Document Ver 202202-1

サーバアクセスログ
ALog ConVerter®

ALog ConVerter V8
バージョンアップガイド

目 次

はじめに

本書は、Windows およびネットワークシステムの基本的な知識をもつシステム管理者を対象に、ALog ConVerter のバージョンアップ手順を記載した文書です。

●表記について

本書では設定や利用上の注意事項や参考情報などを以下のとおり記載します。

表記	説明
 ヒント	参考情報や推奨事項などを記載します。
 注意	利用上または設定上の注意事項を記載します。

第 1 章 バージョンアップの概要

1. V7 から V8 へのバージョンアップについて

ALog ConVerter V7 から V8 へのバージョンアップ手順は、ユーザーガイドの「5. ALog を管理する」-「5.22. ALog のバージョンアップ」と同様の手順です。手順自体は V7 のマイナーバージョンアップ時の手順と変更はありませんが、本文書を一読していただいた後でバージョンアップを実施してください。

ライセンスキーは、V7 ご利用時に適用したライセンスキーを継続して使用することができます。

バージョンアップにおける仕様変更点は別紙をご確認ください。

 注意	バージョンアップ後、ALog サービスの初回起動時に、V7 の各種設定を V8 に移行するための処理が自動で開始されます。移行処理にかかる時間は、検索用 DB に保存されたデータ量に依存します。移行処理が完了し、サービスが起動するまでは、サービスの再起動や停止をしないようにしてください。移行処理が長時間に及ぶ場合は、状況を確認いたしますので、サポートにお問い合わせください。

2. Web コンソールについて

V8 へのバージョンアップ後、Web コンソールは V7 までと同様の URL でログインが可能です。ログインアカウント等も変更の必要はありません。画面デザインには変更がありますが、基本的な操作性には変更はありません。

3. 各種出力データについて

V8 へのバージョンアップに伴うファイル出力関連の仕様変更はありません。

データの種類	バージョンアップ後の状態について
アクセスログ/イベントログバックアップの CSV データ	V7 の Web コンソールにおいて「出力設定」で設定した内容がそのまま引き継がれ、同じ出力先に出力されます。
レポートのファイル出力	V7 のレポート設定がそのまま引き継がれ、同じ出力先に出力されます。

4. V7 時にオプションをご利用のお客様へ

V7 ご利用時に特別なオプションをご利用のお客様は、ご利用のオプション内容と共に ALog シリーズ サポートセンターまでお問合せください。

第 2 章 バージョンアップ手順について

1. 製品ごとのバージョンアップ手順

ご利用の対象サーバ製品ごとに手順が異なります。該当の製品の記述を確認してください。

1. for Windows

Windows の対象サーバが登録されている環境の場合、以下の手順でバージョンアップを行ないます。

	手順	変更の要不要	補足説明
1	ALog のバージョンアップ	必要	最初に ALog のバージョンアップを行ないます。
2	AD 連携対応	必要	AD 連携を行ないます。 「ユーザーガイド」の「3.ALog を使い始める」-「3.1.ALog の構築」-「3.1.3. AD 連携設定」を参照し、以下の手順を実施してください。 ①「AD 連携」画面でドメイン登録 ②「AD 情報取得タスク」の初回実行
3	対象サーバの再登録	不要	ALog のバージョンアップ後、特に再登録は必要ありません。
4	監査ポリシーの設定変更	不要	必要とする監査ポリシー内容に変更はありません。
5	フォルダーの監査設定	不要	必要とするフォルダーの監査設定内容に変更はありません。
6	エージェント方式の場合 エージェントアップデート	必要	エージェントのアップデートを行ないます。 Web コンソール「管理」-「対象サーバ」画面からアップデートを実施してください。
7	動作確認	必要	ログ収集とログ変換を行ない、問題なくタスク実行ができるか等を確認します。

※変換エンジンの刷新による出力内容の変更を回避したい場合は旧変換エンジンをご利用いただけます。但し、今後のメンテナンスは新変換エンジンに対するものとなり、旧変換エンジンは将来的には廃止される予定です。

注意	初期設定の除外フィルターを外す設定が変更されています。本設定をご利用のお客様はお問合せください。

●TSV によるログ収集をしている場合の注意事項

V8 で変換エンジンを刷新した影響で、TSV 形式のログ変換タスクの処理時間が 1.5 倍～2 倍程度に増加しています。そのため TSV によるログ収集を利用している環境では V8 へのバージョンアップは慎重に行なってください。

