

NEC Hyper Converged System for VMware vSAN/CR1.0 スタートアップガイド



目次

1	本ガイドについて	1
1.1	NEC Hyper Converged System	1
1.2	お問い合わせ先	1
1.3	用語の定義	2
2	事前準備	3
2.1	ご用意いただくもの	3
3	受入確認	4
3.1	概要	4
3.2	構成品の確認	5
3.3	本製品の設置	6
3.4	ネットワーク装置への接続	6
3.5	電源の接続	6
3.6	管理ノードの電源オン	7
3.7	Windows PC の準備	8
3.8	Windows PC から管理 VM に接続	8
3.9	DNS 疎通確認	10
3.10	VMware vCenter Server への接続確認	11
3.11	クラスターノード、Witness ノードの電源オン	13
3.12	VMware vCenter Server 上での機器確認	16
3.13	隔離 IP の到達確認	18
3.14	クラスターノード、Witness ノードのメンテナンスモード解除	23
3.15	vSphere の可用性設定	24
3.16	vSAN ストレージプロバイダの同期	26
3.17	VMware vSAN 状態の確認(健全性確認)	28
3.18	NEC Hyper Converged System Console の動作確認	30
4	ライセンス登録	35
4.1	vCenter Server、ESXi、vSAN ライセンスの登録	35
4.2	Windows Server 2016 のライセンス登録	42
4.3	NEC Hyper Converged System Console のライセンス登録	45
5	パスワード変更	46
5.1	概要	46
5.2	クラスターノード、管理ノードの BMC の ID・パスワード変更	48
5.3	クラスターノード、管理ノードの ESXi パスワードの変更	52
5.4	管理ノードの vCSA パスワードの変更	57
5.5	管理ノードの管理 VM(Windows Server 2016)のパスワード変更	63
5.6	管理 VM の ESM/ServerManager のパスワード変更	66
5.7	NEC Hyper Converged System Console のパスワード変更	69
5.8	管理ノードの Witness ノードのパスワード変更	72
5.9	NEC Hyper Converged System Console の登録情報の更新	75
5.10	保守アカウントのパスワード変更	78
6	注意制限事項	84
6.1	iLO Security について	84

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。
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)

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 2016 の仮想マシン。HCS の管理や、HCS 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。
Virtual Appliance Management Infrastructure (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 Web Client (Flash 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 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)
- Windows Server 2016 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)
 - ◇ 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)
- (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 v2.0 インストレーションガイド(1 版、Web ダウンロード)
 - NEC Hyper Converged System Console v2.0 ユーザーズガイド(1 版、Web ダウンロード)
 - NEC Hyper Converged System/運用ガイド (1 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 17 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. クラスタノード、Witness ノードのメンテナンスモード解除
14. vSphere の可用性設定
15. vSAN ストレージプロバイダの同期
16. VMware vSAN 状態の確認
17. NEC Hyper Converged System Console の動作確認

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られません。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

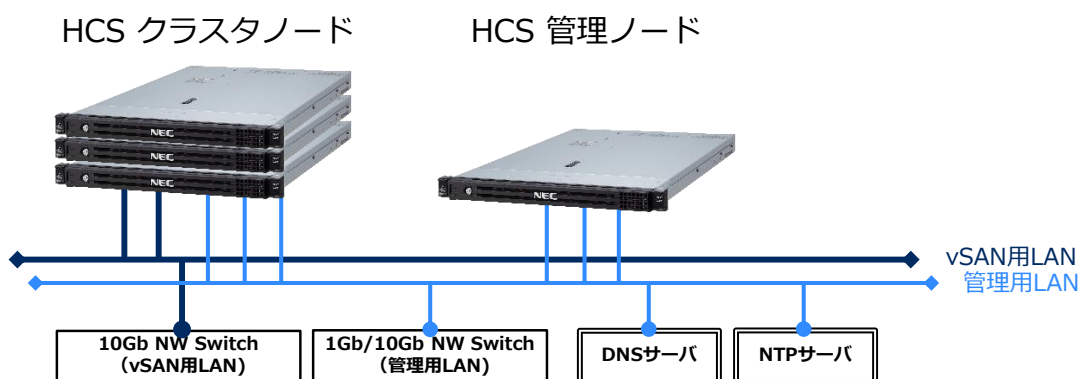
本製品を使用する前に、19 インチラックなど安全に固定できる器具に搭載し、電源を接続する必要があります。本製品に同封されるスタートアップガイド、または NEC Web サイトから入手できる HCS ベースモデル(R120h-1M/2M)の製品マニュアル(ユーザズガイド)を元に、設置を行ってください。

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 0 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。

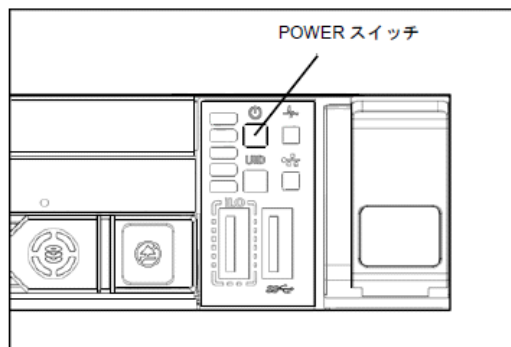
NEC Hyper Converged System 管理ノード(サーバ)の電源をオンにします。DNS サーバ(お客様の DNS サーバを使用する場合)とネットワーク機器の電源オン確認後、管理ノードの電源をオンしてください。

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。

```
VMware ESXi 6.7.0 (VMKernel Release Build 13981272)
NEC Express5800/R120h-1M
2 x Intel(R) Xeon(R) Bronze 3104 CPU @ 1.70GHz
127.7 GiB Memory

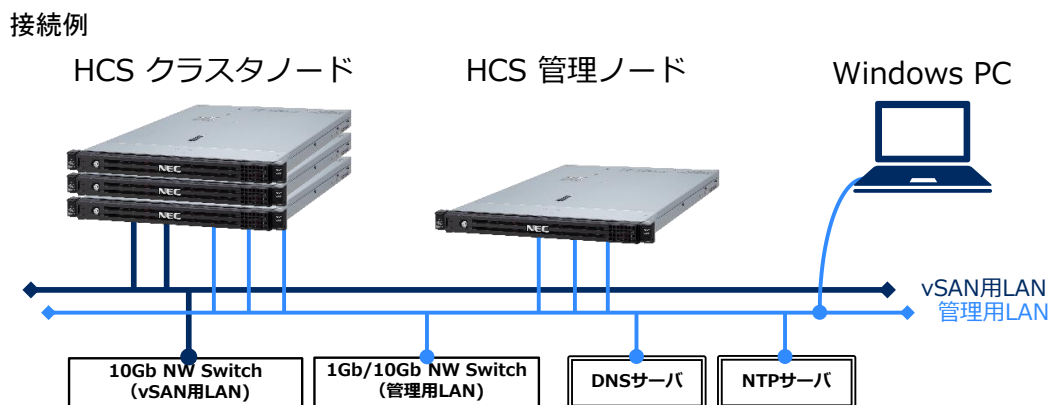
To manage this host go to:
http://nec-esx-ng/
http://192.168.12.10/ (STATIC)
```

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。



《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

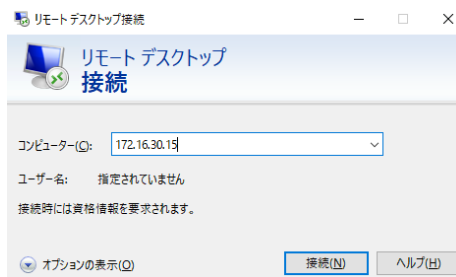
ドキュメント	項目	パラメータ/値 (メモ用)
初期パスワード通知書	Administrator ユーザのパスワード	
ヒアリングシート	管理 VM の IP アドレス (【事前確認項目の転記】の「管理 VM のお客様環境用の IP アドレス」または「管理 VM の管理用ネットワークの IP アドレス」)	
ヒアリングシート	管理 VM のサブネットマスク (【事前確認項目の転記】の「管理 VM のお客様環境用のサブネットマスク」または「管理用ネットワークのサブネットマスク(共通)」)	
	Windows PC に設定する IP アドレス	

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 節の問い合わせ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。

- 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。)
- 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。

- 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	r120h-1m-0.vsan.local	172.16.10.15
例)DNS サーバ	hcsmgr01.vsan.local	172.16.30.15
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		

```

Microsoft Windows [Version 10.0.14393]
(c) 2016 Microsoft Corporation. All rights reserved.

C:\Users\Administrator>nslookup r120h-1m-0.vsan.local
サーバー: hcsmgr01.vsan.local ----->参照元の DNS サーバホスト名
Address: 172.16.30.15 ----->参照元の DNS サーバ IP アドレス

名前: r120h-1m-0.vsan.local ----->nslookup したホスト名
Address: 172.16.10.15 ----->nslookup したホスト名の IP アドレス

-----

C:\User\Administrator>nslookup -type=ptr 172.16.10.15
サーバー: hcsmgr01.vsan.local ----->参照元の DNS サーバホスト名
Address: 172.16.30.15 ----->参照元の DNS サーバ IP アドレス

15.10.16.172.in-addr.arpa name = r120h-1m-0.vsan.local ->nslookup した IP の逆引きアドレスと name (ホ
  
```

- 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

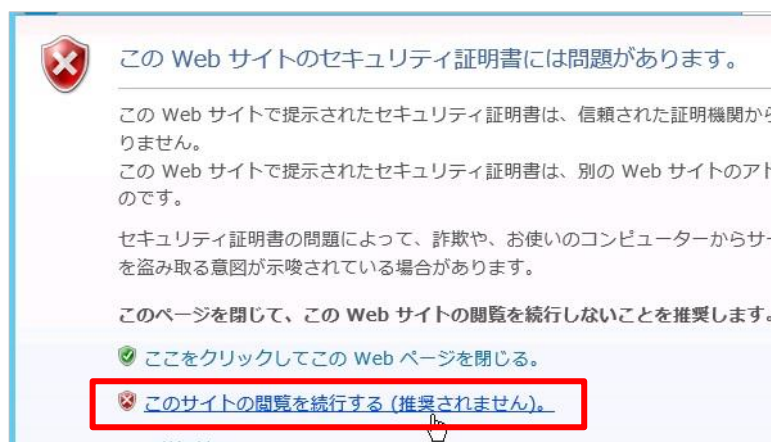
管理 VM 上で Web ブラウザを起動し、VMware vSphere Client (VMware vCenter Server)に接続します。

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(Internet Explorer)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://vcenter.vsan.local/ui>

- ※ 「この Web サイトのセキュリティ証明書には問題があります。」画面が表示された場合は、「このサイトの閲覧を続行する(推奨されません)。」をクリックしてください。

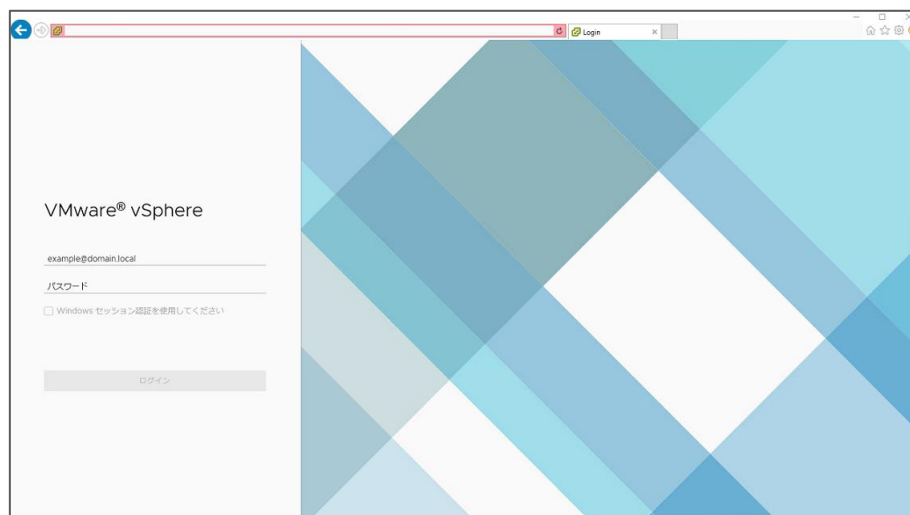


2. 下記図のように VMware vCenter Server のログイン画面が表示されましたら、ユーザ名、パスワードを入力し、ログインします。

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」





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はありませんか？
(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 節の問い合わせ先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。



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。

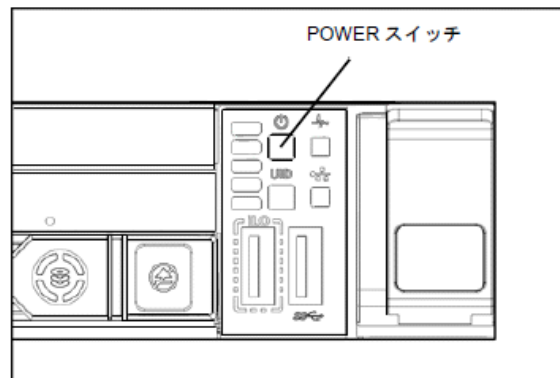
<https://kb.vmware.com/s/article/60424?lang=ja>

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:

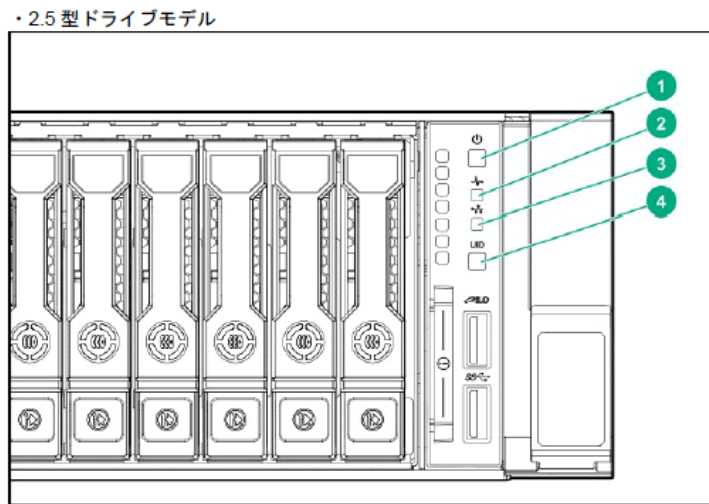
以下の図の POWER スイッチを、各ノード分、順次、押下して、電源オンしてください。

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。

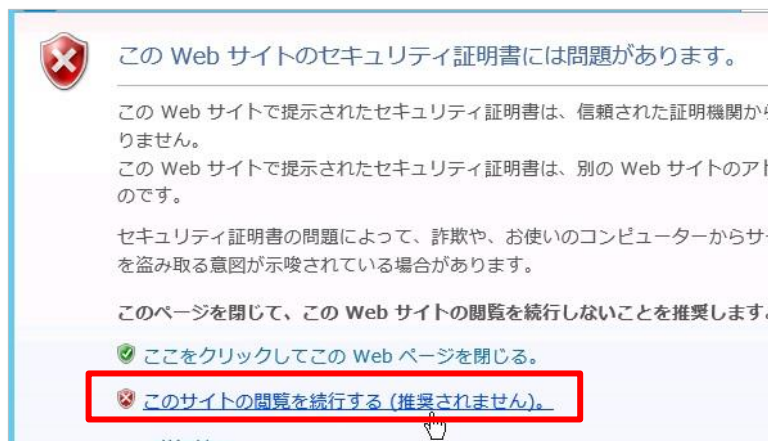


2 ノード構成の場合は、Host Client の画面で以下手順を実行して Witness ノードの電源をオンにしてください。

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`

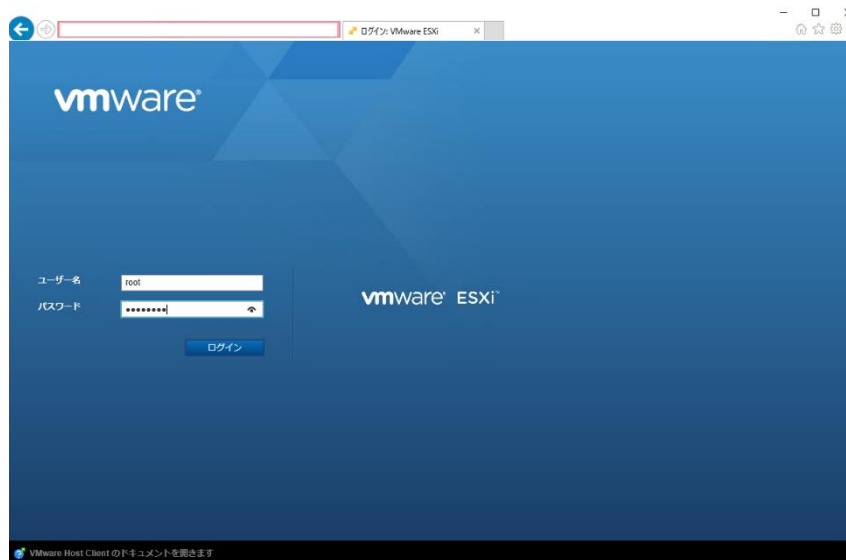
※ 「この Web サイトのセキュリティ証明書には問題があります。」画面が表示された場合は、「このサイトの閲覧を続行する (推奨されません)。」をクリックしてください。



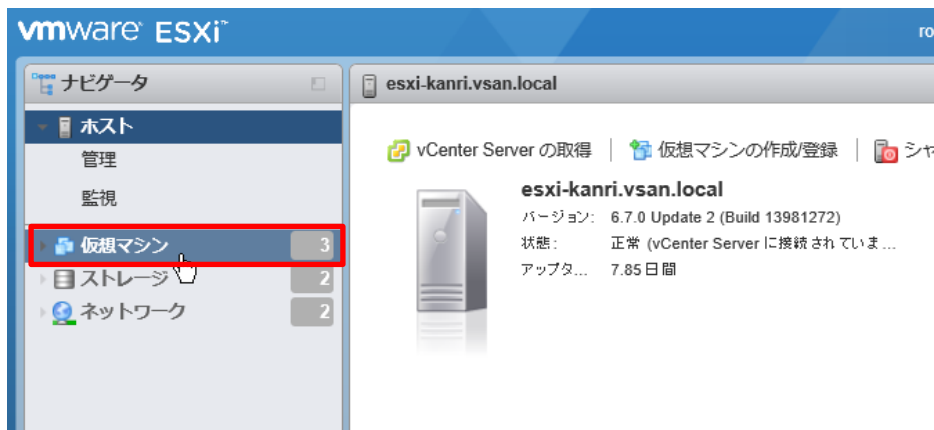
2. 下記図のように Host Client のログイン画面が表示されましたら、ユーザ名、パスワードを入力し、ログインします。

