Virtual Storage Console for VMware vSphere環境を設定します

VSC, VASA Provider, and SRA 9.7

NetApp
March 21, 2024

目次

Virtual Storage Console for VMware vSphere環境を設定します 1
ESXi サーバのマルチパスとタイムアウトを設定 1
Virtual Storage Console の SSL 証明書を再生成する 7
複数の vCenter Server 環境で VSC を登録するための要件 7
VSC プリファレンスファイルを設定する 8
異なるサブネット間でのデータストアのマウントを有効にする 10
VSC、VASA Provider、
SRA仮想アプライアンスのメンテナンスコンソールのオプションにアクセスする 11
管理者パスワードを変更します 13
VSC、VASA Provider、SRA仮想アプライアンスの高可用性を設定する 13
VSC、VASA Provider、SRA仮想アプライアンスでサポートされるMetroCluster 構成 15

Virtual Storage Console for VMware vSphere環境を設定します

（VSC）はさまざまな環境をサポートしています。これらの環境の機能によっては、追加の設定が必要になることがあります。

ESXi ホスト、ゲストオペレーティングシステム、 VSC を設定するには、次の作業の一部が必要になることがあります。

- UNMAP 設定を含む ESXi ホストの設定の確認
- ゲストオペレーティングシステムのタイムアウト値の追加
- VSC の SSL 証明書を再生成します
- ストレージ機能プロファイルとしきい値アラームの作成
- 異なるサブネット間でのデータストアのマウントを有効にするためのプリファレンスファイルの変更

ESXi サーバのマルチパスとタイムアウトを設定

Virtual Storage Console for VMware vSphereは、ESXiホストのマルチパス設定とHBAタイムアウト設定をチェックし、ストレージシステムに最も適した設定を行います。

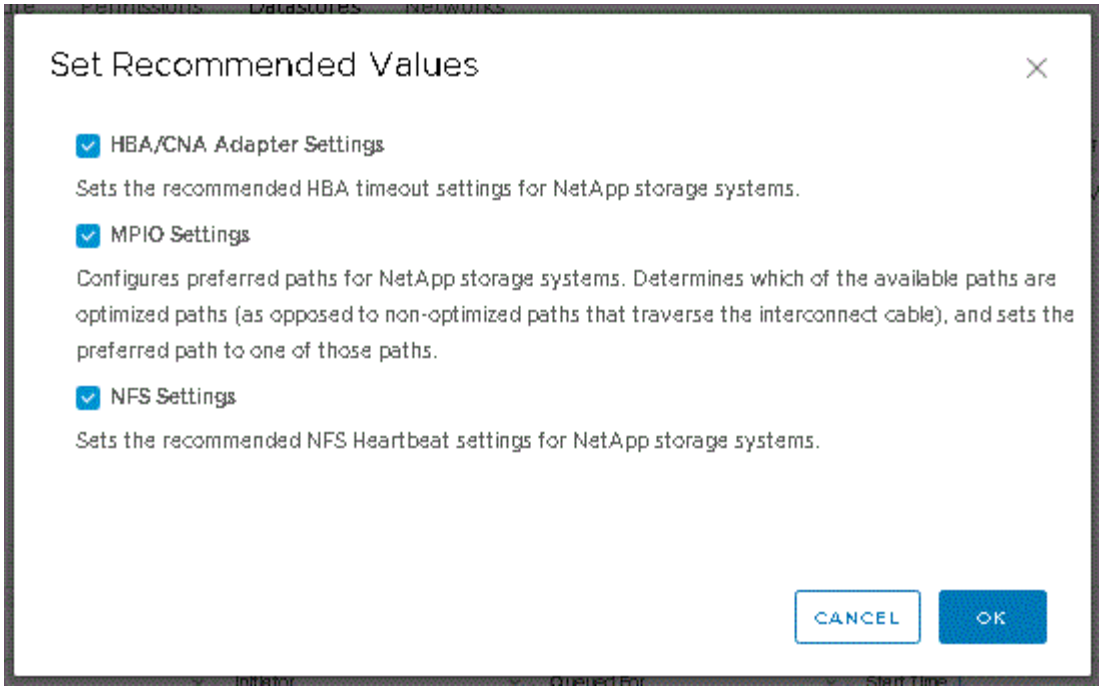
このタスクについて

構成やシステムの負荷によっては、この処理に長時間かかることがあります。タスクの進行状況が*最近のタスク*パネルに表示されます。タスクが完了すると、ホストのステータスアラートアイコンが Normal アイコンまたは Pending Reboot アイコンに変わります。

