障害およびログの表示

この章は、次の内容で構成されています。

- 障害のサマリー （1 ページ）
- 障害履歴 （2 ページ）
- Cisco IMC ログ （2 ページ）
- システム イベント ログ （14 ページ）

障害のサマリー

障害およびログのサマリーの表示

手順

	コマンドまたはアクション	目的
ステップ 1	Server # **scope fault**	障害コマンド モードを開始します。
ステップ 2	Server # **show fault-entries**	すべての障害のログを表示します。

例

次に、障害のサマリーの例を示します。

```
Server # scope fault
Server /fault # show fault-entries
Time                     Severity      Description
------------------------ ------------ -----------------
Sun Jun 27 04:00:52 2013  info         Storage Local disk 12 missing
Sat Jun 26 05:00:22 2013  warning      Power Supply redundancy is lost

Server /fault #
```

障害履歴

障害履歴の表示

手順

	コマンドまたはアクション	目的
ステップ 1	Server # **scope fault**	障害コマンド モードを開始します。
ステップ 2	Server # **show fault-history**	障害の履歴を表示します。

例

次に、障害の履歴を表示する例を示します。

```
Server # scope fault
Server /fault # show fault-history
Time                 Severity  Source  Cause                 Description
-------------------- --------- ------  --------------------
----------------------------------------
2014 Feb 6 23:24:49 error     %CIMC   PSU_REDUNDANCY-FAIL
"[F0743][major][psu-redundancy-fail].....
2014 Feb 6 23:24:49 error     %CIMC   EQUIPMENT_INOPERABLE
"[F0374][major][equipment-inoperable]...
2014 Feb 6 23:24:19 debug     %CIMC   2014 Feb 6 23         "24:19:7:%CIMC::: SEL INIT
DONE"

Server /fault #
```

Cisco IMC ログ

Cisco IMC ログの表示

手順

	コマンドまたはアクション	目的
ステップ 1	Server# **scope cimc**	Cisco IMC コマンド モードを開始します。
ステップ 2	Server /cimc # **scope log**	Cisco IMC ログ コマンド モードを開始します。

	コマンドまたはアクション	目的
ステップ 3	Server /cimc/log # **show entries** [**detail**]	Cisco IMC イベントをタイムスタンプ、イベントを記録したソフトウェア モジュール、およびイベントの説明とともに表示します。

例

次に、Cisco IMC イベントのログを表示する例を示します。

```
Server# scope cimc
Server /cimc # scope log
Server /cimc/log # show entries
Time                 Severity      Source           Description

------------------- ------------ --------------- ---------------------------------------

2012 Jan 30 05:20:45 Informational BMC:ciscoNET:961 " rpc_aim_callback_function_1_svc()
 - result == SUCCESS, callbackData size: 600 "
2012 Jan 30 05:20:45 Informational BMC:ciscoNET:961 rpc_aim_callback_function_1_svc() -
 returned from pFunctionCallback result:0
2012 Jan 30 05:20:45 Informational BMC:ciscoNET:961 " rpc_aim_callback_function_1_svc()
 - szFunctionName:netGetCurrentIfConfig nSize:0 nMaxSize: 600 "
--More--

Server /cimc/log # show entries detail
Trace Log:
    Time: 2012 Jan 30 05:20:45
    Severity: Informational
    Source: BMC:ciscoNET:961
    Description: " rpc_aim_callback_function_1_svc() - result == SUCCESS, callbackData
size: 600 "
    Order: 0
Trace Log:
    Time: 2012 Jan 30 05:20:45
    Severity: Informational
    Source: BMC:ciscoNET:961
    Description: rpc_aim_callback_function_1_svc() - returned from pFunctionCallback
result:0
    Order: 1
Trace Log:
    Time: 2012 Jan 30 05:20:45
    Severity: Informational
    Source: BMC:ciscoNET:961
   Description: " rpc_aim_callback_function_1_svc() - szFunctionName:netGetCurrentIfConfig
 nSize:0 nMaxSize: 600 "
    Order: 2
--More--

Server /cimc/log #
```

Cisco IMC ログのクリア

手順

	コマンドまたはアクション	目的
ステップ 1	Server# **scope cimc**	Cisco IMC コマンド モードを開始します。
ステップ 2	Server /cimc # **scope log**	Cisco IMC ログ コマンド モードを開始します。
ステップ 3	Server /cimc/log # **clear**	Cisco IMC ログをクリアします。