ユーザ名: root

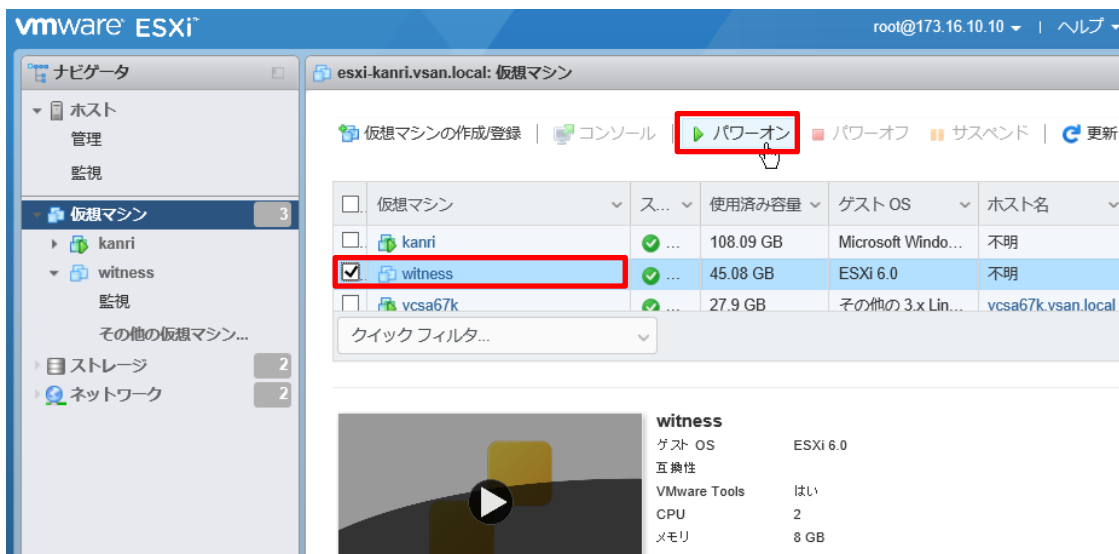
パスワード: 初期パスワード通知書の管理ノードの「ESXi の root パスワード」



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。



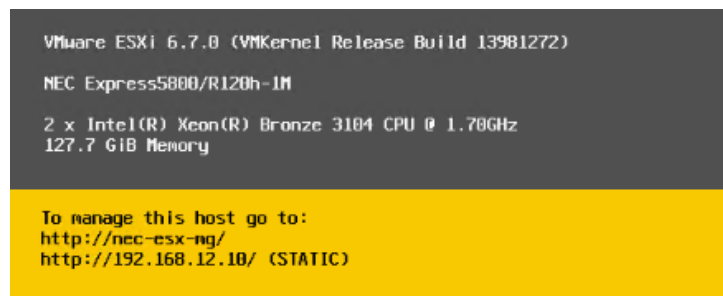
3.12 VMware vCenter Server 上での機器確認

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。

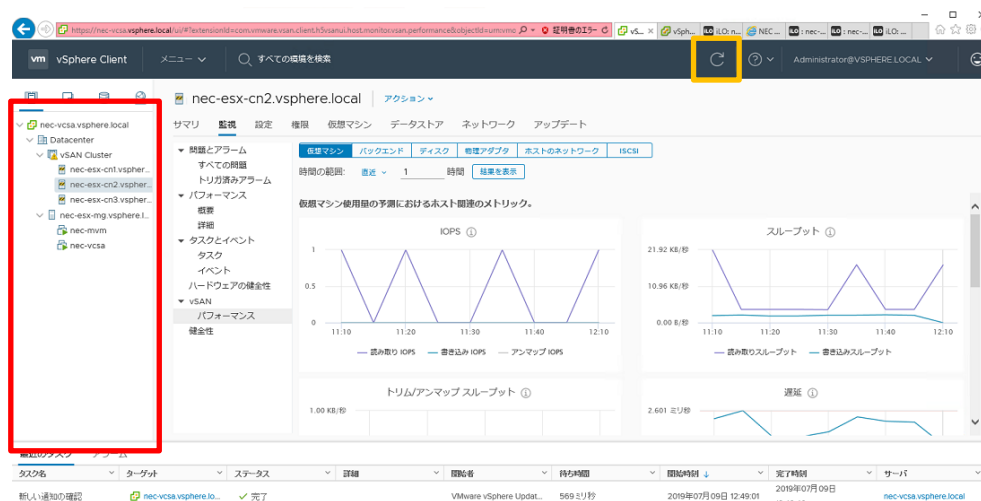
2. 3.10 節で接続した VMware vSphere Client のホーム画面左側のメニュー(下記赤枠)から、[ホストおよびクラスタ]をクリックします。

※ 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。



- 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。



- 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や、表示されている機器に異常がある場合は、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 節の問い合わせ窓口までご連絡ください。

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》

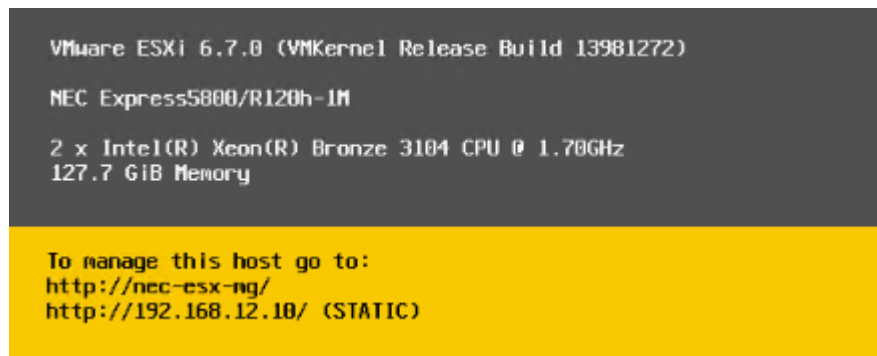
以降の操作は①Windows PC から SSH で ESXi Shell にログイン ②クラスタノードにキーボード・マウスを接続し、ローカルコンソール(ダイレクトコンソール)で ESXi Shell にログイン の 2 方法どちらでも実施することができます。本項では①の方法で確認を行います。

《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。



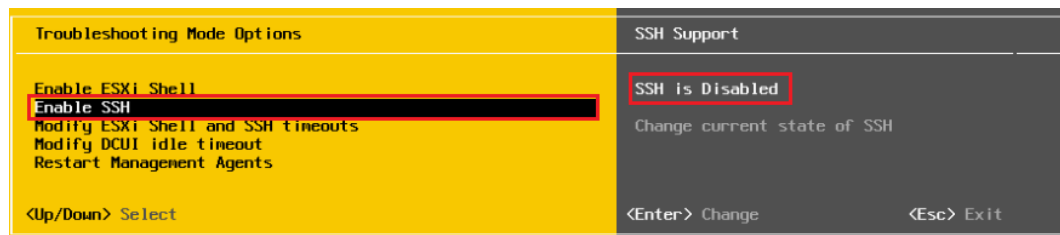
- ③ 「Troubleshooting Mode Options」の画面で[Enable SSH]を選択した状態で[Enter]キーを押下し、画面右のメニューの表示が[SSH is Enabled]に更新されることを確認します。
以上で SSH 有効化は完了です。

※ 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。



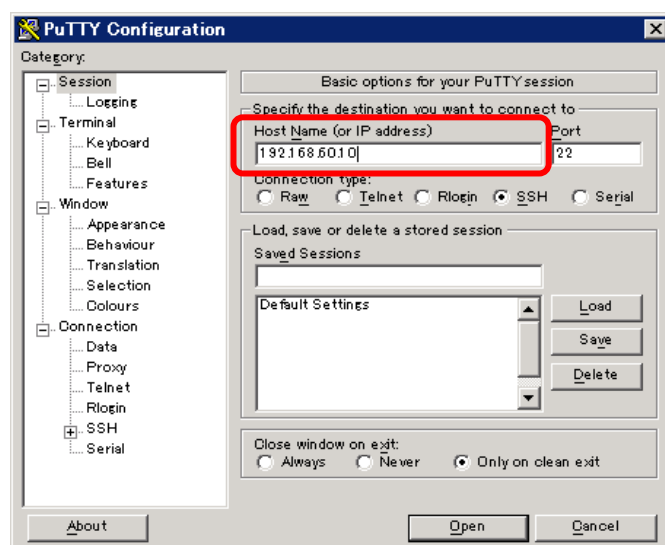
- ④ SSH を無効化する場合は、①から②の操作後、「Troubleshooting Mode Options」の画面で [Disable SSH]を選択した状態で[Enter]キーを押下し、画面左のメニューの表示が[SSH is Disabled]に更新されることを確認します。

※ 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。

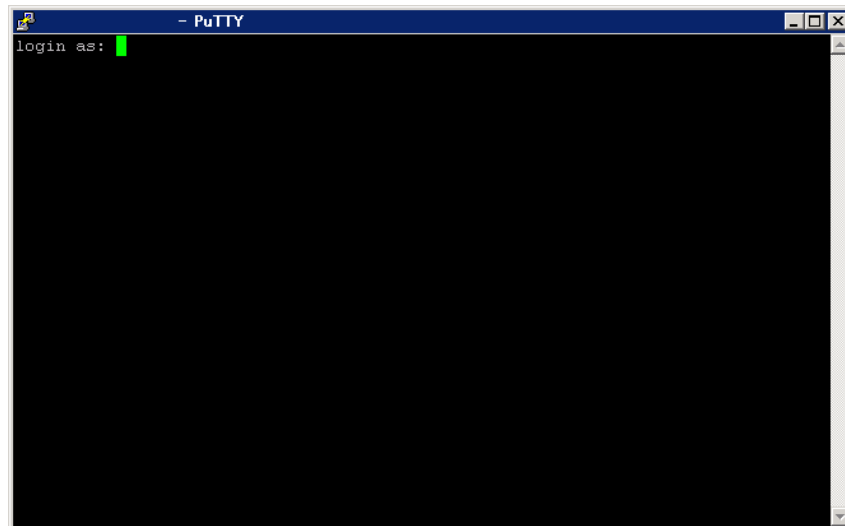


1. Windows PC 上で SSH クライアント(例: PuTTY)を起動します。

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。

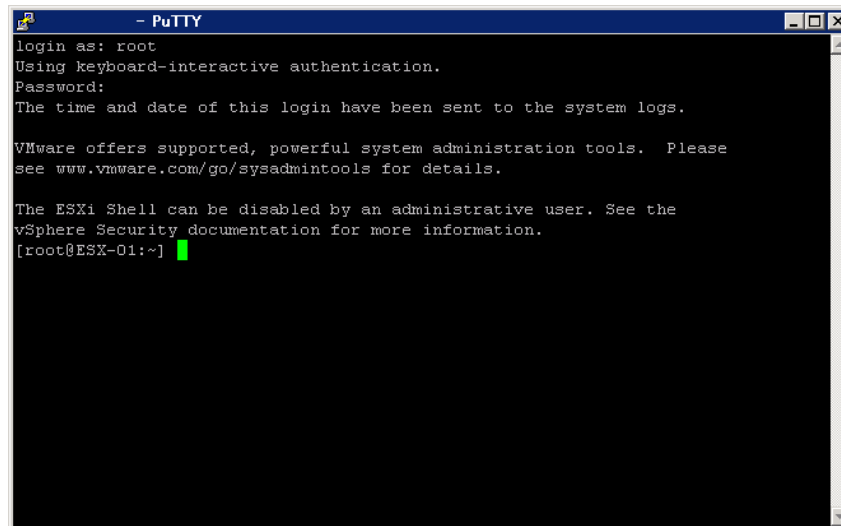
「login as: 」と表示された画面にキーボードで「root」と入力し「Enter」キーを押下します。

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。



```

- PuTTY
login as: root
Using keyboard-interactive authentication.
Password:
The time and date of this login have been sent to the system logs.

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

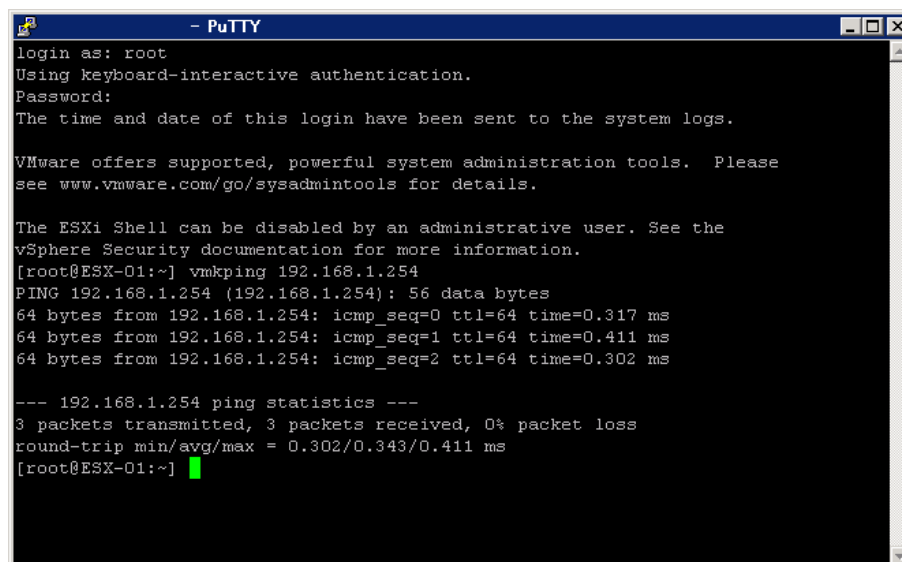
The ESXi Shell can be disabled by an administrative user. See the
vSphere Security documentation for more information.
[root@ESX-01:~]

```

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。



```

- PuTTY
login as: root
Using keyboard-interactive authentication.
Password:
The time and date of this login have been sent to the system logs.

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@ESX-01:~] vmkping 192.168.1.254
PING 192.168.1.254 (192.168.1.254): 56 data bytes
64 bytes from 192.168.1.254: icmp_seq=0 ttl=64 time=0.317 ms
64 bytes from 192.168.1.254: icmp_seq=1 ttl=64 time=0.411 ms
64 bytes from 192.168.1.254: icmp_seq=2 ttl=64 time=0.302 ms

--- 192.168.1.254 ping statistics ---
3 packets transmitted, 3 packets received, 0% packet loss
round-trip min/avg/max = 0.302/0.343/0.411 ms
[root@ESX-01:~]

```

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。

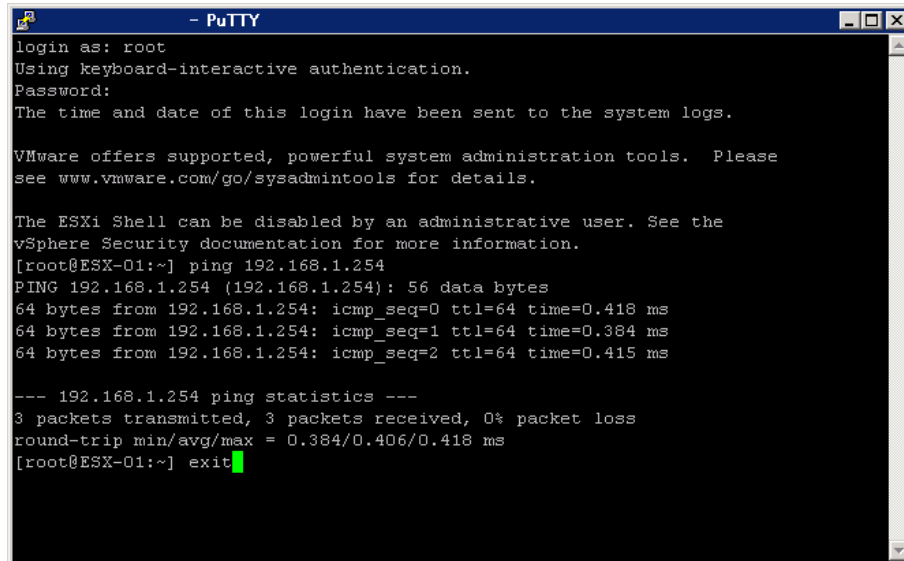
《参考》

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。



```
- PuTTY
login as: root
Using keyboard-interactive authentication.
Password:
The time and date of this login have been sent to the system logs.

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@ESX-01:~] ping 192.168.1.254
PING 192.168.1.254 (192.168.1.254): 56 data bytes
64 bytes from 192.168.1.254: icmp_seq=0 ttl=64 time=0.418 ms
64 bytes from 192.168.1.254: icmp_seq=1 ttl=64 time=0.384 ms
64 bytes from 192.168.1.254: icmp_seq=2 ttl=64 time=0.415 ms

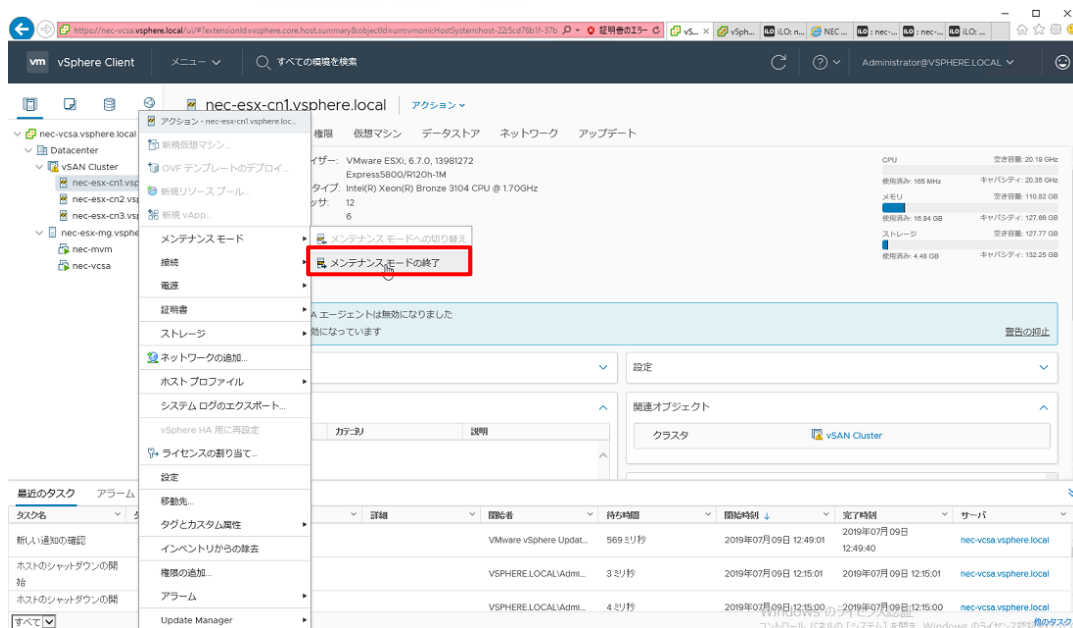
--- 192.168.1.254 ping statistics ---
3 packets transmitted, 3 packets received, 0% packet loss
round-trip min/avg/max = 0.384/0.406/0.418 ms
[root@ESX-01:~] exit
```

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

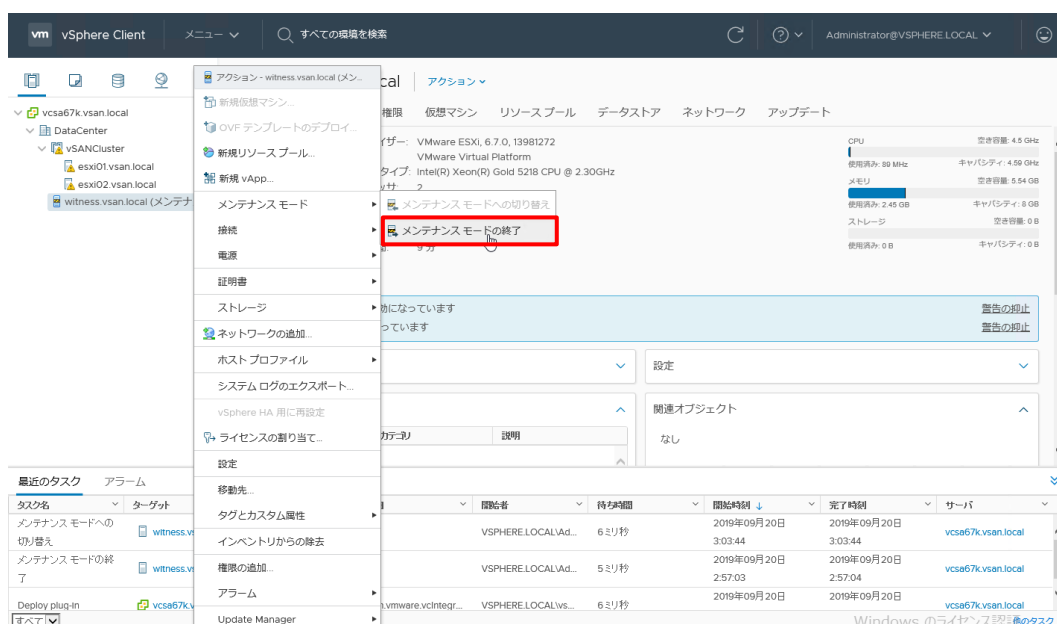
3.14 クラスタノード、Witness ノードのメンテナンスモード解除

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。

- 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 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。



