

NEC Hyper Converged System for VMware vSAN/TR1.1

基本クラスタ スタートアップガイド



2021 年 9 月
第 4.0 版
日本電気株式会社

文書番号: NHS-E-045-040

目次

1	本ガイドについて	4
1.1	NEC Hyper Converged System	4
1.2	お問い合わせ先	4
1.3	用語の定義	5
1.4	関連ドキュメント	6
2	事前準備	7
2.1	ご用意いただくもの	7
3	受入確認	9
3.1	概要	9
3.2	構成品の確認	10
3.2.1	構成表の取り出し	10
3.2.2	構成表の確認	10
3.2.3	製品の外観確認	10
3.3	本製品の設置	11
3.4	ネットワーク装置への接続	11
3.5	電源の接続	11
3.6	クラスタノードの電源オン	12
3.7	管理ノードの電源オン	12
3.8	各クラスタノード、管理ノードの起動確認	13
3.9	Windows PC の準備	14
3.10	Windows PC から管理 VM に接続	15
3.11	NTP サーバの設定	17
3.12	vCenter Server 上での機器確認	19
3.13	管理ノードの確認	23
3.14	クラスタノードの確認	26
3.15	vSAN の健全性確認	28
3.16	vSphere の可用性設定	30
3.17	HCS Console 上での確認	32
4	DNS サーバの設定変更	36
4.1	DNS サーバのゾーン転送設定	36
4.1.1	お客様の DNS サーバの設定	36
4.1.2	管理 VM 上の DNS サーバの設定	40
4.1.3	お客様 DNS サーバでの同期作業	43
4.1.4	ゾーン転送設定の確認	44
4.2	DNS のフォワーダー設定	44
4.3	代替 DNS サーバ設定の確認	47
4.3.1	事前準備	47
5	ライセンス登録	58
5.1	vCenter Server、ESXi、vSAN ライセンスの登録	58
6	パスワード更新	64
6.1	概要	64
6.1.1	準備	64
6.2	vCenter Server の保守アカウントのパスワード更新	65
6.3	管理ノード、クラスタノード、vCenter Server、HCS Console のパスワード更新	67
6.4	管理ノードの管理 VM のパスワード更新	69
6.5	ESMPRO/ServerManager のパスワード更新	72
7	監視通報の変更	75
7.1	vCSA での監視通報	75
7.1.1	アラーム定義の無効化	75
7.1.2	アラーム定義の作成	78

7.1.3	SNMP 設定	107
7.2	ESMPRO での通報設定	110
8	注意制限事項	111
8.1	iLO Security について	111
付録 A)	ネットワーク結線	112
I.	サーバ LAN ポート	114
II.	HCS NW スイッチ(QX-S6648XT-6Q)	115
III.	ネットワークケーブルの接続	116

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 製品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。
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。
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 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。
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。
管理ネットワーク (管理 NW)	VMware ESXi の管理、vSAN、vMotion、iLO、管理 VM との通信を行うお客様の管理ネットワーク。
業務ネットワーク (業務 NW)	業務 VM との通信を行うお客様の業務ネットワーク。
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。ネットワーク経由でもローカルコンソールにアクセスできます。
HCS NW スイッチ	管理 NW に接続されている、10G スイッチ。

1.4 関連ドキュメント

本書に関連するドキュメントは以下の通りです。

名称	説明	備考
NEC Hyper Converged System スターアップガイド	NEC HCS 製品の箱を開けてから利用するまでの手順を説明	本書
NEC Hyper Converged System 運用ガイド(定常運用編)	NEC HCS 製品の定常運用時の利用方法について記載	
NEC Hyper Converged System 運用ガイド(障害復旧編)	NEC HCS 製品の障害発生時の対応方法について記載	
NEC Hyper Converged System 運用ガイド(増設編)	NEC HCS 製品の各種増設時の対応方法について記載	
NEC Hyper Converged System 製品組み立て仕様書(SG 仕様書)	NEC HCS 製品の各種設定および構築情報等記載	
NEC Hyper Converged System 構成品表	NEC HCS 製品の構成品について記載	
PP サポート仕様書	NEC HCS の PP サポート情報について記載	

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 7 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 シリアル番号一覧表 (本製品に同封、以下構成品表)
 - NEC Hyper Converged System 製品組み立て仕様書(SG 仕様書)
(本製品に同封、以下 SG 仕様書)
 - NEC Hyper Converged System 初期パスワード通知書 (本製品に同封)
 - 本書 (NEC Hyper Converged System スタートアップガイド、本製品に同封)
- 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)
ユーザーズガイドは下記より入手できます。
<https://www.support.nec.co.jp/PSHome.aspx>
 - ハードウェア
 - 型番・モデル名から探す
 - モデル名(R120h-1M)を入力し、"モデル名で検索"をクリック
 - 検索結果より"R120h-1M (3rd-Gen)"を選択
 - "製品マニュアル"を選択
 - 検索結果よりユーザーズガイドを選択
 - HCS NW スイッチの製品マニュアル(インストールマニュアル、製品添付 CD-ROM)
- その他
 - 下記要件を満たす Windows PC (Windows10, 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)
 - ◇ VMware 社による vSphere Client のソフトウェア要件(サポート対象の Web ブラウザが必要)
<https://docs.vmware.com/jp/VMware-vSphere/6.7/com.vmware.vcenter.install.doc/GUID-EC80836B-BE02-4CB2-9F40-15928AFB6E20.html>

- (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 v2.0.1 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 v2.0.1 ユーザーズガイド(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)
 - ディスプレイ、キーボード (LCD コンソールユニット等も可)

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

本章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 16 点の実施をお願いいたします。なお、本書に掲載されている図は実際のイメージとは異なる場合がありますので、予めご了承ください。

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. クラスタノードの電源オン
6. 管理ノードの電源オン
7. 各クラスタノード、管理ノードの起動確認
8. Windows PC の準備
9. Windows PC から管理 VM に接続
10. NTP サーバの設定
11. vCenter Server 上での機器確認
12. 管理ノードの確認
13. クラスタノードの確認
14. vSAN の健全性確認
15. vSphere の可用性設定
16. HCS Console 上での確認

3.2 構成品の確認

3.2.1 構成表の取り出し

本製品の構成物を示す「NEC Hyper Converged System シリアル番号一覧表(以下構成表)」は、NEC Hyper Converged System クラスタノードの梱包箱の内側に貼り付けられている封筒内に納品されます。構成表を取り出してください。

3.2.2 構成表の確認

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 シリアル番号一覧表(構成表)」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。

- 構成表は NEC Hyper Converged System クラスタノード#1 の梱包箱に本書と共に同梱されています。
- 梱包箱には機器 ID が記載されたラベルが貼り付けられています。構成表の機器 ID に対応した梱包箱が揃っ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 節の構成表には記載されておりません。同時にご注文いただいた NEC Hyper Converged System 以外の製品は、納品書と納品物の梱包箱の数量、型番が一致していることを確認してください。

3.2.3 製品の外観確認

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

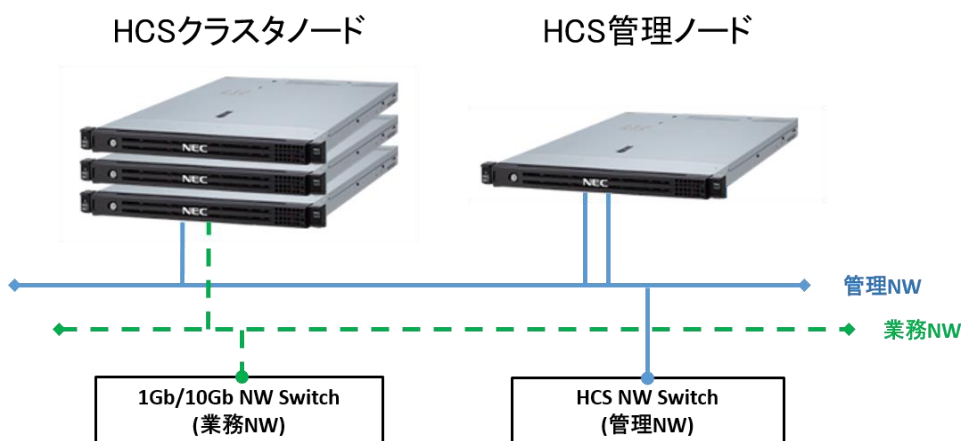
3.3 本製品の設置

本製品を使用する前に、19 インチラックなど安全に固定できる器具に搭載し、電源を接続する必要があります。本製品に同封されるスタートアップガイド、または NEC Web サイトから入手できる HCS ベースモデル (R120h-1M) の製品マニュアル(ユーザーズガイド一式)、HCS NW スイッチ添付 CD-ROM の製品マニュアル(インсталレーションマニュアル)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、あらかじめお客様ネットワークの設計や設定、構築を完了いただき、本書の「付録 A) ネットワーク結線」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。

接続例



3.5 電源の接続

すべての製品の設置が完了後、電源ケーブルを接続します。クラスタノード、管理ノード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。

HCS NW スイッチに同封または Web サイトから入手できるマニュアルを参照し、電源ケーブルを AC 電源に正しく接続してください。電源投入後 SYS LED が緑色で点灯することを確認します。

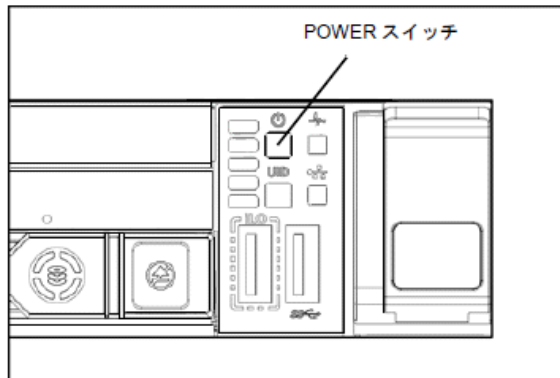
各 NEC Hyper Converged System 管理ノード、クラスタノードに同封されるスタートアップガイド、または NEC Web サイトから入手できる HCS ベースモデル(R120h-1M)の製品マニュアル(ユーザーズガイド)を元に、電源ケーブルを AC 電源に正しく接続して下さい。

3.6 クラスタノードの電源オン

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。

電源をオンにする方法は、以下を参照ください。

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

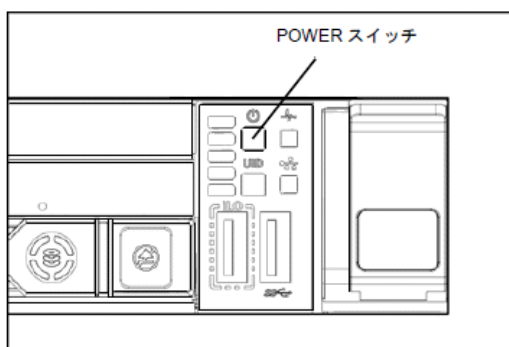


3.7 管理ノードの電源オン

NEC Hyper Converged System 管理ノード(サーバ)の電源をオンにします。

電源をオンにする方法は、以下を参照ください。

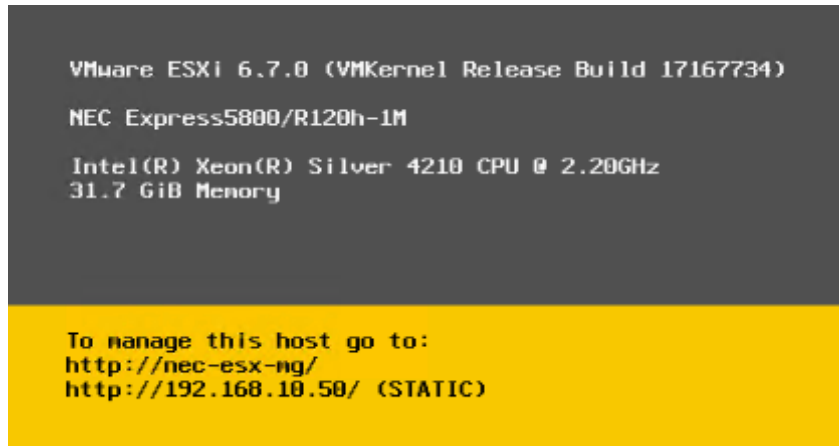
以下の図の POWER スイッチを押下して、電源オンしてください。
正しく電源オンされると、ランプが緑色に点灯します。



3.8 各クラスタノード、管理ノードの起動確認

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

各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。



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(管理ノードの電源オンから 10~20 分程度)を待ってください。

3.9 Windows PC の準備

Windows PC を、管理ネットワークに接続します。

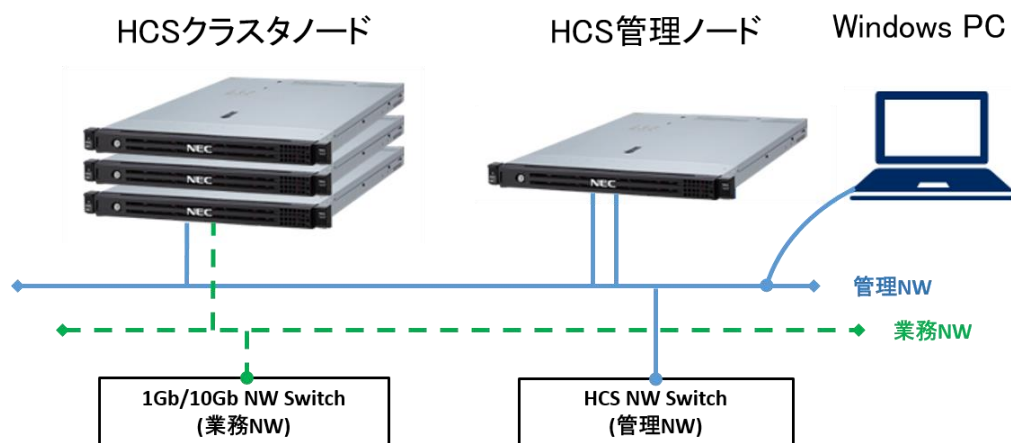
手順実施に必要なパラメータ

ドキュメント	項目	パラメータ/値 (メモ用)
SG 仕様書 [Startup]シート	管理 VM - 管理 NW - IP アドレス	
	管理 VM - 管理 NW - サブネットマスク	
-	Windows PC に設定する IP アドレス	

手順

1. Windows PC のネットワーク設定を、管理ネットワーク上の管理 VM に接続できるよう、変更します。
2. Windows PC を管理ネットワークに接続してください。

接続例



《注意》

Windows PC に設定する IP アドレスは、本製品(※)や管理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。

※HCS では、お客様の管理ネットワークで「管理 VM - 管理 NW - IP アドレス」の IP アドレスを使用します。

3.10 Windows PC から管理 VM に接続

Windows PC から管理 VM に接続します。

手順実施に必要なパラメータ

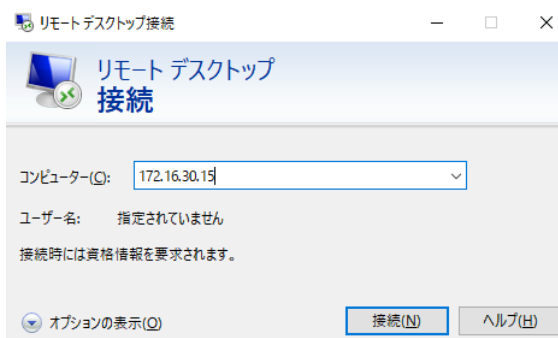
ドキュメント	項目	パラメータ/値 (メモ用)
初期パスワード通知書	管理 VM - Administrator パスワード	
	管理ノード - ESXi の root パスワード	
SG 仕様書 [Startup]シート	管理 VM - 管理 NW - IP アドレス	

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、「管理 VM - 管理 NW - 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: 「管理 VM - 管理 NW - IP アドレス」
- アカウント名: 「administrator」
- パスワード: 「管理 VM - Administrator 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ます。(下記図)

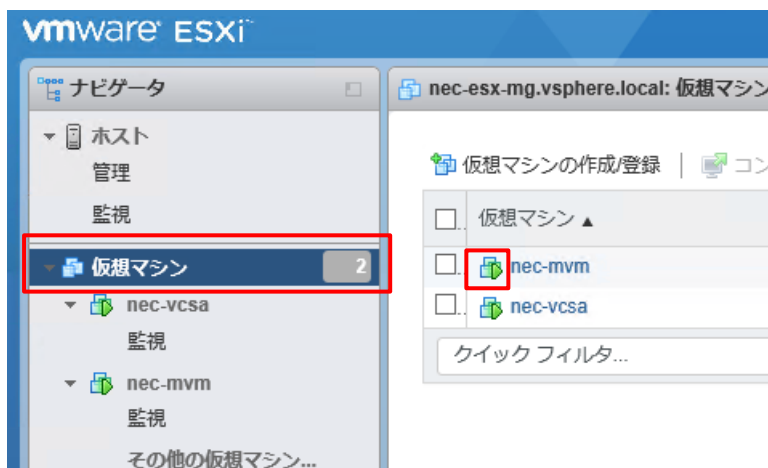


管理 VM にリモートデスクトップ接続ができない場合は、下記を再確認してください。下記を確認しても接続できない場合は、お手数をおかけしますが 1.2 節の問い合わせ窓口までご連絡ください。

- 電源: 管理ノードの電源がオンになっていることを確認後、ディスプレイを接続して 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、「管理 VM - 管理 NW - 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 Internet Explorer を起動し、VMware Host Client で管理ノードの緊急 NW にアクセスし、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。

※Internet Explorer で「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。」と表示される場合は、「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、続行します。

- URL:「https://<管理ノード - 管理 NW - IP アドレス>/ui」
- ユーザー名:「root」
- パスワード:「管理ノード - ESXi の root パスワード」
- 確認手順:Host Client が表示されたら、「仮想マシン」をクリックし、「nec-mvm」のアイコンが  である事を確認します。(※ アイコンが  なら、電源はオンになっています。)
※「仮想マシン」が表示されない場合は、「ナビゲータ」をクリックしてください。



3.11 NTP サーバの設定

管理 VM からアクセスできる上位の NTP サーバとの時刻同期設定を行います。

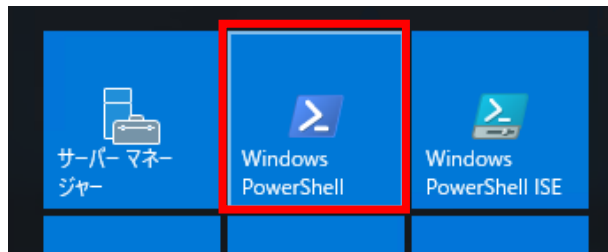
上位の NTP サーバがない場合は、本章の作業は不要です。

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)
-	NTP サーバ - IP アドレス	

手順

1. 管理 VM のスタートメニューから「Windows PowerShell」をクリックし、PowerShell を起動します。



2. 下記のコマンドを実行し、参照先の NTP サーバの設定を行います。

```
> w32tm /config /manualpeerlist:<NTP サーバ - IP アドレス> /syncfromflags:manual
```

```
PS C:\Users\Administrator> w32tm /config /manualpeerlist:192.168.1.252 /syncfromflags:manual
コマンドは正しく完了しました。
PS C:\Users\Administrator>
```

3. 下記のコマンドを実行し、設定の反映を行います。

```
> w32tm /config /update
```

```
PS C:\Users\Administrator> w32tm /config /update
コマンドは正しく完了しました。
PS C:\Users\Administrator>
```

4. 下記のコマンドを実行し、表示される「NtpServer」の項目が手順 2 で設定した NTP サーバになっていることを確認します。

```
> w32tm /query /configuration
```

```
PS C:\Users\Administrator> w32tm /query /configuration
[構成]
EventLogFlags: 2 (ローカル)
AnnounceFlags: 5 (ポリシー)
TimeJumpAuditOffset: 28800 (ローカル)
MinPollInterval: 6 (ローカル)
MaxPollInterval: 10 (ローカル)
MaxNegPhaseCorrection: 54000 (ローカル)
MaxPosPhaseCorrection: 54000 (ローカル)
MaxAllowedPhaseOffset: 1 (ローカル)

FrequencyCorrectRate: 4 (ローカル)
PollAdjustFactor: 5 (ローカル)
LargePhaseOffset: 50000000 (ローカル)
SpikeWatchPeriod: 900 (ローカル)
LocalClockDispersion: 10 (ローカル)
HoldPeriod: 5 (ローカル)
PhaseCorrectRate: 1 (ローカル)
UpdateInterval: 100 (ローカル)

[タイム プロバイダー]
NtpClient (ローカル)
DllName: C:\Windows\System32\w32time.dll (ローカル)
Enabled: 1 (ローカル)
InputProvider: 1 (ローカル)
AllowNonstandardModeCombinations: 1 (ローカル)
ResolvePeerBackoffMinutes: 15 (ローカル)
ResolvePeerBackoffMaxTimes: 7 (ローカル)
CompatibilityFlags: 2147483648 (ローカル)
EventLogFlags: 1 (ローカル)
LargeSampleSkew: 3 (ローカル)
SpecialPollInterval: 86400 (ローカル)
Type: NTP (ローカル)
NtpServer: 192.168.1.252 (ローカル)

NtpServer (ローカル)
DllName: C:\Windows\System32\w32time.dll (ローカル)
Enabled: 1 (ローカル)
InputProvider: 0 (ローカル)
AllowNonstandardModeCombinations: 1 (ローカル)

VMCTimeProvider (ローカル)
DllName: C:\Windows\System32\vmctimeprovider.dll (ローカル)
Enabled: 1 (ローカル)
InputProvider: 1 (ローカル)

PS C:\Users\Administrator>
```

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

3.12 vCenter Server 上での機器確認

vCenter Server 上で、vSAN クラスタ、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。

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	vCSA – SSO administrator パスワード	

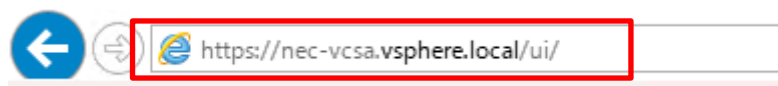
手順

1. 管理 VM より Internet Explorer を起動し、下記の画面が表示されたら、「お勧めのセキュリティ、プライバシー、互換性の設定を使う」を選択した状態で、「OK」をクリックします。

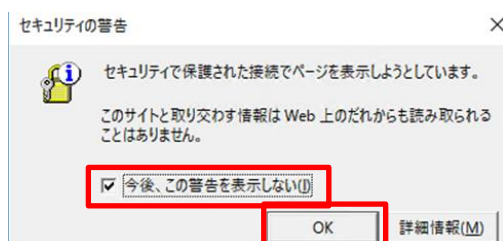


2. 下記の URL を入力し、VMware vSphere Client で vCenter Server に接続します。

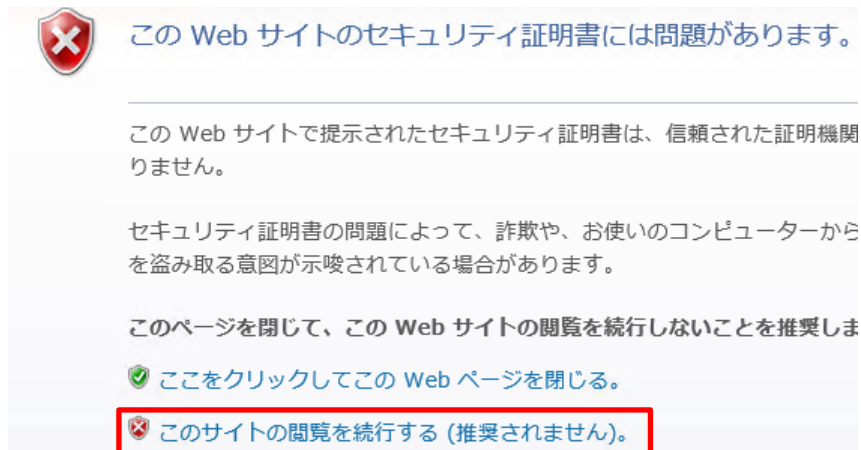
- URL: 「https://nec-vcsa.vsphere.local/ui」



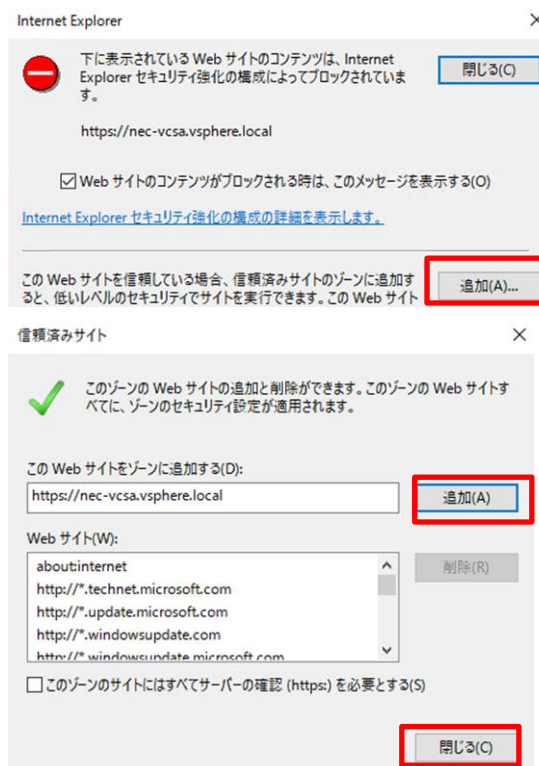
※1 「セキュリティの警告」が表示されたら、「今後、この警告を表示しない」にチェックして、「OK」をクリックし続行します。



※2 「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。」と表示される場合は、「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、続行します。



