ORACLE

Oracle Site Guardを使用したOCI PaaSシステムのディザスタ・リカバリの管理

SOA Cloud Service DR、SOA Market Place DR、WebLogic for OCI DRでのOracle Site Guardの使用

2021年3月 | バージョン2

本書の目的

本書には、PaaSディザスタ・リカバリにおけるOracle Site Guardを使用したスイッチオーバーとフェイルオーバーの管理についての説明、要件の要約、設定手順が記載されています。このホワイト・ペーパーで説明する手順は、オラクルのベスト・プラクティスを基盤とするSOA Cloud Service、SOA Marketplace、Weblogic for OCIの各ディザスタ・リカバリ環境に適用されます。このホワイト・ペーパーの対象読者は、Enterprise Manager、Oracle Site Guard、Oracle Cloud、Oracle WebLogic、Oracle Database、Oracle Data Guardの知識を持つ技術者です。

免責事項

本文書には、ソフトウェアや印刷物など、いかなる形式のものも含め、オラクルの独占的な所有物である占有情報が含まれます。この文書へのアクセスと使用は、締結および遵守に同意したOracle Software License and Service Agreementの諸条件に従うものとします。本文書は、ライセンス契約の一部ではありません。また、オラクル、オラクルの子会社または関連会社との契約に組み込むことはできません。

本書は情報提供のみを目的としており、実装および記載されている製品機能の計画を支援することのみを意図しています。マテリアルやコード、機能の提供をコミットメント（確約）するものではなく、購買を決定する際の判断材料になさらないでください。本書に記載されている機能の開発、リリース、および時期については、弊社の裁量により決定されます。

改訂履歴

このホワイト・ペーパーには下記の改訂が行われてきました。

日付	改訂	コメント
2020年6月	1	初版
2021年3月	2	細かな修正

目次

はじめに

Oracle Maximum Availability Architecture（Oracle MAA）は、オンプレミス、プライベート・クラウド、パブリック・クラウド、またはハイブリッド・クラウドにデプロイされるオラクル製品（データベース、Oracle Fusion Middleware、アプリケーション）のデータを保護し可用性を高めるためのベスト・プラクティス構想です。Oracle Maximum Availability Architectureのベスト・プラクティスを実装することは、すべてのOracleデプロイメントにおける重要な要件の1つです。すべての重要なシステムは、予期せぬ障害や自然災害から保護する必要があります。

この保護能力は、PaaSサービスのようなクラウドにデプロイされているシステムでも必要とされます。Oracle Maximum Availability Architecture（Oracle MAA）は、Oracle CloudのMAAベスト・プラクティスで公開されているSOA Cloud Service、SOA on Marketplace、WebLogic for OCIなどの複数のPaaSサービスのためのディザスタ・リカバリ・ソリューションです。これらのPaaSサービスのディザスタ・リカバリ・アーキテクチャ・ソリューションは、アクティブ-パッシブ・トポロジ（1つのリージョンにプライマリ・ロールのシステムが1つと、別のリージョンにスタンバイ・ロールのセカンダリ・システムが1つ）を基礎としています。スイッチオーバーはこれら2つのサイト間でロールを変更する計画された手順で、プライマリ・サイトがスタンバイになり、セカンダリがプライマリ・ロールを引き継ぎます。このロール変更は、フェイルオーバー手順中でも発生します。フェイルオーバー手順は通常、プライマリが使用不可の場合に実行する必要がある計画外イベントです。どちらの手順とも、さまざまなコンポーネントを停止/開始し、データベースのロール変更を実行するさまざまな手順で構成されています。

これらの手順は、手動で実行するか、またはフル・スタックのスイッチオーバー手順を編成するようにOracle Site Guardを構成することができます。このドキュメントでは、これを実現するための方法を説明します。内容には、PaaSディザスタ・リカバリ環境に応じてOracle Site Guardを構成するための詳細な手順、およびOracle Site Guard操作計画を使用してスイッチオーバー/フェイルオーバーを管理する方法が含まれます。

このホワイト・ペーパーの対象読者は、Oracle Enterprise Manager Cloud Control、Oracle Cloud Infrastructure、Oracle Weblogic Server、Oracle Database、Data Guard、Oracle Databaseのバックアップとリカバリに関する知識を持つ技術者です。

PaaSディザスタ・リカバリ用のOracle Site Guard

Oracle Site Guardは、管理者によるサイト全体のスイッチオーバーやフェイルオーバーの自動化を可能にするディザスタ・リカバリ（DR）ソリューションです。Oracle Fusion Middleware、Oracle Fusion Application、Oracle Databaseを組織化して連係を取りながらフェイルオーバーさせることができます。組織化する対象を、データセンターの他のソフトウェア・コンポーネントまで拡張することもできます。Oracle Site Guardsには次のメリットがあります。

- ディザスタ・リカバリ処理を完全に自動化して1回のクリックで起動
- ディザスタ・リカバリに要する時間の最小化
- 人為的エラーの削減
- 柔軟でカスタマイズ可能
- 特殊なスキルが不要
- 1つの画面でディザスタ・リカバリを管理
- オンデマンドの、またはスケジューリングされたディザスタ・リカバリ・ドリルを使用してディザスタ・リカバリに確実に対応

Oracle Site GuardはEnterprise Manager Cloud Control Fusion Middlewareプラグインに含まれています。WebLogic Marketplace DR環境でOracle Site Guardを使用する場合は、Enterprise Manager Cloud ControlのOracle Management ServerとAgentをデプロイする必要があります。

Oracle Site Guardを使用して、Webサイト「Oracle CloudのMAAベスト・プラクティス」にある次のホワイト・ペーパーで説明されているMAAベスト・プラクティスに従ったPaaSディザスタ・リカバリのシナリオの場合のスイッチオーバーを調整することができます。

- OCIでのSOA Cloud Serviceのディザスタ・リカバリ
- SOA on OCI Marketplaceのディザスタ・リカバリ
- Oracle WebLogic Server for Oracle Cloud Infrastructureのディザスタ・リカバリ

Oracle Site Guardトポロジでのサンプルの PaaSクラウド・ディザスタ・リカバリを以下に示します。

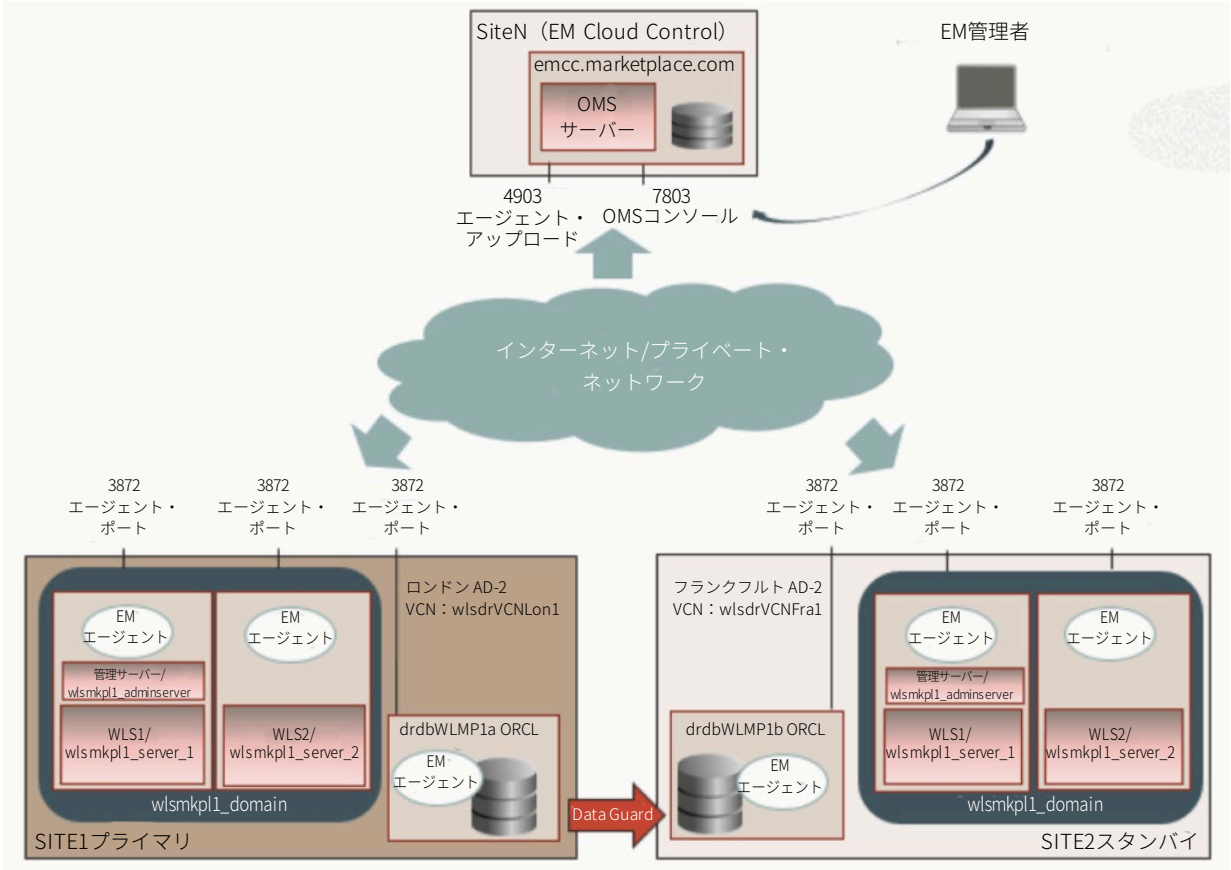

図1 PaaS DRでのOracle Site Guardを使用したスイッチオーバーの管理

このドキュメントで説明するのと同様の単一のEMインストールを使用して、複数の災害保護システムの調整や管理ができます。オラクルでは、Enterprise Managerを、プライマリまたはスタンバイ・サイトに影響する可能性がある停止が起こりにくい、第3のサイトにデプロイすることを強くお奨めします。

