

Express5800/R120h-1E, R120h-2E ご使用時の注意事項

このたびは弊社製品をお買い上げいただき、誠にありがとうございます。

本製品のご使用において、ご注意いただくことがあります。誠におそれ入りますが、ご使用前に下記内容を必ずご一読ください。

なお、本書は必要ときにすぐに参照できるよう大切に保管してください。

- 1) はじめに
- 2) システムROMの機能に関する注意事項
- 3) iLO 5の機能に関する注意事項
- 4) OSに関する注意事項
- 5) 全般の機能に関わる注意事項
- A) ファームウェア変更に伴う変更点
- B) 誤記訂正

1) はじめに

● 本製品のマニュアルについて

本製品に関する詳細は、以下の Web サイトに掲載しているマニュアルに記載しています。

<https://www.support.nec.co.jp/>

「NEC サポートポータル内検索」より、以下の ID で検索してください。

R120h-1E : 3170101982

R120h-2E : 3170101983

また、ESMPRO/ServerManager、ESMPRO/ServerAgentService、エクスプレス通報サービス/エクスプレス通報サービス (HTTPS)/エクスプレス通報サービス (MG) に関しては、

ESMPRO 日本語ポータルサイト<<https://jpn.nec.com/esmsm/>>

NEC サポートポータル<<https://www.support.nec.co.jp/View.aspx?id=9010102124>>

の最新の情報およびバージョンをご確認のうえ、ご利用ください。

● Starter Packについて

本製品で使用する Starter Pack は、以下の Web サイトに最新版が掲載されています。

Web サイトに掲載されている内容を確認し、バージョン S8.10-007.02 以上を適用してください。

<https://www.support.nec.co.jp/>

(「NEC サポートポータル内検索」より、「S8.10-007」を検索)

● VMware ESXi のドライバ・サービスモジュールについて

本製品で使用する VMware ESXi のドライバ・サービスモジュールは、以下の Web サイトに最新版が掲載されています。Web サイトに掲載されている内容を確認し、適切なバージョンを適用してください。

- (1) Agentless Management Service および iLO Channel Interface Driver

<https://www.support.nec.co.jp/>

(「NEC サポートポータル内検索」より、「Agentless Management Service」を検索し、【最新版】と表示される「Agentless Management Service および iLO Channel Interface Driver (VMware ESXi 6.x 版(x=0, 5 または 7), 7.0/8.0 版)」を適用してください)

- (2) WBEM プロバイダおよび CLI ツール

<https://www.support.nec.co.jp/>

(「NEC サポートポータル内検索」より、「WBEM プロバイダ」を検索し、「【最新版】WBEM プロバイダおよび CLI ツール (VMware ESXi 6.x 版(x=0, 5 または 7), 7.0 版)」を適用してください)

- (3) VMware ESXi デバイスドライバ

<https://www.support.nec.co.jp/View.aspx?id=3140105866>

(「PC サーバ/ブレードサーバ (Express5800 シリーズ)」から対象 OS の「デバイスドライバー一覧」を選択)

● 本製品の保守作業時間に関して

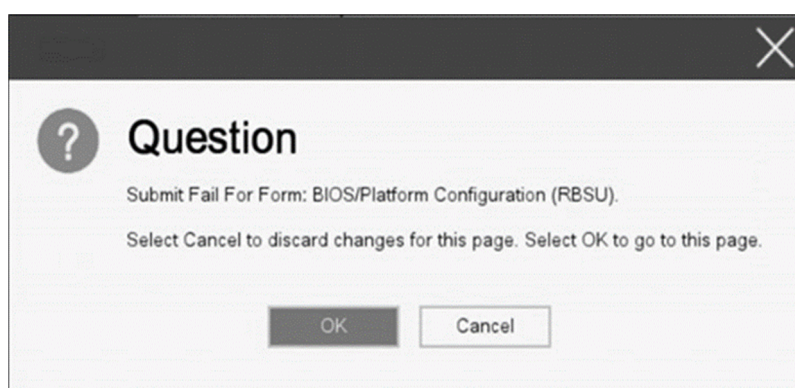
本製品は、障害発生時等に伴う保守作業に際し、保守部材と搭載ファームウェア、ドライバの組み合わせによっては、保守作業に時間を要することがあります。

2) システムROMの機能に関する注意事項

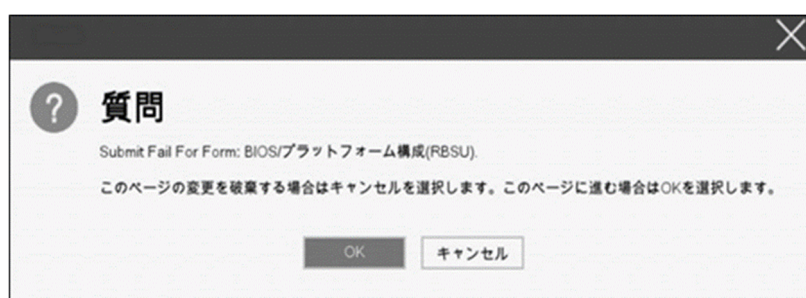
● Submit Fail For FormのQuestion(質問)ポップアップ表示についての注意事項

システムユーティリティにおいて設定の変更中に、次のSubmit Fail For FormのQuestion(質問)ポップアップが表示された場合は、「キャンセル」を選択して変更を破棄してください。

さらに、サーバーの再起動を行ってシステムユーティリティに入りなおしてから設定の変更を再度行ってください。もし「OK」を押してそのまま設定変更を進めると、装置に記録されているSerial Number、Product IDなどの設定情報を消失することがあります。



英語表示の場合



日本語表示の場合

● 「Memory Initialization Start」のメッセージでPOST停止した場合の対処について

「Memory Initialization Start」のメッセージでPOST停止した場合、システムメンテナンススイッチのSW6によりシステム設定をデフォルト値に戻すことで復旧することができます。

詳細な手順は、メンテナンスガイド「1章(7.3.3 システム設定をデフォルト値に戻す)」の項をご参照ください。

● シリアルコンソールにPOSTデバッグ情報が出力される件について

システム ROM v2.32 (03/09/2020)において、POST 実行時、まれに POST デバッグ情報がシリアルポートに出力され、POST 実行時間がおおよそ2分長くなることがあります。

システム ROM v2.34 (04/09/2020)では、この問題が修正されています。

● Extended Memory Testオプションの設定値について

システム ROM のバージョンがv2.36 (07/16/2020)の場合、Extended Memory Test オプションは、自動的に Disabled となります。

System Configuration > BIOS/Platform Configuration (RBSU) > Memory Options > Extended Memory Test

● Server Configuration Lock (SCL) についての注意事項

- (1) システム運用中は SCL 機能を無効にし、使用しないでください。
- (2) SCL 機能有効時に設定するパスワードは大切に保管してください。SCL のパスワードを紛失した状態で、SCL 機能によりロック (OS ブート前に停止) されると、ロック解除できず、二度とブートできなくなります。

ブート可能状態への復旧/回復は有償にて承ることになります。

なお、SCL のパスワードを紛失した場合、SCL のパスワードをクリアする方法はありません。

- (3) 保守を依頼する際は、SCL 機能を無効化していただく必要があります。
SCL 機能を無効にできない場合、保守は有償にて承ることになります。
- (4) RBSU の「Halt on Server Configuration Lock failure detection.」機能は有効化しないでください。もし有効に設定した場合、SCL 機能が回復不能条件の該当を検出し、ロック (OS ブート前に停止) されてしまうと、システムユーティリティも起動できず、二度とサーバー構成ロックを無効にすることができません。

ブート可能状態への復旧/回復は有償にて承ることになります。

SCL 機能の回復不能条件

- RBSU の設定変更によりロックされた場合
- ファームウェア更新によりロックされ、元のファームウェア バージョンに戻すことができない場合
- DIMM、または PCI オプションカードの故障によりロックされた場合

● RESTful インターフェースツールによる RBSU 設定のバックアップ (保存) とリストア (復元) の注意事項

iLO5 ファームウェアバージョン 2.40 以上の場合、RESTful インターフェースツールを使用した RBSU 設定の保存と復元は使用できません。

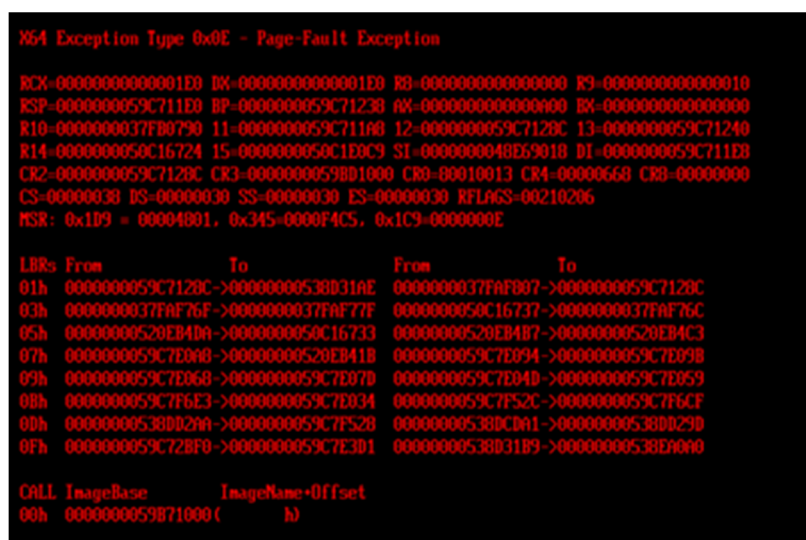
RBSU 設定の保存と復元は、システムユーティリティの Backup and Restore Settings メニューから行ってください (メンテナンスガイド (共通編) の「システムユーティリティの RBSU 設定の保存と復元」を参照)。

● 赤文字画面 (RSOD : Red Screen of Death) が表示された場合の対処について

装置の構成変更や設定変更などシステムの状態を変更した場合や、接続デバイスへのアクセスタイミングにより、OS 起動前に稀に赤文字画面 (RSOD) が表示され、本製品の操作が出来なくなることがあります。構成変更や設定変更に伴う一過性の事象の場合があり電源 OFF/ON によって回復します。

赤文字画面 (RSOD) が表示された場合、装置の電源 OFF/ON をお願いします。

問題が解決しないときは、ファーストコンタクトセンターにお問い合わせください。



赤文字画面の例

● フォールトトレラントメモリ機能 (ADDDC) の仕様変更について

本製品の搭載ファームウェアの更新に伴い、フォールトトレラントメモリ機能 (ADDDC) の仕様に変更があります。下記、変更点を記載します。

- システムROMのバージョンがv2.00 (02/02/2019)以降、CPUあたりDIMM 8枚、もしくはDIMM 12枚以外の構成であっても、フォールトトレラントメモリ機能 (ADDDC) が使用できる構成であれば、本機は自動的に設定が変更し、同機能の使用を始めます。
- システムROMのバージョンがv2.10 (05/21/2019)以降、各チャネルあたりのRANK数の合計が2以上になるようにメモリを搭載しなくても、フォールトトレラントメモリ機能 (ADDDC) は利用できます。
- システムROMのバージョンがv2.10 (05/21/2019)以降、フォールトトレラントメモリ機能 (ADDDC) が使用可能なDIMMとして、N8102-709が加わります。

● SW RAID有効時、内蔵DVDドライブ (N8151-137/138) が2個表示される件について

システムROMバージョンがv2.00 (02/02/2019)以降、v2.32 (03/09/2020)未満の場合、Embedded SATA Configuration設定(*1)を[Smart Array SW RAID Support]設定時、運用環境によりDisk Utilitiesメニュー(*2)に内蔵DVDドライブ情報が2個表示されます。

どちらのドライブを選択した場合でも同じ内蔵DVDドライブの情報が参照できます。

(*1) 「System Configuration > BIOS/Platform Configuration (RBSU) > Storage Options > SATA Controller Options > Embedded SATA Configuration」

(*2) 「System Configuration > HPE Smart Array S100i SR Gen10 > Disk Utilities」

● 工場出荷時の設定について

以下の項目については、工場出荷時に以下のように設定しています。

- (1) System Configuration > BIOS/Platform Configuration (RBSU) > Workload Profileを「Custom」に設定。
- (2) System Configuration > BIOS/Platform Configuration (RBSU) > Power and Performance Options > Minimum Processor Idle Power Core C-Stateを「No C-states」に設定。
- (3) System Configuration > BIOS/Platform Configuration (RBSU) > Power and Performance Options > Minimum Processor Idle Power Package C-Stateを「No Package States」に設定。

● iLOイベントログ (IEL) にIPMI Watchdog Timer Timeoutのログが登録される。

システムROM v2.62 (03/08/2022)が適用されている場合、かつIPMI Watchdog Timerオプションを「Disabled(出荷時の設定)」に設定している場合、iLOイベントログに下記のIPMI Watchdog Timer Timeoutが登録されることがあります。

以下の手順を実施することで本問題が解消します。

iLO IPMI Watchdog Timer Timeout: Action: None, TimerUse: 0x44, TimerActions: 0x00

イベントクラス: 0x23

イベントコード: 0xB3

復旧手順:

以下の復旧手順1、または2のどちらかを実施していただくことで、本問題が解消できます。

復旧手順1

- (1) 装置の電源を切り、電源コードをコンセントから外す。
- (2) 30秒以上経過したのち、電源コードをコンセントに接続する。

復旧手順2

システムユーティリティより、IPMI Watchdog Timerオプションの設定を2回変更します。

- (1) POST中に<F9>キーを押下し、システムユーティリティを起動する。
- (2) System Configuration > BIOS/Platform Configuration (RBSU) > System Options > Server Availability > IPMI Watchdog Timerオプションを「Enabled」に設定する。
- (3) <F12>キーを押下し、設定を保存してシステムを再起動する。
- (4) POST中に<F9>キーを押下し、システムユーティリティを起動する。
- (5) System Configuration > BIOS/Platform Configuration (RBSU) > System Options > Server Availability > IPMI Watchdog Timerオプションを「Disabled」に設定する。
- (6) <F12>キーを押下し、設定を保存してシステム再起動する。

● システムユーティリティおよびワнтаイムブートメニューの表示について

- (1) BMC Configuration Utility 配下のメニューの変更権限については、BMC Configuration Utility > Setting Option > Require user login and configuration privilege for BMC Configuration を有効にすることで保護してください。
BIOS/Platform configuration (RBSU) > Server Security > Set Admin Password の設定では保護されません。
- (2) System Information > Processor Information で表示される L2 Cache、L3 Cache の Maximum Size、Installed Size は 1MB を 1024000 バイトに換算した数値で表示されます。
システム ROM のバージョンが v2.00 (02/02/2019) 以降の場合は、1MB を 1048576 バイトに換算した数値で表示されます。
- (3) システム ROM バージョンが v1.36 (02/14/2018)、または v1.36 (02/15/2018) の場合、システムユーティリティ、またはワнтаイムブートメニューを表示したとき、まれにマウスカーソルが黒い四角形の表示となることがあります。
これは、表示のみの問題であり、システムユーティリティ上の操作は正常に機能します。
また、この状態はマウスを操作することで解消します。
- (4) 以下の発生条件を満たす場合、ワнтаイムブートメニューと RBSU の PCIe Device Configuration メニュー(*)に、RAID コントローラ名が正しく表示されないことがあります。RAID コントローラ名表示のみの問題であり、RAID コントローラに搭載されている HDD/SSD からのブートには影響しません。
(*) BIOS/Platform configuration (RBSU) > PCIe Device Configuration

【発生条件】

- ・ N8103-189、N8103-190、N8103-191、N8103-192、N8103-193、N8103-194、N8103-195、N8103-196、N8103-197、N8103-201、N8103-237、N8103-238 の場合
以下 2 つの条件をすべて満たす場合、発生します。
 1. RAID コントローラファームウェアが v4.11 以上、または v3.01.04.072 以上
 2. システム ROM が v2.68 (07/14/2022) 未満

● PCIe Slot X MCTP Broadcast Support メニューについて (X は PCIe Slot 番号)

システム ROM バージョンが v2.10 (05/21/2019) 以降の装置において、初めて PCIe MCTP Options メニュー(*)を選択した場合、装置のデフォルト設定を強制的に設定する旨のポップアップ(*)が、設定可能な PCIe Slot 数分表示されます。

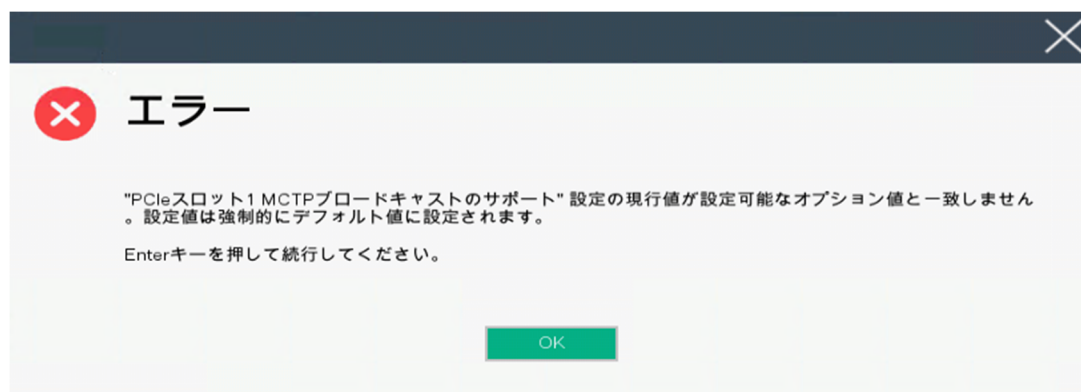
設定を一度保存すると、次回以降ポップアップ表示はされません。

なお、下記システム ROM バージョンの場合、設定保存時にポップアップ(*)が表示され設定は保存されません。保存されないことにより、本メニューを表示させるたびに PCIe Slot 数分のポップアップ(*)が表示されることになります。この場合、MCTP Broadcast は常に有効で動作します。

- ・ v2.22 (11/13/2019)
- ・ v2.32 (03/09/2020)

*1 : System Configuration > BIOS/Platform Configuration (RBSU) > PCIe Device Configuration > Advanced PCIe Configuration > PCIe MCTP Options

*2 :



*3 :



● ネットワークPXEブートでサーバーの操作が出来なくなることがある

システムROM v3.10 (02/22/2024) 未満の場合、ネットワークPXEブートによるOS起動中に、まれに本製品が応答しなくなることがあります。

この問題が発生した場合、以下a)、b)、いずれかの手順を実施し、本製品を再起動してください。

- a) 電源ボタンを長押しして本製品の電源をオフにし、その後、電源ボタンの押下により本製品の電源をオンにしてください。
- b) iLO Webインターフェースから「電源」-「押し続ける」を選択して本製品の電源をオフにし、その後、「電源」-「瞬間的に押す」を選択して本製品の電源をオンにしてください。

システムROMバージョン3.10 (02/22/2024) では、この問題が修正されています。

3) iLO 5の機能に関する注意事項

● iLOの再起動を行う場合の注意事項

サーバー起動からOSの起動完了までの間(POST (Power On Self Test)実行中も含みます)は、iLOの再起動を行わないでください。

また、システムユーティリティの操作途中も、iLOの再起動を行わないでください。

該当タイミングでiLOの再起動を行うと、期待しない動作となる場合があります。

たとえばシステムユーティリティの設定変更途中にiLOの再起動(※)を行うと、直後のシステム再起動処理(Reboot)が正常に動作しない場合や、装置に記録されているSerial Number、Product IDなどの設定情報を消失することがあります。また、POST (Power On Self Test)実行中にiLOの再起動を行うと、iLO Webインターフェース: [Information] - [Overview]ページにおけるUUID、UUID(論理)が不正な表示になる場合があります。不正な表示となった場合は、本体装置の電源をオフ、オンしてください。

＜対象となるiLOの再起動の方法＞

- iLO Webインターフェースなどを利用したネットワーク経由でのiLOの再起動。
- UIDスイッチを使用したiLOの再起動。

※ システムユーティリティの「BMC Configuration Utility」での設定変更後のiLOの再起動については、本書の「システムユーティリティの「BMC Configuration Utility」の操作についての注意事項」を参照して操作してください。

● iLOのダウングレードポリシー機能の注意事項

iLO 5ファームウェア1.40以降でiLOの拡張ライセンスがインストールされている場合、[Security] - [Access Settings] - [Update Service] - [Downgrade Policy]の設定を『Permanently disallow downgrades』に変更しないでください。

『Permanently disallow downgrades』に設定した場合、ファームウェアのダウングレードを行うことができなくなります。また、iLOに対して永続的な変更が行われるため、『Permanently disallow downgrades』に設定後は、iLOの各種インターフェースや各種ユーティリティから本設定の変更を行おうとしても変更することができません。

なお、本設定はSet to factory defaultsオプションからiLOを出荷時のデフォルト設定にリセットを行った場合においても、リセットされず『Permanently disallow downgrades』を維持します。

● iLOのセキュリティ機能の注意事項

iLO 5ファームウェア1.40以上をご使用の場合、iLO Webインターフェースの[Information] - [Security Dashboard] およびiLO Webインターフェース画面の右上部に  リスクが表示される場合があります。
RBSUの設定やiLOの設定の内容によって、iLOセキュリティの状態がリスク状態(赤色)で表示されますので、お客様のセキュアポリシーに応じてセキュリティの対処を行ってください。