※3 「Internet Explorer セキュリティ強化の構成」によってブロックされた場合は、信頼済みサイトのゾーンに追加して、続行します。



※4 「このページは表示できません」が表示された場合は、ブラウザをリロードして続行します。



このページは表示できません

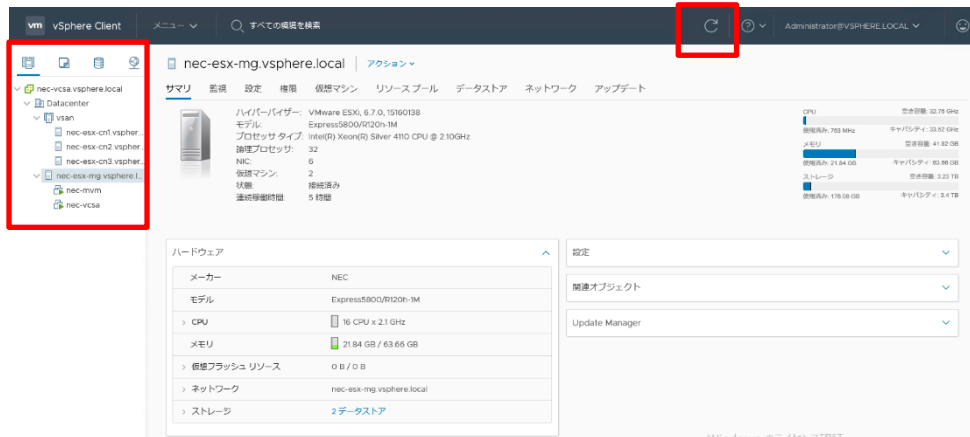
[詳細設定] で TLS 1.0、TLS 1.1、TLS 1.2 を有効にして、もう一度 **https://nec-vcsa.vsphere.local** に接続し、アカウントを入力し、ログインを試みます。発生する場合は、

3. 接続が成功すると、VMware vSphere Client ログイン画面が表示されます(下記図)。
アカウント情報を入力し、ログインします。
接続に失敗した場合、「3.10 Windows PC から管理 VM に接続」の手順2の接続できなかった場合と同様の手順で、「nec-vcsa」の電源がオンになっていることを確認してください。(電源オン後、接続できるまで 5～10 分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」



4. VMware vSphere Client のメイン画面のリフレッシュボタン(画面右上)を押し、ステータスを更新してください。その後ナビゲータ(画面左)を展開すると、Datacenter - クラスタ(vSAN) - クラスターノード(nec-esx-cnN)、管理ノード(nec-esx-mg)が表示されることを確認してください。(※ クラスターノードの N は数字です)
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。



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 管理ノードの確認

VMware vSphere Client 上で、管理ノードの情報を確認します。

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)
SG 仕様書 [Startup]シート	管理ノード - CPU	
	管理ノード - メモリ容量	
	管理ノード - ディスク容量(1)	
	管理ノード - ディスク容量(2)	

手順

1. 管理ノード「nec-esx-mg.vsphere.local」をクリックし、「サマリ」を選択し、「プロセッサタイプ」が「管理ノード - CPU」であること、「メモリ」が約「管理ノード - メモリ容量」(誤差 2%以内)であることを確認します。
(「メモリ」が表示されていない場合は「ハードウェア」をクリックしてください。)

また、電源、ファン、NIC 等に関する警告表示がされず、障害が発生していないことを確認します。

The screenshot shows the VMware vSphere Client interface. On the left, the inventory tree shows the path: Datacenter > vsan > nec-esx-mg.vsphere.local, which is highlighted with a red box. The main pane shows the 'Summary' tab for this host, also highlighted with a red box. The summary information includes:

- ハイパーバイザー: VMware ESXi, 6.7.0, 17167734
- モデル: Express5800/R120h-1M
- プロセッサタイプ: Intel(R) Xeon(R) Silver 4110 CPU @ 2.10GHz (highlighted with a red box)
- 論理プロセッサ: 32
- NIC: 6
- 仮想マシン: 2
- 状態: 接続済み
- 連続稼働時間: 5 時間

Below the summary, the 'Hardware' tab is selected and highlighted with a red box. It displays the following details:

- メーカー: NEC
- モデル: Express5800/R120h-1M
- CPU: 16 CPU x 2.1 GHz
- メモリ: 20.39 GB / 31.82 GB (highlighted with a red box)
- 仮想フラッシュ リソース: 0 B / 0 B
- ネットワーク: nec-esx-mg.vsphere.local
- ストレージ: 2 データストア

《参考》 サマリに警告表示が表示されている場合。

▽電源に障害が発生している場合

サマリ

監視

設定

権限

仮想マシン

データストア

ネットワーク

アップデート



ハイパーバイザー: VMware ESXi, 6.7.0, 17167734

モデル: Express5800/R120h-1M

プロセッサタイプ: Intel(R) Xeon(R) Gold 5218 CPU @ 2.30GHz

論理プロセッサ: 32

NIC: 8

仮想マシン: 0

状態: 接続済み

連続稼働時間: 75 分



① ホストのハードウェアの電源状態

① ほかのホストのハードウェア オブジェクトのステータス

▽ファンに障害が発生している場合

サマリ

監視

設定

権限

仮想マシン

データストア

ネットワーク

アップデート



ハイパーバイザー: VMware ESXi, 6.7.0, 17167734

モデル: Express5800/R120h-1M

プロセッサタイプ: Intel(R) Xeon(R) Gold 5218 CPU @ 2.30GHz

論理プロセッサ: 32

NIC: 8

仮想マシン: 0

状態: 接続済み

連続稼働時間: 2 時間



① ホストのハードウェア ファン ステータス

① ほかのホストのハードウェア オブジェクトのステータス

▽NICに障害が発生している場合

サマリ

監視

設定

権限

仮想マシン

データストア

ネットワーク

アップデート



ハイパーバイザー: VMware ESXi, 6.7.0, 17167734

モデル: Express5800/R120h-1M

プロセッサタイプ: Intel(R) Xeon(R) Gold 5218 CPU @ 2.30GHz

論理プロセッサ: 32

NIC: 8

仮想マシン: 0

状態: 接続済み

連続稼働時間: 5 時間



① ほかのホストのハードウェア オブジェクトのステータス

① ネットワーク アップリンクの冗長性が失われました

2. 「設定」をクリックし、「ストレージデバイス」を選択し、「キャパシティ」に「管理ノード – ディスク容量(1)」、「管理ノード – ディスク容量(2)」があることを確認します。

nec-esx-mg.vsphere.local | アクション ▾

サマリ 監視 **設定** 権限 仮想マシン リソース プール データストア ネットワーク アップデー

▼ ストレージ

- ストレージ アダプタ
- ストレージ デバイス**
- ホスト キャッシュの...
- プロトコル エンドポ...
- I/O フィルタ

▼ ネットワーク

- 仮想スイッチ
- VMkernel アダプタ

ストレージ デバイス

更新 | 添付 | 分離 | 名前の変更...

名前	L...	タイプ	キャパシティ
Local HPE RAID Ctlr (mpx.vmhba1:C2:T1088:L1)	1	array co...	
Local ATA Disk (t10.ATA_____VR000150GWE...	0	disk	223.57 GB
Local HPE Disk (naa.600508b1001c1f4ed34a71...	1	disk	1.64 TB
Local hp CD-ROM (mpx.vmhba0:C0:T3:L0)	0	cdrom	

3. 「物理アダプタ」をクリックし、スイッチに「vSwitchN」(※)が表示されており、実際の速度が「切断」になっているデバイスがないことを確認してください。

(※ スイッチの N は数字です。)

サマリ 監視 **設定** 権限 仮想マシン リソース プール データストア ネットワーク アップデー

▼ ストレージ

- ストレージ アダプタ
- ストレージ デバイス
- ホスト キャッシュの...
- プロトコル エンドポ...
- I/O フィルタ

▼ ネットワーク

- 仮想スイッチ
- VMkernel アダプタ
- 物理アダプタ**
- TCP/IP 設定

物理アダプタ

ネットワークの追加... | 更新 | 編集...

デバイス	実際の速度	設定済み速度	スイッチ
vmnic0	1 Gbit/s	オート ネゴシエーショ...	vSwitch2
vmnic1	1 Gbit/s	オート ネゴシエーショ...	vSwitch2
vmnic2	1 Gbit/s	オート ネゴシエーショ...	vSwitch1
vmnic3	1 Gbit/s	オート ネゴシエーショ...	vSwitch1
vmnic4	10 Gbit/s	オート ネゴシエーショ...	vSwitch0
vmnic5	10 Gbit/s	オート ネゴシエーショ...	vSwitch0

3.14 クラスタノードの確認

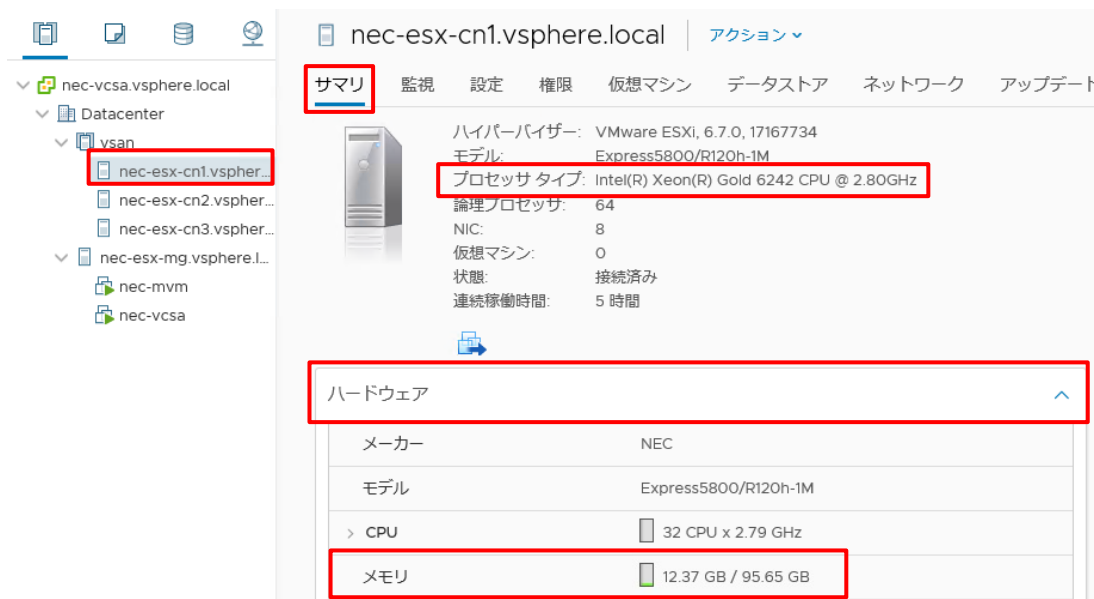
VMware vSphere Client 上で、クラスタノードの情報を確認します。

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)
SG 仕様書 [Startup]シート	クラスタノード - CPU	
	クラスタノード - メモリ容量	
	クラスタノード - ディスク容量(1)	
	クラスタノード - ディスク容量(2)	
	クラスタノード - ディスク容量(2)の数	
	クラスタノード - ディスク容量(3)	
	クラスタノード - ディスク容量(3)の数	

手順

1. クラスタノード「nec-esx-cnN.vsphere.local」(※)をクリックし、「サマリ」を選択し、「プロセッサタイプ」が「クラスタノード - CPU」であること、「メモリ」が約「クラスタノード - メモリ容量」(誤差 2%以内)であることを確認します(※ クラスタノードの N は数字です)。
(「メモリ」が表示されていない場合は「ハードウェア」をクリックしてください。)
また、電源、ファン、NIC 等に関する警告表示がされず、障害が発生していないことを確認します。



2. 「設定」をクリックし、「ストレージデバイス」を選択し、「キャパシティ」に「クラスタノード – ディスク容量(1)」が1つ、「クラスタノード – ディスク容量(2)」が「クラスタノード – ディスク容量(2)の数」、「クラスタノード – ディスク容量(3)」が「クラスタノード – ディスク容量(3)の数」あることを確認します。

Storage Devices Table:

名前	L...	タイプ	キャパシティ	データストア
Local HP Disk (naa.5000c500bd000ed7)	0	disk	2.18 TB	vsanDat...
Local ATA Disk (t10.ATA_____MR000240GWFLU_____)	0	disk	223.57 GB	datastor...
Local HPE RAID Ctr (mpx.vmhba0:C2:T1088:L0)	0	array c...		未消費
Local HPE CD-ROM (mpx.vmhba0:C0:T3:L0)	0	cdrom		未消費
Local HP Disk (naa.5000c500bd29082f)	0	disk	2.18 TB	vsanDat...
Local HP Disk (naa.5000c500bd29965f)	0	disk	2.18 TB	vsanDat...
Local HP Disk (naa.58ce38ee208e7751)	0	disk	372.61 GB	vsanDat...

3. 「物理アダプタ」をクリックし、スイッチに「vSwitchN」(※)が表示されており、実際の速度が「切断」になっているデバイスがないことを確認してください。

(※ スwitchの N は数字です。)

Physical Adapters Table:

デバイス	実際の速度	設定済み速度	スイッチ
vmnic0	1 Gbit/s	オート ネゴシエーショ...	vSwitch2
vmnic1	1 Gbit/s	オート ネゴシエーショ...	vSwitch2
vmnic2	切断	オート ネゴシエーショ...	—
vmnic3	切断	オート ネゴシエーショ...	—
vmnic4	10 Gbit/s	オート ネゴシエーショ...	vSwitch0
vmnic5	1 Gbit/s	オート ネゴシエーショ...	vSwitch1
vmnic6	10 Gbit/s	オート ネゴシエーショ...	vSwitch0
vmnic7	1 Gbit/s	オート ネゴシエーショ...	vSwitch1

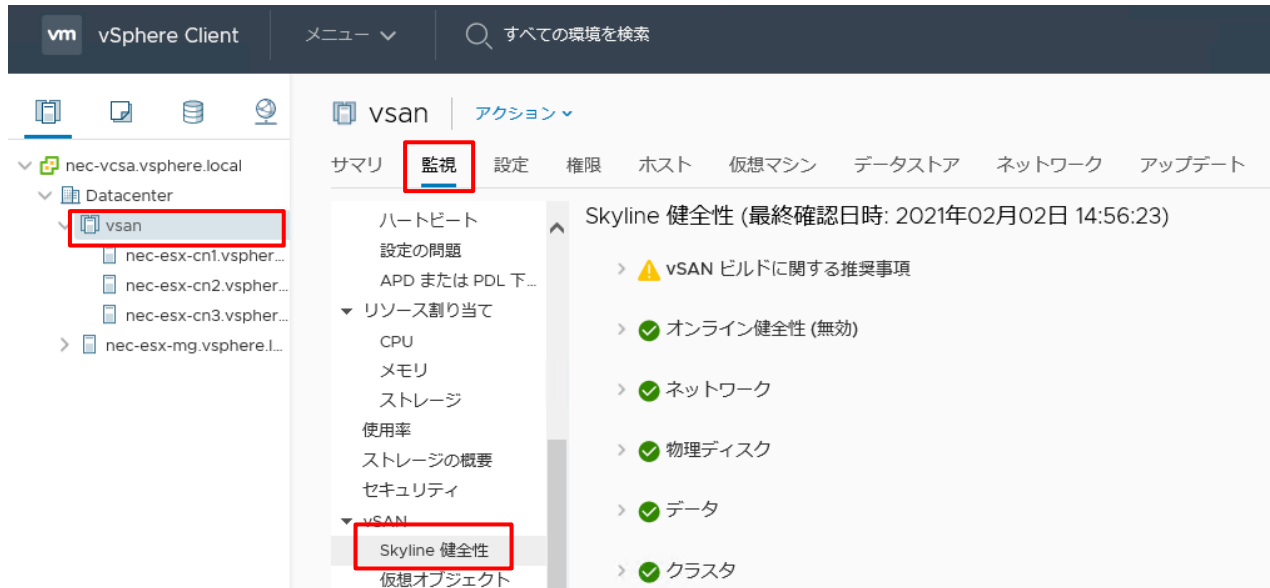
4. 手順 1~3 をすべてのクラスタノードに対して実施します。

3.15 vSAN の健全性確認

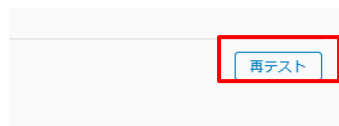
vSAN クラスタの状態を確認し、健全性ツリーにエラーがないことを確認します。

手順

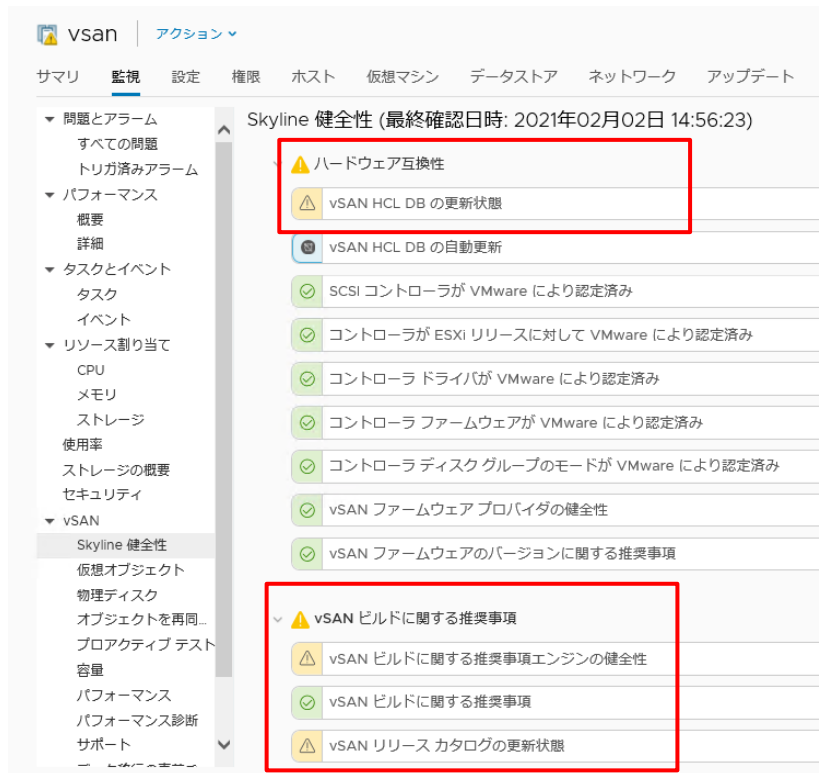
1. vSAN クラスタ「vsan」をクリックし、「監視」、「Skyline 健全性」の順で選択します。



2. 画面右上の「再テスト」をクリックします。



3. 「再テスト」実行後、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 「ハードウェアの互換性」配下の「vSAN HCL DBの更新状態」と「vSAN ビルドに関する推奨事項」配下の「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」の「警告」については無視しても問題ありません。



※2 vSAN クラスタ「vsan」の「サマリ」に出ている警告が、※1 の「警告」である場合は無視しても問題ありません。

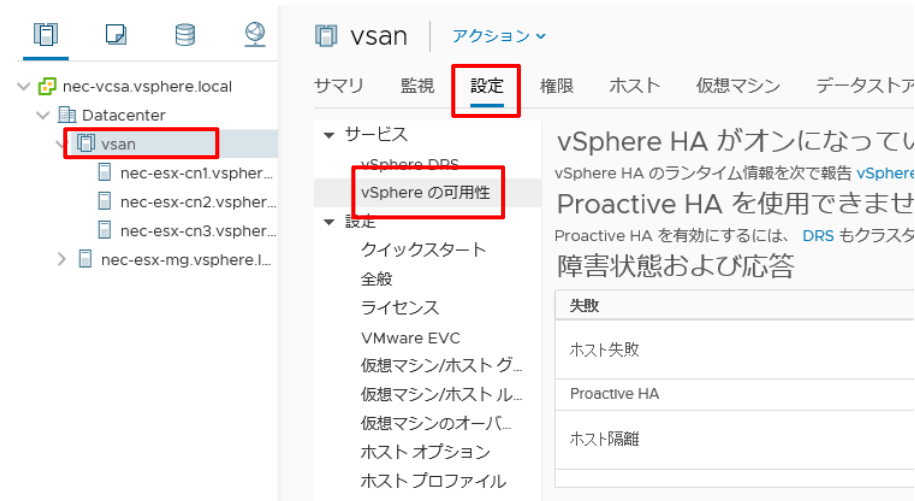


3.16 vSphere の可用性設定

vSAN クラスタの vSphere の可用性を設定します。

手順

1. vSAN クラスタ「vsan」をクリックし、「設定」、「vSphere の可用性」の順に選択します。



2. 画面右上の「編集」をクリックします。



3. 「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。



4. 「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

3.17 HCS Console 上での確認

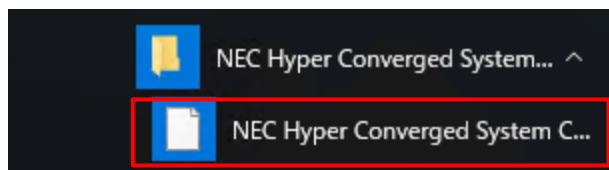
HCS Console 上で、vSAN クラスタ、クラスタノード・管理ノードが正しく表示されていることを確認します。

手順実施に必要なパラメータ

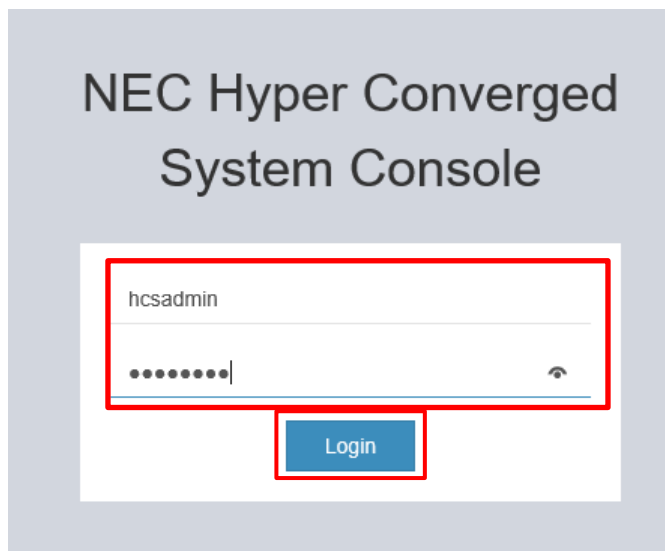
ドキュメント	項目	パラメータ/値 (メモ用)
初期パスワード通知書	NEC HCS Console - 管理パスワード	

手順

1. 管理 VM のスタートメニューから「NEC Hyper Converged System Console」をクリックし、HCS Console を起動します。



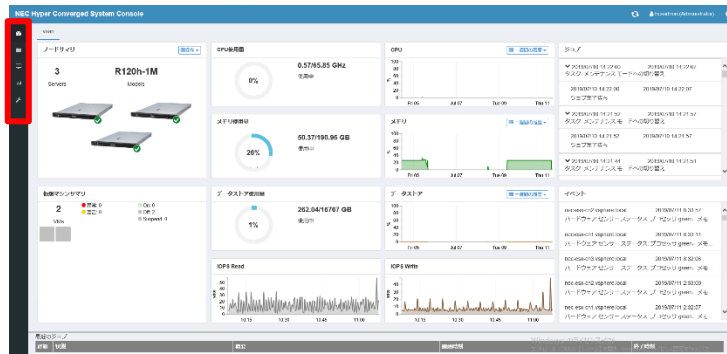
2. HCS Console を起動すると、HCS Console のログイン画面が表示されます。(下記図)
アカウント情報を入力し、ログインします。
 - UserName: 「hcsadmin」
 - Password: 「NEC HCS Console - 管理パスワード」



注意事項

- 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. ログインに成功すると、ポータル画面が表示されます。



アイコン	名称
	ダッシュボード
	ノード
	仮想マシン
	監視
	設定

※左側の枠内のアイコンの各名称は右の表の通りです。

4. 「ダッシュボード」をクリックし、ノードサマリに表示されたクラスタノードの台数を確認します。



注意事項

- 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。

5. 「ノード」をクリックし、ノードの「状態」が「正常」、「電源」が「On」であることを確認します。

NEC Hyper Converged System Console

Show 5 entries

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

Showing 1 to 4 of 4 entries

項目が選択されていません

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。

6. 「仮想マシン」をクリックし、仮想マシンの「状態」が「正常」、「電源」が「On」であることを確認します。

NEC Hyper Converged System Console

Show 5 entries

名前	状態	電源	ノード
nec-mvm	正常	On	nec-esx-mg.vsphere.local
nec-vcsa	正常	On	nec-esx-mg.vsphere.local

Showing 1 to 2 of 2 entries

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。

7. 「監視」をクリックし、ジョブ・イベント・ログ情報を表示できることを確認します。

※製品出荷直後の場合、ジョブとログに何も表示されない場合があります。

NEC Hyper Converged System Console

ジョブ イベント ログ

	詳細	状態	メッセージ
▼	詳細	正常	ジョブの実行 (マネージャ配下の収集)
		正常	指定されたマネージャ配下の収集を実行 (VMware vCenter Serv
▼	詳細	正常	ジョブの実行 (マシンのメンテナンスステータスを切替)
		正常	マシンのメンテナンスステータスを変更
▼	詳細	正常	ジョブの実行 (マシンのメンテナンスステータスを切替)
		正常	マシンのメンテナンスステータスを変更
▼	詳細	正常	ジョブの実行 (マネージャ配下の収集)
		正常	指定されたマネージャ配下の収集を実行 (VMware vCenter Serv
▼	詳細	正常	ジョブの実行 (マシンのメンテナンスステータスを切替)
		正常	マシンのメンテナンスステータスを変更

HCS Console のジョブ・イベント・ログ情報が、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。

