HCI システムインストールサービス (for VMware vSAN) スタートアップガイド

2024 年 7 月
第 2.0 版
日本電気株式会社

文書番号：NHS-E-285-020

目次

1 本ガイドについて

この度は、HCI システムインストールサービス(for VMware vSAN)をご利用いただき、誠にありがとうございます。
本書は、HCI システムインストールサービスによって構築された Hyper Converged Infrastructure(HCI)を、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、1.1 章の問い合わせ窓口までご連絡ください。

1.1 お問い合わせ先

問題が解決しない場合、HCI システムインストールサービス(for VMware vSAN)の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・マネージドサービス事業部門
HCI システムインストールサービス担当

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。

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

1.2 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
Hyper Converged Infrastructure (HCI)	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。
HCI システムインストールサービス(for VMware vSAN) (HCI システムインストールサービス)	お客様がすぐに HCI 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。
管理ノード	HCI 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	HCI 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	HCI 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。HCI では仮想アプライアンスの Witness ノードを使用する。
管理 VM	管理ノードまたは vSAN クラスタ上で動作する、Windows Server の仮想マシン。HCI の管理や、ESMPRO/Server Manager 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。HCI 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。HCI 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スイッチ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。HCI 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。HCI の動作に必要。
Administrator (hcsadmin)	管理者を示す英単語。HCI 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	HCI 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。

1.3 本書で参照するパラメータについて

クラスタノードの IP アドレス、vCSA の FQDN など、本書で参照するパラメータは、
HCI システムインストールサービス (for VMware vSAN) 製品組み立て仕様書（SG 仕様書）の
「StartupGuide 参照値一覧」シートに記載された値を参照します。SG 仕様書はクラスタノード 1 号機に同封されます。(2.1 章参照)

例 1）
本書内の表記：**<vCSA - FQDN>**
参照先：SG 仕様書の「StartupGuide 参照値一覧」シートの項目が「vCSA - FQDN」の値

例 2）
本書内の表記：**<クラスタノード － 管理用 NW － IP アドレス>**
参照先：SG 仕様書の「StartupGuide 参照値一覧」シートの項目が「クラスタノード(N 台目) － 管理用 NW － IP アドレス」の値
※ (N 台目)の部分は、操作対象のクラスタノードに応じて読み替えてください。
※ 本書内で **<クラスタノード(1 台目) － 管理用 NW － IP アドレス>** のように操作対象が記載されている場合は、操作対象のノードのみ実施してください。

パスワードについては、HCI システムインストールサービス (for VMware vSAN) 初期パスワード通知書(初期パスワード通知書)を参照します。初期パスワード通知書もクラスタノード 1 号機に同封されます。

2 事前準備

2.1 ご用意いただくもの

本書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。クラスタノード 1 号機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 Express 5800 サーバ
  - 同時購入いただいたオプション製品等
  - HCI 構成品表 (クラスタノード 1 号機に同封)
  - HCI システムインストールサービス (for VMware vSAN) 製品組み立て仕様書（SG 仕様書）（クラスタノード 1 号機に同封）
  - 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 Infrastructure スタートアップガイド、クラスタノード 1 号機に同封に同封)
  - HCI システムインストールサービス(for VMware vSAN) 初期パスワード通知書 (クラスタノード 1 号機に同封)
  - 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)

- vCenter Server、ESXi、vSAN ライセンス
- Windows Server 2022 ライセンス(管理 VM ありの構成の場合)

- その他
  - 下記要件を満たす作業端末(Windows PC)
    - Windows 10, Windows Server 2016, 2019, 2022
    - LAN インタフェース、LAN ケーブル等(管理用ネットワーク接続用、有線必須）
    - SSH クライアント(Tera Term で動作を確認済み）
    - Microsoft Edge
    - DNS での名前解決が可能であること
  - 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。
    - 管理ノード、クラスタノードの開局キー

- (本書対象外、ご参考)
  - 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)
  - ディスプレイ、キーボード (LCD コンソールユニット等も可)
  - NTP サーバ、DNS サーバ

重要

HCI システムインストールサービスで構築した HCI をご利用いただく場合は、DNS サーバから HCI 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。サーバ、ネットワークスイッチ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、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、HCI 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

本章は受入確認手順を示します。
HCI をご利用頂くためには、下記 19 点の実施をお願いいたします。

1. 構成品の確認
2. 各ノード(サーバ)の設置
3. ネットワーク装置への接続
4. 電源の接続
5. 作業端末の準備
6. 管理ノードの電源オンと vCenter Server への接続確認
7. クラスタノードの電源オンと vCenter Server への接続確認
8. Witness の電源オン
9. vCenter Server 上での機器確認
10. 隔離 IP の到達確認
11. NTP の動作確認
12. Witness ノードのメンテナンスモード解除
13. vSAN サービスの再起動
14. vSAN ストレージプロバイダの同期
15. TPM のリカバリキーのバックアップ
16. vSAN 状態の確認(健全性確認)
17. 管理 VM の起動と接続確認
18. 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)
19. 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

HCI の構成物を示す「HCI 構成品表(以下構成品表)」は、クラスタノード 1 号機の梱包箱の内側に貼り付けられている、「HCI システムインストール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

HCI システムインストールサービスでの構築に使用したサーバと、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。梱包されたサーバが到着されましたら、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、構築したサーバ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》

HCI システムインストールサービスと同時にご注文いただいた、本サービス以外の製品(例: LCD コンソールユニット、Windows Server CAL など)は、3.2.1 章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本サービス以外の製品は、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

各ノード(サーバ)、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 各ノード(サーバ)の設置

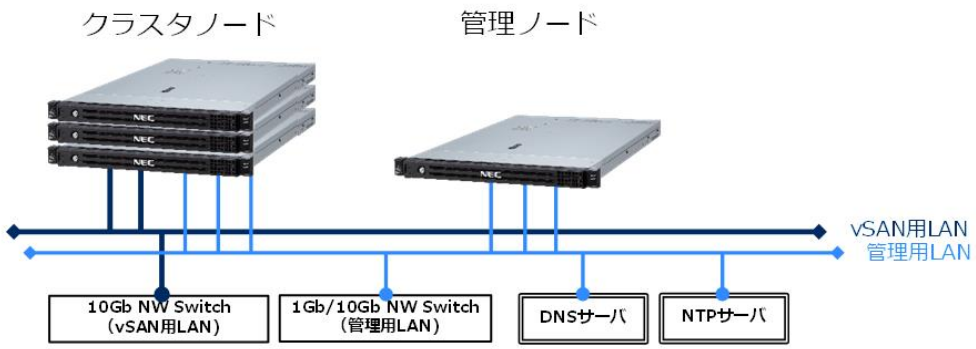
HCI を使用する前に、19 インチラックなど安全に固定できる器具に搭載し、電源を接続する必要があります。本書、または NEC Web サイトから入手できる R120j-1M/2M の製品マニュアル(ユーザーズガイド一式)を元に、設置を行ってください。

3.4 ネットワーク装置への接続

HCI の各ノード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」、「管理ノードの設定」に従ってネットワークスイッチと各ノードを正しく接続してください。

HCI のご利用には、DNS サーバから HCI を構成する 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 3.6.3 章で確認を行います。

接続例



3.5 電源の接続

すべてのノード、ネットワークスイッチの設置が完了後、本書、または NEC Web サイトから入手できる R120j-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。ノードの電源をオンにする前にネットワークスイッチの電源をオンにしてください。

3.6 作業端末の準備

本章では、作業端末のネットワーク接続および設定について記載します。
作業端末では DNS での名前解決、およびシステムとの時刻同期が必要なため、DNS クライアント、NTP クライアントの設定と確認を行います。

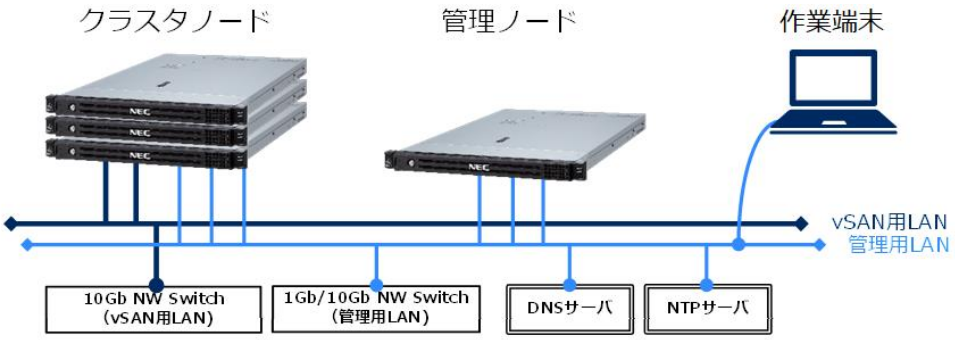
3.6.1 管理用ネットワークへの接続

作業端末を、管理用ネットワークに接続します。

1. 作業端末のネットワーク設定を、管理用ネットワーク上の各ノードに接続できるよう、変更します。

2. 作業端末を管理用ネットワークに接続してください。

接続例



《注意》

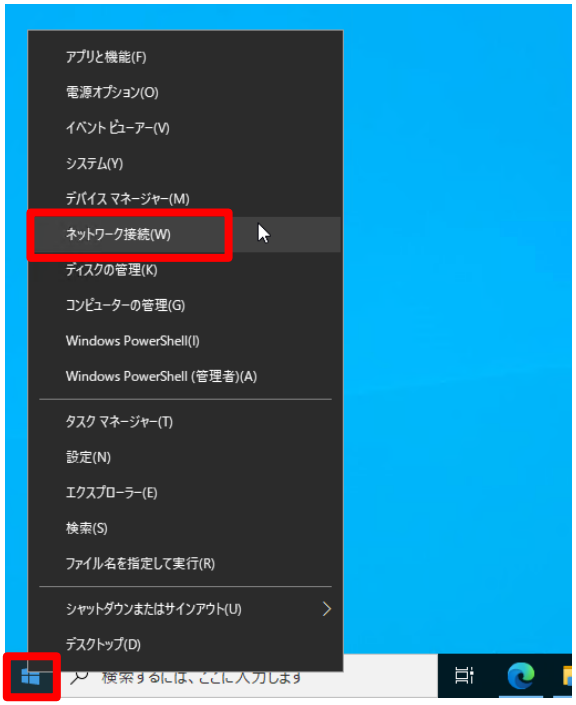
作業端末に設定する IP アドレスは、HCI の各ノードや管理用ネットワークで使われていない IP アドレスを割り当ててください。重複した IP アドレスを設定した場合、システムの動作に影響を与えることがあります。

3.6.2 DNS クライアントの設定

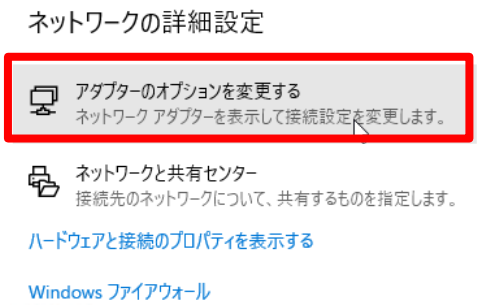
作業端末の DNS クライアントの設定を行います。

※ 本手順は一例です。ご使用の環境によって手順や設定値が異なる場合があります。

1. スタートボタンを右クリックし、[ネットワーク接続]をクリックします。

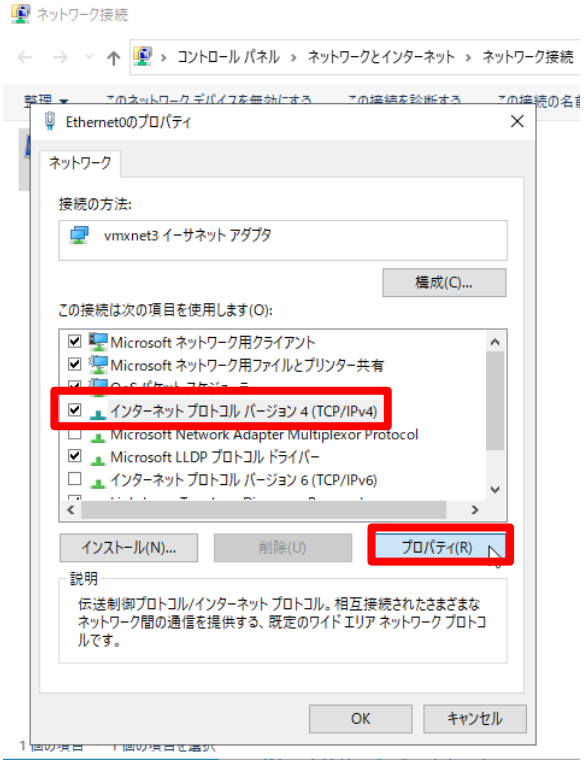


2. [アダプターのオプションを変更する]をクリックします。



3. 設定を行うネットワークのアイコン(本書では「Ethernet0」)を右クリックして表示されるメニューから[プロパティ]を選択します。

4. プロパティ画面で [インターネット プロトコル バージョン4(TCP/IPv4)]→[プロパティ]をクリックします。

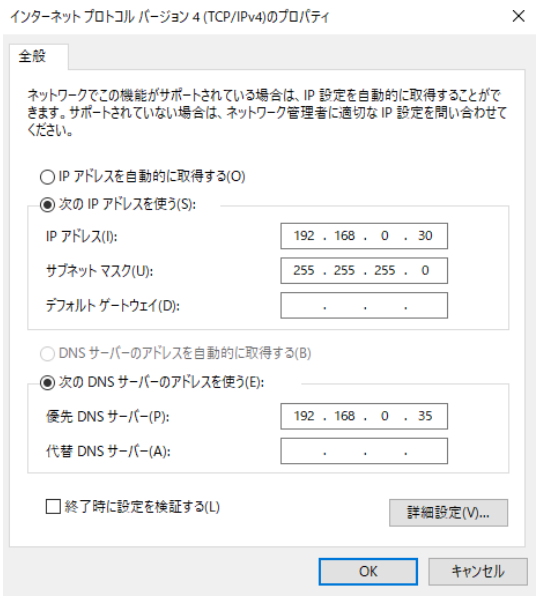


5. [次の DNS サーバーのアドレスを使う]の優先 DNS サーバーに以下のアドレスを入力します。

<プライマリ DNS サーバ - IP アドレス>

6. 必要に応じて代替 DNS サーバーに以下のアドレスを入力し、[OK]をクリックします。

<セカンダリ DNS サーバ - IP アドレス>



3.6.3 DNS の疎通確認

DNS の疎通確認を実施します。

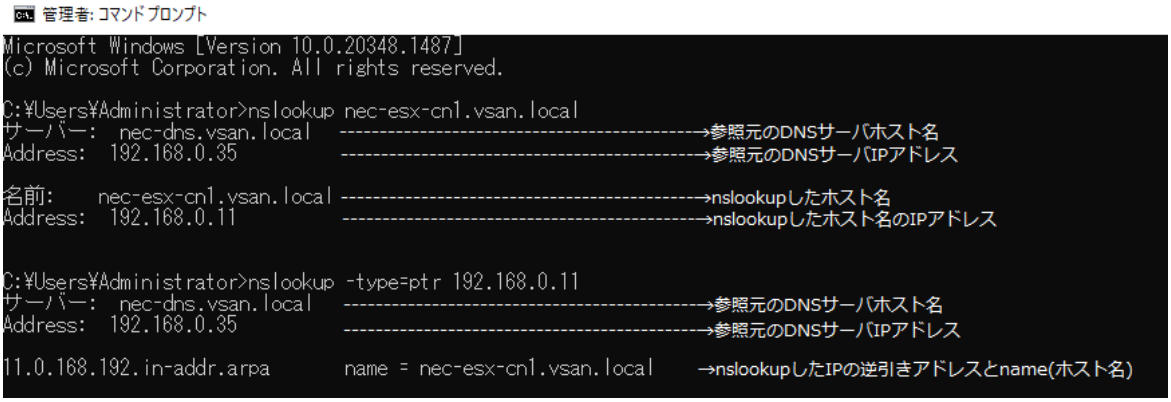
1. 作業端末上で、コマンドプロンプト(cmd を起動します。)
2. コマンドプロンプト上で以下のコマンドを実行し、作業端末から SG 仕様書の「StartupGuide 参照値一覧」シートに記載されている、すべてのクラスタノード, vCenter Server Appliance(vCSA)の FQDN、IP アドレスを正引き、逆引き可能であることを確認してください。
   ご使用の構成にあわせて、管理ノード、管理 VM、Witness ノードの確認も実施してください。

   - 正引き確認：nslookup *FQDN*

     例) nslookup nec-esx-cn1.vsan.local

   - 逆引き確認：nslookup -type=ptr *IP アドレス*

     例) nslookup -type=ptr 192.168.0.11



3. 正引き、逆引き結果が SG 仕様書の FQDN、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。

《注意》

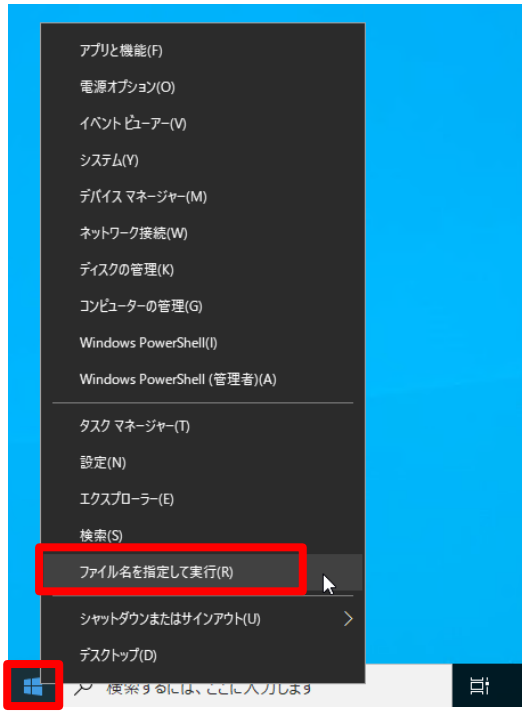
正引き/逆引きができない場合、3.6.4 章以降の手順を実施しないでください。
DNS サーバに SG 仕様書に記載された各ノードの FQDN、IP アドレスが登録されていること、ネットワークケーブルが正しく接続されていることを確認してください。

3.6.4 NTP クライアントの設定

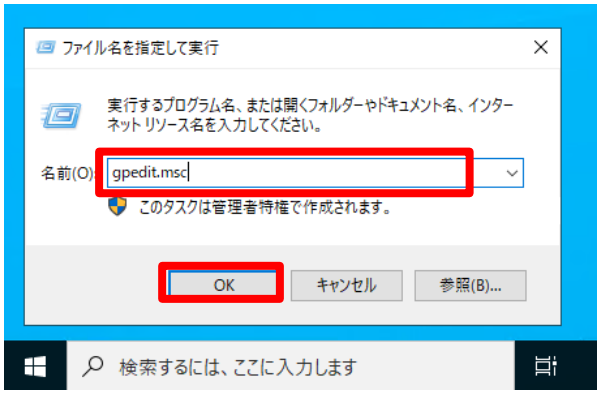
作業端末の NTP クライアントの設定を行います。

※ 本手順は一例です。ご使用の環境によって手順や設定値が異なる場合があります。

1. スタートボタンを右クリックし、[ファイル名を指定して実行]をクリックします。

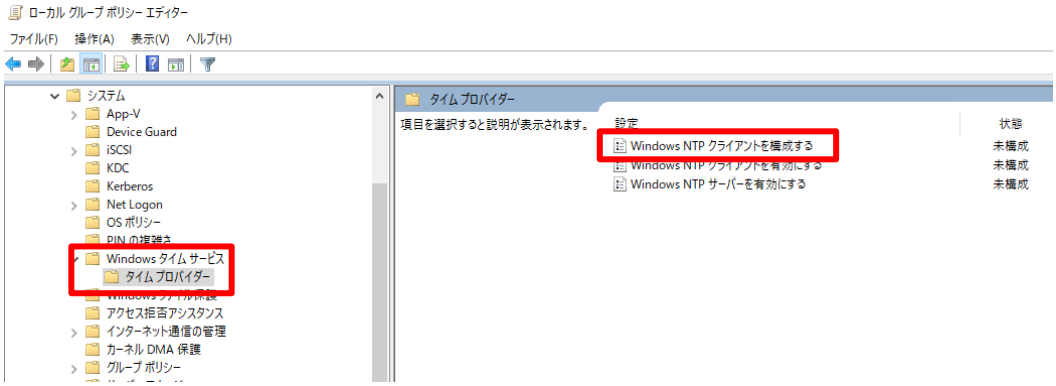


2. [名前]欄に「gpedit.msc」と入力し、[OK]をクリックします。

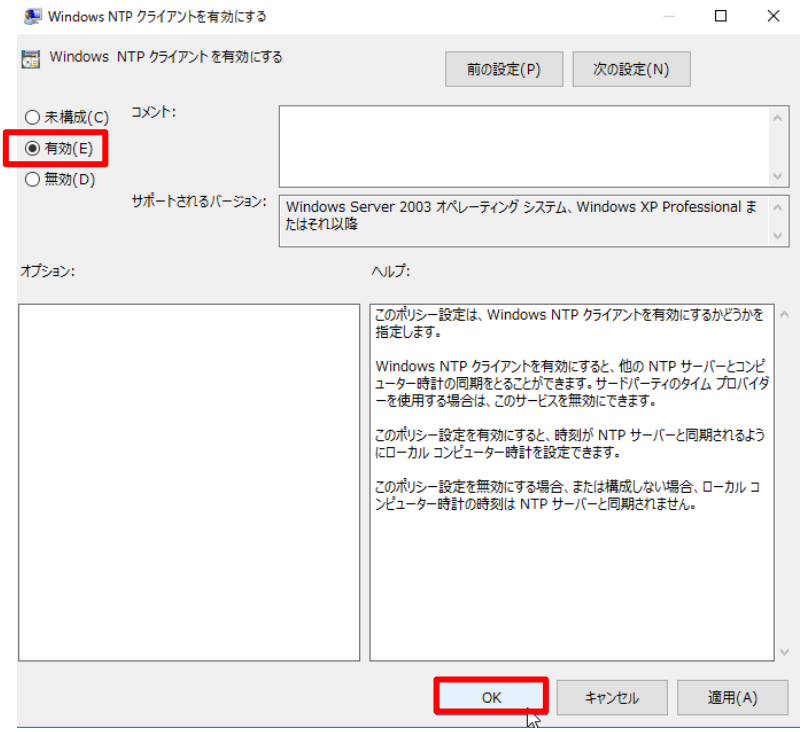


3. [ローカル コンピューター ポリシー]→[コンピューターの構成]→[管理用テンプレート]→[システム]→[Windows タイムサービス]→[タイムプロバイダー]をクリックします。