処理時間がどの程度増加するかは、出力されるイベントログの内容により変動します。増加を見込んだ上で、マネージャーサーバ 1 台で処理できるかどうかを検討いただき、できない場合はマネージャーサーバの増設や、監査設定の見直しによるログ量の削減を行なってください。

2. for NetApp

NetApp の対象サーバが登録されている環境の場合、以下の手順でバージョンアップを行ないます。

	設定	変更の要不要	補足説明
1	ALog のバージョンアップ	必要	最初に ALog のバージョンアップを行ないます。
2	AD 連携対応	不要	NetApp のログ収集/変換と AD 連携機能(AD 情報取得タスク)は関連性がありませんので、設定の必要はありません。
3	対象サーバの再登録	不要	ALog のバージョンアップ後、再登録の必要はありません。
4	監査ポリシーの設定変更	不要	必要とする監査ポリシー内容に変更はありません。
5	フォルダーの監査設定	「アクセス権変更ログ」を取得する場合必要	「CIFS アクセスログ」のみ取得している環境では変更は不要です。 「アクセス権変更ログ」を含むログを取得する場合、V7 までは「フルコントロール」のフォルダーの監査設定を必要としていましたが、V8 ではより少ない監査設定で「アクセス権変更ログ」を取得可能です。 「ユーザーガイド」-「3.3. 監査設定を手動で行う(製品別)」-「3.3.2. NetApp(ONTAP)の場合」-「3.3.2.3. フォルダーの監査オプションの設定」を参照してください。
6	動作確認	必要	ログ収集とログ変換を行ない、問題なくタスク実行ができるか等を確認します。

※変換エンジンの刷新による出力内容の変更を回避したい場合は旧変換エンジンをご利用いただけます。但し、今後のメンテナンスは新変換エンジンに対するものとなり、旧変換エンジンは将来的には廃止される予定です。

注意	初期設定の除外フィルターを外す設定をされているお客様は、解除する手順が変更になっておりますので、お問合せください。
注意	フォルダーの監査設定を今まで通りフルコントロールのままにした場合、V8 では必要とする EventID が増加しているため、ログ変換タスクの実行時間が増大します。

3. for EMC

EMC の対象サーバが登録されている環境の場合、以下の手順でバージョンアップを行ないます。

	設定	変更の要不要	補足説明
1	ALog のバージョンアップ	必要	最初に ALog のバージョンアップを行ないます。
2	AD 連携対応	不要	EMC のログ収集/変換と AD 連携機能(AD 情報取得タスク)は関連性がありませんので、設定の必要はありません。
3	対象サーバの再登録	不要	ALog のバージョンアップ後、再登録の必要はありません。
4	監査ポリシーの設定変更	不要	必要とする監査ポリシー内容に変更はありません。
5	フォルダーの監査設定	不要	必要とするフォルダーの監査設定内容に変更はありません。
6	動作確認	必要	ログ収集とログ変換を行ない、問題なくタスク実行ができるか等を確認します。

4. for PowerScale（for Isilon）

PowerScale(Isilon)の対象サーバが登録されている環境の場合、以下の手順でバージョンアップを行ないます。

	設定	変更の要不要	補足説明
1	ALog のバージョンアップ	必要	最初に ALog のバージョンアップを行ないます。
2	AD 連携対応	必要	PowerScale では V7 でも AD 連携をしていましたが、設定箇所が変更されています。ALog のバージョンアップ時に自動で移行していますが、念のため設定が移行されていることを確認してください。 「ユーザーガイド」の「3.ALog を使い始める」-「3.1.ALog の構築」-「3.1.3. AD 連携設定」を参照し、以下の手順を実施してください。 ①「AD 連携」画面で既存のドメイン設定の移行が行なわれているかの確認、接続テスト ②「AD 情報取得タスク」の初回実行
3	対象サーバの再登録	不要	ALog のバージョンアップ後、再登録の必要はありません。
4	監査設定の変更	必要	V8 では変換エンジンの刷新により close イベントが不要になりました。そのため close イベントを出力しないよう監査設定を変更します。 「ユーザーガイド」の「ALog を使い始める」-「3.3. 監査設定を手動で行う（製品別）」-「3.3.5. PowerScale の場合」を参照し、「成功と失敗に関する監査設定」を変更してください。
5	動作確認	必要	ログ収集とログ変換を行ない、問題なくタスク実行ができるか等を確認します。

