Oracleホワイト・ペーパー
2010年6月

Oracle Enterprise Manager Grid Control 11g Release 1へのセキュリティの配置 - ベスト・プラクティス

ORACLE

はじめに

今日のIT環境の動的で複雑な性質、財務への影響の観点から見たセキュリティ侵害の状況悪化の可能性、信頼の消失、そして厳しい規制要件によって、セキュリティはビジネス・マネージャーおよびITマネージャーが考慮すべき重要な分野となっています。スタンドアロン・アプリケーションにおいて、セキュリティ面を考慮することは重要なことですが、分散システム管理アプリケーションの導入によってそれがますます困難になる可能性があります。また、セキュリティに関する標準化されたベスト・プラクティスはデータベースおよびアプリケーション・サーバーで使用できますが、システム管理製品に特化した標準化されたセキュリティ・ベンチマークは存在しません。

このドキュメントでは、Oracle Enterprise Manager Grid Controlを配置する際のセキュリティを管理するベスト・プラクティスについて説明します。このドキュメントで推奨する事項は、顧客による配置の経験と、オラクル内でのOracle Enterprise Managerの使用経験に基づいています。一部の推奨事項は、CIS（Center for Internet Security）ベンチマークに基づいています。

以下は、Oracle Enterprise Managerアーキテクチャの概略図です。

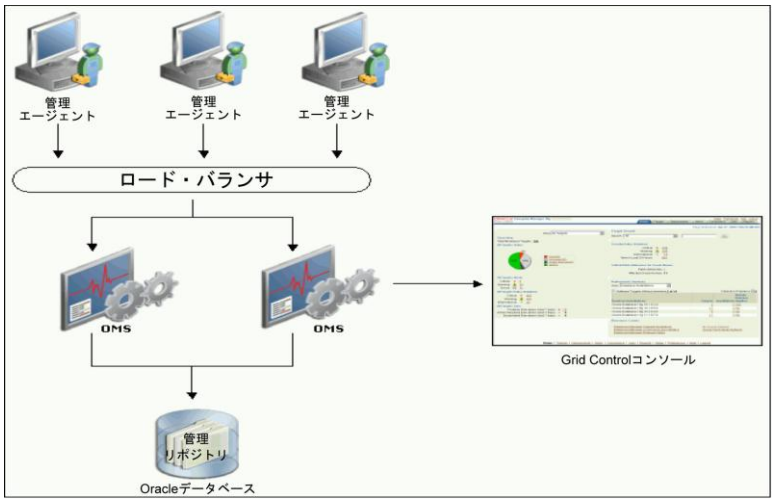

図1 – Oracle Enterprise Manager Grid Controlのアーキテクチャ

このドキュメントに記述するベスト・プラクティスは、Oracle Enterprise Managerのアーキテクチャの主要なコンポーネントに基づいて次の7つのカテゴリに分かれています。

1. Oracle Management Repositoryの保護

2. Oracle Management Serviceの保護

3. Oracle Management Agentsの保護

4. Oracle Enterprise Managerコンポーネント間の通信の保護

5. Grid Controlのユーザー認証

6. Grid Controlの権限/ロール管理

7. 優先資格証明およびターゲット・アクセス

8. 暗号化/復号化

9. 監査

Oracle Management Repositoryの保護

Oracle Enterprise Manager（Oracle EM）の配置を保護するには、Oracle Management ServiceおよびOracle Management Repositoryが存在する基礎となるオペレーティング・システム（OS）からOracle EMコンポーネントにいたるまで、スタックのすべてのレイヤーを保護することが必要です。Oracle Management RepositoryはOracleデータベース内にあるため、Oracleデータベース自体を保護するための多数のベスト・プラクティスをOracle Management Repositoryの保護にも適用できます。Oracleデータベースのセキュリティのベスト・プラクティスについては、以下から入手できる『Oracle Databaseのセキュリティ・チェックリスト』で確認してください。

http://www.oracle.com/technetwork/jp/content/twp-security-checklist-database-133930-ja.pdf

