NEC Hyper Converged System for VMware vSAN/CR2.0
スタートアップガイド

2023 年 11 月
第 1.9 版
日本電気株式会社

文書番号:NHS-E-140-019

目次

1 本ガイドについて

この度は、NEC Hyper Converged System(以下、本製品)をお買い求めいただき、誠にありがとうございます。

本書は、本製品の箱を開けてから使えるようになるまでの手順を説明します。このスタートアップガイドに従って作業を実施してください。本書の確認事項や不明点がありましたら、1.2 節の問い合わせ窓口までご連絡ください。

1.1 NEC Hyper Converged System

NEC Hyper Converged System は、Express5800 シリーズにコンピューティング機能とストレージ機能を統合した仮想化基盤製品です。 HCI の検討から構築、移行、運用管理、データ保護、保守まで一貫したメニューを用意します。
システムのライフサイクルに合わせて最適な機能・サービスを選択できる「NEC Hyper Converged System」は、様々なユースケースで IT インフラの運用管理のシンプル化を実現します。

ご購入いただいた本製品は、VMware ESXi, vSAN, vCenter Server のインストール、セットアップ作業が完了した状態となっております。面倒なセットアップ作業を実施することなく、VMware vCenter Server を利用してすぐに仮想マシン(業務 VM)を作成することができます。

本製品を設置し、電源を入れ、仮想化基盤として使用可能となるまでに必要な準備作業を本書にてご説明します。本書に従って準備作業を実施しても正しく動作しない場合は、お手数をおかけしますが下記までお問い合わせをお願いします。

1.2 お問い合わせ先

問題が解決しない場合、NEC Hyper Converged System の構築サービス窓口にお問い合わせ下さい。

〒211-8666 神奈川県川崎市中原区下沼部 1753
NEC クラウドプラットフォーム事業部
NEC Hyper Converged System 担当

電話番号　044-435-5458
メールアドレス　hcs-inquiry@itpf.jp.nec.com
受付時間　9:00～12:00、13:00～17:00 月曜日～金曜日（祝祭日、NEC 特別休日を除く）

エクスプレス通報サービスの開局手続きについては、エクスプレス受付センターにお問い合わせ下さい。
電話番号　0120-22-3042
メールアドレス　uketuke@express.jp.nec.com
受付時間　9:00～17:00 月曜日～金曜日（祝祭日、NEC 特別休日を除く）

サーバ診断カルテについては、以下のメールアドレスにお問い合わせ下さい。
メールアドレス　karute-tech@express.jp.nec.com

1.3 用語の定義

本書に記載させている用語の定義は以下の通りです。

名称	説明
NEC Hyper Converged System (NEC HCS、HCS)	Express5800 シリーズにコンピューティング機能とストレージ機能を統合した仮想化基盤(HCI)製品。
HCS 構築サービス (構築サービス)	お客様がすぐに HCS を利用開始できるよう、NEC でソフトウェアインストールやセットアップ作業を代行するサービス。
NEC Hyper Converged System Console (HCS Console)	HCS をシンプルに運用管理するソフトウェア。
管理ノード	HCS の構成品。クラスタノードを管理するための、vCSA と管理 VM を動作させるための Express サーバ。
クラスタノード	HCS の構成品。VMware vSAN クラスタを動作させるための Express サーバ群。
Witness ノード	HCS の構成品。VMware vSAN で 2 ノード構成を行う際に必要となるサーバ。HCS では仮想アプライアンスの Witness ノードを使用する。
管理 VM	管理ノード上で動作する、Windows Server 2022 の仮想マシン。HCS の管理や、NEC Hyper Converged System Console の実行環境として使用します。
VMware vCenter Server (vCenter Server)	複数の VMware ESXi および vSAN クラスタを一元運用管理(操作、設定、障害監視、ジョブ管理、稼働統計の管理など)を行うソフトウェア。
VMware vCenter Server Appliance (vCSA)	VMware vCenter Server と動作 OS を組み合わせた仮想マシンアプライアンス。HCS では vCSA を VMware vCenter Server の実行環境として使用します。
vCenter Server 管理インターフェイス (VAMI)	vCSA の管理するためのクライアント。Web ブラウザ上で利用できます。vCSA のネットワーク設定などを変更するために使用します。
VMware vSphere Client (HTML5 版)	VMware vCenter Server を操作・管理するためのクライアント。Web ブラウザ上で利用できます。HCS の運用・管理に使用。
VMware Host Client	VMware ESXi を操作・管理するためのクライアント。Web ブラウザ上で利用できます。詳細のネットワーク設定変更や VMware vCenter Server が利用できない場合のトラブルシューティング等で使用します。
VMware ESXi (ESXi)	仮想マシンや VMware vSAN を動作させるハイパーバイザ(仮想化基盤ソフトウェア)。
VMware vSAN (vSAN)	VMware ESXi 上にソフトウェア定義ストレージ(SDS)を構築する機能。
管理用ネットワーク (管理用 NW)	VMware ESXi の管理用通信をやり取りするネットワーク。
仮想マシン (VM)	ハイパーバイザ上で動作する仮想的な PC(サーバ)。
現調 (現地調整)	サーバやネットワーク機器などを設置場所に設置・固定し、電源やネットワークケーブルの配線を行う作業。
DNS、DNS サーバ	IP アドレスとホスト名を変換する仕組み・機能。HCS の動作に必要。
NTP、NTP サーバ	機器の時間を同期する仕組み・機能。HCS の動作に必要。
Administrator (hcsadmin)	管理者を示す英単語。HCS の管理者ユーザの初期値として使用。
ローカルコンソール	各サーバに搭載される VGA(画面出力端子)、キーボード、マウス。別途リモートマネジメント拡張ライセンスを手配頂くと、ネットワーク経由でローカルコンソールにアクセスできます。
保守アカウント	HCS でクラスタノードの HDD/SSD の交換作業などを行う保守作業員が使用するユーザアカウント。

2 事前準備

2.1 ご用意いただくもの

NEC Hyper Converged System(以下、本製品)をご利用いただく前に、下記 4 点のご準備をお願いいたします。本製品に同封されているものと、Web からダウンロードするものがあります。

- NEC Hyper Converged System モデル(本製品)
  - 同時購入いただいたオプション製品等
  - NEC Hyper Converged System 構成品表 (本製品に同封)
  - NEC Hyper Converged System 製品組み立て仕様書(SG 仕様書)(本製品に同封)
  - ExpressSupportPack, PPSupportPack (パック型保守製品を購入頂いた場合。別途納品)

- ドキュメント一式
  - Express サーバベースモデルの製品マニュアル(ユーザーズガイド、Web ダウンロード)
  - 本書 (NEC Hyper Converged System スタートアップガイド、本製品に同封)
  - NEC Hyper Converged System 初期パスワード通知書 (本製品に同封)
  - 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 (Web ダウンロード、エクスプレス通報サービスを利用する場合)

- Windows Server 2022 ライセンス

- その他
  - 下記要件を満たす Windows PC
    (Windows 7, 10, Windows Server 2012, 2012R2, 2016,2019,2022)
    - ✧ LAN インタフェース、LAN ケーブル等(管理ネットワーク接続用、有線必須)
    - ✧ SSH クライアント(PuTTY0.70 で動作を確認済み)
    - ✧ Microsoft Edge
  - エクスプレス通報サービス設定用ファイル (エクスプレス通報サービスを利用する場合)
    ※ 事前に弊社営業との調整が必要です。詳細は 3.23 節を参照してください。
    - ✧ 管理ノード、クラスタノードの開局キー
    - ✧ 管理 VM 用の開局キー
    - ✧ 管理 VM 用の受信情報設定ファイル (構築サービスでエクスプレス通報サービスを設定した場合は不要)

- (本書対象外、ご参考)
  - NEC Hyper Converged System Console セットアップ用 DVD 媒体、ライセンス (本製品に同封)

- NEC Hyper Converged System Console v3.0 ユーザーズガイド(1.4 版、Web ダウンロード)
- NEC Hyper Converged System/運用ガイド (1.8 版、Web ダウンロード)
- ネットワーク機器類一式 (ネットワークスイッチ、LAN ケーブルなど)
- サーバを設置するための設備一式 (19 インチラック、商用電源など)
- NTP サーバ、DNS サーバ (DNS サーバは、お客様の DNS サーバを使用する場合)
- ディスプレイ、キーボード (LCD コンソールユニット等も可)

本製品をご利用いただく場合は DNS サーバより本製品上で動作する VMware ESXi, vSAN, vCenter Server のホスト名の正引きおよび逆引きができる必要があります。ヒアリングシートにて、お客様の DNS サーバを使用する旨をご指定いただいた場合は、本製品の電源を入れる前に、お客様の DNS サーバに SG 仕様書に記載されているホスト名、ドメインサフィックス、IP アドレスが登録されており、本製品からアクセス可能であることを必ず確認してください。

3 受入確認

2 章の事前準備が完了後、本章の受入確認手順を実施してください。本章の手順が全て完了すると、本製品が正しく動作することの確認が完了します。 本紙最終頁の「別紙　受け入れチェックシート」も必要に応じてご利用ください。

3.1 概要

本節は受入確認手順を示します。
NEC Hyper Converged System(以下、本製品)をご利用頂くためには、下記 23 点の実施をお願いいたします。

1. 構成品の確認
2. 本製品の設置
3. ネットワーク装置への接続
4. 電源の接続
5. 管理ノードの電源オン
6. Windows PC の準備
7. Windows PC から管理 VM に接続
8. DNS 疎通確認
9. VMware vCenter Server への接続確認
10. クラスタノード、Witness ノードの電源オン
11. VMware vCenter Server 上での機器確認
12. 隔離 IP の到達確認
13. NTP の動作確認
14. クラスタノード、Witness ノードのメンテナンスモード解除
15. vSAN クラスタ全台同時停止時の build-in ツールの実行
16. クラスタメンバの更新の有効化
17. vCLS の Retreat モードの無効化
18. vSphere の可用性設定
19. vSAN ストレージプロバイダの同期
20. VMware vSAN 状態の確認
21. NEC Hyper Converged System Console の動作確認
22. エクスプレス通報サービスの開局手続き(エクスプレス通報サービスの申し込みをしている場合)
23. サーバ診断カルテの開局手続き(サーバ診断カルテの申し込みをしている場合)

3.2 構成品の確認

3.2.1 構成品表の取り出し

本製品の構成物を示す「NEC Hyper Converged System 構成品表(以下構成品表)」は、NEC Hyper Converged System 管理ノードの梱包箱の内側に貼り付けられている、「NEC Hyper Converged System 構築サービス関係書類一式在中」と書かれた封筒内に納品されます。構成品表を取り出してください。

3.2.2 構成品表の確認

本製品と、その他同時手配いただいた製品がそれぞれ別の梱包箱に納められた状態でお客様ご指定先へ送付されます。本製品が到着されましたら、「NEC Hyper Converged System 構成品表」をご参照の上、お買い求めいただいた構成品から過不足がないかご確認をお願いします。構成品表は NEC Hyper Converged System 管理ノードの梱包箱の内側に貼り付けられている、「NEC Hyper Converged System 関係書類在中」と書かれた封筒内に納品されます。
構成品表に梱包箱の個数が記載されます。構成品表の梱包箱の個数と、納品物の梱包箱の個数が一致していることを確認してください。

構成品は、ケーブル・レールなどの添付品を除き、全て組み付けられた状態で出荷され、本製品の内部に組みつけられた状態となっており、分解しないと確認できない物も含まれます。

・添付品は、なくさないよう大切に保管してください。

《参考》

NEC Hyper Converged System と同時にご注文いただいた、NEC Hyper Converged System 以外の製品(例: LCD コンソールユニット、Windows Server CAL など)は、3.2.1 節の構成品表には記載されておりません。同時にご注文いただいた NEC Hyper Converged System 以外の製品は、納品書と納品物の梱包箱の数量、型番が一致していることを確認してください。

3.2.3 製品の外観確認

本製品(クラスタノード、管理ノード、ネットワークスイッチ)を梱包箱から取り出し、へこみや汚れ等がないか確認してください。

3.3 本製品の設置

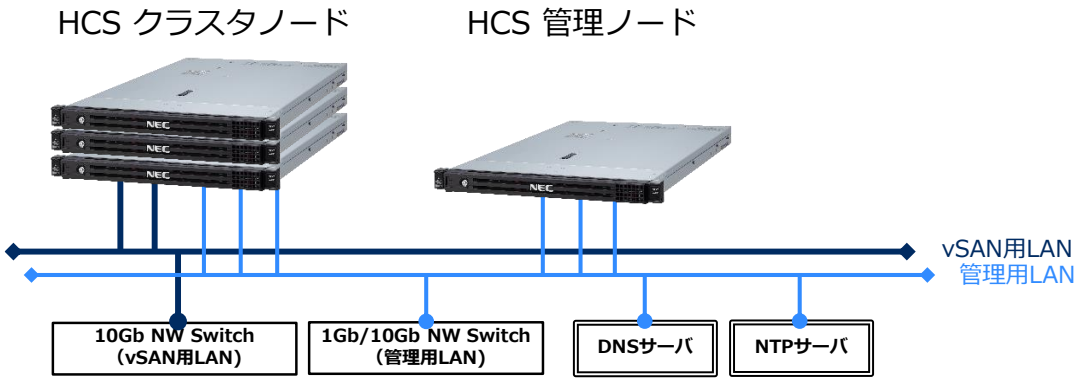
本製品を使用する前に、19 インチラックなど安全に固定できる器具に搭載し、電源を接続する必要があります。本製品に同封されるスタートアップガイド、または NEC Web サイトから入手できる HCS ベースモデル(R120h-1M/2M)の製品マニュアル(ユーザーズガイド一式)を元に、設置を行ってください。

3.4 ネットワーク装置への接続

NEC Hyper Converged System の電源を入れる前に、お客様にご準備頂く NTP サーバ、DNS サーバ(DNS サーバはお客様の DNS サーバを使用する場合)との接続・通信が必要になります。あらかじめネットワーク設計や設定、構築を完了いただき、製品組み立て仕様書(SG 仕様書)に記載されている「LAN ポート対応表」、「クラスタノードの設定」のアダプタ設定、「管理ノードの設定」のアダプタ設定に従ってネットワーク機器と NEC Hyper Converged System を正しく接続してください。

本製品をご利用には、DNS サーバより本製品上で動作する VMware ESXi, vSAN, vCenter Server のホスト名の正引きおよび逆引きができる必要があります。続く本書の 3.9 節で確認を行います。

接続例



3.5 電源の接続

すべての製品の設置が完了後、各 NEC Hyper Converged System 管理ノード、クラスタノードに同封されるスタートアップガイド、または NEC Web サイトから入手できる HCS ベースモデル(R120h-1M/2M)の製品マニュアル(ユーザーズガイド)を元に、電源ケーブルを AC 電源に正しく接続して下さい。本製品の電源をオンにする前にネットワーク機器の電源をオンにしてください。

3.6 管理ノードの電源オン

《注意》

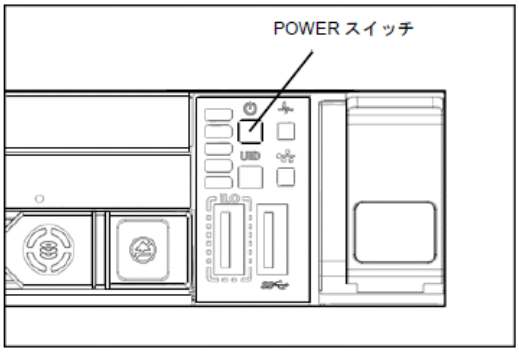
クラスタノードの電源は、DNS 疎通確認が完了するまで入れないでください。

NEC Hyper Converged System 管理ノード(サーバ)の電源をオンにします。DNS サーバ(お客様の DNS サーバを使用する場合)とネットワーク機器の電源オン確認後、管理ノードの電源をオンしてください。

電源をオンにする方法は、以下を参照ください。

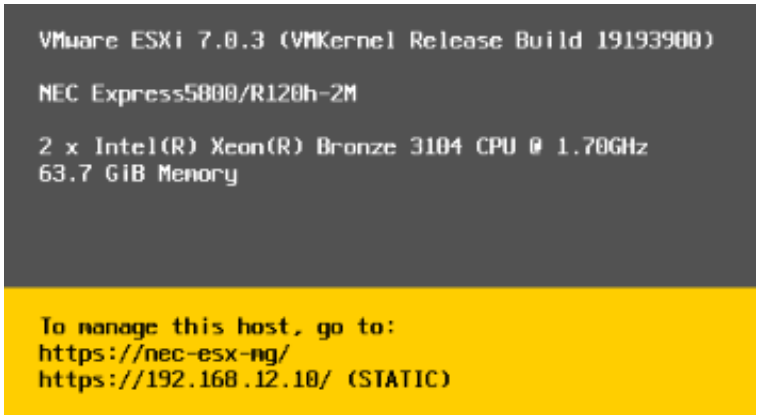
R120h-1M の電源オン:

以下の図の POWER スイッチを押下して、電源オンしてください。
正しく電源オンされると、ランプが緑色に点灯します。



《参考》

管理ノードにディスプレイを接続している場合、ローカルコンソールで下記のような画面が表示されれば、VMware ESXi が起動しています。



管理ノードにディスプレイを接続していない場合、十分な時間を待ってください。

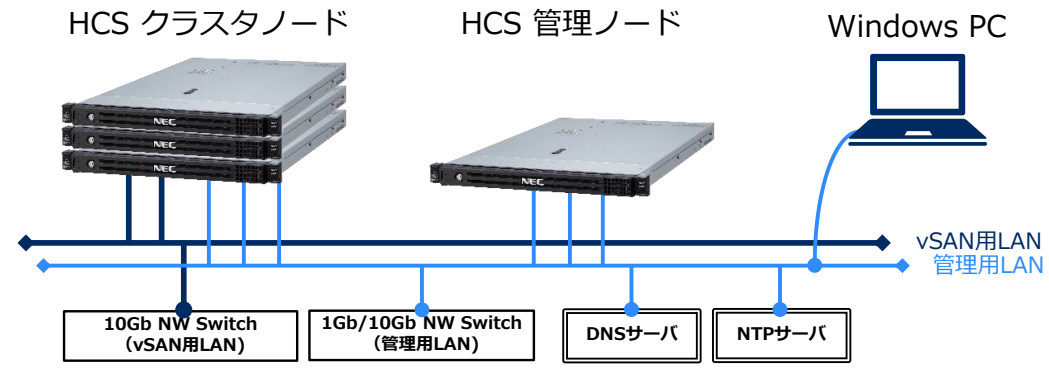
3.7 Windows PC の準備

Windows PC を、管理用ネットワークに接続します。

1. Windows PC のネットワーク設定を、管理用ネットワーク上の管理ノード(vCenter Server, 管理 VM)、クラスタノード(ESXi)に接続できるよう、変更します。

2. Windows PC を管理用ネットワークに接続してください。

接続例



《注意》

Windows PC に設定する IP アドレスは、本製品や管理用ネットワークで使われていない IP アドレスを割り当ててください。重複した IP アドレスを設定した場合、システムの動作に影響を与えることがあります。

3.8 Windows PC から管理 VM に接続

Windows PC を管理用ネットワークに接続し、管理ノード上で動作している管理 VM に接続します。

手順実施に必要なパラメータ

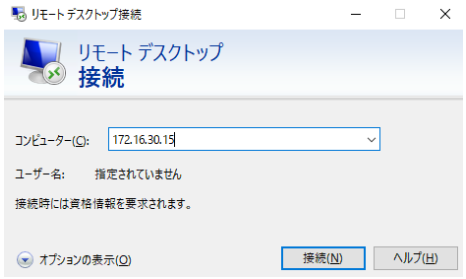
ドキュメント	項目	パラメータ/値（メモ用）
初期パスワード通知書	Administrator ユーザのパスワード	
ヒアリングシート	管理 VM の IP アドレス (【事前確認項目の転記】の「管理 VM のお客様環境用の IP アドレス」または「管理 VM の管理用ネットワークの IP アドレス」)	
ヒアリングシート	管理 VM のサブネットマスク (【事前確認項目の転記】の「管理 VM のお客様環境用のサブネットマスク」または「管理用ネットワークのサブネットマスク(共通)」)	
	Windows PC に設定する IP アドレス	

手順

1. Windows PC から管理 VM にリモートデスクトップ接続します。

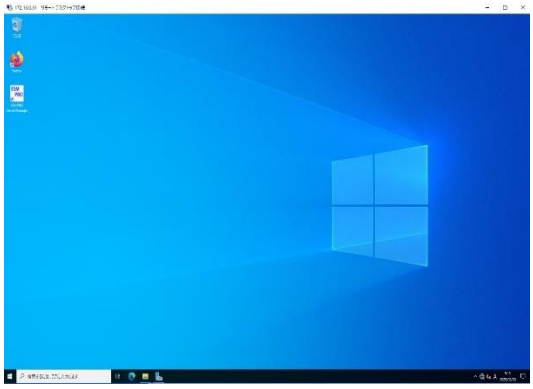
   Windows PC でリモートデスクトップ接続(mstsc)を起動し、ヒアリングシート「管理ネットワーク接続用の IP アドレス」を入力し、管理 VM に接続します。アカウント認証画面が表示されますので、下記アカウント情報を入力し、ログインできるかどうかを確認します。

   - コンピューター: ヒアリングシート「管理 VM の IP アドレス」
   - アカウント名: administrator
   - パスワード: 初期パスワード通知書「Administrator ユーザのパスワード」



2. 管理 VM へのリモートデスクトップ接続が成功し、管理 VM のデスクトップ画面が表示されることを確認します。

   - 正しく接続できた場合: 管理 VM のデスクトップ画面が表示される。(下記図)
   - 接続できない場合: リモートデスクトップ接続できない。またはアカウント情報がエラー。



管理 VM にリモートデスクトップ接続ができない場合は、下記を再確認してください。下記を確認しても接続できない場合は、お手数をおかけしますが 1.2 節の構築サービス窓口までご連絡ください。

- 電源: 管理ノードの電源がオンになり、VMware ESXi が起動していることを確認してください。
- ネットワーク: Windows PC より、ヒアリングシート「管理 VM の IP アドレス」に ping を実施し、通信ができていることを確認してください。
- 管理 VM: Windows PC より、Web ブラウザでヒアリングシート「管理ノードの IP アドレス」を開き、VMWare Host Client 上で管理 VM の電源がオンになっていることを確認してください。

3.9 DNS 疎通確認

管理 VM で、DNS 疎通確認を実施します。

1. 3.8 節でリモートデスクトップ接続した管理 VM 上で、コマンドプロンプト(cmd を起動します。)
2. 管理 VM のコマンドプロンプト上で以下のコマンドを実行し、管理 VM からヒアリングシートに記載されている管理ノード/クラスタノード/vCenter Server Appliance(vCSA)/管理 VM のホスト名、IP アドレスを正引き、逆引き可能であることを確認してください。
   2 ノード構成の場合は、witness ノードの確認も実施してください。

- 正引き確認：nslookup [ヒアリングシートに記載された各ノードのホスト名(FQDN)]
- 逆引き確認：nslookup -type=ptr [ヒアリングシートに記載された各ノードの IP アドレス]

	ホスト名	IP アドレス
例)クラスタノード 1	nec-esx-cn1.vsan.local	192.168.12.11
例)DNS サーバ	nec-mvm.vsan.local	192.168.12.21
管理ノード		
クラスタノード 1		
クラスタノード 2 ・・		
vCSA		
管理 VM		
witness(2 ノード構成の場合)		

3. 正引き、逆引き結果がヒアリングシートのホスト名、IP アドレスと一致していることを確認後、コマンドプロンプトを終了させてください。以降の作業も引き続き管理 VM で実施するため、管理 VM のログオフは必要ありません。

《参考》

管理 VM への接続や、正引き/逆引きができない場合、管理 VM、vCSA、管理ノードの電源をオフにし、DNS サーバにヒアリングシートに記載頂いた各ノードのホスト名、IP アドレスが登録されていること、ネットワークケーブルが正しく接続されているかを確認し、「3.6 節　管理ノードの電源オン」から確認してください。各電源オフの方法は、NEC Hyper Converged System/運用ガイドをご参照ください。

3.10 VMware vCenter Server への接続確認

管理 VM 上で Web ブラウザを起動し、VMware vSphere Client (VMware vCenter Server)に接続します。

1. 3.8 節でリモートデスクトップ接続した管理 VM 上で Web ブラウザを起動し、VMware vCenter Server に接続します。ヒアリングシートの vCSA の「vCSA のホスト名(FQDN)」を参照し、下記ルールで URL を作成し、アクセスします。

   https://< vCSA のホスト名>/ui

   例）<https://nec-vcsa.vsan.local/ui>

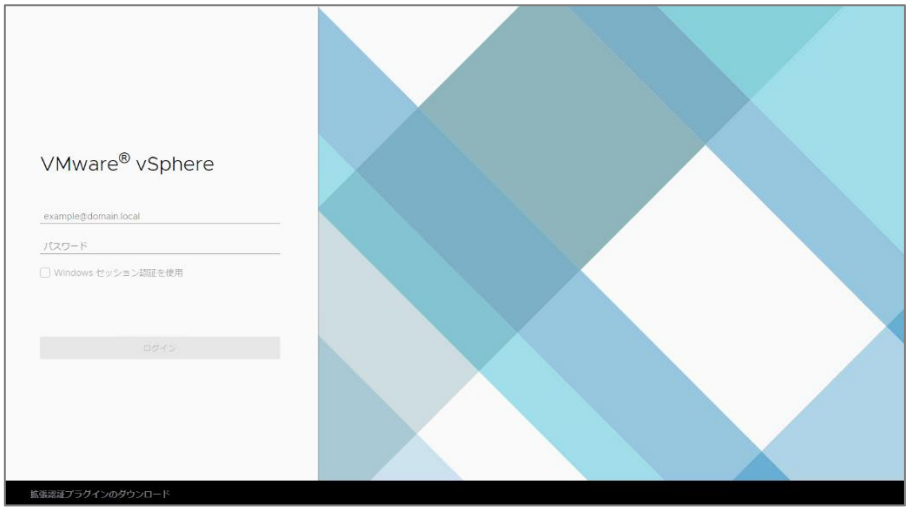
   ※ 「接続がプライベートではありません」画面が表示された場合は、[詳細設定]をクリックし表示された画面で、[<IP アドレスまたは FQDN>に進む(安全ではありません)]クリックしてください。

2. 下記図のように VMware vCenter Server のログイン画面が表示されましたら、ユーザ名、パスワードを入力し、ログインします。

   ユーザ名: “administrator@”＋ SSO ドメイン名

   例）administrator@vsphere.local

   パスワード: 初期パスワード通知書の vCSA の「administrator ユーザのパスワード」

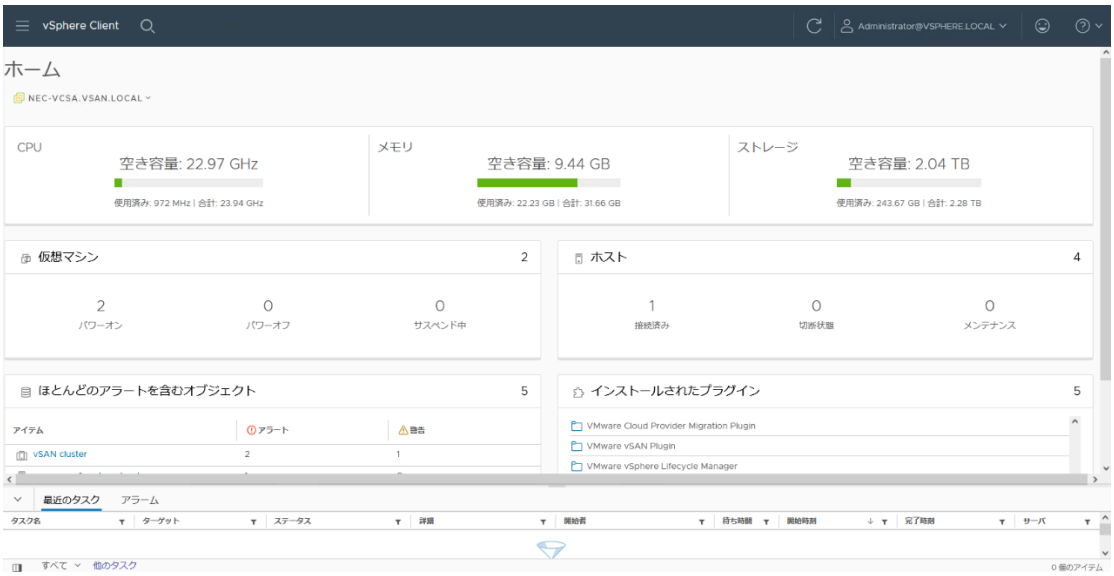


重要 VMware vCenter Server に接続できない時は、まず以下を確認して下さい。

1.	VMware vCenter Serverに接続する情報に誤りがありませんか？ （ヒアリングシートの「vCSAのホスト名(FQDN)」を再度確認ください）
2.	Windows PC上のWebブラウザからVMware vCenter Serverに接続できますか？ (pingコマンド等を使用しネットワーク接続できるかどうかを確認してください)
3.	VMware vCenter Serverは起動していますか？ (管理ノードのVMware Host Clientに接続し、vCSA VMが起動していることを確認してください。 詳細はNEC Hyper Converged System/運用ガイドをご参照ください)

解決しない場合は、御手数ですが、1.2 節の構築サービス窓口までご連絡をお願いいたします。

3. 正常にログインが完了すると、VMware vSphere Client が表示されます。下記図のようなホーム画面が表示されることを確認します。以降の手順も VMware vSphere Client を操作するため、Web ブラウザは起動したまま閉じないでください。



3.11 クラスタノード、Witness ノードの電源オン

NEC Hyper Converged System の全てのクラスタノード(サーバ)の電源をオンにします。クラスタノードの電源オンの順序指定はありません。

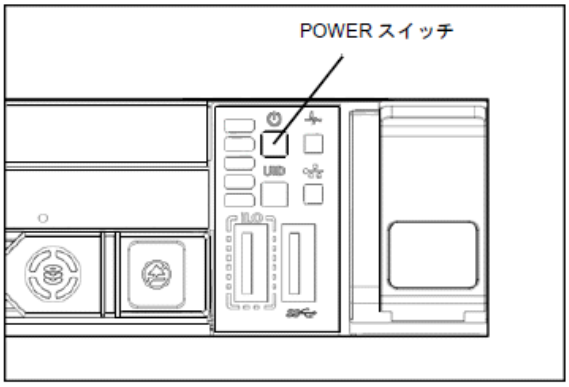
重要

vSAN クラスタの全停止後、起動時にハード障害等が重なると、一部のオブジェクトにアクセスできない事象が発生することがあります。
一度に一台ずつのリブート、パワーサイクルする分には問題は発生しません。
可能な限り vSAN クラスタの全停止を避け、一台ずつのメンテナンスモード移行、リブート、パワーサイクルが有効な回避策となります。
詳細は下記を参照願います。
https://kb.vmware.com/s/article/60424?lang=ja

電源をオンにする方法は、以下を参照ください。

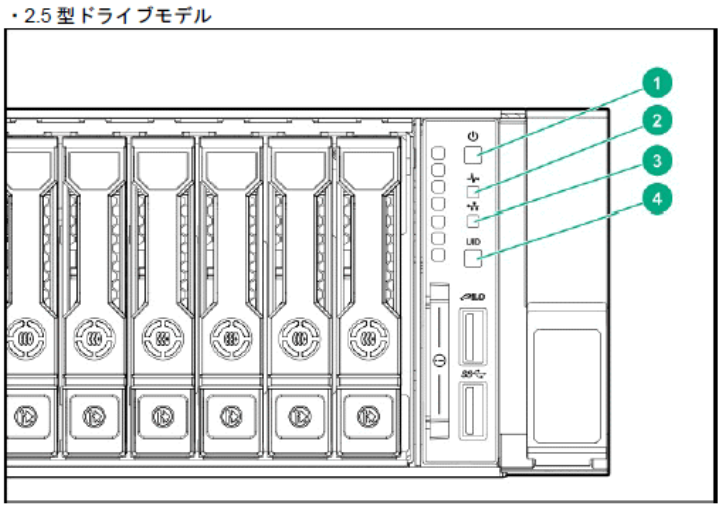
R120h-1M の電源オン:

以下の図の POWER スイッチを、各ノード分、順次、押下して、電源オンしてください。
正しく電源オンされると、ランプが緑色に点灯します。



R120h-2M の電源オン:

以下の図の POWER スイッチを、各ノード分、順次、押下して、電源オンしてください。
正しく電源オンされると、ランプが緑色に点灯します。



2 ノード構成の場合は、Host Client の画面で以下手順を実行して Witness ノードの電源をオンにしてください。

1. 管理 VM にて Web ブラウザを起動し、下記 URL で管理ノードに Host Client で接続してください。

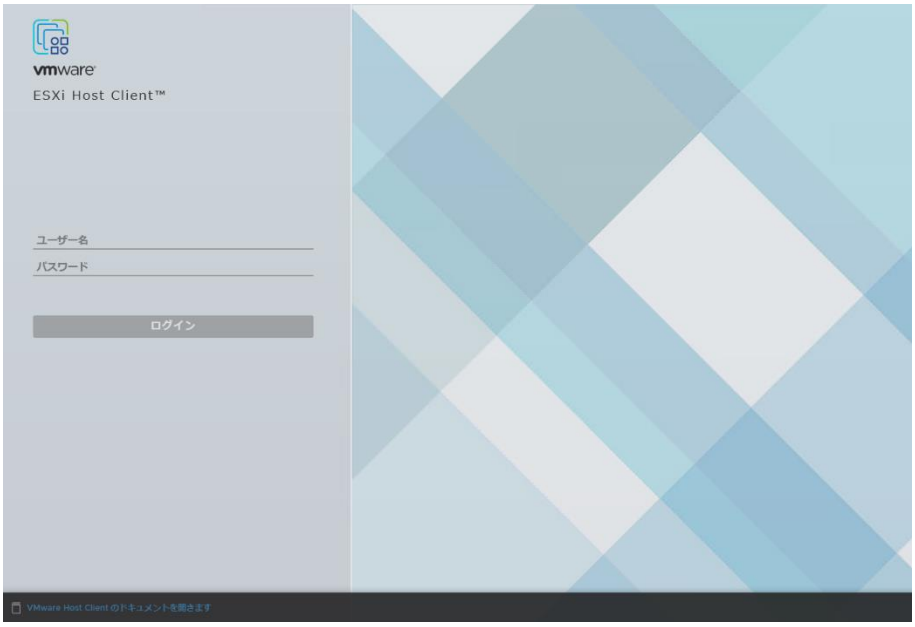
https://<管理ノードの FQDN または IP アドレス>/ui

※ 「接続がプライベートではありません」画面が表示された場合は、[詳細設定]をクリックし表示された画面で、[<IP アドレスまたは FQDN>に進む(安全ではありません)]クリックしてください。

2. 下記図のように Host Client のログイン画面が表示されましたら、ユーザ名、パスワードを入力し、ログインします。

   ユーザ名: root

   パスワード: 初期パスワード通知書の管理ノードの「ESXi の root パスワード」



3. 正常にログインが完了すると、ホスト画面が表示されますので、左メニューから[仮想マシン]をクリックします。

4. 仮想マシン一覧が表示されますので、witness ホスト仮想マシンにチェックを入れ、 [パワーオン]をクリックします。
   以降の手順も Host Client を操作するため、Web ブラウザは起動したまま閉じないでください。

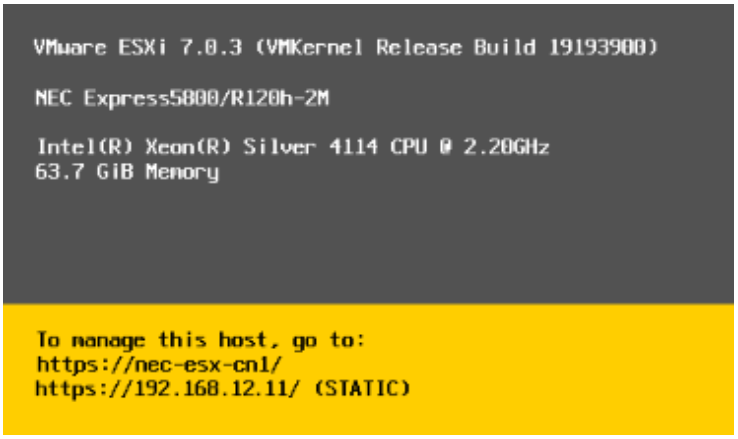
3.12 VMware vCenter Server 上での機器確認

VMware vSphere Client のステータスを更新し、vSAN クラスタ、NEC Hyper Converged System クラスタノード・管理ノードが正しく表示されていることを確認します。

1. 各クラスタノードの VMware ESXi が起動したことを確認します。

《参考》

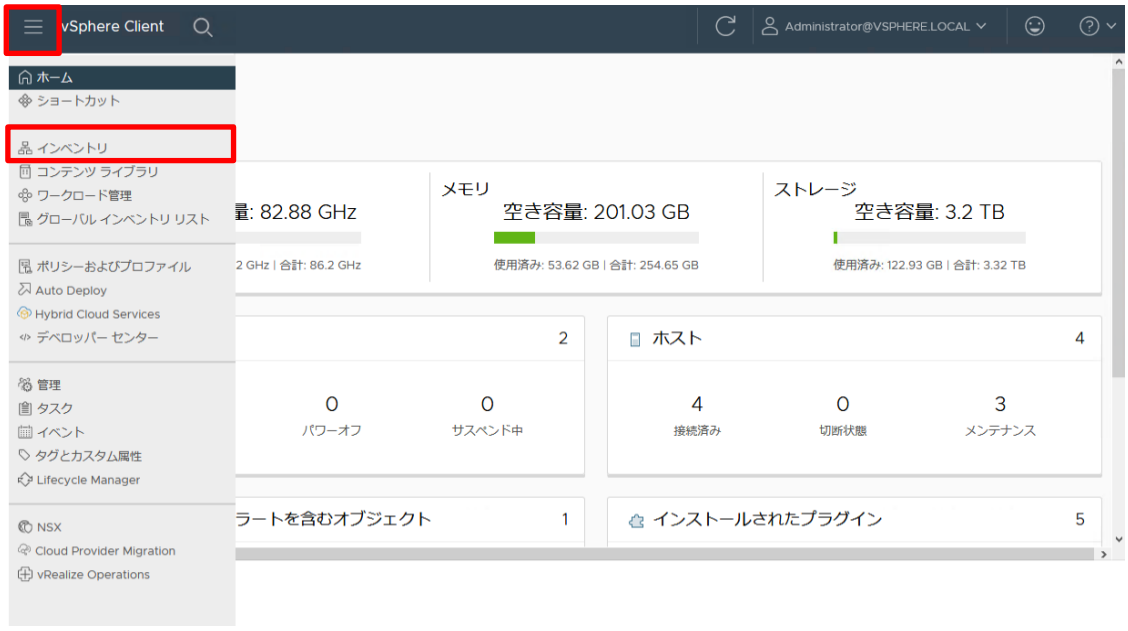
各クラスタノードにディスプレイを接続している場合、ローカルコンソールで下記のような画面が表示されれば、VMware ESXi が起動しています。