初期設定

この設定を行うには、次の手順を実行する必要があります。

- **Enterprise Manager Cloud Controlの設定**
  EM Cloud Control Oracle Management ServerをOracle Cloudにインストールします。Enterprise Manager Cloud Control Serverは、PaaSシステムのいずれかと同じリージョンでも、別のリージョンにでも配置可能です。ただしオラクルでは、Enterprise Managerを、プライマリまたはスタンバイ・サイトに影響する可能性がある停止が起こりにくい、第3のサイトにデプロイすることを強くお奨めします。
- **ネットワークの設定**
  ターゲットとOracle Enterprise Managerの管理サーバー（OMS）の間の通信を許可するために必要なネットワーク・ルールを作成します。
- **エージェントのインストール**
  PaaS DR環境のホストにEnterprise Manager Cloud Control Agentをインストールします。
- **ターゲットの検出**
  Oracle Site Guardで管理するターゲット（WebLogicドメイン、データベースなど）を検出します。
- **Oracle Site Guardの構成**
  PaaS DR環境でのスイッチオーバーやフェイルオーバーを調整するために必要なOracle Site Guard構成（サイト、資格証明、スクリプト、計画など）を行います。

ここでは、必要なEnterprise Manager Cloud ControlのライセンスとOracle Site Guardが使用されているものとします。セットアップを完了するには、Enterprise Manager Cloud Controlの概要および管理に関する技術面の基礎知識が必要です。各手順の詳細については、次の各項を参照してください。

Enterprise Manager Cloud Controlの設定

すでにEnterprise Manager Cloud Controlのインストールと構成が完了している場合はこの手順をスキップして残りの項（ネットワークの設定、エージェントのインストール、Oracle Site Guardの構成）に進んで構いません。

Enterprise Manager Cloud Controlがない場合は、「Setting Up Oracle Enterprise Manager 13.3 on Oracle Cloud Infrastructure」の手順に従って、Marketplace EMイメージを基にクラウド・テナンシーでEMを作成して構成できます。このMarketplaceのイメージには、あらかじめ構成されたOracle Enterprise Manager（13.3 PG）と共同配置されたOracle Database（19.3）が含まれています。その結果、EMホストは“emcc.marketplace.com”という名前で作成されます。このホスト名は、OMSホスト名を参照するために以降のセクションで使用されます。

ネットワークの設定

1. ホスト名の設定

Enterprise Managerのホスト名、およびそのモニター対象のホストは相互に解決可能である必要があります。プライマリ・サイトとスタンバイ・サイトは異なるクラウド・データセンターに配置するのが一般的で、OMSはそのいずれか、または別のもう1つのデータセンターに配置できます。

データセンター間に内部通信がない場合、Enterprise Manager Cloud ControlのOMSとWebLogic Cloud DRのターゲットはパブリックIPを介して相互通信します。オラクルでは、クラウド・ホストのパブリックIPに関連付けけられているホスト名を使用することを推奨しています。そのためには、DNSサーバーにホスト名を登録するか、OMSホストおよびターゲット・ホストの/etc/hostsファイルで名前解決を構成します。

ホストのプライベート名はクラウド・インフラストラクチャによって設定されますが、パブリック名はケースごとに定義またはカスタマイズする必要があります。次に例を示します。

サイト	プライベート名	パブリック名（利用者が定義）	パブリックIP
SiteN	emcc.marketplace.com	emcc.marketplace.com	111111111100
Site1	wlsmkpl1-wls-0.site1cloudinternaldomain.com	wlsmkpl1-wls-0-public.site1.example.com	111.111.111.11

	wlsmkpl1-wls-1.site1cloudinternaldomain.com	wlsmkpl1-wls-1-public.site1.example.com	111.111.111.12
	drdbwlmp1a.site1cloudinternaldomain.com	drdbwlmp1a-public.site1.example.com	111.111.111.13
Site2	wlsmkpl1-wls-0.site2cloudinternaldomain.com	wlsmkpl1-wls-0-public.site2.example.com	222.222.222.11
	wlsmkpl1-wls-1.site2cloudinternaldomain.com	wlsmkpl1-wls-1-public.site2.example.com	222.222.222.12
	drdbwlmp1b.site2cloudinternaldomain.com	drdbwlmp1b-public.site2.example.com	222.222.222.13

以下の例は、パブリックIPを使って通信する場合に、OMSホストと各監視対象ホストで設定される/etc/hostsファイルのエントリです。

```
#########################################################################################################################
# OMSホストのパブリックIP（このエントリは、監視対象ホストに追加するためだけに必要です。OMSがすでに設定されている場合は変更しないでください）
111.111.111.100       emcc.marketplace.com
#########################################################################################################################
# クラウドの監視対象ホストのパブリック名
#########################################################################################################################
# SITE1（次のエントリは、SITE1のホストおよびOMSホストにおいてのみ必要です）
111.111.111.11        wlsmkpl1-wls-0-public.site1.example.com
111.111.111.12        wlsmkpl1-wls-1-public.site1.example.com
111.111.111.13        drdbwlmp1a-public.site1.example.com
# SITE2（次のエントリは、SITE2のホストおよびOMSホストにおいてのみ必要です）
222.222.222.11        wlsmkpl1-wls-0-public.site2.example.com
222.222.222.12        wlsmkpl1-wls-1-public.site2.example.com
222.222.222.13        drdbwlmp1b-public.site2.example.com
```

OMSと監視対象ホストの間で、**プライベート**・ネットワーク（動的ルーティング・ゲートウェイ経由[1]）を使用する通信が可能な場合、Oracle Management Serviceと監視対象ホストでは、パブリックIP/パブリック名の代わりに適切な内部IP/内部名を使用して相互通信できます。その場合、OMSの/etc/hostsファイルには、ホストの内部IPと内部名を含める必要があります。

2. セキュリティ・ルール

Oracle Management Serverは監視対象ホストのエージェントと通信する必要があり、エージェントはOMSサーバーに接続して監視データをアップロードする必要があります。FMWターゲットを検出する場合は、OMSとWebLogicドメイン管理サーバーが通信できる必要があり、データベースを監視する場合は、OMSからターゲット・データベースに接続できる必要があります。セキュア・プロトコル（HTTPS、t3s、ネットワーク暗号化付きSQL*NET[2]）が使用されていれば、このトラフィックはすべて暗号化されます。OMSと監視対象ターゲットとの間には次の通信が必要です。

接続元	接続先	プロトコル
すべての監視対象ホスト	OMSアップロード・ポート（4903）	HTTPS
OMSホスト	すべての監視対象ホストのエージェント・ポート（3872）	HTTPS
OMSホスト	すべてのターゲット・データベースのリスナー・ポート（1521）	SQL（ネットワーク暗号化を使用）
OMSホスト	すべての監視対象ホストのsshポート（22）	SSH（エージェント・ソフトウェアの送信用）
インターネット（管理者ユーザーのネットワークCIDR）	OMSコンソール・ポート（7803）	HTTPS

[1] ネットワーク構成について詳しくは、「動的ルーティング・ゲートウェイ（DRG）」を参照してください。
[2] Setting Up Oracle Enterprise Manager 13.3 on Oracle Cloud Infrastructure

ただし、これらの通信の一部はデフォルトでは許可されていません。通信できるようにするには、セキュリティ・ルールを定義する必要があります。次の各項目に示す手順に沿ってセキュリティ・ルールを作成します。

a) **OMS側でのセキュリティ・ルール**
ターゲットからOMSへの通信を許可するネットワーク・ルールを作成します。
- OCIコンソールにログインします。
- 「Networking」→「Virtual Cloud Networks」の順に移動し、OMSの「Virtual Cloud Network」をクリックします。
- **Security Lists**の下で、ルールを追加するセキュリティ・リストをクリックします。
- **すべての監視対象ホストからOMSアップロード・ポートへの**トラフィックを許可する**受信ルールを追加**（ステートフル）します。
  - Source CIDR： 監視対象ホストのネットワークCIDR[3]。例：111.111.111.0/24
  - IP Protocol： TCP
  - Source Port Range： All
  - Destination Port Range： 4903

  各監視対象ホストのネットワークでこの作業を繰り返します。
- **インターネット（または特定のネットワーク）からOMSコンソール・ポートへの**トラフィックを許可する**受信ルールを追加**（ステートフル）します。
  - Source CIDR： 0.0.0.0/0を使用してすべてのアクセスを許可するか、カスタム・ネットワークCIDRを1つ指定します。
  - IP Protocol： TCP
  - Source Port Range： All
  - Destination Port Range： 7803

b) **ターゲット側でのセキュリティ・ルール**
OMSからホスト・ターゲットへの通信を許可するネットワーク・ルールを作成します。
- OCIコンソールにログインします。
- 「Networking」→「Virtual Cloud Networks」の順に移動し、Site1のターゲットの「Virtual Cloud Network」をクリックします。
- **Security Lists**の下で、ルールを追加するセキュリティ・リストをクリックします。
- **OMSホストから監視対象ホストのエージェント・ポートへの**トラフィックを許可する**受信ルールを追加**（ステートフル）します。
  - Source CIDR： CIDR形式[4]のOMS IP。例：111.111 111.100/32
  - IP Protocol： TCP
  - Source Port Range： All
  - Destination Port Range： 3872
- **OMSホストから監視対象DBホストのDBリスナー・ポートへの**トラフィックを許可する**受信ルールを追加**（ステートフル）します。
  - Source CIDR： CIDR形式[5]のOMS IP。例：111.111 111.100/32
  - IP Protocol： TCP
  - Source Port Range： All
  - Destination Port Range： 1521

Site2のターゲットの仮想クラウド・ネットワークについて、同じ作業を繰り返します。

c) **DBホストのIP表**
OCIネットワーク・セキュリティ・ルールに加えて、次のiptablesルールがターゲットDBシステムで必要になる可能性があります。
- DBシステムのホストにsshで接続します。
- opcとしてログインし、sudoを実行してrootユーザーになります。
- iptablesのコピーをバックアップとして保存します。必要な場合は、コマンド（iptables-restore < /tmp/iptables.orig）を使用して元のファイルをリストアできます。

```
[root@drdbwlmp1a ~]# iptables-save > /tmp/iptables.orig
```

[3] OMSとターゲットの通信がインターネット経由で行われる場合はパブリック・ネットワークCIDRを使用し、プライベートIP経由の通信が可能な場合はプライベート・ネットワークCIDRを使用します。
[4] OMSとターゲットの通信がインターネット経由で行われる場合はパブリックIP CIDRを使用し、プライベートIP経由の通信が可能な場合はプライベートIP CIDRを使用します。
[5] OMSとターゲットの通信がインターネット経由で行われる場合はパブリックIP CIDRを使用し、プライベートIP経由の通信が可能な場合はプライベートIP CIDRを使用します。

- iptablesにルールを追加し、**EMエージェントに対する着信トラフィックを許可します。**次に例を示します。

```
[root@drdbwlmp1a ~]# iptables -I INPUT 8 -p tcp -m state --state NEW -m tcp --dport 3872 -j ACCEPT -m comment --comment "Required for EM agent port"
```