上記のドキュメントには、データベースの保護のために実行する必要があるオペレーティング・システム・レベルの手順も含まれます。また、特にRepositoryの保護を強化するために、以下を推奨します。

1. すべてのSYSオペレーション（SYSはスキーマを所有するアカウントのユーザー名）をデータベース・レベルで監査します。

    a. AUDIT_SYS_OPERATIONSをTRUEに設定します。

    b. Repositoryのデータベース・バージョンが10g Release 2以降の場合に、syslog監査証跡を使用して、データベース管理者などの権限を持つユーザーがオペレーション・システム証跡に保存された監査記録を修正したり削除したりするリスクを最小化します。

        i. 10g Release 2 DBの場合は、syslog監査証跡の詳細について以下のドキュメントを参照してください。

        http://download.oracle.com/docs/cd/B19306_01/network.102/b14266/auditing.htm#CEGJJHJH

        ii 11g DBの場合は、syslog監査証跡を使用できるようにAUDIT_SYS_LEVEL初期化パラメータを適切に設定します。詳細は、以下を参照してください。
        http://download.oracle.com/docs/cd/B28359_01/network.111/b28531/auditing.htm#CEGBIIJD

2. PUBLICプロファイルから、すべてのデータベース・ユーザーがデフォルトで付与される特別な権限を取り消す必要があります。PUBLICから次を取り消します（これらの権限の詳細については、上記のOracle Database Security Checklistを参照してください）。

    a. EXECUTE on UTL_FILE

    b. EXECUTE on UTL_TCP

    c. EXECUTE on UTL_HTTP

    d. EXECUTE on UTL_SMTP

    e. SELECT with GRANT OPTION with ALL_TABLES

    f. SELECT with GRANT OPTION with ALL_TAB_PRIVS

    g. EXECTUE with GRANT OPTION on DBMS_JOB

    h. EXECUTE with GRANT OPTION on DBMS_SCHEDULER

3. Repositoryが存在するホストへのネットワーク・アクセスを制限します。

    a. リポジトリをファイアウォールの内側に置きます。

    b. ネットワークIPアドレスを確認します。次のパラメータを$TNS_ADMIN/protocol.oraファイルに追加することにより、リスナーがOracle Management Serviceノードからのみリクエストを受信するように設定します。

        iii. tcp.validnode_checking =YES

        iv. tcp.excluded_nodes = (list of IP addresses)

        v. tcp.invited_nodes = (list of IP addresses)

    最初のパラメータで機能が有効になります。次のパラメータで、特定のクライアントのIPアドレスとOracleリスナーの接続を拒否および許可します。

詳細は、次の『Secure the Network Connection』のガイドラインを参照してください。

http://download.oracle.com/docs/cd/B28359_01/network.111/b28531/guidelines.htm#CHDJFEFF

4. Oracle Management RepositoryのOracleリスナーのConnection Rate Limiter機能を有効化し、リスナーへのDoS攻撃を軽減します。詳細は、次のリンクを参照してください。

   http://www.oracle.com/technetwork/database/enterprise-edition/oraclenetservices-connectionratelim-133050.pdf

Oracle Management Serviceの保護

Oracle Management Serviceは、Oracle WebLogic Application Server上で動作します。Oracle WebLogic Serverを保護するためのベスト・プラクティスのほとんどは、Oracle Management Serviceの保護にも適用できます。このドキュメントでは、Oracle Management Serviceに特有のセキュリティの側面を説明します。

Oracle WebLogic Serverの保護については、次のドキュメントを参照してください。

http://download.oracle.com/docs/cd/E12839_01/web.1111/e13705/practices.htm#i1134009

