

H3C CAS CVM

ユーザーガイド(クラウドサービスの管理編)

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

クラウドサービスの管理	1
制限事項とガイドライン	1
機能	1
クラウドセキュリティの管理	1
機能	2
パスワードポリシーを構成する	2
制限事項とガイドライン	2
手順	3
パラメーター	3
セキュリティゾーンを構成する	4
前提条件	4
制限事項とガイドライン	5
手順	5
パラメーター	5
秘密ポリシーを構成する	5
前提条件	5
制限事項とガイドライン	6
手順	6
パラメーター	6
アクセスポリシーを管理する	6
制限事項とガイドライン	7
アクセスポリシーを追加する	7
アクセスポリシーを編集する	7
アクセスポリシーを削除する	8
アクセスポリシーに関する詳細情報を表示する	8
パラメーター	8
2要素認証を設定する	8
制限事項とガイドライン	8
手順	9
パラメーター	9
ACL を管理する	10
制限事項とガイドライン	10
ACLを追加する	10
ACL を編集する	11
プライベート ACL をパブリック ACL に変換する	11
ACL をコピー	11
ACL を削除する	11
ACL をフィルターする	12
ACL に関する詳細情報を表示する	12
パラメーター	12
トラフィックブロックログ	13
制限事項とガイドライン	13
トラフィックブロックログを表示する	14
トラフィックブロックログをフィルターリングする	14
トラフィックブロックのログを有効にする	14
データパススルーを有効にする	14
トラフィックブロックログをクリアする	15
トラフィックブロックログを更新する	15
トラフィックブロックのログを無効にする	15

パラメーター.....	15
ネットワークセキュリティ設定を構成する.....	16
制限事項とガイドライン.....	16
vFirewallの管理.....	17
制限事項とガイドライン.....	17
vFirewallを追加する.....	17
vFirewallをインポートする.....	18
vFirewallを編集する.....	18
vFirewallを削除する.....	19
vFirewallをJSONファイルにエクスポートする.....	19
VMにvFirewallを接続する.....	19
VMからvFirewallをデタッチする.....	19
vFirewallをコピーする.....	20
パラメーター.....	20
VLAN透過伝送ポリシーを管理する.....	21
制限事項とガイドライン.....	21
VLAN透過伝送ポリシーを追加する.....	22
VLAN透過伝送ポリシーに関する情報を表示する.....	22
VLAN透過伝送ポリシーを編集する.....	22
VLAN透過伝送ポリシーを削除する.....	22
パラメーター.....	23
レート制限ポリシーを管理する.....	23
制限事項とガイドライン.....	23
レート制限ポリシーを追加する.....	23
レート制限ポリシーを編集する.....	24
プライベートレート制限ポリシーをパブリックレート制限ポリシーに変換する.....	24
レート制限ポリシーをコピーする.....	24
レート制限ポリシーを削除する.....	24
フィルターレート制限ポリシー.....	25
パラメーター.....	25
ウイルス対策サービスを設定する.....	25
制限事項とガイドライン.....	26
手順.....	26
パラメーター.....	27
共通パラメーター.....	27
AsialInfoパラメーター.....	27
QI-ANXINパラメーター.....	27
AsialInfoを設定する.....	28
制限事項とガイドライン.....	28
AsialInfoセキュリティサーバーを追加する.....	28
AsialInfoセキュリティサーバーを編集する.....	29
AsialInfo証明書をアップロードする.....	29
AsialInfoセキュリティサーバーへの接続をテストする.....	29
AsialInfoセキュリティサーバーを削除する.....	29
セキュリティポリシーを表示し、セキュリティポリシーを割り当てる.....	30
VMからセキュリティポリシーを取り戻す.....	30
パラメーター.....	30
セキュリティサービスのワークフローを管理する.....	31
前提条件.....	31
制限事項とガイドライン.....	31
セキュリティサービスのワークフローの詳細を表示する.....	31
セキュリティサービスのワークフローを処理する.....	32
セキュリティサービスワークフローを削除する.....	32

パラメーター.....	32
暗号化アプリケーションのセキュリティ評価を管理する.....	32
制限事項とガイドライン.....	33
暗号化モジュールの設定を構成する.....	33
暗号化モジュールへの接続をテストする.....	33
暗号化を有効にする.....	34
署名検証プラットフォームの設定を構成する.....	34
署名検証プラットフォームへの接続をテストする.....	34
パラメーター.....	34
ポートポリシーの管理.....	35
制限事項とガイドライン.....	35
ポートポリシーを追加する.....	36
ポートポリシーを編集する.....	36
ポートポリシーを削除する.....	36
ポートポリシーを一括削除する.....	36
ポート強化を有効にする.....	37
ポート強化を無効にする.....	37
ポートポリシーをホストに関連付ける.....	37
ポートポリシーにホストを追加する.....	37
ホストとポートポリシー間の関連付けを削除します.....	38
ホストとポートポリシー間の関連付けを一括削除する.....	38
ポートポリシーを関連ホストに同期する.....	38
ポートポリシーに関連付けられたホストを修復する.....	38
パラメーター.....	39
QAXクラウドセキュリティサービスを構成する.....	39
制限事項とガイドライン.....	39
QAXシステムに接続する.....	40
QAXコンソールにアクセスする.....	40
バックアップセンターを管理する.....	40
機能.....	40
VMバックアップの管理.....	40
機能.....	40
バックアップファイルの管理.....	41
バックアップ履歴を表示する.....	41
VM のバックアップ ファイルを一括削除する.....	41
複数の VM のバックアップ ファイルを一括削除する.....	42
パラメーター.....	42
バックアップポリシーの管理.....	42
制限事項とガイドライン.....	43
バックアップポリシーを追加する.....	43
バックアップポリシーを編集する.....	43
バックアップポリシーを削除する.....	44
バックアップポリシーを有効にする.....	44
バックアップポリシーを無効にする.....	44
バックアップ ポリシーから VM を削除する.....	44
バックアップポリシーからディスクを削除する.....	45
パラメーター.....	45
バックアッププールの管理.....	46
バックアッププールを追加する.....	46
バックアッププールを編集する.....	47
バックアッププールを削除する.....	47
パラメーター.....	47

バックアップパラメーターを構成する	48
手順	48
パラメーター	48
CVMバックアップを構成する	49
制限事項とガイドライン	49
機能	49
CVMバックアップパラメーターを構成する	49
制限事項とガイドライン	50
手順	50
パラメーター	50
CVM設定をバックアップする	51
制限事項とガイドライン	51
手順	51
CVMバックアップファイルの管理	52
制限事項とガイドライン	52
バックアップファイル情報を表示する	52
バックアップファイルをダウンロードする	52
バックアップファイルを使用してCVMを復元する	53
バックアップファイルをアップロードする	53
バックアップファイルをインポートする	53
バックアップファイルを削除する	53
パラメーター	54
スナップショットセンターを管理する	54
スナップショットを表示	55
VM のスナップショットを一括削除する	55
スナップショットを一括削除	55
パラメーター	56
DRXを管理する	56
機能	56
DRXサービスの管理	57
制限事項とガイドライン	57
DRXサービスを追加する	57
DRX サービスを編集する	57
DRX サービスを削除する	58
DRXサービスを有効にする	58
DRX サービスを削除する	58
VM を再デプロイする	58
パラメーター	58
DRXサービス監視を構成する	61
手順	62
パラメーター	62
スケジュールされた拡張ポリシーを管理する	62
制限事項とガイドライン	62
スケジュールされた拡張ポリシーを追加する	63
スケジュールされた拡張ポリシーを編集する	63
スケジュールされた拡張ポリシーを削除する	63
スケジュールされた拡張ポリシー情報を表示する	64
パラメーター	64
垂直拡張ポリシーを構成する	64
手順	65
パラメーター	65

LB リソースコラボレーションを構成する	65
前提条件	65
手順	66
パラメーター	66
DRXサービスの概要を表示する	66
手順	67
パラメーター	67
DRX サービスで VM 情報を表示する.....	68
手順	68
パラメーター	68
DRXサービス監視情報を表示する.....	69
手順	69
パラメーター	69
LBコラボレーションリソースを表示する	69
手順	70
パラメーター	70
DRXサービス操作ログを表示する.....	71
手順	71
パラメーター	71
インテリジェントなリソーススケジュールを管理する	72
機能	72
サービステンプレートの管理	72
制限事項とガイドライン	73
サービステンプレートを追加する	73
サービステンプレートを編集する	73
サービステンプレートを削除する	73
サービステンプレートの詳細を表示する	74
パラメーター	74
iRS サービスの管理.....	75
制限事項とガイドライン	75
iRS サービスを追加する	76
iRS サービスを編集する	76
iRS サービスを削除する	76
パラメーター	76
iRS サービスで VM 情報を表示する	77
手順	77
パラメーター	78
iRS サービスに関するパフォーマンス監視情報を表示する	78
手順	78
パラメーター	79
iRS サービスでリソースの詳細を表示する.....	79
手順	79
パラメーター	79
iRS サービスでリソースの使用履歴を表示する.....	80
手順	80
パラメーター	80
災害復旧の管理	81
制限事項とガイドライン	81
機能	82

サイトの管理.....	82
制限事項とガイドライン	82
サイトを追加する.....	82
サイトを編集する.....	83
サイトを削除する.....	83
ストレージレイマネージャーを追加する	83
ストレージレイマネージャーを編集する	83
ストレージレイマネージャーを削除する.....	84
ストレージレプリケーション情報を同期する.....	84
ストレージレプリケーション情報を表示する.....	84
パラメーター.....	84
保護グループの管理	85
制限事項とガイドライン	86
機能	86
保護グループを作成する	86
制限事項とガイドライン	86
手順	87
パラメーター.....	88
保護グループを編集する	89
制限事項とガイドライン	89
手順	89
保護グループを削除する	89
制限事項とガイドライン	89
手順	89
保護グループのリソース マッピング関係を編集する	90
保護グループにVMを追加する.....	90
制限事項とガイドライン	90
手順	90
パラメーター.....	91
保護グループからVMを削除する.....	91
制限事項とガイドライン	91
手順	91
保護グループを同期する	91
制限事項とガイドライン	91
手順	92
保護グループ内のVMを同期する.....	92
制限事項とガイドライン	92
手順	92
復旧計画を管理する.....	92
制限事項とガイドライン	93
機能	93
復旧計画を追加する.....	93
制限事項とガイドライン	93
手順	93
パラメーター.....	94
復旧計画を編集する.....	94
制限事項とガイドライン	94
手順	94
パラメーター.....	94
復旧計画を削除する.....	94

制限事項とガイドライン	95
手順	95
復旧計画を実行する.....	95
制限事項とガイドライン	96
復旧計画をテストする.....	96
スケジュールされたリカバリを実行する.....	96
スケジュールされたリカバリを一括で実行する.....	97
障害回復を実行する.....	97
障害回復を一括で実行する.....	97
リバースリカバリを実行する.....	97
逆レプリケーションを実行する.....	98
リバースリカバリを実行する.....	98
パラメーター.....	98
復旧計画の概要を表示する.....	99
手順.....	99
パラメーター.....	99
復旧タスクの詳細を表示する.....	99
制限事項とガイドライン	99
手順.....	100
パラメーター.....	100
クラウドレインボーを管理する.....	100
前提条件.....	100
制限事項とガイドライン	101
CVMを追加する.....	101
CVMを編集する.....	101
CVMを削除する.....	102
CVM間でVMを移行する.....	102
パラメーター.....	102
異機種間の移行を管理する.....	102
制限事項とガイドライン	103
機能.....	103
移行タスクの管理.....	103
制限事項とガイドライン	103
移行タスクを作成する.....	104
移行タスクを開始する.....	104
移行タスクを一時停止する.....	104
移行タスクを完了する.....	105
移行タスクを削除する.....	105
移行タスクの詳細を表示する.....	105
移行タスクの表示.....	105
パラメーター.....	106
ドライバーを構成する.....	107
制限事項とガイドライン	107
ハードウェア情報をエクスポートする.....	108
ドライバーをインポートする.....	108
異機種移行の概要情報を表示する.....	108
パラメーター.....	108
ソースデバイスを表示.....	109
手順.....	109
パラメーター.....	109
宛先VMを表示する.....	110

手順	110
パラメーター	110
移行クライアントをダウンロードして設定する	111
クライアントプロキシIPアドレスを更新する	111
クライアントをダウンロードする	111
外部バックアップシステムを管理する	111
外部バックアップシステムを構成する	112
外部バックアップシステムコンソールにアクセスする	112
パラメーター	112
CDPベースの災害復旧プラットフォーム	112
サービス設定を構成する	112
コンソールにアクセスする	113
パラメーター	113

クラウドサービスの管理

ARM ホストは IRS または異種移行サービスをサポートしていません。

クラウド サービス管理は、動的なリソース拡張、インテリジェントなリソース スケジューリング、サイトの災害復旧、リソース共有サービスを提供します。

制限事項とガイドライン

ロールベースのアクセス制御 (RBAC) モードでは、システム管理者のみがクラウド サービスを管理できます。

機能

- バックアップセンターを管理する
- スナップショットセンターを管理する
- DRX を管理する
- インテリジェントなリソーススケジュールを管理する
- 災害復旧の管理
- クラウドレインボーを管理する
- 異機種間の移行を管理する
- 外部バックアップシステムを管理する
- CDP ベースの災害復旧プラットフォーム

クラウドセキュリティの管理

ARM ホストは、セキュリティゾーン、秘密ポリシー、またはセキュリティ サービス ワークフローをサポートしていません。

クラウド セキュリティ管理には、パスワード ポリシー、セキュリティゾーン、セキュリティポリシー、アクセス ポリシー、2 要素認証、ACL、ネットワーク セキュリティ構成、vFirewall、ネットワーク レート制限ポリシー、CVM バ

バックアップ、ウイルス対策サービス、セキュリティ サービス ワークフロー、およびポート ポリシーの構成が含まれます。

機能

- パスワードポリシーを構成する
- セキュリティゾーンを構成する
- セキュリティポリシーを構成する
- アクセスポリシーを管理する
- 2 要素認証を設定する
- ACL を管理する
- トラフィックブロックログ
- ネットワークセキュリティ設定を構成する
- vFirewall の管理
- VLAN 透過伝送ポリシーを管理する
- レート制限ポリシーを管理する
- ウイルス対策サービスを設定する
- セキュリティサービスのワークフローを管理する
- 暗号化アプリケーションのセキュリティ評価を管理する
- ポートポリシーの管理
- QAX クラウドセキュリティサービスを構成する

パスワードポリシーを構成する

パスワードの複雑さと有効期間を設定するには、このタスクを実行します。パスワード ポリシーはすべてのオペレーターに適用されます。パスワード ポリシーでは、パスワードの最小長、複雑さの要件、有効期間を定義します。

制限事項とガイドライン

RBAC モードでは、セキュリティ管理者だけがパスワード ポリシーを構成できます。

パスワード ポリシーの変更は、CVM に登録するオペレーターに直ちに有効になり、パスワードの有効期限が切れた後に登録済みオペレーターにも有効になります。

手順

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

Password Policy Details 領域には、現在のパスワード ポリシー設定が表示されます。

3. **Edit** をクリックして、パスワードの最小文字数、複雑さの要件、有効期間、新しいパスワードと異なる必要がある以前のパスワードの数 (現在のパスワードを含む) などのパスワード ポリシー設定を編集します。
4. OK をクリックします。

パラメーター

- **Min Length:** パスワードの最小長を指定します。
- **Complexity:** パスワードの複雑さの要件を選択します。オプションには、**Not limited, Contain letters and numbers, Contain special characters, Contain letters, numbers, and special characters, and Contain uppercase letters, lowercase letters, numbers,** そして **special characters.** があります。特殊文字の詳細については、特殊文字表を参照してください。
- **Validity Period:** パスワードの有効期間を指定します。
- **Most Recent Passwords to Check:** 新しいパスワードが異なる必要がある以前のパスワードの数 (現在のパスワードを含む) を指定します。このパラメーターのデフォルト値は 1 です。たとえば、このパラメーターの値を 1 に設定した場合、新しいパスワードは現在のパスワードと同じにすることはできません。このパラメーターの値を 2 に設定した場合、新しいパスワードは現在のパスワードまたは以前のパスワードと同じにすることはできません。

特殊文字(半角)

キャラクター	名前	キャラクター	名前
~	チルダ	`	アポストロフィ
!	感嘆符	@	アットマーク
#	ポンド記号	\$	ドル記号
%	パーセント記号	^	キャレット
&	アンパサンド記号	*	アスタリスク

キャラクター	名前	キャラクター	名前
()	括弧	=	等号
+	プラス記号		縦棒
-	マイナス記号	-	アンダースコア
	括弧	{}	括弧
:	コロソ	;	セミコロソ
\	バックスラッシュ		クォーテーションマーク
,	コンマ	/	スラッシュ
。	ドット	<>	角括弧
?	疑問符		スペース

セキュリティゾーンを構成する

ARM ホストはセキュリティゾーンをサポートしていません。

のセキュリティゾーンは、その中のクラスターを他のクラスターから分離します。セキュリティゾーン内の VM のシークレットレベルは、シークレット、機密、または極秘である必要があります。セキュリティゾーン内の VM は、VM が属するクラスター内でのみ移行およびクローン作成できます。セキュリティゾーン内の VM は、クローン作成またはテンプレートに変換できません。非セキュリティゾーン内の VM のシークレットレベルは内部使用のみである必要があります、VM は非セキュリティゾーン内でのみ移行およびクローン作成できます。

前提条件

セキュリティゾーンは、セキュアモードが有効になっている場合にのみ使用できます。セキュアモードの詳細については、『システムパラメーターを構成する』を参照してください。

制限事項とガイドライン

RBAC モードでは、セキュリティ管理者だけがセキュリティゾーンを構成できます。

セキュリティゾーン内のホストおよびクラスターは、セキュリティゾーン内にはないホストおよびクラスターと同じ共有ストレージを使用できません。

手順

1. 上部のナビゲーションバーで、**Services** をクリックします。
2. 左側のナビゲーションペインから、**Security > Security Zone** を選択します。
Select Clusters 領域には、現在のクラウドリソースが表示されます。
3. **Edit** をクリックし、セキュリティゾーンに追加するクラスターを選択します。
4. **OK** をクリックします。

パラメーター

Select Clusters: セキュリティゾーンに追加するクラスターを選択します。

秘密ポリシーを構成する

ARM ホストは秘密ポリシーをサポートしていません。

秘密ポリシーは、指定された秘密レベルの VM で実行できる操作と、これらの VM を移行できるホストを制限します。

前提条件

秘密ポリシーは、セキュアモードが有効になっている場合にのみ使用できます。セキュアモードの詳細については、『システムパラメーターを構成する』を参照してください。

制限事項とガイドライン

RBAC モードでは、セキュリティ管理者だけが秘密ポリシーを構成できます。

手順

1. 上部のナビゲーション バーで、**Services** をクリックします。
2. 左側のナビゲーション ペインから、**Security > Secrecy Policy** を選択します。
セキュリティ レベルや信頼できるホストなど、現在の秘密ポリシー設定が表示されます。
3. **Edit** をクリックします。秘密レベルを選択し、信頼ゾーンに追加するホストを選択します。
4. **OK** をクリックします。

パラメーター

- **Security Level:** 対象のシークレット レベルを選択します。選択したシークレット レベルの VM については、クローンを作成したり、ディスクを切断したり、削除中にディスク ファイルをクリアしたりすることはできません。
- **Select Hosts:** 信頼ゾーンに追加するホストを選択します。選択したシークレット レベルの VM は、信頼ゾーン内のホストにのみ移行できます。ホストが選択されていない場合、選択したシークレット レベルの VM は移行できません。

アクセスポリシーを管理する

アクセス ポリシーは、オペレーターへのアクセス制御設定を定義します。管理者はアクセス ポリシーを参照して、オペレーターへの CVM ログインを許可または拒否できます。アクセス ポリシーは、参照された場合にのみ有効になります。

アクセス ポリシーには次の種類があります。

- **Access time control policy-** オペレーターがシステムにアクセスできる時間を制限します。
- **IP control policy-** 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 アドレスを制限します。
- **Access time and IP control policy-** オペレーターのアクセス時間と IP アドレスの両方を制限します。

オペレーターのアクセス時間と IP アドレスの両方が制限されている場合、次のルールが適用されます。

- 有効なアクセス ポリシーのルールで指定された IP アドレスを使用するオペレーターの場合:

- ルールで IP アドレスが許可されている場合、オペレーターは許可された期間内にシステムにアクセスできます。
- ルールによって IP アドレスが拒否された場合、オペレーターはシステムにアクセスできません。
- 有効なアクセス ポリシーのどのルールにも指定されていない IP アドレスを使用するオペレーターの場合:
 - デフォルトのアクションが許可の場合、オペレーターは許可された期間内にシステムにアクセスできます。
 - デフォルトのアクションが拒否の場合、オペレーターはシステムにアクセスできません。

制限事項とガイドライン

- RBAC モードでは、セキュリティ管理者だけがアクセス ポリシーを構成できます。
- アクセス ポリシーのルール内のアクションは、アクセス ポリシーの既定のアクションと同じにすることはできません。
- オペレーターが使用しているアクセス ポリシーは削除できません。
- アクセス ポリシーには複数のルールを含めることができます。

アクセスポリシーを追加する

1. 上部のナビゲーション バーで、**services** をクリックします。
2. 左側のナビゲーション ペインから、**Security > Access Policies** を選択します。
3. **追加** 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。

アクセスポリシーを編集する

1. 上部のナビゲーション バーで、**Services** をクリックします。
2. 左側のナビゲーション ペインから、**Security > Access Policies** を選択します。
3. 対象のアクセス ポリシーを選択し、**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。

アクセスポリシーを削除する

1. 上部のナビゲーション バーで、**Services** をクリックします。
2. 左側のナビゲーション ペインから、**Security > Access Policies** を選択します。
3. 対象のアクセス ポリシーを選択し、**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。

アクセスポリシーに関する詳細情報を表示する

1. 上部のナビゲーション バーで、**Services** をクリックします。
2. 左側のナビゲーション ペインから、**Security > Access Policies** を選択します。
3. 対象のアクセス ポリシーを選択し、**View** をクリックします。

パラメーター

- **Default Action:** アクセスポリシールールに一致しないオペレーターに対して実行するアクションを選択します。オプションには、**Allow** と **Reject** があります。
- **Access Time:** アクセス ポリシーに一致するオペレーターがシステムにアクセスできる時間を設定します。オプションには、**Not Limit**, **Weekly**, **Daily** があります。
- **Start IP:** IP アドレス範囲の開始 IP を入力します。オペレーターの IP アドレスが IP アドレス範囲内にある場合、オペレーターはルールに一致します。
- **End IP:** IP アドレス範囲の終了 IP を入力します。
- **Action:** ルールに一致する演算子に対して実行するアクションを選択します。オプションには、**Allow** と **Reject** があります。

2要素認証を設定する

このタスクを実行すると、オペレーターが証明書認証、ワンタイム パスワード (OTP)、または検証コードを使用してシステムにログインできるようになります。2 要素認証を有効にすると、オペレーターはユーザー名、パスワード、および PIN 番号、OTP、または検証コードを使用してシステムにログインします。

制限事項とガイドライン

RBAC モードでは、セキュリティ管理者だけが 2 要素認証を構成できます。

証明書認証を有効にするには、アップロードされたルート証明書が正しいこと、および USB キーを使用してシステムに正しくログインできることを確認します。

OTP 認証を有効にするには、アップロードされたエージェント構成ファイルが正しいことを確認してください。

手順

1. 上部のナビゲーション バーで、**Services** をクリックします。
2. 左側のナビゲーション ペインから、**Security > 2FA Authentication** を選択します。
現在の 2 要素 (2FA) 認証設定が表示されます。
3. **Edit** をクリックします。
4. 2FA を有効にするには、**Yes** を選択し、認証モードを選択して関連するパラメーターを構成し、**OK** をクリックします。
5. **SMS CAPTCHA** を選択した場合は、**SMS CAPTCHA** 設定をクリックし、**Enable Verification Code** を選択します。詳細については、『**SMS パラメーターの設定**』を参照してください。
6. 2FA 認証設定をクリアして無効化状態に戻すには、**Reset** をクリックします。

パラメーター

- **Enable 2FA:** 2 要素認証を有効にして、オペレーターがユーザー名、パスワード、PIN 番号、OTP、または確認コードを使用してシステムにログインするように設定します。
- **Authentication:** 認証モードを選択します。オプションには、**Certificate Authentication**, **OTP**, **Verification Code**, **SMS CAPTCHA** があります。
 - 証明書認証を有効にする場合は、次のパラメーターも設定する必要があります。
 - **Manufacturer Type:** 製造元タイプを選択します。オプションは **InfoSec** と **Fisec** です。
 - **Root Certificate:** USB キーの検証に使用するルート証明書を選択します。選択したルート証明書は自動的にシステムにアップロードされます。ルート証明書ファイルは 5 MB を超えることはできません。
 - **Scheduled CRL Update:** システムが CRL を定期的に更新できるようにします。この機能を有効にする場合は、次のパラメーターも設定する必要があります。
 - **URL:** CRL をフィルターリングするための Web サイトのアドレスを入力します。
 - **Frequency:** CRL の更新頻度を選択します。オプションには、**Monthly**, **Weekly**, **Daily** があります。
 - **Days:** CRL を更新する日付を指定します。