- ルールが追加されたことを確認します。

```
[root@drdbwlmp1a ~]# service iptables status
```

- 更新したファイルを/etc/sysconfig/iptablesに保存します。

```
[root@drdbwlmp1a ~]# service iptables save
```

- 変更内容はすぐに有効化され、ノードを再起動しても有効化された状態が続きます。

次に示すのは、前の例を使用して作成したセキュリティ・ルールのサマリー例です。

サイト	ルールの種類	接続元のCIDR	プロトコル	接続元ポート	接続先のポート範囲：
SiteN（OMS）	受信ルール	Site1のネットワークCIDRの例：111.111.111.0/24	TCP	すべて	4903（アップロード・ポート）
SiteN（OMS）	受信ルール	Site2のネットワークCIDRの例：22.222.222.0/24	TCP	すべて	4903（アップロード・ポート）
SiteN（OMS）	受信ルール	管理用ネットワークのCIDR（インターネットへのアクセスを許可する場合は0.0.0.0/o）	TCP	すべて	7803（OMSコンソール・ポート）
Site1およびSite2	受信ルール	CIDR形式のOMS IP。例：111.111.111.100/32	TCP	すべて	3872（エージェント・ポート）
Site1およびSite2	受信ルール	CIDR形式のOMS IP。例：111.111.111.100/32	TCP	すべて	1521（DBリスナー・ポート）

注：OMSからホストのsshポート（22）へのアクセスが、すでにオープンになっていることを前提としています。オープンになっていない場合は、OMSのIPからこれらのポートへのトラフィックを許可する適切なルールを上記と同じ方法で追加してください。

エージェントのインストール

Enterprise Manager Cloud Control Agentは、PaaS DR環境内のすべてのホストにインストールする必要があります。

1. ターゲット・ホストの準備

以下の手順を実行して、ターゲット・ホストにエージェントをインストールする準備をします。

a) ユーザーとグループの作成
エージェント・ソフトウェアのインストールや実行に専用ユーザーを使用すると、プロセスや環境変数を監視対象ソフトウェアから切り離すことができます。エージェントをインストールするホストでユーザー（例：**emcadm**）を作成し、クラウド・マシン内でソフトウェアを実行しているユーザーのグループに追加します。これは、中間層ホスト内のoracleグループ（WebLogicまたはSOAホスト）とDBホスト内のoinstallグループです。

中間層ホストの場合、ソフトウェア・グループはoracleです。

```
[root@host]# useradd -g oracle emcadm
```

DBホストの場合、ソフトウェア・グループはoinstallです（oracleグループは存在しません）。

```
[root@host]# useradd -g oinstall emcadm
```

注：エージェント専用のユーザーを必ず使用しなければならないわけではありません。エージェントのインストールと実行にユーザー“oracle”を使用することもできます。監視対象ソフトウェアを実行しているユーザーとは異なるユーザーでエージェントを実行している場合に必要な手順やアクションを識別するために、このドキュメントの手順ではエージェント専用ユーザー（emcadm）を使用します。

b) OMSへの通信の検証
ターゲット・ホスト側で、Enterprise Manager OMSのホスト名とそれ固有のパブリック名（パブリック名を使用する場合）を解決できることを確認します。これは、前の項「ネットワークの設定」の説明に従ってすでに構成済みです。
ncを使用して、Enterprise Manager OMSのアップロード・ポートに到達可能なことを確認します。環境に応じて適切なOMS IP（パブリックまたはプライベート）を使用してください。

```
$ nc -v -w 5 -z <oms_ip> 4903
Connection to <oms_ip> 4903 port [tcp/*] succeeded!
```

c) エージェント・ホーム・ベース・フォルダの作成
エージェント・ホーム・ベース・フォルダには要件がいくつかあります。特に重要なのは、権限委任プロバイダを使用する場合です（資格証明に使用されます）。Enterprise Manager Cloud Controlのドキュメントの「サイレント・モードでのOracle Management Agentのインストール」の章にあるエージェント・ベース・ディレクトリの要件を参照してください。

エージェント・ホーム・ベース用として推奨されるのは、すでにホストにマウントされているストレージ・ボリュームの次のフォルダです。
DBホスト用：　/u01/agent13c　（/u01ボリュームの下）
中間層ホスト用：　/u01/agent13c　（これは/ボリュームの下であることに注意）[6]
<AGENT_BASE_DIR>はエージェント・ベース・フォルダを参照するために使用されます。

- rootユーザーでフォルダを作成します。
  ```
  [root@wlsmkpl1-wls-0~]#  mkdir -p <AGENT_BASE_DIR>
  ```
- このフォルダの所有権を、エージェントを実行するユーザーとグループに変更します。中間層ホストの場合は、次のコマンドを実行します。
  ```
  [root@wlsmkpl1-wls-0~]#  chown emcadm:oracle <AGENT_BASE_DIR>
  ```
  DBホストの場合は、次のコマンドを実行します。
  ```
  [root@drdbwlmp1a]# chown emcadm:oinstall <AGENT_BASE_DIR>
  ```

6 中間層ホストでは、rootボリュームを使用する代わりに、OCIブロック・ボリュームを構成して接続することが推奨されます。OCIドキュメント内のブロック・ボリュームに関するOracleドキュメント『ブロック・ボリュームの概要』を参照してください。

- このフォルダと親フォルダに対する読取りと実行の権限をグループとその他のユーザーに追加します。これは、EMが使用する権限委任機能で必要です。

```
[root@wlsmkpl1-wls-0]# chmod go+rx /u01/agent13c
[root@wlsmkpl1-wls-0]# chmod go+rx /u01
```

d) その他の要件の確認
エージェントのすべての要件の一覧は、Enterprise Manager Cloud Controlのドキュメントの「サイレント・モードでのOracle Management Agentのインストール」の章にある*表6-1「サイレント・モードでOracle Management Agentをインストールするための前提条件」*を参照してください。DBホストはこれらの要件を満たしていて、追加の作業は必要ないことを想定しています。中間層ホストの中には、エージェントで必要とされ、デフォルトではインストールされないオペレーティング・システム・パッケージがいくつかあります。インストールされていない場合、エージェント・インストーラにより次のメッセージが表示されます。

```
Check complete:Passed
=====================================================
Performing check for Packages_agent
Are the required packages installed on the current operating system?Checking
for make-3.82-21; found make-1:3.82-23.el7-x86_64.Passed  Checking for
binutils-2.23; found binutils-2.27-34.base.0.1.el7-x86_64.Passed  Checking for
gcc-4.8.2-16; Not found.Failed <<<<
Checking for libaio-0.3.109-12;  found libaio-0.3.109-13.el7-x86_64.     Passed
Checking for glibc-common-2.17-55;  found glibc-common-2.17-292.0.1.el7-x86_64.Passed
Checking for libstdc++-4.8.2-16;  found libstdc++-4.8.5-39.0.3.el7-x86_64.          Passed
Checking for sysstat-10.1.5-4;  found sysstat-10.1.5-17.el7-x86_64.          Passed
Check complete.The overall result of this check is:Failed <<<<
```

不足しているパッケージをrootユーザーとしてインストールしてください。以下に例を挙げます。

```
[root@wlsmkpl1-wls-0]# yum install gcc
```

2. エージェント・ソフトウェアの取得

“AgentDeploy”方式を使用してエージェント・ソフトウェアを取得します。この方式では、EM CLIを使用して管理エージェント・ソフトウェアをリモートの宛先ホストにダウンロードしてから、スクリプトを実行して管理エージェントをインストールする必要があります。EM CLIを使用する場所は、OMSホストかリモートの宛先ホストのいずれかを選択できます。OMSホストからEM CLIを使用することにした場合は、ダウンロードした管理エージェント・ソフトウェアをリモートの宛先ホストに送信してから、スクリプトを実行して管理エージェントをインストールする必要があります。この方式では多数の追加パラメータがサポートされるため、管理エージェントをカスタマイズしてインストールする場合に最適です。

OMSホストでemcliを使用してエージェント・ソフトウェアをダウンロードし、ターゲット・ホストにコピーします。

a) OMSホストでemcliにログインします（MIDDLEWARE_HOMEは/u01/app/em13c/middlewareです）。

```
[oracle@emcc bin]$ cd $MIDDLEWARE_HOME/bin
[oracle@emcc bin]$ ./emcli login -username=sysman
```

b) 使用可能なソフトウェアを確認し、Linux x86-64プラットフォーム用のエージェント・イメージを取得します。

```
[oracle@emcc bin]$ ./emcli get_supported_platforms
----------------------------------------
Version = 13.3.0.0.0
Platform = Linux x86-64
----------------------------------------
Platforms list displayed successfully.
[oracle@emcc bin]$ ./emcli get_agentimage -destination=/tmp/agent_image -platform="Linux x86-64" -version=13.3.0.0.0
..
Downloading    /tmp/agent_image/13.3.0.0.0_AgentCore_226.zip
Agent Image Download completed successfully.
```

c) たとえば、エージェントがscpを使用してインストールされる各リモート・ホストにエージェント・イメージをコピーします。

```
[oracle@emcc ~]$ scp -i <public_ssh_key>.ppk  /tmp/agent_image/13.3.0.0.0_AgentCore_226.zip  opc@<monitored-host-name>:/tmp/
```

3. エージェントのインストール

エージェントをインストールするホストで次の手順を実行します。

a) エージェント・ソフトウェアのzipファイルをエージェント・ユーザー（例：emcadm）で読み取れるか確認します。
b) エージェント・ユーザー（emcadm）として、ソフトウェアを一時フォルダに解凍します。例：/tmp/agent_image

```
[emcadm@drdbwlmp1a tmp]$ mkdir agent_image
[emcadm@drdbwlmp1a tmp]$ cp 13.3.0.0.0_AgentCore_226.zip agent_image
[emcadm@drdbwlmp1a tmp]$ cd agent_image
[emcadm@drdbwlmp1a agent_image]$ unzip 13.3.0.0.0_AgentCore_226.zip
```

c) エージェントを解凍したフォルダ内で、エージェント・ユーザー（emcadm）と一緒にagenDeploy.shを使ってソフト

```
./agentDeploy.sh AGENT_BASE_DIR=/u01/agent13c OMS_HOST=emcc.marketplace.com EM_UPLOAD_PORT=4903
AGENT_REGISTRATION_PASSWORD=welcome1 LOCALHOST=drdbwlmp1a.site1cloudinternaldomain.com
LOCALPORT=3872 AGENT_PORT=3872 ORACLE_HOSTNAME=drdbwlmp1a-public-site1.example.com
ALLOW_IPADDRESS=TRUE START_AGENT=true
```