推奨値などの詳細については、iLO 5ユーザーズガイドを参照してください。

ただし、『Require Host Authentication』設定については、本書内の「システムユーティリティより、Admin Passwordを設定(※1)した場合や、iLO Webインターフェースから、[ホスト認証が必要]設定を有効(※2)に設定した場合の注意事項」に記載がありますので、ご確認ください。

iLO 5ファームウェアのバージョンによって該当する条件が異なります。

iLO 5ファームウェア	該当条件
バージョン 1.40	(※1)、および(※2)
バージョン 1.43以上	(※2)

iLOの負荷の状態により[Information] - [Security Dashboard]の”全体セキュリティステータス”が『リスク』であっても、iLO Webインターフェース画面の右上部の”iLOセキュリティ”アイコンが無色になる場合があります。[Information] - [Security Dashboard]の”全体セキュリティステータス”が現在のセキュリティ状態を示します。

● システムユーティリティより、Admin Passwordを設定(※1)した場合や、iLO Webインターフェースから、[ホスト認証が必要]設定を有効(※2)に設定した場合の注意事項

(※1) iLO 5ファームウェアバージョン：1.43未満を適用した環境の場合が対象となります。

[System Configuration] - [BIOS/Platform Configuration (RBSU)] - [Server Security]より、Set Admin Password オプションにてパスワードを設定する。

(※2) iLO ファームウェアバージョン：1.40以上を適用した環境の場合が対象となります。

[Security] - [Access Setting] - [iLO]にある[ホスト認証が必要/Require Host Authentication]を『有効』にしないでください。

設定を行った場合、次に示す状況が発生します。

- ・アラートビューアに、“Remote Insight/Integrated Lights-Out 認証されないログイン試行検出”のメッセージが多数表示されます。
- ・Starter Pack (Standard Program Package)を適用するとエラーが発生します。

また、次のサービスや機能をご利用頂けません。

- ・エクスプレス通報サービスにおいてハードウェア障害に関する通報
- ・RAID 通報サービス
- ・サーバ診断カルテのハードウェア診断機能
- ・iLO が収集するハードウェアに関するデバイス情報や設定情報の参照、およびイベントログ採取機能

● iLOの時刻についての注意事項

iLO 5ファームウェア1.45以下でiLOのSNTPの設定が無効の場合、iLOの再起動を行うとiLOの時刻がずれてしまう場合があります。

iLO WebインターフェースにてSNTPの設定を行い、ご使用いただくことを推奨します。

iLOのSNTPの設定方法については、iLO 5ユーザーズガイドを参照してください。

● ネットワークブリッジ構成時のiLO Webインターフェースのネットワーク情報の表示について

ネットワークをブリッジ設定で構成し、iLO 5ファームウェア：2.31以上をご使用の場合、iLO Webインターフェースの[Information] - [Network] - [Physical Network Adapters]に表示される内容がOS上の内容と一致しない場合があります。ブリッジ情報の詳細は、OS上のネットワークアダプタのプロパティにてご確認ください。

● iLO Webインターフェイスのストレージ情報に関する注意事項について

iLO5ファームウェア 3.00以降をご使用の場合:

サーバー再起動後に、iLO 5 Webインターフェイスで [システム情報]-[ストレージ] タブをクリックすると、以下のメッセージが表示され、RAIDコントローラやドライブ情報等のストレージ情報が表示されない場合があります。

“Failed to retrieve complete storage device information. Refresh the page in a few minutes.”

上記メッセージがストレージ情報ページに表示された場合、iLOリセットを行ってください。

● iLO WebインターフェイスのUUID不正値表示について

POST (Power On Self Test) 実行中にiLOの再起動を行うと、iLO Webインターフェイスの[Information] - [Overview] ページのUUID、UUID(論理)の値が稀に不正な表示となることがあります。

不正な表示となった場合は、本体装置の電源をオフ、オンしてください。

● iLO Webインターフェイスのネットワーク情報の表示について

ファイバーチャネルコントローラーが実装されているシステムで、iLO Webインターフェイスの言語に日本語が選択されている場合、[システム情報] - [ネットワーク] で表示されるファイバーチャネルコントローラーの“ポートのステータス”が『下へ』と表示されます。

これはファイバーチャネルコントローラーの接続が『ダウン』の状態であることを示しますので、読み替えてご利用ください。

● iLO WebインターフェイスのVirtual NIC設定の注意事項

[Security] - [iLO] の“Virtual NIC”のデフォルト値は、iLO5ファームウェアのバージョンにより異なります。BMC構成ユーティリティにて“工場出荷時のデフォルトにセット”を実施した場合は、以下をご確認ください。

- (1) iLO 5ファームウェア : 2.10以上 2.18以下をご使用の場合、デフォルト値は『有効(Enabled)』です。
仮想NICをサポートしていないWindows Server 2012 R2やUSB CDC-EEMドライバがインストールされていないWindows Server 2016/2019/2022上のデバイスマネージャーで「Virtual NIC」が警告表示される場合があります。
[Security] - [iLO] の“Virtual NIC”の設定を『無効(Disabled)』に変更してください。
- (2) iLO 5ファームウェア : 1.40以上 1.47以下、もしくは、2.31以上をご使用の場合、デフォルト値は『無効(Disabled)』です。

● Windows上でのvEthernet (Hyper-V Virtual Ethernet Adapter) 構成時のiLO WebインターフェイスのネットワークアダプタのIPv6アドレス表示に関する注意事項

iLO 5ファームウェア : 2.10以上 2.18以下をご使用の場合、Windows OS上でvEthernet (Hyper-V Virtual Ethernet Adapter) が構成されている場合、iLO Webインターフェイスの[Information] - [Network] - [Physical Network Adapters] において、構成されている各[Adapter]の[Network Ports]の“IPv6 Address”において正しいIPv6アドレスが表示されない場合があります。vEthernet構成時のIPv6アドレスに関しては、OS上のネットワークアダプタのプロパティにてご確認ください。

● 物理ドライブのステータス変更時のSNMPトラップ通知のロケーション情報欠損に関する対処について

物理ドライブのステータス変更時のSNMPトラップ通知において、ロケーション情報が欠損する場合があります。ロケーション情報に関しては、iLO5 webインターフェイスの[情報]-[インテグレートドマネジメントログ]で同じイベントのロケーション情報をご確認ください。

例:

Abnormal, physical drive status change detection, iLO SNMP Trap, mgr_WIN-U6HIHPNIH1Q, uru-rhel83, 192.168.0.57, , 2021/10/01 15:22:57, iLO, 0xc0000be6, “A physical drive status change has been detected. Current status is 3. (Location: ot 12 Controller: Slot 12)”, “If the physical drive status is 'failed(3)', 'predictiveFailure(4)',

● iLO WebインターフェースのDevice Inventory情報の表示について

＜R120h-1E LOMカード (N8104-193/194/195) 構成時＞

システムROMのバージョン2.34 (04/08/2020) 以下をご使用の場合、iLO Webインターフェースの[Information] - [Device Inventory]において、LOMカードの表示情報が以下のように表示される場合がありますが、サーバの運用およびLOMカードの動作に影響はありません。

- Location : Unspecified
- Firmware Version : N/A
- Status : Unknown

＜SASエクスパンダカード (N8116-84) 構成時＞

iLO 5ファームウェア:2.31以上をご使用の場合、iLO Webインターフェースの[Information] - [Device Inventory]において、SASエクスパンダカードの表示情報が以下のように表示される場合がありますが、サーバの運用およびSASエクスパンダカードの動作に影響はありません。

- Firmware Version : N/A
- Status : Disabled

● iLO Webインターフェースのセキュリティダッシュボードの注意事項

iLO 5ファームウェア1.43以上、2.10未満をご使用の場合、[Information] - [Security Dashboard]に[Last Firmware Scan Result]が表示されますが、本ハイパーリンクをクリックしないでください。

誤ってクリックした場合、Webサイト内のメニュー間移動が出来なくなります。その場合、ブラウザのリロードボタンをクリックするか、もしくはいったんiLO Webインターフェースのログアウトを実行して再度ログインしてください。

情報 - セキュリティダッシュボード

概要

セキュリティダッシュボード

セッションリスト

iLOイベントログ

インテグレートドマネジメントログ

Active Health Systemログ 診断

全体セキュリティステータス: OK

セキュリティ状態	本番環境	サーバー構成ロック	Disabled
セキュリティパラメーター	↓ステータス	状態	無視
セキュリティオーバーライドスイッチ	OK	Off	☐
IPMI/DCMI over LAN	OK	無効	☐
最小パスワード長	OK	OK	☐
iLO RBSUへのログイン要求	OK	有効	☐
認証失敗ログ	OK	有効	☐
セキュアブート	OK	有効	☐
パスワードの複雑さ	OK	有効	☐
ホスト認証が必要	OK	無効	☐
最新のファームウェアスキャン結果	OK	OK	☐

日本語表示の場合

Information - Security Dashboard			
Overview Security Dashboard Session List iLO Event Log Integrated Management Log Active Health System Log Diagnostics			
Overall Security Status : OK			
Security State Production Server Configuration Lock: Disabled			
Security Parameter	↓ Status	State	Ignore
Security Override Switch	♥ OK	Off	☐
IPMI/DCMI Over LAN	♥ OK	Disabled	☐
Minimum Password Length	♥ OK	OK	☐
Require Login for iLO RBSU	♥ OK	Enabled	☐
Authentication Failure Logging	♥ OK	Enabled	☐
Secure Boot	♥ OK	Enabled	☐
Password Complexity	♥ OK	Enabled	☐
Require Host Authentication	♥ OK	Disabled	☐
Last Firmware Scan Result	♥ OK	OK	☐

英語表示の場合

● iLO WebインターフェースのAgentless Management Service (AMS)のステータスについて

iLO Webインターフェースの[System Information] - [Summary] - [Subsystem and Devices]のAgentless Management Service (AMS)のステータスにおいて、不明(または利用不可能)※と表示された場合、iLOリセットを行ってください。また、その後、10分程度経過した後、以下のAgentless Management Service (AMS)の再起動方法の対象OSを参考に、Agentless Management Service (AMS)を再起動してください。

※ Agentless Management Service (AMS)のステータスが不明(または利用不可能)の状態の場合、iLO Webインターフェースの[System Information] - [Storage] や [Network]の一部の情報が取得できず、正しく表示されません。

< Agentless Management Service (AMS)の再起動方法 >

○ Windowsの場合

Windowsの管理ツール → サービス → “Agentless Management Service” を右クリックし、再起動してください。

○ Red Hat Enterprise Linux 7.x/8.xの場合

以下のコマンドを実行します。

```
# systemctl restart smad
# systemctl restart amsd
```

○ ESXi6.5/6.7の場合

以下のコマンドを実行します。

```
# /etc/init.d/amsd.sh restart
もしくは
# /etc/init.d/ams.sh restart
```

※ お使いのAMSバージョンによりコマンドが異なります。

○ ESXi7.0/8.0の場合

以下のコマンドを実行します。

```
# /etc/init.d/amsd restart
```

● iL05 Ver2. 65以降の注意点

iL0webインターフェースの「システム情報」>「デバイスインベントリ」で BackPlane (BP) の位置情報が不正になる場合がありますが表示だけの問題で動作に影響はありません。

正常時) Slot=#:Port=#I:Box=# ※#は接続先により番号が変わります。

不正時) Slot=#:Port=?I:Box=? 数字の部分が?と表示されます。
または Box=# Box のみ表示されます。

● Java IRCのセッションタイムアウト時に表示に関する注意事項について

Java統合リモートコンソール (Java IRC) 起動中にリモートコンソールのセッションが切れた場合に、セッションが切れたことを示すポップアップと一緒にセッション切れとは直接関係のない内容のポップアップも表示されます。

Java IRC のセッションが切れた場合には、IRCの下部に以下のメッセージが表示されます。本メッセージが表示されている場合には、表示されているポップアップの内容は無視してください。

■ “セッションはタイムアウトか認識されないアクセスによって閉じられました。”

● サーバー再起動時のFAN高速化に関する注意事項について

iL05ファームウェアバージョン2. 90以降をご使用の場合:

サーバーの再起動を行うと、稀にFANの高速回転やうなり音が7分以上継続する場合があります。

この場合は、再度サーバーの再起動を実施してください。

● Rapid Setup実行に関する注意事項について

iL05ファームウェア2. 71または2. 72をご使用の場合:

Smartアレイ SW RAID構成時に、POST 時に[F10]キー押下 > Provisioning > EXPRESSBUILDER からRapid Setupを実行する際は、事前にiL0 Webインターフェースの[System Information] - [Device Inventory]で、Smart Array S100i SRのStatusが” Enabled” になっていることを確認してください。

Statusが” Unknown” と表示されている状態で、Rapid Setupを実行すると推奨されるRAID構成を準備中…” の表示の後に以下のメッセージが表示される場合があります。

■ “Rapid Setupは、このシステムに設置されているサポート対象ディスクを見つけられませんでした。ディスクが設置されていないか、ケーブル接続などの別の問題があります。Rapid Setupを終了し、ハードウェア構成を確認してください。”

● 通報に関する注意事項について

iL05ファームウェアバージョン3. 00以降をご使用の場合:

ESMPRO/ServerManagerをご利用されている場合、物理ドライブの状態変化に伴い、アラートビューアにおいて「物理ドライブのステータス変化検出」のアラートが表示されます。

この際、物理ドライブのステータスに応じて、ロケーション情報が次の二パターンのいずれかで表示されます。

- ① (Location: Slot=(A):Port=(B):Box=(C):Bay=(D) Controller: <NULL>)
- ② (Location: Port=(B):Box=(C):Bay=(D) Controller: Slot (A))

A:コントローラの位置(スロット番号)
B:物理ドライブのポート番号
C:物理ドライブのボックス番号
D:物理ドライブのベイ番号

● Intelligent Platform Management Interface (IPMI) の暗号化スイートを使用する場合の注意事項

iLO 5は、IPMIの暗号化スイート17 をサポートしていません。

“ipmitool”ユーティリティバージョン1.8.18以降を使用して、インターフェイスを“lanplus”、暗号化スイートを“17”に指定し、IPMIコマンドを実行した場合、以下のエラーが発生し、IPMIコマンド実行が失敗します。

```
Error in open session response message : no matching cipher suite  
Error: Unable to establish IPMI v2 / RMCP+ session.
```

● VROCのSATA RAID表示に関する注意事項

iLO5ファームウェアバージョン3.04以降をご使用の場合:

VROCのSATA RAID構成時、iLO Webインターフェースの[System Information] - [Storage] - [Drives]配下にドライブ情報が表示されず、「Unconfigured-Drives」と表示されます。

VROCのSATA RAID構成時のドライブ情報を参照する場合には、OS上のIntel VROC GUIまたはIntel VROC CLIを使用してください。

詳細は、「Intel® Virtual RAID on CPU ユーティリティ VROC8 ユーザーガイド」を参照してください。

4) OSに関する注意事項

● EXPRESSBUILDERでのWindows「手動」インストールについて

EXPRESSBUILDER から Windows をインストールするとき、「手動」オプションを選択した場合であっても、インストール先ディスクのパーティションがすべてクリアされます。再インストール時、ユーザーデータが存在する場合は注意してください。

● Windows Server OS ご使用時の注意事項

サポート対象の Windows Server OS で USB デバイスをお使いの場合、以下のシステムイベントログが採取されることがあります。

これについては、システム動作上問題ありません。

<イベントログ>

ID : 1
ソース : VDS Basic Provider
レベル : エラー
説明 : 予期しないエラーが発生しました。エラーコード:32@01000004

● Windows Server環境でのAgentless Management Service(AMS)の注意事項

Windows Server 2012 R2, Windows Server 2016, Windows Server 2019の環境にAgentless Management Service (AMS) version 1.40.0.0がインストールされている場合、ams.exeプロセスがハンドル数の増加を示します。ハンドルリークはメモリの過剰消費により時間の経過とともにパフォーマンスの問題を引き起こす可能性があります。

◆本件事象はAgentless Management Service (AMS) 1.43.0.0で修正されています。

AMSはStarter Packに含まれています。Starter Pack Version S8.10-006.03以降を適用してください。

すでにAMS 1.40.0.0がインストールされている環境でStarter Pack Version S8.10-006.03を使用する場合は、個別にAMSをアップデートする必要があります。Starter Packが掲載されているWebサイトの内容を確認してアップデートしてください。

◆Agentless Management Service (AMS) 1.40.0.0を使用される場合は、一度以下の手順を実施することでハンドル数は増加しなくなります。

- (1) 以下のコマンドをコマンドプロンプトで実行してAMSを停止します。

```
>net stop ams
```

- (2) "C:\Program Files\OEM\AMS\Service"ディレクトリをエクスプローラで開きます。

- (3) "storelib.dll"のファイル名を"storelib.dll.bak"に変更します。

- (4) 以下のコマンドをコマンドプロンプトで実行してAMSを開始します。

```
>net start ams
```

- (※1) AMS停止時に以下のメッセージが表示されることがありますが問題ありません。

Agentless Management Service サービスを停止中です..

システム エラーが発生しました。

システム エラー 1067が発生しました。

プロセスを途中で強制終了しました。

Agentless Management Service サービスは正常に停止されました。

- (※2) AMS起動時に以下のメッセージが表示されることがありますが問題ありません。

要求したサービスは既に開始されています。

◆Agentless Management Service (AMS) のバージョンの確認方法には以下の2つの方法があります。

・対象装置のOS上で確認する方法

- (1) Windows PowerShellを起動して以下のコマンドを実行します。

```
> Get-WmiObject Win32_Product | Select-Object Name, Version | Select-String "Agentless Management Service"
```

- (2) コマンド実行結果からバージョンを確認します。

・iLO Web インターフェースを利用して、リモートから確認する方法

- (1) リモート環境において、WebブラウザからiLO Web インターフェースにログインします。

- (2) 左メニューの「ファームウェア & OSソフトウェア」を選択し、「ソフトウェア」を選択します。

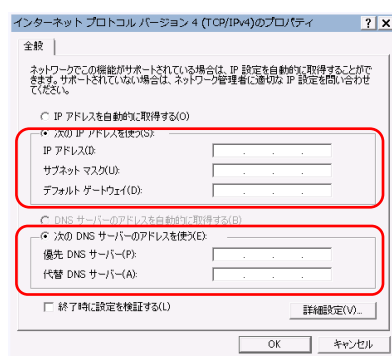
- (3) 画面の「Product Related Software」の「ams.exe」のバージョンを確認します。

● Windows Server 2019/2016/2012 R2 環境構築後、CPUボードの構成変更を行う場合の注意事項

次のOptionに固定IPアドレス/固定DNSを設定している場合、以下の手順で増設CPUボードを増設してください (CPU増設後も固定IPアドレス設定を引き継ぐために本手順が必要です)。

N8104-173 10GBASE-T接続LOMカード (2ch)
N8104-177 25GBASE接続LOMカード (SFP28/2ch)
N8104-182 10GBASE-T 接続ボード (2ch)
N8104-183 10GBASE-T 接続ボード (2ch)
N8104-185 10GBASE 接続基本ボード (SFP+/2ch)
N8104-187 25GBASE 接続基本ボード (SFP28/2ch)
PCI-to-PCI ブリッジを持つ増設PCIカード

- (1) 該当のオプションを参照するサービスが自動起動しないように設定を変更し、サービスを停止する。
また、該当のオプションにストレージを接続している場合、以下の作業前に該当のオプションからLANケーブルを外す等ストレージを認識しないようにする。
- (2) 該当のオプションでLANのチーミング設定をしている場合、チーミングを解除する。
- (3) 該当のオプションのIPアドレス/サブネットマスク/デフォルトゲートウェイ/優先DNSサーバー/代替DNSサーバーを記録する (下記の赤枠部分)。



- (4) 該当のオプションのIPアドレスを「IPアドレスを自動的に取得する」、DNSアドレスを「DNSサーバーのアドレスを自動的に取得する」に設定変更する。
- (5) 増設CPUボードをユーザズガイドに従って増設する。
- (6) 該当のオプションに手順(3)で記録したIPアドレス/サブネットマスク/デフォルトゲートウェイ/優先DNSサーバー/代替DNSサーバーを設定する。
- (7) LANのチーミングを再設定する。
- (8) 手順(1)で設定変更したサービスを自動起動するように再設定する。また、該当のオプションにストレージを接続していた場合、LANケーブルを再接続しストレージを認識できるようにする。



上記手順で行わなかった場合、固定IPアドレスがほかのデバイスで使用されている等のメッセージが表示されて固定IPアドレスが設定できないことがあります。

その場合、以下のコマンドをコマンドプロンプトで実行して、デバイスマネージャーを起動してください。その後、[表示] - [非表示デバイスの表示] をクリックし、ネットワークアダプタツリーを展開し、グレー表示になっている未使用のデバイスを削除してください。

```
>set devmgr_show_nonpresent_devices=1  
>Start DEVMGMT.MSC
```

ESMPRO/ServerManagerでネットワークを参照した場合、増設CPUボードの構成変更後にネットワークカードが重複して表示されます。OS上で見えないネットワークデバイスの詳細は「Unknown」と表示されますので、無視してください。