手順

1. VMware vSphere Web Client * Home *ページで、メニュー：vCenter [Hosts]をクリックします。
2. ホストを右クリックして、メニューを選択します。アクションNetApp VSC >推奨値の設定
3. NetApp Recommended Settings *ダイアログボックスで、ご使用のシステムに最も適した値を選択します。

   標準の推奨値がデフォルトで設定されます。



4. [OK] をクリックします。

Virtual Storage Console for VMware vSphereを使用して設定されるESXiホストの値

フェイルオーバーが最適な状態で確実に実行されるように、Virtual Storage Console for VMware vSphereを使用してESXiホストにタイムアウト値やその他の値を設定することができます。Virtual Storage Console（VSC）で設定される値は、内部テストに基づいています。

ESXi ホストでは、次の値を設定できます。

ESXi の高度な設定

- * VMFS3.HardwareAcceleratedLocking *

  この値を 1 に設定します。

- *VMFS3.EnableBlockDelete *

  この値を 0 に設定します。

NFS 設定

- * Net.TcpipHeHeapSize *

  vSphere 6.0 以降を使用している場合は、この値を 32 に設定します。

- * Net.TcpipHeapMax *

  vSphere 6.0 以降を使用している場合は、この値を 1536 に設定します。

- * NFS.MaxVolumes *

  vSphere 6.0 以降を使用している場合は、この値を 256 に設定します。

- * NFS41.MaxVolumes *

  vSphere 6.0 以降を使用している場合は、この値を 256 に設定します。

- * NFS.MaxQueueDepth *

  vSphere 6.0 以降の ESXi ホストを使用している場合は、キューのボトルネックを回避するためにこの値を 128 以上に設定します。

  vSphere のバージョンが 6.0 より前の場合は、この値を 64 に設定します。

- * nfs.HeartbeatMaxFailures*

  すべての NFS 構成で、この値を 10 に設定します。

- * nfs.HeartbeatFrequency*

  すべての NFS 構成でこの値を 12 に設定します。

- * nfs.HeartbeatTimeout *

  すべての NFS 構成でこの値を 5 に設定します。

FC / FCoE 設定

- * パス選択ポリシー *

  ALUA に対応する FC パスを使用する場合は、この値を「 RR 」（ラウンドロビン）に設定します。

  他のすべての構成では、この値を「固定」に設定する必要があります。

  この値を「 RR 」に設定すると、最適化されたすべてのアクティブなパスでロード・バランシングを行うことができます。値「 fixed 」は、 ALUA に対応していない古い構成に使用され、プロキシ I/O の防止に役立ちます

- * Disk.QFullSampleSize *

  すべての構成でこの値を 32 に設定します。この値を設定すると、 I/O エラーの防止に役立ちます。

- * Disk.QFullThreshold *

  すべての構成でこの値を 8 に設定します。この値を設定すると、 I/O エラーの防止に役立ちます。

- * Emulex FC HBA タイムアウト *

  デフォルト値を使用します。

- * QLogic FC HBA タイムアウト *

デフォルト値を使用します。

iSCSI 設定

- * パス選択ポリシー *

  すべての iSCSI パスに対してこの値を「 RR 」に設定します。

  この値を「 RR 」に設定すると、最適化されたすべてのアクティブなパスでロード・バランシングを行うことができます。

- * Disk.QFullSampleSize *

  すべての構成でこの値を 32 に設定します。この値を設定すると、 I/O エラーの防止に役立ちます。

- * Disk.QFullThreshold *

  すべての構成でこの値を 8 に設定します。この値を設定すると、 I/O エラーの防止に役立ちます。

ゲストオペレーティングシステムスクリプトを設定する

ゲストオペレーティングシステム（OS）スクリプトのISOイメージは、Virtual Storage Console for VMware vSphereサーバにマウントされます。ゲスト OS スクリプトを使用して仮想マシンのストレージタイムアウトを設定するには、 vSphere Client からスクリプトをマウントする必要があります。