※AD 連携について：V7 時に PowerScale(Isilon)経由で SID 情報を取得していた場合、その設定は引き続き「PowerScale の対象サーバ編集画面」に保存されています。バージョンアップ後には念のためご確認ください。
※監査設定を変更することによりログ変換タスクのパフォーマンスが維持されます。不要なイベント(close イベント)が出力されている状態では、その分ログの解析に時間がかかります。監査設定の変更を推奨します。

 注意	V7 ではコンピューターアカウントのログを変換対象としていましたが、V8 では初期状態で出力しないように変更されています。引き続きコンピューターアカウントのログをアクセスログに出力したい場合、オプションの設定を行なう必要がありますのでお問合せください。

5. for SQL Server

ALog V8 の SQL Server では新しい監査方式が追加されています。詳しい説明は別紙を参照して下さい。
V7「SQL トレース(SQL Server Profiler)」
V8「SQL Server 監査」(RAWSQL 以外)と「拡張イベント」(RAWSQL)
V7 からバージョンアップした場合、V7 時点で追加された対象サーバは引き続き「SQL トレース」で動作します。新しい監査方式に変更したい場合、以下の手順で実施してください。

【監査方式の切り替え手順】
※監査方式の変更のために対象サーバの再登録が必要になりますが、単純に削除後に追加すると監査できない時間が発生します。
以下の手順は、監査している時間の重複は発生しますが、空白時間は発生しません。空白時間の発生が許容できる場合は、対象サーバを単純に削除して新たに登録する方法でも問題ありません。ただし、以下の手順にある「トレースファイルの削除」は必ず行ってください。

◆エージェントレス方式

	設定	変更の要不要	補足説明
1	ALog のバージョンアップ	必要	最初に ALog のバージョンアップを行ないます。
2	AD 連携対応	不要	SQL Server のログ収集/変換と AD 連携機能(AD 情報取得タスク)は関連性がありませんので、設定の必要はありません。
3	既存の対象サーバ(A とする)の名前を変更	必要	このあとの手順において同一サーバを対象サーバとして二重登録します。同一サーバ名登録禁止のエラーを回避するため、既存の対象サーバ名を一度変更します。 Web コンソール「管理」-「対象サーバ」-編集画面-「サーバ名の設定」にて、「接続サーバ名」を IP アドレス等に変更してください。
4	対象サーバを新規で追加(B とする)	必要	既存の対象サーバと同じサーバを新たに対象サーバ追加します。対象サーバ追加ウィザードの監査方式の選択画面にて、新監査方式である「SQL Server 監査」を選択して追加します。
5	B の対象サーバの動作確認	必要	B の対象サーバのログ収集とログ変換を行ない、問題なくタスク実行ができるか等を確認します。
6	A のサーバでログ収集/変換を実行	必要	A の対象サーバで旧監査方式の最後のログを収集し、変換します。
7	A の対象サーバを削除	必要	旧監査方式の対象サーバを削除します。 Web コンソール「管理」-「対象サーバ」から削除します。誤って新しい対象サーバを削除しないよう注意してください。
8	トレースファイルの削除	必要	旧監査方式によって作成されたトレースファイルを削除します。 対象サーバ追加時に指定したトレースログ出力先フォルダー内の拡張子が「.trc」であるファイルを削除してください。

◆エージェント方式

	設定	変更の要不要	補足説明
1	ALog のバージョンアップ	必要	最初に ALog のバージョンアップを行ないます。
2	AD 連携対応	不要	SQL Server のログ収集/変換と AD 連携機能(AD 情報取得タスク)は関連性がありませんので、設定の必要はありません。
3	既存の対象サーバ(A とする)の名前を変更	必要	このあとの手順において同一サーバを対象サーバとして二重登録します。同一サーバ名登録禁止のエラーを回避するため、既存の対象サーバ名を一度変更します。 Web コンソール「管理」-「対象サーバ」-編集画面-「サーバ名の設定」にて、「接続サーバ名」を IP アドレス等に変更してください。
4	A の対象サーバのエージェントアップデート実施	必要	エージェントは V7 の状態になっていますのでアップデートをします。 Web コンソール「管理」-「対象サーバ」からアップデートを実施してください。
5	対象サーバを新規で追加(B とする)	必要	既存の対象サーバと同じサーバを新たに対象サーバ追加します。対象サーバ追加ウィザードの監査方式の選択画面にて、新監査方式である「SQL Server 監査」を選択して追加します。 エージェント方式のためエージェント内に同一サーバの設定が 2 つ存在する状態になります。
6	B の対象サーバの動作確認	必要	B の対象サーバのログ収集とログ変換を行ない、問題なくタスク実行ができるか等を確認します。

