NetIQ 製品トラブルシューティング

第 1.1 版 2015/04/22

目次

はじめに 3

Legacy NetIQ Products 4

目的 4

NetIQ AppManager Widows Components 5

動作ログ 5

ログの収集 7

サービスのリセット 9

NetIQ AppManager UNIX Components 12

動作ログ 12

ログの収集 15

サービスのリセット 16

NetIQ AppManager Troubleshooting 17

一般的な問題の手がかり 17

有用なユーティリティ 19

問題の事例 24

NetIQ Aegis 33

動作ログ 33

ログの収集 38

サービスのリセット 39

NetIQ DRA 41

動作ログ 41

ログの収集 42

有用なユーティリティ 45

はじめに

NetIQ Legacy 製品問合せ時のログ収集に関する手順をまとめたものです。

Legacy NetIQ Products

目的

旧 NetIQ 製品である Aegis, AppManager, DRA 各製品のお問合せをいただく時に必要となる動作ログの設定、収集方法について説明いたします。動作ログをお問合せに先んじて収集いただくことで、問題への対応がお客様、弊社双方で円滑に進めることができます。

また、各製品につき簡易なサービスのリセット方法についても説明いたします。

NetIQ AppManager Widows Components

動作ログ

Windows エージェントの主な動作ログの出力先設定とその種類についての資料です。

たとえば Windows Server 2012 R2 上に AppManager v8.2 を既定値でインストールされた場合、C:¥Program Files (x86)¥NetIQ¥temp¥NetIQ_Debug¥マシン名 フォルダ以下に動作ログが作成されます。これらは、弊社に問題をお問合せいただく場合に必要なものです。

最大二世代（ 含む現在 ）のログ管理設定の基点

OS 32 bit / 64 bit	レジストリキー
32 bit	[HKEY_LOCAL_MACHINE¥SOFTWARE¥NetIQ¥Generic¥Tracing]
64 bit	[HKEY_LOCAL_MACHINE¥SOFTWARE¥Wow6432¥NetIQ¥Generic¥Tracing]

出力先とファイルあたりのサイズ

レジストリ値	Version	データ
TraceLogPath	共通	C:¥¥インストールパス ¥¥NetIQ¥¥Temp¥¥NetIQ_Debug
TraceLogMaxSize	AM 6.xJ まで	2,097,152 byte
	AM 7.0J 出荷版	3,145,728 bytes
	AM 7.0J Win 2008 対応以降	6,291,456 bytes
	AM 8.2 QDB	7,320,032 bytes

ログ ファイルの識別子

識別子	意味
接頭辞 O	前回起動時の動作ログ
接尾辞 bkup	現在の動作ログがローテーションにより、バックアップされたもの
拡張子 log	動作ログ 例 : mctrace.log, mctrace.log.bkup, Omctrace.lo

種類（ Windows エージェント ）

ファイル名	目的
mctrace.log	NetIQmcサービス内で発生したジョブの受け入れ、生成、コンパイルや実行など、すべてのアクティビティが記録されます。
ccmtrace.log	NetIQccmサービス内のすべてのアクティビティが記録されます。管理サーバとの通信状況、送信データのフロー制御情報を含みます。
mo.log	ジョブ実行時に呼び出される管理オブジェクトのファンクションコールが記録されます。
ioc.log	サービス間の pipe に関するログ
nqioc_err.log	サービス間の pipe でのエラーログ
KS traces¥[JobID]_[SiteID]	%TraceLogPath%¥mc フォルダに KS 実行時のステップ単位での動作ログを記録します。

種類（ リポジトリ データベース サーバ ）

ファイル名	目的
kscheckin.log	KS のチェックインを記録します。
QDBInstall.log	リポジトリのインストールプロセスを記録します。
QDBUpgrade.log	リポジトリのアップグレードプロセスを記録します。

種類（ 管理サーバ ）

ファイル名	目的
ms.log	netiqms サービス内の動作を記録します。
rplib.log	netiqms, AmOC のデータベースへの動作、ODBC エラーを記録します。
msqdb.log	netiqms / QDB 間のエラーを記録します。
msaction.log	MS, Proxy アクションの詳細を記録します。

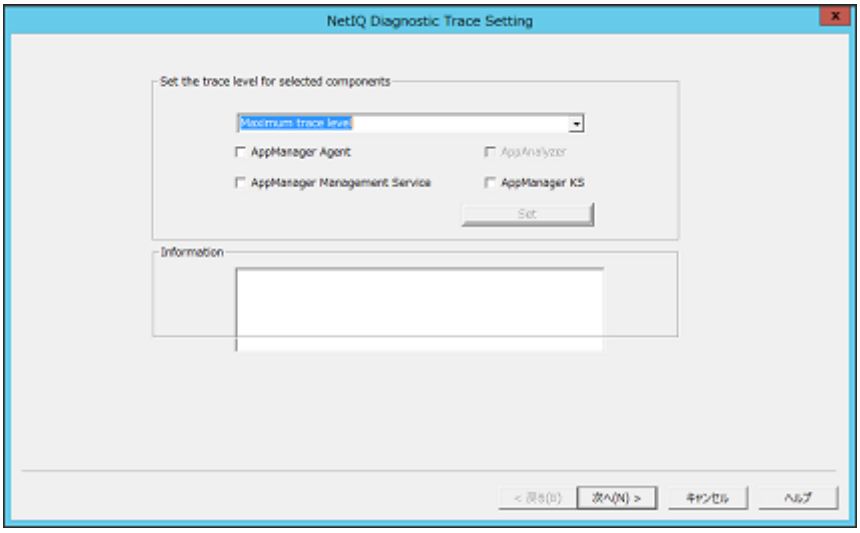
種類（ オペレータ コンソール ）

識別子	意味
rplib.log	netiqms, AmOC のデータベースへの動作、ODBC エラーを記録します。
kscheckin.log	KS のチェックインを記録します。

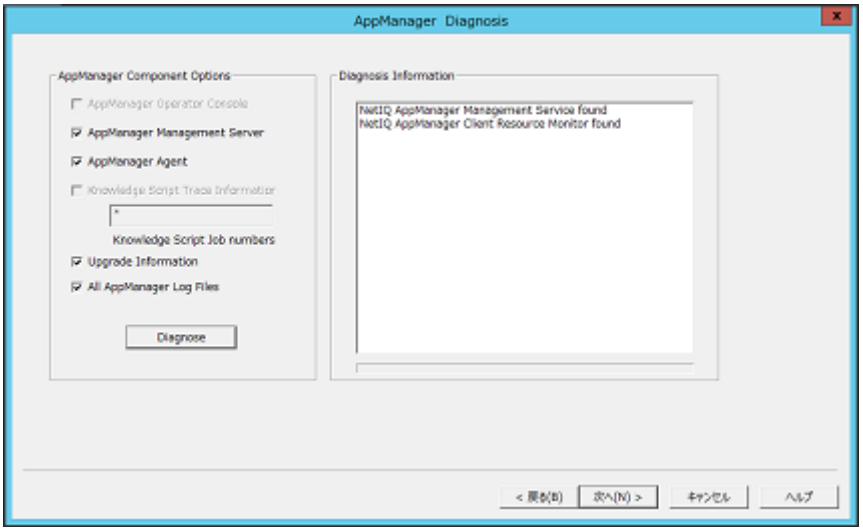
ログの収集

動作ログの収集について説明します。

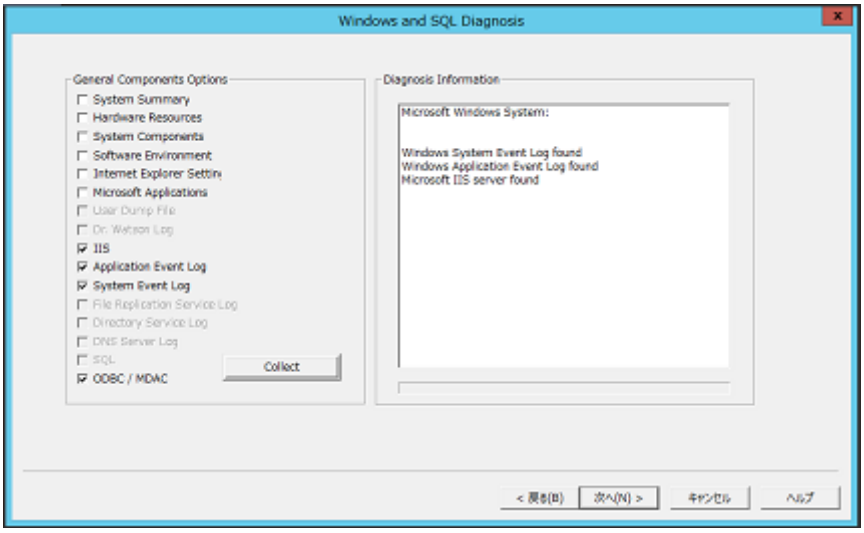
1. 管理者コンソール （[管理者として実行(A)…] で起動されたコマンド プロンプト)から netiqdiag を起動します。［次へ］をクリックします。