- **Time:** CRL が更新される時刻を指定します。
- OTP 認証を有効にする場合は、次のパラメーターも設定する必要があります。
 - **OTP Vendor:** OTP ベンダーを指定します。オプションには、**FEITIAN** と **AISEC** があります。
 - **Primary Authentication Agent Settings:** 認証エージェント構成ファイルをアップロードします。このフィールドは、OTP ベンダーが FEITIAN の場合にのみ必要です。構成ファイルをダウンロードするには、FEITIAN Technologies OPT サーバー管理センターにアクセスできます。
 - **Authentication Server Address:** 認証サーバーのアドレスを指定します。このフィールドは、OTP ベンダーが AISEC の場合にのみ必須です。
- **SMS CAPTCHA** を選択した場合は、**SMS CAPCHASettings** をクリックし、**Enable Verification Code** を選択します。

ACL を管理する

アクセス制御リスト (ACL) は、送信元 IP アドレス、宛先 IP アドレス、ポート番号などの基準に基づいてトラフィックを識別するための一連のルールです。このルールは、許可ステートメントまたは拒否ステートメントとも呼ばれます。

ACL を構成すると、VM へのネットワーク アクセスを制限し、VM 上で実行されているサービスのセキュリティを強化できます。

制限事項とガイドライン

RBAC モードでは、セキュリティ管理者だけが ACL を管理できます。

ポート プロファイルで使用される ACL は削除できません。

ACLを追加する

1. 上部のナビゲーション バーで、**Services** をクリックします。
2. 左側のナビゲーション ペインから、**Security > ACLs** を選択します。
3. **Add** をクリックします。
4. ACL の名前と説明を入力し、デフォルトの受信アクション、デフォルトの送信アクション、ACL タイプ、および所有者を選択します。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。
5. ACL を時間ベースの ACL として設定するかどうかを設定します。設定する場合は、ACL が有効になる時間を指定します。

6. **Add** をクリックして ACL のルールを追加し、『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。
7. ACL ルールの優先順位を変更するには、**Edit Rule Priorities** をクリックし、ルールをドラッグして順序を変更し、**OK** をクリックします。
8. **OK** をクリックします。

ACL を編集する

1. 上部のナビゲーション バーで、**Services** をクリックします。
2. 左側のナビゲーション ペインから、**Security > ACLs** を選択します。
3. 対象の ACL 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、ACL のルールを設定し、ルールの優先順位を設定します。
5. **OK** をクリックします。

プライベート ACL をパブリック ACL に変換する

1. 上部のナビゲーション バーで、**Services** をクリックします。
2. 左側のナビゲーション ペインから、**Security > ACLs** を選択します。
3. ターゲット ACL を選択し、**Convert to Public Policy** 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。

ACL をコピー

1. 上部のナビゲーション バーで、**Services** をクリックします。
2. 左側のナビゲーション ペインから、**Security > ACLs** を選択します。
3. 対象の ACL を選択し、**Copy** 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を設定し、**OK** をクリックします。

ACL を削除する

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

3. 対象の ACL 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。

ACL をフィルターする

1. 上部のナビゲーション バーで、**Services** をクリックします。
2. 左側のナビゲーション ペインから、**Security > ACLs** を選択します。
3. ACL を所有者別にフィルターリングするには、**Used By** フィールドから **Private**、**Public**、または **All** を選択します。

ACL に関する詳細情報を表示する

1. 上部のナビゲーション バーで、**Services** をクリックします。
2. 左側のナビゲーション ペインから、**Security > ACLs** を選択します。
3. 対象の ACL を選択し、**表示** をクリックします。

パラメーター

- **Default Inbound Action:** どのルールにも一致しない受信パケットに対して実行するアクションを選択します。オプションには、**Allow** と **Reject** があります。
- **Default Outbound Action:** どのルールにも一致しない送信パケットに対して実行するアクションを選択します。オプションには、**Allow** と **Reject** があります。
- **ACL Type:** ACL タイプを選択します。オプションには、**IP** と **Layer 2** があります。
 - **IP** ルールは、送信元 IP アドレス、宛先 IP アドレス、IP プロトコルなどのレイヤー 3 およびレイヤー 4 情報に基づいてパケットを照合します。
 - **Layer 2** - ルールは、送信元 MAC アドレスや宛先 MAC アドレスなどのリンク層情報に基づいてパケットを照合します。
- **Used By:** ACL 所有者を選択します。オプションには、**Public** と **Private** があります。パブリック ACL はすべてのユーザーが表示および使用できますが、プライベート ACL は ACL 作成者と同じユーザー グループのユーザーのみが表示および使用できます。
- **Time Based Control:** ACL を時間ベースの ACL として設定するかどうかを設定します。設定する場合は、ACL の有効時間を指定します。時間ベースでない ACL のルールは常に有効です。
- **Direction:** ルールに一致するパケットの方向を選択します。オプションには、**Inbound**、**Outbound**、**Inbound**、**outbound** があります。

- **Action:** ACL ルールに一致するパケットに対して実行するアクションを選択します。オプションには、**Allow** と **Reject** があります。

ACL Type パラメーターに **IP** を選択した場合は、次のパラメーターを設定します。

- **プロトコル:** ルールに一致するパケットのプロトコルを選択します。オプションには、**ALL**、**ICMP**、**TCP**、**UDP** があります。
- **IP Type:** IP プロトコルのバージョンを選択します。オプションには **IPv4** と **IPv6** があります。
- **Source IP :** ルールに一致する送信元 IP アドレスを入力します。
- **Source Subnet Mask:** ルールが一致する送信元サブネットマスクを入力します。
- **Source Network Prefix:** 送信元 IP アドレスのプレフィックス長を入力します。
- **Source Port:** ルールが一致する送信元ポートを指定します。
- **Destination IP :** ルールに一致する宛先 IP アドレスを入力します。
- **Destination Subnet Mask:** ルールが一致する宛先サブネットマスクを入力します。
- **Destination Network Prefix:** 宛先 IP アドレスのプレフィックス長を入力します。
- **Destination Port:** ルールが一致する宛先ポートを指定します。

ACL Type パラメーターに **Layer 2** を選択した場合は、次のパラメーターを設定します。

- **Protocol:** ルールに一致するパケットのプロトコルを選択します。オプションには、**ALL**、**ARP**、**RARP**、**IPv4**、**IPv6** があります。
- **Source MAC :** ルールに一致する送信元 MAC アドレスを入力します。
- **Source MAC Mask:** ルールが一致する送信元 MAC マスクを入力します。MAC マスクは MAC アドレスと同じ形式です。MAC マスクを指定して、ルールが MAC アドレスのクラスに一致するように設定できます。
- **Destination MAC :** ルールに一致する宛先 MAC アドレスを入力します。
- **Destination MAC Mask:** ルールが一致する宛先 MAC マスクを入力します。MAC マスクは MAC アドレスと同じ形式です。MAC マスクを指定して、ルールが MAC アドレスのクラスに一致するように設定できます。

トラフィックブロックログ

トラフィック ブロック ログには、管理プラットフォームによってブロックされたパケットに関する情報が記録されます。これらのログは、トラフィック分析、攻撃検出、ネットワーク動作監査に使用できます。さらに、通信障害が発生した場合は、トラフィック バイパスを有効にして、すべての管理プラットフォーム ネットワーク ポリシーを無効にし、すべてのサービス トラフィックを許可して、障害の原因がネットワーク ポリシーにあるかどうかを判断できます。

制限事項とガイドライン

- トラフィック ブロック ログをフィルターリングするために IP アドレスまたは IP アドレス範囲を指定すると、システムはそれをブロックされたパケットの送信元 IP アドレスと宛先 IP アドレスの両方と照合します。トラフィック ブロック ログ エントリは、その送信元 IP アドレスまたは宛先 IP アドレスが指定された基準と一致する限り表示されます。
- VM ポートにトラフィック ブロック ポリシーを設定し、そのポートをポート ミラー イメージの送信元ポートとして設定した場合、そのポートはトラフィック ブロック ログに記録されません。これは、そのポート ミラー イメージの宛先ポートにパケットを送信できるためです。

トラフィックブロックログを表示する

上部のナビゲーション バーで **Services** をクリックし、左側のナビゲーション ペインから **Security > Traffic Block Logging** を選択します。送信元 IP アドレス、宛先 IP アドレス、宛先ポート、宛先 MAC アドレス、プロトコル、時間、送信元 MAC アドレス、送信元ポート、データ パケット サイズ (バイト)、一致したブロック ルールなど、詳細なネットワーク ログ情報を表示できます。これらのフィールドの説明については、『**パラメーター**』を参照してください。

トラフィックブロックログをフィルターリングする

1. 上部のナビゲーション バーで **Services** をクリックし、左側のナビゲーション ペインから **Security > Traffic Block Logging** を選択します。

2. ページの上部にフィルター条件を入力します。IP アドレスまたは IP アドレス範囲を入力したり、プロトコルを選択したり、一致するブロック ルールを入力したり、時間範囲を指定したりできます。また、複数のフィルター条件を入力することもできます。

IP アドレスまたは IP アドレス範囲でトラフィック ブロック ログをフィルターリングする場合は、単一の IP アドレスまたは IP アドレス範囲を入力できます。たとえば、192.168.252.1、または 192.168.252.1 ~ 192.168.252.10 などです。

3. **Filter** をクリックします。

フィルター条件に一致するすべてのトラフィック ブロック ログがリストに表示されます。

トラフィックブロックのログを有効にする

1. 上部のナビゲーション バーで **Services** をクリックし、左側のナビゲーション ペインから **Security > Traffic Block Logging** を選択します。
2. **Enable Traffic Block Logging** をクリックします。


データパススルーを有効にする

1. 上部のナビゲーション バーで **Services** をクリックし、左側のナビゲーション ペインから **Security >Traffic Block Logging** を選択します。
2. **Enable Data Passthrough** をクリックします。
3. 開いたダイアログボックスで、**OK** をクリックします。

トラフィックブロッックログをクリアする

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

トラフィックブロッックログを更新する

1. 上部のナビゲーション バーで **Services** をクリックし、左側のナビゲーション ペインから **Security >Traffic Block Logging** を選択します。
2. アイコン  をクリックします。
3. ページの右側で更新間隔を選択できます。

トラフィックブロッックのログを無効にする

1. 上部のナビゲーション バーで **Services** をクリックし、左側のナビゲーション ペインから **Security >Traffic Block Logging** を選択します。
2. **Disable Traffic Block Logging** をクリックします。

パラメーター

- **Source IP** : ブロックされたパケットの送信元 IP アドレス。
- **Destination IP** : ブロックされたパケットの宛先 IP アドレス。
- **Destination Port**:ブロックされたパケットの宛先ポート。
- **Destination MAC**:ブロックされたパケットの宛先 MAC アドレス。
- **Protocol**: ブロックされたパケットで使用されるプロトコル。ARP、ICMP、ICMPv6、TCP、または UDP のいずれかです。

- **Time:** パケットがブロックされた時間。
- **Source MAC :** ブロックされたパケットの送信元 MAC アドレス。
- **Source Port:** ブロックされたパケットの送信元ポート。
- **Packet Size (bytes):** ブロックされたパケットのサイズ (バイト単位)。
- **Matched Block Rule:** パケットに一致する ACL または vFirewall の名前。vFirewall 名には **FW_** というプレフィックスが付きます。

ネットワークセキュリティ設定を構成する

この機能を使用すると、VM のネットワーク ポリシー テンプレートを構成できます。ネットワーク ポリシー テンプレートは、ACL、VLAN、QoS などのネットワーク制御機能のグループを定義します。

VM の NIC にネットワーク ポリシー テンプレートを適用すると、次のルールが有効になります。

- ネットワーク ポリシー テンプレートが ACL を参照する場合、仮想スイッチはトラフィックに一致する ACL ルールに従って VM からのトラフィックを処理します。
- VM が属する VLAN は、ネットワーク ポリシー テンプレートで指定された VLAN ID によって決まります。
- VM の NIC のトラフィック レート制限は、次のいずれかの項目によって決まります。
 - ネットワーク ポリシー テンプレートによって参照されるネットワーク レート制限ポリシー。
 - ネットワーク ポリシー テンプレート内で定義された受信トラフィックと送信トラフィックのレート制限。
- VM の NIC は、ネットワーク ポリシー テンプレートで定義された優先度値の降順でネットワークを使用します。

制限事項とガイドライン

この機能は RBAC モードでのみ使用できます。この機能を設定できるのはセキュリティ管理者のみです。

手順

1. 上部のナビゲーション バーで、**Services** をクリックします。
2. 左側のナビゲーション ペインから、**Security > Network Security Settings** を選択します。VM で使用されるネットワーク セキュリティ設定を表示できます。
3. VM のネットワーク セキュリティ設定を編集するには、その VM を選択し、**Edit** をクリックして、目的のネットワーク ポリシー テンプレートを選択します。
4. 必要に応じてネットワーク ポリシー テンプレートを編集し、**OK** をクリックします。

vFirewallの管理

vFirewall はフィルターリング ルールのセットです。vFirewall は VM を攻撃から保護し、データセンター VM のセキュリティと高可用性を向上させます。

vFirewall は、接続ステータスに基づく検出メカニズムを使用します。ファイアウォールは、2 つのピア間の接続で送信されるすべてのパケットをトラフィック フローとして識別します。新しいアプリケーション接続の場合、ファイアウォールはルールをチェックし、ルールによって許可された接続を許可し、接続に関するステータス情報を含むステータス テーブルを生成します。接続の後続のパケットは、ステータス テーブルに一致する限り許可されます。

システムは次の vFirewall タイプをサポートしています。

- **Allowlist firewall**- ルールに一致するトラフィックを許可し、その他のトラフィックをドロップします。
- **Denylist firewall**- ルールに一致するトラフィックをドロップし、他のトラフィックを許可します。

システムは、TCP、UDP、ICMP のルールに加え、DNS、HTTP、HTTPS、IMAP、IMAPS、LDAP、MS SQL、MYSQL、POP3、POP3S、RDP、SMTP、SMTPS、SSH などの一般的なアプリケーション プロトコルもサポートしています。

システムでは、次のファイアウォール ルール タイプが提供されます。

- **Ingress rule**- リモート サイトから開始される接続を制限します。
- **Egress rule**- VM によって開始される接続を制限します。

アプリケーション プロトコルの場合、ルールのデフォルトの方向は入力です。

制限事項とガイドライン

- RBAC モードでは、セキュリティ管理者だけが vFirewall を管理できます。
- vFirewall と ACL は相互に排他的です。VM に vFirewall と ACL の両方が設定されている場合は、vFirewall が有効になります。
- デフォルトでは、vFirewall はすべての DHCP 接続を許可します。VM の DHCP パケットをフィルターリングするには、VM の ACL を設定します。
- VM で使用されている vFirewall は削除できません。

vFirewallを追加する

1. 上部のナビゲーション バーで、**Services** をクリックします。
2. 左側のナビゲーション ペインから、**Security > vFirewalls** を選択します。
3. **Add** をクリックします。

4. vFirewall の名前と説明を入力します。
5. ファイアウォールの種類を選択します。
6. **Add Rule** をクリックします。
7. ルールを追加して **Add Virtual Firewall** ダイアログ ボックスに戻るには、ルールを構成して **OK** をクリックします。ルールを一括で追加するには、各ルールを構成して **Append** をクリックし、必要なルールをすべて追加したら **OK** をクリックします。
8. **OK** をクリックします。

vFirewall をインポートする

システム上の元の vFirewall を誤って削除した場合や、vFirewall をすばやく作成したい場合は、システムからエクスポートされた vFirewall 構成ファイルから vFirewall をインポートできます。vFirewall は、vFirewall 構成ファイルをエクスポートするクラウド管理プラットフォームまたは別のクラウド管理プラットフォームにインポートできます。vFirewall をインポートした後、そのルールを編集または削除できます。vFirewall の名前は、ローカルクラウド管理プラットフォーム内で一意である必要があります。

1. 上部のナビゲーション バーで、**Services** をクリックします。
2. 左側のナビゲーション ペインから、**Security > vFirewalls** を選択します。
3. **Import** をクリックし、vFirewall 設定を含む JSON ファイルを選択します。このような JSON ファイルを取得するには、vFirewall エクスポート機能を使用します。
4. vFirewall の名前と説明を入力します。
5. ファイアウォールの種類を選択します。
6. **Add Rule** をクリックします。
7. ルールを追加して **Import Virtual Firewall** ダイアログ ボックスに戻るには、ルールを構成して **OK** をクリックします。ルールを一括で追加するには、各ルールを構成して **Append** をクリックし、必要なルールをすべて追加したら **OK** をクリックします。
8. **OK** をクリックします。

vFirewall を編集する

1. 上部のナビゲーション バーで、**Services** をクリックします。
2. 左側のナビゲーション ペインから、**Security > vFirewalls** を選択します。
3. vFirewall の **Actions** 列で **Edit** をクリックします。
4. vFirewall の説明を入力します。
5. ファイアウォールのルールを管理します。
 - ルールを追加するには、**Add** をクリックします。

- ルールを編集するには、ルールの **Edit** をクリックします。
 - ルールを削除するには、ルールの **Delete** をクリックします。
6. **OK** をクリックします。

vFirewall を削除する

1. 上部のナビゲーション バーで、**Services** をクリックします。
2. 左側のナビゲーション ペインから、**Security > vFirewalls** を選択します。
3. vFirewall 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。

vFirewall を JSON ファイルにエクスポートする

vFirewall をバックアップ用または別のクラウド管理プラットフォームと同期するために、JSON ファイルにエクスポートできます。JSON ファイルは、それをエクスポートしたクラウド管理プラットフォームまたは別のクラウド管理プラットフォームにインポートできます。

1. 上部のナビゲーション バーで、**Services** をクリックします。
2. 左側のナビゲーション ペインから、**Security > vFirewalls** を選択します。
3. vFirewall の **Actions** 列で **Export** をクリックします。
4. エクスポート操作を確認するには、**OK** をクリックします。
5. JSON ファイルの保存パスを選択し、**Save** をクリックします。

VMにvFirewallを接続する

1. 上部のナビゲーション バーで、**Services** をクリックします。
2. 左側のナビゲーション ペインから、**Security > vFirewalls** を選択します。
3. vFirewall の **Actions** 列で **Attach VMs** をクリックします。
4. VM を選択し、**OK** をクリックします。

VMからvFirewallをデタッチする

1. 上部のナビゲーション バーで、**Services** をクリックします。

2. 左側のナビゲーション ペインから、**Security > vFirewalls** を選択します。
3. vFirewall の **Actions** 列で **Detach VMs** をクリックします。
4. VM を選択し、**OK** をクリックします。

vFirewall をコピーする

既存の vFirewall に基づいて vFirewall を作成するには、このタスクを実行します。新しい vFirewall は、管理プラットフォーム上で一意の名前を使用する必要があります。新しい vFirewall のルールを編集または削除できますが、新しいファイアウォールのファイアウォール タイプを編集することはできません。

1. 上部のナビゲーション バーで、**Services** をクリックします。
2. 左側のナビゲーション ペインから、**Security > vFirewalls** を選択します。
3. vFirewall の **Actions** 列で **Copy** をクリックします。
4. vFirewall の名前と説明を入力します。
5. **Add Rule** をクリックします。
6. ルールを追加して **Copy Virtual Firewall** ダイアログ ボックスに戻るには、ルールを構成して **OK** をクリックします。ルールを一括で追加するには、各ルールを構成して **Append** をクリックし、必要なルールをすべて追加したら **OK** をクリックします。
7. **OK** をクリックします。

パラメーター

vFirewall リスト

- **Firewall Type:** vFirewall のタイプを選択します。オプションには、**Allowlist** と **Denylist** があります。**Allowlist** ファイアウォールは、ルールに一致するトラフィックを許可し、他のすべてのトラフィックをドロップします。**Denylist** ファイアウォールは、ルールに一致するトラフィックをドロップし、他のすべてのトラフィックを許可します。
 - **Allowlist** vFirewall を構成する場合、VM からリモート サイトへのすべてのトラフィックを許可する 2 つのデフォルトの出カルールが存在します。VM で IPv6 が無効になっている場合は、IPv4 の出カルールのみが存在します。デフォルトでは、リモート サイトから VM へのすべてのトラフィックが拒否されます。リモート サイトから VM への特定のトラフィックを許可するには、必要に応じて入カルールを構成します。VM からリモート サイトへのトラフィックを制御するには、2 つのデフォルトの出カルールを削除し、必要に応じて出カルールを構成します。
 - **Denylist** vFirewall を構成する場合、デフォルトのルールは存在せず、すべてのパケットが許可されます。リモート サイトから VM への特定のトラフィックを拒否するには、必要に応じて入カルールを構成します。VM からリモート サイトへの特定のトラフィックを拒否するには、必要に応じて出カルールを構成します。

ルール

- **Direction:** 接続の方向を選択します。Ingress はリモート サイトから開始された接続を示します。Egress は VM によって開始された接続を示します。
- **IP Protocol:** vFirewall がトラフィック制御を実装するプロトコルを選択します。Any はすべてのプロトコルを表します。
- **Port/Type-Code:** TCP または UDP ポート番号を選択するか、ICMP タイプ コードを選択します。
- **Remote CIDR :** リモート サイトの IP アドレスを入力します。0.0.0.0 /0 は任意の IPv4 アドレスを表します。::/0 は任意の IPv6 アドレスを表します。

ルールパラメーター

- **Direction:** 接続の方向を選択します。Ingress はリモート サイトから開始された接続を示します。Egress は VM によって開始された接続を示します。
- **Port:** 開始ポート番号-終了ポート番号の形式で、セミコロンで区切られたポート番号またはポート範囲を入力します (例: 1;2-3;4)。同一のポート番号またはポート範囲を入力することはできません。また、ポート番号とポート範囲は昇順でなければなりません。システムは、ポート番号またはポート範囲ごとにルールを生成します。方向が入力の場合、ポート番号はリモート サイトがアクセスする VM ポートです。方向が出力の場合、ポート番号は VM がアクセスするリモート サイト ポートです。**Custom TCP Rule** または **Custom UDP Rule** を選択した場合、このパラメーターは必須です。
- **Type:** ICMP タイプを選択します。**Custom ICMP Rule** を選択した場合、このパラメーターは必須です。
- **Code:** ICMP コードを選択します。**Custom ICMP Rule** を選択した場合、このパラメーターは必須です。
- **IP Protocol:** vFirewall がトラフィック制御を実装するプロトコルを選択します。このパラメーターは、**その他のルール**を選択した場合に必須です。
- **IP Type:** IP パケット タイプを選択します。オプションには **IPv4** と **IPv6** があります。
- **Remote IP Address:** 23.2.2.2;5.5.5.5 や 20:ef::;21:ef::90/64 など、リモート サイトの IPv4 または IPv6 アドレスをセミコロンで区切って入力します。IP アドレスを入力しない場合、ルールは任意の IP アドレスに一致します。
- **Subnet Mask:** IPv4 リモート サイト アドレスのサブネット マスクを入力します。
- **Network Prefix:** IPv6 リモート サイト アドレスのネットワーク プレフィックスを入力します。

VLAN透過伝送ポリシーを管理する

VLAN 透過伝送ポリシーを設定して、vNIC が稼働中の VM および転送 VLAN によって受信および送信される VLAN タグ付きパケットを識別して処理できるようにします。VLAN 透過伝送ポリシーにより、1 つの vNIC を複数の VLAN に接続できます。

制限事項とガイドライン

NIC が VLAN 透過伝送で構成されている場合、ポート プロファイルの VLAN 設定は NIC では有効になりません。

VLAN透過伝送ポリシーを追加する

1. 上部のナビゲーション バーで、**Services** をクリックします。
2. 左側のナビゲーション ペインから、**Security > VLAN Transparent Transmission** を選択します。
3. **Add** をクリックします。
4. ポリシーの名前と説明を入力します。
5. 必要に応じてポリシーのルールを設定します。ルールを作成するには、**Add Rule** をクリックし、『**パラメーター**』の説明に従ってルールのパラメーターを設定して、**OK** をクリックします。
6. **OK** をクリックします。

VLAN透過伝送ポリシーに関する情報を表示する

1. 上部のナビゲーション バーで、**Services** をクリックします。
2. 左側のナビゲーション ペインから、**Security > VLAN Transparent Transmission** を選択します。
3. 対象ポリシーの **Actions** 列で **View** をクリックします。