8. 「設定」をクリックし、「ノード設定」を選択し、BMC アカウントが「(接続可能)」であることを確認します。



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 DNS サーバの設定変更

お客様 DNS サーバへのゾーン転送設定と、管理 VM 上の DNS サーバにフォワーダー設定を実施する場合の手順を記載しています。

4.1 DNS サーバのゾーン転送設定

本項の操作は、お客様の DNS サーバも Windows2016 上に構築されていることを前提に記載しています。Windows2016 の DNS サーバと異なる場合は、適宜読み替えて設定してください。

また、本項は管理 VM 上の DNS の前方参照ゾーン(vsphere.local)のゾーン転送設定について記載しています。他のゾーンも転送が必要な場合は、追加で設定してください。

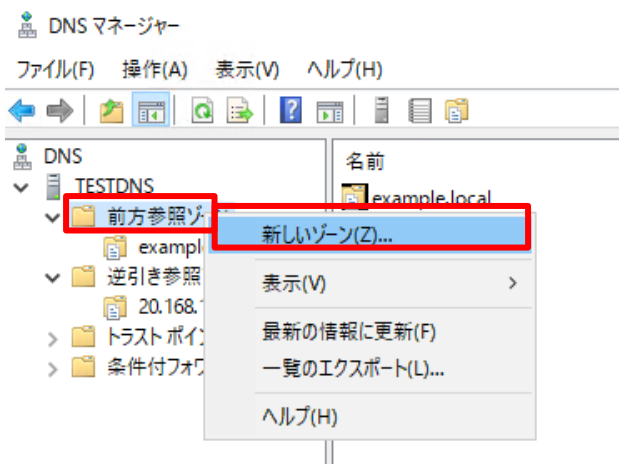
手順実施に必要なパラメータ

ドキュメント	項目	パラメータ/値 (メモ用)
SG 仕様書 [Startup]シート	セカンダリ DNS サーバ - IP アドレス	
SG 仕様書 [Startup]シート	管理 VM - 管理 NW - IP アドレス	

4.1.1 お客様の DNS サーバの設定

お客様の DNS サーバでゾーン転送のためにセカンダリゾーンを作成します。

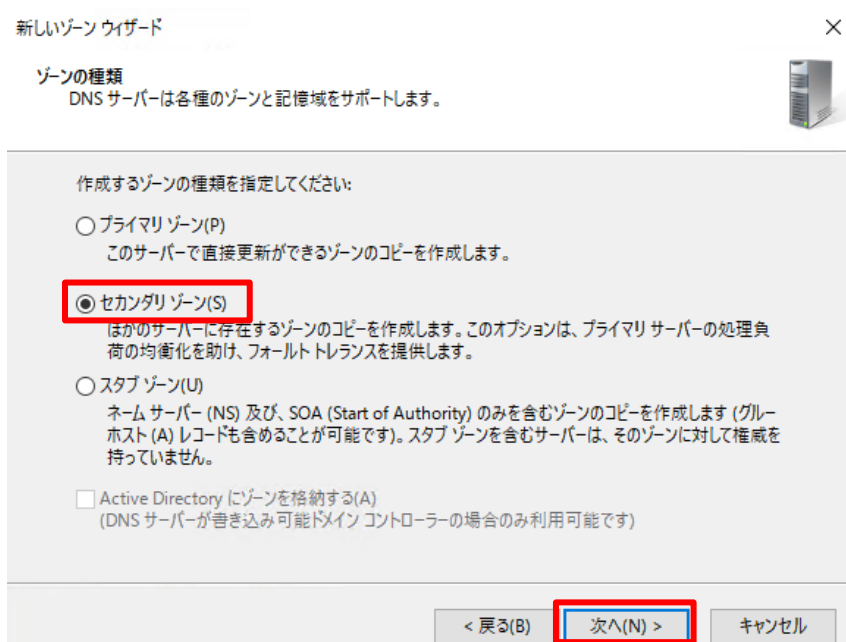
1. サーバマネージャーの画面上部の[ツール]をクリックし、表示されたメニューから[DNS]をクリックして DNS マネージャを起動します。
2. "お客様の DNS サーバ名" - "前方参照ゾーン" を右クリックし、[新しいゾーン]をクリックします。



3. 「新しいゾーン ウィザードの開始」が表示されるので、[次へ]をクリックします。



4. 「ゾーンの種類」画面が表示されますので、[セカンダリゾーン]を選択し、[次へ]をクリックします。



5. 「ゾーン名」の画面が表示されますので、[ゾーン名] に "vsphere.local" を入力し[次へ]をクリックします。

新しいゾーン ウィザード

ゾーン名
新しいゾーンの名前を指定してください。

ゾーン名は、このサーバーが権限を持っている DNS 名前空間の一部を指定します。組織のドメイン名 (例: microsoft.com) やドメイン名の一部 (例: newzone.microsoft.com) があります。ゾーン名は DNS サーバーの名前ではありません。

ゾーン名 (Z):
vsphere.local

< 戻る(B) **次へ(N) >** キャンセル

6. 「マスターDNS サーバー」の画面が表示されますので、「管理 VM - 管理 NW - IP アドレス」を入力し[次へ]をクリックします。

新しいゾーン ウィザード

マスター DNS サーバー
セカンダリゾーンは 1 つ以上の DNS サーバーからコピーされています。

ゾーンのコピー元の DNS サーバーを指定してください。下の一覧にある順で処理されます。

マスター サーバー:

IP アドレス	サーバー FQDN	検証済み
192.168.10.51		

削除(D) 上へ(U) 下へ(O)

< 戻る(B) **次へ(N) >** キャンセル

7. 「新しいゾーンウィザードの完了」の画面が表示されますので、[完了]をクリックします。

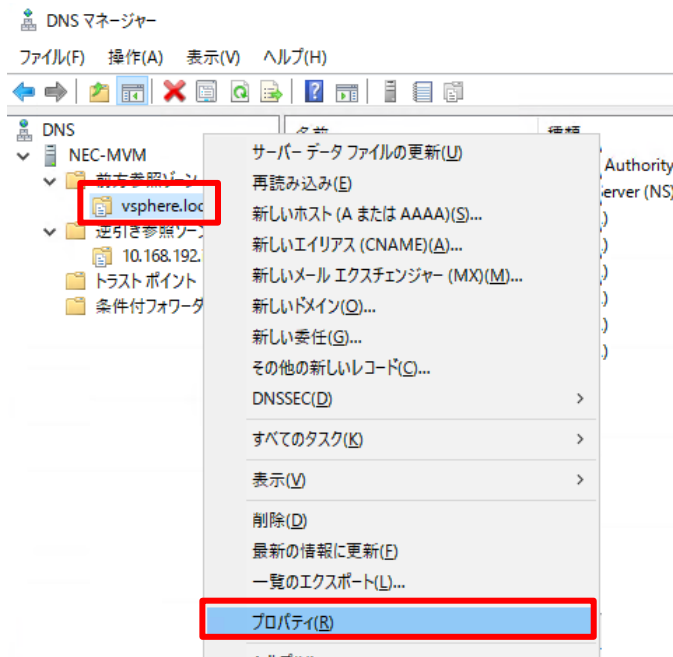


以上でお客様の DNS サーバ設定は完了となります。引き続き 4.1.2 項の操作を行ってください。

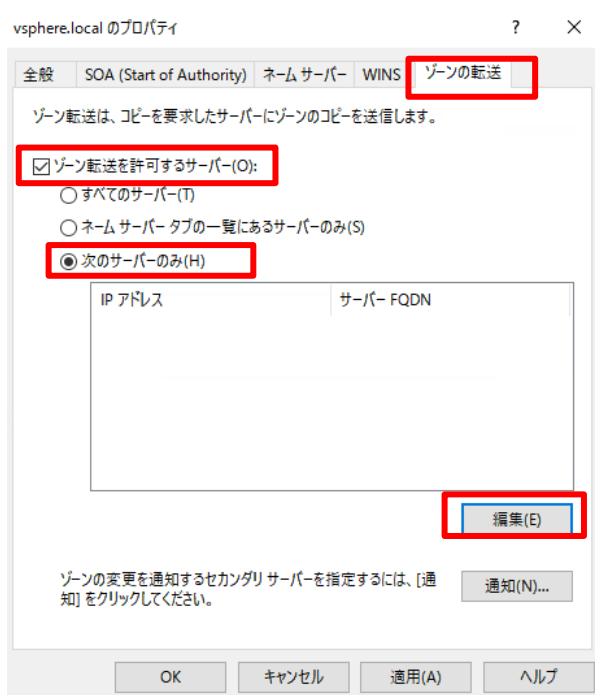
4.1.2 管理 VM 上の DNS サーバの設定

管理 VM 上の DNS サーバでゾーン転送を許可するサーバの設定を実施します。

1. サーバマネージャの画面上部の[ツール]をクリックし、表示されたメニューから[DNS]をクリックして DNS マネージャを起動し、"NEC-MVM" - "前方参照ゾーン" の下の "vsphere.local" を右クリックし、[プロパティ]を選択します。



2. 「vsphere.local のプロパティ」画面が表示されますので、「ゾーンの転送」タブを選択します。
[ゾーン転送を許可するサーバ]にチェックを入れ、[次のサーバーのみ]を選択し、[編集]をクリックします。



3. 「ゾーン転送を許可する」画面が表示されますので、[ここをクリックして IP アドレスまたは DNS 名を追加してください] をクリックして、「セカンダリ DNS サーバ - IP アドレス」を入力し、[OK]をクリックします。

ゾーン転送を許可する

DNS ゾーン(Z):
vsphere.local

セカンダリ サーバの IP アドレス(S):

IP アドレス	サーバ FQDN	検証済み
<ここをクリックして IP アドレスまたは DNS 名を追加してください>		
✖ 192.168.10.61	<解決できません>	この IP アドレスのサーバは、...

適切な逆引き参照ゾーンおよびエントリが構成されていない場合、サーバ FQDN は利用できません。

OK キャンセル

4. 「vsphere.local のプロパティ」画面に戻りますので、[通知]をクリックします。

vsphere.local のプロパティ

全般 SOA (Start of Authority) ネーム サーバ WINS ゾーンの転送

ゾーン転送は、コピーを要求したサーバにゾーンのコピーを送信します。

☒ ゾーン転送を許可するサーバ(O):

☐ すべてのサーバ(T)

☐ ネーム サーバ タブの一覧にあるサーバのみ(S)

☒ 次のサーバのみ(H)

IP アドレス	サーバ FQDN
192.168.10.61	<解決できません>

編集(E)

ゾーンの変更を通知するセカンダリ サーバを指定するには、[通知] をクリックしてください。

通知(N)...

OK キャンセル 適用(A) ヘルプ

5. 「通知」画面が表示されますので、[自動的に通知する]にチェックが入っていることを確認します。
また、[次のサーバのみ]にチェックを入れて、[ここをクリックして IP アドレスまたは DNS 名を追加してください]をクリックして、「セカンダリ DNS サーバ - IP アドレス」を入力し、[OK]をクリックします。

通知

ゾーンに変更があった場合にセカンダリ サーバに自動的に通知するには、[自動的に通知する] チェック ボックスをオンにしてからサーバ名を指定してください。

☒ 自動的に通知する(A):

☐ [ネーム サーバ] タブの一覧にあるサーバのみ(S)

☒ 次のサーバのみ(I)

IP アドレス	サーバ FQDN	検証済み	削除(D)
192.168.10.61			

OK キャンセル

6. 「vsphere.local のプロパティ」画面に戻りますので、[OK]をクリックします。

vsphere.local のプロパティ

全般 SOA (Start of Authority) ネーム サーバ WINS ゾーンの転送

ゾーン転送は、コピーを要求したサーバにゾーンのコピーを送信します。

☒ ゾーン転送を許可するサーバ(O):

☐ すべてのサーバ(T)

☐ ネーム サーバ タブの一覧にあるサーバのみ(S)

☒ 次のサーバのみ(H)

IP アドレス	サーバ FQDN
192.168.10.61	<解決できません>

編集(E)

ゾーンの変更を通知するセカンダリ サーバを指定するには、[通知] をクリックしてください。

通知(N)...

OK キャンセル 適用(A) ヘルプ

以上で管理 VM 上の DNS サーバの設定は完了となります。引き続き 4.1.3 項の操作を行ってください。

4.1.3 お客様 DNS サーバでの同期作業

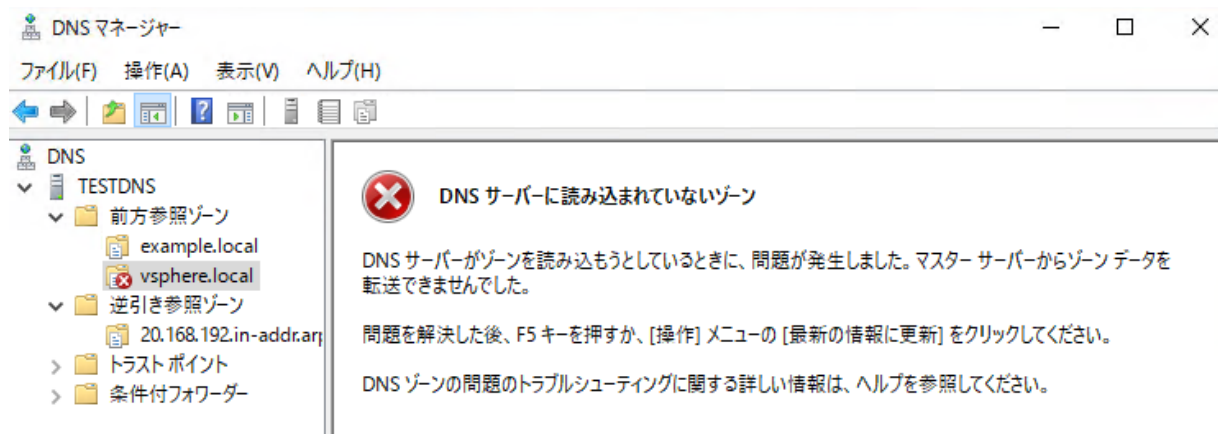
お客様 DNS サーバ上で同期作業を実施します。

1. サーバーマネージャーの画面上部の[ツール]をクリックし、表示されたメニューから[DNS]をクリックして DNS マネージャーを起動し、"お客様のサーバ名(画像だと TESTDNS)" - "前方参照ゾーン"配下の"vsphere.local"を表示し、情報が転送されていることを確認してください。



転送されていない場合は、"vsphere.local"を右クリックし、[マスターから転送]をクリックしてください。

[マスターから転送]をクリックしても以下エラー画面が消えない場合は、DNS マネージャーを再起動してください。



以上でお客様 DNS サーバでの同期作業は完了となります。引き続き 4.1.4 項の操作を行ってください。

4.1.4 ゾーン転送設定の確認

お客様の DNS のみを参照する端末上でコマンドプロンプトを開き、nslookup コマンドで、ゾーン転送で転送した任意のエントリについて名前解決ができるか確認してください。

以上で DNS サーバのゾーン転送設定は完了となります。

4.2 DNS のフォワーダー設定

本項は、すべての DNS クエリを転送する設定を記載しています。

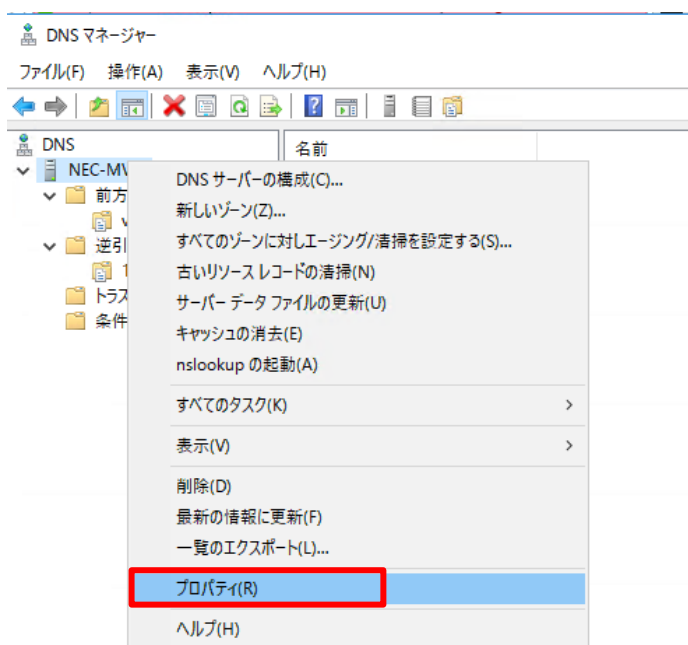
特定のドメインの名前解決のみ転送する場合は条件付きフォワーダーを設定してください。

本項は、HCS の(管理 VM 上の)DNS を操作します。

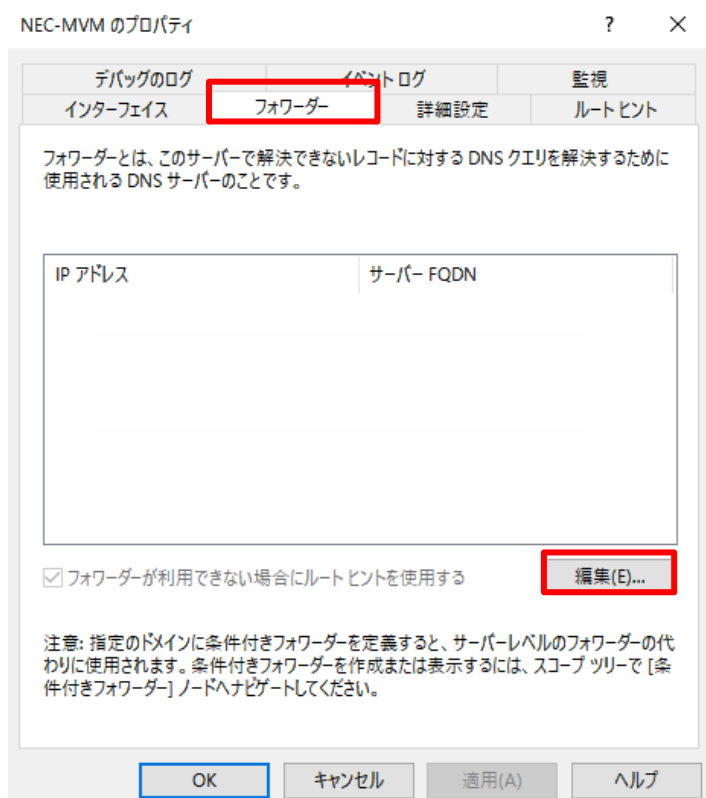
手順実施に必要なパラメータ

ドキュメント	項目	パラメータ/値 (メモ用)
-	DNS フォワード先 - IP アドレス	

1. DNS マネージャを起動し、"NEC-MVM"を右クリックし、[プロパティ]をクリックします。



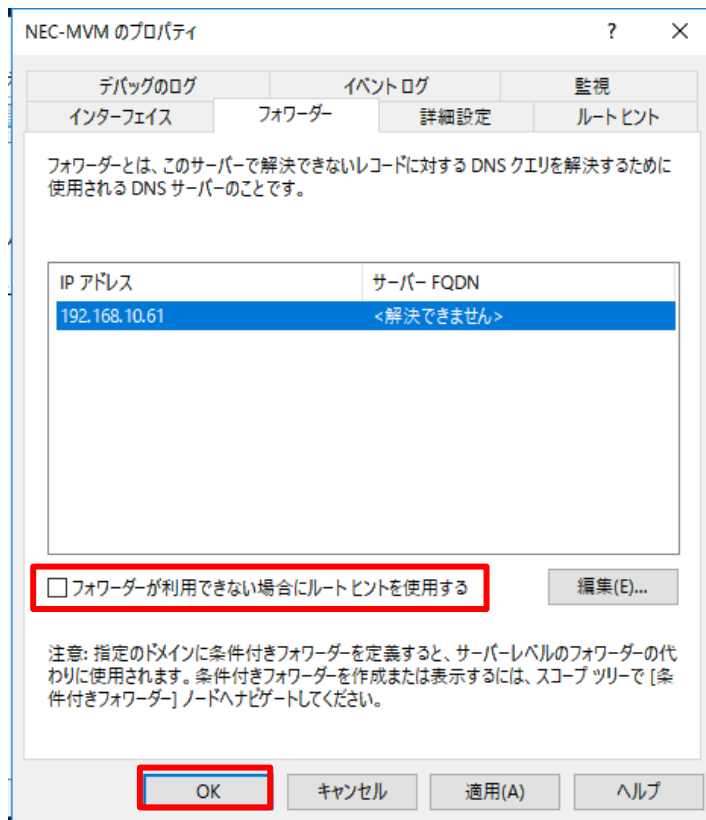
2. 「NEC-MVM のプロパティ」画面が表示されるので、[フォワーダー]タブを選択して、[編集]をクリックします。



3. 「フォワーダーの編集」画面が表示されるので、[ここをクリックして IP アドレスまたは DNS 名を追加してください] をクリックして、「DNS フォワード先 - IP アドレス」を入力し、[OK]をクリックしてください。



4. 「NEC-MVM のプロパティ」画面に戻るので、[フォワーダーが利用できない場合にルートヒントを使用する]のチェックを外し、[OK]をクリックします。



5. 管理 VM 上でコマンドプロンプトを開き、nslookup コマンドで、フォワード先の DNS サーバで名前解決できる DNS 名を入力して名前解決が行えることを確認してください。

```
C:\Users\Administrator>nslookup test1.example.local
サーバー: nec-mvm.vsphere.local
Address: 192.168.10.51

権限のない回答:
名前: test1.example.local
Address: 192.168.20.1
```

以上で DNS のフォワーダー設定は完了となります。

4.3 代替 DNS サーバ設定の確認

本項では、管理 VM、vCSA、ESXi に設定した代替 DNS サーバ設定が動作するか確認します。

確認は、管理 VM 上の DNS サーバを一時的に停止した状態で、管理 VM、vCSA、ESXi 上で FQDN を用いて PING 送信を行います。

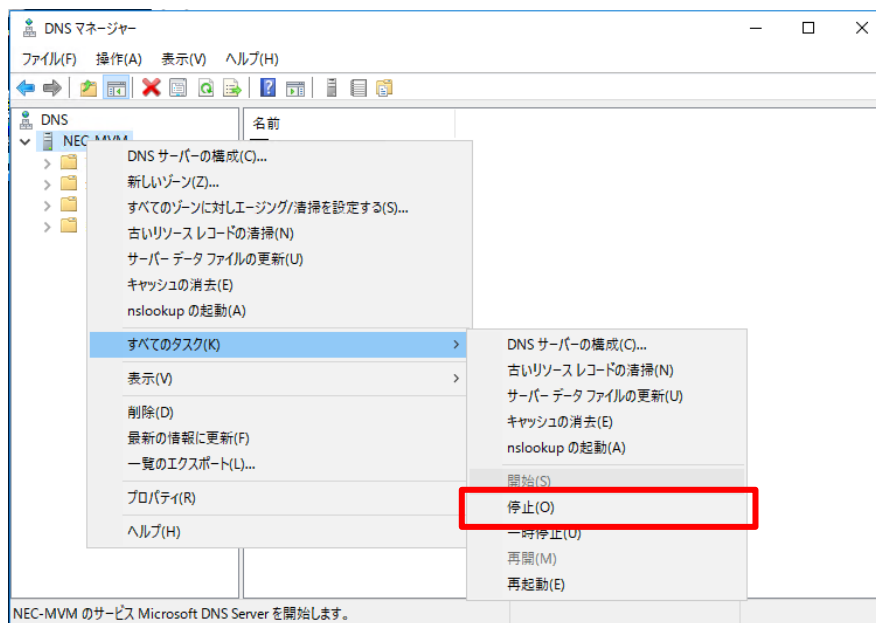
手順実施に必要なパラメータ

ドキュメント	項目	パラメータ/値 (メモ用)
SG 仕様書 [Startup]シート	任意のノード(A) – BMC – IP アドレス	
	任意のノード(B) – FQDN	
初期パスワード通知書	任意のノード(A) – BMC のパスワード	
	任意のノード(A) – ESXi の root パスワード	
	vCSA – 管理インターフェース(VAMI)root パスワード	

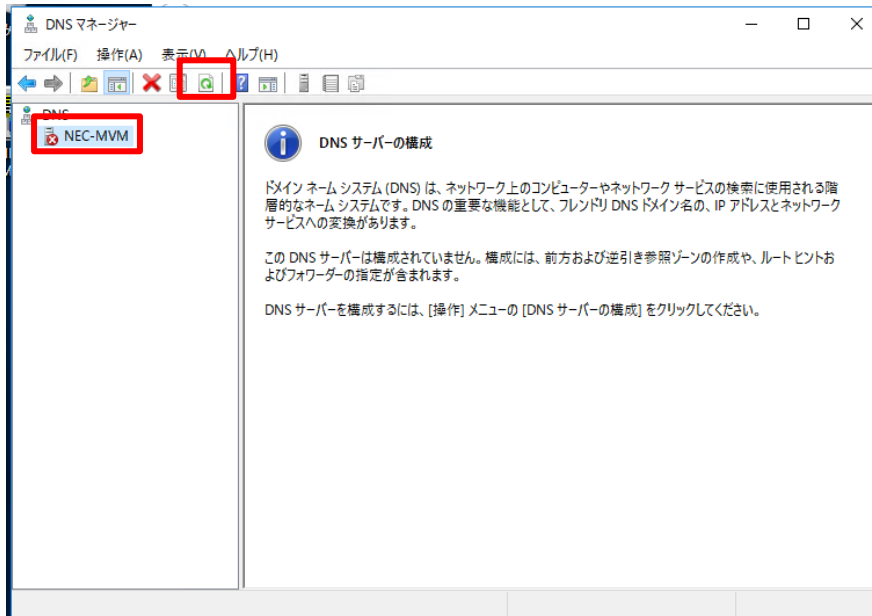
4.3.1 事前準備

以下の手順で管理 VM 上の DNS サーバを一時的に停止します。

1. サーバマネージャの画面上部の[ツール]をクリックし、表示されたメニューから[DNS]をクリックし DNS マネージャを起動し、"NEC-MVM"を右クリックし、[全てのタスク] - [停止] をクリックします。