3.15 vSphere の可用性設定

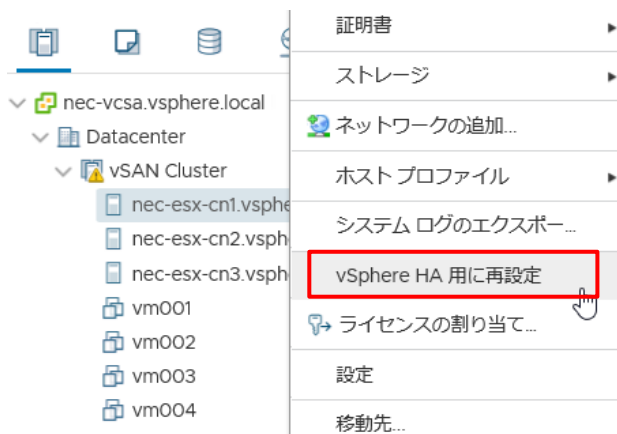
2 ノード構成の場合は、本節の実施は不要です。

vSAN クラスタの vSphere の可用性を設定します。

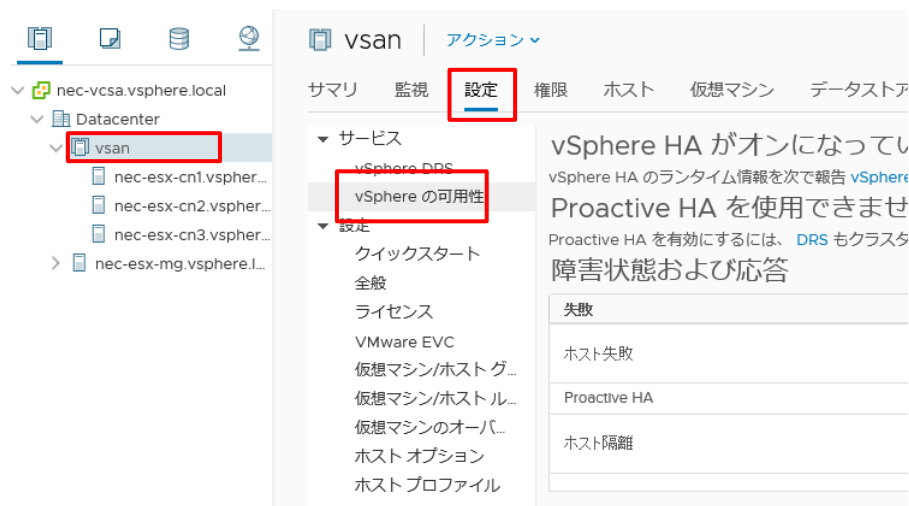
1. 3.10 節で接続した VMware vSphere Client のホーム画面を表示している状態でナビゲータの [ホストおよびクラスタ] をクリックします。



2. 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。



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



4. 画面右上の「編集」をクリックします。



5. 「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。



6. 「障害状態および応答」が下記図の状態（「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。

vSphere HA がオンになっています
vSphere HA のランタイム情報を次で報告 [vSphere HA の監視](#)
Proactive HA を使用できません
Proactive HA を有効にするには、[DRS](#) もクラスタ上で有効にする必要があります。

障害状態および応答

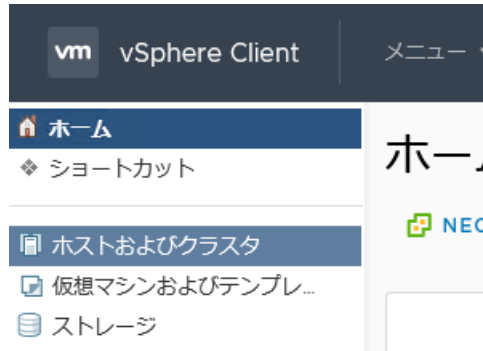
失敗	対応
ホスト失敗	✓ 仮想マシンを再起動
Proactive HA	! 無効
ホスト隔離	✓ 仮想マシンをパワーオフして再起動
PDL (Permanent Device Loss) 状態のデータストア	! 無効

3.16 vSAN ストレージプロバイダの同期

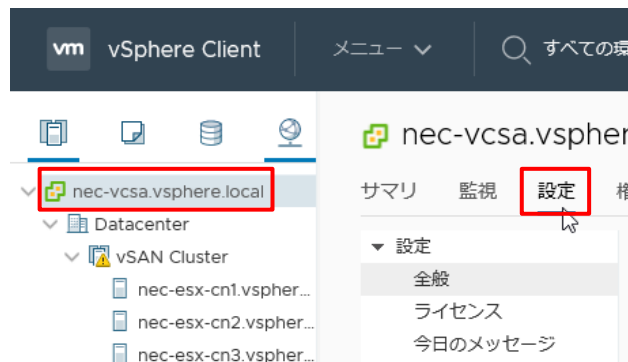
下記の問題を回避するために、vSAN ストレージプロバイダの同期を行います。

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

- 3.10 節で接続した VMware vSphere Client のホーム画面を表示している状態でナビゲータの [ホストおよびクラスタ] をクリックします。



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



- [詳細] → [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。



The screenshot shows the VMware vSphere interface with the 'Storage Providers' tab selected. The 'VMware vSAN' entry is highlighted with a red box. The 'Sync Storage Provider' button is also highlighted with a red box.

ストレージプロバイダ/ストレージ...	ステータス	アクティブ/スタンバイ	優先順位	URL
5d4019d5-0c2e-68f2-7f93-...	有効	1		
▲ IOFILTER Provider nec-esx-cn...	オンライン	--	--	https://nec-esx-cr...
5d4019d1-52f9-449c-1970-...	有効	1		
▲ IOFILTER Provider nec-esx-m...	オンライン	--	--	https://nec-esx-m...
5d4019a8-0dc7-05de-b1fe-...	有効	1		
▲ VMware vSAN	オンライン	--	--	https://nec-vcsa.v...
内部管理対象	--	--		

全般	サポートされるベンダー ID	証明書情報
プロバイダ名	VMware vSAN	
プロバイダ ステータス	オンライン	
アクティブ/スタンバイ ステータス	--	
アクティブ化	自動	
URL	https://nec-vcsa.vsphere.local:443/vsanHealth/vsanvp/version.xml	

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。

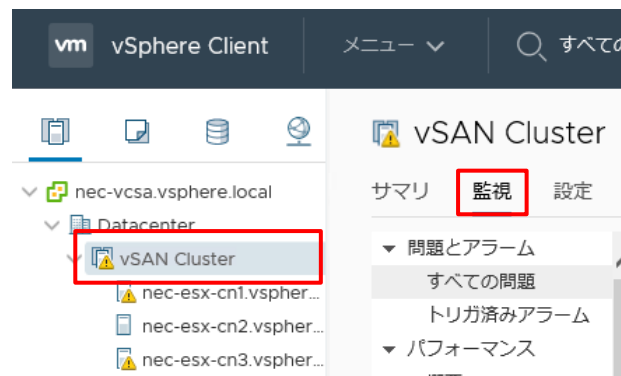
3.17 VMware vSAN 状態の確認(健全性確認)

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 のホーム画面を表示している状態でナビゲータの [ホストおよびクラスタ] をクリックします。



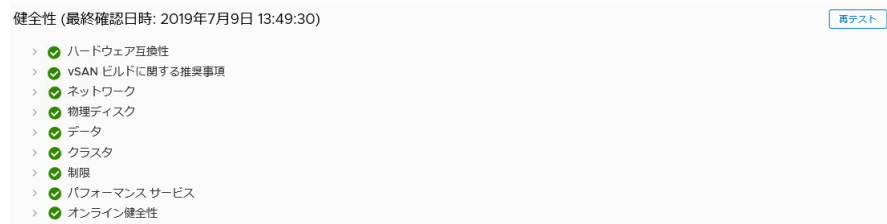
2. オブジェクトで vSAN クラスタ名をクリックし、画面中央上部の[監視]タブをクリックします。



3. [監視]タブの下に[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[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。

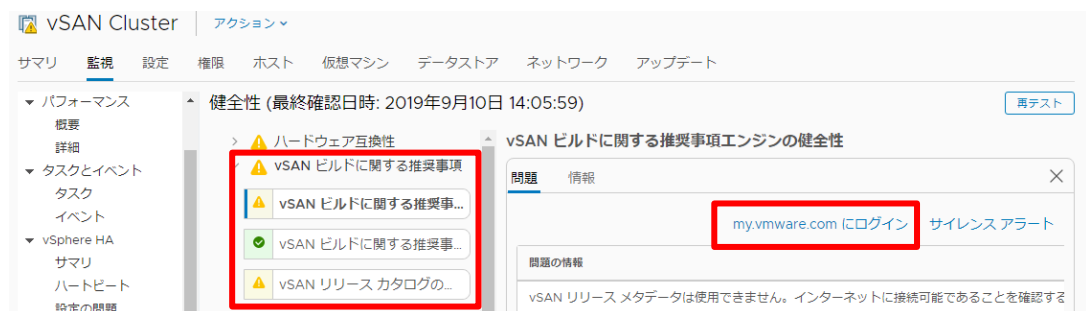


《注意》

vSAN の健全性確認を行った際に、「▼vSAN ビルドに関する推奨事項」に含まれるテスト項目の結果として、「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」で警告が表示される場合があります。

インターネットへの接続を行わない状態で vSAN クラスタを稼働させる場合、これらの警告は無視して問題ありません。

本警告は、vCenter Server Appliance がインターネット接続できないことが原因となっています。本警告を解消する場合は、vCenter Server Appliance からインターネットに接続できることを確認した後、「vSAN ビルドに関する推奨事項エンジンの健全性」の詳細欄にある [my.vmware.com にログイン] をクリックしてください。



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。



3.18 NEC Hyper Converged System Console の動作確認

3.18.1 ログイン

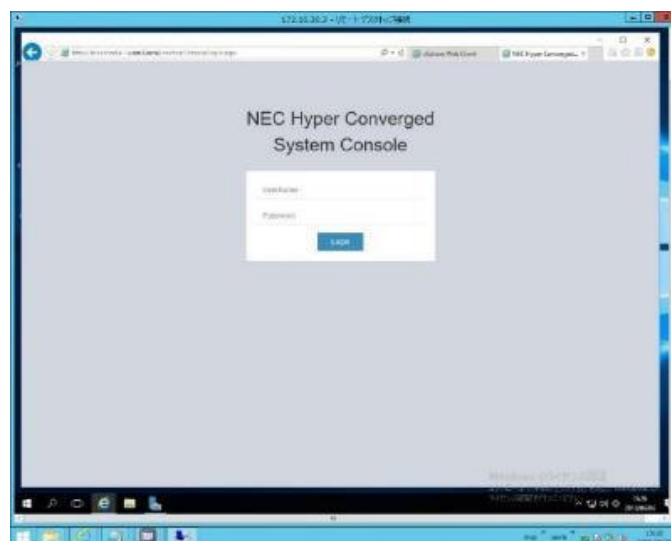
管理 VM 上で Web ブラウザを起動し、NEC Hyper Converged System Console にログインします。

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(Internet Explorer)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 v2.0 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 v2.0 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。

3.18.2 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。

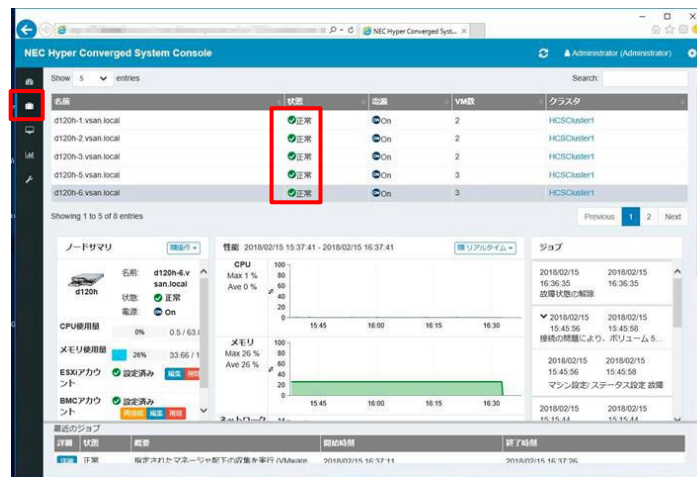
・[ダッシュボード]タブ



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 節の問い合わせ窓口までご連絡ください。

・[node]タブ

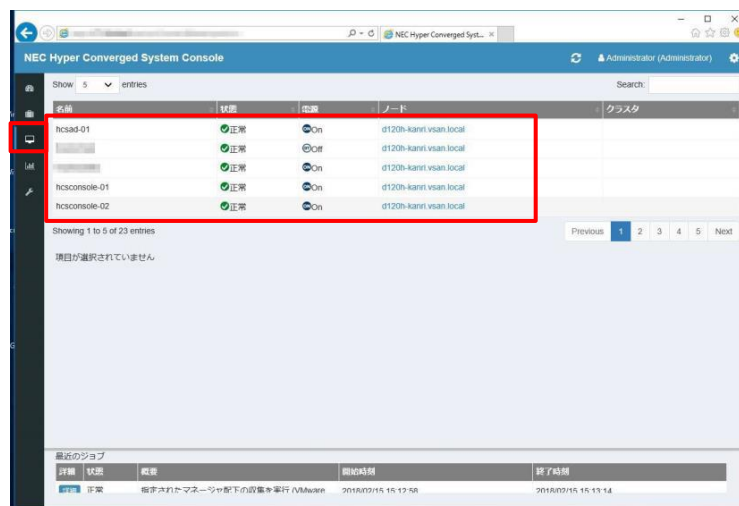


登録したノードと状態がリスト形式で表示されます。

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。ある程度の運用しノードとの通信が行われた後に表示されます。

・[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



ジョブ	イベント	ステータス	メッセージ	開始時刻	終了時刻
▼	詳細	正常	故障状態の解除	2018/02/15 15:16:35	2018/02/15 15:16:35
▼	詳細	正常	故障状態の解除	2018/02/15 15:15:44	2018/02/15 15:15:44
▼	詳細	正常	故障状態の解除	2018/02/15 15:15:38	2018/02/15 15:15:38
▼	詳細	正常	故障状態の解除	2018/02/15 15:15:33	2018/02/15 15:15:33
▼	詳細	正常	故障状態の解除	2018/02/15 15:15:26	2018/02/15 15:15:26
▼	詳細	正常	故障状態の解除	2018/02/15 15:15:09	2018/02/15 15:15:09
▼	詳細	正常	ジョブの実行 (マネージャ配下の収集)	2018/02/15 15:12:58	2018/02/15 15:13:15
		正常	指定されたマネージャ配下の収集を実行 (VMware vCenter Server / hcavcsa-01.vsan.local)	2018/02/15 15:12:58	2018/02/15 15:13:14
▼	詳細	正常	d120h-7.vsan.local 上のアラーム「ホストの接続と電源状態」が赤から緑に変わりました	2018/02/15 15:10:04	2018/02/15 15:10:05
		正常	マシン設定/ステータス設定 正常	2018/02/15 15:10:04	2018/02/15 15:10:05
▼	詳細	正常	接続の断絶により、ボリューム 5a827703-36b44242-840d-1c1b0d0fa7a42 (0377825a-de7a-9c58-9cct-1c1b0d0fa7a42) へのアクセスが失われました。回復処理が実行中です。まもなく結果が報告されます。	2018/02/15 15:10:02	2018/02/15 15:10:03
		正常	マシン設定/ステータス設定 故障	2018/02/15 15:10:03	2018/02/15 15:10:03
▼	詳細	正常	接続の断絶により、ボリューム 5a827695-143a402c-8fa4-1c1b0d0faa385 (6576825a-86b-865a-0bc7-1c1b0d0faa385) へのアクセスが失われました。回復処理	2018/02/15 15:09:56	2018/02/15 15:09:56

NEC HCS 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 節の問い合わせ先までご連絡ください。

4 ライセンス登録

4.1 vCenter Server、ESXi、vSAN ライセンスの登録

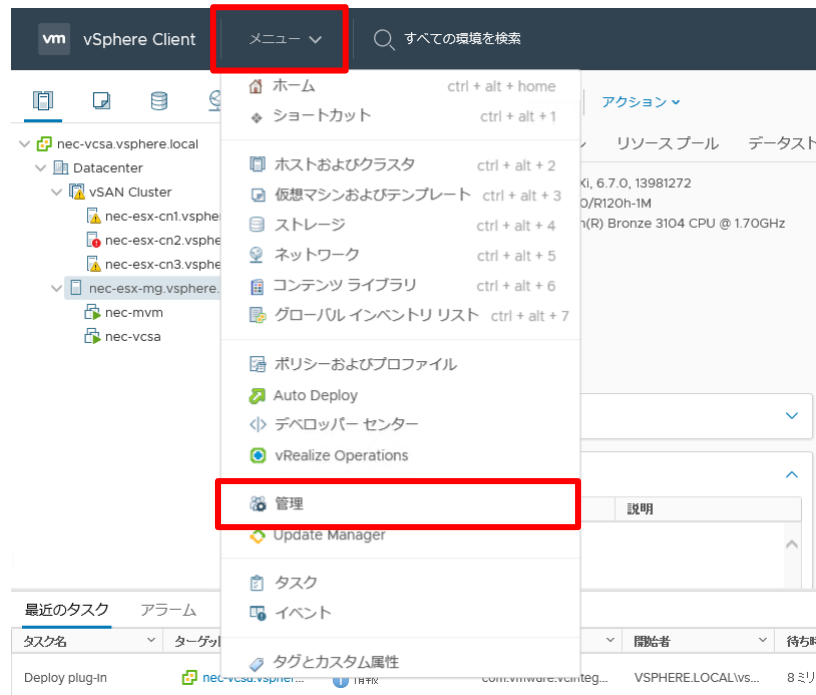
vCenter Server、ESXi および vSAN のライセンスキーの登録および割り当てを行います。

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

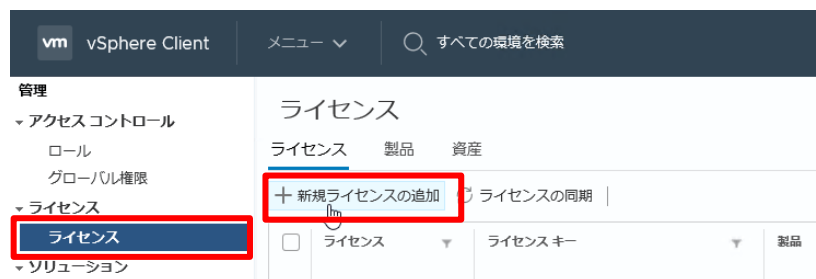
3 ノード以上の構成、または 2 ノード構成でライセンスに vSphere Standard を使用する場合は本項の手順でライセンス登録を実施してください。

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、画面上部のメニューをクリックし、出てく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、[新規ライセンスの追加]をクリックします。



- 「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。

新規ライセンス

- 1 ライセンス キーを入力してください
- 2 ライセンス名を編集
- 3 設定の確認

ライセンス キーを入力してください

ライセンス キー (1行に1つ):

- 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。

新規ライセンス

- 1 ライセンス キーを入力してください
- 2 ライセンス名を編集
- 3 設定の確認

ライセンス名を編集

ライセンス名:	ライセンス	
ライセンス キー:	54C 3A 11 5E 11 5E 11 5E	有効期限: 2019年10月18日
製品:	VMware vCenter Server 6 Standard (インスタンス)	キャパシティ: 1インスタンス

ライセンス名:	ライセンス 2	
ライセンス キー:	54C 3A 11 5E 11 5E 11 5E	有効期限: 2019年10月18日
製品:	VMware vSphere 6 Standard (CPU)	キャパシティ: 16 CPU

- 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。

新規ライセンス

- 1 ライセンス キーを入力してください
- 2 ライセンス名を編集
- 3 設定の確認

設定の確認

ライセンスの数: 2

ライセンス名:	ライセンス 1
ライセンス キー:	54C 3A 11 5E 11 5E 11 5E

ライセンス名:	ライセンス 2
ライセンス キー:	54C 3A 11 5E 11 5E 11 5E

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。

ライセンス

ライセンス 製品 資産 MY VMWARE に移動

+ 新規ライセンスの追加 〇 ライセンスの同期 |

<input type="checkbox"/>	ライセンス	ライセンスキー	製品	使用状況	キャパシティ	状態	有効期限
<input type="checkbox"/>	評価ライセンス	--	--	--	--	割り当て済み	評価 ⚠
<input type="checkbox"/>	ライセンス1	--	VMware vCenter Server 6 Standard (...)	0 インスタ...	1 インスタ...	未割り当て	2019年10...
<input type="checkbox"/>	ライセンス2	--	VMware vSphere 6 Standard (CPU)	0 CPU	16 CPU	未割り当て	2019年10...