VLAN透過伝送ポリシーを編集する

1. 上部のナビゲーション バーで、**Services** をクリックします。
2. 左側のナビゲーション ペインから、**Security > VLAN Transparent Transmission** を選択します。
3. 対象 VLAN 透過伝送ポリシーの **Actions** 列で **Edit** をクリックします。
4. 必要に応じてポリシーの説明を編集します。
5. ポリシー ルールを次のように編集します。
 - ルールを作成するには、**Add Rule** をクリックします。
 - ルールを編集するには、ルールの **Actions** 列で **Edit** をクリックします。
 - ルールを削除するには、ルールの **Actions** 列で **Delete** をクリックします。
6. **OK** をクリックします。

VLAN透過伝送ポリシーを削除する

1. 上部のナビゲーション バーで、**Services** をクリックします。
2. 左側のナビゲーション ペインから、**Security > VLAN Transparent Transmission** を選択します。
3. 対象ポリシーの **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

- **Service VLAN** : VM がトラフィックを送信する VLAN を指定します。
- **Forwarding VLAN** : トラフィックが他のネットワークに転送される VLAN を指定します。

レート制限ポリシーを管理する

レート制限ポリシーは、特定のトラフィック フローの平均帯域幅とバースト バッファを定義する一連のルールです。レート制限ポリシーは、VM とネットワーク サイト間のトラフィックの正確な帯域幅制御を提供します。

VM にレート制限ポリシーを適用するには、ポート プロファイルで指定する必要があります。ポート プロファイルの受信トラフィック制限と送信トラフィック制限と比較すると、レート制限ポリシーではよりきめ細かいトラフィック制御が提供されます。

制限事項とガイドライン

RBAC モードでは、セキュリティ管理者のみがレート制限ポリシーを管理できます。

レート制限ポリシーを追加する

1. 上部のナビゲーション バーで、**Services** をクリックします。
2. 左側のナビゲーション ペインから、**Security > Rate Limit Policies** を選択します。
3. **Add** をクリックします。
4. ポリシー名、説明、所有者を指定します。
5. ポリシーを時間ベースのポリシーとして構成するかどうかを構成します。構成する場合は、ポリシーが有効になる時間を指定します。
6. ルールを追加するには、**Add Rule** をクリックし、ルールを設定して、**Finish** をクリックします。
7. **OK** をクリックします。

レート制限ポリシーを編集する

1. 左側のナビゲーション ペインから、**Security > Rate Limit Policies** を選択します。
2. レート制限ポリシーの **Actions** 列で **Edit** をクリックします。
3. ポリシーの説明を編集します。
4. ポリシーのルールを編集します。
 - ルールを追加するには、**Add Rule** をクリックします。
 - ルールを編集するには、**Action** 列の **Edit** をクリックします。
 - ルールを削除するには、**Action** 列の **Delete** をクリックします。
 - ルールの優先順位を設定するには、**Edit Priority** をクリックします。
5. **OK** をクリックします。

プライベート レート制限ポリシーをパブリック レート制限ポリシーに変換する

1. 上部のナビゲーション バーで、**Services** をクリックします。
2. 左側のナビゲーション ペインから、**Security > Rate Limit Policies** を選択します。
3. プライベートレート制限ポリシーの **Actions** 列で、**More** をクリックし、**Convert to Public Policy** 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。

レート制限ポリシーをコピーする

1. 上部のナビゲーション バーで、**Services** をクリックします。
2. 左側のナビゲーション ペインから、**Security > Rate Limit Policies** を選択します。
3. レート制限ポリシーの **Actions** 列で、**More** をクリックし、**Copy** を選択します。
4. 開いたダイアログボックスでパラメーターを設定し、**OK** をクリックします。

レート制限ポリシーを削除する

1. 上部のナビゲーション バーで、**Services** をクリックします。

2. 左側のナビゲーション ペインから、**Security > Rate Limit Policies** を選択します。
3. レート制限ポリシーの **Actions** 列で、**More** をクリックし、**Delete** 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。

フィルターレート制限ポリシー

1. 上部のナビゲーション バーで、サービス **Services** をクリックします。
2. 左側のナビゲーション ペインから、**Security > Rate Limit Policies** を選択します。
3. レート制限ポリシーを所有者別にフィルターリングするには、**Used By** フィールドから **Public**, **Private**, または **All** を選択します。

パラメーター

- **Used By:** ポリシー所有者を選択します。オプションには、**Public** と **Private** があります。パブリック レート制限ポリシーはすべてのユーザーが表示および使用できますが、プライベート レート制限ポリシーは、ポリシー作成者と同じユーザー グループのユーザーのみが表示および使用できます。
- **Rate Limit Method:** レート制限方法を選択します。オプションには、**IP**、**ARP**、および**ブロードキャスト**があります。
- **Remote CIDR :** CIDR 形式でネットワーク セグメントを入力します。0.0.0.0 /0 は任意の IPv4 アドレスを表します。::/0 は任意の IPv6 アドレスを表します。任意の IP アドレスを指定するには、このフィールドを空のままにします。このパラメーターは、レート制限方法が **IP** の場合にのみ必要です。
- **Direction:** トラフィックの方向を選択します:
 - **Upstream-** VM からリモート サイトへのトラフィック。
 - **Downstream-** リモート サイトから VM へのトラフィック。
- **Average Bandwidth:** 平均帯域幅を Kbps または Mbps で入力します。
- **Burst Buffer:** バースト バッファ サイズを KByte または MByte 単位で入力します。
- **Edit Rule Priorities:** ルールの優先順位を設定します。リモート IP アドレスが同じ方向の 2 つのルールに一致し、高優先順位ルールのネットワーク セグメントに低優先順位ルールのネットワーク セグメントが含まれている場合、システムは高優先順位ルールを使用します。たとえば、ルール A とルール B がアップストリーム方向に適用されます。ルール A にはネットワーク 192.168.100.0/24 が含まれ、ルール B にはネットワーク 192.168.100.40/32 が含まれます。ルール A の優先順位がルール B の優先順位よりも高い場合、ルール A が有効になります。

ウイルス対策サービスを設定する

CVM 内のホストを潜在的な攻撃から保護するには、このタスクを実行します。

ホストのウイルス対策パッケージを構成、アップロード、およびインストールできます。

AsialInfo のウイルス対策ソフトウェアを使用する場合は、次のガイドラインに従ってください:

- アップロードするウイルス対策パッケージは、.tar.gz または zip 形式である必要があります。パッケージが正常にアップロードされたら、**Check** をクリックしてパッケージを手動でインストールできます。さらに、AsialInfo DSM を CAS に組み込むこともできます。詳細については、『AsialInfo を構成する』を参照してください。

制限事項とガイドライン

IRBAC モードでは、セキュリティ管理者のみがウイルス対策サービスを設定できます。システム管理者はウイルス対策設定を表示できますが、ウイルス対策パッケージのアップロード、インストール状態の確認、インストール、アンインストールは実行できません。

アップロード処理中はウィンドウやブラウザを閉じないでください。

ウイルス対策ソフトウェアの製造元として QI-ANXIN を選択した場合は、QI-ANXIN Cloud Security サービスで使用されるポートを許可するようにポート ポリシーを構成します。

QI-ANXIN Legendsec 統合サーバー セキュリティ管理システムは、IPv4 Syslog サーバーのみをサポートします。

手順

1. 上部のナビゲーション バーで、**Services** をクリックします。
2. 左側のナビゲーションペインから、**Security > Anti-Virus** を選択します。
3. ウイルス対策ソフトウェアの製造元として AsialInfo を選択した場合は、次のタスクを実行します:
 - a. ホストの種類を選択し、ウイルス対策パッケージを保存するディレクトリを入力します。
 - b. 点線の領域の任意の領域をクリックして、ウイルス対策パッケージを選択します。
 - c. ウイルス対策パッケージをアップロードするには、**Start** をクリックします。

ウイルス対策パッケージが正常にアップロードされると、システムは CVK ホストにウイルス対策パッケージを自動的にインストールします。

- d. **Check** をクリックして、各ホスト上のウイルス対策パッケージのインストール状態を確認します。
 - e. ホストのウイルス対策パッケージを手動でインストールするには、ホストの **Actions** 列で **Install** をクリックするか、**OK** ボタンの横にある **Install** をクリックします。
4. ウイルス対策ソフトウェアの製造元として QI-ANXIN を選択した場合は、次のタスクを実行します:
 - a. 『パラメーター』の説明に従って、基本パラメーターと Syslog アラーム設定を構成します。

- b. OK をクリックします。

パラメーター

共通パラメーター

Vendor: ウイルス対策ソフトウェアの製造元を選択します。現在のソフトウェア バージョンは AsialInfo のみをサポートしています。

AsialInfoパラメーター

- **CVK Type:** CVK ホスト タイプを選択します。ウイルス対策ベンダーが AsialInfo の場合、使用可能な CVK タイプには、ARM、ARM_E0730、ARM_E0760、x86、x86_CentOS_E0730、x86_Ubuntu_E0730、x86_E0760 が含まれます。
- **Directory:** ウイルス対策パッケージを保存するディレクトリを入力します。
- **Current Package:** 最後にアップロードされたウイルス対策パッケージの名前。
- **Name:** ホストの名前。
- **State:** ホストの状態。
- **CPU Architecture:** x86 と ARM からオプションを選択します。
- **OS:** オペレーティング システムの種類を選択します。
- **IP:** ホストの IP アドレス。
- **Package State:** ホストにウイルス対策パッケージがインストールされているかどうか。
- **Progress:** 動作状態を確認します。
- **Action:** オペレーターがホスト上で実行できるアクション。
 - ホストのウイルス対策パッチをインストールするには、**Install** をクリックします。
 - ホストのウイルス対策パッチをアンインストールするには、**Uninstall** をクリックします。

QI-ANXINパラメーター

QI-ANXIN基本パラメーター

- **Protocol:** QI-ANXIN Legendsec 統合サーバー セキュリティ管理システムにアクセスするために使用されるプロトコル。HTTPS のみが使用可能です。

- **Port Number:** QI-ANXIN Legendsec 統合サーバー セキュリティ管理システムのポート番号を入力します。
- **IP Address:** QI-ANXIN Legendsec 統合サーバー セキュリティ管理システムの IP アドレスを入力します。
- **Username:** QI-ANXIN Legendsec 統合サーバー セキュリティ管理システムにアクセスするためのユーザー名を入力します。
- **Password:** QI-ANXIN Legendsec 統合サーバー セキュリティ管理システムにアクセスするためのパスワードを入力します。

Syslogアラーム設定

- **Protocol:** Syslog データを送信するために使用されるプロトコル。UDP のみが使用可能です。
- **Server Port:** Syslog サーバーのポート番号を入力します。

AsialInfo を設定する

AsialInfo が提供するウイルス対策サービスを使用する場合、AsialInfo DSM を CAS に組み込んで、DSM、VM ウイルス対策、およびウイルス対策ポリシーを管理できます。

制限事項とガイドライン

- CAS に追加できる AsialInfo セキュリティ サーバーは 1 つだけです。
- CAS 上の DSM のセキュリティ ポリシーの割り当てと再利用のみが可能です。CAS 上の DSM のセキュリティ ポリシーを追加、削除、または編集することはできません。


AsialInfoセキュリティサーバーを追加する

1. 上部のナビゲーション バーで、**Services** をクリックします。
2. 左側のナビゲーション ペインから、**Security > Anti-Virus** を選択します。
3. **Security > Anti-Virus** タブをクリックします。
4. **Add** 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。

AsialInfo セキュリティ サーバーを編集する

1. 上部のナビゲーション バーで、**Services** をクリックします。
2. 左側のナビゲーション ペインから、**Security > Anti-Virus** を選択します。
3. **AsialInfo Security Settings** タブをクリックします。
4. AsialInfo セキュリティ サーバーの **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。

AsialInfo 証明書をアップロードする

1. 上部のナビゲーション バーで、**Services** をクリックします。
2. 左側のナビゲーション ペインから、**Security > Anti-Virus** を選択します。
3. **AsialInfo Security Settings** タブをクリックします。
4. AsialInfo セキュリティ サーバーの **Upload** をクリックします。
5.  アイコンをクリックし、AsialInfo 証明書を選択します。
6. **OK** をクリックします。

AsialInfo セキュリティ サーバーへの接続をテストする

1. 上部のナビゲーション バーで、**Services** をクリックします。
 2. 左側のナビゲーション ペインから、**Security > Anti-Virus** を選択します。
 3. **AsialInfo Security Settings** タブをクリックします。
 4. AsialInfo セキュリティ サーバーの **Test Connectivity** をクリックします。
- システムはテスト結果を表示します。

AsialInfo セキュリティ サーバーを削除する

1. 上部のナビゲーション バーで、**Services** をクリックします。

2. 左側のナビゲーション ペインから、**Security > Anti-Virus** を選択します。
3. **AsialInfo Security Settings** タブをクリックします。
4. AsialInfo セキュリティ サーバーの **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。

セキュリティポリシーを表示し、セキュリティポリシーを割り当てる

1. 上部のナビゲーション バーで、**Services** をクリックします。
2. 左側のナビゲーション ペインから、**Security > Anti-Virus** を選択します。
3. **AsialInfo Security Settings** タブをクリックします。
4. **Security Policies** タブをクリックします。
5. セキュリティ ポリシーの **Allocate** をクリックします。
6. VM ウイルス対策が有効になっている VM を選択します。

VMからセキュリティポリシーを取り戻す

1. 上部のナビゲーション バーで、**Services** をクリックします。
2. 左側のナビゲーション ペインから、**Security > Anti-Virus** を選択します。
3. **AsialInfo Security Settings** タブをクリックします。
4. **VM** タブをクリックします。
セキュリティ ポリシーがすでに割り当てられている VM が表示されます。
5. VM の **Cancel** 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。

パラメーター

- **Server Name:** AsialInfo サーバーの名前を入力します。
- **Description:** 説明を入力します。
- **IP Address:** AsialInfo サーバーの IP アドレスを入力します。
- **Port:** AsialInfo サーバーのポート番号を入力します。

- **Username:** DSM にログインするためのユーザー名を入力します。
- **Password:** DSM にログインするためのパスワードを入力します。

セキュリティサービスのワークフローを管理する

ARM ホストはセキュリティ サービス ワークフローをサポートしていません。

セキュリティ サービス ワークフローは、セキュリティ ゾーン内のホストに対して次の操作を実行するために使用されます。

- VM の分類レベルを編集します。
- VM ディスクを追加します。
- VM ディスクを削除します。
- 異常なホストを削除します。

ワークフローを表示、処理、削除できます。

前提条件

セキュリティ サービス ワークフローは、セキュア モードが有効になっている場合にのみ使用できます。セキュア モードの詳細については、『システム パラメーターの構成』を参照してください。

制限事項とガイドライン

RBAC モードでは、セキュリティ管理者のみがセキュリティ サービス ワークフローを管理できます。

保留中のワークフローのみを削除できます。

セキュリティサービスのワークフローの詳細を表示する

1. 上部のナビゲーション バーで、**Services** をクリックします。
2. 左側のナビゲーション ペインから、**Security > Security Service Workflows** を選択します。
3. セキュリティ サービス ワークフローの **Actions** 列で **View** をクリックします。

セキュリティサービスのワークフローを処理する

1. 上部のナビゲーション バーで、**Services** をクリックします。
2. 左側のナビゲーション ペインから、**Security > Security Service Workflows** を選択します。
3. セキュリティ サービス ワークフローの **Actions** 列で **Process** をクリックします。

セキュリティ サービス ワークフローを削除する

1. 上部のナビゲーション バーで、**Services** をクリックします。
2. 左側のナビゲーション ペインから、**Security > Security Service Workflows** を選択します。
3. セキュリティ サービス ワークフローの **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

- **Status:** ワークフローのステータス。オプションには、**Pending, Approved, Rejected** があります。
- **Applicant:** ワークフローを送信した申請者。
- **Submitted At:** ワークフローが送信された時刻。
- **Approver:** ワークフローを処理した承認者。
- **Approved At:** 承認者がワークフローを処理した時刻。
- **Result:** ワークフローの実装結果。結果が失敗の場合、その理由が記録されます。
- **Comment:** 承認者からのコメント。

暗号化アプリケーションのセキュリティ評価を管理する

暗号化アプリケーション セキュリティ評価 (CASE) は、機密データを保護し、アプリケーションのセキュリティとプライバシーを確保するテクノロジーです。CASE は、ネットワークとシステム全体のコンプライアンス、正確性、有効性を評価します。

暗号化モジュールを起動すると、システムはオペレーターの権限の整合性を検証し、その結果をオペレーターリストに表示します。さらに、オペレーターの各アクションが検証され、操作ログと監査ログに記録されます。これにより、オペレーターの情報へのアクセスと操作ログの整合性が確保されます。暗号化モジュールは、システム オペレーターの権限の整合性の暗号化を 10 分ごとに補完し、システムの操作ログの整合性の暗号化を毎日午前 2 時に補完します。

制限事項とガイドライン

- RBAC モードでは、セキュリティ管理者のみが CASE を管理できます。
- CASE を有効にしてバージョンをアップグレードする前に、システム内のすべてのオペレーターの権限の整合性が正しいことを確認してください。アップグレードの前後でオペレーターの権限の整合性が異常な場合、オペレーターはシステムにログインできません。
- ステートフル フェールオーバー システムを設定する前に、プライマリ システムもバックアップ システムも CASE で構成されていないこと、およびプライマリ システムとバックアップ システムの同じディレクトリに同じコンポーネント名を持つ同じコンポーネントが含まれていることを確認します。
- 署名検証プラットフォーム設定を構成するときは、サードパーティ プラットフォームによって提供されるポートを使用します。
- 暗号化モジュールと署名検証プラットフォームは IPv6 アドレスをサポートしていません。
- ログインに 2 要素認証が有効になっている場合は、作成した UKEY の CN フィールドが対応するオペレーターの名前に設定され、簡単にログインして使用できるようになっていることを確認してください。
- システム エラーを回避するために、CASE を構成して暗号化モジュールを起動した後は、プラットフォーム タイプを **None** に変更しないでください。
- 接続障害を回避するには、暗号化モジュールのポート番号を変更した後、**service tomcat8 restart** または **systemctl restart tomcat8.service** コマンドを使用して Tomcat サービスを再起動します。

暗号化モジュールの設定を構成する

暗号化モジュールに接続することで、システムは暗号化モジュールが提供する暗号化アルゴリズムと機能呼び出し、オペレーター パスワード、電話番号、電子メール アドレス、ホスト パスワードなどの重要なデータを保護できます。これにより、データの安全な送信と保存が保証され、システム全体のセキュリティとプライバシーが強化されます。

1. 上部のナビゲーション バーで、**Services** をクリックします。
2. 左側のナビゲーション ペインから、**Security > CASE** を選択します。
3. **Encryption Module Settings** タブで、**Edit** をクリックします。
4. パラメーターを編集し、**OK** をクリックします。

暗号化モジュールへの接続をテストする

このタスクを実行して、システムと暗号化モジュール間の通信が正常であるかどうかを確認し、後続の操作で適切に使用されるようにします。

1. 上部のナビゲーション バーで、**Services** をクリックします。

2. 左側のナビゲーション ペインから、**Security > CASE** を選択します。
3. **Encryption Module Settings** タブで、**Edit** をクリックします。
4. **Encryption Module IP** フィールドの横にある **Test Connectivity** をクリックします。

暗号化を有効にする

暗号化モジュール設定を構成した後にデータ暗号化を実装するには、このタスクを実行します。

1. 上部のナビゲーション バーで、**Services** をクリックします。
2. 左側のナビゲーション ペインから、**Encryption Module Settings** タブで、**Edit** をクリックします。
3. **Enable Encryption** をクリックします。

署名検証プラットフォームの設定を構成する

システムで 2 要素認証が有効になると、署名検証プラットフォームでオペレーターの ID を検証できます。CASE が設定されていない場合は、2 要素認証に Fisec 認証を選択することはできません。

1. 上部のナビゲーション バーで、**Services** をクリックします。
2. 左側のナビゲーション ペインから、**Security > CASE** を選択します。
3. **Signature Verification Platform Settings** タブをクリックし、**Edit** をクリックします。
4. パラメーターを編集し、**OK** をクリックします。

署名検証プラットフォームへの接続をテストする

システムと署名検証プラットフォーム間の通信が正常かどうかを確認するには、このタスクを実行します。

1. 上部のナビゲーション バーで、**Services** をクリックします。
2. 左側のナビゲーション ペインから、**Security > CASE** を選択します。
3. **Signature Verification Platform Settings** タブをクリックし、**Edit** をクリックします。
4. **Signature Verification Platform IP** フィールドの横にある **Test Connectivity** をクリックします。

パラメーター

- 暗号化モジュールの設定:
 - **Encryption Module State:** 暗号化モジュールの現在の状態。

- **Platform Type:** 暗号化モジュールのタイプを選択します。**Fisec** のみがサポートされています。
- **Encryption Module IP :** 暗号化モジュールの IP アドレスを入力します。
- **Encryption Key:** 暗号化モジュールで設定されている暗号化モジュールのキーを入力します。
- **Component Path:** システム内で CASE コンポーネントが保存されているパスを入力します。
- 署名検証プラットフォームの設定:
 - **Signature Verification Platform:** 署名検証プラットフォームを選択します。**Fisec** のみがサポートされています。
 - **Signature Verification Platform IP :** 署名検証プラットフォームの IP アドレスを入力します。
 - **Signature Verification Platform Port::** 署名検証プラットフォームのポート番号を入力します。
 - **Component Path:** システム内で CASE コンポーネントが保存されているパスを入力します。

ポートポリシーの管理

ポート ポリシーを使用すると、ホスト上の特定のポートのみを開くことでアクセスを制御できます。システムには次のデフォルトのポート ポリシーが用意されていますが、これらは編集または削除できません。

- **Host Node Default Policy-** システム内のすべてのホストに関連付けられます。関連付けられているホストを追加または削除することはできません。
- **Management Node Default Policy-** システム内の管理ノードに関連付けられます。関連付けられているホストを追加または削除することはできません。

制限事項とガイドライン

- 現在の管理プラットフォームが展開されているバックアップ ホストに障害が発生し、別のホストを使用してバックアップ ホストを復元する場合、システムはインストール後にデフォルトのルールを保持します。システムでポート強化が有効になっていて、バックアップ ホストにデフォルト以外のポリシーが関連付けられているか、ポート強化が無効になっている場合、管理プラットフォームから構成されたポート ポリシーは、ホストの CLI から構成されたポート ポリシーと一致しません。管理プラットフォームでポート強化を再設定する必要があります。
- ポート強化は IPv4 アドレスに対してのみ有効です。
- 現在の管理ノードの IP アドレスが変更された場合、Web インターフェイスで設定されたポート ポリシーは、ノードの CLI で設定されたポリシーと一致しくなくなります。管理ノードを再起動するか、ノードの CLI から Tomcat サービスを再起動する必要があります。

ポートポリシーを追加する

1. 上部のナビゲーション バーで、**Services** をクリックします。
2. 左側のナビゲーション ペインから、**Security > Port Policies** 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。

ポートポリシーを編集する

1. 上部のナビゲーション バーで、**Services** をクリックします。
2. 左側のナビゲーション ペインから、**Security > Port Policies** を選択します。
3. ポート ポリシーの **Actions** 列で **Edit** をクリックします。
4. 必要に応じてパラメーターを編集します。
5. **OK** をクリックします。

ポートポリシーを削除する

1. 上部のナビゲーション バーで、**Services** をクリックします。
2. 左側のナビゲーション ペインから、**Security > Port Policies** を選択します。
3. ポート ポリシーの **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。

ポートポリシーを一括削除する

デフォルトのサービス ノード ポリシーまたは管理ノード ポリシーは削除できません。

1. 上部のナビゲーション バーで、**Services** をクリックします。
2. 左側のナビゲーション ペインから、**Security > Port Policies** を選択します。
3. 対象のポート ポリシーを選択し、ポート ポリシー リストの上部にある **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。

ポート強化を有効にする

1. 上部のナビゲーション バーで、**Services** をクリックします。
2. 左側のナビゲーション ペインから、**Security > Port Policies** を選択します。
3. **Port Hardening** の横にある切り替えボタンをクリックします。
4. 開いたダイアログボックスで、**OK** をクリックします。

ポート強化を無効にする

1. 上部のナビゲーション バーで、**Services** をクリックします。
2. 左側のナビゲーション ペインから、**Security > Port Policies** を選択します。
3. **Port Hardening** の横にある切り替えボタンをクリックします。
4. 開いたダイアログボックスで、**OK** をクリックします。

ポートポリシーをホストに関連付ける

ポート ポリシーをホストに展開し、そのホスト上の指定されたポートを有効にするには、このタスクを実行します。

1. 上部のナビゲーション バーで、**Services** をクリックします。
2. 左側のナビゲーション ペインから、**Security > Port Policies** を選択します。
3. ポート ポリシーの **Actions** 列で **Associate Host** をクリックします。
4. ホストを選択し、**OK** をクリックします。