ここでは、Oracle Management Serviceの保護のための、その他の推奨事項について説明します。

1. すべてのOracle Management Serviceインストールの Oracleホームすべてを強化します。
   a. sudoまたはPowerBrokerなどのユーティリティを使用することで、これらのOracleホームへの間接的またはなりすましベースのアクセスのみをサポートすることによって、OSアクセスを制限します。
   b. ファイアウォールを使用するホストを保護することにより、これらのOracleホームで動作するソフトウェアを保護するようにしてください。

2. すべてのOracleホームに最新のCPU（Critical Patch Update）レベルまでパッチが適用されるようにします。My Oracle Support資格証明を設定し、新しいセキュリティ・アラートおよびCPUを検出します。Oracle Enterprise Managerは、新規のセキュリティ・アラートおよびCPUを自動的にダウンロードしてPatch Cacheに置きます。ダウンロードされた後にまだ適用されていないセキュリティ・アラートおよびCPUは、Oracle Enterprise Manager Alertsをトリガーします。特にOracle Management Serviceに関連するアラートに注意してください。この推奨事項は、RepositoryおよびAgentsの保護にも適用できます。

3. SYS、SYSMAN、My Oracle Support資格証明のパスワードなど、インストール中に使用したすべてのパスワードを変更します。SYSMANのパスワードを変更するには、Repositoryの保護の項の2.bを参照してください。

4. Linuxプラットフォーム上のrsh、rlogin、telnet、rexecなどの安全性が不十分なサービスを削除することにより、Oracle Management Serviceマシンを強化します（安全性が不十分なサービスのリストと、各種プラットフォーム上でそれらのサービスを削除する方法については、www.cisecurity.orgでCISベンチマークを参照してください）。この推奨事項は、Repositoryをホストするマシンにも適用できます。また、必須でないサービスを止めることを推奨します。これにより、ホストの"攻撃フットプリント"は最小になりますが、要求されないサービスによるリソースの消費が減少し、システム・リソースが開放されてOracle Management Serviceの最善のパフォーマンスが提供されます。

5. Oracle Management Serviceをファイアウォールの内側に置き、ネットワーク・アクセスを制限します。ファイアウォールの設定の詳細については、『Advanced Installation and Configuration Guide』の第19章を参照してください。

Oracle Management Agentsの保護

1. セキュアなSSHプロトコルを使用するGrid ControlのAgent Deploy経由でエージェントをインストールします。

2. 認可されていないエージェントをユーザーがインストールする可能性を防ぐため、永続的な登録パスワードではなく、相応の有効期間があるワンタイム登録パスワードを使用します。

3. 最新のCPUをインストールします。詳細については、前述のOracle Management Serviceの保護の項の推奨事項2を参照してください。

4. Oracle Management Serviceのインストールとは別のユーザーとしてエージェントをインストールし、インストール後はsudoやPowerBrokerなど、このアカウントへのなりすましベースのアクセスのみをサポートします。

Oracle Enterprise Managerコンポーネント間の通信の保護

1. Oracle Management Serviceをすべて"セキュアロック"モードで実行します。"セキュアロック"モードとは、通信がHTTPSポート経由でのみ可能になることを意味します（HTTPポートはロックされます）。

a. これにより、Oracle Management Service-Agentの通信は常に暗号化され、相互に認証されることになります。安全性が不十分なエージェントからのリクエストはすべて、Oracle Management Serviceによって拒否されます。同様に、安全性が不十分なOracle Management Serviceからのリクエストはすべて、エージェントによって拒否されます。これにより、インフラストラクチャ内で発生する悪意ある"中間者"攻撃から管理システムを保護できます。最新のOracle Enterprise Manager Grid Control（Oracle EMGC）11g Release 1のインストールは、デフォルトでセキュアロックされています。Oracle EMGC 11g Release 1へインストールをアップグレードする場合、アップグレード前の環境が保護されていると、アップグレード後もセキュアな状態は維持されますが、Oracle Management Serviceはセキュアロックされません。アップグレード前の環境がすでにセキュアロックされた状態である場合、アップグレード後もOracle Management ServiceとAgent間のセキュアロック・モードが維持されます。