7	A のサーバでログ収集/変換を実行	必要	A の対象サーバで旧監査方式の最後のログを収集し、変換します。
8	A の対象サーバを削除	必要	旧監査方式の対象サーバを削除します。これによりエージェント内のサーバ設定が 1 つになります。 Web コンソール「管理」-「対象サーバ」から削除します。誤って新しい対象サーバを削除しないよう注意してください。
9	トレースファイルの削除	必要	旧監査方式によって作成されたトレースファイルを削除します。 【エージェントインストールフォルダー】¥app_data¥work¥rawLog¥【対象サーバ ID】フォルダー内の拡張子が「.trc」であるファイルを削除してください。

※新監査方式の場合、SQL Server 2012～2016 には制限(アプリケーション名なし)が発生します。SQL Server 2017 へアップデートしてから新監査方式にすることを推奨します。
※新監査方式にて対象サーバの再登録の完了後、マネージャーサーバに構築した作業用 DB（SQL Server）は削除可能です。以後のログ変換タスクでは使用しません。

6. for Oracle

ALog V8.3.0 以降では、Oracle21c 以降で搭載された統合監査に対応しています。(統合監査はエージェントレスのみです)
V7 からバージョンアップした場合、V7 時点で追加された対象サーバは引き続き「標準監査」で動作します。

◆監査方式は「標準監査」のまま、ALog をバージョンアップする手順

	設定	変更の要不要	補足説明
1	ALog のバージョンアップ	必要	最初に ALog のバージョンアップを行ないます。
2	AD 連携対応	不要	Oracle のログ収集/変換と AD 連携機能(AD 情報取得タスク)は関連性がありませんので、設定の必要はありません。
3	対象サーバの再登録	不要	ALog のバージョンアップ後、再登録の必要はありません。
4	監査設定の変更	不要	必要とする監査内容に変更はありません。
5	エージェント方式の場合 エージェントアップデート	必要	エージェントのアップデートを行ないます。 Web コンソール「管理」-「対象サーバ」画面からアップデートを実施してください。
6	動作確認	必要	ログ収集とログ変換を行ない、問題なくタスク実行ができるか等を確認します。

※V8 で不使用となったマネージャーサーバ内の Oracle Client の削除は、ALog のバージョンアップ後であればいつでも可能です。

◆監査方式を「標準監査」から「統合監査」に切り替えつつ ALog をバージョンアップする手順

※監査方式の変更のために対象サーバの再登録が必要になりますが、単純に削除後に追加すると監査できない時間が発生します。
以下の手順は、監査している時間の重複は発生しますが、空白時間は発生しません。空白時間の発生が許容できる場合は、対象サーバを単純に削除して新たに登録する方法でも問題ありません。

	設定	変更の要不要	補足説明
1	ALog のバージョンアップ	必要	最初に ALog のバージョンアップを行ないます。
2	AD 連携対応	不要	Oracle のログ収集/変換と AD 連携機能(AD 情報取得タスク)は関連性がありませんので、設定の必要はありません。
3	既存の対象サーバ(A とする)の名前を変更	必要	このあとの手順において同一サーバを対象サーバとして二重登録します。同一サーバ名登録禁止のエラーを回避するため、既存の対象サーバ名を一度変更します。 Web コンソール「管理」-「対象サーバ」-編集画面-「サーバ名の設定」にて、「接続サーバ名」を IP アドレス等に変更してください。
4	対象サーバを新規で追加(B とする)	必要	既存の対象サーバと同じサーバを新たに対象サーバ追加します。対象サーバ追加ウィザードの監査方式の選択画面にて、新監査方式である「統合監査」を選択して追加します。
5	B の対象サーバの動作確認	必要	B の対象サーバのログ収集とログ変換を行ない、問題なくタスク実行ができるか等を確認します。
6	A のサーバでログ収集/変換を実行	必要	A の対象サーバで旧監査方式の最後のログを収集し、変換します。
7	A の対象サーバを削除	必要	旧監査方式の対象サーバを削除します。 Web コンソール「管理」-「対象サーバ」から削除します。誤って新しい対象サーバを削除しないよう注意してください。 このあとトレースファイルは統合監査では使用しません。不要であれば削除してください。
8	初期化パラメータ audit_trail の変更	必要	ALog で使用する Oracle アカウントもしくは sys ユーザーで以下のクエリを実行してください。 alter system set audit_trail=db scope=spfile;
9	Oracle インスタンスの再起動	必要	初期パラメータ audit_trail の変更を有効にするため、Oracle インスタンスの再起動をしてください。

