トランザクション ログのエクスポート	ディセーブル	「トランザクション ログ ファイルのエクスポート」（p.21-45）を参照してください。
ファイル マーカー	ディセーブル	ファイルの先頭と末尾を示すため、トランザクション ログ ファイルにエントリを追加する際に使用する。
サニタイズ トランザクション ロギング	ディセーブル	「トランザクション ログのサニタイジング」（p.21-44）を参照してください。
アーカイブ間隔	毎日 1 時間ごと	「作業ログのアーカイブ」（p.21-48）を参照してください。
アーカイブファイルの最大サイズ	2,000,000 KB	「作業ログのアーカイブ」（p.21-48）を参照してください。
エクスポート間隔	毎日 1 時間ごと	「トランザクション ログ ファイルのエクスポート」（p.21-45）を参照してください。
トランザクション ログ形式	Squid ネイティブ ログ ファイル形式	「トランザクション ロギングのイネーブル化」（p.21-35）を参照してください。

（注）　SmartFilter によって、許可されるトランザクションと拒否されるトランザクションの URL に関連するカテゴリを示す情報が、トランザクション ログに書き込まれます。この機能を利用する場合、SmartFilter GUI を使用して、すべての SmartFilter ロギング オプションをイネーブルにする必要があります（SmartFilter GUI から **Logging Options** で **All** オプションを選択）。

ACNS トランザクション ログを使用する場合の詳細は、次の項を参照してください。

- トランザクション ロギングのイネーブル化（p.21-35）
- 認証ユーザ名の Windows ドメインの記録（p.21-44）
- トランザクション ログのサニタイジング（p.21-44）
- トランザクション ログ ファイルのエクスポート（p.21-45）
- スタンドアロン Content Engine でのトランザクション ロギングのエクスポート設定の変更（p.21-46）
- スタンドアロン Content Engine でのトランザクション ログ設定の表示（p.21-53）
- 外部 FTP サーバからのパーマネント エラー受信後のエクスポートの再開（p.21-47）

トランザクション ロギングのイネーブル化

ACNS 5.x ソフトウェアでは、Squid、拡張 Squid、または Apache のいずれかのトランザクション ログ形式を選択できます。また、カスタム ログ形式を使用して、ログにフィールドを追加することもできます（表 21-12 を参照）。

表 21-12　サポートされるトランザクション ログ形式のリスト

トランザクション ログ形式のスタイル	詳細
Squid	「Squid スタイルのトランザクション ロギングのイネーブル化」（p.21-36）を参照してください。
拡張 Squid	「拡張 Squid スタイルのトランザクション ロギングのイネーブル化」（p.21-37）を参照してください。
Apache	「Apache スタイルのトランザクション ロギングのイネーブル化」（p.21-37）を参照してください。
カスタム	「トランザクション ロギング時のカスタム形式のイネーブル化」（p.21-38）を参照してください。

（注）　同時にアクティブにできるログ形式は 1 形式のみです。Content Engine GUI からトランザクション ロギングをイネーブルにした場合は、Squid ログ形式が使用されます。

ACNS 5.2.1 ソフトウェアおよびそれ以降のリリースでは、リモート Syslog サーバに HTTP トランザクション ログ メッセージを送信する機能がサポートされています。この機能によって、HTTP トランザクション認証エラーがリアルタイムでモニタリングできます。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 ログ記録は、変更されずに残ります。リアルタイムなトランザクション ロギングの詳細は、「HTTP 要求認証エラーのリアルタイムでのモニタリング」（p.21-50）を参照してください。

FTP クライアント ユーザ名の記録

ACNS 5.4.1 ソフトウェアおよびそれ以降のリリースでは、Content Engine での要求認証（プロキシ認証）が非透過 FTP ネイティブ要求（Reflection X クライアント、WS-FTP クライアント、および UNIX または DOS コマンドライン FTP プログラムなどの FTP クライアントからの非透過 FTP ネイティブ要求）に対して追加されました。

Content Engine が次のいずれかのトランザクション ロギング形式を使用するように設定されている場合は、プロキシ認証が FTP クライアントで正常に行われると、クライアントが指定したユーザ名がトランザクション ログに記録されます。

- 拡張 Squid ロギング
- カスタム ロギング

（注）　カスタム トランザクション ロギングを使用する場合、指定したユーザ名をトランザクション ログに記録するには、**transaction-logs format custom** グローバル コンフィギュレーション コマンドに **%u** 形式指示子を加える必要があります。

FTP クライアントでプロキシ認証が失敗すると、モニタリング目的で、認証の失敗が Syslog に記録されます。スタンドアロン Content Engine 上でトランザクション ロギングをイネーブルにし、設定する方法の詳細については、「トランザクション ロギングのイネーブル化」（p.21-35）を参照してください。

Squid スタイルのトランザクション ロギングのイネーブル化

Squid スタイル形式のトランザクション ロギングをイネーブルにするには、**transaction-logs format squid** 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。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 ファイル形式に対応付けられたネイティブ ログ ファイル形式です。

Squid ログ ファイル形式は、次のとおりです。

```
time elapsed remote host code/status bytes method URL rfc931 peer status/peer host
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 -
```

ACNS 5.4.1 ソフトウェアおよびそれ以降のリリースでは、FTP プロキシ認証がサポートされています。拡張 Squid ロギングまたはカスタム ロギングが Content Engine に設定されている場合に、FTP プロキシ認証が特定のクライアント（Reflection X、WS-FTP クライアント、あるいは UNIX または DOS コマンドライン FTP プログラム）で正常に行われると、FTP プロキシ認証プロセス時にクライアントが指定したユーザ名がトランザクション ログに記録されます。

Squid トランザクション ログは、キャッシュのワークロードやパフォーマンスに関する貴重な情報源です。

表 21-13 に、Squid スタイル形式に関連したフィールドを表示します。

表 21-13　Squid スタイル形式に関する説明

フィールド	説明
Time	ミリ秒単位で表示される Coordinated Universal Time（UTC; 協定世界時）を使用した UNIX タイムスタンプ（秒単位）
Elapsed	キャッシュがトランザクションで使用されていた時間の長さ（ミリ秒） **（注）** エントリがログに記録されるのは、トランザクションの存続中ではなく、応答の送信後です。
Remote host	要求側インスタンスの IP アドレス
Code/status	スラッシュで区切られた 2 つのエントリ。最初のエントリは、トランザクションの結果についての情報（要求の種類、処理の方法、エラー状況など）です。2 番めのエントリには、HTTP 結果コードが含まれています。
Bytes	クライアントに配信されたデータの量。ヘッダーもカウントされているため、オブジェクトの正味のサイズではありません。また、失敗した要求がエラー ページを配信する場合に備えて、そのページのサイズもここに記録されます。
Method	オブジェクトを取得するための要求方式（GET など）
URL	要求された URL
Rfc931	認証サーバの ID、または要求側クライアントの検索名が入る。このフィールドは、常に「-」（ダッシュ）です。