例

次に、Cisco IMC イベントのログをクリアする例を示します。

```
Server# scope cimc
Server /cimc # scope log
Server /cimc/log # clear
```

Cisco IMC ログしきい値の設定

Cisco IMC ログに含まれるメッセージの最低レベルを指定できます。

手順

	コマンドまたはアクション	目的
ステップ 1	Server# **scope cimc**	Cisco IMC コマンド モードを開始します。
ステップ 2	Server /cimc # **scope log**	Cisco IMC ログ コマンド モードを開始します。
ステップ 3	Server /cimc/log # **set local-syslog-severity** *level*	シビラティ（重大度）の *level* には、次のいずれかを指定できます。順にシビラティ（重大度）が下がります。 • emergency • alert • critical • error • warning

	コマンドまたはアクション	目的
		• notice • informational • debug （注） Cisco IMC では、選択したシビラティ（重大度）よりも低いシビラティ（重大度）のメッセージはログに記録されません。たとえば、**error** を選択した場合、Cisco IMC ログにはシビラティ（重大度）が Emergency、Alert、Critical、または Error のすべてのメッセージが含まれます。Warning、Notice、Informational、または Debug のメッセージは表示されません。
ステップ 4	Server /cimc/log # **commit**	トランザクションをシステムの設定にコミットします。
ステップ 5	（任意） Server /cimc/log # **show local-syslog-severity**	設定されたシビラティ（重大度）レベルを表示します。

例

次に、最小シビラティ（重大度）を警告として、メッセージのロギングを設定する例を示します。

```
Server# scope cimc
Server /cimc # scope log
Server /cimc/log # set local-syslog-severity warning
Server /cimc/log *# commit
Server /cimc/log # show local-syslog-severity
    Local Syslog Severity: warning

Server /cimc/log #
```

リモート サーバへの Cisco IMC ログの送信

Cisco IMC ログ エントリを受信するように 1 台または 2 台のリモート syslog サーバのプロファイルを設定できます。

始める前に

- リモート syslog サーバが、リモート ホストからログを受信するように設定されている必要があります。
- リモート syslog サーバが、認証関連のログを含め、すべてのタイプのログを受信するように設定されている必要があります。
- リモート syslog サーバのファイアウォールが、syslog メッセージが syslog サーバに到達するように設定されている必要があります。

手順

	コマンドまたはアクション	目的
ステップ 1	Server# **scope cimc**	Cisco IMC コマンド モードを開始します。
ステップ 2	Server /cimc # **scope log**	Cisco IMC ログ コマンド モードを開始します。
ステップ 3	（任意） Server /cimc/log # **set remote-syslog-severity** *level*	シビラティ（重大度）の *level* には、次のいずれかを指定できます。順にシビラティ（重大度）が下がります。 • emergency • alert • critical • error • warning • notice • informational • debug

	コマンドまたはアクション	目的
		（注） Cisco IMC では、選択したシビラティ（重大度）よりも低いシビラティ（重大度）のメッセージは、リモートでログに記録されません。たとえば、**error** を選択した場合、リモート syslog サーバはシビラティ（重大度）が Emergency、Alert、Critical、または Error のすべての Cisco IMC ログ メッセージを受信します。Warning、Notice、Informational、または Debug のメッセージは表示されません。
ステップ 4	Server /cimc/log # **scope server** {**1** | **2**}	2 台のリモート syslog サーバ プロファイルのいずれかを選択し、プロファイルを設定するコマンド モードを開始します。
ステップ 5	Server /cimc/log/server # **set server-ip** *ipv4 or ipv6 address or domain name*	リモート syslog サーバのアドレスを指定します。 （注） リモート サーバのアドレスとして IPv4 アドレスまたは IPv6 アドレス、あるいはメイン名を設定できます。
ステップ 6	Server /cimc/log/server # **set server-port** *port number*	リモート syslog サーバの宛先ポート番号を設定します。
ステップ 7	Server /cimc/log/server # **set enabled** {**yes** | **no**}	この syslog サーバへの Cisco IMC ログ エントリの送信を有効にします。
ステップ 8	Server /cimc/log/server # **commit**	トランザクションをシステムの設定にコミットします。