オペレーティングシステムタイプ	**60**秒のタイムアウト設定	**190**秒のタイムアウト設定
Linux の場合	`*https*://<apply_ip>:8143/VSC/public/writed/linux_gos_timeout-install.iso	`*https*://<apply_ip>:8143/VSC/public/writable /linux_gos_timeout_190 -install.iso
Windows の場合	`*https*://<apply_ip>:8143/VSC/public/writed/windows_gos_timeout.iso	`*https*://<apply_ip>:8143/VSC/public/writable /windows_gos_timeout_190.isoの形式で指定します
Solaris の場合	`*https*://<apply_ip>:8143/VSC/public/writable /solaris_Gos_timeout-install.iso	`*https*://<apply_ip>:8143/VSC/public/writable /solaris_Gos_timeout_190 -install.iso

仮想マシンを管理している vCenter Server に登録されている VSC インスタンスのコピーからスクリプトをインストールする必要があります。環境に複数の vCenter Server が含まれている場合は、ストレージのタイムアウト値を設定する仮想マシンを含むサーバを選択する必要があります。

仮想マシンにログインし、スクリプトを実行してストレージのタイムアウト値を設定します。

Windows ゲストオペレーティングシステムのタイムアウト値を設定します

Windows ゲストオペレーティングシステムの SCSI I/O タイムアウト設定は、ゲストオペレーティングシステム（ OS ）のタイムアウトスクリプトで設定されます。タイムアウトは 60 秒または 190 秒のどちらかを指定できます。設定を有効にするには、Windows ゲスト OS をリブートする必要があります。

作業を開始する前に

Windows スクリプトを含む ISO イメージをマウントしておく必要があります。

手順

1. Windows 仮想マシンのコンソールにアクセスし、管理者権限を持つアカウントでログインします。
2. スクリプトが自動的に開始されない場合は、 CD ドライブを開き、「 windows_gos_timeout.reg 」スクリプトを実行します。

   レジストリエディタダイアログが表示されます。

3. 続行するには、 [はい] をクリックします。

   「D:\windows_gos_timeout.regに含まれるキーと値がレジストリに正常に追加されました」というメッセージが表示されます

4. Windows ゲスト OS をリブートします。
5. ISO イメージをアンマウントします。

Solaris ゲストオペレーティングシステムのタイムアウト値を設定します

Solaris 10 の SCSI I/O タイムアウト設定は、ゲストオペレーティングシステム（ OS ）のタイムアウトスクリプトで設定されます。タイムアウトは 60 秒または 190 秒のどちらかを指定できます。

作業を開始する前に

Solaris スクリプトを含む ISO イメージをマウントしておく必要があります。

手順

1. Solaris 仮想マシンのコンソールにアクセスし、 root 権限を持つアカウントでログインします。
2. 「 'olaris _gos_timeout-install.sh 」スクリプトを実行します。

   Solaris 10 の場合、次のようなメッセージが表示されます。

   ```
   Setting I/O Timeout for /dev/s-a - SUCCESS!
   ```

3. ISO イメージをアンマウントします。

Linux ゲストオペレーティングシステムのタイムアウト値を設定します

Red Hat Enterprise Linux バージョン 4 、 5 、 6 、 7 および SUSE Linux Enterprise Server バージョン 9 、 10 、 11 の SCSI I/O タイムアウト設定は、ゲストオペレーティングシステム（ OS ）のタイムアウトスクリプトで設定されます。タイムアウトは 60 秒または 190 秒のどちらかを指定できます。Linux を新しいバージョンにアップグレードしたときは、必ずこのスクリプトを実行する必要があります。

作業を開始する前に

Linux スクリプトを含む ISO イメージをマウントしておく必要があります。

手順

1. Linux 仮想マシンのコンソールにアクセスし、 root 権限を持つアカウントでログインします。
2. 「 linux_gos_timeout-install.sh 」スクリプトを実行します。

   Red Hat Enterprise Linux 4 または SUSE Linux Enterprise Server 9 の場合は、次のようなメッセージが表示されます。