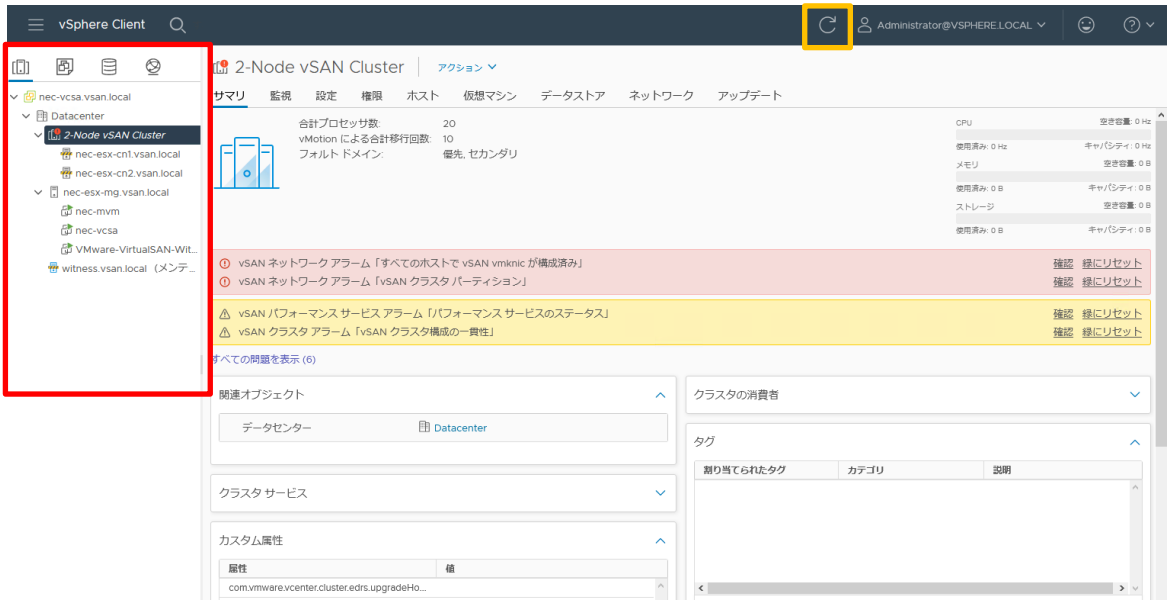
クラスタノードにディスプレイを接続していない場合、十分な時間を待ってください。

2. 3.10 節で接続した VMware vSphere Client のホーム画面左側のメニューアイコンをクリックし、表示されたメニューから [インベントリ]をクリックします。

※ 本書では、以降、以下 VMware vSphere Client の画面左側のメニューを「ナビゲータ」と表記します。



3. リフレッシュボタン(下記図オレンジ枠)を押し、ステータスを更新してください。ナビゲータに vSAN クラスタ、クラスタノード、管理ノード(3 ノード以上の構成、または 2 ノード構成でライセンスに vSphere Standard を使用する場合)が表示され、各クラスタノードがメンテナンスモードとなっていることを確認してください。3 ノード以上の構成、または 2 ノード構成でライセンスに vSphere Standard を使用する場合は以上で本項の作業は終了です。
以降の作業も VMware vSphere Client を使用するため、閉じずにそのままにしてください。



4. 2 ノード構成でライセンスに vSphere Essentials Plus を使用する場合は、引き続き、3.11 節で接続した Host Client を開き、管理 VM、vCSA、Witness ノードが表示されることを確認してください。

構築した機器が表示されない場合は、3.4 節以降の手順を再度見直してください。解決しない場合は、1.2 節の構築サービス窓口までご連絡ください。
vCenter 上の警告が表示されている場合は、以降の作業で解消しますので、引き続き 3.13 節以降の手順を実施してください。

3.13 隔離 IP の到達確認

2 ノード構成の場合は、本節の実施は不要です。

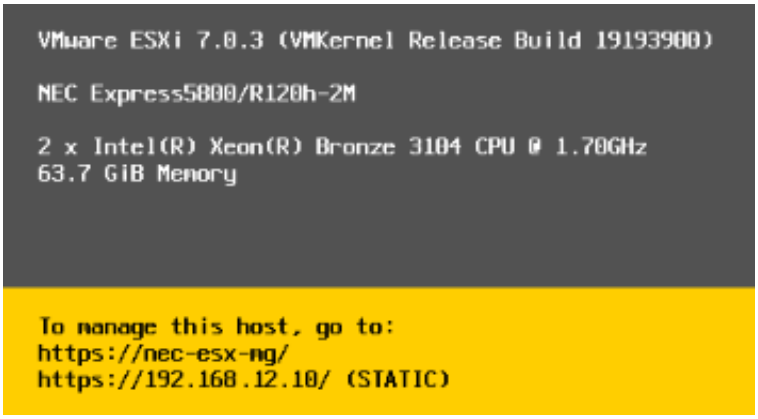
クラスタノードから、vSAN ネットワークスイッチに設定されている隔離 IP へ到達できることを ping により確認します。クラスタノード全台に対して下記手順を実施します。(管理ノードの確認は不要)

《参考》

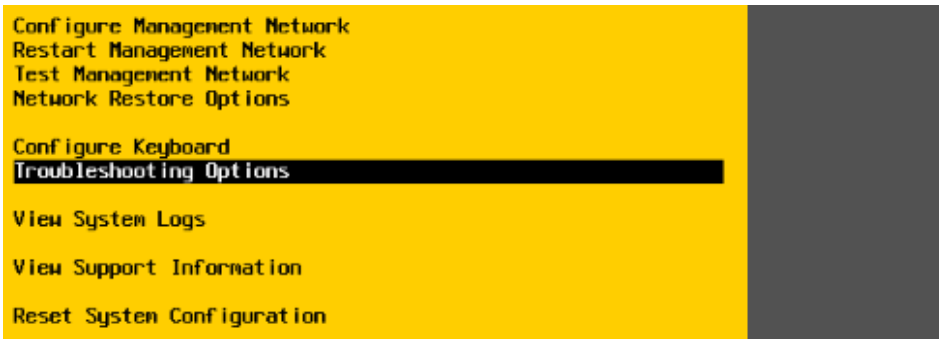
以降の操作は①Windows PC から SSH で ESXi Shell にログイン　②クラスタノードにキーボード・マウスを接続し、ローカルコンソール(ダイレクトコンソール)で ESXi Shell にログイン　の 2 方法どちらでも実施することができます。本項では①の方法で確認を行います。

《補足》
SSH が無効な場合は、ローカルコンソール（ダイレクトコンソール）で、SSH を有効して、本節手順 2 以降の操作を行ってください。本節の確認作業終了後は、SSH を無効にしてください。
SSH を有効および無効にする操作は下記になります。

① ローカルコンソール下記のような画面が表示されれば、VMware ESXi が起動しています。
F2 キーを押下します。ログイン名とパスワードを入力して Enter を押下してください。



② 画面左のメニューで Troubleshooting Options を選択し、Enter を押下します。



③ 「Troubleshooting Mode Options」の画面で[Enable SSH]を選択した状態で[Enter]キーを押下し、画面右のメニューの表示が[SSH is Enabled]に更新されることを確認します。
以上で SSH 有効化は完了です。

※ 上記操作を行う前の時点で画面右側に[SSH is Enabled]と表示されている場合は、本操作は不要です。

④ SSH を無効化する場合は、①から②の操作後、「Troubleshooting Mode Options」の画面で[Disable SSH]を選択した状態で[Enter]キーを押下し、画面左のメニューの表示が[SSH is Disabled]に更新されることを確認します。

※ 上記操作を行う前の時点で画面右側に[SSH is Disabled]と表示されている場合は、本操作は不要です。

《補足》
キーボードレイアウトを”Japanese”に設定しても、ESXi の再起動を行うと、ダイレクトコンソールユーザインターフェイス上で「Configure Keyboard」の設定が"Japanese"と表示されていてもダイレクトコンソールユーザインターフェイス や ESXi Shell へのキーボード入力が英語配列となる場合があります。

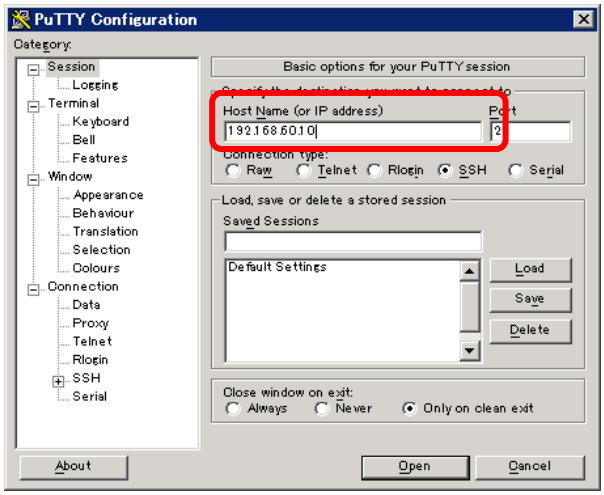
ESXi Shell にログインする際のパスワード入力やコマンド入力が英語配列となることがありますので、ご注意ください。

(“@”は「Shift + 2」で入力することができます。)

本事象が発生した場合は、ダイレクトコンソールユーザインターフェイスにログインして「Configure Keyboard」の値を"Japanese"に設定し直してください。

ESXi7.0Udate1 以降では本問題は解消されています。

1. Windows PC 上で SSH クライアント(例: PuTTY)を起動します。
   Host Name にヒアリングシートのクラスタノード 1 の「管理ネットワーク IP アドレス」を入力し、Open をクリックします。 (下記図では 192.168.60.10)

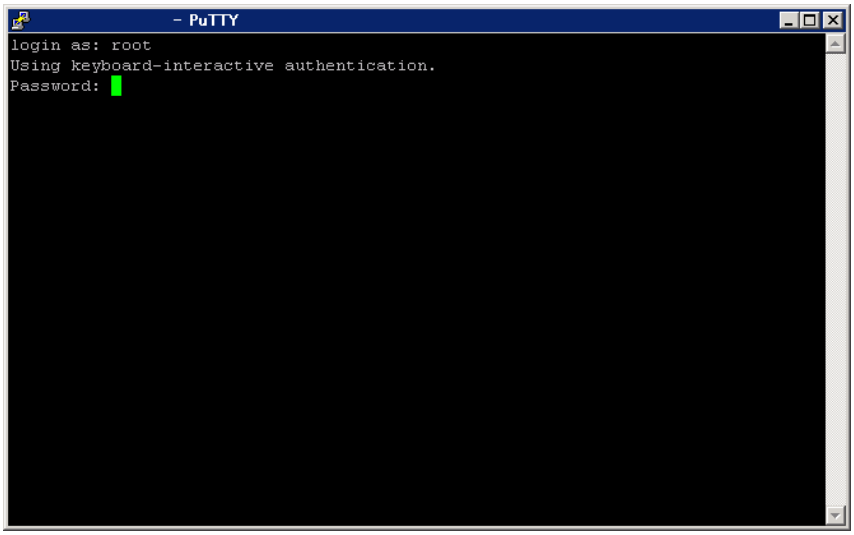


SSH でクラスタノード 1 への接続が成功すると、PuTTY の画面が下記のように変化します。

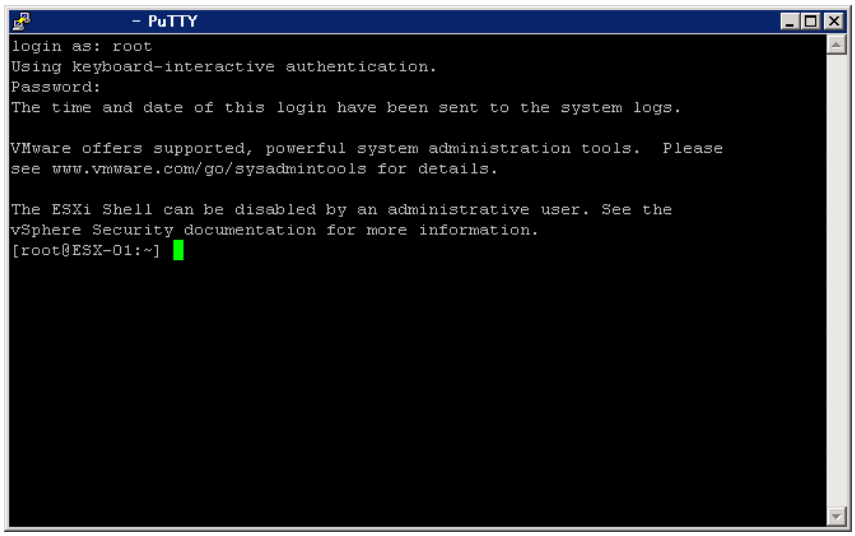
2. ユーザ名 root でログインします。

「login as: 」と表示された画面にキーボードで「root」と入力し「Enter」キーを押下します。
続いて「Password: 」と表示された画面にキーボードで下記パスワードを入力し「Enter」キーを押下します。(パスワードは画面に表示されません)

- パスワード: 初期パスワード通知書記載のクラスタノードの「ESXi の root パスワード」



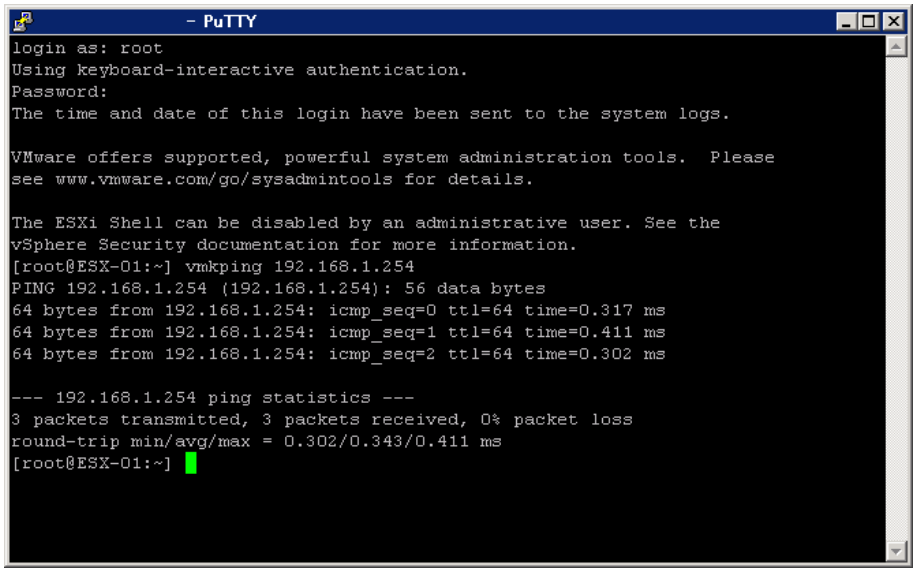
正常にログインが完了すると、下記のように表示されます。



3. ping コマンドを使用し、隔離 IP に ping を行います。

   ヒアリングシートに記載されている 10G スイッチの「10G スイッチの vSAN ネットワーク IP アドレス」または組み立て仕様書(SG 仕様書)に記載されている「das.isolationaddress0」(隔離 IP アドレス)を確認し、SSH クライアントに「ping <隔離 IP アドレス>」を入力し「Enter」キーを押下します。(例: ping 192.168.60.10)

   ping コマンドが実行されると、下記図のように画面が変化し、
   「3 packets transmitted, 3 packets received, 0% packet loss」と表示され、隔離 IP と通信(到達)できていることを確認します。



正しく隔離 IP に到達できていない場合は、
「3 packets transmitted, 0 packets received, 100% packet loss」と表示されます。その場合は、ネットワーク接続や 10G スイッチの設定等を確認した上で、再度 ping コマンドを実行し隔離 IP に到達できることを確認してください。

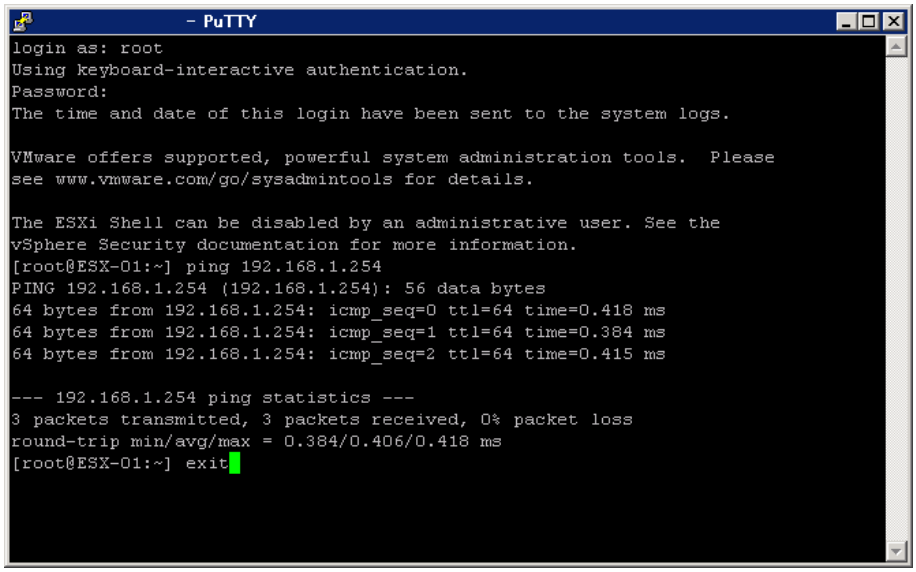
《参考》

ping コマンドを入力した際に、「not found」とエラーが表示される場合は、ping コマンドの代わりに vmkping コマンドを使用してください。使用方法は ping コマンドと同様です。

(例:「ping 192.168.60.10」→「vmkping 192.168.60.10」)

4. 隔離 IP 到達確認後、ESXi Shell を終了します。

PuTTY に「exit」と入力し「Enter」キーを押下します。押下後 PuTTY の画面が閉じることを確認します。



5. 3.14 節、3.16 節、3.17 節で引き続き ESXi Shell を使用しますので、SSH を無効にせず、使用できる状態にしておいてください。
6. 本節 1～5 の手順を他のクラスタノード台数分繰り返します。全てのクラスタノードから隔離 IP に到達できることを確認します。

3.14 NTP の動作確認

各ノードが、NTP サーバに同期できているか確認します。

本節の操作は全てのクラスタノードで実施します。2 ノード構成の場合は、Witness ノードに対しても実施してください。

3 ノード以上の構成の場合、3.13 節で有効にした SSH を利用してクラスタノードの ESXi Shell に接続してください。
2 ノード構成の場合は、3.13 節を参照し、クラスタノードの ESXi Shell に接続してください。
Witness ノードの ESXi Shell に接続する場合は、vSphere Client のオブジェクトナビゲータで Witness host 名をクリックした後、画面右の[サマリ]タブの仮想マシン画面イメージ下にある[WEB コンソールの起動]をクリックします。

1. ユーザ名 root でログインします。
   - パスワード: 初期パスワード通知書記載のクラスタノードの「ESXi の root パスワード」

   正常にログインが完了すると、下記のように表示されます。

```
nec-esx-cn1 login: root
Password:
The time and date of this login have been sent to the system logs.

WARNING:
   All commands run on the ESXi shell are logged and may be included in
   support bundles. Do not provide passwords directly on the command line.
   Most tools can prompt for secrets or accept them from standard input.

VMware offers supported, powerful system administration tools.  Please
see www.vmware.com/go/sysadmintools for details.

The ESXi Shell can be disabled by an administrative user. See the
vSphere Security documentation for more information.
[root@nec-esx-cn1:~]
```

2. 以下のコマンドを実行します。

```
# ntpq -p localhost
```

```
[root@nec-esx-cn1:~] ntpq -p localhost
```

3. サーバと同期されていることを確認します。

実行結果として、参照する NTP サーバ（画像では管理 VM）が表示され、左端に「*」が表示されていることを確認します。

また、offset の絶対値（NTP サーバとの時間差）が 2000（2 秒）以下となっていることを確認します。

offset の値が 2000 以上の場合は、しばらく待ってから再度 ntpq コマンドを実施してください。NTP による時刻同期では、時刻が反映されるまで 15 分以上かかる場合があります。

```
[root@nec-esx-cn1:~] ntpq -p localhost
     remote           refid      st t when poll reach   delay   offset  jitter
==============================================================================
*nec-nvm.vsan.LOCL.              1 u   28   64   17    0.425   -1.061   0.534
[root@nec-esx-cn1:~]
```

4. 以下のコマンドを実行し、ESXi Shell を終了します。

```
# exit
```

```
[root@nec-esx-cn1:~] exit
```

5. 本節の 1～4 の手順をすべてのクラスタノードと Witness ノードに対して実施します。

3.15 クラスタノード、Witness ノードのメンテナンスモード解除

NEC Hyper Converged System の全てのクラスタノードは、出荷時メンテナンスモードに設定されております。VMware vCenter Server より、メンテナンスモードを終了させます。

1. 3.10 節で接続した VMware vSphere Client のメイン画面でクラスタノードを指定し、右クリック→「メンテナンスモード」→「メンテナンスモードの終了」を選択してください。この操作を全てのクラスタノードに対して実施してください。

2. 2 ノード構成の場合は、続いて Witness ノードのメンテナンスモードを解除します。Witness ノード名を指定し、右クリック→「メンテナンスモード」→「メンテナンスモードの終了」を選択してください。

3.16 vSAN クラスタ全台同時停止時の build-in ツールの実行

vSAN クラスタ全台を同時に停止する場合は、build-in ツールの Python スクリプトが実行されており、起動の際にも手動で実行する必要があります。詳細は以下の KB を参照してください。

https://kb.vmware.com/s/article/70650

vSAN クラスタを構成するクラスタノード 1 台に対して本項の手順を実施します。

3 ノード以上の構成の場合、3.13 節で有効にした SSH を利用していずれかのクラスタノードの ESXi Shell に接続してください。
2 ノード構成の場合は、3.13 節を参照し、いずれかのクラスタノードの ESXi Shell に接続してください。

1. ユーザ名 root でログインします。
   - パスワード: 初期パスワード通知書記載のクラスタノードの「ESXi の root パスワード」

   正常にログインが完了すると、下記のように表示されます。

```
nec-esx-cn1 login: root
Password:
The time and date of this login have been sent to the system logs.

WARNING:
   All commands run on the ESXi shell are logged and may be included in
   support bundles. Do not provide passwords directly on the command line.
   Most tools can prompt for secrets or accept them from standard input.

VMware offers supported, powerful system administration tools.  Please
see www.vmware.com/go/sysadmintools for details.

The ESXi Shell can be disabled by an administrative user. See the
vSphere Security documentation for more information.
[root@nec-esx-cn1:~]
```

2. 以下のコマンドを実行します。

```
# python /usr/lib/vmware/vsan/bin/reboot_helper.py recover
```

```
[root@nec-esx-cn1:~]
[root@nec-esx-cn1:~] python /usr/lib/vmware/vsan/bin/reboot_helper.py recover
```

3. 実行結果として「Cluster reboot/poweron is completed successfully!」と表示されていることを確認してください。

```
[root@nec-esx-cn1:~] python /usr/lib/vmware/vsan/bin/reboot_helper.py recover
Begin to recover the cluster...
Time among hosts are synchronized.
Scheduled vSAN cluster restore task.
Waiting for the scheduled task...(44s left)
Waiting for the scheduled task...(14s left)
Checking network status...
Recovery is not ready, retry after 10s...
Network checking done.
Cluster reboot/poweron is completed successfully!
```

※ 実行後、Timeout になる場合があります。その場合は、再度手順 2 のコマンドを実行してください。

```
[root@nec-esx-cn1:~] python /usr/lib/vmware/vsan/bin/reboot_helper.py recover
Begin to recover the cluster...
Time among connected hosts are synchronized.
Scheduled vSAN cluster restore task.
Waiting for the scheduled task...(57s left)
Waiting for the scheduled task...(27s left)
Checking network status...
Recovery is not ready, retry after 10s...
Recovery is not ready, retry after 10s...
Recovery is not ready, retry after 10s...
Timeout, please try again later
[root@nec-esx-cn1:~]
```

4. 以下のコマンドを実行し、ESXi Shell を終了します。

```
# exit
```

```
[root@nec-esx-cn1:~] exit
```

3.17 クラスタメンバの更新の有効化

vSAN クラスタ全台を同時に停止する場合は、クラスタメンバの更新が無効化されているため、起動の際には有効に戻す必要があります。詳細は以下の KB を参照してください。

https://kb.vmware.com/s/article/70650

vSAN クラスタを構成するすべてのクラスタノードに対して本項の手順を実施します。2 ノード構成の場合は、Witness ノードに対しても実施してください。

3 ノード以上の構成の場合、3.13 節で有効にした SSH を利用して各クラスタノードの ESXi Shell に接続してください。
2 ノード構成の場合は、3.14 節を参照し、各クラスタノードと Witness ノードの ESXi Shell に接続してください。

1. ユーザ名 root でログインします。

   - パスワード: 初期パスワード通知書記載のクラスタノードの「ESXi の root パスワード」

   正常にログインが完了すると、下記のように表示されます。

```
The time and date of this login have been sent to the system logs.

WARNING:
   All commands run on the ESXi shell are logged and may be included in
   support bundles. Do not provide passwords directly on the command line.
   Most tools can prompt for secrets or accept them from standard input.

VMware offers supported, powerful system administration tools.  Please
see www.vmware.com/go/sysadmintools for details.

The ESXi Shell can be disabled by an administrative user. See the
vSphere Security documentation for more information.
[root@nec-esx-cn1:~]
```

2. 以下のコマンドを実行します。

```
# esxcfg-advcfg -s 0 /VSAN/IgnoreClusterMemberListUpdates
```

```
[root@nec-esx-cn1:~]
[root@nec-esx-cn1:~] esxcfg-advcfg -s 0 /VSAN/IgnoreClusterMemberListUpdates
```

3. 実行結果として「Value of IgnoreClusterMemberListUpdates is 0」と表示されていることを確認してください。

```
[root@nec-esx-cn1:~] esxcfg-advcfg -s 0 /VSAN/IgnoreClusterMemberListUpdates
Value of IgnoreClusterMemberListUpdates is 0
```

4. 以下のコマンドを実行し、ESXi Shell を終了します。

```
# exit
```

```
[root@nec-esx-cn1:~] exit
```

5. SSH を有効にした場合は、3.13 節の《補足》を参照し、SSH を無効にしてください。

6. 本節の 1～5 の手順をすべてのクラスタノードと Witness ノードに対して実施します。

3.18 vCLS の Retreat モードの無効化

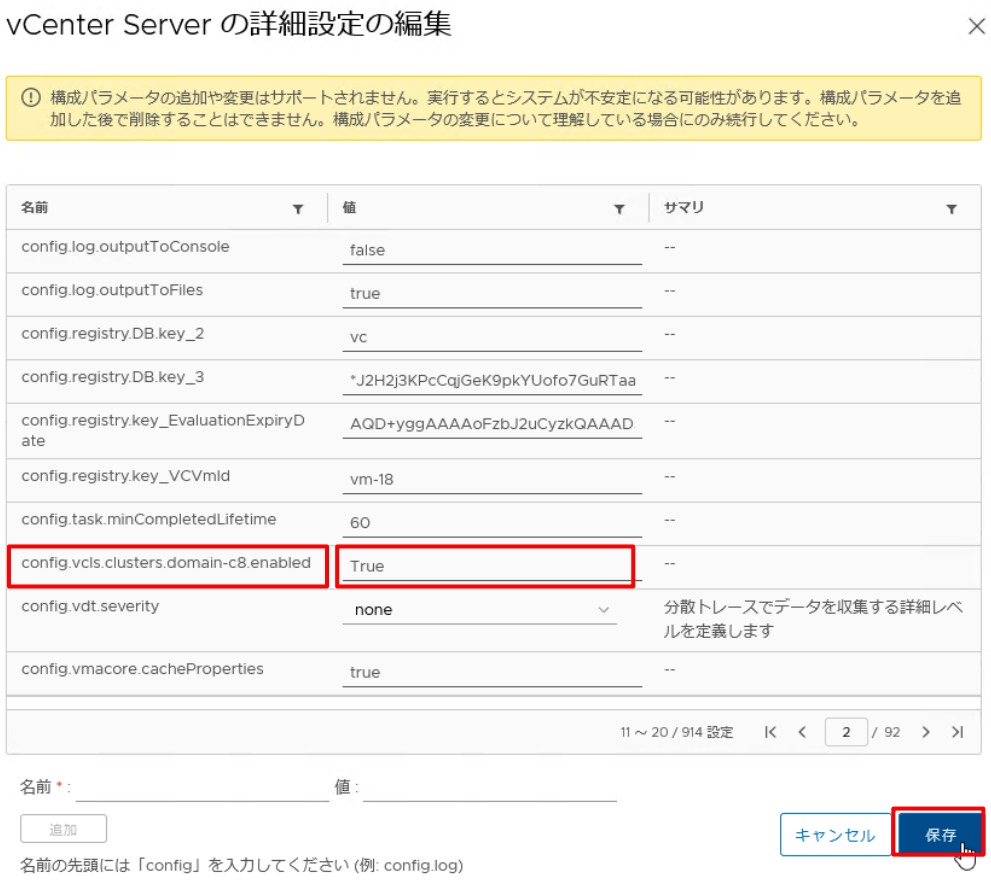
vSphere7.0 Update1 以降では vSphere Cluster Service(vCLS)が導入されたため、以下の手順の実施が必要です。vSphere7.0 Update1 より前の場合は本節の実施は不要です。

vSAN クラスタ全台を同時に停止する場合、vCLS の Retreat モードが有効に設定され vCLS エージェント VM が削除されているため、手動で Retreat モードを無効にして、vCLS エージェント VM を再作成する必要があります。

本項の手順を実施し、Retreat モードを無効化します。

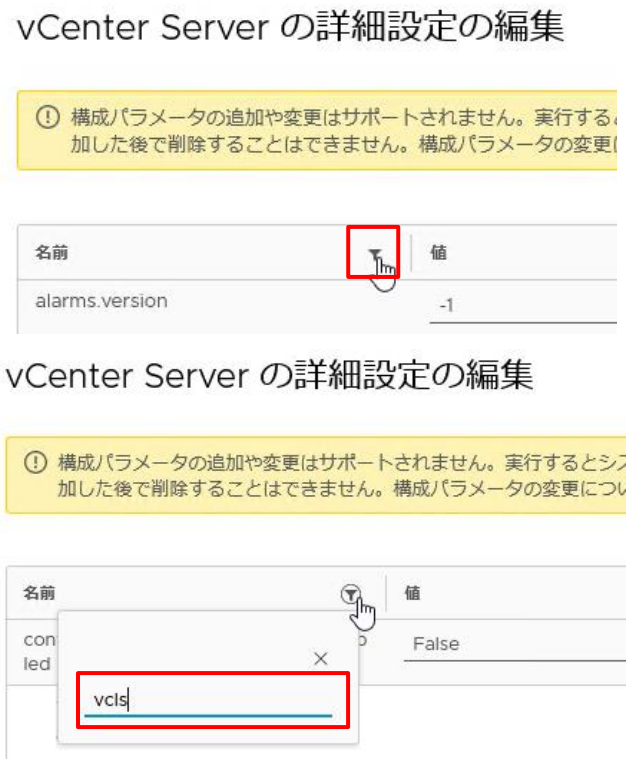
1. オブジェクトナビゲータの vCenter Server 名をクリックし、「構成」→「詳細設定」→「設定の編集」をクリックします。

2. 「vCenter Server の詳細設定の編集」画面が表示されますので、構成パラメータ "config.vcls.clusters.domain-c<number>.enabled"(本書では、<number>=8) の値を確認し、”False”になっている場合は”True”と入力し、「保存」をクリックします。



《補足》

構成パラメータを検索する場合は、名前の右側にあるアイコンをクリックし、「vcls」と入力して表示された結果を確認してください。



《補足》

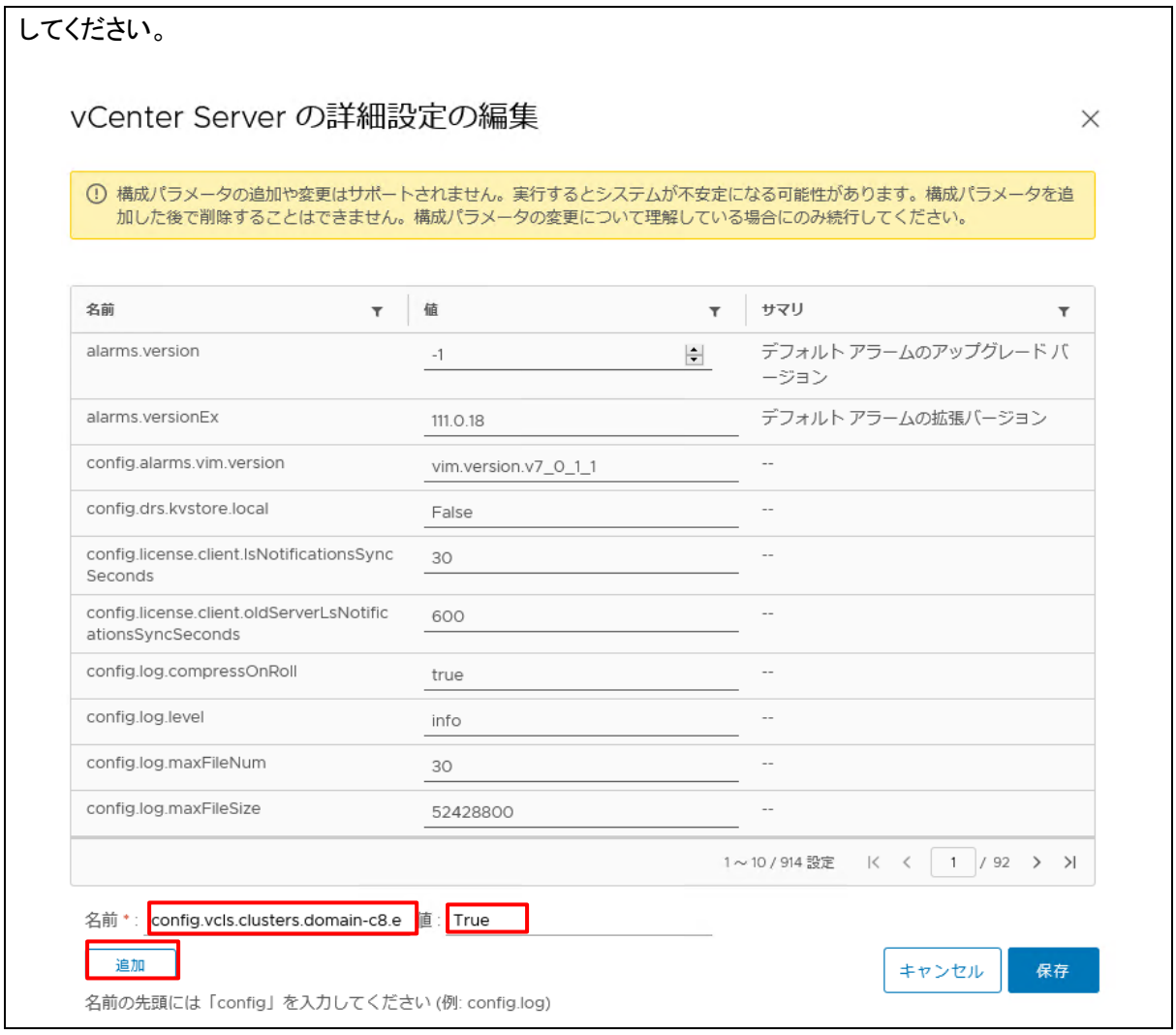
構成パラメータ"config.vcls.clusters.domain-c<number>.enabled"がない場合は、以下の手順で追加します。

1. Retreat モードを無効にする vSAN クラスタを選択した状態で、画面上部の URL からクラスタのドメイン ID を確認します。

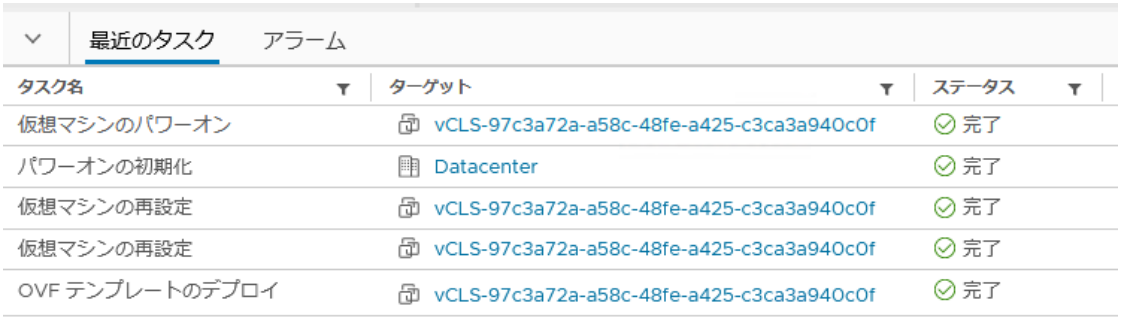
※ “domain-c<number>”などの表記になっています。(本書では“domain-c8”)

2. 本節の手順 1 を参照して「vCenter Server の詳細設定の編集」画面を開き、画面下部の「名前」欄に「config.vcls.clusters.domain-c<number>.enabled」、「値」欄に「True」と入力し、「追加」をクリック

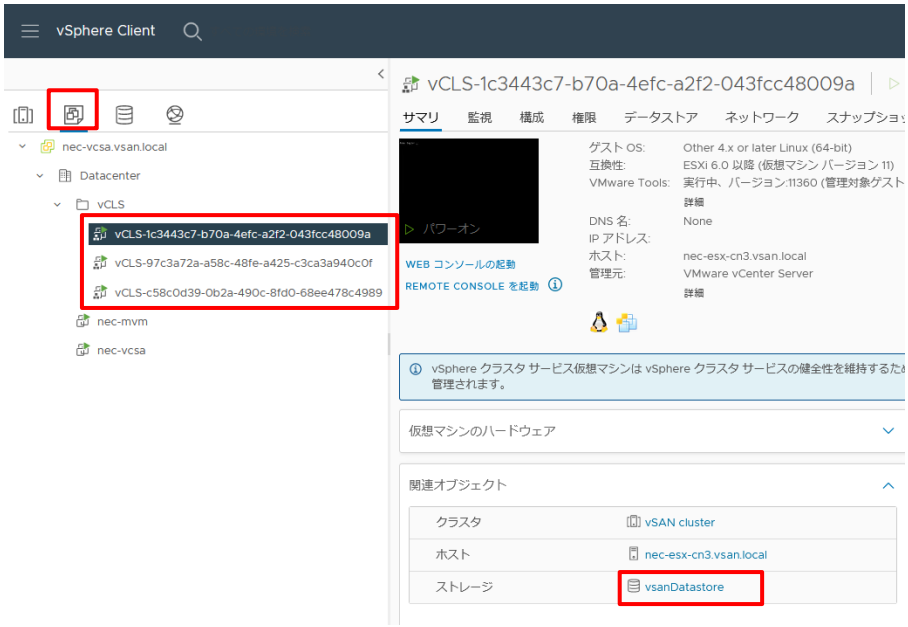
してください。



3. しばらくすると、vCLS エージェント VM のデプロイが開始されます。画面下部の「最近のタスク」に「OVF テンプレートのデプロイ」「仮想マシンのパワーオン」等のタスクが表示されますので、正常に完了することを確認してください。



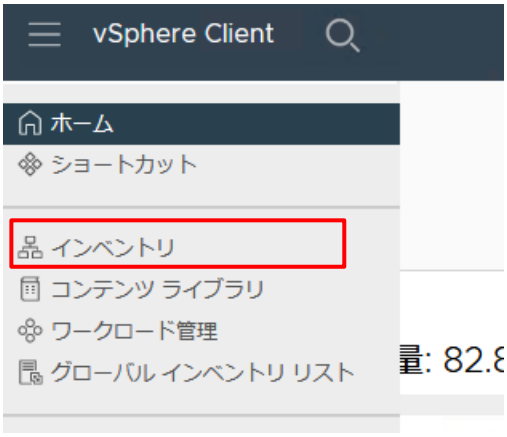
4. オブジェクトナビゲータで、vCLS エージェント VM が 3 台(2 ノード構成の場合は 2 台)作成されていること、電源状態がオンになっていることを確認します。続いて、各 vCLS エージェント VM のサマリから、ストレージが vSAN データストア(本書では vsanDatastore)になっていることを確認します。