コマンド説明：

AGENT_BASE_DIR	エージェントのインストール先フォルダ
OMS_HOST	OMSに接続するための名前。この例の場合：emcc.marketplace.com
EM_UPLOAD_PORT	OMSのアップロード・ポート。通常は4903
AGENT_REGISTRATION_PASSWORD	エージェント登録パスワード

LOCALHOST	**エージェントが**インストールされている**ホストの名前のFQDN**（プライベート名）。例：
	`[root@ wlsmkpl1-wls-0]# hostname – fqdn`
	`wlsmkpl1-wls-0.site1cloudinternaldomain.com`

LOCALPORT/AGENT_PORT	エージェントがリスニングするポート。例：3872
ORACLE_HOSTNAME	OMSとターゲット間の通信がインターネット経由で行われる場合、これは監視対象ホストのパブリック名になります。OMSは、このパブリック名を使用してエージェントと通信します。ホストのパブリックIPか、そのパブリックIPに解決できるパブリック名である必要があります。 OMSとターゲット間の通信がプライベート・ネットワーク経由で行われる（つまり、DRGを使用する）場合、これは監視対象ホストの**プライベート名**（ホスト名のFQDN）になります。 **ヒント：**IPではなくホスト名を使用することをお奨めします。 **重要**：この名前は小文字で記述してください。パブリック名に大文字を使用すると、エージェントの証明書を検証するときにエラーが発生する可能性があります。
ALLOW_IPADDRESS	ORACLE_HOSTNAMEのIPアドレスを指定する場合は、TRUEと入力します。ALLOW_IPADDRESSをFALSEに設定すると、管理エージェントのインストール時にORACLE_HOSTNAMEのIPアドレスを指定すると前提条件のチェックが失敗します。ホスト名を使用する場合は設定不要です。 **ヒント：**IPではなく名前を使用することをお奨めします。
START_AGENT	trueに設定すると、インストール後にエージェントが起動します。

d) インストールが正しく終了したら、rootユーザーでrootスクリプトを実行します。

```
<AGENT_BASE_DIR>/agent_13.3.0.0.0/root.sh
```

注：エージェントのインストールが「Waiting for agent targets to get promoted...」手順で中断し、最終的にエラーが返された場合は、次の手順に従って問題を解決します。

- rootとして<AGENT_BASE_DIR>/agent_13.3.0.0.0/root.shを実行します。

- emcadmとしてエージェントを起動し、内部ターゲットの追加を再試行します。

/u01/agent13c/agent_inst/bin/emctl start agent

/u01/agent13c/agent_inst/bin/emctl config agent addinternaltargets

e) <AGENT_BASE_DIR>/agent_13.3.0.0.0/bin/emctlステータス・エージェントのステータスを確認します。
エージェントURLには、ホストのパブリック・ホスト名（OMSとターゲットがパブリックIP経由で通信する場合）、またはプライベート・ホスト名（OMSとターゲットが内部で通信する場合）が表示されます。
ローカル・エージェントURLでプライベート・ホスト名が使用されていることを確認します。**リポジトリURL**の参照先がOMS名になっていることを確認します。

```
[emcadm@wlsmkpl1-wls-0  bin]$ ./emctl status agent
Oracle Enterprise Manager Cloud Control 13c Release 3
Copyright (c) 1996, 2018 Oracle Corporation.All rights reserved.

---------------------------------------------------
Agent Version          :13.3.0.0.0
OMS Version            :13.3.0.0.0
Protocol Version       :12.1.0.1.0
Agent Home             : /u01/agent13c/agent_inst
Agent Log Directory : /u01/agent13c/agent_inst/sysman/log
Agent Binaries         : /u01/agent13c/agent_13.3.0.0.0
Core JAR Location      : /u01/agent13c/agent_13.3.0.0.0/jlib
Agent Process ID       :16917
Parent Process ID      :16880
Agent URL              : https://wlsmkpl1-wls-0-public.site1.example.com:3872/emd/main/
Local Agent URL in NAT : https://wlsmkpl1-wls-0.wlsdrvcnlon1ad2.wlsdrvcnlon1.oraclevcn.com:3872/emd/main/
Repository URL         : https://emcc.marketplace.com:4903/empbs/upload
Started at             :2020-02-25 10:02:28
Started by user        : emcadm
…

-----------------------------------------------
Agent is Running and Ready
```

f) エージェントのアップロードが正しく実行されることを確認します。

```
[emcadm@wlsmkpl1-wls-0  bin]$ cd <AGENT_BASE_DIR>/agent_inst/bin
[emcadm@wlsmkpl1-wls-0  bin]$ ./emctl upload agent
Oracle Enterprise Manager Cloud Control 13c Release 3
Copyright (c) 1996, 2018 Oracle Corporation. All rights reserved.
---------------------------------------------------------------
EMD upload completed successfully
```

g) エージェントを再起動し、すべてが適切に構成されていることを確認します。

```
[emcadm@maa4-wls-1  bin]$ ./emctl stop agent
Oracle Enterprise Manager Cloud Control 13c Release 3
Copyright (c) 1996, 2018 Oracle Corporation. All rights reserved.
Stopping agent ... stopped.
[emcadm@maa4-wls-1  bin]$ ./emctl start agent
Oracle Enterprise Manager Cloud Control 13c Release 3
Copyright (c) 1996, 2018 Oracle Corporation. All rights reserved.
Starting agent .............  started.
```

h) OMSコンソール（https://<oms_public_ip>:7803/em）にログインし、「Targets」→「Hosts」の順に移動して、ホストが登録されていることを確認します。

注：エラーがありエージェントをインストールし直す必要がある場合は、次のコマンドを使用してインストールを削除できます（エージェントのベース・ディレクトリ以外のフォルダで実行してください）。コマンドは1行で入力します。

<AGENT_BASE_DIR>/agent_13.3.0.0.0/perl/bin/perl<AGENT_BASE_DIR>/agent_13.3.0.0.0/sysman/install/AgentDeinstall.pl -agentHome <AGENT_BASE_DIR>/agent_13.3.0.0.0

エージェントのターゲットのうちOMSに登録されたものがある場合は、エージェントの登録を解除して削除することも必要です。詳しくは、" EM 13C:How to Deinstall the Enterprise Manager 13c Cloud Control Agent（ドキュメントID 2095678.1）"を参照してください。

ターゲットの検出

プライマリとスタンバイのWebLogicドメインとデータベースをEMで検出する必要があります。Oracle Cloudのホスト上で稼働しているターゲットを検出して昇格させる手順は、オンプレミス環境にある通常のホスト上で稼働しているターゲットを検出して昇格させる手順と同じです。

1. 自動検出されたターゲットの昇格

一部のターゲットは自動検出されるため、必要なのは昇格させることだけです。Oracle Databaseホーム、Oracle Grid Infrastructureホーム、Oracle High Availability ServiceおよびClusterの場合はこれが通常のプロセスです。自動検出されたこれらのターゲットを昇格させるために、次の手順を実行します。

a) OMSコンソールにログインします。
b) 「Setup」→「Add Target」→「Configure Auto Discovery」の順に移動します。
c) “Target on Hosts”を表示します。ホストを選択して「Discover now」をクリックします。
d) 「Setup」→「Add Target」→「Auto Discovery Results」の順に移動します。
e) “Targets on Hosts”を表示します。
f) 自動検出されたターゲットを確認し、いずれかをクリックし、「Promote」をクリックします。

Oracle Database、ASMインスタンス、クラスタも自動検出できます。これらを昇格させる手順については、以降の各項目を参照してください。

2. ASMターゲットの検出

ASMインスタンスは通常、自動検出されます。次の手順を実行して検出を行います。

a) ASMデータベースの監視にはASSNMPユーザーを使用するのが一般的です。ASSNMPユーザーのパスワードは自分で変更する必要があります。ASMを使用している任意のターゲットDBホスト（プライマリまたはセカンダリ）で次の手順を実行します。
   - DBホストにopcユーザーとしてログインし、sudoを実行してユーザーgridになります。
   - ASMインスタンスにsysadmとして接続し、ユーザーASMSNMPのパスワードをリセットします。
   - ユーザーASMSNMPのパスワードをリセットします。

```
sqlplus " / as sysasm"
sql> alter user asmsnmp identified by <new password>;
```

b) OMSコンソールのAuto Discovery Resultsで、検出された“Cluster ASM”ターゲットを選択して「Promote」をクリックします。
c) Results画面で、Cluster ASMターゲットを選択して「Configure」をクリックします。
   - Generalタブで、Monitor usernameをASMSNMPに設定し、パスワードを設定します。
   - Instancesタブで、"Listener Machine Name"が、OMSがこのホスト・ターゲットへの接続に使用するホスト名になっていることを確認します。OMSはデータベースに接続する必要があります。ネットワーク・トポロジに応じて、適切なマシンのホスト名（パブリックまたはプライベート）を使用します。
   - 「Test Connection」をクリックして正常に接続できることを確認し、「Save」をクリックします。
d) Results画面に戻り、ASMリスナーも選択されていることを確認します。リスナーはデフォルト値のままにします。ASMリスナー・ターゲットはローカル・エージェントによって監視され、マシンのプライベート名を使用できます。
e) 「Next」をクリックして、「Save」をクリックします。

3. データベース・ターゲットの検出

データベース・ターゲットを昇格または検出するには、次の手順を実行します。

a) データベースの監視にはユーザーDBSNMPを使用するのが一般的です。このユーザー・アカウントはデフォルトでロックされています。プライマリ・データベースにsysdbaとして接続し、必要に応じてロックを解除し、パスワードを設定します。

```
sql> ALTER USER DBSNMP ACCOUNT UNLOCK;
Sql> ALTER USER DBSNMP IDENTIFIED BY password;
```

b) PaaS DRのデータベースではData Guardを使用します。スタンバイ・データベースがオープンしている場合（Active Data Guard）は、通常のロールを持つDBSNMPユーザーでログインできます。スタンバイ・データベースがマウントされている場合（Active Data Guardではない）、ユーザーDBSNMPには、データベースにログインするためにSYSDBA権限が必要です。
   - 下のSQLを実行して、DBSNMPユーザーにSYSDBA権限が付与されているか確認します。

```
SQL> select username, sysdba from v$pwfile_users where username='DBSNMP';
```