2. [最新の情報を更新]をクリックし、DNS サービスが停止されたことを確認します。



4.3.2. 管理 VM での確認

管理 VM から FQDN で任意の ESXi に PING を送信できることを確認します。

1. コマンドプロンプトを開き、以下のコマンドを実行し DNS キャッシュを削除します。

```
# ipconfig /flushdns
```

```
C:\Users\Administrator>ipconfig /flushdns
Windows IP 構成
DNS リゾルバー キャッシュは正常にフラッシュされました。
```

2. 以下のコマンドを入力し、PING が送信できることを確認します。

```
# ping <任意のノード(B) - FQDN>
```

```
C:\Users\Administrator>ping nec-esx-cn1.vsphere.local
nec-esx-cn1.vsphere.local [192.168.10.1]に ping を送信しています 32 バイトのデータ:
192.168.10.1 からの応答: バイト数 = 32 時間 <1ms TTL=64
192.168.10.1 からの応答: バイト数 = 32 時間 <1ms TTL=64
192.168.10.1 からの応答: バイト数 = 32 時間 <1ms TTL=64
192.168.10.1 からの応答: バイト数 = 32 時間 <1ms TTL=64

192.168.10.1 の ping 統計:
    パケット数: 送信 = 4, 受信 = 4, 損失 = 0 (0% の損失),
    ラウンドトリップの概算時間 (ミリ秒):
        最小 = 0ms、最大 = 0ms、平均 = 0ms
```

4.3.3 ESXi での確認

ESXi から FQDN で任意の ESXi に PING を送信できることを確認します。

1. 下記の URL を入力し、任意のノードの iLO に接続します。

`https://<任意のノード(A) - BMC - IP アドレス>/`

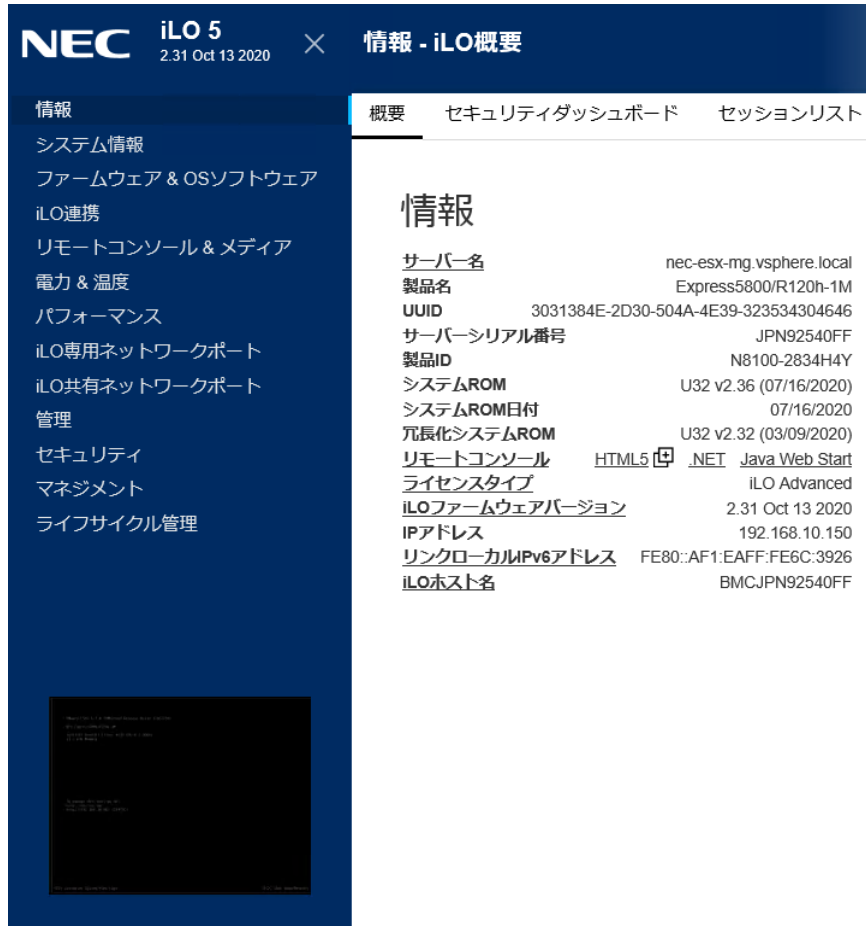


2. iLO のログイン画面が表示されます。(以下図)
アカウント情報を入力し、ログインします。

- ローカル ログイン名: 「hcsadmin」
- パスワード: 「任意のノード(A) - BMC のパスワード」

A screenshot of the iLO 5 login interface. It features a white login form with a red border. The form has two input fields: 'ローカルユーザー名:' (Local username) with the text 'hcsadmin' entered, and 'パスワード' (Password) with masked characters '.....'. To the right of the password field is an eye icon. Below the form is a dark blue button with the white text 'ログイン' (Login).

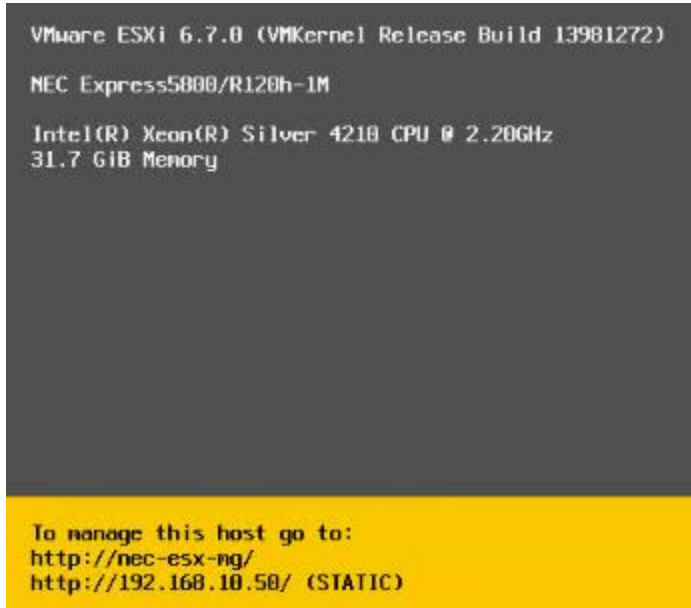
3. 正常にログインすると、iLO の Web インターフェイス画面が表示されます。



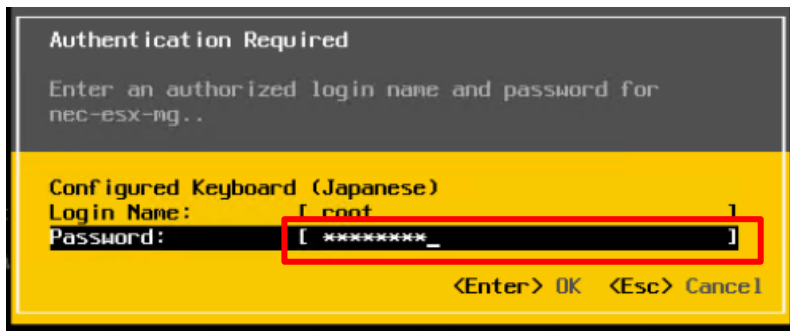
4. iLO の Web インターフェイス画面が表示されたら、画面左下の ESXi コンソールをクリックし、[HTML5 コンソール]を選択します。



5. 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



6. 「Authentication Required」の画面が表示されます。アカウント情報を入力し、[Enter]キーを押下します。
- Login Name: 「root」
 - Password: 「任意のノード(A) – ESXi の root パスワード」



7. 「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。



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

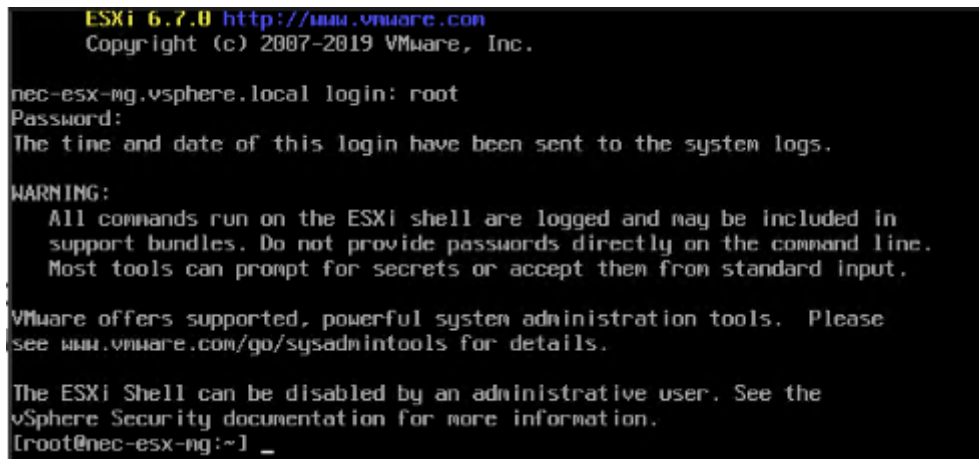
画面左のメニューにおいて[Enable ESXi Shell]を選択した状態で[Enter]キーを押下し、画面左のメニューの表示が[Disable ESXi Shell]に更新されることを確認します。

※ 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 9 の操作を行ってください。



9. [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。

- Login Name: 「root」
- Password: 「任意のノード(A) - ESXi の root パスワード」



10. ESXi Shell で以下のコマンドを実行して、DNS キャッシュを削除します。

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

```
[root@nec-esx-ng:~] /etc/init.d/nscd restart
watchdog-nscd: Terminating watchdog process with PID 2400290
nscd started
```

11. 以下のコマンドを入力し、PING が送信できることを確認します。

```
# ping <任意のノード(B) - FQDN>
```

```
[root@nec-esx-ng:~] ping nec-esx-cn1.vsphere.local
PING nec-esx-cn1.vsphere.local (192.168.10.1): 56 data bytes
64 bytes from 192.168.10.1: icmp_seq=0 ttl=64 time=0.150 ms
64 bytes from 192.168.10.1: icmp_seq=1 ttl=64 time=0.121 ms
64 bytes from 192.168.10.1: icmp_seq=2 ttl=64 time=0.127 ms

--- nec-esx-cn1.vsphere.local ping statistics ---
3 packets transmitted, 3 packets received, 0% packet loss
round-trip min/avg/max = 0.121/0.133/0.150 ms
```

12. 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
```

13. 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、手順 5 から手順 7 の操作を行ってください。
14. 「Troubleshooting Mode Options」の画面が表示されます
15. 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。



4.3.4 vCSA での確認

vCSA から FQDN で任意の ESXi に PING を送信できることを確認します。

1. VMware vSphere Client を開きます。

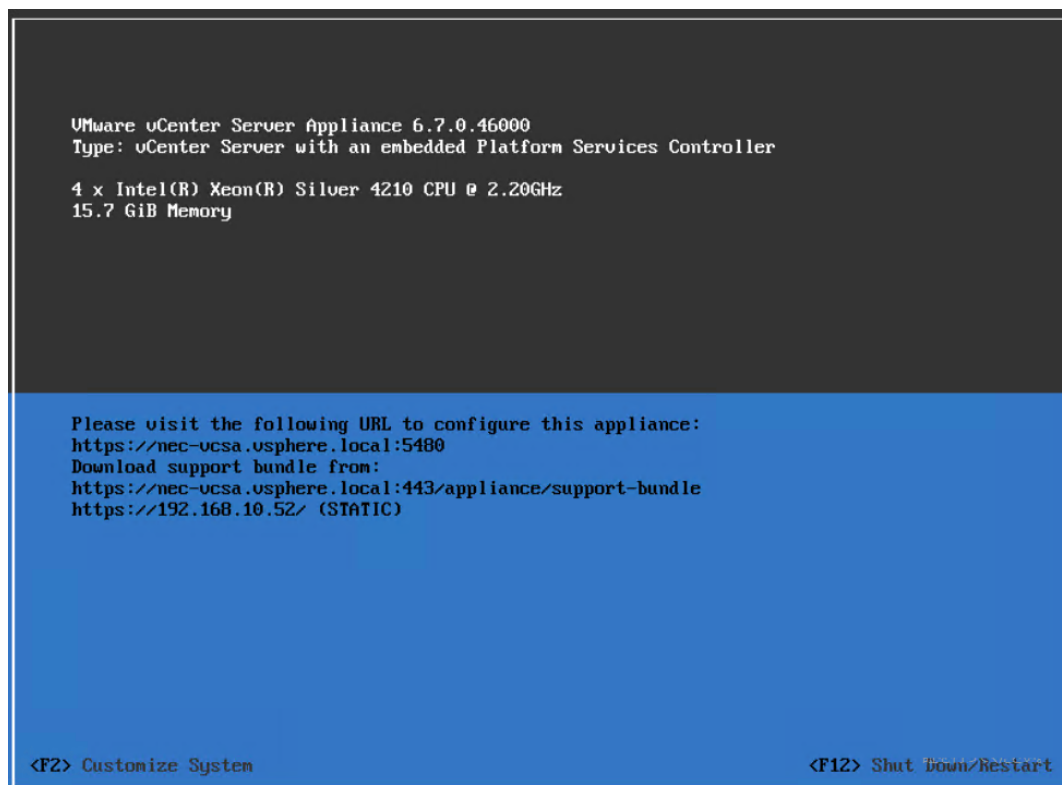
2. vCSA「nec-vcsa」を選択し、赤枠の画面をクリックしコンソールを起動します。



3. [OK]をクリックします。



4. 以下の画像のようなコンソールが起動したら、[Alt + F1]キーを押下して vCSA Shell 画面を表示します。



5. アカウント情報を入力し、[Enter]キーを押下します。

- Login Name: 「root」
- Password: 「vCSA – 管理インターフェース(VAMI)root パスワード」

```
VMware vCenter Server Appliance 6.7.0.46000
Type: vCenter Server with an embedded Platform Services Controller
nec-ucsa login: root
Password:
```

6. "shell"と入力し Bash を起動した後に、以下のコマンドを実行して、DNS キャッシュを削除します。

```
# service dnsmasq restart
```

```
VMware vCenter Server Appliance 6.7.0.31100
Type: vCenter Server with an embedded Platform Services Controller
Connected to service
* List APIs: "help api list"
* List Plugins: "help pi list"
* Launch BASH: "shell"
Command> shell
Shell access is granted to root
root@nec-vcsa [ ~ ]# service dnsmasq restart
root@nec-vcsa [ ~ ]#
```

7. 以下のコマンドを入力し、PING が送信できることを確認します。
(PING は任意のタイミングで Ctrl+C で停止してください。)

```
# ping <任意のノード(B) – FQDN>
```

```
root@nec-vcsa [ ~ ]# ping nec-esx-cn1.vsphere.local
PING nec-esx-cn1.vsphere.local (192.168.10.1) 56(84) bytes of data.
64 bytes from 192.168.10.1: icmp_seq=1 ttl=64 time=0.102 ms
64 bytes from 192.168.10.1: icmp_seq=2 ttl=64 time=0.128 ms
64 bytes from 192.168.10.1: icmp_seq=3 ttl=64 time=0.106 ms
64 bytes from 192.168.10.1: icmp_seq=4 ttl=64 time=0.125 ms
64 bytes from 192.168.10.1: icmp_seq=5 ttl=64 time=0.134 ms
^C64 bytes from 192.168.10.1: icmp_seq=6 ttl=64 time=0.106 ms

--- nec-esx-cn1.vsphere.local ping statistics ---
6 packets transmitted, 6 received, 0% packet loss, time 120059ms
rtt min/avg/max/mdev = 0.102/0.116/0.134/0.018 ms
root@nec-vcsa [ ~ ]#
```

8. 以下のコマンドを二回入力し、vCSA Shell からログアウトし、[Alt + F2]キーを押下します。

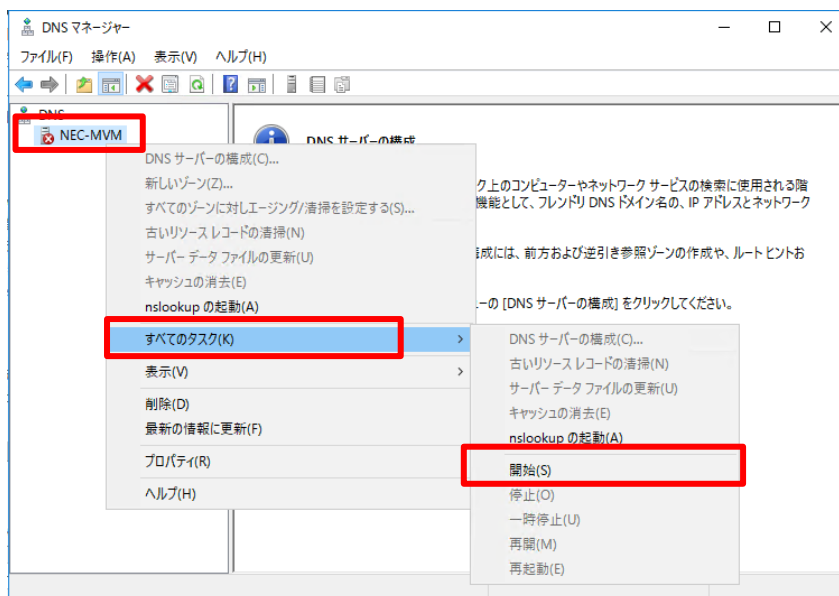
```
# exit
```

```
root@nec-ucsa [ ~ ]# exit
logout
Command> exit
```

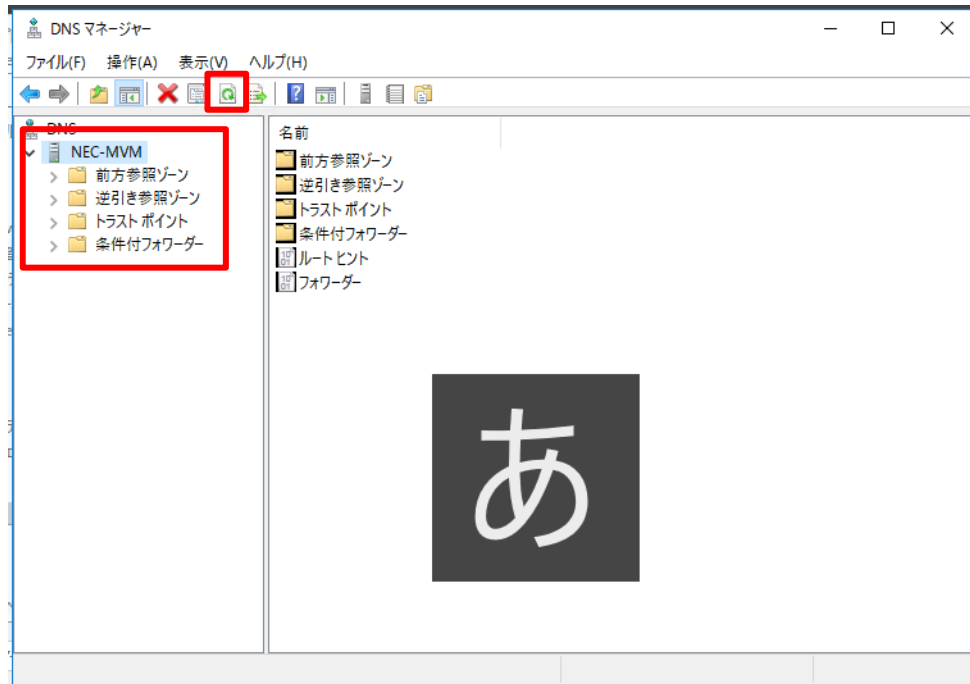
4.3.5 事後の処理

以下の手順で停止した DNS サーバを開始します。

1. DNS マネージャを起動し、"NEC-MVM"を右クリックし、[すべてのタスク] - [開始] をクリックします。



2. [最新の情報を更新]をクリックし、DNS サービスが開始されたことを確認します。



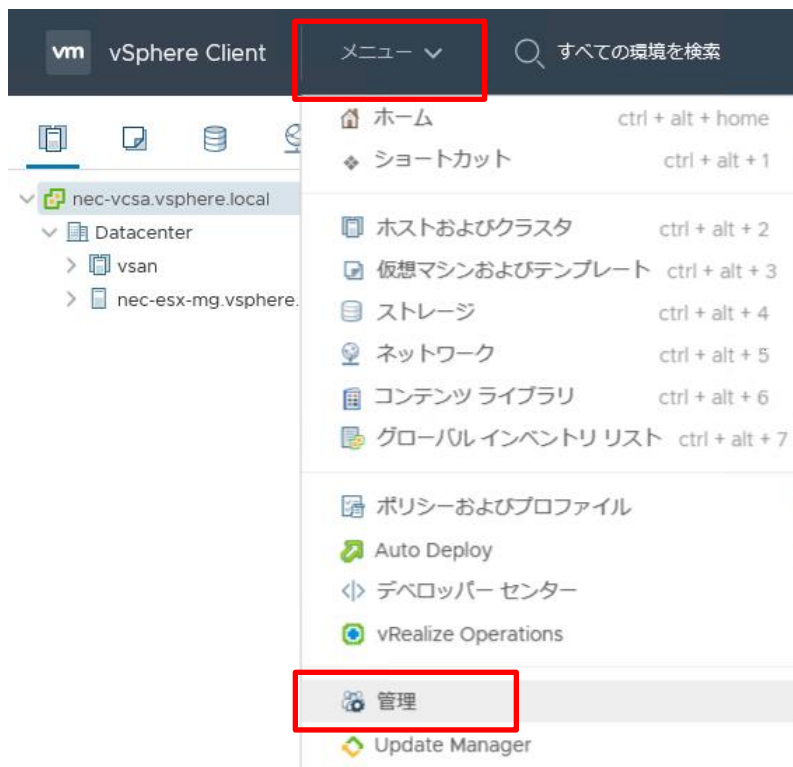
以上で、代替 DNS サーバ設定の確認は終了です。

5 ライセンス登録

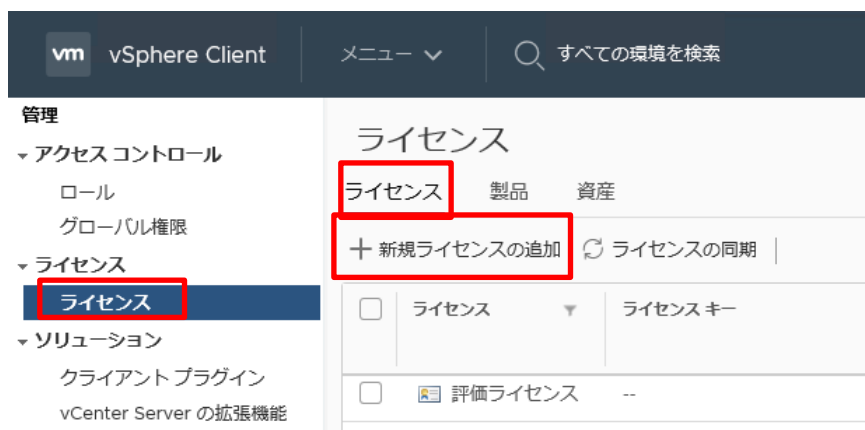
5.1 vCenter Server、ESXi、vSAN ライセンスの登録

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。

1. VMware vSphere Client の画面上部の「メニュー」―「管理」をクリックします。



2. 「ライセンス」をクリックし、「ライセンス」、「新規ライセンスの追加」の順に選択します。



3. 各ライセンスキーを1行に1つ入力し、「次へ」をクリックします。

[illegible]

4. 入力したライセンスキーに応じたライセンス名を編集し、「次へ」をクリックします。
ここでは、ライセンス名を「vCenter Server」、「ESXi」、「vSAN」に編集します。

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: vCenter Server

ライセンスキー: 00000000000000000000000000000000

製品: VMware vCenter Server 6 Standard (インスタンス)

ライセンス名: ESXi

ライセンスキー: 00000000000000000000000000000000

製品: VMware vSphere 6 Standard (CPU)

ライセンス名: vSAN

ライセンスキー: 00000000000000000000000000000000

製品: VMware vSAN Standard (CPU)

5. 入力したライセンスキーを確認し、「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: 3

ライセンス名:	vCenter Server
ライセンスキー:	00000-00000-00000-00000-00000
ライセンス名:	ESXi
ライセンスキー:	00000-00000-00000-00000-00000
ライセンス名:	vSAN
ライセンスキー:	00000-00000-00000-00000-00000

6. 追加したライセンスが一覧に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

+ 新規ライセンスの追加 リценスの同期

☐	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 6 Standard (CPU)	0 CPU
☐	vCenter Server	...	VMware vCenter Server 6 Standard (...)	0 インスタンス
☐	vSAN	...	VMware vSAN Standard (CPU)	0 CPU

7. 「資産」をクリックし、「VCENTER SERVER システム」を選択し、「nec-vcsa.vsphere.local」にチェックを付け、「ライセンスの割り当て」を選択します。

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
☒	nec-vcsa.vsphere.local	1 インスタンス

8. ライセンス「vCenter Server」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
☐	評価ライセンス	--	--
☒	vCenter Server	VMware vCenter Server 6 Stand...	1 インスタンス

9. 「nec-vcsa.vsphere.local」に割り当てたライセンス「vCenter Server」が表示されていることを確認します。



10. 「ホスト」をクリックし、管理ノードとクラスタノードにチェックを付け、「ライセンスの割り当て」を選択します。



11. 「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「ESXi」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 - 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 6 Standard (CP...	5 CPU

13. 管理ノードとクラスタノードに割り当てたライセンス「ESXi」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

VCENTER SERVER システム ホスト クラスタ ソリューション

☐ 資産	使用状況	製品	ライセンス
☐ nec-esx-mg.vsphere.local	2 CPU	VMware vSphere 6 Standard (CPU)	ESXi
☐ nec-esx-cn1.vsphere.local	1 CPU	VMware vSphere 6 Standard (CPU)	ESXi
☐ nec-esx-cn2.vsphere.local	1 CPU	VMware vSphere 6 Standard (CPU)	ESXi
☐ nec-esx-cn3.vsphere.local	1 CPU	VMware vSphere 6 Standard (CPU)	ESXi

14. 「クラスタ」をクリックし、クラスタ「vsan」にチェックを付け、「ライセンスの割り当て」を選択します。

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
☒ vsan	3 CPU	評価モード

15. ライセンス「vSAN」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
☐ 評価ライセンス	--	--	--
☒ vSAN		VMware vSAN Standard (CPU)	• 3 CPU

16. クラスタ「vsan」に割り当てたライセンス「vSAN」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	
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
☒	vsan		3 CPU	VMware vSAN Standard (CPU)
				vSAN

以上で、vCenter Server、ESXi および vSAN へのライセンス登録および割り当ては完了となります。

6 パスワード更新

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。

6.1 概要

本章では、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更新する手段を示します。

6.1.1 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、管理ノード、クラスタノード、管理 VM、vCSA が起動し、利用できる状態としてください。

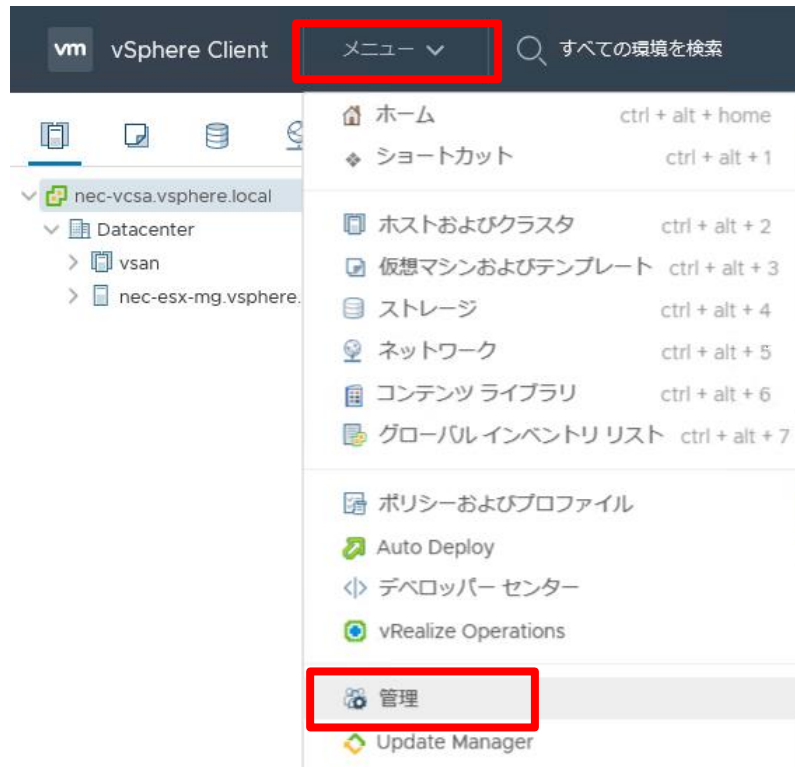
パスワード更新は、管理 VM より行いますので、Windows PC から管理 VM に接続してください。

6.2 vCenter Server の保守アカウントのパスワード更新

vCenter Server(vCSA)の保守アカウント「nec」の初期パスワードを更新します。

手順

1. VMware vSphere Client の画面上部の「メニュー」―「管理」をクリックします。



2. 「ユーザーおよびグループ」をクリックし、「ユーザー」を選択し、ドメインに「vsphere.local」を選択し、ユーザー名に「Administrator」、「nec」が表示されることを確認します。



注意事項

- あらかじめドメインに「vsphere.local」が選択されている場合、ユーザー名に「Administrator」、「nec」が表示されないことがあります。その場合は、ドメインを「localos」に変更して、再度「vsphere.local」に戻してください。数回試し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。

3. ユーザー「nec」の左の赤枠のアイコンをクリックし、「編集」を選択します。



4. 新規のパスワードを入力し、「保存」をクリックします。

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

ユーザーの編集

ユーザー名 *

nec

パスワード

.....

.....

パスワードの確認

.....

名

姓

Eメール

説明

キャンセル

保存

6.3 管理ノード、クラスタノード、vCenter Server、HCS Console のパスワード

更新

管理ノード、クラスタノード、vCenter Server(vCSA)、HCS Console の初期パスワードを更新します。

手順

1. 管理 VM のスタートメニューから「コマンド プロンプト」をクリックし、コマンドプロンプト(cmd)を起動します。



2. 下記のコマンドを実行して、パスワード更新を行います。

※コマンド実行後、警告メッセージが表示されますが動作に影響はございません。