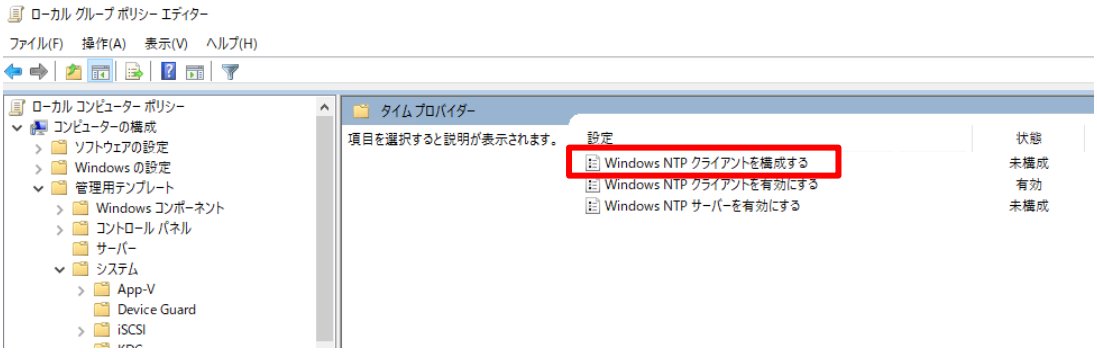
   [Windows NTP クライアントを有効にする]を右クリックし、[編集]を選択します。



4. [有効]にチェックを付け、[OK]をクリックします。



5. [Windows NTP クライアントを構成する]を右クリックし、[編集]を選択します。



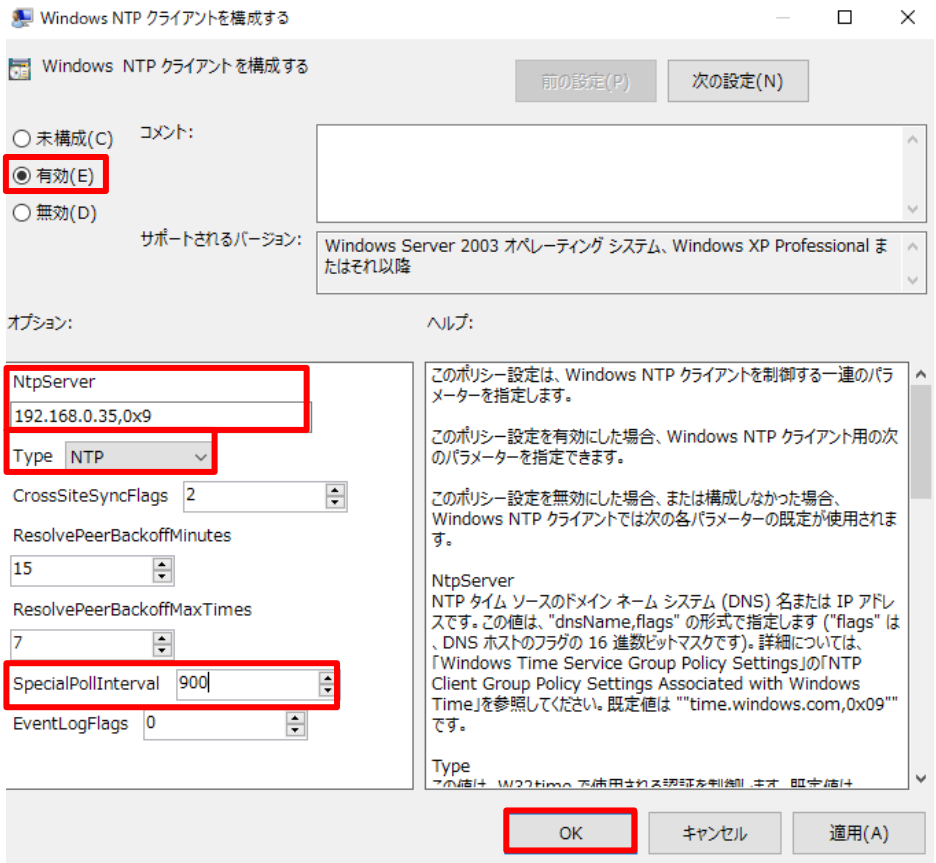
6. [有効]を選択し、[NtpServer]欄に以下の値を入力します。

[**<NTP サーバ - IP アドレス>**,0x9]

NTP サーバが複数ある場合は下記のように半角スペースで区切って[NtpServer]欄に入力します。

[**<NTP サーバ - IP アドレス>**,0x9 **<NTP サーバ 2 - IP アドレス>**,0x9]

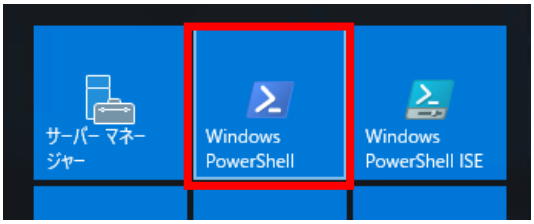
[Type]欄で[NTP]を選択し、[SpecialPollInterval]のパラメータを[900]に変更し、[OK]をクリックします。
その後グループポリシーエディターを閉じます。



3.6.5 NTP の同期確認

NTP の同期確認を実施します。

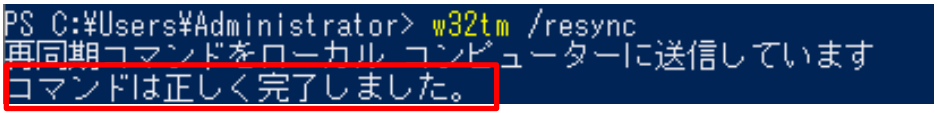
1. スタートメニューから[Windows PowerShell]をクリックし、PowerShell を起動します。



2. 下記コマンドを実施し、NTP サーバとの時刻同期を手動で実施します。

```
> w32tm /resync
```

「コマンドは正しく完了しました。」と表示されることを確認します。
時刻同期が失敗している場合にはもう一度上記コマンドを実施してください。

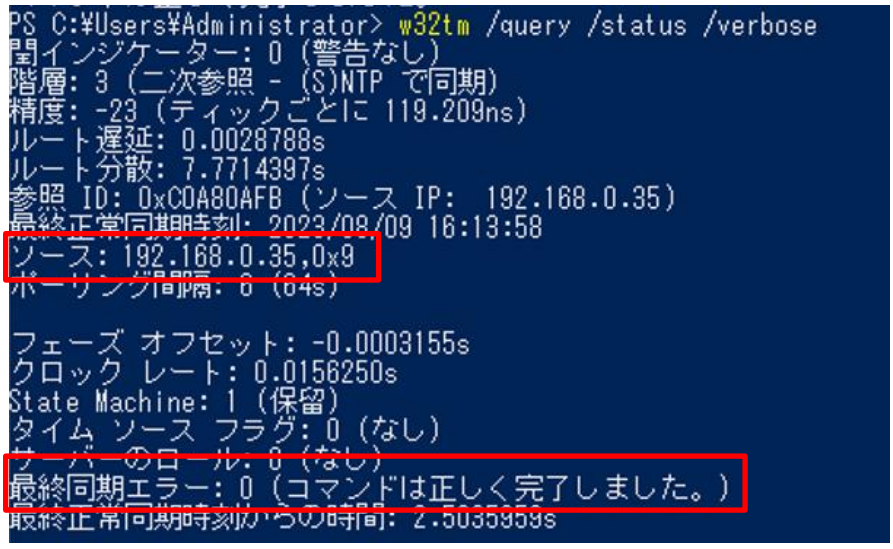


3. 下記コマンドを実施し、時刻同期の状態を確認します。

```
> w32tm /query /status /verbose
```

ソースが< **NTP サーバ - IP アドレス**>の値になっていることを確認してください。
最終同期エラーが 0 になっていることを確認してください。

※ 3.6.4 章で NTP サーバを複数設定している場合は、ソースにいずれかの値が表示されます。



《注意》

<u>最終同期エラーが 0 になっていることが確認できない場合、3.7 章以降の手順を実施しないでください。</u>

4. ウィンドウ右上の[×]をクリックし、PowerShell を閉じます。

3.7 管理ノードの電源オンと vCenter Server への接続確認

本章は、管理ノードがある構成の場合に実施します。

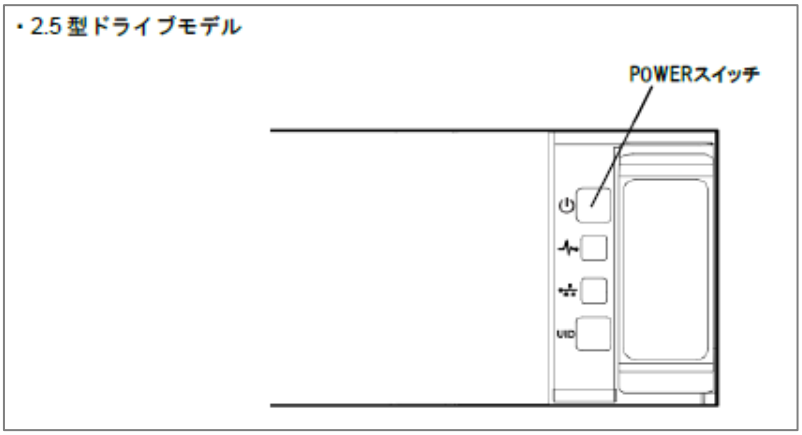
管理ノードがない構成の場合は、3.8 章に進んでください。

1. 管理ノード(サーバ)の電源をオンにします。

電源をオンにする方法は、以下を参照ください。

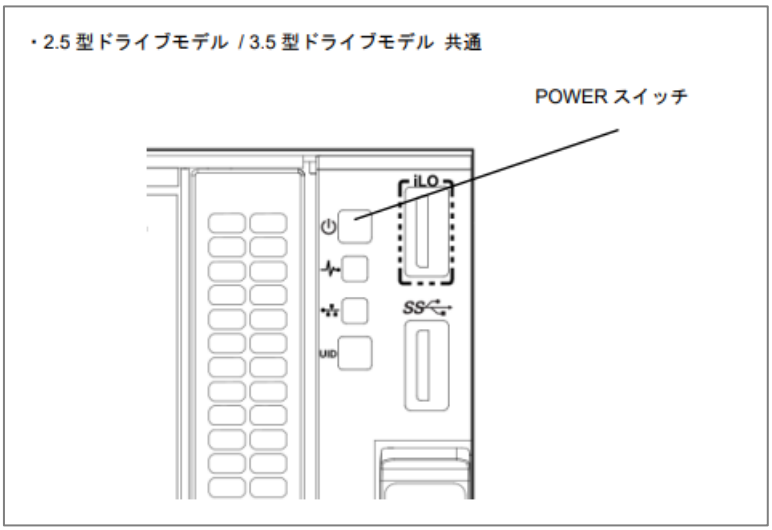
R120j-1M の電源オン:

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。



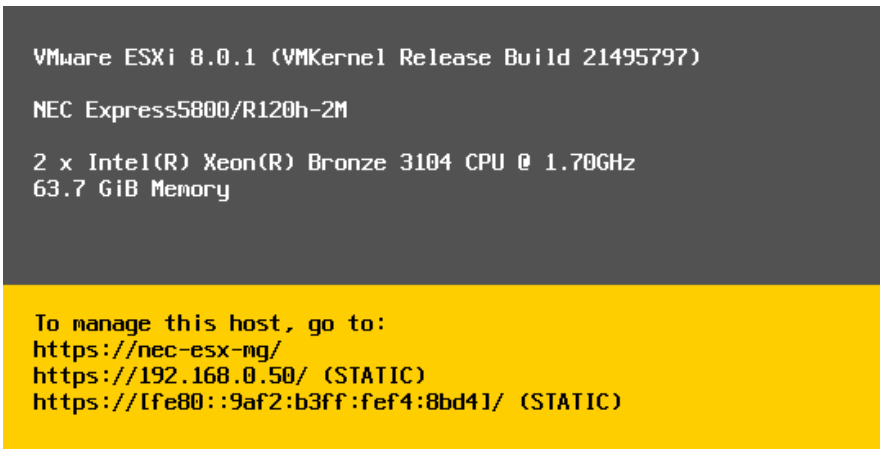
R120j-2M の電源オン:

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、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。

2. 作業端末上で Web ブラウザを起動し、vCenter Server に接続します。
下記の URL にアクセスします。

https://<**vCSA - FQDN**>/ui

例）https://nec-vcsa.vsan.local/ui

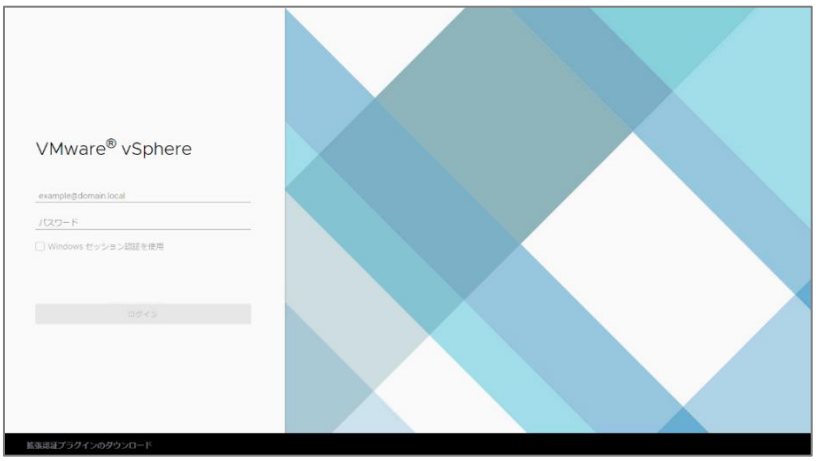
※ 「接続がプライベートではありません」画面が表示された場合は、[詳細設定]をクリックし表示された画面で、[*IP アドレスまたは FQDN* に進む(安全ではありません)]クリックしてください。

3. 下記図のように 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: <**vCSA - SSO ユーザ- 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」

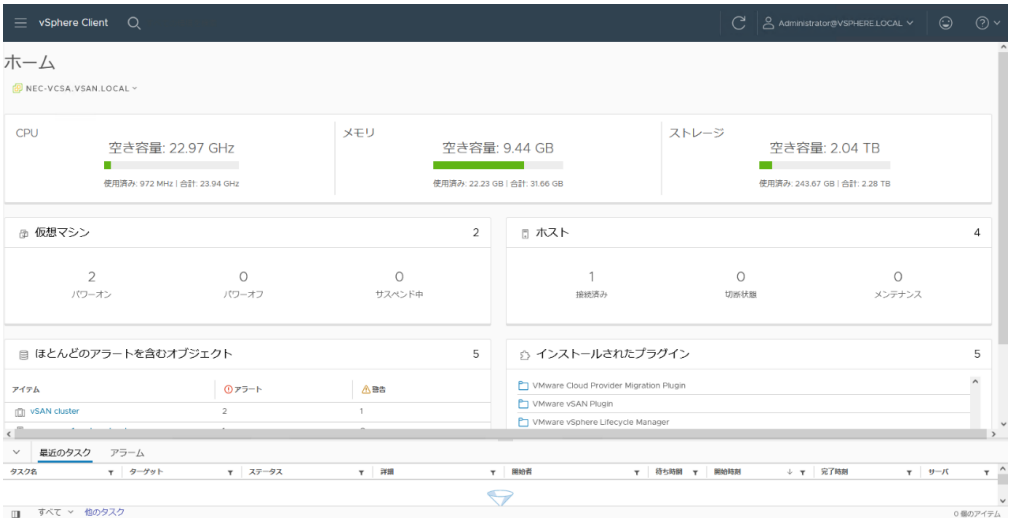


重要 vCenter Server に接続できない時は、まず以下を確認して下さい。

1.	vCenter Serverに接続する情報に誤りがありませんか？ （<**vCSA - FQDN**>を再度確認ください）
2.	作業端末上のWebブラウザから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.	vCenter Serverは起動していますか？ (管理ノードの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。

解決しない場合は、御手数ですが、1.1 章の HCI システムインストールサービス窓口までご連絡をお願いいたします。

4. 正常にログインが完了すると、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 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。



3.8 クラスタノードの電源オンと vCenter Server への接続確認

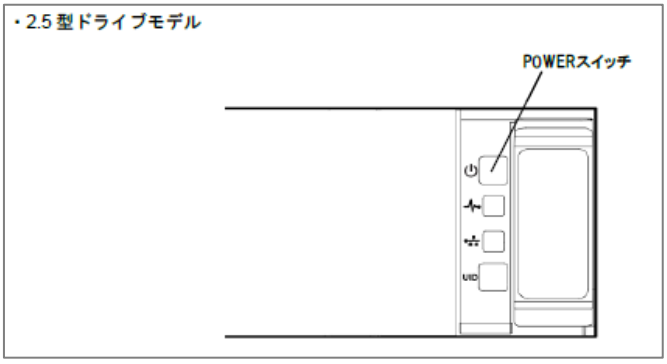
本章では、クラスタノードの電源オンと vCenter Server への接続確認を実施します。

3.8.1 クラスタノードの電源オン

すべ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。
電源をオンにする方法は、以下を参照ください。

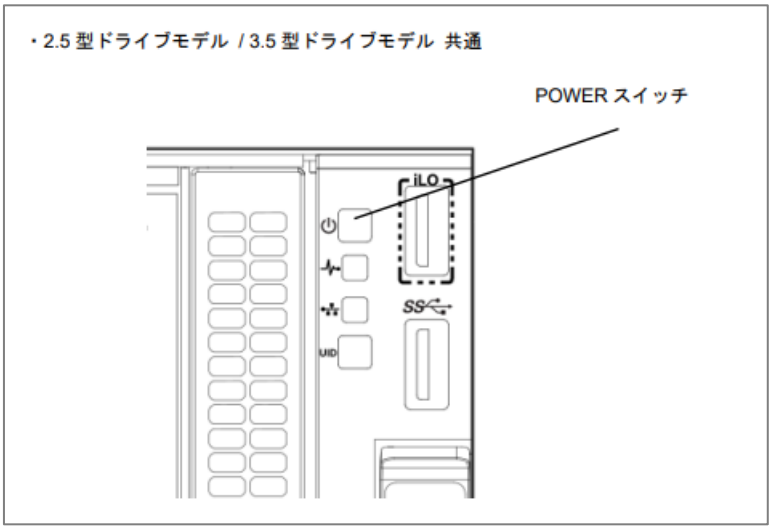
R120j-1M の電源オン:

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。



R120j-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。



3.8.2 vCenter Server への接続確認

電源をオンにしたクラスタノードと仮想マシンの状態を確認します。

2Node 構成の場合は、本章は不要です、3.9 章に進んでください。

3Node 以上の構成で、管理ノードがある場合も本章は不要です、3.10 章に進んでください。

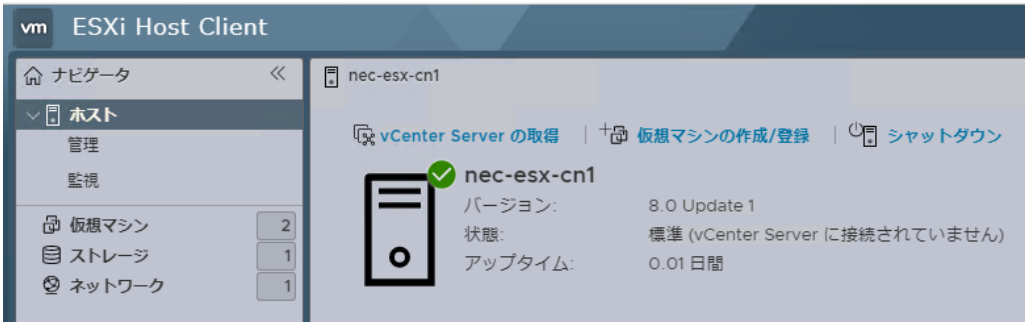
1. 作業端末にて Web ブラウザを起動し、下記 URL でクラスタノードに Host Client で接続してください。

   https://<**クラスタノード(1 台目) – FQDN**>/ui

   または

   https://<**クラスタノード(1 台目) – 管理用 NW – IP アドレス**>/ui

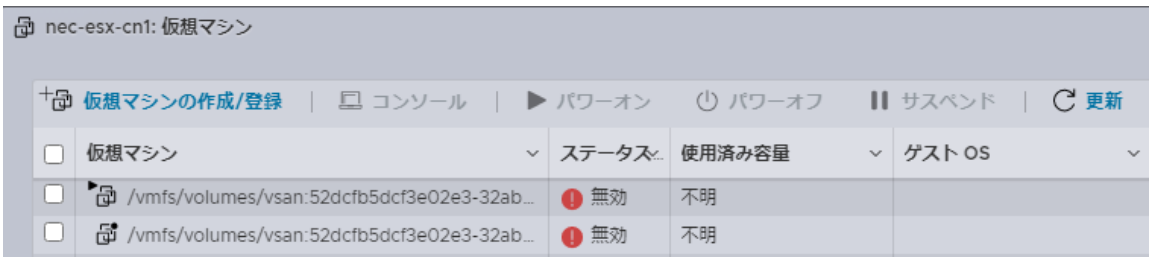
2. クラスタノードのメンテナンスモードが解除され、「ホスト」画面でクラスタノードの状態が「標準」になっていることを確認します。