例

次に、リモート syslog サーバ プロファイルを設定し、シビラティ（重大度）レベル Warning 以上の Cisco IMC ログ エントリの送信を有効にする例を示します。

```
Server# scope cimc
Server /cimc # scope log
Server /cimc/log # set remote-syslog-severity warning
Server /cimc/log *# scope server 1
Server /cimc/log/server *# set server-ip www.abc.com
Server /cimc/log/server *# set server-port 514
Server /cimc/log/server *# set enabled yes
Server /cimc/log/server *# commit
Server /cimc/log/server # exit
Server /cimc/log # show server
Syslog Server 1:
    Syslog Server Address: www.abc.com
    Syslog Server Port: 514
    Enabled: yes

Server /cimc/log # show remote-syslog-severity
    Remote Syslog Severity: warning

Server /cimc/log #
```

リモート サーバへのテスト Cisco IMC ログの送信

始める前に

- リモート syslog サーバが、リモート ホストからログを受信するように設定されている必要があります。
- リモート syslog サーバが、認証関連のログを含め、すべてのタイプのログを受信するように設定されている必要があります。
- リモート syslog サーバのファイアウォールが、syslog メッセージが syslog サーバに到達するように設定されている必要があります。

手順

	コマンドまたはアクション	目的
ステップ 1	Server# **scope cimc**	Cisco IMC コマンド モードを開始します。
ステップ 2	Server /cimc # **scope log**	Cisco IMC ログ コマンド モードを開始します。
ステップ 3	Server /cimc/log # **send-test-syslog**	テスト Cisco IMC ログを設定したリモート サーバに送信します。

例

次に、テスト Cisco IMC の syslog を設定したリモート サーバに送信する例を示します。

```
Server# scope cimc
Server /cimc # scope log
Server /cimc/log # send-test-syslog

Syslog Test message will be sent to configured Syslog destinations.
If no Syslog destinations configured, this command will be silently ignored.
Syslog Test message has been requested.

Server /cimc/log #
```

無効なユーザー名のロギングを有効にする

ロギングの試行が失敗した場合に無効なユーザー名のロギングを有効にするには、次の手順を実行します。

手順

	コマンドまたはアクション	目的
ステップ 1	Server# **scope cimc**	Cisco IMC コマンド モードを開始します。
ステップ 2	Server /cimc # **scope log**	Cisco IMC ログ コマンドモードを開始します。
ステップ 3	Server /cimc/log #**set log-username-on-auth-fail enabled**	無効なユーザー名のロギングを有効にします。
ステップ 4	Server /cimc/log* #**commit**	トランザクションをシステムの設定にコミットします。

例

この例は、無効なユーザー名のロギングを有効にする方法を示しています。

```
Server# scope cimc
Server /cimc # scope log
Server /cimc/log # set log-username-on-auth-fail enabled
Server /cimc/log* #commit
Server /cimc/log
```

リモート Syslog 証明書のアップロード

始める前に

- admin 権限を持つユーザとしてログインする必要があります。
- アップロードする証明書ファイルは、ローカルにアクセスできるファイルシステムに配置されている必要があります。

- 次の証明書形式がサポートされています。
  - .crt
  - .cer
  - .pem

リリース 4.2 (2a) 以降、リモート Syslog 証明書を Cisco UCS C シリーズ サーバーにアップロードできます。証明書を 1 つまたは 2 つの Cisco UCS C シリーズ サーバーにアップロードできます。

手順

ステップ 1 Server # **scope cimc**

Cisco IMC コマンドモードを開始します。

ステップ 2 Server /cimc # **scope log**

Cisco IMC ログ コマンドモードを開始します。

ステップ 3 Server /cimc/log # **scope server{1|2}**

2 つのリモート Syslog サーバー プロファイルのいずれかを選択し、コマンドモードを開始して、リモート Syslog 証明書をアップロードし、選択したサーバーでセキュアなリモート Syslog を有効にします。

ステップ 4 Server /cimc/log/server # **upload-certificate** *remote-protocol server_address path certificate_filename*

