

# H3C CAS CVM

## ユーザーガイド(システム管理編)

ドキュメントバージョン:5W100-20230727

---

Copyright©2023 New H3C Technologies Co.,Ltd. All rights reserved.

本マニュアルのいかなる部分も、New H3C Technologies Co.,Ltd.の書面による事前の同意なしに、いかなる形式または手段によっても複製または送信することはできません。

New H3C Technologies Co.,Ltd.の商標を除き、本書に記載されているすべての商標は、それぞれの所有者に帰属します。

このドキュメントの情報は、予告なしに変更されることがあります。

## 目次

システムを管理する.....	1
機能.....	1
オペレーターとオペレーターグループの管理.....	1
機能.....	2
オペレーターの管理.....	2
制限事項とガイドライン.....	2
オペレーター追加する.....	3
オペレーターを編集する.....	3
オペレーターの削除.....	3
オペレーターのフィルター.....	4
詳細なオペレーター情報を表示する.....	4
オペレーターの承認済みリソースを表示する.....	4
パラメーター.....	4
オペレーターグループの管理.....	5
制限事項とガイドライン.....	6
オペレーターグループを追加する.....	6
オペレーターグループにサブグループを追加する.....	7
オペレーターグループを編集する.....	7
オペレーターグループまたはサブグループを削除する.....	7
詳細なオペレーターグループ情報を表示する.....	8
パラメーター.....	8
オンラインオペレーターの管理.....	8
制限事項とガイドライン.....	8
オンラインオペレーターフィルターする.....	8
オンラインオペレーターを強制的にログオフする.....	9
パラメーター.....	9
タスクを管理する.....	9
制限事項とガイドライン.....	9
自動ホスト検出タスクを追加する.....	10
自動ホスト検出タスクを編集する.....	10
自動ホスト検出タスクを削除する.....	10
自動ホスト検出タスクの詳細情報を表示する.....	10
自動ホスト検出タスクを一括削除.....	11
自動ホスト検出タスクを開始する.....	11
自動ホスト検出タスクの一括開始.....	11
自動ホスト検出タスクを一時停止する.....	11
自動ホスト検出タスクを一括停止する.....	11
パラメーター.....	12
操作ログを管理する.....	12
機能.....	12
操作ログをフィルタリングする.....	13
制限事項とガイドライン.....	13
手順.....	13
パラメーター.....	13
操作ログをクリアする.....	14
手順.....	14
操作ログをダウンロード.....	14
制限事項とガイドライン.....	15
手順.....	15

操作ログをエクスポートする .....	15
手順 .....	15
パラメーター .....	15
ログファイルを収集する .....	16
制限事項とガイドライン .....	16
ホストログファイルを収集する .....	17
手順 .....	17
パラメーター .....	17
コンテナエンジンのログファイルを収集する .....	17
制限事項とガイドライン .....	17
手順 .....	17
システムパラメーターを管理する .....	18
制限事項とガイドライン .....	18
機能 .....	18
システムパラメーターを構成する .....	19
制限事項とガイドライン .....	19
手順 .....	20
パラメーター .....	20
メールサーバーを設定する .....	26
制限事項とガイドライン .....	26
手順 .....	26
パラメーター .....	26
認証サーバーを構成する .....	27
制限事項とガイドライン .....	27
認証設定を構成する .....	27
SSO認証を構成する .....	27
パラメーター .....	28
SMSパラメーターを設定する .....	29
制限事項とガイドライン .....	29
手順 .....	29
パラメーター .....	29
Syslogサーバーを構成する .....	31
制限事項とガイドライン .....	31
手順 .....	31
パラメーター .....	32
ミドルウェアを構成する .....	32
制限事項とガイドライン .....	32
手順 .....	32
パラメーター .....	33
コンテナ設定を構成する .....	33
制限事項とガイドライン .....	33
手順 .....	33
パラメーター .....	33
RDMAを構成する .....	34
手順 .....	34
パラメーター .....	34
ISLPとセキュリティ強化を構成する .....	34
手順 .....	34
パラメーター .....	35
ネットワーク設定を構成する .....	36

制限事項とガイドライン .....	36
手順 .....	36
パラメーター .....	37
<b>ステートフルフェイルオーバを管理する .....</b>	<b>37</b>
前提条件 .....	37
制限事項とガイドライン .....	37
ステートフルフェイルオーバシステムを設定する .....	38
ステートフルフェイルオーバ設定を表示する .....	38
プライマリ/バックアップの手動切り替えを実行する .....	38
ステートフルフェイルオーバホスト情報を表示する .....	39
パラメーター .....	39
<b>ステートフルフェイルオーバを管理する .....</b>	<b>41</b>
前提条件 .....	41
制限事項とガイドライン .....	41
ステートフルフェイルオーバシステムを設定する .....	42
ステートフルフェイルオーバ設定を表示する .....	42
プライマリ/バックアップの手動切り替えを実行する .....	42
ステートフルフェイルオーバホスト情報を表示する .....	42
パラメーター .....	43
<b>ホストのファイアウォール設定を構成する .....</b>	<b>45</b>
制限事項とガイドライン .....	45
ホストのファイアウォール設定を表示する .....	47
ホストのファイアウォール設定を編集する .....	47
ホストのファイアウォール設定を同期する .....	47
<b>CVMコラボレーションリソースの管理 .....</b>	<b>47</b>
コラボレーションリソースを追加する .....	48
コラボレーションリソースを編集する .....	48
コラボレーションリソースを削除する .....	48
コラボレーションリソースの詳細を表示 .....	48
分散仮想スイッチ情報をVCFコントローラと同期する .....	49
パラメーター .....	49
<b>ライセンスの管理 .....</b>	<b>49</b>
制限事項とガイドライン .....	50
機能 .....	50
<b>ライセンスの詳細を表示 .....</b>	<b>50</b>
手順 .....	50
パラメーター .....	50
<b>ローカルライセンス .....</b>	<b>51</b>
ホスト情報ファイルを取得する .....	51
ライセンスを登録する .....	52
ライセンス情報のエクスポート .....	52
ハードウェアコードをダウンロードする .....	52
パラメーター .....	52
<b>ライセンスサーバーのライセンス .....</b>	<b>53</b>
ライセンスを登録する .....	53
ライセンスの拡張またはリリース .....	53
ライセンスの詳細を表示 .....	53
パラメーター .....	54
<b>保証情報を見る .....</b>	<b>54</b>
手順 .....	54
パラメーター .....	55

アップグレードを管理する.....	55
制限事項とガイドライン .....	55
ソフトウェアイメージをアップロードする .....	56
このタスクについて.....	56
手順 .....	56
アップグレードタスクを追加する .....	56
このタスクについて.....	56
手順 .....	56
アップグレードタスクをすぐに実行する .....	57
このタスクについて.....	57
手順 .....	57
ソフトウェアイメージをプッシュする .....	57
このタスクについて.....	57
手順 .....	57
事前チェックを実行する.....	58
アップグレードタスクの詳細情報を表示する.....	58
このタスクについて.....	58
手順 .....	58
アップグレード タスクのアップグレード ログ メッセージを表示する .....	58
このタスクについて.....	58
手順 .....	59
アップグレード ログ メッセージをダウンロードする.....	59
このタスクについて.....	59
手順 .....	59
修正プログラムをロールバックする .....	59
このタスクについて.....	59
手順 .....	60
アップグレードタスクを編集する .....	60
このタスクについて.....	60
手順 .....	60
アップグレードタスクを削除する .....	60
このタスクについて.....	60
手順 .....	61
ソフトウェアイメージを削除する .....	61
このタスクについて.....	61
手順 .....	61
パラメーター.....	61
バージョンリポジトリ情報 .....	61
アップグレードタスクリスト.....	62
アップグレードログ情報 .....	63
コンポーネントを管理する .....	63
コンポーネントをアップロードする .....	64
コンポーネント情報を表示 .....	64
コンポーネントをインストールする .....	64
コンポーネントをアップグレードする.....	64
コンポーネントを削除する.....	64
システム上のデータを移行する .....	65
制限事項とガイドライン .....	65
手順 .....	66
パラメーター.....	66

# システムを管理する

ARM ホストは CVM コラボレーション リソース管理をサポートしていません。

システム管理では、オペレーター、タスク、操作ログ、システム パラメーター、ステートフル フェイルオーバー システム、共同リソース、ライセンス、パッチを管理し、CVM データを移行できます。

## 機能

- オペレーターとオペレーターグループの管理
- タスクを管理する
- 操作ログを管理する
- システムパラメーターを管理する
- ステートフルフェイルオーバーを管理する
- CVM コラボレーションリソースの管理
- ライセンスの管理
- アップグレードを管理する
- コンポーネントを管理する
- システム上のデータを移行する

## オペレーターとオペレーターグループの管理

このタスクでは、CVM 内のオペレーター、オペレーター グループ、およびオンライン オペレーターを管理できます。

オペレーターのグループ化は、ハイパーバイザのインストール時にロールベースのアクセス制御 (RBAC) が有効になっているかどうかによって異なります。インストール後に構成を変更することはできません。デフォルトのオペレーターとオペレーター グループの数とタイプに応じて、RBAC が有効になっているかどうかを識別できます。

- RBAC を無効にすると、オペレーターはすべてのリソースに対する権限を持つスーパー管理者として行動できます。
  - システムにはデフォルトのシステム管理者 **admin** があります。

- システムには、デフォルトのオペレーター グループである **System Administrator Group** と **Security Auditor Group** があります。
- RBAC を有効にすると、ロールベースのアクセス制御において、オペレーターはシステム管理者、セキュリティ管理者、セキュリティ監査人のうち 1 つのロールのみを持つことができます。
  - システムには 3 つのデフォルトのオペレーターがあります：
    - システム管理者 **sysadmin** のデフォルトのパスワードは **Sys@1234** です。
    - セキュリティ管理者 **secadmin** のデフォルトのパスワードは **Sec@1234** です。
    - セキュリティ監査人 **secauditor** のデフォルトのパスワードは **Aud@1234** です。
  - システムには、デフォルトのオペレーター グループ **System Administrator Group**、**Security Administrator Group**、および **Security Auditor Group** があります。

## 機能

- オペレーターの管理
- オペレーターグループの管理
- オンラインオペレーターの管理

## オペレーターの管理

オペレーターは CVM の管理者です。システムのセキュリティを確保するため、ID 認証に合格したオペレーターのみが CVM にログインできます。オペレーターが実行できる操作は、オペレーターに割り当てられた権限によって決まります。

オペレーター管理を使用すると、CVM でオペレーターを表示、追加、編集、削除、フィルタリング、禁止できます。オペレーターを追加または編集するときにオペレーターに権限を割り当て、オペレーターに承認されたリソースを表示できます。

## 制限事項とガイドライン

- RBAC を有効にすると：
  - オペレーターを追加できるのはシステム管理者のみです。
  - オペレーターを編集できるのはセキュリティ管理者のみです。
  - オペレーターを削除できるのは、システム管理者とセキュリティ管理者のみです。オペレーター **sysadmin**、**secadmin**、および **secauditor** は、システムのインストール時に自動的に作成され、削除できません。

- ログインに 3 回失敗したオペレーターは、1 分間ログインできなくなります。ログイン失敗の最大回数とロックアウト期間は、『オペレーターの編集』で編集できます。
- オペレーターには、割り当てられた権限と、オペレーターが属するオペレーター グループの権限が付与されます。RBAC を有効にすると、システム管理者によって追加されたオペレーターは、ホストまたは VM リソースを管理できます。セキュリティ管理者は、オペレーターを編集し、オペレーターに権限を割り当てることができます。
- オンライン オペレーターを編集すると、オペレーターが CVM に再度ログインしたときに新しい設定が有効になります。オンライン オペレーターを削除すると、オペレーターは CVM を使用できなくなります。
- Operator **admin** はシステムのスーパー管理者であり、すべての権限を持ちます。システムのインストール時に自動的に作成され、削除することはできません。

## オペレーター追加する

オペレーターはシステム内のオペレーター アカウントであり、システム管理者またはユーザーに属します。オペレーターに権限を割り当てることができます。

1. 上部のナビゲーション バーで、**System** をクリックします。
2. 左側のナビゲーション ペインから、**Operators & Groups > Operators** を選択します。
3. **Add** をクリックします。
4. 『パラメーター』の説明に従ってパラメーターを設定します。
5. **OK** をクリックします。

## オペレーターを編集する

1. 上部のナビゲーション バーで、**System** をクリックします。
2. 左側のナビゲーション ペインから、**Operators & Groups > Operators** を選択します。
3. 対象の演算子を選択し、**Edit** をクリックします。
4. 『パラメーター』の説明に従ってパラメーターを設定します。
5. **OK** をクリックします。

## オペレーターの削除

スーパー管理者アカウントは削除できません。

1. 上部のナビゲーション バーで、**System** をクリックします。
2. 左側のナビゲーション ペインから、**Operators & Groups > Operators** を選択します。

3. 対象の演算子を選択し、**Delete** をクリックします。
4. 開いたダイアログボックスで、**OK** をクリックします。

## オペレーターのフィルター

1. 上部のナビゲーション バーで、**System** をクリックします。
2. 左側のナビゲーション ペインから、**Operators & Groups > Operators** を選択します。
3. 『パラメーター』の説明に従ってフィルター条件を設定し、**Filter** をクリックします。
4. リストを更新するには、右上隅の  をクリックします。
5. 必要な列を表示するには、右上隅の  をクリックします。
6. フィルター領域を折りたたむには、**Collapse** をクリックします。
7. さらに多くのフィルターを表示するには、**More** をクリックします。

## 詳細なオペレーター情報を表示する

1. 上部のナビゲーション バーで、**System** をクリックします。
2. 左側のナビゲーション ペインから、**Operators & Groups > Operators** を選択します。
3. 対象の演算子を選択し、**View** をクリックします。

## オペレーターの承認済みリソースを表示する

オペレーターの承認済みリソースを編集するには『オペレーターを編集する』を参照してください。

オペレーターの承認済みリソースを表示するには:

1. 上部のナビゲーション バーで、**System** をクリックします。
2. 左側のナビゲーション ペインから、**Operators & Groups > Operators** を選択します。
3. 対象オペレーターを選択します。

**Authorized Resources** 領域には、オペレーターが クラスター、ホスト、および VM タブでそれぞれ管理できる **Clusters, Hosts, および VMs** が表示されます。

## パラメーター

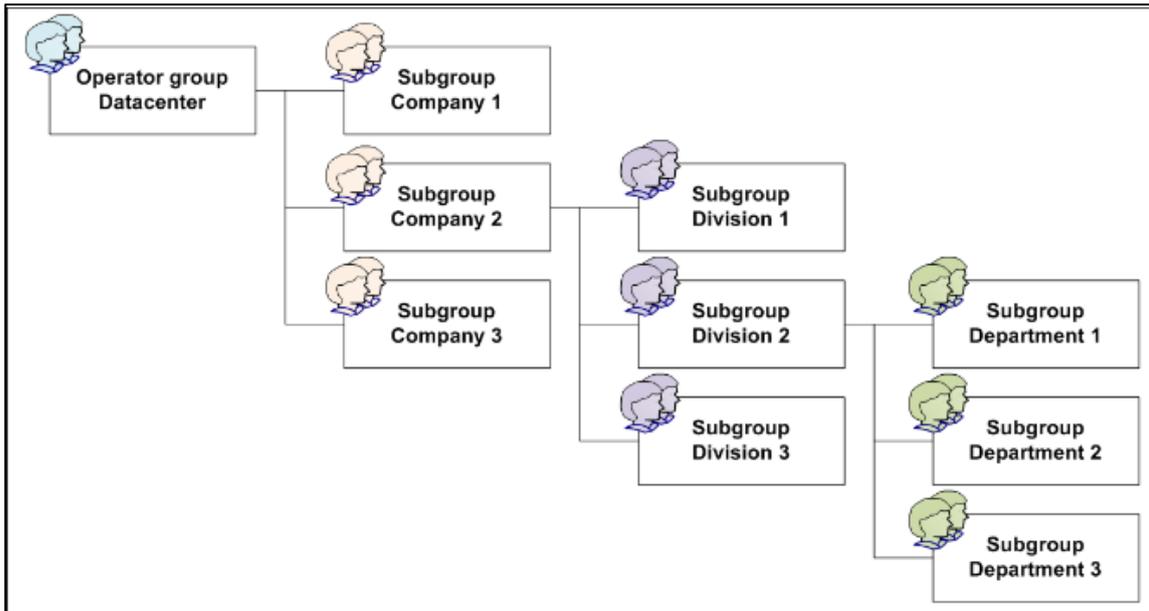
- **Login Name:** オペレーターのログイン名。

- **Authentication:** オペレーターが CVM にログインするために使用する認証モード。
  - **Password Authentication-** オペレーター アカウントとパスワードに基づくローカル認証。
  - **LDAP Authentication-** オペレーター アカウントとパスワードに基づく LDAP 認証。
  - **SSO Authentication-** オペレーターのアカウントとパスワードに基づく SSO 認証。
- **Operator Name:** オペレーターの名前。
- **Operator Group:** オペレーターが所属するオペレーター グループの名前。
- **Authorized Resources:** オペレーターが管理できるリソース。
- **Most Recent Login Time:** オペレーターが管理プラットフォームにログインした最新の時刻。
- **Email:** オペレーターのメール アドレス。メール アドレスの形式が正しいことを確認してください (例: account@domain.com)。メール アドレスが正しくない場合、ユーザーは、ユーザーが属するユーザー グループにシステムから送信される通知を受信できません。
- **Phone:** 正しい電話番号を入力します。電話番号が間違っていると、ユーザーは、所属するユーザー グループにシステムから送信される通知を受信できません。
- **Permission Integrity:** オペレーターの権限の署名検証結果。**Unsigned, Verification Success,** または **Tampered** になります。このパラメーターは、CASE が設定された後にのみ表示されます。
- **Access Policy:** オペレーターに適用されるアクセス ポリシー。
- **Max Online Operators:** オペレーター アカウントを使用して CVM に同時にアクセスできるユーザーの最大数を設定します。
- **Operator Expiration Date:** オペレーター アカウントの有効期限が切れる日付を設定します。たとえば、有効期限を 2023/4/30 に設定すると、オペレーター アカウントは 2023/5/1 の 00:00 に期限切れになります。このフィールドを空のままにすると、オペレーター アカウントは期限切れになりません。
- **Change Password:** オペレーターがこのアカウントを使用してシステムにログインするためのパスワードを変更します。このパラメーターは、オペレーターを編集する場合にのみ使用できます。
  - **New Password:** 新しいパスワードを入力します。新しいパスワードがパスワード ポリシーに準拠していることを確認してください。
  - **Confirm:** 確認パスワードは新しいパスワードと同じである必要があります。
- **Forbid Operator:** オペレーターが CVM にログインすることを禁止するかどうか。
- **Authorities:** オペレーターの操作権限。