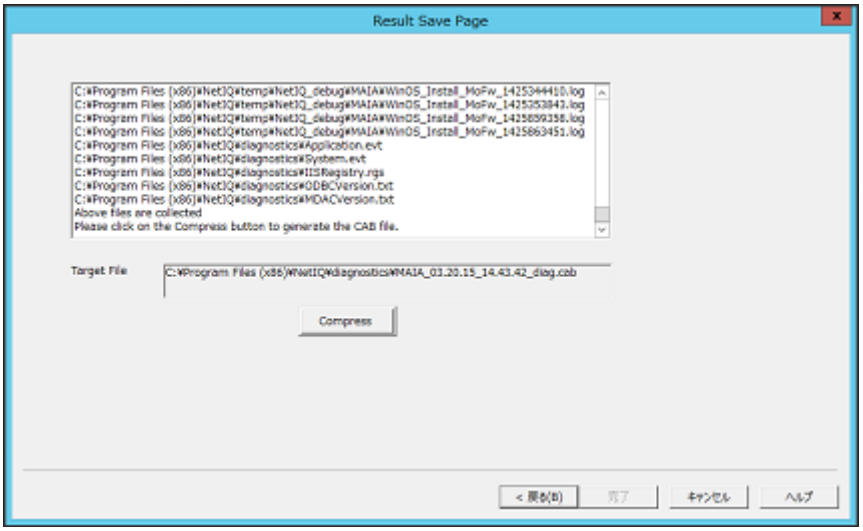
2. [Diagnose] ボタンをクリックします。進行状況に "Everything is done!" が返されたら、[次へ] をクリックします。



3. [Collect] をクリックします。進行状況に "Everything is done!" が返されたら、[次へ] をクリックします。
   なお、お客様のご利用になられている Windows エージェントが AM 7.0J SP1 (mctrace.log などのヘッダ部分に記述されている version が 7.0.10040.1) 以下の場合に OCBD / MDAC のチェックボックスをはずさないとアプリケーションエラーでログの収集ができない場合があります。



4. [Compress] をクリックし、Target File に表示されている書庫ファイルに、取得したログをアーカイブ処理します。"Done!" が返されたら、[完了] をクリックし、Target File を回収します。



サービスのリセット

以下のサービスの内、いずれかが起動できない場合に実施する cold start の手順を説明します。

NetIQ AppManager Client Communication Manager

NetIQ AppManager Client Resource Monitor

作業は管理者コンソール([管理者として実行(A)…] で起動されたコマンド プロンプト)で行います。

1. いずれかのサービスが起動中の場合、これを停止します。

   sc stop netiqmc

   sc stop netiqccm

2. エージェントのインストール パス（例 : C:¥Program Files (x86)¥NetIQ ）を確認し、所定のサブフォルダへ移動、キャッシュの削除。

   cd " C:¥Program Files (x86)¥NetIQ¥AppManager¥dat"

   del *.dat

   cd mapque

   del *.dat

3. mctrace.log や ccmtrace.log に次のエラー

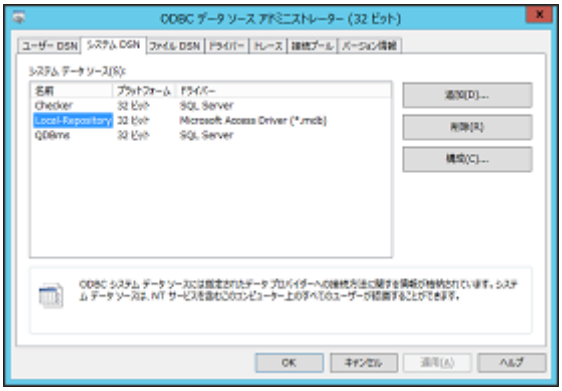
   SQLSTATE=S1001, NativeErr=-1011, msg=<[Microsoft][ODBC Microsoft Access Driver] メモリ不足です。>

   が返される時や NetIQ¥AppManager¥db¥Local-Repository.mdb のサイズが 100 MB を超えているなど大きい時は これを一度修復処理します。

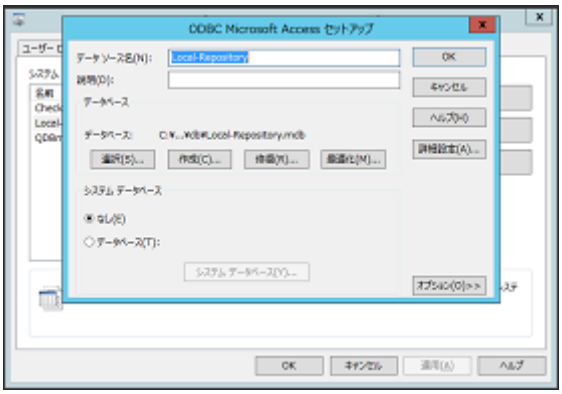
   "C:¥Windows¥Syswow64¥odbcad32.exe" を起動。パスがない場合は、32 bit 機なので、

   "C:¥Windows¥System32¥odbc32.exe" を起動。

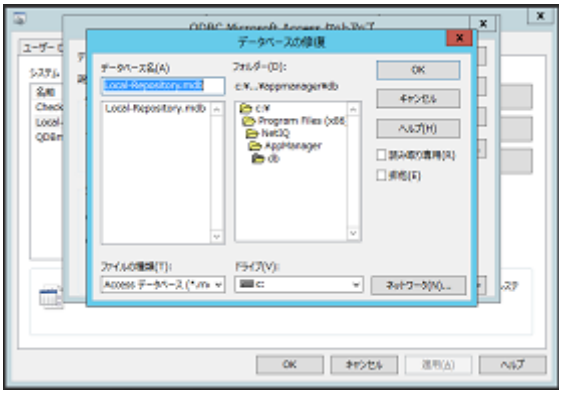
   [システム DSN] から Local-Repository を選択、[構成] をクリック。



4. ［修復］をクリック。



5. ［OK］をクリックし、修復を開始。完了メッセージが返されたら、［OK］を順にクリックし、終了します。



6. ここで、サービスの開始を行います。

```
sc start netiqccm
sc start netiqmc
```

サービスの起動を確認します。

```
sc query netiqccm
sc query netiqmc
```

7. 起動できなかった場合は cold start option の /o を試します。

```
sc start netiqccm /o
sc start netiqmc /o
```

サービスの起動を確認します。

```
sc query netiqccm
sc query netiqmc
```

8. それでもなお起動できなかった場合は cold start option の /oa を試します。

   ```
   sc start netiqccm /oa
   sc start netiqmc /oa
   ```

   サービスの起動を確認します。

   ```
   sc query netiqccm
   sc query netiqmc
   ```

9. Operator Console 上でグレイアウトしたマシンをクリック［コンピュータの接続をチェック］を実施し、F5 キーを押し、画面をリフレッシュします。グレイアウト解消し、cold start により MC can't locate error で停止したジョブがあれば、これを再開します。

   /oa でジョブを開始された場合は、発見処理時に行った AMAdmin_SetPrimaryMS による主、副管理サーバの設定を行ってください。

NetIQ AppManager UNIX Components

動作ログ

UNIX エージェントのログは以下の世代、サイズ、種類があります。

UNIX エージェントの version を確認する方法は /etc/vsaunix.cfg（AM 6.x では存在しません）および nqmdaemon にて環境変数 LD_LIBRARY の設定内容を確認いただき、それを明示し、agent -v を実行いただきますと version が返されます。