表 21-13　Squid スタイル形式に関する説明（続き）

フィールド	説明
Peer status/Peer host	スラッシュで区切られた 2 つのエントリ。最初のエントリは、要求が処理された方法（ピアに要求を転送した、送信元に要求を戻したなど）を説明するコードを表します。2 番めのエントリには、オブジェクトの要求元ホストの名前が含まれています。このホストは、オリジン サイト、親、またはその他のピアである場合があります。ホスト名は数値の場合もあります。
Type	HTTP 応答ヘッダーに表示されるオブジェクトの MIME タイプ。ACNS 5.x ソフトウェアでは、このフィールドには常に「-」（ダッシュ）が入っています。

（注）　公開されているツールの中には、Squid スタイルのトランザクション ログをレポートに変換するツールが多数あります。このツールのリストについては、http://www.squid-cache.org/Scripts を参照してください。

拡張 Squid スタイルのトランザクション ロギングのイネーブル化

拡張 Squid 形式のトランザクション ロギングをイネーブルにするには、**transaction-logs format extended-squid** 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。拡張 Squid 形式では、Squid 形式でロギングされるフィールドのほかに、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 Rfc931 フィールド（表 21-13）が、許可ユーザのログ記録に使用されます。ユーザ情報が入力されていない場合、Rfc931 フィールドには常に「-」（ダッシュ）が入ります。

拡張 Squid スタイルのログ ファイルの形式の例は、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 ロギングのイネーブル化

Apache スタイル形式のトランザクション ロギングをイネーブルにするには、**transaction-logs format apache** 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。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 ファイルの形式の例は、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
```

この形式は、W3C 作業グループによって定義された Common Log File（CLF）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。詳細については、http://www.w3.org/Daemon/User/Config/Logging.html にある W3C CLF 形式の Web サイトを参照してください。

表 21-14 に、Apache CLF 形式に関連したフィールドを示します。

表 21-14　Apache CLF 形式に関する説明

フィールド	説明
Remotehost	リモート ホスト名または IP アドレス
Rfc931	認証サーバの ID、または要求側クライアントの検索名が入る。このフィールドは、常に「-」（ダッシュ）が入っています。
Authuser	ユーザが認証の目的で入力するユーザ名。ユーザ情報が入力されていない場合、このフィールドは常に「-」（ダッシュ）です。
Date	要求の日付と時刻
Request	要求の先頭行
Status	HTTP ステータス コード（例：200）
Bytes	転送された文書のコンテンツの長さ

トランザクション ロギング時のカスタム形式のイネーブル化

定義済みのネイティブ Squid 形式または拡張 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記録するには、**transaction-logs format custom** *log-format-string* 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。

```
ContentEngine(config)# transaction-logs format custom log-format-string
```

log-format-string は、カスタム形式を指定するトークンの引用符付きストリングです。このログ形式ストリングには、表 21-15 に示されたトークンを含めることができ、Apache ログ形式ストリングに似ています。

ログ形式ストリングには、ログ ファイルにコピーされるときに使用される次のリテラル文字を含めることが可能です。

- ダブル バックスラッシュ（\\）は、リテラル バックスラッシュを表す場合に使用できます。
- バックスラッシュに一重引用符（\'）を続けると、リテラル シングル クォートを表すことができます。ダブル クォートをログ形式ストリング中に含めることはできません。
- 制御文字の \t と \n は、それぞれタブおよび改行文字として使用されます。

（注）　ACNS 5.3.1 ソフトウェアおよびそれ以降のリリースでは、無効なカスタム ログ形式ストリングは設定できません。ただし、リリース 5.3 より前のソフトウェア リリースでは、無効なカスタム ログ形式ストリングを設定できます。したがって、Content Engine を ACNS 5.2 ソフトウェアから ACNS 5.3 ソフトウェアまたはそれ以降のリリースにアップグレードすると、すでに設定してある無効なカスタム ログ形式はすべて削除されます。

次の例は、よく知られている Apache CLF 形式を生成するカスタム ログ形式を指定する方法を示しています。

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"

次に示すトランザクション ログ エントリの例は、Apache CLF 形式のもので、上述のカスタム形式ストリングを使用して設定したものです。