オペレーターには、オペレーターが所属するオペレーター グループの権限と、オペレーターに個別に割り当てられている権限があります。

## オペレーターグループの管理

オペレーター グループとは、同じアクセス権限を持つオペレーターのグループです。オペレーター グループに複数レベルのサブグループを構成し、異なるグループに異なる権限を割り当てることができます。



## 制限事項とガイドライン

RBAC を有効にすると:

- オペレーター グループを追加または削除することはできません。
- オペレーター グループを編集できるのはセキュリティ管理者のみです。オペレーター グループの名前と説明のみ編集できますが、権限は編集できません。

RBAC が無効の場合:

- セキュリティ監査グループにサブグループを追加することはできません。
- デフォルトのシステム管理者グループとセキュリティ監査グループを削除することはできません。
- サブグループを持つオペレーター グループは削除できません。このようなグループを削除するには、まずサブグループを削除してください。

## オペレーターグループを追加する

1. 上部のナビゲーション バーで、**System** をクリックします。
2. 左側のナビゲーション ペインから、**Operators & Groups > Operator Groups** を選択します。
3. **Add** をクリックします。
4. 『パラメーター』の説明に従ってパラメーターを設定します。
5. **OK** をクリックします。

## オペレーターグループにサブグループを追加する

1. 上部のナビゲーション バーで、**System** をクリックします。
2. 左側のナビゲーション ペインから、**Operators & Groups > Operator Groups** を選択します。
3. 親グループのサブグループを追加するには、そのグループの **Actions** 列で **Add Subgroup** をクリックします。
4. 子グループのサブグループを追加するには、親グループの左側にある  アイコンをクリックし、その子グループの **Actions** 列で **Add Subgroup** をクリックします。
5. 『パラメーター』の説明に従ってパラメーターを設定します。
6. **OK** をクリックします。

## オペレーターグループを編集する

1. 上部のナビゲーション バーで、**System** をクリックします。
2. 左側のナビゲーション ペインから、**Operators & Groups > Operator Groups** を選択します。
3. 親グループを編集するには、そのグループの **Actions** 列で **Edit** をクリックします。
4. 子グループを編集するには、親グループの左側にある  アイコンをクリックし、その子グループの **Actions** 列で **Edit** をクリックします。
5. 『パラメーター』の説明に従ってパラメーターを設定します。
6. **OK** をクリックします。

## オペレーターグループまたはサブグループを削除する

1. 上部のナビゲーション バーで、**System** をクリックします。
2. 左側のナビゲーション ペインから、**Operators & Groups > Operator Groups** を選択します。
3. 親グループを削除するには、そのグループの **Actions** 列で **Delete** をクリックします。
4. 子グループを削除するには、親グループの左側にある  アイコンをクリックし、その子グループの **Actions** 列で **Delete** をクリックします。
5. 開いたダイアログボックスで、**OK** をクリックします。

# 詳細なオペレーターグループ情報を表示する

1. 上部のナビゲーション バーで、**System** をクリックします。
2. 左側のナビゲーション ペインから、**Operators & Groups > Operator Groups** を選択します。
3. 親グループの詳細情報を表示するには、そのグループの **Actions** 列の **View** をクリックします。
4. 子グループの詳細情報を表示するには、親グループの左側にある  アイコンをクリックし、その子グループの **Actions** 列で **View** をクリックします。

## パラメーター

- **Group Name:** オペレーター グループの名前。
- **Manage Subgroup:** グループのオペレーターがグループのサブグループを管理できるかどうか。
- **Authorities:** オペレーター グループの権限。

## オンラインオペレーターの管理

オンライン オペレーター管理では、オンライン オペレーターを表示およびフィルタリングしたり、指定したオンライン オペレーターを強制的にログオフしたりできます。

## 制限事項とガイドライン

RBAC を有効にすると:

- オンライン オペレーターを表示できるのは、セキュリティ管理者とセキュリティ監査人のみです。
- セキュリティ管理者のみがオペレーターを強制的にログオフします。

RBAC が無効になっている場合、許可されたオペレーターだけが他のオペレーターを強制的にログオフできます。

## オンラインオペレーターフィルターする

1. 上部のナビゲーション バーで、**System** をクリックします。
2. 左側のナビゲーション ペインから、**Operators & Groups > Online Operators** を選択します。
3. 『パラメーター』の説明に従ってパラメーターを設定し、**Filter** をクリックします。

条件に一致するすべてのオンライン オペレーターがリストに表示されます。

4. リストを更新するには、右上隅  をクリックします。
5. 必要な列を表示するには、右上隅  をクリックします。

## オンラインオペレーターを強制的にログオフする

1. 上部のナビゲーション バーで、**System** をクリックします。
2. 左側のナビゲーション ペインから、**Operators & Groups > Online Operators** を選択します。
3. 対象のオンライン オペレーターを選択し、**Log Off** をクリックします。
4. 開いたダイアログボックスで、**OK** をクリックします。

## パラメーター

- **Login Name:** オペレーターのログイン名を入力します。
- **Operator Name:** オペレーターの名前を入力します。
- **Operator Group:** オペレーターが所属するオペレーター グループの名前。
- **Login Time:** オペレーターが CVM にログインした時間。
- **Login Address:** オペレーターが CVM にログインするコンピューターの IP アドレス。
- **Session ID :** CVM へのセッションの ID。

## タスクを管理する

タスク管理を使用すると、CVM 内のタスクを管理できます。

## 制限事項とガイドライン

- クラスターには自動ホスト検出タスクを 1 つだけ追加できます。
- 終了 IP アドレスは開始 IP アドレスよりも大きい必要があります。
- 次の条件が満たされる場合、ホストを検出できません。
  - ホストにアクセスできません。
  - CVM によって管理される CPU の数が制限に達しました。

- ホストの CVK バージョンが現在の CVM バージョンと一致していません。
- ホストは CVM システムによって管理されています。
- ホストのシステム時間とホスト プール内の他のホスト間のオフセットが 5 分を超えています。
- ホストは別の共有ファイルシステムに属しています。

## 自動ホスト検出タスクを追加する

1. 上部のナビゲーション バーで、**System** をクリックします。
2. 左側のナビゲーション ペインから、**Tasks > Auto Host Discovery** を選択します。
3. **Add** をクリックします。
4. 『パラメーター』の説明に従ってパラメーターを設定します。
5. **OK** をクリックします。

## 自動ホスト検出タスクを編集する

1. 上部のナビゲーション バーで、**System** をクリックします。
2. 左側のナビゲーション ペインから、**Tasks > Auto Host Discovery** を選択します。
3. タスクの **Actions** 列で **Edit** をクリックします。
4. 『パラメーター』の説明に従ってパラメーターを設定します。
5. **OK** をクリックします。

## 自動ホスト検出タスクを削除する

1. 上部のナビゲーション バーで、**System** をクリックします。
2. 左側のナビゲーション ペインから、**Tasks > Auto Host Discovery** を選択します。
3. タスクの **Actions** 列で **Delete** をクリックします。
4. 開いたダイアログボックスで、**OK** をクリックします。

## 自動ホスト検出タスクの詳細情報を表示する

1. 上部のナビゲーション バーで、**System** をクリックします。
2. 左側のナビゲーション ペインから、**Tasks > Auto Host Discovery** を選択します。

3. タスクの名前をクリックすると、その情報が表示されます。

## 自動ホスト検出タスクを一括削除

1. 上部のナビゲーション バーで、**System** をクリックします。
2. 左側のナビゲーション ペインから、**Tasks > Auto Host Discover** を選択します。
3. 対象のタスクを選択し、**Delete** をクリックします。
4. 開いたダイアログボックスで、**OK** をクリックします。

## 自動ホスト検出タスクを開始する

1. 上部のナビゲーション バーで、**System** をクリックします。
2. 左側のナビゲーション ペインから、**Tasks > Auto Host Discovery** を選択します。
3. タスクの **Actions** 列で **Start** をクリックします。
4. 開いたダイアログボックスで、**OK** をクリックします。

## 自動ホスト検出タスクの一括開始

1. 上部のナビゲーション バーで、**System** をクリックします。
2. 左側のナビゲーション ペインから、**Tasks > Auto Host Discovery** を選択します。
3. 対象のタスクを選択し、**Start** をクリックします。
4. 開いたダイアログボックスで、**OK** をクリックします。

## 自動ホスト検出タスクを一時停止する

1. 上部のナビゲーション バーで、**System** をクリックします。
2. 左側のナビゲーション ペインから、**Tasks > Auto Host Discovery** を選択します。
3. タスクの **Actions** 列で **Suspend** をクリックします。
4. 開いたダイアログボックスで、**OK** をクリックします。

## 自動ホスト検出タスクを一括停止する

1. 上部のナビゲーション バーで、**System** をクリックします。
2. 左側のナビゲーション ペインから、**Tasks > Auto Host Discovery** を選択します。
3. 対象のタスクを選択し、**Suspend** をクリックします。
4. 開いたダイアログボックスで、**OK** をクリックします。

## パラメーター

- **Host Pool:** タスクのホスト プールを選択します。
- **Cluster:** タスクのクラスターを選択します。
- **Stretched Region:** 検出対象のホストが属するホスト グループ。このフィールドは、ストレッチ クラスターが有効な場合にのみ必要です。
- **Start IP:** 検出可能なホストの IP アドレスの IP アドレス範囲の開始 IP アドレスを入力します。
- **End IP:** 検出可能なホストの IP アドレスの IP アドレス範囲の終了 IP アドレスを入力します。
- **Username:** SSH 経由でホストにアクセスするために使用されるユーザー名。
  - ルート SSH が有効になっている場合は、ユーザールートのみがサポートされます。
  - ルート SSH が有効になっていない場合は、ユーザー **sysadmin** のみがサポートされます。
- **Password:** 検出するホストのパスワードを入力します。ホストが異なるパスワードを使用している場合は、まずパスワードを変更して、すべてのホストが同じパスワードを使用するようにします。ユーザー **sysadmin** のデフォルトのパスワードは **Sys@1234.com** です。
- **Detection Interval:** タスクがホストを検索する間隔 (分) を指定します。
- **Duration:** タスクの期間を時間単位で指定します。期間が過ぎるとタスクは自動的に停止します。
- **Start Now:** タスクをすぐに開始するかどうかを設定します。

## 操作ログを管理する

操作ログには、すべてのオペレーターが CVM で実行する操作が記録されます。ログには、オペレーターのログイン名、オペレーター名、終了時刻、ログイン IP アドレス、操作タイプ、ターゲット、操作の説明、操作結果、および操作の失敗理由が記録されます。RBAC が有効になっている場合、セキュリティ監査人だけがログ ファイルを収集できます。

## 機能

- 操作ログをフィルタリングする
- 操作ログをクリアする

- 操作ログをダウンロード
- 操作ログをエクスポートする
- ログファイルを収集する

## 操作ログをフィルタリングする

操作ログをフィルタリングするには、このタスクを実行します。

## 制限事項とガイドライン

- ログイン名\$SYSTEMの操作ログには、システムの自動操作が記録されます。たとえば、システムが自動 VM バックアップを実行すると、ログイン名\$SYSTEMとオペレーター名\$SYSTEMの操作ログが自動的に生成されます。
- ログイン名admin@VMC-RSの操作ログは、サードパーティのシステムがシステムの REST インターフェースを呼び出したときに生成されるログです。

## 手順

1. 上部のナビゲーション バーで、**System**をクリックします。
2. 左側のナビゲーション ペインから、**Operation Logging > Operation Logs**を選択します。
3. 『パラメーター』の説明に従ってフィルター条件を設定し、**Filter**をクリックします。
4. **Filters**領域を折りたたむには、**Collapse**をクリックします。
5. さらに多くのフィルターを表示するには、**More**をクリックします。
6. リストを更新するには、右上隅  をクリックします。
7. 必要な列を表示するには、右上隅  をクリックします。

## パラメーター

- **Login Name:** オペレーターのログイン名を入力します。
- **Operator Name:** オペレーターの名前を入力します。
- **Start Date:** 操作の開始日を設定します。日付を入力するか、ポップアップ カレンダーから日付を選択できます。
- **End Date:** 操作の終了日を設定します。
- **Completed At:** 操作が完了した時刻。
- **Login Address:** オペレーターが CVM にログインするコンピューターの IP アドレスを入力します。
- **Description:** アクションの説明。

- **Result:** 操作の結果を選択します。オプションには、**All, Succeeded, Failed**, そして **Partially Succeeded** があります。
- **Target:** 操作対象。
- **Risk Level:** 操作のリスクレベルを選択します。オプションには、**All, High, Medium**, と **Low**があります。
- **Integrity Check:** オペレーターによって実行されたアクションの署名検証結果。**Unsigned, Verification Success**, または **Tampered**のいずれかになります。このパラメーターは、CASE が設定された後にのみ表示されます。
- **Reason:** 失敗の詳細な理由。
- **アクション:** アクションを選択します。オプションには、**All, Delete, Restore, Format, Convert, Migrate, Initialize, Add, Edit, Clone, Back Up, Deploy, Enter Maintenance Mode, Exit Maintenance Mode, Copy, Import, Export, Distribute, Configure, Manage, Upgrade, Execute Command, Start, Shut Down, Restart, Suspend, Hibernate, Resume, Log In, Log Out, Connect, Disconnect, Scan, Refresh, Synchronize, Migrate, Install, Uninstall, Register, Check, Collect, Cancel**があります。
- **オペレーションタイプ:** **All Actions, Operator Action, System Configuration, Data Center Action, Host Pool Action, Host Action, Storage Action, Network Action, Cluster Action, VM Action, Template Action, Backup Action, Alarm Management Action, Recovery Action, DRX Action, Virtual Storage Action, SRM Action, Management Platform Action, Storage Adapter Action, Cloud Rainbow Action, Command Line Action, Workflow Action, Heterogeneous Migration Tool Action, Cloud Container Engine Action, Hot Patch Action, External VM Migration Action, External Platform Backup Policy Action, Bare Metal Action, Port Policy Action, Host Firewall Action, OVF Template Action, Action Taken on Tag, Host Profile Action, Confidential Review Action**が含まれます。

## 操作ログをクリアする

指定した日付以前に生成された操作ログをクリアするには、このタスクを実行します。操作ログの有効期間は、『システム パラメーターの設定』で **Operation Log Lifetime** パラメーターを設定することで設定できます。

## 手順

1. 上部のナビゲーション バーで、**System** をクリックします。
2. 左側のナビゲーション ペインから、**Operation Logging > Operation Logs** を選択します。
3. **Clear** をクリックします。
4. 開いたダイアログボックスで **date** を選択します。
5. **OK** をクリックします。