● ESMPRO/ServerManager (Windows版) およびエクスプレス通報サービス (MG) に関する注意事項

本製品の iLO ファームウェアバージョンと、ESMPRO/ServerManager (Windows 版) およびエクスプレス通報サービス (MG) のバージョンの組み合わせによってはESMPRO/ServerManager (Windows 版) および iLO 管理機能向けの受信情報設定ファイルのアップデートが必要になる場合があります。

以下をご参照のうえ、アップデートが必要な場合は、最新バージョンにアップデートしてください。

各バージョンの確認方法については、本注意事項の末尾に記載します。

◆ESMPRO/ServerManager (Windows 版) に関する発生現象

iLO ファームウェア	ESMPRO/ ServerManager (Windows 版)	発生現象
Version 2.10 以上	Version 6.25 未満	- 構成タブ - サーバー状態 “SNMP 通報設定” が “取得に失敗しました” と表示される - リモート制御タブ - iLO 情報 - IML の表示、IML の保存 IML 情報の取得に失敗し、表示および保存ができない - アラートビューア ファームウェアアップデートにともない追加されたハードウェアの障害がアラートビューアに “不明タイプ” のアラートとして表示される
	Version 6.47 未満	アラートビューア ファームウェアアップデートにともない追加されたハードウェアの障害がアラートビューアに表示されない、もしくは “不明タイプ” のアラートとして表示される

◆ESMPRO/ServerManager Ver. 6 (Windows 版) のアップデート方法

- (1) 以下の Web サイトより最新版の ESMPRO/ServerManager をダウンロードします。
<https://www.support.nec.co.jp/View.aspx?id=9010103524>
- (2) 「ESMPRO/ServerManager Ver. 6 インストレーションガイド(Windows 編)」の「2 章 インストール」を参照して ESMPRO/ServerManager をアップデートします。

◆ESMPRO/ServerManager Ver. 7 (Windows 版) へのアップデート方法

- (1) 以下の Web サイトより ESMPRO Platform Management Kit をダウンロードします。
<https://www.support.nec.co.jp/View.aspx?id=9010109532>
ESMPRO/ServerManager Ver. 7 は ESMPRO Platform Management Kit に含まれています。
- (2) ESMPRO Platform Management Kit の ESMPRO インストールツールを起動します。
- (3) インストールツール画面の説明書をクリックし、Software Manuals から ESMPRO/ServerManager をクリックします。
- (4) 「ESMPRO/ServerManager Ver. 7 インストレーションガイド(Windows 編)」をクリックします。
- (5) 「ESMPRO/ServerManager Ver. 7 インストレーションガイド(Windows 編)」の「2 章 インストール」を参照して ESMPRO/ServerManager を Ver. 6 から Ver. 7 へアップデートします。

◆iLO 管理機能向けの受信情報設定ファイル に関する発生現象

※エクスプレス通報サービス (MG) をご利用されている方が対象です。

iLO ファームウェア	iLO 管理機能向けの 受信情報設定 ファイル	発生現象
Version 2.10 以上	ilo_jp.mtb Version 1.4.0 未満	ファームウェアアップデートにともない追加されたハードウェアの障害を検知することができない。当該障害を通報することができない。 ※受信情報設定ファイルをアップデートした場合であっても、ESMPRO/ServerManager がアップデートされていないときは、上記と同様に追加されたハードウェア障害の検知および通報ができない。
	iml_jp.mtb Version 1.5.0 未満 ※iLO 管理機能向けの受信情報設定ファイルは 2 種類あります。	

◆iLO 管理機能向けの受信情報設定ファイルのアップデート方法

- (1) 以下の Web サイトより最新版の受信情報設定ファイル(ilo_jp.mtb、iml_jp.mtd)をダウンロードします。
<https://www.support.nec.co.jp/View.aspx?id=9010100096>
ilo_jp.mtb、iml_jp.mtd は MGMTB.zip に包含しています。
- (2) 「エクスプレス通報サービス (MG) インストレーションガイド(Windows 編)」の「3.1.5 受信情報の設定」または「3.2.4 受信情報の設定」を参照して受信情報の設定画面で登録済みの受信情報を削除します。
- (3) (1) でダウンロードした最新版の受信情報設定ファイルを登録します。
「エクスプレス通報サービス (MG) インストレーションガイド(Windows 編)」は以下の Web サイトからダウンロードしてください。
<https://www.support.nec.co.jp/View.aspx?id=9010102124>

◆ iLO ファームウェアのバージョン確認方法

- ・ Server Health Summary で確認する方法
サーバー本体の UID ボタンを押下して、サーバーに接続されたコンソールに表示される iLO Firmware のバージョンを確認します (Server Health Summary の詳細は iLO 5 ユーザーズガイド参照)。
- ・ ネットワーク経由で確認する方法
iLO にネットワーク接続可能な場合、ブラウザから iLO にログインして、メニュー「ファームウェア & OS ソフトウェア」から iLO のバージョンを確認します。

◆ ESMPRO/ServerManager (Windows 版) のバージョン確認方法

- (1) ESMPRO/ServerManager の Web サイトにログインします。
- (2) 画面右上の「ESMPRO/ServerManager について」のリンクを選択します。
- (3) 表示される ESMPRO/ServerManager のバージョン情報を確認します。

◆ iLO 管理機能向けの受信情報設定ファイルのバージョン確認方法

「エクスプレス通報サービス (MG) インストレーションガイド (Windows 編)」の「3.1.5 受信情報の設定」または「3.2.4 受信情報の設定」を参照して受信情報の設定画面で「詳細情報」が「iLO SNMP Trap」のバージョンを確認します。

● Linux OSを使用する場合の注意事項

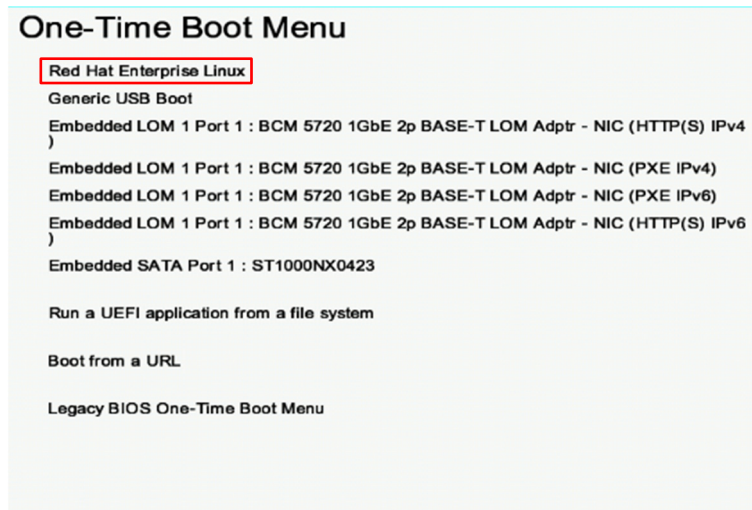
OSが自動的に認識するLOMやオプションNICのデバイス名を使用してください。独自udevルールを追加する際、PCIアドレスを基準にNICデバイス名を変更したり、固定したりする設定は行わないでください。
また、PCIアドレスを含む/dev/disk/by-path/配下のストレージデバイス名は使用しないでください。

PCI アドレスを基準にしたデバイス名を使った運用が必要な場合は、PCI スロットへのカード増設/抜去、および、CPU 構成変更を行わないでください。PCI バスのアドレス情報が変化し、PCI 接続のデバイス名に影響がでることにより、ネットワークやストレージへのアクセスができなくなり、システムが正常に起動できなくなる場合があります。

● Red Hat Enterprise Linux 8.5 以前を使用する場合の注意事項

ワンタイムブートメニューから起動する場合、OSブートマネージャー (例: Red Hat Enterprise Linux) を選択してください。

OSがインストールされたHDDやSSDなどのブートデバイスを選択した場合、Red Screen of Death (RSoD) が発生することがあります。



ワンタイムブートメニュー画面

● VMware ESXiを使用する場合の注意事項

ESXi 起動時の VMware vSphere の監視 > ハードウェア > システムセンサー > センサーの表示について。

- (1) 下記のような Heartbeat Lost センサーの表示が『警告(黄色)』となる場合があります。
[Device] I/O Module (n) LOM_Link_P (n) : Heartbeat Lost-Assert
[Device] I/O Module (n) NIC_Link_P (n) : Heartbeat Lost-Assert
※n: LAN ポート番号の P1~4 を示します。

<iLO 5 ファームウェア: 1.30、1.35、1.38 が適用された環境>
ESXi 起動完了後、Heartbeat Lost センサーの健全性(vCenter: ステータス)の表示が『警告(黄色)』となる場合、LAN ケーブルが接続されたポートは数分お待ちいただくと『警告(黄色)』から『正常(緑色)』に遷移しますので、しばらくお待ちください。LAN ケーブルが接続されていないポートは『警告(黄色)』を継続しますが、運用上問題ありませんのでそのままご使用ください。
なお、LAN ケーブルが接続された環境で『警告(黄色)』が表示され続けた場合は、LAN ケーブルの接続不良の可能性が考えられますので LAN 結線等を再確認してください

<iLO 5 ファームウェア: 1.40 以上が適用された環境>
ESXi 起動完了後、Heartbeat Lost センサーの健全性(vCenter: ステータス)の表示が『警告(黄色)』となる場合、数分お待ちいただくと『警告(黄色)』から『標準(緑色)』に遷移しますので、しばらくお待ちください。

(2) システム ROM のバージョンが v2.16 (05/25/2020) 以前の場合、非冗長 FAN 構成において ESXi 起動完了後、下記のセンサーの健全性(vCenter: ステータス)の表示が『警告(黄色)』となる場合がありますが、ハードウェアの故障を示すものではなく運用に影響ありませんので、そのまま運用いただけます。
- Cooling Unit 1 Fans

(3) ESXi 起動完了後、下記のセンサーの健全性(vCenter: ステータス)の表示が『?』となる場合がありますが、ハードウェアの故障を示すものではなく運用に影響ありませんので、そのまま運用いただけます。
- System Chassis 1 UID

● VMware ESXiでTPMキットを使用する場合の注意事項

システム ROM のバージョンが v2.00 (02/02/2019) 以降、かつ N8115-35 TPM キットが搭載されている場合 TPM Mode (*1)は「TPM 2.0」にて、VMware ESXi をご使用ください。

もし、TPM Mode が「TPM 1.2」に設定されている場合、稀に PSOD (Purple Screen of Death)が発生することがあります。

(*1) 出荷時の初期設定は「TPM 2.0」です。

TPM Mode の確認および設定変更は下記メニューより確認してください。

- ・ System Utilities > System Configuration > RBSU > Server Security > Trusted Platform Module Options > Current TPM Type (設定確認)
> TPM Mode Switch Operation (設定変更)

● RAID監視通報方式の変更について

VMware ESXi において、N8103-189/190/191/192/193/194/195/196/201/237/238/240 RAID コントローラと N8103-239 OS ブート専用 SSD ボードをご使用されている場合、RAID 監視通報は SNMP Trap による通報に変更になります。

詳細は、下記の Web サイトをご確認ください。

- ・ NEC サポートポータル

<https://www.support.nec.co.jp/View.aspx?id=3140108419>

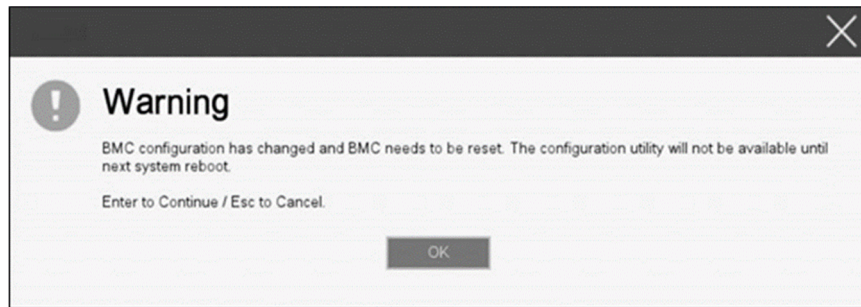
5) 全般の機能に関わる注意事項

● システムユーティリティの「BMC Configuration Utility」の操作についての注意事項

システムユーティリティの「BMC Configuration Utility」での操作において、以下の(1)のポップアップが表示された場合は(2)以降の手順を厳守してください。

注意事項に従った操作を実施されない場合、「Memory Initialization Start」のメッセージでPOST停止、あるいは、装置に記録されているSerial Number、Product IDの消失が発生する場合があります。

- (1) システムユーティリティの「BMC Configuration Utility」において設定の変更を行うと、iLOの再起動を行うために、次のWarning (注意) ポップアップが表示されることがあります。



英語表示の場合

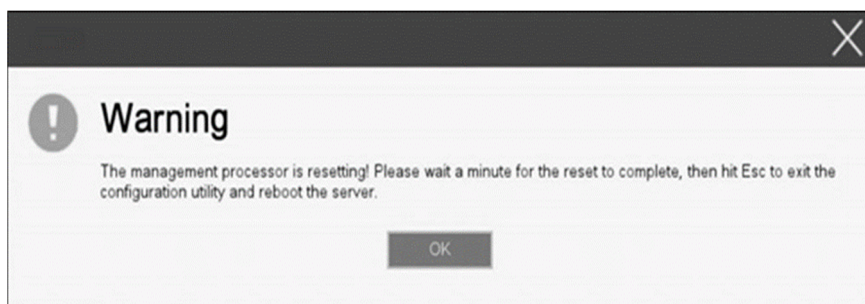


日本語表示の場合

- (2) 「OK」を押して進めます。

- (3) 次のWarning (注意) ポップアップが表示されます。

このWarning (注意) ポップアップが表示されている状態にて、**必ず1分以上お待ちください。**その間、何も操作しないでください。



英語表示の場合



日本語表示の場合

(4) 1分以上経過後、装置前面のステータスランプが緑色で点灯していることを確認してください。

※ iLOが再起動中 : ステータスランプが緑色で点滅 (毎秒1回)

iLOの再起動が完了し正常動作 : ステータスランプが緑色で点灯

(5) 再起動の完了が確認できたら、「OK」を押してください。

(6) <ESC>キーを複数回押してシステムユーティリティの画面に戻ります。

(7) システムユーティリティの「Reboot the System」を選択して再起動します。

● Serial Number、Product IDが消失された場合の対処について

Serial Number、Product IDが消失された場合、以下の手順にて復旧することができます。

- (1) 装置の電源を切り、電源コードをコンセントから外します。
- (2) 30秒以上経過したのち、電源コードをコンセントに接続します。
- (3) POWERスイッチで装置の電源をONにします。
- (4) サーバーが起動し、POST画面が表示されます。
- (5) <F9>キーを押してシステムユーティリティを起動します。もし、システムユーティリティが起動できない状態になっている場合は、「1章(7.3.3 システム設定をデフォルト値に戻す)」を参照し、システムメンテナンススイッチを操作して、RBSU設定の初期化をします。
- (6) システムユーティリティの「System Configuration > BIOS/Platform Configuration (RBSU) > Advanced Options > Advanced Service Options」メニューより、Serial NumberとProduct IDの値を確認します。
- (7) Serial NumberとProduct IDの値が期待する値の場合は、手順(14)に進みます。
- (8) Serial NumberとProduct IDの値が期待する値ではない(消失している)場合は、システムユーティリティから、「System Configuration > BIOS/Platform Configuration (RBSU) > System Default Options」を選択します。
- (9) 「Restore Default Manufacturing Settings」を選択します。
- (10) 「Yes, restore the default settings.」を選択します。
- (11) 自動的に装置が再起動し、POST画面が表示されます。
- (12) <F9>キーを押してシステムユーティリティを起動します。
- (13) 装置のスライドタグに記載されているSerial NumberとProduct IDをシステムユーティリティの「System Configuration > BIOS/Platform Configuration (RBSU) > Advanced Options > Advanced Service Options」メニューより、設定します。



【重要】Product IDとは、『N8100-2602Y』のような型番のことです。

(14) RBSU設定項目をデフォルト値から変更されている場合は、そのRBSU項目の確認と再設定をします。

● 装置情報のラベルについて

本製品には、以下の情報を記載したラベルがサーバーのトップカバーのフロント側に貼られています。

- ・ 製品型番
- ・ 製造番号
- ・ QRコード
- ・ iLOのアカウント情報

保守に備えて、サーバーの設置前にこれらの情報を記録してください。

Express5800/R120h-2E 8x3.5 型モデル以外には、上記の情報を記載したラベルが装置前面のスライドタグにも貼られています。

● 冷却設定の変更について

以下のオプションを搭載する場合は、安定稼働のため本製品の冷却ファンの設定を「Increased Cooling」へ変更してください。

既に冷却ファンの設定を「Increased Cooling」または「Maximum Cooling」に設定されている場合は、本対策を行う必要はありません。

対象オプション

- ・ N8150-551 増設用 300GB HDD
- ・ N8150-552 増設用 600GB HDD
- ・ N8150-553 増設用 900GB HDD
- ・ N8150-602 増設用 900GB HDD
- ・ N8154-107 2.5 型 HDD ケージ (SAS/SATA, リア)
- ・ N8154-120 2.5 型 HDD ケージ (SAS/SATA, リア)
- ・ N8104-195 10GBASE-T 接続 LOM カード (2ch)

※ LAN ファームウェアバージョンが 1.3089 未満の場合は、本対策を行ってください。

LAN ファームウェアバージョンが 1.3089 以上の場合は、本対策の必要はありません

◆ 設定手順

- (1) POST 中に <F9>キーを押下し、System Utilities を起動します。
- (2) System Configuration > BIOS/Platform Configuration (RBSU) > Advanced Options > Fan and Thermal Options を選択します。
- (3) Thermal Configuration メニューを 「希望する設定」に変更します。
- (4) <F12>キーを押下し、設定を保存してシステムを再起動します。

※ 冷却ファン設定の変更に伴い、お客様の運用環境や負荷によっては冷却ファンの回転数が上がることがあります。

● UPS 接続時の注意事項

- ・ UPS をシリアルポートに接続して使用する場合は、以下の設定を無効「Disabled」にしてください。

- (1) System Configuration > BIOS/Platform Configuration (RBSU) > System Options > Serial Port Options > BIOS Serial Console and EMS > BIOS Serial Console Port を「Disabled」に設定してください。
- (2) System Configuration > BMC Configuration Utility > Setting Options > Serial CLI Status を「Disabled」に設定してください。

- ・ N8181-160 電源ユニット (800W/Platinum) を冗長構成で搭載している場合、以下の設定を変更してください。

System Configuration > BIOS/Platform Configuration (RBSU) > Power and Performance Options > Advanced Power Options へと進み、「Redundant Power Supply Mode」を「High Efficiency Mode (Auto)」に設定してください。

※ High Efficiency Mode (Odd Supply Standby)、または、High Efficiency Mode (Even Supply Standby)に設定されているお客様については、上記の変更は不要です。

● N8116-84 SAS エキスパンダカード ご使用時の注意事項

Starter Pack Version S8.10-009.01 に含まれている、N8116-84 SAS エキスパンダカードの下記ファームウェアアップデートモジュール (Ver. 5.08) は、適用しないでください。

[パッケージ名称]

Supplement Update / Online ROM Flash Component for Linux (x64) ? HPE 12Gb/s SAS Expander Firmware for HPE Smart Array Controllers and HPE HBA Controllers
(firmware-smartarray2de15b6882-5.08-1.1x86_64)

詳細につきましては、以下の Web サイトに掲載されている内容を確認してください。

[Starter Pack Version S8.10-009.01]

<https://www.support.nec.co.jp/>

(「NEC サポートポータル内検索」より、「S8.10-009」を検索)

● N8103-184 SAS コントローラ ご使用時の注意事項

N8103-184 SASコントローラを使用する場合、iLO Webインターフェースの[System Information] - [Storage] - [Storage Controller]のStatusが“不明(Unknown)”と表示される場合がありますが動作に影響はありません。

● Smart Storage Battery について

Smart Storage Batteryは、RBSUメニューなどでEnergy Packと表示されることがあります。
適宜、読み替えてください。

● LOM カード (N8104-173/177) FCoE 機能のサポートについて

本製品ではFCoE (FibreChannel over Ethernet)機能を NEC としてサポートしておりません。

N8104-173 では LOM カードに適用されているファームウェアバージョンに関わらず、N8104-177 では Family Firmware Version 8.35.43 以降で FCoE 機能が有効化されています。

OS 上で FCoE デバイスとして認識されますが、OS やドライバで機能利用の設定をしないことで、運用上の影響はありません。

以下のデバイスの検出は無視していただいて構いません。

- HPE 533FLR-T FCoE Device
- HPE 622FLR-SFP28 FCoE Device

● N8104-173 10GBASE-T 接続 LOM カード (2ch) Wake On LAN 機能のサポートについて

N8104-173 10GBASE-T 接続 LOM カード (2ch) のポート 2 側で Wake On LAN 機能を使用する場合は、ファームウェアバージョン 7.19.2 以降をご使用ください。

● サーバ診断カルテについて

サーバ診断カルテは、対象製品の稼働状況を記録し、月ごとに稼働状態の診断カルテを提供するサービスです。
サーバ診断カルテの詳細は、Starter Pack内の「サーバ診断カルテ セットアップガイド」を参照してください。

サーバ診断カルテの注意事項については下記の Web サイトをご確認ください。

■Windows 対応版

NEC サポートポータル (Windows 対応版)