※ ナビゲータのアイコンがメンテナンスモードのままになっている場合がありますが、ブラウザを更新すると元に戻ります。

3. 「仮想マシン」画面を開き、vCSA 仮想マシンが起動していることを確認します。

※ 仮想マシン名が以下画面のような表示になる場合は、画面下部のタスクが完了していることを確認した後に[更新]をクリックしてください。



4. 作業端末上で Web ブラウザを起動し、vCenter Server に接続します。

   ※ クラスタノードの電源をオンにしてから vCenter Server への接続確認ができるようになるまで、約 20 分の時間を要します。

   下記 URL にアクセスします。

   https://<**vCSA - FQDN**>/ui

   例）<https://nec-vcsa.vsan.local/ui>

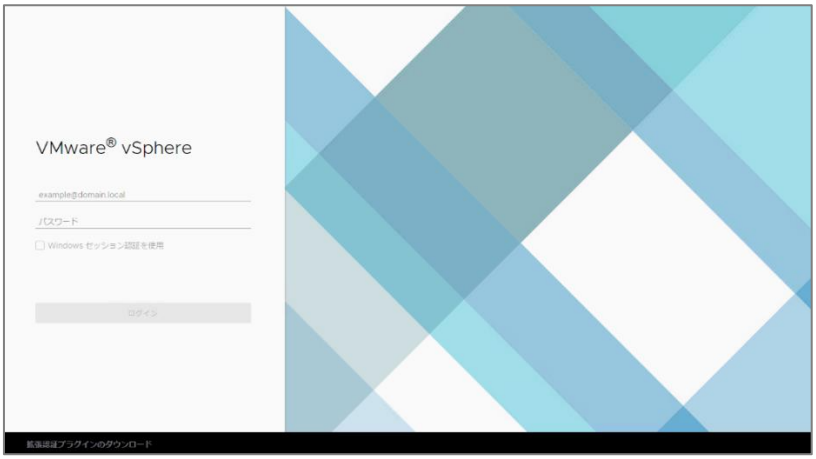
   ※ 「接続がプライベートではありません」画面が表示された場合は、[詳細設定]をクリックし表示された画面で、[*IP アドレスまたは FQDN* に進む(安全ではありません)]クリックしてください。

5. 下記図のように 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: <**vCSA - SSO ユーザ- 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」

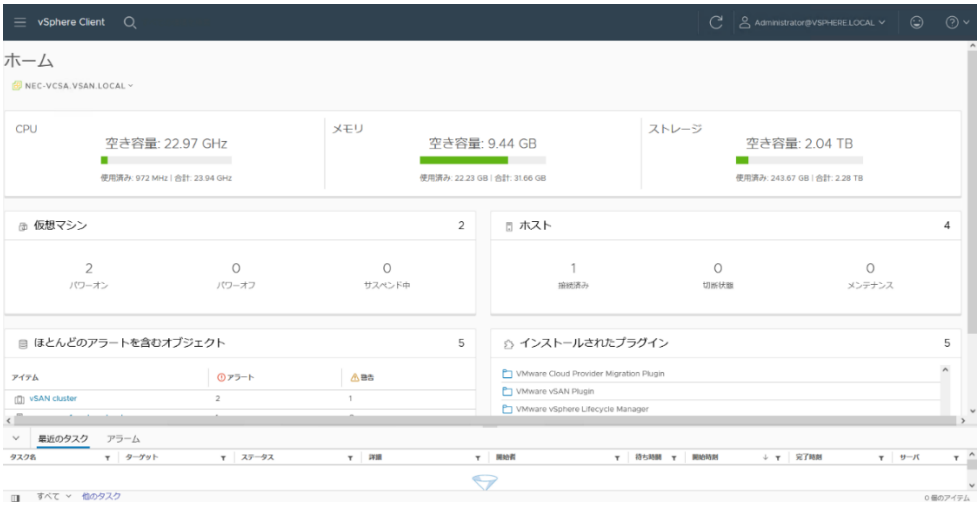


重要 vCenter Server に接続できない時は、まず以下を確認して下さい。

1.	vCenter Serverに接続する情報に誤りがありませんか？ （SG仕様書の<**vCSA - FQDN**>を再度確認ください）
2.	作業端末上のWebブラウザから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.	vCenter Serverは起動していますか？ (vCSAが起動しているクラスタノードの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。

解決しない場合は、御手数ですが、1.1 章の HCI システムインストールサービス窓口までご連絡をお願いいたします。

6. 正常にログインが完了すると、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 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。

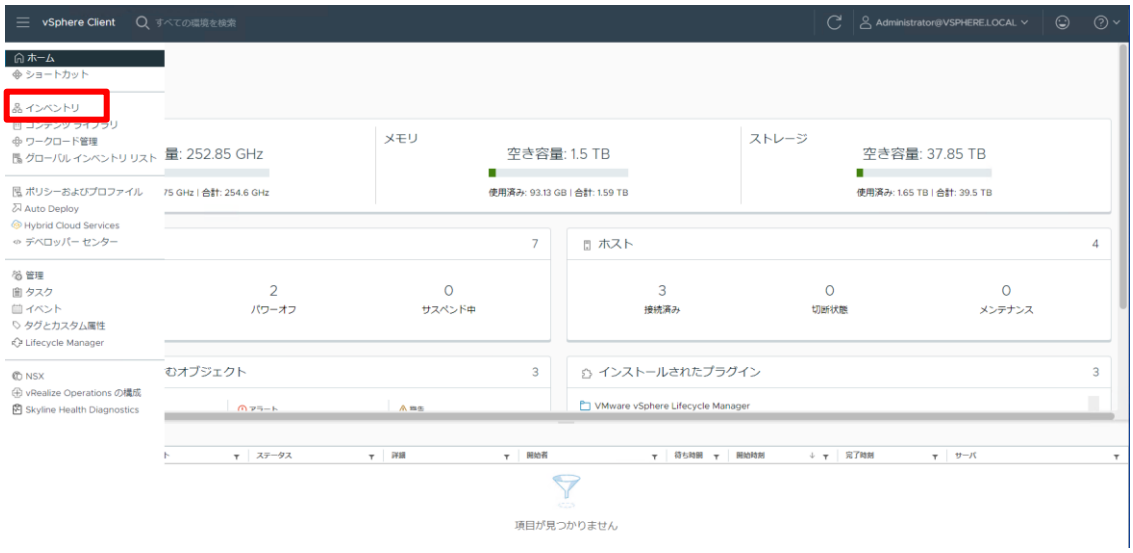


3.9 Witness の電源オン

本章は、2Node 構成の場合に実施します。
該当しない場合は、本章は不要です、3.10 章に進んでください。

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. 3.7 章で接続した 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。



2. Witness ホスト仮想マシンを選択した状態で、画面上部のパワーオンアイコンをクリックします。

3.10 vCenter Server 上での機器確認

vSphere Client のステータスを更新し、vSAN クラスタ、各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 ESXi が起動したことを確認します。

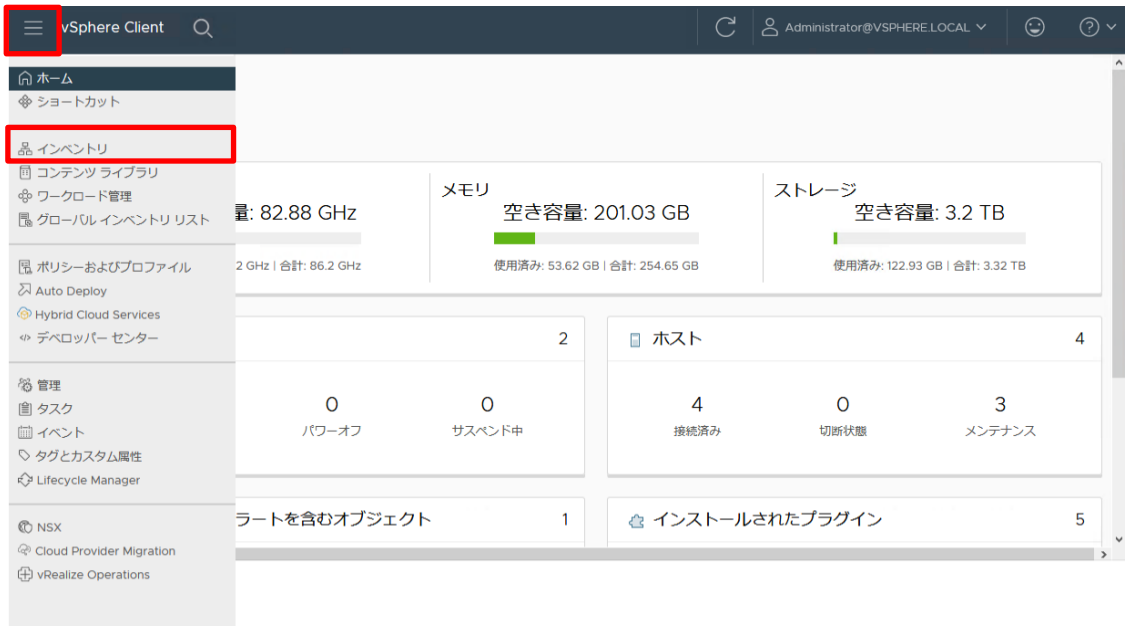
《参考》

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、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. 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 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(管理ノードがある構成の場合)が表示されることを確認します。

また、管理ノードがない構成の場合は各クラスタノードがメンテナンスモード解除の状態、
管理ノードがある構成の場合は各クラスタノードがメンテナンスモードの状態となっていることを確認してください。

以上で本章の作業は終了です。
以降の作業も vSphere Client を使用するため、閉じずにそのままにしてください。

管理ノードレスの場合

管理ノードがある構成の場合(以下画像は 2Node 構成の場合)

※ 構築した機器が表示されない場合は、3.4 章以降の手順を再度見直してください。
解決しない場合は、1.1 章の HCI システムインストール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 3.11 章以降の手順を実施してください。

3.11 隔離 IP の到達確認

2Node 構成の場合は、本章の実施は不要です、3.12 項に進んでください。

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。すべてのクラスタノードに対して下記手順を実施します。

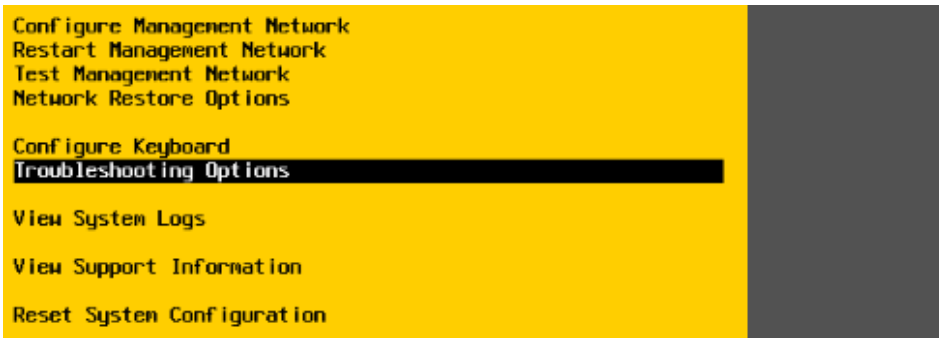
《参考》

以降の操作は①作業端末から 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、本章手順 2 以降の操作を行ってください。本章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、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。

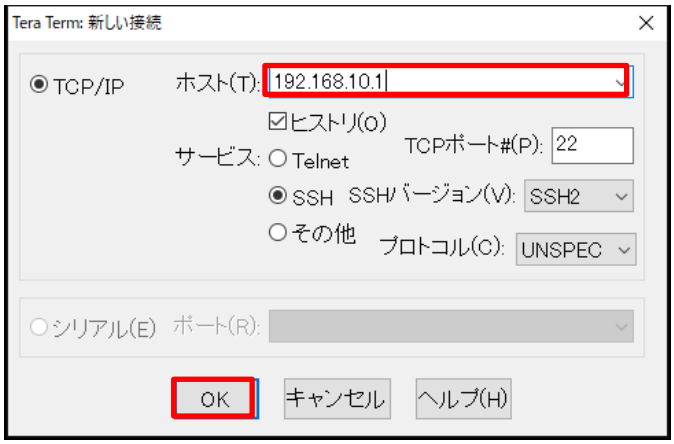
④ SSH を無効化する場合は、①から②の操作後、「Troubleshooting Mode Options」の画面で[Disable SSH]を選択した状態で[Enter]キーを押下し、画面左のメニューの表示が[SSH is Disabled]に更新されることを確認します。

※ 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。

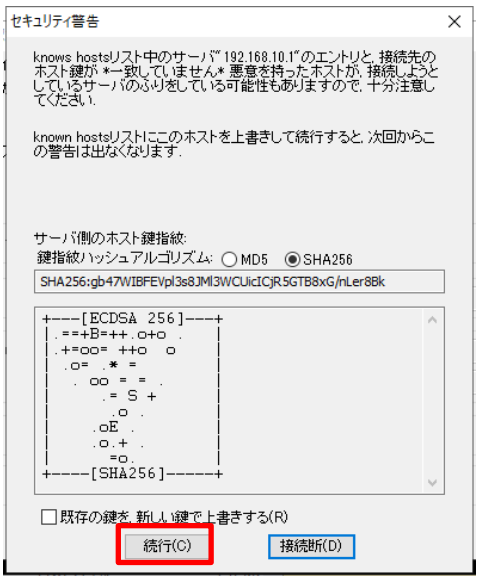
1. 作業端末上で SSH クライアント(例: Tera Term)を起動します。
[ホスト]欄に以下のアドレスを入力した後、[OK]をクリックします。

<クラスタノード - 管理用 NW - IP アドレス>

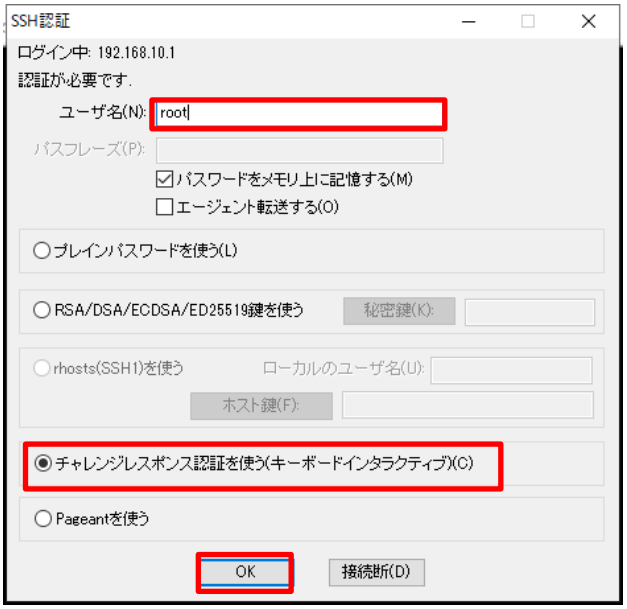
※ 他のターミナルソフトを使用される場合は、本項の内容に相当する操作を行ってください。



[OK]をクリックした後、「セキュリティ警告」のダイアログが表示される場合があります。
その際は[続行]をクリックして操作を継続します。

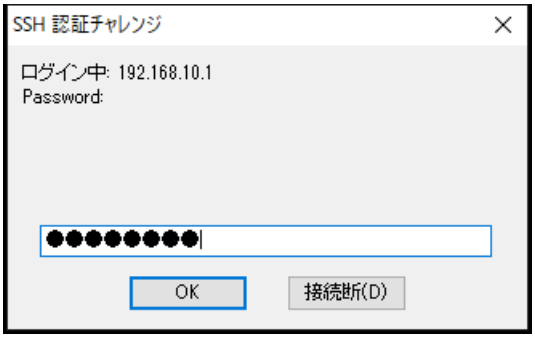


2. 「SSH 認証」のダイアログが表示されます。[ユーザ名]欄に root を入力した後、[チャレンジレスポンス認証を使う]にチェックを付け、[OK]をクリックします。

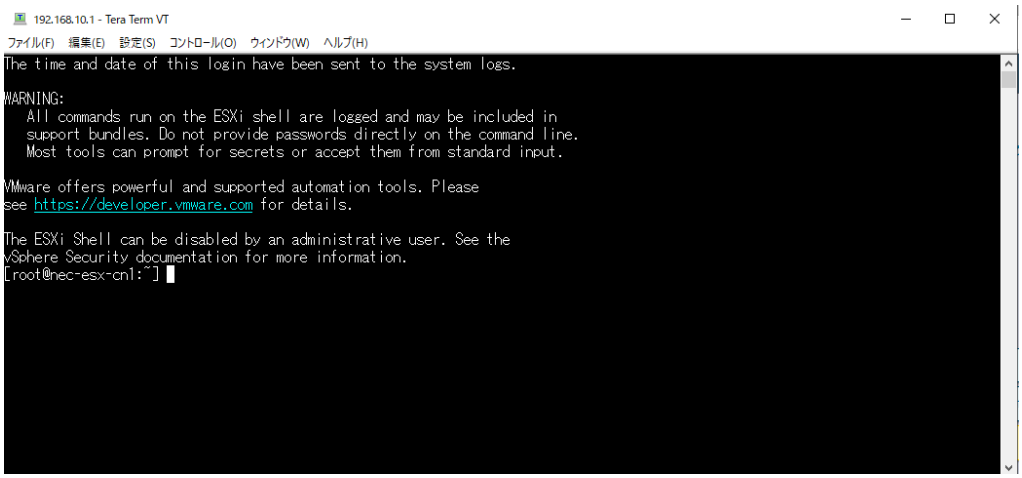


3. 引き続き「SSH 認証チャレンジ」のダイアログが表示されたら、下記パスワードを入力し、[OK]をクリックします

- 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」



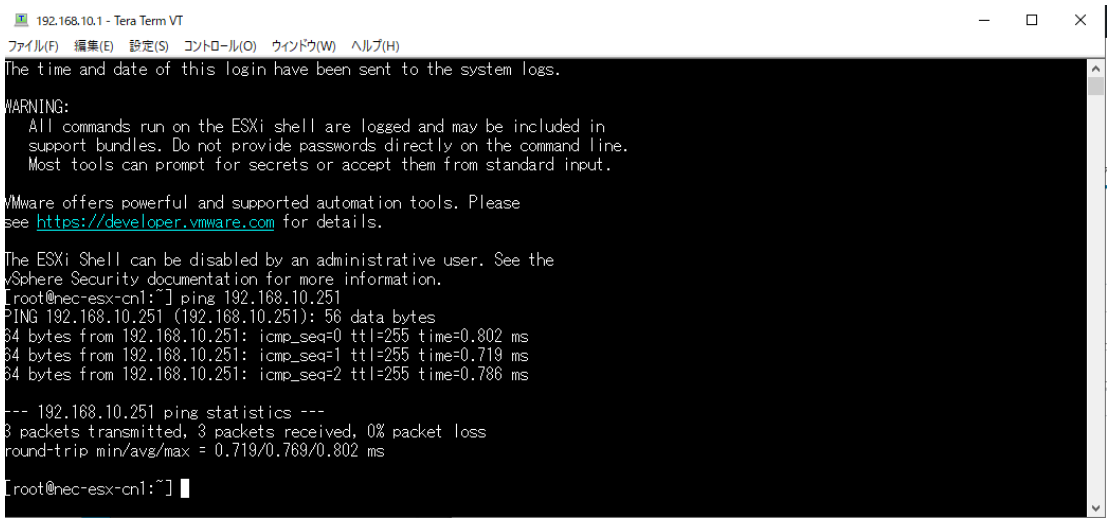
4. 接続すると、ターミナルソフトに ESXi Shell 画面が表示されます。



5. 以下のコマンドを実行し、隔離 IP に ping を行います。

```
# ping <クラスタ – vSphereHA – 隔離アドレス>
```

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。

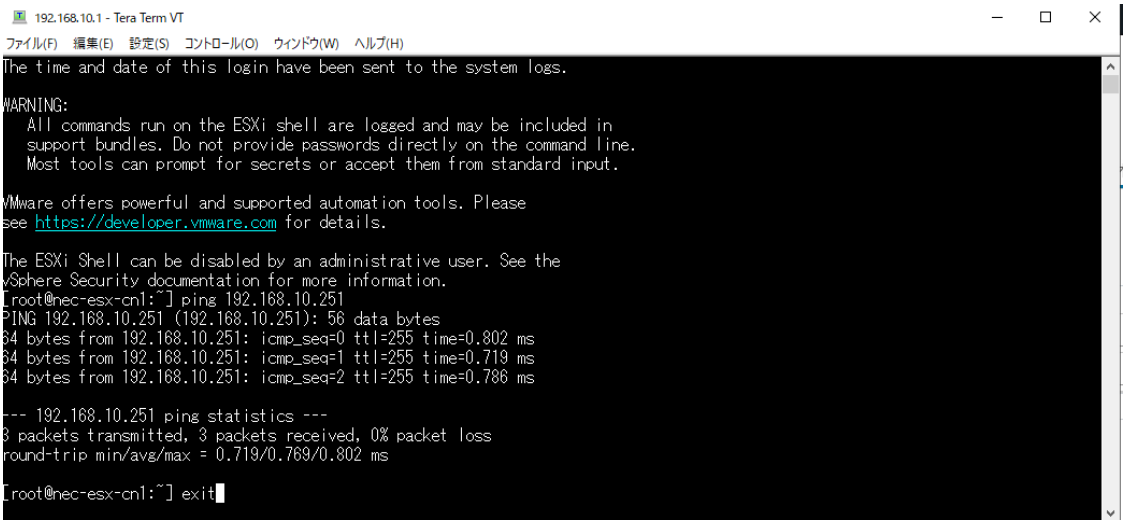
《参考》

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」)