7. for Linux

Linux の対象サーバが登録されている環境の場合、以下の手順でバージョンアップを行ないます。

	設定	変更の要不要	補足説明
1	ALog のバージョンアップ	必要	最初に ALog のバージョンアップを行ないます。
2	AD 連携対応	不要	Linux のログ収集/変換と AD 連携機能(AD 情報取得タスク)は関連性がありませんので、設定の必要はありません。
3	対象サーバの再登録	不要	ALog のバージョンアップ後、再登録の必要はありません。
4	監査設定の変更	不要	必要とする監査内容に変更はありません。
5	動作確認	必要	ログ収集とログ変換を行ない、問題なくタスク実行ができるか等を確認します。

8. ALog EVA

ALog EVA の対象サーバが登録されている環境の場合、以下の手順でバージョンアップを行ないます。

	設定	変更の要不要	補足説明
1	ALog のバージョンアップ	必要	最初に ALog のバージョンアップを行ないます。
2	AD 連携対応	不要	ALog EVA のログ収集/変換と AD 連携機能(AD 情報取得タスク)は関連性がありませんので、設定の必要はありません。
3	対象サーバの再登録	不要	ALog のバージョンアップ後、再登録の必要はありません。
4	監査設定の変更	不要	必要とする監査内容に変更はありません。
5	動作確認	必要	ログ収集とログ変換を行ない、問題なくタスク実行ができるか等を確認します。

2. 共通機能に関する設定変更について

V8 における仕様変更の影響で、すでに保存されている検索条件やレポート設定の変更が必要となるケースがあります。以下の条件に該当する場合、それぞれの設定変更を行なってください。

（補足）

検索条件の保存は上書き保存が可能です。一度保存した検索条件を呼び出し、設定を変更後に再度「検索条件保存」ボタンを押すと、同名のまま上書き保存されます。

●[製品共通]「除外」の検索方法の変更する

☑検索 ☑レポート

V7 で「除外検索」を行ないたい場合には先頭に「-」をつけていましたが、V7.4.0 以降において、検索/レポート画面共に明示的な[除外する]欄の設置を行ないました。これにより、現状は 2 つの除外指定方法が存在しています。しかし、二つの指定方法が残存すると今後の機能拡張性を損なうため、先頭に「-」をつけての除外検索は今後のバージョンで廃止する予定です。V8 からは[除外する]欄を使用してください。すでに設定が保存されている場合、設定変更を行なってください。

●[Windows/NetApp/PowerScale] レポート設定に COPY と MOVE の選択を追加する

☐検索 ☑レポート

ファイルアクセスの操作種別に「COPY」と「MOVE」が追加されました。既存のファイルアクセス関連のレポート設定に対し、必要に応じて「COPY」「MOVE」の選択を追加して保存してください。

●[Windows] ユーザー欄の出力仕様変更に合わせて、検索条件を変更する

☑検索 ☑レポート

AD 連携機能が加わったことにより、ログオンログを取得する環境では「ユーザー」欄の出力が変更になる可能性があります。影響を受けるのはユーザー名のドメイン部分です。ドメイン環境が『ドメイン名と NetBIOS 名が全く違う名前』のようなケースで出力結果が変わります。V8 でのログオンログの出力結果を確認していただき、検索条件を変更してください。

例：ドメイン名「ABC.co.jp」 、NetBIOS 名「DEF」の環境の場合

●[NetApp] 対象欄の出力仕様変更に合わせて、検索条件を変更する

☑検索 ☑レポート

ONTAP 用出力形式オプション「PrefixType」の廃止に伴い、「DSIDPrefix」「NonePrefix」を設定している環境では、「対象」欄の出力が変更になります。V7 と V8 において「対象欄」の先頭のボリューム名の出力を確認していただき、検索条件を変更してください。