   Oracle Management Serviceがセキュアモードで実行されているかどうかを確認するには、次のコマンドを実行します。

   emctl status oms –details

   エージェントがセキュアモードで実行されているかどうかを確認するには、次のコマンドを実行します。

   emctl status agent –secure

   Oracle Management Serviceとエージェント間の通信をセキュアロックするには、次のコマンドを実行します。

   emctl secure lock [-upload]

   いったんOracle Management Serviceがセキュアロック・モードで実行されると、安全性の不十分なエージェントはOracle Management Serviceにデータをアップロードできないことに注意してください。

b. これにより、ブラウザからのコンソール・アクセスもSSL/TSL経由で保護されます。最新のOracle Enterprise Manager Grid Control 11g Release 1のインストールは、デフォルトでセキュアロックされています。アップグレード前の環境がセキュアロックされていない場合、Oracle EMGC 11g Release 1へのアップグレード後に、次のコマンドを実行してコンソール・アクセスをセキュアロックする必要があります。

   emctl secure lock [-console]

c. Oracle Management Serviceおよびエージェントが通信の際にSSL v3の後継であるTLS v1プロトコルのみをサポートするように設定してください。

i. 次のステップに従って、Oracle Management ServiceにTLS v1プロトコルのみを設定してください。

1. 次のコマンドを入力し、Oracle Management Serviceを停止します。

   emctl stop oms

2. 次のコマンドを入力します。

   emctl secure oms -protocol TLSv1

3. -Dweblogic.security.SSL.protocolVersion=TLS1をDomain_Home/bin/startEMServer.shのJAVA_OPTIONSへ追加します。このプロパティがすでに存在する場合は、値をTLS1に更新します。

4. 次のコマンドでOracle Management Serviceを再起動します。

   emctl start oms

ii. エージェントがサーバーとしてリスンしながらTLS v1プロトコルのみをサポートするように構成するには、$AGENT_HOME/sysman/config/emd.propertiesファイルの次のエントリを更新してください。

1. allowTLSOnly=true

d. Oracle Management Serviceとエージェント間の通信で強力な暗号スイートを有効化してください。

i. 指定されていない場合、デフォルトでは、次の暗号スイートが通信に使用されます。

1. SSL_RSA_WITH_RC4_128_MD5
2. SSL_RSA_WITH_RC4_128_SHA
3. SSL_RSA_WITH_3DES_EDE_CBC_SHA

ii. SSLCipherSuites $AGENT_HOME/sysman/configure/emd.properties のパラメータを編集し、強力な暗号スイートがエージェントのSSL/TLS通信に使用されるように設定できます。サポートされる強力な暗号スイートは次のとおりです。

1. SSL_RSA_WITH_AES_128_CBC_SHA
2. SSL_RSA_WITH_AES_256_CBC_SHA
3. SSL_DH_anon_WITH_3DEC_EDE_CBC_SHA
4. SSL_DH_anon_WITH_RC4_128_MD5
5. SSL_DH_anon_WITH_DES_CBC_SHA

6. SSL_RSA_WITH_RC4_128_MD5
7. SSL_RSA_WITH_RC4_128_SHA
8. SSL_RSA_WITH_3DES_EDE_CBC_SHA

iii. Oracle Management Serviceによって使用される強力な暗号スイートを制限するには、$INSTANCE_HOME/WebTierIH1/config/OHS/ohs1/httpd_em.conf および ssl.confファイルのSSLCipherSuiteパラメータを編集して適切な値にしてください。デフォルトの値は次のとおりです。

1. SSL_RSA_WITH_RC4_128_MD5
2. SSL_RSA_WITH_RC4_128_SHA
3. SSL_RSA_WITH_3DES_EDE_CBC_SHA
4. SSL_RSA_WITH_DES_CBC_SHA
5. TLS_RSA_WITH_AES_128_CBC_SHA
6. TLS_RSA_WITH_AES_256_CBC_SHA