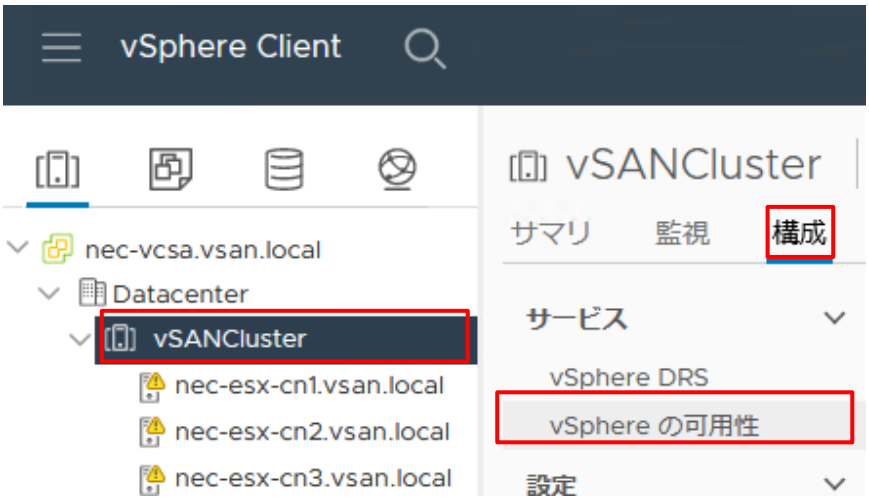
3.19 vSphere の可用性設定

vSAN クラスタの vSphere の可用性を設定します。

1. 3.10 節で接続した VMware vSphere Client の画面左上のメニューアイコンをクリックし、表示されるメニューから[インベントリ]をクリックします。



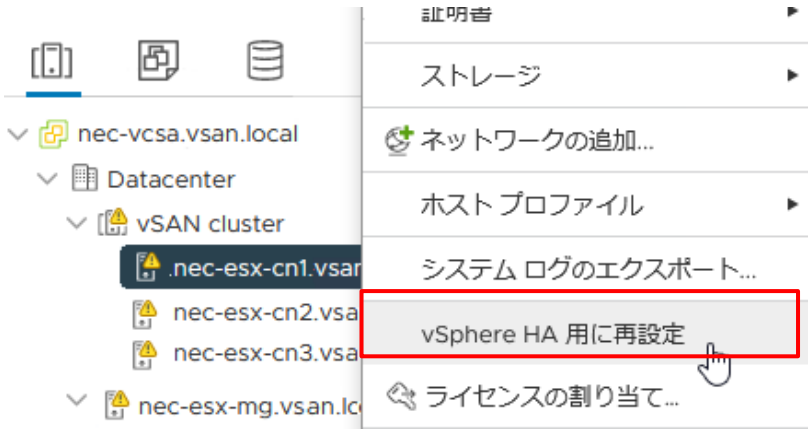
2. vSAN クラスタ名をクリックし、「構成」→「vSphere の可用性」の順に選択します。



3. 画面右上の「編集」をクリックします。

4. 「クラスタ設定の編集」画面が表示されますので、「vSphere HA」を有効にし、「OK」をクリックします。

5. 続いて、VMware vSphere Client のオブジェクトナビゲータで任意のクラスタノード名を右クリックし、表示されるメニューにて[vSphere HA 用に再設定]をクリックします。この操作を、全てのクラスタノードに対して実施します。



6. 再度手順 2 から手順 3 の操作を実施した後、「障害および対応」をクリックし、「ホスト監視の有効化」を有効にし、「OK」をクリックします。

7. 「障害状態および応答」を確認します。

3 ノード以上の構成の場合、「ホスト失敗」が「仮想マシンを再起動」、「ホスト隔離」が「仮想マシンをパワーオフして再起動」になることを確認します。

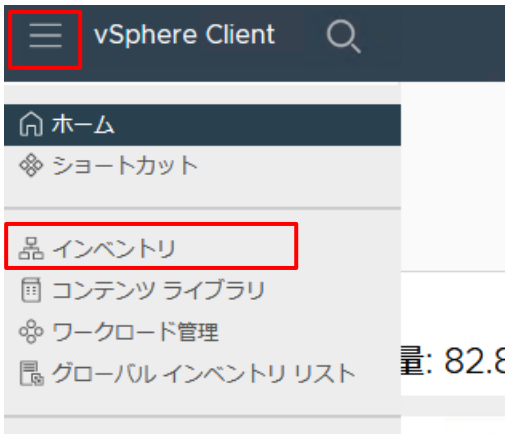
2 ノード構成の場合、「ホスト失敗」が「仮想マシンを再起動」になることを確認します。

3.20 vSAN ストレージプロバイダの同期

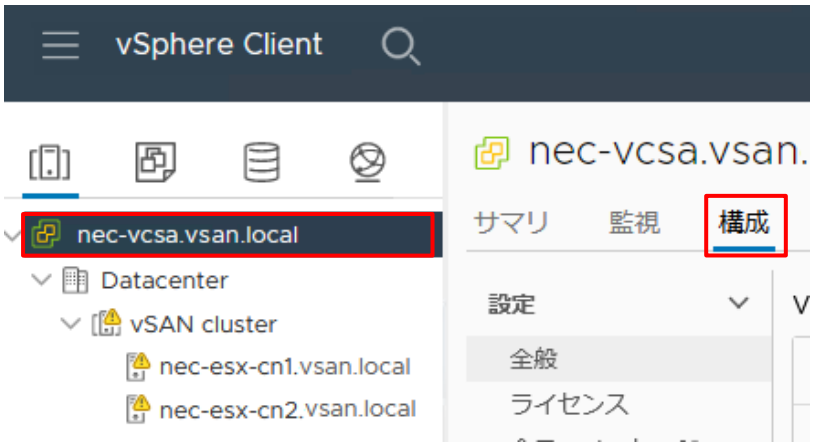
下記の問題を回避するために、vSAN ストレージプロバイダの同期を行います。

https://kb.vmware.com/s/article/52286

1. 3.10 節で接続した VMware vSphere Client の画面左上のメニューアイコンをクリックし、表示されるメニューから[インベントリ]をクリックします。

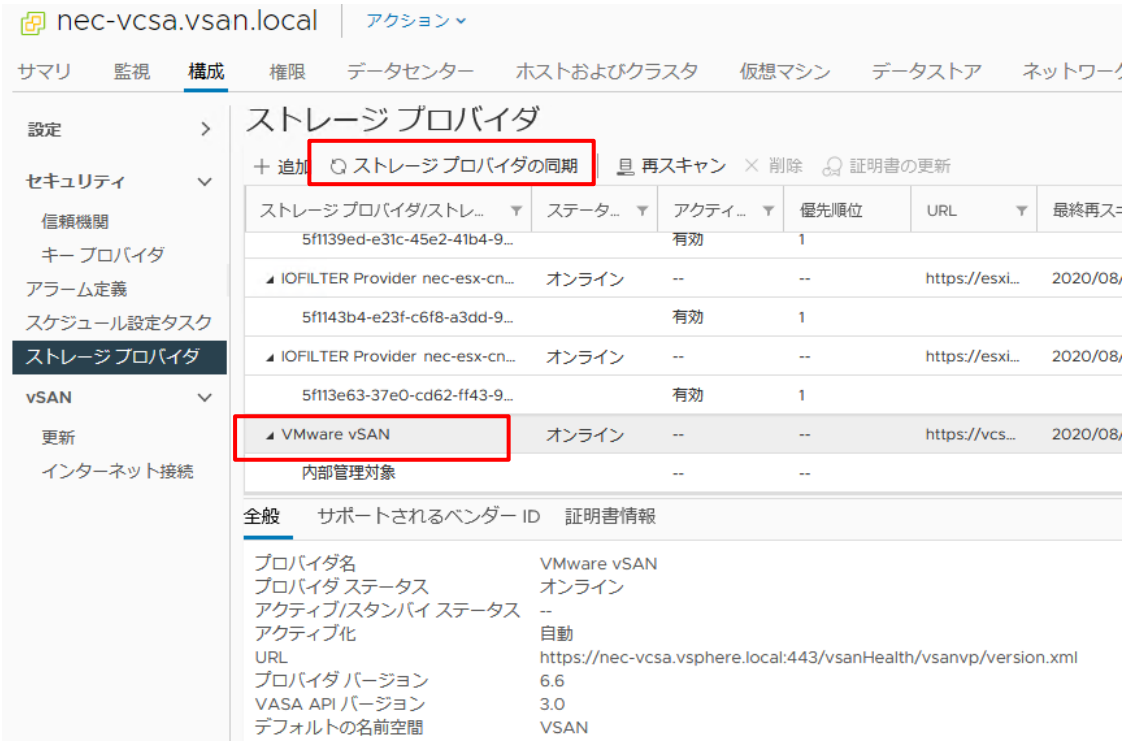


2. オブジェクトで vCenter Server 名をクリックし、画面中央上部の[構成]タブをクリックします。



3. [ストレージプロバイダ]をクリックします。

4. タブ画面右に表示された一覧から「VMware vSAN」を選択し、[ストレージプロバイダの同期]をクリックします。

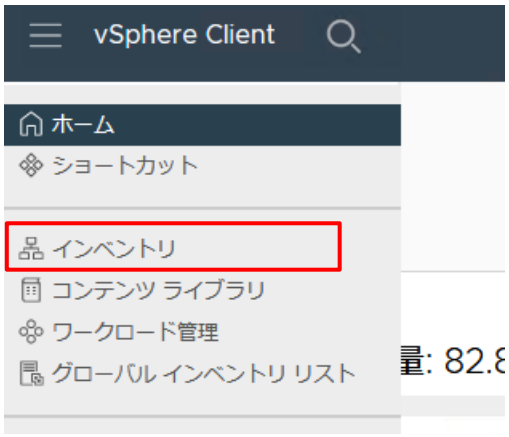


5. 画面が更新されるので、ステータスが「オンライン」になっていることを確認します。

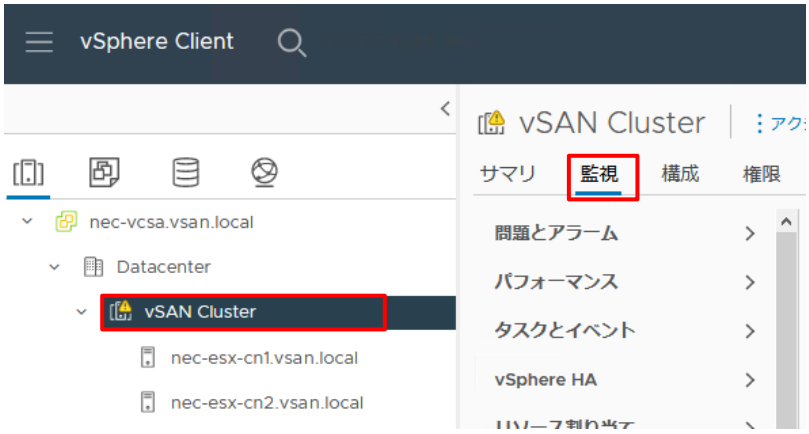
3.21 VMware vSAN 状態の確認(健全性確認)

VMware vSAN クラスタの状態を確認し、健全性ツリーにエラーがでていないことを確認します。

1. 3.10 節で接続した VMware vSphere Client の画面左上のメニューアイコンをクリックし、表示されるメニューから[インベントリ]をクリックします。



2. オブジェクトで vSAN クラスタ名をクリックし、画面中央上部の[監視]タブをクリックします。



3. [監視]タブの下の[vSAN]をクリックし、さらにその下の、タブ画面内左のメニューで[skyline 健全性]をクリックした後、タブ画面右の、一覧の上に表示されている[再テスト]をクリックします。

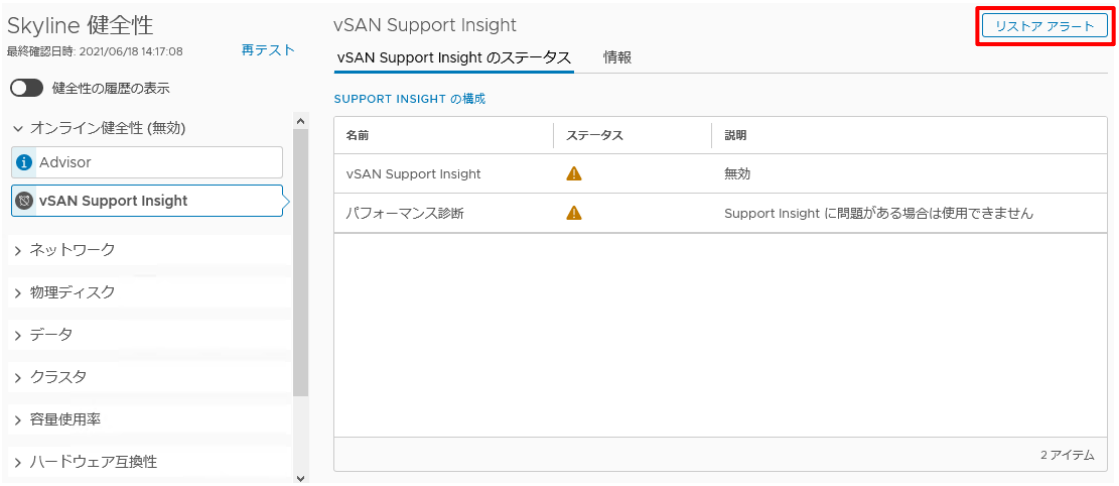
4. vSAN 環境の健全性確認の結果が画面右の一覧に表示されますので、「テスト結果」欄が全てパスであることを確認します。

《注意》

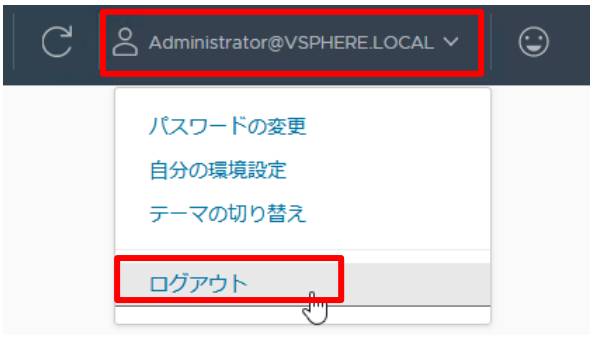
vSAN 健全性で警告が存在すると、vSAN クラスタに登録されているクラスタノードのノード状態が NEC Hyper Converged System Console において警告と表示されます。これを防ぐため、以下の項目は構築時にサイレンスアラートの設定を実施しています。

- vSAN ビルドに関する推奨事項
  - vSAN ビルドに関する推奨事項エンジンの健全性
  - vSAN リリースカタログの更新状態
    ※ vSAN リリースカタログの更新状態は表示されない場合もあります。
- オンライン健全性(無効)
  - vSAN Support Insight
- ハードウェア互換性
  - vSAN HCL DB の更新状態

サイレンスアラートに設定されている項目は [リストアアラート]をクリックすることでリストアできます。各項目でリストアを実施するかは、お客様の環境(インターネット接続可能か)などに応じてお客様自身で検討ください。



5. 以上で VMware vSAN、ESXi の確認は完了です。メイン画面に戻り、VMware vSphere Client からログアウトしてください。



3.22 NEC Hyper Converged System Console の動作確認

3.22.1 ログイン

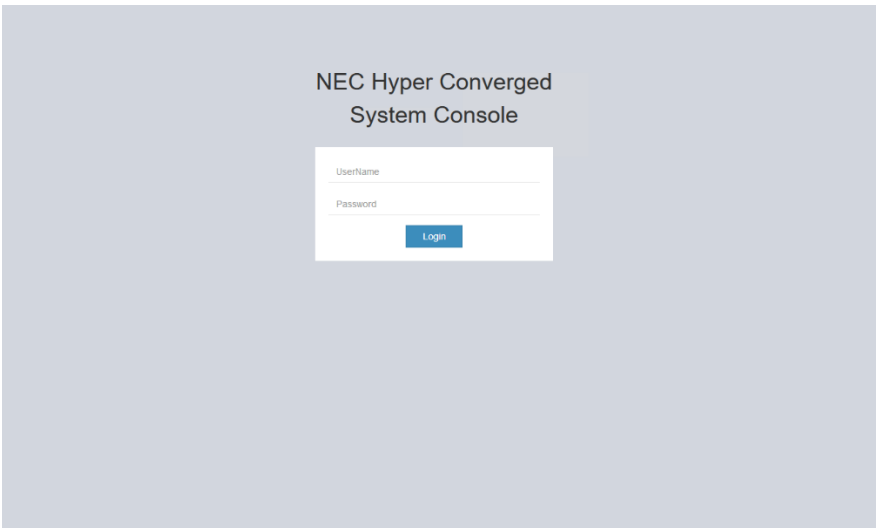
管理 VM 上で Web ブラウザを起動し、NEC Hyper Converged System Console にログインします。

1. 3.8 節でリモートデスクトップ接続した管理 VM 上で Web ブラウザを起動します。
2. Web ブラウザのアドレス欄に以下の URL を入力します。
   - http://<ホスト名>/nechcs/
     ホスト名: ヒアリングシートの管理 VM の「ホスト名(FQDN 名)」
3. 正しく NEC Hyper Converged System Console に接続できると、Web ブラウザに NEC Hyper Converged System Console のログインウィンドウが表示されます。
4. ログインウィンドウにアカウント情報を入力し、NEC Hyper Converged System Console にログインします。
   - ユーザ名: ヒアリングシートの HCS_Console の「HCS_Console: 管理ユーザ ID」
   - パスワード: 初期パスワード通知書の「HCS_Console: 管理パスワード」

【重要】

「NEC Hyper Converged System Console v3.0 ユーザーズガイド」に記載されている初期ユーザ名、パスワードは使用できません。
初期パスワード通知書に記載されているユーザ名、パスワードを入力し、ログインしてください。

NEC Hyper Converged System Console は http 通信のみ有効化しています。https 通信を有効化する場合は、本書手順の完了後「NEC Hyper Converged System Console v3.0 ユーザーズガイド」を参照のうえ有効化手順を実施してください。



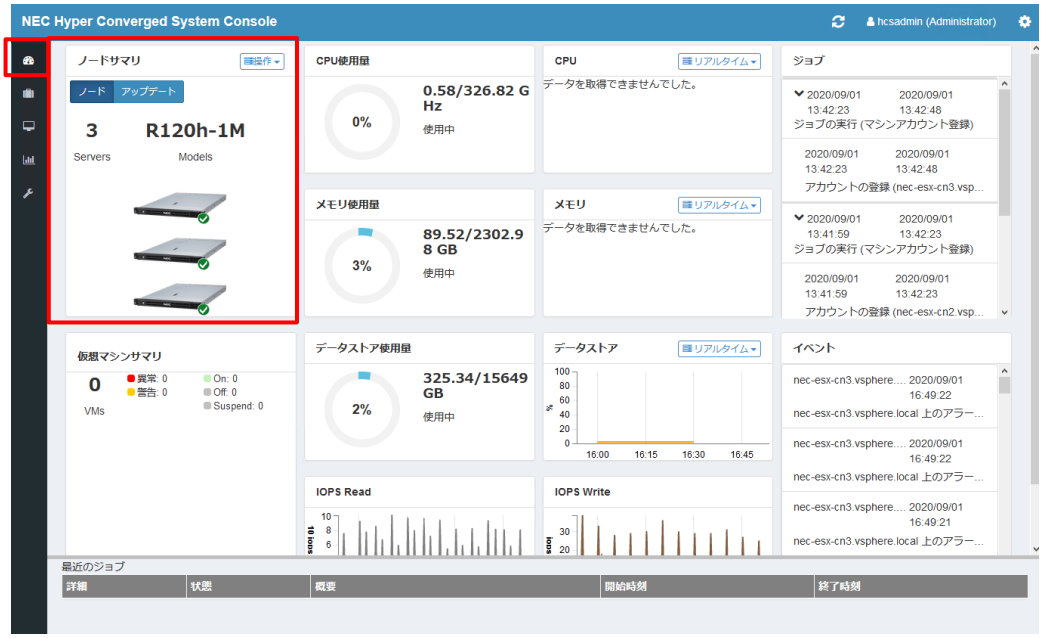
《注意》

- NEC Hyper Converged System が使用するポート番号を組み立て仕様書で既定値(80) から変更している場合は、ホスト名には、「ホスト名(FQDN):ポート番号」を入力してください。
- サービス "PVMService" が起動していない状態で、NEC Hyper Converged System Console を接続しようとするとエラーとなります。NEC Hyper Converged System Console ユーザーズガイドの「SystemProvisioning を起動/ 再起動/ 停止するには」を参照し、手動でサービスを起動してください。

3.22.2 動作確認

NEC Hyper Converged System Console のログインに成功すると、ポータル画面が表示されます。下記手順にて正しく動作していることを確認します。

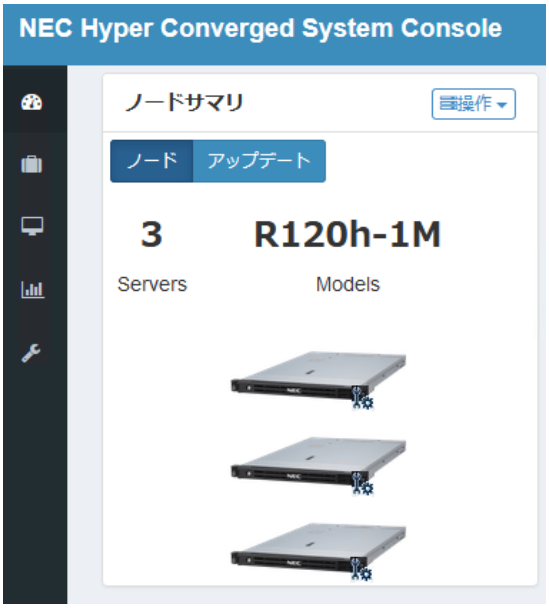
・[ダッシュボード]タブ



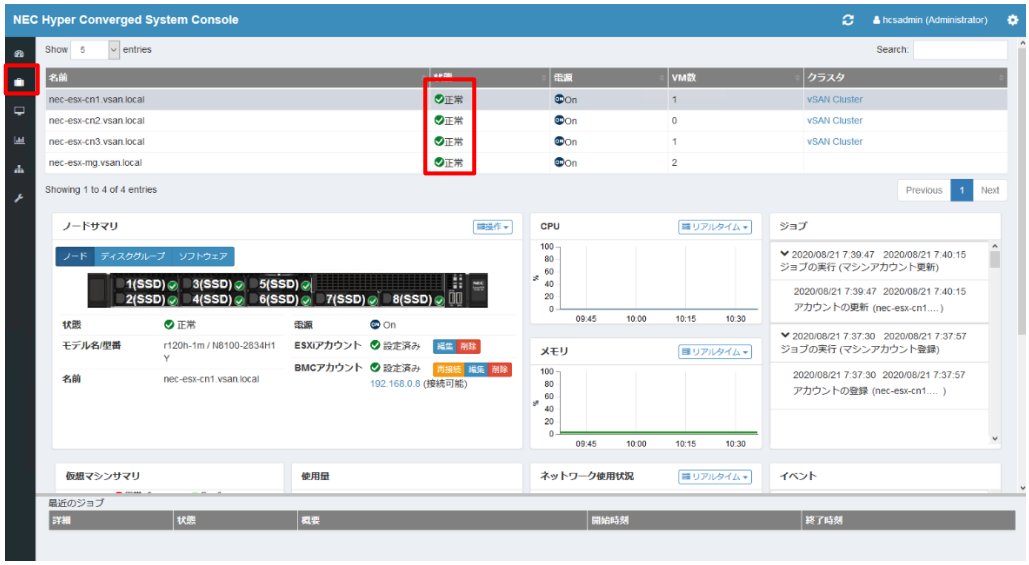
登録したノードが全て、ノードサマリに表示されたノードの台数をご確認ください。

お客様の手元に届いてからしばらくは、CPU 使用率/メモリ使用率など一部の情報が表示されないことがあります。ある程度の時間(目安: 半日)運用し、性能データが蓄積された後に表示されますが、数日経っても表示されない場合は、1.2 節の構築サービス窓口までご連絡ください。

※ NEC Hyper Converged System Console にログイン後、ノードサマリに表示されているアイコンが、[メンテナンスモード]となっている場合があります。本節の[node]タブの説明内の《補足》を参照し、メンテナンスモードを解除してください。



・[node]タブ



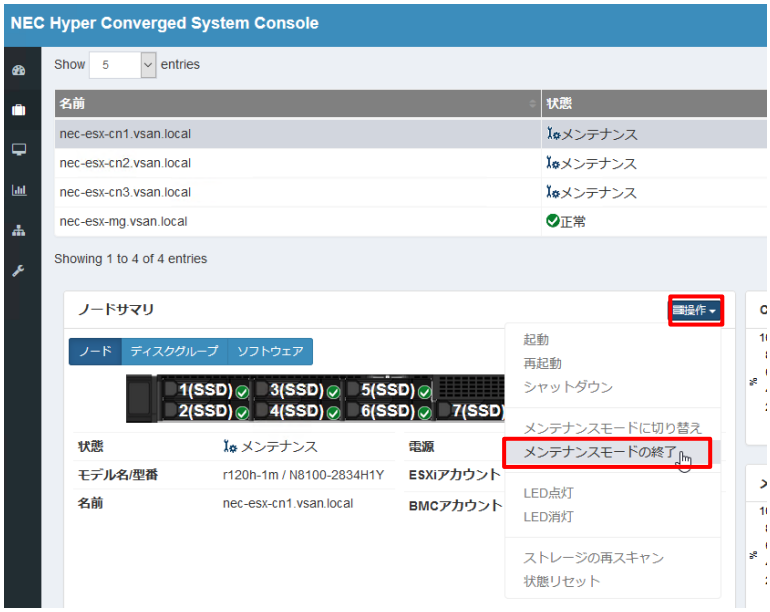
登録したノードと状態がリスト形式で表示されます。

詳細を確認したいノードをクリックすると、各ノードの詳細情報が表示されます。

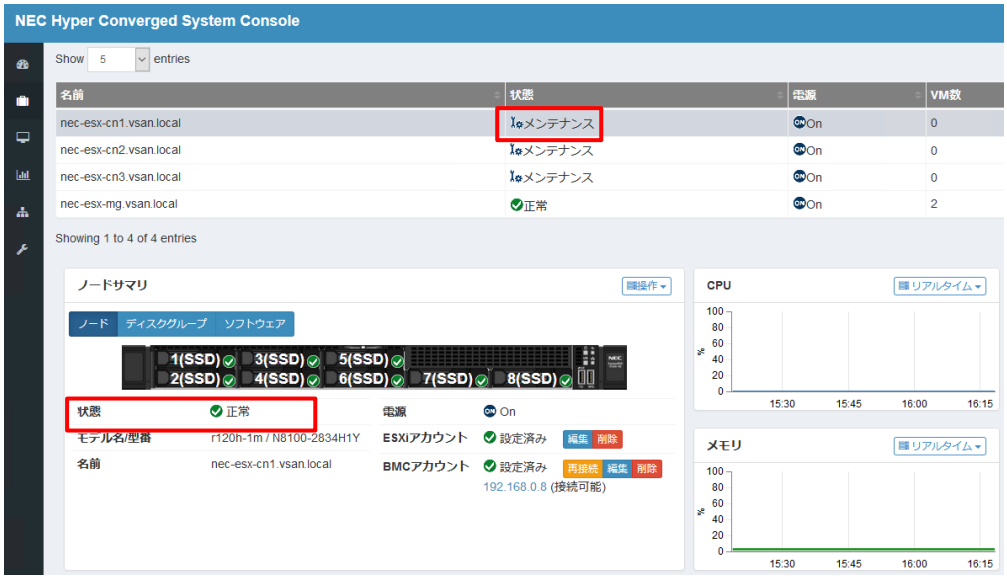
インストール直後は CPU 使用量/メモリ使用量等、一部の情報が表示されません。ある程度運用し、ノードとの通信が行われた後に表示されます。

《補足》
クラスタノードの起動後、3.15 節でメンテナンスモードの解除をしている場合でも
NEC Hyper Converged System Console 上でのノードの状態がメンテナンスモードのままとなる場合があります。

この場合、ノードサマリの[操作]をクリックした後[メンテナンスモードの終了]をクリックし、メンテナンスモードが解除されることを確認します。



ノードサマリ内の状態が”正常”になっていることを確認してください。
画面上部のノード一覧の”状態”表示は、一度[node]タブ以外のタブに切り替えると表示が更新されます。

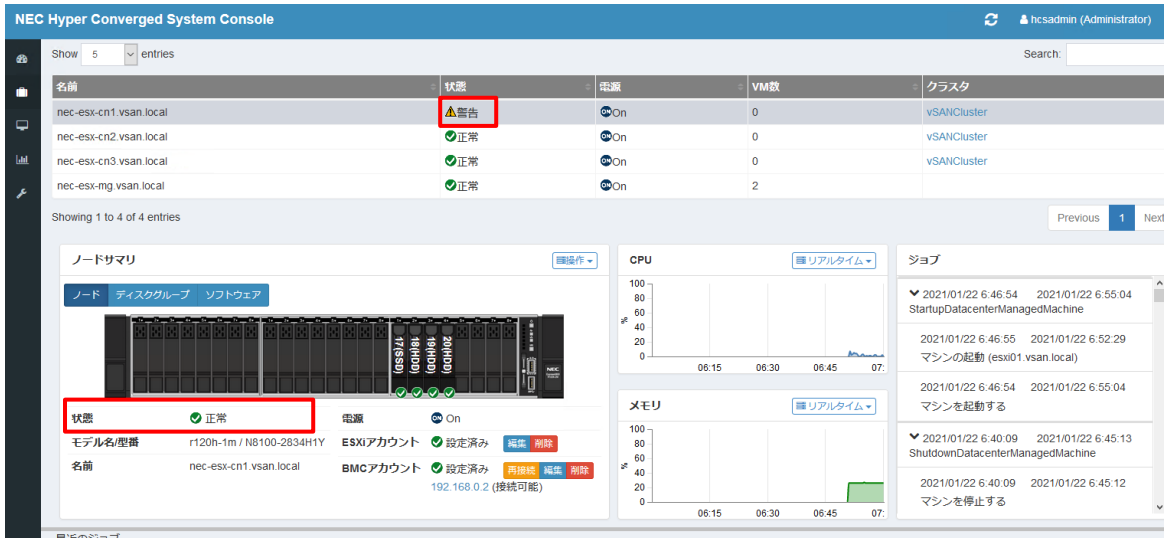


《補足》
クラスタノードの起動およびメンテナンスモードの解除後、3.21 節の健全性テストの結果に問題がない場合においても、NEC Hyper Converged System Console 上でのクラスタノードの状態に「警告」と表示され、ノードサマリの[状態]の数字をクリックして表示される通知一覧に「接続状態」「ストレージ接続性」などが表示されることがあります。

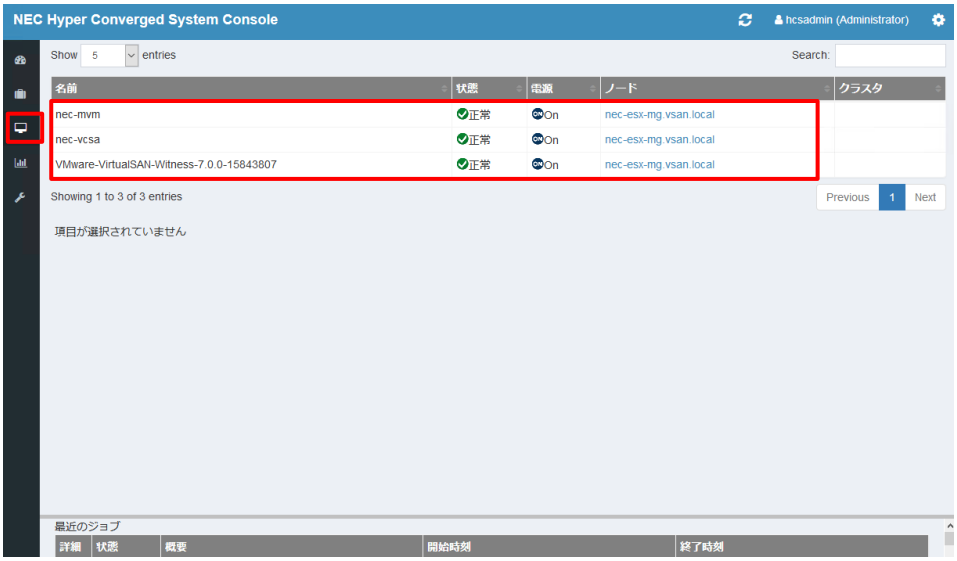
※　下記画像は一例です。複数の警告ではなく、一件の警告のみが表示される場合もあります。

この場合、ノードサマリの[操作]をクリックした後に[状態リセット]をクリックし、その後警告が解消されることを確認してください。

ノードサマリ内の状態が”正常”になっていることを確認してください。
画面上部のノード一覧の”状態”表示は、一度[node]タブ以外のタブに切り替えると表示が更新されます。



・[仮想マシン]タブ



作成した仮想マシン（VM）の一覧と状態がリスト形式で表示されます。

詳細を確認したい仮想マシン（VM）をクリックすると、仮想マシン（VM）の詳細情報が表示されます。

登録した vCenter Server やノード上に仮想マシンを作成していない状態では、表示されません。

・[監視]タブ

NEC Hyper Converged System Console のジョブ・イベント情報が、リスト形式で表示されます

各ジョブの［詳細］をクリックすると詳細情報が表示されます。

以上で受入確認は完了です。正しく動作しない場合は 1.2 節の構築サービス窓口までご連絡ください。

3.23 エクスプレス通報サービスの開局手続き

本節は、エクスプレス通報サービスを利用する場合のみ実施します。

エクスプレス通報サービスの運用を始めるには以下の作業が必要となります。

作業項目	お客様作業	NEC 営業作業
(1)管理ノード/クラスタノードの保守契約締結	○	○
(2)管理ノード/クラスタノードのエクスプレス通報サービス申し込み	○	○
(3)クラスタノード HDD 障害通報の申請	―	○
(4)クラスタノード HDD 障害のエクスプレス通報サービス申し込み	―	○
(5)HCS Console の設定	△*1	―
(6)エクスプレス通報サービス(MG)のインストール	△*2	―
(7)エクスプレス通報サービス(MG)の設定	△*2	―
(8)ESMPRO/SM の設定	△*2	―
(9)開局作業	○	―

△*1:構築サービスを実施している場合は、お客様での作業は不要

△*2:構築サービスでエクスプレス通報サービス設定(オプション項目) 実施している場合は、お客様での作業は不要

事前に作業項目(1)～(4)を実施しておき、(5)以降を実施する際に以下を用意しておく必要があります。

- 管理ノード、クラスタノードの開局キー
- 管理 VM 用の開局キー
- 管理 VM 用の受信情報設定ファイル(構築サービスでエクスプレス通報サービス設定を実施した場合は不要)

事前準備が出来ていない場合は、用意ができてから本項を実施して下さい。

(1)管理ノード/クラスタノードの保守契約締結

管理ノード/クラスタノードの保守を手配してそれぞれの機器管理番号を取得します。

保守の手配方法については、弊社営業にご相談ください。

(2)管理ノード/クラスタノードのエクスプレス通報サービス申し込み

エクスプレス通報サービスの申し込みを行い管理ノード/クラスタノードの開局キーを取得します。

エクスプレス通報サービスの申し込み方法については、以下を参照するか、弊社営業にご相談ください。

NEC エクスプレス通報サービス ご利用の手引き

http://acc.express.nec.co.jp/notice/man/guide.htm

(3)クラスタノード HDD 障害通報の申請

弊社営業が申請作業を行いますので、弊社営業にご相談ください

本作業により、管理 VM 用の受信情報設定ファイルと機器管理番号を取得します。

(4)クラスタノード HDD 障害のエクスプレス通報サービス申し込み

弊社営業が作業を行いますので、弊社営業にご相談ください

本作業により、管理 VM 用の開局キーを取得します。

(5)HCS Console の設定

NEC HCS Console を起動/ログインし、アラートビューア連携機能を有効にして、vCenter Server が検出したアラームを、アラートビューアに表示できるようにします。

1. 画面左側のメニューで[設定]をクリックし、[設定]画面に切り替えます。
2. 画面上部の[通報設定]タブをクリックすると通報設定画面が表示されますので、[編集]をクリックします。

3. 「通報設定」ダイアログが表示されますので、[アラートビューア連携を行う]にチェックを付けた後、表示された入力欄に vCenter アラームの SNMP レシーバ情報（ホスト名/IP アドレス、ポート、SNMP コミュニティ名）を入力して、[適用] をクリックします。

設定項目	説明
アラートビューア連携を行う	アラートビューア連携機能を利用する場合、チェックボックスをオンにします。
ホスト名/IP アドレス	トラップ送信先サーバ名 (ホスト名、または IP アドレス) を入力します。 NEC HCS Console、ESMPRO/ServerManager をインストールした管理サーバを設定してください。入力できる文字数は 63 文字以内です。
ポート	トラップ送信の UDP ポート番号を入力します。 「1～65535」の範囲で設定することができます。既定値は (162) です。
SNMP コミュニティ名	SNMP コミュニティ名を入力します。既定値は (public) です。

4. 設定後、ESMPRO/ServerManager の全てのサービスを停止し、その後全てのサービスを起動してください。

サービス停止/開始順序
サービスを停止/開始する場合は、下記の順序に従ってください。

■停止順序
1. ESMPRO/SM Web Service
2. ESMPRO/SM Task Service
3. DianaScope ModemAgent
4. ESMPRO/SM Web Container
5. ESMPRO/SM Event Manager
6. ESMPRO/SM Base AlertListener
7. ESMPRO/SM Common Component
8. ESM32BridgeService for AlertListener
9. ESM32BridgeService for NvAccessor
10. Alert Manager Socket(R) Service(*)
11. ESMPRO/SM Base Service
12. Dmi Event Watcher(*)
13. ESM Alert Service
14. ESM Command Service
15. ESM Remote Map Service
16. ESM Base Service
17. Alert Manager HTTPS Service(*)
18. Alert Manager WMI Service

■開始順序
1. Alert Manager WMI Service
2. Alert Manager HTTPS Service(*)
3. ESM Base Service
4. ESM Remote Map Service
5. ESM Command Service
6. ESM Alert Service
7. Dmi Event Watcher(*)
8. ESMPRO/SM Base Service
9. Alert Manager Socket(R) Service(*)
10. ESM32BridgeService for NvAccessor
11. ESM32BridgeService for AlertListener
12. ESMPRO/SM Common Component
13. ESMPRO/SM Base AlertListener
14. ESMPRO/SM Event Manager
15. ESMPRO/SM Web Container
16. DianaScope ModemAgent
17. ESMPRO/SM Task Service
18. ESMPRO/SM Web Service

