

NEC Hyper Converged System for VMware vSAN/CR2.0

初期システム構成のバックアップ／リストア 手順書

2023 年 3 月

日本電気株式会社



目次

免責事項	2
商標および著作権	2
改版履歴	2
はじめに	3
本書内の表記	3
1. 管理ノードのバックアップ/リストア	5
1.1. 管理ノードのバックアップ	5
1.2. 管理ノードのリストア	5
本作業による影響	6
作業時間の目安	6
作業実施に必要な環境・機材	6
1.2.1. リストアの準備	7
1.2.2. ソフトウェア(ESXi の設定)のリストア	9
1.2.3. iLO の設定リストア	14
1.2.4. リストア後の HCS 環境の復旧	19
1.2.5. 《参考》リストア後のライセンスの再登録	36
2. クラスターノードのバックアップ/リストア	42
2.1. クラスターノードのバックアップ	42
2.2. クラスターノードのリストア	42
本作業による影響	43
作業時間の目安	43
作業実施に必要な環境・機材	43
2.2.1. リストアの準備	44
2.2.2. ソフトウェア(ESXi の設定)のリストア	50
2.2.3. iLO の設定リストア	53
2.2.4. リストア後のノード再稼働	58
2.2.5. NEC HCS Console の確認	63
3. パスワード更新	64
3.1. 準備	64
3.2. 管理ノードの管理 VM のパスワード更新	64
3.3. 管理ノード、クラスターノード、vCenter Server、Witness ノード、HCS Console のパスワード更新	64
3.4. ESMPRO/ServerManager のパスワード更新	65
3.5. 保守アカウントのパスワード更新	65
4. 補足	66
4.1. VMware vSphere Client の接続方法	66
4.1.1. セキュリティ証明書のインストール	69
4.2. VMware Host Client の接続方法	73
4.3. iLO の接続方法	75
4.4. ESXi Shell の接続方法	77
4.4.1. コンソールを使用する場合	77
4.4.2. ターミナルソフトを使用する場合	80
4.5. NEC HCS Console の接続方法	86

免責事項

本書の内容の一部または全部を無断で複製・改変・再配布することを禁じます。

本書の内容は将来予告なしに変更することがあります。

本書の作成者および作成に関連する部門は、本書の技術的もしくは編集上の誤記・欠落・瑕疵が存在する場合においても、一切の責任を負いません。

本書の作成者および作成に関連する部門は、本書の内容に沿った操作を行って生じた事象（障害・不具合、およびこれに限らず全ての現象）、ならびに、本書の内容に沿った操作を行ったにもかかわらず記載と異なる動作・結果・障害が生じた場合に関して、一切の責任を負いません。

商標および著作権

VMware 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。

Microsoft、Windows、Windows Server、Microsoft Edge は米国 Microsoft Corporation の米国およびその他の国における登録商標または商標です。

その他、本書内に記載されている会社名および製品名は、それぞれの所有者の登録商標または商標です。

なお、VMware 社の商標に関する詳細は <https://www.vmware.com/jp/help/trademarks.html> を参照ください。

本書では、(R)と TM の表記を省略しています。

改版履歴

版	日付	内容
1.0	2020/10	初版作成
1.1	2021/3	vSphere7.0u1 に対応 4.5 項追加
1.2	2021/6	1.2.4.3 項、1.2.4.4 項修正 誤記修正
1.3	2021/12	エクスプレス通報サービスに対応
1.4	2022/3	vSphere7.0u3 に対応 2.2.2 項、2.2.4 項、3.3 項修正
1.5	2022/11	サーバ診断カルテに対応
1.6	2022/11	3 章のパスワード更新手順を修正
1.7	2023/3	Windows Server 2022 に対応 Microsoft Edge に対応 ESMPRO/Server Manager Ver.7 に対応 Firefox を削除

はじめに

本書は、NEC Hyper Converged System 環境(以下、HCS 環境)における、バックアップ・リストア手順について記載しています。

本書に示す手順は、出荷時の HCS 環境の ESXi サーバの設定および仮想マシンのバックアップをリストアするものであり、これに該当しないバックアップ・リストアの操作は対象外となりますのでご注意ください。

本書内の表記

本書内で使用されている略語については、以下の一覧を参照ください。

コンポーネント名	略語
NEC Hyper Converged System	HCS
NEC Hyper Converged System Console	HCS Console
VMware ESXi	ESXi
VMware vCenter Server Appliance	vCSA
VMware Host Client	Host Client
VMware vSphere Client	vSphere Client
VMware vSAN	vSAN
ソリッドステートドライブ	SSD

本書内で使用する表記とその内容については以下を参照ください。

表記	本書での意味・内容
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。
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。
クラスタノード	HCSの構成部品。VMware vSANクラスタを動作させるためのExpressサーバ群。
管理ノード	HCSの構成部品。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。
Witnessノード	HCSの構成部品。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の仮想マシン。HCSの管理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。
VMware vSphere Client (vSphere Client)	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。

VMware Host Client (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。
内部ネットワーク (内部NW)	VMware ESXiの管理、vSAN、vMotion、iLOの通信を行うネットワーク。
管理用ネットワーク (管理用NW)	管理VMとの通信を行うお客様の管理ネットワーク。
緊急ネットワーク (緊急NW)	緊急時に管理ノード、(クラスタノード)との通信を行うお客様の管理ネットワーク。
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)。
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。
Windows PC	オペレータが操作するPC機器。

1. 管理ノードのバックアップ／リストア

本章では、管理ノードのバックアップおよびリストア手順について記載しています。

1.1. 管理ノードのバックアップ

管理ノードのバックアップは、出荷時点で実施済みですので、作業は不要です。

1.2. 管理ノードのリストア

管理ノードのリストアは以下の順序で行います。各項目の詳細は、1.2.1 項から 1.2.4 項を参照ください。



本作業による影響

管理ノードのリストア操作により、管理ノードは再起動を行います。また、管理ノード上の仮想マシンは、全て電源 OFF となり、出荷時にインストール済みの管理 VM、vCSA、(オプション: hcs-backup) のみが実行可能な状態となります。

※ お客様が管理ノードで行った(ライセンスを含む)設定、管理ノード上に作成した仮想マシンは、全てクリアされ(ただし、出荷時にインストールされていなかった仮想マシンのイメージファイルは削除されません)、vCenter Server および管理ノードに登録されていない状態となります。

特に、リストアスクリプトの実行中は、管理ノード、および管理 VM や vCSA を含む管理ノード上の全ての仮想マシンが操作できない状態となりますのでご注意ください。

作業時間の目安

およそ 2 時間

※ 作業時間には、ソフトウェアのリストアからリストア後の環境復旧操作までを含みます。

作業実施に必要な環境・機材

管理ノードのリストア作業の際は、以下の Windows PC が必要となります。

- 管理用 NW に接続している。
- 管理 VM にリモートデスクトップ接続できる。
- 管理ノードに SSH で接続できる。
※ 通常、SSH による接続が可能なターミナルソフトを使用します。

オペレータは、この Windows PC から管理 VM、管理ノードにアクセスして作業を行います。

また、下記のドキュメントもご用意ください。

- NEC Hyper Converged System 初期パスワード通知書

1.2.1. リストアの準備

本項は、管理ノードのリストアを行う前に必要な操作について記載しています。

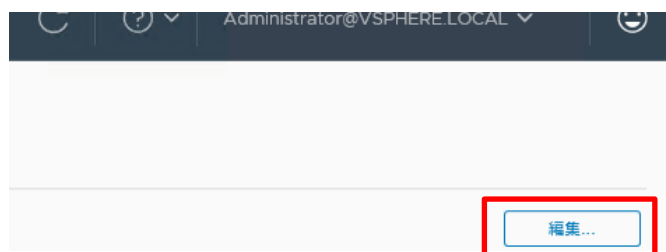
【重要】

リストア操作を行うには、管理ノードは、出荷時と同じハードウェア構成である必要があります。また、出荷時点でインストールされていたパッチとストレージコントローラのデバイスドライバ・ファームウェアが全て適用済みであり、同じビルド番号である必要があります。

1. 管理 VM に管理者権限を有するユーザでサインインし、vSphere Client で vCenter Server に接続します
2. 画面左に表示されるサーバのツリービュー（本書では、以降、下線部分を「オブジェクトナビゲータ」と表記します）で vSAN クラスタ名をクリックした後、[設定]または[構成]タブ – [vSphere の可用性]の順にクリックします。



3. タブ画面内右上の、「vSphere の可用性」の右端に表示される[編集]をクリックします。



4. 「クラスタ設定の編集」ダイアログが表示されますので、ダイアログ内上のメニューで[障害および対応]をクリックした後、[ホスト監視の有効化]の状態を確認します。状態が有効の場合は無効にし、ダイアログ内右下の[OK]をクリックします。

vSphere HA 

障害および対応 アドミッション コントロール

クラスタに障害が発生した場合、vSphere HA でどのように
離、仮想マシン コンポーネント保護 (PDL および APD 状態)

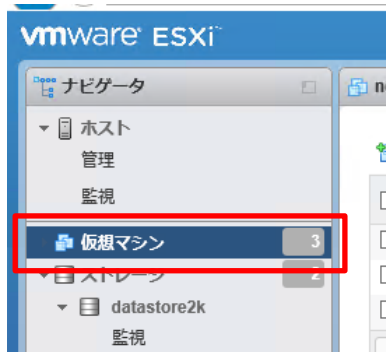
ホスト監視の有効化 

[注意]

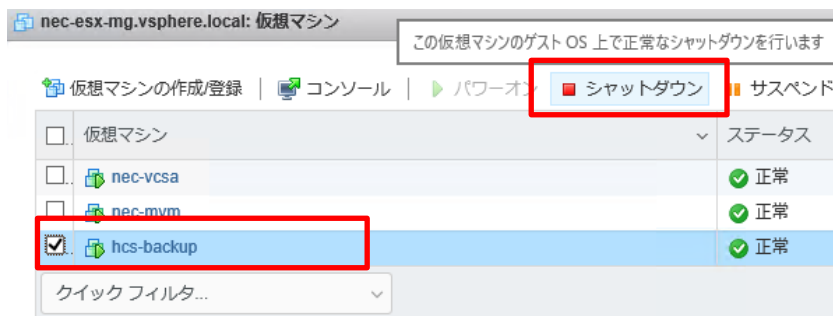
管理ノードに hcs-backup が存在する場合、管理ノードのソフトウェア(ESXiの設定)のリストアを開始する前に、hcs-backup をシャットダウンする必要があります。

hcs-backup のシャットダウン手順は、以下の操作を実施してください。

1. 管理VMから管理ノードのHost Clientにログインします。
2. Host Client 画面左の、[ナビゲータ]枠内の[仮想マシン]をクリックします。



3. 画面右の一覧にある hcs-backup の行頭にチェックを入れ、[シャットダウン]をクリックします。



以上で、hcs-backupのシャットダウンは完了です。

以上で、リストアの準備は完了となります。引き続き、1.2.2 項の作業を行ってください。

1.2.2. ソフトウェア(ESXi の設定)のリストア

バックアップしたデータを管理ノードにリストアする際は、以下の手順で行います。

【重要】

リストア操作を行った場合、vCSAおよび管理VMの設定が全て出荷時の状態に上書きされます。万一の事態に備え、必要な設定およびデータは、リストア実施前に必ずメモに残すかコピーするようにしてください。なお、hcs-backupは、バックアップ／リストアの対象外となっているため、リストア操作を行っても出荷時の状態に戻りません。

リストア前の環境において、お客様が管理ノード上に作成した仮想マシンは、リストアを行うことで、実行可能な仮想マシンとしての登録情報が削除されますが、仮想マシンを構成するファイル(.vmxや.vmdk等)は削除されません。リストア実施後、必要に応じ1.2.4.3項の手順4の「《参考》」の操作を行って、再度実行可能な仮想マシンとして登録してください。また、リストア前の環境で作成した仮想マシンが不要な場合は、1.2.2項の手順2で確認した.vmxファイルが保存されているフォルダを削除してください。

1. WindowsPC からコンソールまたはターミナルソフトでバックアップ対象のクラスタノードの 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、管理ノードに登録されている仮想マシンの情報を表示します。

```
# vim-cmd vmtoolsd/getallvms
```

vCSA、管理 VM、witness および hcs-backup 以外の仮想マシンが登録されている場合は、該当する全ての仮想マシンの.vmx ファイルが保存されているデータストア名(=以下画面の[]内の文字列。以下画面の場合、datastore2k)、および画面に表示されている.vmx ファイルのパス(以下画面の場合、VM01/VM01.vmx)をそれぞれメモに記録してください。

```
[root@nec-esx-mg:~] vim-cmd vmtoolsd/getallvms
Vmid      Name      File
3         nec-vcsa  [datastore2k] nec-vcsa/nec-vcsa_1.vmx
4         nec-mvm   [datastore2k] nec-mvm/nec-mvm_1.vmx
5         hcs-backup [datastore2k] hcs-backup/hcs-backup.vmx
7         VM01      [datastore2k] VM01/VM01.vmx
[root@nec-esx-mg:~]
```

3. 以下のコマンドを実行し、datastore2k データストアが存在することを確認してください。

```
# ls /vmfs/volumes/datastore2k/
```

※ データストアが存在する場合は、以下画面のようにデータストア内に「hcsbackup-initial」、「scripts」フォルダが表示されます。

```
[root@nec-esx-mg:~] ls /vmfs/volumes/datastore2k/
hcs-backup      nec-mvm      scripts
hcsbackup-initial nec-vcsa     sysupdate
[root@nec-esx-mg:~]
```

4. 以下のコマンドを順に実行し、リストアを実行します。

```
# cd /vmfs/volumes/datastore2k/scripts
# ./inithcs.sh
```

```
[root@nec-esx-mg:~] cd /vmfs/volumes/datastore2k/scripts/
[root@nec-esx-mg:/vmfs/volumes/5d36a516-4c969e74-6a3a-f4034357d1c4/scripts] ./inithcs.sh
```

[注意]

スクリプト (inithcs.sh) は、vCSA および 管理 VM の仮想ハードディスクをシンプロビジョニング形式でリストアします。シックプロビジョニング形式でリストアする場合は、inithcs.sh スクリプトの改変 (スクリプト内で vmkfstools コマンドの -d オプションの引数 (以下画面の thin の箇所) を eagerzeroedthick もしくは zeroedthick に変更) を行ってください。

```
vmkfstools -i "$sbeeline" "$srcdir"/"$destvmpath"/"$zbeeline" -d thin
```

スクリプト実行直後に、リストアの開始を確認するメッセージが表示されます。

リストアを開始する場合は、[yes] と入力した後、[Enter] キーを押下します。リストアを中断する場合は、何も入力せずに [Enter] キーを押下してください。

リストアが開始され、その終了後、管理ノードが自動的に再起動し、リストアした内容が反映されます。

※本手順以降、管理ノードの ESXi、管理 VM、vCSA のパスワードが初期パスワードになります。

各初期パスワードは「初期パスワード通知書」を参照ください。サーバ診断カルテを設定している場合は、サーバ診断カルテに登録しているパスワードも同様にバックアップ時点のパスワードになります。

```
[root@nec-esx-mg:/vmfs/volumes/5d36a516-4c969e74-6a3a-f
* This process will INITIALIZE the environment of VMs.
  All of VMs managed by this ESXi will be replaced with
  with initial factory settings.
Do you want to proceed? [*]yes yes

* Restore process started at 20190821-075648 *
-----
* Powering off the VM named "nec-vcsa".
Powering off VM:
* now cheking if VM named "nec-vcsa" is powered off ...
* Unregistering VM named "nec-vcsa".
* Powering off the VM named "nec-mvm".
Powering off VM:
* now cheking if VM named "nec-mvm" is powered off ...0
* Unregistering VM named "nec-mvm".

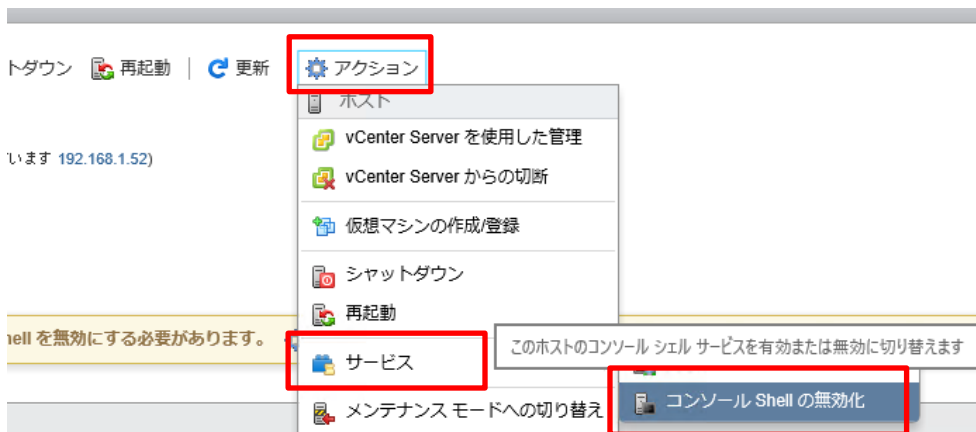
* Restoring a VM named "nec-vcsa" has started.
- Directory to restore: "/vmfs/volumes/datastore2k"
- Old directory "nec-vcsa" was deleted.
- Restoring nec-vcsa_1.vmdk ...
Destination disk format: VMFS thin-provisioned
Cloning disk '/vmfs/volumes/datastore2k/hcsbackup-initi
Clone: 23% done.█
```

5. 管理ノードの再起動後、管理 VM に管理者権限を有するユーザでサインインし、管理ノードの Host Client にログインします。

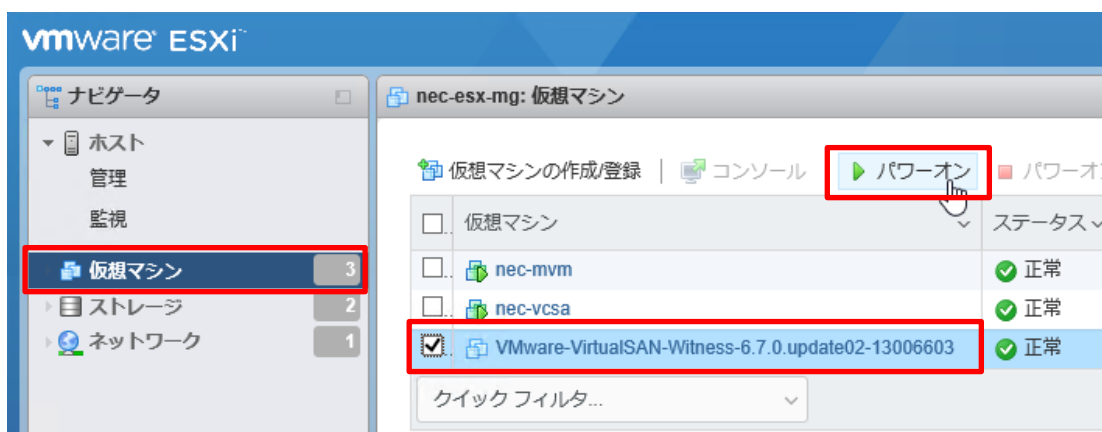
6. Host Client 画面左の、[ナビゲータ]枠内の[ホスト]をクリックします。



7. 画面内右上の[アクション]をクリックし、[サービス] - [コンソール Shell の無効化]を順にクリックします。

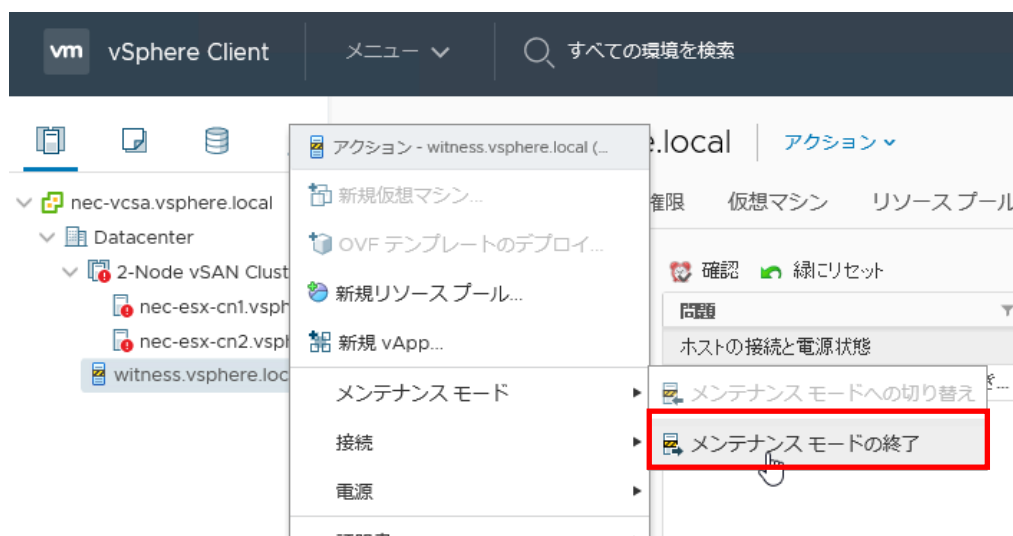


8. 2 Node 構成の場合は[ナビゲータ]枠内の[仮想マシン]をクリックし、仮想マシン一覧の中から witness ノードを選択した状態で、画面上部の[パワーオン]をクリックします。



9. vSphere Client で vCSA にログインします。
10. クラスタノードがメンテナンスモードの場合は、自動で解除されますので解除されるまでお待ちください。
- ※ メンテナンスモード解除されるまで時間がかかることもありますが、解除されない場合は手動で解除してください。

11. 2 Node 構成の場合は、オブジェクトナビゲータから witness ノードを右クリックし、出てきたメニューの中から[メンテナンスモード] – [メンテナンスモードの終了]をクリックします。



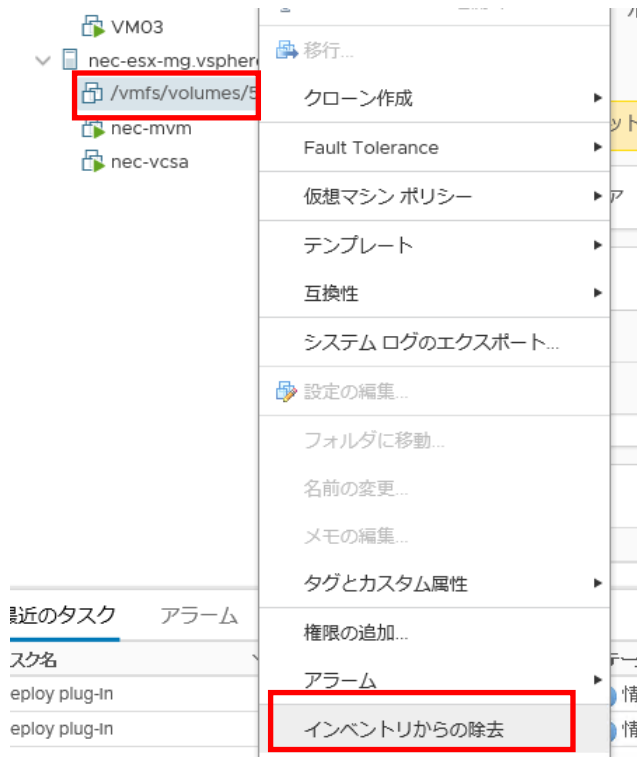
12. vSphere Client でホーム画面を表示している状態でオブジェクトナビゲータの[ホストおよびクラスタ] (vSphere 7.0u3 の場合、画面左上のメニューアイコンをクリックし、[インベントリ])をクリックし、各サーバおよび仮想マシンの状態を確認します。