6. 隔離 IP 到達確認後、ESXi Shell を終了します。

   以下のコマンドを入力し、Tera Term の画面が閉じることを確認します。

```
# exit
```



7. 以降の章で引き続き 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。

   ESXi Shell はセキュリティの観点から運用中は無効にすることが推奨されますので、本ドキュメントのすべての作業が終了したら、無効にすることを推奨します。

8. 本章 1～6 の手順を他のクラスタノードに対して実施します。

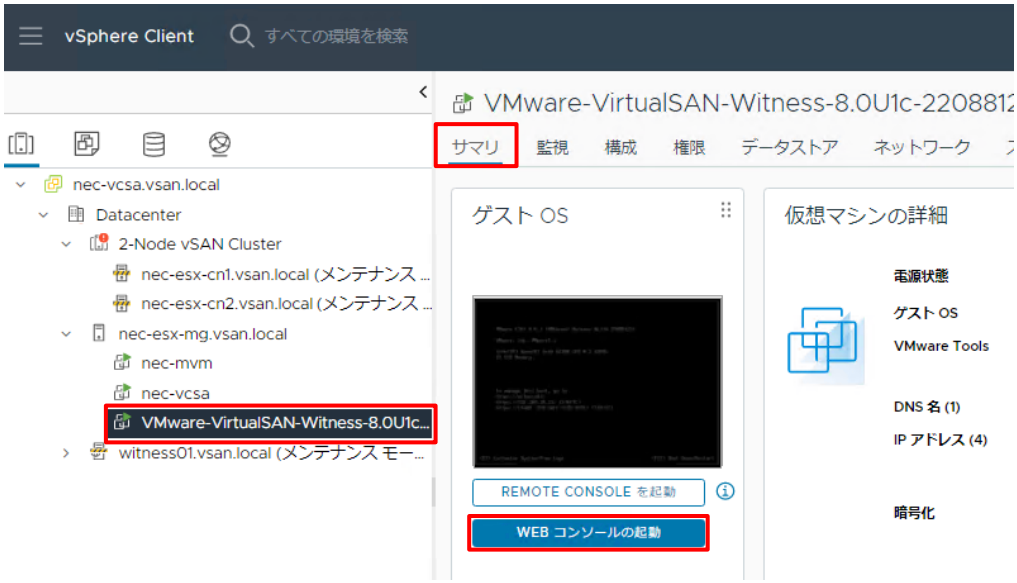
3.12 NTP の動作確認

各ノードが、NTP サーバに同期できているか確認します。

本章の操作は全てのノードで実施します。2Node 構成の場合は、Witness ノードに対しても実施してください。

3.11 章で有効にした 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。

2Node 構成の場合は、3.11 章を参照し、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-ntp.vsan.LOCL.              1 u  677 1024  377    0.520   -0.300   0.183
[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. 本章の 1～4 の手順をすべてのノードと Witness ノードに対して実施します。

3.13 Witness ノードのメンテナンスモード解除

本章は 2Node 構成の場合実施します。

該当しない場合は、本章は不要です、3.14 章に進んでください。

vCenter Server より、Witness ノードのメンテナンスモードを終了させます。

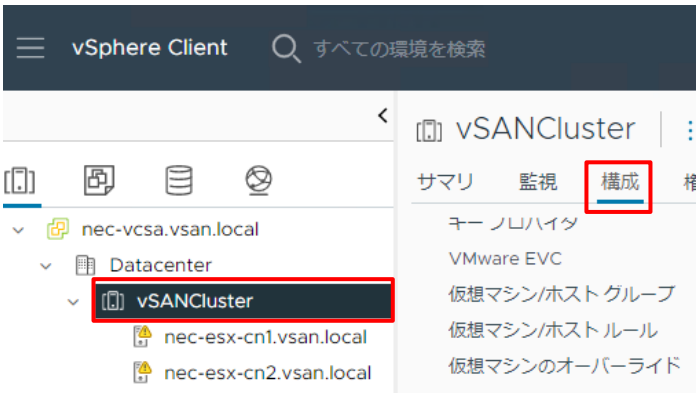
vSphere Client のメイン画面で Witness ノード名を指定した状態で右クリックし、
[メンテナンスモード]-[メンテナンスモードの終了]を選択してください。

3.14 vSAN サービスの再起動

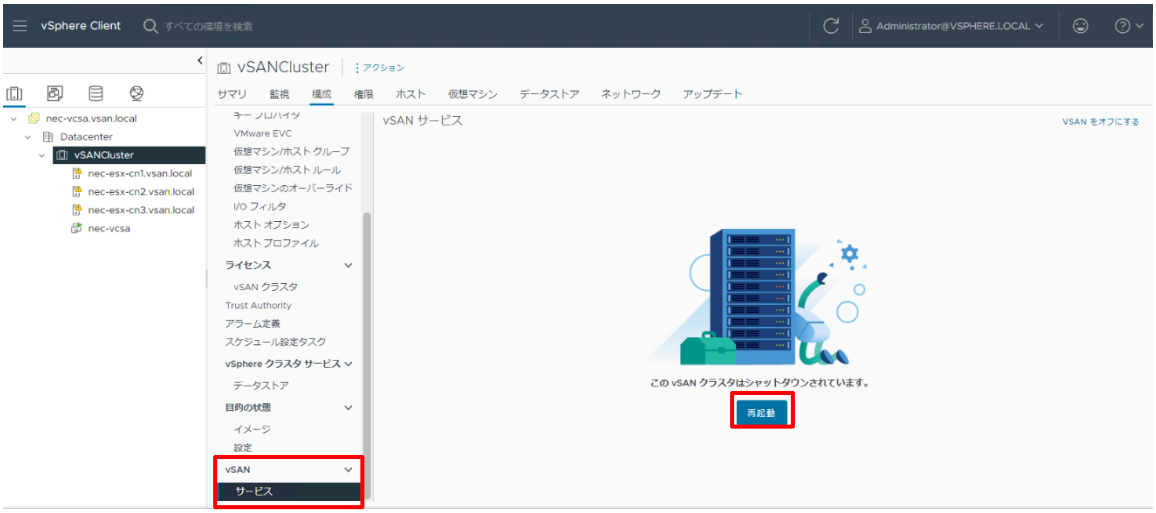
クラスタノードの起動後も、vSAN クラスタはシャットダウンされた状態になっています。

本章では、vSAN サービスの再起動を実施します。

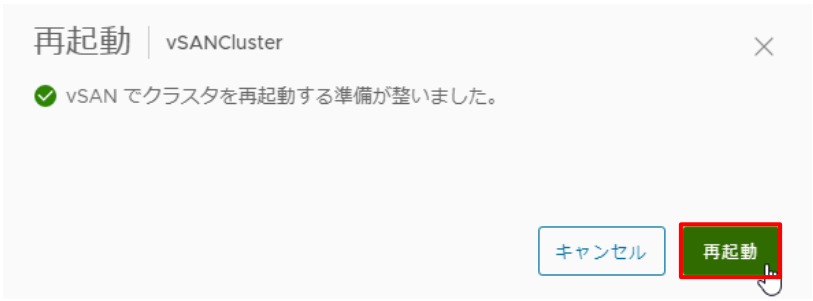
1. vSphere Client のインベントリで vSAN クラスタを選択した状態で[構成]タブをクリックします。



2. [構成]タブ内の[vSAN]-[サービス]をクリックし、画面右に表示される[再起動]をクリックします。

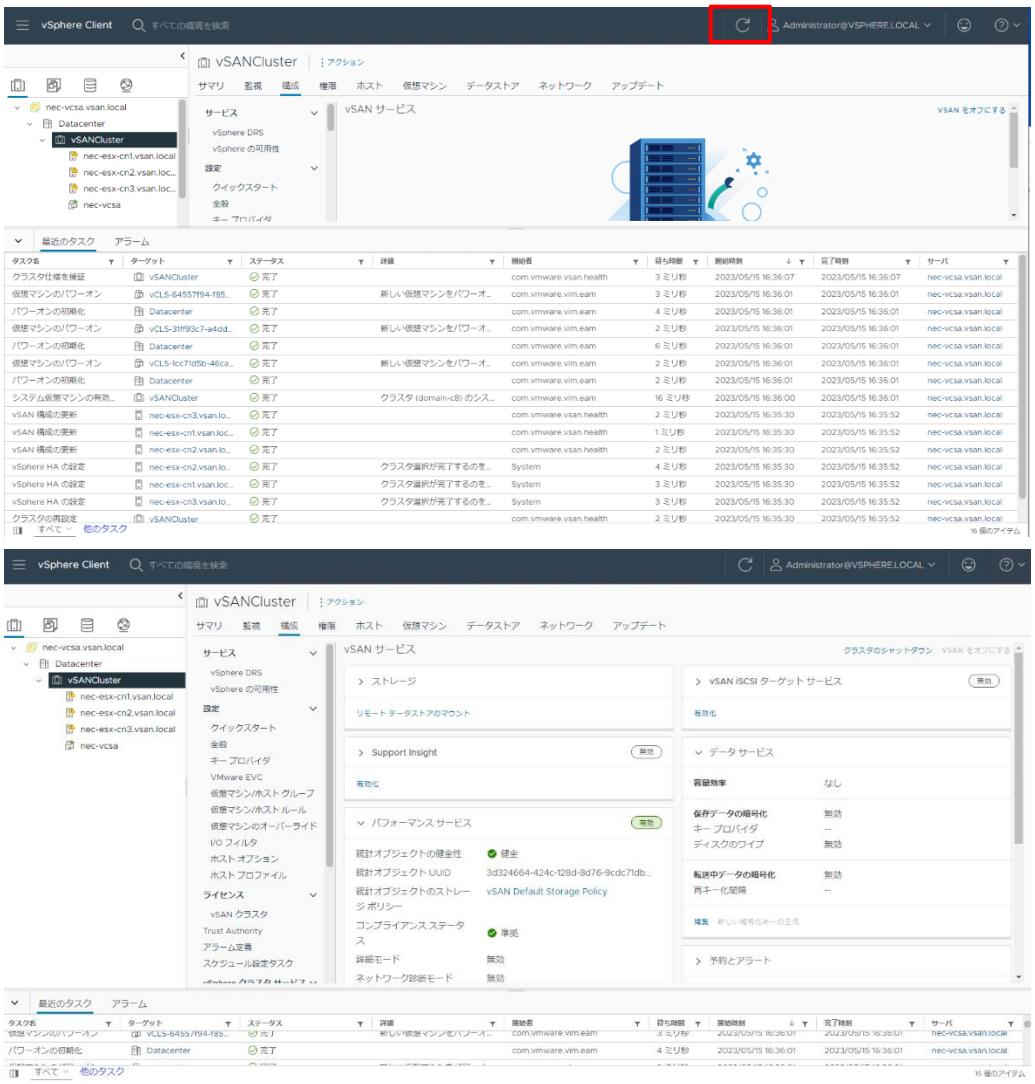


3. 「再起動」ダイアログが表示されますので、[再起動]をクリックします。

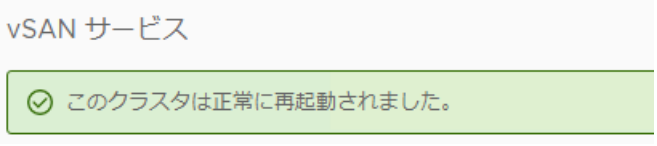


4. vSAN クラスタの再起動が開始されます。画面右側に再起動の経過が表示されます。

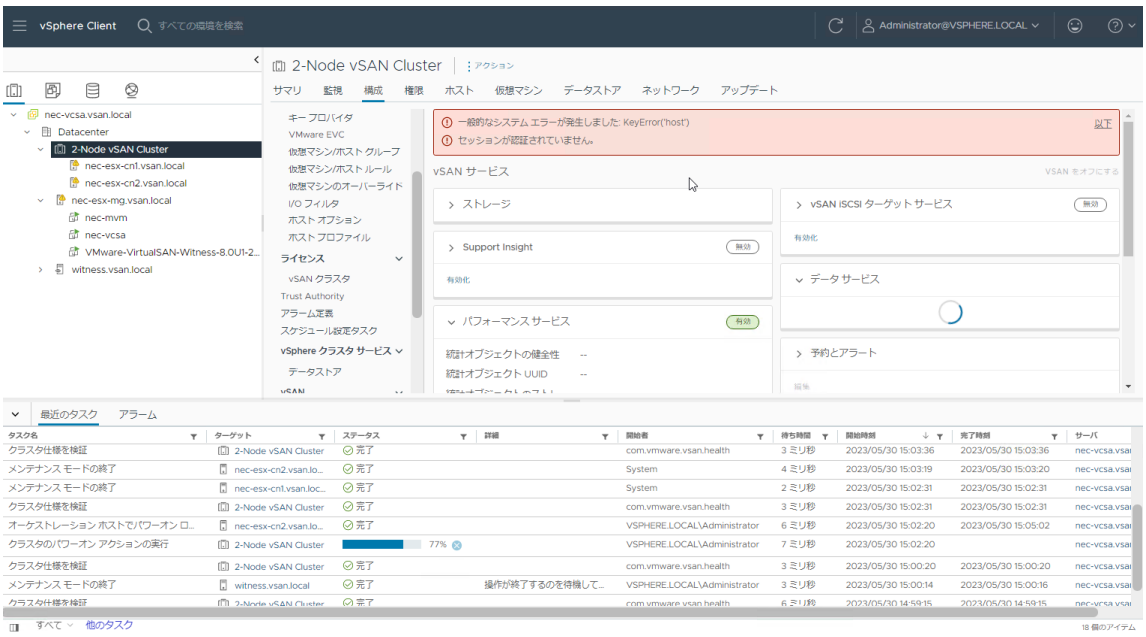
※ 再起動の経過画面に切り替わらない場合は、画面下部に表示されるタスクが全て完了したことを確認したあとに画面更新を実施し、vSAN サービス画面が表示されることを確認してください。手順 5 の確認は不要です。



5. 再起動完了後、「このクラスタは正常に再起動されました。」と表示されることを確認します。



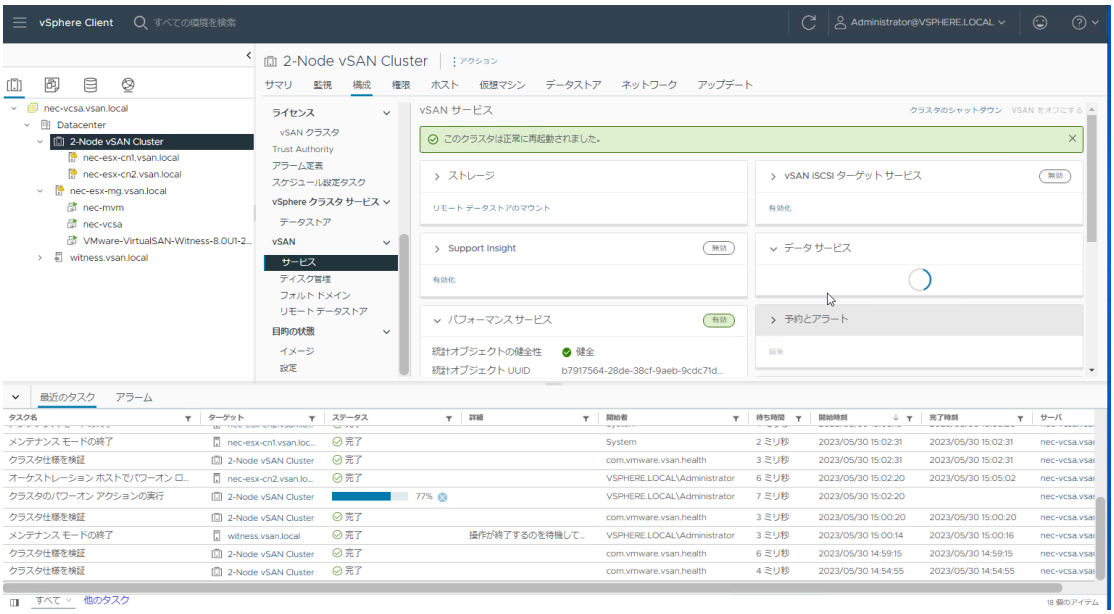
《補足》
vCSA 仮想マシンが再起動対象の vSAN クラスタ外に存在する構成の場合、vSAN クラスタの再起動中にエラーが発生する場合があります。



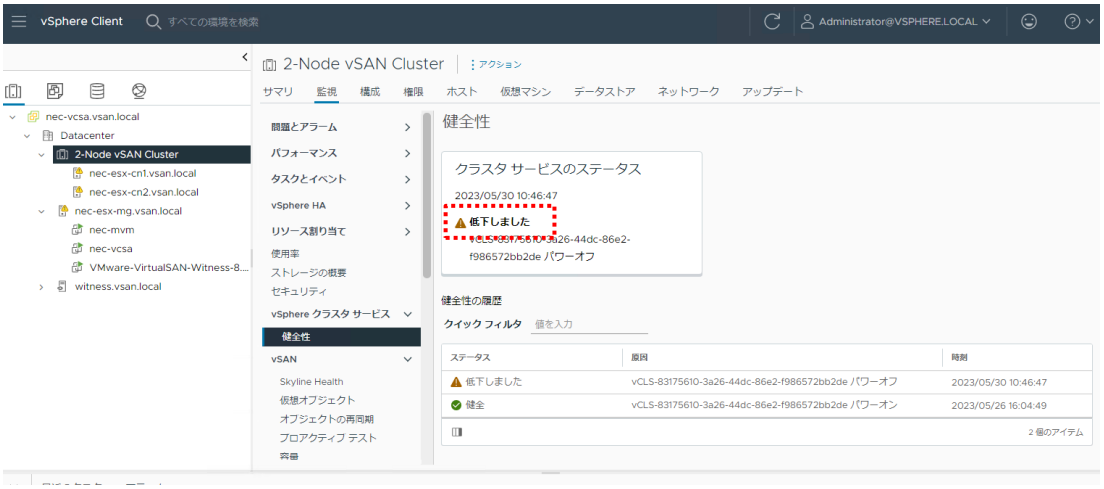
- 対処手順

① [監視]-[vSAN]-[skyline 健全性]など他の画面に一旦切り替え、再度[構成]-[vSAN]-[サービス]を開き、[再起動の再開]を実施してください。
[再起動の再開]が実施できない場合は、この後の「再起動の再開ができない場合」を参照してください。

② 「このクラスタは正常に再起動されました。」と表示されることを確認します。
「クラスタのパワーオンアクションの実行」タスクが 77%で止まっている場合、画面右上の画面更新アイコンをクリックすると完了します。



③ 続いて、vSAN クラスタを選択した状態で[監視]-[vSphere クラスタサービス]-[健全性]をクリックし、「クラスタサービスのステータス」の状態を確認します。「健全」ではなく、「低下しました」になっている場合は、以降の対処が必要です。

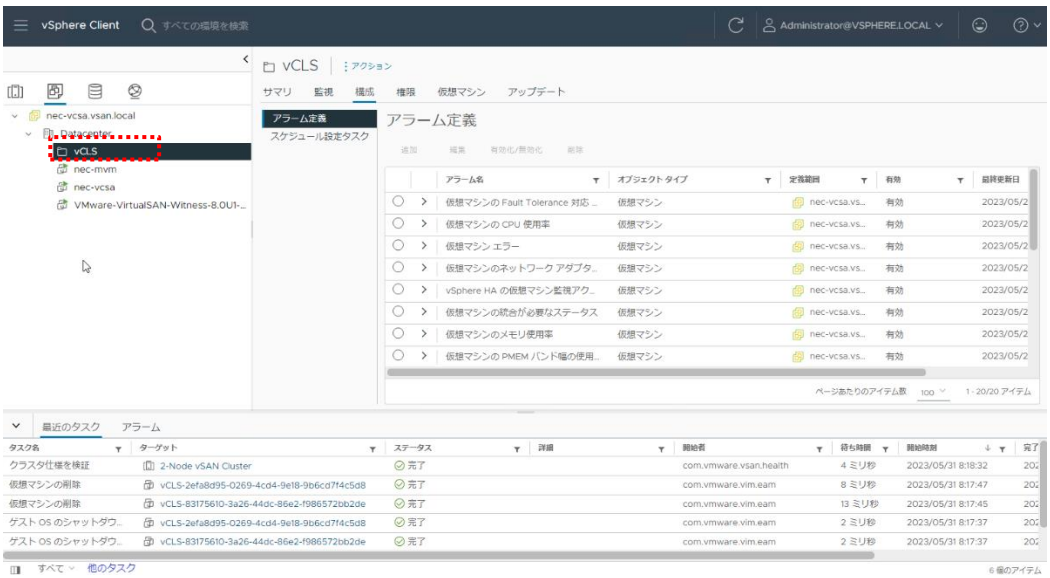


④ vCenter Server 名をクリックして[構成]-[詳細設定]をクリックし、「vCenter Server の詳細設定」画面右上の[設定の編集]をクリックします。

⑤ 「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"」の値を確認します。
”True”になっている場合は”False”と入力し、「保存」をクリックします。