例：

```
$ su -
#LD_LIBRARY_PATH=/usr/netiq/AM/lib:/usr/netiq/AM/lib/5.10.0/i686-linux-thread
-multi/CORE:/lib:/usr/lib /usr/netiq/AM/bin/agent -v
```

ログ ファイルの出力先、世代数、サイズ

Version 6.0

ファイル名	変数名	データ
nqmdaemon	NQHOME	/ベース ディレクトリ/netiq
	NQMAGT_HOME	$NQHOME/UnixAgent
$NQMAGT_HOME/conf/nqmcfg.xml	DEBUG_LOG, DIR	log
	LOGS_TO_KEEP	保存する過去ログ世代数
	SIZE	ログ ファイルあたり最大値

Version 6.5 / 7.0

ファイル名	変数名	データ
nqmdaemon	NQHOME	/ベース ディレクトリ/netiq
	NQMAGT_HOME	$NQHOME/UnixAgent
$NQMAGT_HOME/etc/uaconf.xml	LOGGING, BASENAME	NqmAgt
	LOGS_TO_KEEP	保存する過去ログ世代数
	SIZE	ログ ファイルあたり最大値

Version 7.1 / 7.2 / 7.5 / 8.0

ファイル名	変数名	データ
vsaunix.cfg	PSHOME	ベース ディレクトリ
nqmdaemon	NQHOME	$PSHOME/netiq
	NQMAGT_HOME	$NQHOME/AM
$NQMAGT_HOME/etc/uaconf.xml	LOGGING, BASENAME	NqmAgt
	LOGS_TO_KEEP	保存する過去ログ世代数
	SIZE	ログ ファイルあたり最大値

ログ ファイル

世代数は _世代.log とファイル名に付与されます。

Version 6.0

ディレクトリ名	ファイル名	目的
$NQMAGT_HOME/log	nqmlog.err	agent の親プロセス動作ログ
	nqmlog	agent の監視動作ログ
	nqmlog[TimeStamp]	agent の n 世代前動作ログ

Version 6.5 / 7.0 / 7.1

ディレクトリ名	ファイル名	目的
$NQMAGT_HOME/log	nqmlog.err	agent の親プロセス動作ログ
	NqmAgt.log	agent の監視動作ログ
	agent[TimeStamp].err	agent の標準エラー出力

Ver. 7.2 / 7.5 / 8.0

ディレクトリ名	ファイル名	目的
$NQHOME/common/log	nqmagt.log	agent の親プロセス動作ログ
$NQMAGT_HOME/log	NqmAgt.log	agent の監視動作ログ
	agent[TimeStamp].err	agent の標準エラー出力

ログの収集

動作ログの収集について説明します。

1. $NQMAGT_HOME/bin/NetiqDiag シェルスクリプトを root 権限で実行します。
2. スクリプトはログを収集後、次のメッセージを返します。

   Netiq Diagnostics Utility has completed

   フルパス名

   返されたフルパス名にある書庫ファイルを回収します。

サービスのリセット

nqmdaemon start にてデーモンが開始できない場合や管理サーバにデータ、イベントが送信されない場合に cold start の手順を説明します。

cold start は root 権限で実行します。 cold start の前に rm $NQMAGT_HOME/bin/core* にて core dump の削除実施しておきます。

Version 6.0 / 6.5 / 7.0

nqmdaemon stop 後に、nqmdaemon の起動オプションを追記し、起動します。起動後は追記した内容を削除しておきます。

ファイル名	変数名	データ
nqmdaemon	NIQ_AGENT_STARTUP_OPTIONS_ADDITION	-F を追記

Version 7.1

nqmdaemon stop 後に、nqmdaemon の起動オプションを追記し、起動します。起動後は追記した内容を削除しておきます。

ファイル名	変数名	データ
/etc/vsaunix/cfg	NIQ_AGENT_STARTUP_OPTIONS_ADDITION	-F を追記

あるいは

nqmdaemon の再起動引数に cold を指定します。

ファイル名	引数
namdaemon	cold

Ver. 7.2 / 7.5 / 8.0

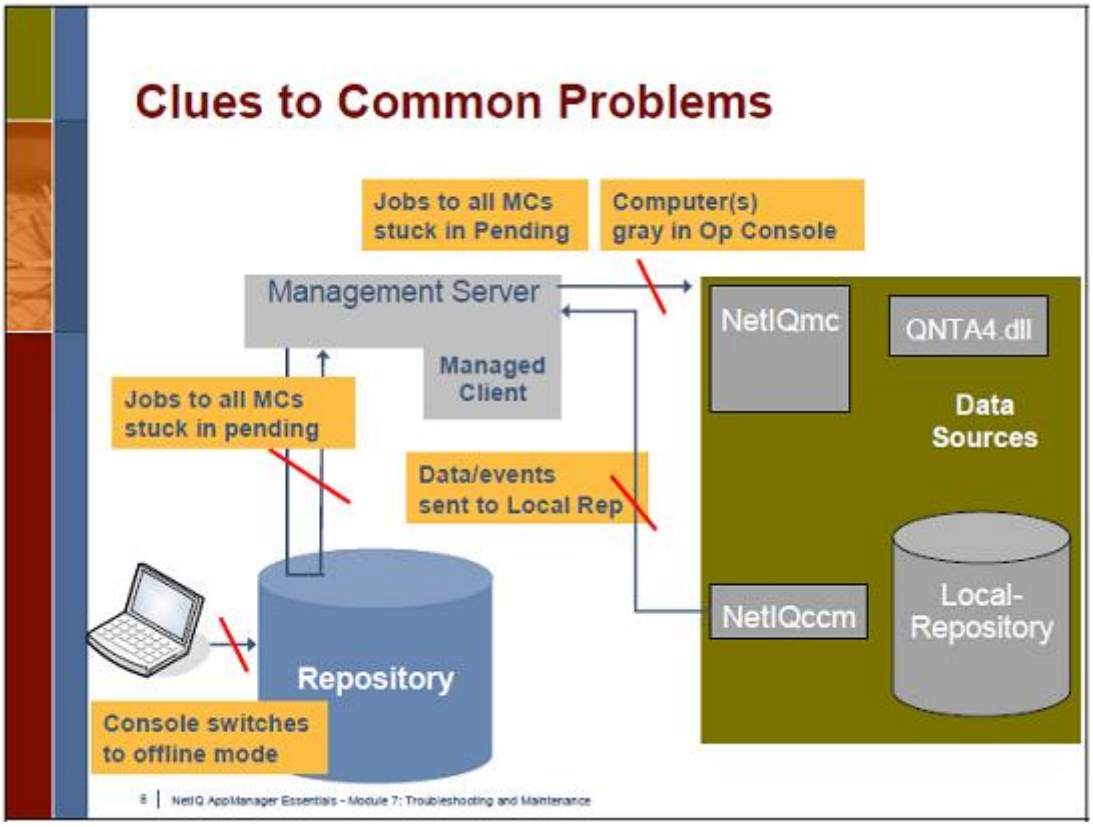
nqmdaemon の再起動引数に frozen を指定します。

ファイル名	引数
namdaemon	frozen

NetIQ AppManager Troubleshooting

一般的な問題の手がかり

どの通信路で問題が発生しているかを切り分けます。



事　象	Operator Console のリポジリデータベースへの接続jが offline になる。
確　認	Console , Repository 間を調べる。

事　象	ジョブが ″準備中(開始)″ や ″準備中(停止)″ でスタックする。
確　認	Repository, Management Server 間を調べる。

事　象	ジョブが ″準備中(開始)″ や ″準備中(停止)″ でスタックする。 マシンが ″グレイ アウト″ 表示になる。
確　認	Management Server, Client Resource Monitor 間を調べる。

事　象	データ、イベントが送信されず、Local-Repository に保存される。
確　認	Client Communication Manager, Management Server 間を調べる。