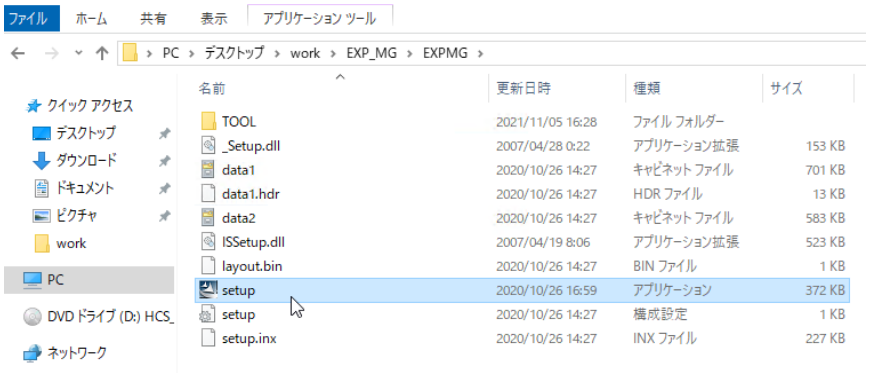
* 設定により停止しています。
停止している場合は、サービスを停止/開始する必要はありません。

(6)エクスプレス通報サービス(MG)のインストール

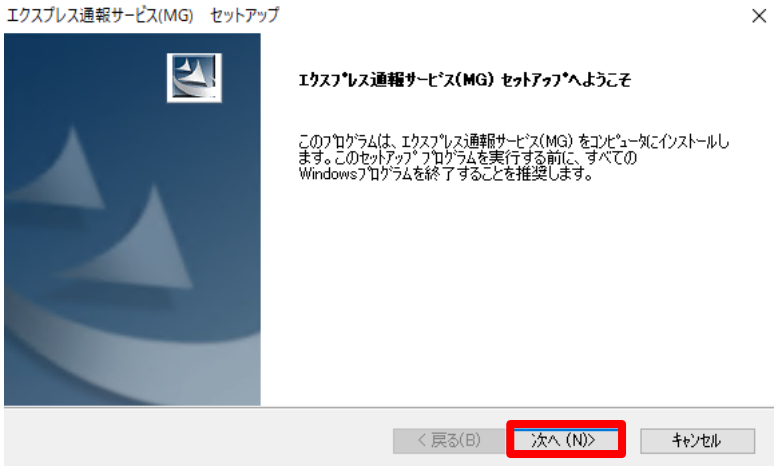
1. インターネットにアクセス可能な Windows 端末で以下 Web ページを表示し、
   エクスプレス通報サービス(MG)のセットアッププログラム(EXP_MG.zip)をダウンロードします。
   https://www.support.nec.co.jp/View.aspx?id=9010102124

2. ダウンロードした zip ファイルを管理 VM 上にコピーし、解凍します。

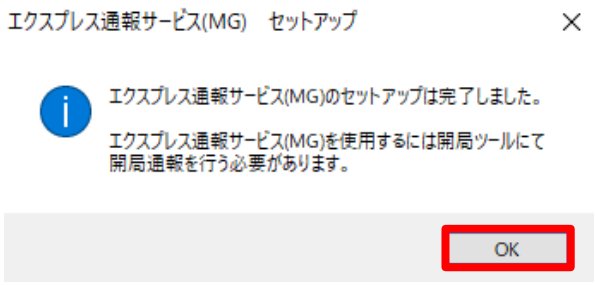
3. [¥EXPMG¥setup.exe]ファイルをダブルクリックします。



4. セットアップ画面が表示されますので、[次へ]をクリックします。



5. 以下の画面が表示されたら、[OK]をクリックします。



6. 管理 VM を再起動します。

以上で、エクスプレス通報サービス(MG)のインストールは完了です。

(7)エクスプレス通報サービス(MG)の設定

エクスプレス通報サービス(MG)に受信情報ファイルを登録します。

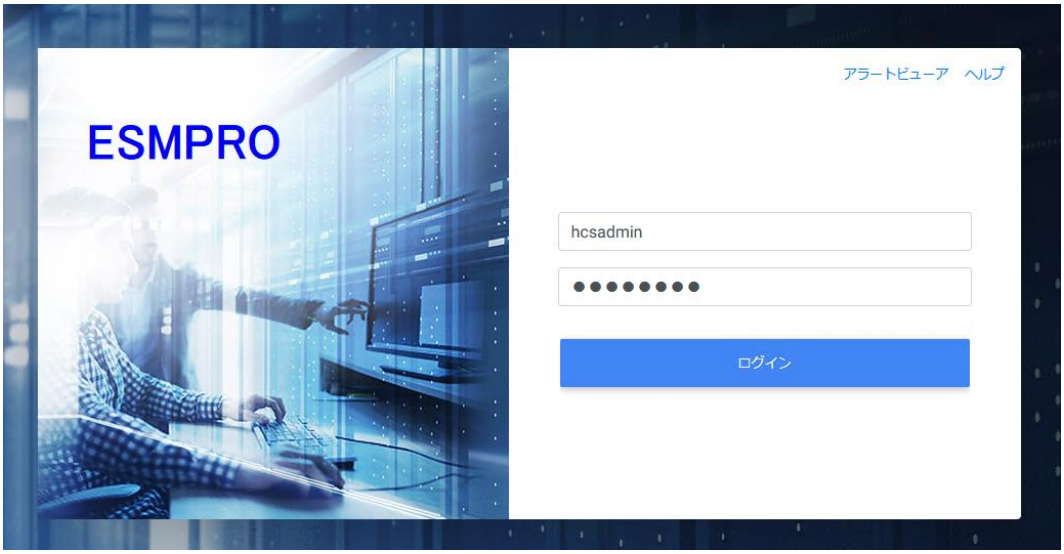
1. 以下の Web ページから iLO 受信情報ファイル(MGMTB.zip)をダウンロードします。

   https://www.support.nec.co.jp/View.aspx?id=9010100096

2. 手順 1 でダウンロードしたファイルと、(3)で弊社営業から入手した管理 VM 用受信情報ファイル(AlertReport.MTB)を管理 VM 上にコピーし、zip ファイルは解凍します。

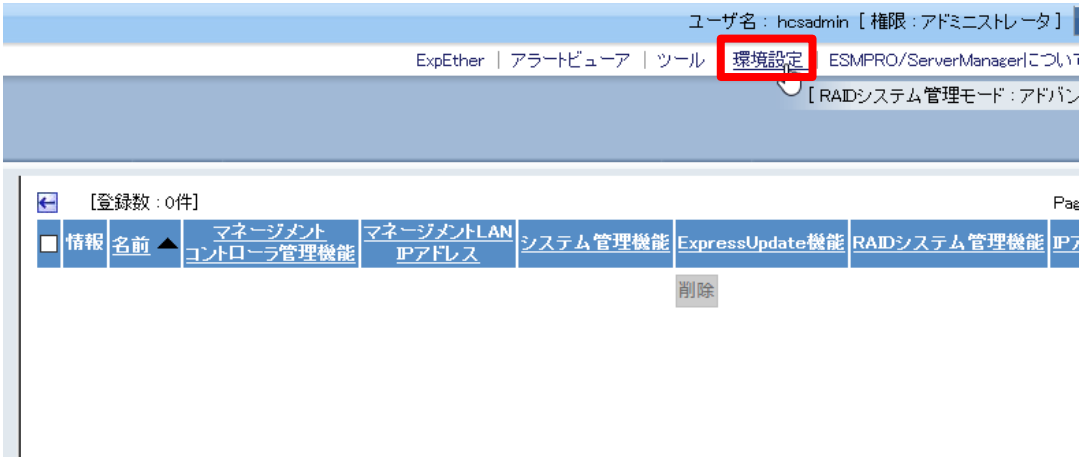
3. 管理 VM で Web ブラウザを起動した後、ESMPRO/ServerManager に接続し、ログインします。

   URL: http:// 管理 VM のホスト名(FQDN 名):21120/esmpro
   (本書では http://nec-mvm.vsan.local:21120/esmpro)



4. 画面右上の[クラシックモード]をクリックし、クラシックモードの画面を開きます。

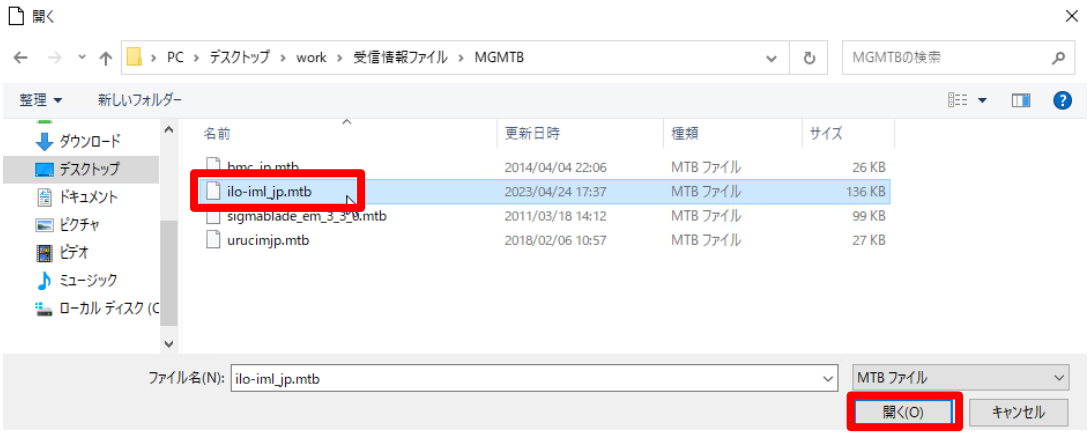
5. 画面右上の[環境設定]をクリックします。



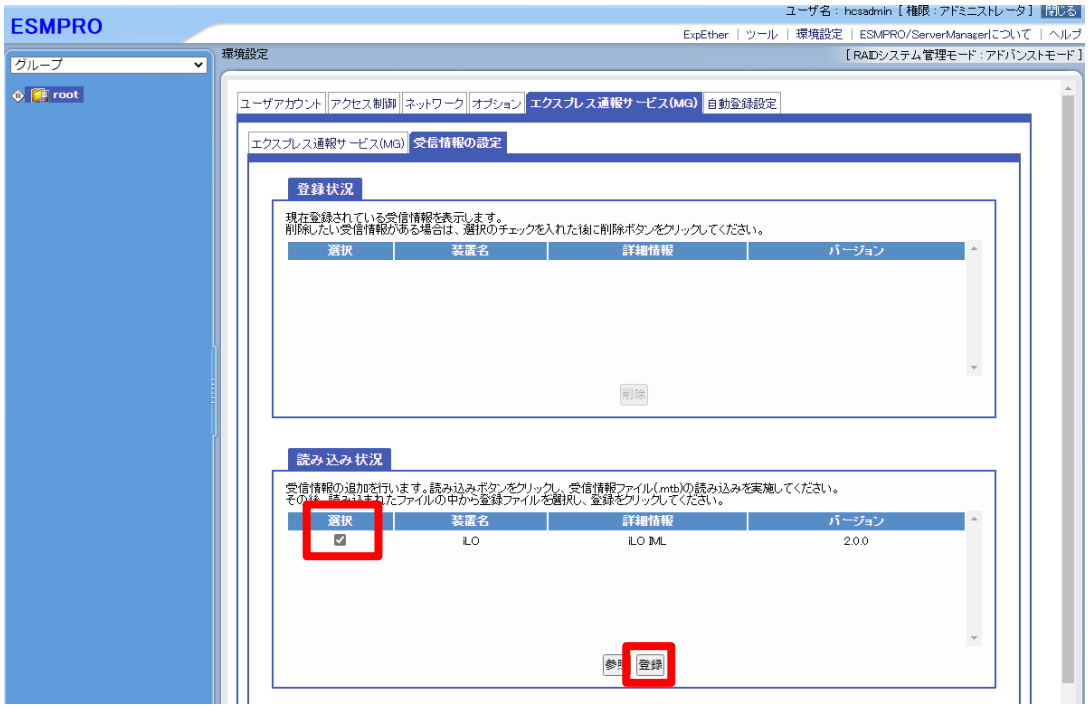
6. 「環境設定」画面が表示されますので、[エクスプレス通報サービス(MG)]タブをクリックします。

7. [受信情報の設定]タブをクリックし、[読み込み状況]配下の[参照]をクリックします。

8. ファイルの選択画面が表示されますので、iLO 用の受信情報ファイル「ilo-iml_jp.mtb」を選択し、[開く]をクリックします。



9. [読み込み状況]配下に、読み込んだ受信情報ファイルが表示されますので、チェックを入れて[登録]をクリックします。



10. [登録状況]配下に登録した受信情報ファイルが表示されます。

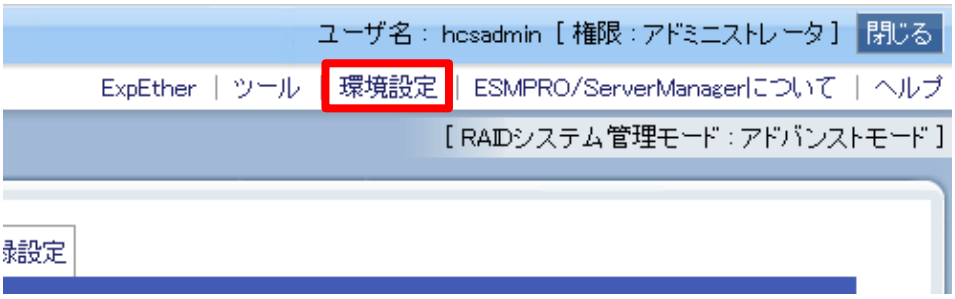
11. 管理 VM 用の受信情報ファイル「AlertReport.MTB」に対しても同様に手順 7 から手順 10 の手順を実施してください。

(8)ESMPRO/SM の設定

ESMPRO/ServerManager にコンポーネントの登録を行います。

(8)-1 環境設定

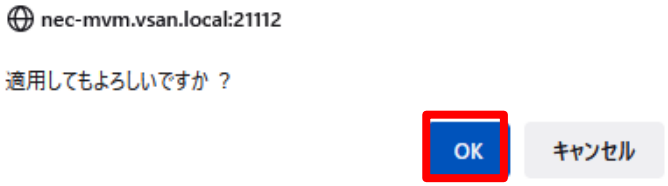
1. (7)の手順 4 を実施してクラシックモードを開いた状態で画面右上の[環境設定]をクリックします。



2. [ネットワーク]タブをクリックし、画面下部の[編集]をクリックします。

3. 「iLO との通信」配下の「自己署名証明」の[許容する]にチェックを入れ、[適用]をクリックします。

4. 以下のダイアログが表示されますので、[OK]をクリックします。



5. 「iLO との通信」配下の「自己署名証明」が「許容する」になっていることを確認し、画面右上の[閉じる]をクリックます。

(8)-2 iLO コンポーネントの登録

ESMPRO/ServerManager に管理ノード、クラスタノードの iLO コンポーネントを登録します。

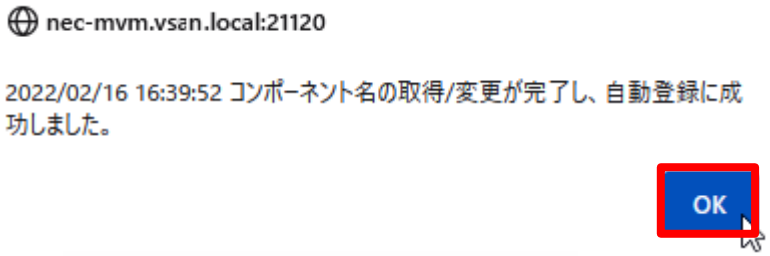
1. 画面上部の[登録]をクリックします。

2. [自動登録]をクリックします。

3. 自動登録画面の「検索範囲」で「検索モード」が「IP アドレス範囲指定検索」になっていることを確認し、検索する iLO の IP アドレスの開始アドレスと終了アドレスを指定します。
   続けて、「サーバ/ストレージ」にチェックを付け、「iLO」を[有効]にし、検索する iLO のユーザとパスワードを入力します。
   「iLO」以外の「検索」は[無効]にし、最後に[検索]をクリックします。


ESMPRO
ダッシュボード
登録
装置
アラートビューア
拡張機能
ツール
環境設定
自動登録
手動登録
登録先グループ
root
検索範囲
検索モード
IPアドレス範囲指定検索
ネットワークアドレス検索
開始アドレス［必須］
172 . 16 . 0 . 7
終了アドレス［必須］
172 . 16 . 0 . 10
サーバ / ストレージ
SNMP（ESMPRO/ServerAgent, iStorage Mシリーズ）
検索
有効
無効
WS-Man (ESMPRO/ServerAgentService, ESXi7以前)
検索
有効
無効
ESXi (ESXi8)
検索
有効
無効
RAIDシステム管理機能
検索
有効
無効
ExpressUpdate機能
検索
有効
無効
BMC（EXPRESSSCOPEエンジン）
検索
有効
無効
iLO
検索
有効
無効
⚠ iLOの管理を行わない場合、装置によってはハードウェア監視を行えない場合があります。装置ごとの詳細については自動登録結果画面を参照してください。
ユーザ名/パスワード［必須］
hcsadmin
/
●●●●●●●●
追加
BMC(その他)
検索
有効
無効
Intel(R) vPro(TM) Technology
検索
有効
無効
UPS
ネットワーク機器
その他コンピュータ機器
検索

4. 検索が開始され、しばらくすると以下のダイアログが表示されますので、[OK]をクリックします。



5. 自動登録結果が表示されますので、指定した iLO コンポーネントが登録されていることを確認し、[装置一覧に戻る]をクリックします。

6. iLO コンポーネントが表示されていることと、状態が「正常」であることを確認します。

状態が「状態取得中」となっている場合、[最新の情報に更新]をクリックし、正常に変わることを確認してください。

《参考》
自動登録の場合、ESMPRO/ServerManager 上でのコンポーネントの名前「コンポーネント名」は、
システム管理が検索できない場合は「ManagementController + 番号」になります。
コンポーネント登録後に名前を変更する場合は、ESMPRO/ServerManager 上でコンポーネントの
[設定]-[接続設定]画面から実施できます。

《参考》
ノード間の iLO の IP アドレスがまばらな場合(*)や自動登録ができない環境などの場合、以下の手順で手動登録を
実施してください。
* 自動登録の場合、検索範囲が広くなると登録に時間がかかります

1. 画面左上の[登録]をクリックします。

2. 「手動登録」タブを開き、「サーバ/ストレージ」を選択します。

3. コンポーネント名を入力し、「"BMC（EXPRESSSCOPE エンジン）" / "iLO" / "BMC（その他）" / "vPro" (Common)」の[管理対象」で iLO を選択して、登録する iLO の[ユーザ名]と[パスワード]を入力します。
続けて[IP アドレス 1]に iLO の IP アドレスを入力します。
「SNMP(ESMPRO/ServerAgent)/WS-Man/ESXi/iStorage」、「RAID システム管理機能」の[管理]と、
「ExpressUpdate 機能」の[ExpressUpdate Agent 経由のアップデート]は未登録を選択します。
入力が完了したら、[追加]をクリックします。

4. 「接続チェック」画面が表示されますので、[接続チェック]をクリックします。

5. 接続チェックが正常に終了し、「検出」「iLO が使用できます。」の結果が表示されることを確認したら、[装置一覧に戻る]をクリックします。引き続き登録する場合は[続けて登録]をクリックし、iLO コンポーネントを登録してください。

6. 追加したコンポーネントの[情報]列のアイコンが緑チェックになっていることを確認します。

状態が「状態取得中」となっている場合、[最新の情報に更新]をクリックし、正常に変わることを確認してください。

以上で iLO コンポーネントの手動登録は完了です。

(8)-3 「アラート受信のみ管理」コンポーネントの追加

「アラート受信のみ管理」コンポーネントに監視対象とする vCenter Server を追加します。

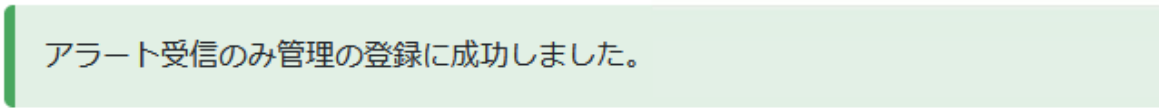
1. 画面上部の[登録]をクリックします。

2. 「アラート受信のみ管理」をクリックします。

3. 設定画面が表示されますので、コンポーネント名と vCenter Server の IP アドレスを入力し、[追加]をクリックします。(本書では vSAN_HDD)

※ コンポーネント名は他のコンポーネントの名前と重ならない名前を設定してください。
空白文字を含む名前は入力できません。大文字と小文字は区別されます。

追加が完了すると、画面下部に「アラート受信のみ管理の登録に成功しました。」と表示されます。



4. 画面上部の[装置]をクリックし、追加したコンポーネントが表示されていることを確認します。

(9)開局作業

開局作業は、管理ノード、クラスタノードの iLO、およびクラスタノードの HDD 障害通報のために「アラート受信のみ管理」コンポーネントとして登録した vCenter Server のそれぞれに対し、対応する開局キーを利用して行います。

開局作業については、「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「2章 インストール」「3. 開局ツール」を参照して行います。

「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ページからダウンロードします。

https://www.support.nec.co.jp/View.aspx?id=9010102124

開局作業についてご不明点がある場合は、1.2節のエクスプレス受付センターにお問い合わせ下さい。

3.24 サーバ診断カルテの開局手続き

本節は、サーバ診断カルテを利用する場合のみ実施します。
サーバ診断カルテを利用するには、あらかじめ 3.23 節のエクスプレス通報サービスのセットアップを全て実施している必要があります。

サーバ診断カルテの運用を始めるには以下の作業が必要となります。

作業項目	お客様作業	NEC 営業作業
(1) ESMPRO/SM の設定	△*1	―
(2)関連プログラムのインストール	△*1	―
(3)サーバ診断カルテの設定	△*1	―
(4)開局作業	○	―

△*1:構築サービスでサーバ診断カルテ設定(オプション項目) 実施している場合は、お客様での作業は不要

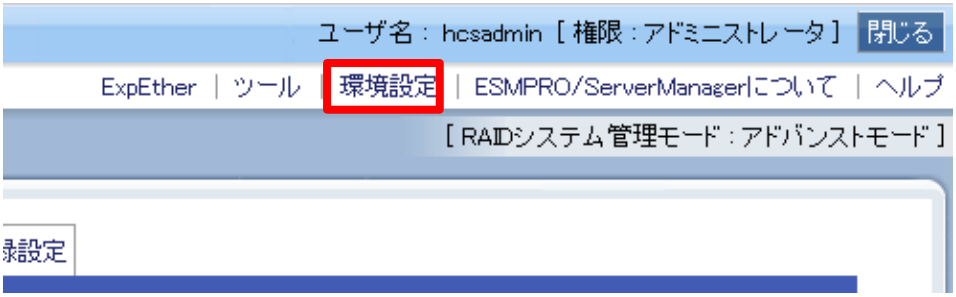
(1)ESMPRO/SM の設定

ESMPRO/ServerManager にコンポーネントの登録を行います。

(1)-1 環境設定

1. 画面右上の[クラシックモード]をクリックし、クラシックモードの画面を開きます。

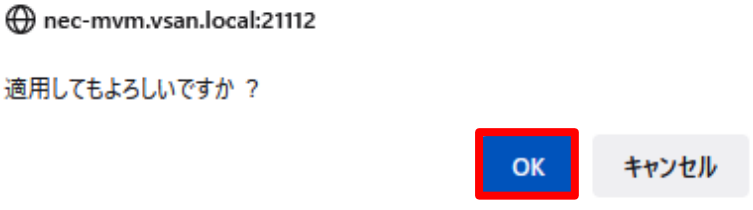
2. 画面右上の[環境設定]をクリックします。



3. [ネットワーク]タブをクリックし、画面下部の[編集]をクリックします。

4. 「WS-Man 通信/ESXi」配下の「自己署名証明」の[許容する]にチェックを入れ、[適用]をクリックします。

5. 以下のダイアログが表示されますので、[OK]をクリックします。



6. 「WS-Man 通信/ESXi」配下の「自己署名証明」が「許容する」になっていることを確認し、画面右上の[閉じる]をクリックします。

(1)-2 ESXi コンポーネントの登録

ESMPRO/ServerManager に管理ノード、クラスタノードの ESXi コンポーネントを登録します。

本項では自動登録の手順を記載しています。
手動登録の場合、3.23 節の(8)-2 で登録した iLO コンポーネントと同じコンポーネントと認識せず、
独立したコンポーネントとして登録されるため、自動登録を実施してください。

《参考》
ESMPRO/ServerManager で ESXi の管理登録(接続チェック)を行う場合、SLP サービスを有効化する必要があります。VMware ESXi 7.0 Update 2c 以降では、潜在的なセキュリティの脆弱性を防ぐために SLP サービスがデフォルトで無効化されおり、ESXi コンポーネントの登録を実施する前に有効化する必要があります。

以下の手順で SLP サービスの起動状態を確認します。

登録対象のノード ESXi Shell を起動し、root ユーザでログインした後、下記のコマンドを実行し、SLP サービスが有効になっているかを確認します。

```
# chkconfig -l | grep slpd
```

無効の場合は以下の出力となります。

```
[root@nec-esx-mg:~] chkconfig -l | grep slpd
slpd                    off
```

下記のコマンドを実行し、SLP サービスが起動しているかを確認します。

```
# /etc/init.d/slpd status
```

停止状態の場合は以下の出力となります。

```
[root@nec-esx-ng:~] /etc/init.d/slpd status
slpd is not running
```

SLP サービスが無効化していた場合は、引き続き以降の手順を実施し、SLP サービスの有効化および
ファイアウォールでの SLP サービスのルールセット有効化手順を実施してください。

- SLP サービスのルールセット有効化手順

1. ファイアウォールで SLP サービスのルールセットを有効にします。

   ```
   # esxcli network firewall ruleset set -r CIMSLP -e 1
   ```

   ```
   [root@nec-esx-ng:~] esxcli network firewall ruleset set -r CIMSLP -e 1
   ```

2. SLP サービス自動起動が無効(off)になっていた場合は有効にします。

   ```
   # chkconfig slpd on
   ```

   ```
   [root@nec-esx-ng:~] chkconfig slpd on
   ```

3. SLP サービスが停止していた場合は起動します。

   ```
   # /etc/init.d/slpd start
   ```

   ```
   [root@nec-esx-ng:~] /etc/init.d/slpd start
   Starting slpd
   ```

4. CIM エージェントを無効にしてから有効にします。以下のコマンドを実行します。

   ```
   # localcli system wbem set -e 0
   ```

   ```
   [root@nec-esx-ng:~] localcli system wbem set -e 0
   ```

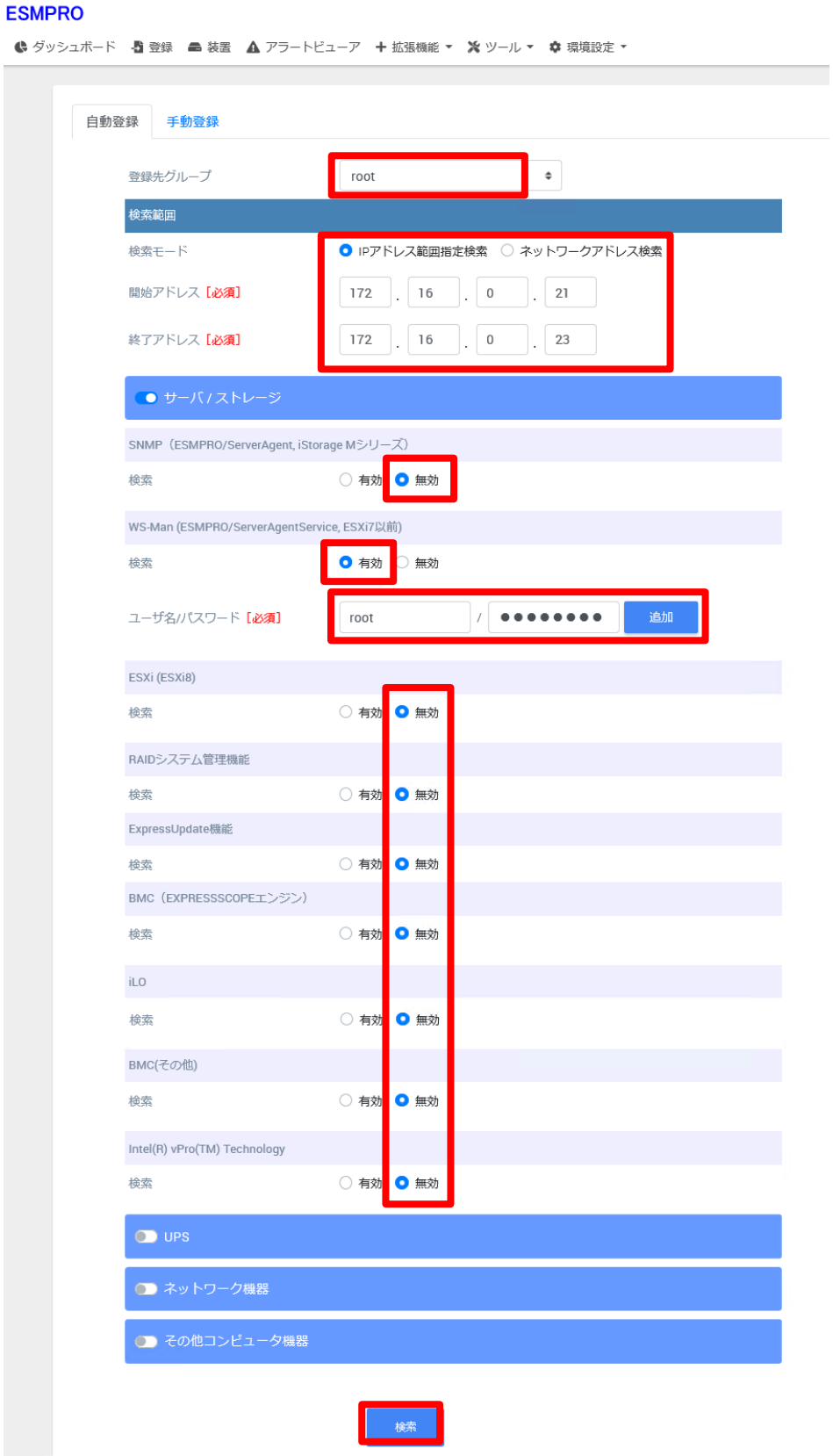
5. CIM エージェントを再度有効にするには、次のコマンドを実行します。

   ```
   # localcli system wbem set -e 1
   ```

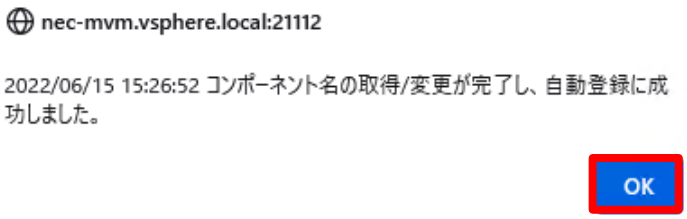
   ```
   [root@nec-esx-ng:~] localcli system wbem set -e 1
   ```

以上で有効化手順は完了です。

1. 3.23 節の(8)-2 の手順 1 から手順 2 を実施して自動登録の設定画面を開きます。
2. 自動登録画面の「検索範囲」で「検索モード」が「IP アドレス範囲指定検索」になっていることを確認し、
   検索する ESXi サーバの IP アドレスの開始アドレスと終了アドレスを指定します。
   続けて、「WS-Man(ESMPRO/ServerAgentService,ESXi7 以前)」の「検索」を有効にし、ESXi のユーザ(root)とパスワードを入力します。
   「WS-Man(ESMPRO/ServerAgentService,ESXi7 以前)」以外の「検索」は[無効]にし、最後に[検索]をクリックします。


ESMPRO
ダッシュボード
登録
装置
アラートビューア
拡張機能
ツール
環境設定
自動登録
手動登録
登録先グループ
root
検索範囲
検索モード
IPアドレス範囲指定検索
ネットワークアドレス検索
開始アドレス［必須］
172 . 16 . 0 . 21
終了アドレス［必須］
172 . 16 . 0 . 23
サーバ / ストレージ
SNMP（ESMPRO/ServerAgent, iStorage Mシリーズ）
検索
有効
無効
WS-Man (ESMPRO/ServerAgentService, ESXi7以前)
検索
有効
無効
ユーザ名/パスワード［必須］
root
/
●●●●●●●●
追加
ESXi (ESXi8)
検索
有効
無効
RAIDシステム管理機能
検索
有効
無効
ExpressUpdate機能
検索
有効
無効
BMC（EXPRESSSCOPEエンジン）
検索
有効
無効
iLO
検索
有効
無効
BMC(その他)
検索
有効
無効
Intel(R) vPro(TM) Technology
検索
有効
無効
UPS
ネットワーク機器
その他コンピュータ機器
検索

3. 検索が開始され、しばらくすると以下のダイアログが表示されますので、[OK]をクリックします。



4. 指定した iLO コンポーネントが登録されていることを確認します。

5. 登録対象の ESXi サーバを全て自動登録します。
自動登録の場合、ESXi コンポーネントと 3.23 節の(8)-2 で登録した iLO コンポーネントが統合され、iLO コンポーネントのコンポーネント名は一覧に表示されなくなります。

《参考》
自動登録の場合、ESMPRO/ServerManager 上でのコンポーネントの名前「コンポーネント名」は、登録した ESXi のホスト名になります。
コンポーネント登録後に名前を変更する場合は、ESMPRO/ServerManager 上でコンポーネントの[設定]-[接続設定]画面から実施できます。

《参考》
(1)-2 の冒頭にある《参考》で SLP サービスのルールセットを有効化した場合は、ESXi コンポーネントの登録完了後に、以下の無効化手順を実施してください。

- SLP サービスのルールセット無効化手順

1. 起動した SLP サービスのルールセットを停止します。

```
# /etc/init.d/slpd stop
```

```
[root@nec-esx-mg:~] /etc/init.d/slpd stop
Stopping slpd
```

2. ファイアウォールで SLP サービスのルールセットを無効にします。

```
# esxcli network firewall ruleset set -r CIMSLP -e 0
```

```
[root@nec-esx-mg:~] esxcli network firewall ruleset set -r CIMSLP -e 0
```

3. SLP サービス自動起動を無効にします。

```
# chkconfig slpd off
```

```
[root@nec-esx-mg:~] chkconfig slpd off
```

以上で無効化手順は完了です。

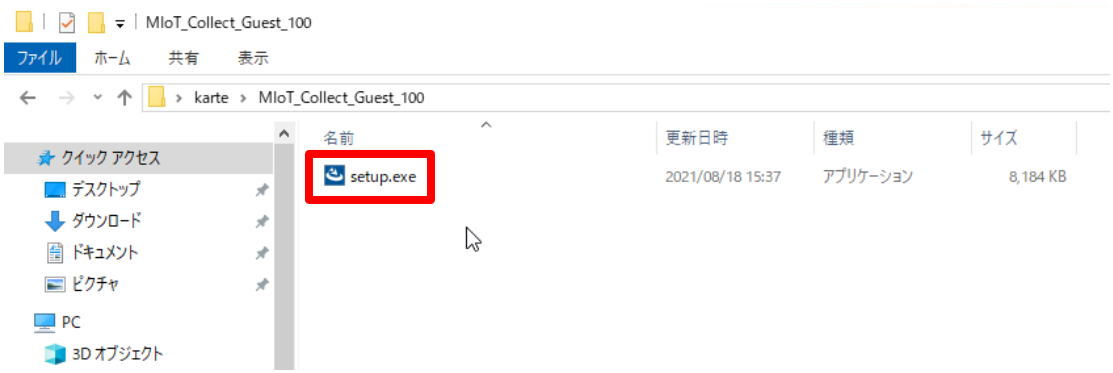
(2)関連プログラムのインストール

サーバ診断カルテ(ゲスト OS 対応版)およびサーバ診断カルテ(VMware ESXi 対応版)のインストールを実施します。

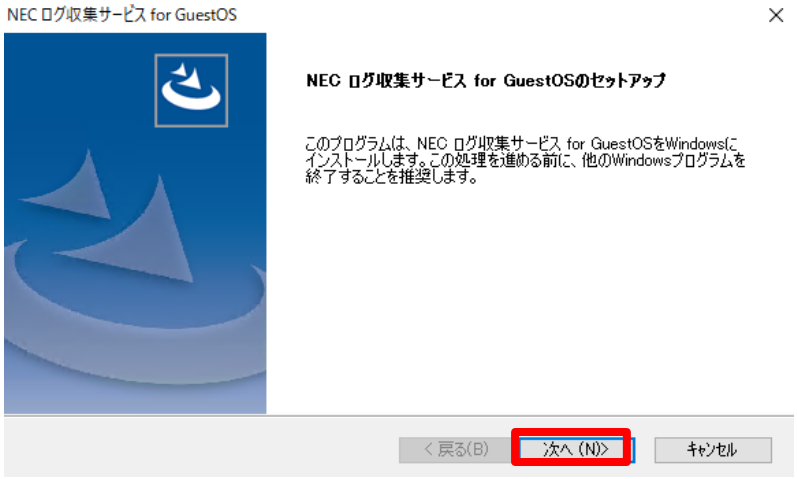
インターネットにアクセス可能な Windows 端末で以下 Web ページを表示し、
サーバ診断カルテ（ゲスト OS 対応版）およびサーバ診断カルテ（VMware ESXi 対応版）の
セットアッププログラムをダウンロードします。
https://www.support.nec.co.jp/View.aspx?id=9010107805
ダウンロード後、zip ファイルを管理 VM 上にコピーし、解凍してください。

(2)-1 サーバ診断カルテ(ゲスト OS 対応版)のインストール

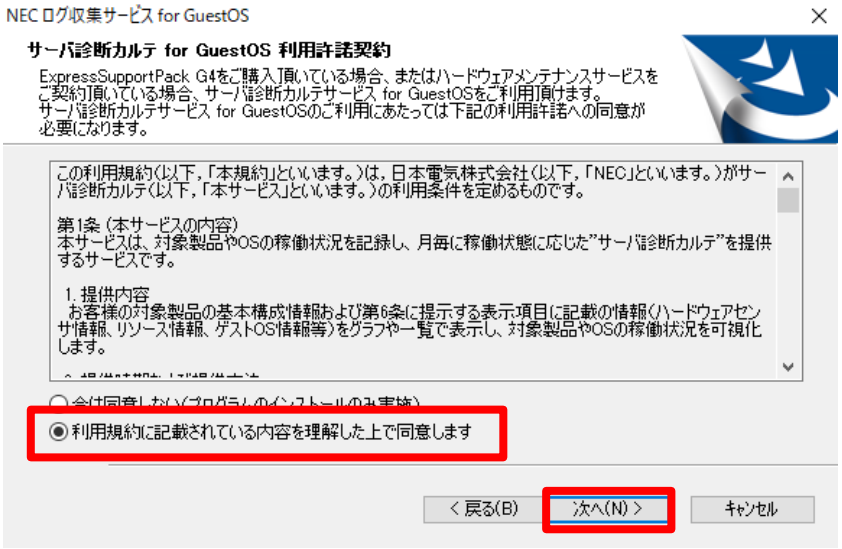
1. (2)でダウンロードしたモジュールを開き、
[¥MIoT_Collect_Guest_***¥setup.exe]ファイルをダブルクリックします。