以下の操作は、リストア後の管理ノードの状況により、必要に応じて行ってください。

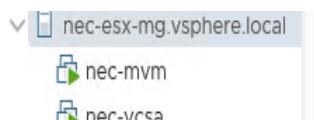
- ◆ リストアを行った後、管理ノード上の仮想マシンのサマリに「この仮想マシンにはネットワークが割り当てられていません。」と表示される場合:



この場合は、vSphere Client の「ホストおよびクラスタ」の画面において、オブジェクトナビゲータで該当する仮想マシン名を右クリックした後、表示されるメニューで[インベントリからの除去]または[インベントリから削除]をクリックします。



上記操作により、サマリに「この仮想マシンにはネットワークが割り当てられていません。」と表示された仮想マシンがインベントリから削除されます。



以上で、管理ノードを構成するソフトウェアのリストアは完了となります。

なお、リストアを行う前の管理ノードにおいて、お客様が作成した仮想マシンが存在し、当該仮想マシンを再度インベントリに登録する場合は、1.2.4.3 項の手順 4 の操作を行ってください。

1.2.3. iLO の設定リストア

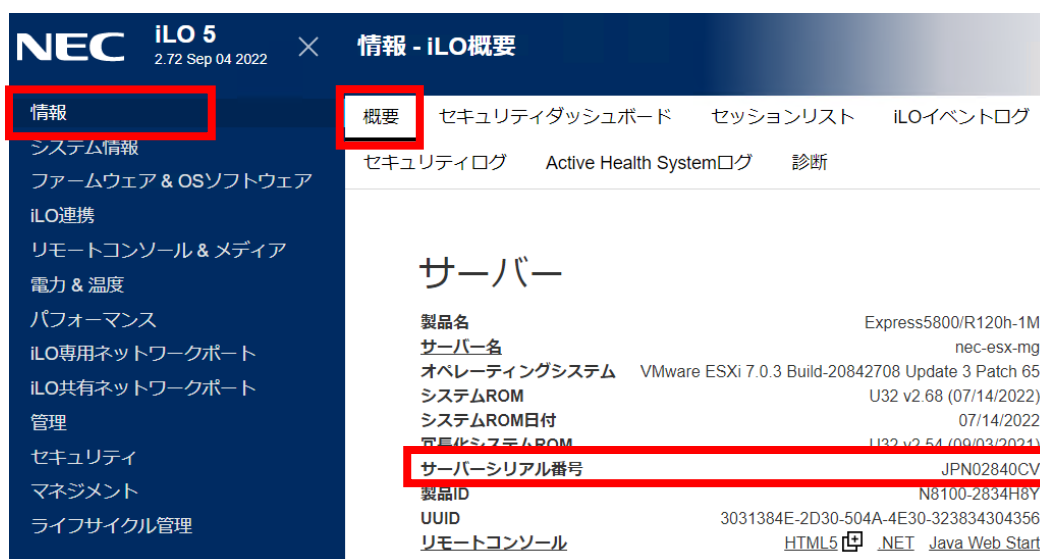
管理ノードとなるサーバ装置における iLO の設定リストアは、以下の手順で行います。

[注意]

iLO の設定バックアップを行った後、リストア対象のノードのマザーボードが故障し交換を行った場合、もしくは Starter Pack により iLO ファームウェアのアップデートを行った場合（一部のバージョンを除く）、アップデート前のバックアップデータはリストアできない状態となりますのでご注意ください。

詳細は、Starter Pack のダウンロードページ内に掲載されている [iLO ファームウェアアップデート補足] を参照ください。

1. 管理 VM に管理者権限を有するユーザでサインインし、管理ノードの iLO にログインします。
2. iLO の Web インターフェイス画面が表示されますので、画面左のメニューで [情報] – [概要] の順にクリックし、「サーバーシリアル番号」を確認します。

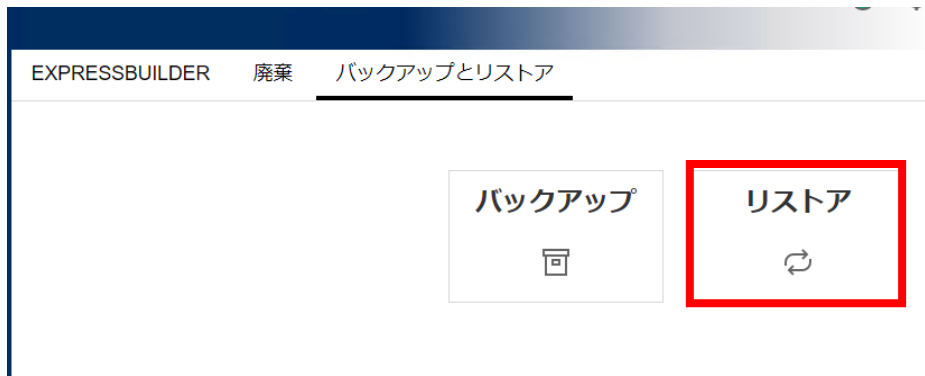


3. 画面左のメニューで [ライフサイクル管理] – [バックアップとリストア] の順にクリックします。

※ iLO FW バージョンによって画面左のメニューが異なる場合があります。[ライフサイクル管理]がない場合は、[管理] – [バックアップとリストア] の順にクリックしてください。



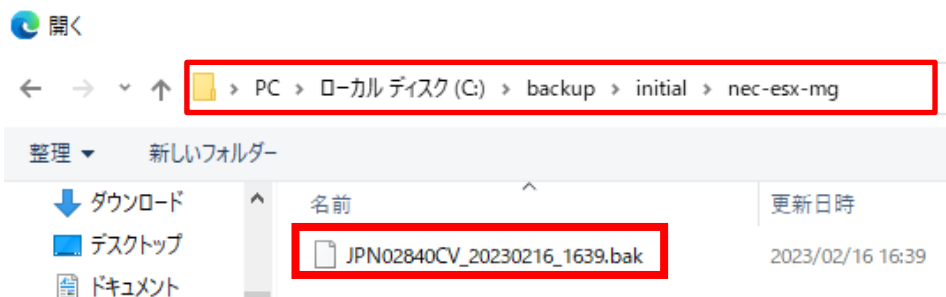
4. 「バックアップとリストア」の画面が表示されますので、[リストア]枠内のアイコン部分をクリックします。



5. 画面右に「リストア」の設定項目が表示されますので、[参照]をクリックします。



6. 「開く」ダイアログが表示されます。「C:¥backup¥initial¥nec-esx-mg」フォルダに移動し、ファイル名に手順2で確認したシリアル番号で始まる.bak ファイルを選択した後、ダイアログ右下の[開く]をクリックします。



7. 「リストア」の画面にフォーカスが戻ります。[バックアップファイル]欄に手順 6 で選択したファイル名が表示されていることを確認した後、[アップロードおよびリストア]をクリックします。

※ iLO のバックアップの際にパスワードを設定した場合は、[アップロードおよびリストア]をクリックする前に、「バックアップファイルパスワード」の下の入力欄にパスワードを入力してください。

リストア



リストアすると、すべての構成設定が置き換えられます。

バックアップファイルパスワード	オプション
バックアップファイル	
ファイルの選択	JPN02840CV_2...30216_1639.bak

アップロードおよびリストア

8. ブラウザの画面右に以下メッセージが表示されます。リストアを行うサーバにおいて、iLO への接続が一時的に切断しても問題が無いことを確認した後、[リストア]をクリックします。



リストアの確認

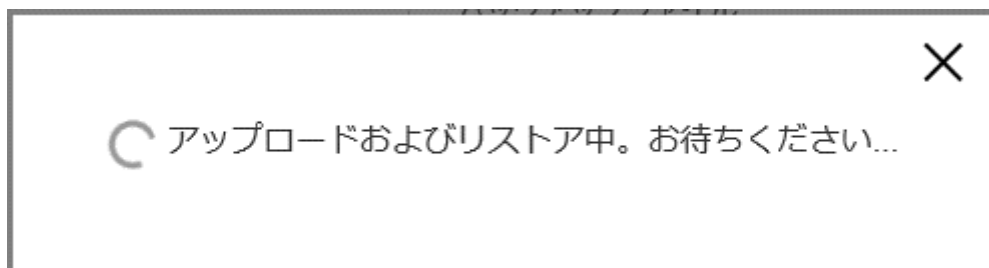
iLOの設定を復元すると、iLOが再起動されます。これにより、リモートコンソールと仮想メディアを含むiLOへの接続がすべて終了します。サーバーは影響を受けません。

リストア

《参考》

この操作により管理ノードとなるサーバ装置のiLOが再起動しますが、当該サーバのESXiは稼働したままの状態を維持しますので、管理ノード上の仮想マシン(vCSAおよび管理VMを含む)は停止しません。

9. 設定情報のリストアが開始され、ブラウザに以下メッセージが表示されます。



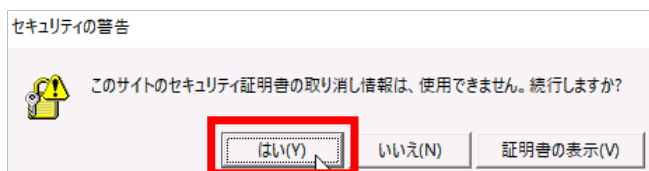
しばらくするとブラウザの表示が更新され、iLO のログインページと共に以下メッセージが画面右下に表示されます。

① **ログアウト: iLOをリセットしています。**

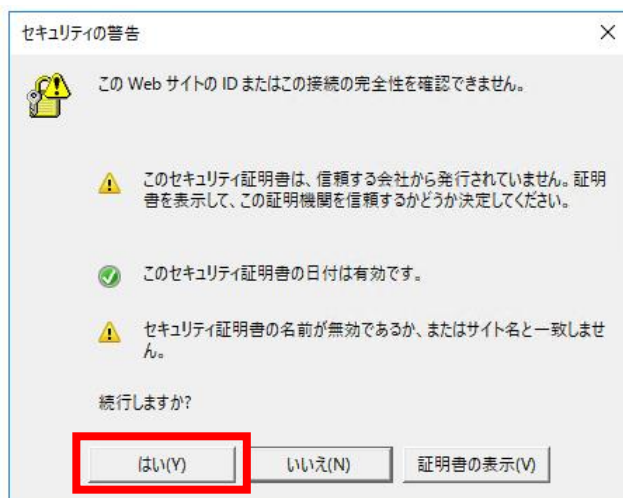
SSLまたはその他の接続エラーメッセージが表示された場合、ブラウザのキャッシュをクリアし、ブラウザを再起動して、再ログインしてください。

この操作は、数分間かかることがあります。

※ 上記画面に続き、以下確認ダイアログが表示される場合があります。この場合、[はい]をクリックして操作を継続してください。



また、以下「セキュリティ警告」のダイアログが表示された場合においても、[はい]をクリックしてください。



10. ブラウザの表示を更新し、iLO のログインページが表示されることを確認します。

※本手順以降、管理ノードの iLO のパスワードが初期パスワードになります。
管理ノードの iLO の初期パスワードは「初期パスワード通知書」を参照ください。

Orchestrating a brighter world **NEC**



※ ブラウザの画面右下に以下メッセージが表示される場合は、しばらく時間を置いた後、再度ブラウザの表示を更新してください。

✖ 接続が確立できません。ネットワークの構成を変更した場合には、SSL接続を再ネゴシエートするために、このページを更新してください。

以上で iLO の設定リストアは完了となります。

1.2.4. リストア後の HCS 環境の復旧

本項は、管理ノードのリストア実施後に必要な操作について記載しています。

1.2.4.1. vCLS の Retreat モード無効化

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

初期システム構成のバックアップデータでは vCLS の Retreat モードが有効に設定されているため、手動で Retreat モードを無効にして、vCLS エージェント VM を再作成する必要があります。

本項の手順を実施し、Retreat モードを無効化します。

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



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

❗ 構成パラメータの追加や変更はサポートされません。実行するとシステムが不安定になる可能性があります。構成パラメータを追加した後で削除することはできません。構成パラメータの変更について理解している場合にのみ続行してください。

名前	値	サマリ
config.log.outputToConsole	false	--
config.log.outputToFiles	true	--
config.registry.DB.key_2	vc	--
config.registry.DB.key_3	*J2H2j3KPcCqjGeK9pkYUofo7GuRTaa	--
config.registry.key_EvaluationExpiryDate	AQD+yggAAAAoFzbJ2uCyzkQAAAD	--
config.registry.key_VCVmId	vm-18	--
config.task.minCompletedLifetime	60	--
config.vcls.clusters.domain-c8.enabled	True	--
config.vdt.severity	none	分散トレースでデータを収集する詳細レベルを定義します
config.vmacore.cacheProperties	true	--

11 ~ 20 / 914 設定 |< < 2 / 92 > >|

名前 *: 値 :

追加

キャンセル

保存

名前の先頭には「config」を入力してください (例: config.log)

《補足》

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

vCenter Server の詳細設定の編集

❗ 構成パラメータの追加や変更はサポートされません。実行するとシステムが不安定になる可能性があります。構成パラメータを追加した後で削除することはできません。構成パラメータの変更について理解している場合にのみ続行してください。

名前	値
alarms.version	-1

vCenter Server の詳細設定の編集

❗ 構成パラメータの追加や変更はサポートされません。実行するとシステムが不安定になる可能性があります。構成パラメータを追加した後で削除することはできません。構成パラメータの変更について理解している場合にのみ続行してください。

名前	値
config.vcls.clusters.domain-c8.enabled	False

vcls

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

最近のタスク		アラーム					
タスク名	ターゲット	ステータス	詳細	開始者	待ち時間	開始時刻	
OVF テンプレートのデプロイ	vCLS (3)	86%	事前チェックを実行しています	com.vmware.vim.e...	2 ミリ秒	2021/02/08 17:26:45	
仮想マシンのパワーオン	vCLS (2)	完了		com.vmware.vim.e...	2 ミリ秒	2021/02/08 17:26:44	
パワーオンの初期化	Datacenter	完了		com.vmware.vim.e...	2 ミリ秒	2021/02/08 17:26:44	
仮想マシンの再設定	vCLS (2)	完了		VSPHERE.LOCAL...	2 ミリ秒	2021/02/08 17:26:44	

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

The screenshot shows the vSphere Client interface. In the left sidebar, the navigation tree is expanded to show 'vCLS (1)' under the 'Datacenter' folder. The main panel displays the summary for vCLS (1). The 'Guest OS' is 'Other 4.x or later Linux (64-bit)', 'VMware Tools' is 'Running', and the 'Storage' is 'vsanDatastore'. The 'Related Objects' section at the bottom shows the storage as 'vsanDatastore'.

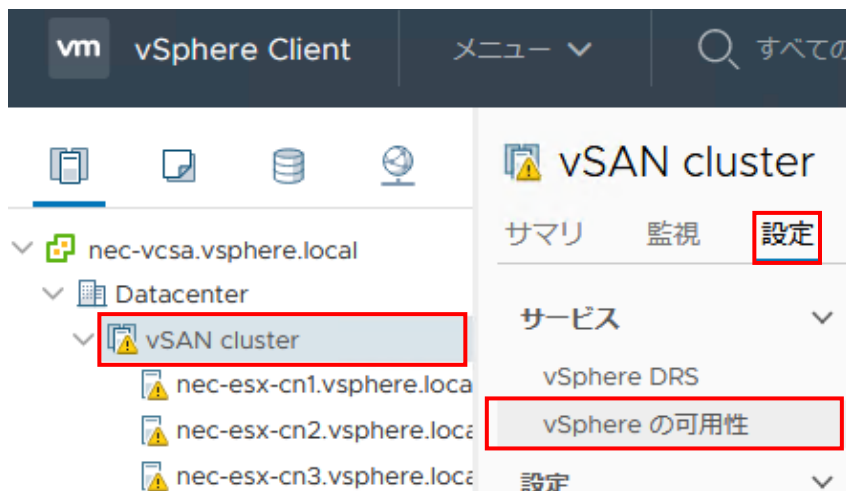
1.2.4.2. vSphere 可用性の設定

vSAN クラスタの vSphere の可用性を設定します。

1. 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] (vSphere 7.0u3 の場合、画面左上のメニューアイコンをクリックし、[インベントリ])をクリックします。



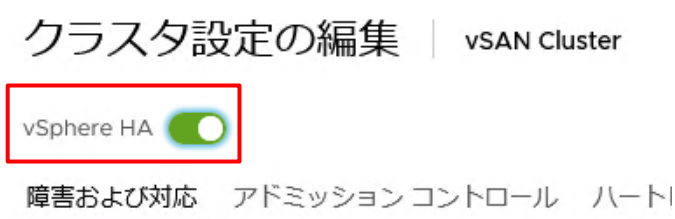
2. vSAN クラスタ名をクリックし、「設定」または「構成」→「vSphere の可用性」の順に選択します。



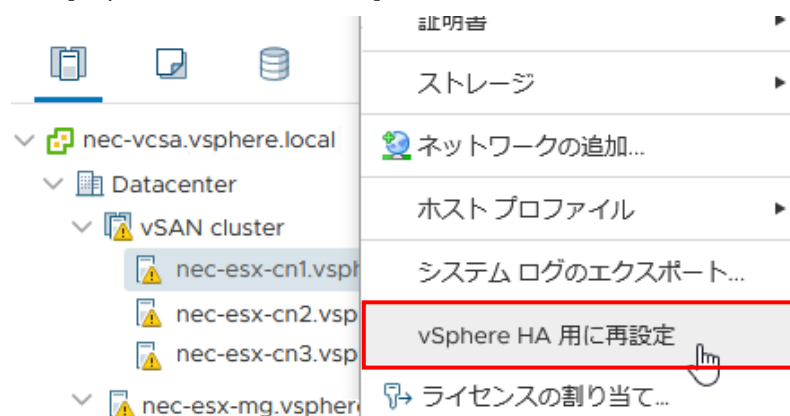
3. 画面右上の「編集」をクリックします。



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



5. 続いて、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。



[注意]

サーバ診断カルテを設定している環境で、管理ノードのリストアを実施することでサーバ診断カルテに登録しているクラスタノードのパスワードと実際のパスワードに差異が生じる場合、この時点でクラスタノードに「xx回ログインに失敗した後、ESXiローカルユーザアカウント「root」のリモートアクセスが900秒間ロックされました。」という警告が表示される場合があります。



この警告は、引き続きクラスタノードのリストアを実施する場合は無視して構いません。

クラスタノードのリストアを実施しない場合は、3.3項を参照し「5.9 NEC Hyper Converged System Consoleの登録情報の更新」および[注意]を実施し、NEC HCS ConsoleおよびESMPRO/ServerManagerに監視対象として登録したiLOやESXiのコンポーネントのパスワードを、現在使用しているパスワードに変更してください。

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

vSphere HA 

障害および対応 アドミッション コントロール ハートビート データストア 詳細

クラスタに障害が発生した場合、vSphere HA でどのように応答するかを設定できます。サボ
離、仮想マシン コンポーネント保護 (PDL および APD 状態のデータストア)、仮想マシン、ま

ホスト監視の有効化 

> ホストの障害応答

仮想マシンを再起動

7. 「障害状態および応答」を確認します。

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

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

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

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	! 無効

1.2.4.3. HCS 環境の復旧

リストア後に表示されるアラートやエラーの確認と復旧作業を行います。

1. vSphere Client のオブジェクトナビゲータで vSAN クラスタ名を選択した状態で、画面中央上部の[監視]をクリックします。続いて、タブ画面内左のメニューで[▼問題とアラーム]の下の[すべての問題]をクリックします。

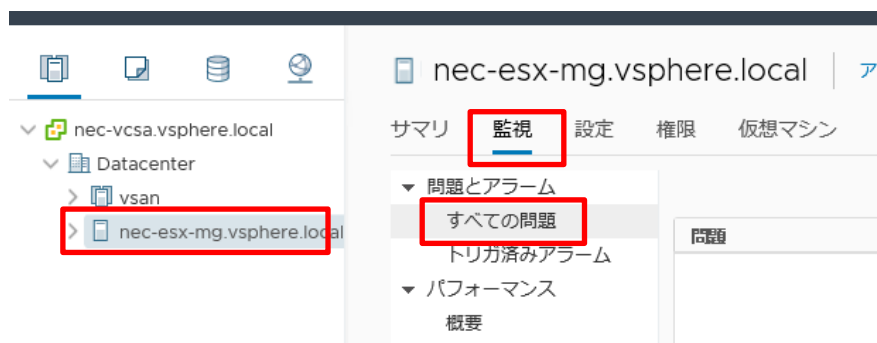


2. 画面内右の一覧にアラートやエラーが表示されていないことを確認します。

以下画面のように何らかのアラートやエラーが発生している場合は、対処済み、および対処不要の内容については、その行を選択した状態で一覧の左上に表示される[緑にリセット]をクリックします。リセットできないアラームが発生した場合は、クリアされるように原因の特定、および復旧作業を行ってください。

限 ホスト 仮想マシン データストア ネットワーク アップデート				
確認 緑にリセット				
問題	タイプ	起動時間	ステータス	
nec-esx-cn1.vsphere.local: ホストの接続と電源状態	トリガ済みアラーム	2019年08月01日 13:30:42	アラート	
nec-esx-cn2.vsphere.local: ホストの接続と電源状態	トリガ済みアラーム	2019年08月01日 13:29:10	アラート	
nec-esx-cn3.vsphere.local: ホストの接続と電源状態	トリガ済みアラーム	2019年08月01日 13:29:10	アラート	
vSAN 健全性アラーム「vSANビルドに関する推奨事項エン...	トリガ済みアラーム	2019年08月01日 13:30:45	警告	
vSAN 健全性アラーム「vSANリリース カタログの更新状態」	トリガ済みアラーム	2019年08月01日 13:30:45	警告	
vSphere HA が、データセンター Datacenter 内のクラスタ v...	設定問題	2019年08月05日 10:18:05		
vSphere HA ホストの監視が無効です。仮想マシンのフェ...	設定問題	2019年08月05日 10:18:05		

3. オブジェクトナビゲータで管理ノード名をクリックして手順 1、手順 2 と同様の操作を行ってください。

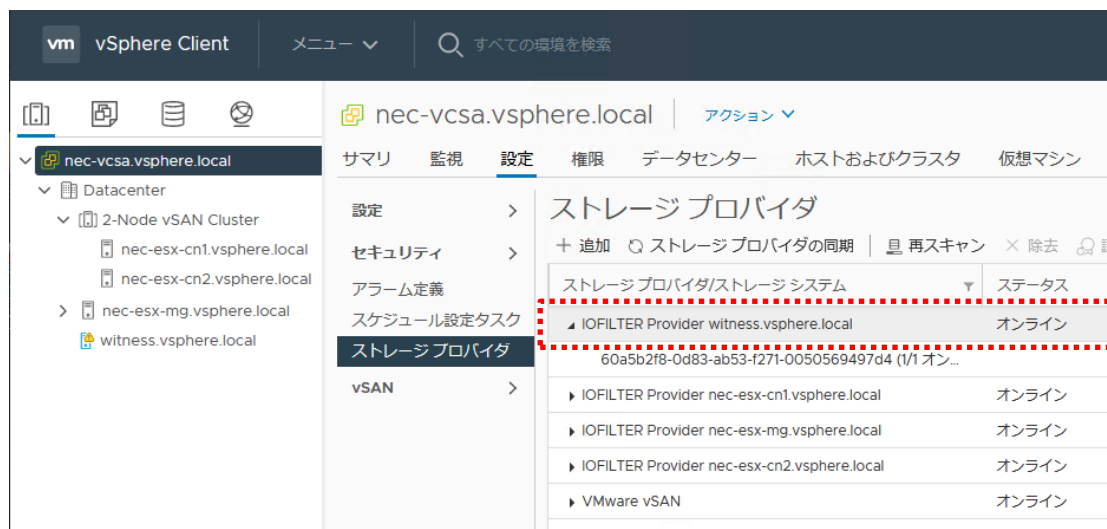


《補足》

2Node構成の場合、witness hostに「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」という警告が残っている場合は、以下の手順を実施してください。