リモート サーバーに接続するためのプロトコルを指定します。次のいずれかのタイプを指定できます。

- TFTP
- FTP
- SFTP
- SCP
- HTTP

（注） FTP、SCP または SFTP としてプロトコルを選択した場合は、ユーザー名とパスワードの入力が求められます。

リモート Syslog 証明書をアップロードする場所からファイルパス、およびリモート プロトコルを入力します。リモート サーバーのユーザー名とパスワードを検証した後、リモート サーバーからリモート Syslog 証明書をアップロードします。

ステップ 5 （オプション）Server /cimc/log/server # **paste-certificate**

これは、リモート Syslog 証明書をアップロードするための追加オプションです。

プロンプトされたら、証明書の内容を貼り付け、Ctrl+D を押します。

ステップ 6 Server /cimc/log/server # **setsecure-enabledyes**

サーバーでセキュアなリモート Syslog を有効にします。

ステップ 7 Server /cimc/log/server # **commit**

トランザクションをシステムの設定にコミットします。

例

- この例では、リモート サーバーからリモート Syslog 証明書をアップロードし、選択したサーバーでセキュアなリモート Syslog を有効にします。

```
Server # scope cimc
Server /cimc # scope log
Server /cimc/log # scope server
Server /cimc/log/server # upload-certificate scp 10.10.10.10
/home/user-xyz/rem-sys-log-certif.cert
Server (RSA) key fingerprint is dd:b5:2b:07:ad:c0:30:b2:d5:6a:6a:78:80:85:93:b0
Do you wish to continue? [y/N]y
Username: user-xyz
Password:
Syslog Certificate uploaded successfully
Server /cimc/log/server # set secure-enabled yes
Server /cimc/log/server # commit
Server /cimc/log/server #
```

- この例では、貼り付けオプションを使用してリモート Syslog 証明書をアップロードします。

```
Server # scope cimc
Server /cimc # scope log
Server /cimc/log # scope server
Server /cimc/log/server # paste-certificate
Please paste your certificate here, when finished, press CTRL+D.
-----BEGIN CERTIFICATE-----
MIIFUDCCBDigAwIBAgIKYRF49gAAAAAAAjANBgkqhkiG9w0BAQUFADBLMRMwEQYK
CZImiZPyLGQBGRYDY29tMRMwEQYKCZImiZPyLGQBGRYDbmV3MR8wHQYDVQQDExZu
ZXctV0lOLU9WQlNBNElFU0NBLUNBMB4XDTE3MDczMDIxNTA1NVoXDTE5MDczMDIy
MDA1NVowSzETMBEGCgmSJomT8ixkARkWA2NvbTETMBEGCgmSJomT8ixkARkWA25l
dzEfMB0GA1UEAxMWbmV3LVdJTi1PVkJTQTRJRUJDQS1DQTCCASIwDQYJKoZIhvcN
AQEBBQADggEPADCCAQoCggEBALd8c+hhJddfUH6XKqBvllZVtIAiHfCx+l7z9o7F
bELOWu0LDVSC9pC1zpJ9wykr6VqUsVhZTkqQan23+84X4lYBsd92shQp9bri2gKj
MGntmnXE6qP3b6Trw94j6JVyWXKImYEda/SFtx722orLap8Sdliurue62JGNfq56
vxXBT1SNUHOmgOdfTOeNjVyeh51jceOCdKTppBij4wuq+jJfkndhW7KKE7ubmyRv
xpRSkiVaqNypf8jv7uG8Kwx1Q8jbCr0wG4nAbPndwhkyJpgyA5zuCdMRU2cN47om
u0VfMzJeVu+HuAif25BqKn4cjwHGOnrWKZcfHtnpKEbbmv0CAwEAAaOCAjQwggIw
MBAGCSsGAQQBgjcVAQQDAgEAMB0GA1UdDgQWBBR2+YJQuCmHKCkBkqVim0/kvfzB
bTAZBgkrBgEEAYI3FAIEDB4KAFMAdQBiAEMAQTAOBgNVHQ8BAf8EBAMCAYYwDwYD
VR0TAQH/BAUwAwEB/zAfBgNVHSMEGDAWgBRo6OQnLNNVa71VtllYAVRPmw8LQjCB
2AYDVR0fBIHQMIHNMIHKoIHHoIHEhoHBbGRhcDovLy9DTj1uZXctV0lOLU9WQlNB
NElFU0NBLUNBLENOPVdJTi1PVkJTQTRJRVNDQSxDTj1DRFAsQ049UHVibGljJTIw
S2V5JTIwU2VydmljZXMsQ049U2VydmljZXMsQ049Q29uZmlndXJhdGlvbixEQz1u
ZXcsREM9Y29tP2NlcnRpZmljYXRlUmV2b2NhdGlvbkxpc3Q/YmFzZT9vYmplY3RD
bGFzcz1jUkxEaXN0cmlidXRpb25Qb2ludDCBxAYIKwYBBQUHAQEEgbcwgbQwgbEG
CCsGAQUFBzAChoGkbGRhcDovLy9DTj1uZXctV0lOLU9WQlNBNElFU0NBLUNBLENO
```

```
PUFJQSxDTj1QdWJsaWMlMjBLZXklMjBTZXJ2aWNlcyxDTj1TZXJ2aWNlcyxDTj1D
b25maWd1cmF0aW9uLERDPW5ldyxEQz1jb20/Y0FDZXJ0aWZpY2F0ZT9iYXNlP29i
amVjdENsYXNzPWNlcnRpZmljYXRpb25BdXRob3JpdHkwDQYJKoZIhvcNAQEFBQAD
ggEBAE8IWaRFEqrrwMHNaJunoomON2rdBWRNAMlJhKdIzi49J/9Yy9IlOGF+l0wR
Q5TeKFYIcWxBj5ltlYVWVdB+9YtTKsoEoq7/MeSg/c5KuprJhugqN3OU6zCqU4vq
rS1UHNnYkOJiSdOjkOdNeT9EG2YUqiDPr6CqIUcdU4+e36LdtQZW0TlIko+0z/be
bwIgtmxzkhlyDU711SuKmyz3uRrKq1CWhiIhSaOq4yYFQ0iw6TmFFKJGZ1KnjOrA
AwHhf8QvBBJhPMOwncWGL6DLFb7md2lE2YBu+zcVPGLdXYm0Xgk8lXsE22bRJYJU
gyHqA2enmHAmJequlUFoSH9apKU=
-----END CERTIFICATE-----
Syslog Certificate pasted successfully.
Server /cimc/log/server #
```