<https://www.support.nec.co.jp/View.aspx?&id=9010106809>

■VMware ESXi 対応版

NEC サポートポータル (VMware ESXi 対応版)

<https://www.support.nec.co.jp/View.aspx?&id=9010107805>

● EXPRESSBUILDER ヘルプについて

EXPRESSBUILDER のヘルプとメンテナンスガイドで記述が異なる場合は、メンテナンスガイドの記載を優先してください。

A) ファームウェア変更に伴う変更点

■ BIOS/Platform Configuration (RBSU) メニューの変更について

本製品の搭載ファームウェアの更新に伴い、メニューの一部に変更があります。
下記、変更点を記載します。

(1) Server Availability メニュー

システムユーティリティから、「System Configuration > BIOS/Platform Configuration (RBSU) > System Options > Server Availability」を選択すると、「Server Availability」メニューが表示されます。

追加のオプションについて、次の表を参照してください。

項目	パラメーター	説明
IPMI Watchdog Timer (注1)	[Disabled] Enabled	IPMI に準拠した起動時の (POST) ウォッチドッグタイマー (WDT) を有効にできます。このタイマーは、ユーザーがシステムに対して IPMI コマンドを発行すると無効になり、自動的には無効になりません。 IPMI ウォッチドッグタイマー (WDT) は、POST 中に <F9> キー、または <F10> キーを押すと停止できます。 POST 中の <F9> キー、または <F10> キーを押した以外の場合、WDT は選択された IPMI ウォッチドッグタイマーのタイムアウト期間の後にタイムアウトし、システムは選択された IPMI ウォッチドッグタイマー動作を続行します。
IPMI Watchdog Timer Timeout (注1)	10 Minutes 15 Minutes 20 Minutes [30 Minutes]	サーバーのロックアップが発生した場合にサーバーに対して必要なタイムアウト動作を実行するまでの待機時間を設定できます。
IPMI Watchdog Timer Action (注1)	[Power Cycle] Power Down Warm Boot	サーバーのロックアップによってウォッチドッグタイマーが時間切れになったときのタイムアウト動作を設定できます。

[]: 出荷時の設定

注 1: システム ROM バージョン 2.54 以降にて利用できるオプションです。

(2) Diagnostics Options メニュー

システムユーティリティから、「System Configuration > BIOS/Platform Configuration (RBSU) > System Options > Diagnostics Options」を選択すると、「Diagnostics Options」メニューが表示されます。

追加のオプションについて、次の表を参照してください。

項目	パラメーター	説明
Embedded Diagnostics	[Enabled] Disabled	本機ではサポートされません。

[]: 出荷時の設定

(3) Memory Optionsメニュー

システムユーティリティから、「System Configuration > BIOS/Platform Configuration (RBSU) > Memory Options」を選択すると、「Memory Options」メニューが表示されます。

追加のオプションについて、次の表を参照してください。

項目	パラメーター	説明
Memory Controller Interleaving	[Auto] Disabled	メモリコントローラー間のインターリーブ動作を選択します。「Auto」を選択した場合、メモリコントローラー間のインターリーブ動作は本機のメモリ構成に応じて自動的に設定されます。「Disabled」を設定した場合、メモリコントローラー間のインターリーブ動作は強制的に無効に設定されます。本オプションは、「Auto」で利用することを推奨します。
Opportunistic Self-Refresh	[Disabled] Enabled	「Opportunistic Self-Refresh」を「Enabled」に設定した場合、メモリがアイドル状態になった場合にメモリのセルフリフレッシュを行います。 [Disabled] の場合は通常のリフレッシュを行います。

[]: 出荷時の設定

(4) Intel UPI Optionsメニュー

システムユーティリティから、「System Configuration > BIOS/Platform Configuration (RBSU) > Power and Performance Options > Intel UPI Options」を選択すると、「Intel UPI Options」メニューが表示されます。

追加のオプションについて、次の表を参照してください。

項目	パラメーター	説明
Direct To UPI (D2K)	[Auto] Enabled Disabled	「Direct To UPI (D2K)」を「Enabled」にすると、Last Level Cacheのキャッシュミスによるレイテンシーを軽減します。指定されない限り、設定変更しないでください。 複数プロセッサ構成の場合のみ表示されます。

[]: 出荷時の設定

(5) Advanced Performance Tuning Options サブメニュー

システムユーティリティから、「System Configuration > BIOS/Platform Configuration (RBSU) > Power and Performance Options > Advanced Performance Tuning Options」を選択すると、「Advanced Performance Tuning Options」メニューが表示されます。

追加のオプションについて、次の表を参照してください。

項目	パラメーター	説明
Processor Jitter Control Optimization	Optimized for Throughput Optimized for Latency [Zero Latency]	本オプションは指定ある場合をのぞいて、出荷時設定から変更しないでください。 このオプションは、プロセッサ周波数変動の自動調整機能の閾値を最適化します。「Optimized for Throughput」を選択すると、総合的な計算処理能力に影響しない変動を許容した制御をします。 「Optimized for Latency」を選択すると、プロセッサ周波数を下げるときに微小変動があることを許容した制御をします。「Zero Latency」を選択すると、周波数変動を取り除くように制御します。
IODC Configuration	[Auto] Enable for Remote InvItom Hybrid Push InvItom AllocFlow InvItom Hybrid AllocFlow Enable for Remote InvItom and Remote WCILF	本オプションは指定ある場合をのぞいて、出荷時設定から変更しないでください。 IODC (IO Direct Cache)の構成を設定します。 このオプションにより、I / Oトランザクションがプロセッサキャッシュと通信するためのポリシーを調整できます。

[]: 出荷時の設定

(6) Server Security メニュー

システムユーティリティから、「System Configuration > BIOS/Platform Configuration (RBSU) > Server Security」を選択すると、「Server Security」メニューが表示されます。

追加のオプションについて、次の表を参照してください。

項目	パラメーター	説明
UEFI Variable Access Firmware Control (注1)	[Disabled] Enabled	オペレーティングシステムなど他のソフトウェアによる特定のUEFI変数の書き込みを、システムBIOSで完全に制御できるように設定します。「Disabled」が選択されている場合は、すべてのUEFI変数が書き込み可能です。「Enabled」が選択されている場合、システムBIOS以外のソフトウェアによって重要なUEFI変数に加えられる変更はすべてブロックされます。例えば、オペレーティングシステムが新しいブートオプションをブート順序の最上位に追加しようとする、実際にはブート順序の最下位に配置されます。注記: UEFI変数アクセスのファームウェアコントロールが有効になっている場合、オペレーティングシステムの機能の一部が期待どおりに動作しないことがあります。新しいオペレーティングシステムのインストール中にエラーが発生する場合があります。

[]: 出荷時の設定

注1: システム ROM バージョン 2.54 以降にて利用できるオプションです。

(a) Trusted Platform Module Optionsメニュー

システムユーティリティから、「System Configuration > BIOS/Platform Configuration (RBSU) > Server Security > Trusted Platform Module Options」を選択すると、「Trusted Platform Module Options」メニューが表示されます。

追加のオプションについて、次の表を参照してください。

項目	パラメーター	説明
Omit Boot Device Event (注1)	[Disabled] Enabled	ブートデバイスイベント省略の記録を設定します。「Enabled」に設定すると、PCRブート試行の測定が無効になり、PCR[4]での測定が記録されなくなります。

[]: 出荷時の設定

注1: システム ROM バージョン 2.80 以降にて利用できるオプションです。

(7) PCIe Devices Configurationメニュー

システムユーティリティから、「System Configuration > BIOS/Platform Configuration (RBSU) > PCIe Devices Configuration」を選択すると、「PCIe Devices Configuration」メニューが表示されます。

追加のオプションについて、次の表を参照してください。

項目	パラメーター	説明
Advanced PCIe Configuration	-	-

(a) Advanced PCIe Configurationメニュー

システムユーティリティから、「System Configuration > BIOS/Platform Configuration (RBSU) > PCIe Devices Configuration > Advanced PCIe Configuration」を選択すると、「Advanced PCIe Configuration」メニューが表示されます。

追加のメニューについて、次の表を参照してください。

項目	パラメーター	説明
PCIe Bifurcation Options	-	-
PCIe MCTP Options	-	-

① PCIe Bifurcation Optionsメニュー

システムユーティリティから、「System Configuration > BIOS/Platform Configuration (RBSU) > PCIe Devices Configuration > Advanced PCIe Configuration > PCIe Bifurcation Options」を選択すると、「PCIe Bifurcation Options」メニューが表示されます。

追加のオプションについて、次の表を参照してください。

項目	パラメーター	説明
PCIe Slot XX Bifurcation	[Auto] Slot Bifurcated	PCIe Slotに実装するPCIe拡張カードがSlot Bifurcation機能をサポートする場合、必要に応じて「Slot Bifurcated」を設定してください。 「Auto」を設定すると、PCIe Slotは、サポートされる最大幅で接続されます。 「Slot Bifurcated」を設定すると、PCIe Slotと拡張カード間の接続が、2個に分割されます。 XX: 1/2/3... (CPU数やライザーカード種類に応じて表示が変わります。)

[]: 出荷時の設定

② PCIe MCTP Optionsメニュー

システムユーティリティから、「System Configuration > BIOS/Platform Configuration (RBSU) > PCIe Devices Configuration > Advanced PCIe Configuration > PCIe MCTP Options」を選択すると、「PCIe MCTP Options」メニューが表示されます。

追加のオプションについて、次の表を参照してください。

項目	パラメーター	説明
PCIe Slot XX MCTP Broadcast Support	[Enabled] Disabled	指定されたスロットのPCIe管理コンポーネント転送プロトコル(MCTP)を制御します。このオプションは、PCIeエンドポイントに対するMCTPサポートを無効にするために使用します。このオプションはシステムの全機能に対して有効に設定することを推奨します。 XX: 1/2/3... (CPU数やライザーカード種類に応じて表示が変わります。)

[]: 出荷時の設定

(8) Fan and Thermal Optionsメニュー

システムユーティリティから、「System Configuration > BIOS/Platform Configuration (RBSU) > Advanced Options > Fan and Thermal Options」を選択すると、「Fan and Thermal Options」メニューが表示されます。

オプションのパラメーター追加について、次の表を参照してください。

項目	パラメーター	説明
Thermal Configuration	[Optimal Cooling] Increased Cooling Maximum Cooling Enhanced CPU Cooling	本機のファン冷却方法を選択します。 「Optimal Cooling」は、適切な冷却を可能にする必要最小限のファン速度に設定することで、最も効率的な冷却方法を実現します。 「Increased Cooling」ではファンを高速で回転させ、冷却能力を高めます。「Increased Cooling」は、他社製のストレージコントローラーが内蔵ハードドライブケージにケーブル接続されている場合、または本機の高温の問題を他の方法で解決できない場合に使用します。 「Maximum Cooling」は、ファンを最高速で回転させ、最も高い冷却方法を実現します。 「Enhanced CPU Cooling」は、プロセッサの冷却をより強化します。プロセッサに負荷のかかるワークロードを実行する場合、プロセッサの冷却強化により、パフォーマンスが改善する場合があります。

[]: 出荷時の設定

(9) Advanced Debug Optionsメニュー

システムユーティリティから、「System Configuration > BIOS/Platform Configuration (RBSU) > Advanced Options > Advanced Debug Options」を選択すると、「Advanced Debug Options」メニューが表示されます。

追加のオプションについて、次の表を参照してください。

項目	パラメーター	説明
Advanced Crash Dump Mode	[Disabled] Enabled	本オプションは指定ある場合を除き、出荷時設定から変更しないでください。 「Enabled」に設定した場合、システムがクラッシュした場合に、AHSログに追加のデバック情報を記録するようにシステムを構成します。

[]: 出荷時の設定

(10) Power and Performance Options メニュー

システムユーティリティから、「System Configuration > BIOS/Platform Configuration (RBSU) > Power and Performance Options」を選択すると、「Power and Performance Options」メニューが表示されます。

追加のオプションについて、次の表を参照してください。

項目	パラメーター	説明
Energy Performance Preference (注1)	[Disabled] Enabled	このオプションを使用して、エネルギーパフォーマンス優先を有効または無効にします。

[]: 出荷時の設定

注1:システムROM バージョン 2.80以降にて利用できるオプションです。

(11) Trusted Platform Module Optionsメニュー

システムユーティリティから、「System Configuration > BIOS/Platform Configuration (RBSU) > Server Security > Trusted Platform Module Options」を選択すると、「Trusted Platform Module Options」メニューが表示されます。

追加のオプションについて、次の表を参照してください。

項目	パラメーター	説明
Omit Boot Device Event (注1)	[Disabled] Enabled	ブートデバイスイベント省略の記録を設定します。「Enabled」に設定すると、PCRブート試行の測定が無効になり、PCR[4]での測定が記録されなくなります。

[]: 出荷時の設定

注1:システムROM Version 2.80 以降にて利用できるオプションです。

(12) Embedded Applications メニュー

システムユーティリティから、「Embedded Applications」を選択すると、「Embedded Applications」メニューが表示されます。

追加のオプションについて、次の表を参照してください。

項目	パラメーター	説明
Embedded Diagnostics	-	本機ではサポートされません。

B) 誤記訂正

ユーザーズガイドに誤記がありましたので、以下に訂正いたします。

■ Express5800/R120h-1E ユーザーズガイドについて

	誤	正																																																				
P. 2 本製品の説明書	電子版としてStarter Pack DVD に格納、 またはWeb サイト (http://jpn.nec.com/) に 公開	電子版としてWeb サイト (https://jpn.nec.com/express/) に公開																																																				
P. 24 3. 特長 - 豊富な機能搭載	POWER スイッチマスク	非対応																																																				
P. 32 5. 5 マザーボード	(3) マイクロSDカードスロット	(3) マイクロSDカードスロット (未サポー ト)																																																				
P. 110 1. 18 4x 3.5 型 光デ ィスクドライブ	光ディスクドライブケーブルキット (K410-375 (00))	不要 (光ディスクドライブに添付)																																																				
P. 111 1. 18 4x 3.5 型 光デ ィスクドライブ	光ディスクドライブ用SATA ケーブル (K410-375 (00))	(添付品)																																																				
P. 114 1. 20.1 RAIDシステム 構築時の注意事項	オプションのRAID コントローラ (N8103- 192/195) を使用する場合、RAID 5、RAID 6、 RAID 50、RAID 60 のRAID システムは構築 できません。 <table border="1"> <thead> <tr> <th rowspan="2">RAIDレベル</th><th colspan="2">RAIDシステム構築に必要な ハードディスクドライブの最小数</th></tr> <tr> <th>N8103-192/195</th><th>N8103-193/201</th></tr> </thead> <tbody> <tr><td>RAID 0</td><td>1</td><td>1</td></tr> <tr><td>RAID 1</td><td>2</td><td>2</td></tr> <tr><td>RAID 5</td><td></td><td>3</td></tr> <tr><td>RAID 6</td><td></td><td>3</td></tr> <tr><td>RAID 10</td><td>4</td><td>4</td></tr> <tr><td>RAID 50</td><td></td><td>6</td></tr> <tr><td>RAID 60</td><td></td><td>6</td></tr> </tbody> </table>	RAIDレベル	RAIDシステム構築に必要な ハードディスクドライブの最小数		N8103-192/195	N8103-193/201	RAID 0	1	1	RAID 1	2	2	RAID 5		3	RAID 6		3	RAID 10	4	4	RAID 50		6	RAID 60		6	オプションのRAID コントローラ (N8103- 192/195) を使用する場合、RAID 6、RAID 50、 RAID 60 のRAID システムは構築できませ ん。 <table border="1"> <thead> <tr> <th rowspan="2">RAIDレベル</th><th colspan="2">RAIDシステム構築に必要な ハードディスクドライブの最小数</th></tr> <tr> <th>N8103-192/195</th><th>N8103-193/201</th></tr> </thead> <tbody> <tr><td>RAID 0</td><td>1</td><td>1</td></tr> <tr><td>RAID 1</td><td>2</td><td>2</td></tr> <tr><td>RAID 5</td><td>3</td><td>3</td></tr> <tr><td>RAID 6</td><td></td><td>4</td></tr> <tr><td>RAID 10</td><td>4</td><td>4</td></tr> <tr><td>RAID 50</td><td></td><td>6</td></tr> <tr><td>RAID 60</td><td></td><td>8</td></tr> </tbody> </table>	RAIDレベル	RAIDシステム構築に必要な ハードディスクドライブの最小数		N8103-192/195	N8103-193/201	RAID 0	1	1	RAID 1	2	2	RAID 5	3	3	RAID 6		4	RAID 10	4	4	RAID 50		6	RAID 60		8
RAIDレベル	RAIDシステム構築に必要な ハードディスクドライブの最小数																																																					
	N8103-192/195	N8103-193/201																																																				
RAID 0	1	1																																																				
RAID 1	2	2																																																				
RAID 5		3																																																				
RAID 6		3																																																				
RAID 10	4	4																																																				
RAID 50		6																																																				
RAID 60		6																																																				
RAIDレベル	RAIDシステム構築に必要な ハードディスクドライブの最小数																																																					
	N8103-192/195	N8103-193/201																																																				
RAID 0	1	1																																																				
RAID 1	2	2																																																				
RAID 5	3	3																																																				
RAID 6		4																																																				
RAID 10	4	4																																																				
RAID 50		6																																																				
RAID 60		8																																																				
P152 2. 4 設定が必要なケース - メモリ関連 - メモリRAS機能を使う	[System Configuration > BIOS/Platform Configuration (RBSU) > System Options > Memory Operations] - [Advanced Memory Protection] を設定してください	[System Configuration > BIOS/Platform Configuration (RBSU) > Memory Options] - [Advanced Memory Protection] を設定し てください																																																				
P. 169 1. 仕様 - 標準インターフ ェース	2x データLAN コネクタ (1000BASE- T/100BASE-TX/10BASE-T 対応 (RJ-45))	2x データLAN コネクタ (1000BASE-T対応 (RJ-45))																																																				

■ Express5800/R120h-2E ユーザーズガイドについて

	誤	正																																																				
P. 2 本製品の説明書	電子版としてStarter Pack DVD に格納、 またはWeb サイト (http://jpn.nec.com/) に 公開	電子版としてWeb サイト (https://jpn.nec.com/express/) に公開																																																				
P. 24 3. 特長 - 豊富な機能搭載	POWER スイッチマスク	非対応																																																				
P. 33 5.5 マザーボード	(3) マイクロSDカードスロット	(3) マイクロSDカードスロット (未サポー ト)																																																				
P. 136 1. 24.1 RAIDシステム 構築時の注意事項	オプションのRAID コントローラ (N8103- 189/195) を使用する場合、RAID 5、RAID 6、 RAID 50、RAID 60 のRAID システムは構築 できません。 <table border="1"> <thead> <tr> <th rowspan="2">RAIDレベル</th><th colspan="2">RAIDシステム構築に必要な ハードディスクドライブの最小数</th></tr> <tr> <th>N8103-189/195</th><th>N8103-190/201</th></tr> </thead> <tbody> <tr> <td>RAID 0</td><td>1</td><td>1</td></tr> <tr> <td>RAID 1</td><td>2</td><td>2</td></tr> <tr> <td>RAID 5</td><td></td><td>3</td></tr> <tr> <td>RAID 6</td><td></td><td>3</td></tr> <tr> <td>RAID 10</td><td>4</td><td>4</td></tr> <tr> <td>RAID 50</td><td></td><td>6</td></tr> <tr> <td>RAID 60</td><td></td><td>6</td></tr> </tbody> </table>	RAIDレベル	RAIDシステム構築に必要な ハードディスクドライブの最小数		N8103-189/195	N8103-190/201	RAID 0	1	1	RAID 1	2	2	RAID 5		3	RAID 6		3	RAID 10	4	4	RAID 50		6	RAID 60		6	オプションのRAID コントローラ (N8103- 189/195) を使用する場合、RAID 6、RAID 50、 RAID 60 のRAID システムは構築できませ ん。 <table border="1"> <thead> <tr> <th rowspan="2">RAIDレベル</th><th colspan="2">RAIDシステム構築に必要な ハードディスクドライブの最小数</th></tr> <tr> <th>N8103-189/195</th><th>N8103-190/201</th></tr> </thead> <tbody> <tr> <td>RAID 0</td><td>1</td><td>1</td></tr> <tr> <td>RAID 1</td><td>2</td><td>2</td></tr> <tr> <td>RAID 5</td><td>3</td><td>3</td></tr> <tr> <td>RAID 6</td><td></td><td>4</td></tr> <tr> <td>RAID 10</td><td>4</td><td>4</td></tr> <tr> <td>RAID 50</td><td></td><td>6</td></tr> <tr> <td>RAID 60</td><td></td><td>8</td></tr> </tbody> </table>	RAIDレベル	RAIDシステム構築に必要な ハードディスクドライブの最小数		N8103-189/195	N8103-190/201	RAID 0	1	1	RAID 1	2	2	RAID 5	3	3	RAID 6		4	RAID 10	4	4	RAID 50		6	RAID 60		8
RAIDレベル	RAIDシステム構築に必要な ハードディスクドライブの最小数																																																					
	N8103-189/195	N8103-190/201																																																				
RAID 0	1	1																																																				
RAID 1	2	2																																																				
RAID 5		3																																																				
RAID 6		3																																																				
RAID 10	4	4																																																				
RAID 50		6																																																				
RAID 60		6																																																				
RAIDレベル	RAIDシステム構築に必要な ハードディスクドライブの最小数																																																					
	N8103-189/195	N8103-190/201																																																				
RAID 0	1	1																																																				
RAID 1	2	2																																																				
RAID 5	3	3																																																				
RAID 6		4																																																				
RAID 10	4	4																																																				
RAID 50		6																																																				
RAID 60		8																																																				
P174 2.5 設定が必要なケース - メモリ関連 - メモリRAS機能を使う	[System Configuration > BIOS/Platform Configuration (RBSU) > System Options > Memory Operations] - [Advanced Memory Protection] を設定してください	[System Configuration > BIOS/Platform Configuration (RBSU) > Memory Options] - [Advanced Memory Protection] を設定し てください																																																				
P. 191 1. 仕様 標準インターフェ ース	2x データLAN コネクタ (1000BASE- T/100BASE-TX/10BASE-T対応 (RJ-45))	2x データLAN コネクタ (1000BASE-T対応 (RJ-45))																																																				