ポートポリシーにホストを追加する

ポート ポリシーにホストを追加すると、そのホストにポート ポリシーが適用され、指定したポートが開きます。ポート ポリシーは、すべてのホスト、すべての管理ノード、すべてのサービス ノード、または選択したホストに関連付けることができます。

1. 上部のナビゲーション バーで、**Services** をクリックします。
2. 左側のナビゲーション ペインから、**Security > Port Policies** を選択します。
3. ポート ポリシーを選択し、**Associated Hosts** フィールドの横にある **Add** をクリックします。
4. ホストを選択し、**OK** をクリックします。

ホストとポートポリシー間の関連付けを削除します

ホストとそれに関連付けられたデフォルトのサービス ノード ポリシーまたは管理ノード ポリシー間の関連付けを削除することはできません。

1. 上部のナビゲーション バーで、**Services** をクリックします。
2. 左側のナビゲーション ペインから、**Security > Port Policies** を選択します。
3. ポート ポリシーを選択し、**Associated Hosts** フィールドの横にある **Remove** をクリックしてから、関連ホストリスト内のホストの **Actions** 列で **Remove** 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。

ホストとポートポリシー間の関連付けを一括削除する

ポート ポリシーが複数のホストに関連付けられている場合は、このタスクを実行して、そのポート ポリシーとターゲット ホスト間の関連付けを一括削除できます。ホストと、それに関連付けられているデフォルトのサービス ノード ポリシーまたは管理ノード ポリシー間の関連付けを削除することはできません。

1. 上部のナビゲーション バーで、**Services** をクリックします。
2. 左側のナビゲーション ペインから、**Security > Port Policies** を選択します。
3. ターゲット ポート ポリシーを選択し、関連付けられたホスト リストでターゲット ホストを選択して、**Associated Hosts** フィールドの横にある **Remove** 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。

ポートポリシーを関連ホストに同期する

ポート ポリシーが変更された場合は、このタスクを実行して、そのポリシーをターゲットの関連ホストに同期できます。

1. 上部のナビゲーション バーで、**Services** をクリックします。
2. 左側のナビゲーション ペインから、**Security > Port Policies** を選択します。
3. ポート ポリシーを選択し、関連付けられたホスト リストでターゲット ホストを選択して、**Associated Hosts** フィールドの横にある **Sync** をクリックします。

ポートポリシーに関連付けられたホストを修復する

システムがポート ポリシーをホストに展開できなかった場合に、システムがポート ポリシーをホストに再展開するには、このタスクを実行します。

1. 上部のナビゲーション バーで、**Services** をクリックします。
2. 左側のナビゲーション ペインから、**Security > Port Policies** を選択します。
3. ポート ポリシー リストでポート ポリシーを選択し、関連付けられているホスト リストでホストを選択して、**Associated Hosts** フィールドの横にある **Repair** をクリックします。
4. システムがホストの修復を完了するまで待ちます。システムは、ターゲット ホストが正常に修復されたことを示すメッセージを表示します。

パラメーター

- **Name:** ポート ポリシー名を指定します。値には、中国語の文字、英字、数字、ハイフン (-)、下線 (_)、スペース、ドット (.) のみを含めることができます。スペースのみを含めることはできません。
- **Port:** カンマ (,) で区切られたポート、またはハイフン (-) で区切られたポート範囲を指定します。

QAXクラウドセキュリティサービスを構成する

QI-ANXIN Legendsec 統合サーバー セキュリティ管理システムは、政府および企業ユーザー向けの仮想、クラウド、データ センター環境におけるサーバー、VM、クラウド ホスト、コンテナなどの IT インフラストラクチャを保護することを目的としています。このシステムは、マイクロセグメンテーション、マルチエンジン協調ファイル保護、ホスト ネットワーク侵入防止により、ワークロード内の悪意のあるスキャン、脆弱性攻撃、ウイルス感染、水平伝播を排除できます。セキュリティ状況認識および視覚化機能と組み合わせることで、このシステムはセキュリティ リスクの統合分析と表示を実行できます。

QI-ANXIN クラウド セキュリティ サービスを使用するには、まず次のタスクを実行します。

1. QI-ANXIN Legendsec 統合サーバー セキュリティ管理システムにアクセスして、アクセス制御を有効にし、Syslog 設定を構成します。
2. CAS にログインし、**Services > Security > Anti-Virus** ページに移動して、QI-ANXIN クラウド セキュリティ サービスの基本パラメーターと Syslog アラーム設定を構成します。

ユーザー名とパスワードを入力せずに、QAX コンソールから QI-ANXIN Legendsec 統合サーバー セキュリティ管理システムにアクセスできます。

制限事項とガイドライン

QI-ANXIN Legendsec 統合サーバー セキュリティ管理システムにアクセスするには、QI-ANXIN クラウド セキュリティ サービスで使用するポートを許可するようにポート ポリシーを構成する必要があります。

QAXシステムに接続する

1. 上部のナビゲーション バーで、**Services** をクリックします。
2. 左側のナビゲーション ペインから、**Security > QAX Cloud Security** を選択します。
3. **Settings** をクリックします。
4. 『ウイルス対策サービスを構成する』の説明に従ってパラメーターを構成します。
5. **OK** をクリックします。

QAXコンソールにアクセスする

1. 上部のナビゲーション バーで、**Services** をクリックします。
2. 左側のナビゲーション ペインから、**Security > QAX Cloud Security** を選択します。
3. **Console** をクリックします。

バックアップセンターを管理する

VM および管理プラットフォームのバックアップ ファイル、バックアップ ポリシー、およびバックアップ パラメーターを管理するには、このタスクを実行します。

機能

- VM バックアップの管理
- CVM バックアップを構成する

VMバックアップの管理

P バックアップ ファイル、バックアップ ポリシー、およびバックアップ パラメーターを管理するには、このタスクを実行します。

機能

- バックアップファイルの管理
- バックアップポリシーの管理
- バックアッププールの管理
- バックアップパラメーターを構成する

バックアップファイルの管理

システムは、VM バックアップを完了するたびに、VM バックアップ ファイルのエイリアス、ホスト名、IP、状態、バックアップ数、最新のバックアップ場所、最新のバックアップ時刻、およびサイズを表示します。実行場所、バックアップ場所、表示場所、またはバックアップ ポリシーによって VM バックアップ情報を表示できます。さらに、管理されていない VM および VMware VM のバックアップ情報を表示できます。

バックアップ履歴を表示する

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

Backup History タブが表示されます。

3. **By Running Location, By Backup Location, By View Location** ,または **By Backup Policy** を選択します。または、VM エイリアスを入力し、リストから **Alias** または **IP** を選択して VM をフィルターします。
4. バックアップ履歴情報を更新するには、 をクリックします。

VM のバックアップ ファイルを一括削除する

VM に複数のバックアップ ファイルがある場合は、このタスクを実行してバックアップ ファイルを一括で削除できます。

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

Backup History タブが表示されます。

3. 1 つまたは複数のバックアップ ファイルを選択します。
4. バックアップ ファイル リストの上部にある **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。

複数の VM のバックアップ ファイルを一括削除する

複数の VM の増分バックアップ ファイルを一括で削除するには、このタスクを実行します。

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

Backup History タブが表示されます。

3. ページの右上隅にある **Bulk Delete Backup Files** をクリックします。
4. 削除するバックアップ ファイルを選択します。
5. **Delete** 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。必要に応じて **Force Delete** をクリックしてバックアップ ファイルを強制的に削除します。

Force Delete を選択すると、バックアップ ファイルのデータベース情報がクリアされます。バックアップ ファイルがリモート サーバーに保存されていて、接続エラーが発生した場合、この操作ではデータベース情報のみが削除されます。接続が回復しても、バックアップ ファイルを使用して VM を復元することはできません。

パラメーター

- **Alias:** VM のエイリアス。
- **Host Name:** VM が存在するホストの名前。
- **IP:** VM の IP アドレス。
- **State:** VM の実行状態。
- **Backup Count:** VM のバックアップ ファイルの数。
- **Most Recent Backup Location:** 最新のバックアップのバックアップ場所。
- **Most Recent Backup Time:** バックアップ ファイルが最後に作成された時刻。
- **Size:** バックアップ ファイルのサイズ。

バックアップポリシーの管理

VM バックアップは安定した災害復旧機能です。VM イメージ ファイルが破損または削除された場合でも、VM のバックアップ ファイルは失われません。

サーバーまたはストレージ デバイスの障害、ソフトウェアのバグやウイルス、または誤操作により VM データが失われた場合は、バックアップ ファイルを使用して VM を復元できます。

バックアップ時間に応じて、VM バックアップには次の種類が含まれます。

- **Backup now-** リアルタイムで手動でデータをバックアップできます。『VM をバックアップする』を参照してください。
- **Scheduled backup-** バックアップ ポリシーを通じてデータをバックアップします。バックアップ ポリシーが VM に適用されると、システムはスケジュールに従って VM または VM ディスクをバックアップし、バックアップ ファイルを生成します。

制限事項とガイドライン

- システムは、VM の権限情報、起動優先順位、自動移行設定、GPU 設定をバックアップしません。
- ブロック デバイスをディスクとして使用する VM や、raw ディスクを使用する VM の場合、オンラインバックアップ、増分バックアップ、差分バックアップはサポートされません。
- スナップショットは、変更ブロック追跡 (CBT) バックアップをサポートしていません。CBT バックアップファイルを使用してスナップショットを含む VM を復元すると、VM のスナップショットは失われます。
- バックアップの失敗を回避するには、CBT バックアップ中に VM の実行状態を変更しないでください。

バックアップポリシーを追加する

1. 上部のナビゲーション バーで、**Services** をクリックします。
2. 左側のナビゲーション ペインから、**Backup Center > VM Backup** を選択します。
3. **Backup Policies** タブをクリックします。
4. **Add** 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。

バックアップポリシーを編集する

1. 上部のナビゲーション バーで、**Services** をクリックします。
2. 左側のナビゲーション ペインから、**Backup Center > VM Backup** を選択します。
3. **Backup Policies** タブをクリックします。
4. バックアップ ポリシーの **Actions** 列で**編集** 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。

バックアップポリシーを削除する

1. 上部のナビゲーション バーで、**Services** をクリックします。
2. 左側のナビゲーション ペインから、**Backup Center > VM Backup** を選択します。
3. **Backup Policies** タブをクリックします。
4. バックアップ ポリシーの **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。

バックアップポリシーを有効にする

1. 上部のナビゲーション バーで、**Services** をクリックします。
2. 左側のナビゲーション ペインから、**Backup Center > VM Backup** を選択します。
3. **Backup Policies** タブをクリックします。
4. バックアップ ポリシーの **Actions** 列で **Start** 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。

バックアップポリシーを無効にする

1. 上部のナビゲーション バーで、**Services** をクリックします。
2. 左側のナビゲーション ペインから、**Backup Center > VM Backup** を選択します。
3. **Backup Policies** タブをクリックします。
4. バックアップ ポリシーの **Actions** 列で **Disable** 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。

バックアップ ポリシーから VM を削除する

1. 上部のナビゲーション バーで、**Services** をクリックします。
2. 左側のナビゲーション ペインから、**Backup Center > VM Backup** を選択します。
3. **Backup Policies** タブをクリックします。
4. **VMs Using the Backup Policy** 領域の VM 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。

バックアップポリシーからディスクを削除する

1. 上部のナビゲーション バーで、**Services** をクリックします。
2. 左側のナビゲーション ペインから、**Backup Center > VM Backup** を選択します。
3. **Backup Policies** タブをクリックします。
4. バックアップ ポリシーをクリックします。
5. **Disks Using the Backup Policy** 領域で、ディスクの **Actions** 列の **Delete** 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。

パラメーター

基本情報

- **Name:** バックアップ ポリシーの名前を指定します。
- **Description:** バックアップ ポリシーの説明を指定します。
- **Disk I/O Threshold:** バックアップ中の VM ディスク I/O の最大値を指定します。バックアップ開始時刻に達すると、VM の I/O スループットがこのしきい値以下に低下した場合にのみ、このバックアップ ポリシーを使用する VM のバックアップが開始されます。VM の I/O スループットがこのしきい値を超えると、次のバックアップ時刻が開始されるまで VM はバックアップされません。このパラメーターは、バックアップ対象の VM が実行状態にある場合にのみ有効になります。
- **Backup Pools:** バックアップ ファイルを保存する場所を指定します。
- **Data:** バックアップの種類を選択します。
 - **Full VM** - VM のディスク データと構成ファイルをバックアップします。バックアップ ファイルを使用して VM 全体を復元できます。
 - **Disk Level** - VM の 1 つまたは複数のディスクのみをバックアップします。構成ファイルはバックアップされません。バックアップ ファイルを使用してディスクのみを復元できます。
- **CBT Backup:** VM の CBT バックアップを有効にするかどうかを選択します。CBT は、最後のバックアップ以降に変更されたデータのみをバックアップするため、時間とシステム リソースを節約できます。CBT バックアップを使用するには、VM が CAS E0525 以降で作成され、インテリジェント (QCOW2) ディスクとシングルレベルのイメージ ファイルを使用していることを確認します。
- **Take Effect Now:** 作成後にバックアップ ポリシーを有効にするかどうかを設定します。

Full Backup

- **Frequency:** 完全バックアップの実行頻度を選択します。
- **Started At:** 実行開始時刻を選択します。

- **To: 実行終了時刻を選択します。** 開始時刻が終了時刻より遅い場合、バックアップは翌日に終了します。終了時刻までに完全バックアップが完了しない場合、システムは VM バックアップの終了後にこのバックアップ タスクを停止し、次のバックアップの開始を待機します。
- **Backups to Save:** ローカルまたはリモート サーバーに保持するバックアップ ファイルの数を指定します。このフィールドを空のままにすると、すべてのバックアップ ファイルが保持されます。
- **Backup Type:** 増分バックアップまたは差分バックアップを有効にします。
 - **Incremental** - 完全バックアップに基づいて増分バックアップを実行します。このモードでは、前回のバックアップ以降に変更されたファイルのみがバックアップされます。
 - **Differential** - 完全バックアップに基づいて差分バックアップを実行します。このモードでは、完全バックアップ以降に変更されたファイルのみがバックアップされます。CBT バックアップが有効になっている場合、差分バックアップはサポートされません。
- **Disk Read Rate Limit:** VM ディスク ファイルを保存するストレージ ボリュームの読み取り速度の制限を指定します。
- **Disk Write Rate Limit:** バックアップ ファイルを保存するストレージ ボリュームの書き込み速度の制限を指定します。
- **Temp Directory:** バックアップ中に使用される一時ディレクトリを入力します。指定したディレクトリが存在しない場合は、バックアップ中にシステムによって自動的にディレクトリが作成されます。
- **Compress:** バックアップ中にディスクイメージを圧縮するかどうかを設定します。

Incremental/Differential Backup

- **Frequency:** バックアップの実行頻度を選択します。
- **Started At:** 実行開始時刻を選択します。
- **To: 実行終了時刻を選択します。** 開始時刻が終了時刻より遅い場合、バックアップは翌日に終了します。終了時刻までに完全バックアップが完了しない場合、システムは VM バックアップの終了後にこのバックアップ タスクを停止し、次のバックアップの開始を待機します。

バックアッププールの管理

バックアッププールは VM バックアップ ファイルを管理します。共有ストレージ プールまたはリモート サーバーは、バックアップ ファイルの統合管理のために VM バックアップ ファイルを保存するためのパスを提供します。

バックアッププールを追加する

1. 上部のナビゲーション バーで、**Services** をクリックします。
2. 左側のナビゲーション ペインから、**Backup Center > VM Backup** を選択します。
3. **Backup Pools** タブをクリックします。
4. **Add** 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。

バックアッププールを編集する

1. 上部のナビゲーション バーで、**Services** をクリックします。
2. 左側のナビゲーション ペインから、**Backup Center > VM Backup** を選択します。
3. **Backup Pools** タブをクリックします。
4. バックアップ プールの **Actions** 列で **Edit** をクリックします。
5. **OK** をクリックします。

バックアッププールを削除する

1. 上部のナビゲーション バーで、**Services** をクリックします。
2. 左側のナビゲーション ペインから、**Backup Center > VM Backup** を選択します。
3. **Backup Pools** タブをクリックします。
4. バックアップ プールの **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。

パラメーター

- **Name:** バックアップ プールの名前を指定します。
- **Backup Location:** VM バックアップ ファイルを保存する場所を選択します。オプションには、**Shared Storage** と **Remote Server** があります。
- **Available Storage Space:** ストレージ プール内の使用可能な共有ストレージ容量、またはリモートサーバー上の使用可能なストレージ容量。

Shared Storage を選択した場合は、共有ストレージ プールを選択する必要があります。

Remote Server を選択した場合は、次のパラメーターを構成します。

- **IP Address:** リモート サーバーの IP アドレスを入力します。
- **Username:** リモート サーバーにログインするためのユーザー名を入力します。アカウントにサーバーへの読み取りおよび書き込みアクセス権があることを確認してください。FTP モードを選択した場合は、リモートサーバーの FTP サーバーにアカウントを作成する必要があります。SCP モードを選択した場合は、リモートサーバーの OS にアカウントを作成する必要があります。
- **Password:** リモート サーバーにログインするためのパスワードを入力します。

- **Connection Mode:** リモート サーバーに接続するためのモードを選択します。オプションには、**FTP** と **SCP** があります。**FTP** を選択した場合は、Server-U、VsFTP、および IIS サーバーのみがサポートされます。
- **Server Port:** サーバーのポート番号を入力します。
- **Test Connectivity:** このボタンをクリックすると、CVM とリモート サーバー間の接続がチェックされます。
- **Backup Directory:** バックアップ ファイルを保存するディレクトリを指定します。ディレクトリは少なくともレベル 3 のディレクトリである必要があります。

バックアップパラメーターを構成する

バックアップパラメーターを設定すると、システムはこれらのパラメーターをデフォルト値として使用します。

手順

1. 上部のナビゲーション バーで、**Services** をクリックします。
2. 左側のナビゲーション ペインから、**Backup Center > VM Backup** を選択します。
3. **Backup Parameters** タブをクリックします。
4. **Edit** をクリックします。
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。

パラメーター

- **Disk Read Rate Limit:** VM ディスク ファイルを保存するストレージ ボリュームの読み取り速度の制限を指定します。
- **Disk Write Rate Limit:** バックアップ ファイルを保存するストレージ ボリュームの書き込み速度の制限を指定します。
- **Compress:** バックアップ中にディスクイメージを圧縮するかどうかを設定します。
- **CBT Backup:** VM の CBT バックアップを有効にするかどうかを選択します。CBT は前回のバックアップ以降に変更されたデータのみをバックアップするため、時間とシステム リソースを節約できます。
- **Temp Directory:** バックアップ中に使用される一時ディレクトリを入力します。指定したディレクトリが存在しない場合は、バックアップ中にシステムによって自動的にディレクトリが作成されます。

- **Retained Full Backup Files:** 同じバックアップ ディレクトリに保持されるフル バックアップ ファイルの数を指定します。このパラメーターを指定しない場合、保持されるフル バックアップ ファイルの数は制限されません。

CVMバックアップを構成する

CVM バックアップを使用すると、CVM データおよび構成ファイルの自動スケジュール バックアップまたは手動バックアップを実行したり、バックアップ履歴レコードを表示したり、バックアップ ファイルをダウンロードしたり、バックアップ ファイルを使用して CVM を復元したりできます。

- **Automatic backup**—システムは、CVM によって管理されるランダムに選択された 3 つのホストに、CVM データと構成ファイルを毎日自動的にバックアップします。バックアップ ファイルの生成後にシステムがアップグレードされた場合でも、各ホストは最新の 7 つのバックアップ ファイルを保持します。
- **Scheduled backup**—システムは、指定された頻度で CVM データと構成ファイルを自動的にバックアップします。スケジュールされたバックアップを設定するには、『CVM バックアップパラメーターを構成する』を参照してください。
- **Manual backup**—手動バックアップを実行するには、『CVM 設定をバックアップする』を参照してください。

制限事項とガイドライン

RBAC モードでは、システム管理者のみが CVM バックアップを構成できます。

機能

- CVM バックアップパラメーターを構成する
- CVM 設定をバックアップする
- CVM バックアップファイルの管理

CVMバックアップパラメーターを構成する

このタスクを実行して、CVM バックアップ ファイルを保存するディレクトリを指定し、自動バックアップ パラメーターを設定します。自動バックアップと手動バックアップのバックアップ ファイルは同じディレクトリに保存されます。

制限事項とガイドライン

CVM バックアップ後に VM とそのイメージ ファイルを削除すると、CVM バックアップ ファイルを使用して CVM を復元しても VM を復元できなくなります。

リモート バックアップを実行する前に、リモート サーバー上にバックアップ ディレクトリを準備します。

手順

1. 上部のナビゲーション バーで、**Services** をクリックします。
2. 左側のナビゲーション ペインから、**Backup Center > CVM Backup** を選択します。
3. 『**パラメーター**』の説明に従って、データ バックアップ パラメーターを設定します。
4. **Save** をクリックします。
5. CVM データをすぐにバックアップするには、**Back Up Now** をクリックします。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

- **Backup Location:** CVM バックアップ 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。

Local Directory を選択した場合は、バックアップ 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。

Remote Server を選択した場合は、次のパラメーターを構成します。

- **IP Address:** リモート サーバーの IP アドレスを入力します。
- **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、リモート サーバーに対する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 サーバーのオペレーティング システム上にアカウントを作成する必要があります。
- **Password:** ユーザー名のパスワードを入力します。
- **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。デフォルトは **FTP** です。FTP を選択した場合、Server-U、VsFTP、および IIS FTP サーバーのみがサポートされます。
- **Backup Directory:** リモート サーバー上でバックアップ ファイルが保存されるディレクトリパスを入力します。ディレクトリがリモート サーバー上に既に存在していることを確認してください。

- **Server Port:** リモート サーバーにアクセスするために使用するポート番号を指定します。デフォルトのポート番号は、FTP 接続モードの場合は 21、SCP 接続モードの場合は 22 です。
- **Test Connectivity:** このボタンをクリックすると、CVM とリモート サーバー間の接続がチェックされます。
- **Scheduled Backup:** スケジュールされたバックアップを有効にするかどうかを選択します。**Yes** を選択した場合は、次のパラメーターを構成します。
 - **Frequency:** バックアップの頻度を選択します。
 - **Time:** バックアップの開始時刻を指定します。
 - **Backups to Save:** システムが保存できる CVM バックアップ ファイルの数を指定します。このパラメーターを空のままにすると、保存できる CVM バックアップ ファイルの数は制限されません。

CVM設定をバックアップする

このタスクを実行して、データ センター、HA、バージョン情報を含む CVM 設定を CVM バックアップ ファイルにバックアップします。CVM に障害が発生した場合、サービスを中断することなく、バックアップ ファイルを使用して迅速に回復できます。

バックアップ操作の結果は次のいずれかになります。

- **Failed** - バックアップ操作が失敗し、バックアップ ファイルは生成されません。
- **Succeeded** — バックアップ操作が成功し、CVK 構成を含むバックアップ ファイルが生成されました。バックアップ ファイルは復元に使用できます。
- **Partially succeeded** - バックアップ操作は部分的に成功し、バックアップ ファイルが生成されましたが、システムは一部の CVK 構成のバックアップに失敗しました。バックアップ ファイルは復元に使用できますが、システムは一部の CVK ホストの構成のバックアップに失敗しました。

制限事項とガイドライン

CVM バックアップ構成ページで CVM データ バックアップ パスを構成できます。デフォルトのパスは /vms です。

手順

1. 上部のナビゲーション バーで、**Resources** をクリックします。
2. ページの右上にある **Back Up CVM Settings** をクリックします。
3. OK をクリックします。

CVMバックアップファイルの管理

システムは、バックアップ ファイル名、作成時刻、バージョン番号、バックアップの場所、バックアップ ディレクトリなど、各 CVM バックアップに関する情報を記録します。

制限事項とガイドライン

- あなたがバックアップ ファイルを使用して CVM を復元する場合は、復元されたデータの可用性を確保するために、以下の手順に従ってください。
 - a. すべてのクラスターの HA を無効にします。
 - b. バックアップ ファイルを使用して CVM を復元します。
 - c. すべてのホストに接続します。
 - d. クラスターの HA を有効にします。
- バックアップ ファイルを使用して CVM を復元するには、ホスト、VM、共有ストレージの数量がバックアップ ファイルが生成された時点と同じであることを確認します。
- 一度に CVM を復元できるのは 1 人のオペレーターのみです。
- バックアップ ファイルをアップロードまたはインポートするときは、バックアップ ファイルのバージョンが現在の CVM バージョンと同じであることを確認してください。

バックアップファイル情報を表示する

1. 上部のナビゲーション バーで、**Services** をクリックします。
2. 左側のナビゲーション ペインから、**Backup Center > CVM Backup** を選択します。
3. **Backup History** タブをクリックします。