```
> %PROGRAMDATA%\NEC\UpdateHcsConsoleAccount.bat
```

```
C:\Users\Administrator>%PROGRAMDATA%\NEC\UpdateHcsConsoleAccount.bat
```

3. メッセージに従って、順次パスワードを入力し、「Enter」キーを押下します。

※各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。

- ① 管理ノードの ESXi の root パスワード
- ② 管理ノードの BMC のパスワード
※hcsadmin のパスワードを変更します。
- ③ クラスタノードの ESXi の root パスワード
- ④ クラスタノードの BMC のパスワード
※hcsadmin のパスワードを変更します。

- ⑤ CMC のパスワード

※CMC は、R120h-1M では未搭載ですが、英数字を 1 文字以上入力してください。

入力した値は、実際には設定されません。

- ⑥ vCSA の root パスワード
- ⑦ vCSA の Administrator パスワード
- ⑧ HCS Console の hcsadmin パスワード

```

管理ノードの ESXi の root パスワードを入力してください。: ***** ①
再度、同じパスワードを入力してください。: *****
管理ノードの BMC のパスワードを入力してください。: ***** ②
再度、同じパスワードを入力してください。: *****
クラスタノードの ESXi の root パスワードを入力してください。: ***** ③
再度、同じパスワードを入力してください。: *****
クラスタノードの BMC のパスワードを入力してください。: ***** ④
再度、同じパスワードを入力してください。: *****
CMC のパスワードを入力してください。: ***** ⑤
再度、同じパスワードを入力してください。: *****
vCSA の root のパスワードを入力してください。: ***** ⑥
再度、同じパスワードを入力してください。: *****
vCSA の Administrator のパスワードを入力してください。: ***** ⑦
再度、同じパスワードを入力してください。: *****
HCS Console のパスワードを入力してください。: ***** ⑧
再度、同じパスワードを入力してください。: *****

```

4. アカウント更新完了のメッセージが表示されたら、「Enter」キーを 2 回押下します。

※「指定されたファイルが見つかりません」というメッセージが表示されますが、問題はありません。

また、アカウント更新に失敗した場合、手順 2 からやり直してください。

```

HCS Console のパスワードを入力してください。: *****
再度、同じパスワードを入力してください。: *****
2019/07/04 09:53:07.747 - nec-esx-cn1 の BMC のパスワードを更新する。
2019/07/04 09:53:26.387 - nec-esx-cn2 の BMC のパスワードを更新する。
2019/07/04 09:53:36.358 - nec-esx-cn3 の BMC のパスワードを更新する。
2019/07/04 09:53:46.364 - nec-esx-mg の BMC のパスワードを更新する。
2019/07/04 09:53:54.885 - nec-vcsa の Administrator@vsphere.local のパスワードを更新する。
2019/07/04 09:54:03.280 - nec-vcsa の root のパスワードを更新する。
2019/07/04 09:54:19.469 - nec-esx-cn1 の root のパスワードを更新する。
2019/07/04 09:55:06.050 - nec-esx-cn2 の root のパスワードを更新する。
2019/07/04 09:55:19.892 - nec-esx-cn3 の root のパスワードを更新する。
2019/07/04 09:55:32.511 - nec-esx-mg の root のパスワードを更新する。
2019/07/04 09:55:46.657 - HCS Console の hcsadmin のパスワードを更新する。
アカウント更新処理に成功しました。
アカウント更新に使用したスクリプトを削除します。
続行するには何かキーを押してください . . .
指定されたファイルが見つかりません。
スクリプトの削除が完了しました。
本バッチファイルも削除してください。
続行するには何かキーを押してください . . .

```

5. 以下のコマンドを実行して、バッチファイルを削除します。