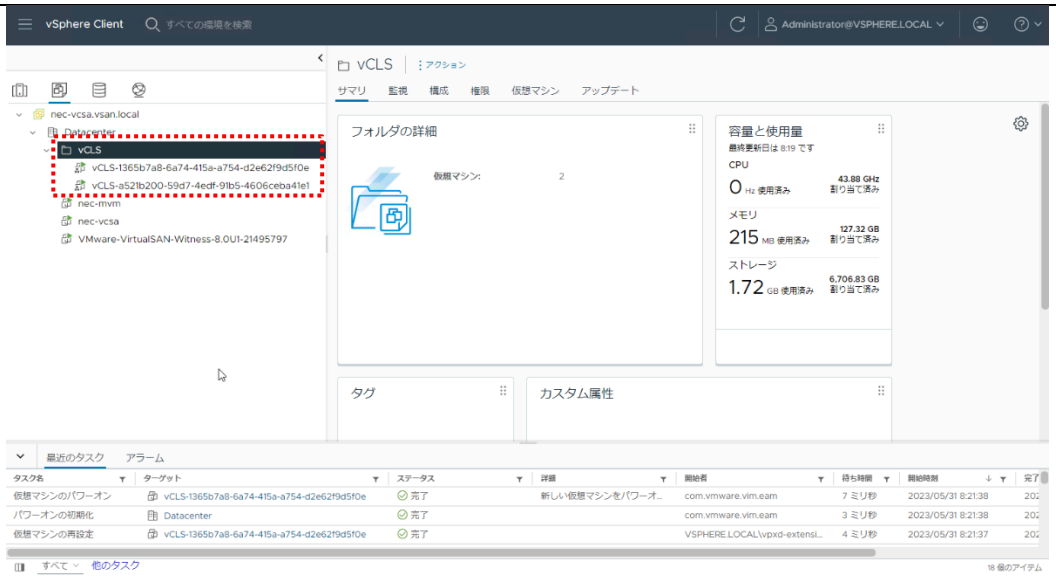
※ 「名前」横のアイコンをクリックし、「vcls」を入力して検索できます。

⑥ vCLS 仮想マシンが削除されることを確認します。



⑦ 再度手順⑤を参照し、「config.vcls.clusters.domain-c<number>.enabled」の値を「False」から「True」に変更します。

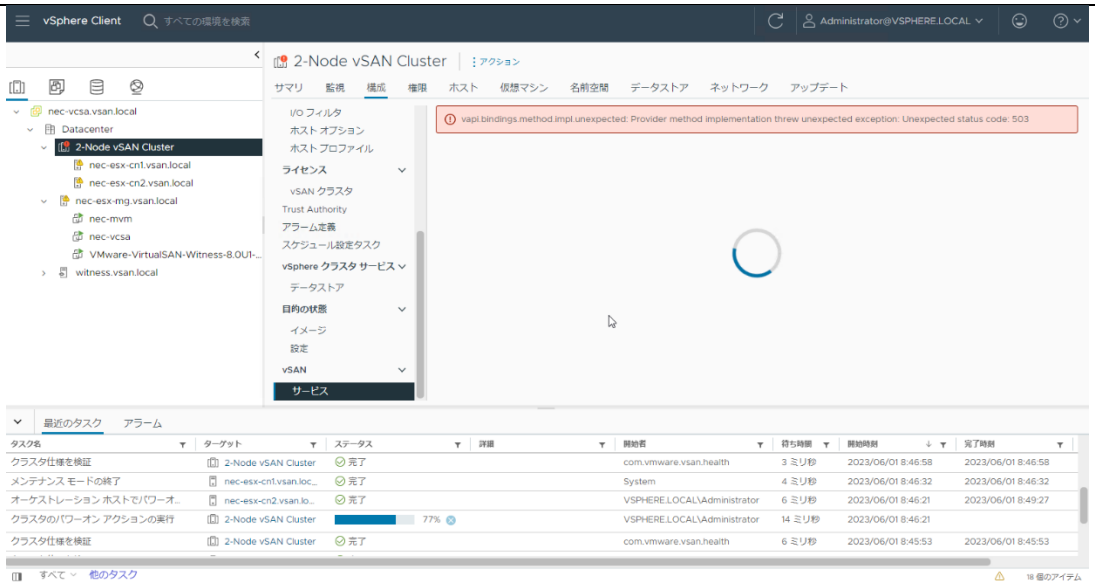
⑧ vCLS 仮想マシンが再作成されることを確認します。



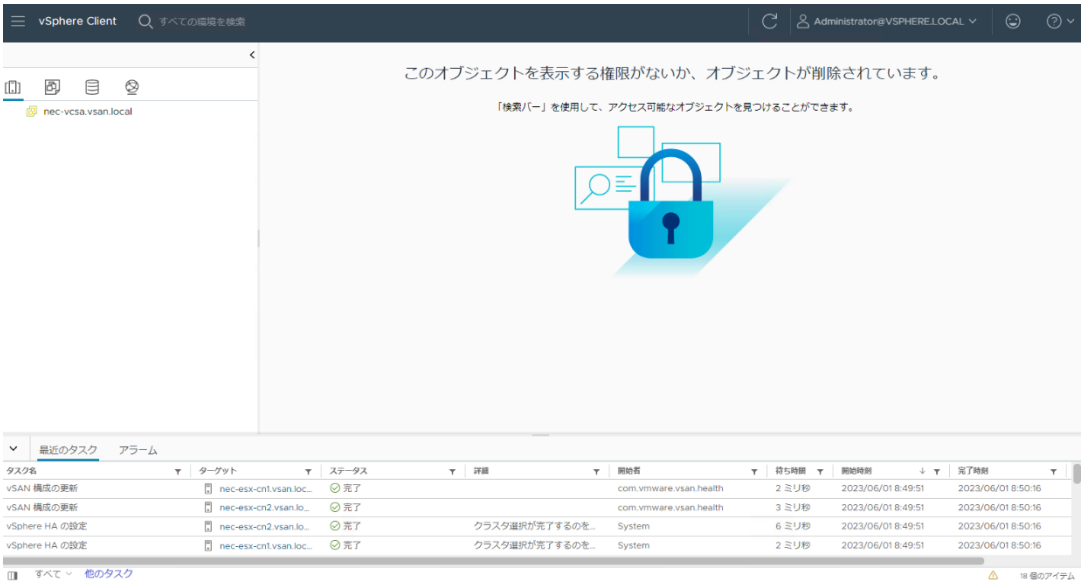
⑨ vSAN クラスタを選択した状態で[監視]-[vSphere クラスタサービス]-[健全性]をクリックし、「クラスタサービスのステータス」の状態が「健全」になっていることを確認します。

- 再起動の再開ができない場合

① vSAN クラスタの再起動中にエラーが発生し、[監視]-[vSAN]-[skyline 健全性]など他の画面に一旦切り替えて再度[構成]-[vSAN]-[サービス]画面を表示しても、[再起動の再開]が表示されずにエラーが表示され続ける場合があります。



この場合、画面右上の更新アイコンをクリックすると「このオブジェクトを表示する権限がないか、オブジェクトが削除されています。」の画面が表示され、vSphere Client 上で操作ができなくなる場合があります。



② vCSA の再起動を実施します。Web ブラウザから vCenter Server 管理インターフェイス(VAMI)に root ユーザでログインします。

https://<**vCSA - FQDN**>:5480/

画面右上の[アクション]-[再起動]をクリックします。

「システムの再起動」画面で[はい]をクリックします。

③ しばらく待ち、再度 vSphere Client に接続します。

④ vSAN クラスタを選択した状態で[構成]-[vSAN]-[サービス]をクリックし、「vSAN サービス」画面で[再起動]をクリックし、再度 vSAN サービスの再起動を実施します。

⑤ 再起動が完了し、「このクラスタは正常に再起動されました。」と表示されることを確認します。

⑥ 本補足の「対処手順」手順③～⑨を実施します。

以上で vSAN サービスの再起動は完了です。

《補足》
本章の時点で「ホスト上のサードパーティ I/O フィルタストレージプロバイダの登録/登録解除に失敗する」の警告が表示される場合があります。

vCSA と ESXi 間の通信に問題が発生した場合に当該のアラームが発生します。
ESXi の再起動直後に、一時的な接続の問題等に関連して当該のアラームが出力される事例が確認されています。
本アラームは Storage I/O control(SIOC) と仮想ディスクの暗号化機能をご利用でない場合は実害を示すものではないため、リセットして問題ありません。

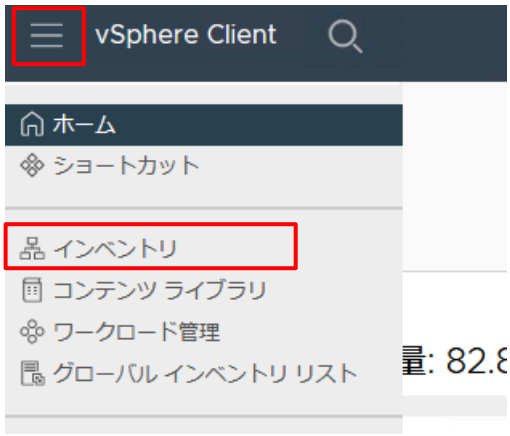
警告が表示されているノードを選択した状態で[監視]-[問題とアラーム]-[すべての問題]を開き、表示された画面で当該アラームにチェックを付け、[緑にリセット]をクリックしてください。

3.15 vSAN ストレージプロバイダの同期

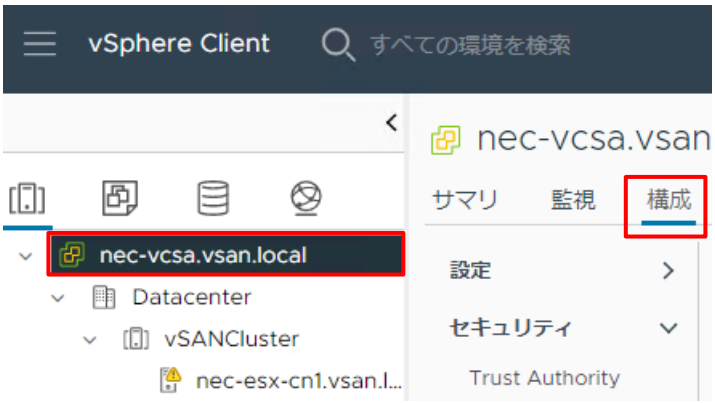
下記の問題を回避するために、vSAN ストレージプロバイダの同期を行います。

https://knowledge.broadcom.com/external/article?legacyId=52966

1. 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. ナビゲータで 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」であることを確認します。

3.16 TPM のリカバリキーのバックアップ

本章は、TPM が搭載されているサーバに対して実施します。

1. TPM が搭載されているサーバ(クラスタノードおよび、管理ノードありの場合は管理ノード)に対し、3.11 章を参照して作業端末上で SSH クライアントを使用し、ESXi Shell にユーザ名 root でログインします。
2. 以下のコマンドを実施し、表示された結果をリカバリキーのバックアップとして控えておきます。

```
# esxcli system settings encryption recovery list
```

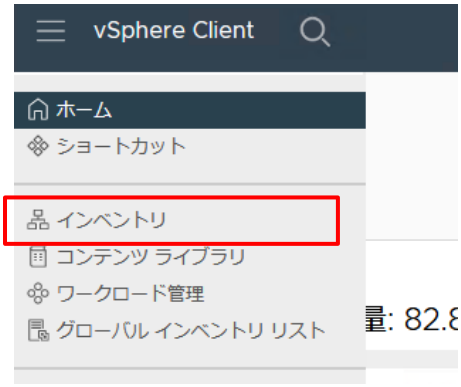
3. vSphere Client のインベントリでリカバリキーのバックアップを実施したノードをクリックし、[監視]-[問題とアラーム]-[すべての問題]をクリックします。
「TPM 暗号化リカバリキーバックアップアラーム」が表示されていないことを確認し、表示されている場合、アラームにチェックを付けて[緑にリセット]をクリックします。

4. TPM が搭載されているサーバ全てに実施します。

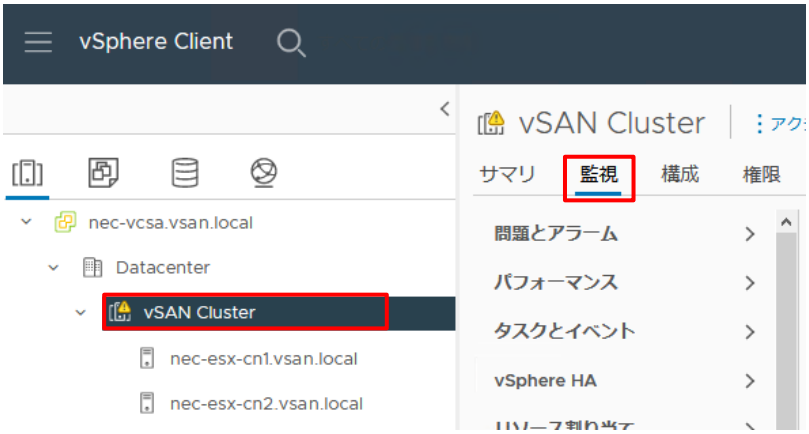
3.17 vSAN 状態の確認(健全性確認)

vSAN クラスタの状態を確認し、健全性にエラーが出ていないことを確認します。

1. 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. ナビゲータで 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 Health]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、「不良」欄が 0 であることを確認します。

《注意》

以下の項目に関して、インターネット接続が不可能な場合、警告となる場合があるため、HCI インストールサービス(for VMware vSAN)ではサイレン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。
- 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。

以上で vSAN の確認は完了です。

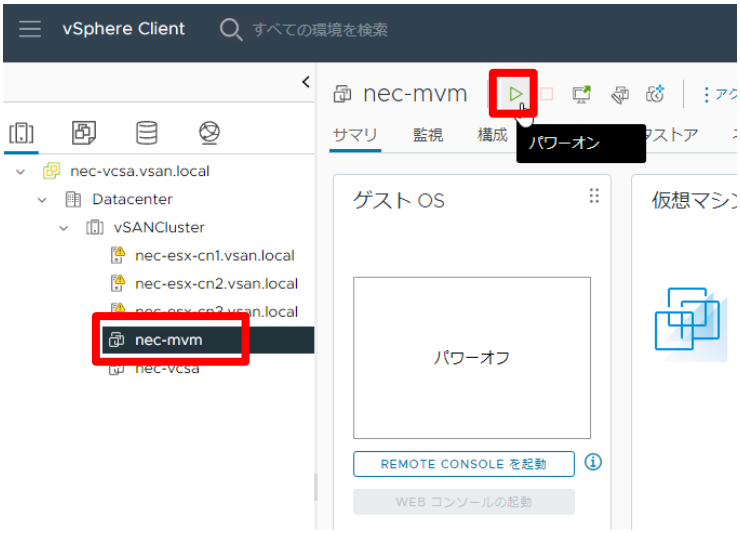
3.18 管理 VM の起動と接続確認

本章は管理 VM がある構成の場合のみ実施します。

管理 VM がない構成の場合は、本章は不要です、4 章に進んでください。

管理 VM の起動と RDP 接続の確認を実施します。

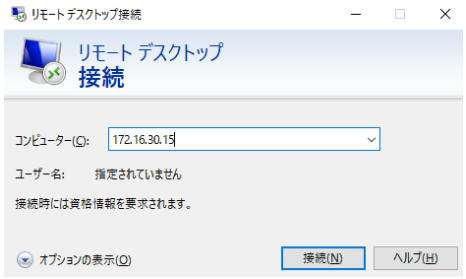
1. 管理 VM の電源をオンにします。vSphere Client のナビゲータで管理 VM を選択し、画面上部の「パワーオン」アイコンをクリックします。



2. 作業端末から管理 VM にリモートデスクトップ接続します。

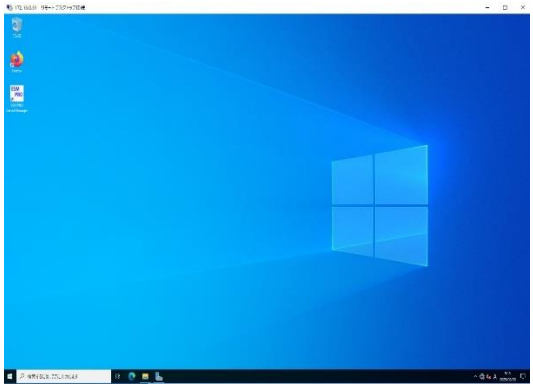
   作業端末でリモートデスクトップ接続(mstsc)を起動します。
   下記アカウント情報を入力し、ログインできるかどうかを確認します。

   - コンピューター: **<管理 VM - 管理用 NW - 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」



3. 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。

- ネットワーク: 作業端末より、以下のアドレスに 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 - 管理用 NW - IP アドレス>

3.19 エクスプレス通報サービスの開局手続き

本章は、管理 VM がある構成の場合で、且つ HCI システムインストールサービスでエクスプレス通報サービスの設定をしている場合に実施します。

本章の作業は管理 VM にリモートデスクトップ接続して実施してください。

開局作業は、各ノードの iLO 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、1.1章のエクスプレス受付センターにお問い合わせ下さい。

3.20 サーバ診断カルテの開局手続き

本章は、管理 VM がある構成の場合で、且つ HCI システムインストールサービスでサーバ診断カルテの設定をしている場合に実施します。
該当しない場合は、本章は不要です、4 章に進んでください。
本章の作業は管理 VM にリモートデスクトップ接続して実施してください。
サーバ診断カルテを利用するには、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。

3.19 章を参照し、各ノードの ESXi に対し、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 3.19 章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

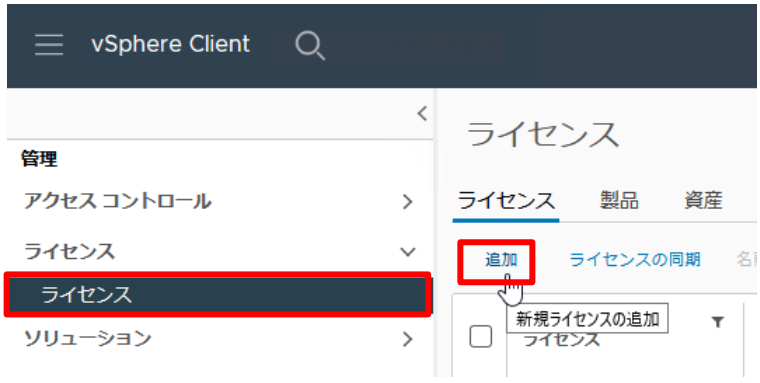
vCenter Server、ESXi および vSAN のライセンスキーの登録および割り当てを行います。

なお、VMware by Broadcom のサブスクリプションモデルのライセンス提供形態である、VCF(VMware Cloud Foundation)および VVF(vSphere Foundation)のソリューションライセンスキーを適用する場合、本項の手順ではなく、以下のページを参照ください。
https://knowledge.broadcom.com/external/article?legacyId=97303

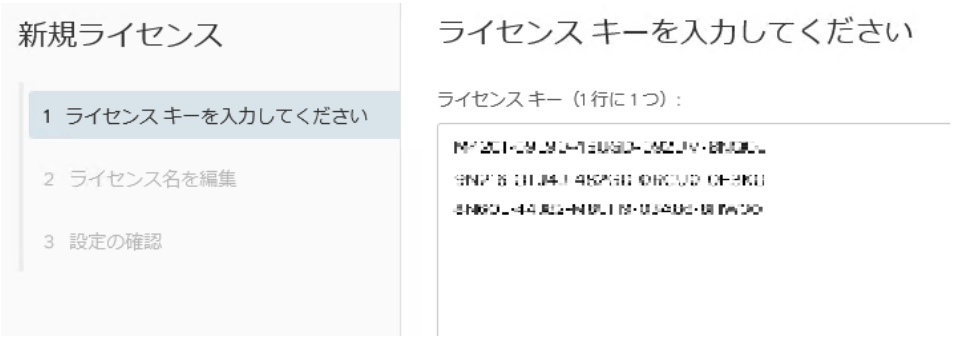
vCenter Server へのライセンスの割り当ては主に手順 7 から手順 9 を、また、ESXi へのライセンスの割り当ては主に手順 10 から手順 13 で行います。vSAN ライセンスの割り当ては手順 14 から手順 16 で行います。

1. 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。

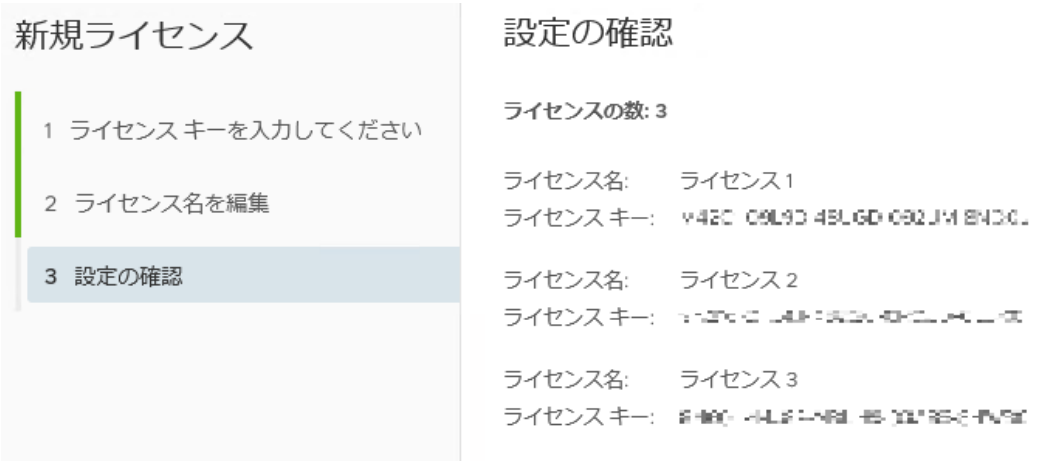


3. 「新規ライセンス」ダイアログが表示されます。「ライセンスキー（1 行に 1 つ）:」のメッセージ下の入力枠に登録するライセンスキーを、1 行に1つ入力した後、[次へ]をクリックします。