バックアップファイルをダウンロードする

1. 上部のナビゲーション バーで、**Services** をクリックします。
2. 左側のナビゲーション ペインから、**Backup Center > CVM Backup** を選択します。
3. **Backup History** タブをクリックします。
4. CVM バックアップ ファイルの **Actions** 列で **Download** をクリックします。

バックアップファイルを使用してCVMを復元する

1. 上部のナビゲーション バーで、**Services** をクリックします。
2. 左側のナビゲーション ペインから、**Backup Center > CVM Backup** を選択します。
3. **Backup History** タブをクリックします。
4. CVM バックアップ ファイルの **Actions** 列で **Restore** 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。

バックアップファイルをアップロードする

1. 上部のナビゲーション バーで、**Services** をクリックします。
2. 左側のナビゲーション ペインから、**Backup Center > CVM Backup** を選択します。
3. **Backup History** タブをクリックします。
4. **Upload** をクリックします。
5. 点線のボックスをクリックし、アップロードするファイルを選択して点線のボックスにドラッグします。『**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. ファイルのアップロードを開始するには、**Start** をクリックします。ファイルがアップロードされたら、**OK** をクリックします。

バックアップファイルをインポートする

1. 上部のナビゲーション バーで、**Services** をクリックします。
2. 左側のナビゲーション ペインから、**Backup Center > CVM Backup** を選択します。
3. **Backup History** タブをクリックします。
4. **Import** 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。

バックアップファイルを削除する

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

3. **Backup History** タブをクリックします。
4. バックアップ ファイルの **Actions** 列で **Backup History** 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。

パラメーター

- **File Name:** CVM バックアップ ファイルの名前。
- **Created At:** CVM バックアップ ファイルが生成された時刻。
- **Version:** バックアップを実行した時点の CVM バージョン。
- **Backup Location:** バックアップ 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。デフォルトは **Local Directory** です。

Local Directory を選択した場合は、バックアップ 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。

Remote Server を選択した場合は、次のパラメーターを構成します。

- **IP Address:** リモート サーバーの IP アドレスを入力します。
- **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、リモート サーバーに対する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 サーバーのオペレーティング システム上にアカウントを作成する必要があります。
- **Password:** ユーザー名のパスワードを入力します。
- **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。デフォルトは **FTP** です。FTP を選択した場合、Server-U、VsFTP、および IIS FTP サーバーのみがサポートされます。
- **Backup Directory:** リモート サーバー上でバックアップ ファイルが保存されるディレクトリパスを入力します。
- **Server Port:** リモート サーバーにアクセスするために使用するポート番号を指定します。デフォルトのポート番号は、FTP 接続モードの場合は 21、SCP 接続モードの場合は 22 です。
- **Server Port:** このボタンをクリックすると、CVM とリモート サーバー間の接続がチェックされます。

スナップショットセンターを管理する

スナップショットセンターは、CVM 上の VM スナップショットを管理し、システムのアップグレード後にスナップショットをデータベースに同期します。

スナップショットを表示

1. 上部のナビゲーション バーで、**Services** をクリックします。
2. 左側のナビゲーション ペインから、**Snapshot Center** を選択します。
3. ページの左側で **By Running Location** または **By View Location** を選択します。
4. スナップショットをフィルターリングするには、**All**、**Internal Snapshot**、または **External Snapshot** を選択します。

または、VM のエイリアスを入力して、その VM のスナップショット情報を表示することもできます。

VM のスナップショットを一括削除する

VM のスナップショットを一括で削除するには、このタスクを実行します。

1. 上部のナビゲーション バーで、**Services** をクリックします。
2. 左側のナビゲーション ペインから、**Snapshot Center** を選択します。
3. 1 つまたは複数のスナップショットを選択し、**Delete Snapshots** をクリックします。
4. 最大削除率を設定し、画像チェーンの統合を有効にするかどうかを選択します。

スナップショット タイプが外部で、VM が実行中または一時停止状態の場合にのみ、最大削除率を設定できます。スナップショット タイプが外部の場合にのみ、イメージ チェーンの統合を有効にできます。

5. **OK** をクリックします。

スナップショットを一括削除

1 つまたは複数の VM の内部スナップショットまたは外部スナップショットを一括で削除するには、このタスクを実行します。

1. 上部のナビゲーション バーで、**services** をクリックします。
2. 左側のナビゲーション ペインから、**Snapshot Center** を選択します。
3. ページの右上隅にある **Bulk Delete Snapshots** をクリックします。
4. 削除する VM スナップショットを選択し、**Delete** をクリックします。
5. 最大削除率を設定し、画像チェーンの統合を有効にするかどうかを選択します。
6. スナップショット タイプが外部で、VM が実行中または一時停止状態の場合にのみ、最大削除率を設定できます。スナップショット タイプが外部の場合にのみ、イメージ チェーンの統合を有効にできます。
7. **OK** をクリックします。

パラメーター

- **Alias:** スナップショットが作成された VM のエイリアス。VM スナップショット管理ページにアクセスするには、VM エイリアスをクリックします。
- **Description:** VM の外部または内部スナップショットが作成されている場合の VM の説明。
- **Snapshots:** VM の外部または内部スナップショットの数。
- **Snapshot Type:** スナップショットのタイプ。
- **First Snapshot Time:** VM の最初のスナップショットが作成された時間。
- **Most Recent Snapshot Time:** VM の最新の外部スナップショットまたは内部スナップショットが作成された時間。
- **Host Name:** スナップショットが作成された VM があるホストの名前。
- **IP:** VM の IP アドレス。
- **State:** VM の実行状態。

DRXを管理する

DRX は定期的にはリソースの使用状況をチェックし、サービス VM の数を動的に調整して、サービス システムに弾力性と拡張性に優れたリソース プールを提供します。

機能

- DRX サービスの管理
- DRX サービス監視を構成する
- スケジュールされた拡張ポリシーを管理する
- 垂直拡張ポリシーを構成する
- LB リソースコラボレーションを構成する
- DRX サービスの概要を表示する
- DRX サービスで VM 情報を表示する
- DRX サービス監視情報を表示する
- LB コラボレーションリソースを表示する
- DRX サービス操作ログを表示する

DRXサービスの管理

DRX は、同じクラスター内で同じサービスを提供する VM を VM グループに追加します。グループ内の VM の接続数、平均 CPU 使用率、平均メモリ使用率を定期的にチェックし、DRX ポリシーとリソース拒否モード、リソース再利用ポリシーと再利用モードに基づいて、グループ内の VM の数を動的に調整します。

DRX を使用すると、単一サービス システムにリソース負荷分散を実装できます。

DRX リソース管理により、オペレーターは DRX サービスを追加、編集、削除、有効化、無効化できます。

制限事項とガイドライン

- 拡張ポリシーと再利用ポリシーに設定されたしきい値が両方とも一致すると、システムは自動的に VM を作成し、再利用ポリシーは有効になりません。
- DRX サービスを削除しても、この DRX サービスによって作成された VM は削除されません。
- リソースのインポート タイプが Fast Clone の場合に VM のすべてのデータを複製するには、まず VM を再デプロイする必要があります。再デプロイ後、VM のイメージがマージされます。

DRXサービスを追加する

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

DRX サービスを編集する

1. 上部のナビゲーション バーで、**services** をクリックします。
2. 左側のナビゲーション ペインから、**DRX** を選択します。
3. DRX サービスの **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。

DRX サービスを削除する

1. 上部のナビゲーション バーで、**services** をクリックします。
2. 左側のナビゲーション ペインから、**DRX** を選択します。
3. DRX サービスの **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。


DRXサービスを有効にする

1. 次のいずれかのタスクを実行します。
 - 上部のナビゲーション バーで **Services** をクリックし、左側のナビゲーション ペインで **DRX** を選択して、DRX サービスの **Actions** 列で **Enable** をクリックします。
 - 上部のナビゲーション バーで **Services** をクリックし、左側のナビゲーション ペインで **DRX** を選択し、DRX サービスの名前をクリックして、**Enable DRX** をクリックします。
2. DRX が有効になる時間を選択し、**OK** をクリックします。

DRX サービスを削除する

1. 上部のナビゲーション バーで、**services** をクリックします。
2. 左側のナビゲーション ペインから、**DRX** を選択します。
3. DRX サービスの **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。

VM を再デプロイする

1. 上部のナビゲーション バーで、**services** をクリックします。
2. 左側のナビゲーション ペインから、**DRX** を選択します。
3. **Summary** タブの **Basic Attributes** 領域で VM のアイコン  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

情報

- **Cluster:** DRX サービスを実行するクラスターの名前を入力します。
- **Storage:** 自動的に作成される VM の共有ストレージ プールを指定します。
- **Backup Cluster:** DRX サービスを実行するバックアップ クラスターを指定します。現在のクラスターが DRX 要件を満たすことができない場合、バックアップ クラスターに VM が作成されます。バックアップ クラスターに VM を作成するには、リソースのインポート タイプが **Fast Clone** に設定されているときに、クラスターとそのバックアップ クラスターが同じ共有ストレージを使用する必要があります。

Storage: 自動的に作成された VM のバックアップ共有ストレージ プールを指定します。

- **Max. VMs:** DRX サービスでサポートされる VM の最大数を指定します。これは、VM グループで許可される VM の最大数です。
- **Effective:** DRX サービスを有効にする方法を選択します。オプションには、**Now**、**Custom**、**No** があります。
 - **Now-** DRX サービスは、作成後すぐに有効になります。
 - **Custom-** DRX サービスは指定された時間範囲で有効になります。
 - **No-** DRX サービスは有効になりません。
- **Start Time:** DRX サービスが有効になる開始時間を指定します。このフィールドは、**Effective** リストから **Custom** を選択した場合に必須です。開始時間のみを設定すると、DRX サービスは常にこの時間から有効になります。
- **End Time:** DRX サービスが有効になる終了時刻を指定します。このフィールドは、**Effective** リストから **Custom** を選択した場合に必須です。終了時刻のみを設定すると、DRX サービスは現在の時刻から終了時刻まで有効になります。
- **Bind LB Resource:** VM を LB デバイスにバインドするかどうかを選択します。はい を選択した場合は、LB 設定を構成する必要があります。

設定

- **Duration:** 拡張監視ポリシーで VM グループ内の VM の平均 CPU 使用率とメモリ使用量、および接続数がしきい値を複数回超える期間、または再利用監視ポリシーでしきい値を複数回下回る期間を指定します。
- **Detection Interval:** VM グループ内の VM の平均 CPU 使用率、平均メモリ使用量、および接続を検出する間隔を指定します。
- **Resource Import:** リソースのインポートの監視ポリシーを選択します。VM グループ内の VM の平均 CPU 使用率、平均メモリ使用量、接続、ネットワークトラフィック、ディスク I/O、および IOPS が、指定された時間内に拡張ポリシーで設定されたしきい値を超えると、VM グループに VM が自動的に作成されます。
- **Resource Import:** VM グループに VM を作成するモードを選択します。オプションには、**Fast Deploy** と **Fast Clone** があります。
 - **Fast Deploy-** 選択した VM テンプレートを通じて VM グループ内に VM が作成されます。
 - **Fast Clone-** クローンする VM を選択して、VM グループ内に VM が作成されます。
- **VMs to Create :** 各 DRX タスクに対して作成する VM の数を 1 ~ 100 の範囲で指定します。このパラメーターを設定する場合、**Percentage of VMs to Add** パラメーターは設定できません。

- **Percentage of VMs to Add:** 各 DRX タスクで作成する VM の割合を 1 ~ 100 の範囲で指定します。作成する VM の数は、実行中の VM の数にこの割合を掛けて、その積を最も近い整数に切り上げて算出されます。たとえば、10 台の VM が実行中で、このパラメーターを 35% に設定すると、システムは DRX タスクで 4 台の VM を作成します。このパラメーターを設定すると、**VMs to Create** パラメーターは設定できません。
- **Resource Reclaim:** リソースの再利用のための再利用監視ポリシーを選択します。VM グループ内の VM の平均 CPU 使用率、平均メモリ使用量、接続、ネットワークトラフィック、ディスク I/O、および IOPS が、指定された時間内に再利用監視ポリシーで設定されたしきい値を下回ると、VM グループ内の VM は自動的に再利用されます。
- **Reclaim Type:** 回収ポリシーを選択します。オプションには、**Reclaim Now** と **Slow-Offline** があります。
 - **Reclaim Now-** 再利用条件が満たされている限り、VM は再利用されます。
 - **Slow-Offline-** 再利用条件が満たされると、システムは VM が TCP パケットを受信できないようにし、VM によって送信されたパケット数が 10 秒ごとにしきい値より小さいかどうかを検出します。数がしきい値より小さい場合、システムは VM を直ちに再利用します。数がしきい値より小さくない場合、システムは数がしきい値より小さくなるまで待機してから VM を再利用するか、タイムアウトに達するまで待機してから VM を再利用します。
 - **Threshold-** 低速オフライン VM 再利用をトリガーできる VM によって送信されるパケットの最大数を指定します。このパラメーターは、再利用モードとして **Slow-Offline** を選択した場合にのみ必要です。
 - **Timeout-** 低速オフライン VM 再利用をトリガーできるタイムアウトを指定します。このパラメーターは、再利用モードとして **Slow-Offline** を選択した場合にのみ必要です。
- **Reclaim Mode:** VM を再利用するモードを選択します。オプションには、**Shut Down**、**Delete**、**Put VM to Sleep** などがあります。
 - **Shut Down VM-** VM の電源をオフにします。
 - **Shut Down VM-** VM を削除します。
 - **Put VM to Sleep-** VM をスリープ状態にします。
- **Min Running VMs:** リソース再利用タスクで実行状態にある必要がある VM の最小数を指定します。

VM の場合

- **Service VM :** 同じサービスを実行する VM を VM グループに追加するには、**Yes** をクリックします。

Extension

- **VM Template:** 高速デプロイメント用の VM テンプレートを選択します。このパラメーターは、リソースのインポート タイプとして **Fast Deployment** を選択した場合にのみ必要です。
- **VM to Clone :** クローンする VM を選択します。このパラメーターは、リソースのインポート タイプとして **Fast Clone** を選択した場合のみ必要です。基本的な DRX 構成でストレージ プールとして共有ファイルシステムを指定した場合、クローンする VM は、イメージ ファイルをディスクとして使用する VM である必要があります。RBD ストレージ プールを指定した場合、クローンする VM は、RBD ストレージ プールと同じ分散ストレージ プールに RBD がマウントされた VM である必要があります、VM は次の要件を満たしている必要があります。

- VM 上に USB、PCI、SR-IOV、または TPM デバイスが存在しません。
- VM は NUMA ノードまたは物理 CPU にバインドされていません。
- VM のストレージ タイプはインテリジェントであり、シン プロビジョニングが使用されます。
- **VM Prefix:** VM のプレフィックスを入力します。
- **Start Number:** VM の開始番号を入力します。このパラメーターは、VM プレフィックスの後に表示されます。作成された VM の数が増えると、最大数に達するまで番号が増加します。
- **IPv4 configuration**
 - **Start IP :** VM の開始 IPv4 アドレスを指定します。
 - **End IP :** VM の終了 IPv4 アドレスを指定します。IP 割り当てに十分な IPv4 アドレスを予約します。
 - **Subnet Mask:** VM のサブネットマスクを指定します。
 - **Default Gateway:** VM のデフォルト ゲートウェイを指定します。
- **IPv6 configuration**
 - **開始 IP :** VM の開始 IPv6 アドレスを指定します。
 - **終了 IP :** VM の終了 IPv6 アドレスを指定します。IP 割り当てに十分な IPv6 アドレスを予約します。
 - **ネットワークプレフィックス:** IPv6 アドレスのプレフィックスの長さを指定します。
 - **デフォルト ゲートウェイ:** VM のデフォルト ゲートウェイを指定します。

LB Config

- **Bound IP Type:** LB デバイスの IP アドレス タイプを選択します。
- **LB Device:** LB デバイスを選択します。LB デバイスは、さまざまなポリシーに基づいてトラフィックを実際のサーバーに分散します。
- **Virtual Server:** 仮想サーバーを選択します。仮想サーバーには仮想 IP があります。仮想サーバーはユーザー要求を受け取り、LB デバイスはユーザー要求に応答する実サーバーを選択します。
- **Real Server Farm:** 実サーバー ファームを選択します。実サーバー ファームには実サーバーが含まれます。
- **VM Service Port:** VM がサービスを提供するポートを入力します。ポートによって提供されるサービスが異なります。

DRXサービス監視を構成する

DRX サービス監視ポリシーを構成するには、このタスクを実行します。

VM グループ内の VM の平均 CPU 使用率とメモリ使用量、接続、ネットワークトラフィック、ディスク I/O、および IOPS が拡張ポリシーで設定されたしきい値を超える期間が指定された期間に達すると、VM グループ内に VM が自動的に作成されます。VM グループ内の VM の平均 CPU 使用率とメモリ使用量、接続、ネットワーク

トラフィック、ディスク I/O、および IOPS が再利用ポリシーで設定されたしきい値を下回る期間が指定された期間に達すると、システムは VM を自動的に再利用します。

手順

1. 上部のナビゲーション バーで、**services** をクリックします。
2. 左側のナビゲーション ペインから、**DRX** を選択します。
3. DRX サービスの名前をクリックします。
4. **Service Monitoring** 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。

パラメーター

- **Duration:** 拡張監視ポリシーで VM グループ内の VM の平均 CPU 使用率とメモリ使用量、および接続数がしきい値を複数回超える期間、または再利用監視ポリシーでしきい値を複数回下回る期間を指定します。
- **Interval:** VM グループ内の VM の CPU 使用率、メモリ使用量、接続を検出する間隔を指定します。
- **Extension Policy:** 拡張ポリシーを選択します。VM グループ内の VM の平均 CPU 使用率とメモリ使用量、接続、ネットワーク トラフィック、ディスク I/O、IOPS が、指定された時間内に拡張ポリシーで設定されたしきい値を超えると、VM グループに VM が自動的に作成されます。ポリシーの条件、演算子、しきい値パラメーターは、必要に応じて設定できます (例: **CPU Usage >= 80%** または **Memory Usage >= 70%** または **Connections >= 100**)。
- **Reclaim Policy:** 再利用ポリシーを選択します。VM グループ内の VM の平均 CPU 使用率とメモリ使用量、接続、ネットワーク トラフィック、ディスク I/O、IOPS が、指定された時間内に再利用ポリシーで設定されたしきい値を下回ると、システムは VM を自動的に再利用します。ポリシーの条件、演算子、しきい値パラメーターは、必要に応じて設定できます (例: **CPU Usage <= 30%** または **Memory Usage <= 20%** または **Connections <=10**)。

スケジュールされた拡張ポリシーを管理する

スケジュールされた拡張ポリシーは、サービス サージが定期的発生するアプリケーション システムで特定の時点で VM を作成するために使用されます。

制限事項とガイドライン

- 頻度を **Daily** に設定し、開始時刻を CVM の現在のシステム時刻よりも早く設定すると、スケジュールされた拡張タスクは翌日に有効になります。
- スケジュールされた拡張のデフォルトのポーリング間隔は 10 分です。指定された期間中は DRX は実行されません。
- スケジュールされた拡張ポリシーで指定されていない期間中、ポリシーを使用して作成された VM は、リソース再利用ポリシーを満たしている場合に再利用されます。

スケジュールされた拡張ポリシーを追加する

1. 上部のナビゲーション バーで、**services** をクリックします。
2. 左側のナビゲーション ペインから、**DRX** を選択します。
3. DRX サービスの名前をクリックします。
4. **Scheduled Extension Policy** をクリックします。
5. **Add** をクリックします。
6. 『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。
7. **OK** をクリックします。

スケジュールされた拡張ポリシーを編集する

1. 上部のナビゲーション バーで、**services** をクリックします。
2. 左側のナビゲーション ペインから、**DRX** を選択します。
3. DRX サービスの名前をクリックします。
4. **Scheduled Extension Policy** をクリックします。
5. **Scheduled Extension Policy** の **Actions** 列で **Edit** をクリックします。
6. 『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。
7. **OK** をクリックします。

スケジュールされた拡張ポリシーを削除する

1. 上部のナビゲーション バーで、**services** をクリックします。
2. 左側のナビゲーション ペインから、**DRX** を選択します。
3. DRX サービスの名前をクリックします。
4. **Scheduled Extension Policy** をクリックします。

5. **Scheduled Extension Policy** の **Actions** 列で **Delete** 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。

スケジュールされた拡張ポリシー情報を表示する




1. 上部のナビゲーション バーで、**services** をクリックします。
2. 左側のナビゲーション ペインから、**DRX** を選択します。
3. DRX サービスの名前をクリックします。
4. **Scheduled Extension Policy** をクリックします。

パラメーター

スケジュールされた拡張ポリシーを追加または編集する

- **VMs to Create** : スケジュールされた拡張タスクごとに作成する VM の数を指定します。
- **Frequency**: スケジュールされた拡張タスクが実行される頻度を選択します。
- **Start Time**: スケジュールされた拡張タスクの開始時刻を指定します。
- **End Time**: スケジュールされた拡張タスクが終了する時刻を指定します。
- **Effective Now**: スケジュールされた拡張タスクをすぐに有効にするかどうかを選択します。

スケジュールされた拡張ポリシーリスト

- **VMs to Create** : スケジュールされた拡張タスクごとに作成する VM の数。
- **Effective Time Period**: スケジュールされた延長ポリシーが有効になる期間。
- **State**: スケジュールされた拡張ポリシーの状態。
- **Actions**: オペレーターがスケジュールされた拡張ポリシーに対して実行できるアクション。
 - スケジュールされた拡張ポリシーを編集するには、 アイコンをクリックします。
 - スケジュールされた拡張ポリシーを削除するには、 アイコンをクリックします。
- スケジュールされた拡張ポリシーを表示するには、 アイコンをクリックします。

垂直拡張ポリシーを構成する

DRX サービスの垂直拡張ポリシーを設定するには、このタスクを実行します。CPU 使用率またはメモリ使用率が垂直拡張ポリシーで設定されたしきい値を超えると、システムは VM に CPU またはメモリを追加します。

手順

1. 上部のナビゲーション バーで、**services** をクリックします。
2. 左側のナビゲーション ペインから、**DRX** を選択します。
3. DRX サービスの名前をクリックします。
4. **Vertical Extension Policy** をクリックします。
5. 必要に応じて、**Configure CPU** または **Configure Memory** を選択します。
 - **Configure CPU** を選択した場合は、CPU 使用率、ステップ、最大制限を入力します。
 - **Configure Memory** を選択した場合は、メモリ使用量、ステップ、最大制限を入力します。
6. **OK** をクリックします。

パラメーター

- **Configure CPU:** CPU 使用率による垂直拡張ポリシーを有効にするには、このオプションを選択します。
- **CPU Usage:** CPU 使用率のしきい値を指定します。このしきい値に達すると、システムは VM に CPU を追加します。
- **Step:** VM に追加する CPU の数を指定します。
- **Max Limit:** VM に追加できる CPU の最大数を指定します。
- **Configure Memory:** メモリ使用量による垂直拡張ポリシーを有効にするには、このオプションを選択します。
- **Memory Usage:** メモリ使用量のしきい値を指定します。このしきい値に達すると、システムは VM にメモリを追加します。
- **Step:** VM に追加するメモリ サイズを指定します。
- **Max Limit:** VM に追加できる最大メモリ サイズを指定します。

LB リソースコラボレーションを構成する

VM グループの LB デバイスを指定するには、このタスクを実行します。このタスクを実行する前に、LB デバイスが使用可能であり、正しく構成されていることを確認してください。

前提条件

このタスクを実行する前に、ロード バランサーが使用可能であり、正しく構成されていることを確認してください。

手順

1. 上部のナビゲーション バーで、**services** をクリックします。
2. 左側のナビゲーション ペインから、**DRX** を選択します。
3. DRX サービスの名前をクリックします。
4. **LB Resource Collaboration** 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. **Finish** をクリックします。



パラメーター

- **Start IP** : VM の開始 IP アドレスを入力します。
- **End IP** : VM の終了 IP アドレスを入力します。
- **LB Device**: LB デバイスを選択します。LB デバイスはトラフィックを実サーバーに分散します。
- **Virtual Server**: 仮想サーバーを選択します。仮想サーバーは仮想 IP を提供します。仮想サーバーはユーザー要求を受信し、LB デバイスは要求に応答する実サーバーを選択します。
- **Real Server Farm**: 実サーバー ファームを選択します。実サーバー ファームには実サーバーが含まれます。
- **VM Service Port**: サービス ポートを入力します。サービス ポートによって提供されるサービスが異なります。
- **Scheduling Algorithm**: スケジューリング アルゴリズムを選択します。LB デバイスは、スケジューリング アルゴリズムに基づいて実サーバーを選択します。
- **Health Check Method**: ヘルス チェック方法を選択します。LB デバイスは、実サーバー ファーム内の実サーバーのヘルス状態をチェックします。実サーバーが使用不可であることが検出された場合、LB デバイスは実サーバーにユーザー要求を配布しません。実サーバーが回復すると、LB デバイスは実サーバーにユーザー要求を配布し続けます。このプロセスは、ユーザーに対して透過的です。