2. 既知の認証局（CA）の証明書を使用してOracle Management Service-Agent間の通信およびコンソール・アクセスを保護し、さまざまな有効時間および鍵サイズを用いた既知の信頼できる証明書を利用します。詳細は、『管理者ガイド』の第2章"Configuring Third Party Certificates"を参照してください。

3. Oracle Management ServiceおよびRepository間のOracle Advanced Security Option（Oracle ASO）を有効化します。Oracle ASOにより、Oracle Management ServiceとRepository間のデータが機密保護および整合性の観点から保護されます。

a. コマンド"emctl set property - name <Property Name> -value <Value>"を発行し、次のプロパティと値を設定します。

i. oracle.sysman.emRep.dbConn.enableEncryption=true
ii. oracle.net.encryption_client=REQUESTED
iii. oracle.net.encryption_types_client={DES40C}
iv. oracle.net.crypto_checksum_client=REQUESTED
v. oracle.net.crypto_checksum_types_client={MD5}

b. 次をTNS_ADMIN/sqlnet.oraなどのRepository Oracleホームへ追加します。

i. SQLNET.ENCRYPTION_SERVER = REQUESTED

上記のパラメータに関する詳細は、次のリンクを参照してください。

http://download.oracle.com/docs/cd/B28359_01/network.111/b28530/asoappa.htm#i634533

Grid Controlのユーザー認証

1. Oracle Enterprise Managerの認証

   a. Oracleシングル・サインオン（SSO）またはエンタープライズ・ユーザー・セキュリティ（EUS）ベースの認証を使用し、エンタープライズ全体の一元化されたID管理を利用します。

   SSOおよびEUSをOracle Enterprise Manager認証でそれぞれ設定する方法については、次のリンクを参照してください。

   http://download.oracle.com/docs/cd/E11857_01/em.111/e16790/security3.htm#BABFIACG

   http://download.oracle.com/docs/cd/E11857_01/em.111/e16790/security3.htm#BABCEGII

2. SYSMANでのコンソールへのログインを無効化します。SYSMANはスキーマの所有者であるため、Oracle Enterprise Managerのスーパー管理者よりも権限があります。SYSMANは、Oracle Enterprise Managerのスーパーユーザーとしてではなく、スキーマ所有者として扱う必要があります。Repository上で次のSQL文を実行することによって、別のスーパー管理者を作成し、SYSMANがコンソールへログインするのを防ぎます。

   UPDATE MGMT_CREATED_USERS
   SET SYSTEM_USER='-1'
   WHERE user_name='SYSMAN'

   SYSMANによるコンソールへのログインを無効にした後は、次を実行することによって有効化できます。

   UPDATE MGMT_CREATED_USERS
   SET SYSTEM_USER='1'
   WHERE user_name='SYSMAN'

3. スーパーユーザーの数を削減します。Oracle Enterprise Managerのスーパー管理者には、ターゲット/レポート/テンプレート/ジョブに対するFULL権限があり、これらのユーザーだけが、他のユーザーおよびスーパー管理者を作成でき、他のユーザーへの権限の付与、または他のユーザーからの権限の取消しを実行できます。そのため、スーパーユーザー

の権限は注意深く付与する必要があります。スーパーユーザーのリストを取得するには、次の問合せを使用します。

SELECT grantee FROM MGMT_PRIV_GRANTS WHERE PRIV_NAME = 'SUPER_USER'

4. パスワード・プロファイルを使用して、Repositoryベースの認証が使用されている際のOracle Enterprise Manager管理者のパスワード制御を強化します。

   a. 標準のパスワード・プロファイルMGMT_ADMIN_USER_PROFILEには、Oracle Enterprise Manager管理者向けに次のパラメータが設定されています。

      i. FAILED_LOGIN_ATTEMPTS=10

      ii. PASSWORD_LIFE_TIME=180

      iii. PASSWORD_REUSE_TIME=UNLIMITED

      iv. PASSWORD_REUSE_MAX=UNLIMITED

      v. PASSWORD_LOCK_TIME=1

      vi. PASSWORD_GRACE_TIME=7

      vii PASSWORD_VERIFY_FUNCTION=MGMT_PASS_VERIFY

   標準のパスワード検証機能MGMT_PASS_VERIFYは、パスワードがユーザー名と同一にならないようにし、最小長は8で、少なくとも1つのアルファベット、数字および句読記号文字が含まれるようにします。