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、[ライセンスの割り当て]をクリックします。

ライセンス

ライセンス 製品 **資産** MY VMWARE に移動

vCENTER SERVER システム ホスト クラスタ ソリューション

🔗 ライセンスの割り当て

<input checked="" type="checkbox"/>	資産	使用状況	製品	ライセンス	ライセンスの有効期限	ライセンス供与済み
<input checked="" type="checkbox"/>	nec-vcsa.vsphere.local	1 インスタンス	評価モード	評価ライセンス	⚠ 評価	いいえ

1 エクスポート 1 アイテム

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。

ライセンスの割り当て

既存のライセンス 新規ライセンス

ライセンス	ライセンスキー	製品	使用状況	キャパシティ	機能
<input type="radio"/>	評価ライセンス	--	--	--	--
<input checked="" type="radio"/>	ライセンス1	VMware vCenter Server 6 Stand...	1 インスタンス	1 インスタンス	①

2 アイテム

※ 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。

ライセンス1の割り当て検証

⚠ 一部の機能が使用できなくなります。

9. 再び VMware vSphere Client 画面にフォーカスが戻ります。手順 5 の画面内のリストにおいて、管理サーバの行の「製品」列の値が vCenter Server 等のライセンス名になっていることを確認します。

ライセンス

ライセンス 製品 資産 MY VMWARE に移動

VCENTER SERVER システム ホスト クラスタ ソリューション

ライセンスの割り当て

資産	使用状況	製品	ライセンス	ライセンスの有効期限	ライセンス供与済み
<input checked="" type="checkbox"/> nec-vcsa.vsphere.local	1 インスタンス	VMware vCenter Server 6 Standard (インスタンス)	ライセンス 1	2019年10月18日	はい

1 エクスポート 1 アイテム

10. 続いて、ESXi にライセンスを割り当てます。[資産]タブの下[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。

ライセンス

ライセンス 製品 資産 MY VMWARE に移動

VCENTER SERVER システム ホスト クラスタ ソリューション

ライセンスの割り当て

資産	使用状況	製品	ライセンス	ライセンスの有効期限	ライセンス供与済み	vCenter Server システム
<input checked="" type="checkbox"/> nec-esx-mg.vsphere.local	2 CPU	評価モード	評価ライセンス	評価	いいえ	nec-vcsa.vsphere.local
<input checked="" type="checkbox"/> nec-esx-cn2.vsphere.local	2 CPU	評価モード	評価ライセンス	評価	いいえ	nec-vcsa.vsphere.local
<input checked="" type="checkbox"/> nec-esx-cn3.vsphere.local	2 CPU	評価モード	評価ライセンス	評価	いいえ	nec-vcsa.vsphere.local

4 エクスポート 4 アイテム

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。

ライセンスの割り当て

このアクションを 4 個のオブジェクトで実行しますか?

いいえ はい

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。

ライセンスの割り当て - 4 オブジェクト

既存のライセンス 新規ライセンス

ライセンス	ライセンスキー	製品	使用状況	キャパシティ	機能
<input type="radio"/> 評価ライセンス	--	--	--	--	--
<input checked="" type="radio"/> ライセンス 2	-----	VMware vSphere 6 Standard (CP_	8 CPU	16 CPU	①

2 アイテム

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 サーバの行の「製品」列の値が vSphere のライセンス名になっていることを確認します。

ライセンス

ライセンス 製品 資産 MY VMWARE に移動

VCENTER SERVER システム ホスト クラスタ ソリューション

🔍 ライセンスの割り当て

資産	使用状況	製品	ライセンス	ライセンスの有効期限	ライセンス供与済み	vCenter Server システム
<input checked="" type="checkbox"/> nec-esx-mg.vsphere.local	2 CPU	VMware vSphere 6 Stand ard (CPU)	ライセンス 2	2019年10月18日	はい	nec-vcsa.vsphere.local
<input checked="" type="checkbox"/> nec-esx-cn2.vsphere.local	2 CPU	VMware vSphere 6 Stand ard (CPU)	ライセンス 2	2019年10月18日	はい	nec-vcsa.vsphere.local
<input checked="" type="checkbox"/> nec-esx-cn3.vsphere.local	2 CPU	VMware vSphere 6 Stand ard (CPU)	ライセンス 2	2019年10月18日	はい	nec-vcsa.vsphere.local
<input checked="" type="checkbox"/> nec-esx-cn1.vsphere.local	2 CPU	VMware vSphere 6 Stand ard (CPU)	ライセンス 2	2019年10月18日	はい	nec-vcsa.vsphere.local

4 エクスポート 1 アイテム

14. 続いて、vSAN にライセンスを割り当てます。[資産]タブの下[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。

ライセンス

ライセンス 製品 資産 MY VMWARE に移動

VCENTER SERVER システム ホスト クラスタ ソリューション

🔍 ライセンスの割り当て

資産	使用状況	製品	ライセンス	ライセンスの有効期限	ライセンス供与済み	vCenter Server システム
<input checked="" type="checkbox"/> vSAN Cluster	6 CPU	評価モード	評価ライセンス	評価	いいえ	nec-vcsa.vsphere.local

1 エクスポート 1 アイテム

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。

ライセンスの割り当て

既存のライセンス 新規ライセンス

ライセンス	ライセンスキー	製品	使用状況	キャパシティ	機能
<input type="radio"/> 評価ライセンス	--	--	--	--	--
<input checked="" type="radio"/> ライセンス 4	-----	VMware vSAN Standard (CPU)	6 CPU	32 CPU	①

2 アイテム

16. 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 vSAN クラスタの行の「製品」列の値が vSAN のライセンス名になっていることを確認します。

ライセンス

ライセンス 製品 資産 MY VMWARE に移動

VCENTER SERVER システム ホスト クラスタ ソリューション

🔍 ライセンスの割り当て

資産	使用状況	製品	ライセンス	ライセンスの有効期限	ライセンス供与済み	vCenter Server システム
<input checked="" type="checkbox"/> vSAN Cluster	6 CPU	VMware vSAN Standard (CPU)	ライセンス 4	2019年10月18日	はい	nec-vcsa.vsphere.local

1 エクスポート 1 アイテム

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。

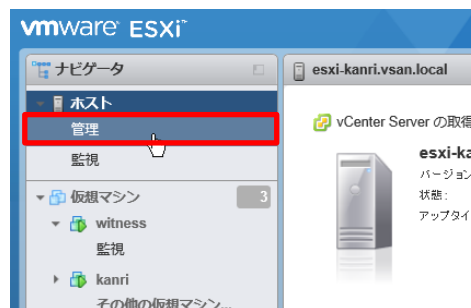
4.1.2 2 ノード構成で vSphere Essentials Plus を使用する場合

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。

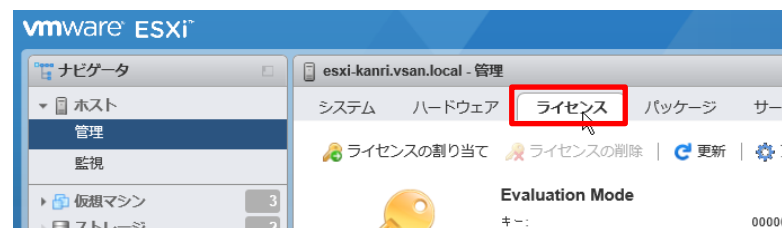
1. My VMware のサイトにログインします。
ESXi のライセンスを取得する際に、ライセンス分割を実施し、2CPU 分のライセンスと 4CPU 分のライセンスに分割してください。
ライセンス分割に関しては以下 KB を参照してください。
<<https://kb.vmware.com/s/article/2006972?lang=ja>>
2. VMware vSphere Client で vCenter Server にログインし、vCenter Server、vSAN および ESXi(4CPU 分)のライセンスを vCenter Server、vSAN、およびクラスタノードに割り当ててください。
具体的な手順は**エラー! 参照元が見つかりません。**項を参照してください。
3. 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。



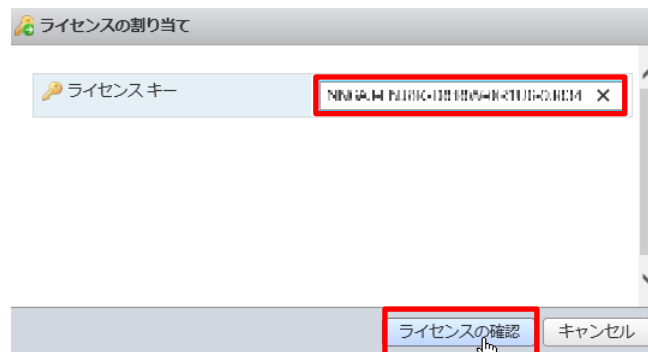
5. 「管理」画面上部の[ライセンス]をクリックします。



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。



- 「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。



- 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。



- 「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 2016 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. 画面の[プロダクトキーを変更します]をクリックします。



3. [プロダクトキーの入力]画面でプロダクトキーを入力します。インターネットに接続されている場合、入力後にライセンス認証が行われます。

プロダクト キーの入力

プロダクト キーは、Windows の販売元または配給元からの電子メールや、Windows の DVD または USB が入っていたパッケージに書かれています。

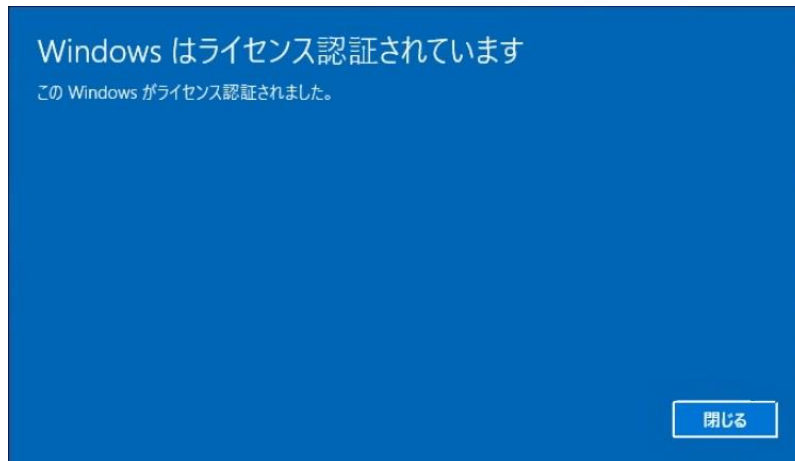
プロダクト キーは次のような形式です:
 プロダクト キー: XXXXX-XXXXX-XXXXX-XXXXX-XXXXX

プロダクト キー

ハイフンは自動的に追加されます

キャンセル

4. ライセンス認証完了後、[閉じる]をクリックします。

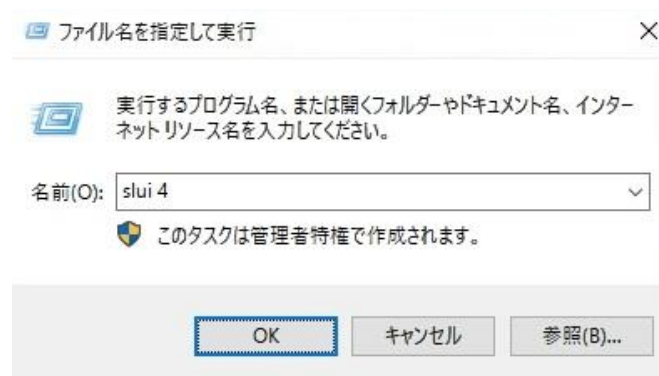


4.2.2 インターネットに接続されていない環境でライセンス登録

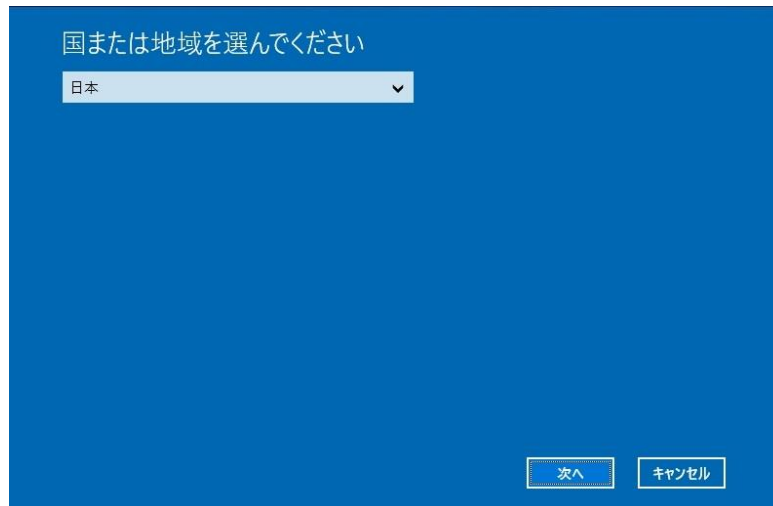
1. 画面の左下の Windows アイコンを右クリックし、[コマンドプロンプト (管理者)]を起動します。
2. 管理者権限のコマンドプロンプトで次のコマンドを入力し、<Enter>キーを押します。

```
>slmgr -ipk <COA ラベルのプロダクトキー>
```

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。



The screenshot shows a blue background with white text. At the top, it says "国または地域を選んでください" (Please select a country or region). Below this is a dropdown menu with "日本" (Japan) selected. At the bottom right, there are two buttons: "次へ" (Next) and "キャンセル" (Cancel).

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。

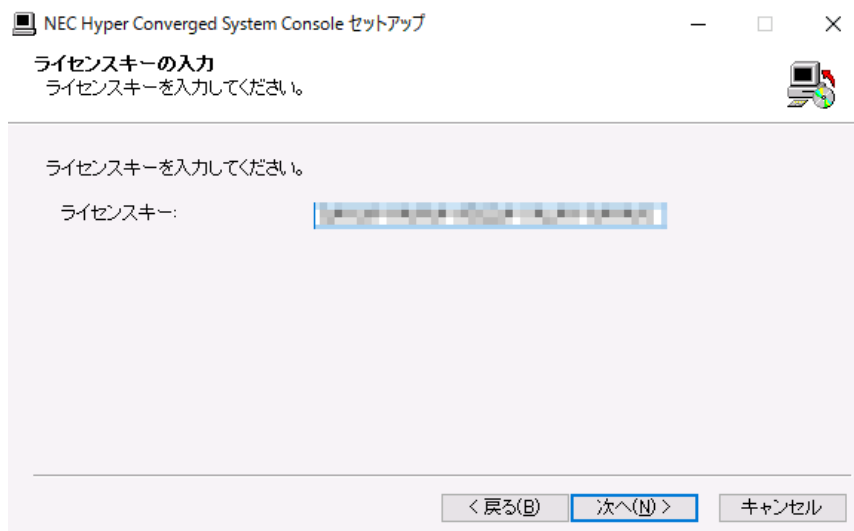
以上で Windows Server へのライセンス登録は完了となります。

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 2016)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管理ノードの Witness ノードのパスワード変更
- ⑨NEC Hyper Converged System Console の登録情報の更新
- ⑩Windows サーバと vCenter Server の保守アカウントパスワード

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



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	—	—	
vCSA の SSO の ID・パスワード	—	○	
管理 VM(Windows Server 2016)の Administrator パスワード	—	—	
ESMPRO/ServerManager の ID・パスワー ド	—	—	
NEC Hyper Converged System Console の ID・パスワード	—	—	
保守アカウント	—	—	
Witness ノードの ID・パスワード	—	○	

※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。

設定登録方法は、ESMPRO/ServerManager セットアップガイドの“第 10 章 VMware ESXi5/6 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

—: 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》

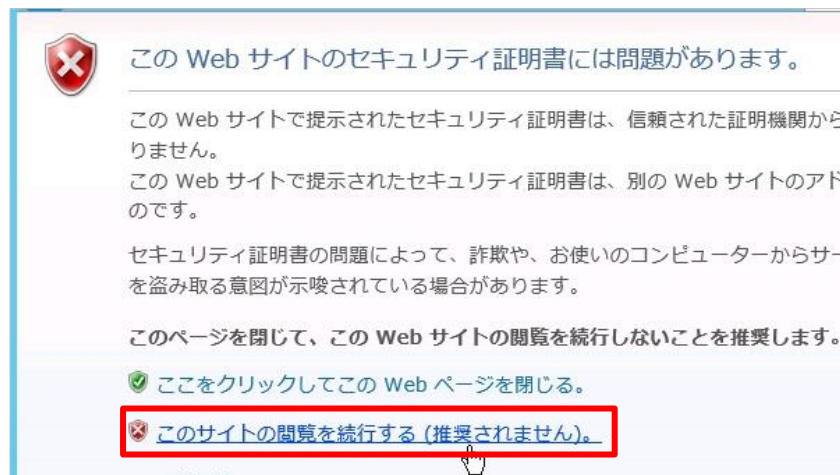
BMC(NEC iLO 5)のパスワードを変更した場合は、変更後に NEC Hyper Converged System 上で登録されている BMC のパスワード情報を更新いただく必要があります。パスワード変更におけるシステム影響を及ぼす関係表は 5.1.2 節を、パスワード情報を更新する手順は 5.9 節を参照ください。

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(Internet Explorer)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)

- ※ 「この Web サイトのセキュリティ証明書には問題があります。」画面が表示された場合は、「このサイトの閲覧を続行する(推奨されません)。」を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)



The image shows the iLO 5 Express5800 login interface. On the left, there is a header with the NEC logo and 'iLO 5 Express5800' text, along with the firmware version '1.20' and BMC address 'BMC:JPN809400Y.vsan.local'. On the right, there is a login form with fields for 'ローカルユーザ名:' (Local User Name) containing 'admin' and 'パスワード:' (Password) with a masked input. Below these fields is a blue 'ログイン' (Login) button. At the bottom, there is a language selector showing 'ja - 日本語'.