   ```
   Restarting udev... this may take a few seconds.
   ```

   ```
   Setting I/O Timeout (60s) for /dev/sda - SUCCESS!
   ```

   Red Hat Enterprise Linux 5 、 Red Hat Enterprise Linux 6 、および Red Hat Enterprise Linux 7 の場合は、次のようなメッセージが表示されます。

   ```
   patching file /etc/udev/rules.d/50-udev.rules
   ```

   ```
   Hunk #1 succeeded at 333 (offset 13 lines).
   ```

   ```
   Restarting udev... this may take a few seconds.
   ```

   ```
   Starting udev: [ OK ]
   ```

   ```
   Setting I/O Timeout (60s) for /dev/sda - SUCCESS!
   ```

   SUSE Linux Enterprise Server 10 または SUSE Linux Enterprise Server 11 の場合は、次のようなメッセージが表示されます。

```
patching file /etc/udev/rules.d/50-udev-default.rules
```

```
Hunk #1 succeeded at 114 (offset 1 line).
```

```
Restarting udev ...this may take a few seconds.
```

```
Updating all available device nodes in /dev:   done
```

3. ISO イメージをアンマウントします。

Virtual Storage Console の SSL 証明書を再生成する

（VSC）をインストールするとSSL証明書が生成されます。この SSL 証明書に対して生成される Distinguished Name （ DN ；識別名）は、クライアントマシンで認識される Common Name （ CN ；共通名）とは異なる場合があります。キーストアと秘密鍵のパスワードを変更して証明書を再生成し、サイト固有の証明書を作成することができます。

このタスクについて

メンテナンスコンソールを使用してリモート診断を有効にして、サイト固有の証明書を生成することができます。

"ネットアップナレッジベースの回答 1075654：「Virtual Storage Console 7.x：Implementing CA signed certificates"

手順

1. メンテナンスコンソールにログインします。
2. 「アプリケーション構成」メニューにアクセスするには、「1」を入力します。
3. [Application Configuration]メニューで「3」と入力して、VSCサービスを停止します。
4. SSL 証明書を再生成するには '7' と入力します

複数の vCenter Server 環境で VSC を登録するための要件

単一のVMware vSphere HTML5クライアントで複数の vCenter Server インスタンスを管理している環境で VSC と vCenter Server を 1 ： 1 のペアにするため、各 vCenter Server に VSC のインスタンスを 1 つ登録する必要があります。そうすることで、vCenter 6.0 以降を実行するすべてのサーバを、単一の vSphere HTML5 クライアントからリンクモードと非リンクモードの両方で管理することができます。

> VSC を vCenter Server で使用する場合は、管理する vCenter Server インスタンスごとに VSC インスタンスを 1 つ設定または登録しておく必要があります。登録する各 VSC インスタンスのバージョンを同じにする必要があります。

リンクモードは、 vCenter Server の導入時に自動的に設定されます。リンクモードでは、 Microsoft Active Directory Application Mode （ ADAM ）を使用して、複数の vCenter Server システムにわたってデータが格納され、同期されます。

vSphere HTML5 クライアントを使用して複数の vCenter Server で VSC タスクを実行するためには、次の条件を満たす必要があります。

- VMware インベントリ内の管理対象の各 vCenter Server に 1 つずつ VSC サーバを登録して一意の 1 ： 1 ペアにする必要があります。

  たとえば、 VSC サーバ A を vCenter Server A に登録し、 VSC サーバ B を vCenter Server B に登録し、 VSC サーバ C を vCenter Server C に登録できます。

  VSC サーバ A を vCenter Server A と vCenter Server B の両方に登録することはできません

  VMware インベントリに VSC サーバが登録されていない vCenter Server が含まれていて、 VSC に登録されている vCenter Server が 1 つ以上ある場合は、 その後、 VSC が登録された vCenter Server に対する VSC のインスタンスを表示して VSC 処理を実行できます。