```
[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)"
```

カスタム形式では現在、次の要求ヘッダーがサポートされています。

- User-Agent
- Referer
- Host
- Cookie

次の各要求に対する出力では、カスタム ログ形式ストリングで指定されている Request、Referer、および User-Agent 形式トークンが、トランザクション ログ エントリ内では常に二重引用符で囲まれています。

%r

%{Referer}i

%{User-Agent}i

%{Cookie}i 形式のトークンは、二重引用符で囲まなくても生成できます。これは Cookie 値がすでに二重引用符で囲まれているからです。Cookie 値には、複数の属性と値のペアがあり、各ペアはスペースで区切られています。この理由により、Cookie 形式トークンをカスタム形式ストリングで使用する場合は、ストリングの最後尾に指定することを推奨します。Cookie 形式トークンを最後尾に指定すると、ログをトランザクション ログ レポーティング ツールで解析するときも簡単になります。または形式トークン ストリングを「\'%{Cookie}i\'」のように使用した場合、Cookie ヘッダーは一重引用符で囲む必要があります。

表 21-15 に、ログ形式ストリングで使用が許されている形式のトークンを示します。表 21-15 に示されている形式トークンの「...」部分は、オプションの条件を表しています。形式トークンのこの部分は、%a のようにブランクにしておくことも可能です。オプションの条件が形式トークンに指定されていて、その条件が合致している場合は、表 21-15 の値欄に示されいる内容がトランザクション ログの出力に含められます。オプションの条件が形式トークンで指定されていて、条件が合致しない場合は、結果のトランザクション ログ出力は、ダッシュ（-）に置き換えられます。条件の形式は、HTTP ステータス コードをリストにしたもので、感嘆符（!）が行頭に付く場合と付かない場合があります。

- 感嘆符は、感嘆符に続くすべてのステータス コードを否定する場合に使用されます。これは、「!」のあとに表示されているステータス コードのいずれもが、要求の HTTP ステータス コードと一致しないときは、形式トークンに関連する値がログに記録されることを意味します。
- 「!」のあとに表示されているステータス 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、ダッシュ（-）がログに記録されます。

たとえば、「%400,501{User-Agent}i」の指定では、エラー 400 および 501 の場合（Bad Request, Not Implemented）のみ、User-Agent ヘッダー値がログに記録されます。「%!200,304,302{Referer}i」の指定では、ノーマル ステータスを戻さなかった要求の場合はすべて、Referer ヘッダー値がログに記録されます。

表 21-15　カスタム ログ形式ストリングの値

形式トークン	値
%...a	要求側クライアントの IP アドレス
%...A	オブジェクトがサービスされたサーバの IP アドレス（オリジン サーバあるいはキャッシュ ミスの場合の発信プロキシ、または、キャッシュ ヒットの場合の 0.0.0.0 など）
%...B %...b	HTTP ヘッダーを除く送信バイト数
%...c	要求の完了時の接続ステータス X：接続は応答が完了する前に異常終了 +：接続は応答後に継続可能 磨 F 接続は応答後に終了
%...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 アドレスがログに記録される）
%...H	要求プロトコル
%...{Foobar}i	Foobar コンテンツ：サーバに送られた要求中のヘッダー行。Foobar 値は、次のヘッダーの 1 つ：User-Agent、Referer、Host、または Cookie
%...l	リモート ログ名。Content Engine には実装されていないため、ダッシュ（-）がログに記録されます。
%...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 には適用されないため、ダッシュ（-）がログに記録されます
%...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、存在しない場合は空のストリング）
%...r	要求の先頭行
%...s	ステータス。translog code 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 21-16 に指定されている形式トークンによって記録される時刻
%...T	要求のサービスに要した時間（秒、小数部 3 桁の浮動小数点数値）
%...u	リモート ユーザ。ACNS 5.4.1 ソフトウェアおよびそれ以降のリリースでは、FTP プロキシ認証がサポートされています。拡張 Squid ロギングまたはカスタム ロギングが Content Engine に設定されている場合に、FTP プロキシ認証が特定のクライアント（Reflection X、WS-FTP クライアント、あるいは UNIX または DOS コマンドライン FTP プログラム）で正常に行われると、FTP プロキシ認証プロセス時にクライアントが指定したユーザ名がトランザクション ログに記録されます。カスタム トランザクション ロギング形式を使用する場合には、**transaction-logs format custom** コマンドの設定時に、**%u** 形式指定子を使用する必要があります。
%...U	要求された URL パス（照会ストリングを含まない）
%...v %...V	要求の中でホストが指定された場合にレポート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 アドレスがレポートされます。

表 21-16 に、表 21-15 で説明した形式トークン、**%...{format}t** で表示される日付と時刻の形式トークンを示します。

表 21-16　日付および時刻を表す形式トークン

形式トークン	値
%a	曜日名（省略形）
%A	曜日名（フルスペル）
%b	月名（省略形）
%B	月名（フルスペル）
%c	日付と時刻
%C	世紀（年を 100 で割り、2 桁の整数で表す）
%d	2 桁で表した日にち（01 ～ 31）
%D	%m/%d/%y に相当（米国以外の国では、%d/%m/%y が一般的。インターナショナルな場では、この形式は誤解を招く可能性があるため、使用を避けることを推奨します）
%e	%d と同じ。ただし、日にちの先頭の数字が 0 の場合は、スペースが代入されます。
%G	ISO 8601 に規定された 10 進数表記の世紀を使用した年。ISO 週数に対応する 4 桁の年数（%V を参照）。これは、%y と同じ形式と値です。ただし、ISO 週数を前年および翌年に含める場合は、その年を使用します。
%g	%G と同様です。ただし、世紀を使用しません。2 桁の年数を使用（00 ～ 99）
%h	%b と同様
%H	24 時間表示を採用する場合の 2 桁で表した時間（00 ～ 23）
%I	12 時間表示を採用する場合の 2 桁で表した時間（01 ～ 12）
%j	3 桁で表した年間の日にち（001 ～ 366）
%k	2 桁で表した時間（24 時間表示）（0 ～ 23）。1 桁の場合、先頭の 0 は省略します（%H も参照）。
%l	2 桁で表した時間（12 時間表示）（1 ～ 12）。1 桁の場合、先頭の 0 は省略します（%I も参照）。
%m	2 桁で表した月（01 ～ 12）
%M	2 桁で表した分（00 ～ 59）
%n	改行文字
%p	所定のタイム値に応じた AM または PM 表示、または現行のロケールに対応するストリング。正午は pm、午前 0 時は am として表示
%P	%p と同様。ただし、小文字で表示。am、pm、または現行ロケールに対応するストリングとして表示
%r	a.m. または p.m. 表示の時刻（「%I:%M:%S %p」と同一）
%R	24 時間表示の時刻（%H:%M）。秒表示を含む場合は、下の %T を参照
%s	新しい年代以降の秒数（1970-01-01 00:00:00 UTC）
%S	2 桁で表した秒（範囲：00 ～ 61）
%t	タブ文字
%T	24 時間表示の時刻（%H:%M:%S）
%u	10 進数表示の曜日（範囲：1 ～ 7、月曜は 1。%w も参照）
%U	2 桁で表した現行年内の週数（範囲：00 ～ 53、年頭の最初の日曜日を 01 週の第 1 日として起算。%V と %W も参照）

表 21-16　日付および時刻を表す形式トークン（続き）

形式トークン	値
%V	ISO 8601：2 桁で表した現行年（1988 年）の週数。範囲は、1 ～ 53。現行年では第 1 週に少なくとも 4 日が存在し、月曜日が週の第 1 日となる（%U と %W も参照）。
%w	10 進数表示の曜日（範囲：0 ～ 6、日曜は 0。%u も参照）
%W	現行年内での週数を 2 桁の数字で表示（範囲：00 ～ 53、年頭の最初の月曜日を 01 週の第 1 日として起算）
%x	日付（時刻は表示しない）
%X	時刻（日付は表示しない）
%y	世紀を表示しない 2 桁で表した年（00 ～ 99）
%Y	世紀を表示する 2 桁で表した年
%z	GMT との偏差時間帯。RFC822 適合日付の発行に必要（「%a, %d　%b　%Y %H:%M:%S %z」を使用）
%Z	時間帯、名称、または略語
%%	リテラル % 文字

W3C のカスタマイズ可能なログ形式は、HTTP Web サーバの観点で定義されているという制限があり、固定 Squid 形式で提供されるような Web キャッシュ固有のカスタム オプションを提供しません。したがって、ACNS 5.3.1 ソフトウェアまたはそれ以降のリリースでは、W3C

のカスタマイズ可能なログ形式を拡張する形式トークンが追加され、Cisco や Squid のようなカスタマイズされたロギング フィールドがサポートされます。これらの新しい形式トークンにより、W3C のカスタマイズ可能なトークン セットから Squid のようなロギング形式がサポートされます。

ACNS 5.3.1 ソフトウェアおよびそれ以降のリリースでは、次のトランザクション ロギング サポートを使用できます。

- W3C 形式でサポートされなかった拡張 Squid-equivalent トークンのサポート
- 設定された HTTP 発信プロキシ（「http 発信プロキシ」）を Squid スタイル「DEFAULT_PARENT」階層イベントとして扱う、追加の階層トークンのサポート

ACNS 5.3.1 ソフトウェア リリースでは、W3C のカスタマイズ可能なログ形式が拡張され、次の特別なトークン シーケンスがサポートされるようになりました。

%...{<translog-token>}C

「...」は、オプションです。このオプションを指定すると、一連の条件付き HTTP 応答コードをカンマで区切ることができます。「C」は大文字で、カスタマイズ可能な拡張動作トークン セットを定義します。この拡張セットのトークンは、<translog-token> ディレクティブで定義されます。これは 2 文字のトークン ディレクティブです。

表 21-17 に、拡張 Squid 形式の、既存および新規の <translog-token> ディレクティブを示します。拡張 Squid 形式は、W3C 定義ではすぐにはサポートされませんが、ACNS 5.3.1 ソフトウェアおよびそれ以降のリリースでサポートされています。

表 21-17　translog トークン ディレクティブ

形式トークン	値
%...{es}C	新しい年代（1970 年 1 月 1 日）以降経過した秒数で表された、現在の時刻
%...{em}C	新しい年代（1970 年 1 月 1 日）以降経過したミリ秒で表された現在の時刻
%...{te}C	要求が完了するまでに経過したミリ秒の数値

表 21-17　translog トークン ディレクティブ（続き）

形式トークン	値
%...{rd}C	Squid のようなキャッシュ状態のコード ストリング（TCP_HIT および TCP_CLIENT_REFRESH_MISS など）
%..{cs}C	クライアントに送信されたバイト数（プロトコル ヘッダーを含む）
%...{rh}C	Content Engine に適用する、厳密な Squid スタイルの階層
%...{rH}C	拡張 Squid スタイルの階層。発信プロキシが明示的に定義され、要求を満たすために使用されて、「DIRECT/*origin_server_ip_address*」の代わりに「DEFAULT_PARENT/*proxy_ip_addess*」が記録された場合を除き、「%...{rh}C」と同じです。
%...{rt}C	応答内のオブジェクトの MIME タイプで、左記のように定義されるプロトコル ヘッダーによって指定。ACNS 5.x ソフトウェアでは、このフィールドには常に「-」（ダッシュ）が入っています。
%...{ru}C	要求されている URL で、追加の照会ストリングを含みます。
%...{as}C	アプリケーション固有の情報。アプリケーションを処理する要求が、このストリングを記録する可能性があります。これは、Squid 形式の仕様の一部としてサポートされます。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るログ情報を記録します。

表 21-17 に表示されているトークンに加え、複数の %...{xx}C スタイル トークンを単一のトークン シーケンスに圧縮して、%...{xx}C スタイル内に組み込むことができます。複数のスタイル トークンを単一の組み込みトークン シーケンスに圧縮するには、中カッコ {} 内に複数のトークンを指定し、各トークンにプレフィクスとして「%」記号を付ける必要があります。次に例を示します。

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

これを、圧縮した組み込みトークン形式で、次のように記述しなおすことができます。

%{%rh %rt %as}C

コマンドライン構文は、次のように記述された単一のトークンを認識します。

%{%rh}C

and

%{rh}C

は同義です。

出力ファイルでは、組み込みトークン シーケンスの一部ではない文字（スペースなど）が、逐語的に繰り返されます。

次の例は、W3C のカスタマイズ可能なログ形式で定義された拡張 Squid です。

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

次の例は、拡張 Squid に類似した形式で、Squid の seconds-since-epoch タイムスタンプ形式の代わりにユーザが読み取り可能なタイムスタンプが使用されることと、設定された発信プロキシ（「%...{rH}C」によって指定）が記録されることを指定しています。

[%{%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

不明またはサポートされていない translog トークンは、ログ ファイルに記録されません。トークンの指定シーケンス外の文字はすべて、ログ ファイルに逐語的に繰り返されます。

認証ユーザ名の Windows ドメインの記録

Content Engine が NTLM 認証用に設定されており、拡張 Squid スタイル形式またはカスタム形式が使用されている場合、**transaction-logs log-windows-domain** グローバル コンフィギュレーション コマンドによって、トランザクション ログのユーザ名フィールド内に、Windows のドメイン名とユーザ名が記録されます。ドメイン名が使用可能な場合、ドメイン名とユーザ名の両方が、ユーザ名フィールドに、ドメイン \ ユーザ名の形式で記録されます。ユーザ名のみが使用可能な場合は、ユーザ名のみがユーザ名フィールドに記録されます。ドメイン名とユーザ名の両方が使用不可能な場合、ダッシュ（-）がこのフィールドに記録されます。

NTLM 認証に使用される Windows ドメイン名は、トランザクション ログのユーザ名フィールドに表示されます。拡張 Squid スタイル形式、または **%u** 形式トークンを使用してユーザ名が含まれているカスタム形式のトランザクション ログでは、ユーザ名がドメイン \ ユーザ名の形式で表示されます。（**%u** 形式トークンでは、曜日が 10 進数で指定されます。範囲は 1 ～ 7 で、1 は月曜日です）。

拡張 Squid スタイルまたはカスタム形式のトランザクション ログで NTLM パラメータのロギングを無効にする場合は、**no transaction-logs log-windows-domain** グローバル コンフィギュレーション コマンドを入力します。

トランザクション ログのサニタイジング

クライアントは、トランザクション ログ ファイルの IP アドレスとユーザ名を偽装することができます。デフォルトでは、このトランザクション ログはサニタイズされません。サニタイズしたトランザクション ログでは、クライアントのネットワーク上の身元を識別する IP アドレスが 0.0.0.0 に変更されて、トランザクション ログに記録されます。

次のインターフェイスを使用すると、トランザクション ログのサニタイズ機能をイネーブルにできます。

- Content Engine GUI：Content Engine GUI で、**Cache > Transaction Logs** を選択します。**Transaction Log Enable** チェックボックスにチェックマークを付けて、Content Engine のトランザクション ロギングをアクティブにします。次に **Sanitize transaction logs** オプション ボタンをクリックして、サニタイズ機能をイネーブルにします。**Update** をクリックして設定値を適用します。
- Content Engine CLI ：**transaction-logs sanitized** 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。

