7 アラーム機能およびモニタ機能

概　要

本装置は、事前に指定しておいたイベントが起きたときに、アラームをコンソールへ送ることができます。また、定期的に状況モニタ・レポートを作成することもできます。アラームおよび監視レポートは、1行のテキスト形式です。アラームは「A」で始まり、監視レポートは「M」で始まります。どちらにもタイムスタンプが付いています。アラームおよび監視レポートは、ローカルの管理コンソールまたはリモート管理セッション(TelnetまたはSecure Shellのみ)に対して作成することができます。
アラームを設定すると、以下の状況を即座にユーザーへ通知することができます。

- 暗号状態の変更
- SSLコネクションの拒否
- ユーティライゼーションしきい値アラーム
- 過負荷アラーム
- ネットワークのリンク状況

デフォルトでは、すべてのアラームが無効になっています。有効にするときは、任意の組み合わせが可能です。

アラームの形式は、次のようになっています。

A:*yyyymmddhhmmss:ALARM_CODE:MODIFIER:EXTENDED_DATA:/*message*/*

ここで、

A: アラームであることを示します。

yyyymmddhhmmss: タイムスタンプ

ALARM_CODE: アラームタイプ
[ESC|RSC|UTL|OVL|NLS]

MODIFIER:アラーム生成源：アラームをトリガしたイベントを示すコードです。

EXTENDED_DATA: 関連する追加の時刻情報

*/*message*/*: どのようなアラームなのかを示す簡単な説明

暗号状態の変更アラーム(ESC)は、詳細情報を表示しません。

アラームを設定するためのCLIコマンドを以下に示します。

コマンド	パラメータ	デフォルト
set alarms	all, esc, rsc, utl, ovl, nls	未設定
show alarms		

コマンドの使用例を以下に示します。

```
Intel 7110> set alarms
Select monitoring fields (all, esc, rsc, utl, ovl, nls) [all]: all
Intel 7110> show alarms
All alarms are enabled.
Intel 7110> set alarms none
Intel 7110> show alarms
Alarms set:
```

アラームのタイプ

設定可能なアラームのタイプを以下に詳しく説明します。

ESC:暗号状態の変更アラーム

このアラームを有効にすると、デバイスがINLINEモード/BYPASSモードの切り替えを行ったときに、アラームが発行されます。このモードの切り替えを行うには、inlineコマンドまたはbypassコマンドをCLIから実行します。デバイスのフロント・パネルのBYPASSボタンを押しても構いません。

形式:

A:*yyyymmddhhmmss*:ESC:HDWR|CONB|CONI|FNTB|FNTI|APPR:/*message*/

ここで、

A:アラームであることを示します。

yyyymmddhhmmss:タイムスタンプ。

ESC:暗号状態変更のアラームであることを示します。

アラームの修飾子

HDWR: 暗号処理ハードウェアに問題があったこと示します。

CONB: コンソールからbypass状態にされたことを示します。

CONI: コンソールからinline状態にされたことを示します。

FNTB: フロントパネルからbypass状態にされたことを示します。

FNTI: フロントパネルからinline状態にされたことを示します。

APPR: indicates application restart

RSC:SSLコネクションの拒否

このアラームを有効にすると、現在指定されている期間(5～65000秒、デフォルトは15秒)の間に、対応暗号の不一致またはクライアント認証の失敗によってSSLコネクションが拒否された場合に、アラームが発行されます。拒否されたSSLコネクションの総数は、拒否の理由とともに報告されます。このアラームは、CLIから有効/無効を切り替えることができます。

形式:

A:yyyymmddhhmmss:RSC:CSMM|CCAF:XXX:/**message**/
ここで、

A: アラームであることを示します。

yyyymmddhhmmss: タイムスタンプ。

RSC: SSLコネクション拒否アラームであることを示します。

アラームの修飾子およびメッセージ

CSMM: Cipher suite mismatch(対応暗号の不一致)

CCAF: client certificate authenticate failure
(クライアント認証の失敗)

詳細情報

XXX:ウィンドウ時間内に拒否されたコネクションの数を示し ます。

RSCアラーム用のCLIコマンド

SSLコネクション拒否アラーム時間ウィンドウを設定するには、以下のコマンドを使用します。

set rsc_window <seconds> (Range: 5-65000, default: 15)

SSLコネクション拒否アラームを表示するには、以下のコマンドを使用します。

show rsc_window

使用例:

Intel 7110> **set rsc_window 10**

Intel 7110> **show rsc_window**
Check refused SSL connections [secs]: 10

UTL:ユーティライゼーションしきい値アラーム

このアラームは、以下の3つのユーティライゼーションしきい値を監視します

- CPU負荷
- 1秒ごとのコネクション数
- 同時オープンコネクション数

このアラームを有効にすると、使用値のいずれかが、規定最大値への割合で指定した上側水準点を超えたときや指定した下側水準点を下回ったときに、アラームが発行されます。上側水準点および下側水準点は、ユーザーが定義します。デフォルトでは、上側水準点は90%、下側水準点は60%です。

- しきい値アラーム用に集められたデータは、バースト性を持つ傾向があります。そのため、アラームが休みなく発行され続けることを防ぐため、スムージング・アルゴリズムが使用されています。この時間の間のデータが収集され、その平均値が計算されます。したがって、間隔を短くすると、無意味なアラームが大量発行されることがあります。この間隔は、5～65000秒の間で設定することができます(デフォルトは15です)。
- ユティライゼーションしきい値アラームにおける100%の値(規定最大値)は以下のようになります。

  1秒毎のコネクション数: 200

  同時オープンコネクション数: 2500

形式:

`A:yyyymmddhhmmss:UTL:ALRT|NMRL:CPU|CON|CPS:/*message*/`

ここで、

`A:` アラームであることを示します。

`yyyymmddhhmmss:` タイムスタンプ。

`UTL:`ユーティライゼーションしきい値アラームであることを 示します。

アラームの修飾子およびメッセージ

`ALRT: message: [CPU|Open connections|CPS] exceed high water mark`

`NMRL: message: [CPU|Open connections|CPS] dorp below low water mark`
(`[CPU|`同時オープンコネクション数`|CPS]` が指定の下側しきい値より小さくなった)

詳細情報

CPU：CPU負荷率がアラームをトリガしたことを示します。

CON：アクティブになっているコネクション数がアラームをトリガしたことを示します。

CPS：秒あたりのコネクション数がアラームをトリガしたことを示します。

UTLアラーム用のCLIコマンド

使用しきい値アラームの時間ウィンドウを設定するには、以下のコマンドを使用します

```
set utl_window <seconds> (Range: 5-65000, default: 15)
```

使用しきい値アラームの上側水準点を設定するには、以下のコマンドを使用します。

```
set utl_high <percentage> (Range: 2-100, default: 90)
```

使用しきい値アラームの下側水準点を設定するには、以下のコマンドを使用します。

```
set utl_low <percentage> (Range: 1-99, default: 60)
```

現在の設定を表示するには、以下のコマンドを使用します。

```
show utl_window

show utl_high

show utl_low
```

例:

```
Intel 7110> set utl_window 10

Intel 7110> show utl_window
Utilization window set [secs]: 10.

Intel 7110> set utl_highwater 80

Intel 7110> show utl_highwater

Utilization High water mark [%]: 80

Intel 7110> set utl_lowwater 60

Intel 7110> show utl_lowwater

Utilization Low water mark [%]: 60
```

OVL:過負荷アラーム

このアラームを有効にすると、過負荷が発生して、現在設定されているアラーム期間(5〜65000秒、デフォルトは15秒)の間にスピルやスロットリングがなされた場合に、アラームが発行されます。

このアラームが発行されると、暗号化/復号化機能は無効になります。

形式:

A:*yyyymmddhhmmss*:OVL:SPIL|THRT:XXX:/**message*/*

ここで、

A: アラームであることを示します。

yyyymmddhhmmss: タイムスタンプ。

OVL: 過負荷アラームであることを示します。

アラームの修飾子およびメッセージ

SPIL: 過負荷によってスピルされたことを示します。 message: Spill mode.

THRT: 過負荷によりスロットリングされたことを示します。 message: Throttle mode.

詳細情報

XXX: ウィンドウ時間内に発生した過負荷状態の数を示します。

OVLアラーム用のCLIコマンド

過負荷アラームの時間ウィンドウを設定するには、以下のコマンドを使用します。

Intel 7110> **set ovl_window <seconds>** (Range: 5-65000, default: 15)

過負荷アラームの時間ウィンドウを表示するには、以下のコマンドを使用します。

Intel 7110> **show ovl_window**

例:

```
Intel 7110> set ovl_window 10

Intel 7110> show ovl_window
Check for overload conditions [sec]: 10
```

NLS:ネットワークのリンク状態アラーム

ネットワークまたはサーバのリンク状態が変わると、アラームが発行されます。

形式:

A:*yyyymmddhhmmss*:NLS:NETL|SVRL:LNKD|10HDX|10FDX|100HDX|100FDX:
/**message**/

ここで、

A: アラームであることを示します。

yyyymmddhhmmss: タイムスタンプ。

NLS: ネットワークのリンク状態変更によるアラームであることを示します。

アラームの修飾子およびメッセージ

NETL: ネットワーク側ポートの状態変更であることを示します。message: [No carrier|10Mb/s|100Mb/s][half duplex|full duplex]

SVRL indicates the server port status. Message: [No carrier|10Mb /s|100Mb/s] [half duplex|full duplex]

詳細情報

LINKD: indicates no carrier.