- オブジェクトナビゲータでvCSA名を選択した状態で、画面中央上部の[設定]または[構成]をクリックします。続いて、タブ画面内左のメニューで[ストレージプロバイダ]をクリックします。
ストレージプロバイダの画面で、witnessが表示されていることを確認します。



- 手順2でwitnessが表示されている場合は、正常ですのでアラートをクリアします。
witness hostの[サマリ]画面を開き、アラートの右側の[緑にリセット]をクリックします。



以上でwitness hostの警告の対処は完了となります。

4. リストアを行う前の管理ノードにおいて、お客様が作成した仮想マシンが存在し、当該仮想マシンを再度インベントリに登録する場合は、以下「《参考》」の操作を行ってください。

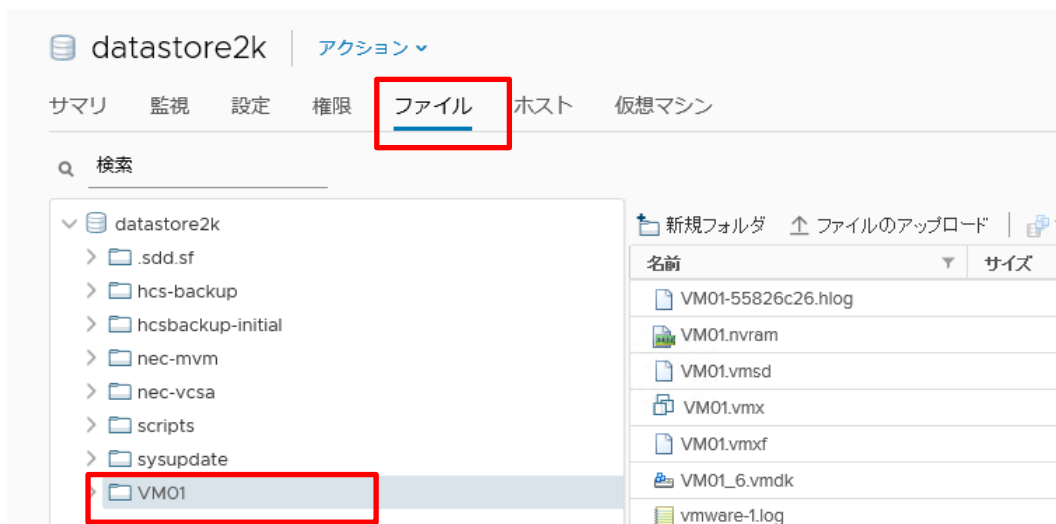
《参考》

出荷時へのリストアを行う前の管理ノード上に、お客様が作成した仮想マシン（以下画面の場合、VM01）が存在する場合、以下の操作でリストア後の管理ノードへの再登録が可能です。

1. vSphere Clientで[Ctrl + Alt + 2]キーを押下して「ホストおよびクラスタ」の画面を表示した後、オブジェクトナビゲータで管理ノード名をクリックし、画面中央上部の[データストア]タブをクリックし、1.2.2項の手順2でメモに記録した.vmxファイルが保存されているデータストア名をクリックします。



2. データストアの画面が表示されます。画面上部の[ファイル]タブをクリックした後、画面左の一覧から再登録する仮想マシン名をクリックします。



3. 画面右の一覧から1.2.2項の手順2でメモに記録したパスに保存されている.vmxファイルをクリックした後、[仮想マシンの登録]をクリックします。

新規フォルダ	↑ ファイルのアップロード	仮想マシンの登録...	ダウンロード	コピー先	→ 移動先	新しい名前
名前	サイズ	変更時刻	タイプ			
VM01-55826c26.hlog	0.37 KB	2019年08月23日 13:46:14	ファイル			
VM01.nvram	8.48 KB	2019年08月23日 14:00:42	不揮発			
VM01.vmsd	0 KB	2019年08月23日 13:46:08	ファイル			
VM01.vmx	3.26 KB	2019年08月23日 14:00:42	仮想マ			
VM01.vmxr	0.05 KB	2019年08月23日 13:46:31	ファイル			
VM01_6.vmdk	10,011,648 KB	2019年08月23日 13:56:38	仮想デ			
vmware-1.log	440.38 KB	2019年08月23日 13:53:31	仮想マ			
vmware.log	326.81 KB	2019年08月23日 14:00:42	仮想マ			

4. 「仮想マシンの登録」ダイアログが表示されますので、「名前とフォルダの選択」画面にて、ダイアログ内右下の[NEXT]をクリックします。

仮想マシンの登録

1 名前とフォルダの選択

2 コンピューティングリソース...

3 設定の確認

名前とフォルダの選択

一意の名前とターゲットの場所を指定します

仮想マシン名: VM01

この仮想マシンの場所を選択してください。

Datacenter

CANCEL

BACK

NEXT

5. 「コンピューティングリソースの選択」画面が表示されますので、画面中央のツリービューで管理ノードをクリックした後、ダイアログ内右下の[NEXT]をクリックします。

仮想マシンの登録

✓ 1 名前とフォルダの選択

2 コンピューティングリソース...

3 設定の確認

コンピューティングリソースの選択

この操作のターゲットコンピューティングリソースを選択します

Datacenter

vsan

nec-esx-mg.vsphere.local

6. 「設定の確認」画面が表示されますので、設定内容を確認し、問題なければダイアログ内右下の[FINISH]をクリックします。

仮想マシンの登録

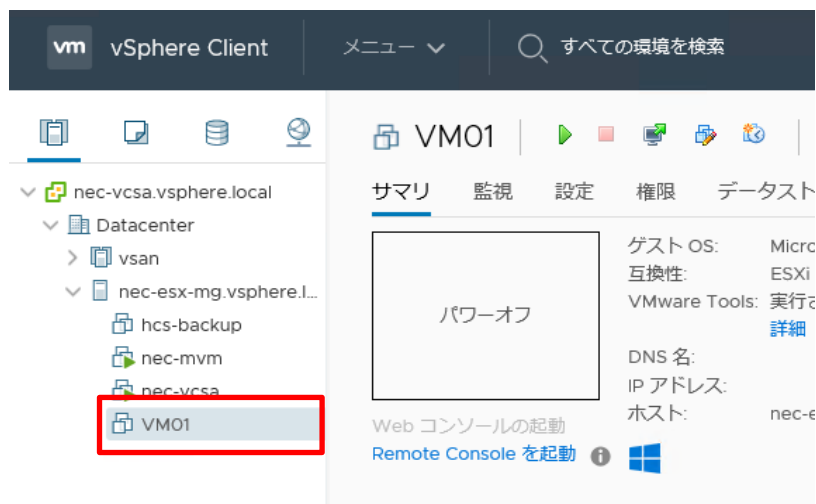
- ✓ 1 名前とフォルダの選択
- ✓ 2 コンピューティングリソース...
- 3 設定の確認**

設定の確認

選択内容を確認し、[終了] をクリックして登録を完了します。

仮想マシン名	VM01
フォルダ	Datacenter
ホスト	nec-esx-mg.vsphere.local

7. vSphere Clientにフォーカスが戻ります。[Ctrl + Alt + 2]キーを押下して「ホストおよびクラスタ」の画面を表示した後、オブジェクトナビゲータで管理ノードに、登録操作を行った仮想マシンが追加されていることを確認します。



以上で仮想マシンの再登録は完了となります。

1.2.4.4. NEC HCS Console の確認

HCS Console にログインし、ノードが正常と表示されている場合は、本項の実施は不要です。

リストア後、vSphere Client 上でホストがメンテナンス解除状態、エラーや警告が表示されていなくても HCS Console 上で表示が残っている場合があります。

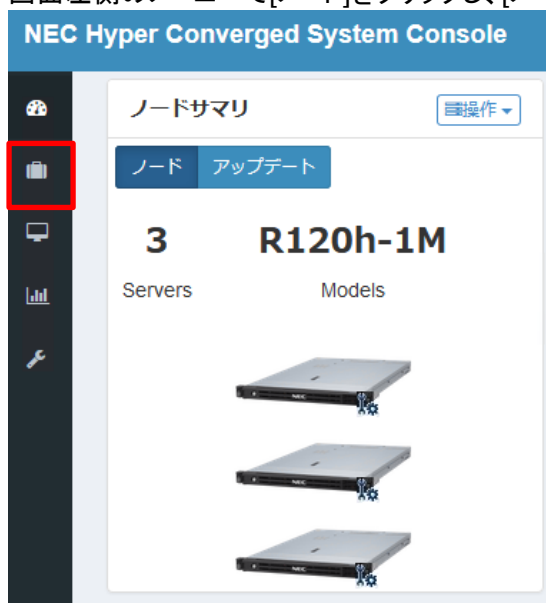
ノードの状況に応じて、下記の操作を実施してください。

接続不可と表示されている場合は、手順 1 から手順 4 の操作を実施してください。

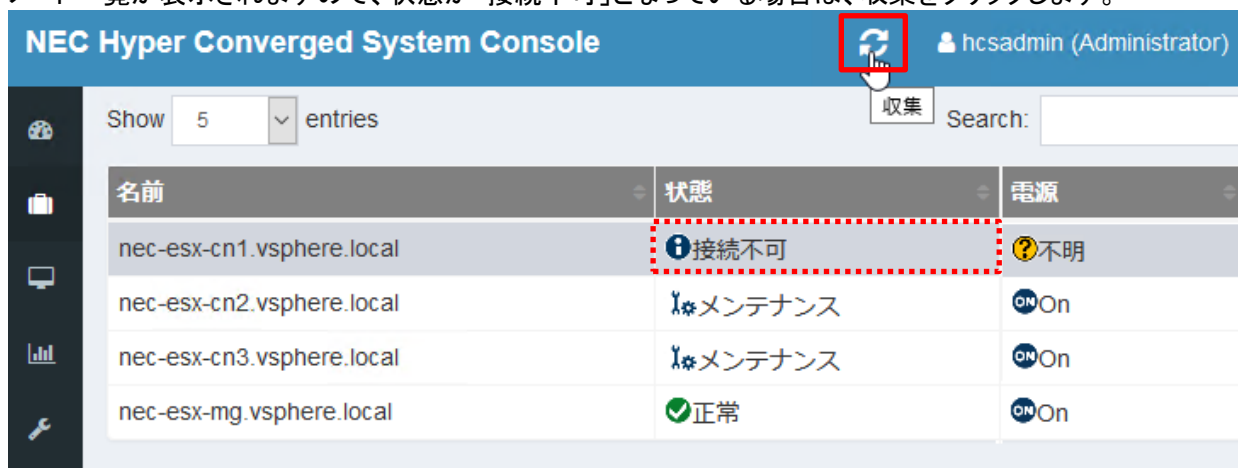
メンテナンス状態の場合は手順 5 から手順 8 の操作を実施してください。

警告が表示されている場合は手順 9 から手順 12 の操作を実施してください。

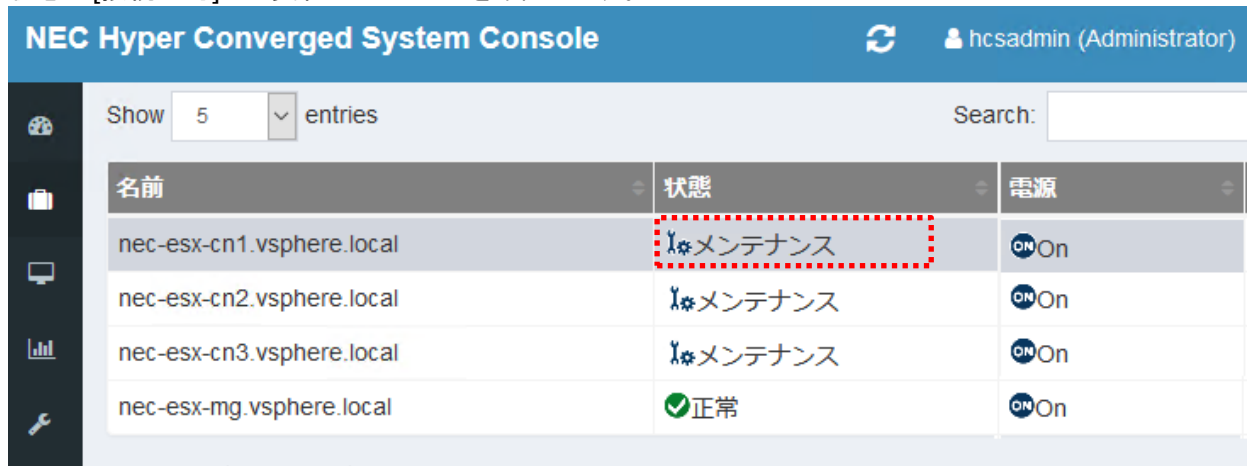
1. 管理 VM に管理者権限を有するユーザでサインインし、HCS Console にログインします。
2. 画面左側のメニューで[ノード]をクリックし、[ノード]画面に切り替えます。



3. ノード一覧が表示されますので、状態が「接続不可」となっている場合は、収集をクリックします。



4. 状態が[接続不可]から変わっていることを確認します。



名前	状態	電源
nec-esx-cn1.vsphere.local	メンテナンス	ON On
nec-esx-cn2.vsphere.local	メンテナンス	ON On
nec-esx-cn3.vsphere.local	メンテナンス	ON On
nec-esx-mg.vsphere.local	正常	ON On

5. [ノード]画面で状態が「メンテナンス」になっているノードをクリックします。
6. ノードサマリの操作メニューから[メンテナンスモードの終了]をクリックします。



ノードサマリ

操作

起動
再起動
シャットダウン
メンテナンスモードに切り替え
メンテナンスモードの終了
LED点灯
LED消灯
ストレージの再スキャン
状態リセット

状態	メンテナンス	電源
モデル名/型番	r120h-2m / N8100-2563H 1Y	ESXiアカウント
名前	nec-esx-cn1.vsphere.local	BMCアカウント

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

NEC Hyper Converged System Console

Show 5 entries

名前	状態
nec-esx-cn1.vsphere.local	メンテナンス
nec-esx-cn2.vsphere.local	メンテナンス
nec-esx-cn3.vsphere.local	メンテナンス
nec-esx-mg.vsphere.local	正常

Showing 1 to 4 of 4 entries

ノードサマリ

ノード ディスクグループ ソフトウェア

状態 正常

電源 On

モデル名/型番 r120h-2m / N8100-2563H1Y ESXiアカウント 設定済み 編集 削除

名前 nec-esx-cn1.vsphere.local BMCアカウント 設定済み 再接続 編集 削除

192.168.0.2 (接続可能)

CPU

メモリ

8. メンテナンス状態になっているすべてのノードで手順 5 から手順 7 の操作を実施してください。警告が出ている場合は引き続き手順 9 を実施してください。
9. 続いて警告が表示されているノードの対処をします。
 [ノード]画面から警告が表示されているノードをクリックします。

[注意]

サーバ診断カルテを設定している環境の場合、「IPMIコマンド状態」「BMC死活監視状態」の警告が表示される場合があります。ノードサマリの状態が「警告」になっている場合、右側の数字をクリックすることで警告の一覧を確認することができます。このとき、BMCアカウントのIPアドレスの右側の状態が「(認証失敗)」と表示されている場合もありますので、以下の対処を実施してください。

NEC Hyper Converged System Console

Show 5 entries

名前	状態
nec-esx-cn1.vsan.local	警告
nec-esx-cn2.vsan.local	警告
nec-esx-mg.vsan.local	警告
witness.vsan.local	正常

Showing 1 to 4 of 4 entries

ノードサマリ

ノード ディスクグループ ソフトウェア

状態 警告

電源 On

モデル名/型番 r120h-2m / N8100-2562Y ESXiアカウント 設定済み 編集 削除

名前 nec-esx-mg.vsan.local BMCアカウント 設定済み 再接続 編集 削除

192.168.0.1 (認証失敗)

通知一覧

メッセージ	状態	日時
IPMIコマンド状態	異常	2022/10/26 15:31:12
BMC 死活監視状態	異常	2022/10/26 15:31:13

メモリ

ネットワーク使用状況

イベント

マシンのメンテナンスステータスを変更

2022/10/26 16:20:18

終了時刻

2022/10/26 16:20:19

上記の警告および認証失敗が表示されているノードが管理ノードの場合は、ノードサマリのBMCアカウ

ント右側の[再接続]をクリックし、IPアドレス右側の状態が「(接続可能)」に変わることを確認します。



その後、右上の[操作]から[状態リセット]をクリックし、警告が解消され「正常」に変わることを確認してください。



クラスタノードで同様の警告および認証失敗が表示されている場合、引き続きリストアを実施する場合はこの時点で対処はせず、以降の作業を実施してください。

クラスタノードのリストアを実施しない場合、1.2.4.2項の手順5の[注意]で、NEC HCS ConsoleおよびESMPRO/ServerManagerに監視対象として登録したiLOやESXiのコンポーネントのパスワード更新を実施していることを確認したうえで、管理ノード同様の手順対処を実施してください。

10. ノードサマリの操作メニューから[状態リセット]をクリックします。

※ サーバ診断カルテを設定している環境のクラスタノードに手順 9 の[注意]の警告が表示された場合で、引き続きクラスタノードのリストアを実施する場合は、本手順は実施しないでください。



11. ノードサマリの状態が“正常”になっていることを確認してください。

※ 画面上部のノード一覧の“状態”表示は、一度[node]タブ以外に切り替えると表示が更新されます。

NEC Hyper Converged System Console

Show 5 entries

名前	状態	電源
nec-esx-cn1.vsphere.local	警告	ON On
nec-esx-cn2.vsphere.local	正常	ON On
nec-esx-cn3.vsphere.local	正常	ON On
nec-esx-mg.vsphere.local	正常	ON On

Showing 1 to 4 of 4 entries

ノードサマリ

ノード ディスクグループ ソフトウェア



状態	電源
正常	ON On

モデル名/型番 r120h-1m / N8100-2834H1Y ESXiアカウント 設定済み 編集 削除

名前 nec-esx-cn1.vsphere.local BMCアカウント 設定済み 再接続 編集 削除

192.168.0.2 (接続可能)

12. 警告が出ているすべてのノードで手順 9 から手順 11 の操作を実施してください。

以上で管理ノードのリストア後の HCS 環境の復旧操作は完了となります。

1.2.4.5. 開局作業

エクスプレス通報サービスを契約していない場合は、本項の実施は不要です。

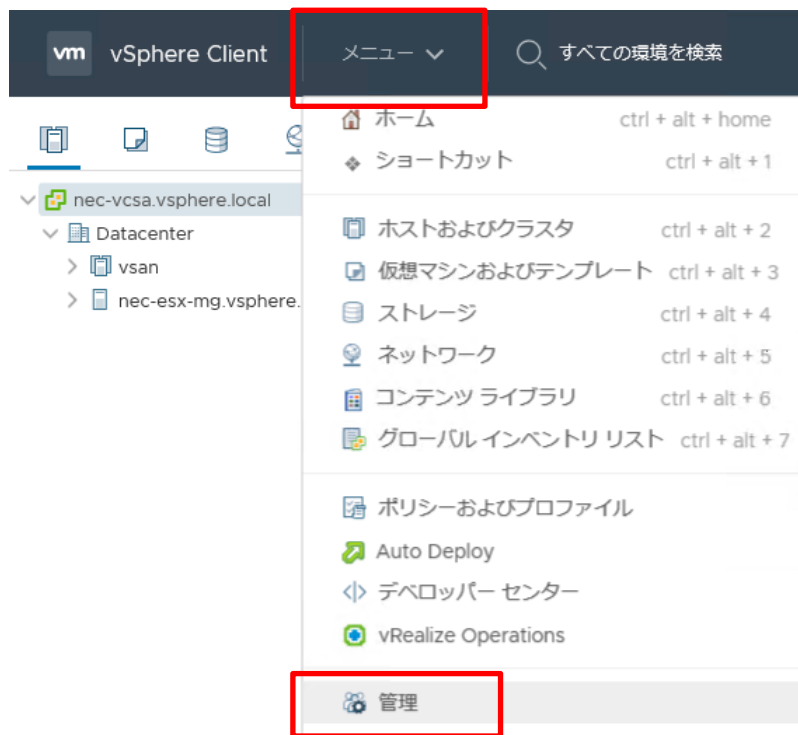
エクスプレス通報サービスを契約している場合、リストア後は出荷時の開局が行われていない状態になります。そのため、リストア後には再度開局を実施してください。

1.2.5. 《参考》 リストア後のライセンスの再登録

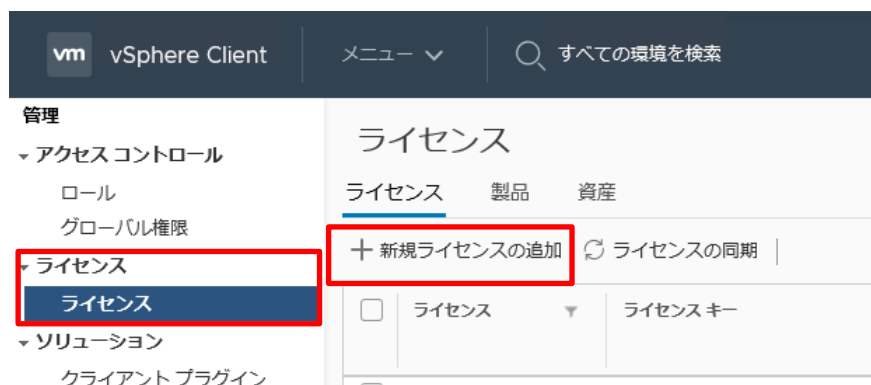
本項は、参考として、リストア操作を行った後の、vSphere Client によるライセンスの再登録および割り当て操作について記載しています。

2Node 構成の場合は、「NEC Hyper Converged System for VMware vSAN/CR2.0 スタートアップガイド」を参照してください。

1. 管理 VM に管理者権限を有するユーザでサインインし、vSphere Client で vCenter Server にログインし、ホーム画面を表示している状態で画面上部の[メニュー](vSphere 7.0u3 の場合、画面左上のメニューアイコン) – [管理]の順にクリックします。



2. 更新されたオブジェクトナビゲータで[▼ ライセンス]の下に[ライセンス]をクリックします。表示される画面中央上部の[ライセンス]タブをクリックした後、ライセンス一覧の左上に表示される「新規ライセンスの追加」をクリックします。



- [illegible]

- ## 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 キー:

製品: VMware vCenter Server 7 Standard

ライセンス名:

ライセンス キー:

製品: VMware vSphere 7 Enterprise Plus

ライセンス名:

ライセンス キー:

製品: VMware vSAN Enterprise

- ### 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: 3

ライセンス名:	vCenter Server
ライセンスキー:	[Redacted]
ライセンス名:	ESXi
ライセンスキー:	[Redacted]
ライセンス名:	vSAN
ライセンスキー:	[Redacted]