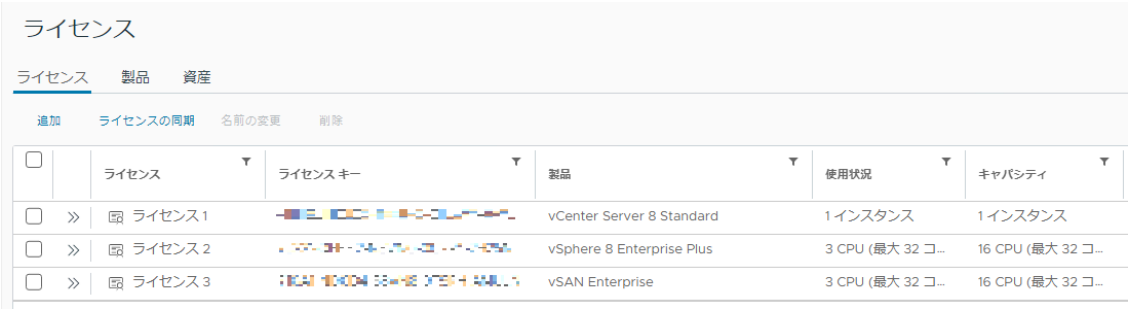


4. 次に「ライセンス名を編集」の画面が表示されます。入力した各ライセンスキーのライセンス名を必要に応じて編集した後、[次へ]をクリックします。

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。

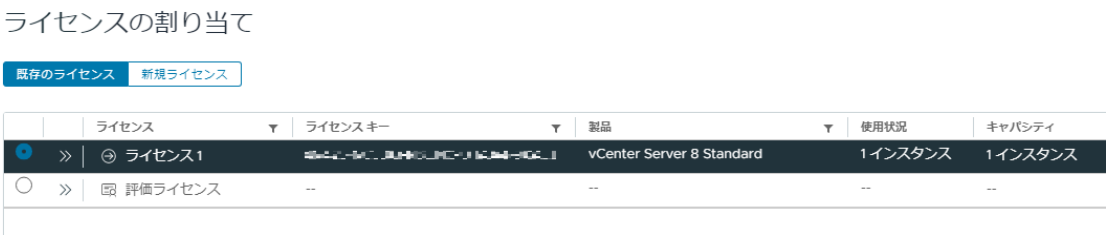


6. vSphere Client にフォーカスが戻ります。[ライセンス]タブ画面内のリストに、登録したライセンスキーが表示されていることを確認します。

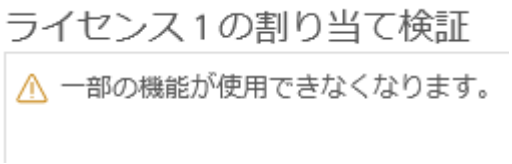


7. [資産]のタブをクリックし、さらにその下の[vCenter Server システム]をクリックします。続いて、資産の一覧内に表示されている vCenter Server の登録名にチェックを付け、[ライセンスの割り当て]をクリックします。

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 vCenter Server 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。



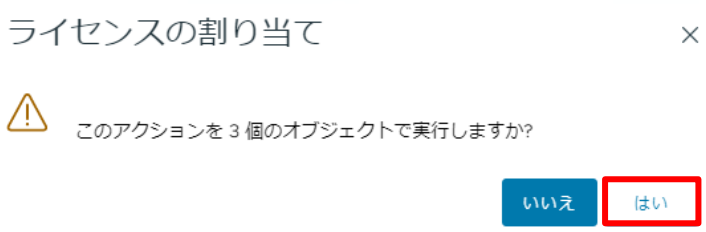
※ 評価ライセンス(Evaluation License)を適用している管理サーバに正規ライセンスを割り当てる場合、割り当て検証欄に「一部の機能が使用できなくなります。」と表示される場合があります。使用不可となる機能の詳細については、割り当て検証欄右端の[詳細]をクリックして確認ください。



9. 再び 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 名左のアイコンをクリックし、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。

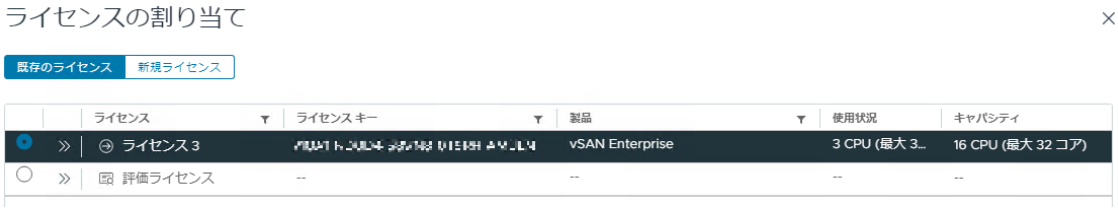


12. 「ライセンスの割り当て」ダイアログが表示されます。手順 8 と同様に、割り当てるライセンスキーの行頭にチェックを付けた状態で[OK]をクリックします。

13. 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 サーバ名左のアイコンをクリックし、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. 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 クラスタ名左のアイコンをクリックし、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。

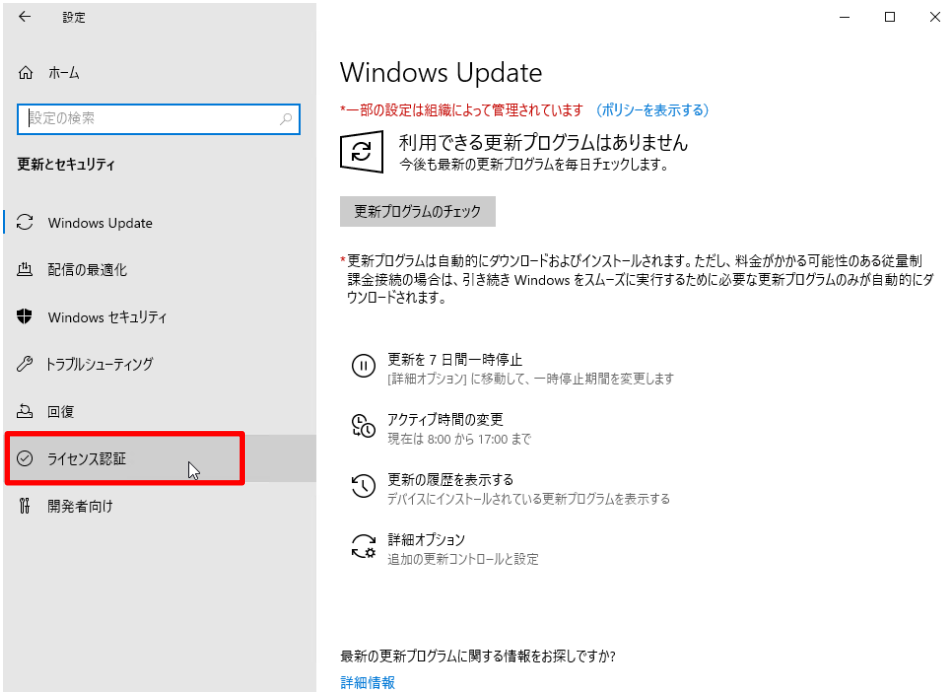
4.2 Windows Server 2022 のライセンス登録

Windows Server のライセンスキーの登録を行います。

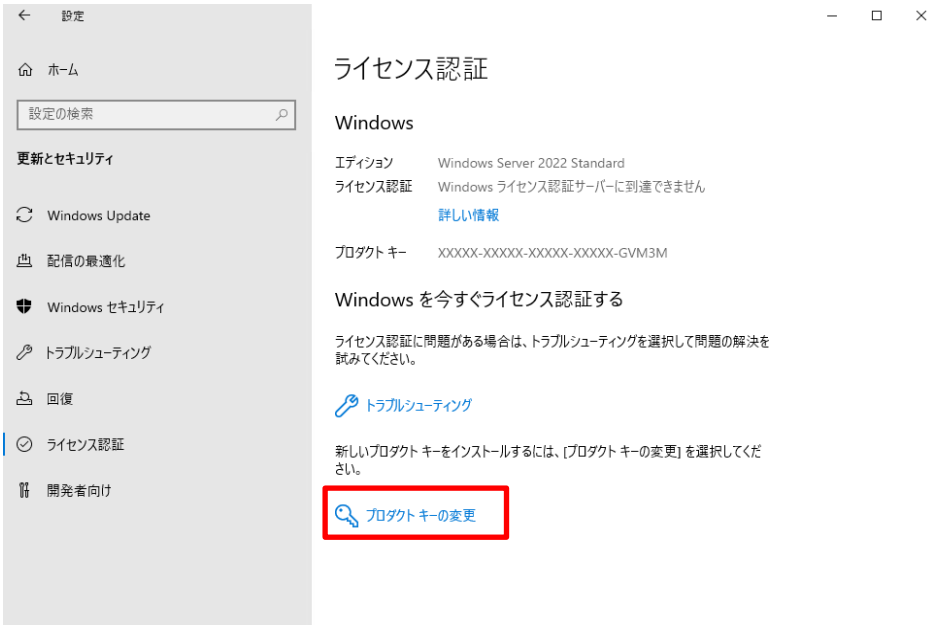
インターネット接続の有無で 2 種類の登録方法がありますので、どちらかを選択してください。

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

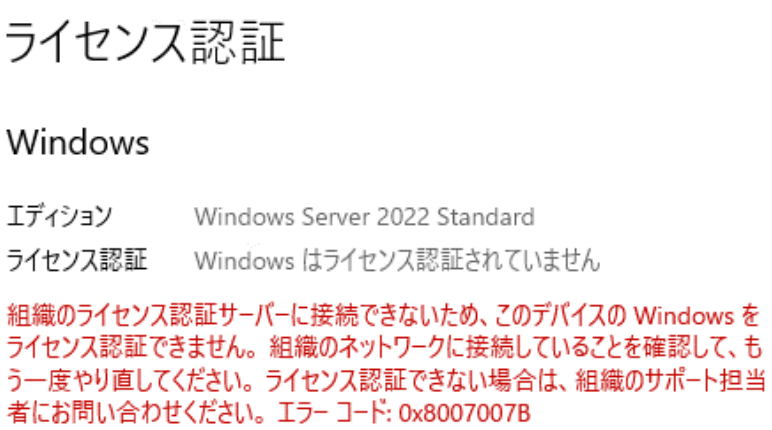
1. 画面の左下の Windows アイコンをクリックし、  アイコンをクリックします。
2. [更新とセキュリティ]をクリックした後、[ライセンス認証]をクリックします。



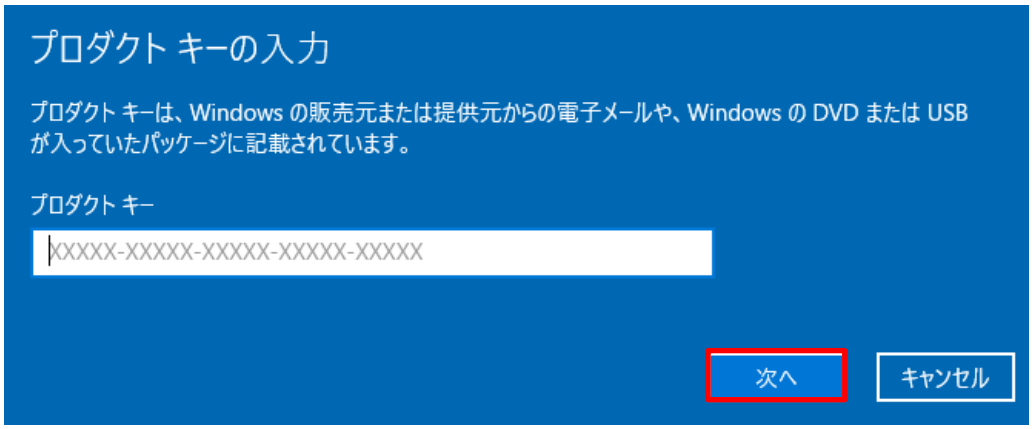
3. 「ライセンス認証」画面が表示されますので、[プロダクトキーの変更]をクリックします。



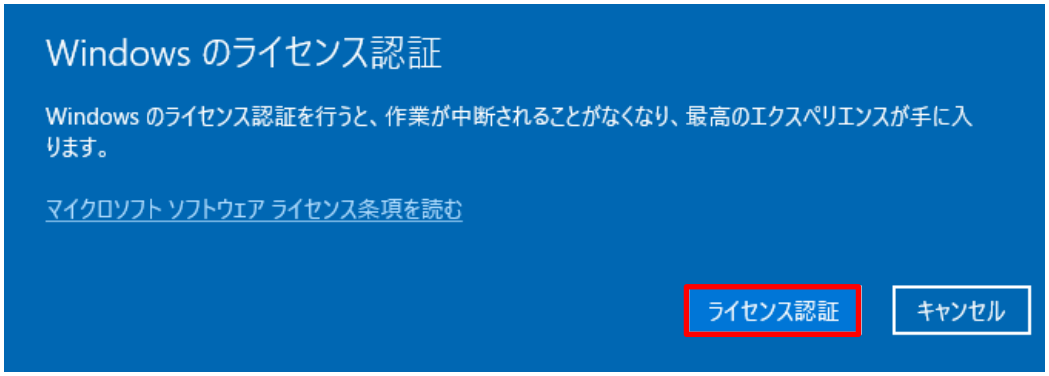
※ 「ライセンス認証」画面では以下のエラーが表示されている場合がありますが、作業に影響はありません。



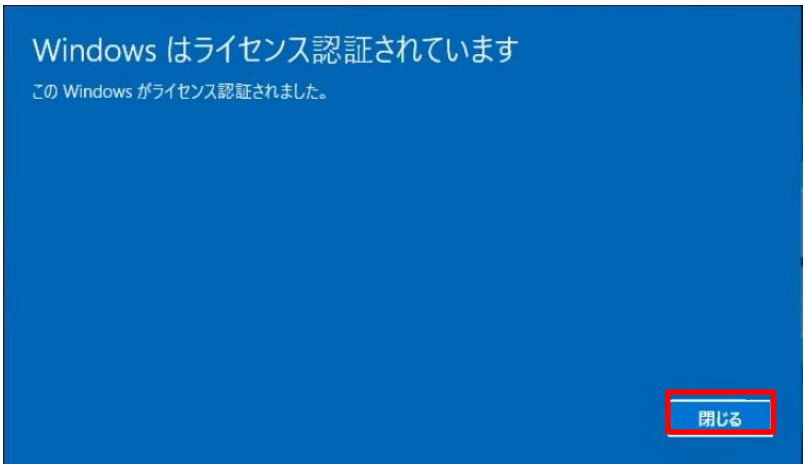
4. 「プロダクトキーの入力]画面でプロダクトキーを入力し、[次へ]をクリックします。



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。

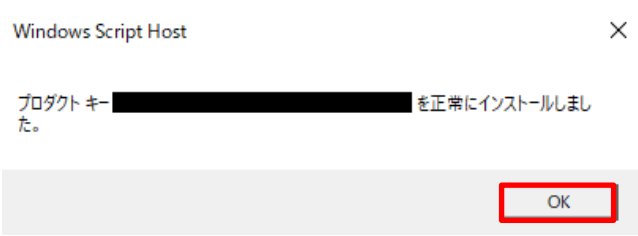


4.2.2 インターネットに接続されていない環境でライセンス登録

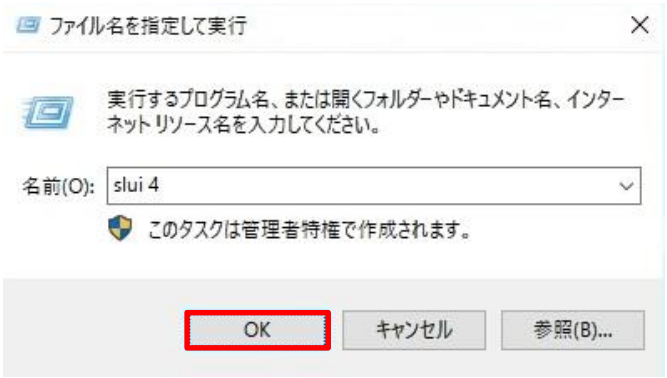
1. 画面の左下の Windows アイコンを右クリックし、[コマンドプロンプト (管理者)]を起動します。
2. 管理者権限のコマンドプロンプトで次のコマンドを入力し、Enter キーを押します。

   >slmgr -ipk *COA ラベルのプロダクトキー*

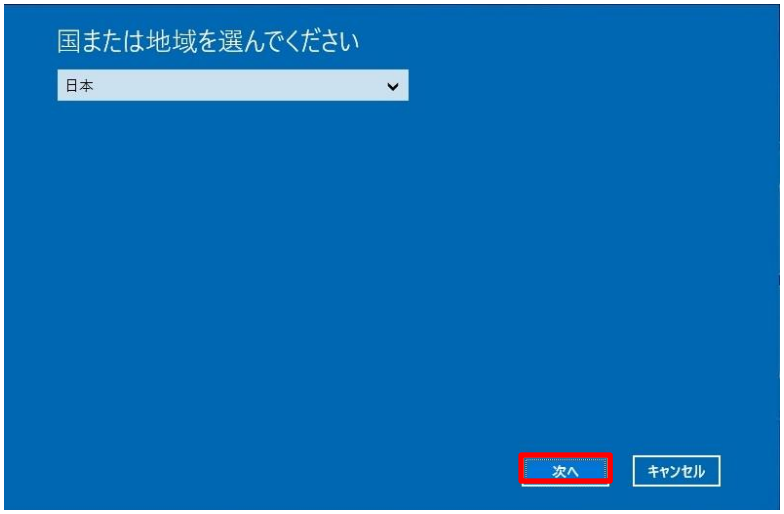
   コマンド入力後、以下の画面が表示されますので、[OK]をクリックします。



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。

5 パスワード変更

《重要》
HCI 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

本章で HCI システムインストールサービス(for VMware vSAN) 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。

① 各ノードの BMC のパスワード
② 各ノードの ESXi の ID、パスワード
③ Witness ノードの ESXi パスワード変更
④ vCenter Server Appliance(vCSA)の root パスワード
⑤ vCenter Server のシングルサインオン(SSO)のパスワード
⑥ vCenter Server の保守アカウントパスワード
⑦ 管理 VM(Windows Server 2022)の Administrator パスワード
⑧ 管理 VM の ESMPRO/ServerManager のパスワード
⑨ 管理 VM の ESMPRO/ServerManager の登録情報の更新
⑩ 管理 VM のサーバ診断カルテの登録情報の更新

5.1.1 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	
	ESMPRO/ ServerManager (※)	サーバ診断カルテ(※)
各ノードの BMC の ID・パスワード	○	―
各ノードの ESXi の ID・パスワード	○	○
管理 VM (Windows Server 2022)の Administrator パスワード	―	○

※ HCI システムインストールサービスで導入している場合のみ影響します。

○: 設定変更が必要　　―: 不要

5.2 各ノードの BMC のパスワード変更

本章は、すべてのクラスタノードの BMC のパスワード変更を実施します。
管理ノードがある構成の場合は、管理ノードの BMC のパスワード変更も実施します。

《注意》

変更後に 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 5.1.1 章を、ESMPRO/ServerManager 上のパスワード情報を更新する手順は 5.9 章を参照ください。

1. 作業端末上で、Web ブラウザを起動し、各ノードの 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 － BMC － IP アドレス**>/

   または

   https://<**管理ノード - BMC - IP アドレス**>/

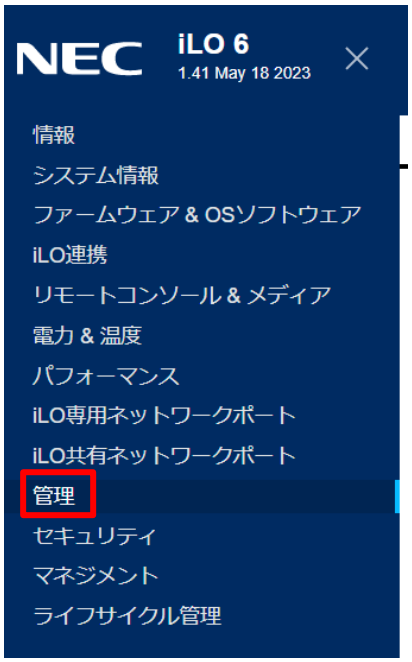
   ※ 「接続がプライベートではありません」画面が表示された場合は、[詳細設定]をクリックし表示された画面で、[*IP アドレスまたは FQDN* に進む(安全ではありません)]クリックしてください。

2. Web ブラウザに BMC のログイン画面が表示されます。

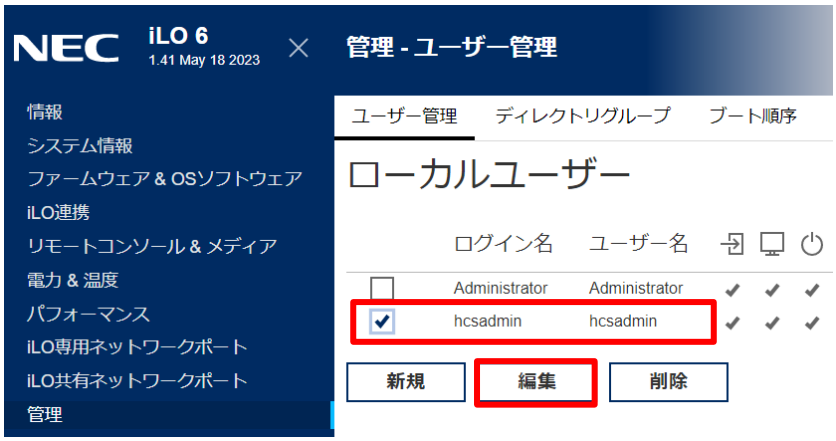
3. ローカルユーザ名、パスワードを入力し、[ログイン]をクリックします。
(ローカルユーザ名、パスワードは、初期パスワード通知書に記載されます)