有用なユーティリティ

どの通信路で問題が発生しているかを切り分けます。

netiqctrl

AM コンポーネントを調べて診断情報を得ます。

サブ コマンド	説明
job	jobは、エージェント上のジョブ情報を表示します。構文は、job <agent> netiqmcです。<agent>の部分には問い合わせ先のエージェント名を指定します。例えば、job netiq00 netiqmcとします。 出力フォーマットは、<jobid>_<siteid> : <info>です。 JobIDは、リポジトリによって割り当てられる子ジョブの識別子です。SiteIDは、QDBを特定するためのサイト識別子でQDBサーバー名とタイムスタンプから構成されています。 ジョブが実行中の場合には、ジョブを実行しているスレッドIDが表示されます。このスレッドIDは、mctrace.logファイルにも記述されているため、特定のジョブの実行履歴を追跡することができます。 Jobコマンドは、ジョブが本当に終了しているのか否かを確認するために役立ちます。例えばジョブがオペレータコンソール上では実行中であるにも関わらず、エージェント上では停止になっている場合には、エージェントが管理サーバーに対してステータスの変更通知が行えない状況になっていると判断できます。
jobsched	JobSchedは、指定したジョブのスケジュールを表示します。このコマンドの実行には、JobIDとそのジョブを送信した管理サーバー名を指定する必要があります。構文は、Jobsched <agent> netiqmc <ms server> <jobid>です。例えば、jobsched netiq00 netiqmc netiq01 51とします。
jobstat	JobStatは、指定したジョブの統計情報を表示します。このコマンドの実行には、JobIDとそのジョブを送信した管理サーバー名を指定する必要があります。構文は、 jobstat <agent> netiqmc <ms server> <jobid>です。 例えば、jobstat netiq00 netiqmc netiq01 51とします。このコマンドは、ジョブによって生成されたイベント、コントロールイベント、データヘッダ、データポイント、ローカルアクションの総数と失敗した数を表示します。この情報は、例えばジョブによってイベントが生成されているはずなのに、オペレータコンソールにイベントが表示されていないような場合に、どの部分に問題があるかを調査するために役立ちます。

サブ コマンド	説明
listms	listmsは、指定したエージェントがやり取りしている管理サーバーのステータスを含めた情報を表示します。エージェントから情報がまったくあがってこないような場合に、このコマンドを使うことでエージェントが認識している管理サーバーのIPアドレスなどを確認することができます。 構文は、listms <agent> netiqmcです。例えば、listms netiq00 netiqmcとします。
listrsc	listrscは、エージェントで実行されているKS分類を表示しAMAdmin_SetResDependency KSを使って定義されている依存するリソースを確認することができます。AMAdmin_SetResDependency KSは、主にクラスタ環境で使用され、サービスやディスクリソースの状態に依存して、指定したKS分類の有効、無効を切り替えます。このコマンドの構文は、listrsc <agent> netiqmcです。 例えば、listrsc netiq00 netiqmcとします。
listupload	listuploadは、エージェントのアップロードスケジュールを表示します。アップロードスケジュールは、AMAdmin_SetSchedUpload KSによって設定されます。構文は、listupload <agent> netiqmc ms <ms server>です。 例えば、listupload netiq00 netiqccm ms netiq01とします。このコマンドは、実際のアップロードスケジュールを確認するのに役立ちます。
machine	machineは、管理サーバーが認識しているエージェントに関する情報を表示します。 例えば、machine netiq01 netiqms netiq00とします。このコマンドを使うことで、エージェントに対して管理サーバーから最後にコンタクトに成功した(失敗した)時刻、送信したジョブ情報、タイムゾーンなどを表示することができます。コマンドの最後にエージェント名を指定すると特定のエージェントの情報を表示し、何も指定しないとすべてのエージェントに関する情報を表示します。
ping	pingコマンドは、指定したコンポーネントにRPC Pingを送信します。ICMP Pingとは異なり、指定したコンポーネントサービスが生きているかを検証します。構文は、ping <agent> <service>です。 例えば、ping netiq00 netiqmcとします。<service>に指定できるのは、netiqmc、netiqccm、netiqmsです。コンポーネントのバージョン、スタートモード、ポート番号(netiqmc, netiqmsの場合)などを表示します。

サブ コマンド	説明
probe	probeは、コマンドを実行したマシンから指定されたコンポーネントに対してprobeパケットを送信し応答を確認します。指定したコンポーネントサービスとのネットワーク接続性を検査します。構文は、 probe <server> <service>です。 例えば、probe netiq00 netiqmsとします。タイムスタンプは、UTCフォーマットで表示されます。各ステージで極端に時間がかかっている場合には、ネットワークに問題があるかも知れません。<service>には、netiqmcもしくはnetiqmsが指定できます。
profile	profileは、エージェントで実行されているKS分類を表示しAMAdmin_SetResDependency KSを使って定義されている依存するリソースを確認することができます。AMAdmin_SetResDependency KSは、主にクラスタ環境で使用され、サービスやディスクリソースの状態に依存して、指定したKS分類の有効、無効を切り替えます。このコマンドの構文は、listrsc <agent> netiqmcです。 例えば、listrsc netiq00 netiqmcとします。
unixjob	unixjob – このコマンドは、Unixエージェント上で実行されているジョブのサマリー情報を表示します。JobIDとステータスを表示します。構文は、UnixJob ms_hostname NetIQms [UNIX_agent_IP]です。
unixmachine	unixmachineは、Unixエージェントの状態を表示します。このコマンドは、エージェントバージョン、プラットフォーム情報、タイムゾーン、実行ジョブ数などの情報を表示します。構文は、UnixMachine ms_hostname NetIQms [UNIX_agent_IP]です。
unixmms	unixmmsは、Unixエージェントに設定されているプライマリおよびセカンダリ管理サーバーを表示します。構文は、UnixMMS ms_hostname NetIQms [UNIX_agent_IP]です。
unixtime	unixtime – このコマンドは、管理サーバーとUnixエージェント間の通信に関する情報を表示します。このコマンドの出力には、管理サーバーが最後に受信したハートビートなどの時刻が表示されます。構文は、UnixTime ms_hostname NetIQms [UNIX_agent_IP]です。

mspioc

管理サーバ（ netiqms.exe ）の PiocData，PiocEvent，PiocJobStat の使用状態を出力します。

構文	説明
mspioc piocファイルへのパス	netiqms が管理クライアントから受信した Data，Event，各job の状態を QDB に書き込む前に置く、バッファとして PiocData，PiocEvent，PiocJobStat ファイルがあります。これを引数に指定すると、< Number of records>,< map file size(header)>，< map file size(used)>，< map file size(not used)>，< map file size(total)>，< map file full>,offset (first record in queue)，offset (next avail addr in queue)および各レコードの大きさをレポートします。

perl

mctrace.log, ccmtrace.log, mo.log などの timestamp を日本標準時間に変換します。

例

```
use 5.010;
use strict;
use warnings;

my $x;
$x = 0;

while (my $line = <>) {
        chomp $line;
        if ($line =~ /^(¥d+) (.*)/) {
                if ($x > $1) {
                        print "WARNING!" . "¥n";
                }
                $x = $1;
                print localtime($1) . " " . $2 . "¥n";
        } else {
                if ($line =~ /^¥*¥*-(¥d+) (.*)/) {
                        print "*-" . localtime($1) . " " . $2 . "¥n";
                } else {
                        print $line . "¥n";
                }
        }
}
```

問題の事例

ジョブ実行に関する事例です。

事　象	KS のコンパイルエラー　CErr<エラー番号>(L<行番号>):説明
原　因	L行番号にて構文エラーが発生
事例 1	MS Action: CErr76(L975):Script is too large to be compiled 発生したイベントのメッセージ サイズが大きく、それを固定文字列として生成されたアクション KSのコンパイルができなかった。
事例 2	MS Action: CErr31(L50):Encountered new-line in string 発生したイベントのメッセージを固定文字列にて分割、継続行で定義したところ、文字列の分割点がマルチバイト文字の上位、下位バイトにあたった。 netiqms.exe (7.0.10040.1) にて修正済み。
事例 3	MS Action: CErr31(L41):Encountered new-line in string 発生したイベントの文字コードが、管理サーバの文字コードと異なるために、文字化けし、取り扱えなかった。

事　象	KS の実行時エラー　RErr<エラー番号>(L<行番号>):説明
原　因	L行番号にて実行時エラーが発生
事例 1	Discovey KS にて RErr2148139013(L356):Application-defined or object-defined error Windows に ADO Stream および文字コード変換テーブルが不足している。
事例 2	MS Action: RErr14(L271):Out of string space アクション実行時に、イベントのメッセージが多く、配列を作成しようとしたところ、スクリプトエンジン内の作業用メモリ不足した。
事例 3	RErr2147944126(L118):OLE Automation error - the remote procedure call failed 該当行にある COM オブジェクトの初期化に失敗した。regsvr32 コマンドにて対応する