- この例では、リモート Syslog 証明書がサーバーに存在し、セキュアなリモート sylog がサーバーで有効になっていることが表示されます。

```
Server # scope cimc
Server /cimc # scope log
Server /cimc/log # scope server
Server /cimc/log/server # show detail
    Syslog Server 1:
    Syslog Server Address: 10.10.10.10
    Syslog Server Port: 514
    Enabled: yes
    Secure Enabled: yes
    Syslog Server protocol: udp
    Certificate Exists: yes
Server /cimc/log/server #
```

リモート Syslog 証明書の削除

始める前に

admin 権限を持つユーザとしてログインする必要があります。

手順

ステップ 1 Server # **scope cimc**

Cisco IMC コマンドモードを開始します。

ステップ 2 Server /cimc # **scope log**

Cisco IMC ログ コマンドモードを開始します。

ステップ 3 Server /cimc/log # **scope server{1|2}**

2つのリモート Syslog サーバープロファイルのいずれかを選択し、選択したサーバーのリモート Syslog 証明書を削除するためのコマンド モードを開始します。

ステップ 4 Server /cimc/log/server # **show detail**

サーバーの詳細を表示し、選択したサーバーにリモート Syslog 証明書が存在することを確認します。

ステップ 5 Server /cimc/log/server # **delete-client-certificate**

確認プロンプトで y と入力して、選択したサーバーからリモート Syslog 証明書を削除します。

ステップ 6 Server /cimc/log/server # **show detail**

サーバーの詳細を表示し、選択したサーバーでリモート Syslog 証明書が使用できないことを確認します。

例

- この例では、サーバー上にリモート Syslog 証明書が存在することが表示されます。

```
Server # scope cimc
Server /cimc # scope log
Server /cimc/log # scope server
Server /cimc/log/server # show detail
Server /cimc/log/server # commit
    Syslog Server 1:
    Syslog Server Address: 10.10.10.10
    Syslog Server Port: 514
    Enabled: yes
    Secure Enabled: yes
    Syslog Server protocol: udp
    Certificate Exists: yes
Server /cimc/log/server #
```