## 操作ログをダウンロード

フィルター条件に一致する操作ログをダウンロードするには、このタスクを実行します。

## 制限事項とガイドライン

CASE を有効にすると、ダウンロードされた操作ログ ファイルに **Integrity Check** 列が含まれないことに注意してください。

## 手順

1. 上部のナビゲーション バーで、**System** をクリックします。
2. 左側のナビゲーション ペインから、**Operation Logging > Operation Logs** を選択します。
3. ダウンロードボタン  をクリックします。
4. **OK** をクリックします。

## 操作ログをエクスポートする

操作ログをエクスポートするには、このタスクを実行します。

## 手順

1. 上部のナビゲーション バーで、**System** をクリックします。
2. 左側のナビゲーション ペインから、**Operation Logging > Operation Logs** を選択します。
3. **Export** をクリックします。
4. 『パラメーター』の説明に従ってパラメーターを設定します。
5. **Save** をクリックします。

## パラメーター

- **Export Location:** エクスポートされた操作ログ ファイルを保存する場所を選択します。オプションには、**Local Directory** と **Remote Server** があります。
- **Export Directory:** **Local Directory** を選択した場合は、ログ ファイルが保存されるローカル ディレクトリ パスを入力します。デフォルトのパスは **/vms** です。ベストプラクティスとして、ディレクトリ / は使用しな

いでください。**Remote Server** を選択した場合は、ログ ファイルが保存されるリモート サーバー上のディレクトリパスを入力します。

- **IP Address:** リモート サーバーの IP アドレスを入力します。**リモート サーバー** を選択した場合は、このパラメーターは必須です。
- **Username:** リモート サーバーにアクセスするために使用するユーザー名を入力します。アカウントには読み取りおよび書き込み権限が必要です。FTP 接続モードを選択した場合は、リモート FTP サーバー上にアカウントを作成する必要があります。SCP 接続モードを選択した場合は、リモート サーバーの OS 上にアカウントを作成する必要があります。**Remote Server** を選択した場合は、このパラメーターは必須です。
- **Password:** ユーザー名のパスワードを入力します。**Remote Server** を選択した場合は、このパラメーターは必須です。
- **Connection Mode:** 接続モードを選択します。オプションには **FTP** と **SCP** があります。**Remote Server** を選択した場合は、このパラメーターは必須です。
- **Server Port:** リモート サーバーのポート番号を指定します。**Remote Server** を選択した場合は、このパラメーターは必須です。デフォルトのポート番号は、FTP 接続モードでは 21、SCP 接続モードでは 22 です。
- **Regular Export:** 自動エクスポートを有効にするかどうかを構成します。
- **Frequency:** 自動エクスポートの頻度を選択します。オプションには、**Monthly**、**Weekly**、および **Daily** があります。
  - **Monthly-** 毎月の指定した日の指定した時間に自動エクスポートを実行します。
  - **Weekly-** 毎週指定された曜日の指定された時間に自動エクスポートを実行します。
  - **Daily-** 毎日指定された時間に自動エクスポートを実行します。
- **Date:** 日付を指定します。**Monthly** を選択した場合は、このパラメーターを設定します。
- **Week:** 曜日を指定します。**Weekly** を選択した場合は、このパラメーターを設定します。
- **Time:** 自動エクスポートを実行する時間を指定します。
- **Retained Files:** システムが保存できるエクスポート ログ ファイルの数を指定します。このパラメーターは空にできません。

## ログファイルを収集する

このタスクを実行して、システム、システムによって管理されるホスト、およびコンテナ エンジンのログ ファイルを収集してダウンロードします。

## 制限事項とガイドライン

RBAC を有効にすると、セキュリティ監査人だけがログ ファイルを収集できるようになります。

システムがホストのログ ファイルの収集に失敗した場合、ログ ファイルの収集後に表示されるページにホスト名が表示されます。

## ホストログファイルを収集する

### 手順

1. 上部のナビゲーション バーで、**System** をクリックします。
2. 左側のナビゲーション ペインから、**Operation Logging > Collect Log Files** を選択します。
3. **Collect Host Log Files** 領域で、ログ ファイルのサイズを入力し、時間範囲を選択し、ログ ファイルのサイズを指定し、ログ収集の対象となるホストを選択して、**Collect** をクリックします。
4. ログ ファイルをダウンロードするには、**Download** をクリックします。ログ ファイルを再度収集するには、**Recollect** をクリックします。

### パラメーター

- **Log File Size:** システムが各ホストに対して収集できるログ ファイルのサイズ (MB 単位) を指定します。ホストのログ ファイル サイズがこの制限を超える場合、システムは超過分のログを収集しません。
- **Time Range:** ログ ファイルの収集期間を選択します。オプションには、**1 day, 2 days, 3 days, 4 days, 5 days, 6 days, 1 week, 1 month**, そして **Not Limited** があります。
- **Select Hosts:** システムがログ ファイルを収集するホストを選択します。

## コンテナエンジンのログファイルを収集する

### 制限事項とガイドライン

このタスクを実行するには、オペレーターはログ ファイルの収集とコンテナエンジンのアクセス許可を持っている必要があります。

### 手順

1. 上部のナビゲーション バーで、**System** をクリックします。
2. 左側のナビゲーション ペインから、**Operation Logging > Collect Log Files** を選択します。

3. **Collect Container Engine Log Files** 領域で、**Collect** をクリックします。
4. ログ ファイルをダウンロードするには、**Download** をクリックします。ログ ファイルを再度収集するには、**Recollect** をクリックします。

## システムパラメーターを管理する

システム パラメーター管理を使用すると、システム設定、電子メール サーバー、認証サーバー、SMS 設定、syslog サーバー、ミドルウェア、コンテナ、RDMA、ISLP およびセキュリティ強化、ネットワーク設定、QR コード ログイン設定を構成できます。

ARM ホストはコンテナ構成をサポートしていません。

## 制限事項とガイドライン

RBAC を有効にすると:

- システム管理者は、メール サーバーと認証サーバーの設定を構成し、SMS、ミドルウェア、コンテナの設定を編集し、syslog サーバーの設定を表示できます。
- セキュリティ管理者は、システム パラメーター、メール サーバー、認証サーバーの設定を構成し、SMS およびミドルウェアの設定を編集し、syslog サーバーの設定を表示できます。
- セキュリティ監査人は、Syslog サーバーの設定を編集し、ミドルウェアとコンテナの設定を表示できます。

## 機能

- システムパラメーターを構成する
- メールサーバーを構成する
- 認証サーバーを構成する
- SMS パラメーターを設定する
- Syslog サーバーを構成する
- ミドルウェアを構成する
- コンテナ設定を構成する
- RDMA を構成する
- ISLP とセキュリティ強化を構成する

- ネットワーク設定を構成する
- QR コードログイン

## システムパラメーターを構成する

CVM のグローバル パラメーターを設定するには、このタスクを実行します。

システム パラメーターには次のものが含まれます。

- **Basic System Parameters:** CVM の基本パラメーターを設定します。
- **Customization Parameters:** CVM インターフェイスのカスタマイズ パラメーターを構成します。
- **Customized Menu Parameters** 他のシステムにアクセスするために使用されるカスタマイズされたメニュー パラメーターを構成します。
- **VNC Proxy Server Parameters** VNC プロキシ サーバー パラメーターを構成します。

仮想ネットワーク コンピューティング (VNC) を使用すると、別のコンピューターをリモートで制御できます。リモート コンピューターの画面をネットワーク経由でローカルに送信します。VNC は、VNC クライアントと VNC サーバーで構成されます。CVM の VM コンソールは VNC クライアントであり、ホスト上の VM は VNC サーバーです。オペレーターは、外部ネットワークからデータ センター内の VM にアクセスする場合があります。データ セキュリティを確保するためのベスト プラクティスとして、VM に VNC プロキシ サーバーを指定します。VNC プロキシ サーバーは、データ センターが外部ネットワークに公開する唯一のノードです。外部ネットワークは、VNC プロキシ サーバーを介してのみ、データ センター内の VM と通信できます。

- **HA Parameters** ホスト ハートビート間隔とストレージ ハートビート間隔を設定します。ホスト ハートビートとストレージ ハートビートにより、CVM はホストを管理し、HA リソースを監視し、クラスター内の障害が発生したホストと VM を検出し、VM を使用可能なホストに移行できます。
- **Image Clean Up-** /vms/nova に保存されたキャッシュされたイメージ (CloudOS およびネイティブ OpenStack との相互運用用のキャッシュされたイメージなど) のリソース使用量しきい値を設定します。使用量しきい値を超えるキャッシュされたイメージは、システムによって自動的にクリーンアップされます。
- **CPU and Memory Parameters** 各ホストの最大 VM CPU およびメモリ割り当て比率を設定します。いずれかの比率に達すると、システムはホスト上に VM を作成しなくなります。
- **Upgrade Parameters** アップグレードを成功させるために、必要に応じて、ホスト アップグレード プロセス中に VM の正常なシャットダウン期間とホストの正常な回復期間を設定します。
- **Performance Monitor Parameters** リアルタイム パフォーマンス データの更新間隔、パフォーマンス データのポーリング間隔、パフォーマンス データ ストレージのディレクトリを設定します。

## 制限事項とガイドライン

RBAC を有効にすると、セキュリティ管理者だけがシステム パラメーターを構成できます。

# 手順

1. 上部のナビゲーション バーで、**System** をクリックします。
2. 左側のナビゲーション ペインから、**Parameters** を選択します。
3. **System Parameters** タブをクリックします。
4. 『パラメーター』の説明に従って、基本システム パラメーター、カスタマイズ パラメーター、カスタマイズされたメニュー パラメーター、VNC プロキシ サーバー パラメーター、HA パラメーター、イメージ クリーンアップ パラメーター、CPU およびメモリ パラメーターを構成します。
5. **Save** をクリックします。

## パラメーター

### 基本的なシステムパラメーター

- **Idle Timeout:** オペレーターのアイドル タイムアウトを指定します。アイドル タイムアウトが経過すると、オペレーターは自動的にシステムからログアウトします。
- **Lockout Period:** オペレーターがシステムにアクセスするために使用する IP アドレスがシステムにログインできない期間を指定します。オペレーターが指定された回数連続してシステムにログインできなかった後、オペレーターの IP アドレスに対してタイマーが開始されます。
- **Max Login Attempts:** 連続ログイン失敗の最大許容回数を指定します。オペレーターが指定された回数システムにログインできなかった場合、オペレーターの IP アドレスは指定された期間内にシステムにログインできません。
- **Max Online Operators:** オンライン オペレーターの最大数を指定します。0 は、オンライン オペレーターの数に制限がないことを示します。
- **Log Level:** ログ レベルを選択します。オプションには、**Error**、**Warning**、と **Tip** があります。
- **Alarm Lifetime:** アラームの有効期間を指定します。アラームの有効期間が 7 日間を超える場合は、単一管理ホストのルート パーティションまたはステートフル フェイルオーバー システムの mysql-share パーティションに十分なスペースがあることを確認してください。十分なスペースがないと、システム障害が発生する可能性があります。
- **Recycled VM Lifetime:** ごみ箱内の VM の有効期間を指定します。VM の有効期間が過ぎると、システムはごみ箱内の VM を自動的に削除します。値が 0 の場合、ごみ箱内の VM は自動的に削除されません。
- **Temporary File Directory:** アップロードおよびダウンロードされたファイル用の一時ディレクトリを入力します。
- **Migration Pause Period:** オンライン移行が完了する前に、残りのダーティ ページを移行するための VM 一時停止期間を設定します。ベスト プラクティスとして、このパラメーターは設定しないでください。

- **Operation Log Lifetime:** 操作ログを削除できない期間を指定します。
- **Encoding Mode:** ホストがアラーム サーバーにアラームを報告するために使用するエンコード モードを選択します。オプションには、**BASE64**、**GBK**、**UTF-8** があります。
- **Intel RDT Noisy Neighbor Quieting:** Intel RDT ノイジー ネイバー クワイエットを有効にするかどうかを選択します。システム パラメーター構成ページでこの機能を有効にした後、VM 編集ページで VM に対してこの機能を有効にできます。VM に対して Intel RDT ノイジー ネイバー クワイエットを有効にするには、VM が存在するホストの物理 CPU がこの機能をサポートしていることを確認します。
- **Max External Snapshots:** VM に保存できる外部スナップショットの最大数を指定します。
- **Max Client Connection:** IP アドレスが CVM に確立できる接続の最大数を指定します。
- **Start VM MAC Address:** 0c:da:41:1d:03:30 から 0c:da:41:1d:ef:a8 の範囲の MAC アドレスを指定します。開始 VM MAC アドレスは、VM MAC アドレスの割り当てに使用される MAC アドレス プールの開始アドレスです。VM は、VM テンプレートに変換されても、割り当てられた MAC アドレスを解放しません。
- **End VM MAC Address:** 0c:da:41:1d:16:b8 から 0c:da:41:1e:03:30 の範囲の MAC アドレスを指定します。終了 VM MAC アドレスは、VM MAC アドレスの割り当てに使用される MAC アドレス プールの終了アドレスです。VM は、VM テンプレートに変換されても、割り当てられた MAC アドレスを解放しません。
- **Storage Pool Level-2 Directory:** システムがストレージ プール内の VM のレベル 2 ディレクトリを作成できるようにします。
  - この機能を有効にすると、VM の展開など、VM イメージ ファイルを作成する操作を実行するときに、システムはストレージ プールのルート ディレクトリに VM 名\_dir という名前のレベル 2 ディレクトリを自動的に作成し、VM イメージ ファイルを保存します。
  - この機能を無効にすると、システムはストレージ プールにレベル 2 ディレクトリを作成せず、既存のレベル 2 ディレクトリを引き続き使用できます。
- **Shared Storage Fault Action:** ホストの共有ストレージに障害が発生した場合に実行するアクションを選択します。オプションには、**Restart Host** と **Do Not Restart Host** があります。デフォルトは、**Do Not Restart Host** です。
- **VM IPv6 Address Management:** VM の IPv6 構成を有効にするかどうかを選択します。**Yes** を選択すると、VM を追加、編集、または複製するとき、またはテンプレートを使用して VM を展開するとき、VM の IPv6 アドレスを構成できます。VM に関する情報を表示すると、その IPv6 アドレスが表示されます。
- **DRX VM Startup:** DRX VM 起動の状態を設定します。この機能を有効にすると、システムはホスト上で VM を起動する前に、ホストが VM 起動要件を満たしているかどうかを確認します。要件が満たされていない場合、システムは VM を起動するのに最適なホストに移行します。この機能は、VM の自動移行が有効になっている場合にのみ有効になります。
- **Shared Storage Overcommitment Limit:** 共有ストレージのオーバーコミット制限を有効にするかどうかを選択します。この機能を無効にすると、共有ストレージのオーバーコミットは制限されません。ベストプラクティスとして、重要なサービスに対してこの機能を有効にします。この機能を有効にすると、共有ストレージのオーバーコミット率を設定できます。この機能を有効にしない場合は、共有ストレージ プールの使用状況を監視します。共有ストレージ プールの使用状況が高い場合は、プールをスケールアップするか、不要なファイルを削除して、読み取り/書き込みサービスの中断を回避します。

## カスタマイズパラメーター

- **System Name:** CAS システムの名前を入力します。
- **Copyright Info:** ログインページで著作権情報を入力します。
- **Homepage Logo:** ホームページ ロゴが保存されているパスを入力します。ロゴはホームページの左上に表示されます。
- **Login Page Logo:** ログイン ページ ロゴが保存されているパスを入力します。
- **Homepage Tiny Logo:** 小さなサイズのホームページ ロゴが保存されているパスを入力します。ナビゲーション ツリーが折りたたまれているときに、ロゴはホームページの左上に表示されます。
- **Favicon:** ファビコンが保存されているパスを入力します。
- **Copyright Logo:** 著作権ロゴが保存されているパスを入力します。
- **Login Page Background:** ログイン ページの背景が保存されているパスを入力します。

## カスタマイズされたメニューパラメーター

- **Menu Name:** CVM からアクセスするシステムの名前を入力します。
- **Menu URL :** システムにアクセスするための URL を入力します。

## VNC プロキシ サーバー パラメーター

- **Server IP :** VNC プロキシ サーバーの IP アドレスを入力します。
- **Username:** VNC プロキシ サーバーにアクセスするために使用するユーザー名を入力します。
- **Password:** ユーザーが VNC プロキシ サーバーにアクセスするためのパスワードを入力します。
- **VNC Console Password:** VM の VNC コンソールに接続するために使用するパスワードを指定します。このパスワードは、パスワード設定後に作成された VM にのみ適用されます。特定の VM の VNC コンソール パスワードを変更するには、VM 編集ページにアクセスします。
- **VNC Password:** VM に VNC ランダム パスワードを使用するかどうかを選択します。この機能を有効にすると、構成された VNC パスワードは無効になります。

## DNS サーバー パラメーター

- **DNS サーバー:** CVM の DNS サーバー IP アドレスをセミコロンで区切って最大 3 つ入力します。この設定は、CVM 上のすべてのホストに適用されます。