	DLL を再登録、サービスの再起動の実施が必要。
事例 4	RErr4133(L行番号):ReadEvent failed on <(関数名)>, last code: エラーコード システムシャットダウン時に KS build 6.x 以前の EventLog 監視ジョブが動作すると発生。

事　象	サービス、ジョブは動作し、リスニング状態だが、データ、イベントが発生しない。
原　因	netiqmc / netiqccm 間の pipe 初期化エラー
事例 1	-- mctrace.log Wed Apr 1 01:19:37 2015 [452] pipe-pDoCmdComm: writing to pipe Wed Apr 1 01:19:37 2015 [452] pipe-pDoCmdComm: reading from pipe Wed Apr 1 01:19:37 2015 [452] pipe-pDoCmdComm: cmd=33 ms= ret=1 Wed Apr 1 01:19:37 2015 [452] pipe-pPingPipeSrv: ping return 1 -- ccmtrace.log Wed Apr 1 01:19:37 2015 [2668] myDispatch: Receiving a cmd <CtrlPing> via pipe .... Wed Apr 1 01:19:37 2015 [2668] cmsite-=: invalid site, name=<> time=0 Wed Apr 1 01:19:37 2015 [2668] pipe-ctrlMain: operation <CtrlPing> complete with rc 1 Wed Apr 1 01:19:37 2015 [2668] pipe-pwrite: writing 136 bytes to pipe x1d4 Wed Apr 1 01:19:37 2015 [2668] pipe-pwrite: before GetOverlappedResult AM704_MC_PF_ENG335072 (7.0.41079.10) にて修正済み。

データベースのサイズ肥大に関する事例です。

事　象	Operator Console の［イベント］ウィンドウが空白
原　因	イベントの過多

事　象	データベースのディスクが不足
原　因	データ、イベントの過多

回避策	**データベースサイズ縮小の手順**
	1. **[オペレータコンソール]-[ファイル(F)]-[ユーザ設定(F)]-[リポジトリ]-[データ]**
	[データテーブルに保存するデフォルト日数]
	各グラフデータの保存最大日数を変更する場合、異なるグラフでの最大値
	[アーカイブポイントを集積テーブルに移動する(C)]
	[何ヶ月後に移動(M)]
	ReportAM 各 KS でレポートを作成するのに必要な最大月数に変更。
	
	2. **[オペレータコンソール]-[ファイル(F)]-[ユーザ設定(F)]-[リポジトリ]-[イベント]**
	[リポジトリのアーカイブテーブルに古いイベントを移動する時期]
	設定変更後のイベントが対象。
	[クローズステータスを保持する日数／時間] n **日**
	[古いイベントがこのイベント数を超える:] 1000 イベント
	
	3. Microsoft SQL Server Management Studio から T-SQL 文で集積表の設定値変更
	`update [QDB].[dbo].[GlobalPref] set val = 1 where name like 'ArcAvgHourlyMonthsKept'`
	`update [QDB].[dbo].[GlobalPref] set val = 1 where name like 'ArcAvgDailyMonthsKept'`
	
	4. グラフデータの最大日数一括更新
	`update [QDB].[dbo].[DataHeader] set LogLimit = ( select val from [QDB].[dbo].[GlobalPref] where name like 'DefaultDataLogLimit' )`
	`update [QDB].[dbo].[ArchiveDataHeader] set LogLimit = ( select val from [QDB].[dbo].[GlobalPref] where name like 'DefaultDataLogLimit' )`
	
	5. n 日以前のイベントに削除フラグを設定。(必要なストアド プロシージャは *1)

	6. SQL Server エージェント サービスのジョブの実行 **NetIQ PurgeData QDB** 毎日6 時間ごとに 10000 行単位で削除。 件数が多い場合、**数時間以上かかる**こともある。 7. SQL Server エージェント サービスのジョブの実行 **NetIQ Purge Archive Event** 午前 2:00 に不要になったイベントを移動、削除。 8. **[Microsoft SQL Server Management Studio]-[オブジェクト エクスプローラ]-[SQL サーバ名]-[データベース]-[QDB]-[タスク]-[圧縮]-[データベース]** で縮小。

***1 n 日以前のイベントを削除指定するストアド プロシージャ**

```
use QDB
go
if exists (select * from sysobjects where id = object_id('dbo.mark_delete_events') and
sysstat & 0xf = 4)
        drop procedure dbo.mark_delete_events
go

create procedure dbo.mark_delete_events
@Ndays as int,
@EventID as int = 2147483647
as
declare @event_id int
declare @status int
declare @actualstatus int
declare @t int
declare @rows int

if @Ndays is NULL
select @Ndays = 10

exec master.dbo.xp_regread 'HKEY_LOCAL_MACHINE',
'SYSTEM¥CurrentControlSet¥Control¥TimeZoneInformation', 'ActiveTimeBias', @param = @t
OUT
-- Bias 値は分なので秒に変換します
select @t = @t * 60
```

```
SELECT EventID, Status INTO #tmptab4Children FROM Event ( nolock ) WHERE EventID <= @EventID
AND Status&0x80000000=0 AND Status&0xFF < 3 and ParentEventID is not NULL and datediff(day,
dateadd(second,  LastOccurTime-(@t), '1970/1/1 0:0:0'), getdate()) > @Ndays

-- N 日以上経過した子イベントを取得
declare my_cur cursor for SELECT EventID, Status FROM #tmptab4Children
open my_cur

select @rows = 0
fetch next from my_cur into @event_id, @status
while ( @@fetch_status = 0 )
begin
    if @rows = 0
        begin transaction UpdChildren
    if @status < 2
    exec dbo.UpdateEventStatus @event_id, 2, @status, @actualstatus output
    exec dbo.DeleteEvent @event_id
    select @rows = @rows + 1
    if @rows > 999
    begin
        commit transaction UpdChildren
        select @rows = 0
    end
    fetch next from my_cur into @event_id, @status
end
if @rows <> 0
    commit transaction UpdChildren
close my_cur
deallocate my_cur

SELECT EventID, Status INTO #tmptab4parents FROM Event ( nolock ) WHERE EventID <= @EventID
AND Status&0x80000000=0 AND Status&0xFF < 3 and ParentEventID is NULL and datediff(day,
dateadd(second,  LastOccurTime-(@t), '1970/1/1 0:0:0'), getdate()) > @Ndays

-- N 日以上経過した親イベントを取得
```

```
declare my_cur cursor for
SELECT EventID, Status FROM #tmptab4parents
open my_cur

select @rows = 0
fetch next from my_cur into @event_id, @status
while ( @@fetch_status = 0 )
begin
    if @rows = 0
        begin transaction UpdParents
    if @status < 2
    exec dbo.UpdateEventStatus @event_id, 2, @status, @actualstatus output
    exec dbo.DeleteEvent @event_id
    select @rows = @rows + 1
    if @rows > 999
    begin
        commit transaction UpdParents
        select @rows = 0
    end
    fetch next from my_cur into @event_id, @status
end
if @rows <> 0
    commit transaction UpdParents
close my_cur
deallocate my_cur
go

grant execute on dbo.mark_delete_events to public
go
```

Analysis Center Issue

Analysis Center 使用時の問題切り分け資料です。

コンソールにログオンできない時

事　象	ログオン時に Invalid URL, Server unavailable メッセージが返される。
原　因	Analysis Center Application Pool identity 用アカウントのパスワードを変更した。
回避策	IIS、Application Pools にある ACAppPool プロパティのパスワードを更新する。

パフォーマンスが上がらない時

事　象	Analysis Center、SQL Reporting Service 各プロセスがシステムリソースを消費する。
回避策	SQL Server の"最大サーバーメモリ"に実装メモリ内で上限を明示する。 E(xtract) T(ransger) L(oad) ジョブのスケジュールを 1 時間ごとに変更する。 OLAP ジョブのスケジュールを 1 時間ごとに変更する。 report subscription, publication をシステムの負荷が低い時に実行する。 他のプロセスが競合しないようにする。 SQL, SQL Analysis サービスのサーバを分離する。 Analysis Center と AppManager は別々のサーバにインストールする。

接続できない時

事　象	接続が切れ、リモートサーバに接続できなくなる。
原　因	Analysis Center Components 間での接続断。
回避策	物理ネットワークの状態確認。 Analysis Center Web サービスをホストしている IIS の動作を確認。