   パスワード・プロファイルは、たとえば、パスワードの複雑さのより厳密な要件に合う新規のパスワード認証機能など、特殊な要件に合うように異なる値を用いてカスタマイズして作成できます。

5. SYSMANおよびMGMT_VIEWのユーザーのパスワードを定期的に変更します。

   a. 次のコマンドにより、SYSMANパスワードを変更します。

      emctl config oms –change_repos_pwd [-change_in_db] [-old_pwd <old_pwd> [-new_pwd <new_pwd> [-use_sys_pwd [-sys_pwd <sys_pwd>]]

      パラメータchange_in_dbは、Repositoryのパスワードが変更されるかどうかを制御します。このパラメータがない場合、コマンドによってOracle Management Serviceの資格証明ストアのSYSMANパスワードのみが更新されます。

      単一のOracle Management Serviceインスタンス環境では、次のコマンドを実行してRepositoryおよびOracle Management Service構成ファイルの両方のSYSMANパスワードを変更します。新旧のSYSMANパスワードを要求されます。

      emctl config oms –change_repos_pwd -change_in_db

      複数のOracle Management Serviceインスタンス環境では、上記のコマンドを少なくとも1つのOracle Management Serviceインスタンスで実行します。次に、Oracle Management Serviceの構成ファイルでSYSMANパスワードを更新するために、以下のコマンドを他のすべてのOracle Management Serviceインスタンスで実行します。

      emctl config oms –change_repos_pwd

      新旧のSYSMANパスワードを要求されます。

   b. 次のコマンドを使用して、MGMT_VIEWのパスワードを変更します。

      emctl config oms –change_view_user_pwd [-sysman_pwd <sysman_pwd>][-user_pwd <user_pwd>][-auto_generate]

      複数のOracle Management Serviceインスタンス環境では、このコマンドを1つのOracle Management Serviceインスタンスで実行するだけで済みます。

      "-auto_generate"が選択されている場合、MGMT_VIEWにランダム・パスワードが生成され、パスワードは誰にも認知されないことに注意してください。

   c. 内部ユーザーのロックアウトによるサービスの中断を回避するために、SYSMANおよびMGMT_VIEWという標準のユーザーがMGMT_INTERNAL_USER_PROFILEと関連付けられており、このパスワード・パラメータはすべてUNLIMITEDに設定されています。さらに、リソース消費制限によるセッション停止や長時間のセッションを回避するため、MGMT_INTERNAL_USER_PROFILEのカーネル・パラメータがデフォルトで設定されており、これもUNLIMITEDです。

Grid Controlの権限/ロール管理

1. ユーザーに権限を付与するのではなくロールを付与することで、Role Based Access Control（RBAC）を可能にします。ロール付与の管理は、権限付与の管理よりも簡単です。有意義なロールを作成し、権限ではなくロールのみを付与します。

2. Privilege Propagation Groupを使用し、グループ管理とともに権限の割当て、取消しおよび管理を簡素化します。

3. 最小権限の原則に従い、必要な場合にのみ詳細レベルの権限/ロールを付与することによって、ユーザーが責任の実行に必要な最小セットの権限のみを付与します。

4. 監査を有効にすることにより、定期的に権限の付与を監視し、どのユーザーにどの権限が実行されるのかも追跡します。

    a. ロールの付与
    b. ターゲット権限の付与
    c. ロールの取消し
    d. ターゲット権限の取消し
    e. システム権限の付与
    f. システム権限の取消し
    g. ジョブ権限の付与
    h. ジョブ権限の取消し