DRXサービスの概要を表示する

DRX サービスの概要とリソース使用状況を表示するには、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、**services** をクリックします。
2. 左側のナビゲーション ペインから、**DRX** を選択します。
3. DRX サービス リストを更新するには、 アイコンをクリックします。
4. 表示する列を選択するには、 アイコンをクリックします。
5. DRX サービスに関する基本情報を表示するには、サービスの名前をクリックします。

パラメーター

- **Basic Attributes:** DRX サービスに関する基本情報。
 - **Service Name:** DRX サービスの名前。
 - **Cluster:** DRX サービスを実行するクラスター。
 - **Max. VMs:** DRX サービスでサポートされる VM の最大数。これは、VM グループで許可される VM の最大数です。
 - **Current VMs :** DRX サービスに対応する VM グループ内の VM の数。
 - **Resource Import:** DRX サービスに対応する VM グループに VM が作成されるモード。
 - **VM/Template:** クローンされた VM の名前または使用中の VM テンプレートの名前。リソースのインポート モードが **Fast Deployment** の場合、この列には **VM のデプロイに使用される VM テンプレートの名前が表示されます**。リソースのインポート モードが **Fast Clone** の場合、この列にはクローンされた VM の名前が表示されます。
 - **VMs to Create :** DRX サービス内の動的リソース拡張ごとに作成する VM の数。
 - **Percentage of VMs to Add:** DRX サービスのすべての動的リソース拡張に対して作成する VM の割合。作成する VM の数は、実行中の VM の数にこの割合を掛けて、その積を最も近い整数に切り上げて算出されます。たとえば、10 台の VM が実行中で、このパラメーターを 35% に設定すると、動的リソース拡張で 4 台の VM が作成されます。
 - **Reclaim Type:** VM を再利用するためのポリシー。
 - **Reclaim Mode:** VM が再利用されるモード。
 - **State:** DRX サービスの現在の状態。
 - **Extension Policy:** VM グループ内の VM のパラメーターが指定された時間内に拡張ポリシーで設定されたしきい値と一致すると、VM は VM グループ内に自動的に作成されます。
 - **Reclaim Policy:** VM グループ内の VM のパラメーターが指定された時間内に再利用ポリシーで設定されたしきい値と一致すると、VM グループ内の VM は自動的に再利用されます。

- **CPU Usage:** 過去 30 分間の VM グループ内で実行中のすべての VM の平均 CPU 使用率傾向グラフ。横軸は時間を表し、縦軸は CPU 使用率をパーセンテージで表します。
- **Memory Usage:** 過去 30 分間の VM グループ内で実行中のすべての VM の平均メモリ使用量傾向グラフ。横軸は時間を表し、縦軸はメモリ使用量をパーセンテージで表します。
- **Connection Statistics:** 過去 30 分間の VM グループ内で実行中のすべての VM の平均接続数傾向グラフ。横軸は時間、縦軸は接続数を表します。
- **Network Traffic Statistics:** 過去 30 分間の VM グループ内で実行中のすべての VM の平均ネットワークトラフィック傾向グラフ。横軸は時間を表し、縦軸は Mbps 単位のネットワークトラフィックを表します。

DRX サービスで VM 情報を表示する

DRX サービスによって監視される VM に関する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、**services** をクリックします。
2. 左側のナビゲーション ペインから、**DRX** を選択します。
3. DRX サービスの名前をクリックします。
4. **VM** タブをクリックします。
5. VM を追加するには、 アイコンをクリックし、VM を選択して、**OK** をクリックします。
6. VM の自動再利用設定を変更するには、 または  ボタンをクリックします。

パラメーター

- **CPU Usage:** 過去 30 分間の VM の CPU 使用率の傾向グラフ。横軸は時間を表し、縦軸は CPU 使用率をパーセンテージで表します。
- **Memory Usage:** 過去 30 分間の VM のメモリ使用量の傾向グラフ。横軸は時間を表し、縦軸はメモリ使用量をパーセンテージで表します。
- **Connections:** 過去 30 分間の VM の接続量の傾向グラフ。横軸は時間、縦軸は接続数を表します。
- **Network Throughput:** 過去 30 分間の VM のネットワーク スループットの傾向グラフ。横軸は時間、縦軸はネットワーク スループットを表します。
- **I/O Throughput:** 過去 30 分間の VM の I/O スループットの傾向グラフ。横軸は時間、縦軸は I/O スループットを表します。

- **IOPS** : 過去 30 分間の VM の IOPS トレンド グラフ。横軸は時間、縦軸は IOPS によるディスク要求数を表します。

DRXサービス監視情報を表示する

VM グループ内の VM の平均リソース使用量を表示するには、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、**services** をクリックします。
2. 左側のナビゲーション ペインから、**DRX** を選択します。
3. DRX サービスの名前をクリックします。
4. **Service Resource Monitoring** タブをクリックします。

パラメーター

- **CPU Usage**: 過去 30 分間の VM グループ内の VM の平均 CPU 使用率の傾向グラフ。横軸は時間を表し、縦軸は CPU 使用率をパーセンテージで表します。
- **Memory Usage**: 過去 30 分間の VM グループ内の VM の平均メモリ使用量の傾向グラフ。横軸は時間を表し、縦軸はメモリ使用量をパーセンテージで表します。
- **Connection Statistics**: 過去 30 分間の VM グループ内の VM の平均接続傾向グラフ。横軸は時間、縦軸は接続数を表します。
- **Network Traffic Statistics**: 過去 30 分間の VM グループ内の VM の平均ネットワークトレンドグラフ。横軸は時間、縦軸はネットワークトラフィックを表します。
- **Disk I/O Usage**: 過去 30 分間の VM グループ内の VM の平均ネットワーク傾向グラフ。横軸は時間、縦軸はネットワークトラフィックを表します。
- **Disk Request Statistics**: 過去 30 分間の VM グループ内の VM の平均ディスク要求傾向グラフ。横軸は時間を表し、縦軸は 1 秒あたりのディスク要求数を表します。

LBコラボレーションリソースを表示する

LB コラボレーション リソースを表示するには、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、**services** をクリックします。
2. 左側のナビゲーション ペインから、**DRX** を選択します。
3. DRX サービスの名前をクリックします。
4. **LB Collaboration Resources** タブをクリックします。

パラメーター

Basic Attributes



- **Device Name:** LB デバイスの名前。
- **Management IP :** LB デバイスの管理 IP アドレス。
- **Virtual Server Name:** 仮想サーバーの名前。
- **Virtual Server Type:** 仮想サーバーのタイプ。
- **Virtual Server IP :** 仮想サーバーがサービスを提供するために使用する IP アドレス。
- **Virtual Server Port:** 仮想サーバーがサービスを提供するために使用するポート。
- **Real Server Farm:** 実サーバー ファームの名前。実サーバー ファームには実サーバーが含まれます。
- **Scheduling Algorithm:** スケジューリング アルゴリズム。LB デバイスは、スケジューリング アルゴリズムに基づいて実サーバーを選択します。
- **Health Check Method:** ヘルス チェック方法。LB デバイスは、実サーバー ファーム内の実サーバーのヘルス状態をチェックします。実サーバーが使用不可であることが検出された場合、LB デバイスは実サーバーにユーザー要求を配布しません。実サーバーが回復した後、LB デバイスは実サーバーにユーザー要求を配布し続けます。このプロセスは、ユーザーに対して透過的です。
- **Virtual Server Connection Statistics:** 仮想サーバー接続の傾向グラフ。横軸は時間、縦軸は接続数を表します。
- **VM LB Statistics:** 実サーバー ファーム内の VM の LB 統計。
- **VM Name:** VM の名前。
- **IP :** VM の IP アドレス。
- **Active Connections:** VM 上のアクティブな接続の数。
- **Max. Connections:** VM 上の同時接続の最大数。
- **Total Connections:** VM 上の同時接続の合計数。
- **B Collaboration State:** VM が実際のサーバー ファームに登録されているかどうか。
- **Actions:** オペレーターが VM 上で実行できるアクション。

- VM に IP アドレスをバインドするには、 アイコンをクリックします。
- VM を登録するには、 アイコンをクリックします。VM が登録されている場合にのみ、VM は LB デバイスによって実サーバーとして使用できます。

DRXサービス操作ログを表示する

DRX サービス操作ログを表示するには、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、**services** をクリックします。
2. 左側のナビゲーション ペインから、**DRX** を選択します。
3. DRX サービスの名前をクリックします。
4. **Tasks** タブをクリックします。
5. タスクをフィルターリングするには、フィルター条件を設定して、**Query** をクリックします。
6. デフォルト以外のフィルター パラメーターを非表示にするには、**Hide** をクリックします。
7. すべてのフィルターパラメーターを表示するには、**More** をクリックします。
8. タスク リストを更新するには、 アイコンをクリックします。
9. 表示する列を選択するには、 アイコンをクリックします。

パラメーター

- **Login Name:** オペレーターが CVM にログインするために使用するログイン名。
- **Operator Name:** オペレーターの名前。
- **Completed At:** オペレーターが操作を完了した時刻。
- **Login Address:** オペレーターが CVM にログインするために使用する IP アドレス。
- **Target:** 実行する DRX サービス。
- **Result:** 操作結果。
 - **Succeeded-** 操作は成功しました。
 - **Partially Succeeded-** 操作は部分的に成功しました。
 - **Failed—** 操作は失敗しました。

- **Reason:** 操作が失敗した理由。
- **Severity Level:** 操作の重大度レベル。
- **Action Type:** オペレーターが実行するアクションのタイプ。

インテリジェントなリソーススケジュールを管理する

ARM ホストは IRS をサポートしていません。

I インテリジェント リソース スケジューリング (iRS) は、同じクラスター内の異なるホスト上のリソースをリソースグループに追加し、同じサービスを提供する VM を VM グループに追加します。

サービス テンプレートは、物理リソースを使用するためにサービス テンプレートを使用する VM の優先順位と、優先順位の低いサービス テンプレートを使用するすべての VM が使用できるリソースの合計比率を定義します。

VM が起動または再起動すると、CVM は、サービス テンプレートの優先順位、リソースグループのリソース使用率、および同じサービス テンプレートを使用するすべての VM が使用するリソースの合計比率に基づいて、VM にリソースを割り当てます。

現在のソフトウェア バージョンでは、GPU および vGPU の iRS サービスと SR-IOV リソースのみがサポートされています。

iRS サービスを構成する前に、必要に応じてサービス テンプレートを構成します。

機能

- サービステンプレートの管理
- iRS サービスの管理
- iRS サービスで VM 情報を表示する
- iRS サービスに関するパフォーマンス監視情報を表示する
- iRS サービスでリソースの詳細を表示する
- iRS サービスでリソースの使用履歴を表示する

サービステンプレートの管理

サービス テンプレートは、VM がホスト上の物理リソース (GPU など) を使用するためのルールを定義します。CVM は、リソースが不足している場合、サービス テンプレートで定義された優先順位に基づいてリソースを割り当てます。優先順位の高い VM が、対応するリソースを最初に使用できます。

デフォルトでは、事前定義されたノンリニア編集サービス テンプレートとトランスコーディング サービス テンプレートがシステムに存在します。必要に応じて、さらにサービス テンプレートを追加できます。

制限事項とガイドライン

VM で使用されるサービス テンプレートは削除できません。

サービステンプレートを追加する

1. 上部のナビゲーション バーで、**services** をクリックします。
2. 左側のナビゲーション ペインから、**iRS** を選択します。
3. **Service Template** をクリックします。
4. **Add** 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。

サービステンプレートを編集する



1. 上部のナビゲーション バーで、**services** をクリックします。
2. 左側のナビゲーション ペインから、**iRS** を選択します。
3. **サ Service Template** をクリックします。
4. サービス テンプレートの **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。

サービステンプレートを削除する

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

3. **Service Template** をクリックします。
4. サービス テンプレートの **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。

サービステンプレートの詳細を表示する

1. 上部のナビゲーション バーで、**services** をクリックします。
2. 左側のナビゲーション ペインから、**iRS** を選択します。
3. **Service Template** をクリックします。
4. テンプレート リストを更新するには、 アイコンをクリックします。
5. 表示する列を選択するには、 アイコンをクリックします。
6. サービス テンプレートに関する情報を表示するには、テンプレートの **View** をクリックします。

パラメーター

- **Priority:** ホストに VM に割り当てることができるリソースがない場合、CVM はこの優先度に基づいてリソースの割り当てを調整します。優先度の高い VM に最初にリソースを割り当てることができます。優先度の低い VM はプリエンプトされる可能性があります。
- **VM Startup Mode:** GPU または vGPU リソース プールのリソースが不足している場合、リソースが割り当てられていない VM の起動モードを設定できます。オプションには次のものがあります。
 - **Not Start-** 使用可能なリソースがない場合、またはリソース プール内の使用可能なリソースが VM の要件を満たせない場合は、システムは VM を起動しません。
 - **Start Without Resources-** リソース プールに使用可能なリソースがない場合、システムは VM にリソースを割り当てずに VM を起動します。リソース プールで使用可能なリソースが VM の要件を満たせない場合、システムは使用可能なリソースを VM に割り当てて VM を起動します。たとえば、リソース プールで 2 つの GPU が使用可能であるが、VM に 3 つの GPU が必要な場合、システムは VM を起動して 2 つの GPU を VM に割り当てます。
 - **Preempt-** 優先度の高い VM は優先度の低い VM をプリエンプトし、優先度の低い VM に割り当てられているリソースを使用できます。
- **Preemption Threshold:** このしきい値を超えると、VM の起動モードが **Preempt** に設定されている場合、優先度の高い VM は優先度の低い VM をプリエンプトしようとします(パーセント単位)。GPU リソース プールに GPU が 10 個あり、しきい値が 20% (2 GPU) に設定されていて、iRS がサービス テンプレートを使用する VM に 5 GPU (50%) を割り当てているとします。優先度の高い VM が起動しても GPU リソース プールに使用可能なリソースがない場合、優先度の高い VM は優先度の低い VM をプリエンプトしようとします。システム内のすべてのサービス テンプレートで構成されているプリエンプションしきい値の合計は、100%

を超えることはできません。このパラメーターは、VM の起動モードが **Preempt** に設定されている場合に必須です。

- **Service Stop Command:** VM の OS によって実行され、VM 上の iRS で構成されたリソースを解放して、他の VM がリソースを使用できるようにするコマンド (シャットダウンなど)。システムは、このパラメーターが正しく構成されている場合のみ、VM によって使用される GPU/vGPU リソースを解放しようとします。このパラメーターは、VM の起動モードが **Preempt** に設定されている場合に必要です。
- **Return Result:** CVM は、返された結果をこのパラメーターと照合して、停止サービス コマンドが正常に実行されたかどうかを判断します。結果が成功した場合、VM はリソースを解放します。結果が失敗した場合、システムは設定された失敗時のアクションを実行します。このパラメーターは、VM の起動モードが **Preempt** に設定されている場合に必要です。
- **Action upon Failure:** サービスの停止に失敗した場合に実行するアクション。このパラメーターは、VM の起動モードが **Preempt** に設定されている場合に必須です。
 - **Find Next-** システムはリソースを解放するために他の VM のサービスを停止しようとします。
 - **Power Off VM-** システムは現在の VM の電源をオフにしてリソースを解放します。

iRS サービスの管理

iRS サービスを構成して、CVM がサービス テンプレートの優先度、リソース グループのリソース使用量、割り当てられたリソース比率に基づいて VM にリソースを動的に割り当てることができるようにします。

たとえば、VM はホスト上の GPU を直接使用しますが、GPU は一度に 1 つの VM でしか使用できません。VM のホストに利用可能な GPU リソースがない場合、システムは VM を空き GPU リソースがある別のホストに移行します。クラスターの GPU リソースが不足している場合、優先度の高いサービス テンプレートを使用する VM は、GPU リソースの優先度の低いサービス テンプレートを使用する VM よりも優先されます。VM によって使用される GPU リソースの合計比率が低い優先度のサービス テンプレートの使用が指定された割り当て比率を超えると、システムは低い優先度の VM の GPU リソースを再利用して、高い優先度の VM が十分な GPU リソースを使用できるようにします。

制限事項とガイドライン

- iRS サービスの VM のイメージ ファイルは共有ストレージ リソースに保存する必要があり、iRS サービス リソースが属するホストは共有ストレージ リソースをマウントしている必要があります。VM のイメージ ファイルが共有ストレージ リソースに保存されていない場合、VM は VM が属するホストの物理リソースのみを使用できます。
- リソース タイプが vGPU の場合、リソース グループ内の vGPU リソースは同じタイプである必要があります。
- 仮想化された GPU リソースは GPU リソース グループに追加できません。
- VM に複数の CPU を割り当てるには、同じリソース プールから CPU を指定する必要があります。

iRS サービスを追加する

1. 上部のナビゲーション バーで、**services** をクリックします。
2. 左側のナビゲーション ペインから、**iRS** を選択します。
3. **Add iRS Service** 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. **Finish** をクリックします。

iRS サービスを編集する

1. 上部のナビゲーション バーで、**services** をクリックします。
2. 左側のナビゲーション ペインから、**iRS** を選択します。
3. iRS サービスの **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. **Finish** をクリックします。

iRS サービスを削除する

1. 上部のナビゲーション バーで、**services** をクリックします。
2. 左側のナビゲーション ペインから、**iRS** を選択します。
3. iRS サービスの **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。

パラメーター

Basic Info

- **Cluster::** iRS サービスを実行するクラスターの名前を入力します。
- **Resource Type:** リソース タイプを選択します。システムは GPU、vGPU、および SR-IOV のみをサポートします。

Resource Info

- **UUID :** vGPU の UUID。このパラメーターは vGPU でのみ使用できます。
- **Name:** vGPU の名前を入力します。このパラメーターは vGPU でのみ使用できます。

- **Type:** vGPU のタイプを選択します。このパラメーターは vGPU でのみ使用できます。
- **Monitor Interfaces:** vGPU でサポートされるモニター インターフェイスの最大数を指定します。このパラメーターは vGPU でのみ使用できます。
- **Buffer:** vGPU のフレーム キャッシュ サイズを指定します。このパラメーターは vGPU でのみ使用できます。
- **Resolution:** vGPU でサポートされる最大解像度を指定します。このパラメーターは vGPU でのみ使用できます。
- **Slot Number:** リソースのスロット番号。
- **Manufacturer:** リソースの製造元。このパラメーターは GPU でのみ使用できます。
- **Host:** リソースが配置されているホスト。
- **Model:** SR-IOV NIC のモデル。このパラメーターは、リソース タイプが SR-IOV の場合にのみ表示されます。



VM

- **Service Template:** VM で使用されるサービス テンプレート。
- **Host:** VM が存在するホスト。
- **Driver:** VM が使用しているリソースのドライバー タイプ。
- **Exclusive Mode:** VM が指定された GPU/vGPU リソースを排他的に使用できるかどうかを選択します。**Yes** を選択した場合、GPU/vGPU リソースは他の VM では使用できません。この機能は、選択した GPU リソース プールに追加された使用可能な GPU/vGPU リソースがホストにある場合にのみ使用できます。この機能が有効になっているときに VM を移行するには、ターゲット ホストで十分な GPU/vGPU リソースが使用可能であることを確認してください。VM は、vGPU リソースを使用する場合、オンライン移行をサポートします。GPU リソースを使用する VM は、シャットダウンされている場合にのみ移行できます。
- **Resource Count::** VM で使用できる GPU/vGPU リソースの最大数を設定します。値は、リソースプールのタイプと排他モード機能の状態によって異なります。
 - vGPU リソース プールを選択した場合、使用できるのは 1 つだけです。
 - GPU リソース プールを選択し、排他モードが無効になっている場合、値はリソース プール内の単一ホスト上の GPU の最大数になります。たとえば、リソース プールに 3 つのホストがあり、ホストにそれぞれ 3、2、2 個の GPU がある場合、値は 3 になります。
- GPU リソース プールを選択し、排他モードが有効になっている場合、値は VM に接続されているホスト上で使用可能な GPU の数になります。

iRS サービスで VM 情報を表示する

iRS サービスで VM 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、**services** をクリックします。
2. 左側のナビゲーション ペインから、**iRS** を選択します。
3. iRS サービスの名前をクリックします。
4. iRS サービス リストを更新するには、 アイコンをクリックします。
5. 表示する列を選択するには、 アイコンをクリックします。

パラメーター

- **Alias:** VM のエイリアス。
- **State:** VM の状態。
- **CPU Usage:** 過去 1 時間の VM の平均 CPU 使用率。
- **Memory Usage:** 過去 1 時間の VM の平均メモリ使用量。
- **OS :** VM 上で実行されるオペレーティング システム。Windows と Linux のみがサポートされています。デフォルトでは、この列は非表示になっています。
- **Service Template:** iRS サービスで使用されるサービス テンプレート。必要に応じてサービス テンプレートを追加できます。
- **Driver Type:** VM のドライバー タイプ。
- **Slot Number:** VM が使用しているリソースのロット番号。
- **Host:** VM が存在するホスト。
- **Exclusive Mode:** VM が GPU/vGPU リソースを排他的に使用できるかどうか。この機能を有効にすると、VM がシャットダウンしても GPU/vGPU リソースは VM にバインドされます。この機能を無効にすると、VM がシャットダウンした後も GPU/vGPU リソースを解放できます。
- **Resource Count:** VM で使用できる GPU/vGPU リソースの数。

iRS サービスに関するパフォーマンス監視情報を表示する

手順

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

3. iRS サービスの名前をクリックします。
4. **Performance Monitoring** タブをクリックします。

パラメーター

- **Usage:** iRS サービス内の VM の過去 30 分間の GPU/vGPU 使用状況の傾向。横軸は時間、縦軸は GPU/vGPU 使用状況を表します。
- **Video Memory Usage:** iRS サービス内の VM の過去 30 分間の GPU/vGPU ビデオ メモリ使用量の傾向。横軸は時間、縦軸は GPU/vGPU ビデオ メモリ使用量を表します。
- **Encoding Rate:** iRS サービス内の VM の過去 30 分間の GPU/vGPU エンコード レートの傾向。横軸は時間、縦軸は GPU/vGPU エンコード レートを表します。
- **Decoding Rate:** iRS サービス内の VM の過去 30 分間の GPU/vGPU デコード レートの傾向。横軸は時間、縦軸は GPU/vGPU デコード レートを表します。
- **SR-IOV NIC Address:** リソースによって使用される SR-IOV NIC アドレス。このパラメーターは、リソース タイプが SR-IOV の場合にのみ使用できます。
- **Physical NIC :** リソースによって使用される物理 NIC。このパラメーターは、リソース タイプが SR-IOV の場合にのみ使用できます。
- **Physical Interface Model:** リソースで使用される物理 NIC モデル。このパラメーターは、リソース タイプが SR-IOV の場合にのみ使用できます。

iRS サービスでリソースの詳細を表示する

iRS サービスでリソー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、**services** をクリックします。
2. 左側のナビゲーション ペインから、**iRS** を選択します。
3. iRS サービスの名前をクリックします。
4. **Resource Details** タブをクリックします。

パラメーター

- **UUID** : vGPU の UUID。このパラメーターは vGPU でのみ使用できます。
- **Name**: vGPU の名前。このパラメーターは vGPU でのみ使用できます。
- **Type**: vGPU のタイプ。このパラメーターは vGPU でのみ使用できます。
- **Monitor Interfaces**: vGPU でサポートされるモニター インターフェイスの最大数。このパラメーターは vGPU でのみ使用できます。
- **Buffer**: vGPU のフレーム バッファ サイズ。このパラメーターは vGPU でのみ使用できます。
- **Resolution**: vGPU でサポートされる最大解像度。このパラメーターは vGPU でのみ使用できます。
- **Slot Number**: リソースのスロット番号。
- **Manufacturer**: リソースの製造元。このパラメーターは GPU でのみ使用できます。
- **Host**: リソースが配置されているホスト。
- **State**: リソースの状態。
- **VM** : リソースを使用している VM。リソースの状態が **Free** の場合、この列は空になります。

iRS サービスでリソースの使用履歴を表示する

iRS サービスでリソースの使用履歴を表示するには、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、**services** をクリックします。
2. 左側のナビゲーション ペインから、**iRS** を選択します。
3. iRS サービスの名前をクリックします。
4. **Resource Usage History** タブをクリックします。

パラメーター

- **UUID** : vGPU の UUID。このパラメーターは vGPU でのみ使用できます。
- **Name**: vGPU の名前。このパラメーターは vGPU でのみ使用できます。
- **Type**: vGPU のタイプ。このパラメーターは vGPU でのみ使用できます。
- **Monitor Interfaces**: vGPU でサポートされるモニター インターフェイスの最大数。このパラメーターは vGPU でのみ使用できます。
- **Buffer**: vGPU のフレーム バッファ サイズ。このパラメーターは vGPU でのみ使用できます。