6. vSphere Client にフォーカスが戻ります。ライセンス一覧に、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た後、[資産]タブをクリックし、さらにタブの下の[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。



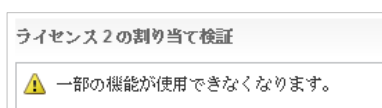
7. 「ライセンスの割り当て」ダイアログが表示されます。ダイアログ内の一覧で vCenter Server に割り当てるライセンスキーの行頭にチェックを付け、ダイアログ内右下の[OK]をクリックします。

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
☐ 評価ライセンス	--	--	--	--
☒ vCenter Server	--	VMware vCenter Server 7 Stand...	• 1 インスタ...	2 インスタンス

- ※ 評価ライセンスを適用している vCenter Server に正規ライセンスを割り当てる際、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。



8. 再び vSphere Client にフォーカスが戻ります。[資産]タブ画面内の一覧において、vCenter Server の「製品」列の値が「VMware vCenter Server 7 Standard」等のライセンス名になっていることを確認します。



9. 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、資産の一覧で、1 ライセンスに対して割り当てが可能な ESXi サーバ名を全て選択した状態で、[ライセンスの割り当て]をクリックします。



※「ライセンスの割り当て」ダイアログが表示されますので、[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

※ 手順 5 までの操作を行った後、手順 2 の操作で表示される画面内の一覧で「キャパシティ」列の値を確認し、手順 9 において ESXi の「使用状況」欄の合計がライセンスの「キャパシティ」列の値以下となるように ESXi を選択してください。

例：以下画面（「キャパシティ」列の値が 32CPU）のケースでは、上記画面で「使用状況」列の値の合計が 32CPU 以下となるように ESXi サーバを選択します。

☐	ライセンス	ライセンス キー	製品	使用状況	キャパシティ
☐	評価ライセンス	--	--	--	--
☐	ESXi	-----	VMware vSphere 7 Enterprise Plus	0 CPUs (up to 32 cores)	32 CPUs (up to 32 cores)
☐	vCenter Server	-----	VMware vCenter Server 7 Standard	1 インスタンス	2 インスタンス
☐	vSAN	-----	VMware vSAN Enterprise	0 CPUs (up to 32 cores)	32 CPUs (up to 32 cores)

10. 「ライセンスの割り当て」ダイアログが表示されます。手順 7 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後、ダイアログ内右下の[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
☐ 評価ライセンス	--	--	--
☒ ESXi		VMware vSphere 7 Enterprise Plus	5 CPUs (up to 32 cores)

11. vSphere Client にフォーカスが戻ります。[資産]タブ画面内の一覧で、ライセンス登録を行った ESXi サーバの「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。

資産	使用状況	製品	ライセンス
☒ nec-esx-cn1.vsphere.local	1 CPUs (up to 32 cores)	VMware vSphere 7 Enterprise Plus	ESXi
☒ nec-esx-mg.vsphere.local	2 CPUs (up to 32 cores)	VMware vSphere 7 Enterprise Plus	ESXi
☒ nec-esx-cn2.vsphere.local	1 CPUs (up to 32 cores)	VMware vSphere 7 Enterprise Plus	ESXi
☒ nec-esx-cn3.vsphere.local	1 CPUs (up to 32 cores)	VMware vSphere 7 Enterprise Plus	ESXi

4 エクスポート

12. 最後に、vSAN クラスタにライセンスを割り当てます。[資産]タブの下に[クラスタ]をクリックし、資産の一覧で、vSAN クラスタ名を選択した状態で、[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

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
☒ vSAN cluster	3 CPU	評価モード	評価ライセンス

- 13.「ライセンスの割り当て」ダイアログが表示されます。手順 7 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後、ダイアログ内右下の[OK]をクリックします。

ライセンスの割り当て



14. vSphere Client にフォーカスが戻ります。[資産]タブ画面内の一覧で、ライセンス登録を行った vSAN クラスターの「製品」列の値がライセンス名になっていることを確認します。



以上でリストア後のライセンスキーの再登録、および vCenter Server、ESXi、vSAN クラスタへのライセンス割り当ては完了となります。

2. クラスタノードのバックアップ／リストア

本章では、クラスタノードのバックアップおよびリストア手順について記載しています。

2.1. クラスタノードのバックアップ

クラスタノードのバックアップは、出荷時点で実施済みですので、作業は不要です。

2.2. クラスタノードのリストア

クラスタノードのリストアは以下の順序で行います。各項目の詳細は、2.2.1 項から 2.2.4 項を参照ください。



本作業による影響

クラスタノードのリストアにおいては、作業中に該当ノードの再起動を行います。そのため、該当ノード上に仮想マシンが存在する場合、本作業を実施する間、該当する全ての仮想マシンを他のクラスタノードに移行する必要がありますのでご注意ください。

作業時間の目安

およそ 1 時間

※ リストアの準備から iLO の設定リストアまでを含みます。HCS 環境の再稼働操作は含みません。
なお、作業時間は、仮想マシンの移行に要する時間、および、vSAN のコンポーネント再同期に要する時間等により、目安よりも長くなる場合があります。

作業実施に必要な環境・機材

クラスタノードのリストア作業の際は、以下の Windows PC が必要となります。

- 管理用 NW に接続している。
- 管理 VM にリモートデスクトップ接続できる。
- クラスタノードに SSH で接続できる。
※ 通常、SSH による接続が可能なターミナルソフトを使用します。

オペレータは、この Windows PC から管理 VM、クラスタノードにアクセスして作業を行います。

また、下記のドキュメントもご用意ください。

- NEC Hyper Converged System 初期パスワード通知書

2.2.1. リストアの準備

本項は、クラスタノードのリストアを行う前に必要な操作について記載しています。

【重要】

リストア操作を行うには、クラスタノードは、出荷時と同じハードウェア構成である必要があります。また、出荷時点でインストールされていたパッチとストレージコントローラのデバイスドライバ・ファームウェアが全て適用済みであり、同じビルド番号である必要があります。

【重要】

全てのクラスタノードにおいてリストア作業を行う場合、1台目のクラスタノードに対して2.2.1項から2.2.3項までの操作を行った後、2台目を含むその他全てのクラスタノードに対して、**必ず1台ずつ**、2.2.1項の手順2から2.2.3項までの操作を順に行ってください。

1. 管理 VM に管理者権限を有するユーザでサインインし、vSphere Client で vCSA にログインします。

2. vSphere Client でホーム画面を表示している状態でオブジェクトナビゲータの[ホストおよびクラスタ] (vSphere 7.0u3 の場合、画面左上のメニューアイコンをクリックし、[インベントリ])をクリックした後、オブジェクトナビゲータにある任意の仮想マシン名をクリックし、[ホスト]を確認します。

リストアを行うクラスタノード上に仮想マシンが存在する場合、リストア実行時に該当する全ての仮想マシンが消去される為、手順 3 から手順 9 までの操作を行い、該当する全ての仮想マシンを別のクラスタノードに移行します。



3. オブジェクトナビゲータで仮想マシン名をクリックした後、[アクション] – [移行]の順にクリックします。



4. 「移行」ダイアログが表示されますので、[コンピューティングリソースのみ変更します]を選択してダイアログ内右下の[NEXT]をクリックします。

VM02 - 移行

1 移行タイプの選択

2 コンピューティングリソース...

3 ネットワークの選択

4 vMotion の優先順位の選択

5 設定の確認

移行タイプの選択

仮想マシンのコンピューティング リソース、ストレージ、またはその両方を変更します。

☒ コンピューティング リソースのみ変更します

仮想マシンを別のホストまたはクラスタに移行します。

☐ ストレージのみ変更します

仮想マシンのストレージを互換性のあるデータストアまたはデータストア クラスタに移行します。

☐ コンピューティング リソースとストレージの両方を変更します

仮想マシンを特定のホストまたはクラスタに移行し、そのストレージを特定のデータストアまたはクラスタに移行します。

5. 一覧から移行先となるクラスタノード名を選択し、ダイアログ内右下の[NEXT]をクリックします。

※本書では[nec-esx-cn2.vsphere.local]を選択。

VM02 - 移行

✓ 1 移行タイプの選択

2 コンピューティングリソース...

3 ネットワークの選択

4 vMotion の優先順位の選択

5 設定の確認

コンピューティングリソースの選択

クラスタ、ホスト、vApp またはリソース プールを選択して、この仮想マシンを実行します。

ホスト クラスタ リソースプール vApps

名前 ↑	状態	ステータス	クラ
nec-esx-cn1.vsphere.local	接続済み	✓ 正常	
nec-esx-cn2.vsphere.local	接続済み	✓ 正常	
nec-esx-cn3.vsphere.local	接続済み	✓ 正常	

6. ダイアログ内右下の[NEXT]をクリックします。

VM02 - 移行

✓ 1 移行タイプの選択

✓ 2 コンピューティングリソース...

3 ネットワークの選択

4 vMotion の優先順位の選択

5 設定の確認

ネットワークの選択

仮想マシンの移行先ネットワークを選択します。

仮想マシンの起点 ①

同じソース ネットワークに接続されたすべての仮想マシン ネットワーク アダプタの新しいターゲット ネットワークを選択することで、仮想マシン ネットワークを移行します。

ソース ネットワーク	使用者	ターゲット ネットワーク
Service	1 仮想マシン/1 ネットワークアダプタ	Service

詳細 >>

互換性

✓ 互換性チェックは成功しました。

CANCEL

BACK

NEXT

7. [vMotion を高優先度でスケジューリング]を選択し、ダイアログ内右下の[NEXT]をクリックします。

VM02 - 移行

✓ 1 移行タイプの選択

✓ 2 コンピューティング リソースの選択

✓ 3 ネットワークの選択

4 vMotion の優先順位の選択

5 設定の確認

vMotion の優先順位の選択

CPU リソースの割り当てに優先順位をつけることで、稼働中の仮想マシンのパフォーマンスの低下を防ぎます。

☒ **vMotion を高優先度でスケジューリング (推奨)**
vMotion に、通常の優先順位の移行に比べて高い CPU スケジュール設定を与えます。vMotion に、通常の優先順位の移行に比べて高い CPU スケジュール設定を与えます。vMotion に、通常の優先順位の移行に比べて高い CPU スケジュール設定を与えます。

☐ 標準 vMotion のスケジュール
vMotion に、高優先順位の移行に比べて低い CPU スケジュール設定を与えます。vMotion に、高優先順位の移行に比べて低い CPU スケジュール設定を与えます。vMotion に、高優先順位の移行に比べて低い CPU スケジュール設定を与えます。

8. 入力した内容が正しく設定されていることを確認し、ダイアログ内右下の[FINISH]をクリックします。

設定の確認

情報が正しいことを確認し、[完了]をクリックして移行を開始します。

移行タイプ	コンピューティング リソースを変更します。仮想マシンは元のストレージに配置したままにします
仮想マシン	VM02
クラスタ	vsan
ホスト	nec-esx-cn2.vsphere.local
vMotion の優先順位	高
ネットワーク	ネットワークの再割り当ては行われていません

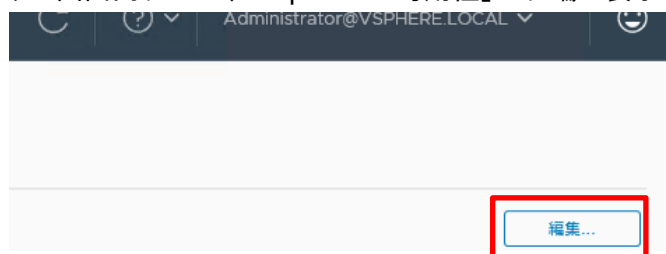
9. オブジェクトナビゲータで仮想マシン名をクリックした後、[サマリ]タブを選択し「ホスト」に表示されているクラスタノード名が手順 5 で選択したクラスタノード名と同じことを確認します。

The screenshot shows the vSphere Client interface. On the left, the object navigator shows the hierarchy: nec-vcsa.vsphere.local > Datacenter > vsan > VM02. The VM02 object is selected and highlighted with a red box. On the right, the 'Summary' tab is active, showing details for VM02. The 'Host' field is highlighted with a red box, displaying 'nec-esx-cn2.vsphere.local'. Other details visible include Guest OS: Microsoft Windows Server 2019 (64-bit), ESXi version: 7.0, and IP address: 192.168.30.2.

10. オブジェクトナビゲータで vSAN クラスタ名をクリックした後、[設定]または[構成]タブ – [vSphere の可用性]の順にクリックします。



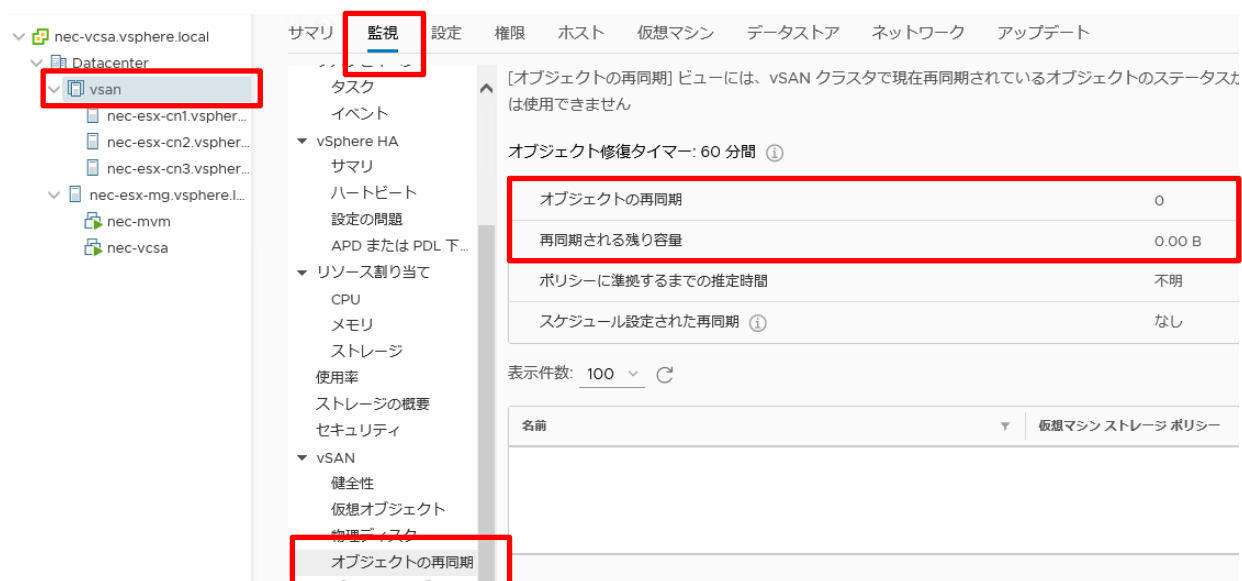
11. タブ画面内右上の、「vSphere の可用性」の右端に表示される[編集]をクリックします。



12. 「クラスタ設定の編集」ダイアログが表示されますので、ダイアログ内上のメニューで[障害および対応]をクリックした後、[ホスト監視の有効化]の状態を確認します。状態が有効の場合は無効にし、ダイアログ内右下の[OK]をクリックします。

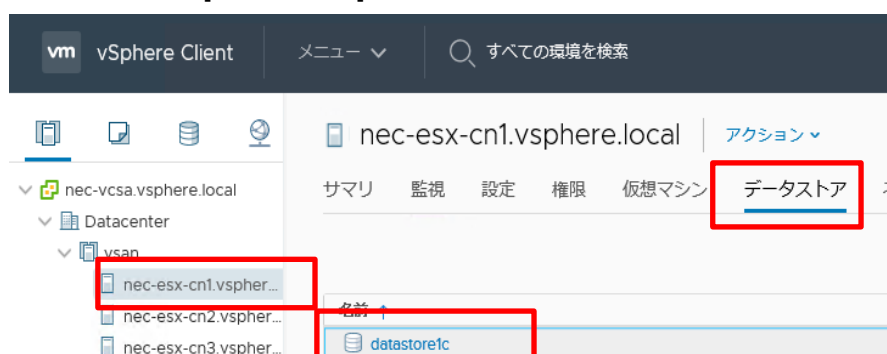


13. オブジェクトナビゲータで vSAN クラスタ名をクリックし、画面中央上部の[監視]タブをクリックした後、タブ画面内左のメニューで[オブジェクトの再同期]をクリックして、タブ画面内右に表示される「オブジェクトの再同期」および「再同期される残り容量」の値が共に 0 であり、再同期を実行していないことを確認します。

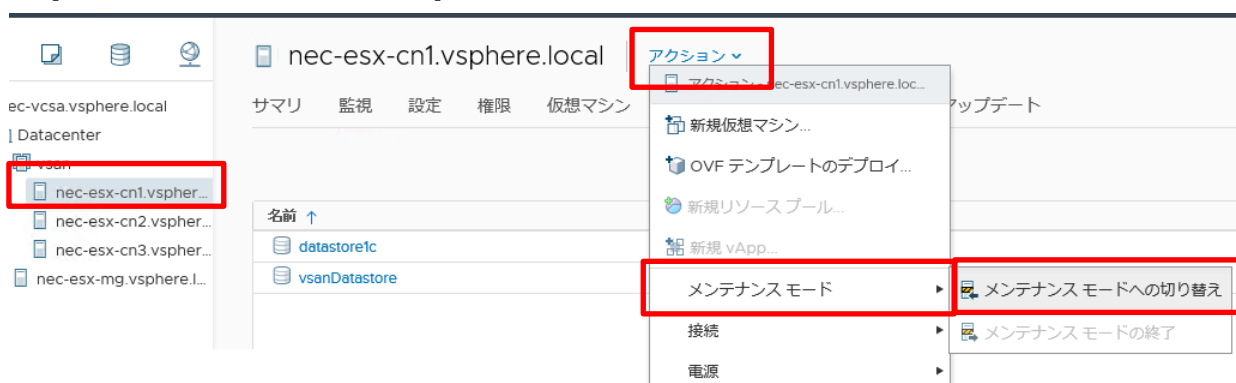


14. オブジェクトナビゲータでリストア対象のクラスタノード名をクリックし、更新された画面中央上部の[データストア]タブをクリックします。画面右の一覧に、vSAN データストア以外の、クラスタノードの内蔵ディスクによるデータストアが存在することを確認します。

※以下画面では[datastore1c]

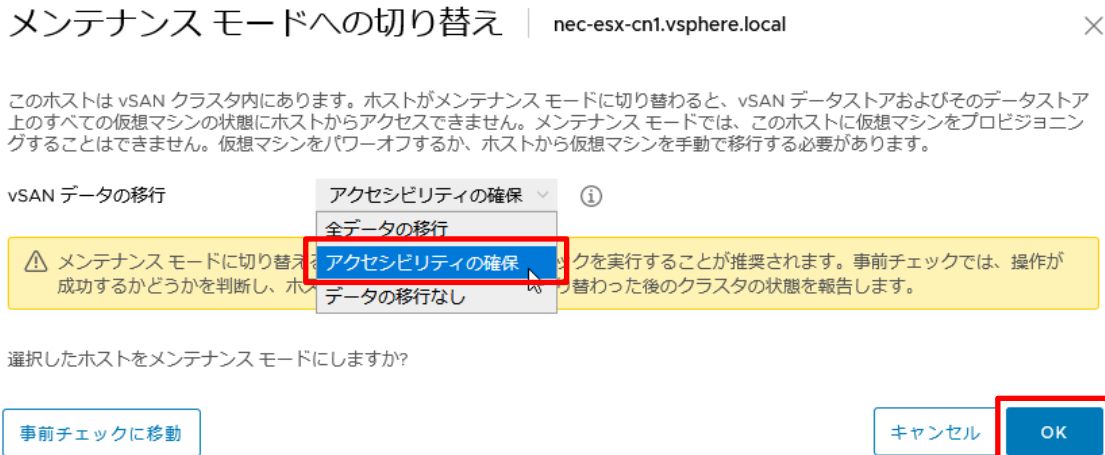


15. オブジェクトナビゲータで、リストア対象のクラスタノード名をクリックし、[アクション] - [メンテナンスモード] - [メンテナンスモードへの切り替え]を順にクリックします。



「メンテナンスモードへの切り替え」ダイアログが表示されますので、「vSAN データの移行」を[アクセシビリティの確保]に変更し、ダイアログ内右下の[OK]をクリックします。

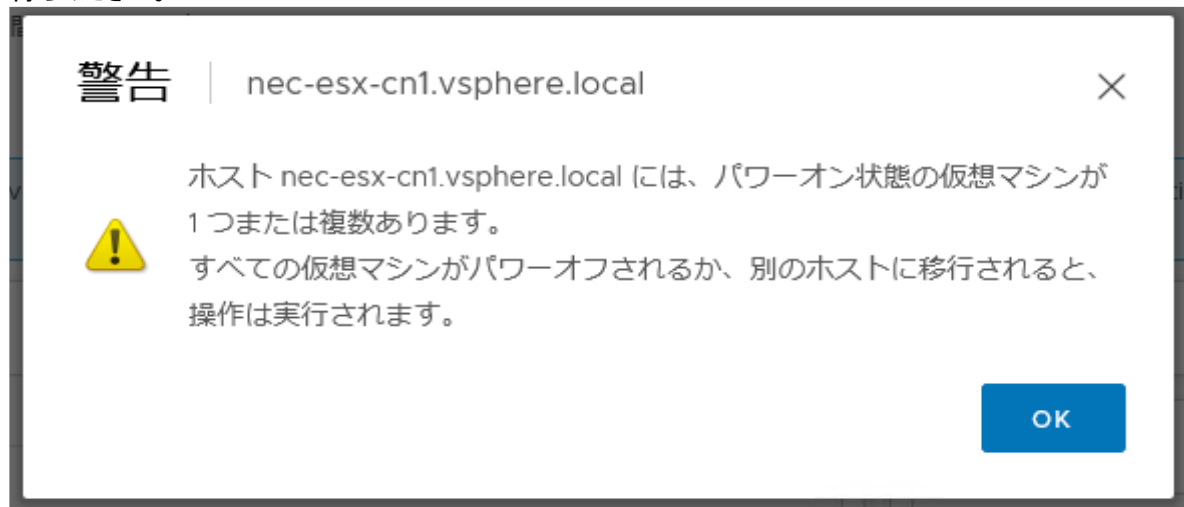
※ 必要に応じて[事前チェックに移動]をクリックして、データ移行オプションの影響を確認してください。



《参考》

vSphere7.0 Update1以降でメンテナンスモードに切り替えるノードにvCLSの仮想マシンが存在する場合、以下の警告が表示されることがあります。

vCLSは自動で他のノードに移行しますので、[OK]をクリックしてメンテナンスモードに切り替わるまでお待ちください。



16. ターミナルソフトを使用する場合、vCSA でリストア対象のクラスタノードの SSH 接続を有効化します。

以上で、リストアの準備は完了となります。引き続き、2.2.2 項の作業を行ってください。

2.2.2. ソフトウェア(ESXi の設定)のリストア

バックアップした ESXi の設定データをクラスタノードにリストアする場合、以下の手順で行います。

1. 管理 VM からリストア対象のクラスタノードの Host Client にログインします。

[注意]

サーバ診断カルテを設定している環境で1.2.4.2項 手順5の[注意]の警告が表示されている場合、ESXiのリモートアクセスがロックアウトされ、Host Clientにログインできなくなります。
以下の手順を実施して管理エージェントを再起動し、一時的にロックアウトを解除してください。