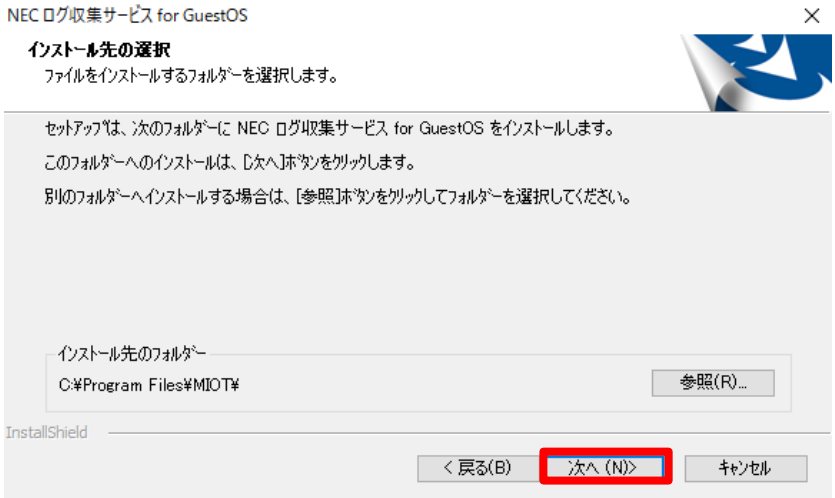
2. セットアップ画面が表示されますので、[次へ]をクリックします。



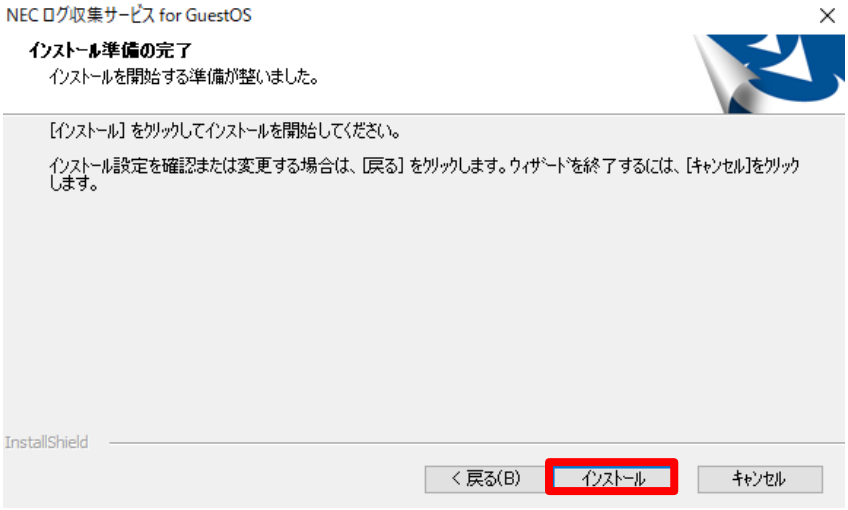
3. 「利用規約に記載されている内容を理解した上で同意します」にチェックを入れ、[次へ]をクリックします。



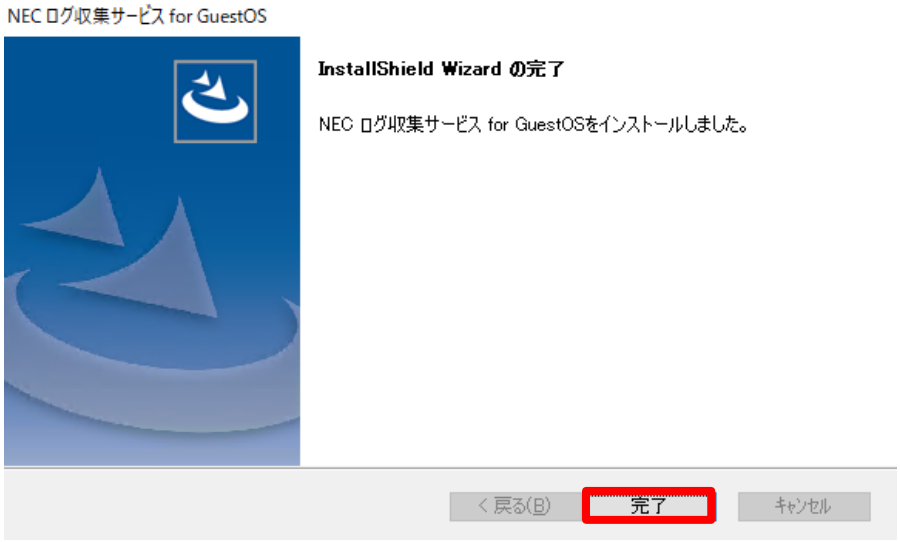
4. インストール先を指定して[次へ]をクリックします。



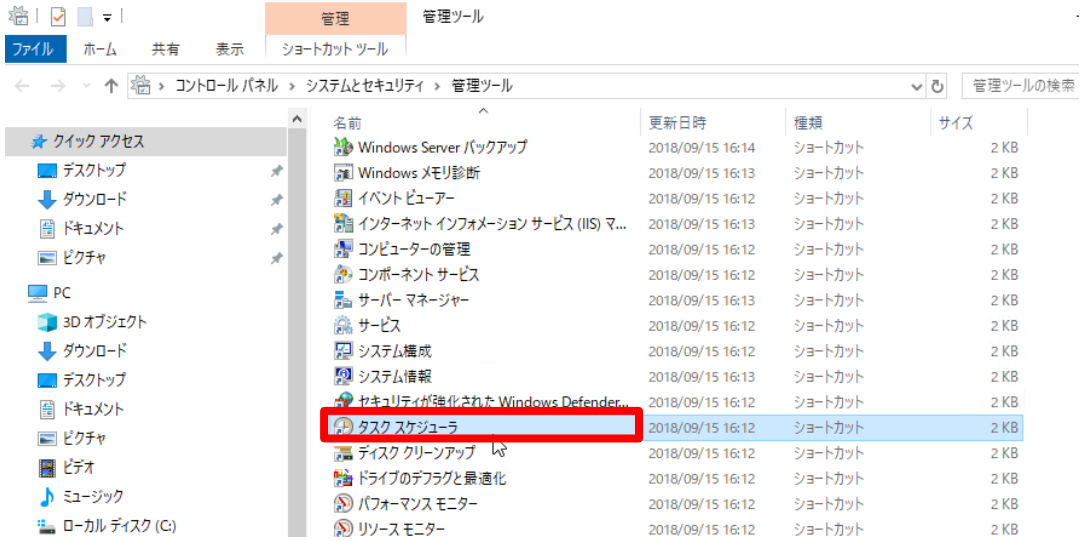
5. [インストール]をクリックしてインストールを開始します。



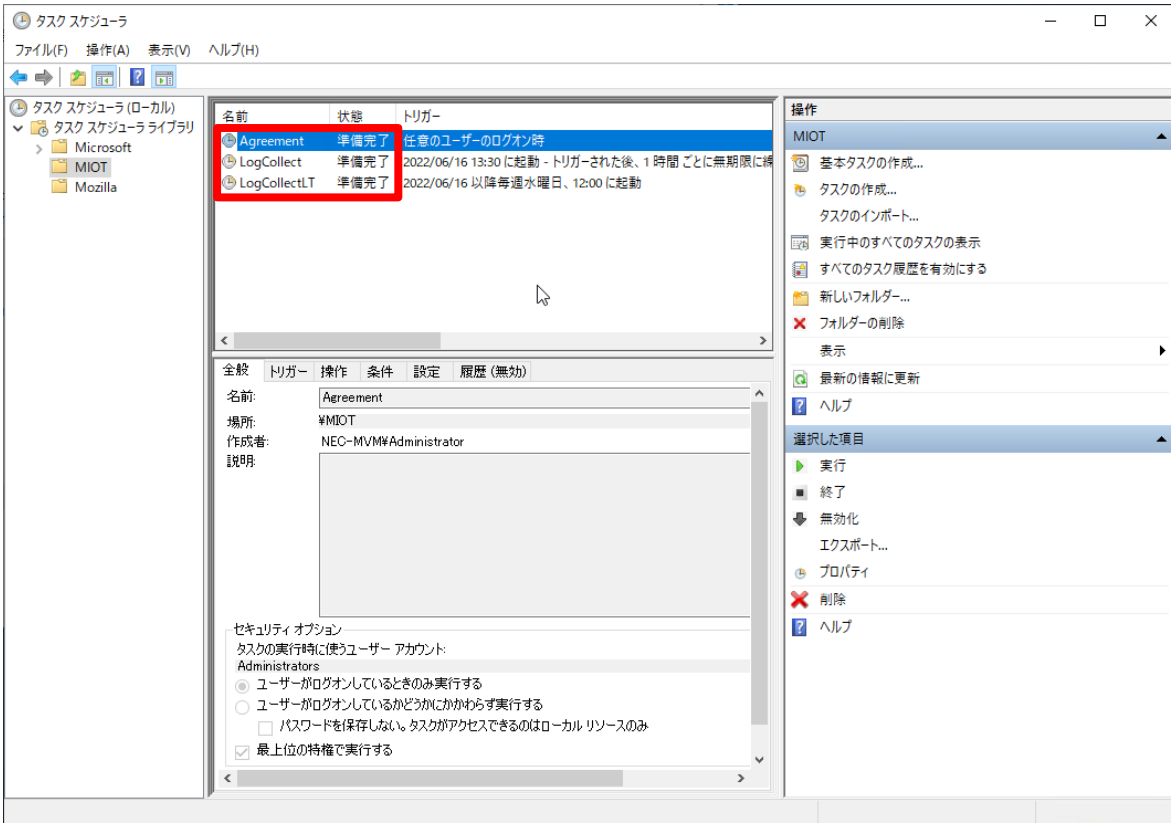
6. インストールが完了したら[完了]をクリックします。



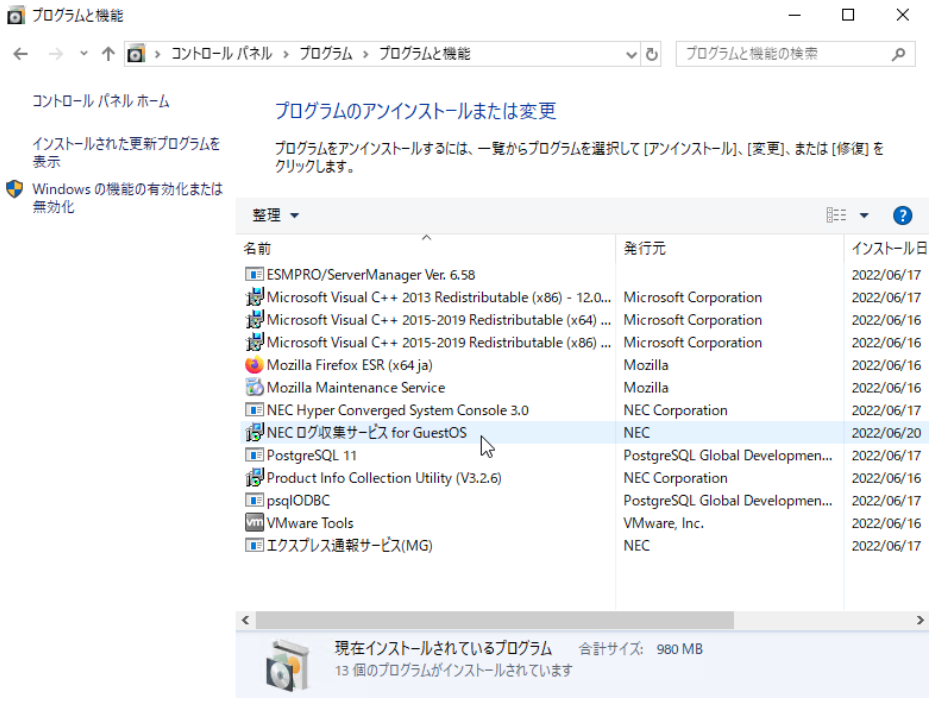
7. スタートメニューから Windows 管理ツールを開き、タスクスケジューラをクリックします。



8. タスクスケジューラが開きますので、「タスク スケジューラ ライブラリ」→「MIOT」の順でクリックし、「LogCollect」「LogCollectLT」「Agreement」タスクが表示され、状態が「準備完了」となっていることを確認します。

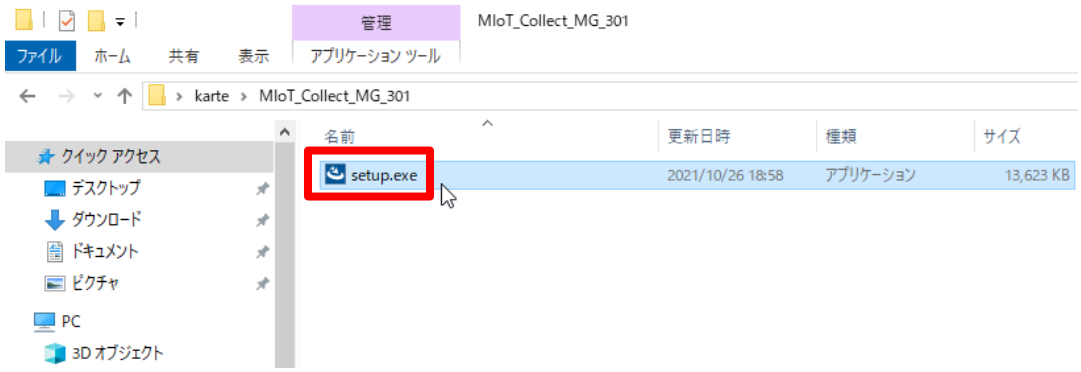


9. 「コントロールパネル」→「プログラム」→「プログラムと機能」を開き、「NEC ログ収集サービス for GuestOS」が表示されていることを確認します。

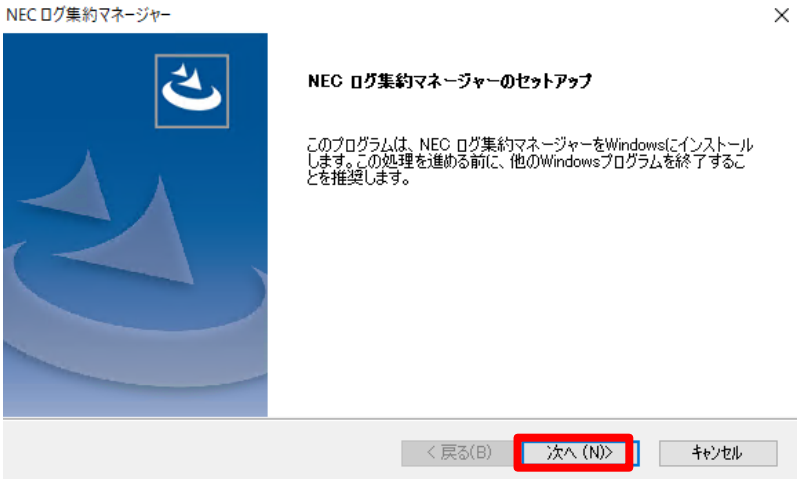


(2)-2 サーバ診断カルテ(VMware ESXi 対応版)のインストール

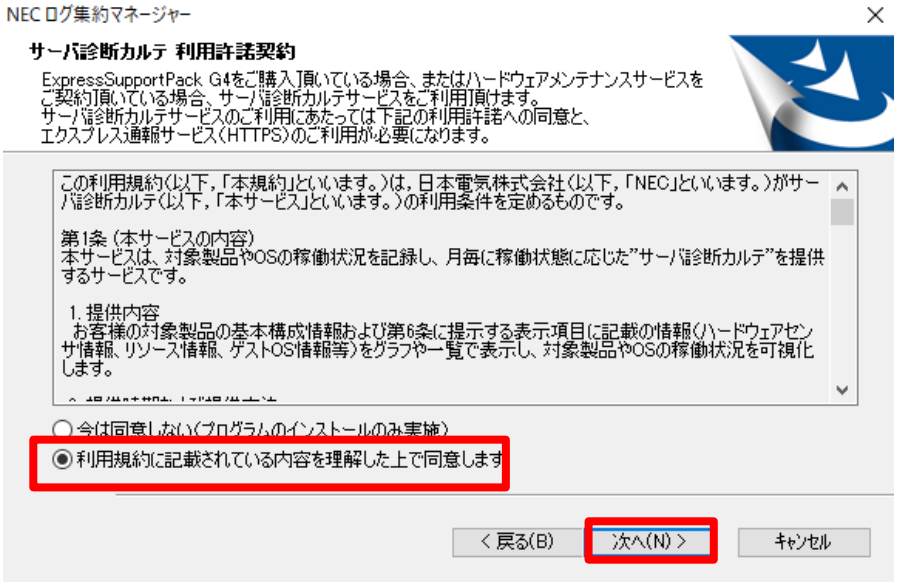
1. (2)でダウンロードしたモジュールを開き、
[¥MIoT_Collect_MG_***¥setup.exe]ファイルをダブルクリックします。



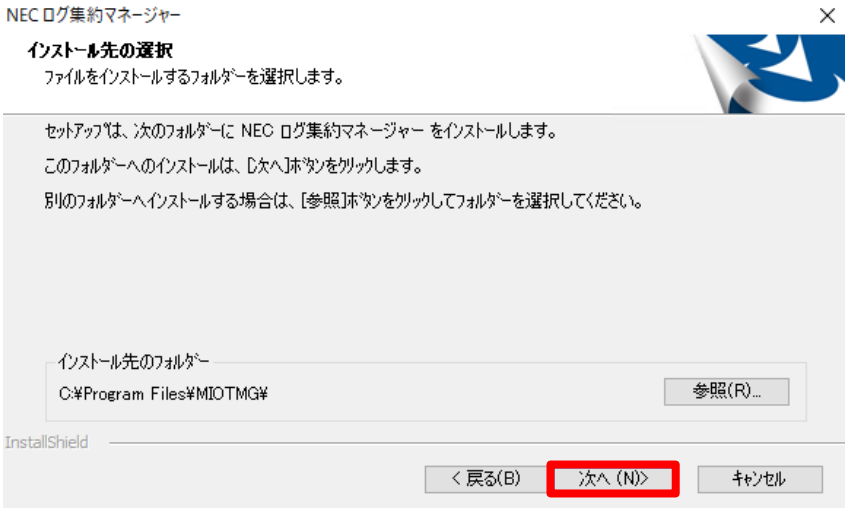
2. セットアップ画面が表示されますので、[次へ]をクリックします。



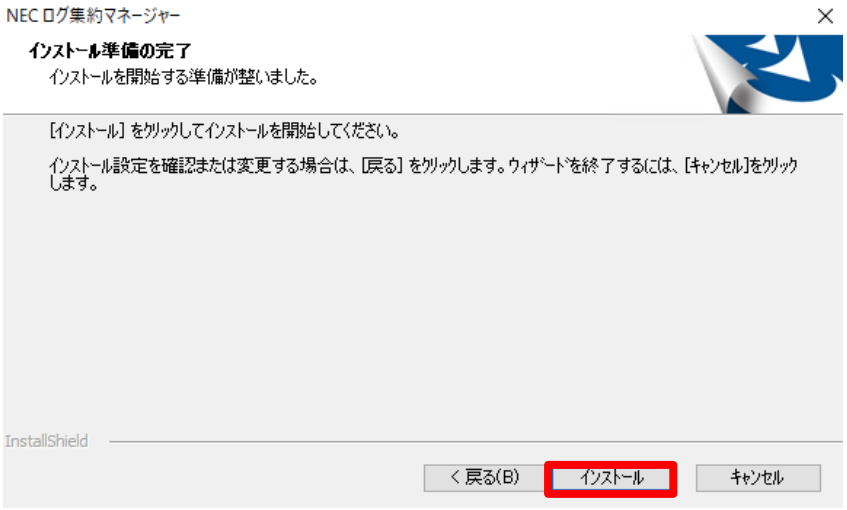
3. 「利用規約に記載されている内容を理解した上で同意します」にチェックを入れ、[次へ]をクリックします。



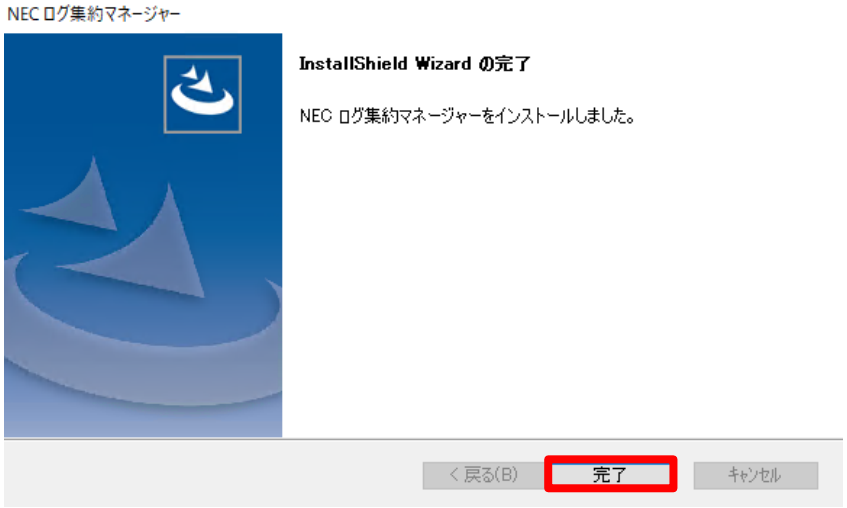
4. インストール先を指定して[次へ]をクリックします。



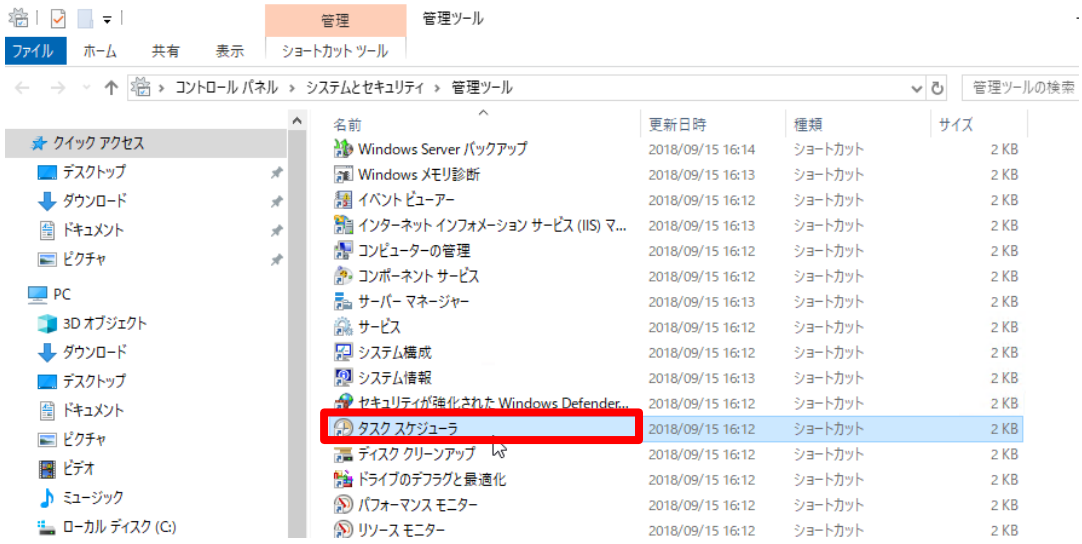
5. [インストール]をクリックしてインストールを開始します。



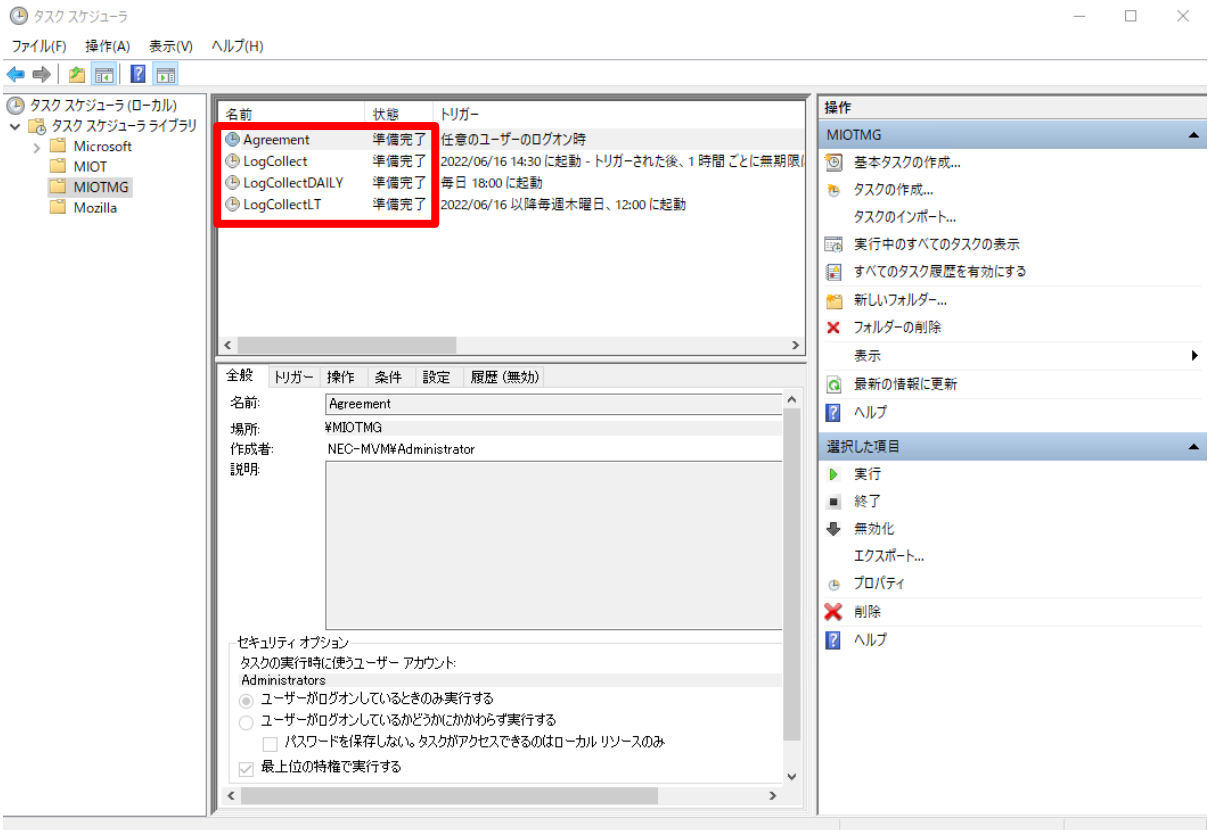
6. インストールが完了したら[完了]をクリックします。



7. スタートメニューから Windows 管理ツールを開き、タスクスケジューラをクリックします。



8. タスクスケジューラが開きますので、「タスク スケジューラ ライブラリ」→「MIOTMG」の順でクリックし、「LogCollect」「LogCollectLT」「LogCollectDAILY」「Agreement」タスクが表示され、状態が「準備完了」となっていることを確認します。



9. 「コントロールパネル」→「プログラム」→「プログラムと機能」を開き、「NEC ログ集約通報サービス」が表示されていることを確認します。

(3)サーバ診断カルテの設定

(3)-1 管理対象の IP アドレス登録

ESMPRO/ServerManager に登録した ESXi および iLO のコンポーネントの IP アドレスをサーバ診断カルテの対象に追加します。

1. 管理 VM にてコマンドプロンプトを管理者権限で起動し、「インストールフォルダ¥tool」に移動します。

   ※ インストールフォルダのデフォルトは「C:¥Program Files¥MIOTMG」です。

```
C:¥Users¥Administrator>cd C:¥Program Files¥MIOTMG¥tool
```

2. 以下のコマンドを実行し、ESXi と iLO の IP アドレスを登録します。

```
# miotmgst.exe /add <ESXi または iLO の IP アドレス>
```

```
C:¥Program Files¥MIOTMG¥tool>miotmgst.exe /add 192.168.0.50
Add servers:
192.168.0.50 : succeed.
```

3. 対象の IP アドレス全ての登録が完了したら、以下のコマンドで登録確認を実施します。

```
# miotmgst.exe /l
```

```
C:¥Program Files¥MIOTMG¥tool>miotmgst.exe /l
Target Servers:
192.168.0.11 Unopened
192.168.0.12 Unopened
192.168.0.13 Unopened
192.168.0.50 Unopened
192.168.0.1 Unopened
192.168.0.2 Unopened
192.168.0.3 Unopened
192.168.0.4 Unopened
```

登録したコンポーネントがエクスプレス通報サービス未開局の状態である場合、コマンド結果に「Unopened」と出力されます。

(3)-2 ゲスト OS 収集タスクの認証情報登録

ログ集約マネージャーの管理サーバユーザー登録コマンドを使用し、管理 VM のアドミニストレータ権限のユーザ登録を実施します。

1. 管理 VM にてコマンドプロンプトを管理者権限で起動し、「インストールフォルダ¥setting」に移動します。

   ※ インストールフォルダのデフォルトは「C:¥Program Files¥MIOTMG」です。

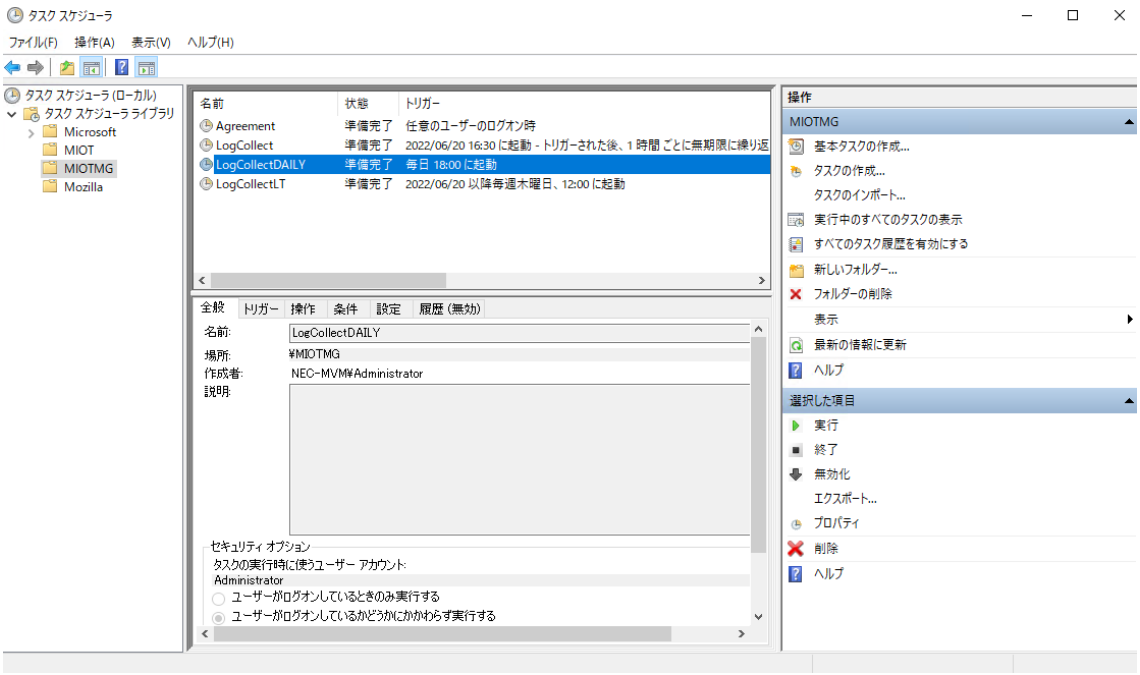
```
C:¥Program Files¥MIOTMG¥tool>cd C:¥Program Files¥MIOTMG¥setting
```

2. 以下のコマンドを実行し、Administrator ユーザの登録を実施します。

```
# MIOT_REG_USER.exe /u Administrator /p <管理 VM のパスワード>
```

```
C:¥Program Files¥MIOTMG¥setting>MIOT_REG_USER.exe /u Administrator /p P@ssw0rd
User and password updates (GuestOS collection) were successful.
```

3. 本節の(2)-2 の手順 7 から 8 を実施してタスクスケジューラを開き、MIOTMG フォルダーの「LogCollectDAILY」のタスクを選択します。
   タスクの実行時に使うユーザーアカウントが、SYSTEM から登録したユーザー名に変更されていることを確認してください。



(3)-3 ESXi/管理 VM への接続認証情報登録

ログ集約マネージャー認証情報管理コマンドを使用し、ESXi サーバおよび管理 VM にログインするための IP アドレス、認証情報の登録を実施します。

1. 管理 VM にてコマンドプロンプトを管理者権限で起動し、「インストールフォルダ¥setting」に移動します。

   ※ インストールフォルダのデフォルトは「C:¥Program Files¥MIOTMG」です。

```
C:¥Program Files¥MIOTMG¥tool>cd C:¥Program Files¥MIOTMG¥setting
```

2. 以下のコマンドを実行し、ESXi サーバと管理 VM の認証情報を登録します。

```
# MIOT_MNG_AUTH.exe /i <ESXi サーバの IP アドレス> /u root /p <ESXi サーバの root パスワード> /y
```

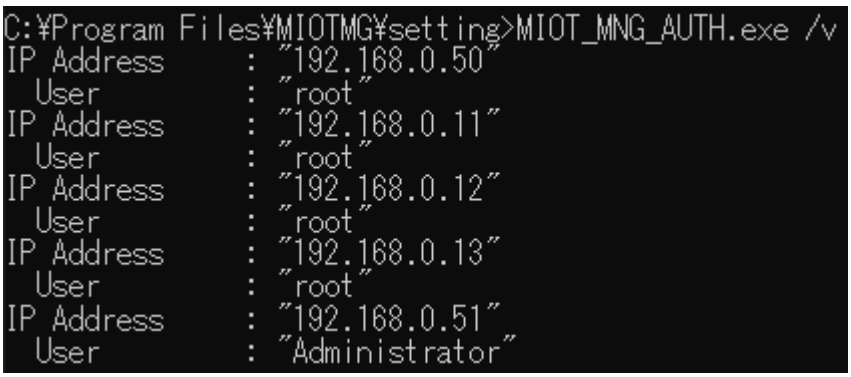
```
C:¥Program Files¥MIOTMG¥setting>MIOT_MNG_AUTH.exe /i 192.168.0.50 /u root /p P@ssw0rd /y
```

```
# MIOT_MNG_AUTH.exe /i <管理 VM の IP アドレス> /u Administrator /p <管理 VM のパスワード> /y
```

```
C:¥Program Files¥MIOTMG¥setting>MIOT_MNG_AUTH.exe /i 192.168.0.51 /u Administrator /p P@ssw0rd /y
```

3. 以下のコマンドを実行し、登録内容の確認を実施します。

```
# MIOT_MNG_AUTH.exe /v
```



(4) 開局作業

3.23 節の(9)を参照し、管理ノード、クラスタノードの ESXi に対して対応する開局キーを利用して開局作業を実施してください。開局キーは 3.23 節の(2)で取得したものと同じキーを使用します。

4 ライセンス登録

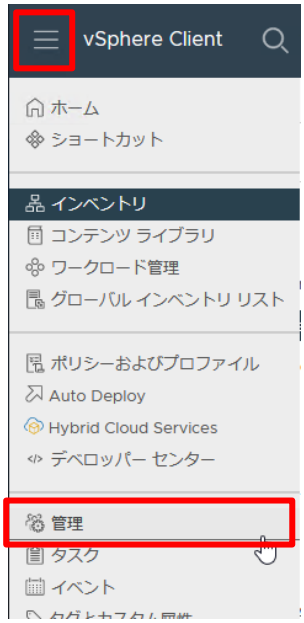
4.1 vCenter Server、ESXi、vSAN ライセンスの登録

vCenter Server、ESXi および vSAN のライセンスキーの登録および割り当てを行います。

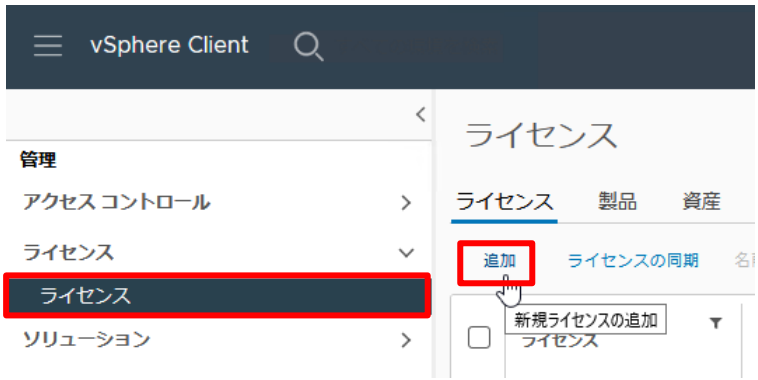
4.1.1 3 ノード以上の構成、2 ノード構成で vSphere Standard を使用する場合

3 ノード以上の構成、または 2 ノード構成でライセンスに vSphere Standard を使用する場合は本項の手順でライセンス登録を実施してください。
vCenter Server へのライセンスの割り当ては主に手順 7 から手順 9 を、また、ESXi へのライセンスの割り当ては主に手順 10 から手順 13 で行います。vSAN ライセンスの割り当ては手順 14 から手順 16 で行います。

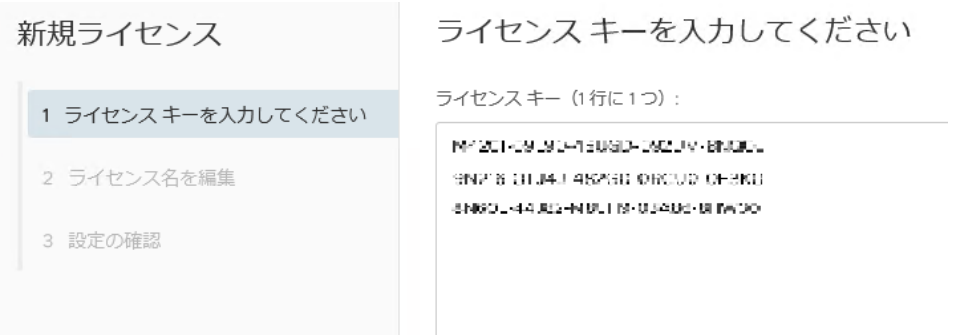
1. VMware vSphere Client で vCenter Server にログインし、画面左上のメニューアイコンをクリックし、表示されるメニュー一覧の中から[管理]をクリックします。



2. 管理メニューの中から[ライセンス]をクリックします。画面が切り替わったら、[追加]をクリックします。



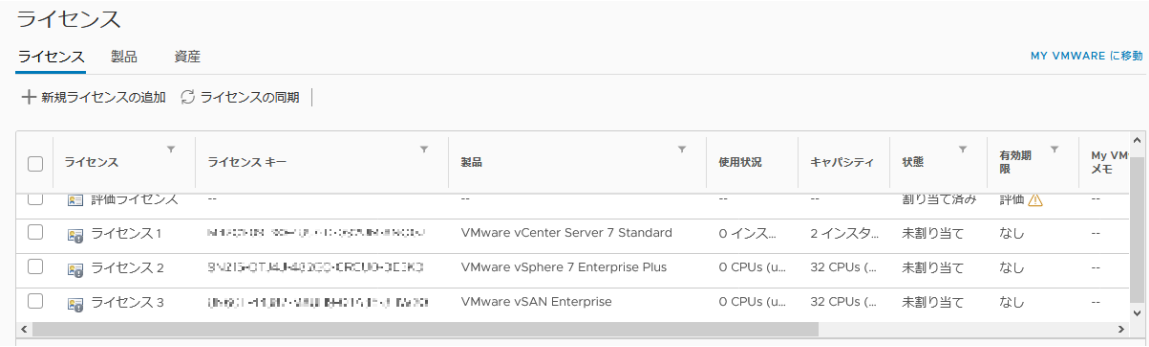
3. 「新規ライセンス」ダイアログが表示されます。「ライセンスキー（1 行に 1 つ）:」のメッセージ下の入力枠に登録するライセンスキーを、1 行に1つ入力した後、[次へ]をクリックします。