- **Resolution:** vGPU でサポートされる最大解像度。このパラメーターは vGPU でのみ使用できます。
- **Slot Number:** リソースのスロット番号。
- **Manufacturer:** リソースの製造元。このパラメーターは GPU でのみ使用できます。
- **SR-IOV NIC Address:** リソースによって使用される SR-IOV NIC アドレス。このパラメーターは、リソース タイプが SR-IOV の場合にのみ使用できます。
- **Physical NIC :** リソースによって使用される物理 NIC。このパラメーターは、リソース タイプが SR-IOV の場合にのみ使用できます。
- **Physical Interface Model:** リソースで使用される物理 NIC モデル。このパラメーターは、リソース タイプが SR-IOV の場合にのみ使用できます。
- **Host:** リソースが配置されているホスト。
- **VM :** リソースを使用している VM。リソースの状態が **Free** の場合、この列は空になります。
- **Start Time:** VM がリソースの使用を開始した時刻。
- **End Time:** VM がリソースの使用を停止した時刻。

災害復旧の管理

災害復旧管理 (DRM) は、異なるサイト間でのサービス復旧を提供します。CVM サイトを保護サイトとして構成し、保護サイトの復旧サイトを構成し、保護サイトと復旧サイトを保護グループに追加できます。保護サイトがサービスの提供を停止すると、構成された復旧計画とポリシーに基づいて復旧サイトが引き継ぎ、中断のないサービスを保証します。

CAS は、ストレージ レプリケーションの障害復旧を提供します。ストレージ レプリケーションの障害復旧は、アレイベースのレプリケーションを利用して、異なるサイト間でサービスのバックアップと復旧を提供します。保護されたサイトと復旧サイトの両方がストレージ レプリケーション アダプタ (SRA) をサポートしている場合、自動サービス復旧を実行できます。サイトのストレージ アレイが SRA をサポートしていない場合は、サイト間でサービスを切り替える前に、ストレージ環境を手動で準備する必要があります。ベストプラクティスとして、SRA をサポートするストレージ アレイを使用します。

制限事項とガイドライン

- 災害復旧では IPv6 ホストまたは vSwitch はサポートされません。
- 暗号化されたディスクを使用する VM は、ストレージ レプリケーションの災害復旧をサポートしません。
- SRA をサポートしていないストレージ アレイを使用してストレージ レプリケーション ディザスタ リカバリを実行し、保護ストレージ プールとリカバリ ストレージ プールで異なる名前が使用されている場合、リカバリ ストレージ プールはイメージ チェーンの関係性を処理できない可能性があります。その結果、システムはリカバリ サイトの VM の外部スナップショット イメージ チェーンを再構築できない可能性があります。

機能

- サイトの管理
- 保護グループの管理
- 復旧計画を管理する

サイトの管理

保護サイトとバックアップ サイトのストレージ アレイが SRA をサポートしている場合は、サイトのストレージ アレイ マネージャーを構成する必要があります。サイトとストレージ アレイ マネージャーを追加したら、ストレージ レプリケーション情報を同期します。1 つのサイトのコンソールからサイト回復設定を構成し、他のサイトに同期することができます。

制限事項とガイドライン

- オペレーターのアイドル タイムアウトが 0 で、パスワードの有効期間が 0 でない場合は、災害復旧の失敗を回避するために、パスワードを適時に確認して変更してください。パスワードの有効期限が切れている場合は、管理インターフェイスで新しいパスワードを設定し、それに応じてサイト パスワードを変更してください。
- システム管理者グループのメンバーでないユーザーは、サイトを追加または構成することはできません。
- サイトが設定されている CVM は、別の CVM のリモート サイトとして設定することはできません。
- 保護グループにバインドされているサイトは削除できません。
- サイトに対応するストレージ アレイが SRA をサポートしていない場合、ストレージ アレイ マネージャーは必要ありません。
- サイト上の CVK ホストがストレージ アレイ マネージャーにアクセスできない場合、接続テストは失敗します。
- マッピングが構成されたデバイスを持つストレージ アレイ マネージャーは変更できません。

サイトを追加する

1. 上部のナビゲーション バーで、**services** をクリックします。
2. 左側のナビゲーション ペインから、**Disaster Recovery Management > Sites** を選択します。
3. **Add Site** 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。

サイトを編集する

1. 上部のナビゲーション バーで、**services** をクリックします。
2. 左側のナビゲーション ペインから、**Disaster Recovery Management > Sites** を選択します。
3. サイトの **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。

サイトを削除する

1. 上部のナビゲーション バーで、**services** をクリックします。
2. 左側のナビゲーション ペインから、**Disaster Recovery Management > Sites** を選択します。
3. サイトの **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。

ストレージレイマネージャーを追加する

1. 上部のナビゲーション バーで、**services** をクリックします。
2. 左側のナビゲーション ペインから、**Disaster Recovery Management > Sites** を選択します。
3. サイトを選択し、**Add Storage Array Manager** 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. **Connectivity Test.** をクリックします。
6. OK をクリックします。

ストレージレイマネージャーを編集する

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

3. サイトを選択し、ストレージ アレイ マネージャーを選択して、マネージャーの **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. **Connectivity Test** をクリックします。
6. **OK** をクリックします。

ストレージアレイマネージャーを削除する

1. 上部のナビゲーション バーで、**services** をクリックします。
2. 左側のナビゲーション ペインから、**Disaster Recovery Management > Sites** を選択します。
3. サイトを選択し、ストレージ アレイ マネージャーを選択して、マネージャーの **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。

ストレージレプリケーション情報を同期する

1. 上部のナビゲーション バーで、**services** をクリックします。
2. 左側のナビゲーション ペインから、**Disaster Recovery Management > Sites** を選択します。
3. **Synchronize Storage Replication** 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。

ストレージレプリケーション情報を表示する

1. 上部のナビゲーション バーで、**services** をクリックします。
2. 左側のナビゲーション ペインから、**Disaster Recovery Management > Sites** を選択します。
3. サイトを選択し、ストレージ アレイ マネージャーを選択して、マネージャーの **Actions** 列で **View** をクリックします。

パラメーター

サイト情報

- **Site Name:** サイトの名前を入力します。

- **Site Type:** サイトタイプを選択します。オプションには、**Local** と **Remote** があります。**Local:** 現在の CVM。**Remote:** その他の CVM。最初に追加されたサイトはローカル サイトであり、後続のサイトはリモート サイトです。
- **IP:** サイトの IP アドレスを指定します。
- **Login Method:** サイトへのログインに使用されるプロトコル (HTTP または HTTPS)。
- **Port:** サイトへのログインに使用するポート番号。ポート番号は、HTTP の場合は 8080、HTTPS の場合は 8443 です。
- **Username:** Web ページ経由でサイトに接続するために使用するユーザー名を入力します。サイトタイプをローカルに設定した場合、ユーザー名は必要ありません。ログインしているユーザーのユーザー名が使用されます。
- **Password:** Web ページ経由でサイトに接続するために使用するパスワードを入力します。サイトの種類をローカルに設定した場合、パスワードは必要ありません。ログインしているユーザーのパスワードが使用されます。
- **Manufacturer:** ストレージ アレイの製造元を選択します。

Storage array 情報

- **Name:** ストレージ アレイ マネージャーの名前を入力します。
- **Local Storage Array IP:** ローカル サイトで使用されるストレージ アレイの IP アドレスを指定します。
- **Local Username:** ローカル サイトに接続されているストレージ アレイ マネージャーにアクセスするためのユーザー名を入力します。
- **Local Password:** ローカル サイトに接続されたストレージ アレイ マネージャ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。
- **Remote Storage Array IP:** ローカル サイトで使用されるストレージ アレイとのレプリケーション関係を確立したリモート ストレージ アレイの IP アドレスを指定します。
- **Remote Username:** リモート ストレージ アレイ マネージャーにアクセスするためのユーザー名を入力します。
- **Remote Password:** リモート ストレージ アレイ マネージャ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。

Storage replication 情報

- **Local LUN:** ローカル ストレージ LUN の名前。
- **Replication Direction:** LUN のレプリケーション方向。
- **Remote LUN:** リモート ストレージ LUN の名前。
- **Remote Storage:** リモート LUN が存在するストレージ アレイ マネージャーの名前。

保護グループの管理

保護グループは、VM または物理デバイスのセットを保護します。ストレージ レプリケーション保護グループを作成できます。保護ポリシーに基づいて、同じストレージ プール (ストレージ アレイ内の LUN) に接続された VM を保護グループに割り当てます。障害が発生すると、アレイベースのレプリケーションを通じて、ローカルストレージ アレイ内の LUN に保存されている VM データがリモート ストレージ アレイ内の LUN にレプリケートされます。

保護グループを作成するときは、保護サイトと回復サイトを保護グループに関連付け、サイトのホスト プールを指定し、リソース マッピング関係を構成する必要があります。

リソース マッピング関係は、保護されたサイト内の保護された VM によって使用されるリソースを、リカバリ サイトのソースに関連付けます。リカバリ サイトで VM がリカバリされると、それらが使用するリソースはリカバリ サイトのリソースに自動的に置き換えられます。vSwitch マッピング、ポート プロファイル マッピング、およびストレージ マッピングを作成できます。CVM が 2 つの LUN 間でデータを複製するには、ストレージ マッピングでそれらを指定します。

制限事項とガイドライン

- ストレージ レプリケーション保護グループ内の VM は、**Storage** および **Host and Storage** の移行タイプをサポートしていません。
- 災害復旧クライアントとともにインストールされた VM をテンプレートに複製または変換する前に、災害復旧クライアントのインストール パスにあるファイル **AentSystemInfo.ini** を削除します。

機能

- 保護グループを作成する
- 保護グループを編集する
- 保護グループを削除する
- 保護グループのリソース マッピング関係を編集する
- 保護グループに VM を追加する
- 保護グループから VM を削除する
- 保護グループを同期する
- 保護グループ内の VM を同期する

保護グループを作成する

制限事項とガイドライン

- CD-ROM またはフロッピー ドライブを備えた VM は保護グループに追加できません。このような VM を保護グループに追加するには、VM から CD-ROM およびフロッピー ドライブをマウント解除します。
- 保護された運用ノードのディスクを拡張または追加するには、まず運用ノードを保護グループから削除する必要があります。ディスクの拡張が完了したら、拡張または追加されたディスクをシステムがバックアップできるように、運用ノードを保護グループに再割り当てします。
- ストレージ レプリケーション保護グループを構成するときは、次の制限とガイドラインに従ってください。
 - ストレージ レプリケーション保護グループには、少なくとも 1 つのストレージ マッピング、1 つの vSwitch マッピング、および 1 つのポート プロファイル マッピングを構成する必要があります。
 - Nimble ストレージのストレージ マッピングを構成する場合は、ストレージ レプリケーショングループ内のすべてのストレージ ボリュームを保護グループに追加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、**services** をクリックします。
2. 左側のナビゲーション ペインから、**Disaster Recovery Management > Protection 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、**Next** をクリックします。
5. ストレージ マッピングを追加するには:
 - a. **Add Storage Mapping Relation** をクリックします。
 - b. 開いたダイアログ ボックスで、ストレージの種類、製造元、ストレージ プールの種類を選択し、**Next** をクリックします。
 - c. 保護サイトとリカバリ サイトがそれぞれ存在するストレージ ボリュームを選択します。または、ストレージ アレイ内のストレージ ボリュームを選択します。**OK** をクリックします。
6. vSwitch マッピングを追加するには:
 - a. **Add vSwitch Mapping Relation** をクリックします。
 - b. 開いたダイアログ ボックスで、保護されたサイトの vSwitch とリカバリ サイトの vSwitch を選択し、**OK** をクリックします。
7. ポート プロファイル マッピングを追加するには:
 - a. **Add Profile Mapping Relation** をクリックします。
 - b. 開いたダイアログ ボックスで、保護されたサイトのポート プロファイルと回復サイトのポート プロファイルを選択し、**OK** をクリックします。
8. **Finish** をクリックします。

パラメーター

ストレージレプリケーション保護グループ

基本情報

- **Disaster Recovery Type:** 災害復旧タイプとして **Name:** 保護グループの名前を入力します。名前は CVM 内で一意である必要があります。
- **Protected Site:** クリックして、保護グループに関連付ける保護されたサイトを選択します。
- **Recovery Site:** クリックして、保護グループに関連付けるリカバリ サイトを選択します。
- **Original Host Pool:** クリックして、保護されたサイトのホスト プールを選択します。
- **Target Host Pool:** クリックして、リカバリ サイトのホスト プールを選択します。
- **Service Type:** 保護グループ内の VM または運用ノードのサービス タイプを選択します。
 - **CAS SRM** - CAS によって管理される VM のみを保護します。
 - **SRM As a Service** - CloudOS によって組み込まれた VM を保護します。
- **Auto VM Protection:** VM が次の要件を満たしている場合、VM は自動的に保護グループに追加されます。
 - これは、DRX 高速展開、DRX 高速クローン、またはフローティング デスクトップ プールを通じて作成されたものではなく、固定デスクトップ プールを通じて展開された保護モードの VM でもありません。
 - VM が使用するストレージ プール、vSwitch、およびポート プロファイルは、保護グループに属します。
 - 保護グループ内に同じ名前の VM が存在しません。
 - VM は、USB デバイス、PCI デバイス、パススルー NIC、TPM デバイス、光学ドライブ、またはフロッピー ドライブを使用せず、物理 CPU にバインドされません。

マッピング関係

Mapping Relationship: 対応するアイコンをドラッグして、ストレージ マッピング、vSwitch マッピング、またはポート プロファイル マッピングを追加します。

ストレージ マッピングの場合は、次のパラメーターを構成します。

Storage Type: ストレージタイプを選択します。

Vendo: SRA ストレージのみのベンダーを選択します。

Storage Pool Type: ストレージ プール タイプを選択します。SRA をサポートしていないストレージ アレイの場合は、共有ファイル システム マッピングのみを作成できます。SRA をサポートするストレージ アレイの場合は、共有ファイル システム マッピングとブロック デバイス マッピングを作成できます。

Select Device: SRA ストレージの場合は、ストレージ レプリケーション グループ内のストレージ ボリュームを選択します。非 SRA ストレージの場合は、保護サイトとリカバリ サイトのストレージ リソースを選択します。

保護グループを編集する

制限事項とガイドライン

保護グループの説明とリソース マッピング関係を編集できます。

手順

1. 上部のナビゲーション バーで、**services** をクリックします。
2. 左側のナビゲーション ペインから、**Disaster Recovery Management > Protection Groups** を選択します。
3. 保護グループの **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、**Next** をクリックします。
5. **Finish.**をクリックします。

保護グループを削除する

制限事項とガイドライン

保護グループは、関連付けられている回復計画が実行されていない場合にのみ削除できます。

手順

1. 上部のナビゲーション バーで、**services** をクリックします。
2. 左側のナビゲーション ペインから、**Disaster Recovery Management > Protection Groups** を選択します。
3. 保護グループの **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。

保護グループのリソース マッピング関係を編集する

1. 上部のナビゲーション バーで、**services** をクリックします。
2. 左側のナビゲーション ペインから、**Disaster Recovery Management > Protection Groups** を選択します。
3. 保護グループの **Actions** 列で **Disaster Recovery Management > Protection Groups** をクリックします。
4. リソース マッピング関係を追加するには、**Add Storage Mapping Relation**, **Add vSwitch Mapping Relation**, または **Add Profile Mapping Relation** をクリックします。
5. リソース マッピング関係を削除するには、リソース マッピング関係を右クリックし、ショートカット メニューから **Delete** を選択します。

保護グループにVMを追加する

制限事項とガイドライン

実稼働環境で保護グループ内の VM の構成を編集すると、テスト リカバリまたは障害リカバリ タスクを実行すると VM の起動が失敗します。必要な場合を除き、実稼働環境で保護グループ内の VM の構成を編集しないでください。特に、VM に vNIC やディスクを追加するなどのハードウェア操作は実行しないでください。保護グループ内の VM を編集する必要がある場合は、まずその VM をグループから削除してください。構成が有効になったら、VM を保護グループに再度追加してください。

手順

1. 上部のナビゲーション バーで、**services** をクリックします。
2. 左側のナビゲーション ペインから、**Disaster Recovery Management > Protection Groups** を選択します。
3. 保護グループをクリックします。保護グループ内の VM が **VMs Under Protection** 領域に表示されます。
4. **Add VM** をクリックします。
5. VM を選択し、**OK** をクリックします。
6. **OK** をクリックします。

パラメーター

VM を選択

- **IP Address:** VM の IP アドレス。

保護グループからVMを削除する

制限事項とガイドライン

デュアルノードまたはクラスター保護グループ内の運用ノードは削除できません。

手順

1. 上部のナビゲーション バーで、**services** をクリックします。
2. 左側のナビゲーション ペインから、**災 Disaster Recovery Management > Protection Groups** を選択します。
3. 保護グループをクリックします。保護グループ内の VM が 保護対象の VM 領域に表示されます。
4. VM の **Actions** 列で **Delete** をクリックするか、対象の VM を選択して VM の削除 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。

保護グループを同期する

システムは、VM の追加や削除、グループの説明の変更など、保護グループの変更をリカバリ サイトに自動的に同期します。ネットワーク障害などの障害によりシステムがグループ情報を同期できない場合は、このタスクを実行して、保護グループの変更をリカバリ サイトに手動で同期できます。

制限事項とガイドライン

- 保護グループは、リカバリ サイトが通常の状態にあり、保護グループのリカバリ プランが準備完了または初期化済みの状態にある場合にのみ同期できます。
- 保護グループを同期すると、保護グループ内の VM も同期されます。

手順

1. 上部のナビゲーション バーで、**services** をクリックします。
2. 左側のナビゲーション ペインから、**Disaster Recovery Management > Protection Groups** を選択します。
3. 保護グループの **Actions** 列で **Synchronize** 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。

保護グループ内のVMを同期する

システムは、VM NIC の追加や変更などの VM フレーバーの変更をリカバリ サイトに自動的に同期します。ネットワーク障害などの障害によりシステムが VM 情報を同期できない場合は、このタスクを実行して、VM フレーバーの変更をリカバリ サイトに手動で同期できます。

制限事項とガイドライン

VM は、リカバリ サイトが通常の状態にあり、保護グループのリカバリ プランが準備完了または初期化済みの状態にある場合にのみ同期できます。

手順

1. 上部のナビゲーション バーで、**services** をクリックします。
2. 左側のナビゲーション ペインから、**Disaster Recovery Management > Protection Groups** を選択します。
3. 保護グループをクリックします。保護グループ内の VM が **保 VMs Under Protection** 領域に表示されます。
4. VM の **Actions** 列で **Synchronize** をクリックするか、1 つまたは複数の VM を選択して **Synchronize VMs in Group** 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。

復旧計画を管理する

リカバリ プランには、保護グループ内の VM をリカバリするための一連のポリシーが含まれています。

制限事項とガイドライン

- CAS は、最大 5 つのストレージ レプリケーション リカバリ プランを同時に実行できます。
- ストレージ レプリケーション復旧プランから復旧された VM では、削除、移行、クローン作成、バックアップ、テンプレート変換、OVF テンプレートのエクスポート、ハードウェアの追加または削除はサポートされません。

機能

- 復旧計画を追加する
- 復旧計画を編集する
- 復旧計画を削除する
- 復旧計画を実行する
- 復旧計画の概要を表示する
- 復旧タスクの詳細を表示する

復旧計画を追加する

リカバリ プランを追加するには、このタスクを実行します。

制限事項とガイドライン

保護グループは、VM が含まれている場合にのみ、リカバリ プランにバインドできます。

手順

1. 上部のナビゲーション バーで、**services** をクリックします。
2. 左側のナビゲーション ペインから、**Disaster Recovery Management > Recovery Plans** を選択します。
3. **Add Recovery Plan** をクリックします。
4. 名前と説明を入力し、保護グループとクラスターを選択します。
5. **OK** をクリックします。

パラメーター

- **Protection Group:** 回復計画がバインドされる保護グループを選択します。
- **Cluster:** 保護グループ内の VM を追加するクラスター (リカバリ サイト内) を選択します。
- **Shared Storage:** 保護グループのストレージ マッピングで構成されているローカル共有ストレージに関する情報。

復旧計画を編集する

リカバリ プランを編集するには、このタスクを実行します。

制限事項とガイドライン

Start Testing, Stop Testing, Scheduled Recovery, Failure Recovery, または Reverse Recovery の状態にあるリカバリ プランは変更できません。

手順

1. 上部のナビゲーション バーで、**services** をクリックします。
2. 左側のナビゲーション ペインから、**災 Disaster Recovery Management > Recovery Plans** を選択します。
3. リカバリ プランの **Actions** 列で **Edit** をクリックします。
4. 説明を編集し、必要に応じて保護グループ、クラスター、および運用ノードを選択します。
5. **OK** をクリックします。

パラメーター

- **Protection Group:** 回復計画がバインドされる保護グループを選択します。
- **Cluster:** 保護グループ内の VM を追加するクラスター (リカバリ サイト内) を選択します。

復旧計画を削除する

リカバリ プランを削除するには、このタスクを実行します。

制限事項とガイドライン

Start Testing, Stop Testing, Scheduled Recovery, Failure Recovery, または Reverse Recovery の状態にあるリカバリ プランは削除できません。

手順

1. 上部のナビゲーション バーで、**services** をクリックします。
2. 左側のナビゲーション ペインから、**Disaster Recovery Management > Recovery Plans** を選択します。
3. リカバリ プランの **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。

復旧計画を実行する

CVM は、次のリカバリ プラン実行オプションを提供します。

- **Testing recovery plans** ト- 保護サイトの障害時にリカバリ サイトでサービスをリカバリするプロセスをシミュレートして、リカバリ プランの正確さを確認します。テストは保護サイトによって提供されるサービスには影響せず、手動で開始および停止します。
- **Executing scheduled recovery**- 両方のサイトが正常に動作している場合、保護サイト内の保護された VM をシャットダウンし、メンテナンスのためにそのデータをリカバリ サイトに複製します。データ レプリケーションが完了すると、VM が起動します。
- **Executing failure recovery**- 保護サイトに障害が発生した場合に、回復サイトで保護された VM を回復します。この操作では、VM のデータが最後のデータ レプリケーションからのものであるため、保護された VM を障害発生時とまったく同じ状態に復元することはできません。
- **Executing reverse recovery**- 保護サイトがデータ損失なしでリカバリされたときに、リカバリ サイト内の保護された VM を元の保護サイトに復元します。リカバリ サイトの VM はシャットダウンされ、ストレージ デバイスは VM からアンマウントされ、VM は使用できません。このオプションは、ストレージ レプリケーション保護グループに適用されます。
- **Executing reverse replication**- スケジュールされたリカバリまたは障害リカバリが正常に実行された後、リカバリ サイトでリバース レプリケーションを実行して、ストレージ レプリケーション保護グループの保護サイトの役割とリカバリ サイトの役割を交換します。

制限事項とガイドライン

- 使用するリカバリ プランが **Ready** または **Initialize** 状態であることを確認します。
- 非保護グループ内のアクティブな VM が保護グループ ストレージ内の CD-ROM ファイルを参照する場合、スケジュールされたリカバリまたはリバース リカバリは失敗します。
- リバース レプリケーションを実行するには、保護されたサイトとリカバリ サイトのストレージ アレイ マネージャーがレプリケーション情報を同期できることを確認します。リバース レプリケーションは並列実行をサポートしていません。
- VM が複数のストレージ プールのストレージ リソースを使用する場合、基礎となるストレージ ボリュームはレプリケーション期間中にアトミック性を維持できない可能性があります。複数のストレージ プールのデータ レプリケーション中に障害回復を実行すると、VM の構成ファイルがストレージ側の構成ファイルと一致なくなり、VM が誤って定義されて回復サイトで起動される可能性があります。
- VM は同時にリカバリされ、特定の順序で起動されるわけではありません。VM の起動中に特定の VM を優先するには、それらの VM を保護グループに割り当て、関連するリカバリ プランを他のリカバリ プランよりも先に実行します。

復旧計画をテストする

1. 上部のナビゲーション バーで、**services** をクリックします。
2. 左側のナビゲーション ペインから、**Disaster Recovery Management > Recovery Plans** を選択します。
3. 回復計画の名前をクリックします。
4. リカバリ プランの **Actions** 列で **Start Testing** をクリックします。
5. 開いたダイアログ ボックスで実行モードを選択し、**OK** をクリックします。
6. テストの詳細を表示するには、**Recovery Tasks** タブをクリックし、回復タスクの実行時間リンクをクリックします。
7. テストが成功した後にテストを停止するには、リカバリ プランの概要ページで **Stop Testing** をクリックします。

スケジュールされたリカバリを実行する

1. 上部のナビゲーション バーで、**services** をクリックします。
2. 左側のナビゲーション ペインから、**Disaster Recovery Management > Recovery Plans** を選択します。
3. 回復計画の名前をクリックします。

4. **Scheduled Recovery** をクリックします。
5. 開いたダイアログ ボックスで実行モードを選択し、**OK** をクリックします。実行モードの詳細については、『パラメーター』を参照してください。