●[PowerScale] ユーザー欄の出力仕様変更に合わせて、検索条件を変更する

☑検索 ☑レポート

「ユーザー」欄の出力について V7 では 2 種類の出力ケースが存在していました。

①UserPrincipalName を利用したユーザー名（順番変更あり） 例：ABC.co.jp¥ユーザー名

②NetBIOS ドメイン名＋SamAccountName のユーザー名 例：ABC¥ユーザー名

V8 では②に統一されたため、①で出力されるケースは存在しません。現在「ユーザー」欄が①の形式で出力されている環境では、V8 バージョンアップ後に変更が生じます。V7 時点の「ユーザー」欄の出力結果を確認の上、①のケースで出力されている場合、検索やレポート設定の変更をしてください。

※①の状況に当てはまる可能性があるのは、主に V7.1.3 以前から ALog をご利用いただいているお客様です。

●[SQL Server] 2012～2016 環境：アプリケーション名で検索している場合

☑検索 ☑レポート

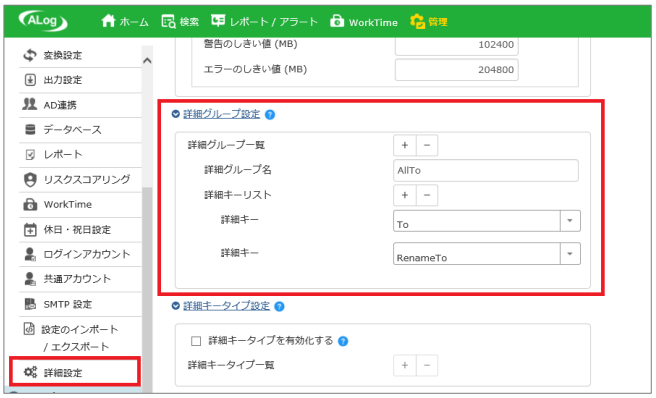
SQL Server の「SQL Server 監査」方式の場合、2012～2016 ではアプリケーション名が出力されていませんので検索やレポート作成をアプリケーション名(AppName)で行なうことは出来ません。SQL Server 2017 以降へバージョンアップすると可能になります。引き続き SQL Server 2012～2016 を利用される場合は、保存した検索条件の削除や、レポート設定を無効にするなどの対応を行なってください。

●[NetApp/Linux]「RenameTo」→「To」への変更に伴う設定変更について

☑検索 ☑レポート

V7 時点で「RENAME」のアクセスログが発生していた場合、詳細項目に「RenameTo」が出力されています。V8 では「RenameTo」を「To」と出力するよう仕様変更したため、V7 で変換したアクセスログの「RenameTo」欄を「To」のフィルターで検索することは出来ず、逆も同様です。どちらの詳細項目も横串で検索したい場合は、Web コンソール「管理」-「詳細設定」-「詳細グループ設定」において、グループを作成し、その中に「RenameTo」と「To」を設定してください。

【詳細グループの設定例とレポート画面での使用例】



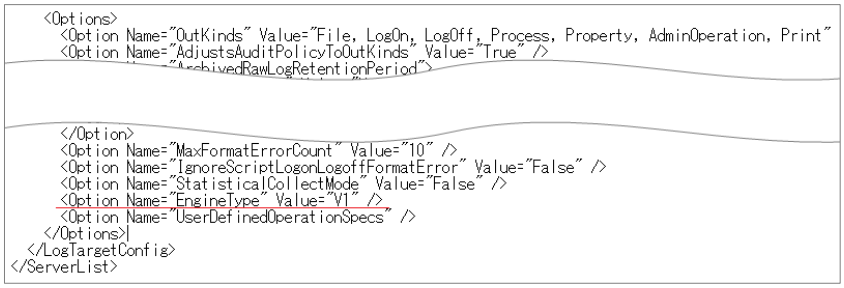
第 3 章　旧変換エンジンを使用する場合について

V8 で新変換エンジンを搭載した製品のうち、Windows と NetApp では旧変換エンジンを使用するためのスイッチを用意しています。すぐにはアクセスログ出力の変更が許容されない環境向けに作成しておりますので、基本的には新変換エンジンをご使用していただくことを推奨しています。今後の新 OS 対応も新変換エンジンに対して行われますので、旧変換エンジンをご使用になる場合も、将来的には新変換エンジンへの切り替えをご検討ください。