## HAパラメーター

- HA システムのデフォルト設定は、可能な限りそのまま使用してください。値が大きすぎたり小さすぎたりすると、CAS の安定性が低下する可能性があります。
- 初期展開のデフォルトの HA 設定を変更しないでください。
  - 一時的に HA 設定を変更するには、まず構成を評価し、変更がサービスに与える影響を理解していることを確認してください。
  - 長期使用のために HA 設定を変更する場合は、テクニカル サポートに連絡してサービスへの影響を評価してください。

- **Host Heartbeat:** CVK ホストが CVM にハートビート パケットを送信する間隔を指定します。CVK ホストに障害が発生すると、ハートビートが中断され、ホスト上の VM は 3 つのホスト ハートビート間隔と 3 つのストレージ ハートビート間隔後に同じクラスター内の他のホストに移行されます。
- **Storage Heartbeat:** CVK がストレージ プールにタイムスタンプを書き込む間隔を指定します。ストレージ ネットワークに障害が発生すると、ハートビートが中断され、影響を受ける VM は 3 回のストレージ ハートビート間隔後に同じクラスター内の他のホストに移行されます。

## イメージクリーンアップパラメーター

- **Max Usage (%) :** イメージのクリーンアップをトリガーするしきい値を指定します。

/vms/nova のスペース使用量が最大使用量しきい値を超えると、システムは、スペースが予約済みスペースよりも大きくなるか、クリーンアップ後に指定されたスペース使用量よりも小さくなるまで、このパスにキャッシュされたイメージをクリーンアップします。

- **Reserved Space:** イメージのクリーンアップ後に予約する必要があるスペースを指定します。
- **Usage After Cleanup:** イメージのクリーンアップ後の最大スペース使用量を指定します。

## CPUとメモリのパラメーター

- **Reserve Host Memory:** ホスト メモリを予約するかどうかを設定します。はいを選択すると、システムはホスト メモリの 20% または 10 GB のホスト メモリ (いずれか小さい方) を予約します。ホストの予約済みメモリは、VM 上で起動された VM や VM に移行された VM では使用できません。
- **Memory Allocation Ratio for All VMs:** すべての VM に割り当てられるメモリとホストの合計メモリ サイズの最大比率を設定します。システムは、次のいずれかのイベントが発生したときに、この比率に達したかどうかを識別します。
  - VM が作成、デプロイ、またはクローンされます。
  - VM は手動で移行されるか、HA または DRS 機能によって自動的に移行されます。
  - VM がごみ箱から復元されます。
  - DRX によって VM が追加されます。
  - VM は Cloud Rainbow を通じてホストに移行されます。

- VM の CPU またはメモリの割り当てが編集されます。
- OVF テンプレートがインポートされます。
- VM はスナップショットまたはバックアップから復元されます。

最大メモリ割り当て率を超えた場合でもサービスの継続性を確保するために、HA または DRS 機能による DRX および VM 移行は引き続き正常に実行されます。

• **Memory Allocation Ratio for Running VMs:** 実行中の VM に割り当てられるメモリとホストの合計メモリ サイズの最大比率を設定します。システムは、次のいずれかのイベントが発生したときに、この比率に達したかどうかを識別します。

- VM が起動します。
- 実行中の VM の CPU またはメモリの割り当てが編集されます。
- VM はメモリ スナップショットから復元されます。
- 実行中の VM は手動で移行されます。
- VM は DRS によって自動的に移行されます。
- DRX によって VM が追加されます。
- VM は Cloud Rainbow を通じてホストに移行されます。

最大メモリ割り当て率を超えた場合でもサービスの継続性を確保するために、HA または DRS 機能による DRX および VM 移行は引き続き正常に実行されます。

• **CPU Overcommit:** CPU オーバーコミットを有効にするかどうかを選択します。オプションには **Yes** と **No** があります。**Yes** を選択した場合、NUMA ノードの物理 CPU にバインドされた vCPU の数は、物理 CPU の数を超えることができます。**No** を選択した場合、NUMA ノードの物理 CPU にバインドされた vCPU の数は、物理 CPU の数を超えることはできません。

• **CPU Allocation Ratio for All VMs:** ホスト上の CPU の合計数に対する、すべての VM に割り当てられる CPU の最大比率を設定します。システムは、次のいずれかのイベントが発生したときに、この比率に達したかどうかを識別します。

- VM が作成、デプロイ、またはクローンされます。
- VM は手動で移行されるか、HA または DRS 機能によって自動的に移行されます。
- VM がごみ箱から復元されます。
- DRX によって VM が追加されます。
- VM は Cloud Rainbow を通じてホストに移行されます。
- VM の CPU またはメモリの割り当てが編集されます。
- OVF テンプレートがインポートされます。
- VM はスナップショットまたはバックアップから復元されます。

最大 CPU 割り当て率を超えた場合でもサービスの継続性を確保するために、HA または DRS 機能による DRX および VM 移行は正常に実行されます。

- **CPU Allocation Ratio for Running VMs:** 実行中の VM に割り当てられる CPU の最大比率を、ホスト上の CPU の合計数に対して構成します。システムは、次のいずれかのイベントが発生したときに、この比率に達したかどうかを識別します。
  - VM が起動します。
  - 実行中の VM の CPU またはメモリの割り当てが編集されます。
  - VM はメモリ スナップショットから復元されます。
  - 実行中の VM は手動で移行されます。
  - VM は DRS によって自動的に移行されます。
  - DRX によって VM が追加されます。
  - VM は Cloud Rainbow を通じてホストに移行されます。

最大 CPU 割り当て率を超えた場合でもサービスの継続性を確保するために、HA または DRS 機能による DRX および VM 移行は正常に実行されます。

## アップグレードパラメーター

- **Graceful VM Shutdown Period (Seconds)** : ホストのアップグレード前に VM をシャットダウンできるように、このパラメーターを設定します。これにより、データの損失やサービスの中断を回避できます。このパラメーターは、アップグレード タスクの VM タスクがオフライン アップグレードに設定され、VM シャットダウンの値が自動的に設定されている場合にのみ有効になります。デフォルトでは、VM の正常なシャットダウン期間は 120 秒です。
- **Graceful Host Recovery Period (Seconds)** : このパラメーターを設定すると、システムは、すべてのホストが正常に再起動して通常の状態に戻るまで、特定の時間待機します。この方法により、ホストがアップグレードを完了し、安定して実行していることを確認してから、VM の実行を継続できます。このパラメーターは、ホストのアップグレードで再起動が必要な場合にのみ有効になります。デフォルトでは、正常なホスト回復期間は 20 秒です。ホストの再起動がタイムアウトすると、タスク コンソールまたはアップグレード レポートに、アップグレード タスクが部分的に成功したことが示されます。この場合、(ping コマンドを使用するか、リモート コンソールにアクセスして) ホストが正常に再起動したかどうかを確認し、手動でメンテナンス モードを終了する必要があります。

## パフォーマンス モニターのパラメーター

- **Monitor Refresh Interval:** リアルタイム パフォーマンス データの更新間隔を設定します。最小間隔は 30 秒、最大間隔は 10 分です。
- **Monitor Data Polling Interval:** システムがパフォーマンスデータを記録する間隔を設定します。最小間隔は 10 秒、最大間隔は 120 秒です。
- **Save To:** システムがパフォーマンス データを保存するディレクトリを指定します。このパラメーターは編集可能です。
- **Save Original Data:** パフォーマンス データの保存用に新しいディレクトリを指定した後、新しいディレクトリに履歴パフォーマンス データを保存するかどうかを選択できます。

- **Reset:** パフォーマンス モニターの設定をデフォルトに戻すには、**リセット**をクリックします。

## メールサーバーを設定する

SMTP サーバーを構成するには、このタスクを実行します。

SMTP は FTP に基づくメール サービスを提供しており、主にシステム メールや通知の転送に使用されます。

## 制限事項とガイドライン

RBAC を有効にすると、システム管理者とセキュリティ管理者だけが SMTP サーバー設定を構成できます。

## 手順

1. 上部のナビゲーション バーで、**System** をクリックします。
2. 左側のナビゲーション ペインから、**Parameters** を選択します。
3. **Email Server** タブをクリックします。
4. 『パラメーター』の説明に従ってパラメーターを設定します。
5. **Email Test** をクリックします。
6. **Save** をクリックします。

## パラメーター

- **Server Address:** SMTP サーバーのドメイン名または IP アドレスを入力します。
- **Port Number:** SMTP サーバーの TCP ポート番号を指定します。
- **Require Auth:** ID 認証を有効または無効にします。デフォルトでは、ID 認証は無効になっています。
- **Encoding Type:** エンコード タイプを選択します。オプションには、**UTF-8** と **GB2312** があります。
- **Username:** SMTP サーバーにアクセスするためのユーザー名を入力します。ID 認証を有効にする場合は、このパラメーターは必須です。
- **Password:** ユーザーが SMTP サーバーにアクセスするためのパスワードを入力します。このパラメーターは、ID 認証を有効にする場合に必須です。
- **Sender Address:** 送信者のメールアドレスを入力します。
- **Sender Name:** 送信者の名前を入力します。

## 認証サーバーを構成する

### 制限事項とガイドライン

- RBAC を有効にすると、システム管理者とセキュリティ管理者だけが認証サーバー設定を構成できます。
- ベストプラクティスとして、SSO 認証と 2 要素認証の両方を有効にしないでください。
- ログイン失敗の原因としては、OSS 認証設定の誤り、システムと OSS サーバー間の接続失敗、またはサーバー障害などが考えられます。この場合、`http://{ ip }?forceSkipSSO=1` または `https://{ip}?forceSkipSSO=1` にアクセスして SSO 認証なしでシステムにログインし、その後 SSO 認証設定を変更するか、SSO 認証を無効にしてください。それでも `http://{ ip }?forceSkipSSO=1` または `https://{ip}?forceSkipSSO=1` からシステムにログインできない場合は、Web ブラウザーのキャッシュをクリアして再度ログインしてください。

### 認証設定を構成する

企業ネットワークには通常、オフィス オートメーション、財務情報フィルター、電子メール、ネットワーク デバイス およびサーバー管理アプリケーションが含まれます。これらすべてのアプリケーションには ID 認証が必要であり、アプリケーションごとに異なる権限が必要です。CVM は、ID 認証情報の集中管理を実行するために LDAP 認証をサポートしています。

このタスクを実行して、LDAP 認証サーバーを構成します。オペレーターが LDAP 認証モードを介して CVM にログインする場合、オペレーターはサーバー上で ID 認証に合格する必要があります。

1. 上部のナビゲーション バーで、**System** をクリックします。
2. 左側のナビゲーション ペインから、**Parameters** を選択します。
3. **Authentication Server** タブをクリックします。
4. **Authentication Server** 領域で **Edit** をクリックします。
5. 『パラメーター』の説明に従ってパラメーターを設定します。
6. 設定を確認するには、**Connectivity Test** をクリックします。
7. **Save** をクリックします。

### SSO認証を構成する

この機能は、CVM と Central Authentication Service (CAS) の連携により、シングル サインオン (SSO) 認証を実装します。この認証方法は、ユーザー認証および承認サービスを提供するオープン ソース ソリューション

であり、ユーザーはシステムに一度ログインした後、資格情報を再入力することなく複数のアプリケーションにアクセスできます。

さらに、CAS サーバーは UCenter に統合されているため、CVM は UC ベースの認証もサポートします。

1. 上部のナビゲーション バーで、**System** をクリックします。
2. 左側のナビゲーション ペインから、**Parameters** を選択します。
3. **Authentication Server** タブをクリックします。
4. **SSO Configuration** 領域で **Edit** をクリックします。
5. 『パラメーター』の説明に従ってパラメーターを設定します。
6. **Save** をクリックします。
7. 開いたダイアログボックスで、**OK** をクリックします。

## パラメーター

認証サーバー:

- **Server Address:** LDAP サーバーの IP アドレスを入力します。
- **Port Number:** LDAP サーバーの TCP ポート番号を入力します。
- **Version:** LDAP バージョンを選択します。オプションには 2 と 3 があります。
- **Type:** LDAP サーバーのタイプを選択します。オプションには、**Generic LDAP Server** と **Microsoft Active Directory** があります。
- **User Naming Attribute:** ユーザー命名属性を入力します。**Type** パラメーターに **Generic LDAP Server** を選択した場合、デフォルトのユーザー命名属性は **cn** です。**Type** パラメーターに **Microsoft Active Directory** を選択した場合、デフォルトのユーザー命名属性は **sAMAccountName** です。
- **Admin Password:** LDAP サーバーにアクセスするために使用するパスワードを入力します。
- **Admin DN :** LDAP サーバーにアクセスするために使用する管理者 DN を入力します (例: **cn=Administrator,cn=users,dc=abc,dc=com**)。最初の cn は LDAP サーバー管理者のユーザー名を表し、2 番目の cn の値は **users** に固定され、最初の dc と 2 番目の dc はそれぞれ識別サーバー名の最初と任意の部分を表します。
- **Base DN :** LDAP サーバーにアクセスするために使用するベース DN を入力します (例: **ou=test,dc=abc,dc=com**)。ou は組織名を表します。管理プラットフォームは、組織内にユーザーが存在する場合にのみ、LDAP サーバーに正常に接続できます。

SSO 構成:

- **SSO Configuration:** SSO 認証ステータス。
- **Authentication Type:** サポートされている認証タイプ。オプションは **CAS** と **UC** です。
- **Server Address:** CAS サーバーのルート URL (例: **http://{ ip }:{ port }/cas**)。
- **Server Login Address:** U-Center に統合された CAS サーバーにログインするための IP アドレス。

## SMSパラメーターを設定する

SMS パラメーターを設定するには、このタスクを実行します。SMS 通知を有効にすると、システムは Jixintong メッセージ プラットフォームや Huawei メッセージ マシンなどの SMS エージェントを通じて管理者に SMS 通知を送信できるようになります。

## 制限事項とガイドライン

RBAC を有効にすると、システム管理者とセキュリティ管理者だけが SMS 設定を構成できます。

SMS 通知を送信するには、次のタスクを実行します。

- SMS 通知を有効にし、SMS パラメーターを構成します。
- SMS 通知パラメーターの設定で『SMS 通知パラメーター』を設定します。

## 手順

1. 上部のナビゲーション バーで、**System** をクリックします。
2. 左側のナビゲーション ペインから、**Parameters** を選択します。
3. **SMS** タブをクリックします。
4. 『パラメーター』の説明に従ってパラメーターを設定します。
5. **SMS Test** をクリックします。
6. **Save** をクリックします。

## パラメーター

- **SMS** : SMS 通知を有効にするかどうかを選択します。SMS 通知を有効にする場合は、以下のパラメーターを設定します。
- **SMS CAPTCHA** : CVM へのログインに SMS CAPTCHA を有効にするかどうかを指定します。
- **SMS Type**: SMS エージェントを選択します。オプションには、**Jixintong Message Platform**, **Huawei Message Machine**, **Mobile Agent Server**, **Ruicheng Message Platform**, **Common SMS Platform**, **NetsUnion Platform**, および **Representational State Transfer** があります。
  - **Jixintong Message Platform**- 登録と展開が必要なサードパーティのメッセージ送信プラットフォーム。詳細については、Jixintong の公式 Web サイトを参照してください。
  - **Huawei Message Machine**— メッセージ送信デバイス。

- **Mobile Agent Server-** サードパーティのメッセージ エージェント サーバー。
- **Ruicheng Message Platform-** 登録と展開が必要なサードパーティのメッセージ送信プラットフォーム。詳細については、Ruicheng の公式 Web サイトを参照してください。
- **Common SMS Platform-** HTTP 要求またはコマンドを通じてメッセージを送信する共通 SMS プラットフォーム。
- **NetsUnion Platform.**
- **Representational State Transfer.**
- **Login Name:** Jixintong message platform、Huawei message machine、RRuicheng message platform、または Representational State Transfer service にアクセスするために使用するログイン名を入力します。
- **Password:** Jixintong message platform、Huawei message machine、Ruicheng message platform、または Representational State Transfer service にアクセスするために使用するパスワードを入力します。
- **HTTP Proxy:** HTTP プロキシを有効にするかどうかを選択します。このパラメーターは、Jixintong Message Platform または Representational State Transfer service を選択した場合にのみ使用できます。HTTP プロキシを有効にする場合は、次のパラメーターを設定します。
  - **Proxy Address:** HTTP プロキシ アドレスを入力します。
  - **Proxy Port:** HTTP プロキシ ポートを入力します。
  - **Proxy Username:** HTTP プロキシのユーザー名を入力します。
  - **Proxy Password:** HTTP プロキシパスワードを入力します。
- **IP Address:** Huawei message machine または mobile agent server の IP アドレスを入力します。このパラメーターは、Huawei message machine、mobile agent server、または Representational State Transfer を選択した場合に必須です。
- **Database Username:** Huawei message machine または mobile agent server のデータベース ユーザー名を入力します。Huawei message machine または mobile agent server を選択した場合、このパラメーターは必須です。
- **Password:** Huawei message machine または mobile agent server のデータベース パスワードを入力します。Huawei message machine または mobile agent server を選択した場合、このパラメーターは必須です。
- **Port Number:** Huawei message machine または mobile agent server のデータベース ポート番号を入力します。このパラメーターは、Huawei message machine、mobile agent server、または Representational State Transfer を選択した場合に必須です。
- **Caller ID :** Huawei Message Machine の発信者 ID を入力します。Huawei Message Machine を選択した場合、このパラメーターは必須です。
- **Service Code:** Huawei Message Machine のサービス コードを入力します。Huawei Message Machine を選択した場合、このパラメーターは必須です。
- **Interface Code:** モバイル エージェント サーバーのインターフェイス コードを入力します。mobile agent server を選択した場合、このパラメーターは必須です。