   - 上のSQLを実行して行が返されなければ、DBSNMPユーザーにSYSDBA権限は付与されていません。プライマリDBシステムにログインし、プライマリ・データベースにsysdbaとして接続して、dbnsmpユーザーにsysdbaを付与します。

```
sqlplus / as sysdba
SQL> grant sysdba to dbsnmp container=all
```

- 12.2より前のバージョンのデータベースの場合は、プライマリ・ホストからスタンバイ・ホストにパスワード・ファイルをコピーします。パスワード・ファイルのデフォルトの場所は$ORACLE_HOME/dbs/orapw$ORACLE_SIDです。

c) データベースが自動検出されなかった場合は検出します。
- **OMSコンソール**（https://<oms_public_ip>:7803/em）にログインします。
- 「**Setup**」→「**Add Target Manually**」の順に移動します。
- “**Add Non-Host Target Using Guided Process**”で「**Add Using Guided Process**」をクリックします。
- 「**Oracle Database, Listener and Automatic Storage Manage**」を選択して「Add..」をクリックします。
- “**Database Discover:Search Criteria**”画面で、データベースを実行しているホストのパブリック名を選択します。
- 見つからない場合は、/etc/oratabにデータベースのエントリがあるかどうか確認し、検索し直します。

d) （自動か手動のいずれかで）データベースを検出したら、**Results**画面でそのデータベースを選択し、「**Configure**」をクリックします。以下の情報を更新します。

Listener Machine Name	OMSがこのホスト・ターゲットへの接続に使用しているdbホスト名に設定されていることを確認します。ネットワーク・トポロジに応じて、適切なマシンのホスト名（パブリックまたはプライベート）を使用してください。
Monitor Username	データベースをOMSから監視するときに使用するデータベース・ユーザーの名前を入力します。通常はdbsnmpです。
Role	「SYSDBA」を選択します。
「SYSDBA」を選択します。	dbsnmpのパスワードを入力します。

e) 「**Test Connection**」をクリックし、正常に接続されていることを確認します。
f) 「**Save**」をクリックします。
g) “**Database Discovery:Results**”ページに戻り、リスナーも選択されていることを確認します。リスナーはデフォルト値のままにします。リスナーはローカル・エージェントで監視され、マシンのプライベート名が使用されます。
h) 「**Next**」をクリックします。
i) “**Database Discovery:Review**”で、「Save」をクリックします。
j) 終了したら、「Targets」→「Databases」の順に移動し、データベースが検出されていることを確認します。

注：重複するターゲットが検出された場合（LISTENERとLISTENER0、またはASM_1、など）は、初出のターゲットを選択し、重複しているターゲットは無視します。

4. WebLogicドメイン・ターゲットの検出

WebLogicドメインおよびこれに関連付けられているターゲットは手動で検出する必要があります。

注：ドメインを検出する場合には、ターゲット・ドメインの管理サーバーとエージェントが稼働している必要があります。

a) OMSコンソールにログインします。
b) 「Setup」→「**Add Target Manually**」の順に移動します。
c) “Add Non-Host Target Using Guided Process”で「Add Using Guided Process」をクリックします。
d) 「**Oracle Fusion Middleware/WebLogic Domain**」を選択して「Add..」をクリックします。
e) 以下の詳細を設定します。

Administrator Server Host	WebLogic管理サーバー・ホストのホスト名に設定します。ここでは**プライベート名**を設定することを推奨します。なぜなら、この名前へは、OMSホストから実行されるエージェントではなく、**WLS管理ホストで実行されるローカルEMエージェントがアクセスする**からです。WLS管理ホストのパブリック名またはIPを設定する場合は、ホストで実行されるエージェントから到達可能であることを確認してください。
Port	WLS管理サーバーのt3sポートです。OCIでは通常、9072です。
Username/Password	weblogic/<weblogic_password>

Node Manager Username/Password	weblogic/<weblogic_password>
Unique Domain Identifier	これは、同じEnterprise Manager内で検出された**同じ名前のWebLogicドメインを区別するため**に使用する識別子です。**WebLogicディザスタ・リカバリ環境では**WebLogicドメイン名がプライマリとスタンバイで同じであるため、**この識別子は非常に重要です**。そのため、これを使用して各ドメインのサイトを識別します。 たとえば次のとおりです。 Site1でWebLogicドメインが検出された場合にはSite1を使用します。 Site2でWebLogicドメインが検出された場合にはSite2を使用します。
Agent	**WLS管理サーバーが稼働しているホストのエージェント**を選択します。
Discover Application versions	Site Guardには関係ありません。チェックを入れても入れなくても構いません。

f) 「Advanced」をクリックして以下を設定します。

JMX Protocol	t3sを使用します。
Discover Down Servers	チェックを入れます。
Enable Automatic Refresh	チェックを入れます。

g) 残りのプロパティはデフォルト（空欄）のままにし、「Continue」をクリックします。

h) “Assign Agents”画面で、各ターゲットに割り当てられているエージェントとホストが正しいことを注意して確認します（2番目のマネージド・サーバーは特に注意）。デフォルトでは、ターゲットと同じホスト上に存在するローカル・エージェントに各ターゲットを割り当てる必要があります。適切なエージェントまたはホストに割り当てられていない場合は、“Change Hostname”または“Assign Agent”を使ってミスマッチを正します。

i) 終了したら、「Targets」→「Middleware」の順に移動して、WebLogicドメインが検出されていることを確認します。

j) ここまでの手順を繰り返して、スタンバイWebLogicドメインを検出します。少なくとも管理サーバーが稼働している必要がありますが、すべてがEMにより正しく検出されるようにするため、スタンバイ・ドメインの検出は管理サーバーと管理対象サーバーの稼働中に実行することを推奨します。これを実行するため、スタンバイ・データベースをスナップショット・スタンバイに変換し、スタンバイ・ドメイン・サーバーを起動して検出を実行することができます。検出後、スタンバイ・ドメインを停止し、フィジカル・スタンバイのスタンバイ・データベースを再び変換します。

Oracle Site Guardの構成

このセクションで説明する手順は、Enterprise Manager Cloud Controlバージョン13.3の『 Site Guard Administrator's Guide』に基づいています。詳しくは、このドキュメントを参照してください。

1. 名前付き資格証明の作成

Oracle Site Guardと関連付けられたターゲット（中間層とdbのホストの場合は、Oracle Node Manager、Oracle WebLogic Server、Oracle Database）の名前付き資格証明を作成する必要があります。次の表に、Oracle Site Guardを使用してWebLogic Cloud DRを管理する場合に必要な最小限の名前付き資格証明をまとめます。

資格証明の名称	認証ターゲットの種類	資格証明の種類	ターゲットの種類	ターゲット	ターゲット・ユーザー名
WLSDR_SITE1_DB_HOST_ORACLE	ホスト	SSH鍵資格証明	ホスト	Site1のDBホスト	opc（sudoを実行してoracle）
WLSDR_SITE2_DB_HOST_ORACLE	ホスト	SSH鍵資格証明	ホスト	Site2のDBホスト	opc（sudoを実行してoracle）
WLSDR_SITE1_WLS_HOSTS_ORACLE	ホスト	SSH鍵資格証明	適用外（グローバル）	適用外（グローバル）	opc（sudoを実行してoracle）
WLSDR_SITE2_WLS_HOSTS_ORACLE	ホスト	SSH鍵資格証明	適用外（グローバル）	適用外（グローバル）	opc（sudoを実行してoracle）
WLSDR_DOMAIN_NODEM	Oracle WebLogicドメイン	ノード・マネージャの資格証明	適用外（グローバル）	適用外（グローバル）	weblogic
WLSDR_DOMAIN_WEBLOGIC	Oracle WebLogicドメイン	WebLogic管理者の資格証明	適用外（グローバル）	適用外（グローバル）	weblogic
WLSDR_ADMIN_WEBLOGIC	Oracle WebLogic Server	Oracle WebLogicの資格証明	適用外（グローバル）	適用外（グローバル）	weblogic
WLSDR_SITE1_DB_SYS	データベース・インスタンス	データベースの資格証明	データベース・インスタンス	プライマリ・データベース	sysdbaとしてのsys
WLSDR_SITE2_DB_SYS	データベース・インスタンス	データベースの資格証明	データベース・インスタンス	スタンバイ・データベース	sysdbaとしてのsys
（任意）*ANY_AUX*_HOST_*USER* 例：OMS_HOST_ROOT OMS_HOST_ORACLE	ホスト	SSH鍵資格証明	ホスト		補助ホストでスクリプトを実行する必要のあるすべてのユーザー。 例：OMSホストのopc（sudoを実行してroot）

注：ノード・マネージャの資格証明、WebLogicの管理者の資格証明、Oracle WebLogicの資格証明は、プライマリとスタンバイのWebLogicドメインで同じです（WebLogic Cloud DR環境では同じにする必要があります）。そのため、ターゲットの資格証明ではなくグローバルな資格証明を使用すると構成が簡素化されます。

クラウドでは、SSH鍵を使用してSSH認証が行われます。**パスフレーズ付きSSH鍵は、現在のところEnterprise Managerではサポートされていません。**使用中のクラウド・インスタンスで使用するSSH鍵にパスフレーズが使用されている場合は、パスフレーズを使用しないSSH鍵をインスタンスに追加する必要があります。新しいSSH鍵を追加するには、クラウドのドキュメント（「Oracle Cloud Infrastructure Documentation」→「Managing Key Pairs on Linux Instances」）を参照してください。クラウド・インスタンスには複数のSSH鍵を構成できます。

a) 権限委任の構成

OCIのホストに直接ログインできるのはopcユーザーのみです。opcユーザーはsudo権限を持っているため、sudoを実行して任意のユーザー（oracle、root）になることができます。Enterprise Managerは、ホストでoracleユーザーとしてタスクを実行する必要があります。それには、ターゲットで権限委任機能を構成する必要があります。

- Enterprise Manager OMSコンソールにログインします。
- 「Setup」→「Security」→「Privilege Delegation Setting」の順に移動します。
- 構成するホストを選択して「Edit」をクリックします。
- 「**Sudo**」を選択し、sudoコマンド“/usr/bin/sudo -i -u %RUNAS% %COMMAND%”を入力します（oracleの.bashrcからenv変数をロードするには、"-i"オプションが必要）。
- 「Save」をクリックします。