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。

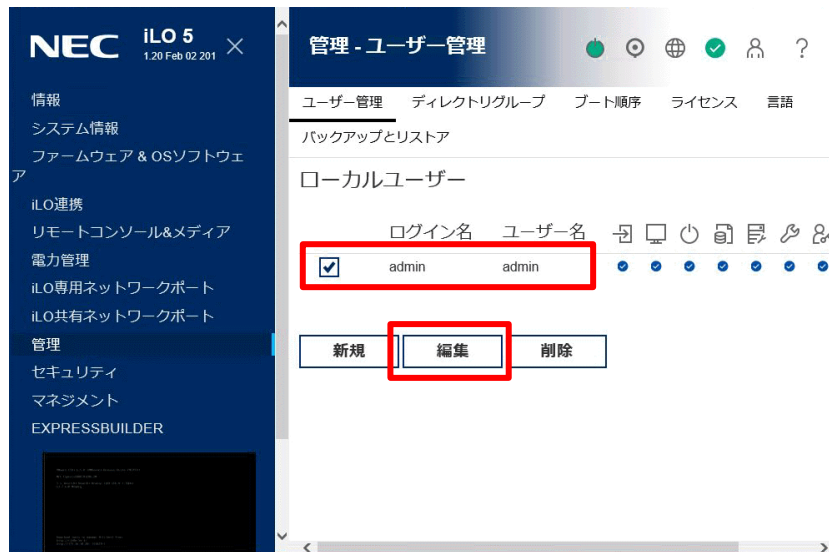


The image shows the iLO 5 Management Overview screen. The left sidebar contains a navigation menu with items like '情報' (Information), 'システム情報' (System Information), 'ファームウェア & OSソフトウェア' (Firmware & OS Software), 'iLO連携' (iLO Integration), 'リモートコンソール&メディア' (Remote Console & Media), '電力管理' (Power Management), 'iLO専用ネットワークポート' (iLO Dedicated Network Port), 'iLO共有ネットワークポート' (iLO Shared Network Port), '管理' (Management), 'セキュリティ' (Security), 'マネジメント' (Management), and 'EXPRESSBUILDER'. The '管理' item is highlighted with a red box. The main content area is titled '情報 - iLO概要' (Information - iLO Overview) and displays a table of system information.

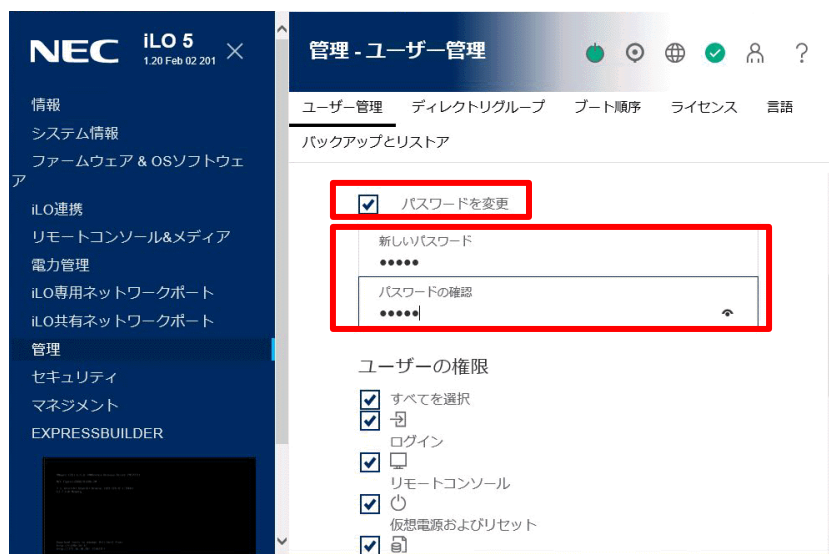
情報	
サーバー名	Express5800/R120h-2M
製品名	3031384E-2D30-504A-4E38-303934303059
UUID	JPN809400Y
サーバーシリアル番号	N8100-2562Y
製品ID	U30 v1.36 (02/15/2018)
システムROM	02/15/2018
システムROM日付	02/01/2018
冗長化システムROM	HTML5 NET Java Web Start
統合リモートコンソール	iLO Advanced Evaluation
ライセンスタイプ	1.20 Feb 02 2018
iLOファームウェアバージョン	172.16.20.20
IPアドレス	FE80::9AF2:B3FF:FEF4:8590
リンクローカルIPv6アドレス	BMC:JPN809400Y.vsan.local
iLOホスト名	

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。



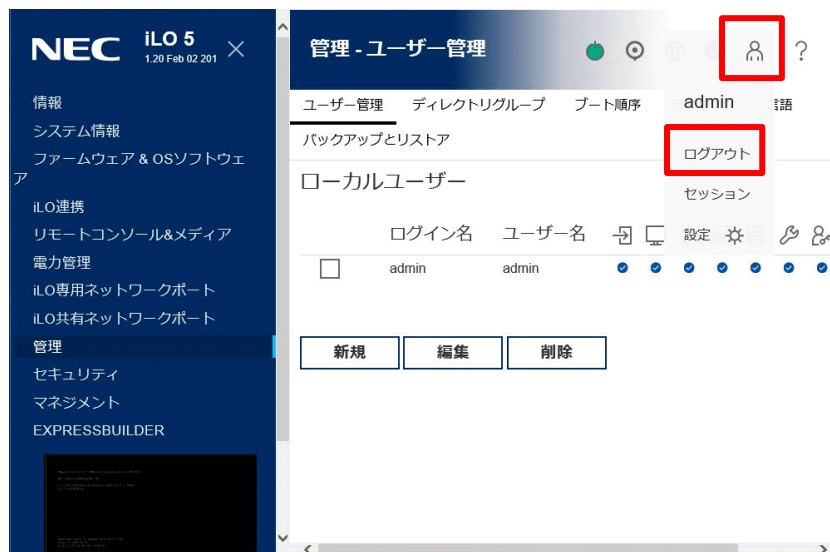
※ パスワードの要件は、初期パスワード通知書の「1.2 パスワード要件」を参照ください。

11. 画面をスクロールし、下部にある[ユーザーの更新]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. すべてのクラスターノード、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

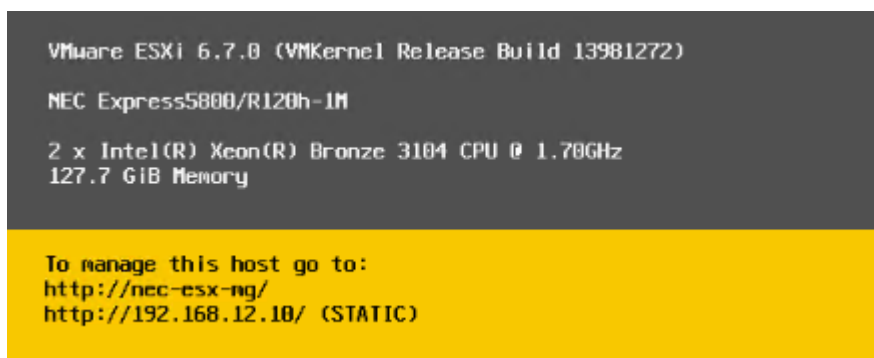
《注意》

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。

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

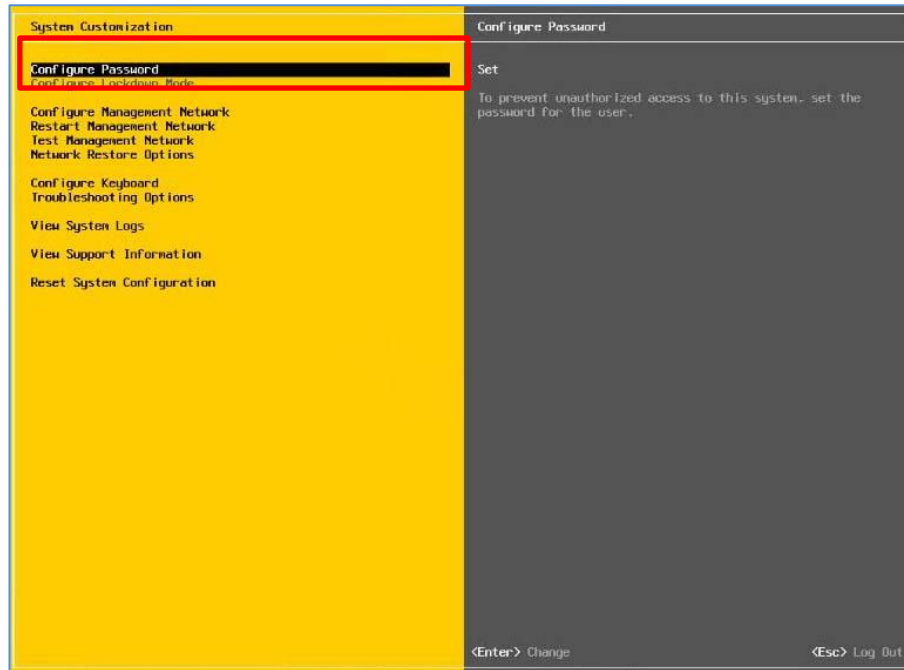
1. クラスタノードまたは管理ノードにディスプレイとキーボードを接続し、ダイレクトコンソール画面を表示します。



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. すべてのクラスターノード、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。

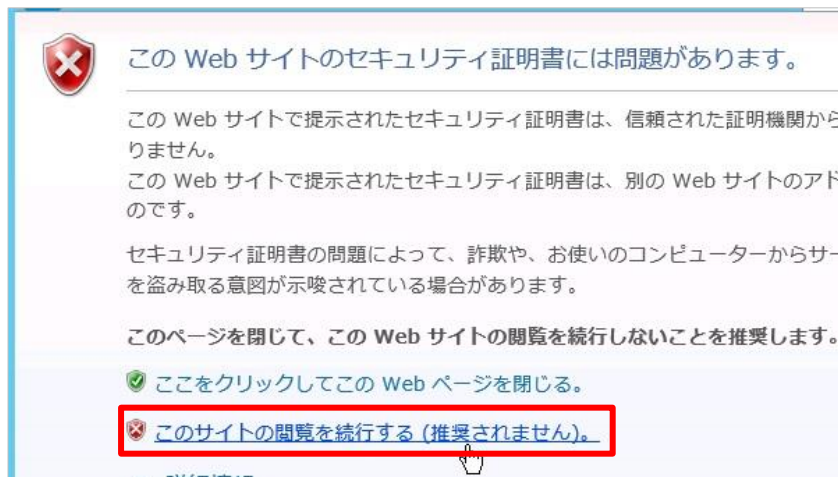
5.3.2 Host Client からの ESXi のパスワード変更

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(Internet Explorer)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。

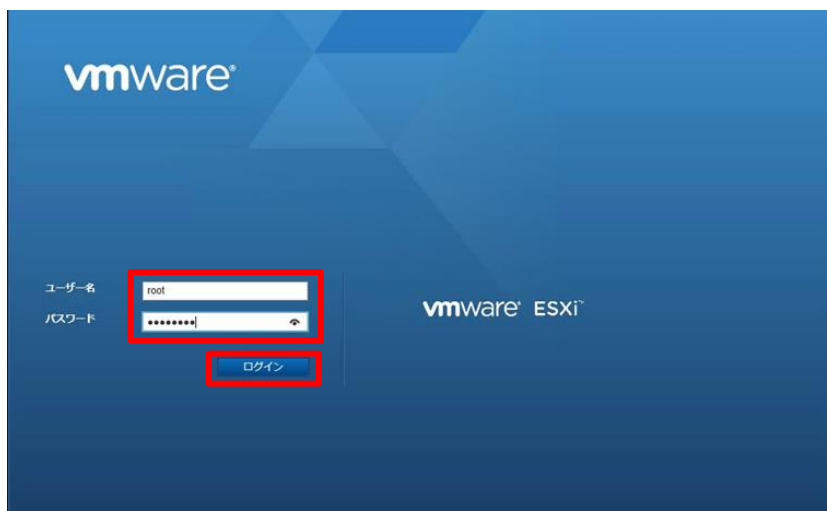
`https://<クラスタノード or 管理ノードの管理用ネットワーク IP アドレス>/ui`

(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)

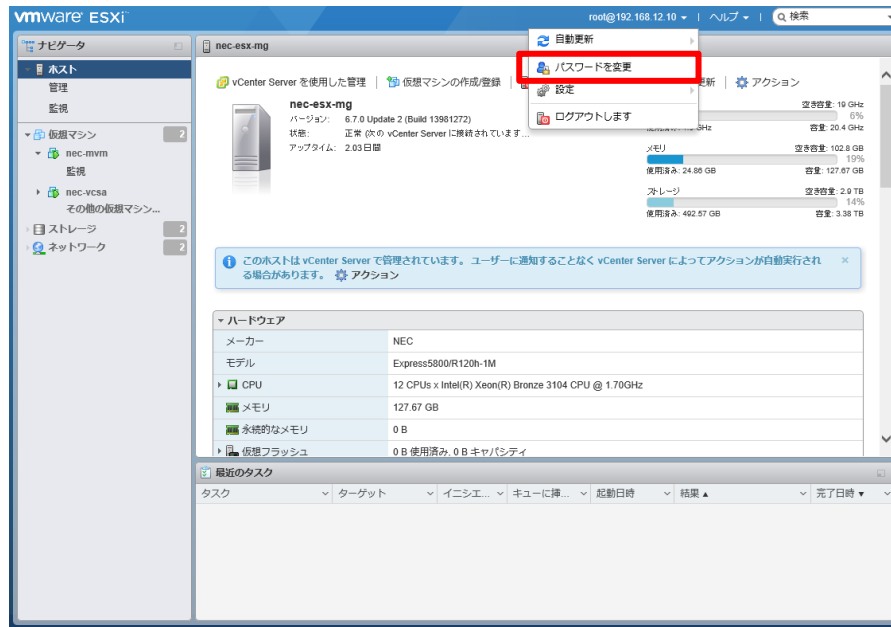
- ※ 「この Web サイトのセキュリティ証明書には問題があります。」画面が表示された場合は、「このサイトの閲覧を続行する(推奨されません)。」をクリックしてください。



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。

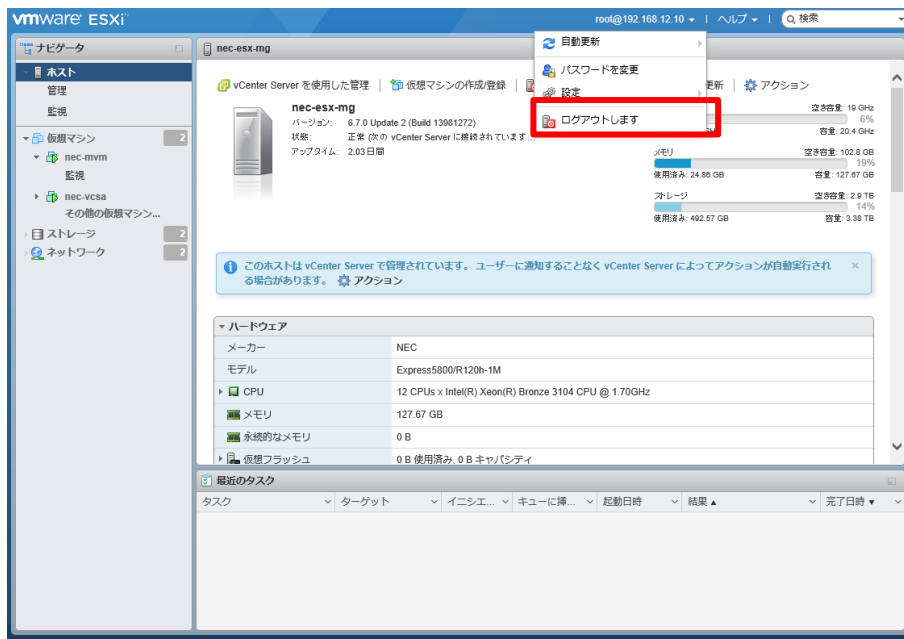


7. パスワードを変更画面が表示されるので、[新しいパスワード]、[新しいパスワードを再作成します]項目に変更したいパスワードを入力し、[パスワードを変更]をクリックします。



※ 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。

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。

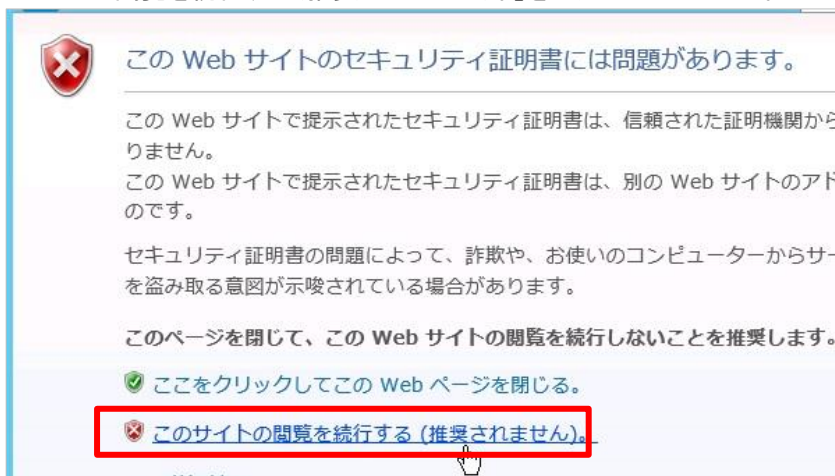
5.4.1 vCSA の vCenterServerAppliance 管理インターフェイス(VAMI)の root パスワードの変更

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(Internet Explorer)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/`

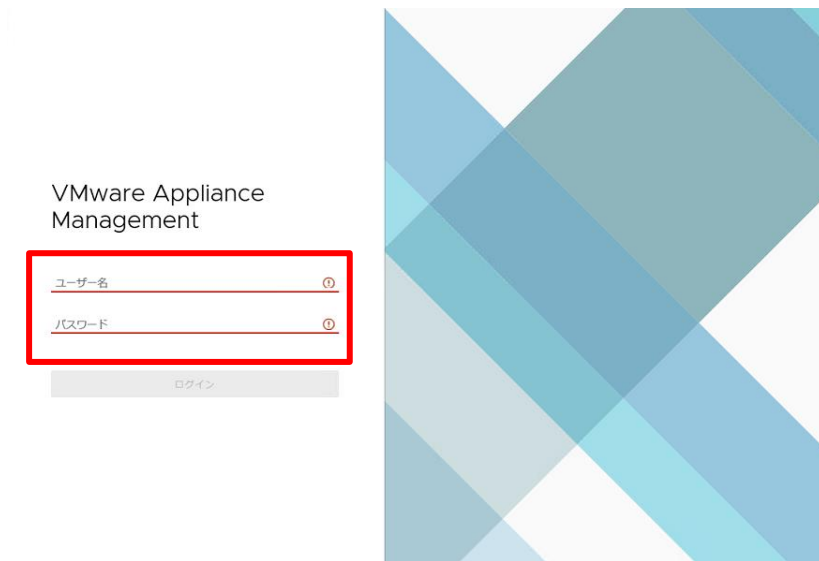
(vCSA のホスト名はヒアリングシートに記載されます)