10HDX: indicates 10Mb/s, half duplex.

10FDX: indicates 10Mb/s, full duplex.

100HDX: indicates 100Mb/s, half duplex.

100FDX: indicates 100Mb/s, full duplex.

アラームのログ

本装置は、発行されたアラームをリング・バッファ上に保持しています。最新のアラームや、例外発生により生成および保存された履歴ログは、コンソールやTelnetリモート・セッション、SSH(Secure Shell)リモート・セッションで参照することができます。最新のアラームを表示するときは、アラーム・バッファが直ちにダンプされます。
履歴ログは、情報のスナップショットからなります。ここでいう情報とは、status lineコマンドを実行してから、例外発生時に存在していたアラーム・バッファをダンプすることにより得られる情報のことです。
発行されたアラームは、CLIコマンドのstatus alarmsを使用して、コンソールに表示することができます。また、例外発生により生成および保存されたログは、CLIコマンドのstatus <log filename>を使用して、表示することができます(list logsコマンドを使用すれば、参照可能なログ・ファイルを表示できます)。
以下は、ログ表示を行うためのCLIコマンドの例です。デフォルトやレンジが設定されたコマンドもあります。
list logsコマンドとstatusコマンドの使用例を示します。

```
Intel 7110> list logs

20000727_145544

Intel 7110> status 20000727_145544

================= STATE ====================

Boot time:                      Thu Jul 27
14:54:21 2000

Curr time:                      Thu Jul 27
14:55:43 2000

Restarts:                       3

KTR Mask:                       0xFFFFF3DD

Total Connections:              0

Active Connections:             0, 0 (cur, max)

Connections/Second:             0, 0 (cur, max)


Util Status:

Secure Bytes Read:              0

Plain Bytes Read:               0

Secure Bytes Wrote:             0

Plain Bytes Wrote:              0

Bytes Allocated to dbufs:       0

Bytes Per dbuf:                 0
```

```
Spill Mode:                     disable

Transactions Spilled:           0

Times Thottled Accepts:         0

Bypass Mode:                    disable

L&M board status:               RESPEND  INLINE
(0x00000060)

Network NIC:                    100baseTX Half
Duplex

                                (0x00000026
0x00000003 0x00000026)

Server NIC:                     No carrier

                                (0x00000023
0x00000001 0x00000023)

Network LED:                    on

Server LED:                     off

SSL Caching:                    Enabled.


--------------- Configuration --------------
conlog 0xffffffef

ilog 0xffffffff

trace 0xfffff3dd

media auto

logport tty01

cache 3

server_tmo 5

client_tmo 30

serverif exp1

netif exp0

map 0.0.0.0 443 80 default

kpanic reboot

monitoring_interval 0

monitoring_fields 0x1f

alarm_mask 0x0000001f

ovl_window 15
```

```
rsc_window 15

utl_window 15

utl_high 90

utl_low 60

idle 300

kstrength 512

con_speed 9600

con_bits 8

con_stop 1

con_parity n

defcert_cname US

defcert_state California

defcert_city San Diego

defcert_orgname Intel Corporation

defcert_orgunit Network Equipment Division

defcert_name www.intel.com

defcert_email support@intel.com

prompt Intel 7110>

trap_authen

remote_if exp0

ip 10.1.11.34

netmask 255.255.0.0

A:07/27/2000 14:54:47:NLS:SVRL:NC:/* Server port status,
No carrier */

A:07/27/2000 14:54:41:NLS:SVRL:100FDX:/* Server port status,
100Mb/s, full dupl/

A:07/27/2000 14:54:21:NLS:NETL:100HDX:/* Network port status,
100Mb/s, half dup/

A:07/27/2000 14:54:21:NLS:SVRL:NC:/* Server port status,
No carrier */

A:01/01/1970 00:00:00:ESC:APPR:3:/* Application Restarted */

Intel 7110>
```

status alarmsコマンドの使用例を示します。

```
Intel 7110> status alarms

A:07/27/2000 14:57:05:ESC:CONI:/* Console inline */

A:07/27/2000 14:57:05:NLS:NETL:100HDX:/* Network port status,
100Mb/s, half dup/

A:07/27/2000 14:57:01:ESC:CONB:/* Console bypass */

A:07/27/2000 14:57:01:NLS:NETL:NC:/* Network port status,
No carrier */

A:07/27/2000 14:56:51:NLS:SVRL:NC:/* Server port status,
No carrier */

A:07/27/2000 14:56:46:NLS:SVRL:100FDX:/* Server port status,
100Mb/s, full dupl/

A:07/27/2000 14:56:30:ESC:CONI:/* Console inline */

A:07/27/2000 14:56:30:NLS:NETL:100HDX:/* Network port status,
100Mb/s, half dup/

A:07/27/2000 14:56:29:NLS:NETL:NC:/* Network port status,
No carrier */

A:07/27/2000 14:56:29:NLS:SVRL:NC:/* Server port status,
No carrier */

Intel 7110>
```