■ Express5800/R120h-1E, R120h-2E インストレーションガイド(Windows編)について

	誤	正
P. 2 本製品の説明書	電子版としてStarter Pack DVDに格納、 またはWeb サイト (http://jpn.nec.com/) に 公開	電子版としてWeb サイト (https://jpn.nec.com/express/) に公開
P. 6 オペレーティングシ ステムの表記	Windows Server 2016 Essentials	非対応
P. 79 4.3.1 セットアップ の流れ	4.8 Windows Server 2016 NICチーミング (LBFO) の設定	4.8 Windows Server 2012 R2 NICチーミン グ (LBFO) の設定
P. 89 4.4.1 セットアップ の流れ	4.8 Windows Server 2016 NICチーミング (LBFO) の設定	4.8 Windows Server 2012 R2 NICチーミン グ (LBFO) の設定

■ Express5800/R120h-1E, R120h-2E メンテナンスガイドについて

	誤	正
P. 2 本製品の説明書	電子版としてStarter Pack DVD に格納、またはWeb サイト (http://jpn.nec.com/) に公開	電子版としてWeb サイト (https://jpn.nec.com/express/) に公開
P. 8 オペレーティングシステムの表記(Windows)	Windows Server 2016 Essentials	非対応
P. 71 7.3.3 システム設定をデフォルト値に戻す	6. 本書の「1 章(7.3.2 システムメンテナンススイッチの操作)」に従い、システムメンテナンススイッチ： SW6 をON に戻します。	6. 本書の「1 章(7.3.2 システムメンテナンススイッチの操作)」に従い、システムメンテナンススイッチ： SW6 をOFF に戻します。
P. 81 Internal SD Card Slot	[Enabled] 内部SD カードスロットを有効または無効にします。無効に設定した場合、SD カードスロットは、SD カードが搭載されているかどうかに関係なく、無効になります。SD カードは、プリブート環境またはオペレーティングシステムにおいて、見えなくなります。	[Disabled] 本オプション設定は現在サポートされておりません。本機では、このオプションに対応するデバイスをサポートしておりません。 工場出荷時に、ユーザーデフォルト設定として、本オプションをDisabledに設定しています。 この項目は出荷時の設定から変更しないでください。
P86 (3) Memory Options メニュー	システムユーティリティから、「System Configuration > BIOS/Platform Configuration (RBSU) > System Options > Memory Options」を選択すると、「Memory Options」メニューが表示されます。	システムユーティリティから、「System Configuration > BIOS/Platform Configuration (RBSU) > Memory Options」を選択すると、「Memory Options」メニューが表示されます。
P87 (a) Persistent Memory Options メニュー	システムユーティリティから、「System Configuration > BIOS/Platform Configuration (RBSU) > System Options > Memory Options > Persistent Memory Options」を選択すると、「Persistent Memory Options」メニューが表示されます。	システムユーティリティから、「System Configuration > BIOS/Platform Configuration (RBSU) > Memory Options > Persistent Memory Options」を選択すると、「Persistent Memory Options」メニューが表示されます。
P. 99 i. (UEFI LAN Driver) メニュー -Target Name	例: iqn.2015-02.com.nec:iscsitarget-iscsidisk-target。	例: iqn.2015-02.com.nec:iscsitarget-iscsidisk-target
P. 109 Redundant Power Supply Mode	システムによる電源冗長構成の処理方法を設定するには、このオプションを使用します。 「Balanced Mode」では、搭載されているすべての無停電電源装置(UPS)間で電源供給を等しく共有します。すべての「High Efficiency Mode」パラメーターは、スタンバイモードのUPS の半分を低消費電力レベルに保つことで、電源効率の高い動作のほとんどに冗長化電源を提供します。「High Efficiency Mode」のパラメーターでは、スタンバイにするUPS をシステムが選択することを可能にします。 「Auto」では、システムグループ内のセミランダムな分布に基づいて奇数または偶数のUPS をシステムが選択することを可能にします。	システムの電源冗長構成の効率モードの設定を行うには、本オプションを使用します。 「Balanced Mode」では、搭載されているすべて(本モデルは最大2台)の電源間で電源供給を等しく共有します。 「High Efficiency Mode」では、搭載されている片側の電源をスタンバイモードにすることにより、低消費電力レベルを保ち、冗長化電源の効率を向上させます。 「High Efficiency Mode」は、スタンバイモードに設定する電源を電源ユニット番号の「奇数(Odd Supply Standard)」、「偶数(Even Supply Standard)」を選択することで指定することができます。 「Auto」設定では、システムグループ内のセミランダムな分布に基づいて、システムが電源ユニット番号の「奇数」、「偶数」を自動で指定します。

■ メモリ搭載順序の訂正

ユーザーズガイドにおいて、メモリの搭載順序に誤記がありました。
 ついては、下記のとおり訂正いたします。

修正箇所

- Express5800/R120h-1E ユーザーズガイド
 2章 準備 1.8 DIMM 1.8.2 DIMMの増設順序
- Express5800/R120h-2E ユーザーズガイド
 2章 準備 1.9 DIMM 1.9.2 DIMMの増設順序

メモリの搭載順序について

メモリの搭載位置、搭載順序は1CPU構成と2CPU構成、また、メモリの搭載枚数によって異なります。

- ・CPU1 だけ実装している場合のメモリ搭載位置、搭載順序

DIMM スロット番号		1	2	3	4	5	6	7	8
メモリ 搭載 枚数と 搭載 順序	DIMM 1枚			1					
	DIMM 2枚		2	1					
	DIMM 3枚	3	2	1					
	DIMM 4枚		2	1			3	4	
	DIMM 5枚	3	2	1			4	5	
	DIMM 6枚	3	2	1			4	5	6
	DIMM 7枚	3	2	1	7		4	5	6
	DIMM 8枚	3	2	1	8	8	4	5	6

- ・CPU1 と CPU2 を実装している場合のメモリ搭載位置、搭載順序

DIMM スロット番号		CPU2								CPU1							
		1	2	3	4	5	6	7	8	1	2	3	4	5	6	7	8
メモリ 搭載 枚数と 搭載 順序	DIMM 2枚			2								1					
	DIMM 3枚			2							3	1					
	DIMM 4枚		4	2							3	1					
	DIMM 5枚		4	2							3	1					
	DIMM 6枚	6	4	2						5	3	1					
	DIMM 7枚	6	4	2						5	3	1			5	7	
	DIMM 8枚		4	2			6	8			3	1			5	7	
	DIMM 9枚		4	2			6	8			3	1			7	9	
	DIMM10枚	6	4	2			8	10		5	3	1			7	9	
	DIMM11枚	6	4	2			8	10		5	3	1			7	9	11
	DIMM12枚	6	4	2			8	10	12	5	3	1			7	9	11
	DIMM13枚	6	4	2			8	10	12	5	3	1	13		7	9	11
	DIMM14枚	6	4	2	14		8	10	12	5	3	1	13		7	9	11
	DIMM15枚	6	4	2	14		8	10	12	5	3	1	13	15	7	9	11
	DIMM16枚	6	4	2	14	16	8	10	12	5	3	1	13	15	7	9	11

- ・DIMM 混在時の注意

複数種の DIMM を混在させる場合、下記に示す優先順位の高い DIMM から、上記表に示した搭載順序に従って、DIMM スロットに実装してください。

(優先度高) N8102-711 → N8102-710 → N8102-709 → N8102-708 (優先度低)

■ 本件に関するお問い合わせについて

本書の内容に不明点がありました場合は、下記ファーストコンタクトセンターまでお問い合わせください。

お問い合わせ先：ファーストコンタクトセンター

TEL : 0120-5800-72

受付時間 : 9:00～12:00 13:00～17:00 月曜日～金曜日(祝日を除く)

※番号をお間違えにならないようお確かめのうえお問い合わせください。

Precautions for Using Express5800/R120h-1E, R120h-2E

Thank you for purchasing our products.

This document provides the precautions on the use of this product.

Please read through the instructions below and keep this document in a safe place for your future reference.

- 1) Introduction
- 2) Notice about the function of the System ROM
- 3) Notice about the function of the iLO5
- 4) Notice about the OS
- 5) Notice of the function in general
- A) The additional options by firmware update
- B) Errata Information

1) Introduction

● About the manual of this product.

For Starter Pack, the user's guide and the other related documents of this product, please refer to Download on the following URL. Regarding Starter Pack, it is also provided as an optional product.

< <https://www.58support.nec.co.jp/global/download/> >
-> Document & Software
-> Rack
-> (Select your server model)

Please check latest information and versions on ESMPRO portal site before using NEC ESMPRO Manager, NEC ESMPRO ServerAgentService and Express Report Service / Express Report Service (HTTPS) / Express Report Service (MG).

< <https://www.58support.nec.co.jp/global/download/> >
-> ESMPRO

● About Starter pack

Please see the following website to check the latest Starter Pack.

< <https://www.58support.nec.co.jp/global/download/> >
-> Document & Software
-> Rack
-> (Select your server model)

● About service and driver modules for VMware ESXi

Please see the following web site to check the latest modules.

(1) Agentless Management Service and iLO Channel Interface Driver

< <https://www.58support.nec.co.jp/global/download/> >
-> VMware

(2) WBEM Provider and CLI tool

< <https://www.58support.nec.co.jp/global/download/> >
-> Utility

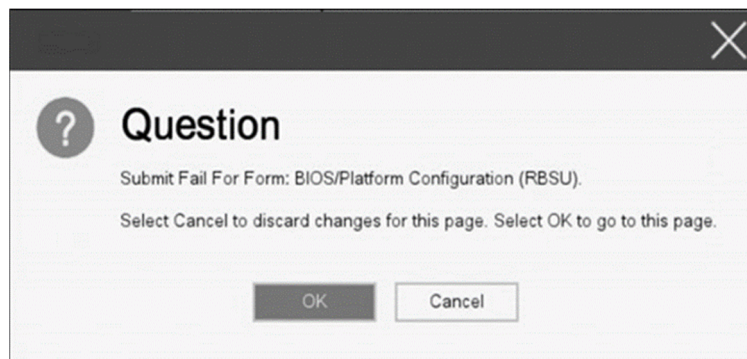
● Notice about service operation time of this product

The service operation hour of this product may require more hours than usual depending on the combination of the equipped firmware and driver.

2) Notice about the function of the System ROM

• Caution for the “Submit Fail For Form” Question pop-up

If you encounter the “Submit Fail For Form” Question pop-up while changing the configuration in the System Utilities, **discard the changes by pressing Cancel**. To apply the desired changes after that, reboot the server and re-enter the System Utilities. Selecting OK to continue the changes may cause some server settings such as Serial Number and Product ID to be lost.



• Caution for recovering from a Red Screen of Death (RSOD) screen

If you have changed the server configuration/settings or the system status, a Red Screen of Death (RSOD) screen appears in rare cases before starting up the OS. This may cause the server to become uncontrollable. However, the server may recover from the RSOD by turning off and then on the power again.

To recover from this condition, power off and then on the server again.

If the problem persists, contact your sales representative for maintenance.

```
X64 Exception Type 0x0E - Page-Fault Exception
RCX-0000000000001E0 BX-0000000000001E0 RB-000000000000000 R9-000000000000000
RSP-0000000059C711E0 BP-0000000059C71230 AX-000000000000000 BX-000000000000000
R10-0000000037FAF790 I1-0000000059C711A0 I2-0000000059C7120C I3-0000000059C71240
R14-0000000050C16724 I5-0000000050C1E0C9 SI-0000000048E69018 DI-0000000059C711E0
CR2-0000000059C7120C CR3-0000000059B01000 CR0-00010013 CR4-00000668 CR8-00000000
CS-00000030 DS-00000030 SS-00000030 ES-00000030 RFLAGS-00210206
MSR: 0x1D9 = 00004001, 0x345=0000F4C5, 0x1C9=0000000E

LBRs From To From To
01h 0000000059C7120C->0000000053B031AE 0000000037FAF007->0000000059C7120C
03h 0000000037FAF76F->0000000037FAF77F 0000000050C16737->0000000037FAF76C
05h 00000000520EB4DA->0000000050C16733 00000000520EB4B7->00000000520EB4C3
07h 0000000059C7E04B->00000000520EB41B 0000000059C7E094->0000000059C7E09B
09h 0000000059C7E06B->0000000059C7E07D 0000000059C7E04B->0000000059C7E059
0Bh 0000000059C7F6E3->0000000059C7E034 0000000059C7F52C->0000000059C7F6CF
0Dh 0000000053B029A->0000000059C7F520 0000000053B0C0A1->0000000053B0D29D
0Fh 0000000059C72BF0->0000000059C7E3D1 0000000053B031B9->0000000053B0E000

CALL ImageBase ImageName+Offset
00h 0000000059B71000( h)
```

• How to recover stop POST by the message of "Memory Initialization Start"

If the server stops POST by a message of "Memory Initialization Start", recover them by setting to the default value by SW6 of the system maintenance switch.

Refer to “Chapter 1 - 7.3.3 Set the System Configuration Back to Default Values” of the maintenance guide.

• About UEFI Serial Debug output on BIOS Serial Console

UEFI Serial Debug output could inadvertently be seen over BIOS Serial Console with System ROM v2.32 (03/09/2020). This issue would be seen periodically on server reboots. And, POST time will increase about 2 minutes. This issue has been fixed in System ROM v2.34 (04/09/2020).

● Notes on the Server Configuration Lock (SCL)

- (1) Set SCL function to disabled and operate the system.
- (2) Set the password when the SCL function is enabled and keep the password in a safe place. If you lose your SCL password and it is locked by the SCL function (stopped before booting the OS), you will not be able to unlock it and you will not be able to boot the server OS again.

You will be charged for recovery / recovery to the bootable state.

If you lose your SCL password, there is no way to clear it.

- (3) When you will be requesting maintenance, it is necessary to disable the SCL function.
If you cannot be disabled the SCL function, **maintenance will be a charged one.**
- (4) Set "Halt on Server Configuration Lock failure detection." option to disabled and operate the system. If it was enabled, when the SCL function detects an unrecoverable condition and is locked (stopped before the OS boots), the system utility will not be able to start and the server configuration lock will never be disabled.

You will be charged for recovering to the bootable state.

Unrecoverable conditions of SCL function:

- When the server boot is locked by the SCL function due to change in the RBSU settings.
- When the server boot is locked by the SCL function due to the update of firmware, and the original firmware version cannot be restored.
- When the server boot is locked by the SCL function due to a failure of the DIMM or PCI option card

● Notice of the backup and restore of RBSU Settings by REST ful interface tool.

In the case of iLO5 firmware version 2.40 or later, backup and restore of RBSU Settings should be done from "Backup and Restore Settings" menu under System Utilities. (See "Backup and Restore of RBSU Settings" in Maintenance Guide (Common).)

● About change of specification in Fault tolerant memory function (ADDDC)

Specification of the Fault tolerant memory function (ADDDC) has been changed by firmware update. Change points are below.

- For the system ROM Version 2.00 (02/02/2019) or later
Even if the system has other than 8 or 12 DIMMs per channel but has the fault tolerant memory function (ADDDC) available configuration, the system will change its setting automatically and starts to use this function.
- For the system ROM Version 2.10 (05/21/2019) or later
 - The Fault tolerant memory function (ADDDC) can be used even if the amount of RANK number per channel does not exceed 2.
 - N8102-709 becomes ready for use of the fault tolerant memory function (ADDDC).

● About the internal DVD-ROM (N8151-137/138) display

When System ROM Version v 2.00 (02/02/2019) or later and Embedded SATA Configuration setting (* 1) is set to [Smart Array SW RAID Support], two internal DVD drive information is displayed in the Disk Utilities menu (* 2) depending on the operating environment.

Both can refer to the same internal DVD information.

(*1) 「System Configuration > BIOS/Platform Configuration (RBSU) > Storage Options > SATA Controller Options > Embedded SATA Configuration」

(*2) 「System Configuration > HPE Smart Array S100i SR Gen10 > Disk Utilities」

● Factory settings on the following items of BIOS/Platform Configuration (RBSU) are as below.

- (1) System Configuration > BIOS/Platform Configuration (RBSU) > Workload Profile : Custom
- (2) System Configuration > BIOS/Platform Configuration (RBSU) > Power and Performance Options > Minimum Processor Idle Power Core C-State : No C-states
- (3) System Configuration > BIOS/Platform Configuration (RBSU) > Power and Performance Options > Minimum Processor Idle Power Package C-State : No Package States

● "IPMI Watchdog Timer Timeout" may be logged in the iLO event log (IEL)

When System ROM is v2.62 (03/08/2022) and the **IPMI Watchdog Timer** option is set to **Disabled** (factory setting), the following "IPMI Watchdog Timer Timeout" may be logged in the IEL:

iLO IPMI Watchdog Timer Timeout: Action: None, TimerUse: 0x44, TimerActions: 0x00.
Event Class: 0x23
Event Code : 0xB3

Recovery procedure:

This problem will be solved by exercising either of the recovery options (A or B) described below.

Recovery option A

1. Power off the server. Then disconnect the plug from the outlet.
2. Wait for 30 seconds. Then plug the server into the outlet again.

Recovery option B

In System Utilities, change the setting of the **IPMI Watchdog Timer** option two times as follows:

1. Power on the server.
2. During the POST, press the F9 key to start System Utilities.
3. In **System Configuration**, select **RBSU > System Options > Server Availability**. Then set the **IPMI Watchdog Timer** option to **Enabled**.
4. Press the F12 key, save the change, and then restart the system.
5. During the POST, press the F9 key to start System Utilities again.
6. In **System Configuration**, select **RBSU > System Options > Server Availability**. Then set the **IPMI Watchdog Timer** option to **Disabled**.
7. Press the F12 key, save the change, and then restart the system.

● About the System Utility and One-Time Boot Menu display

- (1) To protect the change permissions on the menu under BMC Configuration Utility, enable BMC Configuration Utility > Setting Option > Require user login and configuration privilege for BMC Configuration.

It isn't protected by setting of BIOS/Platform configuration (RBSU) > Server Security > Set Admin Password.

- (2) The Maximum Size and Installed Size of L2 and L3 cache in "System Information > Processor Information" are indicated by the values that a 1MB is converted into 1024000 bytes.
When the version of System ROM is v2.00 (02/02/2019) or later, it is indicated by converting 1 MB to 1048576 bytes.

- (3) The mouse cursor may turn into a black square indication when System Utilities screen or One-Time Boot menu is displayed. This is just an indication problem, and the operations of System Utilities work normally. This phenomenon can be solved by operating the mouse.

- (4) In the PCIe Device Configuration menu of BIOS/Platform Configuration (RBSU) (*) and in One-Time Boot Menu, the name of a RAID controller may not be correctly displayed on the following conditions:

- For N8103-189, N8103-190, N8103-191, N8103-192, N8103-193, N8103-194, N8103-195, N8103-196, N8103-197, N8103-201, N8103-237, or N8103-238

The above problem occurs if both of the following conditions are met:

1. The version of the RAID controller firmware is v4.11 or higher, or v3.01.04.072 or higher.
2. The version of System ROM is lower than v2.68 (07/14/2022).

However, the problem does not affect a boot from the HDD/SSD managed by the RAID controller.

* Select BIOS/Platform Configuration (RBSU) > PCIe Device Configuration.

● About the PCIe Slot X MCTP Broadcast Support menu (X is PCIe Slot number)

In the device with the system ROM version v2.10 (05/21/2019) or later, when the PCIe MCTP Options menu is selected (as described in *1 below) for the first time, the pop-ups (*2) informing that the settings for the device will be forcibly set to default will be displayed as many as the number of settable PCIe slots.