優先資格証明およびターゲット・アクセス

1. sudoやPowerBrokerなどの権限委任ユーティリティを使用してターゲットにアクセスし、ジョブを実行してユーザー定義のメトリックを収集します。

2. SYSMANなどのグループ/共通アカウントに優先資格証明を設定しないでください。優先資格証明が共通アカウントに設定されると、この資格証明の使用のアカウンタビリティが失われます。次のSQL文を使用して、優先資格証明を設定したユーザーのリストのレポートを作成できます。

   SELECT t.target_name,tc.user_name,tc.credential_set_name FROM MGMT_TARGET_CREDENTIALS tc, MGMT_TARGETS t WHERE tc.target_guid=t.target_guid

3. Pluggable Authentication Module（PAM）経由でのホスト・ターゲット・アクセスに対するLDAP、RADIUSまたはKerberos認証によってもたらされる、一元化されたIDストレージおよび管理などの利点を利用します。Note 422073.1では、PAMおよびLDAPのエージェントの構成方法を説明しています。

暗号化/復号化

1. 暗号化キーを保護します。暗号化キーは、Repositoryに保存されたパスワードや優先資格証明などの機密データを暗号化/復号化するマスター・キーです。キー自体はもともとRepositoryに保存されており、インストールが実行されるとRepositoryから自動的に削除されます。Repositoryがアップグレードされた場合、キーはRepositoryにとどまるだけで済みます。キーをOracle Enterprise Managerスキーマから分離して保存することにより、Repository内の優先資格証明などの機密情報がRepositoryのスキーマ所有者や他のSYSDBAユーザー（データベース上のメンテナンス・タスクを実行できる権限のあるユーザー）にアクセス不可能な状態を維持できます。また、キーをOracle Enterprise Managerスキーマから分離しておくことにより、Repositoryバックアップにアクセス中でも機密データへのアクセスは不可能になります。さらに、Oracle Enterprise Managerスキーマ所有者によるOracle Management Service/RepositoryのOracleホームへのアクセスは不可能です。次のプロセスに従って、暗号化キーを保護します。

   a. 次のコマンドを実行して暗号化キーをファイルにバックアップし、暗号化ファイルを別のマシンでセキュアに維持します。暗号化キーが失われたり破損したりした場合、リポジトリ内の暗号化データは使用できません。

      emctl config emkey –copy_to_file_from_credstore –emkey_file emkey.ora

2. あるオペレーションでRepositoryにemkeyが必要とされ、そのオペレーションによってemkeyが自動的にRepositoryへコピーされない場合は（または、あとでRepositoryからemkeyが削除される場合は）、以下の手順に従ってemkeyをRepositoryへコピーし、オペレーション後にemkeyをRepositoryから削除してください。

   a. 以下のコマンドを使用して、Repositoryに暗号化キーをコピーします。

      emctl config emkey –copy_to_repos

      YSMANパスワードを要求されます。

   b. オペレーションが実行されたら、Repositoryからキーを削除します。

      emctl config emkey –remove_from_repos

      SYSMANパスワードを要求されます。

監査

1. 次のEMCLI verbを発行して、すべてのセキュリティ・クリティカルなオペレーションへの監査を有効化します。

   emcli enable_audit

   Grid Controlが10g Release 5の場合、Oracle Management Serviceを再起動する必要があることに注意してください。11g Release 1の場合は、再起動の必要はありません。

2. 監査されたオペレーションのサブセットに対する監査を有効化するには、次のEMCLI verbを使用してください。

   emcli update_audit_settings -audit_switch="ENABLE/DISABLE"
   -operations_to_enable="name of the operations to enable,for all oprtations use ALL"
   -operations_to_disable="name of the operations to disable, for all oprtations use ALL"

   Oracle Enterprise Managerによって監査されるオペレーションのリストについては、『管理者ガイド』の第2章中の"Setting up for Auditing System for Enterprise Manager"を参照してください。