  ```
  ContentEngine(config)# transaction-logs sanitize
  ```

  サニタイズ機能をディセーブルにするには、このコマンドの **no** 形式を使用します。
  transaction-logs sanitize コマンドは、CLI で設定された、つまり **transaction-logs format custom** *string* グローバル コンフィギュレーション コマンドで設定された、カスタム ログ形式ストリングに関連するクライアント IP（%a）値には影響しません。このグローバル コンフィギュレーション コマンドの *string* は、カスタム ログ形式を含む引用符付きログ形式ストリングです。カスタム ログ形式のクライアント IP のユーザ ID を隠すには、カスタム ログ形式ストリングに 0.0.0.0 をハード コーディングするか、クライアント IP を表す %a トークンを形式ストリングから除きます。

トランザクション 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、FTP を使用して、設定可能な間隔でログ 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 に使用されるユーザ名とパスワードは設定が可能で、ログ ファイルのアップロード先のディレクトリも設定が可能です。ACNS 5.3.1 ソフトウェアおよびそれ以降のリリースでは、SFTP を使用して、トランザクション ログの内容を外部ホストにエクスポートすることもできます。

ログ ファイルには、自動的に次のファイル名が付けられます。

type_ipaddr_yyyymmdd_hhmmss.txt

ここで各パラメータの意味は、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、および FTP などのキャッシュ ログの場合は *celog*、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、ログがエクスポートのためにアーカイブされた日付と時刻を表します。

（注）　MMS タイプ ログの場合、ファイル名に .txt 拡張子はありません。

トランザクション ログの外部の FTP サーバまたは SFTP サーバへのエクスポート

Content Engine GUI または CLI を使用すると、トランザクション ログを外部の FTP サーバまたは SFTP サーバへエクスポートすることができます。

Content Engine GUI から、**Caching > Transaction Logs** の順に選択します。表示された Transaction Logs ウィンドウを使用して、トランザクション ログを FTP サーバまたは SFTP サーバにエクスポートします。Transaction Logs ウィンドウの使用方法に関する詳細は、ウィンドウの **HELP** ボタンをクリックしてください。

Content Engine CLI を使用して、外部の FTP サーバまたは SFTP サーバへのトランザクション ログ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　トランザクション ログを外部 FTP サーバまたは SFTP サーバへエクスポートできるようにするには、**transaction-logs export enable** 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。

ステップ 2　各ターゲット FTP サーバに、次の情報を指定します。