データソースに関する問題

事　象	OLAP ジョブが失敗する。
原　因	Analysis Center Components 間での接続断。
回避策	SQL と Analysis サービスのデータ ディレクトリを抗ウィルス プログラムの検閲から除外する。 AC_OLAP データベース サイズの 2 倍以上のディスク空き領域を確保する。 ExternarlCommandTimeout 値を、OLAP ジョブが 60 分動作後、継続して失敗する場合には、増やす。

レポート作成時の問題（1）

事　象	Report Server Unavailable メッセージが返される。
原　因	Report server に接続できない。
回避策	Report server へのパスが [Tools]-[Options]-[Reporting Services] に設定する。

レポート作成時の問題（2）

事　象	Report 処理中にエラーが発生。
原　因	レポートを処理するのに必要な接続が確立できない。
回避策	Select shared Report server Data Source を、レポート作成時に使用する。 Shared data source や deployed report のために、report server property に設定された委任状（Credentials）を選択する。

NetIQ Aegis

動作ログ

Windows エージェントのログは以下の世代、サイズ、種類があります。

NetIQ Aegis ベース

OS 32 bit / 64 bit	レジストリキー
32 bit	[HKEY_LOCAL_MACHINE¥SOFTWARE¥NetIQ]
64 bit	[HKEY_LOCAL_MACHINE¥SOFTWARE¥Wow6432¥NetIQ]

サービス名 : **NetIQ Aegis Activity Broke / NetIQ Aegis Engine**

レジストリキー
AegisIQConnect73

レジストリ値	データ
home	例 C:¥Program Files (x86)¥NetIQ¥Aegis¥IQConnect73¥
logLevel	3 : 標準 (既定値) 4 : デバッグ
logRetention	5 (世代数)
logSize	1024000 (Byte/ファイル)

フォルダ名	ファイル名
log	ActivtityBroker_NetIQ_PG_Engine.log
	ProcessGovernanceEngine_NetIQ_PG_Engine.og
HotFixes	HF[番号].hfinfo

サービス名 : **NetIQ Aegis Business Service**

パス	ファイル名	セクション
例 C:¥Program Files (x86)¥NetIQ¥Aegis¥bussrv¥	ProcessGovernanceService.exe.config	<system.diagnostics>

フォルダ名	ファイル名
Logs	AegisBusinessServices.nq1
	AegisBusinessServices.svclog
	IQConnect.log
HotFixes	HF[番号].hfinfo

サービス名 : **NetIQ Aegis Correlation Engine**

パス	ファイル名
例 C:¥Program Files (x86)¥NetIQ¥Aegis¥IQConnect73¥Streambase¥etc¥	log4j.configuration

変数名	データ
log4j.apppender.LogFile	例 C:¥Program Files (x86)¥NetIQ¥Aegis¥IQConnect73¥Streambase¥logs¥AegisCorrelationEngine.log
log4j.apppender.SBD.Threshold	INFO または DEBUG

サービス名 : **NetIQ Aegis Namespace Provider**

レジストリキー
AegisIQConnect73

レジストリ値	データ
home	例 C:¥Program Files (x86)¥NetIQ¥Aegis¥IQConnect73¥
logLevel	3 : 標準 (既定値) 4 : デバッグ
logRetention	5 (世代数)
logSize	1024000 (Byte/ファイル)

フォルダ名	ファイル名
log	VigilEntAgent_2219.log
HotFixes	HF[番号].hfinfo

サービス名 ：NetIQ Aegis Namespace Provider (pre-2.2)

レジストリキー
AegisIQConnect

レジストリ値	データ
home	例 C:¥Program Files (x86)¥NetIQ¥Aegis¥IQConnect¥
logLevel	3 : 標準 (既定値) 4 : デバッグ
logRetention	5 (世代数)
logSize	1024000 (Byte/ファイル)

フォルダ名	ファイル名
log	VigilEntAgent_2220.log
HotFixes	HF[番号].hfinfo

サービス名 ：NetIQ AppManager Integration Adapter Namespace Provider

レジストリキー
AppManagerIntegrationAdapterService

レジストリ値	データ
home	例 C:¥Program Files (x86)¥NetIQ¥AppManagerIntegrationAdapter
logLevel	3 : 標準 (既定値) 4 : デバッグ
logRetention	5 (世代数)
logSize	1024000 (Byte/ファイル)

パス	ファイル名
log	VigilEntAgent_4498.log
HotFixes	HF[番号].hfinfo

サービス名 ：**NetIQ Resource Management Namespace Provider**

レジストリキー
ResourceManagementService

レジストリ値	データ
home	例 C:¥Program Files (x86)¥NetIQ¥ResourceManagementService
logLevel	2 ： 標準（既定値） 4 ： デバッグ
logRetention	5（世代数）
logSize	1024000（Byte/ファイル）

パス	ファイル名
log	VigilEntAgent_10117.log
HotFixes	HF[番号].hfinfo

コンソール: **Configuration Console**

パス	ファイル名
C:¥Users¥[UserName]¥AppData¥Roaming¥NetIQ¥Aegis¥[version]¥Logs	ConfigConsole.nq1

コンソール: **Operations Console**

パス	ファイル名
例 C:¥Program Files (x86)¥NetIQ¥Aegis¥website¥	Dianostics.xml

変数名	値
TraceEnabled	False : 無効(既定値) True : 有効
TraceLevel	0 : Error 1 : Waning 2 : Low = Error, Warning (既定値) 3 : Med Low 4 : Low 5 : Med High 6 : High 7 : Very High 8 : Extremely High 9 : Insanely High
TraceDirectory	C:¥ProgramData¥NetIQ¥Aegis¥Logs¥Operations Console
FileName	OperationsConsole.nq1
MaxFileSizeMB	10 (MB)
MinFreeSpaceMB	100 (MB)
NumBackups	5 (世代数)

ログの収集

Aegis ではインストール パス以下の Logs および Hotfixes のフォルダをそれぞれアーカイブし、それを収集します。自動ではできません。

サービスのリセット

以下のサービスが起動できない場合に実施する cold start の手順を説明します。

NetIQ Aegis Namespace Provider

PG.db, PG_events.db を削除後、起動します。

例 : C:¥Program Files (x86)¥NetIQ¥Aegis¥IQConnect73¥data¥PG

PG.db

PG_events.db

いずれかの worktime が暴走している場合の cold start 手順を説明します。

1. 管理者で NetIQ Aegis Configuration Console を起動、ログオンし、Processes の内 In Production 状態の Revision を Take Revision out of Production します。
2. すべての NetIQ Aegis サービスを停止します。推奨される停止順は
   1) NetIQ Aegis Business Services
   2) NetIQ Aegis Correlation Engine
   3) NetIQ Aegis Activity Broker
   4) NetIQ Aegis Engine
   5) NetIQ Aegis Namespace Provider (pre-2.2)
   6) NetIQ Aegis Namespace Provider
   7) NetIQ Resource Management Namespace Provider
3. Microsoft SQL Server Management Studio の [新しいクエリ] で '実行中' の workitem を抽出します。

   select idWorkitem, State, PendingNodeCount, 'JST'=DATEADD(SECOND, StartTime+32400, '1970/01/01') from [Aegis].[PGE].[WorkItem] where State = 1 order by idWorkitem desc
   一番大きな idworkitem を確認し、
   Update [Aegis].[PGE].[WorkItem] Set State=8, PendingNodeCount=0 Where State = 1 and idWorkItem <= 一番大きな idworkitem
   で '停止' に設定します。

4. [コンピュータの管理]-[サービスとアプリケーション]-[メッセージ キュー]-[専用キュー] から MSMQ に滞留しているメッセージがあれば、それを削除します。

5. Microsoft SQL Server Management Studio の [新しいクエリ] で以下の削除文を実行します。

   Delete [Aegis].[WFE].[DATAObject]

   Delete [Aegis].[WFE].[ELEMENTSTATE]

   Delete [Aegis].[WFE].[ELEMENTINSTANCE]

   Delete [Aegis].[WFE].[WORKFLOWINSTANCE]