- **SMS Code:** エンコード タイプを選択します。オプションには **UTF-8** と **GBK** があります。**Common SMS Platform** を選択した場合、このパラメーターは必須です。
- **Send Type:** メッセージの送信モードを選択します。オプションには、**HTTP Request (POST)**と**コマンド**があります。**Common SMS Platform** を選択した場合、このパラメーターは必須です。
- **Request URL :** メッセージを送信するための共通 SMS プラットフォームのリクエスト URL を入力します。送信タイプが **HTTP リクエスト (POST)**の場合、このパラメーターは必須です。正確なアドレスとアドレス形式を取得するには、SMS プロバイダーにお問い合わせください。例：  
http://192.168.0.1:80/sendSms?userName=a&pwd=b&mobile={Mobile}&content={Content}。ここで、**{Mobile}** はアラーム メッセージを受信する電話番号を表し、**{Content}** はアラーム メッセージの内容を表します。
- **Command:** 共通 SMS プラットフォームがメッセージを送信するためのコマンドを入力します。送信タイプが **Command** の場合、このパラメーターは必須です。スクリプト、スクリプトのインストールパス、およびコマンドライン構文を取得するには、SMS プロバイダーにお問い合わせください。例：  
/vms/sendMsg.sh --mobile {Mobile} --content {Content}。ここで、**{Mobile}** はアラーム メッセージを受信する電話番号を表し、**{Content}** はアラーム メッセージの内容を表します。
- **Auth Method:** 認証方法を指定します。Representational **State Transfer** を選択した場合、このパラメーターは必須です。
- **Protocol:** REST サービスにアクセスするためのプロトコルを指定します。Representational **State Transfer** を選択した場合、このパラメーターは必須です。
- **Interface Address:** REST サービスの API を指定します。Representational **State Transfer** を選択した場合、このパラメーターは必須です。

## Syslogサーバーを構成する

このタスクを実行して、Syslog サーバーを構成します。構成後、システムは特定の操作の Syslog 情報を Syslog サーバーに送信します。

## 制限事項とガイドライン

- RBAC を有効にすると、セキュリティ監査人だけが syslog サーバー設定を編集できます。システム管理者とセキュリティ管理者は syslog サーバー設定を表示できます。
- syslog サーバー上の管理ノードの IP アドレスを指定する必要があります。ステートフル フェイルオーバーが構成されている場合は、プライマリ/バックアップの切り替え後に syslog サーバーがログを正しく取得できるように、プライマリ ノードとバックアップ ノードの両方の IP アドレスを指定する必要があります。

## 手順

1. 上部のナビゲーション バーで、**System** をクリックします。
2. 左側のナビゲーション ペインから、**Parameters** を選択します。
3. **Syslog Server** タブをクリックします。
4. 『パラメーター』の説明に従ってパラメーターを設定します。
5. **Save** をクリックします。

## パラメーター

- **IP Address:** syslog サーバーの IP アドレスを入力します。複数の IP アドレスを入力する場合は、**192.168.0.27;192.168.0.28** または **FC00::1;FC00::2** のように、セミコロンでアドレスを区切ります。
- **Protocol:** syslog メッセージを送信するプロトコルを選択します。オプションには、**UDP** と **TCP** があります。
- **Port Number:** syslog サーバーのポート番号を指定します。

## ミドルウェアを構成する

このタスクを実行して、メッセージ ミドルウェアがサードパーティ サービスと通信するように構成します。CVM でミドルウェア設定を編集した後、その設定をサードパーティ サービスと同期する必要があります。

## 制限事項とガイドライン

RBAC を有効にすると、システム管理者とセキュリティ管理者のみがミドルウェア設定を構成できます。セキュリティ監査人はミドルウェア設定を表示できます。

## 手順

1. 上部のナビゲーション バーで、**System** をクリックします。
2. 左側のナビゲーション ペインから、**Parameters** を選択します。
3. **Middleware Settings** タブをクリックします。
4. 『パラメーター』の説明に従ってパラメーターを設定します。
5. **Save** をクリックします。
6. 初期設定を復元するには、**Reset** をクリックします。

## パラメーター

- **RabbitMQ Server Address:** RabbitMQ サーバーのアドレスを入力します。
- **Port Number:** RabbitMQ サーバーのポート番号を入力します。
- **Username:** RabbitMQ サーバーにアクセスするためのユーザー名を入力します。
- **Password:** RabbitMQ サーバーにアクセスするためのパスワードを入力します。
- **Virtual Host Name:** RabbitMQ サーバーの仮想ホスト名を入力します。
- **Exchange Name for VM Events:** RabbitMQ に VM イベントを保存するためのスイッチの名前を入力します

## コンテナ設定を構成する

コンテナ エンジン サービスを有効または無効にし、コンテナ サーバーの IP アドレスを指定するには、このタスクを実行します。ARM ホストはコンテナ エンジン サービスをサポートしていません。

## 制限事項とガイドライン

RBAC を有効にすると、システム管理者のみがコンテナ設定を編集できます。セキュリティ監査人はコンテナ設定を確認できます。

## 手順

1. 上部のナビゲーション バーで、**System** をクリックします。
2. 左側のナビゲーション ペインから、**Parameters** を選択します。
3. **Container Settings** タブをクリックします。
4. **Edit** をクリックし、必要に応じてパラメーターを編集します。
5. **Save** をクリックします。

## パラメーター

- **Container Settings:** コンテナ エンジン サービスを有効または無効にします。コンテナ エンジン サービスを有効にする場合は、コンテナ サーバーの IP も指定する必要があります。

- **Container Server IP** : コンテナ エンジン イメージがデプロイされているサーバーまたは VM の IP アドレスを指定します。

## RDMAを構成する

SeerAnalyzer (SA) プラットフォーム サーバーを指定すると、システムはインテリジェント物理 NIC の IP アドレス、サーバー名、Rx および Tx パケット統計を収集し、その情報を SA プラットフォームに送信します。SA プラットフォームは、指定された時間範囲内のインテリジェント NIC の CPU 使用率と Rx および Tx 統計を表示します。

## 手順

1. 上部のナビゲーション バーで、**System** をクリックします。
2. 左側のナビゲーション ペインから、**Parameters** を選択します。
3. **RDMA Server** タブをクリックします。
4. 『パラメーター』の説明に従ってパラメーターを設定します。
5. **Save** をクリックします。

## パラメーター

- **RDMA** : RDMA を有効または無効にします。
- **Server IP** : SA プラットフォームの IP アドレスを指定します。
- **Port**: SA プラットフォームのポート番号を指定します。
- **Report Interval**:: システムがインテリジェント NIC 情報を SA プラットフォームに報告する間隔を指定します。

## ISLPとセキュリティ強化を構成する

情報セキュリティレベル保護 (ISLP) とセキュリティ強化により、システムとその機密データが保護されます。

## 手順

1. 上部のナビゲーション バーで、**System** をクリックします。
2. 左側のナビゲーション ペインから、**Parameters** を選択します。
3. **ISLP and Security Hardening** タブをクリックします。
4. **Edit** をクリックし、必要に応じてパラメーターを編集します。
5. **Save** をクリックします。

## パラメーター

- **Secure Mode:** セキュア モードを有効にするかどうかを選択します。セキュア モードは、**Mandatory HTTPS** を有効にした後にのみ有効にできます。システムがセキュア モードを有効にした後にのみ、暗号化された VM を作成できます。セキュア モードを有効にすると、次の制限が適用されます。
  - ストレージ ボリュームは 1 つの VM でのみ使用できます。
  - オペレーターのログイン名は変更できません。
  - オペレーター アカウントは、一度に 1 人のユーザーのみが使用できます。
  - ユーザーは HTTPS 経由でのみ CAS にアクセスできます。
  - セキュリティ ゾーンが設定されている場合は、セキュア モードを無効にすることはできません。
  - セキュリティ ゾーン、機密ポリシー、セキュリティ サービス ワークフローは、セキュア モードが有効な場合にのみ使用できます。セキュア モードが無効になっている場合、これらの機能は使用できません。

VM が VNC コンソールにアクセスするには、セキュア モードまたは必須 HTTPS モードが有効になっているときに VNC プロキシ サーバーを指定する必要があります。

- **Mandatory HTTPS :** セキュア モードが有効な場合、必須 HTTPS モードを有効にするかどうかを選択できます。このモードを有効にすると、HTTPS 経由でのみ CVM にアクセスできます。タスクの失敗を回避するために、システムで他のタスクが実行されているときはこのパラメーターを編集しないでください。
- **Root SSH Login Permission:** CVK ホストでルート SSH ログイン権限を有効にするかどうかを設定します。
  - この機能を有効にすると、オペレーターはユーザー名 **root** を使用してのみ CVK ホストを追加できるようになります。
  - この機能を無効にした場合、オペレーターはユーザー名 **sysadmin** を使用して SSH 経由でのみ CVK ホストを追加またはログインできます。ユーザー **sysadmin** のデフォルトのパスワードは **Sys@1234.com** です。

ルート SSH ログイン権限の状態を変更すると、システムによって管理されるすべてのホストへのログインに使用されるアカウントが切り替わります。システムがパスワードを要求したら、正しいアカウ

ントのパスワードを入力します。パスワードを忘れた場合は、新しいパスワードを直接入力できません。

- **Port Hardening:** ポート強化を有効にするかどうかを構成します。この機能は、CVM ホスト上の特定のポートを開きます。開かれたポートのみがそのホストにアクセスできます。
  - ポート強化を有効にすると、関連するホストのポートを開くようにポートポリシーを設定できるようになります。これにより、CVM ホスト上のポートのきめ細かな制御と管理。サービス要件に応じて異なるポート ポリシーを選択することもできます。
  - ポート強化を無効にすると、CVM は物理ホスト上のすべてのポートを許可します。
- ポート強化は IPv4 ホストでのみ有効です。

ポート強化を有効にした後、サードパーティ製ソフトウェアまたは NetFlow が使用するポートが開いていることを確認してください。対応するポートを開かないと、サードパーティ製ソフトウェアまたは NetFlow が失敗します。

## ネットワーク設定を構成する

vSwitch のデフォルト MTU を設定するには、このタスクを実行します。vSwitch を追加すると、この MTU がその vSwitch のデフォルト MTU として使用されます。すべてのネットワークに対して MTU を設定することも、ネットワークごとに MTU を設定することもできます。

## 制限事項とガイドライン

複数のネットワークを選択した場合、デフォルトの MTU は、選択したネットワークの MTU の中で最小のものになります。

## 手順

1. 上部のナビゲーション バーで、**System** をクリックします。
2. 左側のナビゲーション ペインから、**Parameters** を選択します。
3. **Network Settings** タブをクリックします。
4. **Edit** をクリックし、必要に応じてパラメーターを編集します。
5. **Save** をクリックします。

# パラメーター

## すべてのネットワーク

- **Default MTU** : 異なるネットワーク タイプの vSwitch のデフォルト MTU を指定します。

## ネットワークごと

- **Default MTU**: 新しく追加された管理ネットワーク vSwitch のデフォルトの MTU を指定します。
- **Migration**: 新しく追加された移行ネットワーク vSwitch のデフォルトの MTU を指定します。
- **Service**: 新しく追加されたサービス ネットワーク vSwitch のデフォルトの MTU を指定します。
- **Other**: 他のネットワーク タイプの新しく追加された vSwitch のデフォルトの MTU を指定します。
- **Storage**: 新しく追加されたストレージ ネットワーク vSwitch のデフォルトの MTU を指定します。
- **Backup**: 新しく追加されたストレージ ネットワーク vSwitch のデフォルトの MTU を指定します。

## ステートフルフェイルオーバーを管理する

ステートフル フェイルオーバーにより、プライマリ CVM ホストに障害が発生した場合、CVM はサービスをバックアップ CVM ホストに切り替えることができ、サービスの中断を回避できます。プライマリ CVM ホストは、管理ネットワークを介してデータベース ファイルをバックアップ CVM ホストにリアルタイムで同期します。プライマリ CVM ホストにローカル同期パーティションを作成して、データベース ファイル以外のデータをバックアップ CVM ホストに同期できます。

## 前提条件

ステートフル フェイルオーバー用の 2 つのホストが次の要件を満たしていることを確認します。

- ホストは、CVK ホストや VM が組み込まれていない新しいシステムを使用します。
- ホストには、**isopool** と **defaultpool** の 2 つのストレージ プールのみがあります。
- ホストは同じ CAS バージョンとブート モードを使用し、同じ CAS コンポーネント CVM、CIC、および SSV がインストールされている必要があります。
- 2 つのホスト間のシステム時間オフセットは 5 分以内です。
- /vms パーティションには少なくとも 20G のストレージ スペースがあります。
- 2 つのホストの管理ネットワークは相互に到達可能です。

## 制限事項とガイドライン

- RBAC が有効になっている場合、この機能はシステム管理者のみが使用できます。
- ステートフル フェイルオーバーシステムのセットアップ中は、いかなる操作も実行しないでください。
- ステートフル フェイルオーバーシステムをセットアップした後に CVM 管理プラットフォームに参加するには、CVM ホストが次の要件を満たしている必要があります。
  - このシステムは新しく導入されたシステムです。
  - ホスト上にローカル同期パーティションが存在しません。
- プライマリ/バックアップの切り替え中は、いかなる操作も実行しないでください。
- バックアップ ホストが異常な状態の場合、データが同期中の場合、またはデータ同期が異常な状態の場合は、プライマリ/バックアップの切り替えを実行しないでください。
- プライマリ/バックアップの切り替えが成功するかどうかは、データがプライマリ ホストからバックアップホストに同期されているかどうかによって決まります。
- ステートフル フェイルオーバー構成プロセスは、デフォルトではブラウザの言語で表示されます。

## ステートフルフェイルオーバーシステムを設定する

1. 上部のナビゲーション バーで、**System** をクリックします。
2. 左側のナビゲーション ペインから、**Stateful Failover** を選択します。
3. **Set Up Stateful Failover System** をクリックします。
4. 『パラメーター』の説明に従ってパラメーターを設定します。
5. **OK** をクリックします。

## ステートフルフェイルオーバー設定を表示する

1. 上部のナビゲーション バーで、**System** をクリックします。
  2. 左側のナビゲーション ペインから、**Stateful Failover** を選択します。
- 開いたページには、ホスト名、ステータス、設定が表示されます。

## プライマリ/バックアップの手動切り替えを実行する

1. 上部のナビゲーション バーで、**System** をクリックします。
2. 左側のナビゲーション ペインから、**Stateful Failover** を選択します。
3. **Primary/Backup Switchover** をクリックし、**OK** をクリックします。

# ステートフルフェイルオーバーホスト情報を表示する

1. 上部のナビゲーション バーで、**System** をクリックします。
2. 左側のナビゲーション ペインから、**Stateful Failover** を選択します。  
CVM ホストが CVK ホストとして CVM に追加されていない場合、システムは CVM ホストの **Network** と **Storage Adapters** を表示します。
3. **Network** タブで CVM ホストの vSwitch を管理します。vSwitch を追加、編集、または削除できます。
4. **Storage Adapters** タブで CVM ホストのストレージ アダプタを管理します。IQN を編集したり、ストレージ デバイスをスキャンしたりできます。