```
ContentEngine(config)# transaction-logs export ftp-server {hostname |
server-ip-address} login password directory
```

ここで各パラメータの意味は、次のとおりです。

- *hostname* および *server-ip-address* は、それぞれ、FTP サーバのホスト名と IP アドレスです。

  Content Engine により、DNS 検索を行ってホスト名が変換され、次に設定ファイルにこの IP アドレスが保存されます。
- *login* は、ターゲット FTP サーバに対するユーザのログインです。
- *password* は、ターゲット FTP サーバに対するユーザのパスワードです。

- *directory* は、エクスポートされるファイル（トランザクション ファイル）が書き込まれる、指定の FTP サーバ上のターゲット ディレクトリ パスです。トランザクション ログを格納する作業ディレクトリの名前を指定します。ユーザのログインには、完全修飾パスまたは相対パスを使用します。

（注）　このコマンドの *login* オプションで指定するユーザは、指定されたディレクトリの書き込み許可を持っている必要があります。

この例では、2 つの FTP サーバに対してトランザクション ログをエクスポートするよう、Content Engine が設定されています。

```
ContentEngine(config)# transaction-logs export ftp-server 10.1.1.1
mylogin mypasswd /ftpdirectory
ContentEngine(config)# transaction-logs export ftp-server myhostname
mylogin mypasswd /ftpdirectory
```

ステップ 3　外部 SFTP サーバにトランザクション ログをエクスポートします。

```
ContentEngine(config)# transaction-logs export sftp-server {hostname |
server-ip-address} login password directory
```

ここで各パラメータの意味は、次のとおりです。

- *hostname* および *server-ip-address* は、それぞれ、SFTP サーバのホスト名と IP アドレスです。

  Content Engine により、DNS 検索を行ってホスト名が変換され、次に設定ファイルにこの IP アドレスが保存されます。
- *login* は、ターゲット SFTP サーバに対するユーザのログインです（40 文字未満）。
- *password* は、ターゲット SFTP サーバに対するユーザのパスワードです（40 文字未満）。
- *directory* は、エクスポートされるファイル（トランザクション ファイル）が書き込まれる、指定の SFTP サーバ上のターゲット ディレクトリ パスです。トランザクション ログを格納する作業ディレクトリの名前を指定します。ユーザのログインには、完全修飾パスまたは相対パスを使用します。

ステップ 4　アーカイブしたログ ファイルを外部の FTP サーバまたは SFTP サーバにエクスポートする前に、gzip 形式に圧縮します。

```
ContentEngine(config)# transaction-logs export compress
```

圧縮されたファイル名には、.gz 拡張子が付きます。この機能を使用すると、Content Engine と FTP および SFTP エクスポート サーバの両方において、使用するアーカイブ ファイル用のディスク スペースが少なくなり、エクスポート時に必要な帯域幅も少なくて済みます。

スタンドアロン Content Engine でのトランザクション ロギングのエクスポート設定の変更

トランザクション ロギングのエクスポート設定（「トランザクション ロギングのイネーブル化」を参照）を行ったあとで、ユーザ名、パスワード、ディレクトリを変更する手順は、次のとおりです。

- **transaction-logs export ftp-server** グローバル コンフィギュレーション コマンドを使用して、FTP サーバの現行の設定を変更します。

- **transaction-logs exportsftp-server** グローバル コンフィギュレーション コマンドを使用して、SFTP サーバの現行の設定を変更します。

次の例のように、新しいパラメータ（mynewname、mynewpass、newftpdirectory など）を使用して行全体を入力し直すことにより、ユーザ名、パスワード、またはディレクトリを変更できます。

```
ContentEngine(config)# transaction-logs export ftp-server 10.1.1.1
mynewname mynewpass /newftpdirectory
```

現行の設定から FTP サーバを削除するには、次のように指定します。

```
ContentEngine(config)# no transaction-logs export ftp-server 10.1.1.1
```

現行の設定から SFTP サーバを削除するには、次のように指定します。

```
ContentEngine(config)# no transaction-logs export sftp-server sftphostname
```

外部 FTP サーバからのパーマネント エラー受信後のエクスポートの再開

FTP サーバがスタンドアロン Content Engine にパーマネント エラーを返すと、それ以降、アーカイブ トランザクション ログは、そのサーバにエクスポートされません。このエラー状態をクリアするには、設定に誤りがあるサーバに対して、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する必要があります。**show statistics transaction-logs** EXEC コマンドを使用すると、トランザクション ログのエクスポート準備の現在の状態が表示されます。

パーマネント エラー（Permanent Negative Completion Reply、RFC 959）は、サーバへの FTP コマンドが受信されず、アクションがとられなかったときに発生します。パーマネント エラーの原因は、無効なユーザのログイン、無効なユーザ パスワード、および、十分なアクセス権が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です。

次の例は、無効なユーザ ログイン パラメータが、**transaction-logs export ftp-server** グローバル コンフィギュレーション コマンドに含まれていた例です。**show statistics transaction-logs** EXEC コマンドを使用すると、Content Engine がアーカイブ ファイルのエクスポートに失敗したことが示されます。

```
ContentEngine# show statistics transaction-logs
Transaction Log Export Statistics:

Server:172.16.10.5
      Initial Attempts:1
      Initial Successes:0
      Initial Open Failures:0
      Initial Put Failures:0
      Retry Attempts:0
      Retry Successes:0
      Retry Open Failures:0
      Retry Put Failures:0
      Authentication Failures:1
      Invalid Server Directory Failures:0
```

アーカイブ トランザクション ログのエクスポートを再開するには、**transaction-logs export ftp-server** パラメータを再入力する必要があります。