- シングルサインオン（ SSO ）に登録された各 vCenter Server に、 VSC 固有の View 権限が必要です。

  適切な RBAC アクセス許可も必要です。

vCenter Server の指定が必要なタスクを実行すると、「 * vCenter Server * 」ドロップダウンボックスに、使用可能な vCenter Server が英数字順に表示されます。デフォルトの vCenter Server が、常にドロップダウンリストの先頭のサーバとなります。

ストレージの場所が認識されている場合（たとえば、* Provisioning *ウィザードを使用し、データストアが特定のvCenter Serverで管理されているホスト上にある場合）、vCenter Serverの一覧が読み取り専用オプションとして表示されます。これは、 vSphere Web Client で右クリックオプションを使用して項目を選択した場合にのみ該当します。

VSC で管理していないオブジェクトを選択しようとすると警告が表示されます。

VSC の概要ページで、特定の vCenter Server に基づいてストレージシステムをフィルタリングできます。概要ページは、 vCenter Server に登録されているすべての VSC インスタンスで表示されます。特定の VSC インスタンスと vCenter Server に関連付けられているストレージシステムを管理できますが、複数の VSC インスタンスを実行する場合は、ストレージシステムごとに登録情報を分けておく必要があります。

VSC プリファレンスファイルを設定する

プリファレンスファイルには、Virtual Storage Console for VMware vSphereの処理を制御する設定が含まれています。ほとんどの場合、これらのファイルの設定を変更する必要はありません。どのプリファレンスファイル（VSC）が使用されるかを理解しておくと役立ちます。

VSC には複数のプリファレンスファイルがあります。これらのファイルには、 VSC によるさまざまな処理の

実行方法を決定するエントリキーと値が含まれています。VSC で使用される一部のプリファレンスファイルを次に示します。

/opt/netapp/vscserver/etc/kamino/kaminoprefs.xml が含まれています

「 /opt/NetApp/vscserver /etc/vsc/vscPreferences.xml 」を参照してください

状況によっては、プリファレンスファイルの変更が必要になることがあります。たとえば、 iSCSI または NFS を使用していて、 ESXi ホストとストレージシステムとでサブネットが異なる場合は、のプリファレンスファイルを変更する必要があります。プリファレンスファイルの設定を変更しないと、 VSC でデータストアをマウントできないためにデータストアのプロビジョニングが失敗します。

IPv4または**IPv6**を設定します

プリファレンスファイル「kaminoprefs.xml」に新しいオプションが追加されました。このオプションを設定すると、VSCに追加されるすべてのストレージシステムでIPv4またはIPv6のサポートを有効にすることができます。

- 「 efault.override.option.provision.mount.datastore.address.family` 」パラメータが「 kaminoprefs.xml 」プリファレンスファイルに追加され、データストアプロビジョニング用の優先データ LIF プロトコルが設定されました。

  このプリファレンスは、 VSC に追加されるすべてのストレージシステムに適用されます。

- 新しいオプションの値は 'ipv4’ipv6' および 'none' です
- デフォルトでは、値は「 NONE 」に設定されています。

価値	説明
なし	• プロビジョニングの際、クラスタのタイプまたは管理LIFと同じIPv6またはIPv4アドレスタイプのデータLIFを使用してストレージが追加されます。 • データLIFのIPv6またはIPv4アドレスタイプがで使用されていない場合は、他のタイプのデータLIFがある場合はそのデータLIFを使用してプロビジョニングが行われます。
IPv4	• 選択したのIPv4データLIFを使用してプロビジョニングが実行されます。 • にIPv4データLIFがない場合、で使用可能なIPv6データLIFがあれば、そのデータLIFを使用してプロビジョニングが行われます。
IPv6	• 選択したのIPv6データLIFを使用してプロビジョニングが実行されます。 • にIPv6データLIFがない場合、で使用可能なIPv4のデータLIFがあれば、プロビジョニングはIPv4のデータLIFを介して行われます。

異なるサブネット間でのデータストアのマウントを有効にする

NFSまたはiSCSIを使用していて、ESXiホストとストレージシステムとでサブネットが異なる場合は、Virtual Storage Console for VMware vSphereのプリファレンスファイルを変更する必要があります。プリファレンスファイルを変更しないと、（VSC）でデータストアをマウントできないためにデータストアのプロビジョニングが失敗します。