4. 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。

5. 左ツリーから[管理]をクリックします。



6. [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。
7. 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。



8. 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。

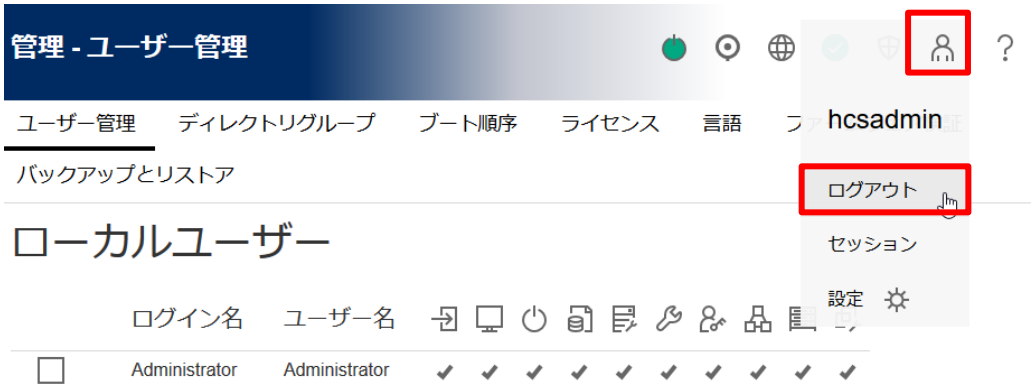
9. [パスワードを変更]チェックボックスをクリックし、新しいパスワード、パスワードの確認項目に変更したいパスワードを入力します。

※ 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。

10. 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。

11. 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。

12. 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。



13. 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。

14. すべてのノードで BMC のパスワード変更をおこなってください。

5.3 各ノードの ESXi パスワードの変更

本章は、すべてのクラスタノードの ESXi のパスワード変更を実施します。
管理ノードがある構成の場合は、管理ノードの ESXi のパスワード変更も実施します。

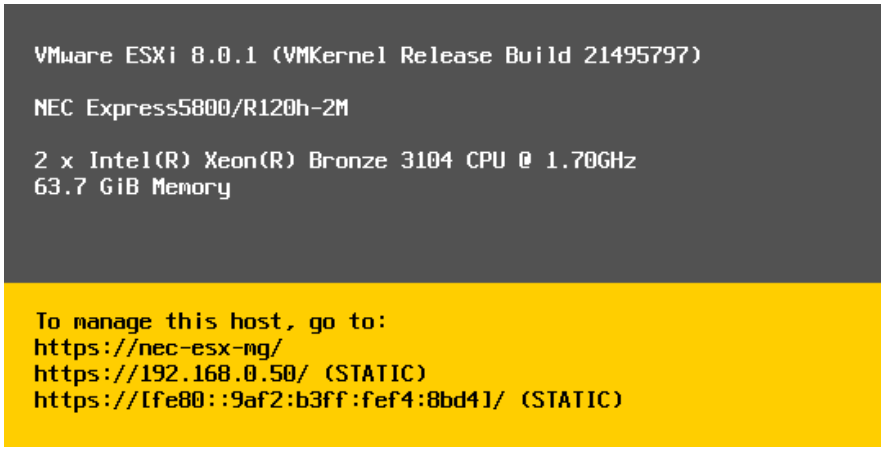
《注意》

変更後に ESMPRO/ServerManager 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 5.1.1 章を、ESMPRO/ServerManager 上のパスワード情報を更新する手順は 5.9 章を参照ください。

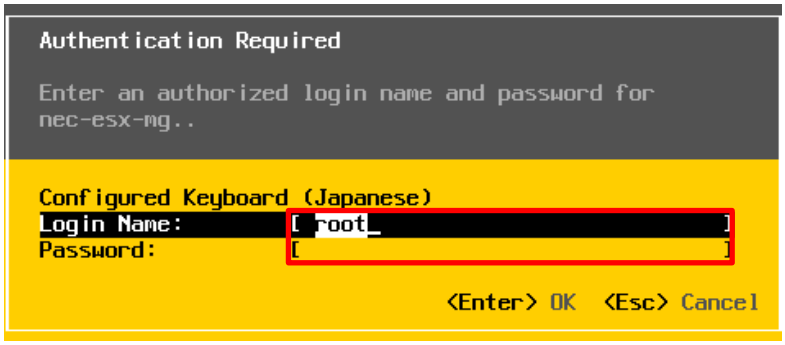
各ノードの ESXi パスワード変更方法手順は同一です。
ESXi パスワード変更方法は、ダイレクトコンソールから変更する方法と、Web ブラウザで Host Client から変更する方法の 2 種類あります。どちらか都合のよい方法を選択し、下記手順を実施してください。

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

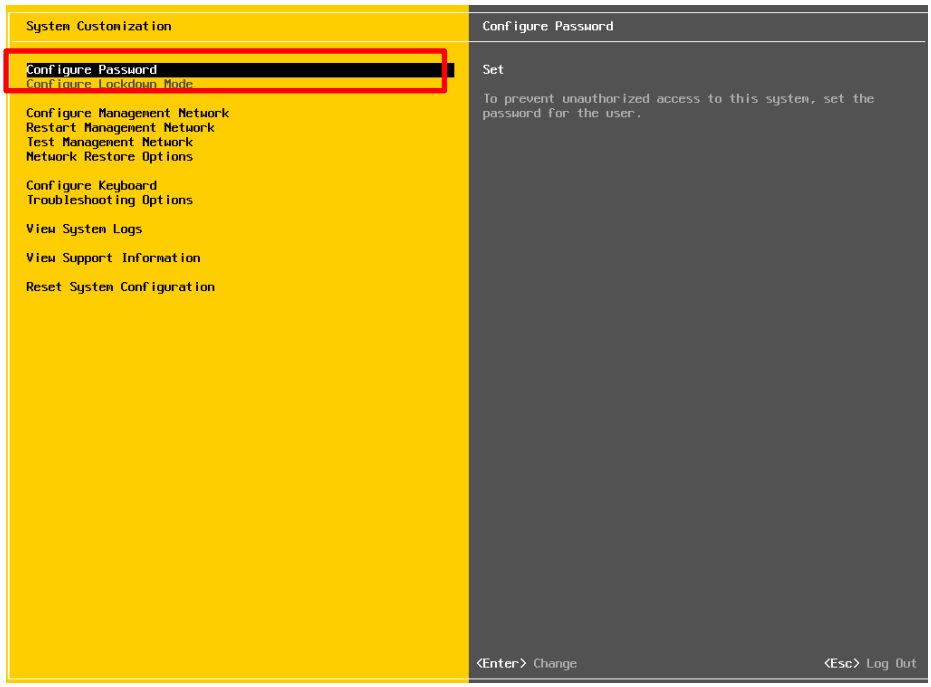
1. ノードにディスプレイとキーボードを接続し、ダイレクトコンソール画面を表示します。



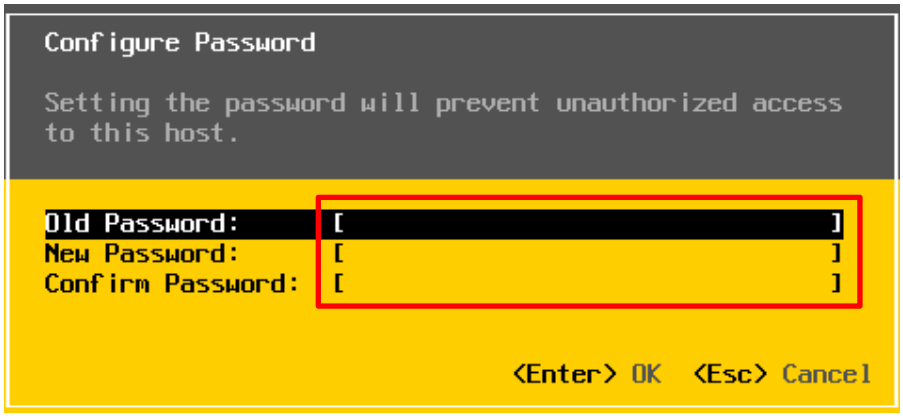
2. ダイレクトコンソール画面から[F2]を押し、ログイン画面を表示します。
   Login Name は「root」とし、Password に root password を入力してログインします。
   (root password は初期パスワード通知書に記載されます)



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. 作業端末上で 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 － 管理用 NW － IP アドレス**>/ui

   または

   https://<**管理ノード － 管理用 NW － IP アドレス**>/ui

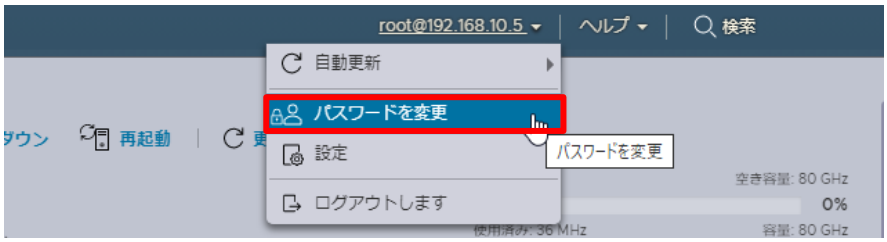
   ※ 「接続がプライベートではありません」画面が表示された場合は、[詳細設定]をクリックし表示された画面で、[*IP アドレスまたは FQDN* に進む(安全ではありません)]クリックしてください。

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

3. 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)

4. 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。

5. 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。



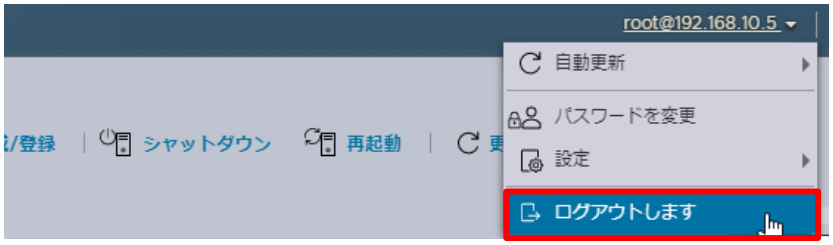
6. パスワードを変更画面が表示されるので、[現在のパスワード]に変更前のパスワードを入力し、[新しいパスワード]、[新しいパスワードの再入力]に変更したいパスワードを入力し、[パスワードを変更]をクリックします。

※ 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。

※ 変更前のパスワードに単語を付け足すだけのような単純な変更をした場合、
以下のエラーが表示されて変更に失敗する場合があります。
詳細は以下の URL を参照してください。

https://knowledge.broadcom.com/external/article?legacyId=2145366

7. 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。



8. 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。

9. すべてのノードで ESXi のパスワード変更を行ってください。

5.4 Witness ノードの ESXi パスワード変更

本章は、2Node 構成の場合のみ実施します。

該当しない場合は、本章は不要です、5.5 章に進んでください。

5.3.1 章または 5.3.2 章を参照し、Witness ノードのパスワードを変更してください。

5.3.1 章を参照してダイレクトコンソールからパスワードを変更する場合、vSphere Client のナビゲータで 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、Witness ノードの ESXi Shell に接続してください。

5.3.2 章を参照して Host Client から ESXi パスワードを更新する場合は、以下の URL を入力して Witness ノードの Host Client に接続します。

https://<**Witness - 管理用 NW – IP アドレス**>/ui

5.5 vCenter Server Appliance(vCSA)のパスワードの変更

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。

5.5.1 vCenter Server Appliance(vCSA)の root パスワードの変更

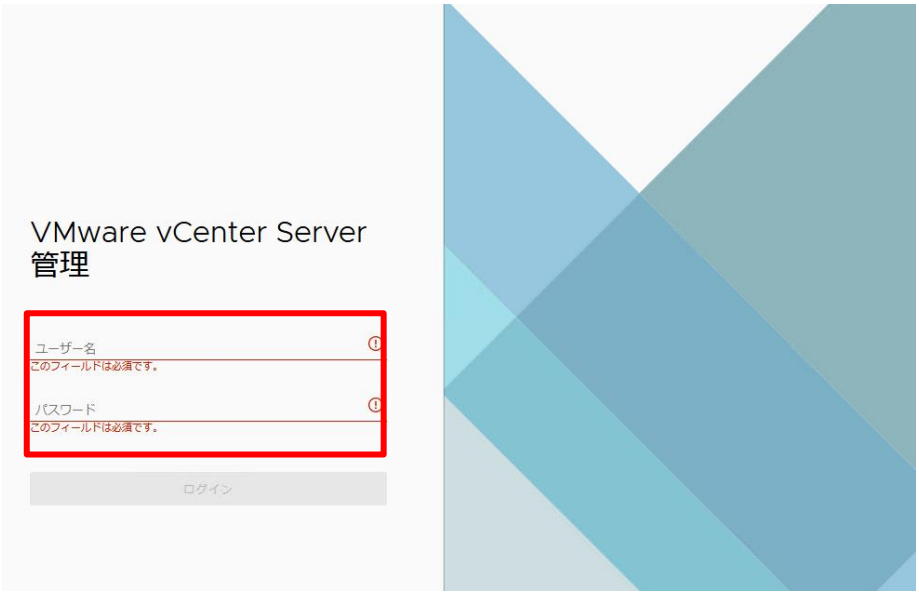
1. 作業端末上で Web ブラウザを起動し、VAMI のログイン用の URL を入力し、VAMI ログイン画面を表示します。

   https://<**vCSA - FQDN**>:5480/

   ※ 「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. Web ブラウザに VAMI のログイン画面が表示されます。

3. 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)

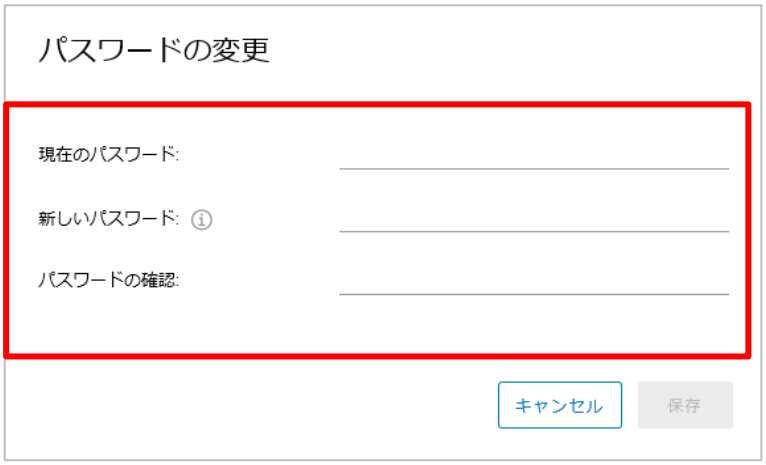


4. 正常にログインすると、Web ブラウザに VAMI の画面が表示されます。

5. 左ツリーから[管理]をクリックします。

6. 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。

7. [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。

8. 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。

9. 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。

5.5.2 vCenter Server の SSO パスワードの変更

1. 作業端末上で、Web ブラウザを起動し、以下の URL を入力し、vSphere Client のログイン画面を表示します。

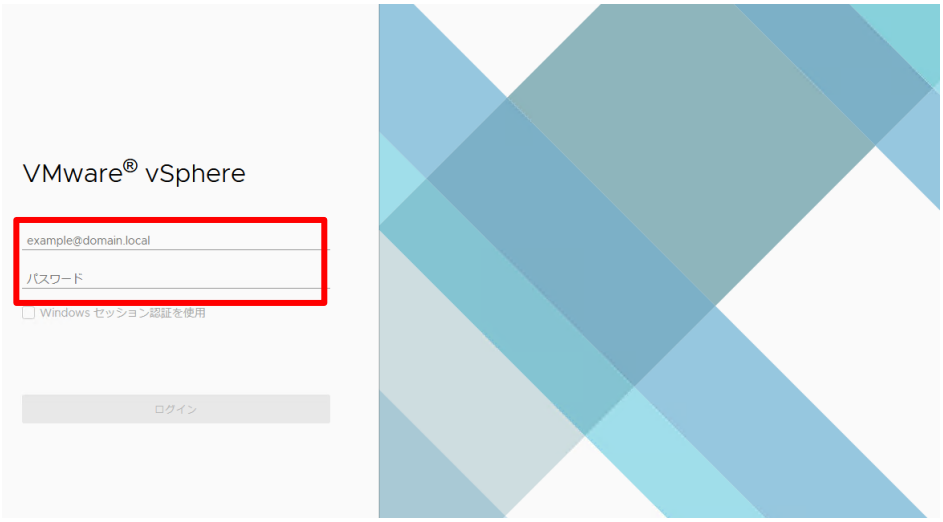
https://<**vCSA - FQDN**>/ui

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

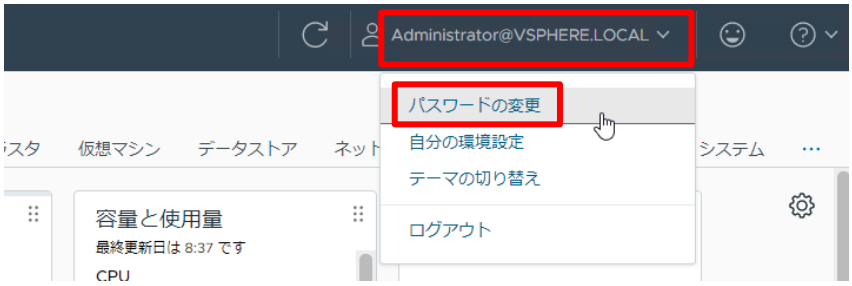
3. ユーザ名、パスワードを入力し、[ログイン]をクリックします。

   ユーザ名: **<vCSA - SSO ユーザ- 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」

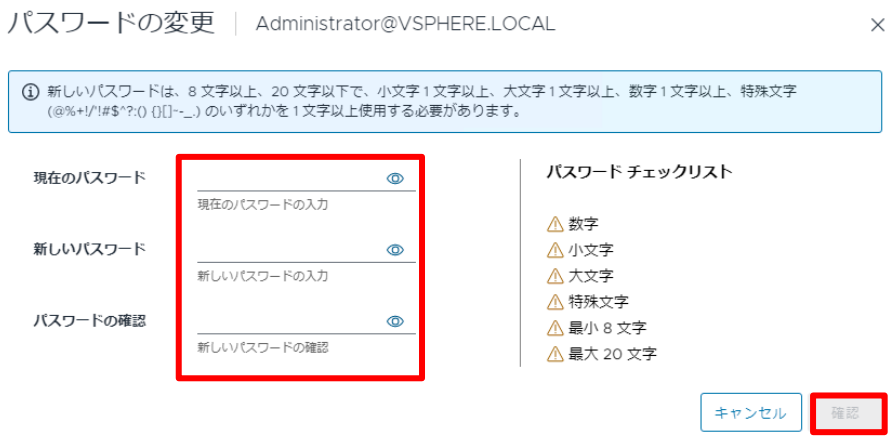


4. 正常にログインすると、vSphere Client の操作画面が表示されます。

5. 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。

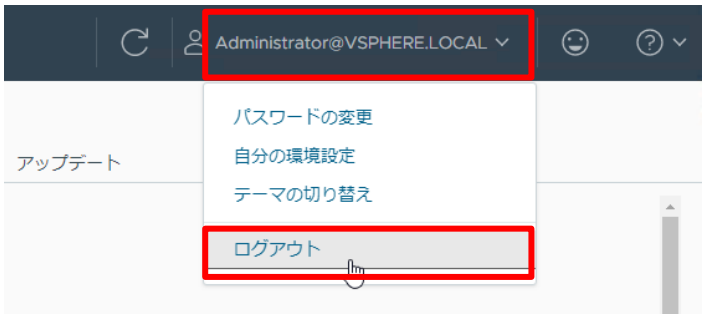


6. パスワードの変更画面が表示されるので、現在のパスワード項目に現在のパスワードを入力し、新しい
パスワード、パスワードの確認項目に変更したいパスワードを入力し、[確認]をクリックします。



※ 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. パスワード変更されたことを確認し、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。



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

5.6 vCenter Server の保守アカウントのパスワード変更

本章では、保守アカウントのパスワード変更について記載します。

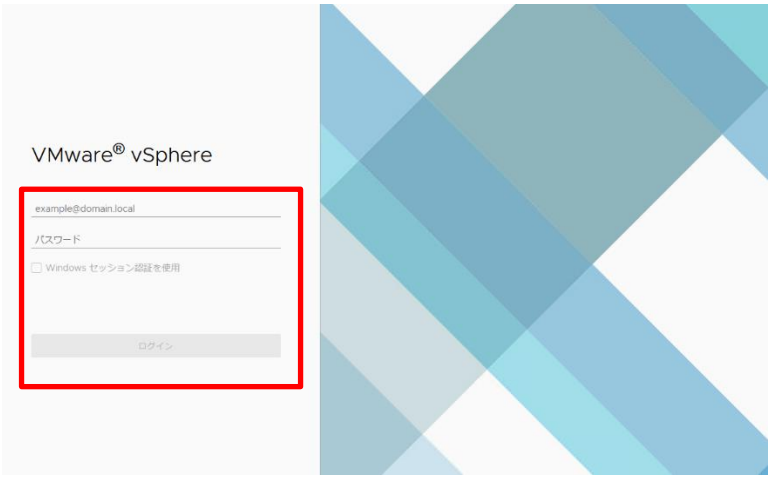
保守アカウントを作成していない場合は本章は不要です。5.7 章に進んでください。