```
ContentEngine(config)# transaction-logs export ftp-server 172.16.10.5
goodlogin pass /ftpdirectory
```

作業ログのアーカイブ

sysfs がマウントされている場所により、次のログ ファイルは、スタンドアロン Content Engine 上のローカル ディスク上にある作業ログに、次のようにロギングされます。

- WMT ログは、次のいずれかのファイル内のローカル ディスクにある作業ログにロギングされます。
  - /local1/logs/export/working.log
  - /local2/logs/export/working.log
- RealProxy ログは、次のいずれかのファイル内のローカル ディスクにある作業ログにロギングされます。
  - /local1/logs/real-proxy/working.log
  - /local2/logs/real-proxy/working.log

ユーザは作業ログをクリアする間隔を設定できます。作業ログのクリアはデータをアーカイブ ログに移動させることで行われます。sysfs ファイルのマウント場所に応じて、アーカイブ ログ ファイルはローカル ディスクのディレクトリ /local1/logs/ または /local2/logs/ に配置されます。

多数のアーカイブ ファイルが保存されるため、ファイル名にはファイルがアーカイブされた日時のタイムスタンプが含まれます。これらのファイルは FTP サーバや SFTP サーバにエクスポート可能なため、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 ファイル名の形式は、次のとおりです。

celog_IPADDRESS_YYYYMMDD_HHMMSS.txt

作業ログをアーカイブする場合は、**transaction-logs archive** 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。

transaction-logs archive interval *seconds*

transaction-logs archive interval every-day {**at** *hour:minute* | **every** *hours*}

transaction-logs archive interval every-hour {at *minute* | every *minutes*}

transaction-logs archive interval every-week [**on** *weekdays* at *hour:minute*]

transaction-logs archive max-file-size *filesize*

表 21-18 に、このコマンドのパラメータを示します。

表 21-18　transaction-logs archive CLI コマンドのパラメータ

パラメータ	説明
archive	アーカイブ パラメータを設定します。
interval	アーカイブ ファイルが保存される頻度を決定します。
seconds	アーカイブの頻度（秒単位、120 ～ 604800）
every-day	アーカイブの間隔が 1 日以内
at	アーカイブが行われる毎日のローカル時刻を指定します。
hour:minute	アーカイブが行われるローカル時刻（時 : 分）
every	間隔（時間単位）。この間隔は、午前 0 時に調整されます。

表 21-18　transaction-logs archive CLI コマンドのパラメータ（続き）

パラメータ	説明
hours	毎日のファイル アーカイブの間隔（時間単位） 1　1 時間ごと 12　12 時間ごと 2　2 時間ごと 24　24 時間ごと 3　3 時間ごと 4　4 時間ごと 6　6 時間ごと 8　8 時間ごと
every-hour	アーカイブの間隔が 1 時間以内
at	アーカイブが行われる毎時の時刻
minute	時間ごとのアーカイブを分単位で指定（0 ～ 59）します。
every	時間ごとのアーカイブの間隔（分）。この間隔は、毎時 0 分に調整されます。
minutes	時間ごとのアーカイブの間隔（分） 10　10 分ごと 15　15 分ごと 2　2 分ごと 20　20 分ごと 30　30 分ごと 5　5 分ごと
every-week	アーカイブの間隔が 1 週間に一度以上
on	（任意）アーカイブが行われる曜日
weekdays	アーカイブが行われる曜日。複数の曜日を指定できます。 Fri　毎週金曜日 Mon　毎週月曜日 Sat　毎週土曜日 Sun　毎週日曜日 Thu　毎週木曜日 Tue　毎週火曜日 Wed　毎週水曜日
at	（任意）アーカイブが行われる毎日のローカル時刻
hour:minute	アーカイブが行われるローカル時刻（時 : 分）
max-file-size	アーカイブ ファイルの最大サイズを設定
filesize	アーカイブ ファイル サイズの最大を KB 単位で指定（1000 ～ 2000000）

スタンドアロン Content Engine でのトランザクション ロギングのエクスポートのディセーブル化

スタンドアロン Content Engine 上で、トランザクション ロギング エクスポートの設定（FTP サーバや SFTP サーバの IP アドレスなどの設定情報など）を残したままトランザクション ロギングのエクスポート機能をディセーブルにするには、**transaction-logs export enable** グローバル コンフィギュレーション コマンドの **no** 形式を使用します。

```
ContentEngine(config)# no transaction-logs export enable
```

HTTP 要求認証エラーのリアルタイムでのモニタリング

ACNS 5.2.1 ソフトウェアおよびそれ以降のリリースでは、リモート Syslog サーバに HTTP トランザクション ログ メッセージを送信する機能がサポートされています。この機能により、リモート Syslog サーバで、HTTP 要求の認証の障害をリアルタイムでモニタできます。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、HTTP 要求認証エラーなどの特定のエラーについて、トランザクション ログをリアルタイムにモニタリングできます。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 ログ記録は、変更されずに残ります。

（注）　Syslog は UDP であるため、リモート Syslog ホストに転送されるメッセージには信頼性がありません。

リアルタイム トランザクション ロギング機能をサポートするため、次の CLI コマンドが ACNS 5.2.1 ソフトウェアおよびそれ以降のリリースでサポートされています。

[**no**] **transaction-logs logging enable**

[**no**] **transaction-logs logging host** {*hostname* | *ipaddr*} [**port** *port-num* **rate-limit** *msgs-per-sec*]
[**no**] **transaction-logs logging facility** *fac-name*

[**no**] **transaction-logs logging entry-type** *entry-type* [**request-auth-failures** | **all**]

これらの CLI コマンドを使用すると、トランザクション ログ メッセージをリアルタイムに受信するリモート Syslog ホストを指定できます。トランザクション ログ プロセスがリモート Syslog サーバへの送信を認められるレート（1 秒ごとのメッセージ数）を制限するため、レート リミット オプション（**rate-limit** オプション）が追加されました。トランザクション ログ メッセージを 1 つのリモート Syslog ホストへリアルタイムに送信するように、Content Engine を設定できます。

リアルタイム トランザクション ロギング機能のデフォルト設定は、次のとおりです。

- リアルタイム トランザクション ロギング機能はディセーブルです（**no transaction-logs logging enable** グローバル コマンド）。
- 指定されているリモート Syslog サーバはありません（**no transaction-logs logging host** グローバル コンフィギュレーション コマンド）。
- 指定されているロギング ファシリティはありません（**no transaction-logs logging facility** グローバル コンフィギュレーション コマンド）。
- 「user」ファシリティ（ユーザ プロセス）のトランザクション ロギング モジュールに対応付けられているファシリティを使用する場合、デフォルト ファシリティは「*」です。
- デフォルト エントリ タイプは、request-auth-failures です。詳細は、「リモート Syslog ホストへのロギングの際のトランザクション ログ エントリ タイプの指定」（p.21-52）を参照してください。
- **transaction-logs logging** オプションのデフォルトは、次のとおりです。
  - ポート 514 が使用されます。このポートは、システム ロギング用の well-known ポートです。
  - レート リミットは 0 に設定されています。これはレート リミットがないことを意味します。指定範囲は 1 秒につき 1 ～ 10,000 メッセージです。

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 ファイルの場合と同じで、シスコの標準 Syslog ヘッダー情報の前に付加されます。

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

ここで各パラメータの意味は、次のとおりです。

- 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 のプロセスの名前です。
- %CE-TRNSLG-6-460012 は、シスコ標準形式の Syslog ヘッダーです。
- <translog formatted msg> は、トランザクション ログ ファイルに表示されるトランザクション ログ メッセージです。

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場合は、次の Content Engine CLI コマンドを使用します。