```
>del %PROGRAMDATA%\NEC\UpdateHcsConsoleAccount.bat
```

```

C:\Users\Administrator>del %PROGRAMDATA%\NEC\UpdateHcsConsoleAccount.bat
C:\Users\Administrator>

```

6.4 管理ノードの管理 VM のパスワード更新

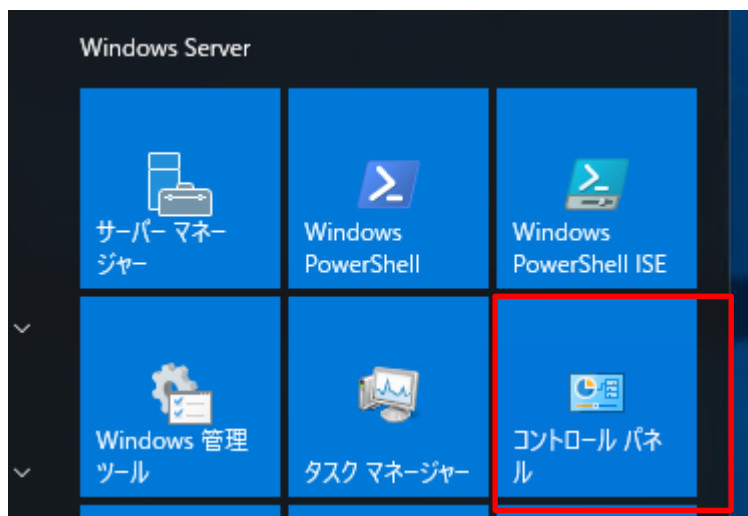
管理 VM の保守用アカウント「nec」と「Administrator」の初期パスワードを更新します。

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	管理 VM – Administrator パスワード	

手順

1. 管理 VM のスタートメニューからコントロールパネルをクリックし、コントロールパネルを起動します。

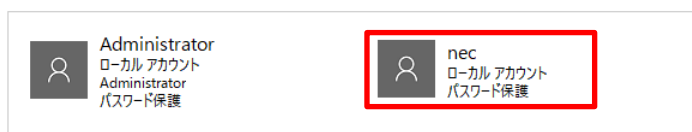


2. 「アカウントの種類の変更」をクリックします。



3. 「nec」をクリックします。

変更するユーザーを選んでください



4. 「パスワードの変更」をクリックします。

nec のアカウントの変更

アカウント名の変更
パスワードの変更
アカウントの種類の変更
アカウントの削除
別のアカウントの管理



5. 保守用アカウント「nec」の「新しいパスワード」、「パスワードのヒント」を入力し、「パスワードの変更」をクリック。

※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。

nec のパスワードの変更

nec
ローカル アカウント
パスワード保護

nec のパスワードを変更しようとしています。変更すると、nec は EFS で暗号化されたファイル、Web サイトやネットワーク リソースのための個人証明書や保存しているパスワードをすべて失います。

●●●●●●●●
●●●●●●●●
パスワードに大文字が含まれる場合は、各回同じように入力する必要があります。
2
パスワードのヒントはこのコンピューターを使用するすべての人が見ることができます。

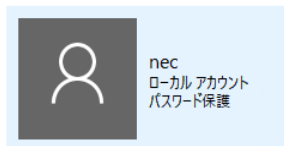
パスワードの変更

キャンセル

6. 「別のアカウントの管理」をクリックします。

nec のアカウントの変更

アカウント名の変更
パスワードの変更
アカウントの種類の変更
アカウントの削除
別のアカウントの管理



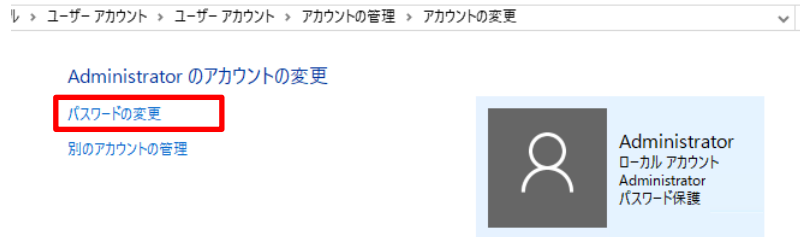
7. 「Administrator」をクリックします。

変更するユーザーを選んでください

Administrator
ローカル アカウント
Administrator
パスワード保護

nec
ローカル アカウント
パスワード保護

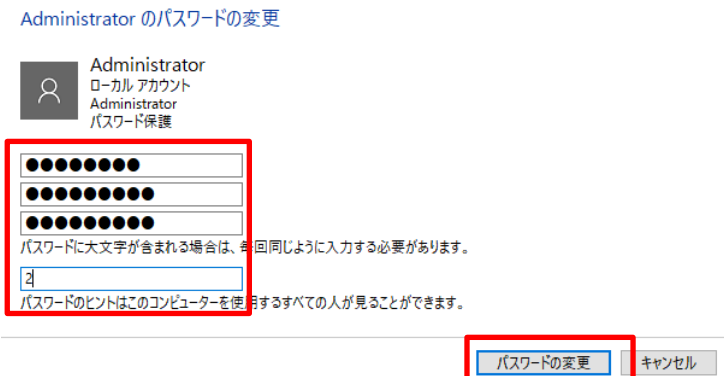
8. 「パスワードの変更」をクリックします。



9. Administrator の「現在のパスワード」と「新しいパスワード」、「パスワードのヒント」を入力し、「パスワードの変更」をクリックします。

パスワードの要件は、手順 5 と同じです。

- 現在のパスワード:「管理 VM – Administrator パスワード」



6.5 ESMPRO/ServerManager のパスワード更新

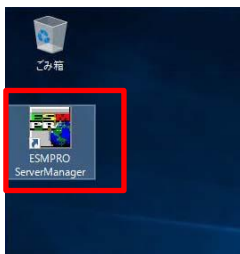
ESMPRO/ServerManager の初期パスワードを更新します。

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	ESMPRO/SM - 管理パスワード	

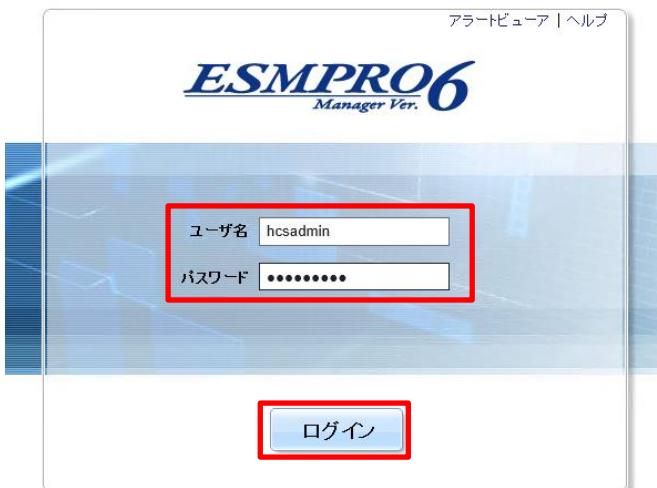
手順

1. 管理 VM のデスクトップの「ESMPRO/ServerManager」をダブルクリックして起動します。

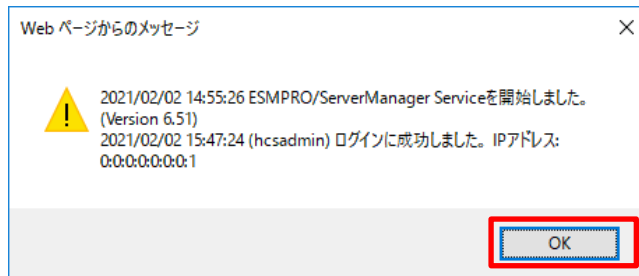


2. ESMPRO/ServerManager のログイン画面が表示されます。(下記図)
アカウント情報を入力し、「ログイン」をクリックします。

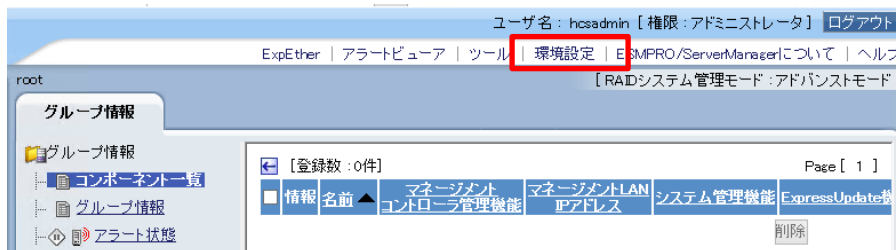
- ユーザ名: 「hcsadmin」
- パスワード: 「ESMPRO/SM - 管理パスワード」



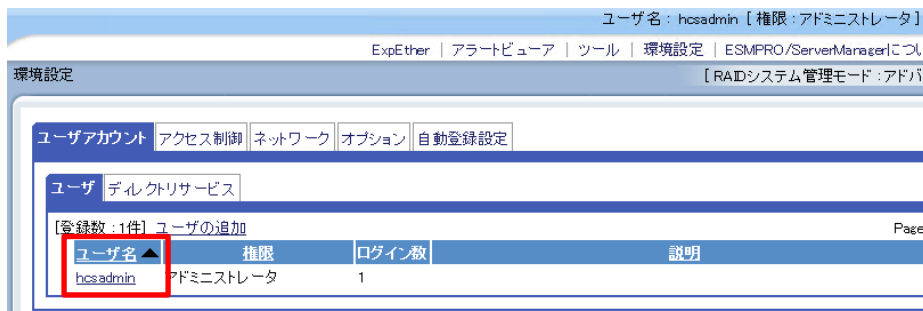
※ログイン後、「Web ページからのメッセージ」が表示されます。(遅れて表示される場合もあります。)
「OK」をクリックしてください。



3. 「環境設定」をクリックします。



4. 「hcsadmin」をクリックします。



5. 「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・新しいパスワードを入力し、「適用」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。

ユーザー名: hcsadmin [権限: アドミニストレータ]

ExpEther | アラートビューア | ツール | 環境設定 | ESMPRO/ServerManagerについて

環境設定 [RAIDシステム管理モード: アドバンス]

ユーザーアカウント | アクセス制御 | ネットワーク | オプション | 自動登録設定

ユーザー | デレトリサービス

項目名	設定値
現在のパスワード [必須]	
新しいパスワード (6 - 16 文字) [必須]	
新しいパスワード (確認用) [必須]	

適用 キャンセル

7. 「OK」をクリックします。

Web ページからのメッセージ

? 適用してもよろしいですか?

OK キャンセル

以上で、パスワード更新は完了となります。

7 監視通報の変更

本章では、監視通報設定の変更について記載します。

7.1 vCSA での監視通報

本項では、vCSA での監視通報設定手順について記載します。

7.1.1 アラーム定義の無効化

本項では、下記 3 点の事前構成済みのアラームの無効化手順を記載します。

- ホストのメモリ使用率
- ホストの CPU 使用率
- ディスク上のデータストア使用率

手順

1. VMware vSphere Client の画面にて、[nec-vcsa.vsphere.local]を選択し、[設定] – [アラーム定義]をクリックしていきます。



2. 「アラーム名」の赤枠部分をクリックし、[使用率]と入力します。



3. 「ホストのメモリ使用率」を選択し、[無効化]をクリックします。



4. 「ホストの CPU 使用率」を選択し、[無効化]をクリックします。



5. 「ディスク上のデータストア使用率」を選択し、[無効化]をクリックします。

アラーム定義

追加 編集 **無効化** 削除

	アラーム名	オブジェクトタイプ
☐	> 仮想マシンのメモリ使用率	仮想マシン
☐	> 仮想マシンの CPU 使用率	仮想マシン
☐	> ホストのメモリ使用率	ホスト
☐	> ホストの CPU 使用率	ホスト
☒	> ディスク上のデータストア使用率	データストア

6. 手順 3～5 で無効化したものが「無効」になっていることを確認します。

アラーム定義

追加 編集 有効化 削除

	アラーム名	オブジェクトタイプ	定義範囲	有効
☐	> 仮想マシンのメモリ使用率	仮想マシン	 このオブジェ...	有効
☐	> 仮想マシンの CPU 使用率	仮想マシン	 このオブジェ...	有効
☒	> ホストのメモリ使用率	ホスト	 このオブジェ...	無効
☐	> ホストの CPU 使用率	ホスト	 このオブジェ...	無効
☐	> ディスク上のデータストア使用率	データストア	 このオブジェ...	無効

7.1.2 アラーム定義の作成

本項では、アラーム定義の作成手順を記載します。

手順

1. [vsan]クラスタを選択し、[設定] – [アラーム定義] – [追加]とクリックしていきます。



2. アラーム名[クラスタノードの CPU 使用率]
説明[クラスタノードの CPU 使用率を監視するアラーム]
ターゲットのタイプ[ホスト]を設定し、[次へ]をクリックします。



3. 赤枠部分をクリックします。

アラーム ルール1 ×

IF

トリガを選択 ▼

THEN

アラームをトリガーして * 重要度を選択 ▼

E メール通知を送信 ☐

SNMP トラップを送信 ☐

スクリプトを実行 ☐

[高度なアクションの追加](#)

他のルールを追加
重複ルール
ルールの削除

4. 「容量と使用量」配下の[ホストの CPU 使用率]を選択します。

IF

検索

> 一般的エラー情報 (3)

▼ 容量と使用量 (7)

ホスト コンソール スワップアウト率

ホスト コンソール スワップイン率

ホスト スワップ ページ書き込み

ホスト ディスクの使用率

ホスト ネットワークの使用率

ホストの CPU 使用率

ホストのメモリ使用率

> 接続とモード (19)

5. それぞれの値を設定します。[次の値より大きい]、[クラスタのノード数に対応したしきい値(※)]、[5 分]、[警告として表示]を選択します。

SNMPトラップの送信設定を行う場合はこのまま手順 6 に進んでください。SNMPトラップの送信設定を行わない場合は手順 6 を省略し手順 7 に進んでください。

(※下記のマクラスタノードの CPU 使用率/アラーム ルール 1 設定値一覧を参照)



マクラスタノードの CPU 使用率/アラーム ルール 1 設定値一覧

クラスタのノード数	演算子	しきい値(%)	時間(分)	アクション
3 ノード	次の値より大きい	60	5 分	警告として表示
4 ノード	次の値より大きい	67	5 分	警告として表示
5 ノード	次の値より大きい	54	5 分	警告として表示
6 ノード	次の値より大きい	60	5 分	警告として表示

6. SNMPトラップの送信を設定する場合は、[SNMPトラップを送信]を有効にします。アラームを繰り返し送信する場合は[繰り返し]をチェックします。

※SNMPトラップ送信を設定する場合には後述の 7.1.3 項の操作を行ってください。

SNMP トラップを送信 ☒ ☒ 繰り返し ⓘ

スクリプトを実行 ☐

7. [他のルールを追加]をクリックします。



8. アラーム ルール 2 画面が表示されます。[トリガを選択]で[ホストの CPU 使用率]を選択します。それぞれの値を設定します。[次の値より大きい]、[90]、[5 分]、[重大として表示]を選択します。SNMP トラップの送信設定を行う場合はこのまま手順 9 に進んでください。SNMP の送信設定を行わない場合は手順 9、11 を省略し手順 10、12 に進んでください。

アラーム ルール 2

IF

ホストの CPU 使用率

次の値より大きい 90 % or 5 分 トリガをさらに追加

THEN

アラームをトリガーして *

重大として表示

E メール通知を送信 ☐

SNMP トラップを送信 ☐

スクリプトを実行 ☐

高度なアクションの追加

9. アラーム ルール 2 に SNMP トラップの送信設定を行う場合は、手順 6 を参照して設定を行ってください。
※SNMP トラップ送信を設定する場合には後述の 7.1.3 項の操作を行ってください。

10. [次へ]をクリックします。



11. ルールのリセット 1 に SNMP トラップの送信設定を行う場合は、手順 6 を参照して設定を行ってください。
※SNMP トラップ送信を設定する場合には後述の 7.1.3 項の操作を行ってください。

ルールのリセット 1

×

IF

警告または重大の条件または状態が解消されました

THEN

アラームを次のように
セットします: *

E メール通知を送信

☐

SNMP トラップを送信

☒

スクリプトを実行

☐

高度なアクションの追加

↑

↓

キャンセル

戻る

次へ

12. [次へ]をクリックします。

キャンセル

戻る

次へ

13. 確認画面が表示されます。左下の「このアラームを有効にする」が有効になっていることを確認し、[作成]をクリックします。

確認

×

アラーム名

クラスタノードのCPU使用率

説明

クラスタノードの CPU 使用率を監視するアラーム

ターゲット

すべて ホスト オン  vsan (3)

アラーム ルール

IF ホストの CPU 使用率 次の値より大きい 60 % for 5 分

THEN 以下の方法でアラームをトリガ  警告

または

IF ホストの CPU 使用率 次の値より大きい 90 % for 5 分

THEN 以下の方法でアラームをトリガ  重大

ルールのリセット

警告または重大の条件または状態が解消された場合

THEN 以下の方法でアラームをトリガ  正常

このアラームを有効にする ☒

キャンセル

戻る

作成

手順 6、9、11 で[繰り返し]にチェックした場合は、確認画面で繰り返す時間を設定できます。

以下の間隔でアクションの繰り返し 分 (確認されるか緑色にリセットされるまで)

14. アラーム定義の画面に戻るので、再度、[追加]をクリックします。



15. アラーム名[クラスタノードのメモリ使用率]
 説明[クラスタノードのメモリ使用率を監視するアラーム]
 ターゲットのタイプは[ホスト]を設定し、[次へ]をクリックします。

名前とターゲット

アラーム名 * クラスタノードのメモリ使用率

説明
 クラスタノードのメモリ使用率を監視するアラーム

ターゲットのタイプ * ホスト

ターゲット
 すべて ホスト オン vsan (3)

16. アラーム ルール 1 画面が表示されます。[トリガを選択]で[ホストのメモリ使用率]を選択します。それぞれの値を設定します。[ホストのメモリ使用率]、[次の値より大きい]、[クラスタのノード数に対応したしきい値(※)]、[5 分]、[警告として表示]を選択します。
- SNMP トラップの送信設定を行う場合はこのまま手順 17 に進んでください。SNMP トラップの送信設定を行わない場合は手順 17 を省略し手順 18 に進んでください。
- (※下記のワクラスタノードのメモリ使用率/アラーム ルール 1 設定値一覧を参照)

アラーム ルール 1

IF

ホストのメモリ使用率

次の値より大きい 60 % for 5 分 トリガをさらに追加

THEN

アラームをトリガーして *

警告として表示

E メール通知を送信 ☐

SNMP トラップを送信 ☐

スクリプトを実行 ☐

ワクラスタノードのメモリ使用率/アラーム ルール 1 設定値一覧

クラスタのノード数	演算子	しきい値(%)	時間(分)	アクション
3 ノード	次の値より大きい	60	5 分	警告として表示
4 ノード	次の値より大きい	67	5 分	警告として表示
5 ノード	次の値より大きい	54	5 分	警告として表示
6 ノード	次の値より大きい	60	5 分	警告として表示

17. SNMP トラップの送信を設定する場合は、[SNMP トラップを送信]にチェックをいれます。アラームを繰り返し送信する場合は[繰り返し]をチェックします。
- ※SNMPトラップ送信を設定する場合には後述の 7.1.3 項の操作を行ってください。

SNMP トラップを送信 ☒ 繰り返し ☒ ⓘ

スクリプトを実行 ☐

18. [他のルールを追加]をクリックします。

他のルールを追加 重複ルール ルールの削除

19. アラーム ルール 2 画面が表示されます。[トリガを選択]で[ホストのメモリ使用率]を選択します。それぞれの値を設定します。[次の値より大きい]、[クラスタのノード数に対応したしきい値(※)]、[5 分]、[重大として表示]を選択します。
- SNMP トラップの送信設定を行う場合はこのまま手順 20 に進んでください。SNMP トラップの送信設定を行わない場合は手順 20、22 を省略し手順 21、23 に進んでください。
- (※下記の▽クラスタノードのメモリ使用率/アラーム ルール 2 設定値一覧を参照)

アラーム ルール 2

▽クラスタノードのメモリ使用率/アラーム ルール 2 設定値一覧

クラスタのノード数	演算子	しきい値(%)	時間(分)	アクション
3 ノード	次の値より大きい	66	5 分	重大として表示
4 ノード	次の値より大きい	75	5 分	重大として表示
5 ノード	次の値より大きい	60	5 分	重大として表示
6 ノード	次の値より大きい	66	5 分	重大として表示

20. アラーム ルール 2 に SNMP トラップの送信設定を行う場合は、手順 17 を参照して設定を行ってください。
※SNMP トラップ送信を設定する場合には後述の 7.1.3 項の操作を行ってください。
21. [次へ]をクリックします。

22. ルールのリセット 1 に SNMP トラップの送信設定を行う場合は、手順 17 を参照して設定を行ってください。
※SNMP トラップ送信を設定する場合には後述の 7.1.3 項の操作を行ってください。

ルールのリセット 1

IF

警告または重大の条件または状態が解消されました

THEN

アラームを次のようにリセットします: *

E メール通知を送信 ☐

SNMP トラップを送信 ☒

スクリプトを実行 ☐

高度なアクションの追加

キャンセル 戻る 次へ

23. [次へ]をクリックします。

キャンセル 戻る **次へ**

24. 左下の[このアラームを有効にする]が有効になっていることを確認し、[作成]をクリックします。

確認

アラーム名 クラスタノードのメモリ使用率

説明 クラスタノードのメモリ使用率を監視するアラーム

ターゲット すべて ホスト オン vsan (3)

アラーム ルール

IF ホストのメモリ使用率 次の値より大きい 64 % for 5 分

THEN 以下の方法でアラームをトリガ ⚠ 警告

または

IF ホストのメモリ使用率 次の値より大きい 95 % for 5 分

THEN 以下の方法でアラームをトリガ ① 重大

ルールのリセット

警告または重大の条件または状態が解消された場合

THEN 以下の方法でアラームをトリガ ② 正常

このアラームを有効にする ☒

キャンセル 戻る **作成**

手順 17、20、22 で[繰り返し]にチェックした場合は、確認画面で繰り返す時間を設定できます。

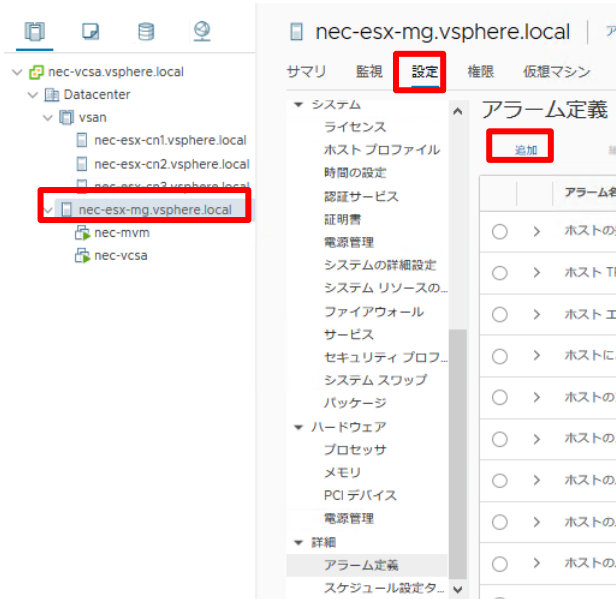
以下の間隔でアクションの繰り返し 10 分 (確認されるか緑色にリセットされるまで)

25. 作成したアラーム定義を確認します。([最終更新日]をクリックしてソートすると上の方にできます。)

アラーム定義

追加 編集 有効化/無効化 削除						
	アラーム名	オブジェクトタイプ	定義範囲	有効	最終更新日	
☐	クラスタノードのメモリ使用率	ホスト	このオブジェクト	有効	2021/04/07 16:49:03	
	名前	クラスタノードのメモリ使用率				
	説明	クラスタノードのメモリ使用率を監視するアラーム				
	ターゲット	クラスタ vsan 内のすべての ホスト				
	アラーム ルール	ホストのメモリ使用率 次の値より大きい 95%/5 分の場合、 ⓘ 重大 としてアラームをトリガする OR ホストのメモリ使用率 次の値より大きい 64%/5 分の場合、 ⚠ 警告 としてアラームをトリガする				
	最終更新日	2021/04/07 16:49:03				
☐	クラスタノードのCPU使用率	ホスト	このオブジェクト	有効	2021/04/07 16:45:28	
	名前	クラスタノードのCPU使用率				
	説明	クラスタノードの CPU 使用率を監視するアラーム				
	ターゲット	クラスタ vsan 内のすべての ホスト				
	アラーム ルール	ホストの CPU 使用率 次の値より大きい 90%/5 分の場合、 ⓘ 重大 としてアラームをトリガする OR ホストの CPU 使用率 次の値より大きい 60%/5 分の場合、 ⚠ 警告 としてアラームをトリガする				
	最終更新日	2021/04/07 16:45:28				

26. 管理ノード[nec-esx-mg.vsphere.local]選択し、[設定] – [アラーム定義] – [追加]をクリックしていきます。



27. アラーム名[管理ノードの CPU 使用率]
 説明[管理ノードの CPU 使用率を監視するアラーム]
 ターゲットのタイプ[ホスト]を設定し、[次へ]をクリックします。
 名前とターゲット

アラーム名 *

管理ノードのCPU使用率

説明

管理ノードの CPU 使用率を監視するアラーム

ターゲットのタイプ *

ホスト

ターゲット

nec-esx-mg.vsphere.local

28. アラームルール 1 画面が表示されます。それぞれの値を設定します。[ホストの CPU 使用率]、[次の値より大きい]、[75]、[5 分]、[警告として表示]を選択します。SNMP トラップの送信設定を行う場合はこのまま手順 29 に進んでください。SNMP トラップの送信設定を行わない場合は手順 29 を省略し手順 30 に進んでください。

アラームルール1



IF

ホストの CPU 使用率

次の値より大きい 75 % for 5 分 トリガをさらに追加

THEN

アラームをトリガーして * 警告として表示

E メール通知を送信 ☐

SNMP トラップを送信 ☐

スクリプトを実行 ☐

高度なアクションの追加

29. SNMP トラップの送信を設定する場合は、[SNMP トラップを送信]にチェックをいれます。アラームを繰り返し送信する場合は[繰り返し]をチェックします。

※SNMPトラップ送信を設定する場合には後述の 7.1.3 項の操作を行ってください。



SNMP トラップを送信 ☒ ☒ 繰り返し ⓘ

スクリプトを実行 ☐

30. [他のルールを追加]をクリックします。



他のルールを追加 重複ルール ルールの削除

31. アラームルール 2 画面が表示されます。それぞれの値を設定します。[ホストの CPU 使用率]、[次の値より大きい]、[90]、[5 分]、[重大として表示]を選択します。

SNMP の送信設定を行う場合はこのまま手順 32 に進んでください。SNMP の送信設定を行わない場合は手順 32、34 を省略し手順 33、35 に進んでください。

アラームルール 2



IF

ホストの CPU 使用率

次の値より大きい 90 % for 5 分 トリガをさらに追加

THEN

アラームをトリガーして * 重大として表示

E メール通知を送信 ☐

SNMP トラップを送信 ☐

スクリプトを実行 ☐

高度なアクションの追加

32. アラーム ルール 2 に SNMP トラップの送信設定を行う場合は、手順 29 を参照して設定を行ってください。
※SNMP トラップ送信を設定する場合には後述の 7.1.3 項の操作を行ってください。

33. [次へ]をクリックします。

キャンセル

戻る

次へ

34. ルールのリセット 1 に SNMP トラップの送信設定を行う場合は、手順 29 を参照してそれぞれ設定を行ってください。

※SNMPトラップ送信を設定する場合には後述の 7.1.3 項の操作を行ってください。

ルールのリセット 1

IF

警告または重大の条件または状態が解消されました

THEN

アラームを次のようにリセットします: *

E メール通知を送信 ☐

SNMP トラップを送信 ☒

スクリプトを実行 ☐

高度なアクションの追加

35. [次へ]をクリックします。

キャンセル

戻る

次へ

36. 確認画面が表示されます。左下の「このアラームを有効にする」がオンになっていることを確認し、[作成]をクリックします。

確認

アラーム名 管理ノードのCPU使用率

説明 管理ノードの CPU 使用率を監視するアラーム

ターゲット nec-esx-mg.vsphere.local

アラーム ルール

IF ホストの CPU 使用率 次の値より大きい 75 % for 5 分

THEN 以下の方法でアラームをトリガ ⚠ 警告

または

IF ホストの CPU 使用率 次の値より大きい 90 % for 5 分

THEN 以下の方法でアラームをトリガ 🚫 重大

ルールのリセット

警告または重大の条件または状態が解消された場合

THEN 以下の方法でアラームをトリガ ✅ 正常

このアラームを有効にする ☒

キャンセル

戻る

作成

手順 29、32、34 で[繰り返し]にチェックした場合は、確認画面で繰り返す時間を設定できます。

以下の間隔でアクションの繰り返し 10 分 (確認されるか緑色にリセットされるまで)

37. 続けて同じくアラーム定義の追加をし、
 アラーム名[管理ノードのメモリ使用率]、
 説明[管理ノードの CPU 使用率を監視するアラーム]
 ターゲットのタイプ[ホスト]を設定し、[次へ]をクリックします。

名前とターゲット ×

アラーム名 * 管理ノードのメモリ使用率

説明 管理ノードのメモリ使用率を監視するアラーム

ターゲットのタイプ * ホスト

ターゲット nec-esx-mg.vsphere.local

38. それぞれ、[ホストのメモリ使用率]、[次の値より大きい]、[90]、[5 分]、[警告として表示]を選択します。
 SNMP トラップの送信設定を行う場合はこのまま手順 39 に進んでください。SNMP のトラップ送信設定を行わない場合は手順 39 を省略し手順 40 に進んでください。

アラーム ルール1 ×

IF

ホストのメモリ使用率

次の値より大きい 90 に 5 分 トリガをさらに追加

THEN

アラームをトリガーして * 警告として表示

E メール通知を送信 ☐

SNMP トラップを送信 ☐

スクリプトを実行 ☐

[高度なアクションの追加](#)

他のルールを追加
重複ルール
ルールの削除

39. SNMP トラップの送信を設定する場合は、[SNMP トラップを送信]にチェックをいれます。アラームを繰り返し送信する場合は[繰り返し]をチェックします。

SNMP トラップを送信 ☒ ☒ 繰り返し ⓘ 操作を行ってください。

スクリプトを実行 ☐

40. [他のルールを追加]をクリックします。



41. それぞれ、[ホストのメモリ使用率]、[次の値より大きい]、[95]、[5 分]、[重大として表示]を選択します。SNMP の送信設定を行う場合はこのまま手順 42 に進んでください。SNMP の送信設定を行わない場合は手順 42、44 を省略し手順 43、45 に進んでください。

アラーム ルール 2

IF

ホストのメモリ使用率

次の値より大きい 95 % to 5 分 リガをさらに追加

THEN

アラームをトリガーして *

重大として表示

E メール通知を送信 ☐

SNMP トラップを送信 ☐

スクリプトを実行 ☐

高度なアクションの追加

42. アラーム ルール 2 に SNMP トラップの送信設定を行う場合は、手順 39 を参照してそれぞれ設定を行ってください。
- ※SNMPトラップ送信を設定する場合には後述の 7.1.3 項の操作を行ってください。

43. [次へ]をクリックします。

キャンセル 戻る 次へ

44. ルールのリセット 1 画面が表示されます。ルールのリセット 1 に SNMP トラップの送信設定を行う場合は、手順 39 を参照してそれぞれ設定を行ってください。

※SNMPトラップ送信を設定する場合には後述の 7.1.3 項の操作を行ってください。