1.旧変換エンジンを使用する方法

手順は Windows/NetApp 共通です。

1) バージョンアップ前に Web コンソールで全タスクを「無効」にしておく
2) V8 へバージョンアップを行なう(方法はユーザーガイド参照)
3) マネージャーサーバで ALog の設定ファイルをエディタで開く
<アプリケーションデータ用フォルダー>¥config¥ace_config.xml
4) ServerList/LogTargetConfig に編集したい対象サーバがあることを確認する
5) <Options>配下の「EngineType」の設定を書き換える
<Option Name="EngineType" Value="V1" />
※「V1＝旧変換エンジン」、「V2＝新変換エンジン」 を指します。
※変更したい対象サーバの数分書き換える必要があります。
※バージョンアップ前から登録されている対象サーバの場合、バージョンアップ直後は EngineType の設定がありません。
下記のいずれかの方法で追加してください。
・1 行を新規で書き加える
・一度対象サーバ編集画面を開いて「OK」ボタンを押すと、「<Option Name="EngineType" Value="Undefined" />」
（Value が「Undefined」の状態）が書き加えられるため、Value を「V1」に変更する
(Windows の例)



6) 書き換え後、変更を保存して XML を閉じる
7) Web コンソールで全タスクを「有効」に戻す
8) エンジンを変更した対象サーバのログ収集タスクを手動実行し、正常終了するかを確認
9) ログ変換タスクを手動実行し、正常終了するかを確認

※Windows-エージェント方式の場合
エージェントモジュールを V8 にアップデートした上で、対象サーバ側の「aae_config.xml」にて同様の編集を行なってください。その上で、Web コンソールの「管理」-「対象サーバ」にて、該当の対象サーバの編集画面を開いて「OK」をクリックすると、「ace_config.xml」に反映されます。

※今後追加する対象サーバも旧変換エンジンで動作させたい場合、以下のデフォルト値のセット部分における EngineType も「V1」に書き換えてください。
<DefaultWindowsLogTargetConfig>～</DefaultWindowsLogTargetConfig>
<DefaultNetAppLogTargetConfig>～</DefaultNetAppLogTargetConfig>

付録

付録 1. ALog ConVerter V7 に対する V8 のログ処理性能比較

製品		管理サーバ 1 台あたりのログ処理量の上限（GB/日）		V7 に対する V8 の性能比率	備考
		ALog v8	ALog v7		
for Windows	エージェントレス方式（EVTX 形式）	1834	1474	124%	
	エージェント方式（TSV 形式）	3245	2860	113%	
for NetApp	7-mode	273	375	73%	
	ONTAP（EVT 形式）	1825	918	199%	
for EMC	アーカイブ方式	536	765	70%	
for PowerScale	－	1324	1107	120%	
for SQL Server	－	625	257	244%	V7 はトレースログ、V8 は監査ログの結果
for Oracle	WindowsOS ※OS 出力 RAWSQL なし	449	377	119%	
	LinuxOS ※OS 出力 RAWSQL なし	188	175	107%	
for Linux	audit ログ	296	444	67%	
	syslog	46	38	120%	
ALog EVA	Windows イベントログデータ	393	418	94%	
	テキストデータ （CSV、TSV、Syslog 等）	84	98	86%	
	テキストデータ Syslog	59	62	95%	
	テキストデータ Json	208	213	98%	
	プレーンテキスト（旧方式）	83	（対象機能なし）	－	
	プレーンテキスト	10	（対象機能なし）	－	
Amazon FSx for Windows File Server		409	（対象機能なし）	－	
Amazon FSx for NetApp ONTAP		1825	（対象機能なし）	－	for NetApp と翻訳エンジンが同じであるため、ONTAP(EVT 形式)の処理量と同じ

※ 2022 年 02 月時点

【測定環境】

OS	Windows Server 2012R2
CPU	Intel® Xeon® CPU E5-2620 V2 @ 2.40GHz 2.40GHz
Memory	32GB
HDD	4TB （SATA3.0 7200rpm）
ALog ConVerter	V8.4.0（NetApp（7-mode）、EMC、Linux は V8.5.0）
	V7.5.3

注 1）測定環境の機器には 12 コアの CPU を搭載していますが、そのうちの 4 コアのみを使用して測定しています。
注 2）本資料の値は、その 4 コアでイベントログの変換を並列処理した場合の理論値です。
注 3）弊社試験環境で測定した結果であり、システム環境により結果が異なる場合がありますのでご注意ください。
注 4）本資料は ALog ConVerter 製品の性能を保証するものではありませんのでご了承ください。