4. 次に「ライセンス名を編集」の画面が表示されます。入力した各ライセンスキーのライセンス名を必要に応じて編集した後、[次へ]をクリックします。

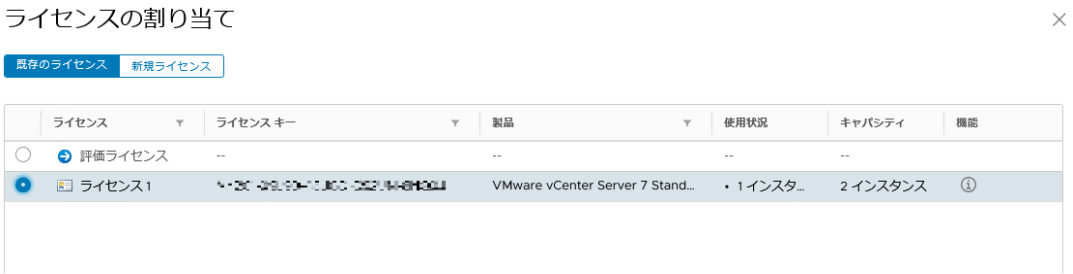
5. 続いて「設定の確認」画面が表示されます。手順 3 で入力したライセンスが正常に追加されたことを確認し、[完了]をクリックします。

6. VMware vSphere Client にフォーカスが戻ります。[ライセンス]タブ画面内のリストに、登録したライセンスキーが表示されていることを確認します。

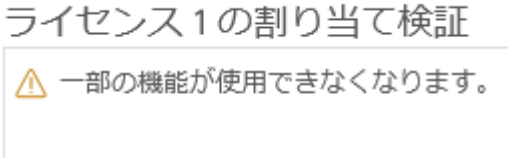


7. [資産]のタブをクリックし、さらにその下の[vCenter Server システム]をクリックします。
続いて、資産の一覧内に表示されている vCenter Server の登録名にチェックを付け、
[ライセンスの割り当て]をクリックします。

8. 「ライセンスの割り当て」のダイアログが表示されます。画面内のリストにて管理サーバに割り当てる
ライセンスキーの行頭にチェックを付け、[OK]をクリックします。



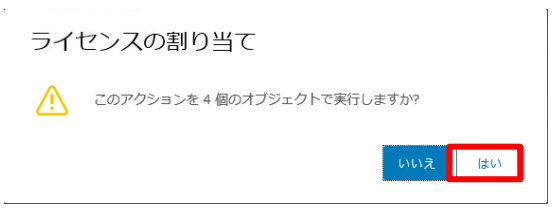
※ 評価ライセンス(Evaluation License)を適用している管理サーバに正規ライセンスを割り当てる
場合、割り当て検証欄に「一部の機能が使用できなくなります。」と表示される場合があります。
使用不可となる機能の詳細については、割り当て検証欄右端の[詳細]をクリックして
確認ください。



9. 再び VMware vSphere Client 画面にフォーカスが戻ります。[資産]タブ画面内の一覧において、vCenter Server の行を選択し、画面下部のサマリ内の「製品」欄の値が、手順 8 で割り当てたライセンスになっていることを確認します。

10. 続いて、ESXi にライセンスを割り当てます。[資産]タブの下の[ホスト]をクリックし、資産のリストにてライセンスを割り当てる ESXi サーバ名を全て選択した状態でリスト左上の[ライセンスの割り当て]をクリックします。

11. ライセンスの割り当てポップアップが出ますので、オブジェクトの数を確認して[はい]をクリックします。



12. 「ライセンスの割り当て」ダイアログが表示されます。手順 8 と同様に、割り当てるライセンスキーの行頭にチェックを付けた状態で[OK]をクリックします。

13. VMware vSphere Client 画面にフォーカスが戻ります。[ホスト]タブ画面内のリストで、ライセンス登録を行った ESXi サーバの行を選択し、画面下部のサマリ内の「製品」欄の値が、手順 12 で割り当てたライセンス名になっていることを確認します。

14. 続いて、vSAN にライセンスを割り当てます。[資産]タブの下の[vSAN クラスタ]をクリックし、資産のリストにてライセンスを割り当てる vSAN クラスタ名を選択した状態でリスト左上の[ライセンスの割り当て]をクリックします。

15. 「ライセンスの割り当て」ダイアログが表示されます。手順 8 と同様に、割り当てるライセンスキーの行頭にチェックを付けた状態で[OK]をクリックします。

16. VMware vSphere Client 画面にフォーカスが戻ります。[クラスタ]タブ画面内のリストで、ライセンス登録を行った vSAN クラスタの行を選択し、画面下部のサマリ内の「製品」欄の値が、手順 15 で割り当てたライセンス名になっていることを確認します。

以上で vCenter Server、ESXi および vSAN へのライセンス登録は完了となります。

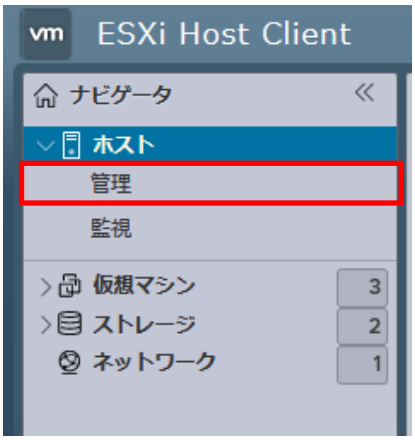
4.1.2 2 ノード構成で vSphere Essentials Plus を使用する場合

2 ノード構成でライセンスに vSphere Essentials Plus を使用する場合は、以下の手順で vCenter Server、ESXi および vSAN のライセンスキーの登録および割り当てを行います。

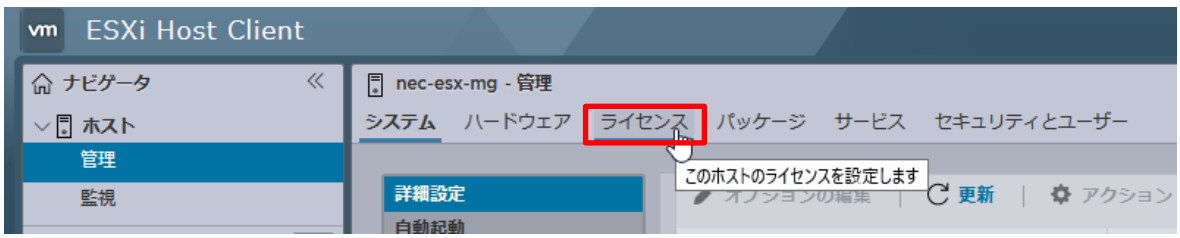
1. My VMware のサイトにログインします。
   vSphere Essentials Plus を使用する場合、クラスタノードの ESXi と管理ノードの ESXi で管理するツールが異なるためライセンスの分割が必要となります。
   ESXi のライセンスを取得する際に、ライセンス分割を実施し、2CPU 分のライセンスと 4CPU 分のライセンスに分割してください。
   ライセンス分割に関しては以下 KB を参照してください。
   <https://kb.vmware.com/s/article/2006972?lang=ja>
2. VMware vSphere Client で vCenter Server にログインし、vCenter Server、vSAN および ESXi(4CPU 分)のライセンスを vCenter Server、vSAN、およびクラスタノードに割り当ててください。
   具体的な手順は 4.1.1 項を参照してください。
3. 以降の手順で管理ノードの ESXi(2CPU 分)のライセンス登録を実施します。
   下記 URL で管理ノードに Host Client で接続します。

   https://<管理ノードの FQDN または IP アドレス>/ui

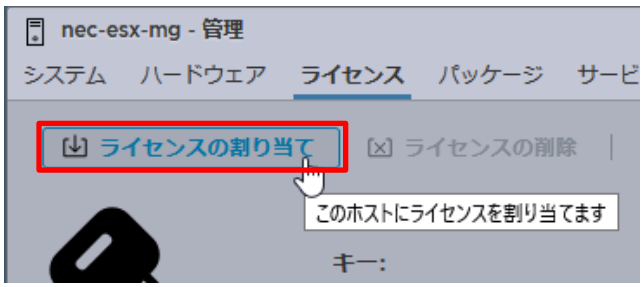
4. ナビゲータから[管理]をクリックします。



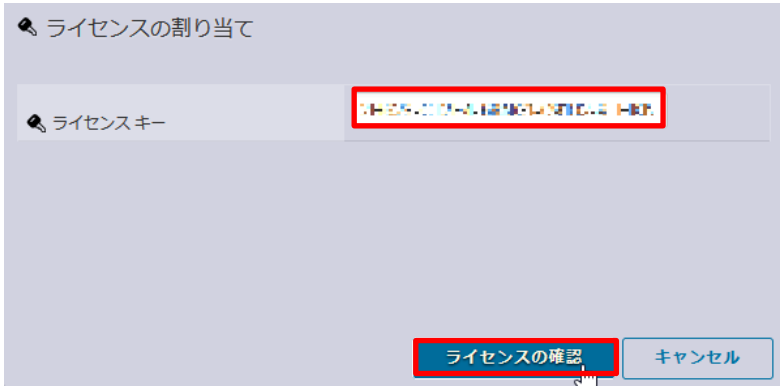
5. 「管理」画面上部の[ライセンス]をクリックします。



6. 「ライセンス」画面左上の[ライセンスの割り当て]をクリックします。

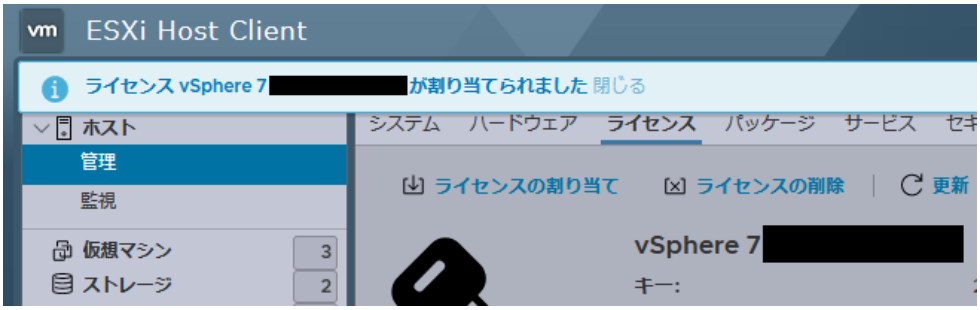


7. 「ライセンス割り当て」ダイアログが表示されますので、ESXi(2CPU 分)のライセンスキーを入力し、[ライセンスの確認]をクリックします。



8. 下記の画面が表示されることを確認し、[ライセンスの割り当て]をクリックします。

9. 「ライセンス」画面に戻りますので、割り当てたライセンスに切り替わっていることを確認します。



以上で、2 ノード構成で vSphere Essentials Plus を使用する場合の vCenter Server、ESXi および vSAN へのライセンス登録は完了となります。

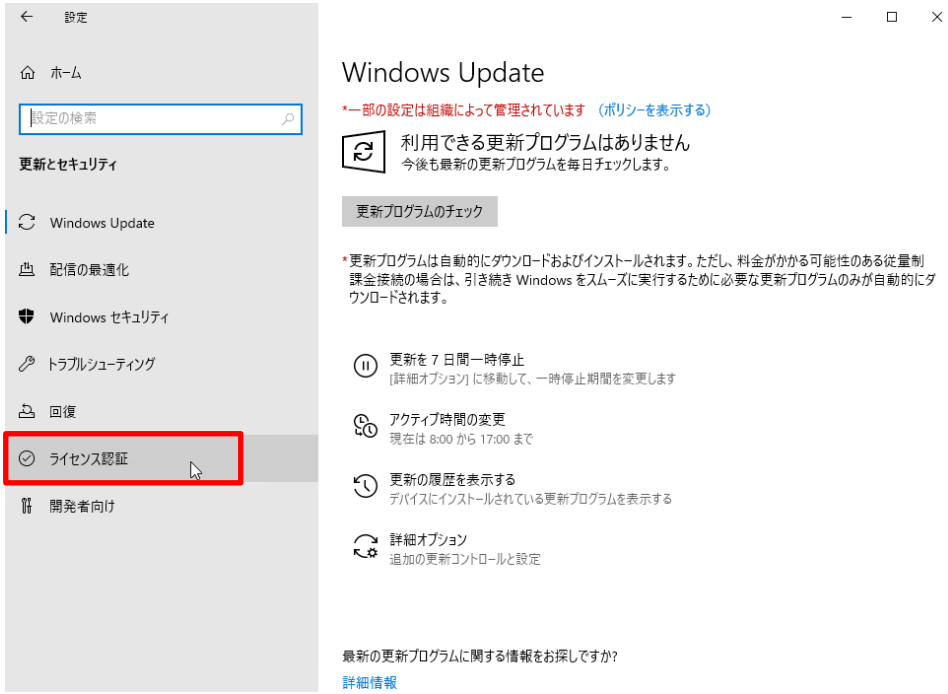
4.2 Windows Server 2022 のライセンス登録

Windows Server のライセンスキーの登録を行います。

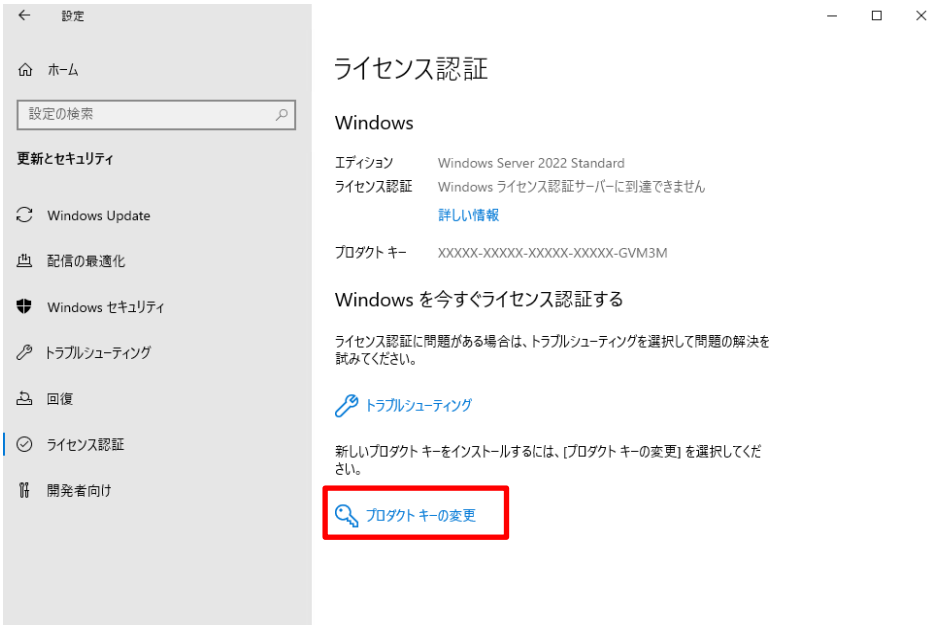
インターネット接続の有無で 2 種類の登録方法がありますので、どちらかを選択してください。

4.2.1 インターネットに接続されている環境でライセンス登録

1. 画面の左下の Windows アイコンをクリックし、  アイコンをクリックします。
2. [更新とセキュリティ]をクリックした後、[ライセンス認証]をクリックします。

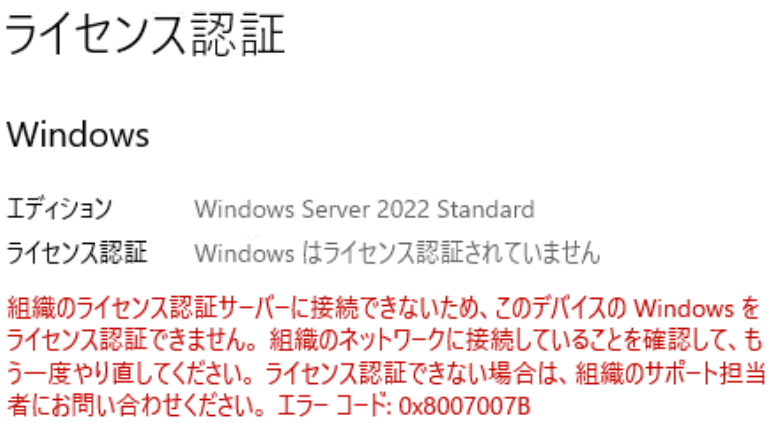


3. 「ライセンス認証」画面が表示されますので、[プロダクトキーの変更]をクリックします。

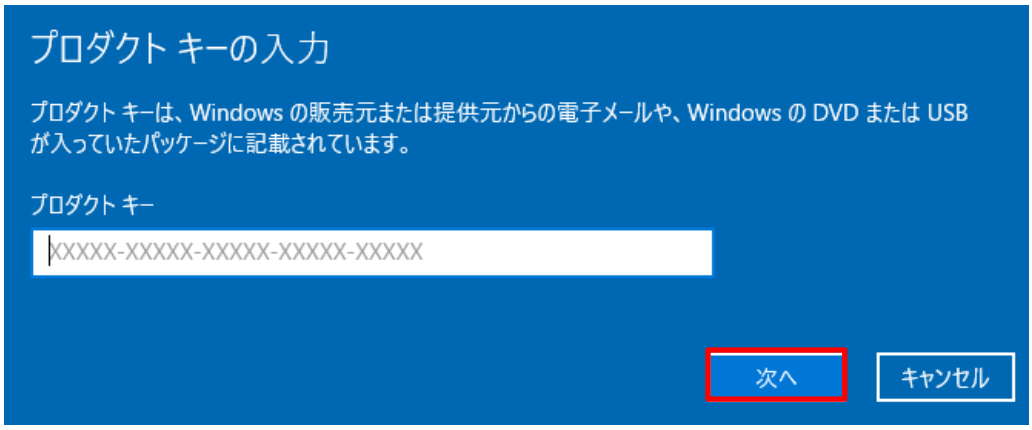


※ 「ライセンス認証」画面では以下のエラーが表示されている場合がありますが、作業に影響はありま

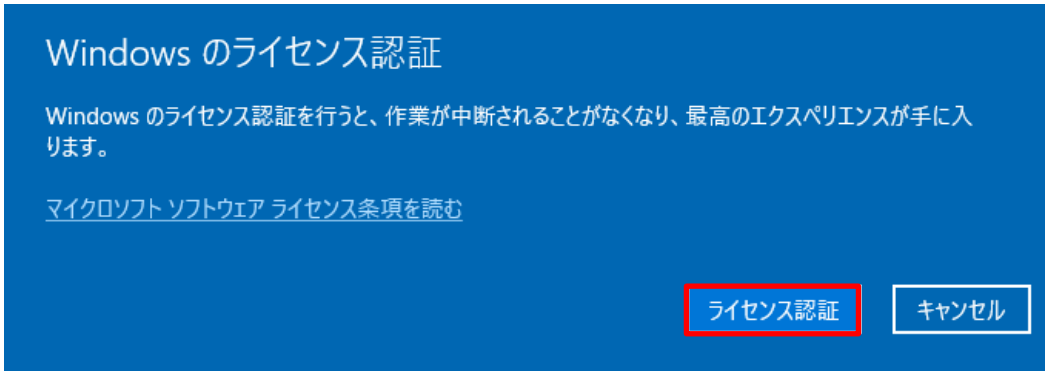
せん。



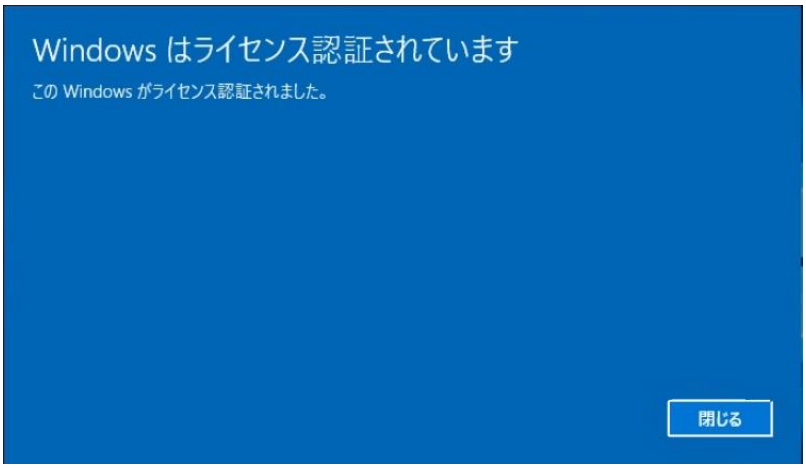
4. 「プロダクトキーの入力]画面でプロダクトキーを入力し、[次へ]をクリックします。



5. 「Windows のライセンス認証」画面で[ライセンス認証]をクリックします。



6. ライセンス認証完了後、[閉じる]をクリックします。



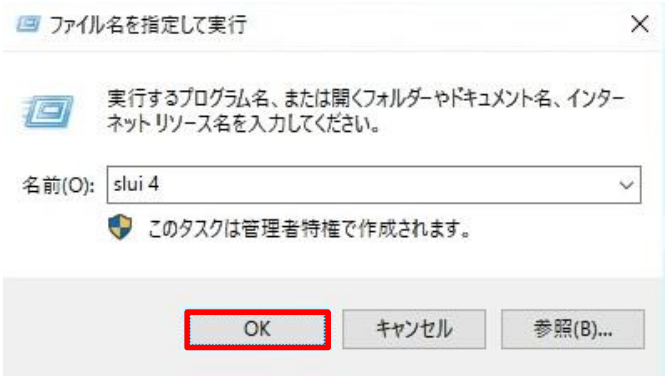
4.2.2 インターネットに接続されていない環境でライセンス登録

1. 画面の左下の Windows アイコンを右クリックし、[コマンドプロンプト (管理者)]を起動します。
2. 管理者権限のコマンドプロンプトで次のコマンドを入力し、<Enter>キーを押します。

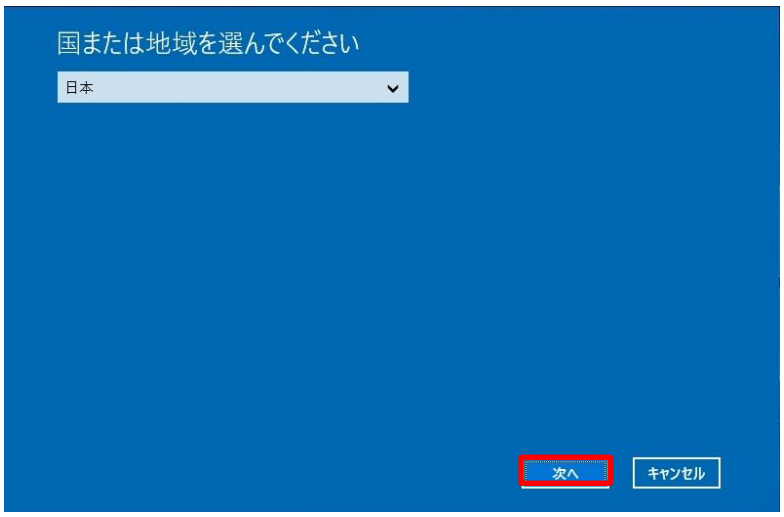
   >slmgr -ipk <COA ラベルのプロダクトキー>

   コマンド入力後、以下の画面が表示されますので、[OK]をクリックします。

3. 画面の左下の Windows アイコンを右クリックし、[ファイル名を指定して実行]をクリックします。
4. 画面の[名前]に「slui 4」と入力し、[OK]をクリックします。



5. 下記の画面が表示されたら適切な国名を選択し、[次へ]をクリックします。



6. 表示された電話番号に電話をかけて、指示に従いライセンス認証を実施してください。

以上で Windows Server へのライセンス登録は完了となります。

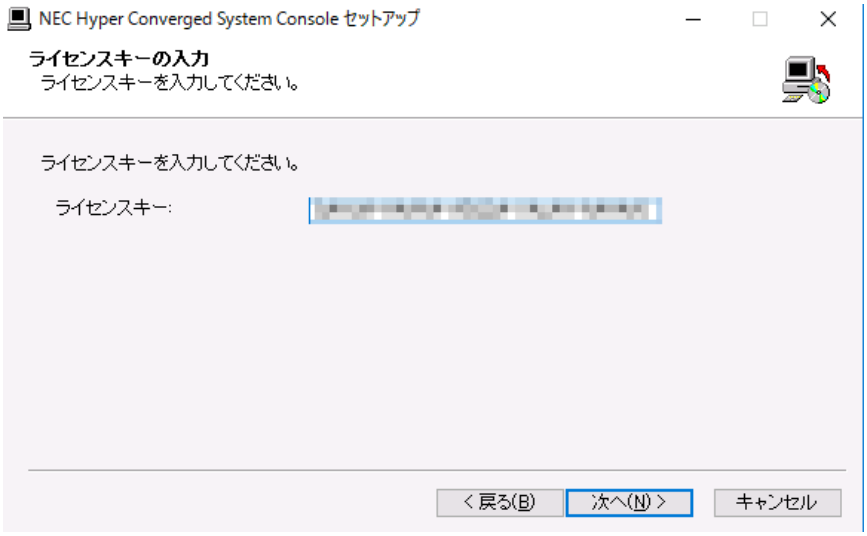
4.3 NEC Hyper Converged System Console のライセンス登録

NEC Hyper Converged System Console のライセンスキーの登録を行います。

※ NEC Hyper Converged System 構築サービスを購入されている場合は既にライセンス登録済みのため、実施不要です。

1. [NEC Hyper Converged System Console インストレーションガイド]を参照し、
   インストールを実施してください。

2. インストール中に「ライセンスキーの入力」画面が表示されますので
   ライセンスキーを入力し、「次へ(N)>」をクリックします。



以上で NEC Hyper Converged System Console へのライセンス登録は完了となります。

5 パスワード変更

《重要》

NEC Hyper Converged System の運用を開始する前に、本手順に従い、必ずお客様のセキュリティポリシーに則ったパスワードへ変更してください。

5.1 概要

本節で NEC Hyper Converged System 初期パスワード通知書に記載されているパスワードを変更する手順を示します。

NEC Hyper Converged System の以下のパスワードを変更します。

① クラスタノード、管理ノードの BMC の ID、パスワード
② クラスタノード、管理ノードの VMware ESXi の ID、パスワード
③ 管理ノードの VMware vCenter Server Appliance(vCSA)の root パスワード
④ 管理ノードの vCSA のシングルサインオン(SSO)のパスワード
⑤ 管理 VM(Windows Server 2022)の Administrator パスワード
⑥ 管理 VM の ESMPRO/ServerManager の監視対象の ID、パスワード
⑦ 管理 VM の NEC Hyper Converged System Console の監視対象の ID、パスワード
⑧ Witness ノードの ESXi パスワード変更
⑨ NEC Hyper Converged System Console の登録情報の更新
⑩ Windows サーバと vCenter Server の保守アカウントパスワード
⑪ ESMPRO/ServerManager の登録情報の更新 (エクスプレス通報サービスを利用する場合)

5.1.1 準備

NEC Hyper Converged System スタートアップガイドの事前準備および受入確認の手順を完了し、NEC Hyper Converged System の電源がオンになり、利用できる状態としてください。

Windows PC を、管理用ネットワークに接続してください。管理用ネットワーク上の管理ノード(vCenter Server, 管理 VM)に接続できるよう、ネットワーク設定を合わせて変更してください。

5.1.2 ID・パスワードの依存関係について

重要 **ID・パスワードを変更した場合は、以下の関係表に従って、影響を受けるソフトウェアに ID・パスワードの再登録をして下さい。**

設定登録方法は、各ソフトウェアのマニュアルを参考にして下さい。

変更対象の ID・パスワード	影響を受けるソフトウェア		備考
	ESMPRO/ ServerManager	NEC Hyper Converged System Console	
R120h-1M/2M BMC の ID・パスワード	△(※1)	○	
クラスタノード、管理ノードの ESXi の ID・パスワード	△(※1)	○	
vCSA の vCenterServerAppliance 管理インターフェイス(VAMI)の ID・パスワード	ー	○	
vCSA の SSO の ID・パスワード	ー	○	
管理 VM(Windows Server 2022)の Administrator パスワード	ー	ー	
ESMPRO/ServerManager の ID・パスワード	ー	ー	
NEC Hyper Converged System Console の ID・パスワード	ー	ー	
保守アカウント	ー	ー	
Witness ノードの ID・パスワード	ー	○	

※1 ESMPRO/ServerManager に BMC が監視対象として設定されている場合、変更が必要です。
構築サービスでエクスプレス通報サービスの設定を実施した場合は、BMC が監視対象として設定されています。
設定登録方法は、ESMPRO/ServerManager セットアップガイドの“第 10 章 VMware ESXi サーバのセットアップ”を参考にして下さい。

○: 設定変更が必要　　△: 場合によって、設定変更が必要　　ー: 不要

5.2 クラスタノード、管理ノードの BMC の ID・パスワード変更

5.2.1 R120h-1M/2M の BMC パスワード変更

《注意》

BMC(NEC iLO 5)のパスワードを変更した場合は、変更後に NEC Hyper Converged System 上および ESMPRO/ServerManager 上で登録されている BMC のパスワード情報を更新いただく必要があります。パスワード変更におけるシステム影響を及ぼす関係表は 5.1.2 節を、ESMPRO/ServerManager 上のパスワード情報を更新する手順は 5.10 節を、NEC Hyper Converged System 上のパスワード情報を更新する手順は 5.9 節を参照ください。

1. Windows PC でリモートデスクトップ接続(mstsc)を起動し、ヒアリングシートに記載されている「管理 VM」の IP アドレスを入力し、管理 VM にログインします。(IP アドレス例: 192.168.100.10:3389)

2. 管理 VM 上で、Web ブラウザを起動し、BMC の URL を入力し、ログイン画面を表示します。

   https://<クラスタノードまたは管理ノードの BMC の IP アドレス>/

   (保守用ネットワーク IP アドレスは、ヒアリングシートに記載されます)

   ※ 「接続がプライベートではありません」画面が表示された場合は、[詳細設定]をクリックし表示された画面で、[<IP アドレスまたは FQDN>に進む(安全ではありません)]クリックしてください。

3. Web ブラウザに BMC のログイン画面が表示されます。

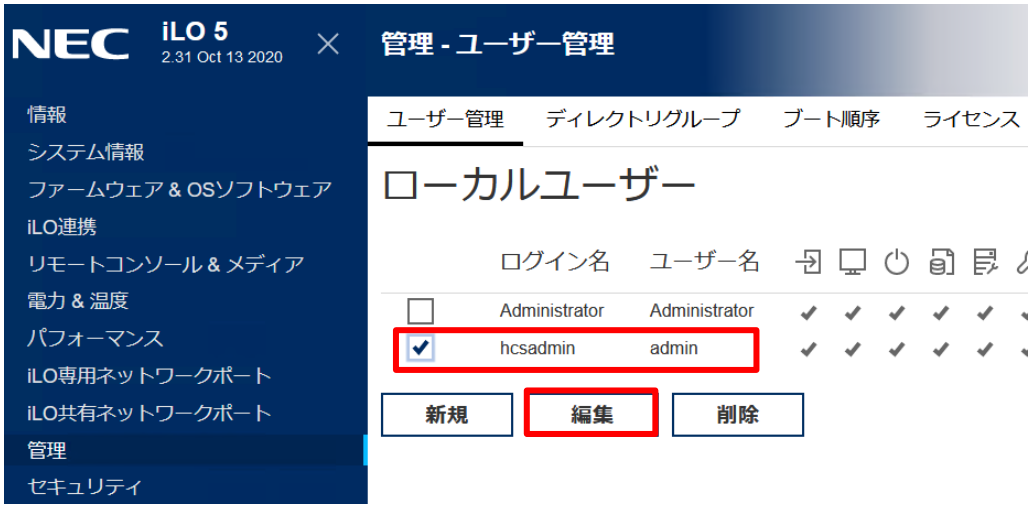
4. ローカルユーザ名、パスワードを入力し、[ログイン]をクリックします。
(ローカルユーザ名、パスワードは、初期パスワード通知書に記載されます)

5. 正常にログインすると、Web ブラウザに[情報-iLO 概要]画面が表示されます。

6. 左ツリーから[管理]をクリックします。

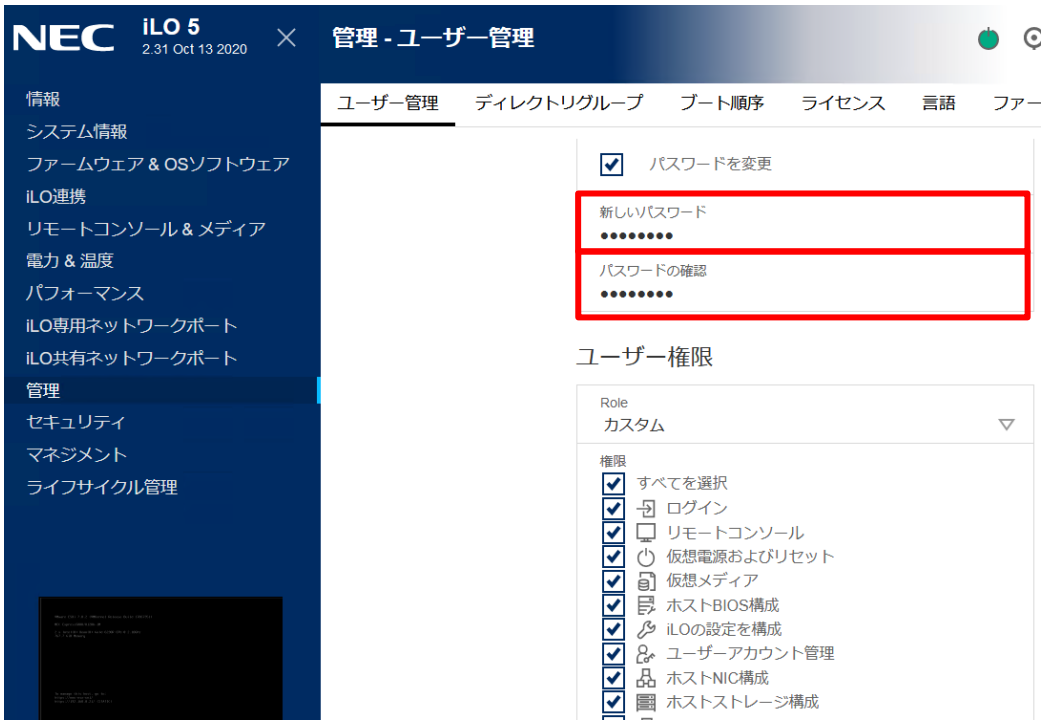
7. [管理–ユーザー管理]のローカルユーザ画面に遷移されることを確認します。

8. 画面内に表示されたユーザにて、パスワードを変更したいユーザ名のチェックボックスをクリックし[編集]をクリックします。



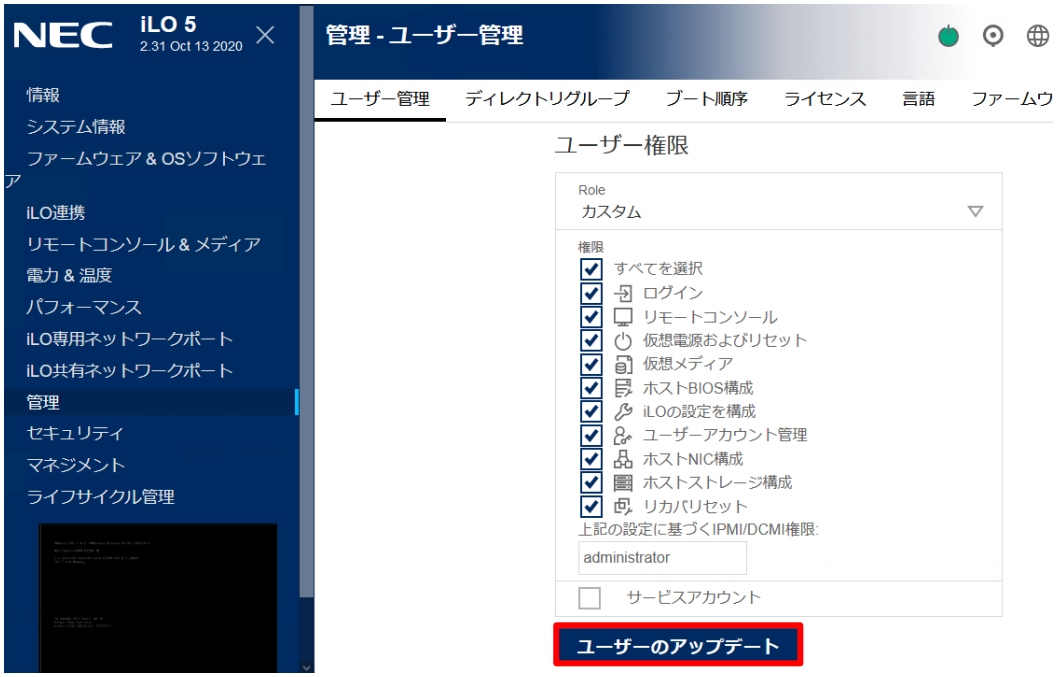
9. ローカルユーザの追加/編集画面に遷移されることを確認します。

10. [パスワードを変更]チェックボックスをクリックし、新しいパスワード、パスワードの確認項目に変更したいパスワードを入力します。



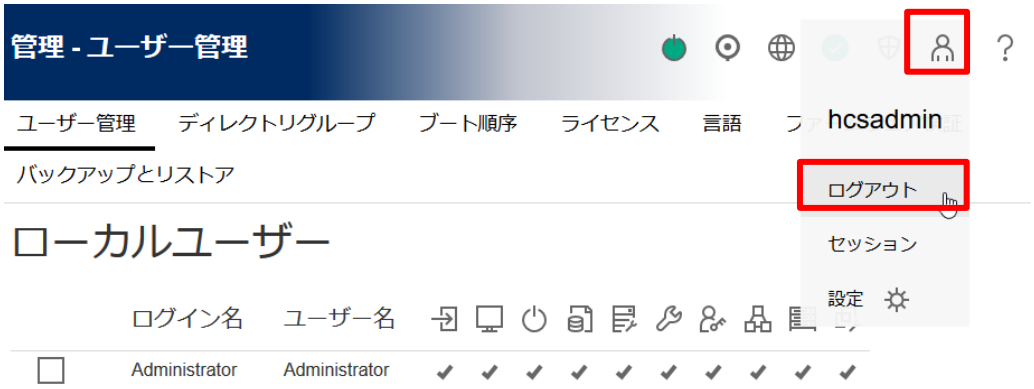
※ パスワードの要件は、初期パスワード通知書の「1.2 パスワード要件」を参照ください。

11. 画面をスクロールし、下部にある[ユーザーのアップデート]をクリックします。



12. パスワードが正常に変更され、ローカルユーザー画面に戻ることを確認します。

13. 画面右上のアカウントアイコンをクリックし、[ログアウト]をクリックします。



14. BMC から正常にログアウトすると、BMC のログイン画面が表示されます。

15. すべてのクラスタノード、管理ノードで BMC のパスワード変更をおこなってください。

5.3 クラスタノード、管理ノードの ESXi パスワードの変更

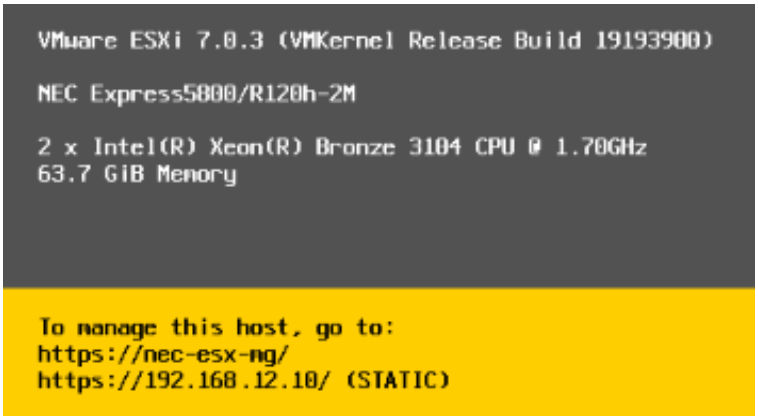
《注意》

クラスタノード、管理ノードの ESXi のパスワードを変更した場合は、変更後に NEC Hyper Converged System 上で登録されている ESXi のパスワード情報を更新いただく必要があります。パスワード変更におけるシステム影響を及ぼす関係表は 5.1.2 節を、パスワード情報を更新する手順は 5.9 節を参照ください。また、サーバ診断カルテを利用している場合は、5.10 節を参照し、ESMPRO/ServerManager の登録情報の更新も実施してください。