- ※ 「この Web サイトのセキュリティ証明書には問題があります。」画面が表示された場合は、「このサイトの閲覧を続行する(推奨されません)」を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。I



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。

パスワードの変更

現在のパスワード:

新しいパスワード: ⓘ

パスワードの確認:

キャンセル

保存

※ 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》

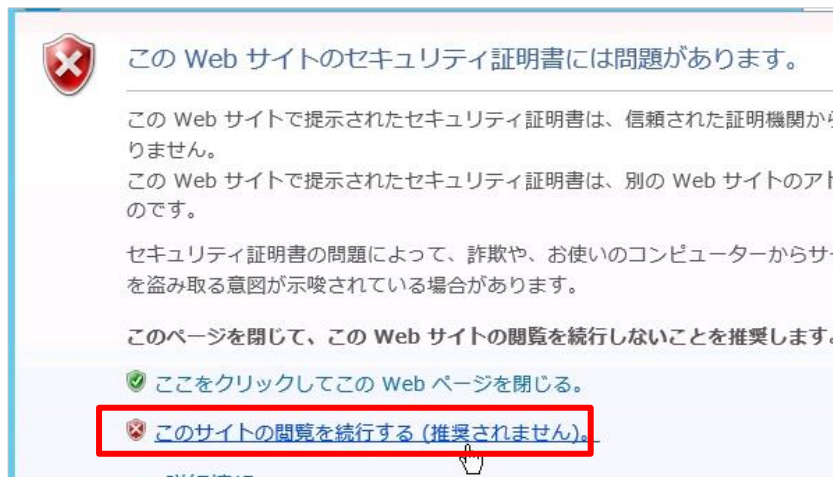
vCSA の SSO ID、パスワードを変更した場合は、変更後に NEC Hyper Converged System 上で登録されている vCSA の SSO のパスワード情報を更新いただく必要があります。パスワード変更におけるシステムへ影響を及ぼす関係表は 5.1.2 節を、パスワード情報を更新する手順は 5.9 節を参照ください。

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(Internet Explorer)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。

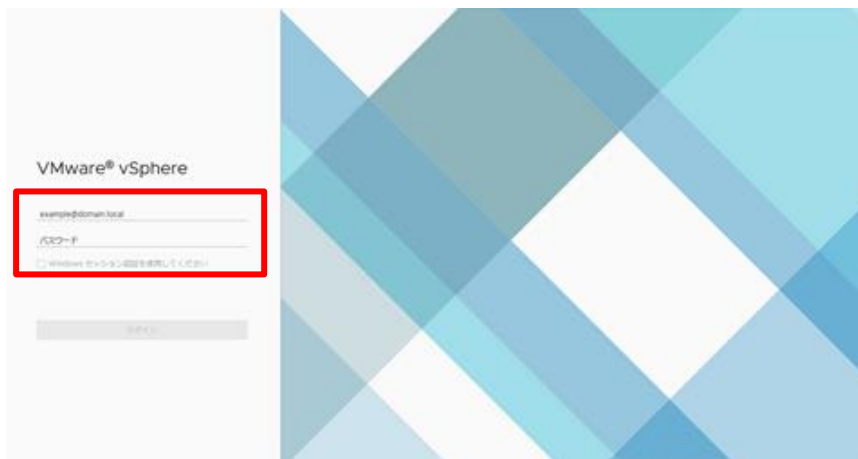
`https://<vCSA のホスト名>/ui`

(vCSA のホスト名はヒアリングシートに記載されます)

- ※ 「この Web サイトのセキュリティ証明書には問題があります。」画面が表示された場合は、「このサイトの閲覧を続行する(推奨されません)。」を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。

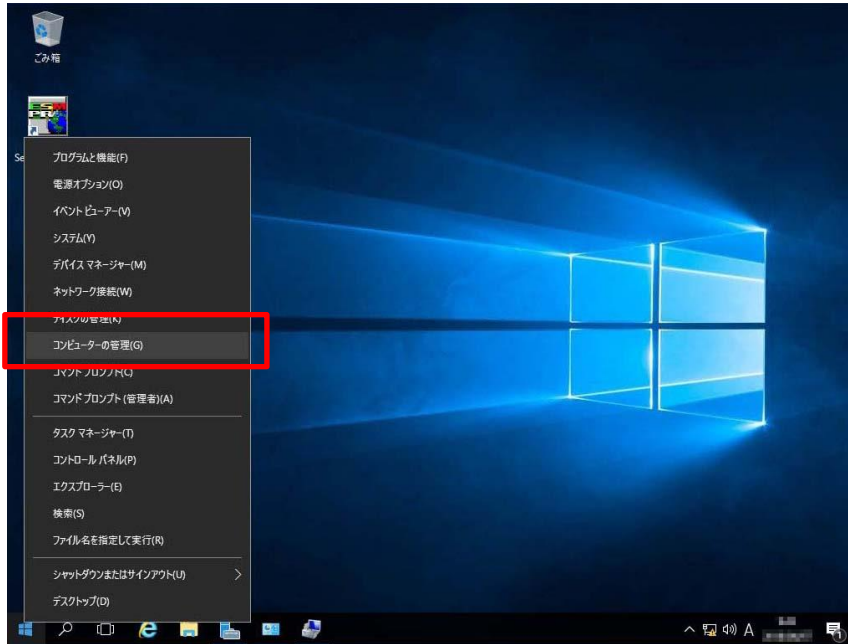
8. パスワード変更されたことを確認し、VMware vSphere Client の画面上部に表示されているユーザ名部分をクリックし、表示されたメニューで[ログアウトします]をクリックします。



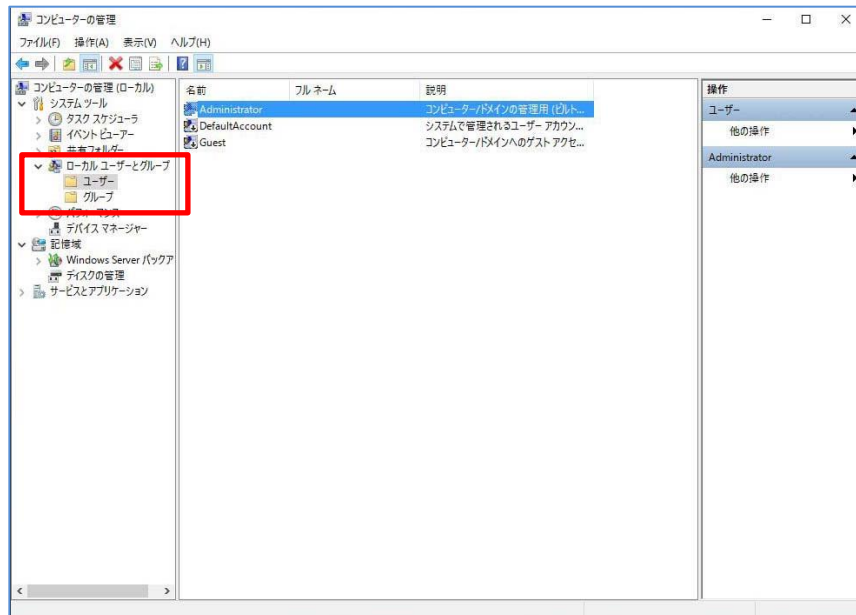
9. VMware vSphere Client から正常にログアウトすると、Web ブラウザに VMware vSphere Client のログイン画面が表示されます。

5.5 管理ノードの管理 VM(Windows Server 2016)のパスワード変更

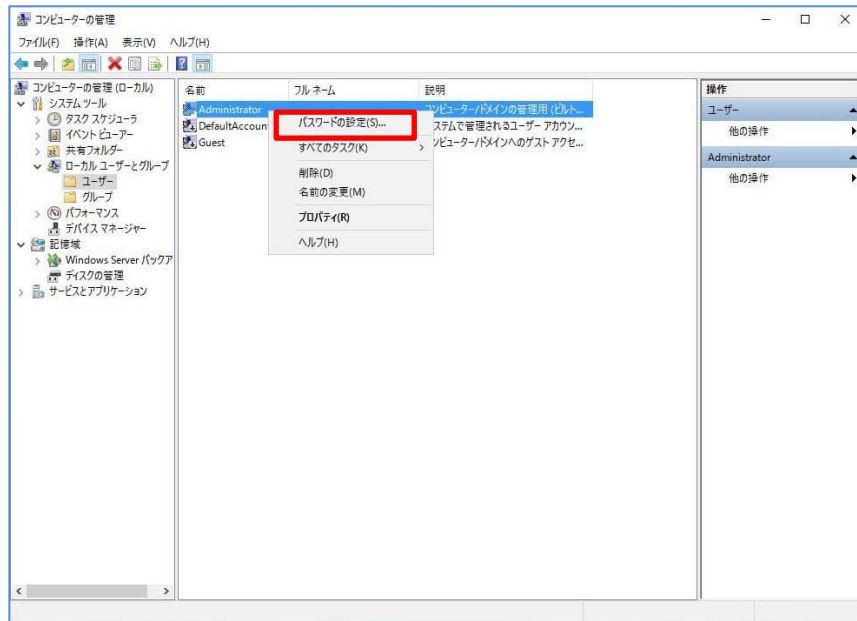
1. Windows PC でリモートデスクトップ接続(mstsc)を起動し、ヒアリングシートに記載されている「管理 VM」の IP アドレスを入力し、管理 VM にログインします。(IP アドレス例: 192.168.100.10:3389)
2. 管理 VM のデスクトップ画面の[Windows キー()]を右クリックして、コンピューターの管理画面を起動します。



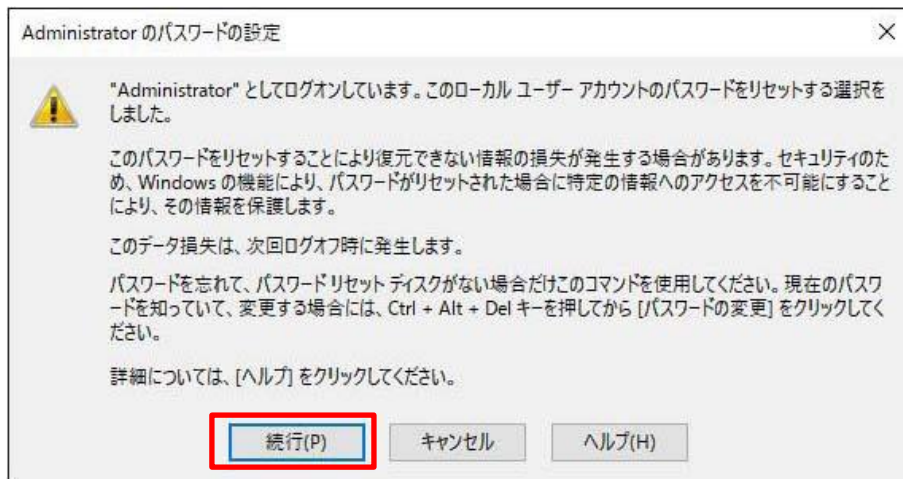
3. コンピューターの管理画面から、[ローカルユーザーとグループ]→[ユーザー]をクリックし、ユーザー一覧を表示させます。



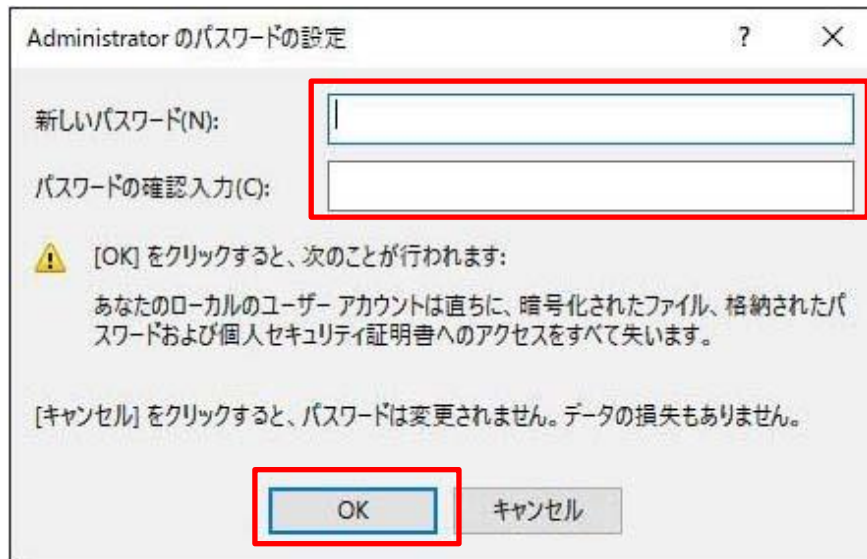
4. “Administrator”ユーザを選択し、マウスを右クリックして、[パスワードの設定]を選択します。



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。

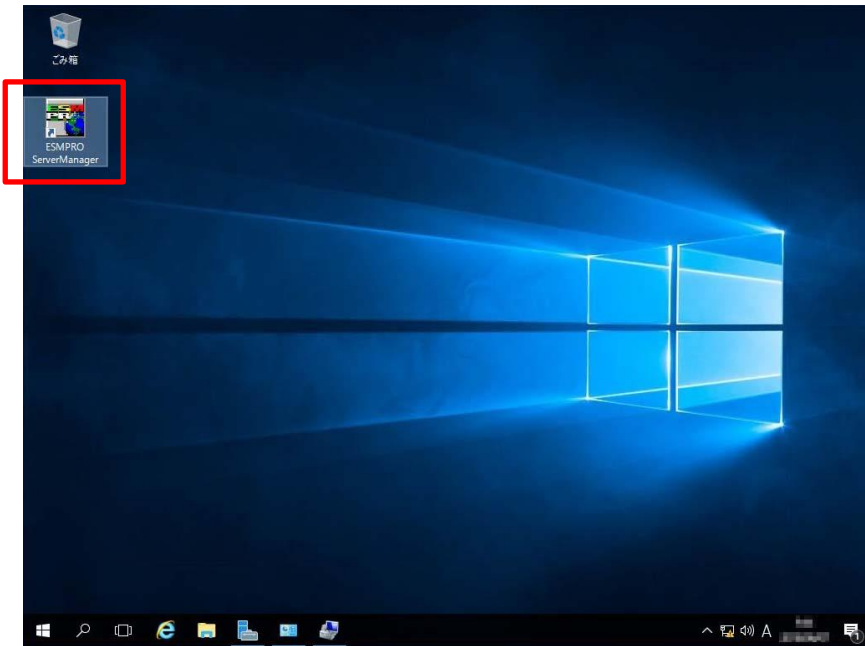


The image shows a Windows-style dialog box titled "Administrator のパスワードの設定" (Administrator Password Setting). It contains two text input fields: "新しいパスワード(N):" (New Password) and "パスワードの確認入力(C):" (Confirm Password). Both fields are highlighted with a red rectangular box. Below the fields, there is a warning icon (yellow triangle with an exclamation mark) followed by the text: "[OK] をクリックすると、次のことが行われます: あなたのローカルのユーザー アカウントは直ちに、暗号化されたファイル、格納されたパスワードおよび個人セキュリティ証明書へのアクセスをすべて失います。" (When you click [OK], the following will occur: your local user account will immediately lose access to encrypted files, stored passwords, and personal security certificates). Below this, it says: "[キャンセル] をクリックすると、パスワードは変更されません。データの損失もありません。" (When you click [Cancel], the password will not be changed. There is no data loss). At the bottom, there are two buttons: "OK" and "キャンセル" (Cancel). The "OK" button is also highlighted with a red rectangular box.

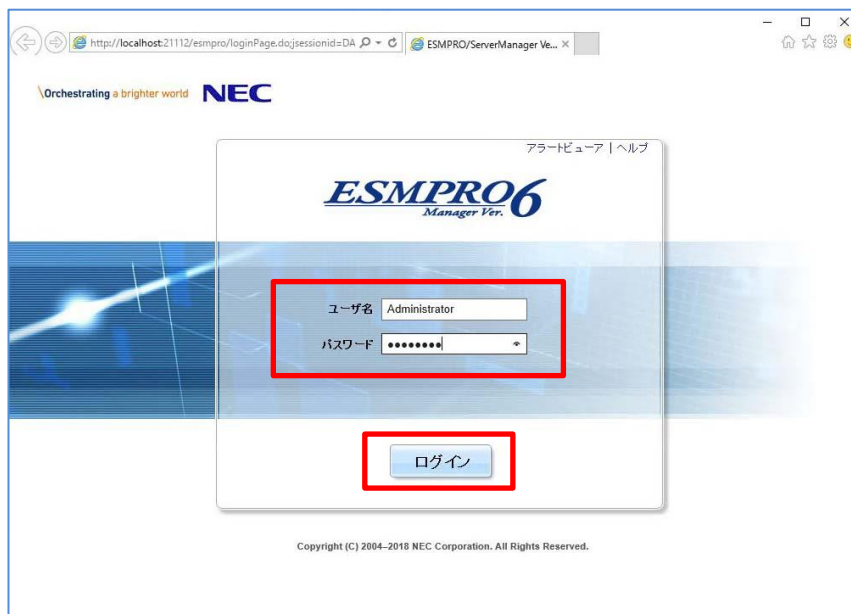
※ パスワードの要件は、初期パスワード通知書の「1.2 パスワード要件」を参照ください。