ルールのリセット 1

IF

警告または重大の条件または状態が解消されました

THEN

アラームを次のようにリセットします: *

Eメール通知を送信 ☐

SNMP トラップを送信 ☒

スクリプトを実行 ☐

高度なアクションの追加

45. [次へ]をクリックします。

キャンセル

戻る

次へ

46. 確認画面が表示されます。左下の「このアラームを有効にする」がオンになっていることを確認し、[作成]をクリックします。

確認

アラーム名 管理ノードのメモリ使用率

説明 管理ノードのメモリ使用率を監視するアラーム

ターゲット `nec-esx-mg.vsphere.local`

アラーム ルール

IF ホストのメモリ使用率 次の値より大きい 90 % for 5 分

THEN 以下の方法でアラームをトリガ ⚠ 警告

または

IF ホストのメモリ使用率 次の値より大きい 95 % for 5 分

THEN 以下の方法でアラームをトリガ 🚨 重大

ルールのリセット

警告または重大の条件または状態が解消された場合

THEN 以下の方法でアラームをトリガ ✅ 正常

このアラームを有効にする ☒

キャンセル 戻る **作成**

手順 39、42、44 で[繰り返し]にチェックした場合は、確認画面で繰り返す時間を設定できます。

以下の間隔でアクションの繰り返し 10 分 (確認されるか緑色にリセットされるまで)

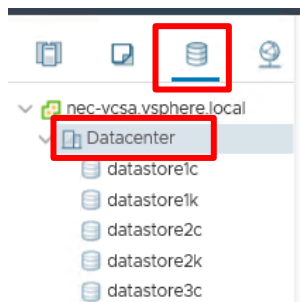
47. 作成したアラーム定義を確認します。([最終更新日]をクリックしてソートすると上の方にできます。)

アラーム定義

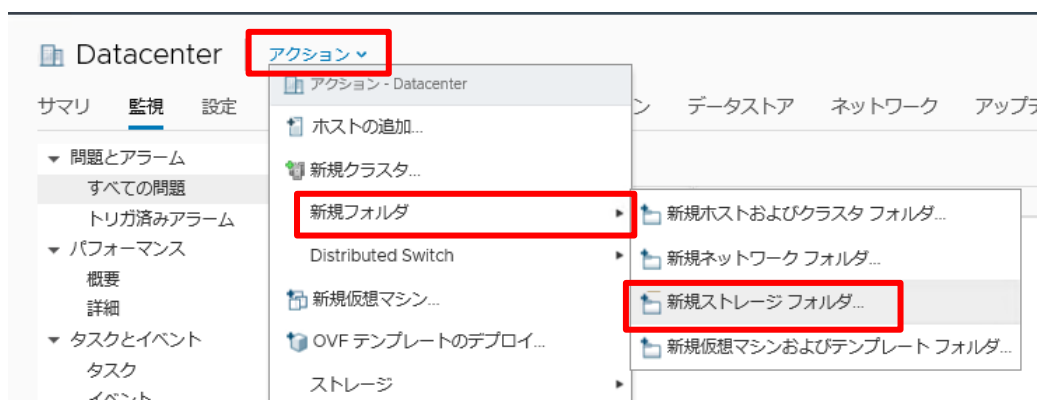
追加 編集 有効化/無効化 削除

	アラーム名	オブジェクトタイプ	定義範囲	有効	最終更新日
☐	管理ノードのメモリ使用率	ホスト	このオブジェクト	有効	2021/04/07 17:00:26
	名前	管理ノードのメモリ使用率			
	説明	管理ノードのメモリ使用率を監視するアラーム			
	ターゲット	ホスト			
	アラーム ルール	ホストのメモリ使用率 次の値より大きい 95%/5 分の場合、 ⓘ 重大 としてアラームをトリガする OR ホストのメモリ使用率 次の値より大きい 90%/5 分の場合、 ⓘ 警告 としてアラームをトリガする			
	最終更新日	2021/04/07 17:00:26			
☐	管理ノードのCPU使用率	ホスト	このオブジェクト	有効	2021/04/07 16:57:59
	名前	管理ノードのCPU使用率			
	説明	管理ノードの CPU 使用率を監視するアラーム			
	ターゲット	ホスト			
	アラーム ルール	ホストの CPU 使用率 次の値より大きい 90%/5 分の場合、 ⓘ 重大 としてアラームをトリガする OR ホストの CPU 使用率 次の値より大きい 75%/5 分の場合、 ⓘ 警告 としてアラームをトリガする			
	最終更新日	2021/04/07 16:57:59			

48. [ストレージ]ビューを開き、[Datacenter]をクリックします。



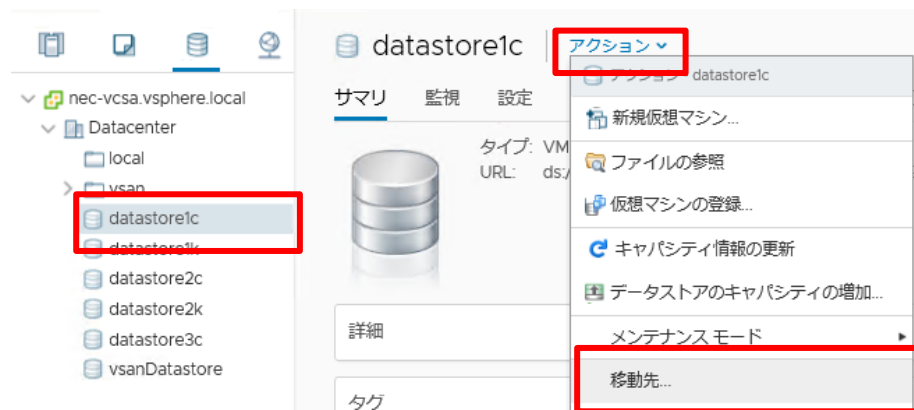
49. [アクション] – [新規フォルダ] – [新規ストレージフォルダ]とクリックしていきます。



50. [local]と入力し、[OK]をクリックします。



51. [datastoreNc](※)を選択し、[アクション] - [移動先]をクリックしていきます。
(※datastoreNc の N は各クラスターノードに合わせた数字となっています。)



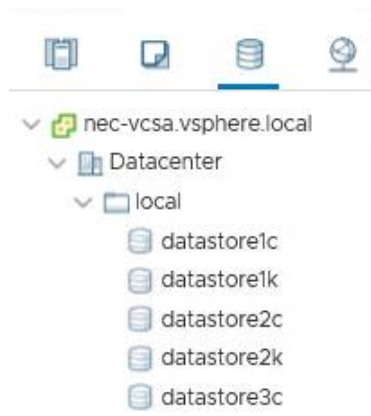
52. [local]を選択し、[OK]をクリックしてください。



53. datastore1k と datastore2k、すべての datastoreNc に対しての手順 51、52 を実施してください。
(※datastoreNc の N は各クラスターノードに合わせた数字となっています。)

54. 移動後、以下のように local フォルダ内に datastore1k、datastore2k、datastoreNc が移動されていることを確認します。

(※datastoreNc の N は各クラスターノードに合わせた数字となっています。)



55. [local]を選択し、[設定] – [アラーム定義] – [追加]をクリックしていきます。



56. アラーム名[local datastore のディスク使用率]
説明[local datastore のディスク使用率を監視するアラーム]
ターゲットのタイプ[データストア]をそれぞれ設定し、[次へ]をクリックします。

名前とターゲット

アラーム名 *

local datastoreのディスク使用率

説明

local datastoreのディスク使用率を監視するアラーム

ターゲットのタイプ *

データストア

ターゲット

すべて データストア オン local (5)

57. アラームルール 1 が表示されます。それぞれの値を設定します。それぞれ、[データストアディスクの使用率]、[次の値より大きい]、[75]、[警告として表示]を選択します。

SNMP トラップの送信設定を行う場合はこのまま手順 58 に進んでください。SNMP トラップの送信設定を行わない場合は手順 58 を省略し手順 59 に進んでください。

アラームルール1

IF

データストアディスクの使用率 次の値より大きい 75 %

トリガをさらに追加

THEN

アラームをトリガーして * 警告として表示

E メール通知を送信 ☐

SNMP トラップを送信 ☐

スクリプトを実行 ☐

他のルールを追加 重複ルール ルールの削除

58. SNMP トラップの送信を設定する場合は、[SNMP トラップを送信]にチェックをいれます。アラームを繰り返し送信する場合は[繰り返し]をチェックします。

※SNMPトラップ送信を設定する場合には後述の 7.1.3 項の操作を行ってください。

SNMP トラップを送信 ☒ 繰り返し ⓘ

スクリプトを実行 ☐

59. [他のルールを追加]をクリックします。

他のルールを追加 重複ルール ルールの削除

60. アラームルール 2 が表示されます。それぞれ、[データストアディスクの使用率]、[次の値より大きい]、[85]、[重大として表示]を選択します。

SNMP の送信設定を行う場合はこのまま手順 61 に進んでください。SNMP の送信設定を行わない場合は手順 61、63 を省略し手順 62、64 に進んでください。

アラームルール 2

IF

データストア ディスクの使用率 次の値より大きい 85 %

トリガをさらに追加

THEN

アラームをトリガーして * 重大として表示

E メール通知を送信 ☐

SNMP トラップを送信 ☐

スクリプトを実行 ☐

61. アラーム ルール 2 に SNMP トラップの送信設定を行う場合は、手順 58 を参照して設定を行ってください。
※SNMP トラップ送信を設定する場合には後述の 7.1.3 項の操作を行ってください。

62. [次へ]をクリックします。

キャンセル 戻る 次へ

63. ルールのリセット 1 が表示されます。ルールのリセット 1 に SNMP トラップの送信設定を行う場合は、手順 58 を参照して設定を行ってください。

※SNMPトラップ送信を設定する場合には後述の 7.1.3 項の操作を行ってください。

ルールのリセット 1

IF

警告または重大の条件または状態が解消されました

THEN

アラームを次のようにリ
セットします: *

E メール通知を送信 ☐

SNMP トラップを送信 ☒

スクリプトを実行 ☐

64. 確認画面が表示されます。左下の「このアラームを有効にする」が有効になっていることを確認し、[作成]をクリックします。

確認

アラーム名 local datastoreのディスク使用率

説明 local datastoreのディスク使用率を監視するアラーム

ターゲット すべて データストア オン ☐ local (5)

アラーム ルール

IF データストア ディスクの使用率 次の値より大きい 75 %

THEN 以下の方法でアラームをトリガ ⚠ 警告

または

IF データストア ディスクの使用率 次の値より大きい 85 %

THEN 以下の方法でアラームをトリガ ⚠ 重大

ルールのリセット

警告または重大の条件または状態が解消された場合

THEN 以下の方法でアラームをトリガ ✅ 正常

このアラームを有効にする ☒

キャンセル 戻る **作成**

手順 58、61、63 で[繰り返し]にチェックした場合は、繰り返す時間を設定できます。

以下の間隔でアクションの繰り返し **10** 分 (確認されるか緑色にリセットされるまで)

65. 作成したアラーム定義を確認します。([最終更新日]をクリックしてソートすると上の方にできます。)

アラーム定義					
追加 編集 有効化/無効化 削除					
	アラーム名	オブジェクトタイプ	定義範囲	有効	最終更新日
☐	local datastoreのディスク使用率	データストア	このオブジェクト	有効	2021年04月09日 10:59:33
名前 local datastoreのディスク使用率 説明 local datastoreのディスク使用率を監視するアラーム ターゲット ストレージ フォルダ local 内のすべての データストア アラーム ルール データストア ディスクの使用率 次の値より大きい 85% の場合、🔴 重大 としてアラームをトリガする OR データストア ディスクの使用率 次の値より大きい 75% の場合、🟡 警告 としてアラームをトリガする 最終更新日 2021年04月09日 10:59:33					

66. [vsanDatastore]を選択し、[設定] – [アラーム定義] – [追加]をクリックしていきます。

📁 nec-vcsa.vsphere.local

📁 Datacenter

📁 local

📁 datastore1c

📁 datastore1k

📁 datastore2c

📁 datastore2k

📁 datastore3c

📁 vsanDatastore

vsanDatastore

アクション ▾

サマリ 監視 **設定** 権限 ファイル

▼ 詳細

アラーム定義

スケジュール設定タ...

全般

ハードウェア アクセラレ...

アラーム定義

追加

📁 アラーム

☐ > 強化

☐ > SIOC

67. アラーム名[vsan datastore のディスク使用率]

説明[vsan datastore のディスク使用率を監視するアラーム]

ターゲットのタイプ[データストア]をそれぞれ設定し、[次へ]をクリックします。

名前とターゲット

アラーム名 * vsan datastoreのディスク使用率

説明 vsan datastoreのディスク使用率を監視するアラーム

ターゲットのタイプ * データストア

ターゲット すべて データストア オン vsan (1)

68. アラーム ルール 1 画面が表示されます。[トリガを選択]で[データストアディスクの使用率]を選択します。それぞれの値を設定します。[次の値より大きい]、[クラスタのノード数に対応したしきい値(※)]、[警告として表示]を選択します。SNMPトラップの送信設定をする場合はこのまま手順 69 に進んでください。SNMPトラップの送信設定を行わない場合は手順 69 を省略し手順 70 に進んでください。

(※下記の▽vsan datastore のディスク使用率/アラーム ルール 1 設定値一覧を参照)

アラーム ルール 1

IF データストア ディスクの使用率 次の値より大きい 70 %

トリガをさらに追加

THEN

アラームをトリガーして * 警告として表示

E メール通知を送信

SNMP トラップを送信

スクリプトを実行

▽vsan datastore のディスク使用率/アラーム ルール 1 設定値一覧

クラスタのノード数	演算子	しきい値(%)	時間(分)	アクション
3 ノード	次の値より大きい	70	5 分	警告として表示
4 ノード	次の値より大きい	52	5 分	警告として表示
5 ノード	次の値より大きい	70	5 分	警告として表示
6 ノード	次の値より大きい	58	5 分	警告として表示

69. SNMP トラップの送信を設定する場合は、[SNMP トラップを送信]にチェックをいれます。アラームを繰り返し送信する場合は[繰り返し]をチェックします。

※SNMPトラップ送信を設定する場合には後述の 7.1.3 項の操作を行ってください。

SNMP トラップを送信 ☒ ☒ 繰り返し ⓘ

スクリプトを実行 ☐

70. [他のルールを追加]をクリックします。

他のルールを追加 重複ルール ルールの削除

71. アラーム ルール 2 画面が表示されます。[トリガを選択]で[データストアディスクの使用率]を選択します。それぞれの値を設定します、[次の値より大きい]、[クラスタのノード数に対応したしきい値(※)]、[重大として表示]を選択しています。

SNMP トラップの送信設定を行う場合はこのまま手順 72 に進んでください。SNMP トラップの送信設定を行わない場合は手順 72、74 を省略し手順 73、75 に進んでください。

(※下記の▽vsan datastore のディスク使用率/アラーム ルール 2 設定値一覧を参照)

アラーム ルール 2

IF

データストアディスクの使用率 次の値より大きい 75 %

トリガをさらに追加

THEN

アラームをトリガーして * 重大として表示

E メール通知を送信 ☐

SNMP トラップを送信 ☐

スクリプトを実行 ☐

▽vsan datastore のディスク使用率/アラーム ルール 2 設定値一覧

クラスタのノード数	演算子	しきい値(%)	時間(分)	アクション
3 ノード	次の値より大きい	75	5 分	重大として表示
4 ノード	次の値より大きい	56	5 分	重大として表示
5 ノード	次の値より大きい	75	5 分	重大として表示
6 ノード	次の値より大きい	62	5 分	重大として表示

72. アラーム ルール 2 に SNMP トラップの送信設定を行う場合は、手順 69 を参照し設定を行ってください。
※SNMP トラップ送信を設定する場合には後述の 7.1.3 項の操作を行ってください。

73. [次へ]をクリックします。



74. ルールのリセット 1 に SNMP トラップの送信設定を行う場合は、手順 69 を参照して設定を行ってください。
※SNMP トラップ送信を設定する場合には後述の 7.1.3 項の操作を行ってください。



75. [次へ]をクリックします。



76. 確認画面が表示されます。左下の「このアラームを有効にする」が有効になっていること確認して、[作成]をクリック

確認

×

アラーム名

vsan datastoreのディスク使用率

説明

vsan datastoreのディスク使用率を監視するアラーム

ターゲット

すべて データストア オン vsan (1)

アラームルール

IF データストア ディスクの使用率 次の値より大きい 70 %

THEN 以下の方法でアラームをトリガ 警告

または

IF データストア ディスクの使用率 次の値より大きい 80 %

THEN 以下の方法でアラームをトリガ 重大

ルールのリセット

警告または重大の条件または状態が解消された場合

THEN 以下の方法でアラームをトリガ 正常

このアラームを有効にする ☒

キャンセル

戻る

作成

手順 69、72、74 で[繰り返し]にチェックした場合は、繰り返す時間を設定できます。

以下の間隔でアクションの繰り返し 分 (確認されるか緑色にリセットされるまで)

77. 作成したアラーム定義を確認します。([最終更新日]をクリックしてソートすると上の方にできます。)

アラーム定義

追加							編集	有効化/無効化	削除
		アラーム名	オブジェクトタイプ	定義範囲	有効	最終更新日			
☐	▼	vsan datastoreのディスク使用率	データストア	 このオブジェクト	有効	2021年04月09日 11:06:32			
		名前	vsan datastoreのディスク使用率						
		説明	vsan datastoreのディスク使用率を監視するアラーム						
		ターゲット	ストレージ フォルダ vsan 内のすべての データストア						
		アラームルール	データストア ディスクの使用率 次の値より大きい 80% の場合、  重大 としてアラームをトリガする OR データストア ディスクの使用率 次の値より大きい 70% の場合、  警告 としてアラームをトリガする						

事前構成済みのアラームを直接変更するのは非推奨です。

事前構成済みのアラームに対して変更(通知設定)を行う場合は、事前構成済みのアラームを無効にし、同様の内容のアラーム定義を 7.1.2 項を参考にして新規に作成をしてください。

変更(通知設定)は新規に作成したアラーム定義に対して行ってください。

7.1.3 SNMP 設定

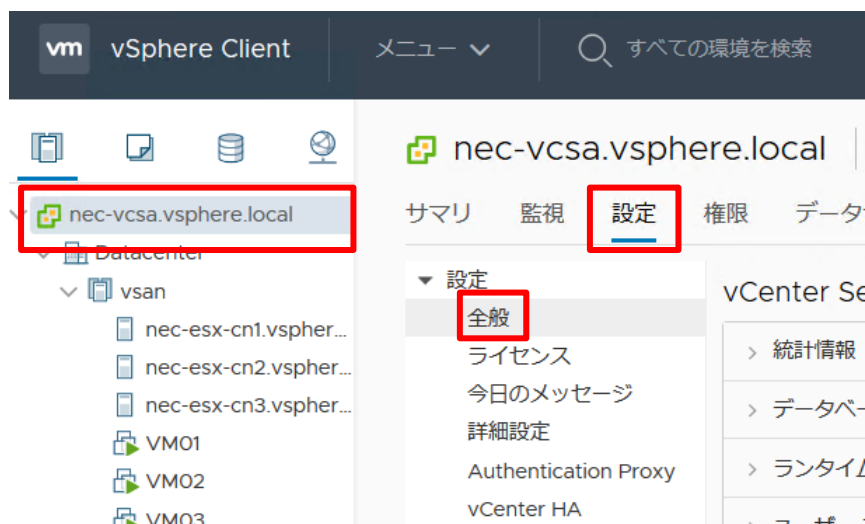
本項では、7.1.2 項で作成したアラーム定義に SNMP トラップの送信設定を行う場合に必要な手順です。
7.1.2 項で作成したアラーム定義に SNMP トラップの送信設定を行わない場合、本手順は不要です。

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)
-	SNMP 受信者のホスト名または IP アドレス	
-	SNMP 受信者のポート番号	
-	SNMP 受信をするコミュニティ識別子	

手順

1. [nec-vcsa.vsphere.local]を選択し、[設定]ー[全般]をクリックします。



2. [編集]をクリックします。



3. 全般設定の編集ダイアログが表示されます。左側のメニューから[SNMP レシーバ]をクリックします。

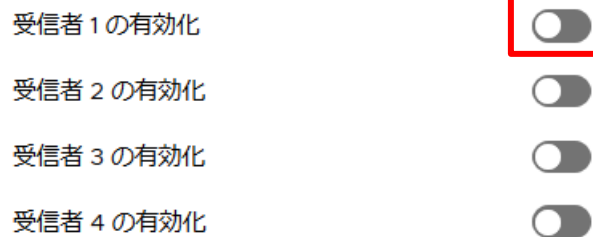
vCenter Server の全般設定の編集



4. SNMP レシーバ画面が表示されます。受信者 1 の有効化を有効にします。

SNMP レシーバ

SNMP アラートを受信する場所を選択します。



5. [プライマリ受信者 URL]、[受信者のポート]、[コミュニティ スtring]を入力します。

[プライマリ受信者 URL]:「SNMP 受信者のホスト名または IP アドレス」

[受信者のポート]:「SNMP 受信者のポート番号」

[コミュニティ スtring]:「SNMP 受信をするコミュニティ識別子」

SNMP レシーバ

SNMP アラートを受信する場所を選択します。

受信者 1 の有効化 ☒

プライマリ受信者 URL

受信者のポート

コミュニティ スtring

受信者 2 の有効化 ☐

受信者 3 の有効化 ☐

受信者 4 の有効化 ☐

6. [保存]をクリックします。



7. SNMP レシーバの設定がされていることを確認します。

サマリ 監視 設定 権限 データセンター ホストおよびクラスタ 仮想マシン データストア

▼ 設定

- 全般
 - ライセンス
 - 今日のメッセージ
 - 詳細設定
 - Authentication Proxy
 - vCenter HA
- ▼ 詳細
 - アラーム定義
 - スケジュール設定タ...
 - キー管理サーバ
 - ストレージ プロバイダ
- ▼ vSAN
 - 更新
 - インターネット接続

vCenter Server 設定

> 統計情報	予想される必要な容量: 16.71 GB
> データベース	最大接続数: 50
> ランタイム設定	vCenter Server 名: nec-vcsa.vsphere.local
> ユーザー ディレクトリ	タイムアウト: 60 秒
> メール	メール サーバ: 192.168.10.253
SNMP レシーバ	
プライマリ受信者 URL	
受信者 1 の有効化	true
受信者のポート	
コミュニティ スtring	

7.2 ESMPRO での通報設定

本項では、ESMPRO/ServerManager での通報定手順について記載します。ESMPRO/ServerManager が受信した通報を、単一の形式(SNMPトラップ)に変換して他社製管理コンソールに送信します。

本項は必須の設定ではありません。必要に応じて下記手順の作業を行ってください。

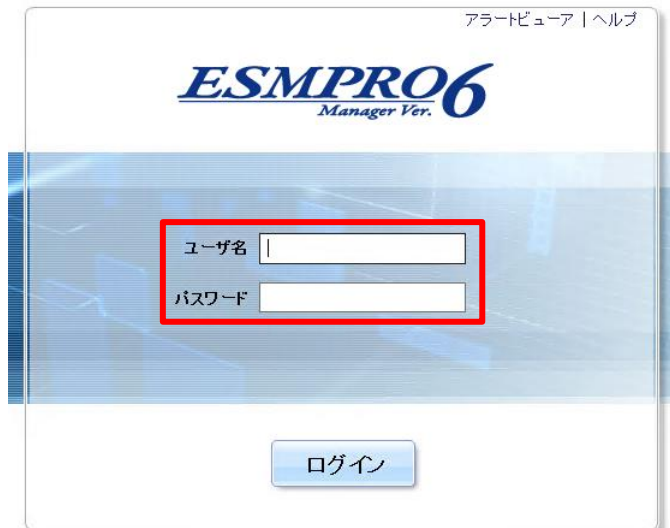
手順実施に必要なパラメータ

ドキュメント	項目	パラメータ/値 (メモ用)
-	SNMP 受信者のホスト名または IP アドレス	
-	SNMP 受信をするコミュニティ識別子	

1. 管理 VM に管理者権限を有するユーザでサインインし、デスクトップの ESMPRO/ServerManager をダブルクリックして起動します。

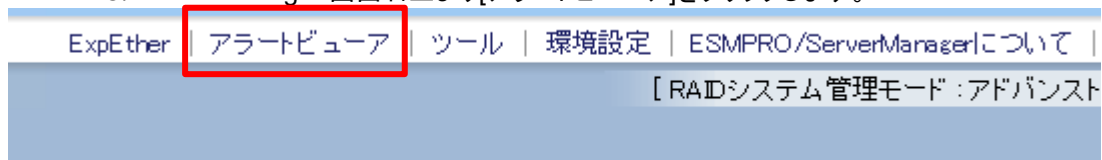


2. ESMPRO/ ServerManager を開きます。ユーザ名とパスワードを入力し、ログインしてください。

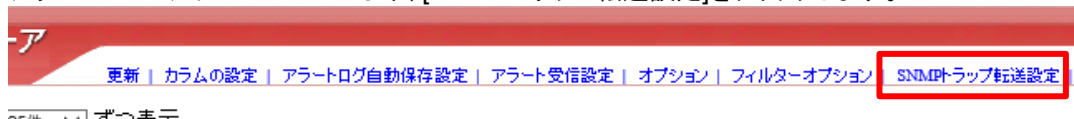


Copyright (C) 2004–2020 NEC Corporation. All Rights Reserved.

3. ESMPRO/ ServerManager 画面右上より[アラートビューア]をクリックします。



4. アラートビューア右上のメニューより、[SNMPトラップ転送設定]をクリックします。



5. SNMP トラップ転送設定が開きます。[ホスト名/IP アドレス]と、[コミュニティ名]を入力します。[追加]をクリックします。

[ホスト名/IP アドレス]:「SNMP 受信者のホスト名または IP アドレス」

[コミュニティ名]:「SNMP 受信をするコミュニティ識別子」

8 注意制限事項

8.1 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。

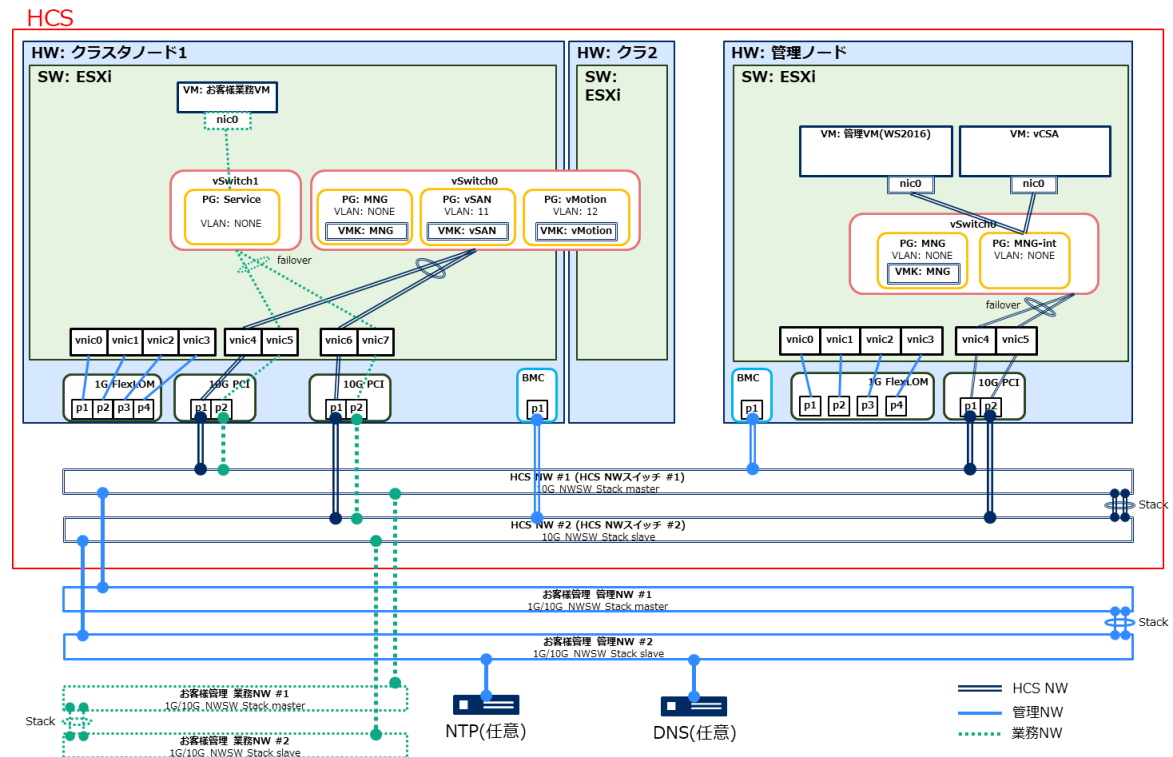
NEC iLO 5 2.10 Oct 30 2019		情報 - セキュリティダッシュボード				
情報 システム情報 ファームウェア & OSソフトウェア iLO連携 リモートコンソール & メディア 電力 & 温度 パフォーマンス iLO専用ネットワークポート iLO共有ネットワークポート 管理 セキュリティ マネジメント EXPRESSBUILDER	概要	セキュリティダッシュボード	セッションリスト	iLOイベントログ	インテグレートドマネジメントログ	セキュリティログ
	全体セキュリティステータス: リスク					
	セキュリティ状態 本番環境		サーバー構成ロック: 無効			
	セキュリティパラメーター				↓ステータス	状態
	IPMI/DCMI over LAN				♥ リスク	有効
	iLO RBSUへのログイン要求				♥ リスク	無効
	セキュアブート				♥ リスク	無効
	パスワードの複雑さ				♥ リスク	無効
	デフォルトSSL証明書が使用中				♥ リスク	真

付録 A) ネットワーク結線

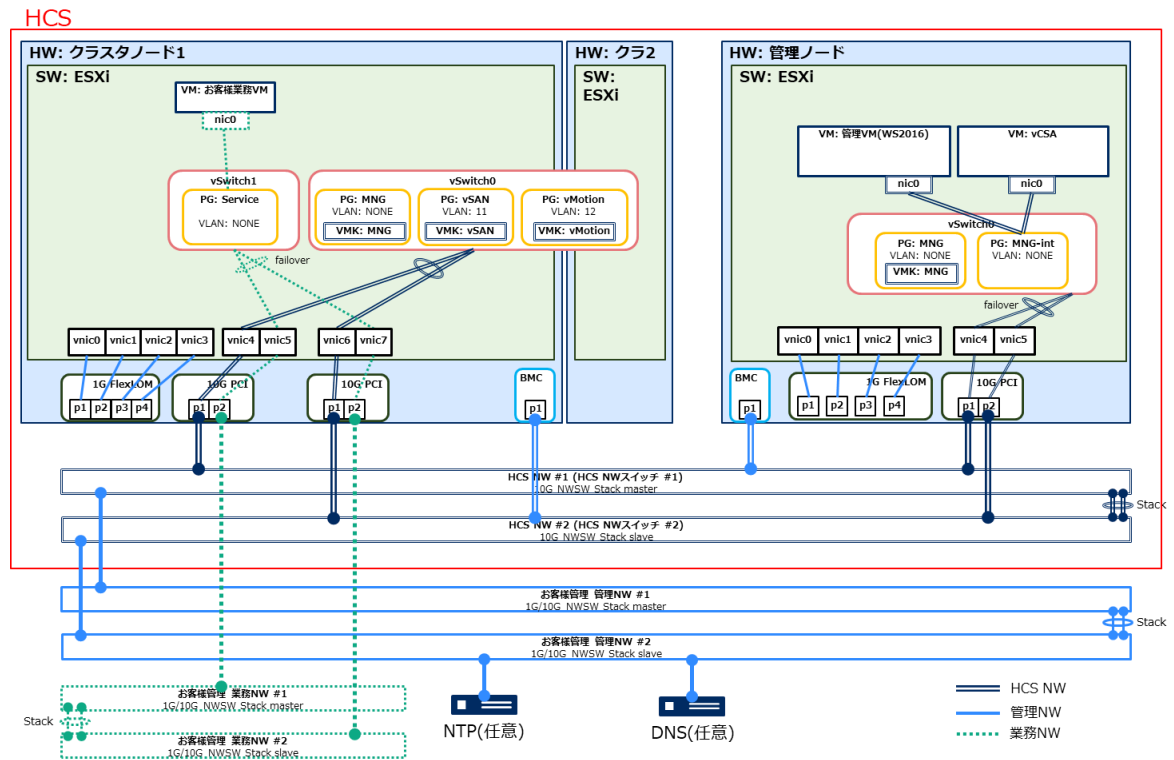
NEC Hyper Converged System の管理ノード、クラスタードと、HCS NW スイッチ間のネットワークケーブルの接続について、説明します。

NEC Hyper Converged System Trust のネットワーク構成は下記になります。

業務 NW 兼用あり



業務 NW 兼用なし

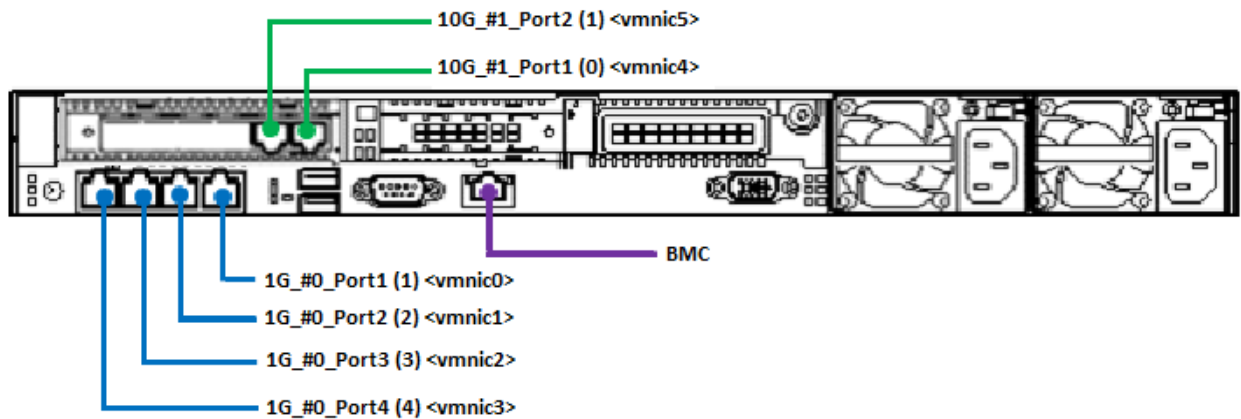


I. サーバ LAN ポート

管理ノードには BMC(iLO)と 1G LAN ポートが 4 つ、10G LAN ポートが 2 つ装着されています。BMC(iLO)および 10G_#1_Port1 (0)と 10G_#1_Port2 (1)を HCS NW スイッチに接続します。管理ノードの LAN ポートの配置は下記の図になります。

管理ノードには XSVR02-01 のラベルが本体前面のスライドタグに張り付けられています。

管理ノード(R120h-1M)

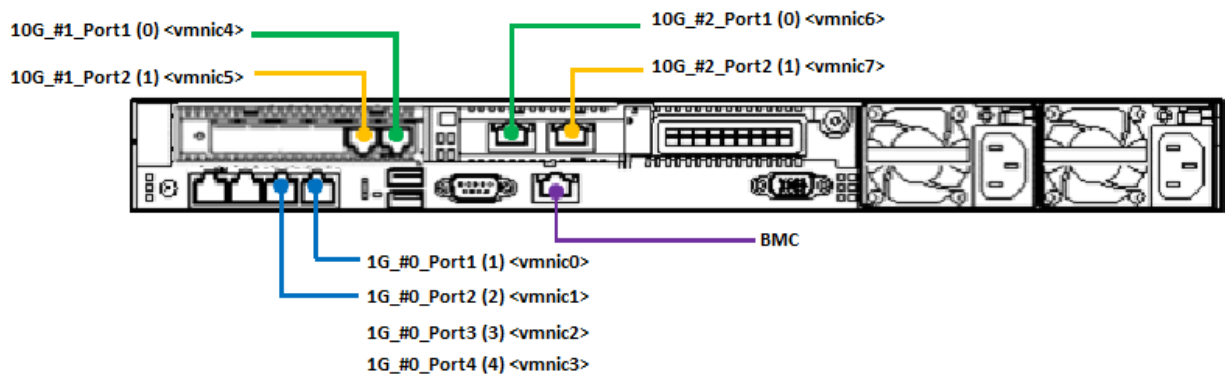


クラスタノードには BMC(iLO)と 1G LAN ポートが 4 つ、10G LAN ポートが 4 つ装着されています。

BMC(iLO)および 10G_#1_Port1 (0)と 10G_#2_Port1 (0)を HCS NW スイッチに接続します。クラスタノードの LAN ポートの配置は下記の図になります。

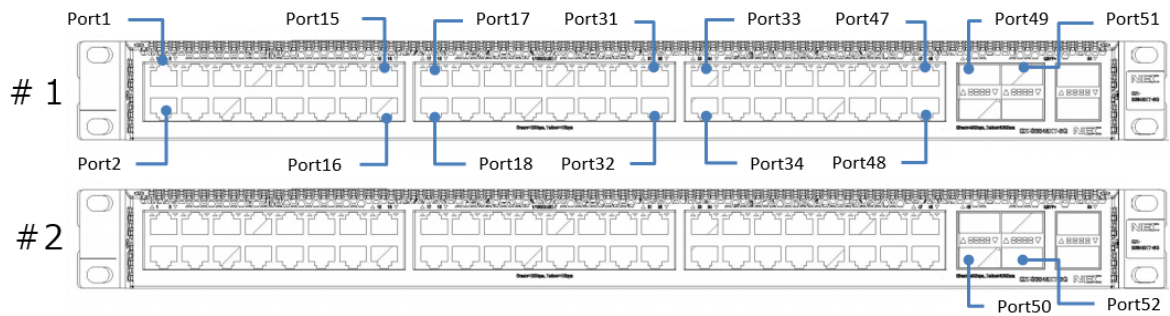
クラスタノードには XSVR01-0n (n はクラスタノード番号)のラベル本体前面のスライドタグに張り付けられています。

クラスタノード(R120h-1M)



II. HCS NW スイッチ(QX-S6648XT-6Q)

HCS NW スイッチのポート番号は下記になります。HCS NW スイッチには本体天面にラベルが張り付けられています。XESW01-01 のラベルが貼り付けられたスイッチが#1、XESW01-02 のラベルが貼り付けられたスイッチが#2 になります。HCS NW スイッチ#1 と 1HCS NW スイッチ#2 はスタックケーブル 2 本で接続し、冗長構成にします。



III. ネットワークケーブルの接続

1) スタックケーブルの接続

HCS NW スイッチ#1 と HCS NW スイッチ#2 をスタックケーブルで接続します。

①HCS NW スイッチ#1 の Port49 と HCS NW スイッチ#2 の Port50 をスタックケーブルで接続します。

②HCS NW スイッチ#1 の Port51 と HCS NW スイッチ#2 の Port52 をスタックケーブルで接続します。

2) LAN ケーブルの接続

管理ノード、クラスタノードの LAN ポートと HCS NW スイッチの LAN ポートを接続します。

下記表に従って接続してください。

増設クラスタを接続する場合は、既設のクラスタノード台数の+1 台目から増設クラスタノード数分を接続してください。

業務 NW 兼用あり

ネットワークケーブル接続						
Express5800/R120h-1M側					接続先(スイッチ)	
装置名	スロット	速度	ポート		装置名	ポート
R120h-1M 管理ノード	標準	1Gbps	BMC(iLO)	----->	HCS NWスイッチ #1	12
	拡張	1Gbps	1G #0 Port1 (1)	----->		
			1G #0 Port2 (2)	----->		
			1G #0 Port3 (3)	----->		
			1G #0 Port4 (4)	----->		
	10Gbps	10G #1 Port1 (0)	----->	HCS NWスイッチ #1	1	
10G #1 Port2 (1)	----->	HCS NWスイッチ #2	1			
Express5800/R120h-1M側					接続先(スイッチ)	
装置名	スロット	速度	ポート		装置名	ポート
R120h-1M クラスタノード 1台目	標準	1Gbps	BMC(iLO)	----->	HCS NWスイッチ #1	13