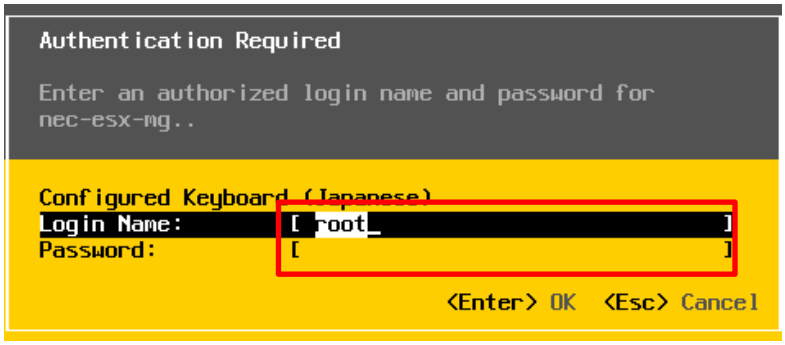
クラスタノード、管理ノードの ESXi パスワード変更方法手順は同一です。クラスタノード、管理ノードの ESXi パスワード変更方法は、ダイレクトコンソールから変更する方法と、Web ブラウザで Host Client から変更する方法の 2 種類あります。どちらか都合のよい方法を選択し、下記手順を実施してください。

5.3.1 ダイレクトコンソールからの ESXi のパスワード変更

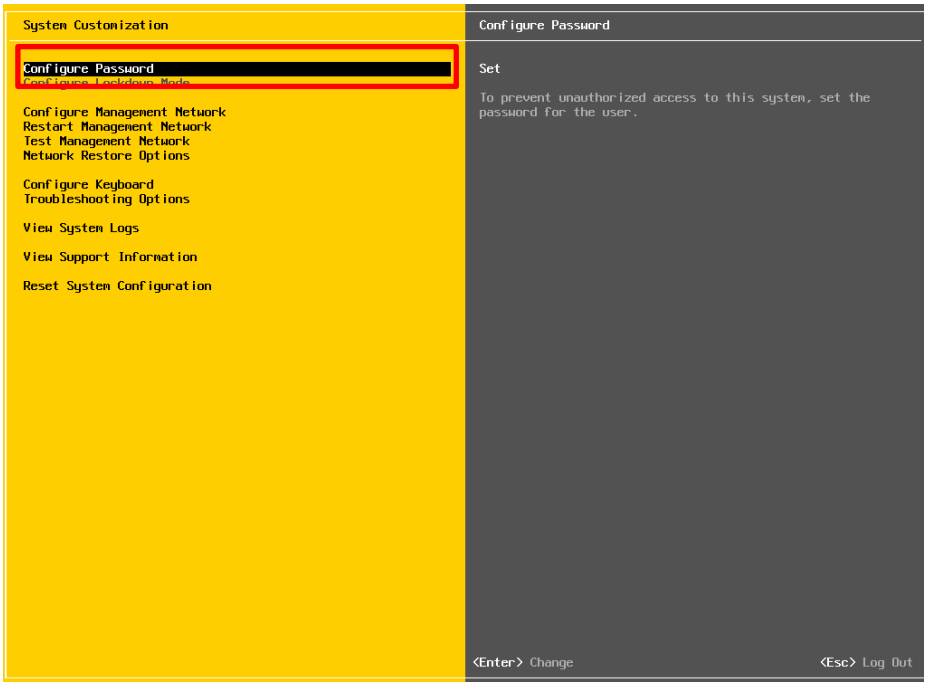
1. クラスタノードまたは管理ノードにディスプレイとキーボードを接続し、ダイレクトコンソール画面を表示します。



2. ダイレクトコンソール画面から[F2]を押し、ログイン画面を表示します。
   Login Name は「root」とし、Password に root password を入力してログインします。
   (root password は初期パスワード通知書に記載されます)



3. ダイレクトコンソール画面のメニューから、[Configure Password]を選択します。



4. 現在のパスワードと新しいパスワード入力して、パスワードを変更します。
(現在のパスワード = root password、初期パスワード通知書に記載されます)

※ パスワードの要件は、初期パスワード通知書の「1.2 パスワード要件」を参照ください。

5. パスワード変更後、[ESC]キーを押してログアウトして下さい。

6. すべてのクラスタノード、管理ノードで ESXi のパスワード変更をおこなってください。

5.3.2 Host Client からの ESXi のパスワード変更

1. Windows PC でリモートデスクトップ接続(mstsc)を起動し、ヒアリングシートに記載されている「管理 VM」の IP アドレスを入力し、管理 VM にログインします。(IP アドレス例: 192.168.100.10:3389)

2. 管理 VM 上で Web ブラウザを起動し、Host Client のログイン用の URL を入力し、
   Host Client ログイン画面を表示します。

   https://<クラスタノード or 管理ノードの管理用ネットワーク IP アドレス>/ui

   (管理用ネットワーク IP アドレスは、ヒアリングシートに記載されます)

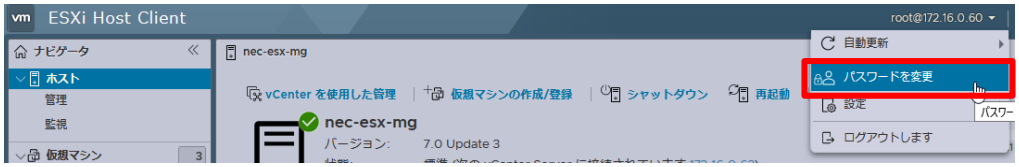
   ※ 「接続がプライベートではありません」画面が表示された場合は、[詳細設定]をクリックし表示された画面で、[<IP アドレスまたは FQDN>に進む(安全ではありません)]クリックしてください。

3. Web ブラウザに Host Client のログイン画面が表示されます。

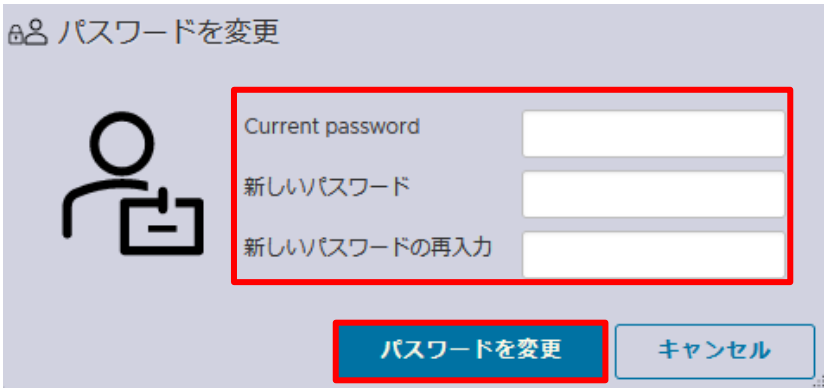
4. ユーザ名、パスワードを入力し、[ログイン]をクリックします。
   (ユーザ名、パスワードは、初期パスワード通知書に記載されます)

5. 正常にログインすると、Web ブラウザにホスト画面が表示されます。

6. Host Client の画面上部に表示されているユーザ名部分をクリックし、表示されたメニューで[パスワードを変更]をクリックします。



7. パスワードを変更画面が表示されるので、[Current password]に変更前のパスワードを入力し、[新しいパスワード]、[新しいパスワードの再入力]に変更したいパスワードを入力し、[パスワードを変更]をクリックします。



※ パスワードの要件は、初期パスワード通知書の「1.2 パスワード要件」を参照ください。

※ 新しいパスワードを「<変更前のパスワード>+2」のような変更前のパスワードに基づいた値にした場合、以下のエラーが表示されて変更に失敗します。

8. パスワード変更されたことを確認し、Host Client の画面上部に表示されているユーザ名部分をクリックし、表示されたメニューで[ログアウトします]をクリックします。

9. Host Client から正常にログアウトすると、Web ブラウザに Host Client のログイン画面が表示されます。

10. すべてのクラスタノード、管理ノードで ESXi のパスワード変更を行ってください。

5.4 管理ノードの vCSA パスワードの変更

VMware vCenter Server Appliance(vCSA)には、vCSA の root パスワードと、管理用のシングルサインオン(SSO)アカウントの ID、パスワードがそれぞれ設定されています。それぞれの変更方法を下記に示します。

5.4.1 vCSA の vCenterServer 管理インターフェイス(VAMI)の root パスワードの変更

1. Windows PC でリモートデスクトップ接続(mstsc)を起動し、ヒアリングシートに記載されている「管理 VM」の IP アドレスを入力し、管理 VM にログインします。(IP アドレス例: 192.168.100.10:3389)

2. 管理 VM 上で Web ブラウザを起動し、VAMI のログイン用の URL を入力し、VAMI ログイン画面を表示します。

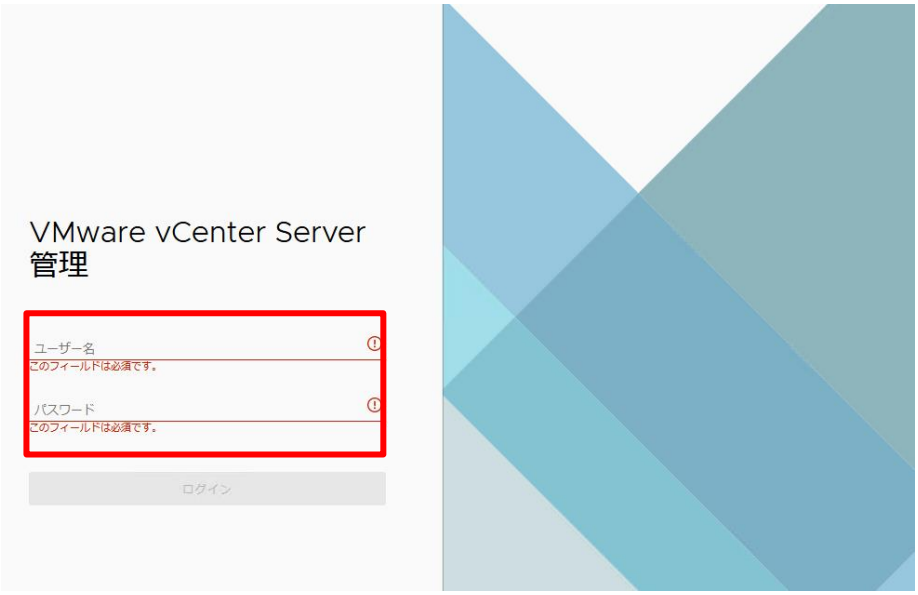
   https://<vCSA のホスト名>:5480/

   (vCSA のホスト名はヒアリングシートに記載されます)

   ※ 「接続がプライベートではありません」画面が表示された場合は、[詳細設定]をクリックし表示された画面で、[<IP アドレスまたは FQDN>に進む(安全ではありません)]クリックしてください。

3. Web ブラウザに VAMI のログイン画面が表示されます。

4. ユーザ名、パスワードを入力し、[ログイン]をクリックします。
   (ユーザ名は root です。パスワードは初期パスワード通知書に記載されます)



5. 正常にログインすると、Web ブラウザに VAMI の画面が表示されます。

6. 左ツリーから[管理]をクリックします。l

7. 管理画面に遷移されることを確認し、画面右上の[変更]をクリックします。

8. [パスワードの変更]ダイアログが表示されますので、現在のパスワード項目に現在のパスワードを入力し、新しいパスワード、パスワードの確認項目に変更したいパスワードを入力し[保存]をクリックします。

※ パスワードの要件は、初期パスワード通知書の「1.2 パスワード要件」を参照ください。

9. パスワード変更されたことを確認し、VAMI の画面上部に表示されている[root]をクリックした後[ログアウト]をクリックします。

10. VAMI から正常にログアウトすると、Web ブラウザに VAMI のログイン画面が表示されます。

5.4.2 vCSA の SSO アカウント ID、パスワードの変更

《注意》

vCSA の SSO ID、パスワードを変更した場合は、変更後に NEC Hyper Converged System 上で登録されている vCSA の SSO のパスワード情報を更新いただく必要があります。パスワード変更におけるシステムへ影響を及ぼす関係表は 5.1.2 節を、パスワード情報を更新する手順は 5.9 節を参照ください。

1. Windows PC でリモートデスクトップ接続(mstsc)を起動し、ヒアリングシートに記載されている「管理 VM」の IP アドレスを入力し、管理 VM にログインします。(IP アドレス例: 192.168.100.10:3389)

2. 管理 VM 上で、Web ブラウザを起動し、VMware vSphere Client のログイン用の URL を入力し、VMware vSphere Client ログイン画面を表示します。

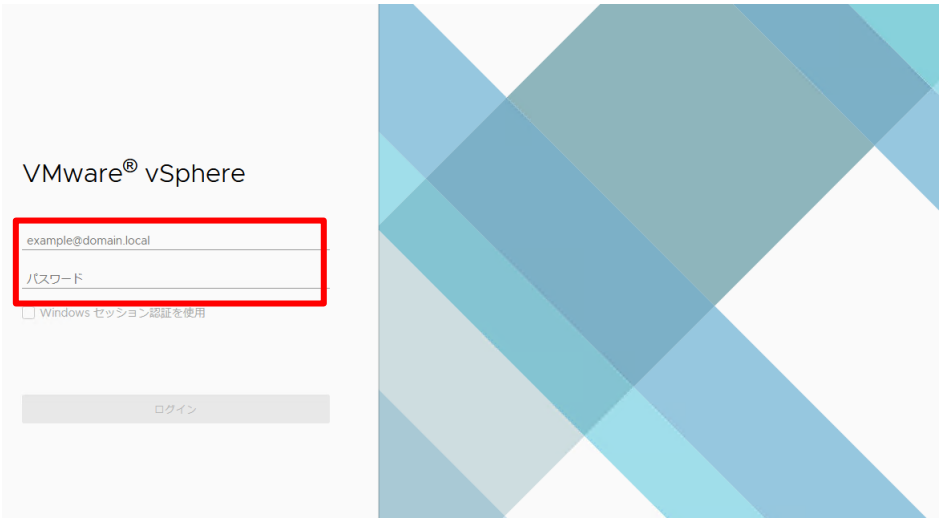
   https://<vCSA のホスト名>/ui

   (vCSA のホスト名はヒアリングシートに記載されます)

   ※ 「接続がプライベートではありません」画面が表示された場合は、[詳細設定]をクリックし表示された画面で、[<IP アドレスまたは FQDN>に進む(安全ではありません)]クリックしてください。

3. Web ブラウザに VMware vSphere Client (vCSA)のログイン画面が表示されます。

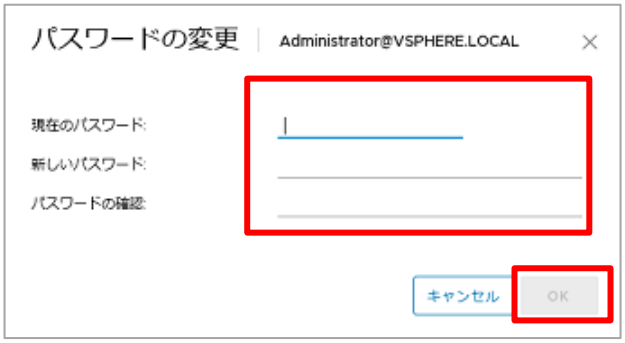
4. ユーザ名、パスワードを入力し、[ログイン]をクリックします。
   - ユーザ名: “administrator@”＋ SSO ドメイン名(SSO ドメイン名はヒアリングシートに記載されます)
   - パスワード: (パスワードは初期パスワード通知書に記載されます)



5. 正常にログインすると、VMware vSphere Client の操作画面が表示されます。

6. VMware vSphere Client の画面上部に表示されているユーザ名部分をクリックし、表示されたメニューで[パスワードの変更]をクリックします。

7. パスワードの変更画面が表示されるので、現在のパスワード項目に現在のパスワードを入力し、新しいパスワード、パスワードの確認項目に変更したいパスワードを入力し、[OK]をクリックします。



※ パスワードの要件は、初期パスワード通知書の「1.2 パスワード要件」を参照ください。

8. パスワード変更されたことを確認し、VMware vSphere Client の画面上部に表示されているユーザ名部分をクリックし、表示されたメニューで[ログアウト]をクリックします。

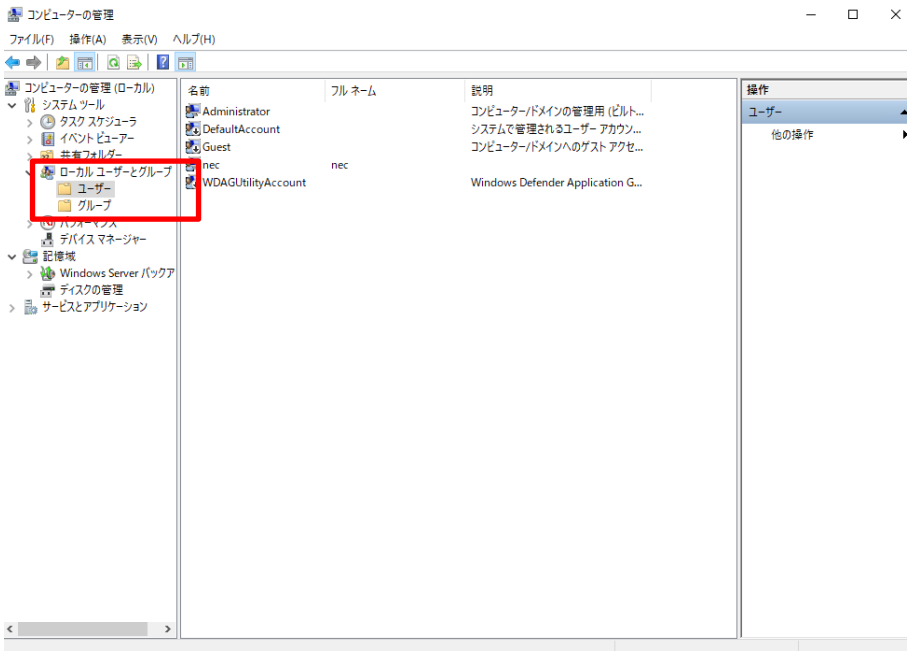
9. VMware vSphere Client から正常にログアウトすると、Web ブラウザに VMware vSphere Client のログイン画面が表示されます。

5.5 管理ノードの管理 VM(Windows Server 2022)のパスワード変更

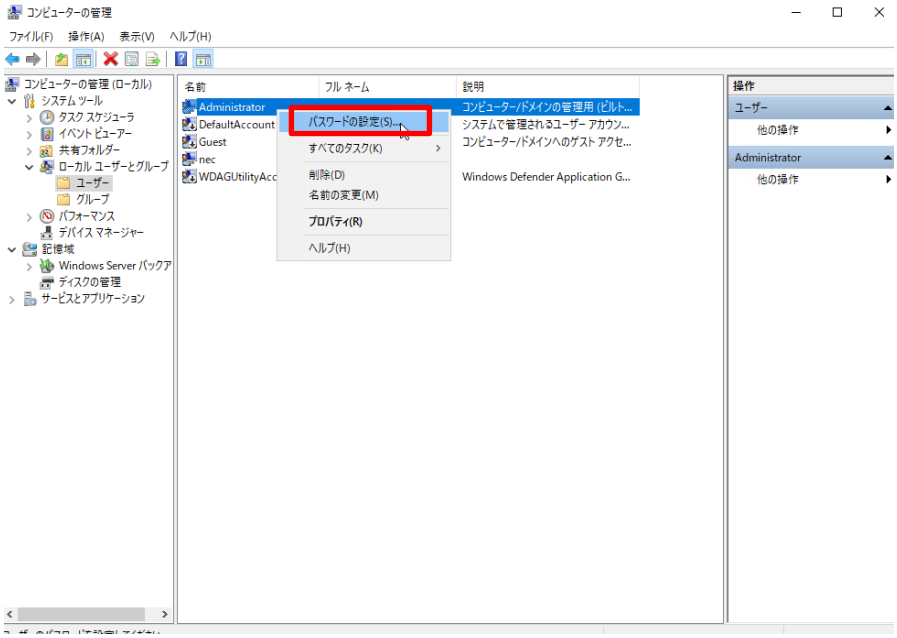
1. Windows PC でリモートデスクトップ接続(mstsc)を起動し、ヒアリングシートに記載されている「管理 VM」の IP アドレスを入力し、管理 VM にログインします。(IP アドレス例: 192.168.100.10:3389)

2. 管理 VM のデスクトップ画面の[Windows キー( )]を右クリックして、コンピューターの管理画面を起動します。

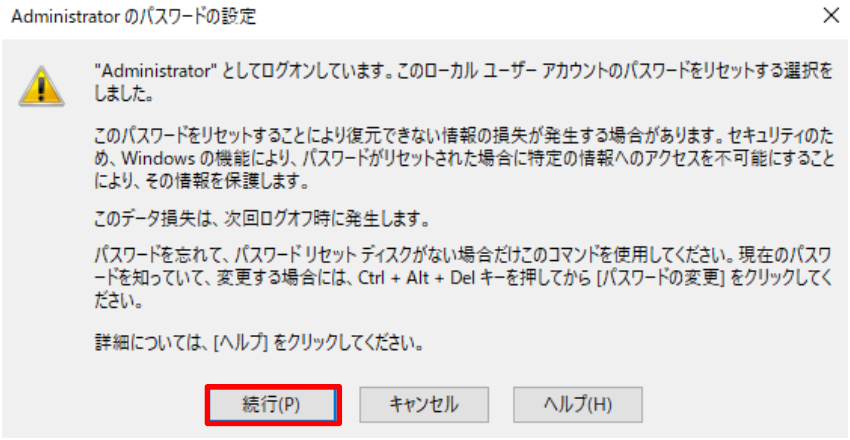
3. コンピューターの管理画面から、[ローカルユーザーとグループ]→[ユーザー]をクリックし、ユーザー覧を表示させます。



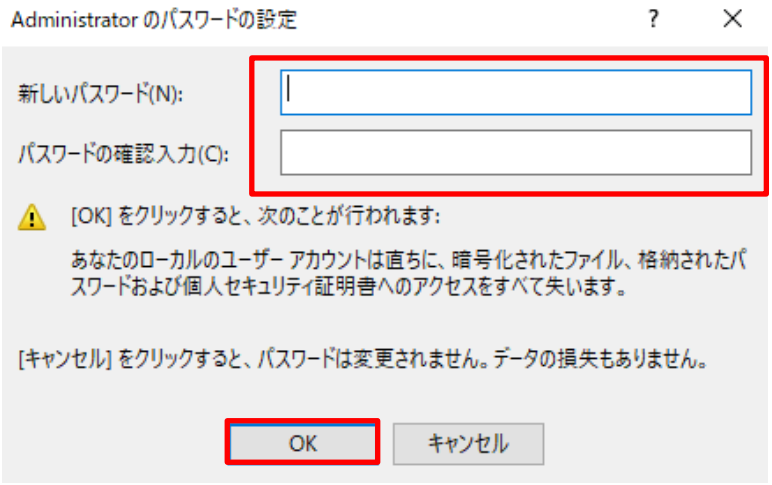
4. “Administrator”ユーザを選択し、マウスを右クリックして、[パスワードの設定]”を選択します。



5. 注意画面がでてくるので、[続行]をクリックします。



6. 新しいパスワードを入力し、[OK]をクリックし、パスワードを変更します。



※ パスワードの要件は、初期パスワード通知書の「1.2 パスワード要件」を参照ください。

5.6 管理 VM の ESMPRO/ServerManager のパスワード変更

1. Windows PC でリモートデスクトップ接続(mstsc)を起動し、ヒアリングシートに記載されている「管理 VM」の IP アドレスを入力し、管理 VM にログインします。(IP アドレス例: 192.168.100.10:3389)

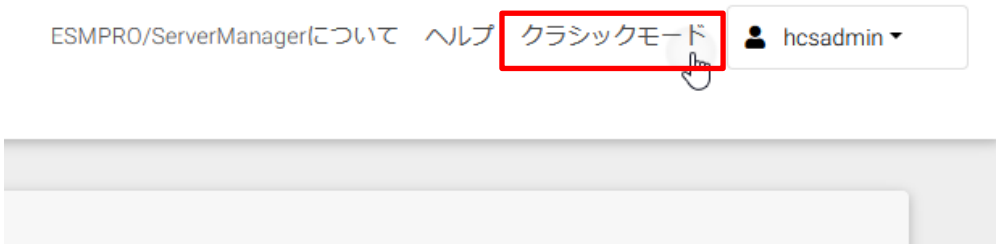
2. 管理 VM 上で、Web ブラウザを起動し、Web ブラウザのアドレス欄に以下の URL を入力します。

   http://<管理 VM のホスト名>:21120/esmpro

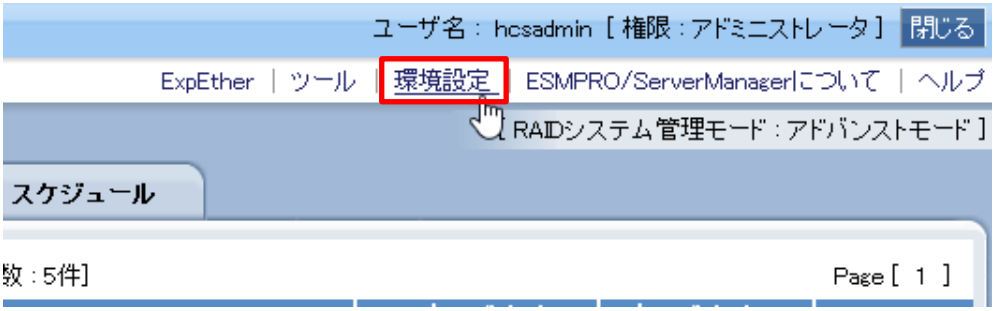
   (管理 VM のホスト名はヒアリングシートに記載されます。)

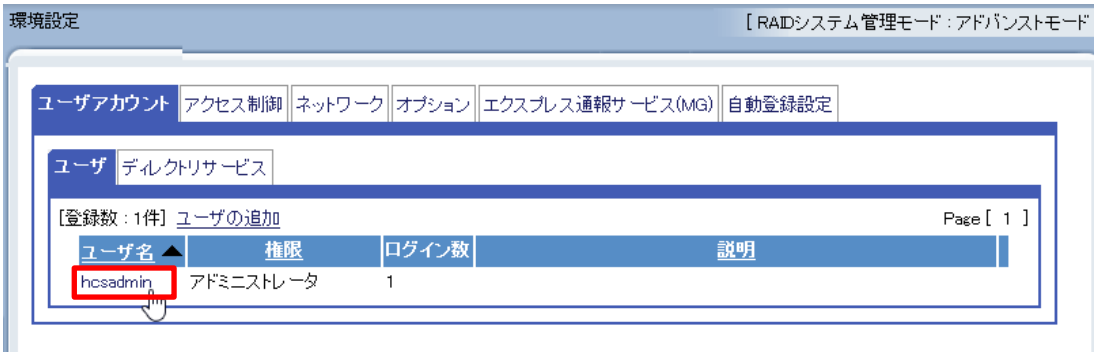
3. ESMPRO/ServerManager のログイン画面で、ユーザ名・パスワードを入力し、ログインします。
   (ユーザ名、パスワードは初期パスワード通知書に記載されます)

4. 画面右上の[クラシックモード]をクリックします。



5. 画面右上の、[環境設定]をクリックし、環境設定画面を表示、初期 ID のユーザ（この手順書では、hcsadmin）をクリックします。

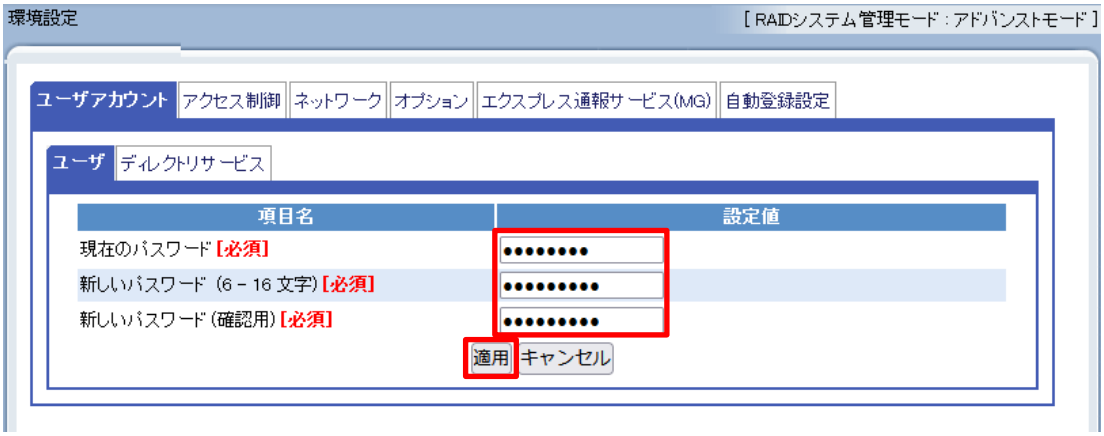




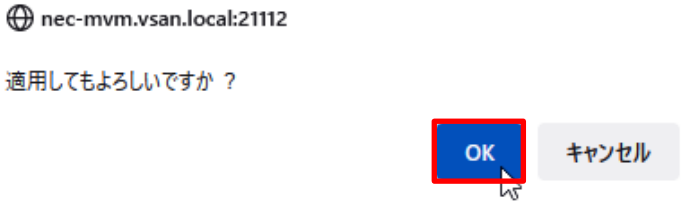
6. 環境設定：ユーザアカウント画面の初期 ID のユーザ情報画面で、[パスワードの変更]をクリックします。

7. パスワード変更画面で、現在のパスワード・新しいパスワード（確認用含む）を入力し、[適用]をクリックしてパスワードを変更します。

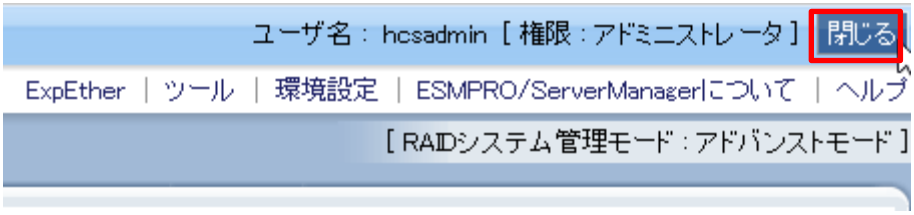
※ パスワードの要件は、初期パスワード通知書の「1.2 パスワード要件」を参照ください。



8. 以下の画面が表示されますので、[OK]をクリックします。



9. 画面右上の[閉じる]をクリックします。



5.7 NEC Hyper Converged System Console のパスワード変更

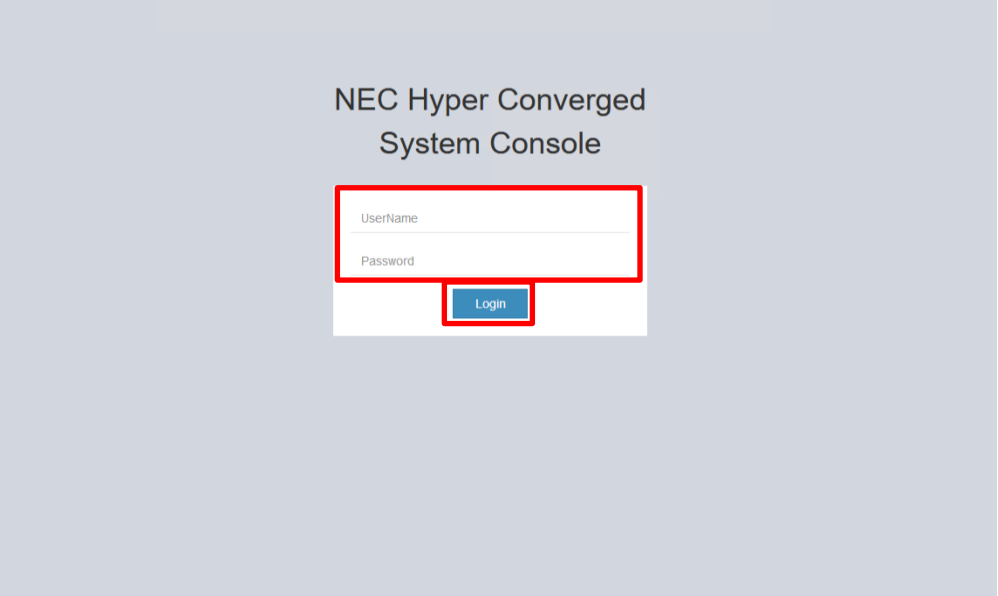
1. Windows PC でリモートデスクトップ接続(mstsc)を起動し、ヒアリングシートに記載されている「管理 VM」の IP アドレスを入力し、管理 VM にログインします。(IP アドレス例: 192.168.100.10:3389)

2. 管理 VM 上で Web ブラウザを起動し、Web ブラウザのアドレス欄に以下の URL を入力します。

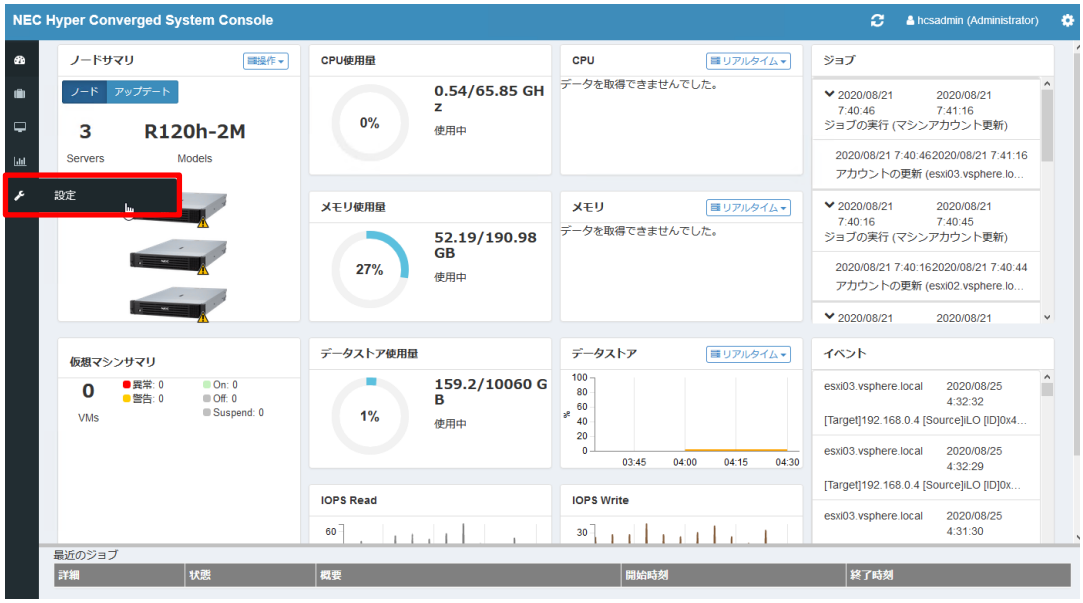
   http://<管理 VM のホスト名>/nechcs/

   (管理 VM のホスト名はヒアリングシートに記載されます。)

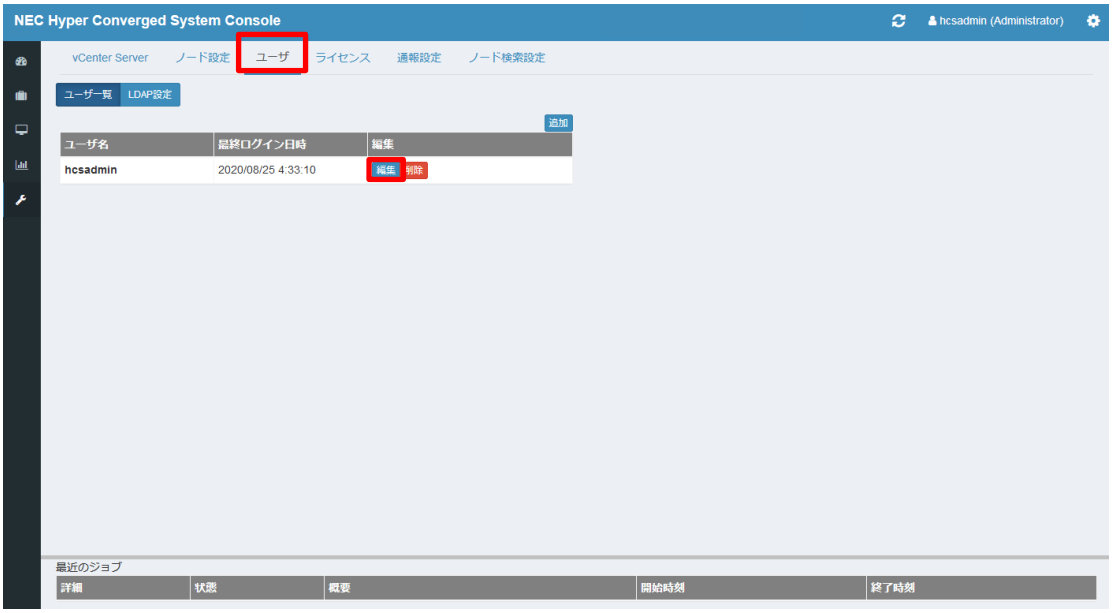
3. NEC Hyper Converged System Console のログイン画面が表示されます。ID・パスワードを入力し、ログインします。
   (ID、パスワードは初期パスワード通知書に記載されます)



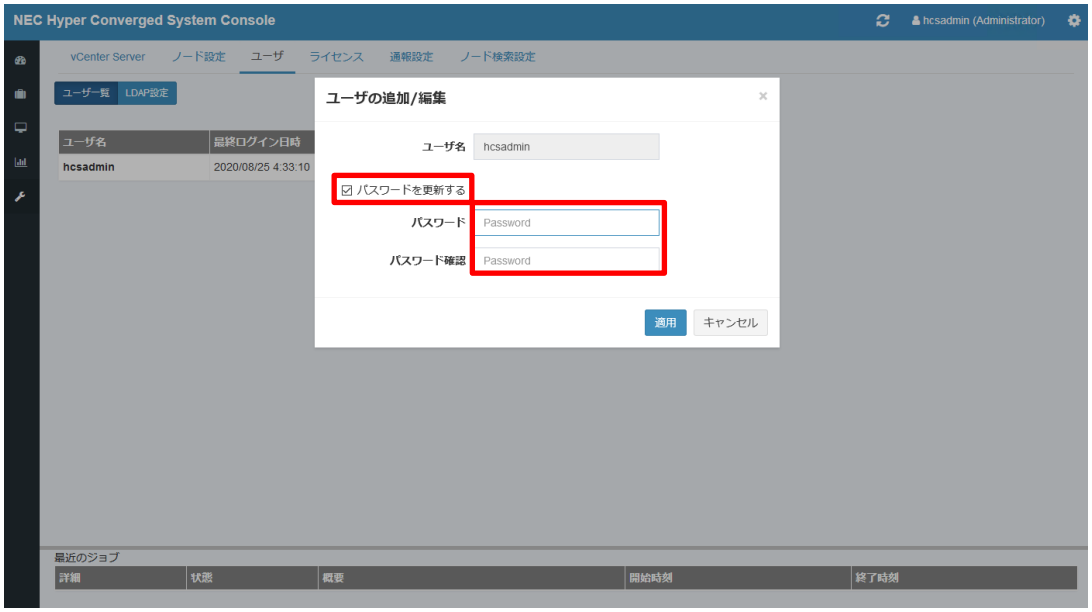
4. NEC Hyper Converged System Console のメイン画面が表示されます。[設定]メニューをクリックし設定画面を表示します。