## パラメーター

### ステートフルフェイルオーバーシステムのセットアップ

- **Virtual IP Address:** CVM にアクセスするための IP アドレスを指定します。使用されていない IP アドレスである必要があります。
- **Mask/Prefix:** 仮想 IP アドレスのサブネット マスクまたはプレフィックスを指定します。
- **Backup Host IP Address:** バックアップ CVM ホストの管理 IP アドレスを指定します。
- **Backup Host Root PWD :** バックアップ CVM ホストのルート パスワードを入力します。
- **Quorum Mode:** クォーラム モードを選択します。オプションには、**Advanced** と **Ping** があります。
  - **Advanced:** クォーラム ホストとして CVK ホストを指定します。プライマリ管理ノードとバックアップ管理ノードが相互に通信できない場合、それぞれの状態情報がクォーラム ホストに送信されます。クォーラム ホストは各ノードの役割を決定し、その役割情報をノードに送信します。クォーラム ホストとプライマリおよびバックアップ CVM ホストの CAS ソフトウェア バージョンは同じである必要があります。
  - **Ping :** 2 つのクォーラム IP アドレスを指定します。プライマリ管理ノードとバックアップ管理ノードが相互に通信できない場合、クォーラム IP アドレスに ping が実行されます。ノードがどのクォーラム IP アドレスにも ping を実行できない場合、そのノードはネットワーク障害が発生していると判断し、バックアップ ノードになります。
- **Quorum Host IP Address:** クォーラム ホストの IP アドレスを指定します。クォーラム ホストには CVK コンポーネントがインストールされている必要があります。
- **Quorum Host Root PWD :** クォーラム ホストのルート パスワードを入力します。
- **Quorum IP Address:** クォーラム IP アドレスとしてアクセスできるゲートウェイの IP アドレス、または常に到達可能なホストの IP アドレスを指定します。クォーラム IP アドレスは、管理ノードのネットワーク接続を確認するために使用されます。ベスト プラクティスとして、ゲートウェイの IP アドレスを指定します。Ping クォーラム モードを選択した場合は、2 つの異なるクォーラム IP アドレスを指定する必要があります。

- **Estimated Host Quantity:** データベースパーティションサイズを計算するために、CVM 内の推定ホスト数を入力します。
- **Estimated VM Quantity:** データベースパーティションサイズを計算するために、CVM 内の推定 VM 数を入力します。
- **Database Partition Size:** データベースパーティションサイズを指定します。データベースパーティションは、プライマリ管理ノードとバックアップ管理ノード間のデータ同期に使用され、/vms パーティションの一部です。データベースパーティションサイズ (MB 単位) = (推定ホスト数 × 7 MB + 推定 VM 数 × 5 MB) × 15 日 / 1024 MB。データベースパーティションサイズは 20 GB 未満にすることはできません。ステートフルフェイルオーバーのセットアップ時間を短縮するためのベストプラクティスとして、データベースパーティションサイズが 200 GB を超える場合は、2 つの CVM ホストの管理ネットワークを 10GE ファイバーケーブルで接続します。

### CVM ホスト情報

- **Physical Interface:** 仮想スイッチが使用する物理 NIC 上のアップリンクインターフェイス。
- **Network Type:** 仮想スイッチのネットワークタイプを選択します。
  - **Mgmt** —CVM とホスト間で管理データを送信します。
  - **Service-** VM のサービスデータを送信します。
  - **Storage-** ホストと分散ストレージシステムまたは IP SAN ストレージサーバーの間でパケットを送信します。このタイプの仮想スイッチは、VM では使用できません。
  - **Backup-** VM のバックアップデータを送信します。ホストにはこのタイプの仮想スイッチまたはサブネットを 1 つだけ設定でき、仮想スイッチは VM では使用できません。
  - **Migration-** VM を移行するためのデータを送信します。ホストにはこのタイプの仮想スイッチまたはサブネットを 1 つだけ設定でき、仮想スイッチは VM では使用できません。
  - **Others-** その他の種類のデータを送信します。
- **Forwarding Mode:** 仮想スイッチの転送モードを選択します。
  - **VEB** — 仮想イーサネットブリッジ (VEB) モードでは、VM 間のトラフィックはソフトウェアを通じて転送されます。
  - **VXLAN(SDN)** : VXLAN(SDN) モードは、SDN コントローラとクラウドコンピューティング管理プラットフォームに基づく VXLAN ソリューション用に設計されています。
- **VLAN ID** : ホストのプロトコルスタックに接続されているインターフェイスの VLAN ID を入力します。
- **State:** 仮想スイッチの状態。
- **IP** : 仮想スイッチの IP アドレス。
- **Mask/Prefix:** IP アドレスのサブネットマスク。
- **Gateway:** 仮想スイッチのゲートウェイ。
- **DPDK State:** 仮想スイッチの DPDK 状態。

### CVM ホスト情報ストレージアダプタ

- **Name:** ストレージアダプタの名前。
- **Model:** ストレージアダプタモデル。

- **Type:** ストレージ アダプタ タイプ。
- **State:** ストレージ アダプタの状態。
- **IQN :** ストレージ アダプタの識別子。
- **Normal Scanning:** 通常のスキャン ルールに従ってデバイスをスキャンします。
- **Forced Scanning:** デバイスを強制的にスキャンします。一部の HBA カードでは、強制スキャン (ストレージ リンクのリセット) によってのみ新しいデバイスを検出できます。この操作により、I/O タイムアウトが発生する可能性があります。

## ステートフルフェイルオーバを管理する

ステートフル フェイルオーバにより、プライマリ CVM ホストに障害が発生した場合、CVM はサービスをバックアップ CVM ホストに切り替えることができ、サービスの中断を回避できます。プライマリ CVM ホストは、管理ネットワークを介してデータベース ファイルをバックアップ CVM ホストにリアルタイムで同期します。プライマリ CVM ホストにローカル同期パーティションを作成して、データベース ファイル以外のデータをバックアップ CVM ホストに同期できます。

## 前提条件

ステートフル フェイルオーバ用の 2 つのホストが次の要件を満たしていることを確認します。

- ホストは、CVK ホストや VM が組み込まれていない新しいシステムを使用します。
- ホストには、**isopool** と **defaultpool** の 2 つのストレージ プールのみがあります。
- ホストは同じ CAS バージョンとブート モードを使用し、同じ CAS コンポーネント CVM、CIC、および SSV がインストールされている必要があります。
- 2 つのホスト間のシステム時間オフセットは 5 分以内です。
- /vms パーティションには少なくとも 20G のストレージ スペースがあります。
- 2 つのホストの管理ネットワークは相互に到達可能です。

## 制限事項とガイドライン

- RBAC が有効になっている場合、この機能はシステム管理者のみが使用できます。
- ステートフル フェイルオーバ システムのセットアップ中は、いかなる操作も実行しないでください。
- ステートフル フェイルオーバ システムをセットアップした後に CVM 管理プラットフォームに参加するには、CVM ホストが次の要件を満たしている必要があります。
  - このシステムは新しく導入されたシステムです。

- ホスト上にローカル同期パーティションが存在しません。
- プライマリ/バックアップの切り替え中は、いかなる操作も実行しないでください。
- バックアップ ホストが異常な状態の場合、データが同期中の場合、またはデータ同期が異常な状態の場合は、プライマリ/バックアップの切り替えを実行しないでください。
- プライマリ/バックアップの切り替えが成功するかどうかは、データがプライマリ ホストからバックアップ ホストに同期されているかどうかによって決まります。
- ステートフル フェイルオーバー構成プロセスは、デフォルトではブラウザーの言語で表示されます。

## ステートフルフェイルオーバーシステムを設定する

1. 上部のナビゲーション バーで、**System** をクリックします。
2. 左側のナビゲーション ペインから、**Set Up Stateful Failover System** をクリックします。
3. 『パラメーター』の説明に従ってパラメーターを設定します。
4. **OK** をクリックします。

## ステートフルフェイルオーバー設定を表示する

1. 上部のナビゲーション バーで、**System** をクリックします。
2. 左側のナビゲーション ペインから、**Stateful Failover** を選択します。

開いたページには、ホスト名、ステータス、設定が表示されます。

## プライマリ/バックアップの手動切り替えを実行する

1. 上部のナビゲーション バーで、**System** をクリックします。
2. 左側のナビゲーション ペインから、**Stateful Failover** を選択します。
3. **Primary/Backup Switchover** をクリックし、**OK** をクリックします。

## ステートフルフェイルオーバーホスト情報を表示する

1. 上部のナビゲーション バーで、**System** をクリックします。
2. 左側のナビゲーション ペインから、**Stateful Failover** を選択します。

CVM ホストが CVK ホストとして CVM に追加されていない場合、システムは CVM ホストの **Network** と **Storage Adapters** タブを表示します。

3. **Network** タブで CVM ホストの vSwitch を管理します。vSwitch を追加、編集、または削除できます。
4. **Storage Adapters** タブで CVM ホストのストレージ アダプタを管理します。IQN を編集したり、ストレージ デバイスをスキャンしたりできます。

## パラメーター

### ステートフルフェイルオーバーシステムのセットアップ

- **Virtual IP Address:** CVM にアクセスするための IP アドレスを指定します。使用されていない IP アドレスである必要があります。
- **Mask/Prefix:** 仮想 IP アドレスのサブネット マスクまたはプレフィックスを指定します。
- **Backup Host IP Address:** バックアップ CVM ホストの管理 IP アドレスを指定します。
- **Backup Host Root PWD :** バックアップ CVM ホストのルート パスワードを入力します。
- **Quorum Mode:** クォーラム モードを選択します。オプションには、**詳細と Ping** があります。
  - **Advanced:** クォーラム ホストとして CVK ホストを指定します。プライマリ管理ノードとバックアップ管理ノードが相互に通信できない場合、それぞれの状態情報がクォーラム ホストに送信されます。クォーラム ホストは各ノードの役割を決定し、その役割情報をノードに送信します。クォーラム ホストとプライマリおよびバックアップ CVM ホストの CAS ソフトウェア バージョンは同じである必要があります。
  - **Ping :** 2つのクォーラム IP アドレスを指定します。プライマリ管理ノードとバックアップ管理ノードが相互に通信できない場合、クォーラム IP アドレスに ping が実行されます。ノードがどのクォーラム IP アドレスにも ping を実行できない場合、そのノードはネットワーク障害が発生していると判断し、バックアップ ノードになります。
- **Quorum Host IP Address:** クォーラム ホストの IP アドレスを指定します。クォーラム ホストには CVK コンポーネントがインストールされている必要があります。
- **Quorum Host Root PWD :** クォーラム ホストのルート パスワードを入力します。
- **Quorum IP Address:** クォーラム IP アドレスとしてアクセスできるゲートウェイの IP アドレス、または常に到達可能なホストの IP アドレスを指定します。クォーラム IP アドレスは、管理ノードのネットワーク接続を確認するために使用されます。ベスト プラクティスとして、ゲートウェイの IP アドレスを指定します。Ping クォーラム モードを選択した場合は、2つの異なるクォーラム IP アドレスを指定する必要があります。
- **Estimated Host Quantity:** データベース パーティション サイズを計算するために、CVM 内の推定ホスト数を入力します。
- **Estimated VM Quantity:** データベース パーティション サイズを計算するために、CVM 内の推定 VM 数を入力します。
- **Database Partition Size:** データベース パーティション サイズを指定します。データベース パーティションは、プライマリ管理ノードとバックアップ管理ノード間のデータ同期に使用され、/vms パーティションの一部です。データベース パーティション サイズ (MB 単位) = (推定ホスト数 × 7 MB + 推定 VM 数 × 5 MB) × 15 日 / 1024 MB。データベース パーティション サイズは 20 GB 未満にすることはできません。ステートフルフェイルオーバーのセットアップ時間を短縮するためのベスト プラクティスとして、データベース パーティション

サイズが 200 GB を超える場合は、2 つの CVM ホストの管理ネットワークを 10GE ファイバー ケーブルで接続します。

### CVM ホスト情報

- **Physical Interface:** 仮想スイッチが使用する物理 NIC 上のアップリンク インターフェイス。
- **Network Type:** 仮想スイッチのネットワーク タイプを選択します。
  - **Mgmt** —CVM とホスト間で管理データを送信します。
  - **Service-** VM のサービス データを送信します。
  - **Storage-** ホストと分散ストレージ システムまたは IP SAN ストレージ サーバーの間でパケットを送信します。このタイプの仮想スイッチは、VM では使用できません。
  - **Backup-** VM のバックアップ データを送信します。ホストにはこのタイプの仮想スイッチまたはサブネットを 1 つだけ設定でき、仮想スイッチは VM では使用できません。
  - **Migration-** VM を移行するためのデータを送信します。ホストにはこのタイプの仮想スイッチまたはサブネットを 1 つだけ設定でき、仮想スイッチは VM では使用できません。
  - **Others-** その他の種類のデータを送信します。
- **Forwarding Mode:** 仮想スイッチの転送モードを選択します。
  - **VEB** — 仮想イーサネット ブリッジ (VEB) モードでは、VM 間のトラフィックはソフトウェアを通じて転送されます。
  - **VXLAN(SDN)** : VXLAN(SDN) モードは、SDN コントローラとクラウド コンピューティング管理プラットフォームに基づく VXLAN ソリューション用に設計されています。
- **VLAN ID** : ホストのプロトコル スタックに接続されているインターフェイスの VLAN ID を入力します。
- **State:** 仮想スイッチの状態。
- **IP** : 仮想スイッチの IP アドレス。
- **Mask/Prefix:** IP アドレスのサブネット マスク。
- **Gateway:** 仮想スイッチのゲートウェイ。
- **DPDK State:** 仮想スイッチの DPDK 状態。

### CVM ホスト情報ストレージアダプタ

- **Name:** ストレージ アダプタの名前。
- **Model:** ストレージ アダプタ モデル。
- **Type:** ストレージ アダプタ タイプ。
- **State:** ストレージ アダプタの状態。
- **IQN** : ストレージ アダプタの識別子。
- **Normal Scanning:** 通常のスキャン ルールに従ってデバイスをスキャンします。
- **Forced Scanning:** デバイスを強制的にスキャンします。一部の HBA カードでは、強制スキャン (ストレージ リンクのリセット) によってのみ新しいデバイスを検出できます。この操作により、I/O タイムアウトが発生する可能性があります。

## ホストのファイアウォール設定を構成する

ホスト ファイアウォールを使用すると、ホストが使用するサービスとサービスのポート番号を表示し、特定のポート番号へのアクセスを許可する IP アドレスを設定できます。これにより、ネットワーク アクセスを効果的に制御し、不正アクセスや攻撃を防止してホストを保護できます。**System > Stateful Failover > Firewall Configuration** ページでは、プライマリ ノードとバックアップ ノードのホスト ファイアウォール設定を一元的に構成できます。

ホスト ファイアウォールは次の機能を提供します。

- ホスト上で実行されているサービスとサービスのポート番号、およびサービスへのアクセスが許可されている IP アドレスを表示します。
- ホスト上の特定のポートへのアクセスを許可する IP アドレスのリストを設定します。たとえば、192.168.1.100/16 がホスト上のポート番号 22 で SSH サービスにアクセスするように設定できます。各ポート番号に対して、許可する IP アドレスのリストを設定できます。たとえば、192.168.1.200/16 と 192.168.1.201/16 がホスト上のポート番号 80 で仮想化 Web サービスにアクセスできるようにし、172.16.1.100/16 がホスト上のポート番号 8443 で HTTPS サービスにアクセスできるようにすることができます。

## 制限事項とガイドライン

- IP アドレスが HTTPS 経由で CVM にアクセスできる場合、VNC Web サービスの許可された IP アドレス リストに含まれていなくても、VNC Web サービスにアクセスできます。
- ファイアウォール機能は、ソフトウェア バージョン E073x および E076x を使用するホストでは使用できません。
- ホスト ファイアウォールは、ホストの受信トラフィックのみを識別して制限します。
- ホストを削除すると、そのホストのファイアウォール設定も削除されます。ホストの XConsole からホストの IP アドレスを変更した後は、そのホストを再起動してファイアウォール設定を更新する必要があります。再起動しないと、元の許可された IP アドレスがすべてのポートの許可された IP アドレス リストに残ります。
- ステートフル フェイルオーバー システムが展開されている場合は、クォーラム ノードのポート 22 が他のノードに到達可能であることを確認する必要があります。ステートフル フェイルオーバー管理のホスト ファイアウォール構成は、プライマリ ノードとバックアップ ノードにのみ適用され、クォーラム ノードには適用されません。
- ステートフル フェイルオーバー後にホストが復元されたら、ステートフル フェイルオーバー管理のファイアウォール構成で **Synchronize** をクリックして、ファイアウォール構成を同期する必要があります。
- システムで実行されている機能に影響を与えないようにするには、許可された IP アドレスのリストを設定するときに次の表を使用します。