- ① コンソールまたはターミナルソフトで、警告が表示されているノードのESXi Shellに rootユーザでログインします。

- ② 以下のコマンドを実行します。

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

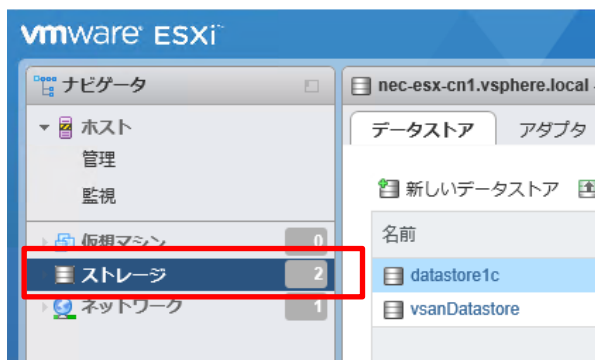
```
[root@nec-esx-ng:~] etc/init.d/hostd restart  
watchdog-hostd[1992931]: Terminating watchdog process with PID 1985179  
hostd stopped.  
hostd started.
```

- ③ 以下のコマンドを実行します。

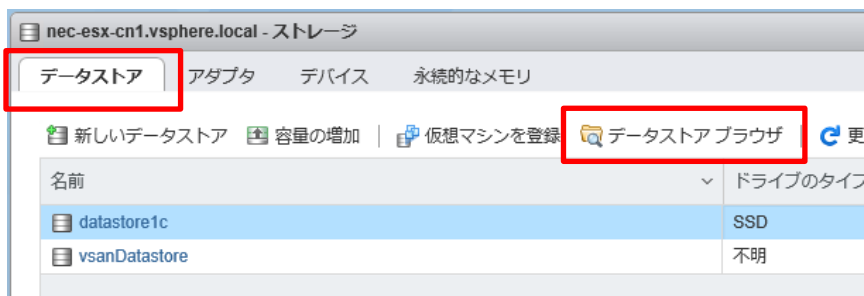
```
# /etc/init.d/vpxa restart
```

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

2. Host Client 画面左の、[ナビゲータ]枠内の[ストレージ]をクリックします。



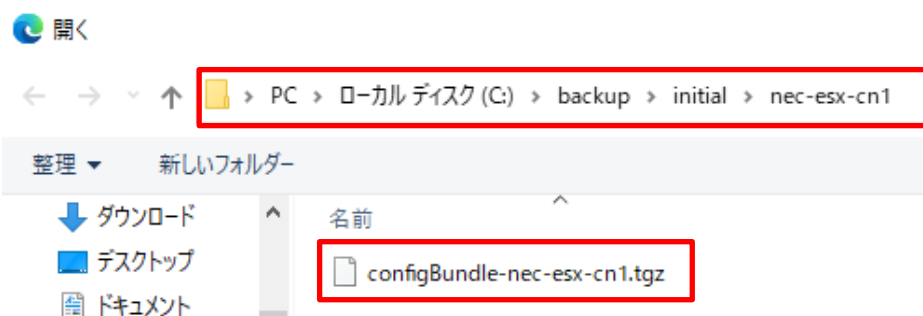
3. Host Client 画面右に表示される「ストレージ」画面において、[データストア]タブをクリックした後、タブ画面内の一覧の上に表示されている[データストアブラウザ]をクリックします。



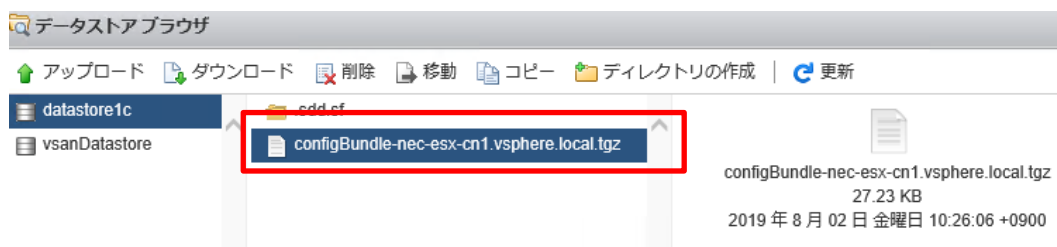
4. データストアブラウザのウィンドウが表示されます。ウィンドウ内左の一覧で、2.2.1 項の手順 14 で確認したデータストア名をクリックした後、ウィンドウ内左上の[アップロード]をクリックします。



5. 「開く」ダイアログが表示されますので、「C:\¥backup¥initial¥<リストア対象のクラスタノードのホスト名>」に移動し、「configBundle-<リストア対象のクラスタノードの FQDN>.tgz」フォルダをクリックし、ダイアログ内右下の[開く]をクリックします。



6. 設定データがアップロードされたことを確認した後、データストアブラウザのウィンドウ右下の[閉じる]をクリックします。



7. コンソールまたはターミナルソフトでクラスタノードの ESXi Shell に root ユーザでログインします。
8. 以下のコマンドを順に実行し、リストアを実行します。なお、/vmfs/volumes/ 以降の部分は、手順 4 で確認したデータストア名、およびバックアップした ESXi の設定ファイル名により構成されます。

```
# mv /vmfs/volumes/<手順 4 で確認したデータストア名>/configBundle-<リストア対象のクラスタノードの FQDN>.tgz /tmp/configBundle.tgz
# vim-cmd hostsvc/firmware/restore_config /tmp/configBundle.tgz
```

```
[root@nec-esx-cn1:~] mv /vmfs/volumes/datastore1c/configBundle-nec-esx-cn1.vsphere.local.tgz /tmp/configBundle.tgz
[root@nec-esx-cn1:~] vim-cmd hostsvc/firmware/restore_config /tmp/configBundle.tgz
[root@nec-esx-cn1:~]
```

コマンド実行直後にクラスタノードが再起動し、バックアップデータが反映されます。

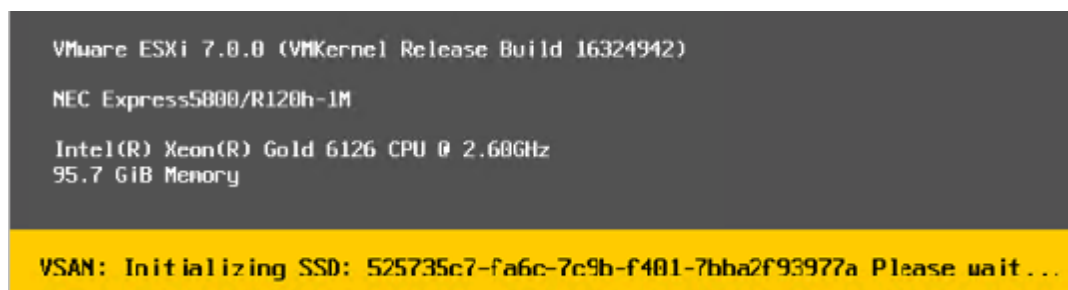
※本手順以降、クラスタノードの ESXi のパスワードが初期パスワードになります。

クラスタノードの ESXi の初期パスワードは「初期パスワード通知書」を参照ください。

【重要】

クラスタノードは、毎起動時に、ディスクグループ単位で、キャッシュデバイス上のメタデータテーブルの生成を目的としたデータ処理およびバッファ内のログエントリの整理を実行します。

※ 上記動作の間は、ESXiの画面に「Initializing SSD:～」と表示されます。



ESXiサーバの再起動時点における書き込み用バッファ内のデータ、もしくはブロックの量が多い場合、上記動作が完了して、ESXiが起動するまでに長時間を要する場合がありますのでご注意ください。

特に、上記画面の表示中にESXiサーバの電源OFF、および、リブートの実行は、vSAN環境の破壊につながる恐れがあるため行わないでください。「Initializing SSD:～」と表示されている時点の、ESXiの起動経過詳細は[Alt + F12]キーを押下して表示されるvmkernelのログ画面で確認ください。

```
vmkernel log (h for help)
2018-10-18T06:02:19.461Z cpu9:65897)PLOG: PLOGAnnounceSSD:7203: Trace task started for d
2018-10-18T06:02:19.461Z cpu9:65897)PLOG: PLOGAnnounceSSD:7215: Successfully added VSAN
2018-10-18T06:02:19.461Z cpu9:65897)VSAN: Initializing SSD: 525735c7-fa6c-7c9b-f401-7bba
2018-10-18T06:02:19.462Z cpu4:66808)PLOG: PLOGNotifyDisks:4495: MD 0 with UUID 526e06c8-
2018-10-18T06:02:19.462Z cpu4:66808)PLOG: PLOGNotifyDisks:4495: MD 1 with UUID 522fa60a-
2018-10-18T06:02:19.462Z cpu4:66808)VSANServer: VSANServer_InstantiateServer:2863: Insta
2018-10-18T06:02:19.478Z cpu6:66522)Created VSAN Slab RcSsdParentsSlab_0x430ced189a40 (o
2018-10-18T06:02:19.480Z cpu6:66522)Created VSAN Slab RcSsdParentsSlab_0x430ced189a40 (o
```

《参考》

異なるサーバ装置のESXiサーバのバックアップをリストアする場合、手順8の2行目のコマンドを以下のコマンドに変更することで、バックアップファイルをUUIDの異なる装置に、強制的にリストアすることが可能です。

```
# vim-cmd hostsvc/firmware/restore_config 1 /tmp/configBundle.tgz
```

ただし、上記コマンドを実行した際に、バックアップ元とリストア先の装置でハードウェアスペックが異なる場合は、同じビルド番号のESXiをインストールした状態においても、正常にリストアされない場合がありますのでご注意ください。

9. 起動後、ESXi Shell の無効化、または、vCSA で SSH 接続を無効化してください。
10. HCS 環境の導入後におこなった追加設定(業務ネットワークの追加など)を必要に応じて実施してください。

以上でクラスタノードにおける ESXi の設定リストアは完了となります。引き続き、2.2.3 項の作業を行ってください。

2.2.3. iLO の設定リストア

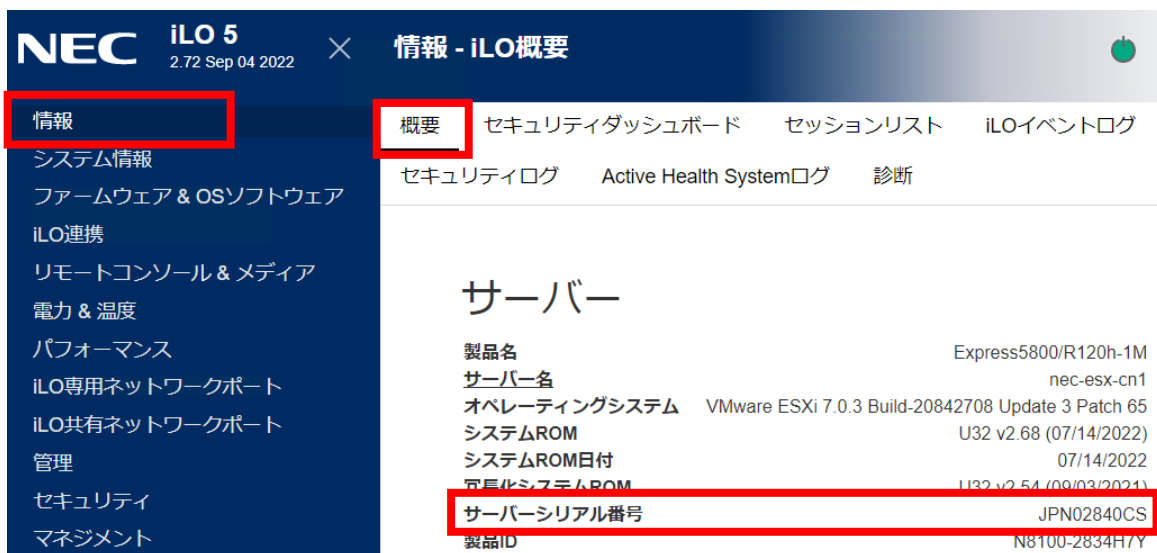
クラスタノードとなるサーバ装置における iLO の設定リストアは、以下の手順で行います。

[注意]

iLO の設定バックアップを行った後、リストア対象のノードのマザーボードが故障し交換を行った場合、もしくは Starter PackI により iLO ファームウェアのアップデートを行った場合（一部のバージョンを除く）、アップデート前のバックアップデータはリストアできない状態となりますのでご注意ください。

詳細は、Starter Pack のダウンロードページ内に掲載されている [iLO ファームウェアアップデート補足] を参照ください。

1. 管理 VM に管理者権限を有するユーザでサインインし、リストア対象のクラスタノードの iLO にログインします。
2. iLO の Web インターフェイス画面が表示されますので、画面左のメニューで [情報] - [概要] の順にクリックし、「サーバーシリアル番号」を確認します。



3. 画面左のメニューで [ライフサイクル管理] - [バックアップとリストア] の順にクリックします。
- ※ iLO FW バージョンによって画面左のメニューが異なる場合があります。[ライフサイクル管理] がない場合は、[管理] - [バックアップとリストア] の順にクリックしてください。



4. 「バックアップとリストア」の画面が表示されますので、[リストア]枠内のアイコン部分をクリックします。

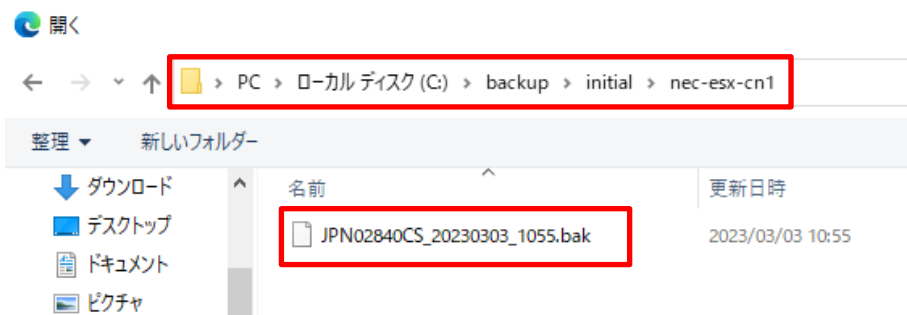
廃棄 バックアップとリストア



5. 画面右に「リストア」の設定項目が表示されますので、[参照]をクリックします。



6. 「開く」ダイアログが表示されます。「C:¥backup¥initial¥<リストア対象のクラスタノードのホスト名>」フォルダに移動し、ファイル名に手順 2 で確認したシリアル番号で始まる.bak ファイルを選択した後、ダイアログ右下の[開く]をクリックします。



7. 「リストア」の画面にフォーカスが戻ります。[バックアップファイル]欄に手順 6 で選択したファイル名が表示されていることを確認した後、[アップロードおよびリストア]をクリックします。
- ※ iLO のバックアップの際にパスワードを設定した場合は、[アップロードおよびリストア]をクリックする前に、「バックアップファイルパスワード」の下の入力欄にパスワードを入力してください。

リストア



リストアすると、すべての構成設定が置き換えられます。

バックアップファイルパスワード	オプション
バックアップファイル	
ファイルの選択	JPN02840CS_2...30216_1627.bak

アップロードおよびリストア

8. ブラウザの画面右に以下メッセージが表示されます。リストアを行うサーバにおいて、iLO への接続が一時的に切断しても問題が無いことを確認した後、[リストア]をクリックします。



リストアの確認

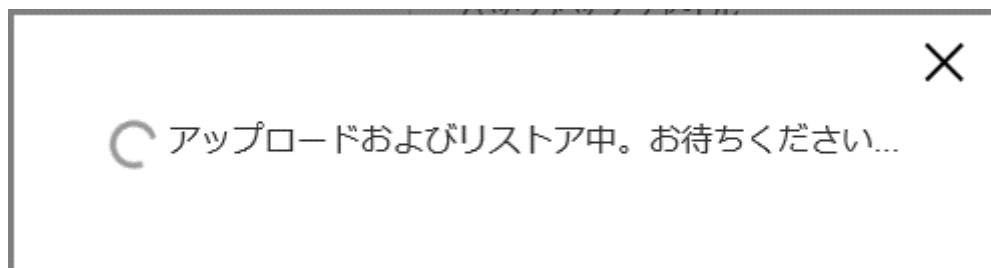
iLOの設定を復元すると、iLOが再起動されます。これにより、リモートコンソールと仮想メディアを含むiLOへの接続がすべて終了します。サーバーは影響を受けません。

リストア

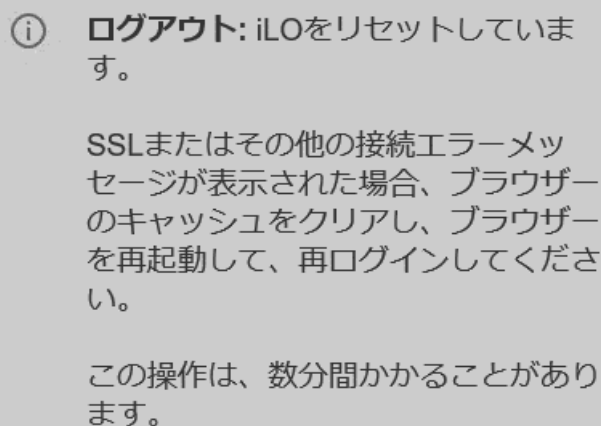
《参考》

この操作によりクラスタノードとなるサーバ装置のiLOが再起動しますが、当該サーバのESXiは稼働したままの状態を維持します。

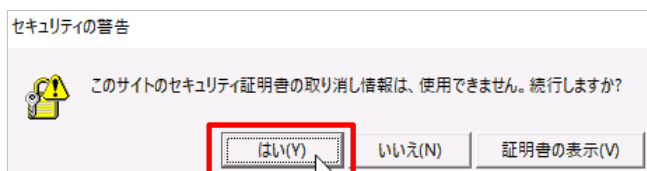
9. 設定情報のリストアが開始され、ブラウザに以下メッセージが表示されます。



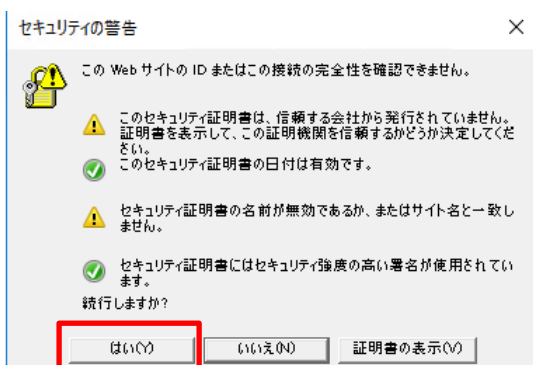
しばらくするとブラウザの表示が更新され、iLO のログインページと共に以下メッセージが画面右下に表示されます。



※ 上記画面に続き、以下確認ダイアログが表示される場合があります。この場合、[はい]をクリックして操作を継続してください。



また、以下「セキュリティ警告」のダイアログが表示された場合においても、[はい]をクリックしてください。



10. ブラウザの表示を更新し、iLO のログインページが表示されることを確認します。

※本手順以降、クラスタノードの iLO のパスワードが初期パスワードになります。
クラスタノードの iLO の初期パスワードは「初期パスワード通知書」を参照ください。

Orchestrating a brighter world **NEC**



※ ブラウザの画面右下に以下メッセージが表示される場合は、しばらく時間を置いた後、再度ブラウザの表示を更新してください。

✖ 接続が確立できません。ネットワークの構成を変更した場合には、SSL接続を再ネゴシエートするために、このページを更新してください。

以上で iLO の設定リストアは完了となります。引き続き、2.2.4 項の作業を行います。なお、複数のクラスタノードに対してリストアを行う場合、2.2.4 項冒頭の「【重要】」の順に作業を実施してください。

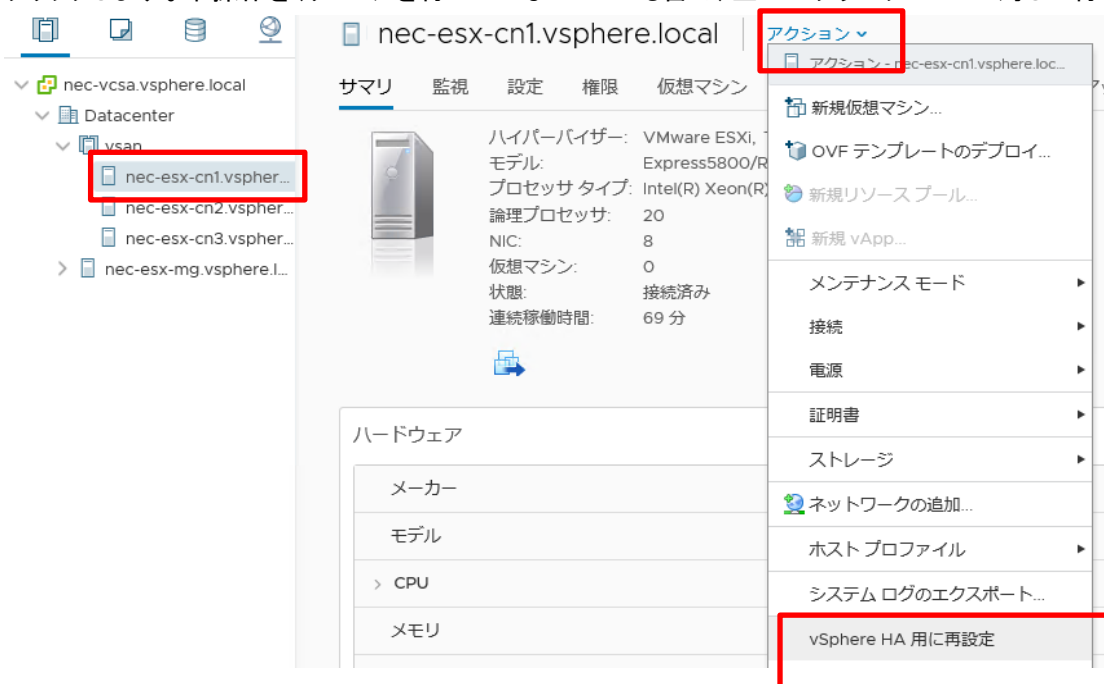
2.2.4. リストア後のノード再稼働

本項は、クラスタノードのリストア実施後に必要な操作について記載しています。

【重要】

本2.2.4項の操作は、すべてのクラスタノードに対してリストア作業(2.2.1項から2.2.3項)を行った後に実施してください。

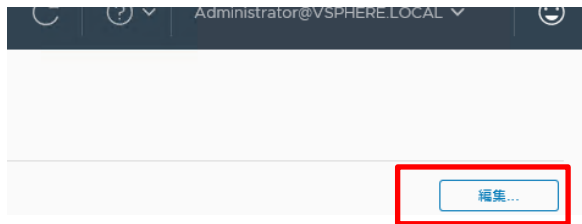
1. 管理 VM に管理者権限を有するユーザでサインインし、vSphere Client で vCSA にログインします。
2. オブジェクトナビゲータでクラスタノード名をクリックし、[アクション] - [vSphere HA 用に再設定]の順にクリックします。本操作を(リストアを行っていないノードも含め)全てのクラスタノードに対して行います。