このタスクについて

データストアのプロビジョニングに失敗した場合、以下のエラーメッセージが記録されます。

' 続行できません。コントローラ上のカーネルIPアドレスとアドレスの相互参照時にIPアドレスが見つかりませんでした

これらのホストにNFSマウント・ボリュームと一致するネットワークが見つかりません `

手順

1. vCenter Server インスタンスにログインします。
2. 統合アプライアンス仮想マシンを使用してメンテナンスコンソールを起動します。

   "VSC、VASA Provider、SRA仮想アプライアンスのメンテナンスコンソールのオプションにアクセスする"

3. *Support and Diagnostics*オプションにアクセスするには'4`を入力します
4. 「2」を入力して、「* Access Diagnostic Shell *」オプションにアクセスします。
5. 「 vi /opt/NetApp/vscserver /etc/kamino/kaminoprefs.xml 」と入力して、「 kaminoprefs.xml 」ファイルを更新します。
6. kaminoprefs.xml ファイルを更新します

を使用する場合	手順
iSCSI	エントリキー「 efault.allow.iscsi.mount.networks` 」の値を「 ALL 」から ESXi ホストのネットワークの値に変更します。
NFS	エントリキー「 efault.allow.nfs.mount.networks` 」の値を「 ALL 」から ESXi ホストのネットワークの値に変更します。

   プリファレンスファイルには、これらのエントリキーのサンプル値が含まれています。

   > 値「 all 」はすべてのネットワークを意味するわけではありません。「all」の値を指定すると、ホストとストレージ・システムの間にある一致するすべてのネットワークが、データストアのマウントに使用されます。ホストネットワークを指定すると、指定したサブネット間でのみマウントを有効にできます。

7. 'kaminoprefs.xml ファイルを保存して閉じます

VSC、VASA Provider、SRA仮想アプライアンスのメンテナンスコンソールのオプションにアクセスする

アプリケーション、システム、およびネットワークの構成は、Virtual Storage Console（VSC）、VASA Provider、Storage Replication Adapter（SRA）仮想アプライアンスのメンテナンスコンソールを使用して管理できます。管理者パスワードとメンテナンスパスワードを変更することができます。サポートバンドルの生成、異なるログレベルの設定、 TLS 設定の表示と管理、およびリモート診断の開始を行うこともできます。

作業を開始する前に

VSC、VASA Provider、SRA仮想アプライアンスの導入後にVMwareツールをインストールする必要があります。

このタスクについて

- ユーザ名に「maint」を使用し、導入時に設定したパスワードを使用して、VSC、VASA Provider、SRA仮想アプライアンスのメンテナンスコンソールにログインする必要があります。
- リモート診断をイネーブルにするときは、「```ip」ユーザのパスワードを設定する必要があります。

手順

1. 導入した仮想アプライアンスの* Summary *タブにアクセスします。
2. をクリックします メンテナンスコンソールを起動します。

   次のメンテナンスコンソールオプションにアクセスできます。

   - アプリケーション構成

     次のオプションを使用できます。

     - サーバステータスの概要を表示します
     - Virtual Storage Console サービスを開始します
     - Virtual Storage Console サービスを停止します
     - VASA Provider および SRA サービスを開始する
     - VASA Provider および SRA サービスを停止する
     - 「管理者」ユーザのパスワードを変更します
     - 証明書を再生成します
     - キーストアと証明書をハードリセットします
     - データベースをハードリセットしました
     - Virtual Storage Console サービスのログレベルを変更します
     - VASA Provider サービスと SRA サービスのログレベルを変更します
     - TLS 設定を表示する
     - TLS プロトコルを有効にします

    - TLS プロトコルを無効にします
  - システム構成

    次のオプションを使用できます。

    - 仮想マシンをリブートします
    - 仮想マシンをシャットダウンします
    - 「 maint 」ユーザのパスワードを変更します
    - タイムゾーンを変更します
    - NTPサーバを変更します