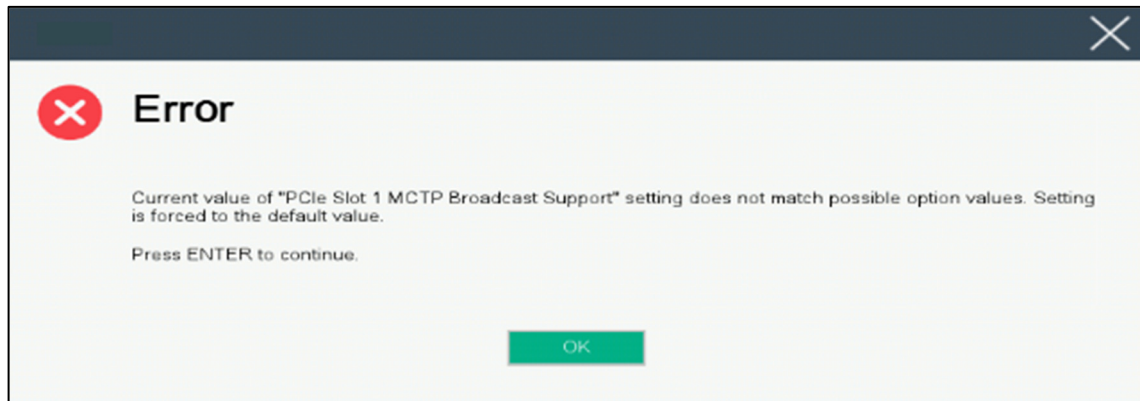
When PCIe MCTP Options menu (*1) for the first time, the pop-ups (*2) with the contents to force the default settings is displayed.

Meanwhile, in the device with the system ROM of the following versions, when the settings are tried to be saved, the pop-up (*3) appears and the settings are not saved. As a result, the pop-ups (*2) will be displayed as many as the number of the PCIe slots every time this menu is displayed. In this case, MCTP Broadcast always operates in an enabled state.

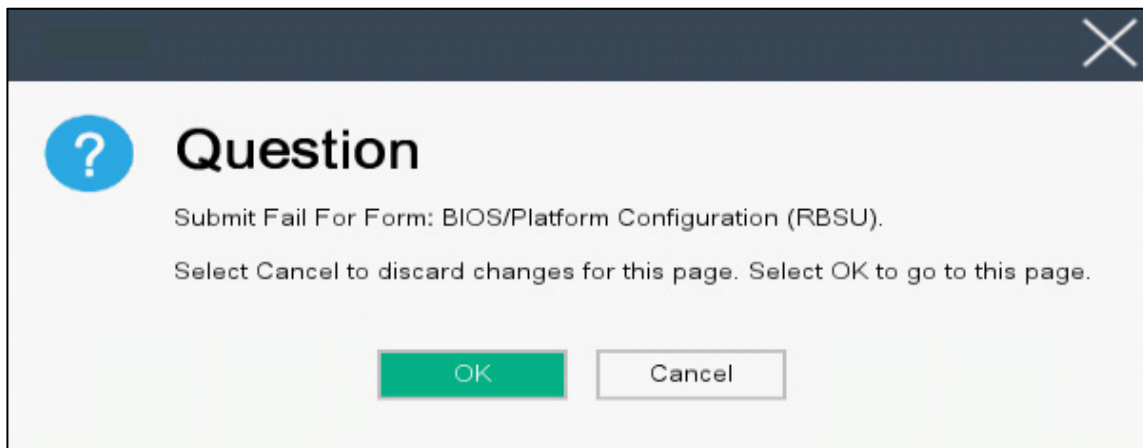
- v2.22 (11/13/2019)
- v2.32 (03/09/2020)

*1 : System Configuration > BIOS/Platform Configuration(RBSU) > PCIe Device Configuration > Advanced PCIe Configuration > PCIe MCTP Options

*2 :



*3 :



- **About set value of Extended Memory Test option**

When System ROM Version is v2.36 (07/16/2020), Extended Memory Test option is set to "Disabled" automatically after a system reboot.

System Configuration > BIOS/Platform Configuration (RBSU) > Memory Options > Extended Memory Test

- **Server may become unresponsive during Network PXE Boot**

When System ROM versions are below v3.10 (02/22/2024), the server may occasionally become unresponsive when booting via Network PXE Boot with an OS. If this issue occurs, please follow one of the procedures below to restart the server:

- a) Press and hold the power button to turn off the server. Then, press the power button again to turn on the server.
- b) Select "Power" -> "Press and Hold" from the iLO Web Interface to turn off the server. Then, select "Power" -> "Momentary Press" from the iLO Web Interface to turn on the server.

This issue has been fixed in System ROM v3.10 (02/22/2024).

3) Notice about the function of the iLO5

● Caution about Reset iLO

Do NOT Reset iLO during the period from server boot start to the completion of OS boot. This period includes the execution of POST (Power On Self Test)
Do NOT Reset iLO while users are using the System Utilities.

Under such circumstances, restarting the iLO may cause unexpected result.
For example, while changing options of the System Utilities, Reset iLO may lead to loss of server settings such as Serial number and Product ID. If the iLO is reset during POST execution, the screen display of UUID and UUID logic in iLO Web Interface : [Information] - [Overview], may be corrupted. Please turn off and turn on the power this product.

iLO Resets which is subject to this caution

- Reset iLO via network such as iLO Web interface
- Reset iLO via UID switch

* Refer to Caution for operating "BMC Configuration Utility" in the System Utilities below, for the cases where iLO is reset after changing the settings in "BMC Configuration Utility" in the System Utilities.

● Caution about iLO time function

This caution is for iLO firmware version lower than 1.45.

In case that SNTP setting is disabled, and if the iLO is reset, iLO time may be slipped.

It is recommended that SNTP is set enabled at iLO Web interface.

For the details of iLO SNTP setting, please refer to iLO5 User's Guide.

● Caution about iLO Downgrade Policy

In case that iLO License for Remote Management is installed with iLO5 firmware 1.40 or latest, Do NOT set "Permanently disallow downgrades" in [Security] - [Access Setting] - [Update Service] - [Downgrade Policy] setting.

If the setting "Permanently disallow downgrades" is set, downgrade of any firmware cannot be done afterward. The setting of this "Permanently disallow downgrades" is permanent and irreversible, and users cannot change this setting from any iLO interfaces or any utilities.

This setting cannot be removed by setting "Set to factory defaults" and the setting "Permanently disallow downgrades" is kept unchanged.

● Caution about iLO security function

In case that iLO5 firmware 1.40 or latest is used,  is always displayed in [Information] - [Security Dashboard] and in iLO Web interface screen.

Depending on the setting of RBSU or iLO, the status of security may be displayed in red showing security is at Risk. Please set security settings appropriately in order to follow customer's security policy.

For the recommended settings, please review the iLO5 User's Guide.

For the settings of "Require Host Authentication", please refer to the other descriptions of **Caution for the case where Admin Password is set from System Utilities(*1), or the case where the setting "Require Host Authentication" is enabled from iLO Web interface(*2).**

The matching condition is different by iLO5 Firmware version.

iLO5 Firmware	matching condition(s)
Version 1.40	(*1), and (*2)
Version 1.43 and later	(*2)

The iLO security icon on the right upper portion of Web interface may be transparent even if "Overall Security Status" of [Security Dashboard] is "Risk".

"Overall Security Status" of [Security Dashboard] indicates the current security status.

- **Caution for the case where Admin Password is set from system utility (*1), or the case where the setting “Require Host Authentication” is enabled from iLO web interface (*2).**

(*1) This caution is for iLO firmware version lower than 1.43.

“System Configuration > BIOS/Platform Configuration (RBSU) > Server Security”
Set password by “Set Admin Password option”

(*2) This caution is for iLO firmware version 1.40 and higher.

Don't set “Require Host Authentication” Enabled in “Security > Access setting > iLO”

When the setting described above is executed, the following symptoms are expected

- Many messages “Remote Insight/Integrated Lights-Out Unauthorized Login Attempts” are displayed in alert viewer.
- Error occurs, when Starter Pack (Standard Program package) is applied.

The following services and functions are not supported

- Report services for hardware faults in Express Report Service
- Report services in RAID Report Service
- Function to display Device information and configuration collected by iLO
- Function to collect event logs collected by iLO

- **About the corrupted screen display of UUID in iLO Web interface**

If the iLO is reset during POST execution, the display of UUID and UUID logic in iLO Web interface : [Information] - [Overview] page may be corrupted.

When any corrupted texts are displayed, please turn off and on the system.

- **Caution about Virtual NIC settings on iLO Web interface**

The default value for “Virtual NIC” in [Security]-[iLO] depends on the version of the iLO 5 firmware.

Check the following when “Set to factory default” is executed in the BMC configuration utility.

(1) If you use iLO 5 firmware version between 2.10 and 2.18, The default value of “Virtual NIC” is “Enabled”.

A warning may be displayed for “Virtual NIC” on the device manager of Windows Server 2012 R2 which does not support virtual NIC or Windows Server 2016/2019/2022 where USB CDC-EEM driver is not installed.

If you do not use the iLO virtual NIC functionality, go to [Security] > [iLO], and disable “Virtual NIC”.

(2) If you use iLO 5 firmware version between 1.40 and 1.47 or 2.31 or later, The default value of “Virtual NIC” is “Disabled”.

When you run “Set factory defaults” on BMC Configuration Utility, [Security] > [iLO] > “Virtual NIC” will be “Disabled”.

- **Caution about IPv6 address of Network Adapter on iLO Web interface if vEthernet(Hyper-V Virtual Ethernet Adapter) is configured on Windows**

If iLO version between 2.10 and 2.18 below is used and vEthernet(Hyper-V Virtual Ethernet Adapter) is configured on Windows, “IPv6 Address” of [Network Ports] in each Adapter may be not accurate on [Information] > [Network] > [Physical Network Adapters].

Please confirm The Property of each network adapter on Windows, if vEthernet(Hyper-V Virtual Ethernet Adapter) is configured on it.

- **Displaying Network information in the iLO web interface**

If iLO version 2.31 or later is used and Bridge of network is configured on OS, the information in each Adapter may be not accurate on [Information] > [Network] > [Physical Network Adapters].

Please confirm The Property of each network adapter on OS, Bridge of network is configured on it.

- **Caution for the Security Dashboard of iLO Web interface**

If you update to iLO5 firmware greater than or equal to 1.43 and lower than 2.10, “Last Firmware Scan Result” is displayed in “Information > Security Dashboard”. Do not click this Hyperlink.

If you click this link by mistake, you won't be able to move between menus and tabs.

In that case, you need to reload the page by the reload button of the browser.

Or you log out the current session of iLO Web interface, and please log in again.

Information - Security Dashboard			
Overview Security Dashboard Session List iLO Event Log Integrated Management Log Active Health System Log Diagnostics			
Overall Security Status : OK			
Security State Production Server Configuration Lock: Disabled			
Security Parameter	↓Status	State	Ignore
Security Override Switch	♥ OK	Off	☐
IPMI/DCMI Over LAN	♥ OK	Disabled	☐
Minimum Password Length	♥ OK	OK	☐
Require Login for iLO RBSU	♥ OK	Enabled	☐
Authentication Failure Logging	♥ OK	Enabled	☐
Secure Boot	♥ OK	Enabled	☐
Password Complexity	♥ OK	Enabled	☐
Require Host Authentication	♥ OK	Disabled	☐
Last Firmware Scan Result	♥ OK	OK	☐

● About Storage Information of iLO web interface

If you are using the iLO5 firmware 3.00 or later

iLO 5 may not retrieve Storage Information after server reboot.

In this case in the iLO 5 web interface, under "System Information," clicking on the "Storage" tab displays the following:
"Failed to retrieve complete storage device information. Refresh the page in a few minutes."

If above the message is displayed on "storage" page in iLO web interface, please run the iLO reset.

● Displaying Device Inventory information in the iLO web interface

< Enviroment with R120h-1E has LOM card (N8104-193/194/195) >

System ROM version lower than v2.34(04/08/2020), LOM card's information might be displayed as follows, but it does not affect server operation and LOM card operation.

- Location : Unspecified
- Firmware Version : N/A
- Status : Unknown

< Enviroment with SAS Expander card (N8116-51) >

iLO firmware version 2.31 or later, SAS Expander card information might be displayed as follows, but it does not affect server operation and SAS Expander card operation.

- Firmware Version : N/A
- Status : Disabled

● What todo when corruption of SNMP alert about the physical drive status changed is recived?

When you recived the corrupted SNMP alert about physical drive status changed,confirm the location information of the same event at "Information" - "Integrated Management log" of iLO5 Web interface.

e.g.:

Abnormal, physical drive status change detection,iLO SNMP Trap,mgr_WIN-U6HIIHPNIH1Q,uru-rhel83,192.168.0.57,,2021/10/01 15:22:57,iLO,0xc0000be6,"A physical drive status change has been detected. Current status is 3.
(Location: ot 12 Controller: Slot 12)","If the physical drive status is 'failed(3)', 'predictiveFailure(4)',

● About status of Agentless Management Service(AMS) on iLO Web interface.

When you received the corrupted SNMP alert about physical drive status changed, confirm the location information of the same event at "Information" - "Integrated Management log" of iLO5 Web interface.

When status of Agentless Management Service(AMS) is "Unknown" or "Not available"(*) on iLO Web interface, please reset iLO.

After about 10 minutes, please restart Agentless Management Service(AMS) by following procedures.

* Verifying AMS status

Please confirm the status from iLO Web interface : [System Information] - [Summary] – [Subsystems and Devices] - "Agentless Management Service".

If the status of Agentless Management Service(AMS) is "Unknown" or "Not available", iLO can't collect some part of information of storage, network and iLO can't display those information correctly.

< Restarting AMS >

Procedure

▪ Windows

Navigate to the Windows Services page and restart AMS.

▪ Red Hat Enterprise Linux 7.x and 8.x

Enter the following command:

```
# systemctl restart smad
# systemctl restart amsd
```

▪ ESXi6.5/6.7

Enter the following command:

```
# /etc/init.d/amsd.sh restart
or
# /etc/init.d/ams.sh restart
```

* Command depends on the version of AMS you are using

▪ ESXi7.0

Enter the following command:

```
# /etc/init.d/amsd restart
```

● About Java IRC session timeout message.

While Integrated Remote Console (Java IRC) is launching, the pop-up messages indicate the IRC session expired appear after that session has expired. At the same time, irrelevant popup appears too together.

When the following message in bottom layer of Java IRC window, ignore description in displayed pop-up message.

- "Sessions Closed due to Timeout or Unauthorized Access."

● Note About Rapid Setup

If you are using the iLO5 firmware 2.71 or 2.72:

Before using Rapid Setup for configuring the Smart Array SW RAID on your system, open the iLO web interface, go to [System Information] > [Device Inventory], and then confirm that "Status" of Smart Array S100i SR is "Enabled". During a POST after that, press the F10 key, select [Provisioning] > [EXPRESSBUILDER], and then run Rapid Setup.

If "Status" is "Unknown", running Rapid Setup may display "Preparing recommended RAID configuration" and then the following message:

- "Rapid Setup did not find any supported disk installed on this system.
Either there is no disk installed, or there is a cabling or other problem.
Please exit Rapid Setup and check your hardware configuration."

● Possible high-speed fan rotation and abnormal sound

If you are using the iLO5 firmware 2.90 or later

Restarting the server can on rare occasions rotate the fan at high speed and emit an abnormal sound.

If this state continues for more than seven minutes, restart the server again.

● SNMP Alert

If you are using the iLO5 firmware 3.00 or later

For NEC ESMPRO Manager, the Alert Viewer notifies you of a change in a physical-drive status when it is detected. Depending on the status, the location information is displayed in either of the following two patterns:

1. (Location: Slot=(A):Port=(B):Box=(C):Bay=(D) Controller: <NULL>)
2. (Location: Port=(B):Box=(C):Bay=(D) Controller: Slot (A))

A: Controller location (slot number)

B: The port number of the physical drive

C: box number of the physical drive

D: The bay number of the physical drive

● Caution about Using Cipher Suite for Intelligent Platform Management Interface (IPMI)

iLO 5 does not support IPMI Cipher suite 17. If you run the "ipmitool" utility version 1.8.18 with the interface specified as "lanplus" and cipher suite as "17" for an iLO 5, the following error will be displayed.

Error in open session response message: no matching cipher suite

Error: Unable to establish IPMI v2 / RMCP+ session.

● VROC SATA RAID

If you are using the iLO5 firmware 3.04 or later

When the VROC SATA RAID is configured, the drive information is not displayed under [System Information] - [Storage] - [Drives] in the iLO web interface, and "Unconfigured-Drives" is displayed.

Refer to the drive information under the VROC SATA RAID configuration using the Intel VROC GUI or Intel VROC CLI on the OS.

For more information, see the Intel® Virtual RAID on CPU Utility VROC8 User Guide.

4) Notice about the OS

● About EXPRESSBUILDER Manual Installation

Partitions in the target disk are deleted when you install the Windows by EXPRESSBUILDER even if you select the "Manual" option.

Pay attention to the user data stored in the system drive when re-installing Windows.

● Notice of Windows Server

When the USB device is used in supported Windows Server OS, the next event log is sometimes registered. But ignore this message since it does not cause any problem for the operation.

```
< Event Log >
ID                  : 1
Source              : VDS Basic Provider
Level              : Error
Unexpected error occurred. Error code :32@01000004
```

● Notice of Agentless Management Service (AMS) on the server running Windows Server OS

The server running a Windows Server 2012 R2, Windows Server 2016, or Windows Server 2019 operating system with Agentless Management Service (AMS) version 1.40.0.0 installed, the ams.exe process will exhibit an increasing handle count. Handle leaks can cause performance issues overtime due to over consumption of memory.

◆ This symptom is fixed in the Agentless Management Service (AMS) 1.43.0.0.

This AMS is included in the Starter Pack. Please apply the Starter Pack Version S8.10-006.03 or later. If the AMS 1.40.0.0 is already installed in your server, and you want to apply Starter Pack Version S8.10-006.03, you need to update the AMS separately. For further explanation about the updating, please check the Starter Pack website.

◆ If you want to use Agentless Management Service (AMS) 1.40.0.0, please do the following steps to stop the increasing of the handle count.

(1) Stop the AMS service by typing "net stop ams" in a command prompt.

(2) Explore to C:\Program Files\OEM\AMS\Service folder.

(3) Rename the file storelib.dll to storelib.dll.bak

(4) Start the AMS service by typing "net start ams" in a command prompt.

(*1) The following message may be displayed when stopping AMS, but there is no problem.

```
A system error has occurred.
System error 1067 has occurred.
The process terminated unexpectedly.
The Agentless Management Service service was stopped successfully.
```

(*2) The following message may be displayed when starting AMS, but there is no problem.

```
The requested service has already been started.
```

◆ There are 2 ways to check the version of Agentless Management Service (AMS).

- The way to confirm on the OS of the target system.

(1) Run the following command on Windows PowerShell.

```
> Get-WmiObject Win32_Product | Select-Object Name,Version | Select-String "Agentless Management Service"
```

(2) Check the version from the command result.

- The way to confirm on the remote system with using iLO Web I/F.

(1) Login to iLO Web I/F with Web browser on the remote system.

(2) Select the "Firmware & OS Software" on the left menu, and then select "Software".

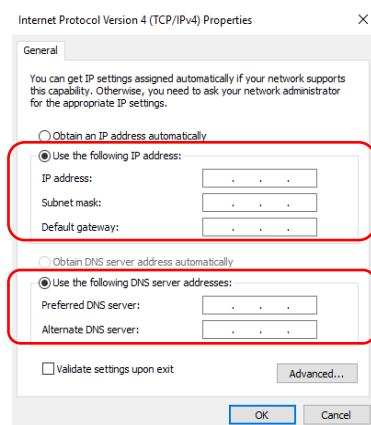
(3) Check the version of "ams.exe" displayed in "Product Related Software".

● Notes on changing configuration of CPU board after setting up Windows Server 2019/2016/2012 R2

When a fixed IP address or DNS is set for the following options, add a CPU board by the following procedure.
(The procedure is necessary to take over the fixed IP address setting even after the CPU expansion.)

N8104-173 Dual Port 10GBASE-T LOM Card
N8104-177 Dual Port 25GBASE SFP+ LOM Card
N8104-182 Dual Port 10GBASE-T Adapter (2ch)
N8104-183 Dual Port 10GBASE-T Adapter (2ch)
N8104-185 Dual Port 10GBASE SFP+ Adapter
N8104-187 Dual Port 25GBASE SFP28 Adapter
Expanded PCI Card with PCI-to-PCI bridge

- (1) Change settings such that the service that refers to the relevant option does not start up automatically and stop service. In addition, when the storage is connected to the option, remove the LAN cable from the option before the following work so that the option does not recognize the storage.
- (2) When setting LAN teaming at the option, cancel teaming.
- (3) Record IP address of the options / sub netmask / default gateway / preferred DNS server / alternate DNS server (the parts in the red frames below.)



- (4) Change the settings of the option as follows: “Obtain an IP address automatically”, for IP address and “Obtain DNS server address automatically.” for DNS address.
- (5) Follow the user’s guide to add a CPU board.
- (6) Set IP address /sub netmask / default gateway / preferred DNS server / alternate DNS server, which are recorded in Step 3), to the option.
- (7) Set LAN teaming again.
- (8) Set up again the service whose setting was changed in Step 1) so that the service starts automatically. When the option is connected to storage, connect the LAN cable again such that the option can recognize the storage.

Tips

If you do not follow above procedure, a message appears, telling for example, that the fixed IP address is used by another device, and you may not be able to set a fixed IP address.