3. 続いて、オブジェクトナビゲータで vSAN クラスタ名をクリックした後、[設定]または[構成]タブ - [vSphere の可用性]の順にクリックします。



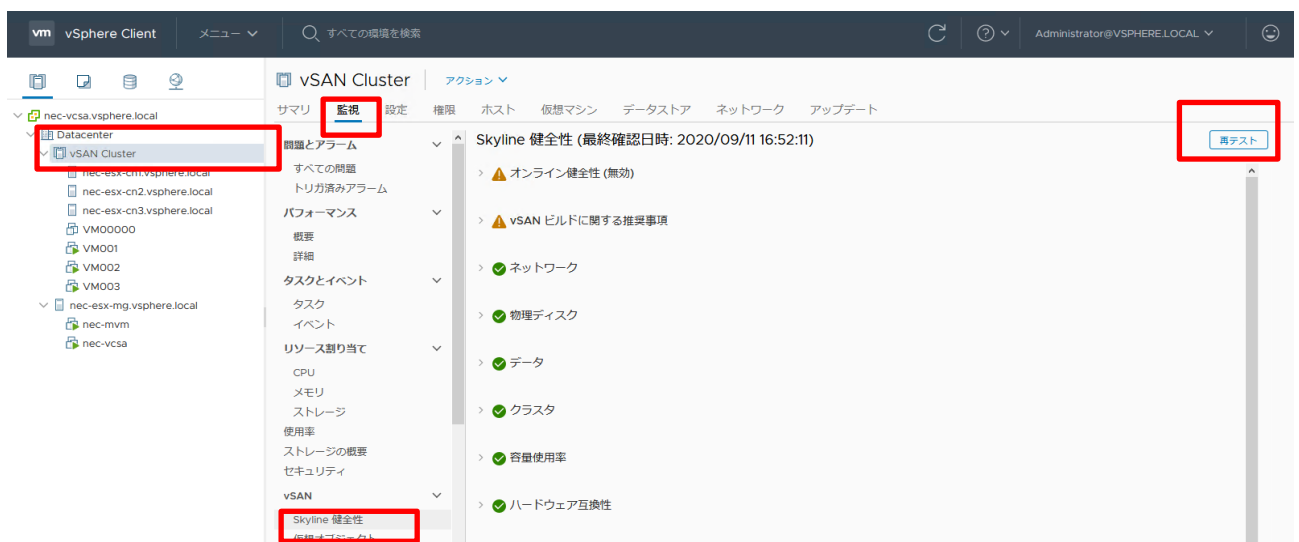
4. タブ画面内右上の、「vSphere の可用性」の右端に表示される[編集]をクリックします。



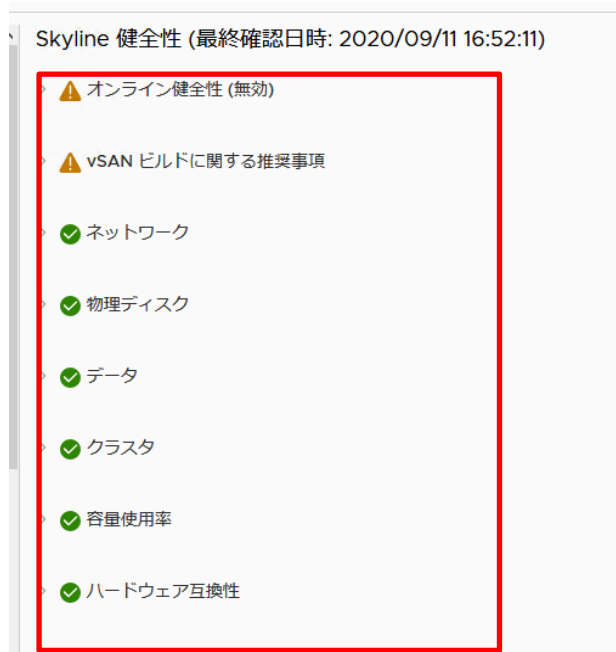
5. 「クラスタ設定の編集」ダイアログが表示されますので、ダイアログ内上のメニューで[障害および対応]をクリックした後、[ホスト監視の有効化]の状態を確認します。状態が無効の場合は有効にし、ダイアログ内右下の[OK]をクリックします。



6. オブジェクトナビゲータで vSAN クラスタ名を選択した状態で、画面中央上部の[監視]タブをクリックし、[▼vSAN]の下に[Skyline 健全性]をクリックした後、画面右上の[再テスト]をクリックします。



7. vSAN 環境の健全性確認の結果が画面右の健全性ツリーに表示されますので参照します。



健全性ツリーに「失敗」の項目が存在する場合、(テスト名の先頭に「▶」が表示されている場合は、「▶」部分をクリックして具体的なテスト名を表示させた後)テスト名をクリックして、失敗した具体的な内容を画面右下の表示で確認した後、原因の対処を行ってください。

※ 「テスト結果」が「警告」となっている項目については、可能な範囲で、結果が「パス」となるように設定を行ってください。HCS をインターネットに接続できない環境に設置している等、意図的に「警告」となる構成としている場合は、「警告」のままで問題ありません。

8. 健全性確認の結果が表示されている状態で、「▼問題とアラーム」の下[すべての問題]をクリックします。



[監視]タブ画面内右の一覧の内容を確認します。「問題」列の値を一件ずつ参照し、対処済み、および対処不要の内容については、その行を選択した状態で一覧の左上に表示される[緑にリセット]アイコンをクリックします。リセットできないアラームが発生した場合は、クリアされるように原因の特定、および復旧作業を行ってください。

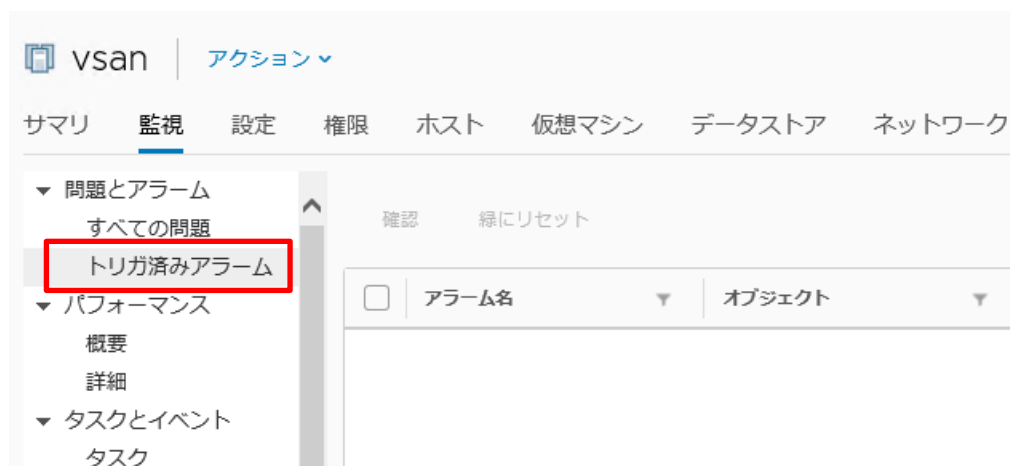
権限 ホスト 仮想マシン データストア ネットワーク アップデート

 確認

 緑にリセット

問題	タイプ	起動時間	ステータス
nec-esx-cn1.vsphere.local: ホストの接続と電源状態	トリガ済みアラーム	2019年08月01日 13:30:42	 アラート
nec-esx-cn2.vsphere.local: ホストの接続と電源状態	トリガ済みアラーム	2019年08月01日 13:29:10	 アラート
nec-esx-cn3.vsphere.local: ホストの接続と電源状態	トリガ済みアラーム	2019年08月01日 13:29:10	 アラート
vSAN 健全性アラーム「vSANビルドに関する推奨事項エン...	トリガ済みアラーム	2019年08月01日 13:30:45	 警告
vSAN 健全性アラーム「vSANリリース カatalogの更新状態」	トリガ済みアラーム	2019年08月01日 13:30:45	 警告
vSphere HA が、データセンター Datacenter 内のクラスタ v...	設定問題	2019年08月05日 10:18:05	
vSphere HA ホストの監視が無効です。仮想マシンのフェ...	設定問題	2019年08月05日 10:18:05	

9. [監視]タブ画面に[すべての問題]の一覧が表示されている状態で、タブ画面内左のメニューで[▼問題とアラーム]の下[トリガ済みアラーム]をクリックし、手順 8 同様にオブジェクトの一覧で、アラーム内容の確認、および復旧作業やリセットを行います。

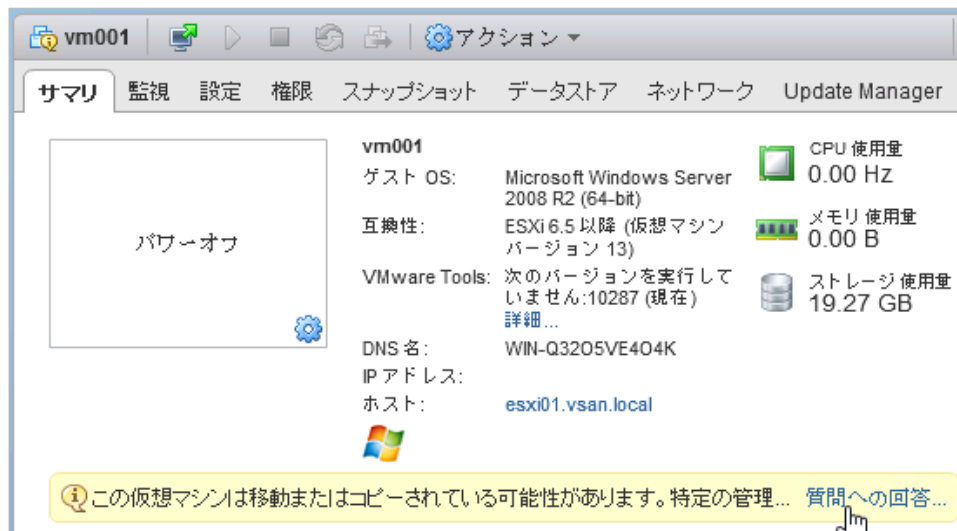


10. 必要に応じて、他のクラスタノードに移行した仮想マシンを、リストアしたクラスタノードに再度移行してください。

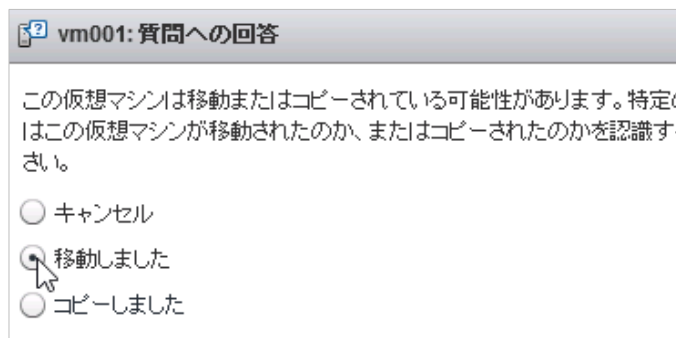
以上でリストア後のノード再稼働は完了となります。

《参考》

リストアの実施後、vSANクラスタ上の仮想マシンの電源をONにした際、オブジェクトナビゲータで仮想マシン名を選択した状態で画面中央上部の[サマリ]をクリックした画面において、「この仮想マシンは移動またはコピーされている可能性があります」の確認メッセージが表示される場合があります。



この場合、[質問への回答]をクリックした後、表示されるダイアログ内で[移動しました]にチェックを付けた後、[OK]をクリックしてください。



《参考》

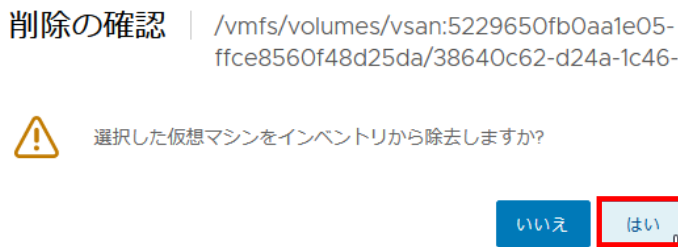
リストアの実施後、クラスターノード上の仮想マシンのサマリに「この仮想マシンにはネットワークが割り当てられていません。」と表示される場合があります。



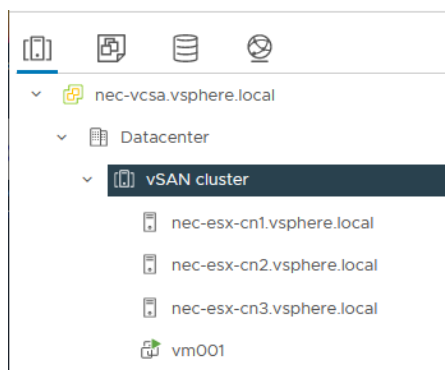
この場合は、vSphere Clientの「ホストおよびクラスタ」の画面において、オブジェクトナビゲータで該当する仮想マシン名を右クリックした後、表示されるメニューで[インベントリからの除去]または[インベントリから削除]をクリックします。



以下のダイアログが表示された場合は、[はい]をクリックします。



上記操作により、サマリに「この仮想マシンにはネットワークが割り当てられていません。」と表示された仮想マシンがインベントリから削除されます。



2.2.5. NEC HCS Console の確認

1.2.4.4 項を参照し、リストア後のノードに警告等が表示されている場合は対処を実施してください。

※ サーバ診断カルテを設定している環境で、1.2.4.4 項手順 9 の[警告]の状態になっている場合、手順を参照し警告および認証失敗の対処を実施してください。

3. パスワード更新

本項では、初期バックアップのリストアによって出荷時の初期パスワードに戻ったパスワードを更新する手順を記載しています。

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に更新してください。変更したパスワードは控えておいてください。

3.1. 準備

パスワード更新は管理 VM より行いますので、Windows PC から管理 VM に接続してください。

3.2. 管理ノードの管理 VM のパスワード更新

「NEC Hyper Converged System for VMware vSAN/CR2.0 スタートアップガイド」の「5.5 管理ノードの管理 VM(Windows Server 2019)のパスワード変更」を参照ください。

3.3. 管理ノード、クラスタノード、vCenter Server、Witness ノード、HCS Console のパスワード更新

「NEC Hyper Converged System for VMware vSAN/CR2.0 スタートアップガイド」の「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」、「5.3 クラスタノード、管理ノードの ESXi パスワードの変更」、「5.4 管理ノードの vCSA パスワードの変更」、「5.7 NEC Hyper Converged System Console のパスワード変更」、「5.8 管理ノードの Witness ノードのパスワード変更」、「5.9 NEC Hyper Converged System Console の登録情報の更新」を参照ください。

[注意]

構築サービスでエクスプレス通報サービスおよびサーバ診断カルテの設定を実施した環境で、BMCやESXiのパスワードを変更した場合、ESMPRO/ServerManagerに監視対象として登録したiLOやESXiのコンポーネントのパスワードも変更する必要があります。詳細は「NEC Hyper Converged System for VMware vSAN/CR2.0 スタートアップガイド」の「5.10 ESMPRO/ServerManagerの登録情報の更新」を参照ください。

また、サーバ診断カルテの設定を実施している環境の場合は「5.11 サーバ診断カルテの登録情報の更新」も実施してください。

3.4. ESMPRO/ServerManager のパスワード更新

「NEC Hyper Converged System for VMware vSAN/CR2.0 スタートアップガイド」の「5.6 管理 VM の ESMPRO/ServerManager のパスワード変更」を参照ください。

3.5. 保守アカウントのパスワード更新

「NEC Hyper Converged System for VMware vSAN/CR2.0 スタートアップガイド」の「5.12 保守アカウントのパスワード更新」を参照ください。

以上で、パスワードの更新は完了です。

4. 補足

4.1. VMware vSphere Client の接続方法

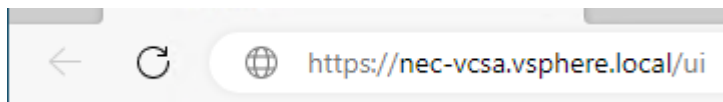
VMware vSphere Client(本書では、「vSphere Client」と表記します)は、vCenter Server、ESXi サーバ、および仮想マシンの管理を行うための Web アプリケーションです。

本項では vSphere Client のログイン/ログアウトについて記載します。

ログイン

1. 管理 VM に管理者権限を有するユーザでサインインし、ブラウザを起動して、以下の URL を入力し、vSphere Client で vCSA に接続します。

`https://<vCSA の FQDN>/ui`

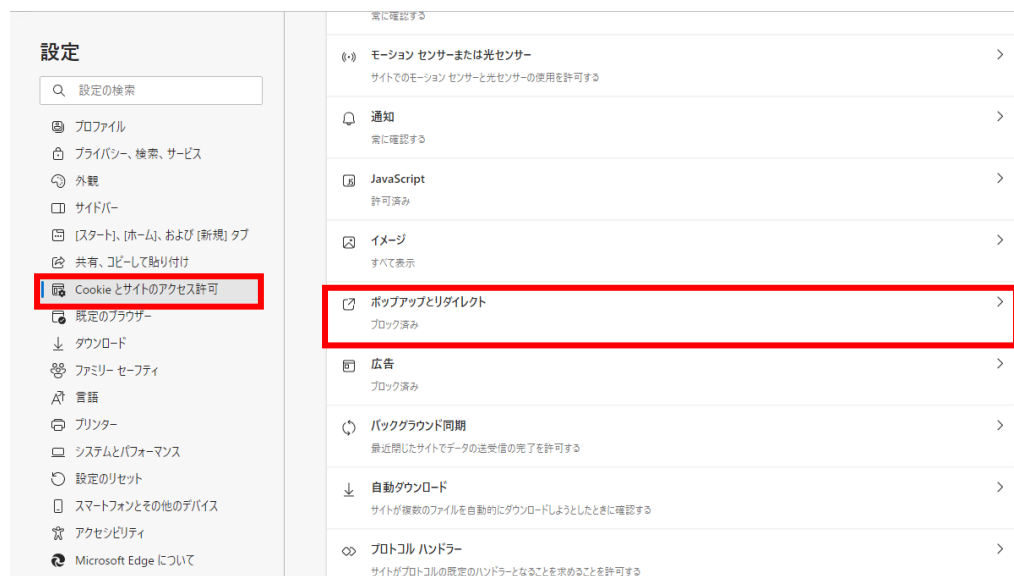


- ※ 上記操作に続いてブラウザに「接続がプライベートではありません」画面が表示された場合は、[詳細設定]をクリックし表示された画面で、[<IP アドレスまたは FQDN>に進む(安全ではありません)]をクリックしてください。

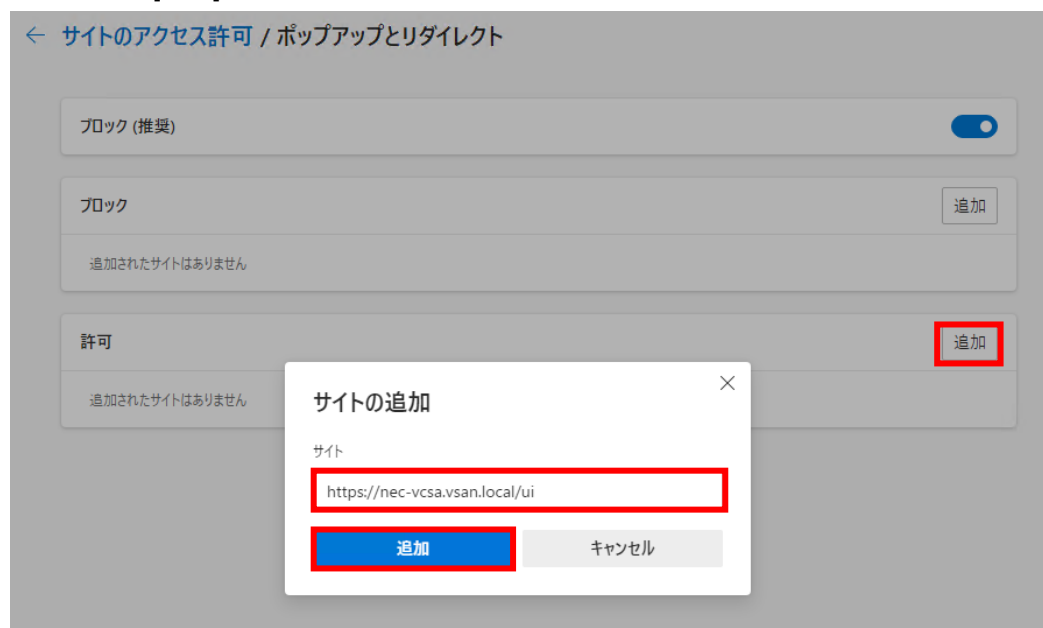


《参考》ポップアップブロックの登録について:

Microsoft Edgeの場合、画面右上のメニューから [設定]—[Cookieとサイトのアクセス許可]を順にクリックし、下にスクロールして「ポップアップとリダイレクト」をクリックします。



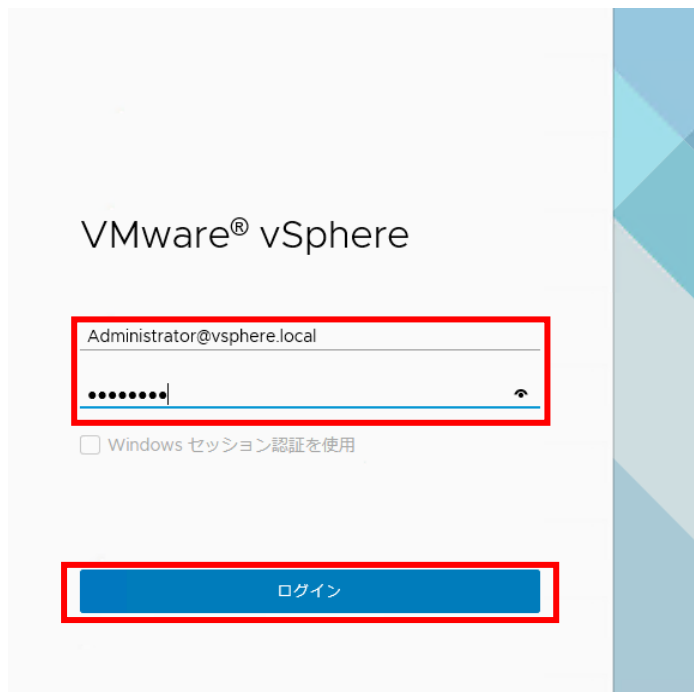
「許可」の右側の[追加]をクリックし、ダイアログが表示されたら、[サイト]欄に登録対象のURLを入力した後、[追加]をクリックします。



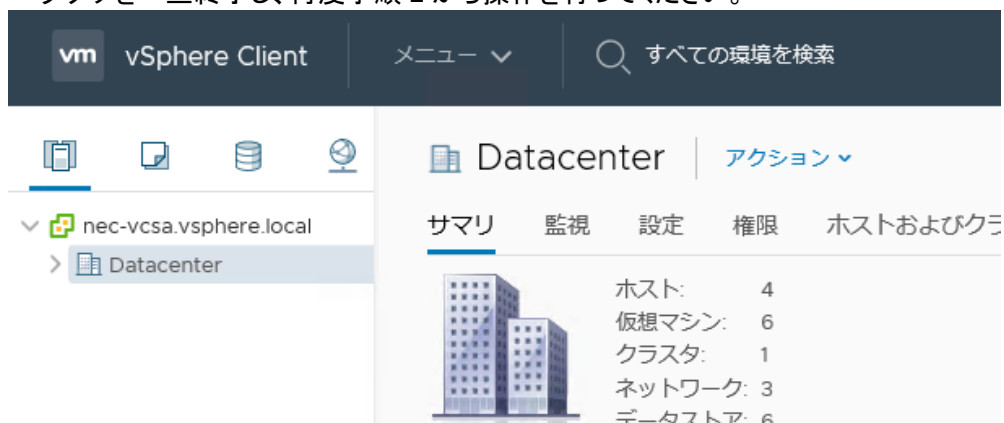
Microsoft Edge以外のWebブラウザにおける操作については、各Webブラウザのドキュメントもしくはヘルプを参照ください。