      NTP サーバの IPv6 アドレスを指定できます。

    - SSHアクセスを有効/無効にします
    - jail ディスクサイズ（ /jail ）の拡張
    - アップグレード
    - VMware Tools をインストールします
  - ネットワーク構成

    次のオプションを使用できます。

    - IP アドレス設定を表示します
    - IP アドレスの設定を変更します

      このオプションを使用すると、導入後に IP アドレスを IPv6 に変更できます。

    - ドメイン名検索設定を表示します
    - ドメイン名検索設定を変更します
    - 静的ルートを表示します
    - 静的ルートを変更します

      このオプションを使用すると、 IPv6 ルートを追加できます。

    - 変更をコミットします
    - ホストに ping を実行します

      このオプションを使用すると、 IPv6 ホストに ping を送信できます。

    - デフォルト設定に戻します
  - サポートと診断

    次のオプションを使用できます。

    - サポートバンドルの生成

- 診断シェルにアクセスします
- リモート診断アクセスを有効にします
  - 関連情報 *

VSC および VASA Provider のログファイル

管理者パスワードを変更します

メンテナンスコンソールを使用して、導入後にVSC、VASA Provider、SRA仮想アプライアンスの管理者パスワードを変更することができます。

手順

1. vCenter Serverで、VSC、VASA Provider、SRA仮想アプライアンスへのコンソールを開きます。
2. maintenance ユーザとしてログインします。
3. メンテナンスコンソールで「1」と入力して、「アプリケーション構成」を選択します。
4. 「6」を入力して、「管理者」ユーザーパスワードの変更*を選択します。
5. 8~63 文字のパスワードを入力します。
6. 確認ダイアログボックスに「 y 」と入力します。

VSC、VASA Provider、SRA仮想アプライアンスの高可用性を設定する

Virtual Storage Console（VSC）、VASA Provider、Storage Replication Adapter（SRA）仮想アプライアンスでは、（HA）構成がサポートされます。これにより、障害時にVSC、VASA Provider、SRAの機能を中断なく提供できます。

VSC、VASA Provider、SRA仮想アプライアンスでは、VMware vSphere（HA）機能とvSphereフォールトトレランス（FT）機能を利用して以下の機能を実現します。（HA）解決策 を使用すると、次のような理由でシステム停止からの迅速なリカバリが可能です。

- ホスト障害です
- ネットワーク障害
- 仮想マシンの障害（ゲスト OS の障害）
- アプリケーション（VSC、VASA Provider、SRA）がクラッシュする

仮想アプライアンスで追加の設定を行う必要はありません。要件に応じて、 vCenter Server ホストと ESXi ホストで VMware vSphere HA または vSphere FT を設定する必要があります。HA と FT のどちらにも、クラスタホストと共有ストレージが必要です。FT には追加の要件と制限事項があります。

VMware vSphere HA解決策 およびvSphere FT解決策 に加え、仮想アプライアンスでもVSC、VASA Provider、SRAのサービスを常時実行できるようになります。仮想アプライアンスのwatchdogプロセスが3つのサービスをすべて定期的に監視し、何らかの障害を検出するとサービスを自動的に再起動します。これにより、アプリケーションの障害を防止できます。

vCenter HAは、VSC、VASA Provider、SRA仮想アプライアンスではサポートされません。

VMware vSphere HA の場合

Virtual Storage Console（VSC）、VASA Provider、Storage Replication Adapter（SRA）仮想アプライアンスが導入されているvSphere環境（HA）を設定することができます。VMware HA は、仮想環境でハードウェアやオペレーティングシステムの障害が発生した場合にフェイルオーバー保護を提供します。

仮想マシンを監視してオペレーティングシステムの障害やハードウェアの障害を検出し、リソースプール内の他の物理サーバ上の仮想マシンを再起動します。サーバの障害が検出された場合、手動での対応は不要です。

VMware HA を設定する手順は、 vCenter Server のバージョンによって異なります。VMware HA の設定手順を確認するには、次の参照先で必要な vCenter Server のバージョンを選択してください。

"VMware vSphere のドキュメント：「 vSphere HA クラスタの作成と使用"