6. Microsoft SQL Server を再起動します。
7. Microsoft SQL Server Management Studio から SQL エージェントにあるジョブ NetIQ hourly cleanup Aegis をステップ実行します。
8. すべての NetIQ Aegis サービスを開始します。推奨される開始順は
   1) NetIQ Resource Management Namespace Provider
   2) NetIQ Aegis Namespace Provider
   3) NetIQ Aegis Namespace Provider (pre-2.2)
   4) NetIQ Aegis Engine
   5) NetIQ Aegis Activity Broker
   6) NetIQ Aegis Correlation Engine
   7) NetIQ Aegis Business Services
9. 管理者で NetIQ Aegis Configuration Console を起動、ログオンし、Processes を In Production します。

NetIQ DRA

動作ログ

Web Console のログ出力の設定

パス	ファイル名
C:¥inetpub¥wwwroot¥DRAWeb¥WebConsole	DebugInfo.asp

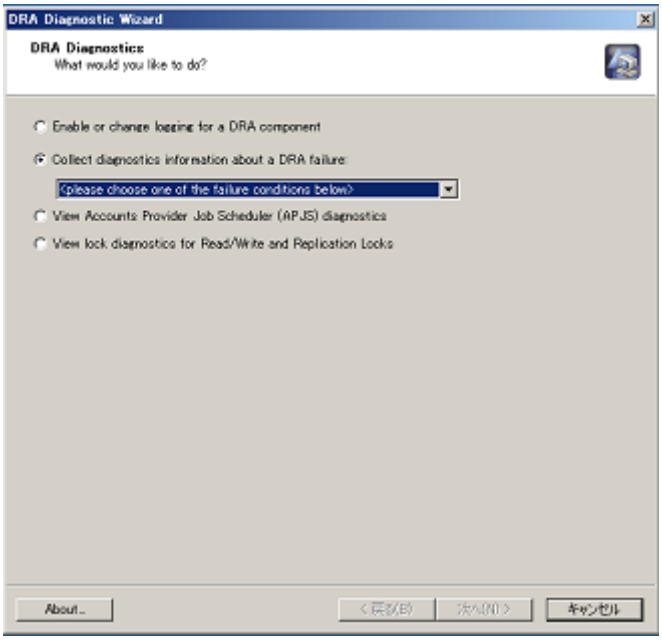
設定値

変数	値
Tracing	False : 作成しない (既定値) True : 作成する
LogLevel	0 : none 1 : Fatal 2 : Error 3 : Warning 4 : Information 5 : more Information 6 : Blocks 7 : Debug 10 : Maximum
LogLocation	%WinDir%¥Temp¥Mission Critical Software
LogSizeMaxMegaBytes	20 (MB)
LogBackups	3 (世代)

ログの収集

動作ログの収集について説明します。

1. 管理者コンソールから DRA インストール フォルダ（ 例 C:¥Program Files (x86)¥NetIQ¥DRA ）以下にある DRADiagnosticUtil.exe を起動します。



2. "Collect diagnostics information about a DRA failure" のラジオボタンをクリックし、リストボックスから症状を選択し、″次へ″をクリックします。

   選択可能な症状は

   "DRA service stopped unexpectedly (crash)"

   "DRA service appears to hang (maximum number of connections is …)"

   "Slow performance of DRA"

   "Server cannot identify the client"

   "General DRA service failure"

   "Unhandled exception in the Win32 user interface"

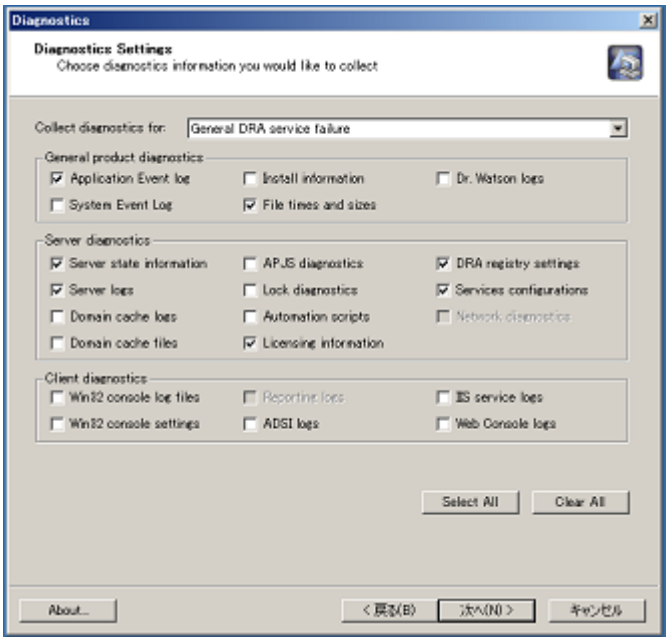
   "General Win32 User Interface failure"

   "General Win32 User Interface failure"

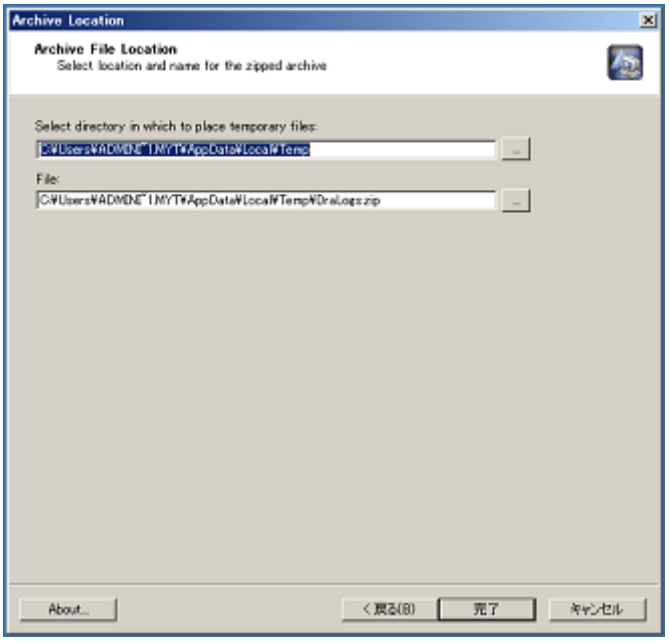
   "General Web Console failure"

   "Other"

3. 選択された症状にあわせて、適切なログが選択されています。″次へ″をクリックします。



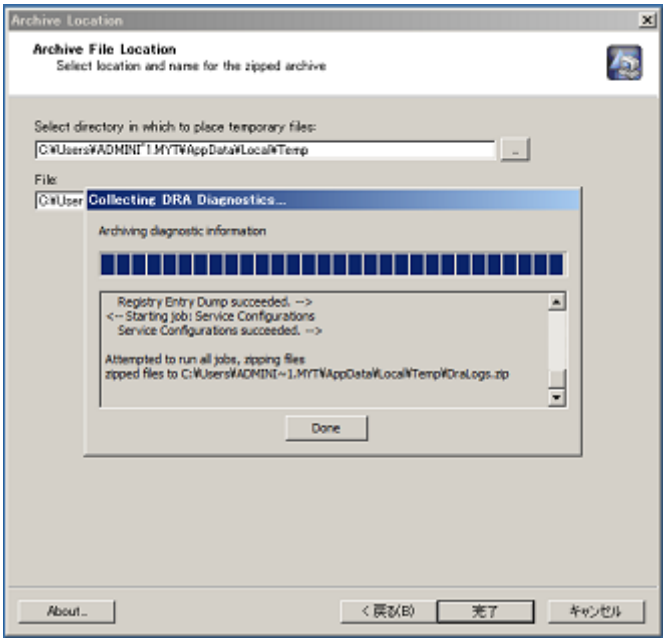
4. "Collect diagnostics information about a DRA failure" のラジオボタンをクリックし、リストボックスから症状を選択し、″次へ″をクリックします。
5. 選択された症状にあわせて、適切なログが選択されています。″次へ″をクリックします。
   収集時に使用される一時ディレクトリと書庫ファイルの出力先が表示されます。問題なければ、″完了″ をクリックし、収集します。



6. 選択された症状にあわせて、適切なログが選択されています。″次へ″をクリックします。

収集時に使用される一時ディレクトリと書庫ファイルの出力先が表示されます。問題なければ、″完了″ をクリックし、収集します。

7. ″Done″ が表示されたら、表示されている書庫ファイルを回収してください。



有用なユーティリティ

Deleted Objects Utility

1. 管理者コンソールから DRA インストール フォルダ（ 例 C:¥Program Files (x86)¥NetIQ¥DRA ）以下にある DraDelObjsUtil.exe を以下の引数で起動し、DRA のサービス アカウントの Deleted Objects コンテナへの読み取りアクセスの有無を確認、これを与奪し、incremental accounts cache refresh の有効・無効を制御します。