5. NEC Hyper Converged System Console の設定画面で、[ユーザ]タブをクリックし、パスワードを変更するユーザの[編集]ボタンをクリックします。



6. ユーザの追加編集画面で、[パスワードの更新]にチェックを入れ、新しいパスワードを入力し、パスワードの変更を行います。



※ パスワードの要件は、初期パスワード通知書の「1.2 パスワード要件」を参照ください。

5.8 Witness ノードの ESXi パスワード変更

3 ノード以上の構成の場合は本節の実施は不要です。

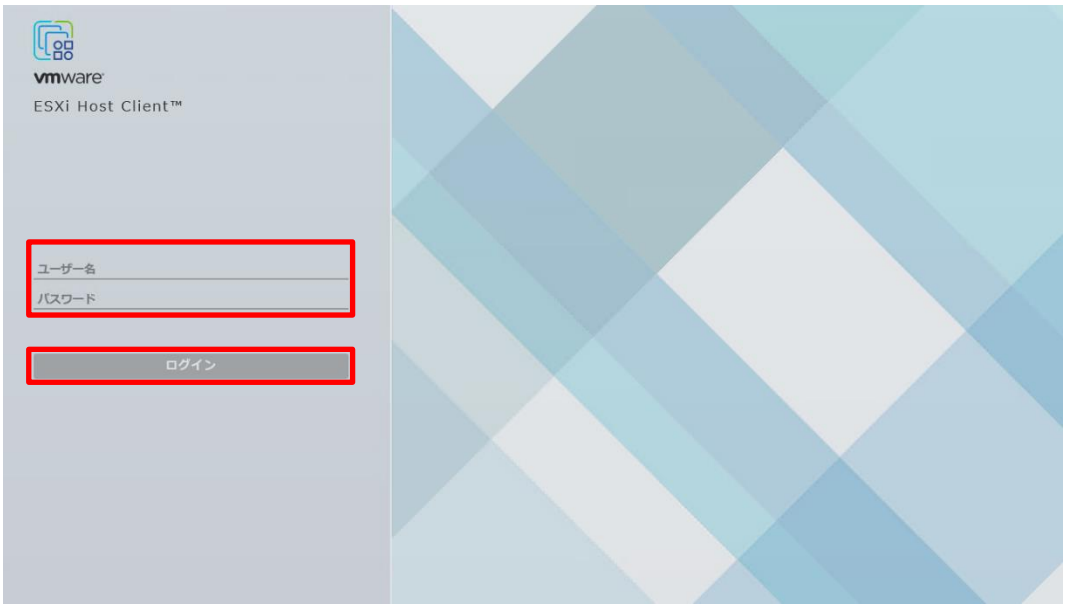
1. Windows PC でリモートデスクトップ接続(mstsc)を起動し、ヒアリングシートに記載されている「管理 VM」の IP アドレスを入力し、管理 VM にログインします。
   (IP アドレス例: 192.168.100.10:3389)
2. 管理 VM 上で Web ブラウザを起動します。
3. Web ブラウザのアドレス欄に以下の URL を入力します。

   http://<Witness ノードの IP アドレス>/

   (Witness ノードの IP アドレスはヒアリングシートに記載されます)

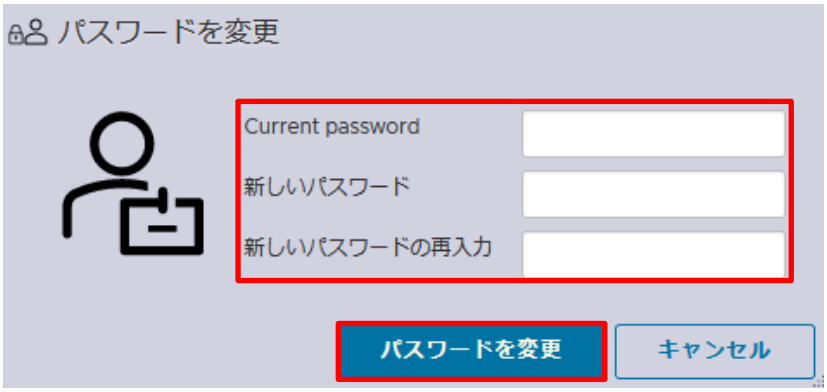
   ※ 「接続がプライベートではありません」画面が表示された場合は、[詳細設定]をクリックし表示された画面で、[<IP アドレスまたは FQDN>に進む(安全ではありません)]クリックしてください。

4. ログイン画面が表示されるので、Witness ノードのユーザ名・初期パスワードでログインして、Host Client の初期画面を表示させます。
   (ユーザ名、初期パスワードは、初期パスワード通知書に記載されます)



5. Host Client の初期画面で、ログイン情報画面をクリックし、[パスワードの変更]をクリックします。

6. パスワード変更画面で新しいパスワードを入力した後、[パスワードを変更]をクリックし、パスワードを変更します。



※ パスワードの要件は、初期パスワード通知書の「1.2 パスワード要件」を参照ください。

※ 新しいパスワードを「<変更前のパスワード>+2」のような変更前のパスワードに基づいた値にした場合、以下のエラーが表示されて変更に失敗します。

7. パスワード変更後、Host Client をログアウトして、ブラウザを閉じて下さい。

5.9 NEC Hyper Converged System Console の登録情報の更新

本節では BMC、ESXi、vCSA、Witness ノードのパスワードを変更した際の NEC Hyper Converged System Console での登録情報の更新手順を記載します。

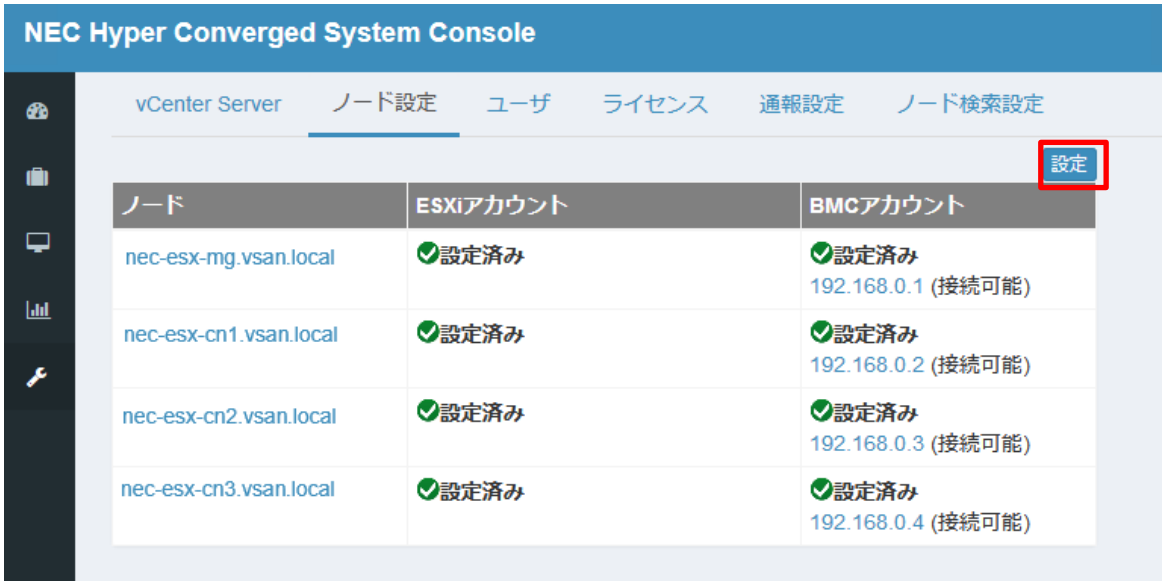
5.7 節の手順 1～3 を参照して、NEC Hyper Converged System Console にログインします。

5.9.1 ノード登録情報の更新

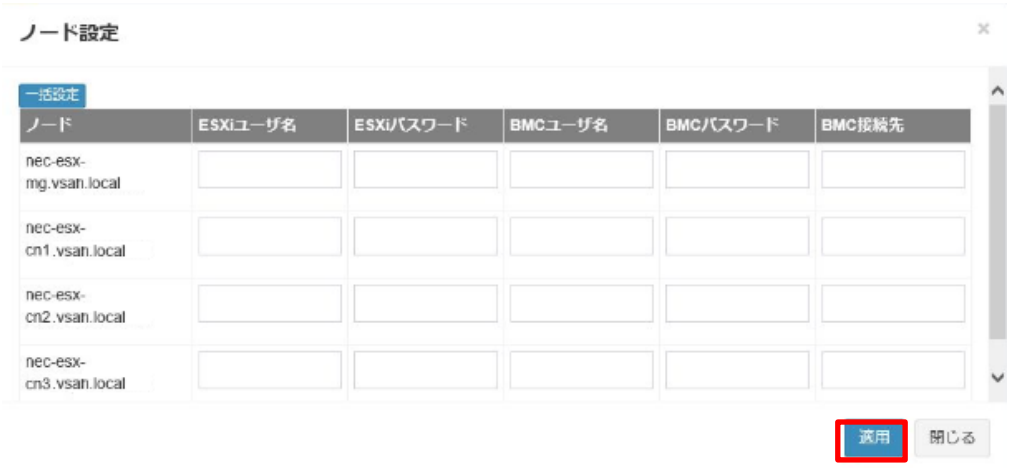
1. 画面左メニューの[設定]をクリックします。

2. 画面上部のメニューから[ノード設定]をクリックします。

3. ノード一覧が表示されますので、一覧右上の[設定]をクリックします。

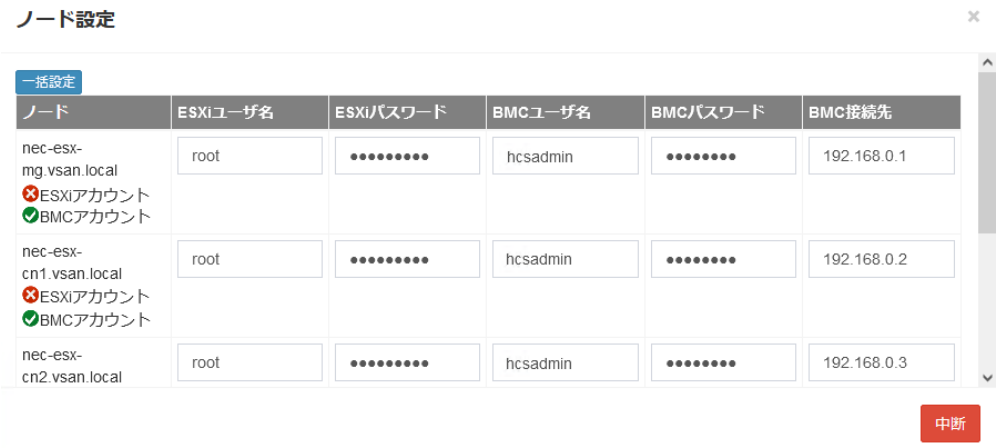


4. ノード設定ダイアログが表示されますので、管理ノード、クラスタノード、Witness ノードそれぞれに変更後の値を入力して[適用]をクリックします。



これでノード登録情報の更新は完了です。

《補足》
サーバ診断カルテを利用している環境でノード登録情報を変更した場合、ESXi パスワードの更新に失敗する場合があります。



ESXi パスワードの更新に失敗した場合、vSphere Client にログインし、以下の警告が表示されていることを確認してください。

この場合、ESXi のリモートアクセスがロックアウトされ、NEC HCS Console や

ESMPRO/ServerManager などの外部ソフトウェアで登録情報の更新ができなくなるため、
管理エージェントを再起動して一時的にロックアウトを解除する必要があります。
以下の手順に従い、登録情報の更新を実施してください。

① 3.14 節を参照し、SSH またはローカルコンソール(ダイレクトコンソール)を使用して
ESXi Shell に root ユーザでログインします。

② 以下のコマンドを実行します。

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

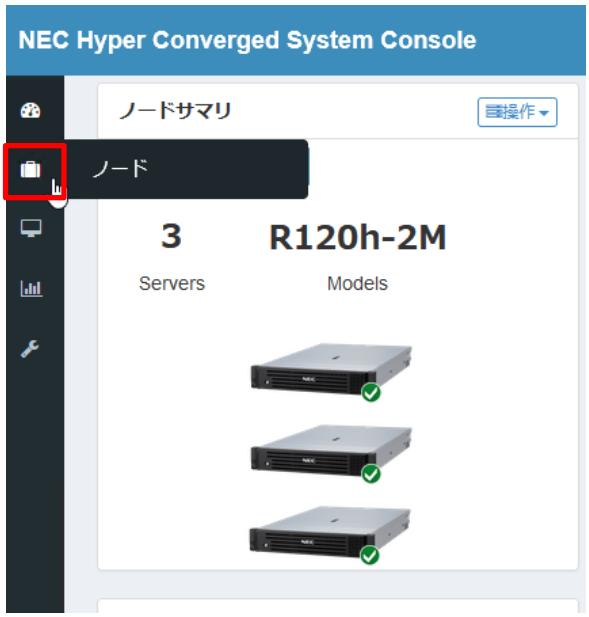
```
[root@nec-esx-ng:~] etc/init.d/hostd restart
watchdog-hostd[1992931]: Terminating watchdog process with PID 1985179
hostd stopped.
hostd started.
```

③ 以下のコマンドを実行します。

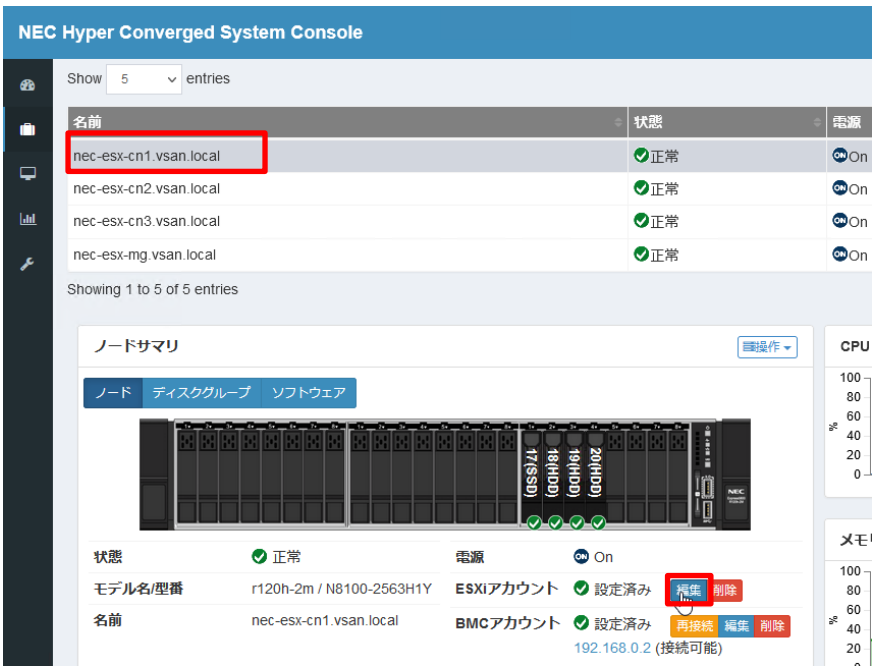
```
# /etc/init.d/vpxa restart
```

```
[root@nec-esx-ng:~] etc/init.d/vpxa restart
watchdog-vpxa[1993130]: Terminating watchdog process with PID 1985342
vpxa stopped.
vpxa started.
```

④ NEC HCS Console にログインし、[ノード]をクリックします。



⑤ ESXi パスワードを更新するノードを選択し、ESXi アカウント右側の[編集] をクリックします。



⑥ 「パスワードを更新する」にチェックを付け、変更後のパスワードを入力し、[適用]をクリックします。

※ 管理エージェントの再起動から時間が経過するなど、ESXi のロックアウトが再度発生してパスワード更新に失敗した場合は、②から③の手順を再度実行し、パスワード更新を実施してください。

※ ノードサマリの状態が「警告」になっており、パスワード更新後も状態が解消されない場合は、[操作]から[状態リセット]を実施してください。

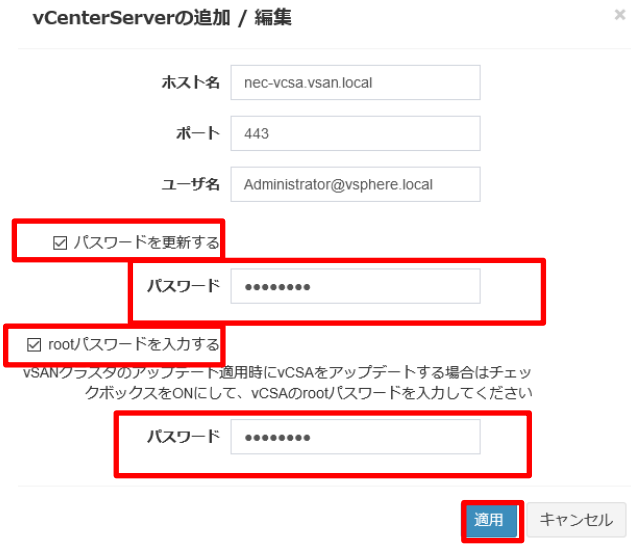
ESXi パスワードの更新に失敗したノード全てで本手順を実施してください。

5.9.2 vCSA 登録情報の更新

1. 画面左メニューの[設定]をクリックします。

2. vCenter Server タブをクリックし、画面右上の[編集]をクリックします。

3. vCenter Server の追加 / 編集ダイアログが開きますので、[パスワード更新を更新する]にチェックを入れて、変更後のパスワードを入力します。その後、[root パスワードを入力する]にチェックを入れて root パスワードを入力し、[適用]をクリックします。



これで vCSA 登録情報の更新は完了です。

5.10 ESMPRO/ServerManager の登録情報の更新

本節は、エクスプレス通報サービスおよびサーバ診断カルテを利用し、ESMPRO/ServerManager に iLO や ESXi コンポーネントを登録している場合のみ実施してください。

登録コンポーネントのパスワードを変更した際の ESMPRO/ServerManager での登録情報の更新手順を記載します。

《参考》

サーバ診断カルテを利用している場合、ESMPRO/ServerManager で ESXi の管理登録(接続チェック)を行う際に、SLP サービスを有効化する必要があります。VMware ESXi 7.0 Update 2c 以降では、潜在的なセキュリティの脆弱性を防ぐために SLP サービスがデフォルトで無効化されおり、登録情報の更新を実施する前に有効化する必要があります。

以下の手順で SLP サービスの起動状態を確認します。

更新対象のノード ESXi Shell を起動し、root ユーザでログインした後、下記のコマンドを実行し、SLP サービスが有効になっているかを確認します。

```
# chkconfig -l | grep slpd
```

無効の場合は以下の出力となります。

```
[root@nec-esx-mg:~] chkconfig -l | grep slpd
slpd                    off
```

下記のコマンドを実行し、SLP サービスが起動しているかを確認します。

```
# /etc/init.d/slpd status
```

停止状態の場合は以下の出力となります。

```
[root@nec-esx-mg:~] /etc/init.d/slpd status
slpd is not running
```

SLP サービスが無効化していた場合は、引き続き以降の手順を実施し、SLP サービスの有効化およびファイアウォールでの SLP サービスのルールセット有効化手順を実施してください。

- SLP サービスのルールセット有効化手順

1. ファイアウォールで SLP サービスのルールセットを有効にします。

   ```
   # esxcli network firewall ruleset set -r CIMSLP -e 1
   ```

   ```
   [root@nec-esx-mg:~] esxcli network firewall ruleset set -r CIMSLP -e 1
   ```

2. SLP サービス自動起動が無効(off)になっていた場合は有効にします。

   ```
   # chkconfig slpd on
   ```

   ```
   [root@nec-esx-mg:~] chkconfig slpd on
   ```

3. SLP サービスが停止していた場合は起動します。

```
# /etc/init.d/slpd start
```

```
[root@nec-esx-ng:~] /etc/init.d/slpd start
Starting slpd
```

4. CIM エージェントを無効にしてから有効にします。以下のコマンドを実行します。

```
# localcli system wbem set -e 0
```

```
[root@nec-esx-ng:~] localcli system wbem set -e 0
```

5. CIM エージェントを再度有効にするには、次のコマンドを実行します。

```
# localcli system wbem set -e 1
```

```
[root@nec-esx-ng:~] localcli system wbem set -e 1
```

以上で有効化手順は完了です。

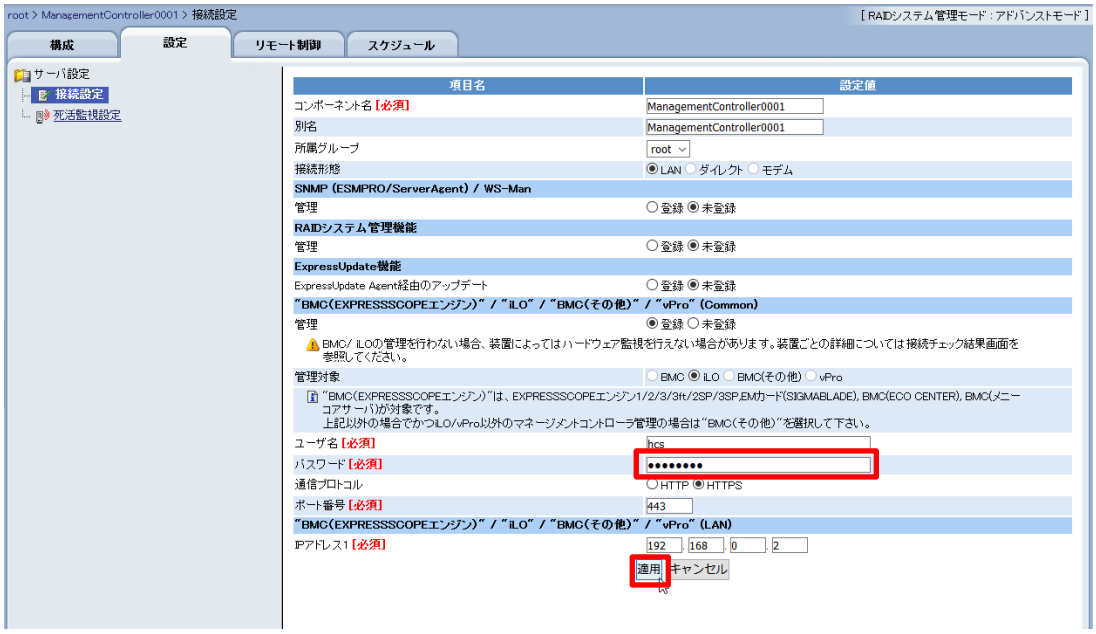
1. 5.6 節の手順 1～4 を参照して、ESMPRO/ServerManager にログインし、クラシックモードを開きます。

2. パスワードを変更したコンポーネントの設定画面を開き、[編集]をクリックします。

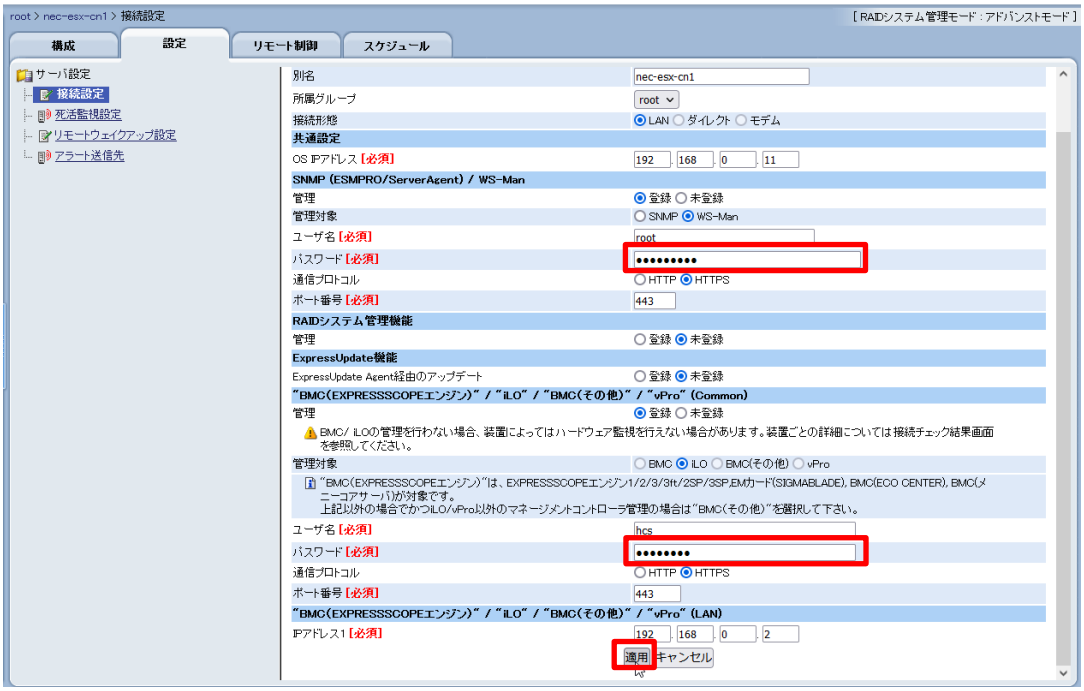
※ サーバ診断カルテの利用状況によっては、コンポーネント名が異なる場合があります。

※ 設定画面が表示されない場合は、クラシックモードを閉じ、装置一覧画面からパスワードを変更したサーバのコンポーネント名をクリックしてください。

3. 変更後の BMC のパスワードを入力し、[適用]をクリックします。



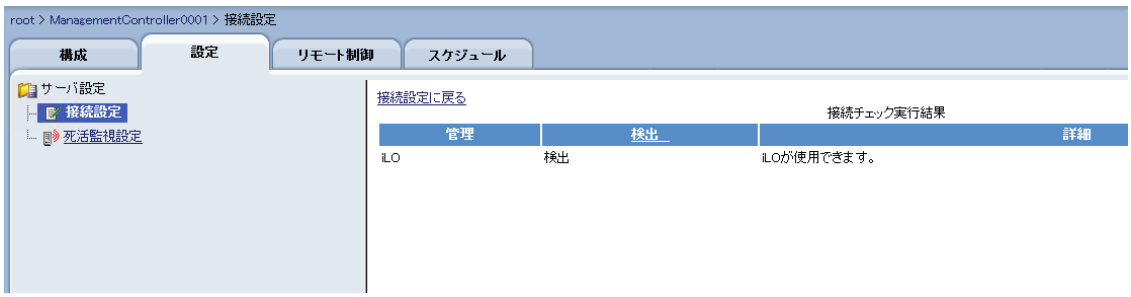
※ サーバ診断カルテを利用している場合は、ESXi(WS-Man)の root パスワードも変更が必要になります。



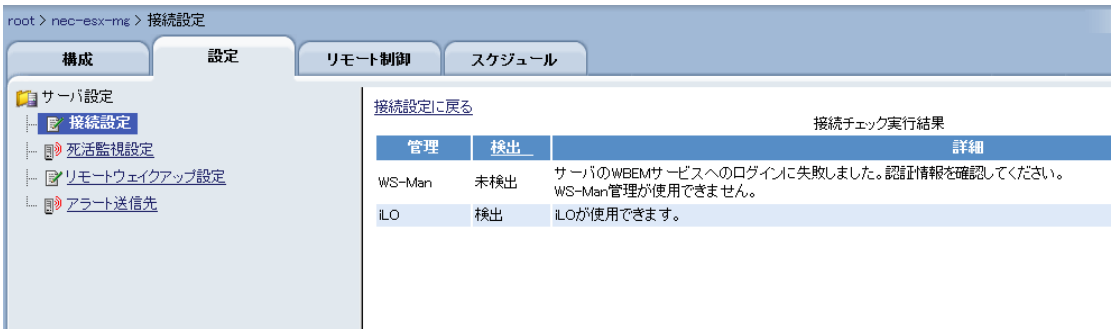
4. 以下のダイアログが表示されますので、[OK]をクリックします。

5. 設定画面に戻りますので、[接続チェック]をクリックします。

6. 「検出」「iLO が使用できます。」の結果が表示されることを確認してください。



※ サーバ診断カルテを利用している環境では、接続チェックの結果 WS-Man が「未検出」となる場合があります。5.9 節の《補足》を参照してリモートアクセスがロックアウトされているかを確認し、①から③の手順を実施して管理エージェントの再起動を実施したうえで、再度本節の手順 5 を実施してください。



《参考》

本節の冒頭にある《参考》で SLP サービスのルールセットを有効化した場合は、登録情報の更新後に以下の無効化手順を実施してください。

- SLP サービスのルールセット無効化手順

1. 起動した SLP サービスのルールセットを停止します。

```
# /etc/init.d/slpd stop
```

```
[root@nec-esx-mg:~] /etc/init.d/slpd stop
Stopping slpd
```

2. ファイアウォールで SLP サービスのルールセットを無効にします。

```
# esxcli network firewall ruleset set -r CIMSLP -e 0
```

```
[root@nec-esx-mg:~] esxcli network firewall ruleset set -r CIMSLP -e 0
```

3. SLP サービス自動起動を無効にします。

```
# chkconfig slpd off
```

```
[root@nec-esx-mg:~] chkconfig slpd off
```

以上で無効化手順は完了です。

以上で登録情報の更新は完了です。

パスワードを変更した他のノードに対しても、同様の作業を実施してください。

5.11 サーバ診断カルテの登録情報の更新

本節は、サーバ診断カルテを利用している場合のみ実施してください。

ゲスト OS 収集タスクの認証情報および ESXi、管理 VM にログインするための接続認証情報の更新を実施します。

1. 管理 VM にてコマンドプロンプトを管理者権限で起動し、「インストールフォルダ¥setting」に移動します。

   ※ インストールフォルダのデフォルトは「C:¥Program Files¥MIOTMG」です。

```
C:¥Program Files¥MIOTMG¥tool>cd C:¥Program Files¥MIOTMG¥setting
```

2. 以下のコマンドを実行し、ゲスト OS 収集タスクの認証情報の更新を実施します。

```
# MIOT_REG_USER.exe /u Administrator /p <変更後の管理 VM のパスワード>
```

```
C:¥Program Files¥MIOTMG¥setting>MIOT_REG_USER.exe /u Administrator /p P@ssw0rd2
User and password updates (GuestOS collection) were successful.
```

3. 以下のコマンドを実行し、ESXi と管理 VM の認証情報の更新を実施します。

```
# MIOT_MNG_AUTH.exe /i <ESXi サーバの IP アドレス> /u root /p <変更後の ESXi サーバの root パスワード>
```

```
C:¥Program Files¥MIOTMG¥setting>MIOT_MNG_AUTH.exe /i 192.168.0.50 /u root /p P@ssw0rd2
```

```
# MIOT_MNG_AUTH.exe /i <管理 VM の IP アドレス> /u Administrator /p <変更後の管理 VM のパスワード>
```

```
C:¥Program Files¥MIOTMG¥setting>MIOT_MNG_AUTH.exe /i 192.168.0.51 /u Administrator /p P@ssw0rd2
```

上記コマンド実行後、「Overwrite Authent ication～」と表示されますので、y と入力し、実行してください。

```
Overwrite Authentication Information of IP address(192.168.0.50). Are you sure (Y/N)? y
```

4. 以下のコマンドを実行し、登録内容の確認を実施します。

```
# MIOT_MNG_AUTH.exe /v
```

```
C:¥Program Files¥MIOTMG¥setting>MIOT_MNG_AUTH.exe /v
IP Address     : "192.168.0.50"
  User         : "root"
IP Address     : "192.168.0.11"
  User         : "root"
IP Address     : "192.168.0.12"
  User         : "root"
IP Address     : "192.168.0.13"
  User         : "root"
IP Address     : "192.168.0.51"
  User         : "Administrator"
```

5.12 保守アカウントのパスワード変更

本節では、保守アカウントのパスワード変更について記載します。

5.12.1 管理 VM の保守アカウントのパスワード変更

5.5 節の手順を参照し、保守アカウントのパスワードを変更します。
手順 4 では保守アカウントとして使用しているユーザを選択してください。

5.12.2 vCenter Server の保守アカウントのパスワード変更

1. Windows PC でリモートデスクトップ接続(mstsc)を起動し、ヒアリングシートに記載されている「管理 VM」の IP アドレスを入力し、管理 VM に保守アカウントでログインします。
   (IP アドレス例: 192.168.100.10:3389)

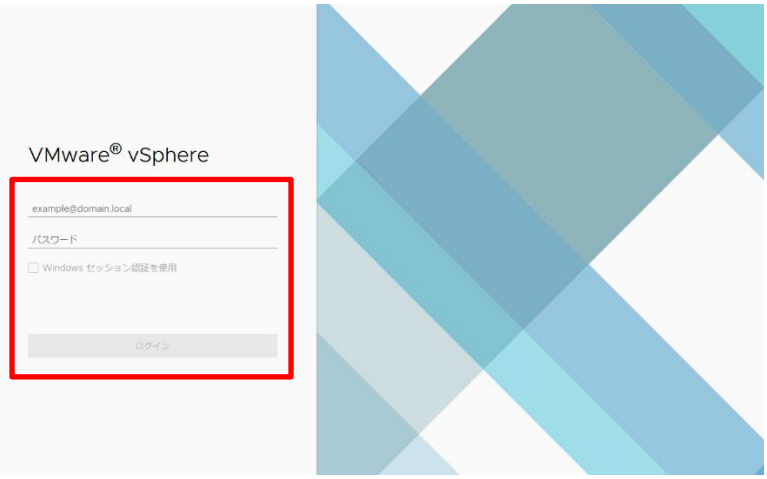
2. 管理 VM 上で Web ブラウザを起動します。

3. Web ブラウザのアドレス欄に以下の URL を入力します。

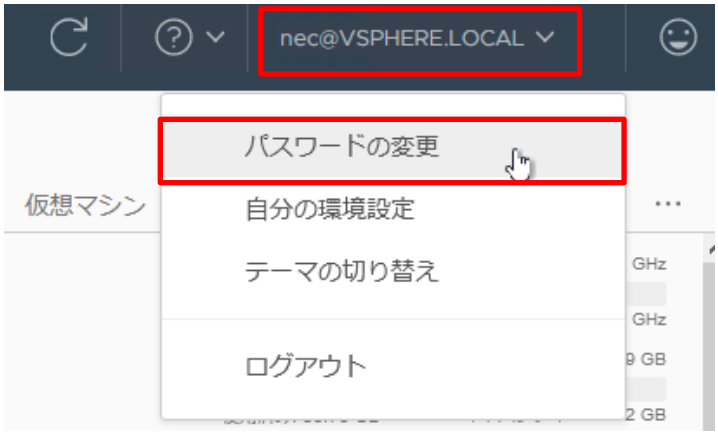
   http://<vCSA のホスト名>/ui

   ※ 「接続がプライベートではありません」画面が表示された場合は、[詳細設定]をクリックし表示された画面で、[<IP アドレスまたは FQDN>に進む(安全ではありません)]クリックしてください。

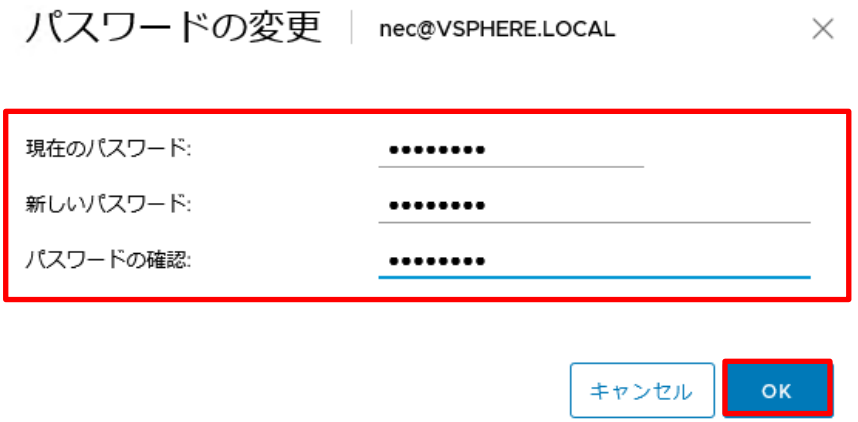
4. 下図のようにログイン画面が表示されたら、保守アカウントでログインします。



5. ログインしたら、画面右上のアカウント名をクリックし、[パスワードの変更]をクリックします。



6. 現在のパスワードと新しいパスワード、パスワードの確認を入力したら OK をクリックします。



※ パスワードの要件は、初期パスワード通知書の「1.2 パスワード要件」を参照ください。

7. パスワード変更後、VMware vSphere Client をログアウトして、ブラウザを閉じ、管理 VM からログオフし、リモートデスクトップ接続を終了してください。

6 注意制限事項

6.1 iLO Security について

iLO Security において、「IPMI/DCMI Over LAN」と「セキュアブート(Secure Boot)」はステータスが「リスク(Risk)」になっていますが、「IPMI/DCMI Over LAN」は「有効(Enabled)」、「セキュアブート」は「無効(Disabled)」の状態にしておいてください。

商標について

EXPRESSBUILDER と ESMPRO は日本電気株式会社の登録商標です
Microsoft Windows, Windows Server, Microsoft Edge は米国 Microsoft Corporation の米国 およびその他の国における登録商標または商標です。
VMware、VMware vSphere、VMware ESXi、および VMware ロゴは、米国およびその他の地域における VMware, Inc.の登録商標または商標です。
その他、記載の会社名および商品名は各社の商標または登録商標です。

本書に関する注意と補足

1. 本書の内容の一部または全部を無断転載することは禁止されています。
2. 本書の内容に関しては将来予告なしに変更することがあります。
3. NEC の許可なく複製、改変などを行うことはできません。
4. 本書の内容について万全を期して作成いたしましたが、万一ご不審な点や誤り、記載漏れなどお気づきのことがありましたら、本書の問い合わせ先にご連絡ください。
5. 運用した結果の影響については、4 項に関わらず責任を負いかねますのでご了承ください。

MEMO

別紙　受入検査チェックシート

検査日＿＿＿＿＿＿＿＿＿＿＿＿

ご担当＿＿＿＿＿＿＿＿＿＿＿＿

	項目	チェック	確認者	メモ
1	構成品の確認	□		
2	本製品の設置	□		
3	ネットワーク装置への接続	□		
4	電源の接続	□		
5	管理ノードの電源オン	□		
6	Windows PCの準備	□		
7	Windows PCから管理VMに接続	□		
8	DNS疎通確認	□		
9	VMware vCenter Serverへの接続確認	□		
10	クラスタノード、Witnessノードの電源オン	□		
11	VMware vCenter Server上での機器確認	□		
12	隔離IPの到達確認	□		
13	NTPの動作確認	□		
14	クラスタノード、Witnessノードのメンテナンスモード解除	□		
15	vSANクラスタ全台同時停止時のbuild-inツールの実行	□		
16	クラスタメンバの更新の有効化	□		
17	vCLSのRetreatモードの無効化	□		
18	vSphereの可用性設定	□		
19	vSANストレージプロバイダの同期	□		
20	VMware vSAN状態の確認(健全性確認)	□		
21	NEC Hyper Converged System Consoleの動作確認	□		
22	エクスプレス通報サービスの開局手続き	□		
23	サーバ診断カルテの開局手続き	□		