プライマリ・サイトとスタンバイ・サイトのすべてのホスト、およびOMSホストでここまでの手順を繰り返します（OMSホストは一部の後処理スクリプトを実行するための補助ホストとして後ほど構成されます）。

b) 名前付き資格証明の作成

表XXXで説明されている資格証明を作成するには、以下の手順を実行します。

- OMSコンソールで、「Setup」→「Security」→「Named Credentials」の順に選択します。
- 「Create」をクリックし、表での説明に従って名前付き資格証明を作成します。
- テストして保存します。
- 同じ手順を繰り返し、このホストまたは他の補助ホストに追加する必要があるほかの資格証明をすべて作成します。

2. 優先資格証明の構成

名前付き資格証明を作成したら、優先資格証明としてターゲットに割り当てることができます。Site Guardの構成を簡略化するために、この方法を推奨します。次の手順を実行して、ターゲットの優先資格証明を構成します。

a) EMにログインし、「Setup」→「Security」→「Preferred Credentials」の順に選択します。
b) ターゲットの種類（Database Instance、hosts、WebLogic Domainなど）を選択し、「Manage Preferred Credentials」をクリックします。
c) ターゲット資格証明ごとに優先資格証明を設定するため、各行をクリックし、「Set」をクリックして、前の手順で作成した適切な名前付き資格証明を選択します。
d) 次のターゲットについてこの手順を実行します。
   - **プライマリとスタンバイのデータベース・インスタンス**（少なくとも、sysdbaの資格証明、各データベース・ホストの資格証明が必要）
   - **プライマリとスタンバイのWebLogicドメイン**（ターゲットの種類“Oracle WebLoigc Domain”。資格証明：weblogic管理者の資格証明、ホストの資格証明）
   - **プライマリとスタンバイの管理サーバー**（ターゲットの種類“Oracle WebLogic Server”。資格証明：Oracle WebLogic管理の資格証明、ホストの資格証明）
   - **プライマリ・ホストとスタンバイ・ホスト**。ターゲットの種類はホストです。一般に、DRの管理に必要なのは“通常のホスト資格証明”のみです。
   - **その他の補助ホストすべて**。OMSホストは一部の後処理スクリプトを実行するための補助ホストとして後で構成されます。このホストの通常の優先資格証明と特権優先資格証明を設定します。

3. EMでのプライマリおよびスタンバイのサイト・システムの定義

Oracle Site Guardで管理されるディザスタ・リカバリ・サイトは、Oracle Enterprise Managerでは汎用システム・ターゲット・タイプとしてモデル化されています。次の手順を実行して、Site1用の汎用システムを作成します。

a) EM OMSコンソールにログインします。
b) 「Targets」→「Systems」の順に選択します。
c) 「Add」→「Generic System」の順にクリックします。
d) Generic System:General画面が表示されます。
e) システムの名前を入力します。例：SITE1_wlsdr
f) 任意でシステムのプロパティ（Department、Line of Business、Locationなど）を追加できます。
g) システムにメンバーを追加します。プライマリ・サイトには以下を追加します。
   プライマリWebLogicドメイン・ターゲット
   プライマリ・データベース・インスタンス・ターゲット

他のコンポーネント（ホスト、ノード・マネージャなど）を明示的に追加する「必要はありません」。

注：データベース・システム・ターゲットそのものは追加しないでください。構成要素であるData Guardシステムが追加され、そこにプライマリ・データベースとスタンバイ・データベースが組み込まれます。

h) 「Next」をクリックします。
i) **Generic System:Define Associations**。デフォルトのままで「Next」をクリックして構いません。
j) **Generic System:Availability Criteria**。データベースをおもなメンバーとして追加し、「Next」をクリックします。
k) **Generic System:Charts Screen**。デフォルトのままで「Finish」をクリックして構いません。同じ手順を繰り返してスタンバイ・サイト・システムを作成します（例：SITE2_wlsdr）。

4. サイト・ロールの定義

Oracle Site Guardで管理されるディザスタ・リカバリ・サイトをOracle Enterprise Managerの汎用システム・ターゲットとしてモデル化したら、そのサイトをプライマリ・サイトまたはスタンバイ・サイトとして指定します。これには、次の手順を実行します。

a) EMにログインし、「Targets」→「Systems」の順に選択します。
b) **プライマリ**・サイト・システムの名前をクリックします。
c) システムのホームページで、「Generic System」メニューから、「**Site Guard**」→「**Configure**」の順に選択します。
d) **General**タブで「**Create**」をクリックします。
e) **General**タブの**Standby System(s)**セクションで、「**Add**」をクリックします。
f) **スタンバイ**・システムを選択し、「**Select**」をクリックします。
g) 「**Save**」をクリックし、「**OK**」をクリックして操作を確定します。Site Guardにスタンバイ・システムの構成が保存されます。
h) ロールが割り当てられていることを確認します。
プライマリ・サイト・システムのOracle Site Guard ConfigurationのGeneralタブに次のように表示されるはずです。
Current Role Primary
セカンダリ・サイト・システムのOracle Site Guard ConfigurationのGeneralタブに次のように表示されるはずです。
Current Role Standby

5. 補助ホストの構成

Oracle Enterprise Managerによって管理される1つ以上のホストを、サイトの補助ホストとして構成できます。補助ホストはシステムには含まれませんが、前処理スクリプト、後処理スクリプト、ストレージ・スクリプトをサイトで実行するときに使用できます。補助ホストをシステムに追加する場合は、次のコマンドを実行します。

```
emcli add_siteguard_aux_hosts  -system_name="system_name"  -host_name="host_name"
```

PaaS DRのSite Guard構成には次の補助ホストが必要です。

a) 他のサイトでWLSドメイン構成のレプリケーション用スクリプトを実行するための補助ホスト

この補助ホストが必要になるのは、MAA OTNページの対応するDRホワイト・ペーパーで説明されているように、スクリプト（最新バージョンの*dbfscopy.shまたはconfig_replica.sh*）を使用してプライマリとスタンバイの間で構成変更を伝播するときです。

このスクリプトは、最初にプライマリの中間層host1で実行し、プライマリWebLogicドメイン構成からの変更をステージング・ファイルシステム（dbfsまたはFSS）と同期します。次にスタンバイの中間層host2で実行し、ステージング・ファイルシステム（dbfsまたはFSS）からの変更をスタンバイWebLogicドメインの構成と同期します。これは、しばらく間隔を置いてスケジュールするようお奨めします。ただし、可能であればスイッチオーバー操作よりも前にスクリプトを実行し、新しいスタンバイの構成を最新の状態にすることもお奨めできます。このスクリプトの実行はSite Guard計画に含めることができます。

Site Guardでこれをモデル化するには、Site2の中間層host1をSite1の補助ホストとして定義し、Site1の中間層host1をSite2の補助ホストとして定義する必要があります。次の手順を実行します。

- Enterprise Managerホストにログインし、emcliにログインします。

```
[oracle@emcc bin]$ cd /u01/app/em13c/middleware
[oracle@emcc bin]$ ./emcli login -username=sysman
```

- emcliを使用して、**Site2の中間層host1**を**Site1の補助ホスト**として追加します。EMに登録されたときのホスト名を使用します。以下に例を挙げます。

```
[oracle@emcc bin]$ ./emcli add_siteguard_aux_hosts -system_name="SITE1_wlsdr" -host_name="wlsmkpl1-wls-0-public.site2.example.com"
Auxiliary host(s) added to system SITE1_wlsdr
```

- emcliを使用して、**Site1の中間層host1**を**Site2の補助ホスト**として追加します。EMに登録されたときのホスト名を使用します。例：

```
[oracle@emcc bin]$ ./emcli add_siteguard_aux_hosts -system_name="SITE2_wlsdr" -host_name="wlsmkpl1-wls-0-public.site1.example.com"
Auxiliary host(s) added to system SITE2_wlsdr
```

b) DNSまたは/etc/hostsの変更を実行するための補助ホスト

アプリケーション・コンシューマ（WebLogicドメインのフロントエンドとして定義済み）が使用するパブリック名の参照先は、常に、プライマリ・ロールを持つサイト内のフロントエンド・ロードバランサ（LBR、OTDなど）が使用するパブリックIPになっている必要があります。そのため、毎回スイッチオーバーの最後には、DNSプッシュを実行するかファイル・ホスト解決を変更して、そのアドレスの参照先が新しいプライマリ・サイトのLBRが使用するパブリックIPになるようにする必要があります。

注：中間層ホストの場合、名前解決は変更されず、参照先は常にホスト自体のLBRになります。変更は、アプリケーション・クライアントに対して有効である必要があります。

/etc/hostsファイルを変更したりDNSサーバーに変更をプッシュするカスタム・スクリプトを、Site Guardを使用して実行することができます。スクリプトを実行するホスト（1つまたは複数）をEnterprise Managerで検出し、補助ホストとしてシステムに追加する必要があります。

このドキュメントの例では、EMホスト（つまり、emcc.marketplace.com）が、そのホストの/etc/hostファイルでフロントエンド名のIP変更を行うスクリプトを実行するため、補助ホストとしてサイトに追加されます。

```
[oracle@emcc bin]$ ./emcli add_siteguard_aux_hosts -system_name="SITE1_wlsdr" -host_name="emcc.marketplace.com"
Auxiliary host(s) added to system SITE1_wlsdr

[oracle@emcc bin]$ ./emcli add_siteguard_aux_hosts -system_name="SITE2_wlsdr" -host_name="emcc.marketplace.com" Auxiliary host(s) added to system SITE2_wlsdr
```

6. 資格証明のアソシエーション

資格証明をターゲットと関連付けておくと、操作計画を実行したときにOracle Site Guardによって使用されます。プライマリ・システムとスタンバイ・システムについてこのアソシエーションを構成する必要があります。

a) Enterprise Managerにログインします。
b) 「Targets」メニューから「**Systems**」をクリックします。
c) Systemsページで、資格証明のアソシエーションを構成するシステムの名前をクリックします。
d) システムのホームページで、「Generic System」メニューから、「**Site Guard**」→「**Configure**」の順に**選択します**。
e) 「**Credentials**」タブをクリックします。今度は、さまざまなタイプの資格証明を関連付けます。
f) **Normal Host Credentials**セクションで「Add」をクリックし、「**All**」を選択して「**Preferred**」→「**Normal Host Credentials**」の順にチェックを入れます。「Save」をクリックします。
g) Site Guardのスクリプトはoracleユーザーで実行されるため、WLSホストとDBホストの場合、**特権ホスト資格証明**は不要です。ただし、rootユーザーでスクリプトを実行する補助ホストでは特権資格証明が必要になる場合があります（/etc/hostsファイルの更新など）。このような場合は、補助ホストに特権ホスト資格証明を追加します（ここでは例としてEMホストを補助ホストとして使用しています）。
h) **Oracle Node Manager Credentials**セクションで「Add」をクリックし、「**All**」と「**NAMED**」を選択します。先ほど作成したNodeManagerの資格証明を選択します。例：WLSDR_DOMAIN_NODEM。「Save」をクリックします。
i) WebLogic Administration Credentialsセクションで「Add」をクリックし、「All」と「Preferred」を選択します。「Save」をクリックします。
j) **SYSDBA Database Credentials**セクションで「Add」をクリックし、「**All**」と「**Preferred, “SYSDBA Database Credentials”**」を選択します。「Save」をクリックします。