```
ContentEngine(config)# transaction-logs log-windows-domain
```

これによって、NTLM 認証に使用される Windows ドメイン名が、トランザクション ログのユーザ名フィールドに表示されます。拡張 Squid スタイル形式、または **%u** 形式トークンを使用してユーザ名が含まれているカスタム形式のトランザクション ログでは、ユーザ名がドメイン\ユーザ名の形式で表示されます。HTTP トランザクション ログのプロキシ要求認証エラーは、401/407 エラーとしてレポートされ、ユーザ名が含まれます。このエラーのタイプーは、HTTP 認証エラーであることを示します。これらのエラーは、システムの Syslog にも含められます。

リアルタイム トランザクション ロギングのためのリモート Syslog ホストの設定

リモート Syslog ホストにリアルタイムでトランザクション ログ メッセージを送信するようスタンドアロン Content Engine を設定する場合は、**transaction-logs logging host** 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。

ACNS 5.2.1 ソフトウェアおよびそれ以降のリリースでは、トランザクション ロギングが設定されたリモート Syslog ホストとの通信エラーをレポートするため、Content Engine のシステム Syslog メッセージがサポートされています。%CE-TRNSLG-6-460013 から %CE-TRNSLG-3-460016 までの範囲の Syslog メッセージは、エラー メッセージです。最後のエラー メッセージ（%CE-TRNSLG-3-460016）は、レベル 6（情報レベル メッセージ）ではなく、レベル 3（エラー レベル メッセージ）です。情報レベルのメッセージは、レート リミットが原因でメッセージが廃棄された場合に、廃棄されたメッセージ数とともにレポートされます。

リモート Syslog ホストへのロギングの際のトランザクション ログ ファシリティの設定

リモート Syslog ホストにトランザクションを記録する際に、トランザクション ログ ファシリティを設定するには、**transaction-logs logging facility** 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。

```
ContentEngine(config)# transaction-logs logging facility ?
  auth    Authorization system
  daemon  System daemons
  kern    Kernel
  local0  Local use
  local1  Local use
  local2  Local use
  local3  Local use
  local4  Local use
  local5  Local use
  local6  Local use
  local7  Local use
  mail    Mail system
  news    USENET news
  syslog  Syslog itself
  user    User process
  uucp    UUCP system
```

リアルタイム トランザクション ログ エントリ用に、リモート Syslog ホスト上に別のログを作成する場合は、Content Engine 上に一意のファシリティ（local1 など）を設定します。

```
ContentEngine(config)# transaction-logs logging facility local1
```

リモート Syslog ホスト上で、この一意のファシリティからのメッセージが別のファイルへ記録されるように設定します。リモート Syslog ホストが UNIX サーバの場合の設定例は、次のとおりです。

1. /etc/syslog.conf ファイルを編集し、local1 の情報レベル メッセージが、local1 ファシリティに対応付けられている /var/log/translog-messages ファイルに書き込まれるよう、次の行を追加します。

   ```
   local1.=info /var/log/translog-messages
   ```

2. 標準出力ファイル（/var/log/messages ファイル）から情報レベル メッセージが除外されるよう、/etc/syslog.conf ファイルの次の行を変更します。

   *.info;mail.none;news.none;authpriv.none;cron.none;local1.none /var/log/messages

   UNIX システムでは、/etc/syslog.conf ファイルの構文に関するヘルプが、man syslog.conf コマンドで表示されます。

   UNIX システムでは、Syslog デーモンのポートが /etc/services で定義されています。

   ```
   syslog       514/udp
   ```

ポート 514 以外のポートが Syslog ホスト上で設定されている場合は、それと同じポートを Content Engine に設定する必要があります（**transaction-logs logging host** {*hostname* | *ipaddr*} [**port** *port-num*] グローバル コンフィギュレーション コマンド）。

リモート Syslog ホストへのロギングの際のトランザクション ログ エントリ タイプの指定

ACNS 5.2.1 ソフトウェアおよびそれ以降のリリースでは、HTTP 要求認証エラーに関連した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 Content Engine を設定できます。

企業などは、一般に、セキュリティの目的で、HTTP 要求認証エラーのみに注目します。企業は、リアルタイムでこのタイプの認証エラーをモニタリングすることにより、どのエンド ユーザが Content Engine を介した認証に失敗したかを特定できます。

```
ContentEngine(config)# transaction-logs logging entry-type ?
   all          Log all transaction messages to remote syslog host
   request-auth-failures  Log transactions CE failed to authenticate with the auth
server
```

認証サーバとの通信を試みているエンド ユーザに関連する認証エラー トランザクションのみが記録されます。認証サーバとの通信を試行しているトランザクションからの応答を待っている 保留中のトランザクションは、記録されません。この方法によって、Content Engine での認証に失敗したユーザを特定するために必要な情報が得られ、Syslog ホストに対するトラフィックは最小限に抑えられます。認証に失敗したユーザをトラッキングするためには、拡張 Squid 形式、またはカスタム形式トークン **%u** を設定したカスタム ログ形式のいずれかで設定することにより、ユーザ名を記録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 ログ形式の指定に関する詳細は、「トランザクション ロギングのイネーブル化」（p.21-35）を参照してください。

transaction-logs logging enable グローバル コンフィギュレーション コマンドが指定されると、HTTP 要求認証エラーのみの記録がデフォルトになります。このデフォルト設定を変更し、すべてのトランザクションを記録する場合は、Content Engine 上で **transaction-log logging entry-type all** グローバ

ル コンフィギュレーション コマンドを入力する必要があります。ただし、すべてのトランザクションを記録すると、Syslog ホストが着信トラフィックを処理できなくなった場合、UDP のドロップレートが急増する可能性があります。

スタンドアロン Content Engine でのトランザクション ログ設定の表示

スタンドアロン Content Engine 上でトランザクション ロギングの現在の設定に関する情報を表示する場合は、**show transaction-log** EXEC コマンドまたは **show transaction-logging** EXEC コマンドを使用します。この 2 つの EXEC コマンドによる出力は同じです。トランザクション ログ ファイル情報は、TFTP トランザクションと ICAP トランザクションの場合だけでなく、HTTP および WMT キャッシング プロキシ トランザクションの場合も表示されます。出力例については、以下を参照してください。

（注） セキュリティを確保するため、**show transaction-log** EXEC コマンドによる出力ではパスワードが表示されません。

```
ContentEngine# show transaction-log
Transaction log configuration:
---------------------------------------
Logging is enabled.
End user identity is visible.
File markers are disabled.
Archive interval: every-day every 1 hour
Maximum size of archive file: 2000000 KB
Log File format is squid.
Windows domain is not logged with the authenticated username

Exporting files to ftp servers is disabled.
File compression is disabled.
Export interval: every-day every 1 hour

HTTP Caching Proxy logging to remote syslog host is disabled.
Remote syslog host is not configured.
Facility is the default "*" which is "user".
Log HTTP request authentication failures with auth server to remote syslog host.