   次のコマンドにより、Oracle Enterprise Managerが監査できるオペレーションのリストが表示されます。

   emcli show_operations_list

   次のコマンドは、Oracle Enterprise ManagerがGrid Controlにおけるユーザーのログインおよびログオフ・オペレーションを監査することのみを有効化します。

   emcli update_audit_settings –audit_switch=”ENABLE”
   –operations_to_enable=”LOGIN;LOGOUT”

3. 監査が有効化されると、監査レコードはRepositoryのMGMT$AUDITLOG表に維持されます。監査データを監視するには、Grid controlのGUIツールを使用してください。Grid Controlの監査データを監視する手順は次のとおりです。

    a. スーパー管理者としてGrid Controlにログインします。

    b. "Setup"に移動します。

    c. 「Management Services and Repository」タブをクリックします。

    d. ページをAuditセクションまでスクロールし、「Audit Data」リンクをクリックして、監査データを監視するページに移動します。

4. EMCLI verb update_audit_settings経由で外部化サービスを設定し、監査データをRepositoryから外部ファイル・システムへ定期的に外部化します。監査ログ・ファイル用のディレクトリに十分な領域があるようにしてください。

    emcli update_audit_settings -file_prefix=<file_prefix> -directory_name=<directory_name> -file_size = <file size> -data_retention_period=<period in days>

    - *file_prefix：監査データを含むファイルの接頭辞*
    - *directory_name：OSディレクトリにマッピングされるデータベース・ディレクトリの名前*
    - *file_size：データが書き込まれるファイルのサイズ*
    - *data_retention_period：リポジトリ内に維持される監査データの期間*

    次の例は、監査データがRepository内に60日間維持され、消去されるとデータはデータベース・ディレクトリEM_DIRに対応するOSディレクトリにemgc_auditの接頭辞を付けたファイル名で保存され、ファイル・サイズはそれぞれ1Mバイトになることを示しています。

    emcli update_audit_setting -directory="EM_DIR"
    -file_prefix="emgc_audit"
    -file_size="1000000"
    -data_retention_period="60"

5. 外部化された監査データが保存されるディレクトリへのアクセスを制限することにより、職務分離を実行します。Oracle Enterprise Managerユーザーは、外部化された監査データへのアクセスはできません。

Oracle Enterprise Manager Auditingの詳細については、『管理者ガイド』の第2章を参照してください。

http://download.oracle.com/docs/cd/E11857_01/em.111/e16790/security3.htm#insertedID8

結論

セキュリティの重要性は、非常に大きいものです。これは、広範囲に及ぶ性質を持つOracle Enterprise Managerにとっても明らかです。Oracle Enterprise Managerは、セキュアなユーザー・モデルへのセキュアなフレームワーク・レベルの通信を始めとする、一連の堅牢なセキュリティ機能を提供します。可能な限り、オラクルは現場で学んだベスト・プラクティスを製品に組み込もうと努力しています。標準で提供されるターゲット・セキュリティ・ポリシーの豊富なセットは、この努力の一例です。ただし、システムに弱い部分があるとシステム全体が脆弱になります。上記のベスト・プラクティスは、Oracle Enterprise Managerの配置のセキュリティ全般を体系的に強化するために設計されています。これらの推奨事項を利用して、Oracle Enterprise Managerの配置をセキュリティの観点から堅牢なものにすることをお薦めします。

ORACLE

Oracle Enterprise Manager Grid Control 11g Release 1への
セキュリティの配置 -
ベスト・プラクティス
2010年6月
著者：Huaqing Wang
共著者：Ravi Pinnamaneni
Andrew Bulloch、Werner De Gruyter

Oracle Corporation
World Headquarters
500 Oracle Parkway
Redwood Shores, CA 94065
U.S.A.
海外からのお問い合わせ窓口：

電話：+1.650.506.7000
ファクシミリ：+1.650.506.7200
www.oracle.com

Oracle is committed to developing practices and products that help protect the environment