スケジュールされたリカバリを一括で実行する

1. 上部のナビゲーション バーで、**services** をクリックします。
2. 左側のナビゲーション ペインから、災 **Disaster Recovery Management > Recovery Plans** を選択します。
3. 対象のリカバリ プランを選択し、**Bulk Operation** をクリックして、**Scheduled Recovery** 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。

障害回復を実行する

1. 上部のナビゲーション バーで、**services** をクリックします。
2. 左側のナビゲーション ペインから、**Disaster Recovery Management > Recovery Plans** を選択します。
3. 回復計画の名前をクリックします。
4. **Failure Recovery** をクリックします。
5. 開いたダイアログ ボックスで実行モードを選択し、**OK** をクリックします。実行モードの詳細については、『パラメーター』を参照してください。

障害回復を一括で実行する

1. 上部のナビゲーション バーで、**services** をクリックします。
2. 左側のナビゲーション ペインから、**Disaster Recovery Management > Recovery Plans** を選択します。
3. 対象のリカバリ プランを選択し、**Bulk Operation** をクリックして、**Failure Recovery** 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。

リバースリカバリを実行する

1. 上部のナビゲーション バーで、**services** をクリックします。
2. 左側のナビゲーション ペインから、**Disaster Recovery Management > Recovery Plans** を選択します。
3. 回復計画の名前をクリックします。
4. **Reverse Recovery** をクリックします。
5. 開いたダイアログ ボックスで実行モードを選択し、**OK** をクリックします。実行モードの詳細については、『パラメーター』を参照してください。

逆レプリケーションを実行する

1. 上部のナビゲーション バーで、**services** をクリックします。
2. 左側のナビゲーション ペインから、**Disaster Recovery Management > Recovery Plans** を選択します。
3. 回復計画の名前をクリックします。
4. **Reverse Replication** をクリックします。
5. クラスタを選択します。
6. **OK** をクリックします。

リバースリカバリを実行する

1. 上部のナビゲーション バーで、**services** をクリックします。
2. 左側のナビゲーション ペインから、**Disaster Recovery Management > Recovery Plans** を選択します。
3. 対象のリカバリ プランを選択し、**Bulk Operation** をクリックして、**Reverse Recovery** 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。

パラメーター

- **Execution Mode:** ストレージ レプリケーション保護グループのリカバリ プランの実行モードを選択します。
- **Execute Plan:** 回復手順に従って回復計画を実行するには、このオプションを選択します。
 - **Restore VM:** VM を直接復元するには、このオプションを選択します。このモードは時間を節約し、VM の復元前にリカバリ プランのすべての手順が準備されている状況に適用できます。

復旧計画の概要を表示する

リカバリ プランの概要を表示するには、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、**services** をクリックします。
2. 左側のナビゲーション ペインから、**Disaster Recovery Management > Recovery Plans** を選択します。
3. 回復計画の名前をクリックします。

パラメーター

Basic Attributes

- **Protection Group:** リカバリ プランがバインドされている保護グループ。
- **Protection Site:** 保護グループに構成された保護サイトの名前。
- **Recovery Site:** 保護グループ用に構成されたリカバリ サイトの名前。
- **Cluster:** 保護グループ内の VM が追加されるクラスター (リカバリ サイト内)。
- **State:** リカバリ計画またはテストまたはリカバリ結果の状態。

VMs Under Protection

- **Alias:** VM のエイリアス。
- **Recovery State:** VM の初期状態、またはリカバリ プランが実行された後の VM の状態。

Shared Storages

- **Shared Storages:** 保護グループのストレージ マッピングで構成されているローカル共有ストレージに関する情報。

復旧タスクの詳細を表示する

リカバリ プランの詳細を表示するには、このタスクを実行します。

制限事項とガイドライン

- リカバリ プランの状態をクリックすると、最新のリカバリ タスクの詳細ページが表示されます。
- スケジュールされたリカバリ タスクまたはフェールオーバー リカバリ タスクが失敗した場合は、VM 名の右側にある **Restore VM** をクリックして、VM を直接復元できます。

手順

1. 上部のナビゲーション バーで、**services** をクリックします。
2. 左側のナビゲーション ペインから、**Disaster Recovery Management > Recovery Plans** を選択します。
3. 回復計画の名前をクリックします。
4. **Recovery Tasks** タブをクリックします。
5. 回復タスクの実行時間リンクをクリックします。

パラメーター

- **Recovery Steps:** 回復手順に関する詳細情報。
- **State:** 各回復ステップの状態。
- **Reason:** 各回復手順の失敗理由。

クラウドレインボーを管理する

Cloud Rainbow を使用すると、サービス中断なしでデータセンター間で CVM リソースの共有と手動の VM 移行が可能になります。

Cloud Rainbow のレート制限機能を使用するには、vSwitch に移行ネットワークを追加し、帯域幅比率を設定します。詳細については、『サブネットの管理』を参照してください。



前提条件

- VM 移行のソース ホストとターゲット ホストは、クラスターに参加するために同じ IP プロトコル バージョンの IP アドレスを使用する必要があります。
- データ キャッシュ モードが None または Directsync で、ディスクが NFS にある VM の移行を正常に行うには、移行前に VM をシャットダウンします。

制限事項とガイドライン

- CVM 間で VM を移行する場合、移行先 CVM のバージョンが移行元 CVM のバージョンよりも低い場合、VM の CAStools バージョンは変更されません。これは機能には影響しないため、何もする必要はありません。
- CVM 間の VM 移行中は、ホストを CVM に接続しないでください。
- 暗号化されたディスクを使用する VM は、クラウド レインボー ベースのオンライン移行をサポートしません。


CVMを追加する

1. 上部のナビゲーション バーで、**services** をクリックします。
2. 左側のナビゲーション ペインから、**Cloud Rainbow** を選択します。
3. ページの右側にある  アイコンをクリックします。
4. **OK** をクリックします。
5. ローカル データ センター名と IP アドレスを入力し、ログイン モード (HTTP または HTTPS) を選択し、ポート番号を入力して、**OK** をクリックします。
6. ページの右側にある  アイコンをクリックします。
7. データセンター名、説明、IP アドレスを入力し、ログイン モード (HTTP または HTTPS) を選択し、デフォルトのポート番号とユーザー名とパスワードを入力します。
8. **OK** をクリックします。

CVMを編集する

1. 上部のナビゲーション バーで、**services** をクリックします。
2. 左側のナビゲーション ペインから、**Cloud Rainbow** を選択します。
3. CVM については、 アイコンをクリックしてください。
4. **データセンターの構成** 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。




CVMを削除する

1. 上部のナビゲーション バーで、**services** をクリックします。
2. 左側のナビゲーション ペインから、**Cloud Rainbow** を選択します。
3. CVM の  アイコンをクリックします。
4. 開いたダイアログボックスで、**OK** をクリックします。

CVM間でVMを移行する

1. 上部のナビゲーション バーで、**services** をクリックします。
2. 左側のナビゲーション ペインから、**Cloud Rainbow** を選択します。
3. ターゲット VM の名前を入力して **Enter** キーを押すか、ホストをダブルクリックします。ホスト上のすべての VM が表示されます。
4. VM をターゲット ホストにドラッグします。
5. 開いたダイアログ ボックスで、『パラメーター』の説明に従ってパラメーターを設定し、**Next** をクリックします。
6. **OK** をクリックします。

パラメーター

- **Data Center Node:**  をクリックすると CVM に関する情報が表示されます。
- **Cluster Node:**  をクリックするとクラスターに関する情報が表示されます。
- **Host Node:**  をクリックするとホストに関する情報が表示されます。
- **Timeout:** 実行中の VM を移行するための移行タイムアウトを入力します。たとえば、移行タイムアウトは 20 分に設定されます。VM を 20 分以内に移行できない場合、システムは VM を一時停止し、移行後に VM を復元します。このパラメーターを 0 に設定すると、システムは移行中に VM を一時停止しません。
- **Compress:** 送信するデータを圧縮するには、このオプションを選択します。

異機種間の移行を管理する

ARM ホストは異種移行をサポートしていません。

異機種間移行により、x86 サーバーまたは VM 上のデータを CAS VM に移行できます。移行クライアントがインストールされた物理サーバーまたは VM をソース デバイスとして使用し、デバイス上のデータを、P2V または V2V 移行用の適切な移行クライアントで構成された CAS VM に移行します。

制限事項とガイドライン

異機種間の移行では IPv6 はサポートされません。

Windows オペレーティング システムを使用するソース デバイスから移行クライアントをアンインストールした後 (移行前または移行後)、ソース デバイスを再起動する必要があります。再起動によって実行中のサービスに影響が及ばないことを確認してください。

機能

- 移行タスクの管理
- ドライバーを構成する
- 異機種移行の概要情報を表示する
- ソースデバイスを表示
- 宛先 VM を表示する
- 移行クライアントをダウンロードして設定する

移行タスクの管理

移行タスクは次のように管理できます。

- 単一のタスクを作成するか、複数のタスクを一括で作成します。
- タスクの作成後すぐに移行タスクを開始するか、タスクを保存してから必要に応じて特定の時間にタスクを開始します。
- タスクの作成後に、移行タスクを開始、一時停止、終了、または削除します。

制限事項とガイドライン

- 移行タスクでは、ライセンスされたデバイスのみをソース デバイスとして指定できます。ライセンスされたソース デバイスは、移行タスクを通じて複数回移行できます。ライセンスされたソース デバイスを使用して、複数の移行タスクを作成できます。
- 移行タスクが保存または開始されると、移行ライセンスはタスク内のソース デバイスに付与され、取り消すことはできません。システムがデバイスの移行タスクの作成に失敗しても、ソース デバイスは移行ライセンスを解放しません。この状況では、ソース デバイスの移行タスクを再度作成してください。
- 移行タスクは、デフォルトではソース デバイスの名前と同じ名前が付けられます。
- 移行タスクが完了したら、**Finish** ボタンをクリックする必要があります。**Finish** をクリックしないと、システムは設定された間隔で自動増分移行を自動的に実行します。
- 移行タスクの進行状況は、スケジュールされたサンプリングによって計算されます。移行タスクに複数のディスクが関係する場合、システムは全体のタスク進行状況を時間内に更新できない可能性があります。デバイス情報で各ディスクの移行状態を表示して、タスクの進行状況を監視できます。

移行タスクを作成する

1. 上部のナビゲーション バーで、**services** をクリックします。
2. 左側のナビゲーション ペインから、**Heterogeneous Migration** を選択します。
3. **Create Migration Task** をクリックします。
4. ソース デバイス、ターゲット VM を選択し、各ソース ディスクに一致するディスクを選択して、**Next** をクリックします。複数の移行タスクを作成するには、**Add Migration Task** をクリックしてタスクを追加し、タスクを構成して、**Next** 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. 移行タスクをすぐに開始するには、**Start** をクリックします。移行タスクを特定の時間に開始するには、**Save** をクリックしてタスクを移行タスク リストに保存し、必要に応じて特定の時間にタスクを開始します。

移行タスクを開始する

1. 上部のナビゲーション バーで、**services** をクリックします。
2. 左側のナビゲーション ペインから、**Heterogeneous Migration** を選択します。
3. **Migration Tasks** タブをクリックします。
4. 移行タスクを選択し、タスクの **Actions** 列で **Start** をクリックし、表示されるダイアログ ボックスで **OK** をクリックします。

移行タスクを一時停止する

1. 上部のナビゲーション バーで、**services** をクリックします。
2. 左側のナビゲーション ペインから、**Heterogeneous Migration** を選択します。
3. **Migration Tasks** タブをクリックします。
4. 移行タスクを選択し、タスクの **Actions** 列で **Suspend** をクリックし、表示されるダイアログ ボックスで **OK** をクリックします。

移行タスクを完了する

1. 上部のナビゲーション バーで、**services** をクリックします。
2. 左側のナビゲーション ペインから、**Heterogeneous Migration** を選択します。
3. **Migration Tasks** タブをクリックします。
4. 移行タスクを選択し、タスクの **Actions** 列で **Finish** をクリックし、表示されるダイアログ ボックスで **OK** をクリックします。

移行タスクを削除する

1. 上部のナビゲーション バーで、**services** をクリックします。
2. 左側のナビゲーション ペインから、**Heterogeneous Migration** を選択します。
3. **Migration Tasks** タブをクリックします。
4. タスクの **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。


移行タスクの詳細を表示する

1. 上部のナビゲーション バーで、**services** をクリックします。
2. 左側のナビゲーション ペインから、**Heterogeneous Migration** を選択します。
3. **Migration Tasks** タブをクリックします。
4. ソースデバイスの名前をクリックします。

移行タスクの表示

このタスクを実行して、すべての移行タスクを表示し、移行タスクを開始、終了、または復元します。

移行タスク リストを表示するには:

1. 上部のナビゲーション バーで、**services** をクリックします。
2. 左側のナビゲーション ペインから、**Heterogeneous Migration** を選択します。
3. **Migration Tasks** タブをクリックします。システムは 30 秒ごとにタスク リストを更新します。
4. タスクを状態別にフィルターリングし、 アイコンをクリックしてタスク リストを更新できます。

パラメーター

移行タスクを作成します。

Destination Match

- **Source Device:** データを移行する VM またはベア メタル サーバーを選択します。VM またはベア メタル サーバーは、オペレーティング システムに一致する移行クライアントがインストールされている場合にのみ、ソース デバイスとして使用できます。
- **Destination VM :** 宛先 VM を選択します。VM は、CAS によって管理され、一致する移行クライアントがインストールされている場合にのみ、宛先 VM として使用できます。
- **Disk Selection and Match:** ソース ディスクと宛先ディスクを選択します。宛先ディスクの容量と数量がソース ディスクより小さくないことを確認してください。システム ディスクとデータ ディスクのみを移行できます。

Task Settings

- **Automatic Incremental Migration Interval::** ソース デバイスのデータ変更によってトリガーされる移行タスクと別の移行タスクの間隔を設定します。オプションには、**Seconds, Minutes, Hours, と Days** があります。システムは、**Finish** をクリックして手動でタスクを完了するまで、指定された間隔で自動増分移行を実行します。
- **Migration Speed Limit:** サービスへの影響を軽減するために、データ移行で使用される帯域幅に制限を設定します。0 は、帯域幅制限が設定されていないことを示します。
- **Migration Method:** 移行方法を選択します。オプションには、**Full** と **Simple** があります。完全移行ではディスク上のすべてのデータが移行され、シンプル移行ではディスク上の有効なデータ ブロックのみが移行されます。
- **Data Compression:** データを圧縮してから移行するかどうかを選択します。データ圧縮により移行帯域幅の要件が軽減されますが、ソース デバイスのリソース消費が増加し、ソース デバイスの動作に影響する可能性があります。
 - **Off-** データを圧縮しないため、ネットワーク リソースの消費量が増えます。
 - **Compression Ratio First** -移行前のデータ圧縮率は 50% で、CPU リソースをより多く消費します。
 - **Performance First** -移行前に 30% のデータ圧縮率を実現し、CPU リソースの消費を抑えます。

移行タスクの詳細を表示する

- **Task Progress:** 現在の移行タスクの進行状況。
 - **Create Task:** 移行タスクが作成されました。
 - **To Start:** 移行タスクが作成され、開始を待機しています。
 - **In Progress:** 移行タスクが進行中です。
 - **Suspended:** 移行タスクは一時停止されています。
 - **To Finish:** データは移行されており、移行タスクは完了を待機しています。
 - **Finished:** 移行タスクが終了しました。
 - **Failed:** データの移行に失敗しました。
- **Policy Info:** タスク作成時に構成された移行設定。

デバイス情報

- **Source Device:** ソースディスク名。
- **Mount Point:** ソース デバイス ディスクのマウント ポイント。
- **File:** ソース デバイス ディスクのファイル システム。
- **Capacity:** ソースデバイスまたは宛先 VM のディスク容量。
- **Destination VM:** 宛先ディスク名。
- **State:** ディスク移行の進行中。

移行タスクの表示

- **Source VM Name:** ソース VM の名前。
- **Source VM IP :** ソース VM の IP アドレス。
- **Migration State:** 現在の移行タスクの状態。
- **Migration Progress:** 現在の移行タスクの進行状況。
- **Estimated Time:** 移行タスクを完了するまでの推定時間。
- **Destination VM Name:** 宛先 VM の名前。
- **Destination VM IP :** 宛先 VM の IP アドレス。

ドライバーを構成する

システムがソース デバイスとターゲット VM 間の非互換性リスクを通知した場合、ドライバーと互換性がない可能性があるハードウェアをエクスポートし、正しいドライバーをターゲット VM にインポートできます。

制限事項とガイドライン

- ダウンロード ウィンドウが表示されない場合は、ブラウザーのダウンロード ディレクトリで、宛先 VM に対応するハードウェア情報ファイルを取得します。
- 一度にインポートできるのは、1つのドライバーとその依存関係のみです。複数のドライバーをインポートするには、インポート操作を繰り返します。

ハードウェア情報をエクスポートする

1. 左側のナビゲーション ペインから、**Services > Heterogeneous Migration > Migration Task Name**を選択します。
2. **Set Driver** をクリックします。
3. **Export Hardware Info** をクリックします。対象デバイスのハードウェア情報が .txt 形式でエクスポートされます。

ドライバーをインポートする

1. 左側のナビゲーション ペインから、**Services > Heterogeneous Migration > Migration Task Name**を選択します。
2. **Set Driver** をクリックします。
3. ターゲット ハードウェアを選択し、**Import** アイコン  をクリックします。
4. エクスポートしたハードウェア情報に基づいて正しいドライバーを選択します。

異機種移行の概要情報を表示する

タスク統計、宛先 VM 統計、ライセンス統計と拡張、すべてのタスクとその状態などの異機種移行の概要情報を表示するには、このタスクを実行します。

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

パラメーター

タスク統計

- **To Start:** 作成され、開始を待機している移行タスク。
- **In Progress:** 進行中または中断されている移行タスク。

- **To Finish:** データ移行は完了しているが、手動で完了するのを待機している移行タスク。
- **Finished:** 完了した移行タスク。
- **Failed:** 移行タスクが失敗しました。

宛先 VM

- **Configured:** 移行タスクが構成されている宛先 VM。
- **Not Configured:** 移行タスクが構成されていない宛先 VM。

ライセンス統計

- **Used:** 使用済みのライセンス。
- **Available:** 利用可能なライセンス。
- **Expand:** ライセンスをさらに登録するには、ライセンス ファイルをさらにインポートします。ソース デバイスの移行タスクを構成すると、新しいソース デバイスごとに 1 つのライセンスが占有されます。
- **Current Tasks:** すべての移行タスクとその状態。

ソースデバイスを表示

VM またはベアメタル サーバーは、そのオペレーティング システムと一致する移行クライアントがインストールされていれば、ソース デバイス リストに表示されます。ソース デバイスの移行タスクの詳細を表示するには、ソース デバイス名のリンクをクリックします。

手順

1. 上部のナビゲーション バーで、**services** をクリックします。
2. 左側のナビゲーション ペインから、**Heterogeneous Migration** を選択します。
3. **Source Devices** タブをクリックします。

パラメーター

- **Device State:** ソース デバイスがオンラインかどうか。移行タスクはオンライン デバイスに対してのみ作成できます。
- **Migration State:** ソース デバイスに移行タスクが構成されているかどうか、および移行タスクの状態。オプションには次のものがあります。
 - **Not Configured:** ソース デバイスに移行タスクが構成されていません。
 - **To Start:** 移行タスクが構成され、開始を待機しています。

- **In Progress:** 移行タスクが進行中で、データが移行されています。
- **Suspended:** 移行タスクは一時停止されています。
- **To Finish:** 移行は完了しており、手動でタスクを完了するのを待機しています。
- **Finished:** データが正常に移行され、移行タスクが完了しました。
- **Failed:** データの移行に失敗しました。
- **Licensed:** ソース デバイスに異種移行ライセンスが付与されているかどうか。

宛先VMを表示する

PE イメージがマウントされ、移行クライアントが構成された VM は、データ移行の宛先 VM として機能できます。

手順

1. 上部のナビゲーション バーで、**services** をクリックします。
2. 左側のナビゲーション ペインから、**Heterogeneous Migration** を選択します。
3. **Destination VMs** タブをクリックします。

パラメーター

- **Device State:** 宛先 VM がオンラインかどうか。宛先 VM として使用できるのはオンライン VM のみです。
- **Migration State:** 移行先 VM に移行タスクが構成されているかどうか、および移行タスクの状態。オプションには次のものがあります。
 - **Not Configured:** 移行先 VM に移行タスクが構成されていません。
 - **To Start:** 移行タスクが構成され、開始を待機しています。
 - **In Progress:** 移行タスクが進行中で、データが移行されています。
 - **Suspended:** 移行タスクは一時停止されています。
 - **To Finish:** 移行は完了しており、手動でタスクを完了するのを待機しています。
 - **Finished:** データが正常に移行され、移行タスクが完了しました。
 - **Failed:** データの移行に失敗しました。

移行クライアントをダウンロードして設定する

移行クライアントをダウンロードし、クライアントプロキシ IP アドレスを構成するには、このタスクを実行します。ソース デバイスは、そのオペレーティング システムと一致する移行クライアントがインストールされている場合にのみ移行できます。各クライアントには、サーバーおよび CVM と通信するためのプロキシ IP アドレスが必要です。クライアント プロキシ IP アドレスは、デフォルトでは CVM ホストの管理 IP アドレスです。CVM ホストの管理 IP アドレスが変更されている場合は、クライアント プロキシ IP アドレスを更新します。

クライアントプロキシIPアドレスを更新する

1. 上部のナビゲーション バーで、**services** をクリックします。
2. 左側のナビゲーション ペインから、**Heterogeneous Migration** を選択します。
3. **Download Client** タブをクリックします。
4. **Update Client Proxy IP** をクリックします。クライアント プロキシ IP アドレスが自動的に更新されます。

クライアントをダウンロードする

1. 上部のナビゲーション バーで、**services** をクリックします。
2. 左側のナビゲーション ペインから、**Heterogeneous Migration** を選択します。
3. **Download Client** タブをクリックします。
4. 特定のオペレーティング システムのダウンロード リンクをクリックして、クライアントをダウンロードします。

外部バックアップシステムを管理する

外部バックアップ システムは、サービス システムに必要なデータ保護機能を提供します。誤操作、システム障害、事故などの人的要因によるデータ損失を回避できます。データ損失が発生した場合に重要なサービス データをタイムリーに回復できるだけでなく、アプリケーションのタイムリーな引き継ぎも保証し、アプリケーション システムへの障害の影響を最小限に抑えます。

外部バックアップ システムは、CAS CVM のエージェントレス バックアップを提供します。エージェントレス バックアップにより、VM にエージェント ソフトウェアをインストールしなくても、VM の高速バックアップと復元が可能になります。バックアップ サーバーで CAS CVM 設定を構成するだけで済みます。

外部バックアップシステムを構成する

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

外部バックアップシステムコンソールにアクセスする

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

パラメーター

- **Protocol:** 外部バックアップ システムにアクセスするために使用するプロトコルを選択します。HTTP と HTTPS が使用できます。
- **Port Number:** 外部バックアップ システムのポート番号を入力します。
- **IP Address:** 外部バックアップ システムの IP アドレスを入力します。
- **Username:** 外部バックアップ システム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:** 外部バックアップ システム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。

CDPベースの災害復旧プラットフォーム

災害復旧プラットフォームは、包括的なデータ資産保護を提供します。サービス異常が発生した場合、バックアップ データを使用して緊急引き継ぎを行うことで、サービスの継続性を確保し、最小限のリソースで災害復旧を実現できます。サービスが正常に実行されている場合、バックアップ データをシミュレーション テストや災害復旧テストに使用して、バックアップ データとリソースを再利用できます。

サービス設定を構成する

1. 上部のナビゲーション バーで、**services** をクリックします。
2. 左側のナビゲーション ペインから、**CDP-Based Disaster Recovery Platform** を選択します。
3. **Settings** をクリックします。
4. プロトコルを選択し、『**パラメーター**』の説明に従ってポート番号、IP アドレス、ユーザー名、およびパスワードを指定します。
5. **OK** をクリックします。

コンソールにアクセスする

1. 上部のナビゲーション バーで、**services** をクリックします。
2. 左側のナビゲーション ペインから、**CDP-Based Disaster Recovery Platform** を選択します。
3. **Console** をクリックして、CDP ベースの災害復旧プラットフォームにアクセスします。

パラメーター

- **Protocol:** CDP ベースの災害復旧プラットフォームにアクセスするための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:** CDP ベースの災害復旧プラットフォームにアクセスするためのポート番号を入力します。
- **IP Address:** CDP ベースの災害復旧プラットフォームにアクセスするための IP アドレスを入力します。
- **Username:** CDP ベースの災害復旧プラットフォームにアクセスするためのユーザー名を入力します。
- **Password:** CDP ベースの災害復旧プラットフォームにアクセスするためのパスワードを入力します。