特徴	説明	推奨される操作
ステートフルフェイルオーバー	ステートフル フェイルオーバー システムをセットアップするときに、SSH サービスに対して許可された IP アドレスのリストが設定されている場合は、すべての IP アドレスを許可し、クォーラム ノードが SSH 経路でプライマリ ノードとバックアップ ノードに到達できることを確認する必要があります。	すべての IP アドレスを許可し、ステートフル フェイルオーバー システムを設定します。
CloudOS、UIS Cloud、またはサードパーティの相互運用	CAS を CloudOS、UIS Cloud、または Aishu の AnyBackup、Runstor、Qianxin、AsialInfo などのサードパーティ ソフトウェアと相互運用するには、関連する IP アドレスが HTTP サービスなどのポートにアクセスできるようにします。	CloudOS、UIS Cloud、またはサードパーティ製ソフトウェアに関連する IP アドレスへのすべてのポートを開きます。
外部プラットフォームの追加	CAS システムを外部プラットフォームとして追加する場合は、ポート 8080 または 8443 が必要です。	ポート 8080 と 8443 を開きます。
ベアメタル管理	CVM ホストからベアメタル サーバーにファイルをコピーするには、SCP サービスを使用する必要があります。	ポート 22 を開きます。
サイトの災害復旧	サイトの災害復旧では、保護されたサイトと復旧サイトでポート 8080 と 8443 を使用する必要があります。	ポート 8080 と 8443 を開きます。
ウイルス対策	CloudOS、UIS Cloud、またはサードパーティの相互運用と同じです。	CloudOS、UIS Cloud、またはサードパーティの相互運用と同じです。
クラウドレインボー	サイトの組み込みと VM の移行には、ポート 8080、8443、および 22 を使用する必要があります。	ポート 8080、8443、22 を開きます。
VM 移行	VM の移行には、ポート 8080、8443、および 22 を使用する必要があります。	ポート 8080、8443、22 を開きます。
ログのバックアップ	ログ バックアップでは、宛先のポート 22 を使用する必要があります。	ポート 22 を開きます。
バックアップ管理におけるリモート	データのバックアップには、保存先のポート 22 を使用する必要があります。	ポート 22 を開きます。

特徴	説明	推奨される操作
サーバーへのデータバックアップ		

## ホストのファイアウォール設定を表示する

1. 上部のナビゲーション バーで、**System** をクリックします。
2. 左側のナビゲーション ペインから、**Stateful Failover** を選択します。
3. **Firewall Configuration** ボタンをクリックします。現在のホストのすべてのファイアウォール ポリシーが表示されます。

## ホストのファイアウォール設定を編集する

1. 上部のナビゲーション バーで、**System** をクリックします。
2. 左側のナビゲーション ペインから、**Stateful Failover** を選択します。
3. **Firewall Configuration** ボタンをクリックします。
4. サービスの **Actions** 列で **Edit** をクリックします。
5. すべての IP アドレスを許可するには、**Allow Access from Any IP address** を選択します。1 つまたは複数の指定された IP アドレスのみを許可するには、このオプションをオフにし、IP アドレスまたは IP アドレスのコンマ区切りリストを入力します (例: 1.1.1.1,12.3.0.0/16,1:1:1:1:1:1/64)。

## ホストのファイアウォール設定を同期する

1. 上部のナビゲーション バーで、**System** をクリックします。
2. 左側のナビゲーション ペインから、**Stateful Failover** を選択します。
3. **Firewall Configuration** ボタンをクリックします。

ファイアウォール設定を同期する必要がある場合は、ポップアップ ウィンドウの左上隅に **Synchronize** ボタンが表示されます。このボタンをクリックして、ファイアウォール設定を同期します。

## CVMコラボレーションリソースの管理

ARM ホストは CVM コラボレーション リソース管理をサポートしていません。

リソース コラボレーションにより、CVM はリソース情報を他の管理システムと同期できます。たとえば、CVM は VCF コンポーネントと連携し、REST API インターフェイスを使用して VCF コントローラと通信できます。VCF コントローラは、CVM 内の vSwitch にネットワーク ポリシーを管理および展開します。リソース コラボレーションを構成する前に、CVM で VCFC リソース アクセス モードを構成する必要があります。

## コラボレーションリソースを追加する

1. 上部のナビゲーション バーで、**System** をクリックします。
2. 左側のナビゲーション ペインから、**Collaborative Managers** を選択します。
3. **Add** をクリックします。
4. 『パラメーター』の説明に従ってパラメーターを設定します。
5. **OK** をクリックします。

## コラボレーションリソースを編集する

1. 上部のナビゲーション バーで、**System** をクリックします。
2. 左側のナビゲーション ペインから、**Collaborative Managers** を選択します。
3. コラボレーション リソースの **Actions** 列で **Edit** をクリックします。
4. 『パラメーター』の説明に従ってパラメーターを設定します。
5. **OK** をクリックします。

## コラボレーションリソースを削除する

1. 上部のナビゲーション バーで、**System** をクリックします。
2. 左側のナビゲーション ペインから、**Collaborative Managers** を選択します。
3. コラボレーション リソースの **Actions** 列で **Delete** をクリックします。
4. 開いたダイアログボックスで、**OK** をクリックします。

## コラボレーションリソースの詳細を表示

1. 上部のナビゲーション バーで、**System** をクリックします。
2. 左側のナビゲーション ペインから、**Collaborative Managers** を選択します。
3. コラボレーション リソースの **Actions** 列で **View** をクリックします。

## 分散仮想スイッチ情報をVCFコントローラと同期する

1. 上部のナビゲーション バーで、**System** をクリックします。
2. 左側のナビゲーション ペインから、**Collaborative Managers** を選択します。
3. コラボレーション リソースの **Actions** 列で **Sync** をクリックします。
4. 開いたダイアログボックスで、**OK** をクリックします。

## パラメーター

- **IP Address:** リソースの IP アドレスを入力します。
- **Protocol:** リソースへのアクセスに使用するプロトコルを選択します。オプションには、**HTTP** と **HTTPS** があります。
- **Port Number:** リソースにアクセスするために使用するポート番号を入力します。
- **Collaboration Type:** リソース コラボレーション タイプを選択します。オプションには、**Strong** と **Weak** があります。
  - **Strong-** CVM は VCFC コントローラと対話します。
  - **Weak-** クラウド OS は VCFC コントローラと対話します。
- **Username:** リソースにアクセスするために使用するユーザー名を入力します。
- **Password:** ユーザーがリソースにアクセスするためのパスワードを入力します。
- **Root Path:** CVM が REST API インターフェイスを介して VCF コントローラと通信するための URL を入力します。

## ライセンスの管理

CVM 試用版は 180 日間ご利用いただけます。試用版から正式版へのアップグレードにはライセンスを申請できます。試用版と正式版の機能は同じです。ライセンスを取得するには、フランチャイザーにお問い合わせください。

ライセンス管理では、ライセンスの詳細を表示したり、ライセンスを申請したり、ライセンスを登録したりできます。

ライセンスは、ローカル ライセンスまたはライセンス サーバー ライセンスを通じて登録できます。

# 制限事項とガイドライン

- RBAC が有効になっている場合、この機能はシステム管理者のみが使用できます。
- 異機種移行機能には専用のライセンスが必要です。詳細については、ライセンス使用ガイドを参照してください。
- コンテナ エンジン機能には専用のライセンスが必要です。詳細については、ライセンス使用ガイドを参照してください。
- CVM がネストされた仮想化を使用する場合、リモート ライセンスのみを実行できます。CVM がネストされた仮想化を使用する場合、CVM は VM 上に展開されます。

## 機能

- ライセンスの詳細を表示
- ローカルライセンス
- ライセンスサーバーライセンス
- 保証情報を見る

## ライセンスの詳細を表示

ライセンスの詳細を表示するには、このタスクを実行します。

## 手順

1. 上部のナビゲーションバーで、**System** をクリックします。
2. 左側のナビゲーションパネルから、**Licenses** を選択します。

## パラメーター

- **CVM ライセンス**
  - **Manageable CPUs:** コンテナ クラスターを除き、ライセンスによって CVM が管理できる物理 CPU の数。
  - **Managed CPUs:** コンテナ クラスターを除き、CVM によって管理される物理 CPU の数。

- **CPUs Manageable by Container Cluster:** ライセンスにより CVM コンテナ クラスターが管理できる物理 CPU の数。
- **CPUs Managed by Container Cluster:** CVM コンテナ クラスターによって管理される物理 CPU の数。
- **Authorization Code:** CVM コンポーネントの認証コード。
- **Version:** CVM バージョン (標準、エンタープライズ、拡張エンタープライズ バージョンを含む)。
- **License Validity:** ライセンスの残りの有効日数。
- **異機種移行ライセンス**
  - **Total Licenses:** 異機種移行ライセンスの合計数。
  - **Used Licenses:** 使用されている異機種移行ライセンスの数。
  - **Available Licenses:** 利用可能な異機種移行ライセンスの数。

## ローカルライセンス

ローカルライセンスを通じてライセンスを登録するには、次のようにします。:

1. CVM がインストールされたホストのホスト情報ファイルを取得します。ホスト情報ファイルはライセンスのアクティベーションに使用されます。異機種移行ライセンスを要求するには、ハードウェア コード ファイルを取得します。
2. ホスト情報ファイルを使用してライセンス アクティベーション ファイルを取得します。詳細については、製品のライセンス登録ガイドを参照してください。
3. ライセンス登録を完了するには、ライセンス アクティベーション ファイルを CVM にインポートします。
4. 登録したライセンスが正式なライセンスである場合は、ライセンスアクティベーションファイル (`casLicense.lic`) をローカルディスクにエクスポートすることもできます。

## ホスト情報ファイルを取得する

1. 上部のナビゲーションバーで、**System** をクリックします。
2. 左側のナビゲーションパネルから、**Licenses** 選択します。
3. **Local Licensing** をクリックします。
4. 『パラメーター』の説明に従ってパラメーターを設定します。
5. **Download** をクリックします。

ホスト情報ファイルは自動的にローカル ディスクにダウンロードされます。ホスト情報ファイルの名前はデフォルトで `host.info` です。

## ライセンスを登録する

1. 上部のナビゲーションバーで、**System** をクリックします。
2. 左側のナビゲーションパネルから、**Licenses** を選択します。
3. **Register** をクリックします。
4. **Browse** をクリックします。
5. CVM にインポートするライセンス アクティベーション ファイルを選択します。
6. **OK** をクリックします。

## ライセンス情報のエクスポート

1. 上部のナビゲーションバーで、**System** をクリックします。
2. 左側のナビゲーションパネルから、**Licenses** を選択します。
3. **Export** をクリックします。

ライセンス アクティベーション ファイルはローカル ディスクにダウンロードされます。アクティベーション ファイルの名前は、デフォルトでは **casLicense.lic** です。

## ハードウェアコードをダウンロードする

1. 上部のナビゲーションバーで、**System** をクリックします。
2. 左側のナビゲーションパネルから、**Licenses** を選択します。
3. **Heterogeneous Migration License** エリアで、**Download Host Info File** をクリックします。

ハードウェア コード ファイルは自動的にローカル ディスクにダウンロードされます。ハードウェア コード ファイルの名前は、デフォルトでは **HardInfo.dat** です。

## パラメーター

- **End User Info**
  - **User Name:** エンドユーザーの名前を入力します。
  - **Country/Region:** エンドユーザーが居住する国/地域を選択します。
  - **Province/City:** エンドユーザーが居住する都道府県/市区町村の名前を入力します。
  - **Company/Org:** エンドユーザーが所属する会社または組織の名前を入力します。

- **Address:** エンドユーザーの詳細な住所を入力します。
- **Postcode:** エンドユーザーが居住する地域の郵便番号を入力します。
- **Email:** エンドユーザーのメールアドレスを入力します。
- **Telephone:** エンドユーザーの電話番号を入力します。
- **Applicant Info**
  - **Name:** 申請者の名前を入力してください。
  - **Company/Org:** 申請者が所属する会社名または団体名を入力してください。
  - **Email:** 申請者のメールアドレスを入力してください。
  - **Telephone:** 申請者の電話番号を入力してください。

## ライセンスサーバーのライセンス

ライセンス サーバーを通じてライセンスを要求するには、このタスクを実行します。その後、ライセンスを表示、展開、および解放できます。

## ライセンスを登録する

1. 上部のナビゲーションバーで、**System** をクリックします。
2. 左側のナビゲーションパネルから、**Licenses** を選択します。
3. **License Server Licensing** をクリックします。
4. 『パラメーター』の説明に従ってパラメーターを設定します。

## ライセンスの拡張またはリリース

1. 上部のナビゲーションバーで、**System** をクリックします。
2. 左側のナビゲーションパネルから、**Licenses** を選択します。
3. **Request/Release Licenses** をクリックします。
4. 『パラメーター』の説明に従ってパラメーターを設定します。

## ライセンスの詳細を表示

1. 上部のナビゲーションバーで、**System** をクリックします。

2. 左側のナビゲーションパネルから、**Licenses** を選択します。  
開いたページには詳細なライセンス情報が表示されます。

## パラメーター

- **Basic Info**
  - **License Server IP:** ライセンス サーバーの IP アドレスを指定します。
  - **License Server Port:** ライセンス サーバーのポート番号を指定します。
  - **Client Name:** ライセンス サーバー上の CVM システムの名前を指定します。
  - **Client Password:** ライセンス サーバー上の CVM システムのパスワードを指定します。
- **CPU Licensing**
  - **Manageable CPUs:** CVM が管理できる物理 CPU の数。
  - **Managed CPUs:** CVM によって管理される物理 CPU の数。
  - **Edition:** ライセンス版。
  - **Available CPUs:** ライセンス サーバーが許可できる物理 CPU の数。
  - **Assigned CPUs:** ライセンス サーバーが CVM システムに付与した物理 CPU の数。
  - **Actions:** ライセンスを拡張するか解放するかを選択します。
  - **CPUs:** 要求または解放する物理 CPU の数を指定します。
- **License Details**
  - **License Code:** ライセンス キー。
  - **Type:** ライセンスが正式なものか一時的なものか。
  - **Remaining Time:** ライセンスの残りの有効日数。

## 保証情報を見る

CAS システムの保証情報を表示するには、このタスクを実行します。

## 手順

1. 上部のナビゲーションバーで、**System** をクリックします。
2. 左側のナビゲーションパネルから、**Licenses** を選択します。
3. **Warranty Info** タブをクリックします。

# パラメーター

- **SN:** 保証サービスの一意的識別子。システムに登録されたライセンスのライセンス番号と同じです。ライセンスを登録した後にのみ、保証サービスと保証サービス情報を取得できます。各ライセンスには独自の保証サービス情報があります。
- **Warranty State:** システムの保証状態。
  - **No Warranty**—このライセンスには保証サービスは含まれません。
  - **Due to Expire**—このライセンスの保証サービスは 1 か月以内に期限切れになります。保証サービスの期限切れを通知するメッセージが表示されます。
  - **Expired**—このライセンスの保証サービスは期限切れです。期限内に保証サービスを更新する必要があります。
  - **Under Warranty**—このライセンスにおける保証サービスは有効です。
- **Warranty Validity Period:** 本ライセンスにおける保証サービスの有効期間。
- **Time Left:** このライセンスにおける保証サービスの残りの有効期間。

## アップグレードを管理する

ソフトウェア イメージのアップロードやアップグレード タスクの作成と実行など、ソフトウェア イメージを管理するには、このタスクを実行します。

## 制限事項とガイドライン

- アップグレード タスクを実行するには、**System > Parameters > ISLP and Security Hardening** ページで root SSH 権限を有効にする必要があります。
- アップグレード タスクを実行する前に事前チェックが成功するようにするには、クラスター名 > HA ページで HA を無効にします。
- CVM がタスクを実行していないときにアップグレード操作を実行します。CVM がタスクを実行中にアップグレード操作を実行すると、タスクが失敗する可能性があります。
- アップグレード タスクの実行が開始されると、CVM は一時的に切断されます。
- 同時アップグレードで最大数のクラスターとホストが設定されたアップグレード タスクを実行する前に、システムに十分なネットワーク帯域幅リソースがあることを確認してください。そうでない場合、ソフトウェア イメージをホストにプッシュせずにアップグレード タスクを実行すると、システムはアップグレード中にソフトウェア イメージをプッシュする必要があり、CVM のネットワーク使用率に影響します。
- E0730P08 より前のバージョンでは、バックアップ場所に関する制限はありませんでした。E0730P08 以降のバージョンでは、VM のバックアップ場所は少なくとも 3 レベルのディレクトリである必要が

あります。システムを E0730P08 より前のバージョンから E0730P08 以降にアップグレードすると、一部のディレクトリが有効にならない可能性があり、VM のバックアップが失敗する可能性があります。ベスト プラクティスとして、アップグレードが完了したら、ストレージ プール内の VM のバックアップ場所を 3 レベルのディレクトリに変更してください。

## ソフトウェアイメージをアップロードする

### このタスクについて

CVM をアップグレードしたり、CVM パッチをインストールしたりする前に、管理目的でこのタスクを実行して、必要なソフトウェア イメージを CVM にアップグレードします。

### 手順

1. 上部のナビゲーション バーで、**System** をクリックします。
2. 左側のナビゲーション ペインから、**Upgrade Management** を選択します。
3. **Upload** をクリックします。
4. グリッドをクリックし、アップロードするソフトウェア イメージを選択します。または、対象のソフトウェア イメージをグリッドにドラッグします。
5. **Start** をクリックします。