VMware vSphere フォールトトレランス

VMware vSphereのフォールトトレランス（FT）機能を使用すると（HA）のレベルが高くなり、データや接続が失われないよう仮想マシンを保護することができます。VSC、VASA Provider、SRA仮想アプライアンスのvSphere FT機能をvCenter Serverから有効または無効にする必要があります。

環境内の仮想アプライアンスに必要な数のvCPU（少なくとも2個、大規模環境の場合は4個）とFTがvSphereライセンスでサポートされていることを確認してください。

vSphere FT を使用すると、サーバの障害時にも仮想マシンを継続的に稼働できます。仮想マシンで vSphere FT が有効になっている場合は、 Distributed Resource Scheduler （ DRS ）で選択された別のホスト（セカンダリ仮想マシン）にプライマリ仮想マシンのコピーが自動的に作成されます。DRS が有効になっていない場合は、使用可能なホストの中からターゲットホストが選択されます。vSphere FT では、プライマリ仮想マシンとセカンダリ仮想マシンをロックステップモードで運用し、それぞれの仮想マシンの実行状態をセカンダリ仮想マシンにミラーリングします。

ハードウェアに障害が発生してプライマリ仮想マシンに障害が発生すると、セカンダリ仮想マシンはプライマリ仮想マシンが停止した場所をすぐに検出します。ネットワーク接続、トランザクション、データが失われることなく、セカンダリ仮想マシンの実行が継続されます。

vCenter Server インスタンスで vSphere FT を設定するには、システムが CPU 要件、仮想マシンの制限要件、およびライセンス要件を満たしている必要があります。

HA を設定する手順は、 vCenter Server のバージョンによって異なります。HA の設定手順を確認するには、次の参照先で必要な vCenter Server のバージョンを選択してください。

"VMware vSphere のドキュメント：「 Fault Tolerance の要件、制限、およびライセンス"

VSC、VASA Provider、SRA仮想アプライアンスでサポートされるMetroCluster 構成

Virtual Storage Console（VSC）、VASA Provider、Storage Replication Adapter（SRA）仮想アプライアンスでは、ONTAP のMetroCluster IP構成とFC構成を使用する環境がサポートされます。このサポートはほぼ自動的に行われます。ただし、 MetroCluster 環境で VSC および VASA Provider を使用している場合はいくつかの違いがあります。

MetroCluster 構成と VSC

プライマリサイトとセカンダリサイトで VSC がストレージシステムコントローラを検出することを確認する必要があります。通常、 VSC は自動的にストレージコントローラを検出します。クラスタ管理 LIF を使用している場合は、 VSC が両方のサイトでクラスタを検出していることを確認することを推奨します。検出されていない場合は、手動でストレージコントローラを VSC に追加できます。VSC がストレージコントローラへの接続に使用するユーザ名とパスワードのペアを変更することもできます。

スイッチオーバーが発生した場合、セカンダリサイトのがテイクオーバーします。これらの名前には「-mc」サフィックスが付加されています。データストアのプロビジョニングなどの処理の実行中にスイッチオーバー操作が発生すると、データストアが存在するの名前が「-mc」サフィックスのついたものに変わります。スイッチバックが発生してプライマリサイトのに制御が戻ると、このサフィックスは削除されます。

> MetroCluster 構成を直接VSCに追加した場合は、スイッチオーバー後にSVM名の変更（「-mc」サフィックスの追加）が反映されません。他のスイッチオーバー操作は、いずれも引き続き通常どおりに実行されます。

スイッチオーバーまたはスイッチバック後、 VSC で自動的にクラスタが検出されて認識されるまでに数分かかる場合があります。データストアのプロビジョニングなどの VSC 処理を実行中にスイッチオーバーまたはスイッチバックが発生した場合、処理に遅れが生じることがあります。

MetroCluster 構成と VASA Provider

VASA Provider では、 MetroCluster 構成を使用する環境が自動的にサポートされます。VASA Provider 環境では、スイッチオーバーは透過的に行われます。VASA Providerに直接を追加することはできません。

> VASA Providerでは、スイッチオーバー後にセカンダリサイトのの名前に「-mc」というサフィックスが付加されません。

MetroCluster 構成とSRA

SRA では、 MetroCluster 構成がサポートされません。