	拡張	1Gbps	1G #0 Port1 (1)	----->		
			1G #0 Port2 (2)	----->		
			1G #0 Port3 (3)	----->		
			1G #0 Port4 (4)	----->		
	10Gbps	10G #1 Port1 (0)	----->	HCS NWスイッチ #1	2	
		10G #1 Port2 (1)	----->	(10Gスイッチ/お客様管理 業務NW#1)		
		10G #2 Port1 (0)	----->	HCS NWスイッチ #2	2	
		10G #2 Port2 (1)	----->	(10Gスイッチ/お客様管理 業務NW#2)		
R120h-1M クラスタノード 2台目	標準	1Gbps	BMC(iLO)	----->	HCS NWスイッチ #1	14
	拡張	1Gbps	1G #0 Port1 (1)	----->		
			1G #0 Port2 (2)	----->		
			1G #0 Port3 (3)	----->		
			1G #0 Port4 (4)	----->		
	10Gbps	10G #1 Port1 (0)	----->	HCS NWスイッチ #1	3	
		10G #1 Port2 (1)	----->	(10Gスイッチ/お客様管理 業務NW#1)		
		10G #2 Port1 (0)	----->	HCS NWスイッチ #2	3	
		10G #2 Port2 (1)	----->	(10Gスイッチ/お客様管理 業務NW#2)		
R120h-1M クラスタノード 3台目	標準	1Gbps	BMC(iLO)	----->	HCS NWスイッチ #1	15
	拡張	1Gbps	1G #0 Port1 (1)	----->		
			1G #0 Port2 (2)	----->		
			1G #0 Port3 (3)	----->		
			1G #0 Port4 (4)	----->		
	10Gbps	10G #1 Port1 (0)	----->	HCS NWスイッチ #1	4	
		10G #1 Port2 (1)	----->	(10Gスイッチ/お客様管理 業務NW#1)		
		10G #2 Port1 (0)	----->	HCS NWスイッチ #2	4	
		10G #2 Port2 (1)	----->	(10Gスイッチ/お客様管理 業務NW#2)		

Express5800/R120h-1M側					接続先(スイッチ)	
装置名	スロット	速度	ポート		装置名	ポート
R120h-1M クラスターノード 4台目	標準	1Gbps	BMC(iLO)	----->	HCS NWスイッチ #1	16
	拡張	1Gbps	1G #0.Port1 (1)	----->		
			1G #0.Port2 (2)	----->		
			1G #0.Port3 (3)	----->		
			1G #0.Port4 (4)	----->		
		10Gbps	10G #1.Port1 (0)	----->	HCS NWスイッチ #1	5
			10G #1.Port2 (1)	----->	(10Gスイッチ/お客様管理 業務NW#1)	
			10G #2.Port1 (0)	----->	HCS NWスイッチ #2	5
			10G #2.Port2 (1)	----->	(10Gスイッチ/お客様管理 業務NW#2)	
R120h-1M クラスターノード 5台目	標準	1Gbps	BMC(iLO)	----->	HCS NWスイッチ #1	17
	拡張	1Gbps	1G #0.Port1 (1)	----->		
			1G #0.Port2 (2)	----->		
			1G #0.Port3 (3)	----->		
			1G #0.Port4 (4)	----->		
		10Gbps	10G #1.Port1 (0)	----->	HCS NWスイッチ #1	6
			10G #1.Port2 (1)	----->	(10Gスイッチ/お客様管理 業務NW#1)	
			10G #2.Port1 (0)	----->	HCS NWスイッチ #2	6
			10G #2.Port2 (1)	----->	(10Gスイッチ/お客様管理 業務NW#2)	
R120h-1M クラスターノード 6台目	標準	1Gbps	BMC(iLO)	----->	HCS NWスイッチ #2	12
	拡張	1Gbps	1G #0.Port1 (1)	----->		
			1G #0.Port2 (2)	----->		
			1G #0.Port3 (3)	----->		
			1G #0.Port4 (4)	----->		
		10Gbps	10G #1.Port1 (0)	----->	HCS NWスイッチ #1	7
			10G #1.Port2 (1)	----->	(10Gスイッチ/お客様管理 業務NW#1)	
			10G #2.Port1 (0)	----->	HCS NWスイッチ #2	7
			10G #2.Port2 (1)	----->	(10Gスイッチ/お客様管理 業務NW#2)	
R120h-1M クラスターノード 7台目	標準	1Gbps	BMC(iLO)	----->	HCS NWスイッチ #2	13
	拡張	1Gbps	1G #0.Port1 (1)	----->		
			1G #0.Port2 (2)	----->		
			1G #0.Port3 (3)	----->		
			1G #0.Port4 (4)	----->		
		10Gbps	10G #1.Port1 (0)	----->	HCS NWスイッチ #1	8
			10G #1.Port2 (1)	----->	(10Gスイッチ/お客様管理 業務NW#1)	
			10G #2.Port1 (0)	----->	HCS NWスイッチ #2	8
			10G #2.Port2 (1)	----->	(10Gスイッチ/お客様管理 業務NW#2)	
R120h-1M クラスターノード 8台目	標準	1Gbps	BMC(iLO)	----->	HCS NWスイッチ #2	14
	拡張	1Gbps	1G #0.Port1 (1)	----->		
			1G #0.Port2 (2)	----->		
			1G #0.Port3 (3)	----->		
			1G #0.Port4 (4)	----->		
		10Gbps	10G #1.Port1 (0)	----->	HCS NWスイッチ #1	9
			10G #1.Port2 (1)	----->	(10Gスイッチ/お客様管理 業務NW#1)	
			10G #2.Port1 (0)	----->	HCS NWスイッチ #2	9
			10G #2.Port2 (1)	----->	(10Gスイッチ/お客様管理 業務NW#2)	
R120h-1M クラスターノード 9台目	標準	1Gbps	BMC(iLO)	----->	HCS NWスイッチ #2	15
	拡張	1Gbps	1G #0.Port1 (1)	----->		
			1G #0.Port2 (2)	----->		
			1G #0.Port3 (3)	----->		
			1G #0.Port4 (4)	----->		
		10Gbps	10G #1.Port1 (0)	----->	HCS NWスイッチ #1	10
			10G #1.Port2 (1)	----->	(10Gスイッチ/お客様管理 業務NW#1)	
			10G #2.Port1 (0)	----->	HCS NWスイッチ #2	10
			10G #2.Port2 (1)	----->	(10Gスイッチ/お客様管理 業務NW#2)	
R120h-1M クラスターノード 10台目	標準	1Gbps	BMC(iLO)	----->	HCS NWスイッチ #2	16
	拡張	1Gbps	1G #0.Port1 (1)	----->		
			1G #0.Port2 (2)	----->		
			1G #0.Port3 (3)	----->		
			1G #0.Port4 (4)	----->		
		10Gbps	10G #1.Port1 (0)	----->	HCS NWスイッチ #1	11
			10G #1.Port2 (1)	----->	(10Gスイッチ/お客様管理 業務NW#1)	
			10G #2.Port1 (0)	----->	HCS NWスイッチ #2	11
			10G #2.Port2 (1)	----->	(10Gスイッチ/お客様管理 業務NW#2)	

業務 NW 兼用なし

ネットワークケーブル接続						
Express5800/R120h-1M側					接続先(スイッチ)	
装置名	スロット	速度	ポート		装置名	ポート
R120h-1M 管理ノード	標準	1Gbps	BMC(iLO)	----->	HCS NWスイッチ #1	21
	拡張	1Gbps	1G #0 Port1 (1)	----->		
			1G #0 Port2 (2)	----->		
			1G #0 Port3 (3)	----->		
			1G #0 Port4 (4)	----->		
	10Gbps	10G #1 Port1 (0)	----->	HCS NWスイッチ #1	1	
10G #1 Port2 (1)			----->	HCS NWスイッチ #2	1	
Express5800/R120h-1M側					接続先(スイッチ)	
装置名	スロット	速度	ポート		装置名	ポート
R120h-1M クラスターノード 1台目	標準	1Gbps	BMC(iLO)	----->	HCS NWスイッチ #1	22
	拡張	1Gbps	1G #0 Port1 (1)	----->		
			1G #0 Port2 (2)	----->		
			1G #0 Port3 (3)	----->		
			1G #0 Port4 (4)	----->		
	10Gbps	10G #1 Port1 (0)	----->	HCS NWスイッチ #1	2	
		10G #1 Port2 (1)	----->	(お客様管理 業務NW#1)		
		10G #2 Port1 (0)	----->	HCS NWスイッチ #2	2	
		10G #2 Port2 (1)	----->	(お客様管理 業務NW#2)		
	R120h-1M クラスターノード 2台目	標準	1Gbps	BMC(iLO)	----->	HCS NWスイッチ #1
拡張		1Gbps	1G #0 Port1 (1)	----->		
			1G #0 Port2 (2)	----->		
			1G #0 Port3 (3)	----->		
			1G #0 Port4 (4)	----->		
10Gbps		10G #1 Port1 (0)	----->	HCS NWスイッチ #1	3	
		10G #1 Port2 (1)	----->	(お客様管理 業務NW#1)		
		10G #2 Port1 (0)	----->	HCS NWスイッチ #2	3	
		10G #2 Port2 (1)	----->	(お客様管理 業務NW#2)		
R120h-1M クラスターノード 3台目		標準	1Gbps	BMC(iLO)	----->	HCS NWスイッチ #1
	拡張	1Gbps	1G #0 Port1 (1)	----->		
			1G #0 Port2 (2)	----->		
			1G #0 Port3 (3)	----->		
			1G #0 Port4 (4)	----->		
	10Gbps	10G #1 Port1 (0)	----->	HCS NWスイッチ #1	4	
		10G #1 Port2 (1)	----->	(お客様管理 業務NW#1)		
		10G #2 Port1 (0)	----->	HCS NWスイッチ #2	4	
		10G #2 Port2 (1)	----->	(お客様管理 業務NW#2)		
	R120h-1M クラスターノード 4台目	標準	1Gbps	BMC(iLO)	----->	HCS NWスイッチ #1
拡張		1Gbps	1G #0 Port1 (1)	----->		
			1G #0 Port2 (2)	----->		
			1G #0 Port3 (3)	----->		
			1G #0 Port4 (4)	----->		
10Gbps		10G #1 Port1 (0)	----->	HCS NWスイッチ #1	5	
		10G #1 Port2 (1)	----->	(お客様管理 業務NW#1)		
		10G #2 Port1 (0)	----->	HCS NWスイッチ #2	5	
		10G #2 Port2 (1)	----->	(お客様管理 業務NW#2)		
R120h-1M クラスターノード 5台目		標準	1Gbps	BMC(iLO)	----->	HCS NWスイッチ #1
	拡張	1Gbps	1G #0 Port1 (1)	----->		
			1G #0 Port2 (2)	----->		
			1G #0 Port3 (3)	----->		
			1G #0 Port4 (4)	----->		
	10Gbps	10G #1 Port1 (0)	----->	HCS NWスイッチ #1	6	
		10G #1 Port2 (1)	----->	(お客様管理 業務NW#1)		
		10G #2 Port1 (0)	----->	HCS NWスイッチ #2	6	
		10G #2 Port2 (1)	----->	(お客様管理 業務NW#2)		
	R120h-1M クラスターノード 6台目	標準	1Gbps	BMC(iLO)	----->	HCS NWスイッチ #1
拡張		1Gbps	1G #0 Port1 (1)	----->		
			1G #0 Port2 (2)	----->		
			1G #0 Port3 (3)	----->		
			1G #0 Port4 (4)	----->		
10Gbps		10G #1 Port1 (0)	----->	HCS NWスイッチ #1	7	
		10G #1 Port2 (1)	----->	(お客様管理 業務NW#1)		
		10G #2 Port1 (0)	----->	HCS NWスイッチ #2	7	
		10G #2 Port2 (1)	----->	(お客様管理 業務NW#2)		
R120h-1M クラスターノード 7台目		標準	1Gbps	BMC(iLO)	----->	HCS NWスイッチ #1
	拡張	1Gbps	1G #0 Port1 (1)	----->		
			1G #0 Port2 (2)	----->		
			1G #0 Port3 (3)	----->		
			1G #0 Port4 (4)	----->		
	10Gbps	10G #1 Port1 (0)	----->	HCS NWスイッチ #1	8	
		10G #1 Port2 (1)	----->	(お客様管理 業務NW#1)		
		10G #2 Port1 (0)	----->	HCS NWスイッチ #2	8	
		10G #2 Port2 (1)	----->	(お客様管理 業務NW#2)		

Express5800/R120h-1M側					接続先(スイッチ)	
装置名	スロット	速度	ポート		装置名	ポート
R120h-1M クラスタノード 8台目	標準	1Gbps	BMC(iLO)	----->	HCS NWスイッチ #1	29
	拡張	1Gbps	1G #0 Port1 (1)	----->		
			1G #0 Port2 (2)	----->		
			1G #0 Port3 (3)	----->		
			1G #0 Port4 (4)	----->		
		10Gbps	10G #1 Port1 (0)	----->	HCS NWスイッチ #1	9
			10G #1 Port2 (1)	----->	(お客様管理 業務NW#1)	
			10G #2 Port1 (0)	----->	HCS NWスイッチ #2	9
			10G #2 Port2 (1)	----->	(お客様管理 業務NW#2)	
R120h-1M クラスタノード 9台目	標準	1Gbps	BMC(iLO)	----->	HCS NWスイッチ #1	30
	拡張	1Gbps	1G #0 Port1 (1)	----->		
			1G #0 Port2 (2)	----->		
			1G #0 Port3 (3)	----->		
			1G #0 Port4 (4)	----->		
		10Gbps	10G #1 Port1 (0)	----->	HCS NWスイッチ #1	10
			10G #1 Port2 (1)	----->	(お客様管理 業務NW#1)	
			10G #2 Port1 (0)	----->	HCS NWスイッチ #2	10
			10G #2 Port2 (1)	----->	(お客様管理 業務NW#2)	
R120h-1M クラスタノード 10台目	標準	1Gbps	BMC(iLO)	----->	HCS NWスイッチ #1	31
	拡張	1Gbps	1G #0 Port1 (1)	----->		
			1G #0 Port2 (2)	----->		
			1G #0 Port3 (3)	----->		
			1G #0 Port4 (4)	----->		
		10Gbps	10G #1 Port1 (0)	----->	HCS NWスイッチ #1	11
			10G #1 Port2 (1)	----->	(お客様管理 業務NW#1)	
			10G #2 Port1 (0)	----->	HCS NWスイッチ #2	11
			10G #2 Port2 (1)	----->	(お客様管理 業務NW#2)	
R120h-1M クラスタノード 11台目	標準	1Gbps	BMC(iLO)	----->	HCS NWスイッチ #2	21
	拡張	1Gbps	1G #0 Port1 (1)	----->		
			1G #0 Port2 (2)	----->		
			1G #0 Port3 (3)	----->		
			1G #0 Port4 (4)	----->		
		10Gbps	10G #1 Port1 (0)	----->	HCS NWスイッチ #1	12
			10G #1 Port2 (1)	----->	(お客様管理 業務NW#1)	
			10G #2 Port1 (0)	----->	HCS NWスイッチ #2	12
			10G #2 Port2 (1)	----->	(お客様管理 業務NW#2)	
R120h-1M クラスタノード 12台目	標準	1Gbps	BMC(iLO)	----->	HCS NWスイッチ #2	22
	拡張	1Gbps	1G #0 Port1 (1)	----->		
			1G #0 Port2 (2)	----->		
			1G #0 Port3 (3)	----->		
			1G #0 Port4 (4)	----->		
		10Gbps	10G #1 Port1 (0)	----->	HCS NWスイッチ #1	13
			10G #1 Port2 (1)	----->	(お客様管理 業務NW#1)	
			10G #2 Port1 (0)	----->	HCS NWスイッチ #2	13
			10G #2 Port2 (1)	----->	(お客様管理 業務NW#2)	
R120h-1M クラスタノード 13台目	標準	1Gbps	BMC(iLO)	----->	HCS NWスイッチ #2	23
	拡張	1Gbps	1G #0 Port1 (1)	----->		
			1G #0 Port2 (2)	----->		
			1G #0 Port3 (3)	----->		
			1G #0 Port4 (4)	----->		
		10Gbps	10G #1 Port1 (0)	----->	HCS NWスイッチ #1	14
			10G #1 Port2 (1)	----->	(お客様管理 業務NW#1)	
			10G #2 Port1 (0)	----->	HCS NWスイッチ #2	14
			10G #2 Port2 (1)	----->	(お客様管理 業務NW#2)	
R120h-1M クラスタノード 14台目	標準	1Gbps	BMC(iLO)	----->	HCS NWスイッチ #2	24
	拡張	1Gbps	1G #0 Port1 (1)	----->		
			1G #0 Port2 (2)	----->		
			1G #0 Port3 (3)	----->		
			1G #0 Port4 (4)	----->		
		10Gbps	10G #1 Port1 (0)	----->	HCS NWスイッチ #1	15
			10G #1 Port2 (1)	----->	(お客様管理 業務NW#1)	
			10G #2 Port1 (0)	----->	HCS NWスイッチ #2	15
			10G #2 Port2 (1)	----->	(お客様管理 業務NW#2)	
R120h-1M クラスタノード 15台目	標準	1Gbps	BMC(iLO)	----->	HCS NWスイッチ #2	25
	拡張	1Gbps	1G #0 Port1 (1)	----->		
			1G #0 Port2 (2)	----->		
			1G #0 Port3 (3)	----->		
			1G #0 Port4 (4)	----->		
		10Gbps	10G #1 Port1 (0)	----->	HCS NWスイッチ #1	16
			10G #1 Port2 (1)	----->	(お客様管理 業務NW#1)	
			10G #2 Port1 (0)	----->	HCS NWスイッチ #2	16
			10G #2 Port2 (1)	----->	(お客様管理 業務NW#2)	

s				接続先(スイッチ)		
装置名	スロット	速度	ポート		装置名	ポート
R120h-1M クラスタノード 16台 目	標準	1Gbps	BMC(iLO)	----->	HCS NWスイッチ #2	26
	拡張	1Gbps	1G #0 Port1 (1)	----->		
			1G #0 Port2 (2)	----->		
			1G #0 Port3 (3)	----->		
			1G #0 Port4 (4)	----->		
		10Gbps	10G #1 Port1 (0)	----->	HCS NWスイッチ #1	17
			10G #1 Port2 (1)	----->	(お客様管理 業務NW#1)	
			10G #2 Port1 (0)	----->	HCS NWスイッチ #2	17
			10G #2 Port2 (1)	----->	(お客様管理 業務NW#2)	
R120h-1M クラスタノード 17台 目	標準	1Gbps	BMC(iLO)	----->	HCS NWスイッチ #2	27
	拡張	1Gbps	1G #0 Port1 (1)	----->		
			1G #0 Port2 (2)	----->		
			1G #0 Port3 (3)	----->		
			1G #0 Port4 (4)	----->		
		10Gbps	10G #1 Port1 (0)	----->	HCS NWスイッチ #1	18
			10G #1 Port2 (1)	----->	(お客様管理 業務NW#1)	
			10G #2 Port1 (0)	----->	HCS NWスイッチ #2	18
			10G #2 Port2 (1)	----->	(お客様管理 業務NW#2)	
R120h-1M クラスタノード 18台 目	標準	1Gbps	BMC(iLO)	----->	HCS NWスイッチ #2	28
	拡張	1Gbps	1G #0 Port1 (1)	----->		
			1G #0 Port2 (2)	----->		
			1G #0 Port3 (3)	----->		
			1G #0 Port4 (4)	----->		
		10Gbps	10G #1 Port1 (0)	----->	HCS NWスイッチ #1	19
			10G #1 Port2 (1)	----->	(お客様管理 業務NW#1)	
			10G #2 Port1 (0)	----->	HCS NWスイッチ #2	19
			10G #2 Port2 (1)	----->	(お客様管理 業務NW#2)	
R120h-1M クラスタノード 19台 目	標準	1Gbps	BMC(iLO)	----->	HCS NWスイッチ #2	29
	拡張	1Gbps	1G #0 Port1 (1)	----->		
			1G #0 Port2 (2)	----->		
			1G #0 Port3 (3)	----->		
			1G #0 Port4 (4)	----->		
		10Gbps	10G #1 Port1 (0)	----->	HCS NWスイッチ #1	20
			10G #1 Port2 (1)	----->	(お客様管理 業務NW#1)	
			10G #2 Port1 (0)	----->	HCS NWスイッチ #2	20
			10G #2 Port2 (1)	----->	(お客様管理 業務NW#2)	

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 2017-2021

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			
	・ 構成部品表（シリアル番号一覧表）に記載されている機器 I D に対応した梱包箱が揃っているか	☐		
	・ 製品にへこみや汚れ等がないか	☐		
2	本製品の設置			
	・ 19 インチラックなど安全に使用できる環境に本製品を設置したか	☐		
3	ネットワーク装置への接続			
	・ 10Gスイッチ間をスタックケーブルで接続したか	☐		
	・ 管理ノード、クラスタノードのサーバと10Gスイッチ、お客様スイッチの間をネットワークケーブルで接続したか	☐		
4	電源の接続			
	・ 10Gスイッチに電源ケーブルを接続したか	☐		
	・ 管理ノード、クラスタノードの電源ケーブルを接続したか	☐		
5	クラスタノードの電源オン			
	・ 全てのクラスタノードでのランプが緑色で点灯したか	☐		
6	管理ノードの電源オン			
	・ 管理ノードのランプが緑色で点灯したか	☐		
7	各クラスタノード、管理ノードの起動確認			
	・ 全てのクラスタノード、管理ノードにてVMware ESXiが起動しているか	☐		
8	WindowsPCの準備			
	・ WindowsPCを管理NWに接続したか	☐		
9	WindowsPCから管理VMに接続			
	・ リモートデスクトップで管理VMのデスクトップ画面が表示されたか	☐		
10	NTPサーバの設定			
	・ NTPサーバが正しく設定されたか	☐		
11	vCenter Server上での機器確認			
	・ vSANクラスタ(vsan)、クラスタノード、管理ノードは表示されたか	☐		
	・ 表示されたvSANクラスタ、各ノードに異常はないか	☐		
12	管理ノードの確認			
	・ メモリ、ディスク容量、ネットワーク設定が正しいか	☐		
13	クラスタノードの確認			
	・ メモリ、ディスク容量、ディスク本数、ネットワーク設定が正しいか	☐		
14	vSAN健全性確認			
	・ vSANの健全性確認でエラーが表示されていないか	☐		
15	vSphereの可用性設定			
	・ 「障害状態および応答」の画面が正しく表示されたか	☐		
16	HCS Console上での確認			
	・ ダッシュボード、ノード、仮想マシン、監視、設定の各画面が正しく表示されたか	☐		

以上