1. Web ブラウザのアドレス欄に以下の URL を入力します。

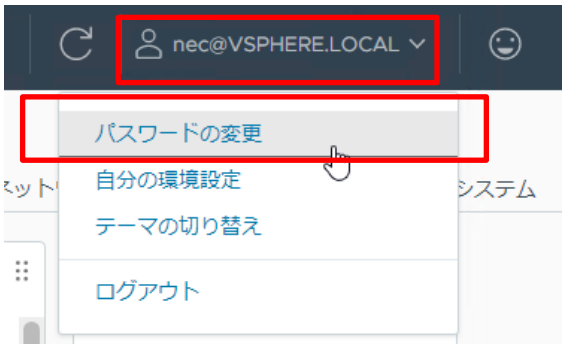
   http://<**vCSA - FQDN**>/ui

   ※ 「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。

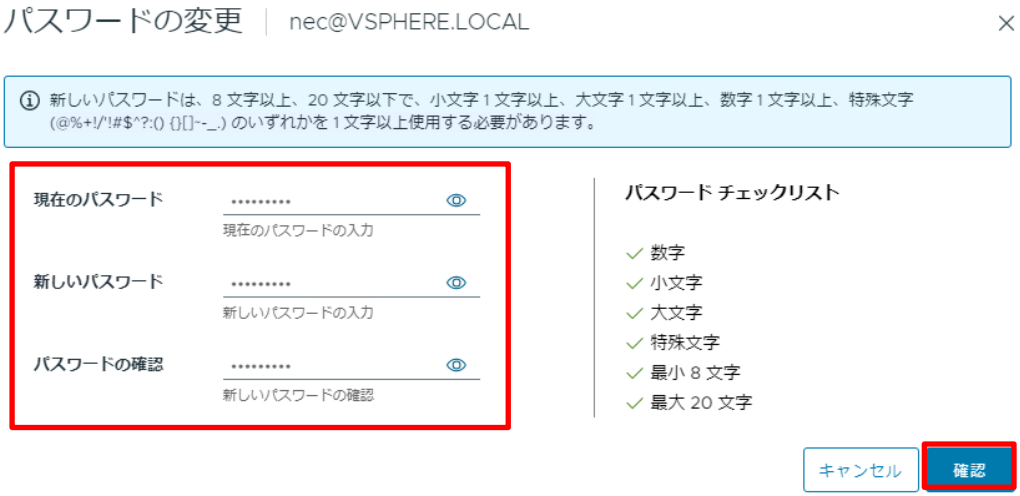
2. 下図のようにログイン画面が表示されたら、保守アカウントでログインします。



3. 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。



4. 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。

5. パスワード変更後、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。

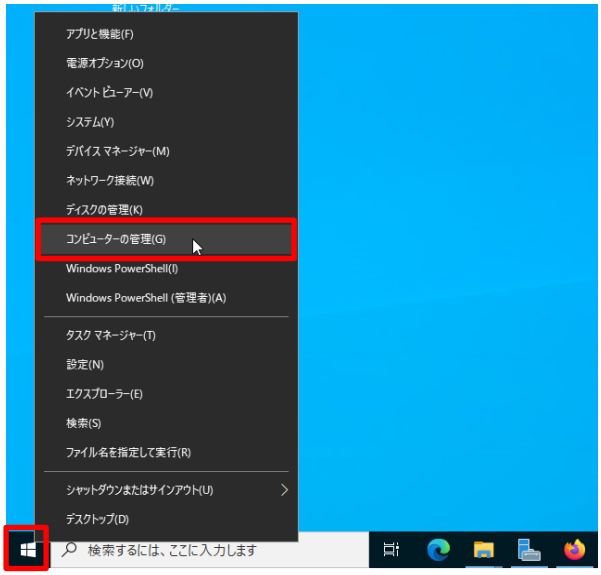
5.7 管理 VM(Windows Server 2022)のパスワード変更

本章は、管理 VM がある構成の場合のみ実施します。

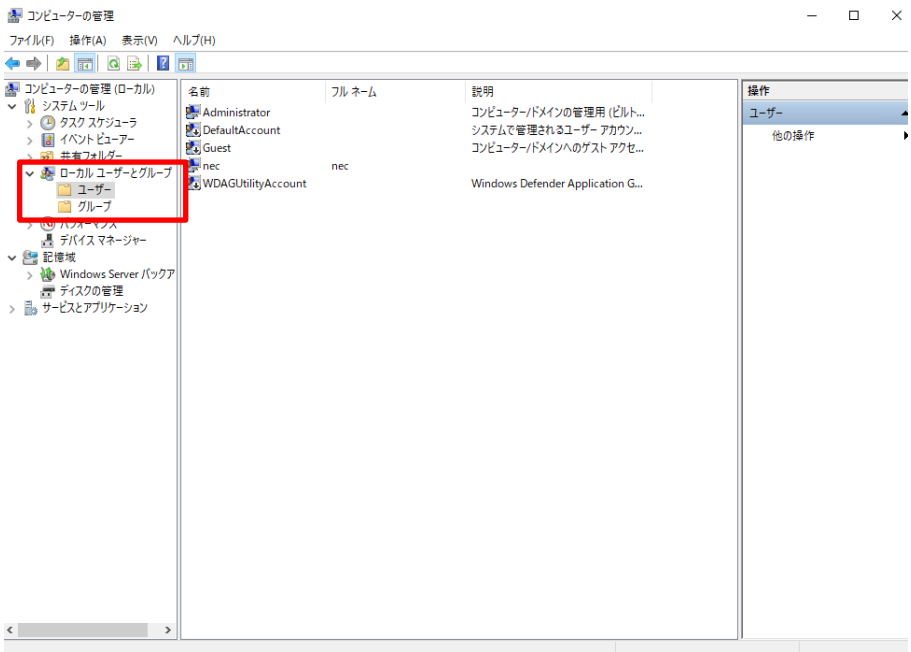
管理 VM がない構成の場合は、6 章に進んでください。

1. 作業端末上でリモートデスクトップ接続(mstsc)を起動し、 **<管理 VM - 管理用 NW - IP アドレス>** を入力し、管理 VM にログインします。

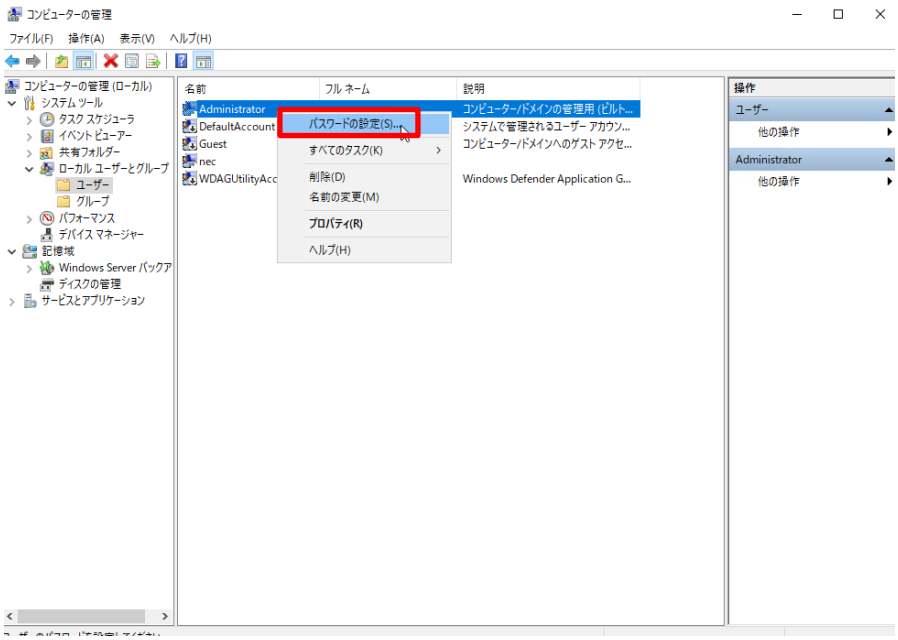
2. 管理 VM のデスクトップ画面のスタートボタンを右クリックして、コンピューターの管理画面を起動します。



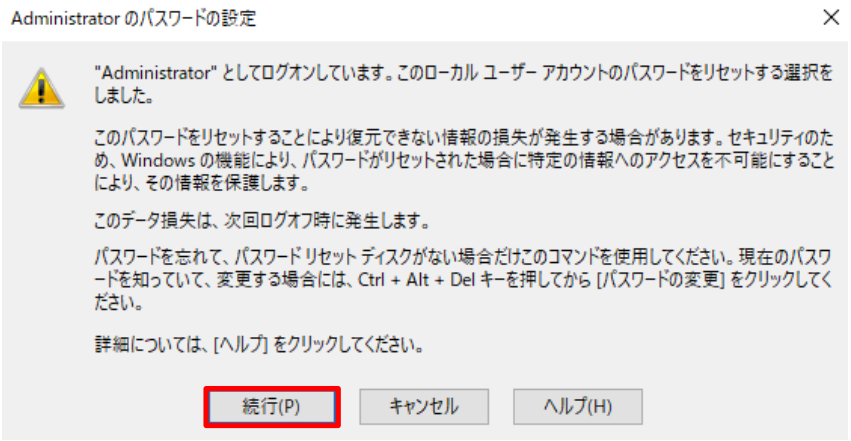
3. コンピューターの管理画面から、[ローカルユーザーとグループ]-[ユーザー]をクリックし、ユーザー一覧を表示させます。



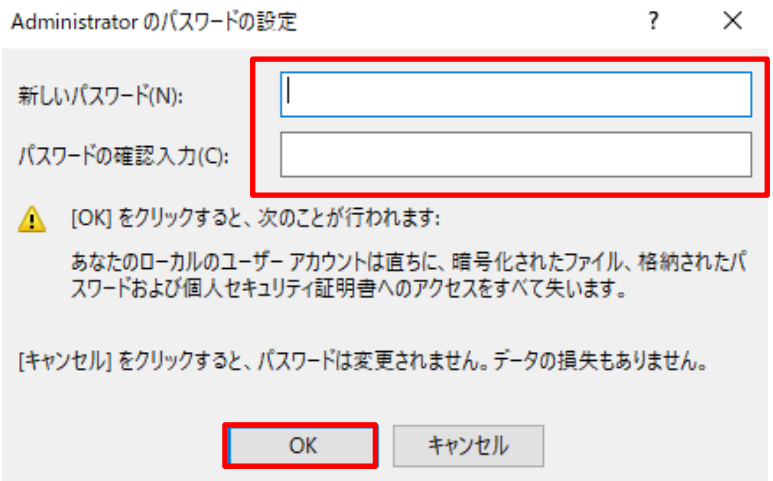
4. “Administrator”ユーザを選択し、マウスを右クリックして、[パスワードの設定]”を選択します。



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。

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

本章は、管理 VM がある構成の場合のみ実施します。

管理 VM がない構成の場合は、6 章に進んでください。

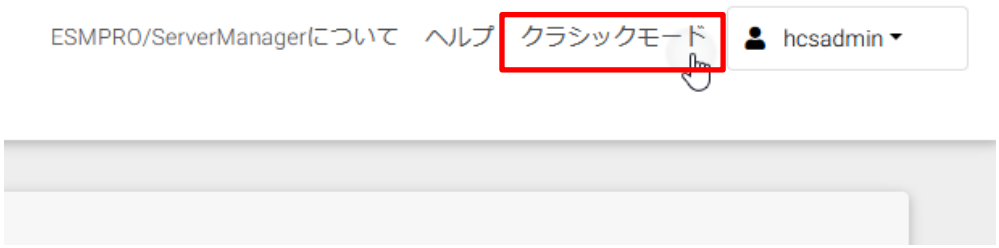
1. 作業端末上でリモートデスクトップ接続(mstsc)を起動し、 **<管理 VM - 管理用 NW - IP アドレス>** を入力し、管理 VM にログインします。

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。

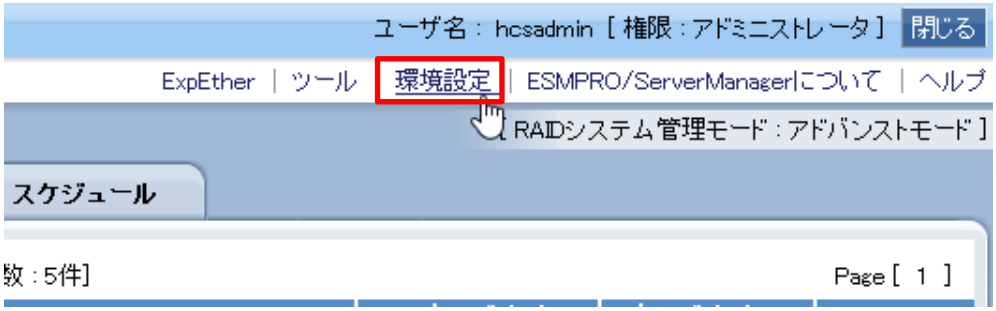
   http://<**管理 VM - FQDN**>:21120/esmpro

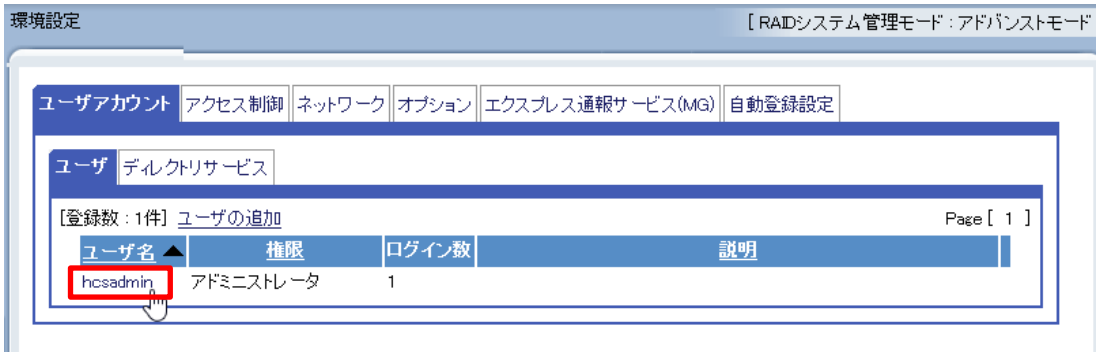
3. ESMPRO/ServerManager のログイン画面で、ユーザ名・パスワードを入力し、ログインします。
   (ユーザ名、パスワードは初期パスワード通知書に記載されます)

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。

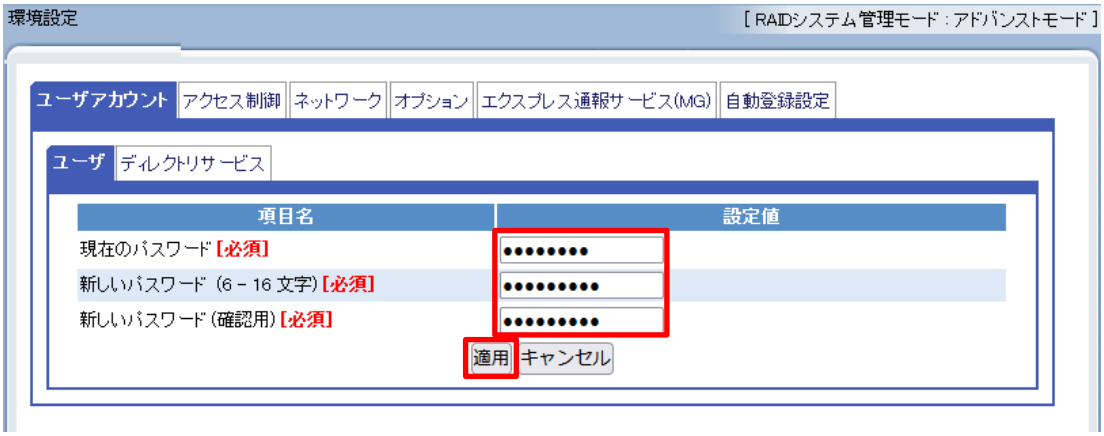




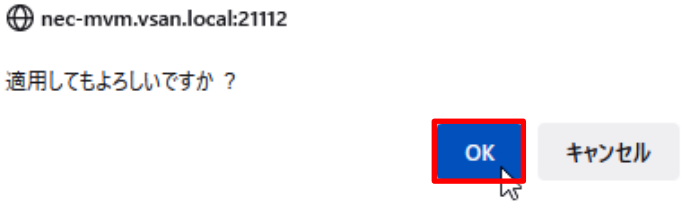
6. 環境設定：ユーザアカウント画面の初期 ID のユーザ情報画面で、[パスワードの変更]をクリックします。

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。

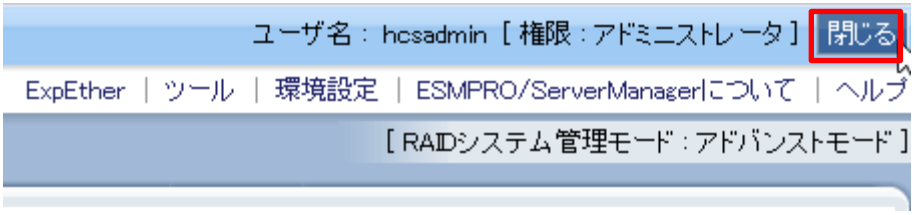
※ パスワードの要件は、初期パスワード通知書の「1.2 パスワード要件」を参照ください。



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。



5.9 ESMPRO/ServerManager の登録情報の更新

本章は、管理 VM がある場合のみ実施してください。

管理 VM がない構成の場合は、6 章に進んでください。

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。

1. 5.8 章の手順 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。

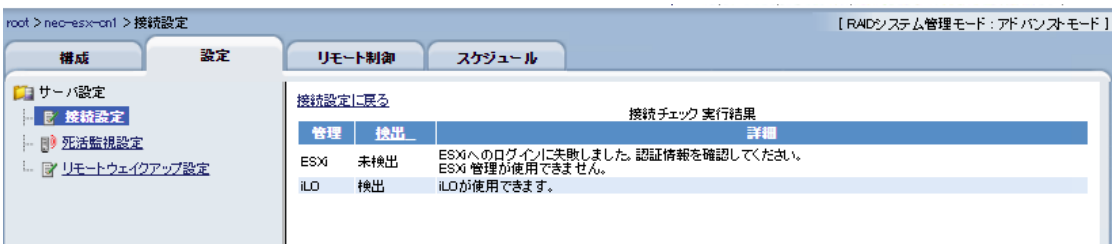
3. 変更後の BMC および ESXi のパスワードを入力し、[適用]をクリックします。

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

《補足》
接続チェックの結果 ESXi が「未検出」となる場合があります。



この場合、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、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 3.11 章を参照し、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-cn1:~] /etc/init.d/hostd restart
watchdog-hostd[1610194]: Terminating watchdog process with PID 1051550 1050944
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-cn1:~] /etc/init.d/vpxa restart
watchdog-vpxa[1610569]: Terminating watchdog process with PID 1052064
vpxa stopped.
vpxa started.
```

この後、再度本章の手順 5 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。

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。

5.10 サーバ診断カルテの登録情報の更新

本章は、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。

サーバ診断カルテを利用していない場合は、6 章に進んでください。

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 <クラスタノード- 管理用 NW - 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 192.168.0.11 /u root /p P@ssw0rd2
```

```
# MIOT_MNG_AUTH.exe /i <管理 VM - 管理用 NW - 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 192.168.0.15 /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(192.168.0.15). 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     : "192.168.0.11"
  User         : "root"
IP Address     : "192.168.0.12"
  User         : "root"
IP Address     : "192.168.0.13"
  User         : "root"
IP Address     : "192.168.0.15"
  User         : "Administrator"
```

6 チェックシートの確認

本書の作業が完了しましたら、本書の最後にある別紙の「受入検査チェックシート」を参照し、
作業漏れがないことを確認してください。

7 注意制限事項

7.1 iLO Security について

iLO Security において、TPM が搭載されていないサーバの場合、
「セキュアブート(Secure Boot)」のステータスが「リスク(Risk)」になっていますが、「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

本書に関する注意と補足

MEMO

別紙　受入検査チェックシート

検査日＿＿＿＿＿＿＿＿＿＿

ご担当＿＿＿＿＿＿＿＿＿＿

	実施対象	項目	チェック	確認者	メモ
1	すべて	構成品の確認	□		
2	すべて	各ノード(サーバ)の設置	□		
3	すべて	ネットワーク装置への接続	□		
4	すべて	電源の接続	□		
5	すべて	管理用ネットワークへの接続	□		
6	すべて	DNSクライアントの設定	□		
7	すべて	DNSの疎通確認	□		
8	すべて	NTPクライアントの設定	□		
9	すべて	NTPの同期設定	□		
10	すべて	作業端末の準備	□		
11	管理ノードあり	管理ノードの電源オンとvCenter Serverへの接続確認	□		
12	すべて	クラスタノードの電源オン	□		
13	管理ノードなし	vCenter Serverへの接続確認	□		
14	2Node構成	Witnessの電源オン	□		
15	すべて	vCenter Server上での機器確認	□		
16	2Node構成以外	隔離IPの到達確認	□		
17	すべて	NTPの動作確認	□		
18	2Node構成	Witnessノードのメンテナンスモード解除	□		
19	すべて	vSANサービスの再起動	□		
20	すべて	vSANストレージプロバイダの同期	□		
21	TPMあり	TPMのリカバリキーのバックアップ	□		
22	すべて	vSAN状態の確認(健全性確認)	□		
23	管理VMあり	管理VMの起動と接続確認	□		
24	エクスプレス通報サービスあり	エクスプレス通報サービスの開局手続き	□		
25	サーバ診断カルテあり	サーバ診断カルテの開局手続き	□		
26	すべて	ライセンス登録	□		
27	すべて	パスワード変更	□		