スタンバイ・ホストで同じ手順を繰り返します。

7. 必要なスクリプトの構成

Oracle Site Guardには、ディザスタ・リカバリ操作の管理用スクリプトを構成するためのメカニズムがあります。Site Guardにはさまざまなスクリプトを定義できます。

SiteGuardスクリプト	詳細
事前チェック、マウント、アンマウント、またはストレージ	WLSおよびSOA PaaS DRでは不要
前処理スクリプト	WLSドメイン構成の同期を実行するスクリプトは前処理スクリプトとして実行できます。 例： /u01/install/config_replica.sh in mid-tier host 1 of Site1, run as oracle. /u01/install/config_replica.sh in mid-tier host 1 of Site2, run as oracle. (also named “dbfscopy.sh in previous versions)
後処理スクリプト	この例では、以下のスクリプトが後処理スクリプトとして実行されます。 • スイッチオーバー/フェイルオーバーの後に、ホストの**/etc/hostsでフロントエンドの仮想ホスト名IPを更新する後処理スクリプト**。スクリプトの実行されているホストでフロントエンドIPを変更します。次の例では、EMホストでこのスクリプトが実行されます。例： /root/scripts/change_frontend_ip_from_SITE1_to_SITE2.sh[7] /root/scripts/change_frontend_ip_from_SITE2_to_SITE1.sh • スイッチオーバー/フェイルオーバーの後に、**DNSでフロントエンドの仮想ホスト名IPを更新する後処理スクリプト**。外部フロントエンドの解決にDNSを使用するシナリオでは（Oracle Cloud DNS、商用DNSなど）、適切なAPIを使用して変更をプッシュすることができます。Oracle Cloud DNSでこの変更をプッシュする例についてはこちらを参照してください。 • スイッチオーバーまたはフェイルオーバーの完了後に、正常にスイッチオーバーしたことを検証するため、**サンプル・アプリのurlをチェックする後処理スクリプト**。サンプル・スクリプトについては、次のファイルを参照してください。 check-sample-url.zip（WLSの場合（サンプル・アプリurl）） check-soainfra.zip（SOAの場合（soa-infra url））

PaaS DRのための前処理スクリプトを構成するには、次の手順を実行します。

a) EMにログインし、「Targets」→「Systems」の順に選択します。
b) スクリプトを構成するシステムをクリックします。
c) 「Site Guard」→「Configure」→「Pre/Post scripts」タブの順にクリックします。
d) **Site1**システムに**前処理スクリプト**を追加します。
   - WLS構成のレプリカを作成するスクリプトへのスクリプト・パスを挿入します。例：/u01/install/config_replica.sh（または/u01/install/dbfscopy.sh）
   - スクリプト・タイプの選択：Global-PreScript
   - 操作の選択：　Switchover
   - Site1の中間層host1とSite2の中間層host1（このサイトの補助ホスト）をターゲットとして選択します。
   - 各ホストの通常の優先資格証明を選択します。

注：dbfscopy.shを実行すると、デフォルトではsysdbaのパスワードの入力を求められますが、スクリプトをカスタマイズしてパスワードを引数として渡すようにすると、Oracle Site Guardから実行できるようになります。パスワードの入力を求める行をコメントアウトし、スクリプト内で直接にその値と一緒にパスワード変数を定義します（値には二重引用符を使用）。

e) **Site2**システムに**前処理スクリプト**を追加します。
   - WLS構成のレプリカを作成するスクリプトへのパスを挿入します。例：/u01/install/config_replica.sh（または/u01/install/dbfscopy.sh）

7 サンプル・スクリプトchange_frontend_ip_from_SITE1_to_SITE2.sh：
```
# /etc/hostsファイルのエントリmywebapp.mycompany.comip（/etc/hostファイルにエントリが存在することが必要）を
# SITE1 LBR IP:111.111.111.10から
# SITE2 LBR IP:222.222.222.20へ変更するスクリプト。
sed -i 's/111.111.111.10/222.222.222.20/g'  /etc/hosts
```

- スクリプト・タイプの選択： Global-PreScript
- 操作の選択： Switchover
- ロールの選択： Primary
- Site2の中間層host1とSite1の中間層host1（このサイトの補助ホスト）をターゲットとして選択します。
- 各ホストの通常の優先資格証明を選択します。

PaaS DRのための後処理スクリプトを構成するには、次の手順を実行します。

a) **Site2からSite1へのスイッチオーバー後**に実行する**後処理スクリプト**を**Site1**システムに追加します。
   - dnsの**名前をSite1のLBRのパブリックIP**に変更するスクリプトへのパスを挿入します。
     例：/root/scripts/change_frontend_ip_from_SITE2_to_SITE1.sh
   - **スクリプトの種類**を選択： Global-PostScript（Site1に切り替えるときの操作計画の最後に実行されます）
   - **操作**を選択： Switchover
   - ホスト・ファイルを更新する補助ホスト（**この場合はOMSホスト**）を選択します。
   - あらかじめ、このホストの**特権付き**優先資格証明を選択します（ホスト・ファイルを変更できるのはrootのみです）。
b) 次の手順を実行して、Site2からSite1へのフェイルオーバー操作用に同じ後処理スクリプトを作成します。
   - 前の手順で作成した後処理スクリプトを選択し、「Add Like」をクリックします。
   - 操作を“Failover”に変更します。
   - 「Save」をクリックします。
c) Site1からSite2へのスイッチオーバー後に実行する**後処理スクリプト**を**Site2**システムに追加します。
   - 名前をSite2のLBRのパブリックIPに変更するスクリプトへのパスを挿入します。
     例：/root/scripts/change_frontend_ip_from_SITE1_to_SITE2.sh
   - **スクリプトの種類**を選択： Global-PostScript（Site2に切り替えるときの操作計画の最後に実行されます）
   - **操作**を選択： Switchover
   - ホスト・ファイルを更新する補助ホスト（**この場合はOMSホスト**）を選択します。
   - このホストの**特権付き**優先資格証明を選択します（ホスト・ファイルを変更できるのはrootのみです）。
d) 次の手順を実行して、Site1からSite2へのフェイルオーバー用に同じ後処理スクリプトを作成します。
   - 前の手順で作成した後処理スクリプトを選択し、「Add Like」をクリックします。
   - 操作を“Failover”に変更します。
   - 「Save」をクリックします。
e) 手順を繰り返して、その他の後処理スクリプト（サンプル・アプリurl検証スクリプトなど）を追加します。

8. 適用ラグおよび転送ラグのしきい値の構成

Site Guardは事前チェックとスイッチオーバー時にData Guardの適用ラグと転送ラグを検証します。デフォルトでは、0（ゼロ）以外の値の場合には事前チェックに不合格となり、スイッチオーバーが実行されません。数秒のラグを許容するしきい値を定義すれば、チェックをゆるくすることができます。しきい値を10秒に設定する例を示します。

a) OMSホストにSSHで接続します。
b) 次のコマンドでemcliにログインします。

```
[oracle@emcc bin]$ cd $EM_HOME/middleware/bin
[oracle@emcc bin]$ ./emcli login -username=sysman
```

c) 両方のサイトのしきい値を10秒に設定します。

```
[oracle@emcc]$ ./emcli configure_siteguard_lag -system_name=SITE1_wlsdr -property_name=apply_lag -value=10
[oracle@emcc]$ ./emcli configure_siteguard_lag -system_name=SITE2_wlsdr -property_name=apply_lag -value=10

[oracle@emcc]$ ./emcli configure_siteguard_lag -system_name=SITE1_wlsdr -property_name=transport_lag -value=10
[oracle@emcc]$ ./emcli configure_siteguard_lag -system_name=SITE2_wlsdr -property_name=transport_lag -value=10
```

9. スイッチオーバーとフェイルオーバーの操作計画の作成

操作計画とは、ディザスタ・リカバリ操作のときにOracle Site Guardで実行する手順のフローを記述したもので、順次またはパラレルで実行できるアクションが（順番に）並んでいます。サイトのトポロジとOracle Site Guardの構成に基づくデフォルト・バージョンの操作計画は自動的に作成されます。個々の構成に応じて、このデフォルトの操作計画を使用することも、カスタマイズすることもできます。

PaaS DRの場合には、次の操作計画をお奨めします。

計画	説明
SWITCHOVER_SITE1_TO_SITE2_WITH_SYNC	Site1からSite2へのスイッチオーバー。WLSドメイン構成のレプリケーション用スクリプト（*config_replica.sh*または*dbfscopy.sh*）に基づいてWLS構成の同期も実行されます。
SWITCHOVER_SITE2_TO_SITE1_WITH_SYNC	Site2からSite1へのスイッチオーバー。WLSドメイン構成のレプリケーション用スクリプト（*config_replica.sh*または*dbfscopy.sh*）に基づいてWLS構成の同期も実行されます。
SWITCHOVER_SITE1_TO_SITE2	Site1からSite2へのスイッチオーバー。WLSドメイン構成の同期は行いません（RTOが短縮されます）。
SWITCHOVER_SITE2_TO_SITE1	Site1からSite2へのスイッチオーバー。WLSドメイン構成の同期は行いません（RTOが短縮されます）。
FAILOVER_SITE1_TO_SITE2	Site1からSite2へのフェイルオーバー。フェイルオーバーはプライマリ・サイトが使用できなくなったときに発生する計画外イベントであるため、WLSドメイン構成の同期は行いません。
FAILOVER_SITE2_TO_SITE1	Site2からSite1へのフェイルオーバー。フェイルオーバーはプライマリ・サイトが使用できなくなったときに発生する計画外イベントであるため、WLSドメイン構成の同期は行いません。

a) SWITCHOVER_SITE1_TO_SITE2_WITH_SYNCの作成

Site1からSite2へのスイッチオーバーを実行するための操作計画。スイッチオーバーの前にWLSドメイン構成の同期が実行されます。

- EMにログインし、「Target」→「Systems」の順に選択します。
- 「Site1 System」をクリックし、「Site Guard」→「Operations」の順に移動します。
- 「**Create**」をクリックします。
- 計画の名前を入力します。例：SWITCHOVER_SITE1_TO_SITE2_WITH_SYNC
- 操作の種類を選択：**スイッチオーバー**
- 他方のサイト（Site2）をスタンバイ・システムとして選択します。
- 「Save」をクリックします。
- デフォルトで作成された計画は**カスタマイズする必要があります**。計画を編集します。以下の点に注意してください。
- 重要：**WLS構成の同期の前処理スクリプトがSerialモードで実行される**ことを確認します（デフォルトではパラレルで実行されます）。
- 重要：前処理スクリプトの**最初の**実行が、**この計画での元のプライマリである**サイトで行われることを確認します。たとえば、Site1からSite2にスイッチオーバーするように計画が定義されている場合、config_replica.sh（または*dbfscopy.sh*）は必ず最初にSite1の中間層host1で実行されます。必要に応じて上下に移動します。
- **ノード・マネージャの停止と起動の手順を無効にします**。これらの手順は不要であるため、スキップすることでRTOを短縮します。