- この例では、サーバー上のリモート Syslog 証明書を削除します。

```
Server # scope cimc
Server /cimc # scope log
Server /cimc/log # scope server
Server /cimc/log/server # show detail
    Syslog Server 1:
    Syslog Server Address: 10.10.10.10
    Syslog Server Port: 514
    Enabled: yes
    Secure Enabled: yes
    Syslog Server protocol: udp
    Certificate Exists: yes
Server /cimc/log/server # delete-client-certificate
You are going to delete the Syslog Certificate.
Are you sure you want to proceed and delete the Syslog Certificate? [y|N]y
Syslog Certificate deleted successfully
Server /cimc/log/server #
```

システム イベント ログ

システム イベント ログの表示

手順

	コマンドまたはアクション	目的
ステップ 1	Server# **scope sel**	システム イベント ログ（SEL）コマンド モードを開始します。
ステップ 2	Server /sel # **show entries** [**detail**]	システム イベントについて、タイムスタンプ、イベントのシビラティ（重大度）、およびイベントの説明を表示します。 **detail** キーワードを指定すると、表形式ではなくリスト形式で情報が表示されます。

例

次に、システム イベント ログを表示する例を示します。

```
Server# scope sel
Server /sel # show entries
Time                 Severity      Description
-------------------- ------------- ----------------------------------------
[System Boot]        Informational " LED_PSU_STATUS: Platform sensor, OFF event was
asserted"
[System Boot]       Informational " LED_HLTH_STATUS: Platform sensor, GREEN was asserted"

[System Boot]       Normal        " PSU_REDUNDANCY: PS Redundancy sensor, Fully Redundant
 was asserted"
[System Boot]       Normal        " PSU2 PSU2_STATUS: Power Supply sensor for PSU2, Power
 Supply input lost (AC/DC) was deasserted"
[System Boot]       Informational " LED_PSU_STATUS: Platform sensor, ON event was asserted"

[System Boot]       Informational " LED_HLTH_STATUS: Platform sensor, AMBER was asserted"

[System Boot]        Critical      " PSU_REDUNDANCY: PS Redundancy sensor, Redundancy
Lost was asserted"
[System Boot]       Critical      " PSU2 PSU2_STATUS: Power Supply sensor for PSU2, Power
 Supply input lost (AC/DC) was asserted"
[System Boot]        Normal        " HDD_01_STATUS: Drive Slot sensor, Drive Presence was
 asserted"
[System Boot]       Critical      " HDD_01_STATUS: Drive Slot sensor, Drive Presence was
 deasserted"
[System Boot]       Informational " DDR3_P2_D1_INFO: Memory sensor, OFF event was asserted"

2001-01-01 08:30:16 Warning       " PSU2 PSU2_VOUT: Voltage sensor for PSU2, failure
event was deasserted"
2001-01-01 08:30:16 Critical      " PSU2 PSU2_VOUT: Voltage sensor for PSU2,
non-recoverable event was deasserted"
```

```
2001-01-01 08:30:15 Informational " LED_PSU_STATUS: Platform sensor, ON event was asserted"

2001-01-01 08:30:15 Informational " LED_HLTH_STATUS: Platform sensor, AMBER was asserted"

2001-01-01 08:30:15 Informational " LED_HLTH_STATUS: Platform sensor, FAST BLINK event
was asserted"
2001-01-01 08:30:14 Non-Recoverable " PSU2 PSU2_VOUT: Voltage sensor for PSU2,
non-recoverable event was asserted"
2001-01-01 08:30:14 Critical      " PSU2 PSU2_VOUT: Voltage sensor for PSU2, failure
event was asserted"
--More--
```

システム イベント ログのクリア

手順

	コマンドまたはアクション	目的
ステップ 1	Server# **scope sel**	システム イベント ログ コマンド モードを開始します。
ステップ 2	Server /sel # **clear**	処理の確認を求めるプロンプトが表示されます。プロンプトに**y**と入力すると、システム イベント ログはクリアされます。

例

次に、システム イベント ログをクリアする例を示します。

```
Server# scope sel
Server /sel # clear
This operation will clear the whole sel.
Continue?[y|N]y
```

翻訳について
このドキュメントは、米国シスコ発行ドキュメントの参考和訳です。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動/変更されている場合がありますことをご了承ください。あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。