2. 接続が成功すると、vSphere Client のログイン画面が表示されます。(以下図)
アカウント情報を入力し、ログインします。
※管理ノードを起動してから vCSA に接続できるようになるまでに 10 分程度の時間がかかります。

- アカウント: 「Administrator@vsphere.local」
- パスワード: 「vCSA – SSO administrator パスワード」



3. 正常にログインすると、vSphere Client の操作画面が表示されます。
※ 稀に、以下の画面が表示されず、背景色のみが表示された状態が継続する場合があります。
手順 2 の操作を行った後、2 分程経過しても vSphere Client の操作画面が表示されない場合、Web ブラウザを一旦終了し、再度手順 1 から操作を行ってください。



※ 本書では、本項の操作を「vSphere Client で vCSA にログインする」と表記します。

ログアウト

1. vSphere Client の画面上部に表示されているユーザ名（以下画面例の場合、[Administrator@VSPHERE.LOCAL]の箇所）をクリックします。表示されたメニューから[ログアウト]をクリックします。



2. 正常にログアウトすると、ログイン画面が表示されます。

4.1.1. セキュリティ証明書のインストール

「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。」などの画面が表示されるのを抑止するには、セキュリティ証明書を管理VMにインストールする必要があります。

ここでは、vCenter Serverが発行する自己署名証明書をインストールする手順を記載します。

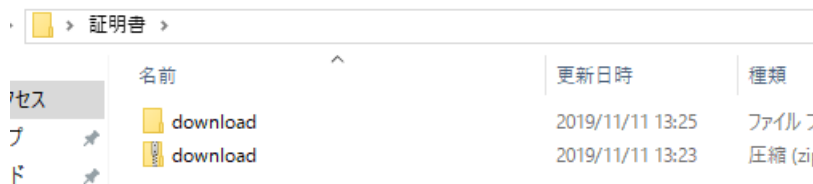
1. セキュリティ証明書を入手するには、管理VMのWebブラウザのアドレス欄に以下のURLを入力します。

<https://nec-vcsa.vsphere.local/>

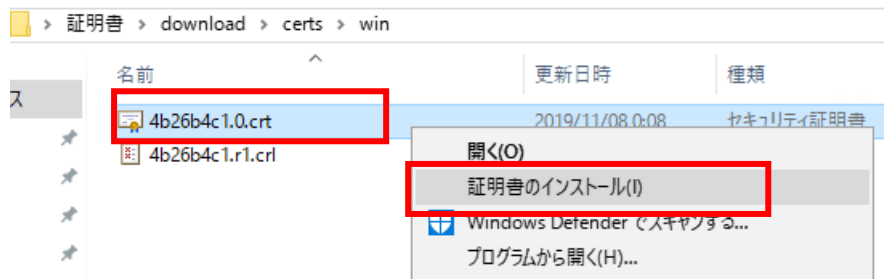
※ ブラウザに「接続がプライベートではありません」画面が表示された場合は、[詳細設定]をクリックし表示された画面で、[<IPアドレスまたはFQDN>に進む(安全ではありません)]をクリックしてください。

2. 以下の画面が表示されたら、「信頼されたルートCA証明書をダウンロード」を右クリックし、「名前を付けてリンクを保存」をクリックした後、管理VM上の任意のディレクトリにzipファイルを保存し、展開します。





3. [download] — [certs] — [win]を順にフォルダを開き、ルート証明書ファイル(拡張子が.crtのもの)を右クリックし、[証明書のインストール]をクリックします。



4. 「証明書のインポートウィザード」ダイアログが表示されたら、[現在のユーザ]を選択して[次へ]をクリックします。

証明書のインポートウィザード

証明書のインポートウィザードの開始

このウィザードでは、証明書、証明書信頼リスト、および証明書失効リストをディスクから証明書ストアにコピーします。

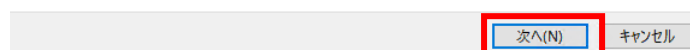
証明機関によって発行された証明書は、ユーザー ID を確認し、データを保護したり、またはセキュリティで保護されたネットワーク接続を提供するための情報を含んでいます。証明書ストアは、証明書が保管されるシステム上の領域です。

保存場所

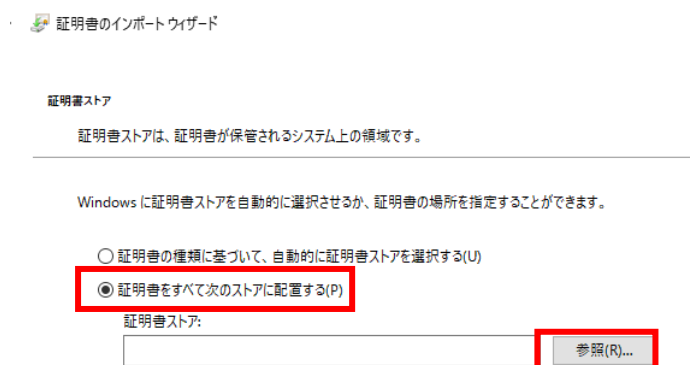
☒ 現在のユーザー(C)

☐ ローカル コンピューター(L)

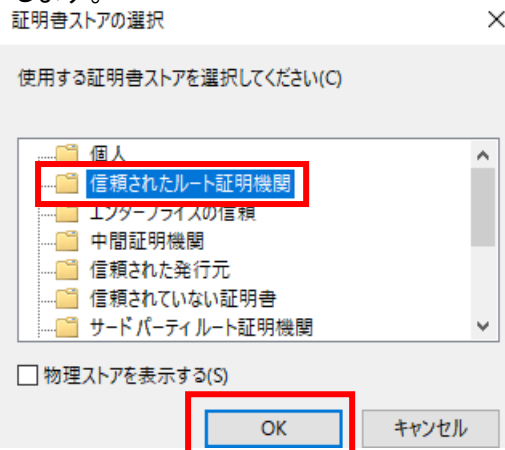
続行するには、[次へ] をクリックしてください。



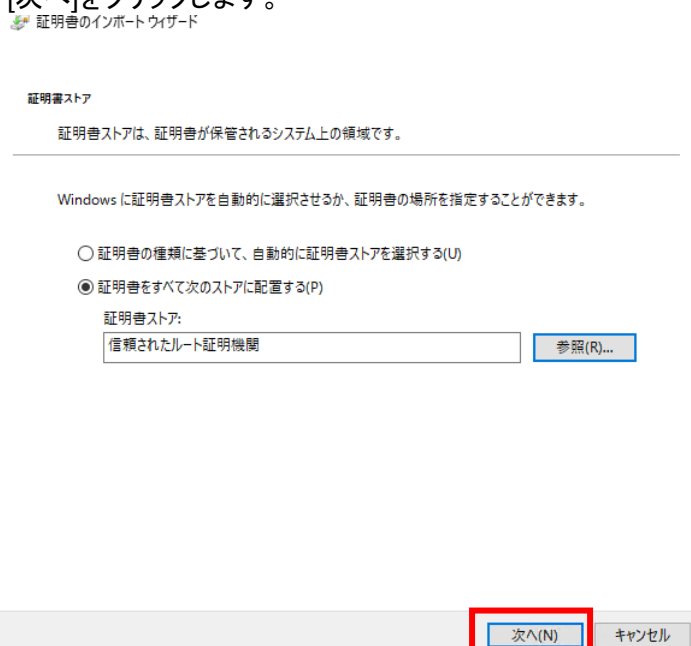
5. 下図の画面が表示されたら、[証明書をすべて次のストアに配置する]を選択し、[参照]をクリックします。



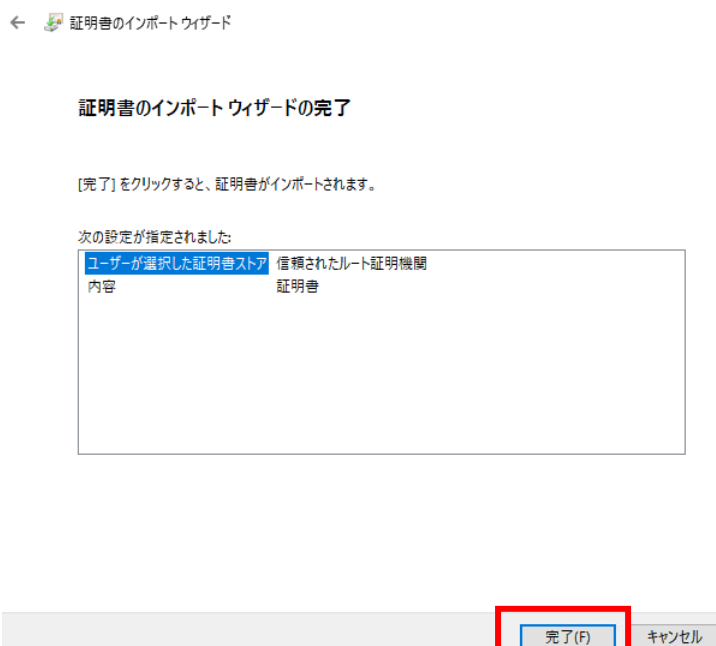
6. 「証明書ストアの選択」ダイアログが表示されたら、[信頼されたルート証明機関]を選択して[OK]をクリックします。



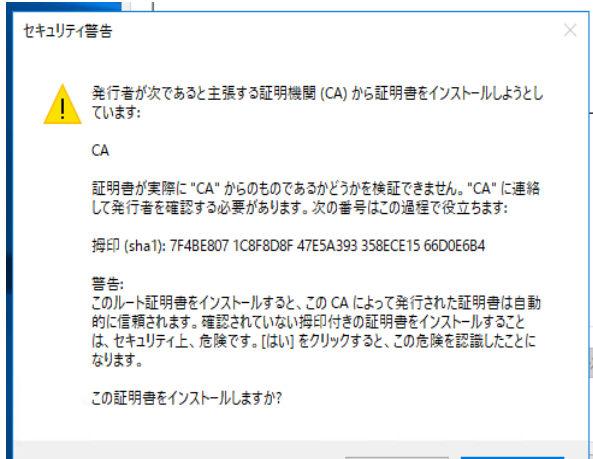
7. [次へ]をクリックします。



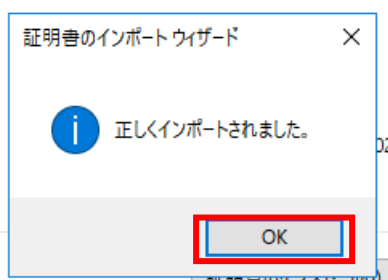
8. [完了]をクリックします。



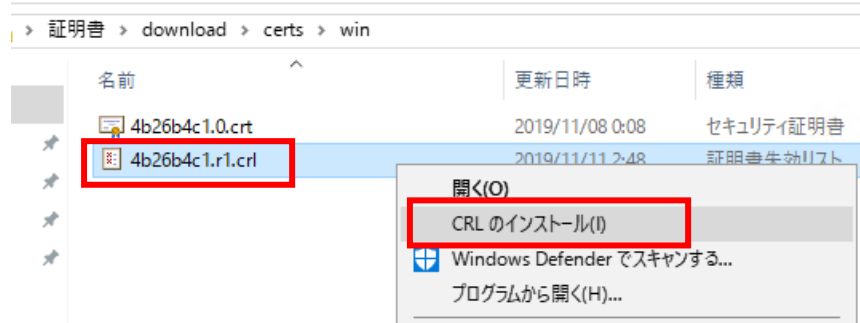
9. 「セキュリティ警告」ダイアログが表示されたら、[はい]をクリックします。



10. 「証明書のインポートウィザード」が表示されたら、[OK]をクリックします。



11. 証明書失効リストファイル(拡張子が.crl)を右クリックし、[CRLのインストール]をクリックします。



12. 手順4から手順10を実施し、同様の手順にて証明書失効リストファイル(拡張子が.crl)をインストールしてください。

全てのインストール作業が完了したらブラウザを再起動してください。

4.2. VMware Host Client の接続方法

VMware Host Client(本書では、「Host Client」と表記します)は、単一の ESXi サーバに対して操作・管理を行うための Web アプリケーションです。

本項では Host Client のログイン/ログアウトについて記載します。

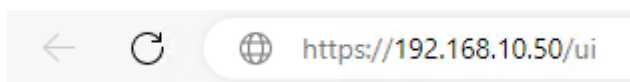
※本項の操作に関する詳細は、以下 Web ページを参照ください。

<<https://docs.vmware.com/jp/VMware-vSphere/7.0/com.vmware.vsphere.hostclient.doc/GUID-4EAF4E4-D666-4E40-8CF9-7B96418DD3DB.html>>

ログイン

1. 管理 VM に管理者権限を有するユーザでサインインし、ブラウザを起動して、以下の URL 入力し、管理ノードもしくはクラスタノードの Host Client に接続します。

`https://<管理ノードもしくはクラスタノードの管理用 NW の IP アドレス>/ui`



※ 上記操作に続いてブラウザに「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)]をクリックしてください。

2. 接続が成功すると、Host Client のログイン画面が表示されます。(以下図)
アカウント情報を入力し、ログインします。

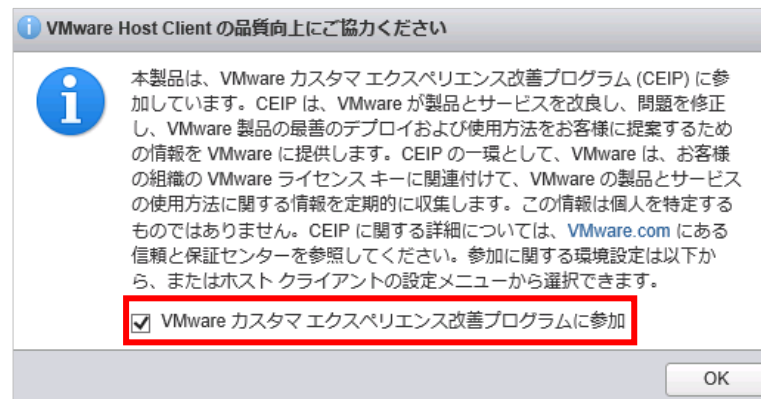
- ユーザー名: 「root」
- パスワード: 「管理ノードもしくはクラスタノード - ESXi の root パスワード」



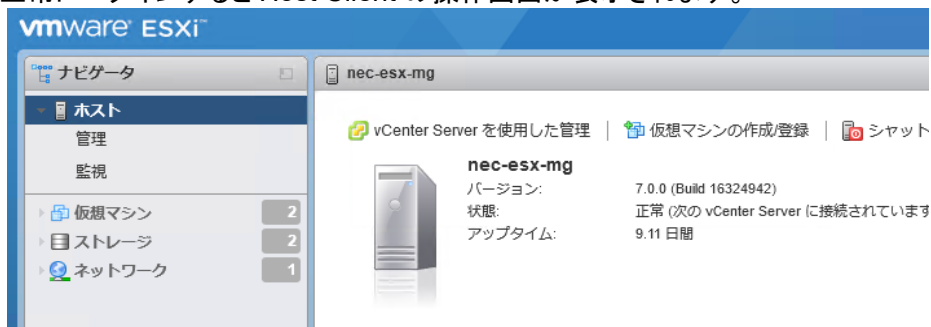
《参考》

手順2の操作を行った後、以下のダイアログが表示される場合があります。VMware社のカスタマエクスペリエンス改善プログラム(CEIP)へ参加する場合は、[CEIPへの参加]にチェックを付けた状態で[OK]をクリックします。CEIPの詳細については、以下Webページを参照ください。

<<https://docs.vmware.com/jp/VMware-vSphere/7.0/com.vmware.vsphere.vcenterhost.doc/GUID-64717014-F7F5-4DBD-ABE8-0057161A1046.html>>



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



※ 本書では、本項の操作を「Host Client にログインする」と表記します。

ログアウト

1. Host Client の画面上部に表示されているユーザ名部分(以下画面例の場合、[root@192.168.10.50] の箇所)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。



2. 正常にログアウトすると、ログイン画面が表示されます。

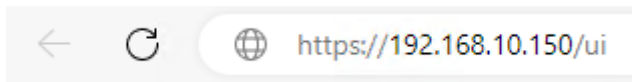
4.3. iLO の接続方法

本項では iLO のログイン/ログアウトについて記載します。

ログイン

1. 管理 VM もしくは、Windows PC に管理者権限を有するユーザでサインインし、ブラウザを起動して、以下 URL を入力し、iLO に接続します。

`https://<管理ノードもしくはクラスタノードの iLO (BMC) の IP アドレス>/`



※ 上記操作に続いてブラウザに「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)]をクリックしてください。

2. iLO のログイン画面が表示されます。(以下図)
アカウント情報を入力し、ログインします。

- ローカル ログイン名: 「hcsadmin」
- パスワード: 「管理ノードもしくはクラスタノード - BMC のパスワード」



iLO 5

ローカル ログイン 名

hcsadmin

パスワード

●●●●●●●●

ログイン

ja - 日本語 

3. 正常にログインすると、iLO の Web インターフェイス画面が表示されます。

※ 本書では、本項の操作を「iLO にログインする」と表記します。

ログアウト

1. iLO の Web インターフェイス画面右上の赤枠のアイコンを選択し、[ログアウト]をクリックします。

2. 正常にログアウトすると、ログイン画面が表示されます。

4.4. ESXi Shell の接続方法

ESXi Shell は ESXi のトラブルシューティングを目的として使用するコマンドラインインターフェイスのシェルです。

特に、パッチやドライバの追加・削除、vSphere Client から設定できない項目の操作・表示に使用します。

ESXi Shell は、コンソールもしくは、ターミナルソフトで接続して使用します。

コンソールでの接続方法は、「4.4.1 コンソールを使用する場合」、

ターミナルソフトでの接続方法は、「4.4.2. ターミナルソフトを使用する場合」をそれぞれ参照ください。

4.4.1. コンソールを使用する場合

本項では、Web コンソールを使用して ESXi Shell に接続する方法について記載します。

《注意》

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

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

("@" は「Shift + 2」で入力することができます。)

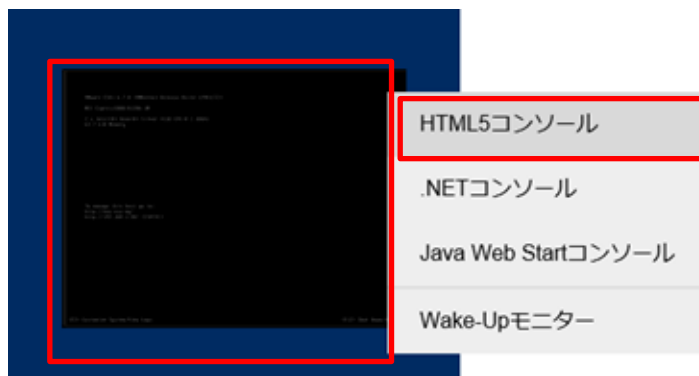
本事象が発生した場合は、ダイレクトコンソールユーザインターフェイスにログインして「Configure Keyboard」の値を"Japanese"に設定し直してください。

ESXi7.0Update1 以降では本問題は解消されています。

サーバにディスプレイ/キーボードを接続しローカルからアクセスするか、iLO に接続し、コンソールを起動してください。

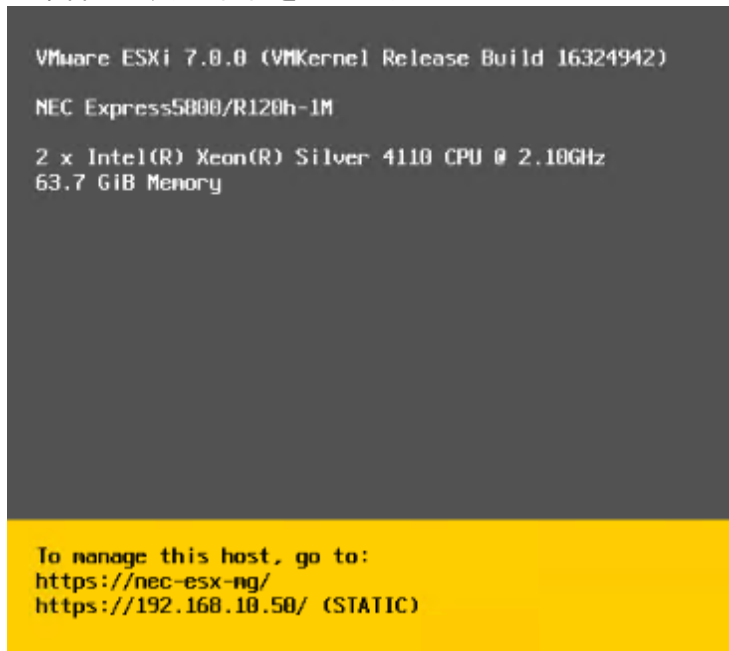
《参考》 iLOに接続しコンソールを起動する手順について：

1. 管理VMもしくは、Windows PCに管理者権限を有するユーザでサインインし、iLOにログインします。
2. iLOのWebインターフェイス画面が表示されたら、画面左下のESXiコンソールをクリックし、[HTML5コンソール]を選択します。



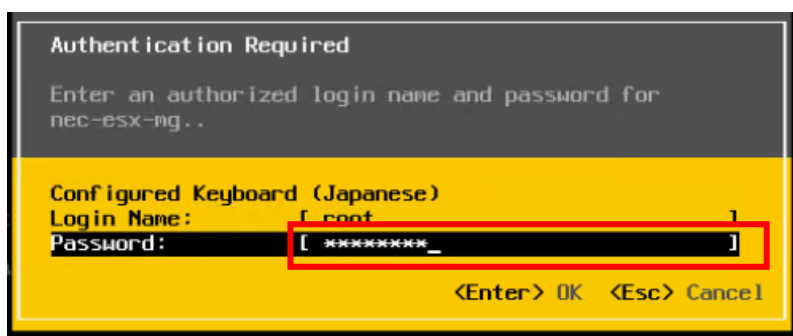
ESXi Shell 有効化とログイン

1. ESXi が起動し、以下画面が表示されている状態で[F2]キーを押下します。
※本書では、以下画面を「ダイレクトコンソールユーザインターフェイスの初期画面」と表記します



2. 「Authentication Required」の画面が表示されたら、アカウント情報を入力し、[Enter]キーを押下します。

- Login Name: 「root」
- Password: 「管理ノードもしくはクラスタノード - ESXi の root パスワード」



3. 「System Customization」の画面が表示されます。
画面左のメニューにおいて[Troubleshooting Options]を選択し、[Enter]キーを押下します。



4. 「Troubleshooting Mode Options」の画面が表示されます。

画面左のメニューにおいて[Enable ESXi Shell]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[Disable ESXi Shell]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左のメニューに[Disable ESXi Shell]と表示されている場合は、操作を行わず、そのまま手順 5 の操作を行ってください。

Troubleshooting Mode Options	ESXi Shell
Disable ESXi Shell	ESXi Shell is Enabled
Disable SSH	
Modify ESXi Shell and SSH timeouts	Change current state of the ESXi Shell

5. [Alt + F1]キーを押下して ESXi Shell 画面を表示した後、root ユーザでログインします。

```
ESXi 7.0.0 http://www.vmware.com
Copyright (c) 2007-2020 VMware, Inc.

nec-esx-ng.vsphere.local 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-ng:~] _
```