HTTP Caching Proxy Transaction Log File Info
  Working Log file - None existing

WMT MMS Caching Proxy/Server Transaction Log File Info
  Working Log file - size : 584
                     age: 404
  Archive Log file - mms_export_10.1.1.21_20040622_230415 size: 584
  Archive Log file - mms_export_1.1.1.1_20040623_205825 size: 584
Translog directory doesn't exist.  Maybe because /local1 has no sysfs mounted.
Translog directory doesn't exist.  Maybe because /local1 has no sysfs mounted.

TFTP Transaction Log File Info
  Working Log file - size : 88
                     age: 403
  Archive Log file - tftp_server_10.1.1.21_20040622_230415 size: 88
  Archive Log file - tftp_server_1.1.1.1_20040623_205826        size: 88

ICAP Transaction Log File Info
  Working Log file - size : 61
                     age: 403
  Archive Log file - icap_10.1.1.21_20040622_230415 size: 61
  Archive Log file - icap_1.1.1.1_20040623_205826 size: 61
```

特定の URL のパフォーマンスのモニタリング

ACNS 5.2.3 ソフトウェアおよびそれ以降のリリースでは、特定の URL のパフォーマンスをモニタリングするよう Content Engine を設定する機能がサポートされています。Content Engine には、各モニタ対象 URL のさまざまな応答特性に関する統計情報が保持されています。(新しい **show statistics http monitor** コマンドを使用すると、これらの統計情報を表示できます。後述の使用方法を参照)。

http monitor url *url* グローバル コンフィギュレーション コマンドを使用すると、Content Engine でモニタリングする最大 10 の URL を指定できます。

```
ContentEngine(config)# http monitor url ?
  WORD  URL for monitoring
```

http monitor url *url* コマンドには、**acceptable-delay** および **interval** の 2 つのコマンド オプションがあります。次の出力例では、**acceptable-delay** オプションを使用して、許容可能な遅延秒数（指定したモニタリング対象の URL の取得に要する最大秒数）を指定しています。デフォルトの許容可能遅延秒数は 60 秒です。

```
Content Engine(config)# http monitor url http://www.abc.com/ ?
  acceptable-delay  Threshold time in seconds before which the URL should be
  retrieved.(default is 60 seconds)
  interval          Interval in seconds for monitoring the URL.(default is 60 seconds)
  <cr>
```

次のコマンドの出力例では、**acceptable-delay** オプションを使用して、許容可能な遅延時間（指定した URL の取得に要する最大秒数）を指定しています。

```
Content Engine(config)# http monitor url http://www.abc.com/ acceptable-delay ?
  <1-3600>  Acceptable delay in seconds
```

（注）　**http monitor url** *url* コマンドを使用して同一の URL に異なる間隔または許容可能遅延時間を設定すると、最も新しい設定が優先され、その特定の URL について以前に設定した内容は無効になります。

次のコマンドの出力例では、**interval** オプションを使用してモニタリング間隔（Content Engine が特定の URL の要求をモニタリングする頻度）を指定しています。モニタリング間隔は、秒単位で指定します。デフォルトの監視間隔は 60 秒です。

```
ContentEngine(config)# http monitor url http://www.abc.com/ acceptable-delay 100
interval ?
  <1-3600>  Monitor interval in seconds
```

次の例では、デフォルト値（間隔および許容可能遅延時間がそれぞれ 60 秒）を使用して http://www.abc.com/ という URL をモニタリングするように Content Engine を設定しています。

```
http monitor url http://www.abccorp.com/
```

次の例では、http://www.abc.com/ という URL をモニタリングするように Content Engine を設定しています。Content Engine は、URL を取得するまでに最大 100 秒待機し、URL への要求を 100 秒ごとにモニタリングするように設定されています。

```
ContentEngine(config)# http monitor url http://www.abc.com/ acceptable-delay 100
interval 100
```

URL が取得されるまでに 100 秒以上が経過すると、指定した許容可能遅延時間を超えます。Content Engine は、応答時間（最小および最大遅延時間）と、特定の URL について許容可能遅延時間を超えた回数をトラッキングします。これらの統計情報は、新しい **show statistics http monitor** EXEC コマンドの出力に表示されます。

モニタリング対象の URL の統計情報を表示するには、**show statistics http monitor** EXEC コマンドを入力します。

```
ContentEngine# show statistics http monitor
HTTP Monitor URL statistics
---------------------------

Monitor URL                              = http://www.abc.com/
Total requests                           = 118
Failed requests                          = 30
Requests above acceptable delay          = 37
Minimum response time                    = 8.183 seconds
Maximum response time                    = 210.021 seconds

Monitor URL                              = http://www.abccorp.com/
Total requests                           = 275
Failed requests                          = 44
Requests above acceptable delay          = 26
Minimum response time                    = 0.071 seconds
Maximum response time                    = 164.061 seconds
```

このコマンド出力では、次のことが適用されます。

- Failed requests は、成功しなかった要求（URL のドメイン名の解決に失敗した要求など）です。
- Requests above acceptable delay は、指定の許容可能遅延時間（acceptable-delay 設定で指定した最大秒数）を超えた要求です。

show running-configuration EXEC コマンドの出力には、URL モニタリング設定に関する情報が含まれます。次の例で、**show running-configuration** コマンドの出力からの抜粋で、この特定の情報がボールドで強調されています。

```
ContentEngine# show running-configuration
! ACNS version 5.4
!
!
hostname sust-7320-ce1
!
http persistent-connections timeout 300
http proxy incoming 8080
http proxy outgoing preserve-407
http tcp-keepalive enable
http monitor url http://www.abc.com/ interval 100 acceptable-delay 100
http monitor url http://www.abccorp.com/
!
ftp proxy incoming 8080
!
clock timezone US/Eastern -5 0
!
!
.
.
.
```

show running-configuration コマンドからの出力には、デフォルト以外の値のみが表示されます。したがって、Content Engine がデフォルト値を使って URL http://www.abccorp.com をモニタリングするように設定されているため、出力例には、その URL に関する値が表示されていません。

モニタリング対象の各 URL についての間隔および許容可能遅延時間の設定を含め、モニタリング対象の URL のリストを表示するには、**show http monitor** EXEC コマンドを入力します。

```
ContentEngine# show http monitor

Monitor URL: http://www.abc.com/
Monitor Interval: 100
Acceptable Delay: 100

Monitor URL: http://www.abccorp.com/
Monitor Interval: 60
Acceptable Delay: 60
```