In that case, execute the commands below by command prompt and boot the device manager. Then, click [View] - [Show hidden devices] and expand the network adapter tree, and then delete the grayed out devices that are not in use.

```
>set devmgr_show_nonpresent_devices=1  
>Start DEVMGMT.MSC
```

When you refer to network of NEC ESMPRO Manager, a duplicate network card will be displayed after the configuration of the expanded CPU board is changed CPU processor kit. Please ignore the network device that is not displayed on the OS, and the detail information of the network device will be displayed as “Unknown”.

• Note on using NEC ESMPRO Manager (Windows) and Express Report Service (MG)

Depending on the combination of iLO firmware version of this product with NEC ESMPRO Manager (Windows) and Express Report Service (MG) (Windows), it may be necessary to update NEC ESMPRO Manager (Windows) and iLO Receiving Information (ilo_en.mtb). Please refer to the end of this chapter to confirm/update to the latest version, if needed.

◆Phenomena regarding NEC ESMPRO Manager (Windows)

iLO firmware version	NEC ESMPRO Manager (Windows) Version	Phenomena
2.10 or higher	Lower than 6.25	- Configuration Tab - Server Status screen "SNMP Alert setting" will show error message "Failed to get SNMP Alert setting". - Remote Control Tab - iLO Information - Show IML or Save IML NEC ESMPRO Manager will fail to get IML information and Show IML or Save IML feature will not work. - AlertViewer New Alerts of hardware failure added with firmware update will be displayed as "Unknown" alert on AlertViewer.
	Lower than 6.47	AlertViewer New Alerts of hardware failure added with firmware update will be displayed as "Unknown" alert on AlertViewer, or they will not be displayed on AlertViewer.

◆Updating NEC ESMPRO Manager Ver 6 (Windows)

- (1) Download the latest version of NEC ESMPRO Manager from the following website.

<https://www.58support.nec.co.jp/global/download/index.html>

- ESMPRO tab
- NEC ESMPRO Manager

- (2) Update NEC ESMPRO Manager. For details, refer to Chapter 2 Installation in "NEC ESMPRO Manager Ver. 6 Installation Guide (Windows) [PDF]".

◆Updating NEC ESMPRO Manager Ver 7 (Windows)

- (1) Download the latest version of NEC ESMPRO Manager from the following website.

<https://www.58support.nec.co.jp/global/download/index.html>

- ESMPRO tab
- NEC ESMPRO Manager

- (2) Launch the ESMPRO installation tool included in the ESMPRO Platform Management Kit.

- (3) On the "Installation Tools screen" click on "Instructions", then from Software Manuals click on "ESMPRO/ServerManager."

- (4) Click on "ESMPRO/ServerManager Ver.7 Installation Guide (Windows)".

- (5) For more details on "Update NEC ESMPRO Manager from Ver 6 to Ver 7", refer to Chapter 2 Installation in "NEC ESMPRO Manager Ver. 7 Installation Guide (Windows) [PDF]".

◆Phenomena regarding iLO Receiving Information (ilo_en.mtb)

* Intend for users of NEC Express Report Service (MG)

iLO firmware version	iLO Receiving Information Version	Phenomena
2.10 or higher	ilo_en.mtb Lower than 1.4.0	It is impossible to detect a failure of the hardware added along with the update of hardware and to issue an alert of this failure. * If iLO Receiving Information has been updated and NEC ESMPRO Manager has not been updated, it is impossible to detect the failure of the added hardware and issue the alert of the failure, as with the above.
	iml_en.mtb Lower than 1.5.0	
	* There are 2 kinds of iLO Receiving Information.	

◆ Updating iLO Receiving Information

- (1) Download the latest version of iLO Receiving Information (ilo_en.mtb, iml_en.mtd) from the following website.
<https://www.58support.nec.co.jp/global/download/index.html>
 - ESMPRO tab
 - Express Report Service (MG) (Windows) Receiving Information
 - iLO.zip
 - (2) Delete current Receiving Information from Express Report Service (MG) (Windows).
For details refer to "3.1.5 Setting for Receiving Information" or "3.2.4 Setting for Receiving Information" in "Express Report Service (MG) Installation Guide (Windows)".
 - (3) Set the latest version of Receiving Information downloaded in step (1) to Express Report Service (MG)
- * Download "Express Report Service (MG) Installation Guide (Windows)" from the following website.
<https://www.58support.nec.co.jp/global/download/index.html>
 - ESMPRO tab
 - Express Report Service (MG) (Windows)

◆ The steps of confirmation for iLO FW version

- Server Health Summary
Push the UID button on the server and check the version of the iLO firmware on the console connected to the server.
(For the detail, refer to Server Health Summary in iLO5 user guide.)
- Remote
Check the version of the iLO firmware on "Firmware & OS Software - Installed Firmware" by iLO web interface.

◆ The steps of confirming version for NEC ESMPRO Manager (Windows)

- (1) Log in NEC ESMPRO Manager.
- (2) Click the "About NEC ESMPRO Manager" link at the top right of the screen.
- (3) Confirm the version information of NEC ESMPRO Manager.

◆ The steps of confirming version for iLO Receiving Information (ilo_en.mtb, iml_en.mtd)

Confirm the version of "iLO SNMP Trap" in "Setting for receiving information" screen.
Regarding "Setting for receiving information" screen, refer to 3.1.5 Setting for Receiving Information or 3.2.4 Setting for Receiving Information in "Express Report Service (MG) Installation Guide (Windows)".

● Note on using VMware ESXi

This caution is about the screen display of VMware vSphere : Monitor > Hardware > System Sensor > Sensor when the ESXi is booted.

- (1) There are cases where the following Heartbeat Lost sensor displays "Warning(Yellow)".

[Device] I/O Module (n) LOM_Link_P (n) : Heartbeat Lost-Assert

[Device] I/O Module (n) NIC_Link_P (n) : Heartbeat Lost-Assert

*n represents LAN port number P1-P4

<Environment :iLO5 firmware 1.30、1.35、1.38 is applied >

In case that the screen display of Heartbeat Lost sensor Health (vCenter : Status) shows "Warning (Yellow)" after ESXi completes boot, for the ports whose cables are connected, the "Warning (Yellow)" will disappear and turn to "Normal (Green)" within a couple of minutes after connecting LAN cable. Please wait for a couple of minutes. For the ports without LAN cables, the "Warning (Yellow)" will be continuously displayed, but this does not indicate hardware malfunction and there is no impact to the system operation. Please continue operating the system as is. If a LAN cable is connected and the "Warning (Yellow)" does not disappear, there is a possibility that the connection of the cable is bad, so please check the LAN cable connection.

<Environment iLO5 firmware : 1.40 or latest is applied>

In case that the screen display of Heartbeat Lost sensor Health (vCenter : Status) shows "Warning (Yellow)" after ESXi completes boot, the "Warning (Yellow)" will disappear and turn to "Normal (Green)" within a couple of minutes. Please wait for a couple of minutes.

(2) In case of non-redundant FAN configuration, there are cases where the screen display of following sensor Health (vCenter : Status) shows "Warning (Yellow)" after ESXi completes boot, This "Warning (Yellow)" does not indicate hardware malfunction and there is no impact to the system operation.

- Cooling Unit 1 Fans

(3) There are some cases where the screen display of following sensor Health (vCenter : Status) shows " ? " after ESXi completes boot, this does not indicate hardware malfunction and there is no impact to the system operation.

- System Chassis 1 UID

● Notes for using TPM in VMware ESXi

If your system has TPM kit (N8115-35) and OS is VMware ESXi with System ROM Version v 2.00 (02/02/2019) or later and the, should be used "TPM 2.0" in TPM Mode.(*1).

PSOD (Purple Screen of Death) occasionally occurs when TPM Mode is set to "TPM 1.2".

(*1) The factory default setting is "TPM 2.0".

Check TPM Mode and change setting from the following menu.

Menu Location : System Utilities > System Configuration > RBSU > Server Security > Trusted Platform Module Options

Indicating : Current TPM Type

Settings : TPM Mode Switch Operation

● Change of RAID monitoring and reporting method

If VMware ESXi uses N8103-189/190/191/192/193/194/195/196/201/237/238/240 RAID controller and N8103-239 SSD Adapter for OS Boot, the RAID monitoring report will be changed to snmp trap reporting.

For details, please check the following website.

NEC Support Portal

http://www.58support.nec.co.jp/global/download/N8103-239/WBEM_uninstall_en.pdf

● Cautions on using Linux OS

Use the device name of LOM or optional NIC which the OS automatically recognizes. When adding a unique udev rule, do not change or fix the NIC device name based on the PCI address.

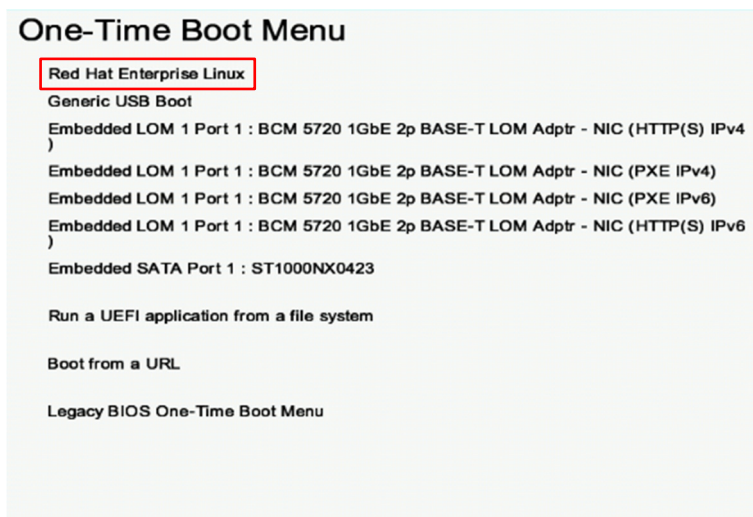
In addition, do not use the storage device name under /dev/disk/by-path/ that includes the PCI address.

If operation using a device name based on the PCI address is required, do not add/remove the card to/from the PCI slot, or change the CPU configuration. If the PCI bus address information changes and the name of the PCI-connected device is affected, you may not be able to access the network or storage, and the system may not boot normally.

● Cautions on using Red Hat Enterprise Linux 8.5 or earlier

Select "OS Boot Manager" when booting OS from "One-Time Boot Menu".

Selecting an OS boot device such as HDD/SSD on the "One-Time Boot Menu" may cause RSoD (Red Screen of Death).



One-Time Boot Screen

5) Notice of the function in general

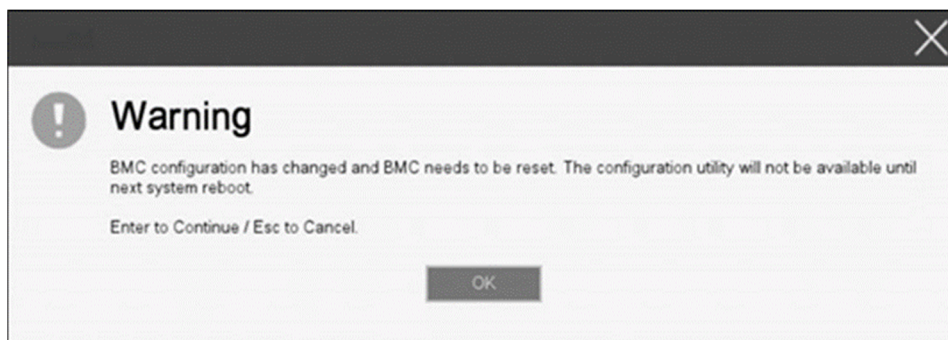
● Caution for operating BMC Configuration Utility in the System Utilities

If you execute POST or change the BMC configuration while rebooting the iLO, some server settings such as Serial Number and Product ID may be lost.

In addition, there is a possibility that it does not operate normally in the restart process immediately after.

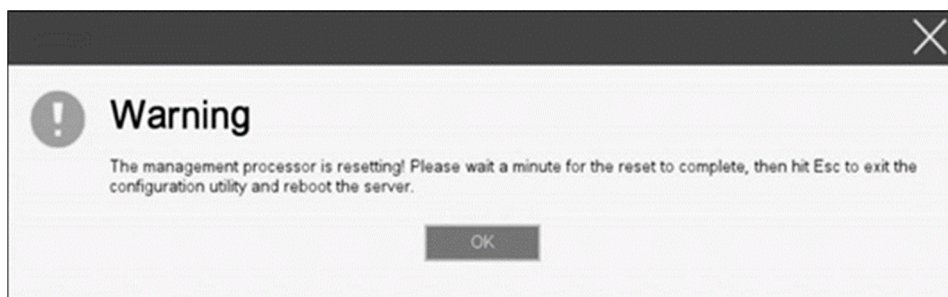
To avoid this trouble in rebooting the iLO, follow these steps:

- (1) In the System Utilities, changing the settings of BMC Configuration Utility may display the following pop-up before rebooting the iLO:



- (2) Press OK to proceed.

- (3) The iLO will start to reboot and then the following pop-up appears:



- (4) Leave this pop-up at least for one minute.

- (5) Confirm if the iLO reboot is completed.

※the iLO is restarting : the Status LED flashes in green (once per second) the iLO is operating normally through the restart completion : the Status LED lights in green.

- (6) If the confirmation succeeds, press OK to proceed.

- (7) Press the ESC key several times to return to the top screen of the System Utilities.

- (8) From the top screen, select Reboot the System to reboot the server.

● How to recover lost Serial Number and Product ID

If the server loses Serial Number and Product ID, recover them as follows:

- (1) Power off the server. Then disconnect the plug from the outlet.

- (2) Wait 30 seconds. Then plug the server into the outlet again.

- (3) Turn on the server with the POWER button.

- (4) The server starts up and the POST screen appears.

- (5) Press the F9 key to enter the System Utilities.

If this fails, initialize the RBSU settings with the system maintenance switch (refer to "Chapter 1 7.3.3 Set the System Configuration Back to Default Values" of the maintenance guide).

- (6) Check the values of Serial Number and Product ID by selecting the menu of the System Utilities: System Configuration > BIOS/Platform Configuration (RBSU) > Advanced Options > Advanced Service Options.
- (7) If the values of Serial Number and Product ID are satisfactory, go to step 14.
- (8) If the values are unexpected or lost, select the menu of the System Utilities: System Configuration > BIOS/Platform Configuration (RBSU) > System Default Options.
- (9) Select the Restore Default Manufacturing Settings option.
- (10) Select this option: Yes, restore the default settings.
- (11) The server restarts automatically and the POST screen appears.
- (12) Press the F9 key to enter the System Utilities.
- (13) Set the proper Serial Number and Product ID (indicated on the pull-out tab of the server) via the menu of the System Utilities: System Configuration > BIOS/Platform Configuration (RBSU) > Advanced Options > Advanced Service Options.



【Important】 Product ID is the model number like "N8100-2602F". Product ID is not PID.

- (14) If the RBSU settings have been changed from the defaults, check and configure the new values.

● About labels of server information

A label with the following information are attached on the top front edge of the server.

- Product code
- Serial number
- QR code
- Default iLO account information

Please record these informations before installing server for maintenance.

Other than the Express5800/R120h-2E 3.5-inch model, the label described the above information is attached on Pull-out Tab.

● Note on using UPS

- When connecting UPS to a serial port, set the items to "Disabled" in the following settings as below:
 - (1) System Configuration > BIOS/Platform Configuration (RBSU) > System Options > Serial Port Options > BIOS Serial Console and EMS > BIOS Serial Console Port → [Disabled]
 - (2) System Configuration > BMC Configuration Utility > Setting Options > Serial CLI Status → [Disabled]
- If the N8181-160 (power supply unit [800W/Platinum]) is used by redundant configuration, change the following settings:

System Configuration > BIOS/Platform Configuration (RBSU) > Power and Performance Options > Advanced Power Options > Redundant Power Supply Mode → [High Efficiency Mode (Auto)]

※ The customer set as High Efficiency Mode (Odd Supply Standby) or High Efficiency Mode (Even Supply Standby) is unnecessary for change above-mentioned.

● Changing the cooling setting

This topic pertains to the following Options:

N8150-551 300GB 15K Hot Plug 2.5-inch SAS HDD
N8150-552 600GB 15K Hot Plug 2.5-inch SAS HDD
N8150-553 900GB 15K Hot Plug 2.5-inch SAS HDD
N8150-602 900GB 15K Hot Plug 2.5-inch SAS HDD
N8154-107 2.5-inch Hot Plug Drive Cage Kit
N8154-120 2.5-inch Hot Plug Drive Cage Kit

If your HDD is any of the above, but its current cooling fan setting is Increased Cooling or Maximum Cooling, leave it as it is (i.e., no need to change the setting). With neither of the two specified, for the HDD's stable operation, please change the setting to Increased Cooling as follows:

◆ Procedure for changing the setting

- (1) Power on the server. During the POST, press the F9 key to start **System Utilities**.
- (2) Select **System Configuration > BIOS/Platform Configuration (RBSU) > Advanced Options > Fan and Thermal Options > Thermal Configuration**.
- (3) Change the setting to **Increased Cooling**.
- (4) Press the F12 key, save the change, and then restart the system.

Note:

Changing the cooling fan setting may increase the cooling fan speed, which depends on the operating environment for and the load on the system.

● Note on using N8116-84 SAS Expander Card

When updating firmware from this Starter Pack (Ver S8.10-009.01), please do NOT apply the following firmware update module (Ver.5.08).

[Package Name]

Supplement Update / Online ROM Flash Component for Linux (x64) ? HPE 12Gb/s SAS Expander Firmware for HPE Smart Array Controllers and HPE HBA Controllers
(firmware-smartarray2de15b6882-5.08-1.1x86_64)

Please check the following Starter Pack Version S8.10-009.01 public page for detailed application procedures.

[Starter Pack Version S8.10-009.01]

< <https://www.58support.nec.co.jp/global/download/> >

-> Document & Software

-> Rack

-> (Select your server model)

● Notes of using SAS controller (N8103-184)

When using N8103-184, "Status" of iLO Web interface [System Information] - [Storage] - [Storage Controller] is might display to "Unknown", but it does not affect server operation and SAS Controller operation.

● About FCoE function in N8104-173/177

The FCoE function (Fibre Channel over Ethernet) isn't supported with this product as NEC.

The FCoE function is enabled in N8104-173 in spite of the LOM firmware version, in N8104-177 with Family Firmware Version after 8.35.43.

It is recognized as the FCoE device on the OS, but when not using it from OS and drivers it does not cause any problem for the operation.

Please ignore detection of the following device.

-HPE 533FLR-T FCoE Device

-HPE 622FLR-SFP28 FCoE Device

● About Wake On LAN function in N8104-173

When using the Wake On LAN function with PORT2 in N8104-173 (Dual Port 10GBASE-T LOM Card), update the firmware version to 7.19.2 or higher in advance.

● About Smart Storage Battery

Smart Storage Battery is indicated with Energy Pack on the RBSU menu. Please paraphrase.

● About EXPRESSBUILDER Help

If the EXPRESSBUILDER help is different from Maintenance Guide, do not use the help but the guide.

A) The additional options by firmware update

■ About changing the BIOS/Platform Configuration (RBSU) menu

Some options are added or changed by firmware update of this product.
The additional options are listed below.

(1) Server Availability Menu

When you select **System Configuration > BIOS/Platform Configuration (RBSU) > System Options > Server Availability** from the System Utilities, the **Server Availability** menu appears.

For details about the additional options, see the table below.

Option	Parameter	Description
IPMI Watchdog Timer *1	[Disabled] Enabled	Use this option to enable a Boot Time (POST) IPMI compliant Watchdog Timer (WDT) that is disabled when an IPMI command is issued to the system by the user and will not automatically be disabled.
IPMI Watchdog Timer Timeout *1	10 Minute 15 Minute 20 Minute [30 Minute]	Use this option to set the wait timer before performing the desired timeout action on the server in the event of a server lockup.
IPMI Watchdog Timer Action *1	[Power Cycle] Power Down Warm Boot	Use this option to set the timeout action upon expiration of the watchdog timer due to a server lockup.

[]: Default setting

*1: an option usable with System ROM Version 2.54 or later.

(2) Diagnostics Options Menu

When you select **System Configuration > BIOS/Platform Configuration (RBSU) > System Options > Diagnostics Options** from the System Utilities, the **Diagnostics Options** menu appears.

For details about the additional options, see the table below.

Option	Parameter	Description
Embedded Diagnostics	[Enabled] Disabled	This product does not support it.

[]: Default setting

(3) Memory Options Menu

When you select **System Configuration > BIOS/Platform Configuration (RBSU) > Memory Options** from the System Utilities, the **Memory Options** menu appears.

For details about the additional options, see the table below.

Option	Parameter	Description
Memory Controller Interleaving	[Auto] Disabled	Use this option to control the Memory Controller Interleaving option. When set to Auto, the system will automatically enable or disable memory controller interleaving based on the configuration of the system. When set to disabled, the user may force disable memory controller interleaving. In certain memory configurations, setting this option to disabled has showed a performance benefit across all memory in the system. It is recommended to leave this option to set to Auto.
Opportunistic Self-Refresh	[Disabled] Enabled	When "Enabled" is selected, self-refresh of memory is performed when the main memory is in the idle state. When "Disabled" is selected, regular-refresh of memory is performed.

[]: Default setting

(4) Intel UPI Options Menu

When you select **System Configuration > BIOS/Platform Configuration (RBSU) > Power and Performance Options > Intel UPI Options** from the System Utilities, the **Intel UPI Options** menu appears.