注：コンポーネントに関連する起動/停止手順のうち不要なものは、削除するのではなく無効にすることを推奨します。システムを構成する一部のコンポーネントの起動/停止手順を削除すると、計画を実行したときにトポロジの事前チェックが失敗し、"This operation plan is out of sync with current topology of the system."という警告が表示されることがあります。ただし、起動/停止手順を無効にしても警告は表示されません[8]。

- dnsまたはhostsファイルの更新後にサンプル・アプリurlテストが実行されたことをチェックする後処理スクリプトを確認します。
- 必要な手順がすべて含まれていること、および抜けている手順がないことを確認します。
- 操作計画の変更を保存します。

b) SWITCHOVER_SITE2_TO_SITE1_WITH_SYNCの作成

Site2システムで前項と同じ手順を実行します。

Site1をスタンバイとして選択し、前処理スクリプト*dbfscopy.sh/config_replica.sh*がSite2の中間層host1で最初に実行されることを確認します。

c) SWITCHOVER_SITE1_TO_SITE2の作成

8 バグ29005772 - TOPOLOGY PRECHECKS FAIL IN SG RUN PRECHECKS WHEN SOME COMPONENT START/STOP STEPS ARE DELETED

計画SWITCHOVER_SITE1_TO_SITE2_WITH_SYNCを選択し、「Create like」をクリックします。

この計画を編集し、*dbfscopy.sh/config_replica.sh*スクリプトの実行がスキップされるよう、グローバルの前処理スクリプトの手順を**削除**します。

d) SWITCHOVER_SITE2_TO_SITE1の作成

SWITCHOVER_SITE2_TO_SITE1_WITH_SYNCを選択し、「Create like」をクリックします。

この計画を編集し、*dbfscopy.sh/config_replica.sh*スクリプトの実行がスキップされるよう、グローバルの前処理スクリプトの手順を**削除**します。

e) FAILOVER_SITE1_TO_SITE2の作成

Site1からSite2へのフェイルオーバー実行するための操作計画です。フェイルオーバーはプライマリ・サイトが使用できなくなったときに発生する計画外イベントであるため、WLSドメイン構成の同期は行いません。

- EMにログインし、「Target」→「Systems」の順に選択します。
- 「Site1 System」をクリックし、「Site Guard」→「Operations」の順に移動します。
- 「Create」をクリックします。
- 計画の名前を入力します。例：FAILOVER_SITE1_TO_SITE2
- 操作の種類を選択：Failover
- 他方のサイト（Site2）をスタンバイ・システムとして選択します。
- 「Save」をクリックします。
- 作成した計画を選択し、「Edit」をクリックします。作成した計画はカスタマイズする必要があります。
- *dbfscopy.sh/config_replica.sh*の前処理スクリプトが計画に含まれていないことを確認します。
- ノード・マネージャの起動の手順を無効にします。これらの手順は不要であるため、スキップすることでRTOを短縮します。
- 後処理スクリプトが正しい順序で含まれていることを確認し、必要に応じて順序を変更します（サンプル・アプリ・チェックは最後にする必要がります）。
- 変更を保存します。

f) FAILOVER_SITE2_TO_SITE1の作成

Site2システムで前項と同じ手順を実行します。Site1をスタンバイ・システムとして選択します。

注：これらの操作計画は、管理サーバーがスタンバイですでに起動している場合にも有効です。管理サーバーの起動を試行する前にそのステータスをチェックし、すでに稼働している場合は起動をスキップします。

Site Guardを使用したスイッチオーバーの実行

操作計画を作成したら、Enterprise Manager Site Guardを使用してPaaS DRサイト全体のスイッチオーバーを実行できます。OMSコンソールを使用してスイッチオーバー操作を実行する場合は次の手順を実行します。

a) EMにログインし、「Target」→「Systems」の順に選択します。
b) 現行のプライマリ・サイト・システムをクリックします。
c) 「Site Guard」→「Operations」の順に選択します。
d) 実行する操作計画を選択します。
e) 「Execute Operation」をクリックします。

代わりの方法として、EMCLIを使用して操作計画を実行することもできます。

a) oracleユーザーでSSHからOMSホスト（または、EM CLIがインストールされている他のホスト）に接続します。
b) emcliにログインします。

```
[oracle@emcc bin]$ cd $EM_HOME/middleware/bin
[oracle@emcc bin]$ ./emcli login -username=sysman
```

c) 操作計画を送信します。

```
emcli submit_operation_plan –name="name_of_operation_plan"
```

Site Guardはスイッチオーバー計画に定義されたすべての手順を次の要領で実行します。

- Oracle Site Guardが事前チェック手順を実行します。関係するホストのエージェントのステータスのチェックや、汎用システムから追加または削除されたターゲットの有無のチェックを実行し、Oracle Data Guard Brokerの事前チェックを実行してデータベースでロール・リバーサルの準備ができているかどうかを確認します。
- 前処理スクリプトを実行します。前の項での定義に従いdbfscopy.shが計画に含まれている場合は、プライマリ・サイトのWLS host1でdbfscopy.shを実行した後、スタンバイ・サイトのWLS host1でdbfscopy.shを実行し、WebLogicドメイン構成を同期します。
- プライマリ・サイトのWebLogicドメインが停止します。最初にWebLogic管理対象サーバーが（パラレルに）停止し、その後WebLogic管理サーバーが停止します。
- Oracle Site GuardはData Guardのブローカを使用してプライマリ・データベースからスタンバイ・データベースへのデータベース・スイッチオーバーを実行します。
- データベースのスイッチオーバーが完了したら、スタンバイ・サイトのWebLogicドメインを起動します。最初にWebLogic管理サーバーを起動し、その後WebLogic管理対象サーバーを（パラレルに）起動します。
- 後処理スクリプトが定義されていれば、それらをすべて実行します（フロントエンドの解決の変更や、アプリケーションurlのステータスの確認など）。
- すべて成功すると、Site Guardのメタデータ・スキーマでサイトのロールが更新されます。
- 操作計画の進捗状況はOMSコンソールで「System」→「Site Guard」→「Operations」→「Operation Activities」の順に選択して監視できます。各手順の詳細（タイミング、アクション、結果など）が表示されます。失敗した手順があれば、やり直すことができます。
- 終了したら、「System」→「Site Guard」→「Configure」→「General」画面の順に選択し、サイトのロール変更を検証できます。

Site Guardを使用したフェイルオーバーの実行

Site Guardを使用してフェイルオーバーを実行するには、前の項の説明に沿ってOMSコンソールまたはEMCLIを使用してフェイルオーバーの操作計画を実行します。Site GuardはPaaS DRのフェイルオーバー手順を次のように編成します。

- Oracle Site Guardは事前チェック手順を実行します。関係するホストのエージェントのステータスをチェックし、Oracle Data Guard Brokerの事前チェックを実行します。
- 前処理スクリプトは実行しません。スクリプト*dbfscopy.sh/config_replica.sh*はフェイルオーバー操作用に定義されていません。フェイルオーバーはプライマリ・サイトが使用できなくなったときに発生する計画外イベントであるため、構成の同期は想定されていません。
- フェイルオーバー時は、プライマリ・サイトのWebLogicドメインを停止する手順はスキップされますが、必要に応じて手動で有効にすることができます。
- Oracle Site GuardはData Guardのブローカを使用してプライマリ・データベースからスタンバイ・データベースへのデータベース・フェイルオーバーを実行します。
- データベースのフェイルオーバーが完了したら、スタンバイ・サイトのWebLogicドメインを起動します。まず、WebLogic管理サーバーを起動し、その後WebLogic管理対象サーバーをパラレルに起動します。
- 後処理スクリプトを実行し、フロントエンドの解決の変更や、サンプル・アプリurlのステータスの確認などを行います。
- すべて成功すると、Site Guardのメタデータ・スキーマでサイトのロールが更新されます。

フェイルオーバー操作後、フェイルオーバーを発生させた問題を解決し、データベースを再インスタンス化するなど、関連する作業を実施して元のプライマリ・サイトを正常な状態に戻す必要があります。その後、Site Guardを使用してスイッチバックを実行できます。

結論

Enterprise Manager Cloud Control Site Guardを使用して、WebLogic for OCI、SOA Cloud Service、またはSOA MarketplaceなどのPaaS DRシステムのスイッチオーバーとフェイルオーバーを管理することができます。設定には、このドキュメントで説明するいくつかの初期手順が必要ですが、一度構成すれば、Site Guardにより、2、3回のクリックでフル・スタック・スイッチオーバーを完全に実行することができます。これにより、ディザスタ・リカバリ管理が大幅に簡素化されます。ディザスタ・リカバリ時間が最小限に抑えられ、ヒューマン・エラーが減少し、特殊なスキルが不要になります。加えて、柔軟でカスタマイズ可能なため、使用環境に特有の他の特別な手順を含めるように適応させることもできます。

CONNECT WITH US

+1.800.ORACLE1までご連絡いただくか、oracle.comをご覧ください。
北米以外の地域では、oracle.com/contactで最寄りの営業所をご確認いただけます。

blogs.oracle.com facebook.com/oracle twitter.com/oracle

WebLogic Cloud on Marketplaceディザスタ・リカバリ
2021年3月