   DraDelObjsUtil /domain:Domain [/dc:Computer]
   {/delegate:AcctName1|/verify:AcctName2|/remove:AcctName3|/display
   [/right]}

   /domain:Domain - ドメイン名

   /dc:Computer - ドメイン コントローラのマシン名か、IP address

   /delegate:AcctName1 - Deleted Objects コンテナへの読取を委譲するアカウント

   /verify:AcctName2 - Deleted Objects コンテナへの読取を確認するアカウント

   /remove:AcctName3 - Deleted Objects コンテナへの読取をはく奪するアカウント

   /display - Deleted Objects コンテナのセキュリティ表示

   /right - 指定したアカウントが Synchronize directory service data user 権限を持っていることの確認

Recycle Bin Utility

1. 管理者コンソールから DRA インストール フォルダ（ 例 C:¥Program Files (x86)¥NetIQ¥DRA ）以下にある DraRecycleBinUtil.exe を以下の引数で起動し、DRA のサービス アカウントの NetIQRecycleBin コンテナ（隠し）へのアクセスの有無を確認、これを与えます。

   DraRecycleBBinUtil /domain:Domain
   /delegate:AcctName1|/verify:AcctName2|/display [/dc:Computer]

   /domain:Domain - ドメイン名

   /delegate:AcctName1 - NetIQRecycleBin コンテナへの権限を委譲するアカウント

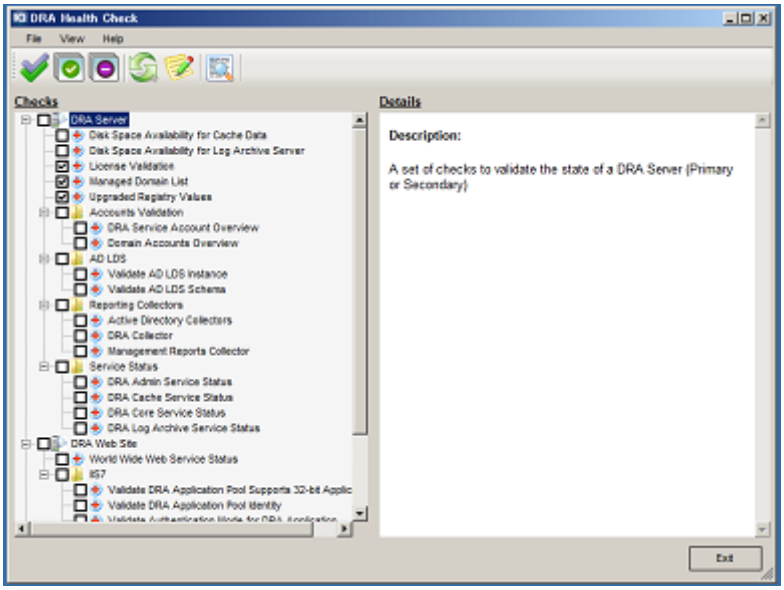
   /verify:AcctName2 - NetIQRecycleBin コンテナへの権限を確認するアカウント

   /display - NetIQRecycleBin コンテナのセキュリティ表示

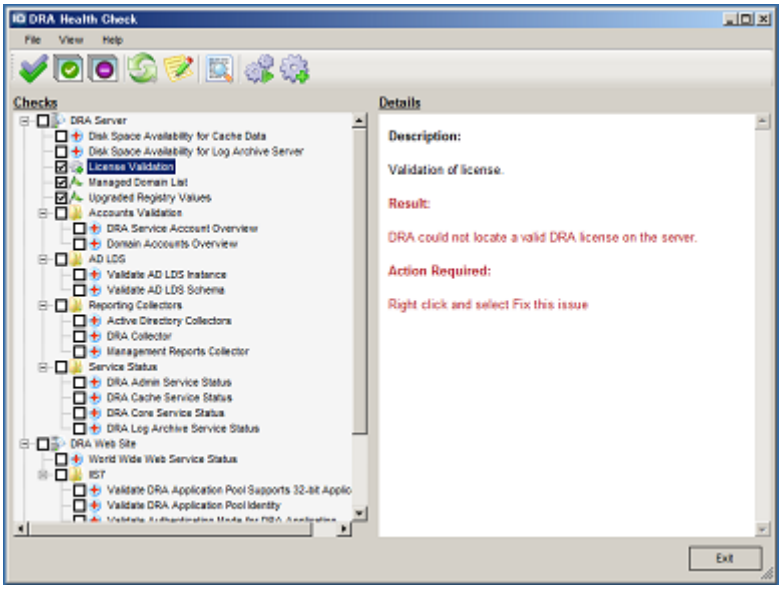
   /dc:Computer - ドメイン コントローラのマシン名か、IP address

Health Check Utility

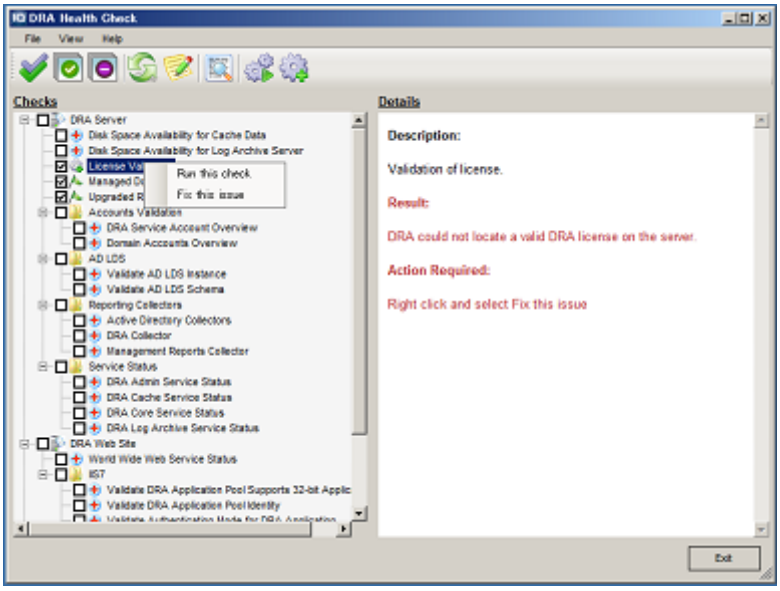
1. DRA では、ライセンス数が上限に達すると、オブジェクトへの一切の操作ができなくなります。そのため、間もなくライセンス数の上限に達する場合、事前に警告メッセージが発生します。その場合には、できるだけ早期にライセンスを追加してください。ライセンスは拡張子 lic のファイルにて配られます。
2. Health Check Utility を起動します。 License Validation にチェックが入っていることを確認後、メニューバー直下のダブル チェック アイコンをクリック、検査します。



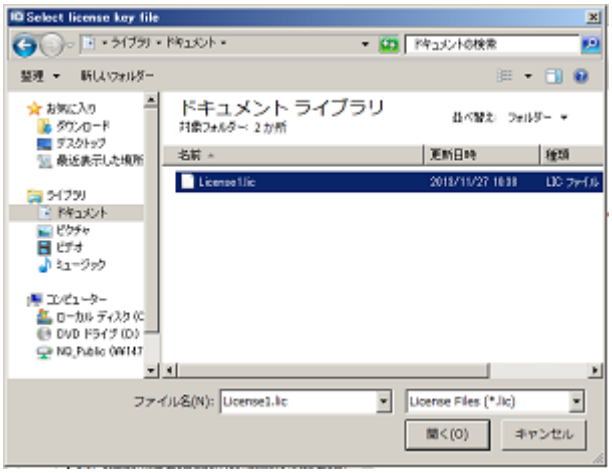
3. Details に表示された結果を確認します。



4. License Validation をクリック、Fix This issue をクリックします。



5. 新しいライセンスキー（ 拡張子 lic ）を開き、取り込みます。ライセンスキーは上書きになります。



6. Health Check Utility を起動します。 License Validation にチェックが入っていることを確認後、メニューバー直下のダブル チェック アイコンをクリック、再度検査し、問題が解決されたことを確認します。