For details about the additional options, see the table below.

Option	Parameter	Description
Direct To UPI (D2K)	[Auto] Enabled Disabled	When "Enabled" is selected, Latency of the last level cache is reduced. Please don't change this setting unless it's designated. This options appears on only dual processor configuration.

[]: Default setting

(5) Advanced Performance Tuning Options Menu

When you select **System Configuration > BIOS/Platform Configuration (RBSU) > Power and Performance Options > Advanced Performance Tuning Options** from the System Utilities, the **Advanced Performance Tuning Options** menu appears.

For details about the additional options, see the table below.

Option	Parameter	Description
Processor Jitter Control Optimization	Optimized for Throughput Optimized for Latency [Zero Latency]	This option optimizes the thresholds used when the Auto-tuned function detects fluctuations in processor frequency. Optimized for throughput allows only the amount of fluctuations that doesn't impact overall compute throughput. Optimized for Latency allows for a very small amount of occasional fluctuations to occur before reducing processor frequency. Zero Latency attempts to eliminate any frequency fluctuations.
IODC Configuration	[Auto] Enable for Remote Invltom Hybrid Push Invltom AllocFlow Invltom Hybrid AllocFlow Enable for Remote Invltom and Remote WvILF	Enable/Disable IODC (IO Direct Cache): Generate snoops instead of memory lookups, for remote Invltom (IIO) and/or WCILF (cores)

[]: Default setting

(6) Server Security Menu

When you select **System Configuration > BIOS/Platform Configuration (RBSU) > Server Security > Advanced Security Options > Advanced Security Options** from the System Utilities, the **Server Security** menu appears.

For details about the additional options, see the table below.

Option	Parameter	Description
UEFI Variable Access Firmware Control *1	[Disabled] Enabled	Use this option to allow the system BIOS to completely control certain UEFI variables from being written to by other software such as an OS. When Disabled is selected, all UEFI variables are writable. When Enabled is selected, all changes made by software other than the system BIOS to critical UEFI variables will be blocked. For instance, new boot options the OS attempt to add to the top of BootOrder will actually be placed at the bottom of the Boot Order. Note: When UEFI Variable Access Firmware Control is Enabled, some OS functionality may not work as expected. Errors may occur while installing a new OS.

[]: Default setting

*1: an option usable with System ROM Version 2.54 or later.

(a) Trusted Platform Module Options Menu

When you select **System Configuration > BIOS/Platform Configuration (RBSU) > Server security > Trusted Platform Module Options >** from the System Utilities, the menu appears.

For details about the additional options, see the table below.

Option	Parameter	Description
Omit Boot Device Event *1	[Disabled] Enabled	Use this option to record Omit Boot Device Event. If enabled, PCR Boot Attempt Measurements will be disabled and measurement in PCR[4] will not be recorded.

[]: Default setting

*1: an option usable with System ROM Version 2.80 or later.

(7) PCIe Devices Configuration Menu

When you select **System Configuration > BIOS/Platform Configuration (RBSU) > PCI Device Configuration** from the System Utilities, the **PCI Device Configuration** menu appears.

For details about the additional options, see the table below.

Option	Parameter	Description
Advanced PCIe Configuration	-	-

(a) Advanced PCIe Configuration Menu

When you select **System Configuration > BIOS/Platform Configuration (RBSU) > PCIe Device Configuration > Advanced PCIe Configuration** from the System Utilities, the **Advanced PCIe Configuration** menu appears.

For details about the additional options, see the table below.

Option	Parameter	Description
PCIe Bifurcation Options	-	-
PCIe MCTP Options	-	-

i. PCIe Bifurcation Options

When you select **System Configuration > BIOS/Platform Configuration (RBSU) > PCIe Devices Configuration > Advanced PCIe Configuration > PCIe Bifurcation Options** from the System Utilities, the **PCIe Bifurcation Options** menu appears.

For details about the additional options, see the table below.

Option	Parameter	Description
PCIe Slot XX Bifurcation	[Auto] Slot Bifurcated	If the device installed in the slot supports this capability, the "Slot Bifurcated" can be selected. When "Auto" is selected, the PCIe slot will train at the maximum width supported by the slot and end point. When "Slot Bifurcated" is selected, the PCIe slot will be bifurcated into two equal width slots. XX: 1/2/3... (XX appears as specific slot number by the processor or the riser card configuration.)

[]: Default setting

ii. PCIe MCTP Options

When you select **System Configuration > BIOS/Platform Configuration (RBSU) > PCIe Devices Configuration > Advanced PCIe Configuration > PCIe MCTP Options** from the System Utilities, the **PCIe MCTP Options** menu appears.

For details about the additional options, see the table below.

Option	Parameter	Description
PCIe Slot XX MCTP Broadcast Support	[Enabled] Disabled	Use this option to control the PCIe Management Component Transport Protocol (MCTP) Support for a given slot. This option can be used to disable MCTP support to a given PCIe endpoint that may not properly support this protocol. It is recommended that this option remain enabled for full system functionality. XX: 1/2/3... (XX appears as specific slot number by the processor or the riser card configuration.)

[]: Default setting

(8) Fan and Thermal Options Menu

When you select **System Configuration > BIOS/Platform Configuration (RBSU) > Advanced Options > Fan and Thermal Options** from the System Utilities, the **Fan and Thermal Options** menu appears.

For details about the additional parameter, see the table below.

Option	Parameter	Description
Thermal Configuration	[Optimal Cooling] Increased Cooling Maximum Cooling Enhanced CPU Cooling	Use this option to select the fan cooling solution for the system. "Optimal Cooling" provides the most efficient solution by configuring fan speeds to the minimum required speed to provide adequate cooling. "Increased Cooling" runs fans at higher speeds to provide additional cooling. Select "Increased Cooling" when third-party storage controllers are cabled to the embedded hard drive cage, or if the system is experiencing thermal issues that cannot be resolved. "Maximum Cooling" provides the maximum cooling available on this platform. "Enhanced CPU Cooling" provides additional cooling to the processors. When running certain processor intensive workloads, this option can provide additional cooling to the processors which can result in improved performance.

[]: Default setting

(9) Advanced Debug Options Menu

When you select **System Configuration > BIOS/Platform Configuration (RBSU) > Advanced Options > Advanced Debug Options** from the System Utilities, the **Advanced Debug Options** menu appears.

For details about the additional options, see the table below.

Option	Parameter	Description
Advanced Crash Dump Mode	[Disabled] Enabled	Use this option to enable the Advanced Crash Dump Mode. When enabled, the system will be configured to log additional debug information to the Active Health System logs when an unexpected system crash is experienced. This option should only be enabled when directed by qualified service personnel.

[]: Default setting

(10) Power and Performance Options Menu

In **System Utilities**, selecting **System Configuration > BIOS/Platform Configuration (RBSU) > Power and Performance Options** displays the **Power and Performance Options** menu.

Its additional options are described in the following table:

Option	Parameter	Description
Energy Performance Preference *1	[Disabled] Enabled	Use this option to enable/disable Energy Performance Preference.

[]: Default setting

*1: an option usable with System ROM Version 2.80 or later.

(11) Trusted Platform Module Options Menu

When you select **System Configuration > BIOS/Platform Configuration (RBSU) > Server security > Trusted Platform Module Options** from the System Utilities, the **Trusted Platform Options** menu appears.

For details about the additional options, see the table below.

Option	Parameter	Description
Omit Boot Device Event *1	[Disabled] Enabled	Use this option to record Omit Boot Device Event. If enabled, PCR Boot Attempt Measurements will be disabled and measurement in PCR[4] will not be recorded.

[]: Default setting

*1: an option usable with System ROM Version 2.80 or later.

(12) Embedded Applications Menu

When you select Embedded Applications from the System Utilities, the Embedded Applications menu appears. For details about the options, see the table below.

Option	Parameter	Description
Embedded Diagnostics	-	This product does not support it.

B) Errata Information

The following table covers corrections for User's Guide.
Please read the following information and use it as reference.

■ Errata Information for Express5800/R120h-1E User's Guide

	Error	Correct																																																				
P.2 Manuals	Storing the electronic edition in Starter Pack DVD or releasing in the Website (http://jpn.nec.com/)	The electronic edition has been published on a website (https://www.nec.com/express/).																																																				
P.23 3.Features - Many built-in Features	Power switch mask	Incompatible																																																				
P.30 5.5 Motherboard	(3) Micro SD card slot	(3) Micro SD card slot (Unsupported)																																																				
1.18 4x 3.5-inch drive model Optical Disk Drive	Optical disc drive cable kit (K410-375(00))	(Unnecessary (It's attached to an optical disk drive.))																																																				
1.18 4x 3.5-inch drive model Optical Disk Drive	the SATA cable (K410-375(00))	(accessory)																																																				
P.116 11.20.1 Notes on Building RAID System	If the optional RAID Controller (N8103-189/195) is used, the RAID System cannot be built in RAID5/RAID6/RAID50/RAID60. <table border="1"> <thead> <tr> <th rowspan="2">RAID level</th><th colspan="2">The minimum number of hard disk drives required to set up a RAID System</th></tr> <tr> <th>N8103-192/195</th><th>N8103-193/201</th></tr> </thead> <tbody> <tr> <td>RAID 0</td><td>1</td><td>1</td></tr> <tr> <td>RAID 1</td><td>2</td><td>2</td></tr> <tr> <td>RAID 5</td><td></td><td>3</td></tr> <tr> <td>RAID 6</td><td></td><td>3</td></tr> <tr> <td>RAID 10</td><td>4</td><td>4</td></tr> <tr> <td>RAID 50</td><td></td><td>6</td></tr> <tr> <td>RAID 60</td><td></td><td>6</td></tr> </tbody> </table>	RAID level	The minimum number of hard disk drives required to set up a RAID System		N8103-192/195	N8103-193/201	RAID 0	1	1	RAID 1	2	2	RAID 5		3	RAID 6		3	RAID 10	4	4	RAID 50		6	RAID 60		6	If the optional RAID Controller (N8103-192/195) is used, the RAID System cannot be built in RAID6/RAID50/RAID60. <table border="1"> <thead> <tr> <th rowspan="2">RAID level</th><th colspan="2">The minimum number of hard disk drives required to set up a RAID System</th></tr> <tr> <th>N8103-192/195</th><th>N8103-193/201</th></tr> </thead> <tbody> <tr> <td>RAID 0</td><td>1</td><td>1</td></tr> <tr> <td>RAID 1</td><td>2</td><td>2</td></tr> <tr> <td>RAID 5</td><td>3</td><td>3</td></tr> <tr> <td>RAID 6</td><td></td><td>4</td></tr> <tr> <td>RAID 10</td><td>4</td><td>4</td></tr> <tr> <td>RAID 50</td><td></td><td>6</td></tr> <tr> <td>RAID 60</td><td></td><td>8</td></tr> </tbody> </table>	RAID level	The minimum number of hard disk drives required to set up a RAID System		N8103-192/195	N8103-193/201	RAID 0	1	1	RAID 1	2	2	RAID 5	3	3	RAID 6		4	RAID 10	4	4	RAID 50		6	RAID 60		8
RAID level	The minimum number of hard disk drives required to set up a RAID System																																																					
	N8103-192/195	N8103-193/201																																																				
RAID 0	1	1																																																				
RAID 1	2	2																																																				
RAID 5		3																																																				
RAID 6		3																																																				
RAID 10	4	4																																																				
RAID 50		6																																																				
RAID 60		6																																																				
RAID level	The minimum number of hard disk drives required to set up a RAID System																																																					
	N8103-192/195	N8103-193/201																																																				
RAID 0	1	1																																																				
RAID 1	2	2																																																				
RAID 5	3	3																																																				
RAID 6		4																																																				
RAID 10	4	4																																																				
RAID 50		6																																																				
RAID 60		8																																																				
P.154 2.4 Cases that Require Configuration - Memory - Use memory RAS feature	Set System Configuration > BIOS/Platform Configuration (RBSU) > System Options > Memory Operations - Advanced Memory Protection	Set System Configuration > BIOS/Platform Configuration (RBSU) > Memory Options - Advanced Memory Protection																																																				
P.171 1.specifications - Standard interface	2x LAN (1000BASE-T/100BASE-TX/10BASE-T, RJ-45)	2x LAN (1000BASE-T, RJ-45)																																																				

■ Errata Information for Express5800/R120h-2E User's Guide

	Error	Correct
P.2 Manuals	Storing the electronic edition in Starter Pack DVD or releasing in the Website (http://jpn.nec.com/)	The electronic edition has been published on a website (https://www.nec.com/express/).
P.23 3.Features - Many built-in Features	Power switch mask	Incompatible
P.31 5.5 Motherboard	(3) Micro SD card slot	(3) Micro SD card slot (Unsupported)

P.137 1.24.1 Notes on Building RAID System	If the optional RAID Controller (N8103-189/195) is used, the RAID System cannot be built in RAID5/RAID6/RAID50/RAID60. <table border="1"> <thead> <tr> <th rowspan="2">RAID level</th><th colspan="2">The minimum number of hard disk drives required to set up a RAID System</th></tr> <tr> <th>N8103-189/195</th><th>N8103-190/201</th></tr> </thead> <tbody> <tr><td>RAID 0</td><td>1</td><td>1</td></tr> <tr><td>RAID 1</td><td>2</td><td>2</td></tr> <tr><td>RAID 5</td><td></td><td>3</td></tr> <tr><td>RAID 6</td><td></td><td>3</td></tr> <tr><td>RAID 10</td><td>4</td><td>4</td></tr> <tr><td>RAID 50</td><td></td><td>6</td></tr> <tr><td>RAID 60</td><td></td><td>6</td></tr> </tbody> </table>	RAID level	The minimum number of hard disk drives required to set up a RAID System		N8103-189/195	N8103-190/201	RAID 0	1	1	RAID 1	2	2	RAID 5		3	RAID 6		3	RAID 10	4	4	RAID 50		6	RAID 60		6	If the optional RAID Controller (N8103-189/195) is used, the RAID System cannot be built in RAID6/RAID50/RAID60. <table border="1"> <thead> <tr> <th rowspan="2">RAID level</th><th colspan="2">The minimum number of hard disk drives required to set up a RAID System</th></tr> <tr> <th>N8103-189/195</th><th>N8103-190/201</th></tr> </thead> <tbody> <tr><td>RAID 0</td><td>1</td><td>1</td></tr> <tr><td>RAID 1</td><td>2</td><td>2</td></tr> <tr><td>RAID 5</td><td>3</td><td>3</td></tr> <tr><td>RAID 6</td><td></td><td>4</td></tr> <tr><td>RAID 10</td><td>4</td><td>4</td></tr> <tr><td>RAID 50</td><td></td><td>6</td></tr> <tr><td>RAID 60</td><td></td><td>8</td></tr> </tbody> </table>	RAID level	The minimum number of hard disk drives required to set up a RAID System		N8103-189/195	N8103-190/201	RAID 0	1	1	RAID 1	2	2	RAID 5	3	3	RAID 6		4	RAID 10	4	4	RAID 50		6	RAID 60		8
RAID level	The minimum number of hard disk drives required to set up a RAID System																																																					
	N8103-189/195	N8103-190/201																																																				
RAID 0	1	1																																																				
RAID 1	2	2																																																				
RAID 5		3																																																				
RAID 6		3																																																				
RAID 10	4	4																																																				
RAID 50		6																																																				
RAID 60		6																																																				
RAID level	The minimum number of hard disk drives required to set up a RAID System																																																					
	N8103-189/195	N8103-190/201																																																				
RAID 0	1	1																																																				
RAID 1	2	2																																																				
RAID 5	3	3																																																				
RAID 6		4																																																				
RAID 10	4	4																																																				
RAID 50		6																																																				
RAID 60		8																																																				
P.174 2.4 Cases that Require Configuration - Memory - Use memory RAS feature	Set System Configuration > BIOS/Platform Configuration (RBSU) > System Options > Memory Operations - Advanced Memory Protection	Set System Configuration > BIOS/Platform Configuration (RBSU) > Memory Options - Advanced Memory Protection																																																				
P.190 1.specifications - Standard interface	2x LAN (1000BASE-T/100BASE-TX/10BASE-T, RJ-45)	2x LAN (1000BASE-T, RJ-45)																																																				

■ Errata Information for Express5800/ R120h-1E, R120h-2E Maintenance Guide

	Error	Correct
P.2 Manuals	Storing the electronic edition in Starter Pack DVD or releasing in the Website (http://jpn.nec.com/)	The electronic edition has been published on a website (https://www.nec.com/express/).
P.8 Abbreviations of Operating Systems (Windows)	Windows Server 2016 Essentials	Incompatible
P.65 7.3.3 Set the System Configuration Back to Default Values	6. Follow Chapter 1 (7.3.2 Operation Procedure of System Maintenance Switch) of this document to set the system maintenance switch: SW6 back to ON.	6. Follow Chapter 1 (7.3.2 Operation Procedure of System Maintenance Switch) of this document to set the system maintenance switch: SW6 back to OFF.
P.75 Internal SD Card Slot	[Enabled] Use this option to enable or disable the Internal SD Card Slot. When set to disabled, the SD card slot is disabled, regardless of whether an SD Card is installed or not. The SD Card will not be visible in the pre-boot environment or under the operating system.	[Disabled] This option setting is not currently supported. The equipment do not support devices dealing with this option. This option is set as Disabled as the user default setting in time of shipment from factory. Do not change this item from the default setting.
P.80 (3) Memory Options Menu	When you select System Configuration > BIOS/Platform Configuration (RBSU) > System Options > Memory Options from the System Utilities, the Memory Options menu appears.	When you select System Configuration > BIOS/Platform Configuration (RBSU) > Memory Options from the System Utilities, the Memory Options menu appears.
P.82 (a) Persistent Memory Options Menu	When you select System Configuration > BIOS/Platform Configuration (RBSU) > System Options > Memory Operations > Persistent Memory Options from the System Utilities, the Persistent Memory Options menu appears.	When you select System Configuration > BIOS/Platform Configuration (RBSU) > Memory Options > Persistent Memory Options from the System Utilities, the Persistent Memory Options menu appears.
P.93 i. (UEFI LAN Driver) Menu -Target Name	For example: iqn.2015-02.com.nec:iscsitarget-iscsidisk-target.	For example: iqn.2015-02.com.nec:iscsitarget-iscsidisk-target

■ **Errata Information for Express5800/R120h-1E, R120h-2E Installation Guide (Windows)**

	Error	Correct
P.2 Manuals	Electronic manuals are stored on Starter Pack DVD or on the website (http://www.nec.com/express/).	The electronic edition has been published on a website (https://www.nec.com/express/).
P.6 Abbreviations of Operating Systems (Windows)	Windows Server 2016 Essentials	Incompatible

■ Correction of DIMM installation order

There are misdescription about DIMM installation order in user's guides.
The following is the correction.

Correction point

- Express5800/120h-1E User's Guide

Chapter 2 Preparations 1.8 DIMM 1.8.2 DIMM installation order

(Continue to the next page)

- Express5800/120h-2E User's Guide

Chapter 2 Preparations 1.9 DIMM 1.9.2 DIMM installation order

DIMM installation order

The order of installation may be different on x1CPU configuration, x2CPU configuration, and mounted number of the DIMM.

- When only CPU1 is mounted

DIMM slot number	1	2	3	4	5	6	7	8
DIMM Mounted number and installation order								
1 DIMM			1					
2 DIMM		2	1					
3 DIMM	3	2	1					
4 DIMM		2	1			3	4	
5 DIMM	3	2	1			4	5	
6 DIMM	3	2	1			4	5	6
7 DIMM	3	2	1	7		4	5	6
8 DIMM	3	2	1	7	8	4	5	6

- When CPU1 and CPU2 are mounted

DIMM slot number	CPU2							
	1	2	3	4	5	6	7	8
DIMM Mounted number and installation order								
2 DIMM			2					
3 DIMM			2					
4 DIMM		4	2					
5 DIMM		4	2					
6 DIMM	6	4	2					
7 DIMM	6	4	2					
8 DIMM		4	2			6		
9 DIMM		4	2			6	8	
10 DIMM	6	4	2			8	8	
11 DIMM	6	4	2			8	10	
12 DIMM	6	4	2			8	10	12
13 DIMM	6	4	2			8	10	12
14 DIMM	6	4	2	14		8	10	12
15 DIMM	6	4	2	14		8	10	12
16 DIMM	6	4	2	14	16	8	10	12

CPU1							
1	2	3	4	5	6	7	8
		1					
	3	1					
	3	1					
	3	1					
5	3	1					
5	3	1					
	3	1			5	7	
	3	1			5	7	
5	3	1			7	9	
5	3	1			7	9	11
5	3	1			7	9	11
5	3	1	13		7	9	11
5	3	1	13		7	9	11
5	3	1	13	15	7	9	11
5	3	1	13	15	7	9	11

- Notice for the combination of DIMM

When more than one kinds of DIMM is combined, install them in the order from the following list to the installation order on the above table.

(High priority) N8102-711 > N8102-710 > N8102-709 > N8102-708 (Low priority)

■ **For Inquiries Regarding this Matter**

If you have any questions on the contents of this document, please contact the dealer where you purchased the product or our sales representative.

NEC

August 2024 21th Edition

GZS-000755-032-15