※ 本書では、本項の操作を「コンソールで ESXi Shell に root ユーザでログインする」と表記します。

ESXi Shell 無効化とログアウト

1. 以下のコマンドを入力し、ESXi Shell からログアウトします。

```
> exit
```

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

2. ESXi Shell 画面が表示されている状態で[Alt + F2]キーを押下します。

※この時ダイレクトコンソールユーザインターフェイスの初期画面が表示された場合、ログイン手順の手順 1 から手順 3 の操作を行ってください。

3. 「Troubleshooting Mode Options」の画面が表示されます

4. 画面左のメニューにおいて[Disable ESXi Shell]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[Enable ESXi Shell]に更新されることを確認します。

Troubleshooting Mode Options	ESXi Shell
Enable ESXi Shell	ESXi Shell is Disabled
Disable SSH	
Modify ESXi Shell and SSH timeouts	Change current state of the ESXi Shell
Modify DCUI idle timeout	

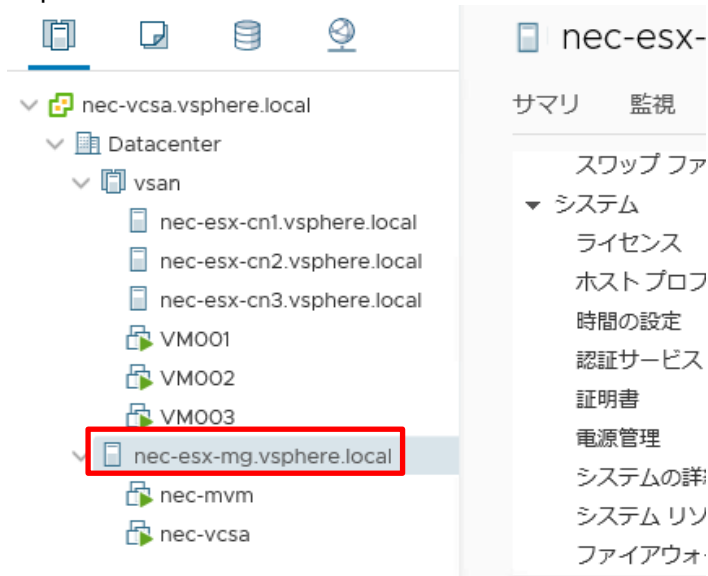
※ 本書では、手順 1 から手順 4 の操作を「ESXi Shell を無効にする」と表記します。

4.4.2. ターミナルソフトを使用する場合

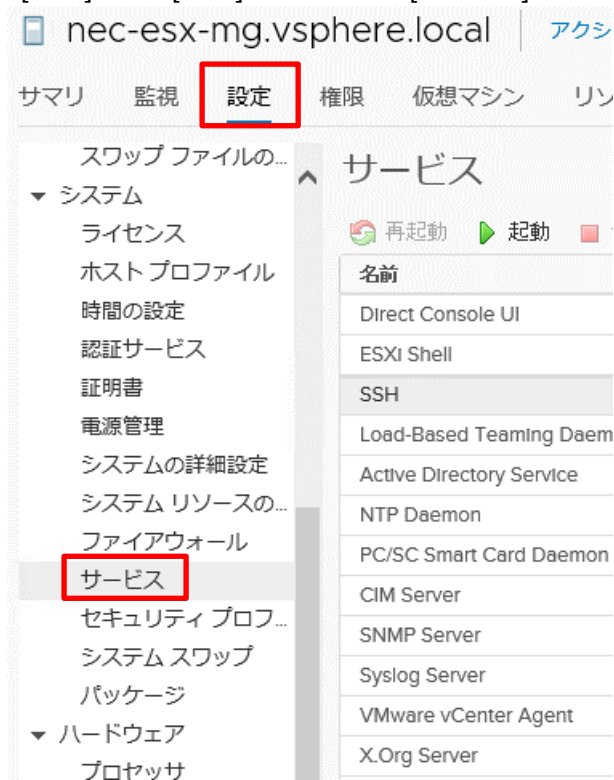
本項では、ターミナルソフトを使用して ESXi Shell に接続する方法と、SSH 接続の有効化/無効化について記載します。

vSphere による SSH の有効化

1. 管理 VM に管理者権限を有するユーザでサインインし、vSphere Client で vCSA にログインします。
2. vSphere Client の画面が表示されたら、画面左の SSH 接続を有効化するノードをクリックします。



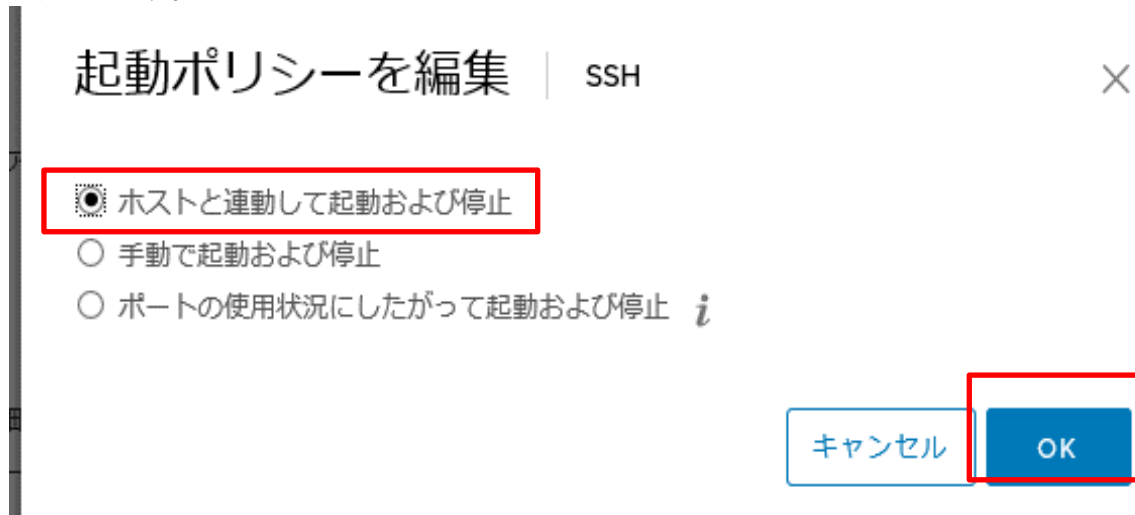
3. [設定]または[構成]タブを選択し、[サービス]をクリックします。



4. 「サービス」の一覧にある[SSH]をクリックし、[起動ポリシーを編集]をクリックします。



5. 「起動ポリシーを編集」ダイアログが表示されたら、[ホストと連動して起動および停止]をクリックし、[OK]をクリックします。



6. 「SSH」の起動ポリシーが「ホストと連動して起動および停止」になっていることを確認したら、[起動]をクリックします。



7. 「SSH」のデーモンが「実行中」になっていることを確認します。



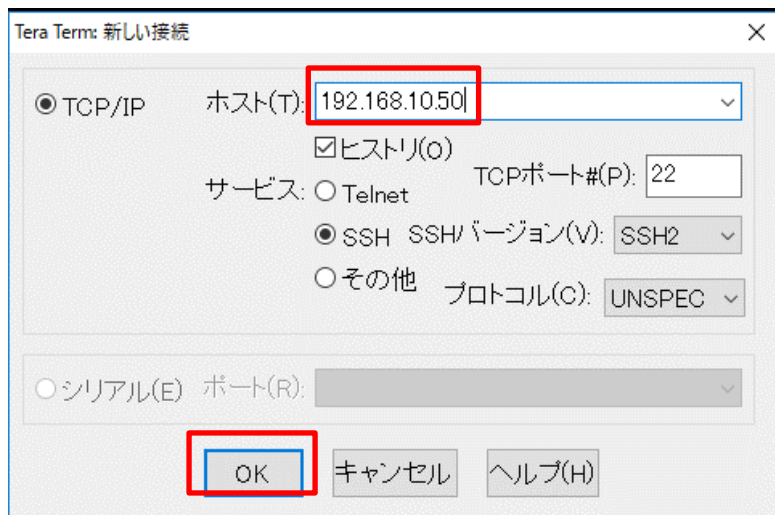
※ 本書では、本項の操作を「vCSA で SSH 接続を有効化する」と表記します。

ターミナルソフトでのログイン

1. ターミナルソフト(本書では、TeraTerm を使用しています)を起動し、[ホスト]欄に、以下アドレスを入力した後、[OK]をクリックします。

<管理ノード(もしくはクラスタノード)の管理用 NW の IP アドレス>

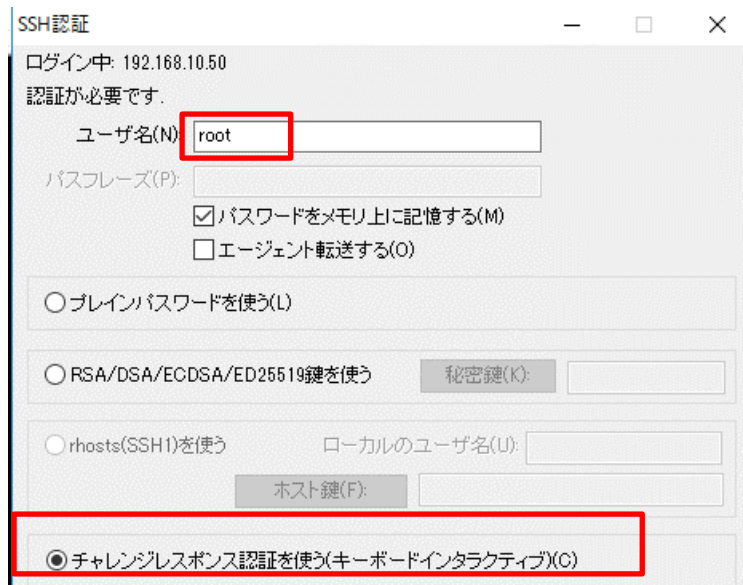
※ 他のターミナルソフトを使用される場合は、本項の内容に相当する操作を行ってください。



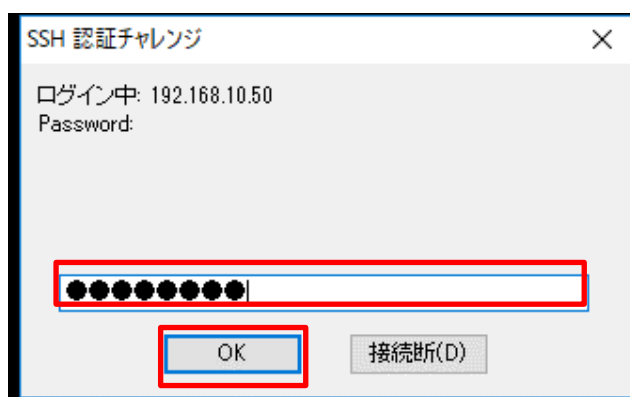
※ [OK]をクリックした後、「セキュリティ警告」のダイアログが表示される場合があります。その際は、[続行]をクリックして操作を続けます。



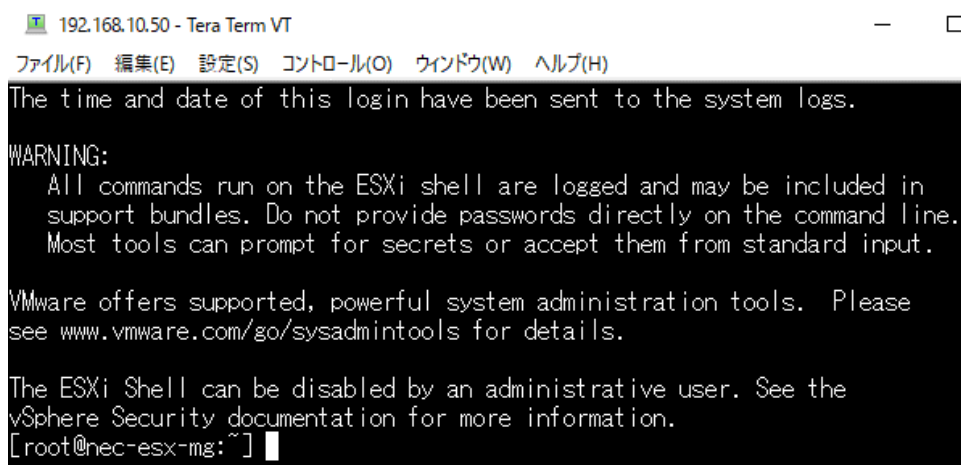
2. 「SSH 認証」のダイアログが表示されたら、[ユーザ名]欄に root を入力した後、[チャレンジレスポンス認証を使う]にチェックを付け、[OK]をクリックします。



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、root ユーザのパスワードを入力し、[OK]をクリックします。



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。



※ 本書では、本項の操作を「ターミナルソフトで ESXi Shell に root ユーザでログインする」と表記します。

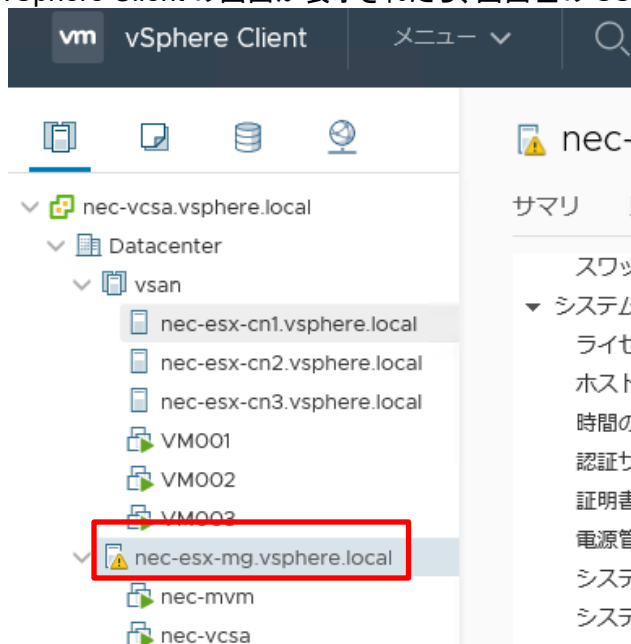
vSphere による SSH 無効化とログアウト

1. 以下のコマンドを入力し、SSH 接続を終了します。

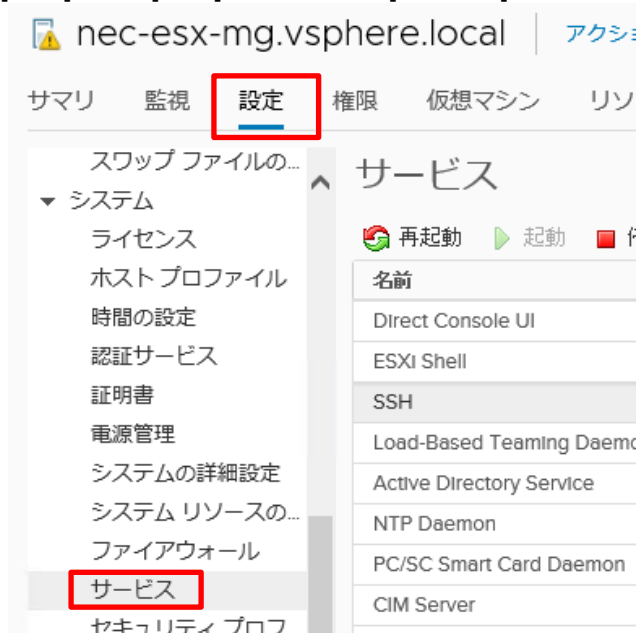
```
> exit
```

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

2. 管理 VM に管理者権限を有するユーザでサインインし、vSphere Client で vCSA にログインします。
3. vSphere Client の画面が表示されたら、画面左の SSH 接続を無効化するノードをクリックします。



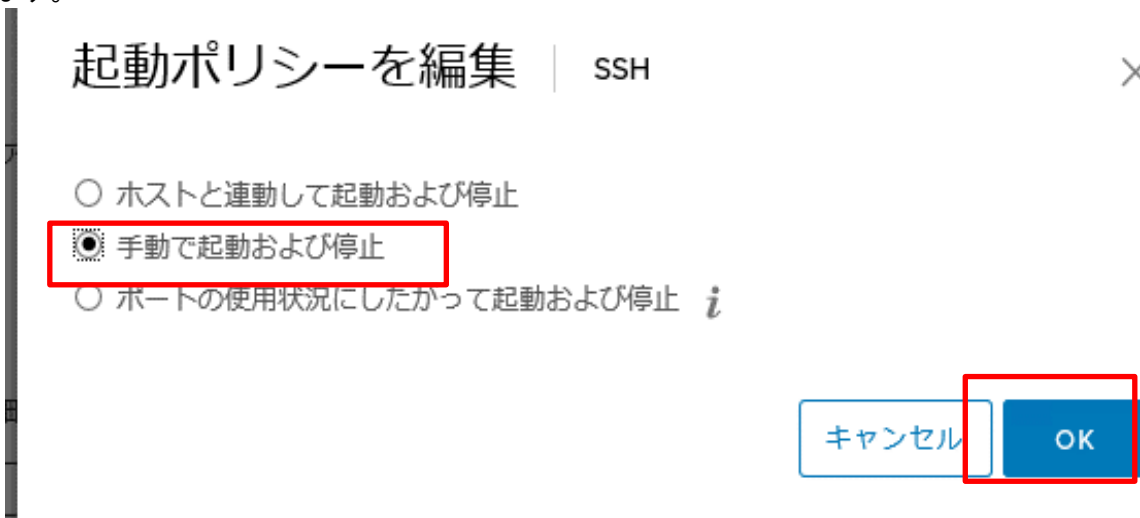
4. [設定]または[構成]タブを選択し、[サービス]をクリックします。



5. 「サービス」の一覧にある[SSH]をクリックし、[起動ポリシーを編集]をクリックします。



6. 「起動ポリシーを編集」ダイアログが表示されたら、[手動で起動および停止]をクリックし、[OK]をクリックします。



7. 「SSH」の起動ポリシーが「手動で起動および停止」になっていることを確認したら、[停止]をクリックします。



8. 「SSH」のデーモンが「停止」になっていることを確認します。



※ 本書では、本項の操作を「vCSA で SSH 接続を無効化する」と表記します。

4.5. NEC HCS Conosle の接続方法

本項では、定常運用で使用する NEC HCS Console のログイン/ログアウト操作について記載しています。

《参考》

管理PCから管理VMにリモートデスクトップ接続でログインし、webブラウザが利用できる状態で操作してください。

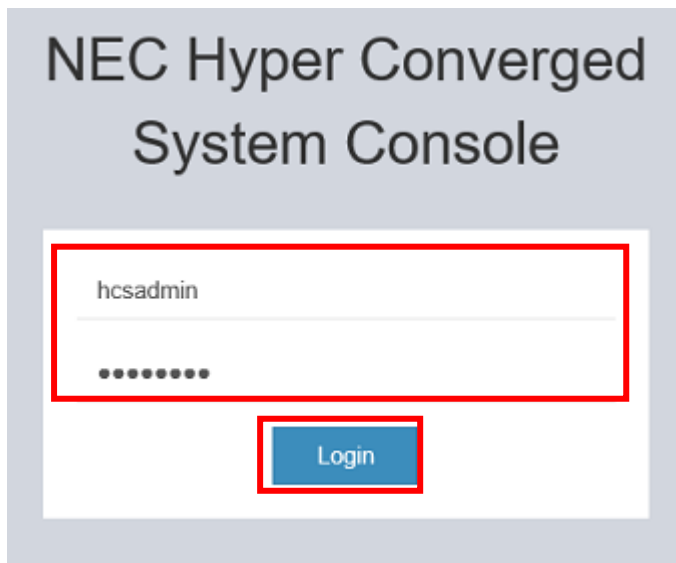
ログイン操作

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

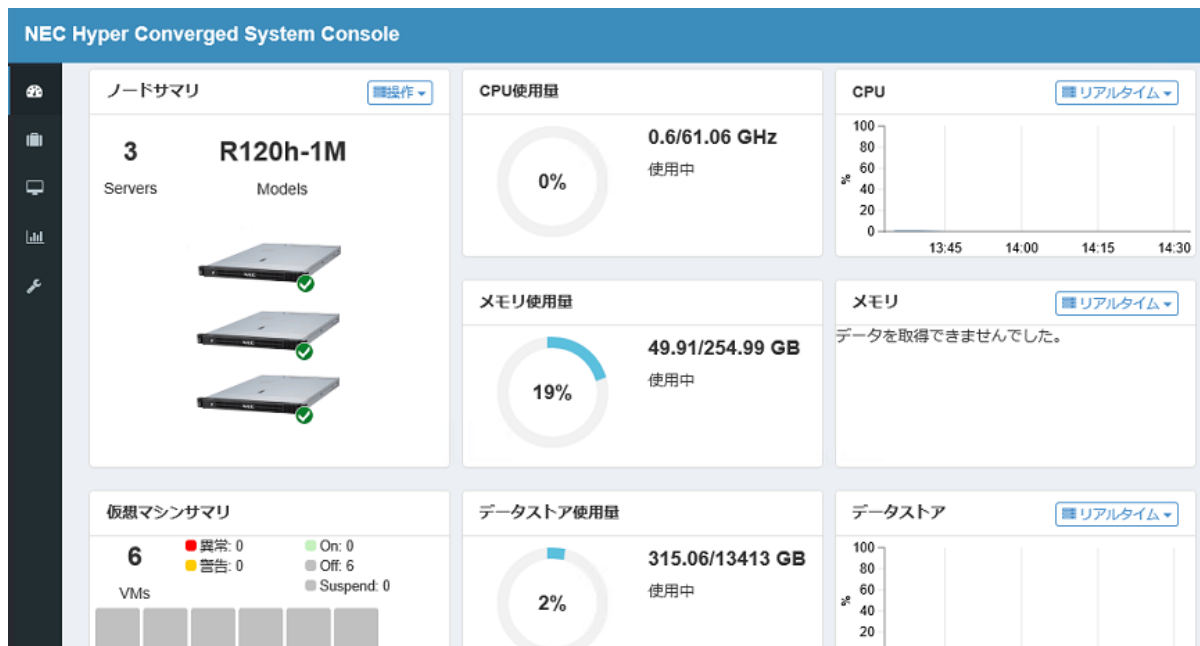
`http:// <管理 VM ホスト>/nechcs`

(管理 VM ホスト)には、管理 VM の FQDN、または IP アドレスを入力してください

3. NEC HCS Console のログイン画面が表示されます。
4. ユーザー名とパスワードを入力し[Login]をクリックします。

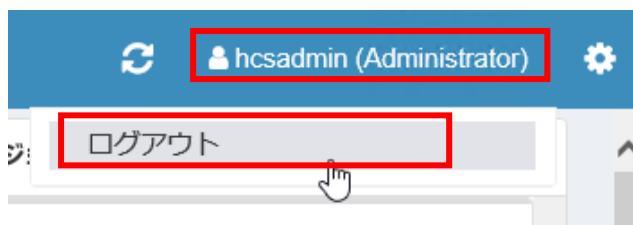


5. 正常にログインすると Web ブラウザに NEC HCS Console のダッシュボード画面が表示されます。



ログアウト操作

1. NEC HCS Console の画面上部に表示されているユーザー名 (以下画面例の場合、[hcsadmin(Administrator)])をクリックします。
2. 表示されたメニューで[ログアウト]をクリックします。



3. 正常にログアウトすると、Web ブラウザに NEC HCS Console のログイン画面が表示されます。

文書番号:NHS-E-144-017

**NEC Hyper Converged System
for VMware vSAN/CR2.0
初期システム構成のバックアップ／リストア
手順書**

2023 年 3 月 第 1.7 版

© 2018-2023 NEC Corporation

本書中の記載内容および図を作成者からの許可なしに、その全体または一部について
改変・複製することを禁じます。

その他、本書の免責事項は「免責事項」の項を参照ください。