モニタ

モニタ・レポート

モニタ・レポートは、ユーザーが設定することのできる1行のテキストです。指定した5～65000秒の間隔で、コンソールに表示されます。間隔のデフォルト値は15秒です。
デフォルトでは、モニタ・レポート機能は無効になっています。有効にするには、CLI monitor...コマンド・セットを使用します。監視アプリケーションは、これらのコマンドが届けられたポートを検知して、それと同じポートにレポートを送信します。そのため、監視レポートは、そのコマンドが出されたのと同じコンソールに表示されます。

レポートの設定

ユーザーは、各レポートに表示するフィールドを指定することができます。レポートは「M」で始まり(監視レポートの場合。アラーム・レポートと区別するための文字です)、それに続いて、タイムスタンプが示されます。この他に表示するフィールドは、CLIコマンドを使用して選択することができます(このすぐ後の「CLIコマンド」を参照してください)。標準のデフォルト・フィールドは、mode、failmode、CPU、SSLCS、およびOVRです。モニタ・レポート機能は、デフォルトでは無効になっています。
監視レポートの形式は、次のようになっています。

M:*yyyymmddhhmmss*:*mode*:*failmode*:CPU;*i*,*k*,*a*:SSLCS;
c,*m*,*t*:OVR;*r*,*c*,*m*,*t*:
NetIF;*s*:SvrIF;*s*:BES;*c*,*m*,*t*;BDS;*c*,*m*,*t*

ここで、

M: モニタ・レポートであることを示します。

yyyymmddhhmmss: タイムスタンプ。

mode: BypassモードかInlineモードか：[INLINE|BYPASS]

failmode: フェイル・モード状態：[SAFE|THRU]

CPU;*i*,*k*,*a* CPU負荷(%);それぞれ*i*はアイドル、 *k*はカーネル、 *a*はアプリケーション部の負荷率を示します。

SSLCS;c,m,t 秒ごと(トータルは除く)の処理されているSSL コネクション数を示し、cは現在の状態、mは最大値、tは直前の起動から処理したSSLコネクションのトータルの値を示します。

OVR;*r*,*c*,*m*,*t* 過負荷状態； *r*は [SPIL¦THRT]、*c*は現在の状態、*m*は最大値、*t*は直前の起動後に発生したトータルの過負荷状態数

NetIF;*s*ネットワーク側インタフェースの状態；
*s*は [NC¦10HDX¦10FDX¦100HDX¦100FDX]です。

SvrIF;*s*サーバ側インタフェースの状態；
*s*は [NC¦10HDX¦10FDX¦100HDX¦100FDX]です。

BES;*c*,*m*,*t* 暗号化処理速度；*c*は現在の秒ごとの処理バイト数、*m*は最大の秒ごとの処理バイト数、*t*は直前の起動後からの総処理バイト数

BDS;*c*,*m*,*t* 復号処理速度；*c*は現在の秒毎の処理バイト数、*m*は最大の秒ごとの処理バイト数、*t*は直前の起動後からの総処理バイト数

モニタ・レポート用のCLIコマンド

以下は、コンソールでモニタを行うのためのCLIコマンドです。デフォルトやレンジが設定されたコマンドもあります。

```
set monitoring_interval <seconds> (範囲: 5-65000; Default: 15 )

show monitoring_interval

set monitoring_fields <fields> (範囲: all, mode, failmode, cpu, cps,
ovrld, link, enc, dec; Default: mode, failmode, cpu, cps, ovrld)

show monitoring_fields

set monitoring enable|disable (デフォルト: disable)

show monitoring
```

例:

```
Intel 7110> set monitoring_interval 15

Intel 7110> show monitoring_interval

Monitoring report interval [secs]: 15

Intel 7110> set monitoring disable

Intel 7110> show monitoring

The monitoring report is disabled for this CLI.

Intel 7110> set monitoring_fields

Select monitoring fields (all, mode, failmode, cpu, cps, ovrld, link,
enc,

dec) [all]: all

Intel 7110> show monitoring_fields

All monitoring fields are enabled.

Intel 7110> set monitoring enable

Intel 7110> show monitoring

The monitoring report is enabled for this CLI.
```