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

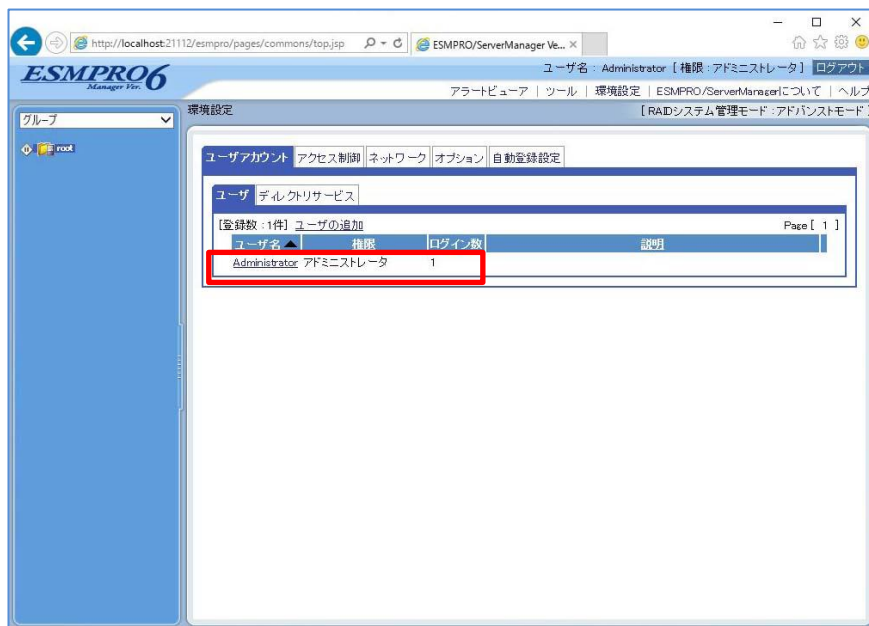
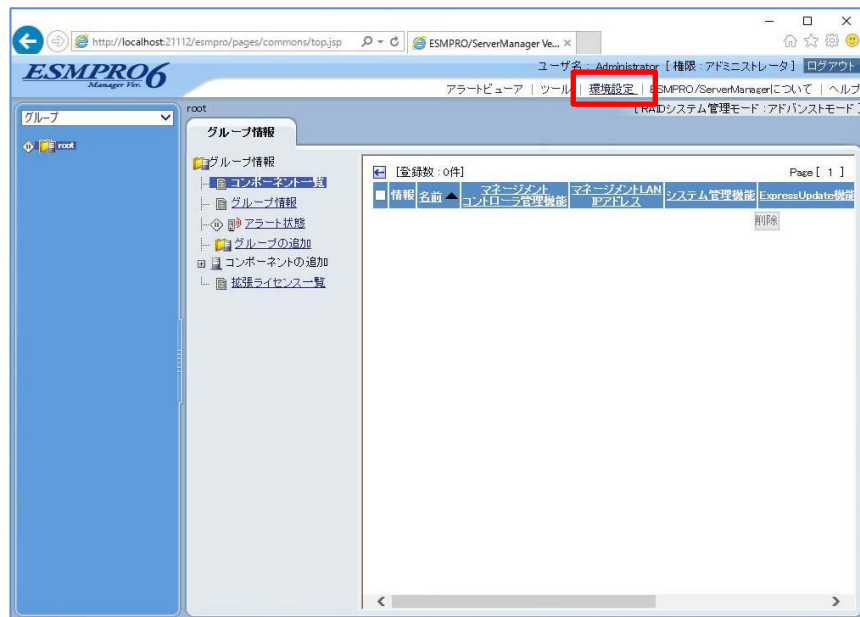
1. Windows PC でリモートデスクトップ接続(mstsc)を起動し、ヒアリングシートに記載されている「管理 VM」の IP アドレスを入力し、管理 VM にログインします。(IP アドレス例: 192.168.100.10:3389)
2. 管理 VM 上で、ESMPRO/ServerManager をダブルクリックして起動し、ESMPRO/ServerManager のログイン画面を表示します。



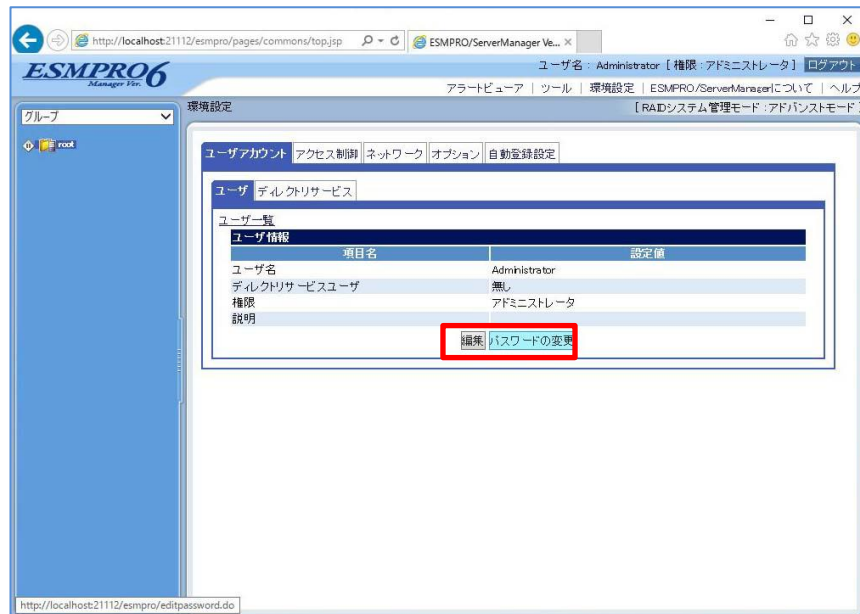
3. ESMPRO/ServerManager のログイン画面で、ユーザ名・パスワードを入力し、ログインします。
(ユーザ名、パスワードは初期パスワード通知書に記載されます)



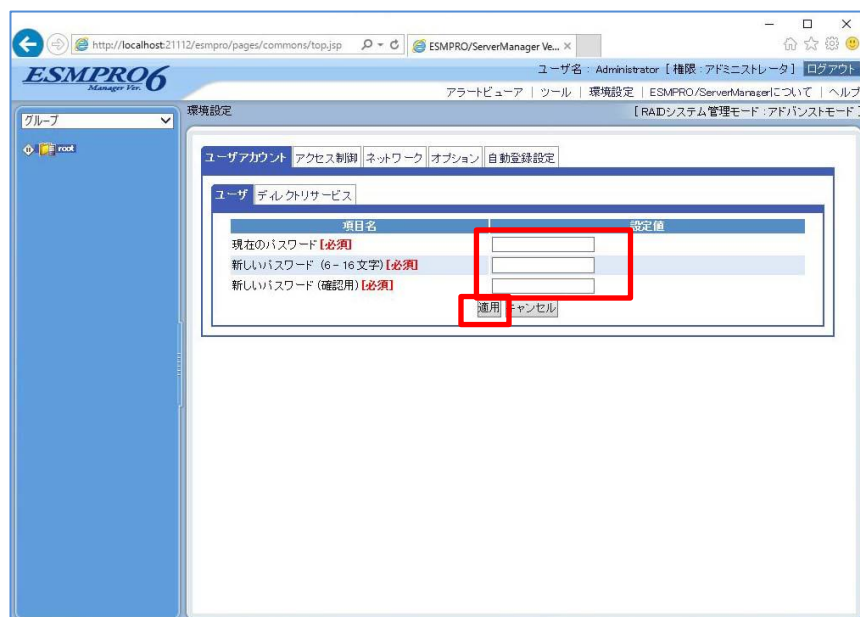
- ESMPRO/ServerManager のメニュー画面で、[環境設定]をクリックし、環境設定画面を表示、初期 ID のユーザ(この手順書では、Administrator)をクリックします。



5. 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。



6. 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。

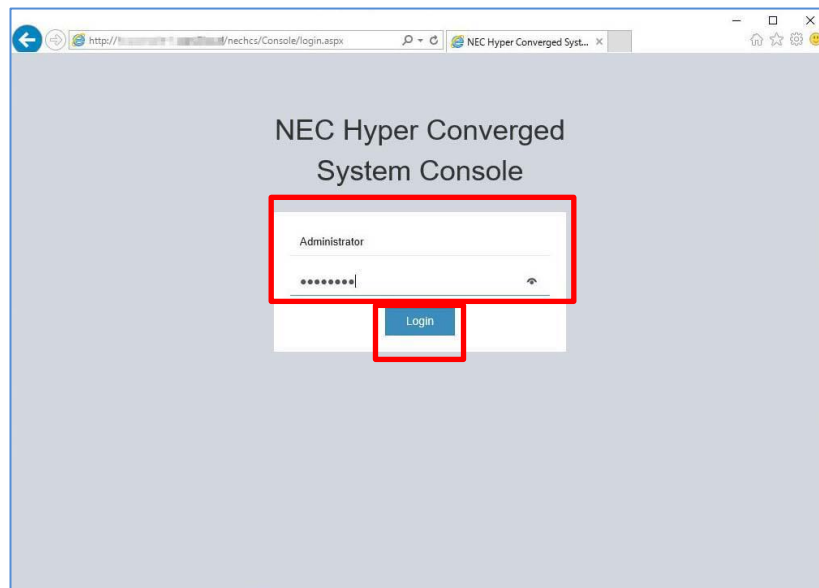
5.7 NEC Hyper Converged System Console のパスワード変更

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(Internet Explorer)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。

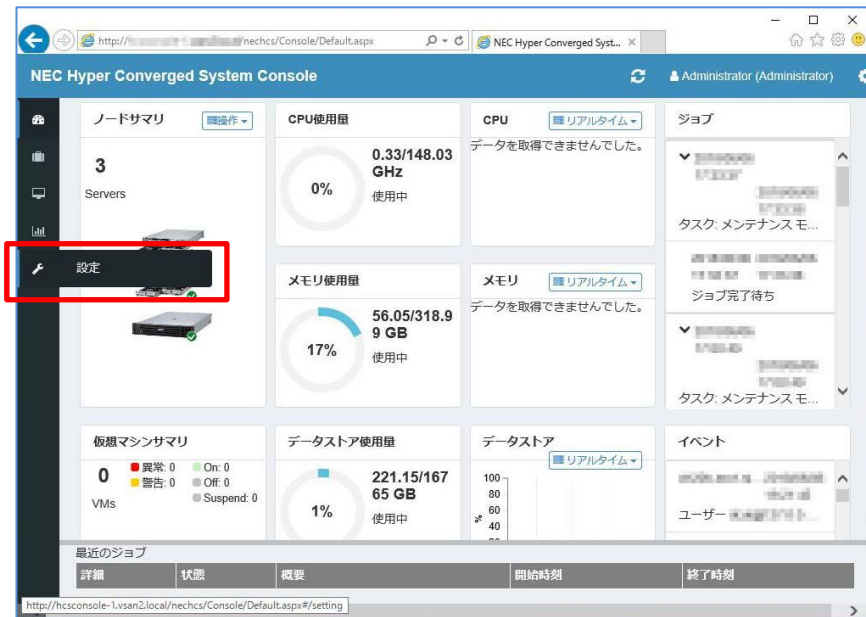
`http://<管理 VM のホスト名>/nechcs/`

(管理 VM のホスト名はヒアリングシートに記載されます。)

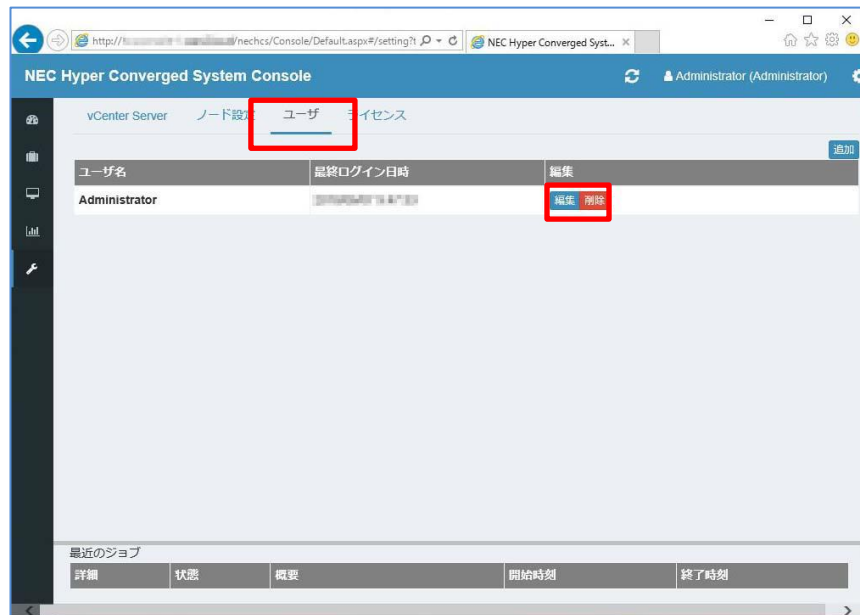
3. NEC Hyper Converged System Console のログイン画面が表示されます。ID・パスワードを入力し、ログインします。
(ID、パスワードは初期パスワード通知書に記載されます)



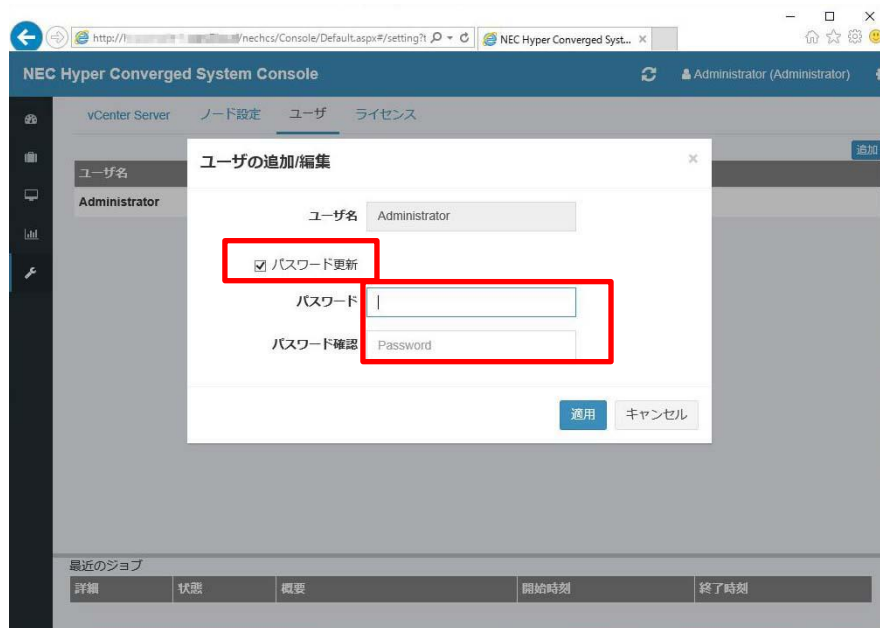
4. NEC Hyper Converged System Console のメイン画面が表示されます。[設定]メニューをクリックし設定画面を表示します。



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 管理ノードの Witness ノードのパスワード変更

3 ノード以上の構成の場合は本節の実施は不要です。

《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、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(Internet Explorer)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。

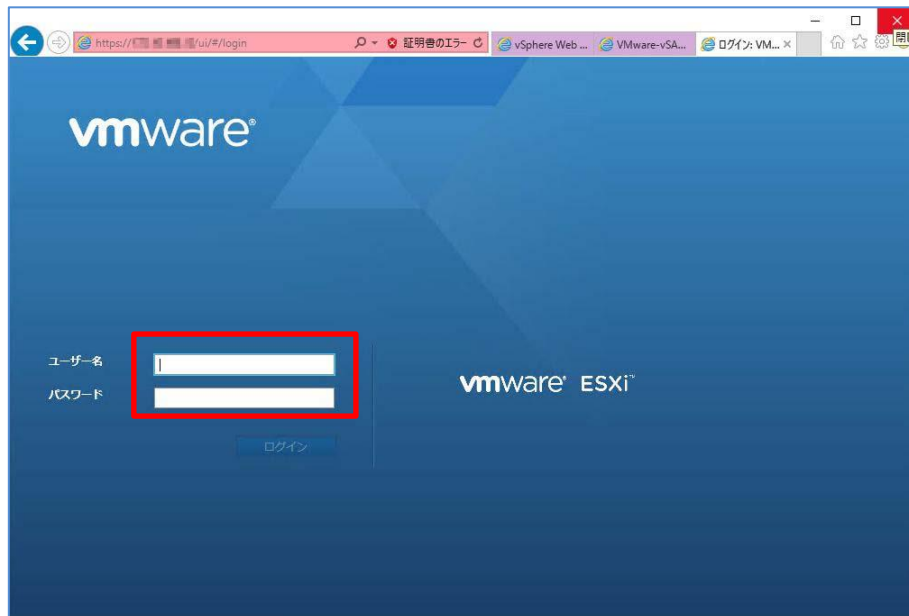
`http://<Witness ノードの IP アドレス>/`

(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)

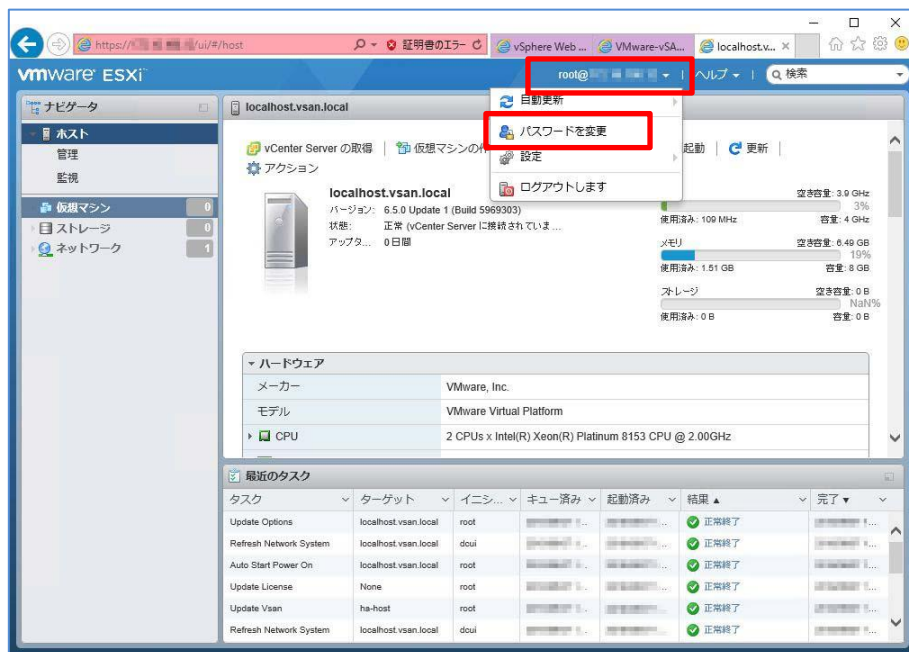
警告画面がでて、[このサイトの閲覧を続行する(推奨されません)]をクリックして、ログイン画面を表示します。



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。

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。

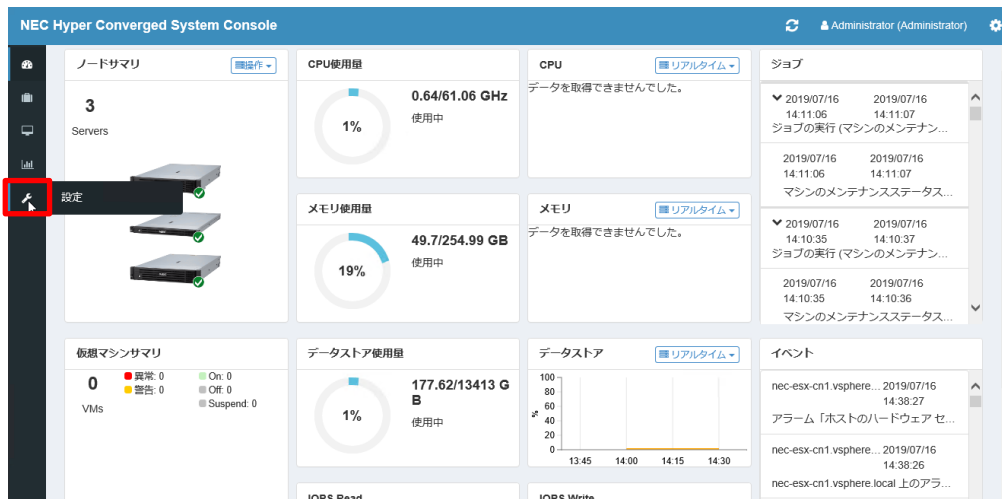
5.9 NEC Hyper Converged System Console の登録情報の更新

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

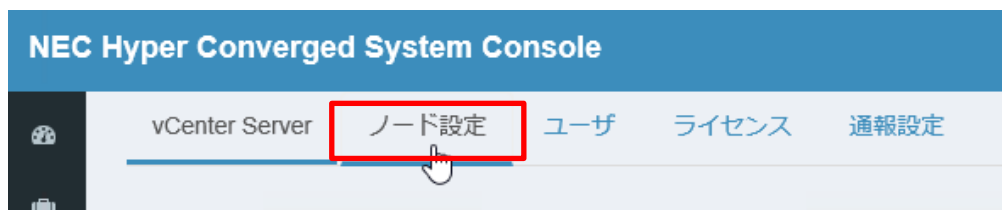
5.7 節の手順 1～3 を参照して、HCS Console にログインします。