アップロードされたすべてのソフトウェア イメージの詳細情報を表示できます。

## アップグレードタスクを追加する

### このタスクについて

必要なソフトウェア イメージを CVM にアップロードした後、このタスクを実行して、アップグレード管理の目的でアップグレード タスクを作成します。

### 手順

1. 上部のナビゲーション バーで、**System** をクリックします。
2. 左側のナビゲーション ペインから、**Upgrade Management** を選択します。

3. **Upgrade Task** タブをクリックします。**Add Task** をクリックします。
4. 必要に応じてパラメーターを設定し、**OK** をクリックします。

パラメーターの詳細については、『パラメーター』を参照してください。

## アップグレードタスクをすぐに実行する

### このタスクについて

アップグレード タスクを作成した後、そのアップグレード タスクをすぐに実行するかどうかを選択できます。

### 手順

1. 上部のナビゲーション バーで、**System** をクリックします。
2. 左側のナビゲーション ペインから、**Upgrade Management** を選択します。
3. **Upgrade Task** タブをクリックします。
4. アップグレード タスクの **Actions** 列で **Run Now** をクリックします。
5. 開いたダイアログボックスで、**OK** をクリックします。

## ソフトウェアイメージをプッシュする

### このタスクについて

ソフトウェア イメージをホストにプッシュするには、このタスクを実行します。システムはアップグレードを事前チェックし、ソフトウェア イメージがホストにプッシュされた場合にのみアップグレード タスクを実行できます。

### 手順

1. 上部のナビゲーション バーで、**System** をクリックします。
2. 左側のナビゲーション ペインから、**Upgrade Management** を選択します。
3. **Upgrade Task** タブをクリックします。アップグレード タスク **Push** を選択します。
4. 開いたダイアログボックスで、**OK** をクリックします。

## 事前チェックを実行する

1. 上部のナビゲーション バーで、**System** をクリックします。
2. 左側のナビゲーション ペインから、**Upgrade Management** を選択します。
3. **Upgrade Task** タブをクリックします。
4. アップグレード タスクの **Actions** 列で **Precheck** をクリックします。
5. **Start** をクリックします。

## アップグレードタスクの詳細情報を表示する

### このタスクについて

アップグレード タスクの設定を表示するには、このタスクを実行します。

### 手順

1. 上部のナビゲーション バーで、**System** をクリックします。
2. 左側のナビゲーション ペインから、**Upgrade Management** を選択します。
3. **Upgrade Task** タブをクリックします。
4. アップグレード タスクの **Actions** 列で **More** をクリックし、**View** を選択します。

## アップグレード タスクのアップグレード ログ メッセージを表示する

### このタスクについて

アップグレード タスクのアップグレード ログ メッセージを表示するには、このタスクを実行します。アップグレード ログ メッセージには、アップグレード ターゲット、アップグレード結果、失敗の理由など、アップグレードに関する詳細情報が含まれます。

## 手順

1. 上部のナビゲーション バーで、**System** をクリックします。
2. 左側のナビゲーション ペインから、**Upgrade Management** を選択します。
3. **Upgrade Task** タブをクリックします。
4. **upgrade task** の **Actions** 列で **More** をクリックし、**Upgrade Log** を選択します。

# アップグレード ログ メッセージをダウンロードする

## このタスクについて

アップグレード タスクのアップグレード ログ メッセージをダウンロードするには、このタスクを実行します。現在のソフトウェア バージョンでは、アップグレード ログ メッセージを一括でダウンロードすることはできません。

## 手順

1. 上部のナビゲーション バーで、**System** をクリックします。
2. 左側のナビゲーション ペインから、**Upgrade Management** を選択します。
3. **Upgrade Task** タブをクリックします。
4. **upgrade task** の **Actions** 列で **More** をクリックし、**Upgrade Log** を選択します。
5. アップグレード ログの **Actions** 列の **Download** をクリックします。
6. ログファイルを保存するパスを選択し、ダウンロードを完了します。

# 修正プログラムをロールバックする

## このタスクについて

システム全体を再インストールせずに、システムを以前の安定したバージョンに復元するには、このタスクを実行します。この機能は、セキュリティの脆弱性、操作障害、主要機能の欠陥などの緊急の問題に対処し、システムの継続的かつ安定した動作を復元します。**Repository** タブのソフトウェアイメージの **Uninstall** 列に **Support** が表示されている場合にのみ、ホットフィックスをロールバックできます。

## 手順

1. 上部のナビゲーション バーで、**System** をクリックします。
2. 左側のナビゲーション ペインから、**Upgrade Management** を選択します。
3. **Upgrade Task** タブをクリックします。
4. **upgrade task** の **Actions** 列で **More** をクリックし、**Upgrade Log** を選択します。
5. アップグレード ログの **Actions** 列で **Uninstall** をクリックします。
6. 開いたダイアログボックスで、**OK** をクリックします。

# アップグレードタスクを編集する

## このタスクについて

アップグレード タスクの設定を修正または編集するには、このタスクを実行します。

## 手順

1. 上部のナビゲーション バーで、**System** をクリックします。
2. 左側のナビゲーション ペインから、**Upgrade Management** を選択します。
3. **Upgrade Task** タブをクリックします。
4. アップグレード タスクの **Actions** 列で **More** をクリックし、**Edit** を選択します。
5. 必要に応じてパラメーターを編集します。
6. **OK** をクリックします。

# アップグレードタスクを削除する

## このタスクについて

CVM からアップグレード タスクとその構成情報を削除するには、このタスクを実行します。

## 手順

1. 上部のナビゲーション バーで、**System** をクリックします。
2. 左側のナビゲーション ペインから、**Upgrade Management** を選択します。
3. **Upgrade Task** タブをクリックします。
4. アップグレード タスクの **Actions** 列で **More** をクリックし、**Delete** を選択します。
5. 開いたダイアログボックスで、**OK** をクリックします。

# ソフトウェアイメージを削除する

## このタスクについて

CVM から不要なソフトウェア イメージを削除するには、このタスクを実行します。

## 手順

1. 上部のナビゲーション バーで、**System** をクリックします。
2. 左側のナビゲーション ペインから、**Upgrade Management** を選択します。
3. ソフトウェア イメージの **Actions** 列で **Delete** をクリックします。
4. 開いたダイアログボックスで、**OK** をクリックします。

# パラメーター

## バージョンリポジトリ情報

- **Name:** アップロードされたソフトウェア イメージの名前。
- **Software Image Type:** アップロードされたソフトウェア イメージのタイプ。サポートされているタイプは次のとおりです。
  - **Patch Version:** アップロードされたソフトウェア イメージには 1 つのパッチのみが含まれています。
  - **Patch Group:** アップロードされたソフトウェア イメージには複数のパッチが含まれています。

- **Full Version:** アップロードされたソフトウェア イメージには、アップグレード用の完全なソフトウェア リリースが含まれています。
- **Published At:** ソフトウェア イメージが CVM にアップロードされた時刻。
- **Compatibility:** ソフトウェア イメージが現在の CVM バージョンと互換性があるかどうか。
- **Size:** ソフトウェア イメージのサイズ。
- **Requirements:** アップグレードの完了後にホストの再起動が必要かどうか。
- **Vendor Info:** ソフトウェア イメージが属するベンダー。
- **MD5:** ソフトウェア イメージの MD5 値。
- **Uninstall:** ソフトウェア イメージをアンインストールできるかどうか。

## アップグレードタスクリスト

- **Name:** アップグレード タスクの名前。
- **Description:** アップグレード タスクの説明。
- **Software Image:** ソフトウェア イメージを選択します。使用可能なソフトウェア イメージは、リポジトリにアップロードされたソフトウェア イメージによって異なります。選択したソフトウェア イメージがパッチ グループの場合は、それをクリックしてパッチを選択します。選択したソフトウェア イメージに含まれるすべてのパッチを選択するには、パッチを選択しないでください。
- **Upgrade Target:** アップグレードするホストを選択します。ホスト プールまたはクラスターを選択すると、ホストを一括選択できます。管理ホストの名前の横に CVM が表示されます。
- **Clusters in Concurrent Upgrade:** アップグレード タスクを同時に実行できるクラスターの数を指定します。このパラメーターの最大値は 5 です。
- **Hosts in Concurrent Upgrade:** クラスター内で同時にアップグレードできるホストの数を指定します。
  - 指定された VM のアップグレード方法が **Online Upgrade** の場合、このパラメーターの値は 1 のみになります。システムは、各クラスターで 1 つのホストのみをアップグレードして、最大 5 つのクラスターのアップグレード タスクを同時に実行できます。この場合、最大 5 つのホストを同時にアップグレードできます。
  - 指定された VM のアップグレード方法が **Offline Upgrade** の場合、このパラメーターの最大値は 10 です。システムは、最大 5 つのクラスターのアップグレード タスクを同時に実行でき、各クラスターで最大 10 台のホストをアップグレードできます。この場合、最大 50 台のホストを同時にアップグレードできます。
- **VM Upgrade:** VM のアップグレード方法を選択します。このパラメーターは、選択したソフトウェア イメージのアップグレード後にホストの再起動が必要な場合にのみ使用できます。オプションには、**Online Upgrade** と **Offline Upgrade** があります。
  - **Online Upgrade** を選択した場合、アップグレード プロセス中に VM はシャットダウンされません。

- **Offline Upgrade** を選択した場合は、アップグレード前に VM を手動でシャットダウンするか、システムが自動的に VM をシャットダウンするように設定することができます。
- **Shut Down VM:** このパラメーターは、**Offline Upgrade** を選択した場合に設定できます。オプションには、**Manual Shut Down** と **Auto Shut Down** があります。

## アップグレードログ情報

- **Upgrade Target:** アップグレード タスクを実行するホスト。
- **Upgrade Result:** ホスト上のアップグレード タスクの結果。オプションは次のとおりです。
  - **Not Started。**
  - **In Progress。**
  - **Finish。**
  - **Partially Succeeded。**
  - **Failed。**
- **Failure Reason:** アップグレードの失敗または部分的な失敗の理由。失敗の理由に基づいて問題をトラブルシューティングできます。
- **Uninstall Result:** 修正プログラムのロールバック操作の結果。オプションは次のとおりです。
  - **Not Started。**
  - **In Progress。**
  - **Finish。**
  - **Partially Succeeded。**
  - **Failed。**
- **Uninstall Failure Reason:** 修正プログラムのロールバック失敗または部分的な失敗の理由。失敗の理由に基づいて、問題をトラブルシューティングできます。

## コンポーネントを管理する

システムをインストールした後、特定の機能を使用するには、対応するコンポーネントをインストールする必要があります。システムは次のコンポーネントをサポートしています。

- **Heterogeneous platform migration component:** 異種プラットフォーム移行機能のサポートを提供します。システム インストール パッケージにはコンポーネントが含まれており、システムのインストール後に `/vms/component` ディレクトリに保存されます。コンポーネント管理ページでコンポーネント情報を表示できます。

## コンポーネントをアップロードする

1. 上部のナビゲーション バーで、**System** をクリックします。
2. 左側のナビゲーション ペインから、**Component Management** を選択します。
3. **Heterogeneous Platform Migration** タブをクリックします。
4. **Upload** をクリックし、コンポーネント ファイルを選択して、**Upload** をクリックします。

## コンポーネント情報を表示

1. 上部のナビゲーション バーで、**System** をクリックします。
2. 左側のナビゲーション ペインから、**Component Management** を選択します。
3. **Heterogeneous Platform Migration** タブをクリックします。
4. コンポーネント名、バージョン、状態、ストレージ パス、インストール時間を表示します。

## コンポーネントをインストールする

1. 上部のナビゲーション バーで、**System** をクリックします。
2. 左側のナビゲーション ペインから、**Component Management** を選択します。
3. **Heterogeneous Platform Migration** タブをクリックします。
4. インストール可能なコンポーネントを選択し、**Install** をクリックします。
5. 開いたダイアログボックスで、**OK** をクリックします。

## コンポーネントをアップグレードする

1. 上部のナビゲーション バーで、**System** をクリックします。
2. 左側のナビゲーション ペインから、**Component Management** を選択します。
3. **Heterogeneous Platform Migration** タブをクリックします。
4. アップグレード可能なコンポーネントを選択し、**Upgrade** をクリックします。
5. 開いたダイアログボックスで、**OK** をクリックします。

## コンポーネントを削除する

1. 上部のナビゲーション バーで、**System** をクリックします。
2. 左側のナビゲーション ペインから、**Component Management** を選択します。
3. **Heterogeneous Platform Migration** タブをクリックします。
4. 対象コンポーネントを選択し、**Delete** をクリックします。
5. 開いたダイアログボックスで、**OK** をクリックします。

## システム上のデータを移行する

CAS E0780 以降のバージョンでは、CVM システムは Euler オペレーティング システムを使用します。CVM システムを Euler オペレーティング システムを使用するバージョンにアップグレードするには、このタスクを実行して、Euler オペレーティング システムを使用する CVM システムにデータを移行します。データの移行後、Euler オペレーティング システムを使用する CVM システムは、ソース CVM システムによって管理されるすべてのホストに接続します。ただし、Euler オペレーティング システムを使用する CVM システムの新機能は、それらのホストでは使用できません。データの移行後、ソース CVM システムは使用できません。

## 制限事項とガイドライン

- データを移行する前に、次の情報を確認してください。
  - Euler オペレーティング システムを使用する CVM システムには、ホスト プール、クラスター、ホスト、または VM データは存在しません。
  - ソース CVM システム上のデータベース パーティションのサイズは、Euler オペレーティング システムを使用する CVM システム上のデータベース パーティションのサイズより大きくありません。
  - ソース CVM システムには凍結された VM が存在しません。
  - ソース CVM システムと、Euler オペレーティング システムを使用する CVM システムの両方に CIC および SSV コンポーネントがインストールされているか、またはどちらもインストールされていません。
  - 同じクラスター内のホストは同じソフトウェア バージョンを使用し、共有ファイル システムまたは RBD ネットワーク ストレージは 1 つのクラスターでのみ使用されます。
  - ステートフル フェイルオーバーのシナリオでは、CVM 情報を構成するときにプライマリ ノードの IP アドレスを入力します。
  - RBAC が無効になっている場合は、データ移行にシステム管理者 **admin** を使用します。RBAC が有効になっている場合は、データ移行にシステム管理者 **sysadmin** を使用し、Euler バージョンと非 Euler バージョンの両方で RBAC が有効になっていることを確認します。
- コンテナ エンジンがソース CVM システムにデプロイされている場合、データ移行後はコンテナ エンジンを使用できなくなります。コンテナ エンジンを使用するには、次のタスクを実行します。

- a. ソース CVM システムのコンテナ エンジン バージョンを、Euler オペレーティング システムを使用する CVM システムのコンテナ エンジンにアップグレードします。
- b. **System > Parameters > Container Settings** ページでコンテナ エンジンを再構成します。
  - CVM データを移行する場合は、まず、ソース vSwitch (管理、ストレージ、移行、およびバックアップタイプ) で、宛先タイプが VM であるポート ミラーリングが有効になっているかどうかを確認します。有効になっている場合は、CVM データの移行を続行する前に構成を削除します。
  - ソース CVM システムのバックアップ ポリシーは、Euler CVM システムでも使用できます。ただし、バックアップ ポリシー プールを手動で追加する必要があります。
  - データ移行後、iSCSI テンプレート プールを手動で再起動する必要があります。
  - ベスト プラクティスとして、上位バージョンのシステムで作成された VM テンプレートを使用して、下位バージョンのソフトウェアを使用する CVK ホストに VM を展開しないでください。

## 手順

1. 上部のナビゲーション バーで、**System** をクリックします。
2. 左側のナビゲーション ペインから、**Data Migration** を選択します。
3. **Migrate** をクリックします。
4. 開いたダイアログ ボックスで、『パラメーター』の説明に従って、CVM システムの OS へのログイン、互換性チェック、データ移行、クラスター HA の再有効化、ホストの接続に関するパラメーターを設定します。
5. **Finish Migration** をクリックします。
6. **OK** をクリックします。

## パラメーター

- **CVM アクセス情報の設定**
  - **IP Address:** 非 Euler CVM システムの IP アドレスを指定します。データ移行をサポートするのは、E0730P06 および E0730P06 以降の E0730 バージョンと E076X 非 Euler CVM システムのみです。
  - **Username:** 非 Euler CVM システムの OS にログインするために使用するルート ユーザー名を指定します。
  - **Password:** 非 Euler CVM システムの OS にログインするときに使用するルート パスワードを指定します。
- **クラスターHA を再度有効にする**
  - **Cluster Name:** 非 Euler CVM システム上のクラスターの名前。
  - **Result:** クラスター HA を再度有効にした結果。

- **すべてのホストを接続**
  - **Host Name:** ホストの名前。
  - **Connection State:** ホストが正常に接続されているかどうか。