5.9.1 ノード登録情報の更新

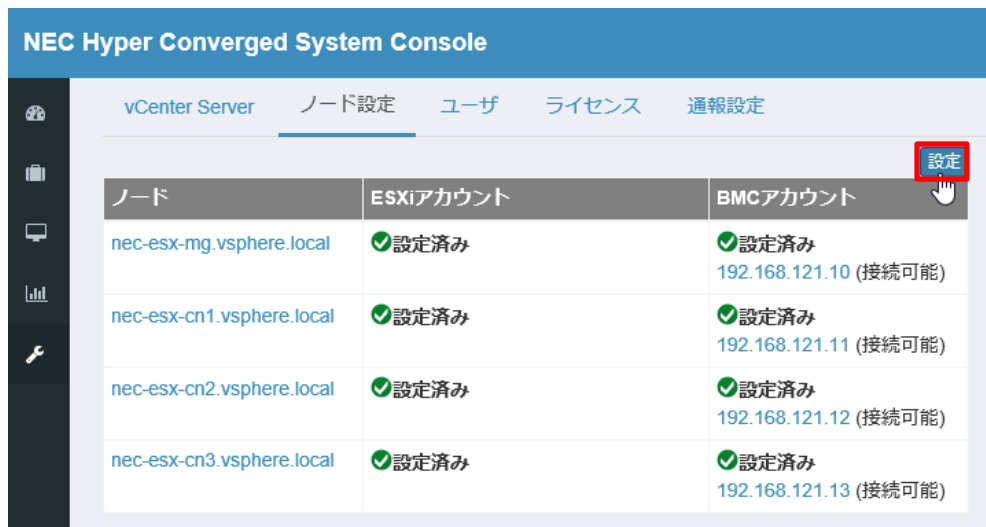
1. 画面左メニューの[設定]をクリックします。



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。
 - ※ 2 ノード構成の場合、witness ノードには BMC がありませんが、空白の状態では適用時にエラーになりますので、BMC ユーザ名、BMC パスワード、BMC 接続先に任意の値を入力して下さい。
 - ※ 上記のため、2 ノード構成の場合、ジョブの実行結果がかならず失敗となります。witness ノードの BMC アカウント以外が正常に登録されていることを確認してください。

ノード設定
×

一括設定

ノード	ESXiユーザ名	ESXiパスワード	BMCユーザ名	BMCパスワード	BMC接続先
nec-esx-mg.vsphere.local	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>
nec-esx-cn1.vsphere.local	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>
nec-esx-cn2.vsphere.local	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>
nec-esx-cn3.vsphere.local	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>

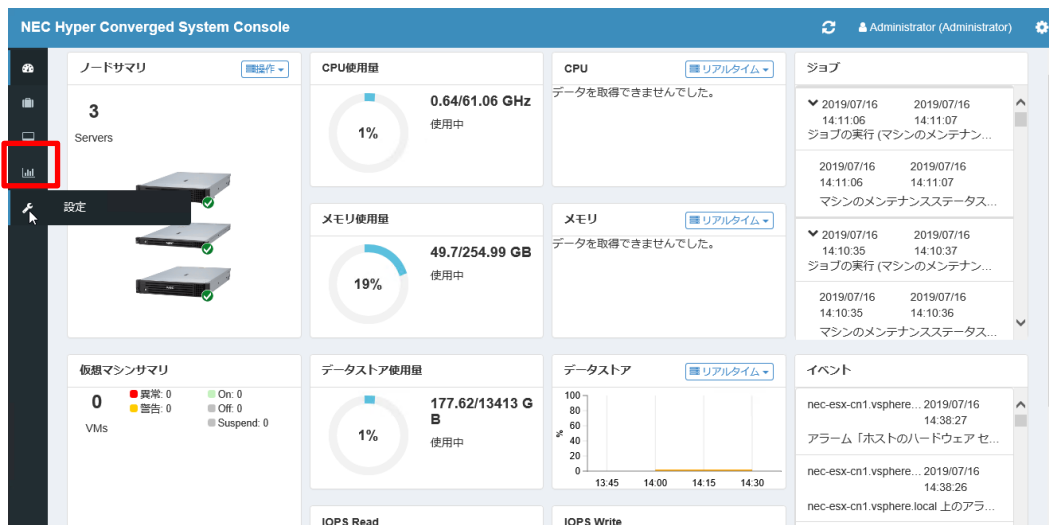
適用

閉じる

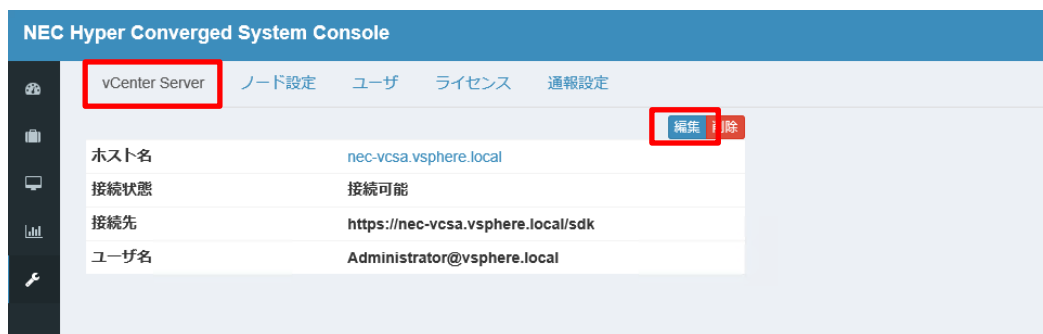
5. これでノード登録情報の更新は完了です。

5.9.2 vCSA 登録情報の更新

- 画面左メニューの[設定]をクリックします。



- 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。



- vCenter Server の追加 / 編集ダイアログが開きますので、パスワード更新にチェックを入れて、変更後のパスワードを入力して[適用]をクリックします。

vCenterServerの追加 / 編集 ✕

ホスト名

ポート

ユーザ名

☒ パスワード更新

パスワード


- これで vCSA 登録情報の更新は完了です。

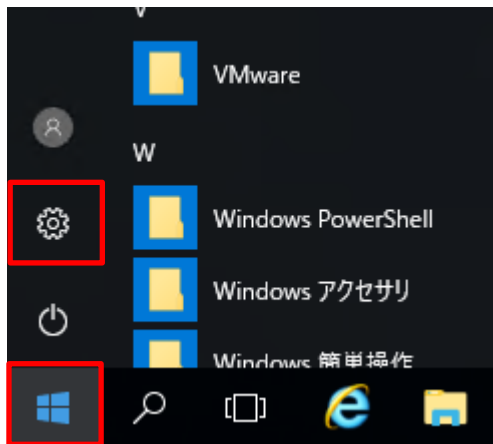
5.10 保守アカウントのパスワード変更

本項では、保守アカウントのパスワード変更について記載します。

5.10.1 管理 VM 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)

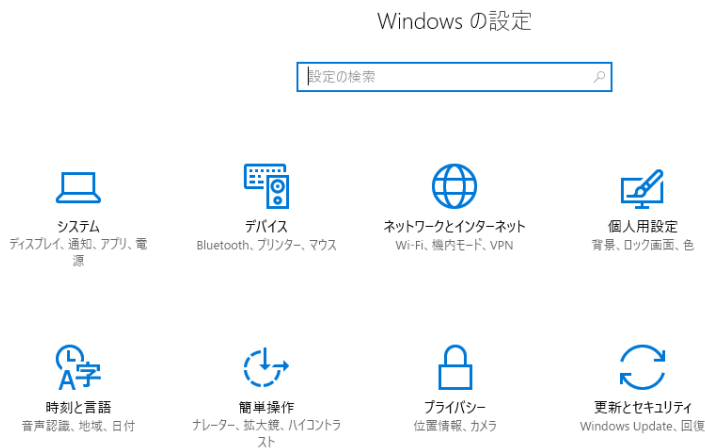
2. 管理 VM 上で、スタートボタンをクリックし、アイコンをクリックします。



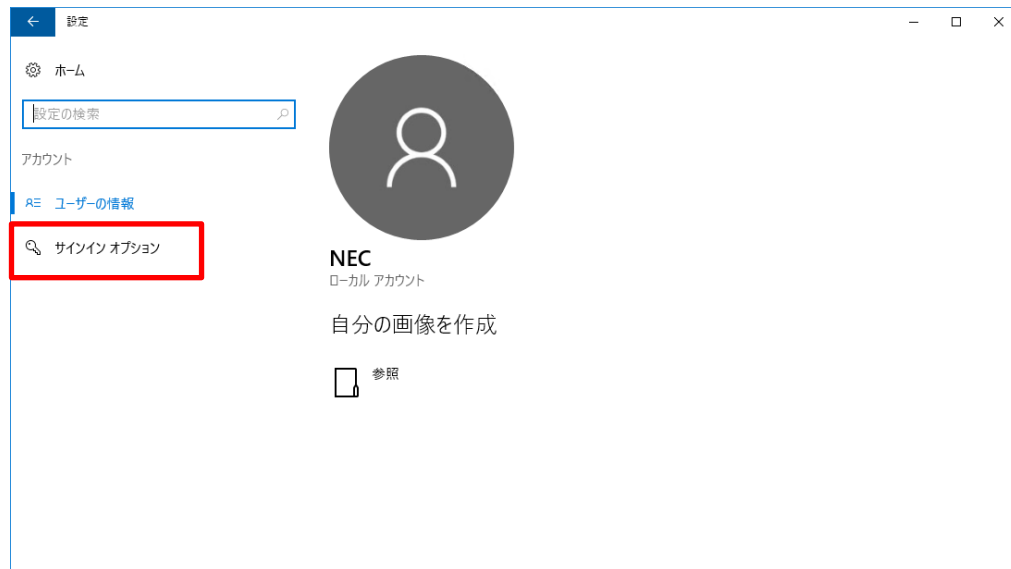
3. Windows の設定画面が開くので、[アカウント]をクリックします。

設定

— □ ×



4. 画面左側のメニューで[サインイン オプション]をクリックします。



5. 画面右側のパスワード項目にある[変更]をクリックします。



6. 現在のパスワードを入力して、[次へ]をクリックします。

個人用パスワードの変更

まず、現在のパスワードを入力してください。

nec

現在のパスワード

次へ キャンセル

7. 新しいパスワードとパスワードのヒントを入力し[次へ]をクリックします。

個人用パスワードの変更

新しいパスワード

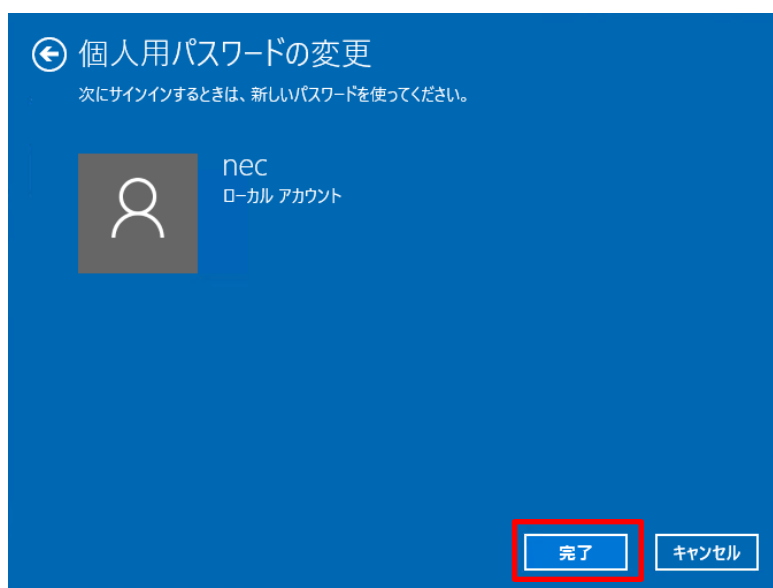
パスワードの確認入力

パスワードのヒント

次へ キャンセル

※ 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. 最後に[完了]をクリックして終了です。

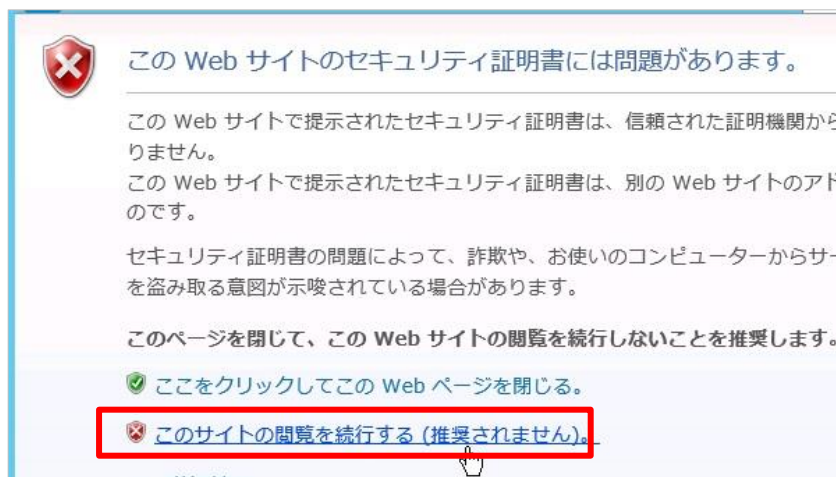


5.10.2 vCenter Server の保守アカウントのパスワード変更

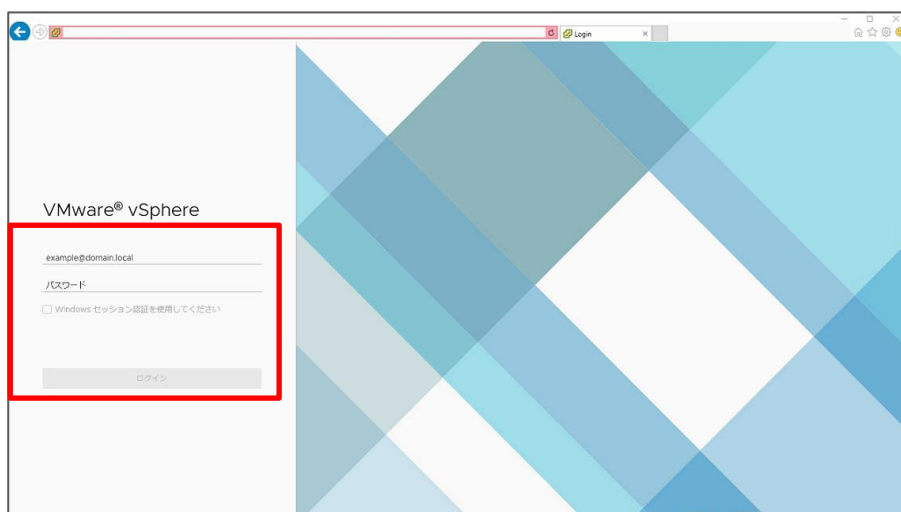
1. Windows PC でリモートデスクトップ接続(mstsc)を起動し、ヒアリングシートに記載されている「管理 VM」の IP アドレスを入力し、管理 VM に保守アカウントでログインします。
(IP アドレス例: 192.168.100.10:3389)
2. 管理 VM 上で Web ブラウザ(Internet Explorer)を起動します。
3. Web ブラウザのアドレス欄に以下の URL を入力します。

`http://<vCSA のホスト名>/ui`

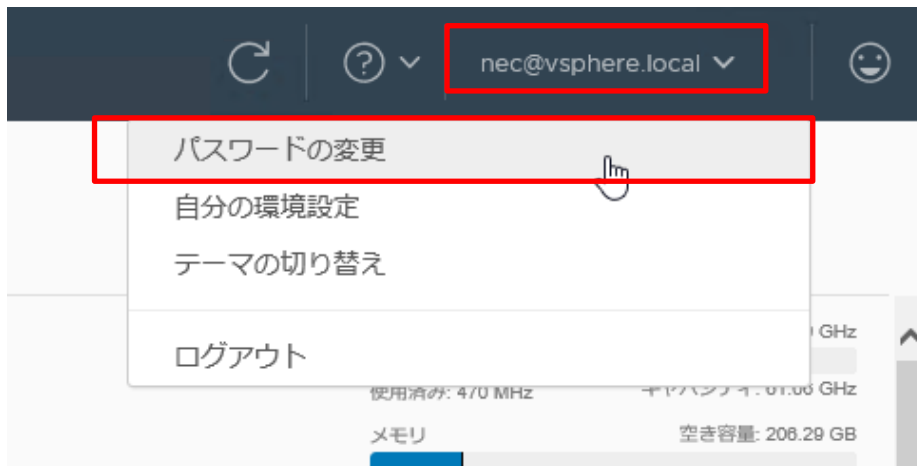
※ 「この Web サイトのセキュリティ証明書には問題があります。」画面が表示された場合は、「このサイトの閲覧を続行する(推奨されません)。」をクリックしてください。



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。

パスワードの変更 | nec@vsphere.local ×

現在のパスワード:
新しいパスワード:
パスワードの確認:

キャンセル OK

※ 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「Secure Boot」はステータスが「Risk」になっていますが、「IPMI/DCMI Over LAN」は「Enabled」、「Secure Boot」は「Disabled」の状態にしておいてください。

NEC iLO 5 1.43 May 23 2019 × 情報 - Security Dashboard

概要 Security Dashboard セッションリスト iLOイベントログ インテグレートドマネジメントログ Active Health Systemログ

情報 システム情報 ファームウェア & OSソフトウェア iLO連携 リモートコンソール & メディア 電力 & 温度 Intelligent System Tuning iLO専用ネットワークポート iLO共有ネットワークポート 管理 セキュリティ マネジメント EXPRESSBUILDER

Overall Security Status : Risk

セキュリティ状態 本番環境
Server Configuration Lock: Disabled

Security Parameter	↓ステータス	状態
<u>IPMI/DCMI Over LAN</u>	♥ Risk	Enabled
<u>Require Login for iLO RBSU</u>	♥ Risk	Disabled
<u>Secure Boot</u>	♥ Risk	Disabled
<u>Password Complexity</u>	♥ Risk	Disabled
<u>Security Override Switch</u>	♥ OK	Off
<u>Minimum Password Length</u>	♥ OK	OK

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 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。

NEC Corporation 2017-2019

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	<input type="checkbox"/>		
2	本製品の設置	<input type="checkbox"/>		
3	ネットワーク装置への接続	<input type="checkbox"/>		
4	電源の接続	<input type="checkbox"/>		
5	管理ノードの電源オン	<input type="checkbox"/>		
6	Windows PCの準備	<input type="checkbox"/>		
7	Windows PCから管理VMに接続	<input type="checkbox"/>		
8	DNS疎通確認	<input type="checkbox"/>		
9	VMware vCenter Serverへの接続確認	<input type="checkbox"/>		
10	クラスタノードの電源オン	<input type="checkbox"/>		
11	VMware vCenter Server上での機器確認	<input type="checkbox"/>		
12	隔離IPの到達確認	<input type="checkbox"/>		
13	クラスタノードのメンテナンスモード解除	<input type="checkbox"/>		
14	VMware vSAN状態の確認	<input type="checkbox"/>		
15	NEC Hyper Converged System Consoleの動作確認	<input type="checkbox"/>		

以上